**A LÓGICA DOS FEIXES
SOBRE QUANTAIS
RIGHT-SIDED E IDEMPOTENTES**

Marcelo Esteban Coniglio

TESE APRESENTADA

AO

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

DA

UNIVERSIDADE DE SÃO PAULO

PARA

OBTENÇÃO DO GRAU

DE

DOUTOR EM MATEMÁTICA

Área de Concentração: **Matemática**

Orientador: **Prof. Dr. Francisco Miraglia**

O Autor Recebeu o Apoio Financeiro da CAPES e da FAPESP

– São Paulo, agosto de 1997 –

A LÓGICA DOS FEIXES SOBRE QUANTAIS RIGHT-SIDED E IDEMPOTENTES

Este exemplar corresponde à redação final da tese
apresentada por Marcelo Esteban Coniglio,
devidamente corrigida e aprovada pela comissão julgadora.

São Paulo, agosto de 1997.

Banca Examinadora:

Prof. Dr. Francisco Miraglia (Orientador)	IME-USP
Prof. Dr. Ricardo Bianconi	IME-USP
Prof. Dr. Ruy de Queiroz	UFPe
Prof. Dr. Luiz Carlos Pereira	PUC-RJ
Profa. Dra. Ítala d'Ottaviano	UNICAMP

Resumo

Neste trabalho, apresentamos uma lógica de primeira ordem com tipos para as categorias $Psh(Q)$ e $Sh(Q)$ dos prefeixes e feixes sobre quantais (right-sided e idempotentes). São estudadas as propriedades das operações lógicas entre sub-objetos em $Psh(Q)$ com relação ao cálculo da imagem inversa por morfismos (interpretando a substituição de uma variável por um termo numa fórmula), estabelecendo condições suficientes, expressáveis na linguagem de primeira ordem, que garantem a preservação das operações. Em particular, é discutida a noção de extensão de sub-prefeixes -construídos a partir de sub-prefeixes elementares- por novos prefeixes, inerente ao processo de combinar fórmulas com variáveis de tipos diferentes. Portanto, as regras de lógica possuem cláusulas que prescrevem as condições de extensão, o que garante a correteza da lógica. São analisadas propriedades de primeira ordem das relações binárias em $Psh(Q)$, assim como algumas estruturas algébricas, tais como anéis, módulos e corpos. É provado na lógica um teorema de I. Kaplansky, que diz serem livres os módulos projetivos finitamente gerados sobre um anel local.

Abstract

We present a first-order logic many-sorted for presheaves and sheaves over right-sided idempotent quantales. We study the properties of the logical operations between sub-objects in $Psh(Q)$ and the inverse image by a morphism (interpreting the substitution of a variable by a term), establishing sufficient conditions, expressible in the first-order language, which guarantee the preservation of the operations. In particular, we discuss the notion of extension of sub-presheaves -built from elementary ones- by other presheaves, arising in the process of combining formulas with variables of different sorts. Therefore, the rules of the logic have clauses which prescribe the requirements of extension, ensuring the soundness of the calculus. We analyze first-order properties of binary relations in $Psh(Q)$, as well as some algebraic structures, such as rings, modules and fields. We prove (in the logic) a theorem due to I. Kaplansky, showing that finitely generated projective modules over a local ring are free.

Agradecimentos

Ao meu orientador, Francisco Miraglia, pela sua grande dedicação, pelo seu constante apoio e encorajamento, e por todos os conhecimentos transferidos em todos estes anos que me permitiram ampliar a minha visão como matemático, dentro de um ambiente de trabalho excelente.

Às pessoas do IME, pela hospitalidade com que me acolheram.

Aos professores Daniel Levcovitz, Ruy Excel, Paolo Piccione, Odilón Otávio Luciano, Newton C.A. Da Costa, Jean-Yves Béziau, Jacob Zimbarg e Flávio Corrêa, que, através de discussões e comentários, contribuíram, direta ou indiretamente, para a elaboração deste trabalho. Em especial, ao professor Ricardo Bianconi, quem me sugeriu o esquema da demonstração do Lema 4.1.19.

À Lilian, a Francisca, o Feijão e o Pinho, pela sua eficiência e simpatia.

Aos meus colegas e amigos, Jesús, Verónica, Viviana, Cristian, Ernandes e Hugo, pelos agradáveis momentos compartilhados nestes anos de estudo.

Ao Flávio e o César, grandes amigos dentro e fora do IME, pela grande ajuda computacional.

Aos meus queridos amigos Pedro, Sonia e Patricia, colegas desde a nossa infância matemática, por tantos anos de amizade.

Aos meus grandes amigos Falleroni, Bonato, Finkel e El Turco, pelas risadas e pelos bons momentos que passamos juntos.

Aos meus pais, meus irmãos Corina e Horacio, meu cunhado Eduardo e meus sobrinhos Sebastián, Julieta, Mariano e Marcelito, pelo imenso apoio, carinho e compreensão.

Finalmente, à CAPES e à FAPESP pelo apoio financeiro durante a elaboração deste trabalho.

Sumário

Introdução	1
1 A Estrutura das Funções Características	7
1.1 Feixes sobre Quantais Right-sided e Idempotentes	7
1.2 Extensão de Sub-prefeixes Fechados	19
1.3 Imagem Inversa de Morfismos	27
1.4 Funções Características como Fórmulas	32
2 Uma Lógica de Primeira Ordem para Estruturas em $\text{Psh}(\mathbf{Q})$	48
2.1 Sintaxe	48
2.2 Semântica em $\text{Psh}(\mathbf{Q})$	51
2.3 Cláusulas de Extensão e Redução de Sequentes	63
2.4 O Cálculo (QPC)	75
2.5 Teorema de Corretude	82
2.6 Teoremas Básicos em (QPC)	93
2.7 O Cálculo (QPC1) para Extents Constantes	110
3 Estruturas Algébricas em $\text{Psh}(\mathbf{Q})$	113
3.1 Relações Binárias	113
3.2 Estruturas Algébricas em $\text{Psh}(\mathbf{Q})$	121

3.3	Naturais, Inteiros e Racionais em $Sh(Q)$	134
4	Módulos Projetivos sobre Anéis Locais em $Sh(Q)$	149
4.1	Definições e Resultados Preliminares	149
4.2	O Teorema de Kaplansky em $Sh(Q)$	167
	Bibliografia	189
	Apêndice I : Equality in Linear Logic	193

Introdução

O célebre Teorema de Representação de Gelfand-Naimark pode ser considerado, sem dúvida, o "Teorema Fundamental das C^* -álgebras comutativas". Ele estabelece uma dualidade entre as categorias de espaços topológicos Hausdorff localmente compactos e de álgebras C^* comutativas, restringindo-se a uma dualidade entre a categoria dos Hausdorff compactos e C^* -álgebras comutativas com identidade. Desta maneira, toda álgebra C^* é da forma $\mathcal{A} = C_0(K)$, a C^* -álgebra das funções contínuas sobre o espaço topológico K (Hausdorff localmente compacto) a valores complexos nulas no infinito. O espaço K é chamado o espectro de $\mathcal{A}$, e é da forma

$$\text{Spec}\mathcal{A} = \{f : \mathcal{A} \rightarrow \mathbb{C} : f \text{ é estado puro}\} \simeq \{I \subseteq \mathcal{A} : I \text{ é ideal bilateral fechado maximal}\}.$$

Quando passamos ao caso não comutativo, a situação muda radicalmente; não existe uma caracterização tão definida das C^* -álgebras em geral, e a técnica de investigar o espectro dos ideais bilaterais maximais tem evidenciado as suas limitações; existem exemplos elementares de álgebras simples, i.e., sem ideais bilaterais não triviais (por exemplo $\mathcal{A} = \mathbb{C}^{n \times n}$ ou $\mathcal{A} = \mathcal{LC}(\mathcal{H})$, a álgebra dos operadores lineares compactos num espaço de Hilbert $\mathcal{H}$). A idéia é poder representar de alguma maneira na definição da topologia a não comutatividade existente na álgebra. Ou seja, a extensão da dualidade de Gelfand exige a definição de alguma forma de "topologia não comutativa". Em 1969, de maneira independente, Akemann ([Ak1], [Ak2], [Ak3]), por um lado, e Giles e Kummer ([GK]), pelo outro, conseguiram refinar a ideia de espectro de uma C^* -álgebra, obtendo o fator de não comutatividade considerando ideais laterais (no caso, a esquerda) de maneira de ter a informação necessária para descrever a álgebra original num contexto de topologia não comutativa. A técnica consiste em considerar a C^* -álgebra $\mathcal{A}$ naturalmente imersa (e σ -densa) numa álgebra de von Neumann atômica $\mathcal{B}$, junto com reticulados $\text{Lid } \mathcal{A}$ e $\text{Lid } \mathcal{B}$ dos ideais à esquerda de $\mathcal{A}$ fechados em norma e os ideais à esquerda de $\mathcal{B}$ fechados na topologia fraca, e funções de extensão e especialização

$$\alpha : \text{Lid } \mathcal{A} \rightarrow \text{Lid } \mathcal{B} ; \quad \beta : \text{Lid } \mathcal{B} \rightarrow \text{Lid } \mathcal{A}$$

de maneira que $\text{Lid } \mathcal{B}$ e $\text{Lid } \mathcal{A}$ são o análogo não comutativo dos reticulados das partes do espectro de $\mathcal{A}$ e dos abertos do espectro de $\mathcal{A}$, respectivamente; α e β correspondem à "inclusão" e ao "interior", respectivamente. O estudo é feito via projeções de $\mathcal{B}$, pois o reticulado das projeções é isomorfo a $\text{Lid } \mathcal{B}$, obtendo-se um análogo não comutativo do Teorema de Gelfand. A estrutura das projeções "abertas" é o que Mulvey ([Mu2]) chamou de quantal, uma estrutura de ordem que generaliza naturalmente as álgebras de Heyting completas (ou locais), que são a estrutura de ordem das topologias "clássicas". Mulvey reconheceu a possibilidade de estudar as representações

de álgebras C^* não comutativas (e consequentemente os fundamentos da mecânica quântica) em termos de certas lógicas não comutativas, caracterizando a lógica dos ideais laterais, i.e., os quantais. Num trabalho de Borceaux, van den Bossche e Rosicky ([BvdBR]) foi provado que uma C^* -álgebra $\mathcal{A}$ do tipo postliminary é completamente determinada pelo quantal $Rid\ \mathcal{A}$ dos ideais à direita fechados em norma (ou, equivalentemente, por $Lid\ \mathcal{A}$), indicando as boas perspectivas que oferece o estudo das álgebras C^* utilizando a teoria dos quantais. O passo seguinte foi a questão da generalização ao contexto não comutativo da noção de feixe sobre álgebras de Heyting completas (denotadas, daqui em diante, por cHa).

A teoria de feixes é baseada no estudo da transferência de propriedades locais a propriedades globais. Há uma excelente história da teoria na introdução do volume 753 da Springer Lecture Notes in Mathematics.

A partir dos trabalhos de Grothendieck em geometria algébrica, foi formulada em 1970 por Lawvere ([Law]) uma noção mais geral, a de feixes sobre um sítio ou topos, sendo provado que essas categorias possuem a estrutura necessária para interpretar lógica intuicionista de ordem superior, dando origem à chamada “geometrização da lógica”. Porém, a representação categórica sobre um topos arbitrário resulta ser em geral extremamente abstrata. Os trabalhos D. Scott ([Sco]), e Fourman-Scott ([FS]) foram orientados para o caso particular de feixes sobre uma cHa, generalizando, por sua vez, os modelos topológicos e de Kripke da lógica intuicionista. Esta escolha está justificada pelo fato de que a estrutura de reticulado dos abertos de um espaço topológico é uma cHa (sendo um exemplo fundamental de cHa), existindo portanto numerosas aplicações provenientes da álgebra (reticulados de ideais) da análise e da topologia.

Uma cHa é um reticulado completo Ω tal que $a \wedge (\bigvee_i a_i) = \bigvee_i (a \wedge a_i)$ para todo $a, a_i \in \Omega$, o que permite definir (por adjunção) a noção de implicação: $a \rightarrow b = \bigvee \{c : a \wedge c \leq b\}$. As cHa são para a lógica intuicionista o que as álgebras de Boole completas são para a lógica clássica. A relação entre cHa e espaços topológicos pode ser caracterizada do modo seguinte: toda cHa Ω da origem a um espaço topológico X_Ω ; porém, nem toda cHa é da forma $\Omega(X_\Omega)$; de fato, definimos uma cHa Ω como sendo espacial ou com suficientes pontos se satisfaz: $\Omega \simeq \Omega(X_\Omega)$ (considerando como morfismos as aplicações que preservam supremos arbitrários e ínfimos finitos). Por outro lado, um espaço topológico X é sóbrio se e somente se $X \simeq X_{\Omega(X)}$. Temos assim uma dualidade entre a categorias dos espaços topológicos sóbrios e as cHa com suficientes pontos. O trabalho de [FS] fornece uma definição alternativa de feixes e prefeixes sobre uma cHa, a partir de $\mathcal{H}$ -sets (*Heyting-valued sets*), que generalizam os clássicos *Boolean-valued sets*. Esta caracterização alternativa da definição categórica (i.e., funtores contravariantes de Ω em (Set)) resulta ser mais operacional, interpretando a lógica de maneira natural via a noção de igualdade com valores em Ω . Assim, pensando nos feixes ou $\mathcal{H}$ -sets como coleções de elementos “variando continuamente” sobre um domínio (onde a condição de extensionalidade corresponde ao requerimento de definir as operações e relações localmente), a lógica intuicionista de Scott ([Sco]) resulta ser uma lógica das propriedades locais de elementos variáveis.

Na mesma linha de pesquisa, C. Mulvey ([Mul1]) estuda as representações de anéis como as

seções globais de um feixe sobre um espaço topológico X através de uma lógica intuicionista de ordem superior (uma representação de um anel é um homorfismo do anel no anel de seções de um feixe de anéis sobre um espaço topológico). A idéia principal é que o feixe obtido da representação do anel pode ser examinado na teoria de módulos e anéis da categoria $Sh(\Omega(X))$ de feixes do espaço de representação X ; o feixe resultante é um anel, possuindo, frequentemente, melhores propriedades algébricas do que o anel original. Os teoremas intuicionistas (válidos portanto na categoria $Sh(\Omega)$) podem ser aplicados no anel obtido da representação. Fica evidente a necessidade da utilização de uma linguagem para descrever essas construções, junto com uma noção apropriada de interpretação, sendo que os feixes correspondem a conjuntos no caso clássico (se X consiste num ponto só, a categoria de feixes é exatamente a categoria (*Sets*), e as noções de interpretação coincidem). A técnica consiste então em, a partir da representação de um anel, considerar as propriedades algébricas do anel obtido em $Sh(\Omega(X))$. A partir daí, são procurados teoremas conhecidos sobre esse tipo de anéis, que sejam intuicionisticamente prováveis; logo, as conclusões desses teoremas serão válidas no anel em $Sh(\Omega(X))$. Finalmente, é necessário externalizar o teorema a partir da noção de interpretação. Aplicando esta técnica ao anel $C(X)$ (X compacto) obtemos, a partir do feixe de germes de funções contínuas, um anel local em $Sh(\Omega(X))$ (de fato, o corpo dos números reais). Aplicando a este anel local um teorema de Kaplansky ([Kap]), que assegura que todo módulo projetivo finitamente gerado sobre um anel local é livre, obtemos, externalizando o resultado, um teorema de Swan que estabelece a dualidade entre a categoria dos fibrados vetoriais reais de dimensão finita sobre um espaço topológico compacto X e a categoria dos módulos projetivos finitamente gerados sobre o anel $C(X)$. A contundência deste resultado, junto com a generalização do teorema de Gelfand-Naimark de Giles-Kummer-Akemman, evidenciaram a necessidade de generalizar a noção de $\mathcal{H}$ -sets, feixes e prefeixes ao caso não comutativo, i.e., substituir a cha Ω por um quantal Q right-sided e idempotente (denotado daqui em diante RSI).

Um quantal é um reticulado completo satisfazendo

$$a \& (\bigvee_i a_i) = \bigvee_i (a \& a_i), \quad (\bigvee_i a_i) \& a = \bigvee_i (a_i \& a)$$

para todo $a, a_i \in Q$, onde $\&$ é uma operação associativa (representando uma conjunção não comutativa; devemos observar que no artigo clássico de Ward e Dilworth [WD] foi considerado pela primeira vez um produto num reticulado completo que distribui com o supremo). Temos que Q é RSI se, adicionalmente, $\top \& a = a = a \& a$, onde $\top$ denota o máximo elemento de Q . O produto $\&$ produz duas implicações diferentes:

$$a \rightarrow_r b = \bigvee \{c : a \& c \leq b\}, \quad a \rightarrow_l b = \bigvee \{c : c \& a \leq b\}.$$

Existem diversos trabalhos de F. Borceaux, G. van den Bossche *et al* sobre Q -sets, prefeixes e feixes sobre um quantais, com definições diferentes. Porém, o enfoque de F. Miraglia e U. Solitro ([MS]) representa a generalização mais fiel do trabalho de Fourman-Scott. A partir do conceito de sub-prefeixe fechado, é definida em [MS] a generalização natural de função característica, sendo possível definir operações lógicas entre funções características que fornecem uma estrutura de right-quantal (i.e., só temos a distributividade $h \& \bigvee_i h_i = \bigvee_i (h \& h_i)$). Além disso, são definidas as

noções de quantificação $\forall, \exists$ como os adjuntos à direita e à esquerda da imagen inversa da projeção, respectivamente. Portanto, os conceitos desenvolvidos em [MS] formam a base apropriada para definir uma lógica de primeira ordem a ser interpretada nas categorias $Psh(Q)$ e $Sh(Q)$ dos prefeixes e feixes sobre quantais.

Por outro lado, J.Y. Girard, motivado por questões da teoria da prova, publica em 1987 os fundamentos da lógica linear ([Gir]), uma lógica construtiva que refina as lógicas clássica e intuicionista no sentido de manter controle das hipóteses ou “recursos” utilizados numa prova, o que permite formalizar de maneira apropriada procesos computacionais de concorrência. A ideia básica é considerar as hipóteses como “recursos”, que são portanto limitados. Além disso, uma vez que um recurso é utilizado ele já não é mais disponível, pois foi “consumido”. Assim, ter uma hipótese ϕ duas vezes, por exemplo, é diferente do que ter ϕ uma vez só. Essa é a diferença principal com as lógicas clássica e intuicionista, onde, por causa das regras de *weakening* e *contraction*, uma hipótese pode ser usada tanto ou tão pouco quanto quizermos. A proposta de Girard é, numa primeira etapa, eliminar essas regras estruturais. Isto obriga, numa segunda etapa, a uma releitura da definição da conjunção. Com efeito, as definições alternativas

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi} \qquad \frac{\Gamma \vdash \phi \quad \Delta \vdash \psi}{\Gamma, \Delta \vdash \phi \wedge \psi}$$

são equivalentes na presença de *weakening* e *contraction*. Sem as regras estruturais, a situação muda, originando duas conjunções diferentes: a primeira (denotada por $\&$) é chamada de aditiva pois, para a sua execução, é necessário identificar os contextos ou “compatilhar os recursos” Γ . A segunda (denotada por $\otimes$) é chamada de multiplicativa, pois obriga à concatenação dos contextos Γ, Δ , i.e., não “compartilhamos os recursos”. Assim, vamos ter

$$\phi \vdash \phi \& \phi \qquad \text{e} \qquad \phi, \phi \vdash \phi \otimes \phi$$

correspondendo à ideia de que $\phi \otimes \phi$ codifica duas cópias de ϕ , enquanto $\phi \& \phi$ codifica uma cópia só. Finalmente, numa terceira etapa, é recuperado o poder expressivo das lógicas clássica e intuicionista a través de duas modalidades (denotadas $! \text{ e } ?$), chamadas de exponenciais. A lógica clássica é reproduzida na álgebra de Boole (dentro da álgebra de Lindembaum da lógica) das fórmulas da forma $!\phi$, enquanto a lógica intuicionista é codificada nas fórmulas da forma $!\phi$, que formam uma álgebra de Heyting na álgebra de Lindembaum da lógica.

Foi D. Yetter ([Yet]) quem revelou que a semântica algébrica (espaços de fases) definida por Girard não é outra coisa que quantais satisfazendo certas propriedades específicas (impostas pela lógica), hoje chamados quantais de Girard. Além das vantagens óbvias de poder estudar a semântica algébrica dentro de uma teoria bem desenvolvida, abre-se também a possibilidade de estudar extensões e generalizações da lógica linear utilizando quantais apropriados como uma classe consistente e completa de modelos algébricos para cada uma dessas lógicas (no Apêndice I, prova-se que os quantais unitais comutativos e os quantais unitais são uma classe consistente e completa de modelos para a lógica linear intuicionista comutativa e para a lógica linear intuicionista não comutativa, respectivamente). Mais ainda, é possível definir uma certa lógica de tipo linear de maneira que os quantais em geral (sem propriedade particular nenhuma) sejam uma classe consistente e

completa de modelos.

O presente trabalho tem como objetivo, a partir das considerações anteriores, a definição de uma lógica *many-sorted* que represente de maneira correta as construções nas categorias $Psh(Q)$ e $Sh(Q)$, completando desta maneira as dualidades

$$\text{topologia comutativa/topologia não comutativa}, \quad \Omega \text{ cHa}/Q \text{ quantal RSI}, \quad Sh(\Omega)/Sh(Q).$$

Assim, a lógica definida tem características da lógica linear, podendo ser considerada uma lógica intuicionista não comutativa.

No primeiro capítulo, são estudadas as relações entre o cálculo da imagem inversa por um morfismo e as operações lógicas entre funções características; é estabelecido que, diferente do caso comutativo, as operações entre funções características (com exceção dos quantificadores e da conjunção “clásica”) não são respeitadas, a menos que certas relações entre os extents dos objetos envolvidos sejam satisfeitas; em particular, a mera extensão $R \times A$ de um sub-prefixe $R \subseteq B$ por um novo prefixe A (considerando como morfismo a projeção $\pi : B \times A \rightarrow B$) não respeita as operações de disjunção, nem o produto $\&$ nem a implicação à direita $\rightarrow$, isto é,

$$(R \& S) \times A \neq (R \times A) \& (S \times A), \quad (R \vee S) \times A \neq (R \times A) \vee (S \times A), \quad (R \rightarrow S) \times A \neq (R \times A) \rightarrow (S \times A).$$

Este resultado indica que os sub-objetos da categoria são suscetíveis às “perturbações” originadas pela aparição de outros objetos; logo, o seu valor depende do contexto ou “meio” em que sejam considerados.

No capítulo 2 é introduzido o cálculo de sequentes (QPC) a partir de uma linguagem de primeira ordem *many-sorted*, assim como uma noção de interpretação em $Psh(Q)$ e $Sh(Q)$, fornecendo o marco sintático apropriado para representar conceitos nessas categorias. Os termos são interpretados como morfismos e uma fórmula $\phi(x_1, \dots, x_n)$ com x_i variável do tipo t_i gera uma função característica com domínio $\prod_{i=1}^n A_{t_i}$, onde A_{t_i} é o prefixe que interpreta o tipo t_i . Para isso, é introduzida a noção de contexto, que indica de maneira única (salvo isomorfismos) os domínios das funções características necessários para interpretar as fórmulas. Dado o comportamento complexo das funções características mencionado acima, esta informação é crítica. As regras de (QPC) têm a particularidade de virem acompanhadas de cláusulas, cujos elementos, chamados de justificativas, são conjuntos finitos de sequentes; para poder aplicar uma regra, será necessário provar todos os sequentes de alguma justificativa. As cláusulas contêm condições suficientes para assegurar a corretude da aplicação da regra, i.e., as relações entre extents (representados por fechos existenciais) mencionadas acima. O caso particular em que todos os prefixes envolvidos têm o mesmo extent produz um cálculo chamado de ($QPC1$), drasticamente mais simples que o geral, suficiente para provar o teorema de Kaplansky do último capítulo. Se ignorarmos as cláusulas, o sistema (QPC) é muito parecido com o sistema de lógica linear intuicionista não comutativa com igualdade introduzido no Apêndice I, o que coincide com a nossa intuição original.

No capítulo 3 discutimos algumas construções algébricas em $Psh(Q)$, tais como grupo, anel e módulo. Prova-se que um prefixe A é um modelo destas estruturas sse o conjunto $A(p)$ de

seções sobre p possui a estrutura correspondente, evidenciando seu carácter local. O conceito de corpo, não sendo equacionalmente definível, apresenta diferentes possibilidades de axiomatização, como acontece no caso intuicionista ([Mul1]). As duas noções de anel local introduzidas em [Mul1] resultam ser equivalentes em (QPC) , repetindo a situação intuicionista. Finalmente, é introduzido o feixe $\tilde{N}$ dos números naturais em $Sh(Q)$, a partir do qual é definido o feixe $\tilde{Z}$ dos inteiros, mediante a relação de equivalência usual; esta construção pode ser internalizada na lógica mediante a fórmula óbvia, só que o feixe das classes de equivalência não pode ser descrito internamente, pois a linguagem é de primeira ordem. Analogamente, a partir do feixe dos inteiros é definido o feixe dos números racionais $\tilde{Q}$ mediante a relação de equivalência usual (que pode ser descrita na linguagem). Nos três casos, os objetos resultam ser localmente os conjuntos definidos, isto é, $\tilde{N}$, $\tilde{Z}$ e $\tilde{Q}$ são isomorfos aos feixes constantes sobre N , Z e Q , respectivamente. A definição do feixe dos naturais permite definir sequências de elementos do tipo A (como sendo objetos do tipo $A^{\tilde{N}}$), assim como realizar em (QPC) provas por indução, a partir do axioma

$$\phi(0) \otimes (\forall n)(\phi(n) \multimap \phi(n+1)) \vdash (\forall n)\phi(n).$$

Finalmente, no capítulo 4, utilizamos $(QPC1)$ para provar uma versão do teorema de Kaplansky, constituindo-se na principal aplicação do sistema $(QPC1)$ aqui apresentada. Assim, dada uma álgebra C^* não comutativa $\mathcal{A}$, a obtenção de um feixe F sobre $Q = Rid \mathcal{A}$ (satisfazendo o axioma de anel local) que represente $\mathcal{A}$ implicaria numa generalização do teorema de Swan ao contexto não comutativo, aplicando o resultado anterior e as técnicas de [Mul1]. Logo, podemos dizer que uma parte do caminho foi percorrida.

Adicionalmente, incluímos no Apêndice I um trabalho conjunto com F. Miraglia sobre lógica linear com igualdade (a ser publicado em "Logique et Analyse"). Nele, é introduzida uma noção de igualdade na lógica linear clássica, sendo estabelecido que, para satisfazer a lei de substituição de Leibnitz a partir das fórmulas atômicas, o predicado de igualdade deve satisfazer

$$(x = y) \multimap (x = y) \quad (\text{no sistema completo});$$

$$(x = y) \otimes (x = y) \multimap (x = y), \quad (x = y) \vdash \mathbf{1} \quad (\text{no fragmento multiplicativo-aditivo}).$$

A partir de uma formulação mais geral da teoria linear da igualdade, são definidos cálculos lineares com igualdade que contêm as teorias da igualdade obtidas codificando as teorias da igualdade clássica e intuicionista dentro da lógica linear.

Finalmente, são definidos cálculos lineares intuicionistas comutativos e não comutativos que têm como modelos os quantais unitais comutativos e não comutativos, respectivamente.

Há ainda muitas questões a ser estudadas. A teoria da prova em (QPC) (eliminação dos cortes, normalização), a representação de álgebras C^* em $Sh(Q)$, a definição do feixe dos números reais e a extensão da lógica a ordens superiores, são os primeiros exemplos que vêm à mente. Em relação à Teoria dos Modelos em $Psh(Q)$, poderíamos mencionar a questão da completude de (QPC) , a noção apropriada de subestrutura elementar e o Teorema de Lowenheim-Skolem, como temas a desenvolver.

A Estrutura das Funções Características

Neste capítulo estudaremos os quantais de funções características em prefeixes sobre um quantal RSI (i.e., right-sided e idempotente). Na primeira seção serão introduzidos os conceitos e resultados principais da teoria dos Q -sets, prefeixes e feixes sobre quantais RSI, definidos em [MS]. Nas seções seguintes, estudamos o comportamento da imagem inversa por um morfismo em relação às operações fundamentais entre funções características. Estes resultados irão caracterizar os axiomas e a semântica de uma lógica de primeira ordem apropriada à teoria dos modelos definida em prefeixes sobre um quantal RSI.

1.1 Feixes sobre Quantais Right-sided e Idempotentes

As noções de $\mathcal{H}$ -set, feixe e prefeixe sobre uma álgebra de Heyting completa (ou locale) e a possibilidade de interpretar a Lógica Intuicionista nestas categorias tem sido intensamente estudado ([FS], [Mul1], [MR], [Mir]); a noção de igualdade que aparece em [FS] é um modo conveniente de trabalhar com a semântica de prefeixes, mais operacional que a semântica funtorial, permitindo ainda uma interpretação natural da igualdade intuicionista em termos do predicado de existência de Scott ([Sco]).

O conceito de quantal ([Mul2]) aparece como mais uma ferramenta para o estudo das álgebras C^* não comutativas. Uma classe importante de quantais RSI é justamente a dos ideais laterais fechados em uma álgebra C^* não comutativa. Os trabalhos de Akemann ([Ake1], [Ake2], [Ake3]) e Giles e Kummer ([GK]) generalizam o Teorema de Gelfand para o contexto não comutativo. Era natural, portanto, o passo de estender as noções de prefeixe e feixe a este novo contexto ([Naw], Borceaux *et al*). Adotaremos [MS] como base de nosso desenvolvimento, por considerar que se trata da mais exata generalização de [FS]. Todas as definições e resultados desta seção foram introduzidos em [MS]. A referência fundamental sobre quantais é [Ros].

Definição 1.1.1 *Um quantal é um reticulado completo Q munido de um produto associativo $\& : Q \times Q \longrightarrow Q$ que distribui à esquerda e à direita de supremos arbitrários, i.e.,*

$$[Q1] \quad a \& (b \& c) = (a \& b) \& c, \quad \text{para todo } a, b, c \in Q$$

$$[Q2] \quad a \& (\bigvee_{i \in I} a_i) = \bigvee_{i \in I} (a \& a_i), \quad (\bigvee_{i \in I} a_i) \& a = \bigvee_{i \in I} (a_i \& a).$$

Dizemos que Q é right-sided se $a \& \top \leq a$ para todo $a \in Q$, onde $\top$ denota o elemento máximo de Q . Q é idempotente se $a = a \& a$ para todo $a \in Q$. Portanto, Q é right-sided e idempotente (denotado RSI) sse $a \& \top = a = a \& a$ para todo $a \in Q$.

Um morfismo de quantais é uma função que preserva supremos arbitrários e a operação $\&$.

A partir da definição de quantal, é fácil provar que $\&$ é crescente nas duas coordenadas, i.e.,

$$a \leq a', \quad b \leq b' \quad \text{implica} \quad a \& b \leq a' \& b'.$$

Por causa de [Q2] obtemos duas implicações diferentes, dadas por

$$a \rightarrow_r b = \bigvee \{c \in Q : a \& c \leq b\}, \quad a \rightarrow_l b = \bigvee \{c \in Q : c \& a \leq b\},$$

chamadas de implicação à direita e implicação à esquerda, respectivamente. Logo,

$$c \leq a \rightarrow_r b \quad \text{sse} \quad a \& c \leq b; \quad c \leq a \rightarrow_l b \quad \text{sse} \quad c \& a \leq b.$$

No que se segue, o termo “quantal” denota um quantal RSI.

Definição 1.1.2 : Seja Q um quantal, e $p, q \in Q$; dizemos que p é two-sided em q se $q \& p = p$. Se p é two-sided em $\top$, então p é two-sided. Denotamos por

$$q \downarrow = \{p \in Q : q \& p = p\}, \quad \Omega(Q) = \{p \in Q : \top \& p = p\}$$

os conjuntos dos two-sided em q e os two-sided de Q , respectivamente. Se $p \in Q$, então $\bar{p} = \top \& p$ é o fecho de p em Q ; $\bar{p}$ é o mínimo two-sided $\geq p$.

Frequentemente, escreveremos $\prod_{i=1}^n a_i$ para denotar $a_1 \& \cdots \& a_n$, onde $a_1, \dots, a_n \in Q$; $p^\leftarrow$ indicará o conjunto $\{q \in Q : q \leq p\}$, $p \in Q$.

Proposição 1.1.3 : Seja Q um quantal e p, q elementos de Q .

(1) $p \& q \leq p$; $p \leq q$ implica $p = p \& q$.

(2) Se $p_1, \dots, p_n \in Q$ são two-sided, então

$$p \& \prod_{i=1}^n p_i = p \wedge \bigwedge_{i=1}^n p_i;$$

logo, $p \& q = p \wedge q$ para todo p, q two-sided, e temos a **regra de exchange**:

$$p \& \prod_{i=1}^n q_i = p \& \prod_{i=1}^n q_{\sigma(i)}$$

para todo $p, q_1, \dots, q_n \in Q$ e toda permutação σ de $\{1, \dots, n\}$.

(3) Para todo $p_1, \dots, p_n \in Q$, $\bigwedge_{i=1}^n p_i \leq \prod_{i=1}^n p_i$.

(4) Para todo $\emptyset \neq S \subseteq Q$, $(\bigwedge_{q \in S} q) \& p = \bigwedge_{q \in S} (q \& p)$.

(5) $p \& q = p \wedge \bar{q}$.

Definição 1.1.4 : Seja Q um quantal e $|A|$ um conjunto. Um Q -set A de domínio $|A|$ consiste numa aplicação

$$[* = *] : |A| \times |A| \longrightarrow Q$$

satisfazendo as condições seguintes para $x, y, z \in |A|$:

$$[EQ1] \quad \overline{[x = y]} = \overline{[y = x]}; \quad [EQ2] \quad [x = y] \& [y = z] \leq [x = z].$$

Os elementos de $|A|$ são seções de A ; denotamos $[x = x]$ por Ex , o extent de x . Definimos $EA = \bigvee_x Ex$, o extent de A . Para $p \leq EA$, $A(p) = \{x \in |A| : Ex = p\}$ é o conjunto das seções de A sobre p . Assumimos que A possui uma única seção $*$ sobre 0 , i.e., $A(0) = \{*\}$.

Observe que $[EQ1]$ exige a simetria só no fecho da igualdade. A motivação é a seguinte: queremos, dado o conjunto $|A|$, medir o nível de “semelhança” ou o “tempo em que coincidem” dois elementos $x, y \in |A|$; os valores são “medidos” no quantal Q , sendo que Ex indica “quanto tempo” existe o elemento x , ou “o quanto mede”. A teoria dos $\mathcal{H}$ -sets estabelece os mesmos princípios, só que a “medida” está numa cHa. Um exemplo típico é considerar $|A| = \bigcup_{V \in \Omega(X)} C(V)$, onde $\Omega(X)$ denota a cHa dos abertos de X e $C(V)$ é o anel das funções reais contínuas sobre o aberto V , com a igualdade entre duas funções f, g dada por

$$[f = g] = \bigcup \{U \subseteq \text{Dom}(f) \cap \text{Dom}(g) \text{ aberto} : f|_U = g|_U\}$$

e o “período de existência” ou “tamanho” de uma $f \in |A|$ sendo portanto

$$Ef = [f = f] = \text{Dom}(f).$$

Lema 1.1.5 : Seja A um Q -set e x, y, z seções de A .

(a) Para todo $p \in Q$, $p \& [x = y] = p \& [y = x]$. Mais ainda,

$$[x = y] \& [x = z] = [x = y] \& [y = z].$$

(b) Temos que:

$$Ex \& [x = y] = [x = y] \& Ex = [x = y] \& Ey = [x = y]; \quad Ey \& [x = y] = [y = x];$$

$$[x = y] \in (Ex \& Ey) \downarrow \subseteq Ex \downarrow.$$

(c) Sejam $s_i, t_i \in |A|$ tais que $Es_i = Es_j$ ($i, j = 1, \dots, n$). Então,

$$\prod_{i=1}^n [s_i = t_i] = \bigwedge_{i=1}^n [s_i = t_i] = \prod_{i=1}^n [s_{\sigma(i)} = t_{\sigma(i)}]$$

para toda permutação σ de $\{1, \dots, n\}$.

Vamos exigir que os nossos Q -sets satisfaçam a seguinte condição de separação ou extensionalidade:

Definição 1.1.6 : Um Q -set A é dito extensional ou separado se, para todo $x, y \in |A|$, temos:

$$[EXT] \quad Ex = Ey = [x = y] \quad \text{sse} \quad x = y.$$

A condição $[EXT]$ coincide, no caso clássico, com a noção usual de separação, i.e., duas seções de mesmo extent, que têm as mesmas restrições aos elementos de uma cobertura do seu extent, são iguais.

Observação 1.1.7 : Se A é um Q -set, considere a relação

$$x \approx y \quad \text{sse} \quad Ex = Ey = [x = y].$$

Então, $\approx$ é relação de equivalência. Se $|\eta A| = \{x/\approx : x \in |A|\}$ é o conjunto das classes de equivalência, então ηA é um Q -set extensional via $[x/\approx = y/\approx] \equiv_{def} [x = y]$. $\square$

Definição 1.1.8 : Sejam A, B Q -sets. Um morfismo de A em B é uma aplicação $f : |A| \rightarrow |B|$ satisfazendo para todo $x, y \in |A|$:

$$[mor1] \quad Ef(x) = Ex \quad [mor2] \quad [x = y] \leq [f(x) = f(y)].$$

Observe que a existência de um morfismo $f : A \rightarrow B$ implica que $EA \leq EB$. A composição de dois morfismos é um morfismo e a função identidade é um morfismo. Temos assim a categoria dos Q -sets, indicada por $Qs(Q)$. A definição de morfismo dada acima difere da encontrada em [Naw], [BBC] e [BC1]; nesses casos, A é isomorfo a ηA , para todo Q -set A .

Lema 1.1.9 : Seja $f : A \rightarrow B$ um morfismo de Q -sets.

(a) Considere as condições

$$(1) \quad [x = y] = [fx = fy] \quad \text{para todo } x, y \in |A|.$$

$$(2) \quad f \text{ é injetora como função de } |A| \text{ em } |B|.$$

$$(3) \quad f \text{ é mônico em } Qs(Q).$$

$$\text{Então, } (1) \Rightarrow (2) \Rightarrow (3).$$

(b) As seguintes condições são equivalentes:

$$f \text{ é épico em } Qs(Q); \quad \text{Para todo } b \in |B|, \quad Eb = \bigvee_{a \in |A|} [b = fa].$$

Definição 1.1.10 : Seja A um Q -set, e $S, T \subseteq |A|$. Dizemos que S é denso em T se, para todo $t \in T$, $Et = \bigvee_{s \in S} [t = s]$. O conjunto S é denso se for denso em $|A|$.

Lema 1.1.11 : Dois morfismos que coincidem em um denso são iguais.

Proposição 1.1.12 : (a) Seja A_i ($i \in I$) uma família de Q -sets. O produto $\prod_{i \in I} A_i$ em $Qs(Q)$ é dado por

$$\begin{aligned} |\prod_{i \in I} A_i| &= \{(x_i) \in \prod_{i \in I} |A_i| : Ex_i = Ex_j \text{ para todo } i, j \in I\}; \\ [(x_i) = (y_i)] &\equiv_{def} \bigwedge_{i \in I} [x_i = y_i]; \quad \pi_j : |\prod_{i \in I} A_i| \longrightarrow |A_j|, \quad (x_i) \mapsto x_j, \end{aligned}$$

enquanto que o coproduto $\coprod_{i \in I} A_i$ é dado por

$$|\prod_{i \in I} A_i| = \bigsqcup_{i \in I} |A_i| = \bigcup_{i \in I} |A_i| \times \{i\}, \quad (*, i) \equiv_{def} * \quad \forall i \in I,$$

$$[(x, i) = (y, j)] = \begin{cases} [x = y] & \text{se } i = j \\ \mathbf{0} & \text{em caso contrário} \end{cases},$$

$$\lambda_j : |A_j| \longrightarrow |\prod_{i \in I} A_i|, \quad x \mapsto (x, j).$$

Assim, $E \prod_i A_i = \bigvee \{p \leq \bigwedge_i EA_i : A_i(p) \neq \emptyset \quad \forall i \in I\} \leq \bigwedge_i EA_i$, e $E \coprod_i A_i = \bigvee_i EA_i$.

(b) O objeto final na categoria $Qs(Q)$, $\mathbf{1}$, é dado por

$$|\mathbf{1}| = Q, \quad [p = q] \equiv_{def} p \& q.$$

(c) Se $f, g : A \longrightarrow B$ são morfismos, o equalizador $Eq(f, g)$ em $Qs(Q)$ é dado por

$$|Eq(f, g)| = \{x \in |A| : fx = gx\}; \quad \text{igualdade herdada de } A.$$

Observe que, no exemplo “intuicionista” das funções contínuas sobre X , temos a noção de restrição, que foi utilizada para definir a igualdade; esta noção é generalizada na

Definição 1.1.13 : Seja Q um quantal, e $|P|$ um conjunto; um prefeixe P com domínio $|P|$ consiste em duas funções

$$E : |P| \longrightarrow Q, \quad x \mapsto Ex \quad (\text{extent})$$

$$*|_* : |P| \times (EP)^{\leftarrow} \longrightarrow |P|, \quad (x, p) \mapsto x|_p \quad (\text{restrição})$$

onde $EP = \bigvee_x Ex$, satisfazendo:

$$[REST1] \quad x|_{Ex} = x \quad [REST2] \quad (x|_p)|_q = x|_{q \& p}$$

$$[REST3] \quad E(x|_p) = p \& Ex \quad [ext] \quad Ex = Ey = \bigvee \{p \in Ex \downarrow : x|_p = y|_p\} \text{ implica } x = y.$$

Dado um prefeixe P , podemos definir para $x, y \in |P|$:

$$[*] \quad [x = y] \equiv_{def} \bigvee \{p \in (Ex \& Ey) \downarrow : x|_p = y|_p\}$$

obtendo assim um Q -set extensional que satisfaz a condição

$$[R] \quad [x|_p = x] = p \& E x = E(x|_p) \quad \text{para todo } p \leq EP, x \in |P|.$$

Reciprocamente, todo Q -set extensional P com uma função

$$*|_* : |P| \times (EP)^{\leftarrow} \longrightarrow |P|$$

satisfazendo $[R]$ é um prefeixe. Considerando como morfismo entre prefeixes os morfismos de Q -sets (os quais satisfarão: $f(x|_p) = (fx)|_p$), prova-se que a categoria $Psh(Q)$ de prefeixes sobre Q é cartesiana fechada. Se $(x_i) \in |\prod_{i \in I} A_i|$, e $p \leq E \prod_{i \in I} A_i$, então $(x_i)|_p \equiv_{def} (x_i|_p)$. Além disso, se $(x, i) \in |\prod_{i \in I} A_i|$, $q = \bigvee_i EA_i$, $EA_i \in q \downarrow$ para todo i , e $p \leq q$, então $(x, i)|_p \equiv_{def} (x|_p \& EA_i, i)$. Se I é finito, então $E \prod_{i \in I} A_i = \bigwedge_{i \in I} EA_i$. Temos:

Lema 1.1.14 : *Seja P um prefeixe sobre Q , $[* = *]$ a igualdade induzida por $[*]$, $x, y \in |P|$ e $p, q \leq EP$.*

- (a) $[x|_p = y|_q] = p \& [x = y] \& q$.
- (b) $[x|_p = y] = p \& [x = y]$.
- (c) $[x = y|_q] = [x = y] \& q$. Em particular, $[x = x|_p] = Ex \& p$.
- (d) $x|_{[x=y]} = y|_{[x=y]}$.

Lema 1.1.15 : *Seja $f : A \longrightarrow B$ um morfismo de prefeixes. São equivalentes:*

- (1) para todo $x, y \in |A|$, $[x = y] = [fx = fy]$.
- (2) f é injetora como função de $|A|$ em $|B|$.
- (3) f é mônico em $Psh(Q)$.

Definição 1.1.16 : *Seja A um prefeixe sobre Q . Um sub-prefeixe S de A é um subconjunto $|S| \subseteq |A|$, fechado por restrições para todo $p \leq ES = \bigvee_{s \in |S|} Es$. Escreveremos $S \subseteq A$; $\mathcal{P}(A)(EA)$ denotará o conjunto dos sub-prefeixes de A ; $\mathcal{P}(A)(EA)$ é parcialmente ordenado pela inclusão (conjuntista).*

Teorema 1.1.17 : (a) *Sejam S_i sub-prefeixes de A ($i \in I$); então*

$$|\bigwedge_{i \in I} S_i| = \bigcap_{i \in I} |S_i|; \quad |\bigvee_{i \in I} S_i| = \{s|_p \in |A| : s \in \bigcup_{i \in I} |S_i|, p \leq \bigvee ES_i\}$$

são o supremo e o ínfimo (em $\mathcal{P}(A)(EA)$), respectivamente, da família (S_i) .

(b) *A operação*

$$|S \& T| \equiv_{def} \{s|_{[s=t]} : s \in |S|, t \in |T|\}$$

*induz em $\mathcal{P}(A)(EA)$ uma estrutura de **right-quantal** RSI , i.e.,*

$$S \& \bigvee_{i \in I} S_i = \bigvee_{i \in I} (S \& S_i);$$

além disso,

$$(\bigvee_{i \in I} S_i) \& S = \bigvee_{i \in I} (S_i \& S) \quad \text{sse} \quad \bigvee_{i \in I} E(S_i \& S) \in (\bigvee_{i \in I} E S_i) \downarrow.$$

Temos que $E(S \& T) \leq ES \& ET$, não valendo, em geral, a igualdade.

Voltando ao exemplo das funções contínuas, observemos que temos a seguinte propriedade adicional: se $\{f_i\}$ é uma família de funções contínuas, cada f_i com domínio U_i , tal que $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$, para todo i, j (uma família compatível), então existe f definida em $U = \bigcup_i U_i$ dada por $f|_{U_i} = f_i$, que estende cada f_i . A possibilidade de “colar” famílias compatíveis é o que distingue os **feixes** entre os prefeixes (sobre uma cHa). Passando ao caso não comutativo, temos a seguinte

Definição 1.1.18 : Seja A um Q -set extensional, $S \subseteq |A|$ um conjunto de seções e $p \leq EA$.

(a) Dizemos que S é compatível sobre p se, para todo $s, t \in S$, vale $p \& [s = t] = p \& Es \& Et$.

(b) Dizemos que S é compatível se, para todo $s, t \in S$, vale $[s = t] = Es \& Et$.

(c) A é um feixe se satisfaz:

$[glu\ p]$ para todo $p \leq EA$ e para todo $S \subseteq |A|$ compatível sobre p , existe $x \in |A|$ satisfazendo:

$$[s = x] = Es \& p \quad \text{para todo} \quad s \in S; \quad Ex = p \& \bigvee_{s \in S} Es.$$

$[glu]$ para todo $S \subseteq |A|$ compatível, existe $x \in |A|$ (o join de S) satisfazendo:

$$[s = x] = Es \quad \text{para todo} \quad s \in S; \quad Ex = \bigvee_{s \in S} Es.$$

Proposição 1.1.19 : Seja A um prefeixe, $S \subseteq |A|$, e $p \leq EA$.

(a) As três condições seguintes são equivalentes:

S é compatível sobre p ; $s|_{p \& Es \& Et} = t|_{p \& Es \& Et}$ para todo $s, t \in S$;

$S|_p$ é compatível, onde $S|_p = \{s|_p : s \in S\}$.

(b) As duas condições seguintes são equivalentes:

S é compatível; $s|_{Es \& Et} = t|_{Es \& Et}$ para todo $s, t \in S$.

(c) Se S é compatível sobre p , e $x \in |A|$, são equivalentes:

x verifica $[glu\ p]$ para S ; $x|_{p \& Es} = s|_p$ para todo $s \in S$, e $Ex = p \& \bigvee_{s \in S} Es$.

(d) Se S é compatível, e $x \in |A|$, são equivalentes:

x verifica $[glu]$ para S ; $x|_{Es} = s$ para todo $s \in S$, e $Ex = \bigvee_{s \in S} Es$.

(e) Um Q -set extensional é um feixe sse é um prefeixe satisfazendo $[glu]$.

Considerando como morfismos de feixes os morfismos de Q -sets, obtemos uma categoria denotada por $Sh(Q)$.

Definição 1.1.20 : *Seja A um feixe. Um sub-feixe de A é um sub-prefeixe de A satisfazendo $[glu]$. Denotamos por $\mathcal{P}(A)(EA)$ o right-quantal dos sub-feixes de A .*

Exemplos 1.1.21 : (1) $\mathbb{1}$ é um feixe; a restrição é dada por $p|_q = q \& p$.

(2) Dado um Q -set A e $p \leq EA$, então

$$|A|_p = \{x \in |A| : Ex \leq p\}$$

com a igualdade induzida é um Q -set com extent $\leq p$. Se A é um prefixe (um feixe), então $A|_p$ é um prefixe (um feixe) com a restrição induzida, e $E(A|_p) = p$ (pois $x|_p \in |A|_p$ para todo $x \in |A|$).

(3) Seja X um conjunto, $p \in Q$, e considere

$$\mathcal{C}_X(p) = \{X \xrightarrow{f} p \downarrow : \forall x, y (x \neq y \Rightarrow f(x) \& f(y) = \mathbf{0}), p = \bigvee_x f(x)\}.$$

Seja $|\mathcal{C}_X| = \bigsqcup_p \mathcal{C}_X(p) = \bigcup_p \mathcal{C}_X(p) \times \{p\}$ e defina

$$[* = *] : |\mathcal{C}_X| \times |\mathcal{C}_X| \longrightarrow Q, \quad [(f, p) = (g, q)] = \bigvee_x f(x) \& g(x),$$

$$*|_* : |\mathcal{C}_X| \times Q \longrightarrow |\mathcal{C}_X|, \quad (f, p)|_r = (r \& f, r \& p), \quad [r \& f](x) = r \& f(x).$$

Com essas definições, $\mathcal{C}_X$ é um feixe com $E\mathcal{C}_X = \top$. Para $x \in X$, considere o seguinte elemento de $\mathcal{C}_X(\top)$:

$$\text{Se } y \in X, \quad \tilde{x}(y) = \begin{cases} \top & \text{se } y = x \\ \mathbf{0} & \text{se } y \neq x. \end{cases}$$

A aplicação $x \mapsto \tilde{x}$ é injetora ($\tilde{x} = \tilde{y}$ sse $x = y$), nos fornecendo uma cópia de X densa em $\mathcal{C}_X$. O feixe $\mathcal{C}_X$ é chamado de feixe constante sobre X .

(4) Sejam A, B prefixes (resp. feixes) sobre Q ; para cada $p \leq EA$, seja $B^A(p) = \text{Hom}(A|_{EA \& p}, B)$, e considere $|B^A| = \bigcup_{p \leq EA} B^A(p) \times \{p\}$. Temos um prefixe (resp. um feixe) dado por

$$E : |B^A| \longrightarrow Q, \quad *|_* : |B^A| \times (EA)^\leftarrow \longrightarrow |B^A|,$$

onde $E(f, p) = p$, $(f, p)|_q = (f|_{EA \& q \& p}, q \& p)$ e $f|_r$ é a restrição de f a $A|_r$. Assim, $EB^A = \bigvee \{p \leq EA : \text{Hom}(A|_{EA \& p}, B) \neq \emptyset\}$. O prefixe B^A é chamado de prefixe de morfismos (resp. feixe de morfismos) de A em B . O morfismo de cálculo num ponto é dado por

$$ev : B^A \times A \longrightarrow B, \quad ((f, p), x) \mapsto fx. \quad \square$$

Teorema 1.1.22 : *Em $Psh(Q)$ (resp. em $Sh(Q)$), as operações de produto cartesiano e exponenciação são adjuntas, i.e., existe uma bijeção natural entre $\text{Hom}(\mathcal{C}, B^A)$ e $\text{Hom}(\mathcal{C} \times A, B)$ dada por*

$$f \in \text{Hom}(\mathcal{C}, B^A) \longmapsto ev \circ (f \times id_A) \in \text{Hom}(\mathcal{C} \times A, B).$$

Proposição 1.1.23 : (a) A caracterização de mônicos e épicos em $Psh(Q)$ vale para $Sh(Q)$.

(b) Seja A um Q -set, B um feixe, $S \subseteq |A|$ denso, e $f_0 : S \rightarrow |B|$ satisfazendo para todo $s, t \in S$:

$$Ef_0s = Es; \quad [s = t] \leq [f_0s = f_0t].$$

Se $EA \leq EB$, f_0 tem uma única extensão a um morfismo $f : A \rightarrow B$, onde $f(a)$ é o join em B do conjunto compatível $\{(f_0(s))_{[a=s]} : s \in S\}$ para todo $a \in |A|$. Mais ainda, se A é prefeixe, então f é mônico sse $[s = t] = [f_0s = f_0t]$, para todo $s, t \in S$.

Teorema 1.1.24 : Seja A um Q -set. Então, existe um feixe cA sobre Q e um morfismo $c : A \rightarrow cA$ tal que

(a) Para todo $a, b \in |A|$, $[a = b] = [ca = cb]$;

(b) Para todo $x \in |cA|$, $Ex = \bigvee_{a \in |A|} [x = ca]$;

(c) Se B é um feixe e $f : A \rightarrow B$ é um morfismo, então existe um único morfismo $g : cA \rightarrow B$ tal que $g \circ c = f$.

A operação que associa a um Q -set A o feixe cA , denomina-se **completamento ou feixificação**.

Corolário 1.1.25 : A categoria $Sh(Q)$ é completa, possuindo objeto inicial e coequalizadores. Além disso, tem coproduto de todas as famílias $\{A_i : i \in I\}$ de objetos tais que $EA_j \in (\bigvee_i A_i) \downarrow$, para todo $j \in I$.

Definição 1.1.26 : Seja A um prefeixe e $S \subseteq |A|$ um conjunto de seções. Definimos

(a) O fecho de S em A como sendo

$$cl(S) = \{x \in |A| : Ex \leq \bigvee_{s \in S} [s = x]\};$$

(b) O 2-fecho de S em A como sendo

$$tcl(S) = \{x \in |A| : Ex = \bigvee_{s \in S} [x = s]\}.$$

(c) S é fechado se $S = cl(S)$; S é 2-fechado se $S = tcl(S)$. Seja $c\mathcal{P}(A)(EA)$ e $t\mathcal{P}(A)(EA)$ a coleção de sub-prefeixes fechados e 2-fechados de A , respectivamente.

Proposição 1.1.27 : Se A é um prefeixe, então $c\mathcal{P}(A)(EA)$ e $t\mathcal{P}(A)(EA)$ são reticulados completos, onde

$$|\bigwedge S_i| = \bigcap_i |S_i|; \quad |\bigvee S_i| = cl(\bigvee' S_i),$$

onde $\bigvee'$ indica a operação de supremo descrita no item (a) do Teorema 1.1.17.

Com a operação $\&$ induzida, $c\mathcal{P}(A)(EA)$ é um right-quantal tal que a cHa dos elementos two-sided é $t\mathcal{P}(A)(EA)$. Além disso, temos que

$$|S \rightarrow T| = \{x \in |A| : \forall p \leq EA(x|_p \in |S| \Rightarrow x|_p \in |T|)\}$$

é a implicação à direita em $c\mathcal{P}(A)(EA)$. Se A é um feixe, então os sub-prefeixes fechados de A são exatamente os sub-feixes de A . Logo, a família de sub-feixes de A , $\mathcal{P}(A)(EA)$, é um right-quantal onde a cHa dos seus elementos two-sided é exatamente $t\mathcal{P}(A)(EA)$.

Corolário 1.1.28 : Seja Q um quantal. A aplicação $p \mapsto \mathbb{1}_p$ é um isomorfismo de quantais de Q em $\mathcal{P}(\mathbb{1})(\top)$ tal que, restrita a $\Omega(Q)$, produz um isomorfismo de cHa entre $\Omega(Q)$ e $t\mathcal{P}(\mathbb{1})(\top)$.

Exemplo 1.1.29 : Seja A um prefixe e considere, para $p \leq EA$ e $S \in c\mathcal{P}(A)(EA)$,

$$|S_p| = \{s|_{Es \& p} : s \in |S|\}.$$

Então, $S_p \in c\mathcal{P}(A)(EA)$, $A|_p \in c\mathcal{P}(A)(EA)$ e $S_p = S \& A|_p$. Definimos

$$c\mathcal{P}(A)(p) = \{(S, p) : S \in c\mathcal{P}(A)(EA), ES \& p = ES\}, \quad |c\mathcal{P}(A)| = \bigcup_{p \leq EA} c\mathcal{P}(A)(p),$$

$$E : |c\mathcal{P}(A)| \longrightarrow Q, \quad E(S, p) = p,$$

$$*_{|*} : |c\mathcal{P}(A)| \times EA^{\leftarrow} \longrightarrow |c\mathcal{P}(A)|, \quad (S, p)|_q = (S_q, q \& p).$$

Com estas definições, $c\mathcal{P}(A)$ é um prefixe, o prefixe dos sub-prefeixes fechados de A . Se A é um feixe, então $c\mathcal{P}(A)$ é um feixe, o feixe dos sub-feixes de A , denotado por $\mathcal{P}(A)$. $\square$

Finalmente descreveremos as funções características, que correspondem aos sub-prefeixes fechados, e as funções 2-características, correspondendo aos sub-prefeixes 2-fechados.

Definição 1.1.30 : Sejam $A_1, \dots, A_n$ prefixes e $w = \bigwedge_{i=1}^n EA_i$.

(a) Uma função característica é uma função $h : \prod_{i=1}^n |A_i| \longrightarrow Q$ tal que, para todo $\vec{x}, \vec{y} \in \prod_{i=1}^n |A_i|$:

$$[char1] \quad h(\vec{x}) \& E\vec{x} = h(\vec{x}) \leq w;$$

$$[char2] \quad h(\vec{x}) \& [\vec{x} = \vec{y}] \leq h(\vec{y});$$

$$[char3] \quad Eh \& h = h,$$

onde $[\vec{x} = \vec{y}] = \prod_{i=1}^n [x_i = y_i]$, $E\vec{x} = \prod_{i=1}^n Ex_i$ e $Eh = \bigvee_{\vec{x} \in \prod_{i=1}^n |A_i|} h(\vec{x})$.

(b) Uma função 2-característica é uma função $\tau : \prod_{i=1}^n |A_i| \longrightarrow Q$ tal que, para todo $\vec{x}, \vec{y} \in \prod_{i=1}^n |A_i|$:

$$[tchar0] \quad E\tau \& w = E\tau;$$

$$[tchar1] \quad E\vec{x} \& \tau(\vec{x}) = \tau(\vec{x});$$

$$[tchar2] \quad [\vec{y} = \vec{x}] \& \tau(\vec{x}) \leq \tau(\vec{y}),$$

onde $E\tau = \bigvee_{\vec{x}} \tau(\vec{x})$.

Na seguinte proposição são estabelecidas propriedades das funções características frequentemente utilizadas.

Proposição 1.1.31 : *Sejam $A_1, \dots, A_n$ prefeixes sobre Q , $w = \bigwedge_i EA_i$, $h : \prod_i |A_i| \rightarrow Q$ uma função característica, e $\vec{x} \in \prod_i |A_i|$.*

(a) *Seja α um subconjunto de $\{1, \dots, n\}$ e σ uma permutação de α . Então, $h(\vec{x}) \& \prod_{i \in \alpha} Ex_{\sigma(i)} = h(\vec{x})$.*

(b) *Para todo $p_i \leq EA_i$ ($i = 1, \dots, n$), temos que $h(x_1|_{p_1}, \dots, x_n|_{p_n}) = h(\vec{x}) \& \prod_{i=1}^n p_i$. Em particular, $h(\vec{x}|_{h(\vec{x})}) = h(\vec{x}|_{w \& E\vec{x}}) = h(\vec{x})$.*

(c) *Seja $S_i \cup \{x_i\} \subseteq |A_i|$, $p_i = \bigvee_{s \in S_i} [x_i = s]$ ($i = 1, \dots, n$), e $S = \prod S_i$. Então,*

$$h(\vec{x}) \& \prod_{i=1}^n p_i = \bigvee_{\vec{s} \in S} (h(s_1, \dots, s_n) \& [\vec{s} = \vec{x}]).$$

Em particular, se $K \subseteq Q$, $p = \bigvee K$, $x \in |A_i|$ e $\vec{a} \in \prod_{j \neq i} |A_j|$, então $h(x|_p, \vec{a}) = \bigvee_{k \in K} h(x|_k, \vec{a})$.

(d) *Seja S um conjunto de seções denso em $\prod_{i=1}^n A_i$. Então, duas funções características que coincidem em S são iguais.*

Proposição 1.1.32 : *Sejam $A_1, \dots, A_n$ prefeixes sobre Q , e $P = \prod_{i=1}^n A_i$ o prefeixe produto.*

(a) *Com a ordem pontual, as funções características são um right-quantal $Ch(A_1, \dots, A_n)$, onde as operações são dadas por :*

$$(\bigvee h_i)(\vec{x}) = (\bigvee_i Eh_i) \& \bigvee h_i(\vec{x}) \quad (\text{supremos});$$

$$(\bigwedge h_i)(\vec{x}) = \bigwedge h_i(\vec{x}) \quad (\text{ínfimos});$$

$$(h \& k)(\vec{x}) = h(\vec{x}) \& k(\vec{x}) \quad (\text{produto});$$

$$(h \rightarrow k)(\vec{x}) = (\bigwedge EA_i) \& (h(\vec{x}) \rightarrow_r k(\vec{x})) \& E\vec{x} \quad (\text{implicação à direita}).$$

(b) *As funções 2-características constituem uma cHa $Cht(A_1, \dots, A_n)$, com as operações definidas ponto a ponto, isomorfa à cHa dos elementos two-sided de $Ch(A_1, \dots, A_n)$ via*

$$\tau \in Cht(A_1, \dots, A_n) \mapsto (\bigwedge EA_i) \& \tau \in Ch(A_1, \dots, A_n).$$

(c) *$Ch(A_1, \dots, A_n)$ é isomorfo a $c\mathcal{P}(P)(EP)$ via*

$$h \mapsto |S_h| = \{\vec{x} \in |P| : E\vec{x} = Ex_1 = \dots = Ex_n \leq h(\vec{x})\},$$

$$S \mapsto h_S(\vec{x}) = \bigvee_{\vec{s} \in |S|} [\vec{s} = \vec{x}].$$

Logo, se cada A_i é um feixe, então $Ch(A_1, \dots, A_n) \simeq \mathcal{P}(P)(EP)$.

(d) *$Cht(A_1, \dots, A_n)$ é isomorfo a $t\mathcal{P}(P)(EP)$ via*

$$\tau \mapsto |S_\tau| = \{\vec{x} \in |P| : E\vec{x} = Ex_1 = \dots = Ex_n = \tau(\vec{x})\},$$

$$S \mapsto \tau_S(\vec{x}) = \bigvee_{\vec{s} \in |S|} [\vec{x} = \vec{s}].$$

Se $S \in t\mathcal{P}(P)(EP)$, a função característica associada é dada por $EP \& \tau_S$. Logo, se cada A_i é um feixe, então $Cht(A_1, \dots, A_n)$ é isomorfo à cHa dos sub-feixes 2-fechados de P .

Exemplo 1.1.33 : Se A é um prefeixe e $\Delta_n = \{\overbrace{(a, \dots, a)}^{n \text{ vezes}} : a \in |A|\}$, então Δ_n é um sub-prefeixe 2-fechado de A^n (para $n \geq 1$) tal que

$$\tau_{\Delta_n}(\vec{x}) = \prod_{i=1}^n [x_i = x_i], \quad h_{\Delta_n}(\vec{x}) = EA \& \prod_{i=1}^n [x_i = x_i]$$

são as funções 2-característica e característica associadas, respectivamente. Em particular, se $n = 2$, então $\tau_{\Delta_2}(x, y) = [x = y]$ é a função 2-característica da diagonal de A^2 , cuja função característica associada é $h_{\Delta_2}(x, y) = EA \& [x = y]$. Se $n = 1$, então $\tau_{\Delta_1}(x) = Ex = \tau_{|A|}(x)$, com função característica associada $h_{\Delta_1}(x) = EA \& Ex = h_{|A|}(x)$; estes são os elementos máximos em $Cht(A)$ e $Ch(A)$, respectivamente. $\square$

Podemos definir quantificadores com a noção de imagem inversa.

Proposição 1.1.34 : Sejam A, B prefeixes sobre Q , e $f : |A| \longrightarrow |B|$ um morfismo.

(a) Se $R \subseteq B$ é sub-prefeixe fechado com $F : |B| \longrightarrow Q$ função característica associada, então

$$|f^*R| = \{a \in |A| : f(a) \in |R|\}$$

é sub-prefeixe fechado de A , com função característica

$$G : |A| \longrightarrow Q, \quad G(a) = (ER \wedge EA) \& F(f(a)),$$

e $Ef^*R = E(R \wedge Imf)$.

(b) Se $R, S \subseteq B$ são sub-prefeixes fechados, então

$$f^*(R \& S) \supseteq f^*(R) \& f^*(S);$$

$$f^*(R \vee S) \supseteq f^*(R) \vee f^*(S);$$

$$f^*(R \wedge S) = f^*(R) \wedge f^*(S).$$

No caso clássico, os quantificadores surgem considerando as projeções $\pi_i : \prod_j A_j \longrightarrow \prod_{k \neq i} A_k$, sendo que $\exists x_i$ é o adjunto à esquerda de π_i^* , enquanto $\forall x_i$ é o seu adjunto à direita. Para simplificar a notação, consideramos $P = A \times \prod_{i=1}^n A_i$, e $\pi : P \longrightarrow (\prod_{i=1}^n A_i)_{|EP}$; assim, para todo $T \in c\mathcal{P}(\prod_i (A_i)_{|EP})(EP)$ e $S \in c\mathcal{P}(P)(EP)$,

$$\pi^*T \subseteq S \text{ sse } T \subseteq \forall a S, \quad S \subseteq \pi^*T \text{ sse } \exists a S \subseteq T$$

ou, equivalentemente, de $\pi^*T = A \times T$, obtemos

$$\forall aS = \bigvee \{T \in c\mathcal{P}(\prod_i (A_i)_{|EP})(EP) : A \times T \subseteq S\},$$

$$\exists aS = \bigwedge \{T \in c\mathcal{P}(\prod_i (A_i)_{|EP})(EP) : S \subseteq A \times T\}.$$

Vamos denotar $h_S(\vec{x})$ (para $S \in c\mathcal{P}(P)(EP)$) por $[S(\vec{x})]$. Então temos :

Proposição 1.1.35 : *Seja $P = A \times \prod_{i=1}^n A_i$, e $S \in c\mathcal{P}(P)(EP)$. Então, para todo $\vec{x} \in \prod_{i=1}^n |A_i|$:*

$$(a) [\exists aS(\vec{x})] = \bigvee_{a \in |A|} [S(a; \vec{x})].$$

$$(b) [\forall aS(\vec{x})] = (EP \wedge \bigwedge_{a \in |A|} (Ea \rightarrow_l [S(a; \vec{x})])) \& E \vec{x},$$

onde $\rightarrow_l$ denota a implicação à esquerda em Q .

1.2 Extensão de Sub-prefixes Fechados

A idéia básica é a seguinte: uma função característica $h : \prod_{i=1}^n |A_i| \rightarrow Q$ define um único sub-prefixe fechado de $\prod_{i=1}^n A_i$, portanto é possível interpretar h como uma fórmula de primeira ordem $\phi(x_1, \dots, x_n)$, sendo que cada x_j é uma variável de tipo j , a ser interpretada como uma seção de A_j . Os conectivos da lógica representarão as operações existentes entre funções características. Para que essas operações estejam definidas vamos levar os parâmetros a um domínio comum, isto é, devemos dar uma noção correta de “extensão” de sub-prefixes fechados. Temos três noções de extensão que surgem naturalmente, e provaremos que elas são equivalentes:

Lema 1.2.1 : *Sejam $h : \prod_{i=1}^n |A_i| \rightarrow Q$ uma função característica, $P = \prod_i A_i$, $S \subseteq P$ o sub-prefixe associado com h , e A um prefixe sobre Q . Considere as aplicações de $\prod_i |A_i| \times |A|$ em Q seguintes:*

$$(i) \quad h_1(\vec{x}, a) = (Eh \wedge EA) \& h(\vec{x}) \& Ea;$$

$$(ii) \quad h_2(\vec{x}, a) = (h(\vec{x}) \wedge EA) \& E(\vec{x}) \& Ea \text{ (se } n \neq 0);$$

$$(iii) \quad h_3 = h_{S \times A}.$$

Então, as três funções coincidem.

Demonstração: Seja $P = \prod_i |A_i|$. Temos que

$$h_1(\vec{x}, a) \leq EA \& h(\vec{x}) \& Ea = EA \& h(\vec{x}) \& E(\vec{x}) \& Ea \leq EA \& E(\vec{x}) \& Ea,$$

$$h_1(\vec{x}, a) \leq Eh \& h(\vec{x}) \& Ea = h(\vec{x}) \& E(\vec{x}) \& Ea, \text{ logo}$$

$$h_1(\vec{x}, a) \leq (EA \& E(\vec{x}) \& Ea) \wedge (h(\vec{x}) \& E(\vec{x}) \& Ea) = (EA \wedge h(\vec{x})) \& E(\vec{x}) \& Ea = h_2(\vec{x}, a).$$

Por outro lado,

$$h_3(\vec{x}, a) = \bigvee_{(\vec{s}, b) \in |S \times A|} [(\vec{s}, b) = (\vec{x}, a)] = \bigvee_{(\vec{s}, b) \in |S \times A|} ([\vec{s} = \vec{x}] \& [b = a]).$$

Dado $(\vec{x}, a) \in P \times |A|$, então existe $(\vec{x}_{|_{h_2(\vec{x}, a)}}, a_{|_{h_2(\vec{x}, a)}}) = (\vec{s}, b) \in |S \times A|$; logo,

$$h_2(\vec{x}, a) = [\vec{s} = \vec{x}] \& [b = a] \leq \bigvee_{(\vec{s}, b) \in |S \times A|} ([\vec{s} = \vec{x}] \& [b = a]) = h_3(\vec{x}, a).$$

Fixe agora $(\vec{x}, a) \in P \times |A|$, e seja $(\vec{s}, b) \in |S \times A|$; logo,

$$[\vec{s} = \vec{x}] \& [b = a] = E(\vec{s}) \& [\vec{s} = \vec{x}] \& [a = b] \leq (Eh \wedge EA) \& (\bigvee_{t \in |S|} [\vec{t} = \vec{x}]) \& Ea = h_1(\vec{x}, a),$$

pois $\vec{s} \in |S|$, $E(\vec{s}) = Ea$, e então $h_3(\vec{x}, a) \leq h_1(\vec{x}, a)$. $\square$

Definição 1.2.2 : Com a notação do lema 1.2.1, dizemos que $h_{S \times A}$ é a extensão de h por A . Se $n = 0$, i.e., $h : \mathbb{1} \rightarrow Q$, então identificamos h com Eh , pelo corolário 1.1.28, portanto a extensão de h por A é

$$k : |A| \rightarrow Q, \quad k(x) = (Eh \wedge EA) \& Ex.$$

Corolário 1.2.3 : Sejam $h : \prod_{i=1}^n |A_i| \rightarrow Q$ uma função característica, $P = \prod_{i=1}^n A_i$, $S \subseteq P$ o sub-prefeixe associado com h , e $B_1, \dots, B_k$ prefeixes sobre Q . Então, a extensão iterada de S por $B_1, \dots, B_k$ tem associada a função característica

$$h_{(\dots(S \times B_1) \times \dots) \times B_k}(\vec{x}; \vec{b}) = (Eh \wedge \bigwedge_j EB_j) \& h(\vec{x}) \& E\vec{b}$$

onde $\vec{x} \in \prod_i |A_i|$ e $\vec{b} \in \prod_j |B_j|$, i.e., o prefeixe definido é idêntico com o prefeixe obtido pela extensão de h por $B_1 \times \dots \times B_k$.

Demonstração: Seja h_1 a extensão de h por B_1 ; pelo lema 1.2.1,

$$h_1(\vec{x}; b_1) = (Eh \wedge EB_1) \& h(\vec{x}) \& Eb_1$$

para todo $\vec{x} \in \prod_i |A_i|$ e $b_1 \in |B_1|$. Observe que, pelo lema 1.2.1, $Eh_1 = Eh \wedge EB_1$. Estendendo h_1 por B_2 , obtemos

$$\begin{aligned} h_2(\vec{x}; b_1, b_2) &= (Eh_1 \wedge EB_2) \& h_1(\vec{x}; b_1) \& Eb_2 \\ &= ((Eh \wedge EB_1) \wedge EB_2) \& ((Eh \wedge EB_1) \& h(\vec{x}) \& Eb_1) \& Eb_2 \\ &= (Eh \wedge (EB_1 \wedge EB_2)) \& h(\vec{x}) \& Eb_1 \& Eb_2 \end{aligned}$$

pois $(Eh \wedge (EB_1 \wedge EB_2)) \leq (Eh \wedge EB_1)$. O resultado agora segue por indução. $\square$

Sob certas condições, a extensão tem uma forma simples:

Lema 1.2.4 : *Seja $h : \prod_i |A_i| \rightarrow Q$ função característica, e A um prefeixe tal que $Eh \leq EA$. Então a função característica da extensão de h por A vem dada por*

$$k(\vec{x}; x) = h(\vec{x}) \& Ex.$$

Demonstração: $(Eh \wedge EA) \& h(\vec{x}) \& Ex = Eh \& h(\vec{x}) \& Ex = h(\vec{x}) \& Ex. \quad \square$

Daremos agora um exemplo especial de quantal RSI, que será muito utilizado.

Exemplo 1.2.5 : Considere A uma álgebra C^* não comutativa simples, i.e., sem ideais bilaterais fechados em norma não triviais (por exemplo $A = M_n(\mathbb{C})$ ou $A = \mathcal{LC}(\mathcal{H})$). O quantal associado $QS = Rid A$ satisfaz a propriedade seguinte: para todo $I \in QS$, $A \& I = A$ (se $I \neq (0)$), e $A \& I = (0)$ (se $I = (0)$), portanto, dado que, em todo quantal RSI, $a \& b = a \wedge (\top \& b)$ para todo a, b , então a tabela do produto $\&$ é a seguinte:

$$I \& J = \begin{cases} I & \text{se } J \neq (0) \\ (0) & \text{se } J = (0) \end{cases}.$$

Observe que as respectivas implicações são dadas pelo seguinte:

$$I \rightarrow_r J = \bigvee \{K : I \& K \leq J\} = \begin{cases} \bigvee QS = \top & \text{se } I \leq J \\ \bigvee \{(0)\} = (0) & \text{se } I \not\leq J \end{cases},$$

$$I \rightarrow_l J = \bigvee \{K : K \& I \leq J\} = \begin{cases} \bigvee QS = \top & \text{se } I = (0) \\ \bigvee \{K : K \leq J\} = J & \text{se } I \neq (0) \end{cases}. \quad \square$$

Todo quantal com a tabela do produto $\&$ idêntica à de acima será indicado por QS ; ele será utilizado para fornecer alguns contraexemplos, assim como o seguinte

Lema 1.2.6 : *Seja B um prefeixe, e $p, q \leq EB$. Então:*

- (a) $B|_p \vee B|_q = B|_{p \vee q}$;
- (b) $B|_p \wedge B|_q = B|_{p \wedge q}$;
- (c) $B|_p \& B|_q = B|_{p \& q}$;
- (d) $B|_p \rightarrow B|_q = B|_{EB \wedge (p \rightarrow_r q)}$.

Demonstração: (a) Claramente, as funções características associadas com os três sub-prefeixes têm a forma

$$h_p(\vec{x}) = p \& E(\vec{x}), \quad h_q(\vec{x}) = q \& E(\vec{x}), \quad h_{p \vee q}(\vec{x}) = (p \vee q) \& E(\vec{x}),$$

respectivamente. Assim,

$$\begin{aligned} [h_p \vee h_q](\vec{x}) &= (p \vee q) \& (p \& E(\vec{x}) \vee q \& E(\vec{x})) \\ &= (p \vee q) \& (p \vee q) \& E(\vec{x}) = (p \vee q) \& E(\vec{x}) = h_{p \vee q}(\vec{x}). \end{aligned}$$

(b), (c) As operações são calculadas ponto a ponto, donde segue-se o resultado.

(d) Temos que

$$|B|_p \rightarrow |B|_q = \{x \in |B| : \forall s \leq EB (s \& Ex \leq p \Rightarrow s \& Ex \leq q)\},$$

$$|B|_{EB \wedge (p \rightarrow_r q)} = \{x \in |B| : p \& Ex \leq q\}.$$

Sendo $p \& Ex \leq p$, então $|B|_p \rightarrow |B|_q \subseteq |B|_{EB \wedge (p \rightarrow_r q)}$. Por outro lado, temos o seguinte

Fato: $(s \rightarrow_r p) \wedge (p \rightarrow_r q) \leq s \rightarrow_r q$ para todo $p, q, s \in Q$.

Com efeito,

$$s \& ((s \rightarrow_r p) \wedge (p \rightarrow_r q)) \leq s \& (s \rightarrow_r p) \& (p \rightarrow_r q) \leq p \& (p \rightarrow_r q) \leq q$$

provando o fato. Assim, seja $x \in |B|_{EB \wedge (p \rightarrow_r q)}$, logo $Ex \leq p \rightarrow_r q$. Seja $s \leq EB$ tal que $s \& Ex \leq p$, logo $Ex \leq s \rightarrow_r p$, donde

$$Ex \leq (s \rightarrow_r p) \wedge (p \rightarrow_r q) \leq s \rightarrow_r q$$

pelo fato acima. Assim, $s \& Ex \leq q$ e então $x \in |B|_p \rightarrow |B|_q$. $\square$

A definição de extensão pode ser utilizada para combinar objetos de diferentes domínios; sintacticamente, corresponde a dar sentido a fórmulas do tipo

$$R(x, y, z) = S(x, y) \vee T(y, z)$$

interpretando $S(x, y)$ e $T(y, z)$ como funções características em $A \times B$ e em $B \times C$, respectivamente. O problema que surge em relação ao caso intuicionista é que a extensão não pode ser feita em ordem arbitrária com relação às operações de sub-prefixes, i.e., em geral

$$(R * T) \times A \neq (R \times A) * (T \times A),$$

onde $*$ é uma operação binária entre sub-prefixes.

Lema 1.2.7 : *Sejam A, B prefixes e $S, T \subseteq B$ sub-prefixes fechados.*

(a) $(S \& T) \times A \supseteq (S \times A) \& (T \times A)$; a igualdade não vale em geral.

(b) $(S \rightarrow T) \times A \subseteq (S \times A) \rightarrow (T \times A)$; a igualdade não vale em geral.

(c) $(S \vee T) \times A \supseteq (S \times A) \vee (T \times A)$; a igualdade não vale em geral.

(d) $(S \wedge T) \times A = (S \times A) \wedge (T \times A)$.

(e) *Seja $P \subseteq A \times B$ sub-prefixe fechado, e C um prefixe. Logo,*

$$\exists a(P \times C) = (\exists a P) \times C, \quad \forall a(P \times C) = (\forall a P) \times C.$$

Demonstração: (a) Por definição,

$$|(S \times A) \& (T \times A)| = \{(s, a)_{|[(s, a) = (t, b)]} : s \in |S|, t \in |T|, a, b \in |A|, Es = Ea, Et = Eb\},$$

$$|(S \& T) \times A| = \{(s_{|[s=t]}, a) : s \in |S|, t \in |T|, a \in |A|, Ea = [s = t]\}.$$

Considere

$$x = (s, a)_{|[s=a]=(t,b)]} = (s_{|[s=t] \& [b=a]}, a_{|[s=t] \& [b=a]}) \in |(S \times A) \& (T \times A)|.$$

Como $[b = a] \leq Eb = Et \leq ET$, então existe $t' = t_{|[b=a]} \in |T|$ tal que $[s = t] \& [b = a] = [s = t']$. Logo, como $a' = a_{|[s=t']} \in |A|$, então $x = (s_{|[s=t']}, a') \in |(S \& T) \times A|$.

Como contraexemplo da igualdade, considere B um prefeixe sobre QS , e

$$S = B_{|p}, \quad T = B_{|q}, \quad A = B_{|r}.$$

Logo, pelo lema 1.2.6 (c),

$$(S \times A) \& (T \times A) = (B \times B)_{|(p \wedge r) \& (q \wedge r)},$$

$$(S \& T) \times A = (B \times B)_{|(p \& q) \wedge r}.$$

Escolhendo $q, r \in QS$ não nulos tais que $q \wedge r = \mathbf{0}$ e $p = \top$, então

$$(p \wedge r) \& (q \wedge r) = r \& \mathbf{0} = \mathbf{0},$$

$$(p \& q) \wedge r = r \wedge (\top \& q) = r \& q = r \neq \mathbf{0}.$$

Observe que sempre temos $(p \wedge r) \& (q \wedge r) \leq p \& q \wedge r$.

(b) Por (a),

$$(S \times A) \& ((S \rightarrow T) \times A) \subseteq (S \& (S \rightarrow T)) \times A \subseteq T \times A$$

donde $(S \rightarrow T) \times A \subseteq (S \times A) \rightarrow (T \times A)$.

Como contraexemplo da igualdade, considere $p, q, r, s \in QS$ diferentes de $\mathbf{0}$ tais que $p, q \leq s$, $p \wedge r = \mathbf{0}$, $s \wedge r \neq \mathbf{0}$, $p \not\leq q$. Logo, $(p \rightarrow_r q) \wedge s \wedge r = \mathbf{0} \neq s \wedge r$. Sejam A e B prefeixes sobre QS com $EA = r$, $EB = s$ e considere $S = B_{|p}$, $T = B_{|q}$. Logo, por 1.2.6 (d),

$$(S \rightarrow T) \times A = (B_{|p} \rightarrow B_{|q}) \times A = B_{|(p \rightarrow_r q) \wedge s} \times A = (B \times A)_{|(p \rightarrow_r q) \wedge s \wedge r},$$

$$(S \times A) \rightarrow (T \times A) = (B \times A)_{|p \wedge r} \rightarrow (B \times A)_{|q \wedge r} = \mathbf{0} \rightarrow (B \times A)_{|q \wedge r} = B \times A$$

donde a inclusão é estrita. Observe que, neste exemplo, $S \rightarrow T = \mathbf{0}_B$, mas $(S \times A) \rightarrow (T \times A) = B \times A$.

(c) Temos que

$$S \times A \subseteq (S \vee T) \times A \text{ e } T \times A \subseteq (S \vee T) \times A \text{ implica } (S \times A) \vee (T \times A) \subseteq (S \vee T) \times A.$$

Como contraexemplo da igualdade, sejam $p, q, r \in QS$ tais que $(p \wedge r) \vee (q \wedge r) < (p \vee q) \wedge r$, sejam A, B prefeixes sobre QS com $EA = r$ e considere $S = B_{|p}$, $T = B_{|q}$.

(d) Temos que

$$(S \cap T) \times A \subseteq S \times A \text{ e } (S \cap T) \times A \subseteq T \times A \text{ implica } (S \cap T) \times A \subseteq (S \times A) \cap (T \times A).$$

Por outro lado, se $(b, a) \in |(S \times A) \cap (T \times A)|$, então $b \in |S \cap T|$, $a \in |A|$ e $Eb = Ea$, donde $(b, a) \in |(S \cap T) \times A|$.

(e) Considere

$$h_{\exists a P}(\vec{x}) = \bigvee_{a \in |A|} h_P(a; \vec{x}), \quad h_{P \times C}(a; \vec{x}; c) = (EP \wedge EC) \& h_P(a; \vec{x}) \& Ec.$$

Sendo $Eh_{\exists a P} = \bigvee_{\vec{x}} \bigvee_a h_P(a; \vec{x}) = EP$, então

$$h_{\exists a(P \times C)}(\vec{x}; c) = \bigvee_a h_{P \times C}(a; \vec{x}; c) = (Eh_{\exists a P} \wedge EC) \& h_{\exists a P}(\vec{x}) \& Ec = h_{(\exists a P) \times C}(\vec{x}; c).$$

Para a segunda parte, considere

$$h_1(b, c) = (EA \wedge EB \wedge EC \wedge \bigwedge_{a \in |A|} (Ea \rightarrow_l (EP \wedge EC) \& [P(a, b)] \& Ec)) \& Eb \& Ec,$$

$$h_2(b, c) = (E\forall a P \wedge EC) \& h_{\forall a P}(b) \& Ec$$

as funções características associadas a $\forall a(P \times C)$ e $(\forall a P) \times C$, respectivamente. Sejam $b \in |B|$ e $c \in |C|$; logo, para todo $a \in |A|$,

$$h_1(b, c) \& Ea \leq (Ea \rightarrow_l (EP \wedge EC) \& [P(a, b)] \& Ec) \& Ea \leq (EP \wedge EC) \& [P(a, b)] \leq [P(a, b)],$$

portanto

$$h_1(b, c) \leq (EA \wedge EB \wedge \bigwedge_{a \in |A|} (Ea \rightarrow_l [P(a, b)])) \& Eb = h_{\forall a P}(b) \leq E\forall a P$$

e então $h_1 \leq h_2$. Por outro lado,

$$A \times (\forall a P) \subseteq P \text{ implica } A \times ((\forall a P) \times C) \subseteq P \times C \text{ implica } (\forall a P) \times C \subseteq \forall a(P \times C). \quad \square$$

Observações 1.2.8 : (1) A operação de extensão de prefeixes não é em geral associativa para operações associativas. Por exemplo, sejam A, B, C e D prefeixes, $P \subseteq A \times B$, $R \subseteq A \times C$, $S \subseteq A \times D$ sub-prefeixes fechados, e considere

$$S_1 = ((P)_{A \times B \times C} \& (R)_{A \times B \times C})_{A \times B \times C \times D} \& (S)_{A \times B \times C \times D},$$

$$S_2 = (P)_{A \times B \times C \times D} \& ((R)_{A \times C \times D} \& (S)_{A \times C \times D})_{A \times B \times C \times D}.$$

Então, em geral $S_1 \neq S_2$.

Com efeito, defina em QS os sub-prefeixes fechados

$$P = (A \times B)_{|p}, \quad R = (A \times C)_{|r}, \quad S = (A \times D)_{|s}.$$

Logo, pelo lema 1.2.6 (c),

$$(P)_{A \times B \times C} \simeq (A \times B \times C)_{|(p \wedge EC)}, \quad (R)_{A \times B \times C} \simeq (A \times B \times C)_{|(r \wedge EB)},$$

$$(P)_{A \times B \times C} \& (R)_{A \times B \times C} \simeq (A \times B \times C)_{|(p \wedge EC) \& (r \wedge EB)},$$

$$((P)_{A \times B \times C} \& (R)_{A \times B \times C})_{A \times B \times C \times D} \simeq (A \times B \times C \times D)_{|((p \wedge EC) \& (r \wedge EB)) \wedge ED},$$

$$(S)_{A \times B \times C \times D} \simeq (A \times B \times C \times D)_{|(s \wedge EB \wedge EC)},$$

$$S_1 \simeq (A \times B \times C \times D)_{|((p \wedge EC) \& (r \wedge EB)) \wedge ED) \& (s \wedge EB \wedge EC)}.$$

Por outro lado,

$$\begin{aligned} (R)_{A \times C \times D} &\simeq (A \times C \times D)_{|(r \wedge ED)}, \quad (S)_{A \times C \times D} \simeq (A \times C \times D)_{|(s \wedge EC)}, \\ ((R)_{A \times C \times D} \& (S)_{A \times C \times D})_{A \times B \times C \times D} &\simeq (A \times B \times C \times D)_{|((r \wedge ED) \& (s \wedge EC)) \wedge EB}, \\ S_2 &\simeq (A \times B \times C \times D)_{|(p \wedge EC \wedge ED) \& (((r \wedge ED) \& (s \wedge EC)) \wedge EB)}. \end{aligned}$$

Logo, $S_1 = S_2$ sse

$$(*) \quad (((p \wedge EC) \& (r \wedge EB)) \wedge ED) \& (s \wedge EB \wedge EC) = (p \wedge EC \wedge ED) \& (((r \wedge ED) \& (s \wedge EC)) \wedge EB).$$

Considere $EA = EB = EC = p = \top$; logo, $(*)$ reduz a

$$(**) \quad ((\top \& r) \wedge ED) \& s = ED \& (r \wedge ED) \& s.$$

Assim, escolhendo $r, s, ED \in QS$ não nulos tais que $r \wedge ED = 0$, a afirmação $(**)$ não será satisfeita em QS , portanto $S_1 \neq S_2$.

(2) Sejam $S, T \subseteq B$ sub-prefeixes fechados e A prefixe tal que $ES \leq EA$. Logo, $S \times A \subseteq T \times A$ implica que $S \subseteq T$. Com efeito, sejam $s \in |S|$ e $a \in |A|$. Logo,

$$(s_{|Es \& Ea}, a_{|Es \& Ea}) \in |S \times A| \subseteq |T \times A|$$

pois $Es \& Ea \leq ES \leq EA$, e logo $s_{|Es \& Ea} \in |T|$ para todo $a \in |A|$. Assim,

$$\begin{aligned} Es &= Es \& EA = Es \& \bigvee_{a \in |A|} Ea = \bigvee_{a \in |A|} (Es \& Ea) \\ &= \bigvee_{a \in |A|} [s_{|Es \& Ea} = s] \leq \bigvee_{t \in |T|} [t = s] \end{aligned}$$

e então $s \in |cl(T)| = |T|$ (usando a definição 1.1.26).

(3) Se $R \subseteq S \subseteq A \times B$, então $\forall a R \subseteq \forall a S$.

Com efeito,

$$A \times (\forall a R) \subseteq R \subseteq S \text{ implica } \forall a R \subseteq \forall a S.$$

(4) Se $R \subseteq S \subseteq A \times B$, então $\exists a R \subseteq \exists a S$.

Com efeito,

$$R \subseteq S \subseteq A \times (\exists a S) \text{ implica } \exists a R \subseteq \exists a S.$$

(5) Se $R \subseteq A \times B$, então $(\forall a) R \subseteq (\exists a) R$.

Com efeito, $A \times (\forall a) R \subseteq R \subseteq A \times (\exists a) R$, e $E((\forall a) R) \leq EA$, donde segue-se o resultado por (2).

□

Estes resultados sugerem o seguinte:

Definição 1.2.9 : Sejam A, A_j^i prefixes ($j = 1, \dots, r_i, i = 1, \dots, n$), $P_i \subseteq A$ ($i = 1, \dots, k$), $Q_i \subseteq A \times \prod_{j=1}^{r_i} A_j^i$ sub-prefeixes fechados ($i = 1, \dots, n$), e $R = R(P_1, \dots, P_k, Q_1, \dots, Q_n) \subseteq A$ um sub-prefeixe fechado construído a partir de $P_1, \dots, P_k, Q_1, \dots, Q_n$ utilizando as operações $\vee, \wedge, \rightarrow, \&, \forall$,

$\exists$, em finitos passos (as quantificações atingindo os Q_i). Dizemos que R é extensível à esquerda com relação a A , se

$$R(P_1 \times A, \dots, P_k \times A, Q_1 \times A, \dots, Q_n \times A) \subseteq R \times A.$$

Analogamente, R é extensível à direita se

$$R(P_1 \times A, \dots, P_k \times A, Q_1 \times A, \dots, Q_n \times A) \supseteq R \times A,$$

onde $R(P_1 \times A, \dots, P_k \times A, Q_1 \times A, \dots, Q_n \times A)$ é construído exatamente como R , com $P_i \times A$ e $Q_j \times A$ no lugar dos P_i e Q_j . Dizemos que R é extensível (com relação a A) se é extensível à direita e à esquerda (com relação a A); se R é extensível (à direita, à esquerda) com relação a A para todo A , dizemos que R é extensível (à direita, à esquerda).

Por simplicidade, vamos escrever $R(P_1, \dots, P_k)$ no lugar de $R(P_1, \dots, P_k, Q_1, \dots, Q_n)$ quando não houver risco de confusão.

Exemplo 1.2.10 : Sejam B, A_1, A_2, A prefeixes, e

$$P_1 \subseteq B \times A_1 \times A_1, \quad P_2 \subseteq B, \quad P_3 \subseteq B \times A_1 \times A_2, \quad P_4 \subseteq B,$$

e defina

$$R = R(P_1, P_2, P_3, P_4) = P_2 \vee (\exists a_1((\exists b_1 P_1) \rightarrow (\forall a_2 P_3)) \& P_4) \subseteq B.$$

Assim, vamos ter

$$R(P_1 \times A, P_2 \times A, P_3 \times A, P_4 \times A) = (P_2 \times A) \vee (\exists a_1((\exists b_1(P_1 \times A)) \rightarrow (\forall a_2(P_3 \times A))) \& (P_4 \times A))$$

sub-prefeixo fechado de $B \times A$. $\square$

Definição 1.2.11 : Com a notação anterior, dizemos que $R(P_1 \times A, \dots, P_n \times A)$, denotado por R_A , é a extensão de R por A .

O objetivo dos P_i na definição 1.2.11 é representar a interpretação das fórmulas atômicas; $R = R(P_1, \dots, P_n)$ representa a interpretação de uma fórmula complexa (obtida das fórmulas atômicas P_i), e a extensão de R por A é a maneira correta de interpretar a imersão de $R \subseteq B$ em $B \times A$, para evitar ambigüedades no sentido da observação 1.2.8 (1). A idéia detrás das definições 1.2.9 é a preservação das relações de inclusão por extensões. Assim, se $R \subseteq T$, e temos que R é extensível à esquerda por A , e T é extensível à direita por A , então

$$R_A \subseteq R \times A \subseteq T \times A \subseteq T_A.$$

1.3 Imagem Inversa de Morfismos

Nesta seção discutiremos a imagem inversa de sub-prefeixos fechados por morfismos, que será utilizada para interpretar a substituição de uma variável por um termo dentro de uma fórmula. A operação de extensão de prefixos que acabamos de estudar é um caso particular de imagem inversa, onde o morfismo é a projeção canônica. Como no caso da extensão, vamos estudar o comportamento da função inversa para as operações lógicas que temos no quantal de sub-prefeixos.

Lema 1.3.1 : *Sejam A, B prefixos sobre Q e $f : |A| \longrightarrow |B|$ morfismo.*

(a) *Se C é prefixo sobre Q e $R \subseteq B \times C$ é sub-prefixo fechado, considere*

$$g = f \times id_C : A \times C \longrightarrow B \times C, \quad g(a, c) = (fa, c).$$

Então,

$$f^*(\forall c R) = \forall c (g^* R); \quad f^*(\exists c R) = \exists c (g^* R).$$

(b) *Sejam $R, S \subseteq B$ sub-prefixos fechados.*

(b.1) *Se $EA \wedge E(R \& S) \leq (EA \wedge ER) \& (EA \wedge ES)$, então*

$$f^*(R \& S) = f^*(R) \& f^*(S).$$

(b.2) *Considere as seguintes condições:*

[V1] $(ER \vee ES) \wedge EA \leq q \wedge r$, onde

$$q = (Ef^*R \vee Ef^*S) \& (ER \wedge EA), \quad r = (Ef^*R \vee Ef^*S) \& (ES \wedge EA);$$

[V2] $ER \vee ES \leq Ef^*R \vee Ef^*S$;

[V3] $((ER \vee ES) \wedge EA) \& ER \leq ER \wedge EA$ e $((ER \vee ES) \wedge EA) \& ES \leq ES \wedge EA$.

Então, se vale alguma das três condições acima, temos que

$$f^*(R \vee S) = f^*(R) \vee f^*(S).$$

(b.3) *A implicação à direita $\rightarrow$ satisfaz*

$$f^*(R \rightarrow S) \subseteq f^*(R) \rightarrow f^*(S).$$

(b.4) *Se $(EB \& EA) \wedge ER \leq EA$, então*

$$f^*(R \rightarrow S) = f^*(R) \rightarrow f^*(S).$$

Demonstração: (a) Seja $(a, c) \in |A \times C|$ tal que $fa \in |\forall cR|$; logo,

$$g(a, c) = (fa, c) \in |(\forall cR) \times C| \subseteq |R|$$

e então $(a, c) \in |g^*R|$. Assim, $f^*(\forall cR) \times C \subseteq g^*R$, donde $f^*(\forall cR) \subseteq \forall c(g^*R)$. Considere agora

$$\begin{aligned} [\forall c(g^*R)](a) &= ((EC \wedge EA) \wedge \bigwedge_{c \in |C|} (Ec \rightarrow_l [g^*R](a, c))) \& Ea \\ &= ((EC \wedge EA) \wedge \bigwedge_{c \in |C|} (Ec \rightarrow_l (EA \wedge ER) \& [R](g(a, c)))) \& Ea, \\ [\forall cR](b) &= ((EC \wedge EB) \wedge \bigwedge_{c \in |C|} (Ec \rightarrow_l [R](b, c))) \& Eb \end{aligned}$$

para todo $a \in |A|$, $b \in |B|$. Seja $a \in |\forall c(g^*R)|$, logo $Ea \leq [\forall c(g^*R)](a)$; provaremos que $E(fa) = Ea \leq [\forall cR](fa)$, i.e., $a \in |f^*(\forall cR)|$. Com efeito,

$$E(fa) = Ea \leq EC \wedge EA \leq EC \wedge EB.$$

Além disso, se $c \in |C|$, então

$$Ea \leq Ec \rightarrow_l (EA \wedge ER) \& [R](g(a, c))$$

donde

$$Ea \& Ec \leq (EA \wedge ER) \& [R](g(a, c)) \leq ER \& [R](fa, c) = [R](fa, c),$$

portanto $E(fa) \leq Ec \rightarrow_l [R](fa, c)$ para todo c , donde

$$E(fa) \leq (EC \wedge EB) \wedge \bigwedge_{c \in |C|} (Ec \rightarrow_l [R](fa, c))$$

e, finalmente, $E(fa) \leq [\forall cR](fa)$.

Com relação a $\exists c$, considere $(a, c) \in |g^*R|$, logo $(fa, c) \in |R| \subseteq |(\exists cR) \times C|$ e então $fa \in |\exists cR|$, i.e., $a \in |f^*(\exists cR)|$, portanto $(a, c) \in |f^*(\exists cR) \times C|$. Assim, $g^*R \subseteq f^*(\exists cR) \times C$, donde

$$\exists c(g^*R) \subseteq f^*(\exists cR).$$

Reciprocamente, como $ER \leq EC \wedge EB \leq EC$, então

$$[\exists c(g^*R)](a) = \bigvee_{c \in |C|} [g^*R](a, c) = (EA \wedge ER) \& \bigvee_{c \in |C|} [R](fa, c)$$

para todo $a \in |A|$. Por outro lado,

$$[\exists cR](fa) = \bigvee_{c \in |C|} [R](fa, c).$$

Assim, seja $a \in |f^*(\exists cR)|$, logo $fa \in |\exists cR|$, donde

$$E(fa) = Ea \leq \bigvee_{c \in |C|} [R](fa, c).$$

Mas $a \in |f^*(\exists cR)|$, logo

$$Ea \leq Ef^*(\exists cR) = E((\exists cR) \wedge Imf) \leq ER, \quad Ea \leq EA$$

e portanto

$$Ea \leq (ER \wedge EA) \& \bigvee_{c \in |C|} [R](fa, c) = [\exists c(g^*R)](a),$$

donde $a \in |\exists c(g^*R)|$, i.e., $f^*(\exists cR) = \exists c(g^*R)$.

(b.1) Dado $a \in |A|$, então, por 1.1.34 (a) e por hipótese,

$$\begin{aligned} [f^*(R \& S)](a) &= (EA \wedge E(R \& S)) \& [R \& S](fa) \\ &\leq (EA \wedge ER) \& (EA \wedge ES) \& [R \& S](fa) \\ &= (EA \wedge ER) \& (EA \wedge ES) \& [R](fa) \& [S](fa) \\ &= ((EA \wedge ER) \& [R](fa)) \& ((EA \wedge ES) \& [S](fa)) \\ &= [f^*R](a) \& [f^*S](a) = [f^*R \& f^*S](a). \end{aligned}$$

(b.2) Assuma que $p \leq q \wedge r$, onde $p = (ER \vee ES) \wedge EA$. Dado $a \in |A|$, então

$$\begin{aligned} [f^*(R \vee S)](a) &= (E(R \vee S) \wedge EA) \& [R \vee S](fa) \\ &= p \& (ER \vee ES) \& ([R](fa) \vee [S](fa)) \\ &= p \& ([R](fa) \vee [S](fa)) \\ &= p \& [R](fa) \vee p \& [S](fa). \end{aligned}$$

Logo, por 1.1.34 (a),

$$\begin{aligned} [f^*(R \vee S)](a) &= p \& [R](fa) \vee p \& [S](fa) \leq q \& [R](fa) \vee r \& [S](fa) \\ &= (Ef^*R \vee Ef^*S) \& ((ER \wedge EA) \& [R](fa) \vee (ES \wedge EA) \& [S](fa)) \\ &= (Ef^*R \vee Ef^*S) \& ([f^*R](a) \vee [f^*S](a)) = [f^*R \vee f^*S](a). \end{aligned}$$

Por outro lado, se $ER \vee ES \leq Ef^*R \vee Ef^*S$, então, por 1.1.34 (a), $ER \leq EA$ e $ES \leq EA$; assim, $p = ER \vee ES$ e

$$\begin{aligned} [f^*(R \vee S)](a) &= (ER \vee ES) \& ([R](fa) \vee [S](fa)) \\ &\leq (Ef^*R \vee Ef^*S) \& ((ER \wedge EA) \& [R](fa) \vee (ES \wedge EA) \& [S](fa)) \\ &= (Ef^*R \vee Ef^*S) \& ([f^*R](a) \vee [f^*S](a)) = [f^*R \vee f^*S](a). \end{aligned}$$

Finalmente, se $p \& ER \leq ER \wedge EA$ e $p \& ES \leq ES \wedge EA$, então:

$$\begin{aligned} [f^*(R \vee S)](a) &= p \& [R](fa) \vee p \& [S](fa) = (p \& ER) \& [R](fa) \vee (p \& ES) \& [S](fa) \\ &\leq (ER \wedge EA) \& [R](fa) \vee (ES \wedge EA) \& [S](fa) = [f^*R](a) \vee [f^*S](a) \\ &\leq (Ef^*R \vee Ef^*S) \& ([f^*R](a) \vee [f^*S](a)) = [f^*R \vee f^*S](a). \end{aligned}$$

(b.3) Por 1.1.27,

$$\mathcal{P} = |f^*R \rightarrow f^*S| = \{x \in |A| : \forall p \leq EA \ (f(x)|_p \in |R| \Rightarrow f(x)|_p \in |S|)\},$$

$$\mathcal{Q} = |f^*(R \rightarrow S)| = \{x \in |A| : \forall q \leq EB \ (f(x)|_q \in |R| \Rightarrow f(x)|_q \in |S|)\}.$$

Seja então $x \in Q$ e $p \leq EA$ tal que $f(x)|_p \in |R|$. Logo, dado que $EA \leq EB$, então $f(x)|_p \in |S|$. Portanto, $x \in P$.

(b.4) Seja $x \in P$ e $q \leq EB$ tal que $f(x)|_q \in |R|$. Logo,

$$p = q \& Ex = E(f(x)|_q) \leq ER,$$

$$p = q \& Ex \leq EB \& EA$$

donde $p \leq (EB \& EA) \wedge ER \leq EA$, por hipótese. Por outro lado,

$$f(x)|_p = f(x)|_{q \& Ex} = f(x|_{Ex})|_q = f(x)|_q.$$

Assim, $p \leq EA$ é tal que $f(x)|_p \in |R|$; logo $f(x)|_p \in |S|$, pois $x \in P$. Portanto, $f(x)|_q = f(x)|_p \in |S|$, donde $x \in Q$. $\square$

Observação 1.3.2 : As três condições exigidas em 1.3.1 (b.2) são independentes. Com efeito:

$[V1] \not\Rightarrow [V2]$, $[V3] \not\Rightarrow [V2]$: Suponha que $ER \vee ES \neq 0 = (ER \vee ES) \wedge EA$. Logo, vale $[V1]$ e $[V3]$. Mas então temos que $Ef^*R \leq ER \wedge EA = 0$ e analogamente com Ef^*S ; assim,

$$ER \vee ES \not\leq Ef^*R \vee Ef^*S = 0.$$

$[V2] \not\Rightarrow [V1]$: Considere $R = 0$ e $ES = Ef^*S \neq 0$. Logo, $Ef^*R = 0$ e vale $[V2]$, mas $ER \wedge EA = 0$, portanto

$$ES = (ER \vee ES) \wedge EA \not\leq (Ef^*R \vee Ef^*S) \& (ER \wedge EA) = 0.$$

$[V1] \not\Rightarrow [V3]$: Em QS , é fácil provar que $Ef^*R = ER \wedge EA$ (se existe $x \in |A|$ tal que $[R](f(x)) \neq 0$). Logo, escolhendo $0 < ER < ES$ e $ES \wedge EA > ER \wedge EA \neq 0$, então $p = (ER \vee ES) \wedge EA = ES \wedge EA$ e vale $[V1]$. Mas $p \& ER = p = ES \wedge EA \not\leq ER \wedge EA$.

$[V3] \not\Rightarrow [V1]$: Suponha que $R = 0$ e $ES \wedge EA \neq 0$. Logo, a condição $[V3]$ é satisfeita, mas

$$ES \wedge EA = (ER \vee ES) \wedge EA \not\leq (Ef^*R \vee Ef^*S) \& (ER \wedge EA) = 0.$$

$[V2] \not\Rightarrow [V3]$: Em QS , suponha que $0 < ER < ES \leq EA$; logo, a condição $[V2]$ é satisfeita, mas $[V3]$ exige ter

$$ES = ((ER \vee ES) \wedge EA) \& ER \leq ER \wedge EA = ER,$$

o qual não é satisfeito.

Definição 1.3.3 : Sejam $R = R(P_1, \dots, P_k, Q_1, \dots, Q_n) \subseteq B$, $f : A \rightarrow B$, onde $P_i \subseteq B$ ($i = 1, \dots, k$) e $Q_j \subseteq B \times B_j$ ($j = 1, \dots, n$), e seja $f_j = f \times id_{B_j}$. Definimos a imagem inversa de R por f como sendo

$$R(f^*) = R(f^*P_1, \dots, f^*P_k, f_1^*Q_1, \dots, f_n^*Q_n) \subseteq A.$$

Observação 1.3.4 : A operação de extensão é um caso particular de imagem inversa. Com efeito, se $R = R(P_1, \dots, P_k, Q_1, \dots, Q_n) \subseteq B$, A é prefeixe e $\pi : B \times A \rightarrow B$ é a projeção canônica, então

$$R_A = R(P_1 \times A, \dots, P_k \times A, Q_1 \times A, \dots, Q_n \times A) = R(\pi^*).$$

Dado que $\pi : B \times A \rightarrow B$, então 1.3.1 (b.4) exige ter

$$(EB \& (EB \wedge EA)) \wedge ER \leq EA \wedge EB$$

para atingir a igualdade $(R \times A) \rightarrow (S \times A) = (R \rightarrow S) \times A$.

Para a operação $\vee$, 1.3.1 (b.2) exige ter, no primeiro caso,

$$(ER \vee ES) \wedge EA \leq ((ER \wedge EA) \vee (ES \wedge EA)) \& (ER \wedge EA),$$

$$(ER \vee ES) \wedge EA \leq ((ER \wedge EA) \vee (ES \wedge EA)) \& (ES \wedge EA)$$

para atingir a igualdade $(R \times A) \vee (S \times A) = (R \vee S) \times A$, enquanto que, no segundo caso, a condição exigida é

$$ER \vee ES \leq (ER \wedge EA) \vee (ES \wedge EA)$$

ou, equivalentemente,

$$ER \vee ES \leq EA. \quad \square$$

Um caso particular importante de projeção é quando $A = \mathbb{1}_p$, i.e., $\pi : B \times \mathbb{1}_p \rightarrow B$. Observe que $a \mapsto (a, Ea)$ é um isomorfismo entre $B|_{EB \wedge p}$ e $B \times \mathbb{1}_p$, de maneira que, via esse isomorfismo, a projeção equivale à imersão $i : B|_{EB \wedge p} \rightarrow B$. Este tipo de projeção (ou imersão) aparecerá na extensão de fórmulas por constantes.

Sob certas condições, a imagem inversa por um morfismo é calculada trivialmente:.

Proposição 1.3.5 : *Sejam A e B prefeixes. Seja $R = R(P_1, \dots, P_k) \subseteq B$ o sub-prefeixe fechado construído conforme a definição 1.2.9. Suponha que todo prefeixe S obtido nos passos intermediários da construção de R , satisfaz $ES \leq EA$. Seja $f : A \rightarrow B$ um morfismo de prefeixes.*

(a) *Se R não tem $\vee$, então $R(f^*) = f^*R$.*

(b) *Se R tem $\vee$ e todo sub-prefeixe $S \vee T$ obtido nos passos intermediários satisfaz $ES \vee ET = Ef^*S \vee Ef^*T$, então $R(f^*) = f^*R$.*

Demonstração: (a) Por indução no número m de passos requeridos para obter R . Se $m = 0$, então $R = P_i$ e vale o resultado por definição.

Se $R = S \wedge T$, ou $R = \forall cS$ ou $R = \exists cS$, vale o resultado por hipótese de indução e 1.1.34, 1.3.1.

Se $R = S \& T$, então $R(f^*) = S(f^*) \& T(f^*) = f^*S \& f^*T$, por hipótese de indução. Por hipótese, $ES, ET \leq EA$, logo $E(S \& T) \leq ES \& ET \leq ES \leq EA$, portanto

$$EA \wedge E(S \& T) = E(S \& T) \leq ES \& ET = (EA \wedge ES) \& (EA \wedge ET)$$

portanto $R(f^*) = f^*S \& f^*T = f^*(S \& T) = f^*R$, por 1.3.1 (b.1).

Se $R = S \rightarrow T$ então, por hipótese de indução,

$$[R(f^*)](a) = [S(f^*) \rightarrow T(f^*)](a) = [f^*S \rightarrow f^*T](a) = EA \& ([f^*S](a) \rightarrow_r [f^*T](a)) \& Ea$$

$$= EA \& ((EA \wedge ES) \& [S](fa) \rightarrow_r (EA \wedge ET) \& [T](fa)) \& Ea = EA \& ([S](fa)) \rightarrow_r [T](fa) \& Ea$$

para todo $a \in |A|$, pois $ES, ET \leq EA$ por hipótese. Por outro lado,

$$\begin{aligned} [f^*R](a) &= [f^*(S \rightarrow T)](a) = (EA \wedge E(S \rightarrow T)) \& [S \rightarrow T](fa) = (EA \& [S \rightarrow T](fa)) \wedge [S \rightarrow T](fa) \\ &= (EA \& ([S](fa) \rightarrow_r [T](fa)) \& Ea) \wedge (EB \& ([S](fa) \rightarrow_r [T](fa)) \& Ea) \\ &= EA \& ([S](fa) \rightarrow_r [T](fa)) \& Ea = [R(f^*)](a) \end{aligned}$$

pois $Efa = Ea$ e $EA \leq EB$.

(b) Só falta considerar na indução o caso $R = S \vee T$. Por hipótese de indução, $S(f^*) = f^*S$ e $ES \leq A$, logo $[f^*S](a) = [S](fa)$, e o mesmo vale para T . Assim,

$$\begin{aligned} [R(f^*)](a) &= [S(f^*) \vee T(f^*)](a) = [f^*S \vee f^*T](a) = (Ef^*S \vee Ef^*T) \& ([S](fa) \vee [T](fa)) \\ &= (ES \vee ET) \& ([S](fa) \vee [T](fa)) = (E(S \vee T) \wedge EA) \& (ES \vee ET) \& ([S](fa) \vee [T](fa)) \\ &= (E(S \vee T) \wedge EA) \& [S \vee T](fa) = [f^*R](a). \quad \square \end{aligned}$$

Corolário 1.3.6 : Nas condições de 1.3.5, suponha que todo S obtido na construção de R , incluindo R , satisfaz $ES \leq A$. Então,

(a) Se R não utiliza $\vee$, então $[R(f^*)](a) = R(fa)$ para todo $a \in |A|$.

(b) Se todo $S \vee T$ obtido nos passos intermediários satisfaz $ES \vee ET = Ef^*S \vee Ef^*T$, então $[R(f^*)](a) = R(fa)$ para todo $a \in |A|$.

Corolário 1.3.7 : Se A é um prefeixe e $R = R(P_1, \dots, P_n)$ é tal que todo prefeixe S , obtido na sua construção a partir de $P_1, \dots, P_n$ satisfaz $ES \leq EA$, então R é extensível com relação a A .

Corolário 1.3.8 : Seja A um prefeixe e $R = R(P_1, \dots, P_n)$ tal que todo prefeixe S obtido nos passos intermediários (incluindo R) satisfaz $ES \leq EA$. Seja h a função característica associada com R_A . Então, $h(\vec{x}; a) = h_R(\vec{x}) \& Ea$ e $Eh = ER$.

1.4 Funções Características como Fórmulas

Vamos considerar agora algumas questões técnicas que serão utilizadas no próximo capítulo, na definição de um cálculo lógico a ser interpretado na categoria $Psh(Q)$. Definiremos a maneira de interpretar o equivalente das fórmulas atômicas e logo daremos a noção de esquema, estabelecendo uma relação entre funções características e fórmulas de primeira ordem. Logo, será definido o valor máximo que pode tomar um esquema, correspondendo ao valor de um teorema. Finalmente, será estudada a imagem inversa de um esquema por um morfismo, correspondendo ao efeito de substituir uma variável por um termo na fórmula associada. Por outro lado, as seções globais de um prefeixe serão a interpretação dos símbolos de constante, justificado pelo seguinte:

Lema 1.4.1 : Seja A um prefeixe sobre Q , e $\mathbf{1}$ o objeto inicial da categoria dos prefeixes sobre Q . Então,

$$\varphi : \text{Hom}(\mathbf{1}_{|EA|}, A) \longrightarrow A(EA), \quad f \mapsto f(EA)$$

é uma bijeção com inversa $s \mapsto f_s$, $f_s(p) = s|_p$.

Demonstração: Seja $\varphi : \text{Hom}(\mathbf{1}_{|EA|}, A) \longrightarrow A(EA)$, $\varphi(f) = f(EA)$. Para $p \in |\mathbf{1}_{|EA|}| = EA^{\leftarrow}$, temos que $p = Ep = Ef(p)$; em particular, $EA = Ef(EA)$, portanto $\varphi(f)$ é uma seção global de A . Se $f, g : \mathbf{1}_{|EA|} \longrightarrow A$ tal que $f(EA) = g(EA)$ então, para todo $p \leq EA$:

$$f(p) = f(EA|_p) = f(EA)|_p = g(EA)|_p = g(EA|_p) = g(p)$$

e assim φ é injetora. Por outro lado, dada $s \in A(EA)$, considere a aplicação $f_s : |\mathbf{1}_{|EA|}| \longrightarrow |A|$, $p \mapsto s|_p$. Temos que $Ef_s(p) = E(s|_p) = p \& Es = p \& EA = p = Ep$. Além disso,

$$[p = q] = p \& q = p \& [s = s] \& q = [s|_p = s|_q] = [f_s(p) = f_s(q)]$$

de onde f_s é morfismo tal que $\varphi(f_s) = f_s(EA) = f_s(Es) = s|_{Es} = s$. $\square$

Lema 1.4.2 : Sejam A, B prefeixes, $a \in |B|$ seção global e $p = EA \wedge EB$. Então

$$f : |A|_p \longrightarrow |B|, \quad f(x) = a|_{Ex}$$

é morfismo de prefeixes.

Demonstração: Se $x \in |A|_p$, então $Ex \leq p \leq EB$, portanto existe $a|_{Ex}$ e a aplicação é bem definida. Sendo $Ea = EB$, as propriedades [mor1] e [mor2] são imediatas. $\square$

Definição 1.4.3 : Sejam $A, A_1, \dots, A_n$ prefeixes e $f_i : A \longrightarrow A_i$ ($i = 1, \dots, n$) morfismos. Definimos $\langle f_1, \dots, f_n \rangle : A \longrightarrow \prod_{i=1}^n A_i$ como sendo o único morfismo f tal que $\pi_i \circ f = f_i$, onde $\pi_i : \prod_{j=1}^n A_j \longrightarrow A_i$ é a projeção canônica ($i = 1, \dots, n$).

As fórmulas atômicas correspondem a certos sub-prefeixes P (ou funções características h_P) “básicos”, fixados de antemão, de maneira que $h_P(\vec{x})$ denota o valor da fórmula atômica $P(\vec{x})$; avaliar $P(f_1(\vec{y}_1), \dots, f_n(\vec{y}_n))$, onde $f_i(\vec{y}_i)$ é um termo substituindo a variável x_i , é avaliar f^*P , onde $f = \langle \vec{f}_1, \dots, \vec{f}_n \rangle$, e $\vec{f}_i$ é o morfismo interpretando f_i . Dado que as variáveis têm tipos, interpretados como prefeixes fixos, então o domínio de f^*P deve ser o produto (em *Set*) dos tipos das variáveis envolvidas. O seguinte resultado sobre extensão do domínio de funções características é enunciado em [MS]:

Lema 1.4.4 : Sejam $A_1, \dots, A_n$ prefeixes sobre Q , $q = \bigwedge_i EA_i$ e $F : |\prod_i A_i| \longrightarrow Q$ função característica definindo um sub-prefeixe fechado $S \subseteq |\prod_i A_i|$. Então, a aplicação

$$G : \prod_i |A_i| \longrightarrow Q, \quad G(\vec{x}) = F(\vec{x}_{|q \& E(\vec{x})})$$

é uma função característica que define o prefeixe S .

Demonstração: Sejam $P = \prod_i |A_i|$, $\vec{x} \in P$. Observe que $q \& E(\vec{x}) \leq q \leq E(A_i)$ para todo $i = 1, \dots, n$, logo existe $x_{i|q \& E(\vec{x})} \in |A_i|$ e

$$E(x_{i|q \& E(\vec{x})}) = q \& E(\vec{x}) \& E x_i = q \& E(\vec{x}),$$

portanto $\vec{x}_{|q \& E(\vec{x})} \in \prod_i A_i$ e a G é bem definida. Logo, usando $[char1]$ para F e $exchange$,

$$\begin{aligned} G(\vec{x}) \& E(\vec{x}) &= (F(\vec{x}_{|q \& E(\vec{x})}) \& E(\vec{x}_{|q \& E(\vec{x})})) \& E(\vec{x}) \\ &= F(\vec{x}_{|q \& E(\vec{x})}) \& E(\vec{x}_{|q \& E(\vec{x})}) = F(\vec{x}_{|q \& E(\vec{x})}) = G(\vec{x}) \leq q \end{aligned}$$

portanto G satisfaz $[char1]$. Se $\vec{x}, \vec{y} \in P$, então

$$\begin{aligned} G(\vec{x}) \& [\vec{x} = \vec{y}] &= F(\vec{x}_{|q \& E(\vec{x})}) \& [\vec{x} = \vec{y}] \& E(\vec{x}) \& E(\vec{y}) \& q \\ &= F(\vec{x}_{|q \& E(\vec{x})}) \& [\vec{x}_{|q \& E(\vec{x})} = \vec{y}_{|q \& E(\vec{y})}] \leq F(\vec{y}_{|q \& E(\vec{y})}) = G(\vec{y}) \end{aligned}$$

portanto G satisfaz $[char2]$. Finalmente, se $\vec{x}, \vec{y} \in P$, então

$$G(\vec{y}) \& G(\vec{x}) = F(\vec{y}_{|q \& E(\vec{y})}) \& F(\vec{x}_{|q \& E(\vec{x})}) \leq F(\vec{x}_{|q \& E(\vec{x})}) = G(\vec{x})$$

e assim G satisfaz $[char3]$, sendo portanto uma função característica definindo um sub-prefeixe fechado $T \subseteq D = \prod_i A_i$. Vamos provar que $T = S$. Primeiro de tudo, é fácil ver que $G|_D = F$. De fato, se $\vec{x} \in D$,

$$\begin{aligned} G(\vec{x}) &= F(\vec{x}_{|q \& E(\vec{x})}) \& E(\vec{x}) = F((\vec{x}_{|q \& E(\vec{x})})_{|E(\vec{x})}) \\ &= F(\vec{x}_{|E(\vec{x}) \& q \& E(\vec{x})}) = F(\vec{x}_{|E(\vec{x})}) = F(\vec{x}). \end{aligned}$$

Assim, temos que

$$S = \{\vec{x} \in D : E(\vec{x}) \leq F(\vec{x})\} = \{\vec{x} \in D : E(\vec{x}) \leq G(\vec{x})\} = T$$

como queríamos provar. $\square$

Corolário 1.4.5 : Sejam A_j ($j = 1, \dots, n$), B_i ($i = 1, \dots, k$) prefeixes sobre Q . Seja $p_j \leq EA_j$ ($j = 1, \dots, n$) e suponha que $f_i : \prod_{j=1}^n (A_j)_{|p_j} \rightarrow B_i$ são morfismos ($i = 1, \dots, k$). Finalmente, seja $F : \prod_{i=1}^k B_i \rightarrow Q$ uma função característica com prefeixe associado T e considere o morfismo

$$f = \langle f_1, \dots, f_k \rangle : \prod_{j=1}^n (A_j)_{|q} \rightarrow \prod_{i=1}^k B_i$$

onde $q = \bigwedge_{j=1}^n p_j$. Então, f^*T tem como função característica associada

$$G : \prod_{j=1}^n |(A_j)_{|p_j}| \rightarrow Q, \quad G(\vec{x}) = (q \wedge ET) \& F(f(\vec{x}_{|q \& E(\vec{x})})).$$

Demonstração: Seja

$$D = \left| \prod_{j=1}^n (A_j)_{|q} \right| = \left| \prod_{j=1}^n (A_j)_{|p_j} \right|.$$

Pela proposição 1.1.34, a função característica de f^*T vem dada por

$$G_1 : D \longrightarrow Q, \quad G_1(\vec{x}) = (q \wedge ET) \& F(f(\vec{x})).$$

Pelo lema 1.4.4, estendemos G_1 a

$$G : \prod_{j=1}^n |(A_j)_{|p_j}| \longrightarrow Q$$

onde

$$G(\vec{x}) = G_1(\vec{x}_{|q \& E(\vec{x})}) = (q \wedge ET) \& F(f(\vec{x}_{|q \& E(\vec{x})}))$$

e o prefeixe definido por G é f^*T , como queríamos provar. $\square$

Exemplos 1.4.6 : (a) Suponha que os A_j têm todos o mesmo extent q .

Nesse caso, dado $\vec{x} \in \prod_j |A_j|$,

$$\begin{aligned} G(\vec{x}) &= (q \wedge ET) \& F(f(\vec{x}_{|q \& E(\vec{x})})) \& E(\vec{x}) \\ &= (q \wedge ET) \& F(f((\vec{x}_{|q \& E(\vec{x})})_{|E(\vec{x})})) \\ &= (q \wedge ET) \& F(f(\vec{x}_{|E(\vec{x})})). \end{aligned}$$

(b) Se os A_j e os B_i têm todos o mesmo extent, então

$$G(\vec{x}) = F(f(\vec{x}_{|E(\vec{x})})).$$

Com efeito, $ET \leq q$, portanto aplicamos a observação anterior e $[char3]$ para F .

(c) Se $F : |\prod_{i=1}^n A_i| \longrightarrow Q$ e $f = id : |\prod_i A_i| \longrightarrow |\prod_i A_i|$, então a G obtida em 1.4.5 é a extensão canônica da F a $\prod_i |A_i|$ do lema 1.4.4. Com efeito, sendo $ET \leq q$, então $G : \prod_{i=1}^n |A_i| \longrightarrow Q$ satisfaz:

$$G(\vec{x}) = (ET \wedge q) \& F(id(\vec{x}_{|q \& E(\vec{x})})) = F(\vec{x}_{|q \& E(\vec{x})}). \quad \square$$

Dado que contamos com uma implicação à direita e temos, para todo prefeixe A , o prefeixe nulo $0 = A_{|0} = \{*\}$, então podemos definir a negação (à direita), como

$$\neg S = S \rightarrow 0 \quad \text{para todo } S \in c\mathcal{P}(A)(EA).$$

Vamos definir o máximo valor que pode tomar uma função característica com uma sintaxe dada. Para isso, vamos primeiro reformular a noção utilizada até agora de prefeixe $R(P_1, \dots, P_k, Q_1, \dots, Q_n)$.

Definição 1.4.7 : Considere em $Psh(Q)$ o seguinte:

(1) Uma família não vazia $\mathbf{T}_0 = \{A_i : i \in I\}$ de prefeixes sobre Q ;

(2) Um conjunto de morfismos $\mathcal{M}_0 \subseteq \cup \{Hom(A, B) : A, B \in PF(\mathbf{T})\}$, sendo $PF(\mathbf{T})$ o conjunto de todos os produtos (em $Psh(Q)$) de seqüências finitas de objetos em $\mathbf{T}$, onde

$$\mathbf{T} = \mathbf{T}_0 \cup \{\mathbf{1}_{|EA_i} : i \in I\};$$

(3) Uma família não vazia de funções características $\mathbf{P} = \{h_j : D_j \rightarrow Q : j \in J\}$ tal que, para todo $j \in J$, D_j é um produto (em (Set)) de uma sequência finita de domínios de objetos em $\mathbf{T}_0$.

Seja $\mathcal{M}_1$ o conjunto de todos os morfismos identidade e as projeções existentes entre objetos de $PF(\mathbf{T})$ e seja $\mathcal{M}$ o mínimo conjunto de morfismos contendo $\mathcal{M}_0 \cup \mathcal{M}_1$ fechado por composição, a operação 1.4.3 e o produto finito de morfismos. Definimos uma estrutura em $Psh(Q)$ como sendo uma tripla $\mathcal{I} = \langle \mathbf{T}, \mathcal{M}, \mathbf{P} \rangle$.

Dada uma estrutura $\mathcal{I}$, podemos definir, a partir das h_j básicas, funções características complexas, denominadas esquemas, utilizando a noção de imagem inversa (por morfismos em $\mathcal{M}$) e as operações descritas na primeira seção. Por uma questão técnica que ficará clara no próximo capítulo após a definição da linguagem da lógica e a noção de interpretação, vamos exigir que o domínio dos esquemas sejam conjuntos da forma $D \doteq \prod_{i=1}^n |(B_i)_{|p_i}|$, com $B_i \in \mathbf{T}_0$, $n \in \mathbb{N}$ e $p_i = EB_i \wedge q_i$, onde q_i é o ínfimo de uma família finita de extents de objetos em $\mathbf{T}_0$. Se $h_j \in \mathbf{P}$, $h_j : D_j \rightarrow Q$, $P_j \in PF(\mathbf{T})$ é o prefeixe correspondente a D_j e $f : \prod_{i=1}^n (B_i)_{|p_i} \rightarrow P_j$ é um morfismo em $\mathcal{M}$, com $B_i \in \mathbf{T}_0$, podemos então calcular f^*h_j ; o domínio desta função característica obtido de $\prod_{i=1}^n (B_i)_{|p_i}$, ainda exigindo que seja da forma “normal” apontada antes, não é unicamente determinado (embora o sub-prefixe associado é o mesmo, pelo corolário 1.4.5), por causa de que podemos ter em $\mathbf{T}_0$ prefeixes da forma $\mathbb{I}_{|EA_i}$; caso contrário, poderíamos associar a cada $P = (\prod_i A_i)_{|p \wedge \bigwedge_i EA_i} \in PF(\mathbf{T})$ um único domínio, da forma $D = \prod_i |(A_i)_{|EA_i \wedge p}|$. Assim, se $P \in PF(\mathbf{T})$, então $DF(P)$ denotará o conjunto de todos os produtos finitos (em (Set)) obtidos de P da forma “normal” definida acima. É claro que todo $D \in DF(P)$ define P (salvo isomorfismos em $Psh(Q)$). Assim,

$$|A_1| \times |(A_2)_{|EA_2 \wedge EA_3}|, |(A_1)_{|EA_1 \wedge EA_2 \wedge EA_3}| \times |(A_2)_{|EA_2 \wedge EA_1}|, |(A_1)_{|EA_1 \wedge EA_3}| \times |(A_2)_{|EA_2 \wedge EA_3}|$$

são alguns dos elementos de $DF(A_1 \times A_2 \times \mathbb{I}_{|EA_3}) = DF((A_1 \times A_2)_{|EA_1 \wedge EA_2 \wedge EA_3})$; no caso em que $\mathbb{I}_{|EA_3} \in \mathbf{T}_0$, então também podemos acrescentar, por exemplo, o domínio $|A_1| \times |A_2| \times |\mathbb{I}_{|EA_3}|$ a $DF((A_1 \times A_2)_{|EA_1 \wedge EA_2 \wedge EA_3})$. Logo, a notação correta seria $DF(P, \mathbf{T}_0)$ mais do que $DF(P)$.

Definição 1.4.8 O conjunto $\mathcal{E}$ dos esquemas de uma estrutura $\mathcal{I}$ é definido da maneira seguinte:

(E1) Se $h_j \in \mathbf{P}$, $h_j : D_j \rightarrow Q$, $P_j \in PF(\mathbf{T})$ é o prefeixe obtido de D_j , $f : P \rightarrow P_j$ é um morfismo em $\mathcal{M}$ e $D \in DF(P)$, seja $(f^*h_j)_D : D \rightarrow Q$ definida como em 1.4.5. Logo, $(f^*h_j)_D \in \mathcal{E}$, formando o conjunto dos esquemas atômicos;

(E2) $\alpha, \beta \in \mathcal{E}$, $Dom \alpha = Dom \beta$ implica que $\alpha * \beta \in \mathcal{E}$ ($*$ = $\&$, $\wedge$, $\vee$, $\rightarrow$);

(E3) $\phi \in \mathcal{E}$ implica que $\neg\phi \in \mathcal{E}$;

(E4) $\phi \in \mathcal{E}$, $\phi : |A|_p \times D \rightarrow Q$, $A \in \mathbf{T}_0$ implica que $(\forall a)\phi, (\exists a)\phi \in \mathcal{E}$, com domínio D ;

(E5) Seja $\phi \in \mathcal{E}$, $\phi : D \rightarrow Q$, $P \in PF(\mathbf{T})$ obtido de D , $f \in \mathcal{M}$, $f : P' \rightarrow P$, e considere $D' \in DF(P')$. Suponha que

$$\phi = \phi(f_1^*h_1, \dots, f_n^*h_n; g_1^*k_1, \dots, g_m^*k_m) : D \rightarrow Q$$

é construído a partir dos esquemas atômicos $f_i^*h_i$ e $g_j^*k_j$, onde $\text{Dom } f_i^*h_i = D$, $\text{Dom } g_j^*k_j = D \times D_j$, sendo que D_j é o produto dos domínios dos prefeixes das variáveis das quantificações em ϕ atingindo $g_j^*k_j$ ($i = 1, \dots, n$; $j = 1, \dots, m$). Logo, se $\lambda_j = f \times \text{id}_{P_j}$, onde $P_j \in PF(\mathbf{T})$ é obtido de D_j , então

$$\phi(f^*) \equiv_{\text{def}} \phi((f_1 \circ f)^*h_1, \dots, (f_n \circ f)^*h_n; (g_1 \circ \lambda_1)^*k_1, \dots, (g_m \circ \lambda_m)^*k_m)$$

é um esquema com domínio D' , onde $(f_i \circ f)^*h_i$ e $(g_j \circ \lambda_j)^*k_j$ são calculados em D' e $D' \times D'_j$, respectivamente; aqui, D'_j é arbitrário, com a única restrição que $D' \times D'_j \in DF(P' \times P_j)$ e de maneira tal de manter consistência com relação às operações que definem ϕ (isto é, se dois esquemas α, β obtidos no processo de formação de ϕ têm o mesmo domínio, de maneira que realizamos uma operação $\alpha * \beta$ no processo, então $\alpha(f \times \text{id}_R)^*$ e $\beta(f \times \text{id}_R)^*$ têm que ser calculados no mesmo domínio).

O número de operações envolvendo a definição do esquema ϕ é chamado de complexidade de ϕ . Os esquemas intermediários obtidos no processo de formação do esquema ϕ (incluindo ϕ) são chamados de sub-esquemas de ϕ . Se $\phi : D \rightarrow Q$ é um esquema e $B \in PF(\mathbf{T})$ é o prefeixe associado a D , diremos que ϕ é um esquema em B .

A noção de estrutura e esquema pode ser dada em termos de sub-prefeixes fechados, dada a proposição 1.1.32. É claro que a definição de esquema é uma formalização de $R(P_1, \dots, P_k, Q_1, \dots, Q_n)$ definido 1.2.9, portanto a notação $\phi(f^*)$ tem que ser interpretada no sentido da definição 1.3.3. De fato, se f^*h é um esquema atômico e g é um morfismo, então é fácil provar que

$$(f^*h)(g^*) = g^*(f^*h) = (f \circ g)^*h,$$

independentemente dos domínios escolhidos para definir as funções características. Com efeito, se $\text{Dom } f^*h = D$, $\text{Dom } g^*(f^*h) = D'$, P e P' são os prefeixes associados a D e D' , respectivamente, $g : P' \rightarrow P$ e $p = EP \geq EP' = q$, então

$$\begin{aligned} F(\vec{x}) &= f^*h(\vec{x}) = (Eh \wedge p) \& h(f(\vec{x}_{|p \& E \vec{x}})), \\ H(\vec{z}) &= (f \circ g)^*h(\vec{z}) = (Eh \wedge q) \& h(f(g(\vec{z}_{|q \& E \vec{z}}))), \\ G(\vec{z}) &= g^*(f^*h)(\vec{z}) = (EF \wedge q) \& F(g(\vec{z}_{|q \& E \vec{z}})) \\ &= (EF \wedge q) \& (Eh \wedge p) \& h(f(g(\vec{z}_{|q \& E \vec{z}})_{|p \& q \& E \vec{z}})) \leq H(\vec{z}), \end{aligned}$$

pois $EF \wedge q \leq Eh \wedge p$. Por outro lado,

$$\begin{aligned} H(\vec{z}) &\leq F(g(\vec{z}_{|q \& E \vec{z}})) \& h(f(g(\vec{z}_{|q \& E \vec{z}}))) \leq EF \& h(f(g(\vec{z}_{|q \& E \vec{z}}))), \\ H(\vec{z}) &\leq q \& h(f(g(\vec{z}_{|q \& E \vec{z}}))), \end{aligned}$$

e então, obtemos que

$$H(\vec{z}) \leq (EF \wedge q) \& h(f(g(\vec{z}_{|q \& E \vec{z}}))) = G(\vec{z}),$$

pois $EF \wedge q = (EF \wedge q) \& (Eh \wedge p)$. De fato, provar que $G = H$ é óbvio, se consideramos os sub-prefeixes associados. Com relação à escolha para o domínio do esquema, a definição da linguagem

da lógica e a noção de interpretação irão determinar de maneira única os domínios dos esquemas interpretando as fórmulas numa estrutura dada. A escolha dos domínios D'_j na cláusula (E5) é irrelevante (e é por isso que a definição é boa), como provaremos a continuação.

Lema 1.4.9 : *Sejam A e A_i prefeixes em $\mathbf{T}_0$, $P = (A \times \prod_{i=1}^n A_i)_{|p} \in PF(\mathbf{T})$ e considere $D_1 = |A| \times \prod_i |(A_i)_{|p_i}|$, $D_2 = |A|_{|q} \times \prod_i |(A_i)_{|p_i}|$ em $DF(P)$. Sejam $h_i : D_i \rightarrow Q$ ($i = 1, 2$) duas funções características definindo o mesmo sub-prefeixe fechado $R \subseteq P$. Então, temos o seguinte:*

(a) $h_1(a, \vec{x}) = h_2(a_{|q}, \vec{x})$ para todo $(a, \vec{x}) \in D_1$.

(b) $(\forall a)h_1 = (\forall a)h_2$ e $(\exists a)h_1 = (\exists a)h_2$.

Demonstração: (a) Pela proposição 1.1.32 (c), temos que, para todo $(a, \vec{x}) \in D_1$,

$$\begin{aligned} h_2(a_{|q}, \vec{x}) &= \bigvee_{(b, \vec{z}) \in R} [b = a_{|q}] \& [\vec{z} = \vec{x}] = (\bigvee_{(b, \vec{z}) \in R} [b = a] \& [\vec{z} = \vec{x}]) \& q \\ &= h_1(a, \vec{x}) \& q = h_1(a, \vec{x}), \end{aligned}$$

pois, por definição, $q \geq p = q \wedge \bigwedge_i p_i \geq E h_1$.

(b) Considere as funções características

$$F_1(\vec{x}) = [(\forall a)h_1](\vec{x}) = (p \wedge \bigwedge_{a \in |A|} (Ea \rightarrow_l h_1(a, \vec{x}))) \& E \vec{x},$$

$$F_2(\vec{x}) = [(\forall a)h_2](\vec{x}) = (p \wedge \bigwedge_{a \in |A|_{|q}} (Ea \rightarrow_l h_2(a, \vec{x}))) \& E \vec{x}.$$

Assim, dado $a \in |A|$ e $\vec{x} \in \prod_i |(A_i)_{|p_i}|$, então $a_{|q} \in |A|_{|q}$, donde, por (a),

$$F_2(\vec{x}) \& Ea \leq (E(a_{|q}) \rightarrow_l h_2(a_{|q}, \vec{x})) \& q \& Ea \leq h_2(a_{|q}, \vec{x}) = h_1(a, \vec{x}),$$

portanto $F_2(\vec{x}) \leq Ea \rightarrow_l h_1(a, \vec{x})$ para todo $a \in |A|$ e então $F_2 \leq F_1$. Por outro lado, se $a \in |A|_{|q}$, então

$$F_1(\vec{x}) \& Ea \leq (Ea \rightarrow_l h_1(a, \vec{x})) \& Ea \leq h_1(a, \vec{x}) = h_2(a_{|q}, \vec{x}) = h_2(a, \vec{x}) \& q = h_2(a, \vec{x})$$

portanto $F_1 \leq F_2$, i.e., $F_1 = F$. A operação $\exists$ é tratada similarmente. $\square$

Exemplo 1.4.10 : (1) Seja $\mathcal{I}$ uma estrutura, $h_1, h_2 \in \mathbf{P}$ e $f, g_a, h \in \mathcal{M}_0$ tais que

$$h_1 : |A_1| \times |A_2| \rightarrow Q, \quad h_2 : |A_4| \times |A_3| \rightarrow Q,$$

$$f : A_5 \times A_6 \rightarrow A_1, \quad g_a : \mathbf{1}_{|EA_2} \rightarrow A_2, \quad h : A_5 \rightarrow A_3.$$

Considere $A_4 \times \mathbf{1}_{|EA_2} \simeq (A_4)_{|EA_4 \wedge EA_2}$ e os morfismos em $\mathcal{M}$

$$\pi : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \rightarrow A_5 \times A_6, \quad (x, y, z) \mapsto (x, y);$$

$$\pi_1 : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \rightarrow \mathbf{1}_{|EA_2}, \quad (x, y, z) \mapsto Ex \text{ (como projeção);}$$

$$g_1 = g_a \circ \pi_1 : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \rightarrow A_2, \quad (x, y, z) \mapsto a_{|Ex}, \text{ onde } a = g_a(EA_2) \text{ (1.4.1);}$$

$$f_1 = \langle f \circ \pi, g_1 \rangle : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \longrightarrow A_1 \times A_2, \quad f_1(x, y, z) = (f(x, y), a_{|Ex});$$

$$\pi_2 : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \longrightarrow (A_4)_{|EA_4 \wedge EA_2}, \quad (x, y, z) \mapsto z;$$

$$\pi_3 : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \longrightarrow A_5, \quad (x, y, z) \mapsto x;$$

$$f_2 = \langle \pi_2, h \circ \pi_3 \rangle : A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2} \longrightarrow (A_4)_{|EA_4 \wedge EA_2} \times A_3, \quad (x, y, z) \mapsto (z, h(x)).$$

Assim, se $D = |(A_5)_{|EA_5 \wedge EA_2}| \times |(A_6)_{|EA_6 \wedge EA_2}| \times |(A_4)_{|EA_4 \wedge EA_2}|$, então

$$f_1^* h_1 : D \longrightarrow Q, \quad [f_1^* h_1](x, y, z) = (Eh_1 \wedge p) \& h_1(f((x, y)_{|r}), a_{|r}),$$

$$f_2^* h_2 : D \longrightarrow Q, \quad [f_2^* h_2](x, y, z) = (Eh_2 \wedge p) \& h_2(z_{|r}, h(x_{|r}))$$

são esquemas atômicos, onde $p = EA_2 \wedge EA_4 \wedge EA_5 \wedge EA_6$ e $r = p \& Ex \& Ey \& Ez$. Assim, $\phi = f_1^* h_1 \vee f_2^* h_2$ é um esquema com domínio D , representando a fórmula $P(f(x, y), a) \vee Q(z, h(x)) = \phi(x, y, z)$, com P e Q símbolos de predicado (como será visto no próximo capítulo). Para calcular o análogo a $\phi[g(x_1, b)/x]$, i.e., a substituição da variável x pelo termo $g(x_1, b)$ em ϕ , suponha que g e b são representados em $\mathcal{I}$ pelos morfismos de $\mathcal{M}_0$

$$g : A_7 \times A_8 \longrightarrow A_5, \quad g_b : \mathbb{I}_{|EA_8} \longrightarrow A_8, \quad b = g_b(EA_8),$$

e sejam (identificando $(A_4)_{|EA_4 \wedge EA_2 \wedge EA_8}$ com $(A_4)_{|EA_4 \wedge EA_2} \times \mathbb{I}_{|EA_8}$)

$$\pi_4 : A_7 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8} \longrightarrow \mathbb{I}_{|EA_8}, \quad (x_1, y, z) \mapsto Ex_1 \text{ (projeção)};$$

$$\pi_5 : A_7 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8} \longrightarrow A_7, \quad (x_1, y, z) \mapsto x_1 \text{ (projeção)};$$

$$\pi_6 : A_7 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8} \longrightarrow A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8}, \quad (x_1, y, z) \mapsto (y, z) \text{ (projeção)};$$

$$\pi_7 : A_7 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8} \longrightarrow (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8}, \quad (x_1, y, z) \mapsto z \text{ (projeção)};$$

$$g_2 = \langle g \circ \langle \pi_5, g_b \circ \pi_4 \rangle, \pi_6 \rangle : A_7 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8} \longrightarrow A_5 \times A_6 \times (A_4)_{|EA_4 \wedge EA_2 \wedge EA_8};$$

logo, $g_2(x_1, y, z) = (g(x_1, b_{|Ex_1}), y, z)$. Portanto, se $D' = |(A_7)_{|EA_7 \wedge q}| \times |(A_6)_{|EA_6 \wedge q}| \times |(A_4)_{|EA_4 \wedge q}|$, onde $q = EA_2 \wedge EA_8$, definimos

$$(f_1 \circ g_2)^* h_1, (f_2 \circ g_2)^* h_2 : D' \longrightarrow Q$$

de maneira que

$$\begin{aligned} \phi(g_2^*) &= (f_1^* h_1 \vee f_2^* h_2)(g_2^*) = (f_1^* h_1)(g_2^*) \vee (f_2^* h_2)(g_2^*) \\ &= g_2^*(f_1^* h_1) \vee g_2^*(f_2^* h_2) = (f_1 \circ g_2)^* h_1 \vee (f_2 \circ g_2)^* h_2 \end{aligned}$$

representa a fórmula $\phi[g(x_1, b)/x]$.

(2) Suponha que $\phi : D \longrightarrow Q$ é dado por

$$\phi(f_1^* h_1, f_2^* h_2, f_3^* h_3) = (\forall x_3)[(\exists x_1)f_1^* h_1 \& (\forall x_2)f_2^* h_2] \wedge (\exists x_4)(\forall x_1)f_3^* h_3,$$

$$f_1^* h_1 : D \times |(A_3)_{|r_3}| \times |(A_1)_{|p_1}|, \quad f_2^* h_2 : D \times |(A_3)_{|p_3}| \times |(A_2)_{|p_2}|,$$

$$f_3^* h_3 : D \times |(A_4)_{|p_4}| \times |(A_1)_{|r_1}|,$$

onde necessariamente $r_3 = p_3$, pela construção da ϕ , isto é: os sub-esquemas $\alpha = (\exists x_1) f_1^* h_1$ e $\beta = (\forall x_2) f_2^* h_2$ de ϕ devem ser calculados no mesmo domínio, para poder construir o sub-esquema $\alpha \& \beta$ de ϕ . Seja P o prefeixe obtido de D , $f : P' \rightarrow P$ em $\mathcal{M}$ e $D' \in DF(P')$. Assim, para calcular $\phi(f^*)$ em D' , devemos considerar a restrição mencionada acima, i.e., se

$$(f_1 \circ \lambda_1)^* h_1 : D' \times |(A_3)_{|s_3}| \times |(A_1)_{|q_1}| \rightarrow Q,$$

$$(f_2 \circ \lambda_2)^* h_2 : D' \times |(A_3)_{|q_3}| \times |(A_2)_{|q_2}| \rightarrow Q,$$

$$(f_3 \circ \lambda_3)^* h_3 : D' \times |(A_4)_{|q_4}| \times |(A_1)_{|s_1}| \rightarrow Q,$$

então, pela construção da ϕ , somos obrigados a considerar $s_3 = q_3$ (arbitrário) para então poder calcular o sub-esquema $\alpha(f \times id_{B_3})^* \& \beta(f \times id_{B_3})^*$ de $\phi(f^*)$, onde $B_3 = (A_3)_{|s_3}$; os outros valores podem ser arbitrários (e independentes) e o resultado de calcular $\phi(f^*)$ com as diferentes escolhas de restrições será o mesmo, pelo lema 1.4.9. $\square$

Suponha agora que $R = \forall a S \subseteq B$; sendo que R é sub-prefeixo de B , estaríamos tentados em pensar que o valor máximo que pode tomar ER é EB ; mas, na realidade, dado que $S \subseteq A \times B$, então $ER = E(\forall a S) \leq E(\forall a (A \times B)) = EA \wedge EB$. Isto motiva a seguinte

Definição 1.4.11 : *Seja ϕ um esquema em B .*

(a) O extent máximo de ϕ é um elemento $\tilde{E}(\phi) \leq EB$ de Q definido por indução na complexidade de ϕ :

(i) ϕ é atômico; logo, $\tilde{E}(\phi) = EB$;

(ii) $\phi = \neg \alpha$; logo, $\tilde{E}(\phi) = EB$;

(iii) $\phi = \alpha \rightarrow \beta$; logo, $\tilde{E}(\phi) = EB$;

(iv) $\phi = \alpha * \beta$, com $*$ = $\wedge, \vee, \&$. Logo, $\tilde{E}(\phi) = \tilde{E}(\alpha) * \tilde{E}(\beta)$;

(iv) $\phi = (Qa)\alpha$, com $Q = \forall, \exists$. Logo, $\tilde{E}(\phi) = \tilde{E}(\alpha)$.

(b) O valor máximo de ϕ é o sub-prefeixo fechado $VM(\phi)$ de B dado por $B_{|\tilde{E}(\phi)}$ ou, equivalentemente, a função característica $x \mapsto \tilde{E}(\phi) \& Ex$.

Exemplo 1.4.12 : Para simplificar a notação, consideremos esquemas como sub-prefeixes; assim, sejam B, A_i prefeixes ($i = 1, 2, 3$) e

$$Q_i \subseteq B \times A_i \ (i = 1, 2, 3), \quad P_i \subseteq B \ (i = 1, 2),$$

$$\phi(P_1, P_2, Q_1, Q_2, Q_3) = (P_1 \wedge P_2) \& ((\exists a_1 Q_1) \vee (\forall a_2 Q_2)) \& (\forall a_3 Q_3).$$

Assim,

$$\tilde{E}(\phi) = (EB \wedge EB) \& (q_1 \vee q_2) \& q_3 = EB \& (q_1 \vee q_2) \& q_3,$$

onde $q_i = EB \wedge EA_i$ ($i = 1, 2, 3$). $\square$

Lema 1.4.13 : *Seja ϕ um esquema em B . Logo, $\phi \subseteq VM(\phi)$.*

Demonstração: Por indução na complexidade de ϕ . Assim, se ϕ é atômico, então o resultado é óbvio. O mesmo vale nos casos $\phi = \neg\alpha$, $\phi = \alpha \rightarrow \beta$.

Se $\phi = \alpha * \beta$, com $*$ = $\vee, \wedge, \&$, então, por hipótese de indução,

$$\alpha \subseteq B_{|\tilde{E}(\alpha)}, \quad \beta \subseteq B_{|\tilde{E}(\beta)},$$

logo, pelo lema 1.2.6, e dado que $*$ é crescente nas duas coordenadas,

$$\phi = \alpha * \beta \subseteq B_{|\tilde{E}(\alpha)} * B_{|\tilde{E}(\beta)} = B_{|\tilde{E}(\alpha) * \tilde{E}(\beta)} = B_{|\tilde{E}(\phi)} = VM(\phi).$$

Se $\phi = (\mathcal{Q}a)\alpha$, com $\mathcal{Q} = \forall, \exists$, então, por hipótese de indução,

$$\alpha \subseteq (A \times B)_{|\tilde{E}(\alpha)} = A \times B_{|\tilde{E}(\alpha)}$$

e então

$$\phi = (\mathcal{Q}a)\alpha \subseteq B_{|\tilde{E}(\alpha)} = B_{|\tilde{E}(\phi)} = VM(\phi). \quad \square$$

Finalmente, estudaremos a relação entre a imagem inversa de um esquema por um morfismo e o cálculo do esquema no morfismo, visando à definição das regras de substituição e de quantificação. Suponha que, dada uma estrutura $\mathcal{I}$, ϕ é um esquema em $P \times B$ (representando uma fórmula) e $g : B \times A \rightarrow P$ é um morfismo (representando um termo); sejam

$$\pi_1 : B \times A \rightarrow B, \quad \pi : (P \times B) \times A \rightarrow P \times B$$

as projeções canônicas, $f = \langle g, \pi_1 \rangle : B \times A \rightarrow P \times B$, $D \in DF(B \times A)$ e $D' = D_1 \times D \in DF(P \times B \times A)$. O problema a ser estudado é o seguinte: sob quais condições vamos ter:

$$[S E] \quad \phi(f^*)(u, v) \leq \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \quad \text{para todo } (u, v) \in D,$$

$$[S =] \quad \phi(f^*)(u, v) = \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \quad \text{para todo } (u, v) \in D,$$

$$[S D] \quad \phi(f^*)(u, v) \geq \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \quad \text{para todo } (u, v) \in D,$$

onde $p = EA \wedge EB = EA \wedge EB \wedge EP$. Observe que $\phi(f^*)$ representa o cálculo de ϕ substituindo a variável de tipo P pelo termo g , enquanto que

$$\phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) = \phi(\pi^*)(g((u, v)_{|p \& Eu \& Ev}), u, v)$$

representa o cálculo de ϕ em g no domínio gerado por todas as variáveis (o fato de calcular f em $(u, v)_{|p \& Eu \& Ev}$ permite que D_1 seja arbitrário para o domínio de $\phi(\pi^*)$). Logo, se ϕ e $f = \langle g, \pi_1 \rangle$ satisfazem $[S E]$, então

$$\phi(f^*)(u, v) \leq \phi(\pi^*)(g((u, v)_{|p \& Eu \& Ev}), u, v) \leq [(\exists x)\phi(\pi^*)](u, v),$$

enquanto que, satisfazendo $[S D]$, vamos ter

$$\phi(f^*)(u, v) \geq \phi(\pi^*)(g((u, v)_{|p \& E u \& E v}), u, v) \geq [(\forall x)\phi(\pi^*)](u, v);$$

essa será a base da definição, no próximo capítulo, das regras de quantificação (e de substituição) de maneira correta.

Definição 1.4.14 : *Com a notação anterior, dizemos que ϕ é consistente (à esquerda, à direita) para f se satisfaz a condição $[S =]$ ($[S E]$, $[S D]$, respectivamente).*

Definição 1.4.15 : *Sejam A , B e P prefeixes, ϕ um esquema em $P \times B$, $f : B \times A \rightarrow P \times B$ um morfismo e $\pi : (P \times B) \times A \rightarrow P \times B$ a projeção canônica, no marco de uma estrutura $\mathcal{I}$.*

(i) *Um sub-esquema $\alpha \vee \beta$ de ϕ em $E \times P \times B$, é (f, ϕ) -consistente se satisfaz*

$$[C1] \quad E\alpha(id_E \times \pi)^* \vee E\beta(id_E \times \pi)^* \leq E\alpha(id_E \times f)^* \vee E\beta(id_E \times f)^*,$$

ou, então, as duas condições seguintes:

$$[C2] \quad E\beta(id_E \times f)^* \& E\alpha(id_E \times f)^* \leq E\alpha(id_E \times f)^*,$$

$$E\alpha(id_E \times f)^* \& E\beta(id_E \times f)^* \leq E\beta(id_E \times f)^*;$$

$$[C3] \quad E\beta(id_E \times \pi)^* \& E\alpha(id_E \times \pi)^* \leq E\alpha(id_E \times \pi)^*,$$

$$E\alpha(id_E \times \pi)^* \& E\beta(id_E \times \pi)^* \leq E\beta(id_E \times \pi)^*;$$

(aqui, E representa o domínio das variáveis das quantificações em ϕ atingindo $\alpha \vee \beta$; observe que o domínio escolhido para calcular as imagens inversas é irrelevante para o cálculo dos extents).

(ii) *Definimos $C_=(f)$ como sendo a classe dos esquemas ϕ em $P \times B$ tais que todo sub-esquema $\alpha \vee \beta$ de ϕ é (f, ϕ) -consistente.*

(iii) *Definimos $C_E(f)$ como sendo a classe dos esquemas ϕ em $P \times B$ tais que para cada sub-esquema $\delta \rightarrow \gamma$ de ϕ e para cada sub-esquema $\alpha \vee \beta$ de δ , temos que $\alpha \vee \beta$ é (f, ϕ) -consistente.*

(iv) *Definimos $C_D(f)$ como sendo a mínima classe de esquemas em $P \times B$ satisfazendo o seguinte:*

$$[CD1] \quad C_=(f) \subseteq C_D(f);$$

$$[CD2] \quad \alpha, \beta \in C_D(f) \text{ e } Dom \alpha = Dom \beta \text{ sse } \alpha * \beta \in C_D(f) \quad (* = \wedge, \&);$$

$$[CD3] \quad \alpha \in C_D(id_E \times f) \text{ sse } (\mathcal{Q}e)\alpha \in C_D(f) \quad (\mathcal{Q} = \forall, \exists);$$

$$[CD4] \quad \alpha, \beta \in C_D(f), Dom \alpha = Dom \beta \text{ e } \alpha \vee \beta \text{ é } (f, \alpha \vee \beta)\text{-consistente sse } \alpha \vee \beta \in C_D(f);$$

$$[CD5] \quad \alpha \in C_E(f), \beta \in C_D(f) \text{ e } Dom \alpha = Dom \beta \text{ sse } \alpha \rightarrow \beta \in C_D(f);$$

$$[CD6] \quad \alpha \in C_E(f) \text{ sse } \neg \alpha \in C_D(f).$$

Observações 1.4.16 : (a) Suponha que ϕ é um esquema em $P \times B$, $f : B \times A \rightarrow P \times B$ é um morfismo e $\alpha \vee \beta$ é um sub-esquema de um sub-esquema δ de ϕ . Se δ é um esquema em

$E \times (P \times B)$ (onde E representa o domínio das quantificações em ϕ atingindo δ), então, $\alpha \vee \beta$ é (f, ϕ) -consistente sse é $(id_E \times f, \delta)$ -consistente.

(b) $C_=(f)$ satisfaz a seguinte propriedade: se $\phi \in C_=(f)$ e δ é um sub-esquema de ϕ , então $\delta \in C_=(id_E \times f)$, onde E representa o domínio das quantificações em ϕ atingindo δ .

(c) $C_E(f)$ satisfaz as seguintes propriedades:

$$\alpha * \beta \in C_E(f) \text{ sse } \alpha, \beta \in C_E(f) \text{ e } Dom \alpha = Dom \beta \quad (* = \wedge, \&, \vee);$$

$$(\mathcal{Q}e)\alpha \in C_E(f) \text{ sse } \alpha \in C_E(id_E \times f) \quad (\mathcal{Q} = \forall, \exists);$$

$$\alpha \rightarrow \beta \in C_E(f) \text{ sse } \alpha \in C_=(f), \beta \in C_E(f) \text{ e } Dom \alpha = Dom \beta; \text{ em particular,}$$

$$\neg \alpha \in C_E(f) \text{ sse } \alpha \in C_=(f).$$

(d) Sejam α e β esquemas em B , com $Dom \alpha = Dom \beta$ e $f : A \rightarrow B$ um morfismo, tal que

$$E\beta(f^*) \& E\alpha(f^*) \leq E\alpha(f^*); \quad E\alpha(f^*) \& E\beta(f^*) \leq E\beta(f^*).$$

Logo, por [char3], temos que

$$\begin{aligned} [\alpha(f^*) \vee \beta(f^*)](a) &= (E\alpha(f^*) \vee E\beta(f^*)) \& (\alpha(f^*)(a) \vee \beta(f^*)(a)) \\ &= (\alpha(f^*)(a) \vee E\beta(f^*) \& E\alpha(f^*) \& \alpha(f^*)(a)) \vee (E\alpha(f^*) \& E\beta(f^*) \& \beta(f^*)(a) \vee \beta(f^*)(a)) \\ &= \alpha(f^*)(a) \vee \beta(f^*)(a) \end{aligned}$$

para todo $a \in D = Dom \alpha(f^*) = Dom \beta(f^*)$. $\square$

Lema 1.4.17 : No contexto de uma estrutura $\mathcal{I}$ dada, sejam A, B e P prefeixes, ϕ um esquema em $P \times B$ e $f : B \times A \rightarrow P \times B$ morfismo. Seja $\pi : (P \times B) \times A \rightarrow P \times B$ a projeção canônica. Fixe domínios $D \in DF(B \times A)$ e $D' = D_1 \times D \in DF(P \times B \times A)$, onde calculamos $\phi(f^*)$ e $\phi(\pi^*)$, respectivamente.

(a) Se $\phi \in C_=(f)$, então ϕ é consistente para f .

(b) Se $\phi \in C_E(f)$, então ϕ é consistente à esquerda para f .

(c) Se $\phi \in C_D(f)$, então ϕ é consistente à direita para f .

Demonstração: Ao longo da prova, $p = EA \wedge EB \wedge EP = EA \wedge EB$.

(a) Por indução na complexidade de ϕ (argumento legitimado pela observação 1.4.16 (b)).

Se ϕ é atômico, então

$$\begin{aligned} \phi(f^*)(u, v) &= f^*(\phi)(u, v) = (p \wedge E\phi) \& \phi(f((u, v)|_{p \& Eu \& Ev})) \\ &= \pi^*(\phi)(f((u, v)|_{p \& Eu \& Ev}), v) = \phi(\pi^*)(f((u, v)|_{p \& Eu \& Ev}), v) \end{aligned}$$

pois $EA \wedge E\phi$, o fator de correção de $\pi^*(\phi)$, coincide com $p \wedge E\phi$.

Assuma o resultado verdadeiro para todo esquema de complexidade $\leq k$, com $0 \leq k$, e seja ϕ um esquema de complexidade $k + 1$.

Se $\phi = \alpha * \beta$, com $*$ = $\wedge$, $\&$, então vale o resultado pela hipótese de indução para α e β e pelo fato de calcular as operações ponto a ponto.

Se $\phi = \alpha \rightarrow \beta$, então, por hipótese de indução,

$$\begin{aligned}\phi(f^*)(u, v) &= p \& (\alpha(f^*)(u, v) \rightarrow_r \beta(f^*)(u, v)) \& Eu \& Ev \\ &= p \& (\alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \rightarrow_r \beta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v)) \& Ef((u, v)_{|p \& Eu \& Ev}) \& Ev \\ &= \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v).\end{aligned}$$

O caso $\phi = \neg \alpha$ é um caso particular do anterior.

Se $\phi = (\mathcal{Q}e)\alpha$, onde $\mathcal{Q} = \forall$ ou $\mathcal{Q} = \exists$ e α é esquema em $P \times E \times B$ com domínio $|E| \times D''$ (sendo que $Dom \phi = D''$ e $E = (A_e)_{|s}$, com $A_e \in \mathbf{T}_0$), considere (salvo isomorfismos na ordem de formação dos produtos em $Psh(Q)$ e em (Set)) os morfismos

$$f_1 = id_E \times f : (E \times B) \times A \longrightarrow P \times (E \times B),$$

$$\pi_1 = id_E \times \pi : (P \times (E \times B)) \times A \longrightarrow P \times (E \times B)$$

e considere $D_2 = |E| \times D \in DF(E \times B \times A)$ e $D_3 = D_1 \times D_2 \in DF(P \times E \times B \times A)$. Logo, salvo isomorfismos na ordem dos argumentos, e por hipótese de indução, temos que, se $q = p \wedge s$, então

$$\begin{aligned}\alpha(f_1^*)(d, b, a) &= \alpha(\pi_1^*)(f_1((d, b, a)_{|q \& Ea \& Ed \& Eb}), a) \\ &= \alpha(\pi_1^*)(d_{|q \& Ea \& Ed \& Eb}, f((b, a)_{|(q \& Ed) \& (p \& Ea \& Eb)}), a) \\ &= \alpha(\pi_1^*)(d, f((b, a)_{|p \& Ea \& Eb})_{|q \& Ed}, a) = \alpha(\pi_1^*)(d, f((b, a)_{|p \& Ea \& Eb}), a) \& q \& Ed \\ &= \alpha(\pi_1^*)(d, f((b, a)_{|p \& Ea \& Eb}), a).\end{aligned}$$

Logo, substituindo a igualdade na expressão correspondente para ϕ , obtemos o resultado.

Se $\phi = \alpha \vee \beta$, então, como $\alpha \vee \beta$ é (f, ϕ) -consistente, por hipótese, suponha que $\alpha \vee \beta$ satisfaz [C1]. Logo, temos que

$$E\alpha(f^*) \vee E\beta(f^*) \geq E\alpha(\pi^*) \vee E\beta(\pi^*).$$

Mas, pela hipótese de indução,

$$\alpha(f^*)(u, v) = \alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \leq E\alpha(\pi^*),$$

portanto, tomando supremo sobre $(u, v) \in D$ (e com o mesmo raciocínio para β), temos que

$$E\alpha(f^*) \leq E\alpha(\pi^*), \quad E\beta(f^*) \leq E\beta(\pi^*),$$

e então

$$E\alpha(f^*) \vee E\beta(f^*) = E\alpha(\pi^*) \vee E\beta(\pi^*).$$

Portanto,

$$\begin{aligned}\phi(f^*)(u, v) &= [\alpha(f^*) \vee \beta(f^*)](u, v) = (E\alpha(f^*) \vee E\beta(f^*)) \& (\alpha(f^*)(u, v) \vee \beta(f^*)(u, v)) \\ &= (E\alpha(\pi^*) \vee E\beta(\pi^*)) \& (\alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \vee \beta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v))\end{aligned}$$

$$= [\alpha(\pi^*) \vee \beta(\pi^*)](f((u, v)_{|p \& Eu \& Ev}), v) = \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v).$$

Por outro lado, se $\alpha \vee \beta$ satisfaz [C2] e [C3], então

$$\begin{aligned} E\beta(f^*) \& E\alpha(f^*) &\leq E\alpha(f^*), & E\alpha(f^*) \& E\beta(f^*) &\leq E\beta(f^*); \\ E\beta(\pi^*) \& E\alpha(\pi^*) &\leq E\alpha(\pi^*), & E\alpha(\pi^*) \& E\beta(\pi^*) &\leq E\beta(\pi^*). \end{aligned}$$

Assim, pela observação 1.4.16 (d) e pela hipótese de indução,

$$\begin{aligned} [\alpha(f^*) \vee \beta(f^*)](u, v) &= \alpha(f^*)(u, v) \vee \beta(f^*)(u, v) \\ &= \alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \vee \beta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \\ &= [\alpha(\pi^*) \vee \beta(\pi^*)](f((u, v)_{|p \& Eu \& Ev}), v). \end{aligned}$$

(b) Assuma como hipótese de indução que $\phi(f^*)(u, v) \leq \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v)$; os casos $\&$, $\wedge$ e os quantificadores são provados como no item anterior e usando a observação 1.4.16 (c).

Se $\phi = \alpha \vee \beta$, observe que, por hipótese de indução e similarmente ao item (a), temos que

$$E\alpha(f^*) \leq E\alpha(\pi^*), \quad E\beta(f^*) \leq E\beta(\pi^*)$$

e então

$$\begin{aligned} \phi(f^*)(u, v) &= [\alpha(f^*) \vee \beta(f^*)](u, v) = (E\alpha(f^*) \vee E\beta(f^*)) \& (\alpha(f^*)(u, v) \vee \beta(f^*)(u, v)) \\ &\leq (E\alpha(\pi^*) \vee E\beta(\pi^*)) \& (\alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \vee \beta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v)) \\ &= [\alpha(\pi^*) \vee \beta(\pi^*)](f((u, v)_{|p \& Eu \& Ev}), v) = \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v). \end{aligned}$$

Se $\phi = \delta \rightarrow \gamma$, temos que $\delta \in C_=(f)$ e $\gamma \in C_E(f)$, pela observação 1.4.16 (c). Portanto, por (a) aplicado a δ ,

$$\delta(f^*)(u, v) = \delta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v)$$

e então, por hipótese de indução para γ ,

$$\begin{aligned} \phi(f^*)(u, v) &= p \& (\delta(f^*)(u, v) \rightarrow_r \gamma(f^*)(u, v)) \& Eu \& Ev \\ &\leq p \& (\delta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \rightarrow_r \gamma(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v)) \& Ef((u, v)_{|p \& Eu \& Ev}) \& Ev \\ &= \phi(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v). \end{aligned}$$

O caso $\phi = \neg \alpha$ é um caso particular do anterior.

(c) Por indução na etapa em que é introduzida ϕ (com relação às regras de formação de $C_D(f)$). Assim, se $\phi \in C_=(f)$, então vale o resultado trivialmente.

Se $\phi = \alpha * \beta$, com $*$ = $\wedge$, $\&$, então vale o resultado, pois estas operações são calculadas ponto a ponto e são crescentes nas duas coordenadas.

Se $\phi = (\mathcal{Q}d)\alpha$, com $\mathcal{Q} = \forall, \exists$, então a prova é análoga à do mesmo caso no item (a) (substituindo a igualdade pela relação “ $\geq$ ” na aplicação da hipótese de indução).

Se $\phi = \alpha \vee \beta$ e ϕ satisfaz [C1], então

$$\alpha(f^*)(u, v) \geq \alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v),$$

$$\beta(f^*)(u, v) \geq \beta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v),$$

$$E\alpha(f^*) \vee E\beta(f^*) \geq E\alpha(\pi^*) \vee E\beta(\pi^*),$$

donde segue-se o resultado. Por outro lado, se ϕ satisfaz [C1] e [C2] então, por 1.4.16 (d) e hipótese de indução,

$$\begin{aligned} [\alpha(f^*) \vee \beta(f^*)](u, v) &= \alpha(f^*)(u, v) \vee \beta(f^*)(u, v) \\ &\geq \alpha(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \vee \beta(\pi^*)(f((u, v)_{|p \& Eu \& Ev}), v) \\ &= [\alpha(\pi^*) \vee \beta(\pi^*)](f((u, v)_{|p \& Eu \& Ev}), v). \end{aligned}$$

Finalmente, se $\phi = \alpha \rightarrow \beta$, ou $\phi = \neg \alpha = \alpha \rightarrow 0$, então $\alpha \in C_E(f)$ e $\beta \in C_D(f)$, por definição; logo, o resultado segue aplicando a hipótese de indução a β , a parte (b) a α e considerando que

$$a \leq a', b \geq b' \text{ implica } a \rightarrow_r b \geq a' \rightarrow_r b' \quad \forall a, a', b, b' \in Q. \quad \square$$

É importante observar que, no caso de Q ser uma cHa, a teoria das funções características simplifica-se consideravelmente:

Corolário 1.4.18 : *Suponha que Q é uma cHa, i.e., $\& = \wedge$ e sejam $\mathcal{I}$ uma estrutura em $Psh(Q)$, ϕ um esquema em $P \times B$ e $f : B \times A \rightarrow P \times B$ um morfismo em $\mathcal{M}$. Logo:*

- (i) $\phi(f^*) = f^*(\phi)$. Em particular, todo esquema é extensível por todo prefeixe A .
- (ii) $\phi \in C_=(f)$. Logo, $\phi(f^*)(u, v) = \phi(f(u, v))$ para todo $(u, v) \in |B \times A|$.

Demonstração: (i) Basta observar que as condições do lema 1.3.1 são satisfeitas para cada uma das operações, substituindo $\&$ por $\wedge$ nos cálculos efetuados em Q . Assim, $R \& S$ coincide com $R \wedge S = R \cap S$ e a condição (b.1) é satisfeita:

$$EA \wedge E(R \wedge S) \leq (EA \wedge ER) \wedge (EA \wedge ES),$$

pois $E(R \wedge S) \leq ER \wedge ES$.

Com relação à operação de supremo, a condição que sempre é verificada em Q é [V3], que agora tem a forma:

$$((ER \vee ES) \wedge EA) \wedge ER \leq ER \wedge EA, \quad ((ER \vee ES) \wedge EA) \wedge ES \leq ES \wedge EA.$$

Finalmente, a implicação à direita (que agora é simplesmente uma implicação) também é respeitada pela imagem inversa: a condição exigida por (b.4) agora tem a forma

$$(EB \wedge EA) \wedge ER \leq EB \wedge EA,$$

condição que é sempre satisfeita.

(ii) Dado um esquema ϕ em $P \times B$ e $\alpha \vee \beta$ um sub-esquema em $E \times P \times B$, então $\alpha \vee \beta$ é (f, ϕ) -consistente para todo morfismo $f : B \times A \rightarrow P \times B$. Com efeito, as condições [C2] e [C3] são sempre satisfeitas, observando que agora elas têm a forma:

$$\begin{aligned}
E\beta(id_E \times f)^* \wedge E\alpha(id_E \times f)^* &\leq E\alpha(id_E \times f)^*, \\
E\alpha(id_E \times f)^* \wedge E\beta(id_E \times f)^* &\leq E\beta(id_E \times f)^*; \\
E\beta(id_E \times \pi)^* \wedge E\alpha(id_E \times \pi)^* &\leq E\alpha(id_E \times \pi)^*, \\
E\alpha(id_E \times \pi)^* \wedge E\beta(id_E \times \pi)^* &\leq E\beta(id_E \times \pi)^*.
\end{aligned}$$

Assim, combinando com (i), obtemos, para todo $(u, v) \in |B \times A|$:

$$\phi(f^*)(u, v) = \phi(\pi^*)(f(u, v), v) = [\pi^*\phi](f(u, v), v) = (EA \wedge E\phi) \wedge \phi(f(u, v)) \wedge Ev = \phi(f(u, v)),$$

pois, agora, $h(x) \leq Ex$ para toda função característica (deduzido de [char1]); logo, por [mor1], $\phi(f(u, v)) \leq Ef(u, v) = Eu = Ev \leq EA \wedge EB$. É claro que $\phi(f^*)(u, v) = \phi(f(u, v))$ poderia ser deduzido utilizando simplesmente o resultado (i) para f . $\square$

O resultado 1.4.18 põe em evidência as diferenças entre feixes sobre quantais e feixes sobre cHa. Neste último caso, a combinação de sub-prefixes de diferentes domínios é feita de maneira natural (correspondendo à combinação de fórmulas com variáveis de diferentes tipos). Logo, não temos interferência alguma entre os diferentes tipos; assim, o fato de ter, por exemplo, $\phi \subseteq \psi$ (como esquemas) implica automaticamente que $\phi_A \subseteq \psi_A$ para todo novo prefixe A . No caso não comutativo, esta última afirmação está longe de ser verdadeira; um esquema em B pode ser nulo (como função característica), mas, para um novo tipo A , a extensão $\phi(\pi^*)$ a $B \times A$ pode produzir $B \times A$, como foi mostrado no lema 1.2.7 (b). De maneira mais geral, o cálculo da imagem inversa por um morfismo funciona nas cHa da maneira esperada: para calcular um esquema ϕ composto com um morfismo f em (u, v) (correspondendo ao cálculo de ϕ substituindo uma variável livre por um termo), basta calcular ϕ no valor $f(u, v)$ produzido pelo morfismo em (u, v) . A situação é bem distinta para quantais: calcular um esquema $\phi = \alpha \rightarrow \beta$ num morfismo $f(u, v)$ pode dar como resultado uma função característica (dos parâmetros (u, v)) que não seja uma implicação à direita. Mais precisamente:

$$h : |B| \times |A| \longrightarrow Q, \quad h(u, v) = [\alpha \rightarrow \beta](f(u, v)_{|p \& Eu \& Ev})$$

não denota uma implicação à direita como sugere a sintaxe de ϕ ; o mesmo fenômeno acontece com a operação de supremo. Desta maneira, fica claro que na generalização ao caso não comutativo, as combinações de fórmulas com tipos diferentes produzem perturbações relevantes no valor das fórmulas envolvidas.

Uma Lógica de Primeira Ordem para Estruturas em $\text{Psh}(\mathcal{Q})$

Neste capítulo será introduzido um sistema lógico de primeira ordem com tipos para representar as operações descritas no capítulo anterior, onde cada tipo t terá associado um prefeixe A_t sobre $\mathcal{Q}$ ($\mathcal{Q}$ fixo), de maneira de interpretar as variáveis e constantes do tipo t como sendo seções de A_t e as fórmulas como sendo funções características (i.e., sub-prefeixes fechados). Assim, uma fórmula $\phi(v_1, \dots, v_n)$ (com variáveis livres $v_1, \dots, v_n$, cada v_i de tipo t_i) será interpretada por uma função característica $h_\phi : \prod_i |(A_{t_i})_{|p_i}| \rightarrow \mathcal{Q}$, i.e., um sub-prefixe fechado $|\phi| \subseteq |\prod_i (A_{t_i})_{|p_i}|$ (a restrição p_i vem das constantes da fórmula). Os sub-prefeixes 2-fechados (tais como os gerados pelas funções $[\cdot = \cdot]$ e $E(\cdot)$) serão considerados via a sua imersão como funções características $\tau \mapsto \omega \& \tau$ (1.1.32 (b)); em princípio, só consideraremos como predicados 2-característicos os dois indicados acima. Os símbolos funcionais representarão morfismos de prefeixes e as constantes (do tipo t) serão seções globais de A_t (e logo, morfismos com imagem em A_t). Na declaração de um símbolo funcional $f : t_1 \times \dots \times t_n \rightarrow t$ na linguagem, deveremos considerar a restrição sobre os modelos relativa aos extents (i.e., $\bigwedge_i EA_{t_i} \leq EA_t$). Desta maneira, uma fórmula $\phi(\alpha_1, \dots, \alpha_n)$ construída a partir das fórmulas atômicas α_i poderá ser identificada com um esquema ϕ numa estrutura (definição 1.4.8), as fórmulas atômicas sendo os esquemas atômicos, uma vez que uma interpretação $\mathcal{I}$ (i.e., uma estrutura) é dada. As regras da lógica serão construídas adaptando o cálculo (*NCLLI*) (com igualdade) do Apêndice I, acrescentando as características de *right-sideness* e idempotência inerentes aos modelos.

2.1 Sintaxe

(a) Linguagem $\mathbb{L}$:

- (a.1) um conjunto (não vazio) de tipos, TIPOS ;
- (a.2) para cada tipo t , um conjunto enumerável $\mathcal{V}_t$ de símbolos de variáveis do tipo t ,

$$\mathcal{V}_t = \{v_n^t : n \in \mathbb{N}\}, \quad \mathcal{V} = \bigcup_{t \in \text{TIPOS}} \mathcal{V}_t;$$

(a.3) para cada tipo t , um conjunto de símbolos de constantes (do tipo t) $\mathcal{C}_t$ (eventualmente $\mathcal{C}_t = \emptyset$), sendo

$$\mathcal{C} = \bigcup_{t \in TIPOS} \mathcal{C}_t;$$

(a.4) um conjunto de símbolos de funções $\mathcal{F}$ (eventualmente $\mathcal{F} = \emptyset$), da forma $\langle f, t_1, \dots, t_n, t \rangle$, onde f é o nome da função, $t_1, \dots, t_n$ são os tipos do domínio de f e t é o tipo do contradomínio de f . Frequentemente escreveremos $f : t_1 \times \dots \times t_n \longrightarrow t$ para denotar $\langle f, t_1, \dots, t_n, t \rangle \in \mathcal{F}$;

(a.5) um conjunto de símbolos de predicados

$$\mathcal{P} = \mathcal{P}_1 \bigcup \{ \langle =_t, 2, t, t \rangle : t \in TIPOS \} \bigcup \{ \langle E_t, 1, t \rangle : t \in TIPOS \}$$

(eventualmente $\mathcal{P}_1 = \emptyset$), da forma $\langle P, n, t_1, \dots, t_n \rangle$, onde P é o nome do predicado, n é a aridade do predicado e $t_1, \dots, t_n$ é a lista dos tipos dos argumentos de P , na ordem dada. Assim, $\langle =_t, 2, t, t \rangle$ indica que o predicado de nome $=_t$ tem dois argumentos, de tipo $t \in TIPOS$;

(a.6) conectivos $\vee, \wedge, \neg, \otimes, \neg$;

(a.7) quantificadores $\forall, \exists$;

(a.8) símbolos especiais $(,), \top$.

(b) Termos de $\mathbb{L}$, $T(\mathbb{L})$:

(b.1) para cada $t \in TIPOS$, $\mathcal{V}_t \cup \mathcal{C}_t \subseteq T(\mathbb{L})$ (termos de tipo t);

(b.2) se $(f : t_1 \times \dots \times t_n \longrightarrow t) \in \mathcal{F}$ e $\tau_1, \dots, \tau_n \in T(\mathbb{L})$, cada τ_i de tipo t_i , então $f(\tau_1, \dots, \tau_n) \in T(\mathbb{L})$ é de tipo t .

(c) Fórmulas de $\mathbb{L}$, $FOR(\mathbb{L})$:

(c.0) $\top \in FOR(\mathbb{L})$;

(c.1) se $\langle P, n, t_1, \dots, t_n \rangle \in \mathcal{P}$ e $\tau_1, \dots, \tau_n \in T(\mathbb{L})$, cada τ_i de tipo t_i , então $P(\tau_1, \dots, \tau_n) \in FOR(\mathbb{L})$, formando (junto com $\top$) o conjunto $ELF(\mathbb{L})$ das fórmulas atômicas;

(c.2) se $\phi, \psi \in FOR(\mathbb{L})$, então $(\phi * \psi) \in FOR(\mathbb{L})$, onde $*$ $\in \{\vee, \wedge, \neg, \otimes\}$;

(c.3) se $\phi \in FOR(\mathbb{L})$, então $(\neg\phi) \in FOR(\mathbb{L})$;

(c.4) se $\phi \in FOR(\mathbb{L})$, $x \in \mathcal{V}$, então $(\forall x)(\phi)$ e $(\exists x)(\phi) \in FOR(\mathbb{L})$.

Definição 2.1.1 : (a) A complexidade de uma fórmula é o número de conectivos e quantificadores que ocorrem na fórmula.

(b) Por recursão, definimos o conjunto $SFE(\phi)$ das subfórmulas estritas de uma fórmula ϕ da maneira seguinte:

Se ϕ é atômica, então $SFE(\phi) = \emptyset$;

Se $\phi = (\alpha * \beta)$, com $*$ $= \wedge, \vee, \neg, \otimes$, então $SFE(\phi) = SFE(\alpha) \cup SFE(\beta) \cup \{\alpha, \beta\}$;

Se $\phi = (\neg\alpha)$, então $SFE(\phi) = SFE(\alpha) \cup \{\alpha\}$;

Se $\phi = (Qv)(\alpha)$, com $Q = \forall, \exists$, então $SFE(\phi) = SFE(\alpha) \cup \{\alpha\}$ (α é o escopo de Q).

(c) O conjunto das subfórmulas de ϕ é $SF(\phi) = SFE(\phi) \cup \{\phi\}$.

Definição 2.1.2 : Uma ocorrência de uma variável x numa fórmula é ligada se estiver dentro de uma subfórmula da forma $(\forall x)(\psi)$, $(\exists x)(\psi)$; quaisquer outra ocorrência é dita livre. Uma fórmula é uma sentença se todas suas (eventuais) variáveis só têm ocorrências ligadas; se $\phi \in FOR(\mathbb{L})$, definimos

$$VAR(\phi) = \{v \in \mathcal{V} : v \text{ ocorre livre em } \phi\};$$

$$CONS(\phi) = \{c \in \mathcal{C} : c \text{ ocorre em } \phi\}.$$

Por definição, $VAR(\top) = CONS(\top) = \emptyset$. Se τ_i é termo do tipo t_i , $x_i \in \mathcal{V}_{t_i}$, $\vec{\tau} = \tau_1, \dots, \tau_n$ e $\vec{x} = x_1, \dots, x_n$, então $\phi[\vec{\tau}/\vec{x}]$ é a fórmula obtida de ϕ substituindo **simultaneamente** todas as (eventuais) ocorrências livres de x_i em ϕ por τ_i . Se τ é termo do tipo t , $v \in \mathcal{V}_t$ e nenhuma variável x de τ ocorre no escopo de um quantificador sobre x em $\phi[\tau/v]$, então dizemos que τ é livre para v em ϕ .

Para simplificar a notação, omitiremos em geral os parênteses externos nas fórmulas $(\alpha * \beta)$, com $*$ $\in \{\wedge, \vee, \&, \neg\}$ e em $(\neg\phi)$; também escreveremos $(Qv)\alpha$ no lugar de $(Qv)(\alpha)$, quando não houver risco de confusão. Além disso, a notação utilizada para $=_t(\tau, \kappa)$ será $(\tau = \kappa)_t$, ou ainda $(\tau = \kappa)$; da mesma maneira, frequentemente escreveremos $E(\tau)$ no lugar de $E_t(\tau)$.

Definição 2.1.3 : Se ϕ é fórmula com $VAR(\phi) = \{x_1, \dots, x_m\}$, então definimos o fecho universal e o fecho existencial de ϕ , denotados respectivamente por $(\forall)\phi$ e $(\exists)\phi$, como sendo

$$(\forall)\phi \equiv_{def} (\forall x_1) \cdots (\forall x_m)\phi,$$

$$(\exists)\phi \equiv_{def} (\exists x_1) \cdots (\exists x_m)\phi,$$

onde, por convenção, $(\forall)\phi = \phi = (\exists)\phi$ se $VAR(\phi) = \emptyset$.

Observação 2.1.4 : A ordem de aplicação dos quantificadores (da mesma classe) deve ser irrelevante (em termos de prova) para que a definição anterior seja boa; isto será provado após a definição das regras da lógica. Por enquanto, podemos assumir que *TIPOS* é um ordinal, de maneira tal que as variáveis são totalmente ordenadas pela ordem lexicográfica. Desta maneira, na definição acima exigimos: se $i < j$, então $x_i < x_j$. $\square$

Definição 2.1.5 : Seja ϕ uma fórmula. Definimos:

$$Etipos(\phi) = \{t \in TIPOS : t \text{ é o tipo de } v \in VAR(\phi) \cup CONS(\phi)\}.$$

Observe que $Etipos(\top) = \emptyset$. A função $Etipos(\phi)$ indica as extensões a serem feitas para interpretar um sequente, pois ela fornece os prefeixes envolvidos no domínio da função característica que resultará da interpretação da fórmula ϕ (não é exatamente o domínio, pois nele poderíamos ter repetições de prefeixes).

2.2 Semântica em $Psh(Q)$

Para que fiquem mais claras as regras da lógica que discutiremos abaixo, introduzimos a noção de interpretação para as fórmulas de uma linguagem $\mathbb{L}$.

Definição 2.2.1 : *Seja $\mathbb{L}$ uma linguagem como descrita acima. Uma interpretação $\mathcal{I}$ para $\mathbb{L}$ consiste no seguinte:*

- (i) *um quantal RSI fixo, Q ;*
- (ii) *para cada $t \in TIPOS$, um prefeixe A_t sobre Q , denotando a igualdade e o extent de A_t por $[\cdot = \cdot]_t$ e $E_t(\cdot)$, respectivamente, exigindo-se o seguinte:*
 - (a) *se $(f : t_1 \times \cdots \times t_n \rightarrow t) \in \mathcal{F}$, então $\bigwedge_{i=1}^n EA_{t_i} \leq EA_t$;*
 - (b) *se $C_t \neq \emptyset$, então $A_t(EA_t) \neq \emptyset$;*
- (iii) *para cada $\langle P, n, t_1, \dots, t_n \rangle \in \mathcal{P}$, uma função característica $h_P : \prod_i |A_{t_i}| \rightarrow Q$, onde, para cada $t \in TIPOS$ e $u, v \in |A_t|$:*

$$h_{=t}(u, v) = EA_t \& [u = v]_t, \quad h_{E_t}(u) = EA_t \& E_t(u);$$

- (iv) *para cada $(f : t_1 \times \cdots \times t_n \rightarrow t) \in \mathcal{F}$, um morfismo de prefeixes $f^{\mathcal{I}} : \prod_i A_{t_i} \rightarrow A_t$;*
- (v) *para cada $c \in C_t$ ($t \in TIPOS$), uma seção global $c^{\mathcal{I}} \in |A_t|$.*

Definição 2.2.2 : *Seja ϕ uma fórmula e $\vec{x}, \vec{a}$ seqüências finitas (eventualmente vazias) de variáveis e constantes diferentes, respectivamente. Dizemos que $C = (\vec{x}; \vec{a})$ é um contexto para ϕ se toda variável livre de ϕ aparece em $\vec{x}$ e toda constante de ϕ ocorre em $\vec{a}$. Se C consiste exatamente nas variáveis livres e constantes de ϕ , então C é o contexto de ϕ , denotado $C(\phi)$; é claro que $C(\phi)$ é único, a menos de permutações. Da mesma maneira, definimos um contexto para um termo τ , $C(\tau)$. Se C e D são dois contextos tais que todas as variáveis e constantes de C ocorrem em D , então escreveremos $C \subseteq D$ (ou $D \supseteq C$). Se C é um contexto e x (a) é uma variável (resp., constante) que não ocorre em C , então escreveremos (x, C) (resp., (C, a)) para denotar o contexto obtido acrescentando-se x (resp., a) a C . Identificaremos dois contextos cujas seqüências respectivas coincidem a menos de permutação.*

Definição 2.2.3 : *Sejam $C = (\vec{x}; \vec{a})$ um contexto, com $\vec{x} = (x_1, \dots, x_n)$ e $\vec{a} = (a_1, \dots, a_m)$, onde $x_i \in \mathcal{V}_{t_i}$ e $a_j \in \mathcal{C}_{s_j}$ ($i = 1, \dots, n$; $j = 1, \dots, m$). Considere $\mathcal{I}$ uma interpretação e $q = \bigwedge_{j=1}^m EA_{s_j}$.*

Definimos o prefeixe associado com C em $\mathcal{I}$, denotado por $P_C^{\mathcal{I}}$, por

$$P_C^{\mathcal{I}} = \prod_{i=1}^n (A_{t_i})_{|p_i} = \prod_{i=1}^n (A_{t_i})_{|p}, \quad .$$

onde $p_i = EA_{t_i} \wedge q$ ($i = 1, \dots, n$) e $p = q \wedge \bigwedge_i EA_{t_i} = \bigwedge_i p_i$. Em particular, se $\vec{x} = \emptyset$ e $\vec{a} \neq \emptyset$, então $P_C^{\mathcal{I}} = \mathbf{1}_{|q|}$; se $\vec{a} = \emptyset$ e $\vec{x} \neq \emptyset$, então $P_C^{\mathcal{I}} = \prod_{i=1}^n A_{t_i}$. Finalmente, se $C = \emptyset$, então $P_C^{\mathcal{I}} = \mathbf{1}$.

Dizemos que o domínio associado com C em $\mathcal{I}$, denotado por $D_C^{\mathcal{I}}$, é o produto (em (Set))

$$D_C^{\mathcal{I}} = \prod_{i=1}^n |(A_{t_i})_{|p_i|}|,$$

com os mesmos casos particulares vistos acima.

Dado que

$$\prod_{i=1}^n A_i \simeq \prod_{i=1}^n A_{\sigma(i)}$$

em $Psh(Q)$ e em (Set) para toda permutação σ de $\{1, \dots, n\}$, então $P_C^{\mathcal{I}}$ e $D_C^{\mathcal{I}}$ estão bem definidos (salvo isomorfismos) com relação à identificação de contextos feita acima (definição 2.2.2).

Uma interpretação vai associar, para cada fórmula ϕ e cada contexto $C = (\vec{x}; \vec{a})$ para ϕ , um sub-prefeixe fechado $|\phi|_C^{\mathcal{I}} \subseteq P_C^{\mathcal{I}}$ ou, equivalentemente, uma função característica $\llbracket \phi \rrbracket_C^{\mathcal{I}} : D_C^{\mathcal{I}} \rightarrow Q$. No caso em que $\vec{x} = \emptyset$, identificaremos, como é usual, a função característica com o seu extant, definindo um valor em Q (o seu valor de verdade). Nos parágrafos seguintes, $\mathcal{I}$ denotará uma interpretação dada, $C = (\vec{x}; \vec{a})$ denotará um contexto (eventualmente vazio) para os termos e fórmulas indicados, com $\vec{x} = (x_1, \dots, x_n)$, $\vec{a} = (a_1, \dots, a_k)$; aqui, x_i é de tipo t_i ($i = 1, \dots, n$), $a_j \in \mathcal{C}_{s_j}$, $q = \bigwedge_j EA_{s_j}$ (ou $q = \top$ se $\vec{a} = \emptyset$), $p_i = q \wedge EA_{t_i}$, $p = q \wedge \bigwedge_i EA_{t_i}$ e $A = P_C^{\mathcal{I}} = \prod_{i=1}^n (A_{t_i})_{|p_i|}$; observe que, se $\vec{x} = \emptyset$, então $A = \mathbf{1}_{|q|}$.

(1) Interpretação de termos:

(i) se $x \in \mathcal{V}$ e $x = x_j$ para algum j , então

$$\llbracket x \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} : A \rightarrow A_{t_j}, \quad \llbracket x \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = u_j;$$

(ii) se $a \in \mathcal{C}_t$, com $a = a_j$ para algum j , definimos (ver lema 1.4.2)

$$\llbracket a \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} : A \rightarrow A_t, \quad \llbracket a \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = a_{|E(\vec{u})}^{\mathcal{I}};$$

(iii) se $f : r_1 \times \dots \times r_k \rightarrow t$, e $\tau_j \in T(\mathbb{L})$ de tipo r_j já foi interpretado como um morfismo $\llbracket \tau_j \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} : A \rightarrow A_{r_j}$, então $\llbracket f(\tau_1, \dots, \tau_k) \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} = f^{\mathcal{I}} \circ \langle \llbracket \tau_1 \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}, \dots, \llbracket \tau_k \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \rangle$, i.e.,

$$\llbracket f(\tau_1, \dots, \tau_k) \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} : A \rightarrow A_t,$$

$$\llbracket f(\tau_1, \dots, \tau_k) \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = f^{\mathcal{I}}(\llbracket \tau_1 \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}), \dots, \llbracket \tau_k \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u})).$$

(2) Interpretação de fórmulas:

Dada $\phi \in FOR(\mathbb{L})$, vamos ter $\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} : \prod_i |(A_{t_i})_{|p_i|}| \rightarrow Q$ função característica, ou $\llbracket \phi \rrbracket_a^{\mathcal{I}} \in Q$ se $\vec{x} = \emptyset$, definida como segue (assumamos primeiro que $\vec{x} \neq \emptyset$):

(a.0) Se $\phi = \top \in ELF(\mathbb{L})$, então

$$\llbracket \top \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = (p \wedge \top) \& E(\vec{u}) = p \& E(\vec{u}).$$

(a.1) Suponha que $\phi \in ELF(\mathbb{L})$ é da forma $\phi = P(\tau_1, \dots, \tau_m)$, onde $\langle P, m, l_1, \dots, l_m \rangle \in \mathcal{P}$ e $\tau_i \in T(\mathbb{L})$ e todas as variáveis e constantes de ϕ ocorrem em C .

Seja A_{l_i} o prefeixe interpretando o tipo l_i ($i = 1, \dots, m$), considere os morfismos

$$f_i = \llbracket \tau_i \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} : A \longrightarrow A_{l_i}, \quad i = 1, \dots, m,$$

e seja $f = \langle f_1, \dots, f_m \rangle : A \longrightarrow \prod_{i=1}^m A_{l_i}$.

Definimos (ver corolário 1.4.5),

$$\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = (p \wedge Eh_P) \& h_P(f(\vec{u}_{|p \& E(\vec{u})})).$$

(a.2) Se $\phi = (\alpha \otimes \beta)$, então

$$\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \& \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}](\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) \& \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u})].$$

(a.3) Se $\phi = (\alpha \wedge \beta)$, então

$$\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \wedge \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}](\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) \wedge \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u})].$$

(a.4) Se $\phi = (\alpha \vee \beta)$, então

$$\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \vee \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}](\vec{u}) = (E[\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \vee E[\llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}] \& ([\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) \vee \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u})]).$$

(a.5) Se $\phi = (\alpha \multimap \beta)$, então

$$\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \rightarrow \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}](\vec{u}) = p \& ([\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) \rightarrow_r \llbracket \beta \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u})] \& E(\vec{u})).$$

(a.6) Se $\phi = \neg \alpha$, então

$$\llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) = [\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}} \rightarrow 0](\vec{u}) = p \& ([\llbracket \alpha \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) \rightarrow_r 0] \& E(\vec{u})).$$

(a.7) Se $\phi = (\forall x)\psi$, com $x \in \mathcal{V}_t$; seja y a primeira variável livre para x em ψ , distinta de todas as variáveis em $\vec{x}$. Então (ver 1.4.9),

$$\begin{aligned} \llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) &= (EA_t \wedge p \wedge \bigwedge_{b \in |A_t|} (Eb \rightarrow_l [\llbracket \psi[y/x] \rrbracket_{(\vec{x}; y); \vec{a}}^{\mathcal{I}}(\vec{u}; b_{|q \wedge EA_t})]) \& E(\vec{u})) \\ &= (EA_t \wedge q \wedge \bigwedge_{b \in |(A_t)_{|q \wedge EA_t}|} (Eb \rightarrow_l [\llbracket \psi[y/x] \rrbracket_{(\vec{x}; y); \vec{a}}^{\mathcal{I}}(\vec{u}; b)]) \& E(\vec{u})). \end{aligned}$$

(a.8) Se $\phi = (\exists x)\psi$, com $x \in \mathcal{V}_t$; seja y a primeira variável livre para x em ψ , distinta de todas as variáveis em $\vec{x}$. Então,

$$\begin{aligned} \llbracket \phi \rrbracket_{\vec{x}; \vec{a}}^{\mathcal{I}}(\vec{u}) &= \bigvee_{b \in |A_t|} \llbracket \psi[y/x] \rrbracket_{(\vec{x}; y); \vec{a}}^{\mathcal{I}}(\vec{u}; b|_{q \wedge EA_t}) \\ &= \bigvee_{b \in |(A_t)|_{q \wedge EA_t}|} \llbracket \psi[y/x] \rrbracket_{(\vec{x}; y); \vec{a}}^{\mathcal{I}}(\vec{u}; b). \end{aligned}$$

No caso em que $\vec{x} = \emptyset$, as definições acima tomam a forma seguinte:

$$(a.0) \quad \llbracket \top \rrbracket_a^{\mathcal{I}} = q \wedge \top = q \in Q;$$

(a.1) Temos $f_i : \mathbb{1}_q \longrightarrow A_{t_i}$ ($i = 1, \dots, m$), $f = \langle f_1, \dots, f_m \rangle : \mathbb{1}_q \longrightarrow \prod_{i=1}^m A_{t_i}$; assim (ver 1.1.34), se T é o prefeixe definido por h_P , então $h_{f \circ T} = F : \mathbb{1}_q \longrightarrow Q$, $F(r) = (q \wedge Eh_P) \& h_P(f(r))$. Definimos

$$\llbracket P(\tau_1, \dots, \tau_m) \rrbracket_a^{\mathcal{I}} = EF = (q \wedge Eh_P) \& h_P(f(q)) \in Q;$$

$$(a.2) \quad \llbracket \alpha \otimes \beta \rrbracket_a^{\mathcal{I}} = \llbracket \alpha \rrbracket_a^{\mathcal{I}} \& \llbracket \beta \rrbracket_a^{\mathcal{I}} \in Q;$$

$$(a.3) \quad \llbracket \alpha \wedge \beta \rrbracket_a^{\mathcal{I}} = \llbracket \alpha \rrbracket_a^{\mathcal{I}} \wedge \llbracket \beta \rrbracket_a^{\mathcal{I}} \in Q;$$

$$(a.4) \quad \llbracket \alpha \vee \beta \rrbracket_a^{\mathcal{I}} = \llbracket \alpha \rrbracket_a^{\mathcal{I}} \vee \llbracket \beta \rrbracket_a^{\mathcal{I}} \in Q;$$

$$(a.5) \quad \llbracket \alpha \multimap \beta \rrbracket_a^{\mathcal{I}} = q \wedge (\llbracket \alpha \rrbracket_a^{\mathcal{I}} \rightarrow_r \llbracket \beta \rrbracket_a^{\mathcal{I}}) = q \& (\llbracket \alpha \rrbracket_a^{\mathcal{I}} \rightarrow_r \llbracket \beta \rrbracket_a^{\mathcal{I}}) \in Q;$$

$$(a.6) \quad \llbracket \neg \alpha \rrbracket_a^{\mathcal{I}} = q \wedge (\llbracket \alpha \rrbracket_a^{\mathcal{I}} \rightarrow_r 0) = q \& (\llbracket \alpha \rrbracket_a^{\mathcal{I}} \rightarrow_r 0) \in Q;$$

$$\begin{aligned} (a.7) \quad \llbracket (\forall x) \psi \rrbracket_a^{\mathcal{I}} &= EA_t \wedge q \wedge \bigwedge_{b \in |A_t|} (Eb \rightarrow_l \llbracket \psi \rrbracket_{x; \vec{a}}^{\mathcal{I}}(b|_{q \wedge EA_t})) \\ &= EA_t \wedge q \wedge \bigwedge_{b \in |(A_t)|_{q \wedge EA_t}|} (Eb \rightarrow_l \llbracket \psi \rrbracket_{x; \vec{a}}^{\mathcal{I}}(b)) \in Q; \end{aligned}$$

$$(a.8) \quad \llbracket (\exists x) \psi \rrbracket_a^{\mathcal{I}} = \bigvee_{b \in |A_t|} \llbracket \psi \rrbracket_{x; \vec{a}}^{\mathcal{I}}(b|_{q \wedge EA_t}) = \bigvee_{b \in |(A_t)|_{q \wedge EA_t}|} \llbracket \psi \rrbracket_{x; \vec{a}}^{\mathcal{I}}(b) \in Q.$$

Observações 2.2.4 : (1) Como a interpretação de uma fórmula atômica (num contexto fixo) produz uma função característica e a interpretação de fórmulas complexas utiliza apenas operações entre funções características, está claro que a interpretação de qualquer fórmula, relativamente a um contexto dado, é uma função característica.

(2) A definição de interpretação de uma fórmula atômica ϕ num contexto $(\vec{x}; \vec{a})$ poderia ter sido a seguinte: interpretar ϕ (segundo (a.1)) no contexto $(\vec{y}; \vec{b})$ das variáveis e constantes de ϕ , obtendo uma função característica

$$F : \prod_{i=1}^m |(A_{t_i})_{q_i}| \longrightarrow Q,$$

e depois, sendo $p = EP_{(\vec{x}; \vec{a})}$, estender ao contexto $(\vec{x}; \vec{a})$ via

$$G : \prod_{i=1}^n |(A_{t_i})_{p_i}| \longrightarrow Q, \quad G(\vec{u}; \vec{v}) = (EF \wedge p) \& F(\vec{u}|_{p \& E(\vec{u}) \& E(\vec{v})}) = (EF \wedge p) \& F(\vec{u}) \& E(\vec{v}).$$

No lema 2.2.5 provaremos que as duas definições coincidem.

(3) Como uma fórmula é construída a partir das fórmulas atômicas utilizando os conectivos e os quantificadores, a noção de interpretação fornece uma ligação entre a sintaxe da lógica e as construções concretas entre sub-prefeixos vistas no capítulo anterior; assim, as fórmulas atômicas

que compõem uma fórmula ϕ são o equivalente aos sub-prefixes fechados $f_i^* h_i$ para o esquema $\phi(f_1^* h_1, \dots, f_n^* h_n)$ da definição 1.4.8. Com efeito, dada uma interpretação $\mathcal{I}$, considere

$$\begin{aligned} \mathbf{T}_0 &= \{A_t : t \in \text{TIPOS}\}; \\ \mathcal{M}_0 &= \{a^{\mathcal{I}} : \mathbb{1}_{|EA_t|} \longrightarrow A_t : a_t \in \mathcal{C}_t, t \in \text{TIPOS}\} \\ &\cup \{f^{\mathcal{I}} : \prod_{i=1}^n A_{t_i} \longrightarrow A_t : \langle f, t_1, \dots, t_n, t \rangle \in \mathcal{F}\}; \\ \mathbf{P} &= \{h_P : P \in \mathcal{P}\}. \end{aligned}$$

Então, $\mathcal{I}$ induz uma estrutura $\langle \mathbf{T}, \mathcal{M}, \mathbf{P} \rangle$, que identificamos com $\mathcal{I}$. Dados ϕ uma fórmula e $C = (\vec{x}; \vec{a})$ um contexto para ϕ , sejam $\psi_1, \dots, \psi_k$ as subfórmulas atômicas de ϕ que não ocorrem no escopo de nenhum quantificador e $h_i = \llbracket \psi_i \rrbracket_C^{\mathcal{I}} : D_C^{\mathcal{I}} \longrightarrow Q$. Sejam $\varphi_1, \dots, \varphi_m$ as fórmulas atômicas de ϕ que ocorrem no escopo de algum quantificador; suponha que φ_i ocorre no escopo de quantificadores em variáveis $x_j^i \in \mathcal{V}_{r_j^i}$ ($j = 1, \dots, d_i$). Sejam $y_j^i \in \mathcal{V}_{r_j^i}$ novas variáveis, livres para x_j^i em φ_i e $p_j^i = q \wedge EA_{r_j^i}$, com $q = EP_{\vec{a}}$. Se definimos

$$g_i = \llbracket \varphi_i[y_1^i/x_1^i] \cdots [y_{d_i}^i/x_{d_i}^i] \rrbracket_{(\vec{x}; y_1^i, \dots, y_{d_i}^i); \vec{a}}^{\mathcal{I}} : D_C^{\mathcal{I}} \times \prod_{j=1}^{d_i} |(A_{r_j^i})_{|p_j^i}| \longrightarrow Q,$$

podemos considerar

$$\llbracket \phi \rrbracket_C^{\mathcal{I}} = \phi(h_1, \dots, h_k, g_1, \dots, g_m) : D_C^{\mathcal{I}} \longrightarrow Q$$

como um esquema ϕ em $P_C^{\mathcal{I}}$ construído a partir dos esquemas atômicos h_i, g_j . Como foi adiantado no capítulo anterior, o domínio dos esquemas numa estrutura $\mathcal{I}$, que interpreta as fórmulas num contexto C , é automaticamente deduzido do contexto de interpretação, sendo sempre da forma $D_C^{\mathcal{I}}$. Dada uma fórmula $\phi(x; \vec{x})$ e um termo τ do tipo de x , se $(x, \vec{x}; \vec{a}) \supseteq C(\phi(x; \vec{x}))$ e $(\vec{y}; \vec{b})$ são as variáveis e constantes em τ não presentes em $(\vec{x}; \vec{a})$, seja $\psi \in SF(\phi)$ atômica, no escopo de um quantificador em $y \in A_t$; na fórmula $\phi[\tau/x]$, ψ será quantificada no domínio $|(A_t)_{|EA_t \wedge p}|$, onde $p = EP_{(\vec{a}; \vec{b})}$. Assim, a exigência de consistência na escolha dos domínios D'_j da condição (E5) da definição 1.4.8 está garantida, sendo inclusive automática. Como observado em (2), a extensão de uma fórmula por novos tipos é feito em nível atômico. Isto corresponde à definição de extensão de prefixes, onde a extensão simples $R \times A$ é feita só no nível dos P_i . $\square$

Daqui em diante, quando não houver risco de confusão, escreveremos $\llbracket \phi \rrbracket_C$ e $\llbracket \tau \rrbracket_C$ no lugar de $\llbracket \phi \rrbracket_C^{\mathcal{I}}$ e $\llbracket \tau \rrbracket_C^{\mathcal{I}}$, para $\phi \in FOR(\mathbb{L})$, $\tau \in T(\mathbb{L})$, C um contexto e $\mathcal{I}$ uma interpretação. Mais ainda, se $C = \emptyset$, escreveremos $\llbracket \phi \rrbracket$ no lugar de $\llbracket \phi \rrbracket_C$. Analogamente, escreveremos P_C e D_C no lugar de $P_C^{\mathcal{I}}$ e $D_C^{\mathcal{I}}$

Lema 2.2.5 : *Sejam $\phi \in FOR(\mathbb{L})$, $C' \supseteq C \supseteq C(\phi)$, $\mathcal{I}$ uma interpretação e $\pi : P_{C'} \longrightarrow P_C$ a projeção. Então, $\llbracket \phi \rrbracket_{C'} = \llbracket \phi \rrbracket_C(\pi^*)$. Em particular, se ϕ é atômica, $C = C(\phi)$, $p = EP_{C'}$, $F = \llbracket \phi \rrbracket_C$ e $H = \llbracket \phi \rrbracket_{C'}$, então $H(\vec{u}; \vec{v}) = (EF \wedge p) \& F(\vec{u}) \& E(\vec{v})$.*

Demonstração: É imediata a partir da definição de interpretação, da observação 2.2.4 (3) e do fato de ter $g^*(f^*h) = (f \circ g)^*h$, para toda função característica h e morfismos f, g . $\square$

Exemplos 2.2.6 : (1) Sejam a, b, c símbolos de constantes diferentes, x, y, z, w variáveis diferentes, sendo x de tipo t_x , a de tipo t_a etc., com $t_x = t_z = t_c$ e considere

$$\langle g, t_x, t_x, t \rangle, \langle f, t, t_a, t_1 \rangle \in \mathcal{F}; \quad \langle P, 4, t_1, t, t_y, t_x \rangle \in \mathcal{P}_1.$$

Seja $C = (x, y, z, w; a, b, c)$, $p = EP_C$ numa interpretação $\mathcal{I}$, $q = EA_a \wedge EA_b \wedge EA_c$ e

$$p_x = EA_x \wedge q, \quad p_y = EA_y \wedge q, \quad p_z = EA_z \wedge q, \quad p_w = EA_w \wedge q,$$

$$\vec{u} = (u_1, u_2, u_3, u_4) \in D_C = |(A_{t_x})_{|p_x}| \times |(A_{t_y})_{|p_y}| \times |(A_{t_z})_{|p_z}| \times |(A_{t_w})_{|p_w}|.$$

Assim, se $\vec{v} = \vec{u}_{|p \& E(\vec{u})}$ e $r = E(\vec{v}) = p \& E(\vec{u})$, então

$$\begin{aligned} F(\vec{u}) &= \llbracket P(f(g(x, c), a), g(z, x), y, x) \rrbracket_C(\vec{u}) \\ &= (p \wedge Eh_P) \& h_P(f^{\mathcal{I}}(\llbracket g(x, c) \rrbracket_C(\vec{v}), \llbracket a \rrbracket_C(\vec{v})), g^{\mathcal{I}}(\llbracket z \rrbracket_C(\vec{v}), \llbracket x \rrbracket_C(\vec{v})), \llbracket y \rrbracket_C(\vec{v}), \llbracket x \rrbracket_C(\vec{v})) \\ &= (p \wedge Eh_P) \& h_P(f^{\mathcal{I}}(g^{\mathcal{I}}(\llbracket x \rrbracket_C(\vec{v}), \llbracket c \rrbracket_C(\vec{v})), a_{|r}^{\mathcal{I}}), g^{\mathcal{I}}(u_{3|r}, u_{1|r}), u_{2|r}, u_{1|r}) \\ &= (p \wedge Eh_P) \& h_P(f^{\mathcal{I}}(g^{\mathcal{I}}(u_{1|r}, c_{|r}^{\mathcal{I}}), a_{|r}^{\mathcal{I}}), g^{\mathcal{I}}(u_{3|r}, u_{1|r}), u_{2|r}, u_{1|r}) = [f_1^* h_P](\vec{u}), \end{aligned}$$

sendo que

$$f_1 : P_C \longrightarrow A_{t_1} \times A_t \times A_{t_y} \times A_{t_x}, \quad (u_1, u_2, u_3, u_4) \mapsto (f^{\mathcal{I}}(g^{\mathcal{I}}(u_1, c_{|Eu_1}^{\mathcal{I}}), a_{|Eu_1}^{\mathcal{I}}), g^{\mathcal{I}}(u_3, u_1), u_2, u_1).$$

(2) Sejam a, b, c símbolos de constantes diferentes e

$$\langle f, t_a, t_1 \rangle, \langle g, t_a, t_c, t_2 \rangle \in \mathcal{F}, \quad \langle P, 3, t_1, t_2, t_b \rangle \in \mathcal{P}_1.$$

Então, dada $\mathcal{I}$, sendo $p = EA_{t_a} \wedge EA_{t_b} \wedge EA_{t_c}$ e $\vec{a} = (a, b, c)$, obtemos

$$\begin{aligned} \llbracket P(f(a), g(a, c), b) \rrbracket_{\vec{a}} &= (p \wedge Eh_P) \& h_P(f^{\mathcal{I}}(a_{|p}^{\mathcal{I}}, g^{\mathcal{I}}(a_{|p}^{\mathcal{I}}, c_{|p}^{\mathcal{I}}), b_{|p}^{\mathcal{I}})) \\ &= (p \wedge Eh_P) \& h_P(f^{\mathcal{I}}(a^{\mathcal{I}}), g^{\mathcal{I}}(a_{|p}^{\mathcal{I}}, c_{|p}^{\mathcal{I}}), b^{\mathcal{I}}) = q \in Q. \end{aligned}$$

Portanto, se $(\vec{x}; \vec{b})$ é um contexto tal que $\vec{a} \cap \vec{b} = \emptyset$, $C = (\vec{x}; \vec{a}, \vec{b})$ e $s = EP_C$, então, por 2.2.5,

$$\llbracket P(f(a), g(a, c), b) \rrbracket_C(\vec{u}) = (q \wedge s) \& E(\vec{u}).$$

Na estrutura $\mathcal{I}$, o cálculo é realizado da maneira seguinte:

$$f_1 : \mathbb{I}_{|p} \longrightarrow A_{t_1} \times A_{t_2} \times A_{t_b}, \quad r \mapsto (f^{\mathcal{I}}(a_{|r}^{\mathcal{I}}, g^{\mathcal{I}}(a_{|r}^{\mathcal{I}}, c_{|r}^{\mathcal{I}}), b_{|r}^{\mathcal{I}}),$$

$$f_1^* h_P : \mathbb{I}_{|p} \longrightarrow Q, \quad r \mapsto (p \wedge Eh_P) \& h_P(f^{\mathcal{I}}(a_{|r}^{\mathcal{I}}, g^{\mathcal{I}}(a_{|r}^{\mathcal{I}}, c_{|r}^{\mathcal{I}}), b_{|r}^{\mathcal{I}}))$$

tal que $E f_1^* h_P = [f_1^* h_P](p) = q$. Logo, Se $\pi : P_C \longrightarrow \mathbb{I}_{|p}$ é a projeção, então

$$\begin{aligned} \pi^*(f_1^* h_P)(\vec{u}) &= (q \wedge s) \& [f_1^* h_P](\pi(\vec{u}_{|s \& E \vec{u}})) = (q \wedge s) \& [f_1^* h_P](s \& E \vec{u}) \\ &= (q \wedge s) \& [f_1^* h_P]((s \& E \vec{u}) \& p) = (q \wedge s) \& [f_1^* h_P](p_{|s \& E \vec{u}}) \\ &= (q \wedge s) \& [f_1^* h_P](p) \& s \& E \vec{u} = (q \wedge s) \& q \& s \& E \vec{u} = (q \wedge s) \& E \vec{u}. \end{aligned}$$

Estas são alternativas ao cálculo direto, utilizando a noção de interpretação:

$$f_2 : P_C \longrightarrow A_{t_1} \times A_{t_2} \times A_{t_b}, \quad \vec{u} \mapsto (f^{\mathcal{I}}(a_{|E \vec{u}}^{\mathcal{I}}, g^{\mathcal{I}}(a_{|E \vec{u}}^{\mathcal{I}}, c_{|E \vec{u}}^{\mathcal{I}}), b_{|E \vec{u}}^{\mathcal{I}}),$$

$$f_2^* h_P : D_C \longrightarrow Q, \quad \vec{u} \mapsto (s \wedge Eh_P) \& h_P(f^{\mathcal{I}}(a_{|s \& E\vec{u}}^{\mathcal{I}}), g^{\mathcal{I}}(a_{|s \& E\vec{u}}^{\mathcal{I}}, c_{|s \& E\vec{u}}^{\mathcal{I}}), b_{|s \& E\vec{u}}^{\mathcal{I}}).$$

(3) Seja ϕ fórmula, $x \in \mathcal{V}_t$, $\vec{a}$ uma sequência finita de constantes diferentes e seja $\vec{x}$ uma sequência finita de variáveis diferentes e distintas de x ; note que $C = ((\vec{x}, x); \vec{a})$ é um contexto para ϕ . Dada uma interpretação $\mathcal{I}$, com $p = EP_{(\vec{x}; \vec{a})}$, então, pela cláusula (a.1) da definição de interpretação de fórmulas, obtemos

$$F(u) = \llbracket Ex \rrbracket_x(u) = EA_t \& E(u)$$

para todo $u \in |A_t|$ e $EF = EA_t$. Portanto, pelo lema 2.2.5,

$$\llbracket Ex \rrbracket_C(\vec{u}; u) = (p \wedge EA_t) \& (EA_t \& Eu) \& E(\vec{u}) = (p \wedge EA_t) \& Eu \& E(\vec{u})$$

para todo $(\vec{u}, u) \in D_C$. Assim,

$$\begin{aligned} \llbracket \phi \otimes Ex \rrbracket_C(\vec{u}; u) &= \llbracket \phi \rrbracket_C(\vec{u}; u) \& \llbracket Ex \rrbracket_C(\vec{u}; u) \\ &= \llbracket \phi \rrbracket_C(\vec{u}; u) \& (p \wedge EA_t) \& E(\vec{u}) \& Eu = \llbracket \phi \rrbracket_C(\vec{u}; u), \end{aligned}$$

por $[char1]$ aplicado a $\llbracket \phi \rrbracket_C$.

(4) Sejam $x \in \mathcal{V}_s$, $y \in \mathcal{V}_t$, $f : t \longrightarrow s$ em $\mathcal{F}$. Logo, dada $\mathcal{I}$, então $EA_t \leq EA_s$, donde

$$\begin{aligned} \llbracket (x = f(y)) \rrbracket_{(x,y)}(x_1, y_1) &= (EA_t \wedge EA_s) \& EA_s \& [x_1 = f^{\mathcal{I}}(y_1)]_s \\ &= EA_t \& [x_1 = f^{\mathcal{I}}(y_1)]_s \end{aligned}$$

para todo $x_1 \in |A_s|$ e $y_1 \in |A_t|$. Seja $R \subseteq |A_s \times A_t|$ o sub-prefixe associado. Seja $(a, b) \in |A_s \times A_t|$ tal que $E_s a = E_t b \leq EA_t \& [a = f^{\mathcal{I}}(b)]_s$; então,

$$\begin{aligned} E_s a &= E_t b \& E_s a \leq E_t b \& EA_t \& [a = f^{\mathcal{I}}(b)]_s \\ &= E_t b \& [a = f^{\mathcal{I}}(b)]_s = [f^{\mathcal{I}}(b) = a]_s \end{aligned}$$

donde, por $[EXT]$, $a = f^{\mathcal{I}}(b)$. Reciprocamente, se $a = f^{\mathcal{I}}(b)$, é claro que

$$E_s a = E_t b \leq EA_t \& [a = f^{\mathcal{I}}(b)]_s$$

e então

$$R = \{(a, b) : E_s a = E_t b \leq EA_t \& [a = f^{\mathcal{I}}(b)]_s\} = \{(a, b) : a = f^{\mathcal{I}}(b)\} = \{(f^{\mathcal{I}}(b), b) : b \in A_t\}.$$

Assim, $\llbracket (x = f(y)) \rrbracket_{(x,y)}$ representa o monomorfismo

$$\langle f^{\mathcal{I}}, id \rangle : A_t \longrightarrow A_s \times A_t,$$

i.e., o gráfico de $f^{\mathcal{I}}$, análogo à [MR], pag. 83.

(5) Sejam $x \in \mathcal{V}_s$, $y \in \mathcal{V}_t$, $f : t \longrightarrow s$ em $\mathcal{F}$. Dada $\mathcal{I}$, (4) nos fornece

$$\llbracket (x = f(y)) \rrbracket_{(x,y)}(x_1, y_1) = EA_t \& [x_1 = f^{\mathcal{I}}(y_1)]_s$$

para todo $x_1 \in |A_s|$ e $y_1 \in |A_t|$, portanto

$$\llbracket (\exists y)(x = f(y)) \rrbracket_x(x_1) = \bigvee_{y_1 \in |A_t|} \llbracket (x = f(y)) \rrbracket_{(x,y)}(x_1, y_1)$$

$$= \bigvee_{y_1 \in |A_t|} EA_t \& [x_1 = f^{\mathcal{I}}(y_1)]_s = EA_t \& \bigvee_{y_1 \in |A_t|} [x_1 = f^{\mathcal{I}}(y_1)]_s.$$

Assim,

$$\llbracket (\forall x)(\exists y)(x = f(y)) \rrbracket = EA_s \wedge \bigwedge_{x_1 \in |A_s|} (Ex_1 \rightarrow_l (EA_t \& \bigvee_{y_1 \in |A_t|} [x_1 = f^{\mathcal{I}}(y_1)]_s)).$$

(6) Sejam $g : r \rightarrow s$, $f : s \rightarrow t$ e $h : r \rightarrow t$ em $\mathcal{F}$ e $x \in \mathcal{V}_r$. Como $EA_r \leq EA_t$,

$$\begin{aligned} \llbracket (f(g(x)) = h(x)) \rrbracket_x(a) &= (EA_r \wedge EA_t) \& EA_t \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t \\ &= EA_r \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t \end{aligned}$$

para todo $a \in |A_r|$. Seja $R \subseteq A_r$ o sub-prefixe gerado e seja $a \in |A_r|$ tal que

$$E_r a \leq EA_r \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t;$$

então, $E_r a = E_r a \& E_r a \leq E_r a \& EA_r \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t$

$$= E_r a \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t = [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t$$

donde, por $[EXT]$, $f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)$. Reciprocamente,

$$f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)$$

implica

$$E_r a \leq [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t$$

e então

$$E_r a = E_r a \& E_r a \leq EA_r \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t.$$

Assim,

$$R = \{a \in |A_r| : E_r a \leq EA_r \& [f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)]_t\} = \{a \in |A_r| : f^{\mathcal{I}}(g^{\mathcal{I}}(a)) = h^{\mathcal{I}}(a)\},$$

i.e., $(R, i) = eq(f^{\mathcal{I}} \circ g^{\mathcal{I}}, h^{\mathcal{I}})$ em $Psh(Q)$, onde $i : R \rightarrow |A_t|$ é o morfismo de inclusão. Isto é análogo ao encontrado em $[MR]$, pag. 83. $\square$

Para determinar se uma fórmula é válida, devemos calcular o valor máximo que a função característica gerada (num contexto dado) pode atingir, no sentido da definição 1.4.11. Devemos então adaptar a linguagem para definir $VM(\phi)$ relativamente a um contexto C e uma interpretação $\mathcal{I}$.

Definição 2.2.7 : (1) Seja $T = \{t_1, \dots, t_n\}$ um conjunto finito de tipos. O extent de T é a fórmula

$$\epsilon(T) \equiv_{def} (\exists y_1)Ey_1 \wedge \dots \wedge (\exists y_n)Ey_n$$

onde $y_i \in \mathcal{V}_{t_i}$ ($i = 1, \dots, n$). Se $T = \emptyset$, então $\epsilon(T) \equiv_{def} \top$.

(2) Seja C um contexto (eventualmente vazio). O conjunto dos tipos das variáveis e constantes de C , denotado **tipos**(C), é chamado de tipos do contexto C . Definimos o extent do contexto C como sendo a fórmula $\epsilon(\mathbf{tipos}(C))$, a qual será denotada frequentemente por $\epsilon(C)$.

(3) Se τ é um termo, definimos **tipos**(τ) como sendo **tipos**($C(\tau)$).

Para que $\epsilon(T)$ seja bem definida, é necessário que $(\exists x)E_t x$ e $(\exists y)E_t y$ sejam equivalentes para todo $x, y \in \mathcal{V}_t$ e para todo tipo t ; de fato, isto será provado depois. Por enquanto, podemos assumir que a variável escolhida para cada tipo de T é a primeira, i.e., $y_i = v_0^{t_i}$ e $y_1 < \dots < y_n$.

Definição 2.2.8 : *Seja ϕ uma fórmula e C um contexto para ϕ . Sejam $\vec{y} = (y_1, \dots, y_m)$ as variáveis em C que não pertencem a $VAR(\phi)$ e $\vec{b} = (b_1, \dots, b_n)$ as constantes em C que não aparecem em ϕ . Definimos ϕ no contexto C como sendo a fórmula*

$$\phi_C = \phi \otimes (Ey_1 \otimes \dots \otimes Ey_m \otimes Eb_1 \otimes \dots \otimes Eb_n).$$

Novamente, devemos assumir uma forma canônica para que ϕ_C seja bem definida; assim, podemos supor que C é totalmente ordenado e que $y_1 < \dots < y_m$ e $b_1 < \dots < b_n$, na ordem de C .

Definição 2.2.9 : *Sejam ϕ uma fórmula, C um contexto para ϕ e $\epsilon(C)$ o exten de C . Definimos o valor máximo de ϕ em C , denotado $V_C(\phi)$, por indução na complexidade de ϕ :*

- (i) Se $\phi \in ELF(\mathbb{L})$, então $V_C(\phi) = \epsilon(C)$;
- (ii) Se $\phi = \alpha \multimap \beta$, então $V_C(\phi) = \epsilon(C)$;
- (iii) Se $\phi = \neg \psi$, então $V_C(\phi) = \epsilon(C)$;
- (iv) Se $\phi = \alpha * \beta$, então $V_C(\phi) = V_C(\alpha) * V_C(\beta)$, onde $*$ = $\wedge, \vee, \otimes$;
- (v) Se $\phi = (\forall x)\alpha$ ou $\phi = (\exists x)\alpha$, então $V_C(\phi) = V_{(y,C)}(\alpha[y/x])$,

onde y é a primeira variável livre para x em α , que não ocorre em C .

Estamos agora em condições de definir e interpretar os sequentes da lógica.

Definição 2.2.10 : *Dada uma linguagem $\mathbb{L}$, definimos um sequente em $\mathbb{L}$ como sendo um objeto da forma*

$$\Gamma \vdash \Delta$$

onde tanto Γ , quanto Δ , são sequências finitas de fórmulas de $\mathbb{L}$, não simultaneamente vazias e o comprimento de Δ é ≤ 1 (i.e., Δ tem no máximo uma fórmula).

Definição 2.2.11 : *Seja $S : \Gamma \vdash \Delta$ um sequente, C um contexto para todas as fórmulas de S (nesse caso, C é dito um contexto para S) e seja $\mathcal{I}$ uma interpretação.*

Dizemos que S é válido em $\mathcal{I}$ e C , $(\mathcal{I}, C) \models S$, se vale o seguinte:

- (i) Se $S : \phi_1, \dots, \phi_n \vdash \phi$, exigimos que $[\phi_1]_C \& \dots \& [\phi_n]_C \leq [\phi]_C$;
- (ii) Se $S : \phi_1, \dots, \phi_n \vdash$, exigimos que $[\phi_1]_C \& \dots \& [\phi_n]_C = 0$;
- (iii) Se $S : \vdash \phi$, exigimos que $[\phi]_C = [V_C(\phi)]_C$.

Dizemos que S é válido em $\mathcal{I}$, $\mathcal{I} \models S$, se $(\mathcal{I}, C(S)) \models S$, onde $C(S)$ é o contexto formado pelas variáveis livres e constantes das fórmulas de S , chamado de contexto de S . Finalmente, dizemos que S é válido se ele é válido em toda interpretação $\mathcal{I}$.

Vamos agora provar algumas propriedades básicas da função de valor máximo.

Lema 2.2.12 : *Seja ϕ uma fórmula, $C = (\vec{x}; \vec{a})$ um contexto para ϕ e $D = (\vec{y}; \vec{b})$ um contexto qualquer; denotemos por $(C; D - C)$ o contexto $((\vec{x}; \vec{y} - \vec{x}); (\vec{a}; \vec{b} - \vec{a}))$. Então, para toda interpretação $\mathcal{I}$,*

$$\llbracket V_C(\phi) \rrbracket_D(\vec{u}) = \llbracket V_{C; D-C}(\phi) \rrbracket \& E(\vec{u}).$$

Em particular,

$$\llbracket V_C(\phi) \rrbracket_C(\vec{u}) = \llbracket V_C(\phi) \rrbracket \& E(\vec{u}).$$

Demonstração: Por indução na complexidade de ϕ . Sejam $\epsilon(T)$ e $\epsilon(S)$ os extents de C e $(C; D - C)$, respectivamente. Assim,

$$\epsilon(T) = (\exists x_1)Ex_1 \wedge \dots \wedge (\exists x_n)Ex_n,$$

$$\epsilon(S) = \epsilon(T) \wedge (\exists x_{n+1})Ex_{n+1} \wedge \dots \wedge (\exists x_m)Ex_m$$

se $\text{tipos}(D) - \text{tipos}(C) \neq \emptyset$, ou $\epsilon(S) = \epsilon(T)$ em caso contrário. Assim, se $\mathcal{I}$ é uma interpretação, seja $p = \llbracket \epsilon(S) \rrbracket$, $q = EP_D$ e $r = EP_{\vec{b}}$; logo, se $x_i \in \mathcal{V}_{t_i}$ para todo $i = 1, \dots, n$, então

$$\begin{aligned} \llbracket (\exists x_i)Ex_i \rrbracket_D(\vec{u}) &= \bigvee_{v \in |A_{t_i}|} \llbracket Ez \rrbracket_{(z,D)}(v|_{r \wedge EA_{t_i}}, \vec{u}) \\ &= \bigvee_{v \in |A_{t_i}|} (q \wedge EA_{t_i}) \& Ev \& E(\vec{u}) = (q \wedge EA_{t_i}) \& E(\vec{u}), \end{aligned}$$

donde

$$\llbracket \epsilon(T) \rrbracket_D(\vec{u}) = \bigwedge_{i=1}^n (q \wedge EA_{t_i}) \& E(\vec{u}) = (q \wedge \llbracket \epsilon(T) \rrbracket) \& E(\vec{u}) = p \& E(\vec{u}) = \llbracket \epsilon(S) \rrbracket \& E(\vec{u}).$$

Logo, o resultado vale se ϕ é atômica. Suponha o resultado verdadeiro para toda fórmula de complexidade $\leq k$, com $k \geq 0$ e seja ϕ de complexidade $k + 1$.

Se $\phi = \neg\alpha$, ou $\phi = \alpha \circ \beta$, então o resultado vale pela definição de valor máximo e pelo provado acima.

Se $\phi = \alpha * \beta$, com $*$ = $\wedge, \otimes$ e $*$ ' é a operação correspondente, então, pela definição de valor máximo e hipótese de indução,

$$\begin{aligned} \llbracket V_C(\phi) \rrbracket_D(\vec{u}) &= \llbracket V_C(\alpha) \rrbracket_D(\vec{u}) *' \llbracket V_C(\beta) \rrbracket_D(\vec{u}) \\ &= \llbracket V_{C; D-C}(\alpha) \rrbracket \& E(\vec{u}) *' \llbracket V_{C; D-C}(\beta) \rrbracket \& E(\vec{u}) = \llbracket V_{C; D-C}(\phi) \rrbracket \& E(\vec{u}). \end{aligned}$$

Se $\phi = \alpha \vee \beta$, então, por hipótese de indução, $\llbracket V_C(\alpha) \rrbracket_D(\vec{u}) = \llbracket V_{C; D-C}(\alpha) \rrbracket \& E(\vec{u})$, logo

$$E(\llbracket V_C(\alpha) \rrbracket_D) = \llbracket V_{C; D-C}(\alpha) \rrbracket,$$

e analogamente para β (aqui, usamos o fato, que pode facilmente ser provado por indução na complexidade da fórmula ϕ , de que $\llbracket V_C(\phi) \rrbracket \leq \llbracket \epsilon(C) \rrbracket$ para toda ϕ e todo contexto C para ϕ). Portanto,

$$\begin{aligned} \llbracket V_C(\phi) \rrbracket_D(\vec{u}) &= \llbracket V_C(\alpha) \rrbracket_D \vee \llbracket V_C(\beta) \rrbracket_D(\vec{u}) \\ &= (\llbracket V_{C; D-C}(\alpha) \rrbracket \vee \llbracket V_{C; D-C}(\beta) \rrbracket) \& (\llbracket V_{C; D-C}(\alpha) \rrbracket \& E(\vec{u}) \vee \llbracket V_{C; D-C}(\beta) \rrbracket \& E(\vec{u})) \end{aligned}$$

$$= ([V_{C;D-C}(\alpha)] \vee [V_{C;D-C}(\beta)]) \& E(\vec{u}) = [V_{C;D-C}(\phi)] \& E(\vec{u}).$$

Finalmente, se $\phi = (\mathcal{Q}v)\alpha$, com $\mathcal{Q} = \forall, \exists$, então, escolhendo y livre para x em α que não ocorre em C nem em D ,

$$\begin{aligned} [V_C((\mathcal{Q}v)\alpha)]_D(\vec{u}) &= [V_{(y,C)}(\alpha[y/v])]_D(\vec{u}) \\ &= [V_{(y,C);D-(y,C)}(\alpha[y/v])] \& E(\vec{u}) = [V_{(y;(C;D-C))}(\alpha[y/v])] \& E(\vec{u}) \\ &= [V_{C;D-C}(\phi)] \& E(\vec{u}). \quad \square \end{aligned}$$

Corolário 2.2.13 : *Sejam ϕ uma fórmula, C um contexto para ϕ e $\mathcal{I}$ uma interpretação. Então, $[V_C(\phi)] = \tilde{E}([\phi]_C)$. Portanto, $[V_C(\phi)]_C = VM([\phi]_C)$ e*

$$[\phi]_C(\vec{u}) = [\phi_C]_C(\vec{u}) \leq [V_C(\phi)]_C(\vec{u}).$$

Demonstração: Seja $\mathcal{I}$ uma interpretação, $\epsilon(C)$ o extant de C , $p = [\epsilon(C)] = EP_C$ e

$$\phi_C = \phi \otimes (Ex_1 \otimes \cdots \otimes Ex_k \otimes Ea_1 \otimes \cdots \otimes Ea_m).$$

Para todo $i = 1, \dots, k$ e todo $j = 1, \dots, m$,

$$[Ex_i]_C(\vec{u}) = p \& E(\vec{u}) = [Ea_j]_C(\vec{u})$$

donde, por [char1] e a definição de interpretação, temos

$$[\phi]_C(\vec{u}) = [\phi]_C(\vec{u}) \& p \& E(\vec{u}) = [\phi_C]_C(\vec{u}).$$

Vamos provar a primeira parte do corolário por indução na complexidade da ϕ .

Suponha então que $\phi \in ELF(\mathbb{L})$; então

$$[V_C(\phi)] = [\epsilon(C)] = EP_C = \tilde{E}([\phi]_C).$$

Se $\phi = \neg\alpha$, ou $\phi = \alpha \multimap \beta$, a prova é análoga. Se $\phi = \alpha * \beta$, com $*$ = $\vee, \wedge, \otimes$, então, por hipótese de indução e pelas definições,

$$[V_C(\phi)] = [V_C(\alpha)] *' [V_C(\beta)] = \tilde{E}([\alpha]_C) *' \tilde{E}([\beta]_C) = \tilde{E}([\phi]_C),$$

onde $*'$ é a operação em Q correspondente ao conectivo $*$. Se $\phi = (\forall v)\alpha$ ou $\phi = (\exists v)\alpha$, então, pela hipótese de indução e as definições,

$$[V_C(\phi)] = [V_{(y,C)}(\alpha[y/v])] = \tilde{E}([\alpha[y/v]]_{(y,C)}) = \tilde{E}([\phi]_C).$$

Assim, temos que $[V_C(\phi)] = \tilde{E}([\phi]_C)$, donde, por 2.2.12,

$$[V_C(\phi)]_C(\vec{u}) = [V_C(\phi)] \& E(\vec{u}) = \tilde{E}([\phi]_C) \& E(\vec{u}) = VM([\phi]_C)(\vec{u}).$$

Finalmente, pelo lema 1.4.13,

$$[\phi]_C \leq VM([\phi]_C) = [V_C(\phi)]_C. \quad \square$$

Exemplos 2.2.14 : (i) Com a mesma notação do exemplo 2.2.6 (5), temos que

$$\mathcal{I} \models (\vdash (\forall x)(\exists y)(x = f(y))) \quad \text{e} \quad \mathcal{I} \models ((\exists x)E_s x \vdash ((\exists x)E_s x) \otimes ((\exists y)E_t y))$$

sse o morfismo $f^{\mathcal{I}} : A_t \longrightarrow A_s$ é épico em $Psh(Q)$. Com efeito,

$$\llbracket V_{\emptyset}((\forall x)(\exists y)(x = f(y))) \rrbracket = \llbracket (\exists x)Ex \wedge (\exists y)Ey \rrbracket = EA_t \wedge EA_s = EA_t$$

pois $EA_t \leq EA_s$, logo

$$\mathcal{I} \models (\vdash (\forall x)(\exists y)(x = f(y))) \quad \text{e} \quad \mathcal{I} \models ((\exists x)E_s x \vdash ((\exists x)E_s x) \otimes ((\exists y)E_t y))$$

se e somente se $EA_s = EA_s \& EA_t$ e

$$\llbracket (\forall x)(\exists y)(x = f(y)) \rrbracket = EA_s \wedge \bigwedge_{x_1 \in |A_s|} (Ex_1 \rightarrow_l (EA_t \& \bigvee_{y_1 \in |A_t|} [x_1 = f^{\mathcal{I}}(y_1)]_s)) = EA_t$$

se e somente se

$$(1) \quad EA_s = EA_s \& EA_t \quad \text{e} \quad EA_t \& Ea = EA_t \& \bigvee_{b \in |A_t|} [a = f^{\mathcal{I}}(b)]_s \quad \forall a \in |A_s|.$$

Suponha agora que vale (1) e seja $a \in |A_s|$; logo, $Ea = Ea \& EA_s \& EA_t = Ea \& EA_t \& EA_s = Ea \& EA_t$. Assim,

$$\begin{aligned} Ea &= Ea \& EA_t \& Ea = Ea \& EA_t \& \bigvee_{b \in |A_t|} [a = f^{\mathcal{I}}(b)]_s \\ &= \bigvee_{b \in |A_t|} Ea \& [a = f^{\mathcal{I}}(b)]_s = \bigvee_{b \in |A_t|} [a = f^{\mathcal{I}}(b)]_s, \end{aligned}$$

portanto $f^{\mathcal{I}}$ é épico em $Psh(Q)$ (lema 1.1.9 (b)). Reciprocamente, se $f^{\mathcal{I}}$ é épico, então $A_s = tcl(f^{\mathcal{I}}(A_t))$, logo $EA_s = EA_s \& E(f^{\mathcal{I}}(A_t)) = EA_s \& EA_t$ ([MS]). Além disso,

$$Ea = \bigvee_{b \in |A_t|} [a = f^{\mathcal{I}}(b)]_s \quad \forall a \in |A_s|,$$

portanto

$$EA_t \& Ea = EA_t \& \bigvee_{b \in |A_t|} [a = f^{\mathcal{I}}(b)]_s \quad \forall a \in |A_s|.$$

Isto prova (1) e que

$$\mathcal{I} \models (\vdash (\forall x)(\exists y)(x = f(y))) \quad \text{e} \quad \mathcal{I} \models ((\exists x)E_s x \vdash ((\exists x)E_s x) \otimes ((\exists y)E_t y)).$$

(ii) Os monomorfismos também podem ser caracterizados por uma fórmula de primeira ordem natural. De fato, dada $f : s \longrightarrow t$, então

$$\mathcal{I} \models (\vdash (\forall x)(\forall y)((f(x) = f(y)) \multimap (x = y)))$$

se e somente se $f^{\mathcal{I}} : A_s \longrightarrow A_t$ é mônico em $Psh(Q)$. Com efeito,

$$\llbracket V_{\emptyset}((\forall x)(\forall y)((f(x) = f(y)) \multimap (x = y))) \rrbracket = \llbracket (\exists x)Ex \wedge (\exists y)Ey \rrbracket = EA_s \wedge EA_t = EA_s$$

pois $EA_s \leq EA_t$, logo

$$\mathcal{I} \models (\vdash (\forall x)(\forall y)((f(x) = f(y)) \multimap (x = y)))$$

se e somente se

$$\llbracket (\forall x)(\forall y)((f(x) = f(y)) \multimap (x = y)) \rrbracket = EA_s$$

se e somente se

$$EA_s \leq \bigwedge_{a \in |A_s|} (Ea \rightarrow_t (EA_s \wedge \bigwedge_{b \in |A_s|} (Eb \rightarrow_l \llbracket (f(x) = f(y)) \multimap (x = y) \rrbracket_{(x,y)}(a, b))) \& Ea)$$

se e somente se

$$EA_s \& Ea \& Eb \leq EA_s \& [f^I(a) = f^I(b)]_t \rightarrow EA_s \& [a = b]_s \quad \forall a, b \in |A_s|$$

se e somente se

$$(1) \quad EA_s \& [f^I(a) = f^I(b)]_t \leq EA_s \& [a = b]_s$$

pois, em todo right-quantal RSI,

$$\top \leq X \rightarrow Y \quad \text{see} \quad X \leq Y$$

e $R = Ch(A_s, A_s)$ é um right-quantal RSI, onde $\top(a, b) = EA_s \& Ea \& Eb$. Assim, se vale (1), então, como $Ef^I(a) = Ea \leq EA_s$,

$$[f^I(a) = f^I(b)]_t = Ea \& (EA_s \& [f^I(a) = f^I(b)]_t) \leq Ea \& (EA_s \& [a = b]_s) = [a = b]_s$$

donde, por [mor2],

$$(2) \quad [f^I(a) = f^I(b)]_t = [a = b]_s \quad \forall a, b \in |A_s|$$

e f^I é mônico (lema 1.1.15). Como é claro que (2) implica (1),

$$\vdash (\forall x)(\forall y)((f(x) = f(y)) \multimap (x = y))$$

é uma caracterização de mônico. $\square$

2.3 Cláusulas de Extensão e Redução de Sequentes

Para que as regras da lógica (QPC) a ser definida na seção seguinte sejam corretas, será frequentemente necessário que as fórmulas no lado esquerdo do sequente gerem um sub-prefixe extensível à esquerda e que a fórmula do lado direito gere um sub-prefixe extensível à direita, por tipos apropriados. Uma possibilidade seria exigir regras da forma

$$\frac{\Gamma_1 \vdash \Delta_1}{\Gamma_2 \vdash \Delta_2} \quad \frac{\Gamma_1 \vdash \Delta_1 \quad \Phi_1 \vdash \Theta_1}{\Gamma_2 \vdash \Delta_2}$$

onde todos os sequentes têm os mesmos tipos; mas esta exigência é muito estrita (não poderíamos em geral misturar tipos nas deduções). Por analogia com 1.2.9, temos a

Definição 2.3.1 : Seja ϕ uma fórmula, $C = (\vec{x}; \vec{a})$, $D = ((\vec{x}; \vec{y}); (\vec{a}; \vec{b}))$ contextos para ϕ , e $\mathcal{I}$ uma interpretação. Dizemos que ϕ é extensível à esquerda (à direita) de C para D (em $\mathcal{I}$) se, denotando por $|\phi| \subseteq P_C = B$ o sub-prefeixe fechado associado a $\llbracket \phi \rrbracket_C$, e $\pi : B \times A \rightarrow B$ é a projeção, onde $A = P_{(\vec{y}; \vec{b})}$ (portanto $B \times A = P_D$), então

$$|\phi|(\pi^*) \subseteq \pi^*|\phi| = |\phi| \times A \quad (\text{resp., } |\phi|(\pi^*) \supseteq \pi^*|\phi| = |\phi| \times A).$$

Se ϕ é extensível à direita e à esquerda de C para D em $\mathcal{I}$, ϕ é dita extensível de C para D (em $\mathcal{I}$). Observe que $|\phi|(\pi^*)$ é o prefixe associado com $\llbracket \phi \rrbracket_D$.

A partir daqui, vamos dar uma formulação sintáctica das propriedades de extensão de fórmulas provadas até agora. Como pode ser observado, as operações corretas de extensão e de imagem inversa dependem de encontrar relações $\leq$ entre extents; assim, a aplicação das regras da lógica dependerá em geral da comparação de extents. Estes são representados por fechos existenciais, como é fácil provar:

Lema 2.3.2 : (a) Seja ϕ uma fórmula, $C = (\vec{x}; \vec{a})$ um contexto para ϕ e $\mathcal{I}$ uma interpretação. Logo, $\llbracket (\exists)\phi_C \rrbracket_{\vec{a}} = E\llbracket \phi \rrbracket_C$.

(b) Seja C um contexto, $\epsilon(C)$ o extent de C e $\vec{a}$ uma sequência finita de constantes diferentes, com extent $\epsilon(T)$. Então, para toda interpretação $\mathcal{I}$, temos que $\llbracket \epsilon(C) \rrbracket_{\vec{a}} = \llbracket \epsilon(C) \rrbracket \wedge \llbracket \epsilon(T) \rrbracket$.

Demonstração: (a) Pela definição de interpretação e 2.2.13,

$$\llbracket (\exists)\phi_C \rrbracket_{\vec{a}} = \bigvee_{\vec{u} \in D_C} \llbracket \phi_C \rrbracket_C(\vec{u}) = \bigvee_{\vec{u} \in D_C} \llbracket \phi \rrbracket_C(\vec{u}) = E\llbracket \phi \rrbracket_C.$$

(b) Dada $\mathcal{I}$, seja $q = \llbracket \epsilon(T) \rrbracket = EP_{\vec{a}}$, e suponha que $\epsilon(C) = (\exists x_1)Ex_1 \wedge \dots \wedge (\exists x_n)Ex_n$, com $x_i \in \mathcal{V}_{t_i}$ (o caso em que $\epsilon(C) = \top$ é óbvio). Então

$$\begin{aligned} \llbracket (\exists x_i)Ex_i \rrbracket_{\vec{a}} &= \bigvee_{u \in A_{t_i}} \llbracket Ey_i \rrbracket_{y_i; \vec{a}}(u|_{q \wedge EA_{t_i}}) \\ &= \bigvee_{u \in A_{t_i}} (q \wedge EA_{t_i}) \& EA_{t_i} \& E(u|_{q \wedge EA_{t_i}}) = q \wedge EA_{t_i} \end{aligned}$$

para todo $i = 1, \dots, n$, donde segue-se o resultado. $\square$

As propriedades de extensão e de imagem inversa com relação às operações entre prefikes serão dadas como conjuntos finitos $CL = \{x_1, \dots, x_n\}$, chamados de cláusulas, onde cada x_i consiste, por sua vez, num conjunto finito de sequentes, chamado de justificativa. Logo, toda regra da lógica estará munida de uma cláusula, a cláusula da regra, cujo objetivo é informar, através das justificativas, dos sequentes que devem ser provados previamente à aplicação da regra; assim, para legitimar a aplicação da regra, deve existir alguma justificativa na cláusula tal que todos os sequentes da justificativa devem ser provados. A nível de interpretações, temos a

Definição 2.3.3 Seja CL uma cláusula e $\mathcal{I}$ uma interpretação. Dizemos que $\mathcal{I}$ satisfaz CL se existe uma justificativa $x \in CL$ tal que $\mathcal{I} \models S$ para todo sequente S de x .

Para simplificar as definições a serem feitas abaixo, introduzimos a justificativa trivial, definida como $x_{\top} = \{\vdash \top\}$. A primeira propriedade a ser traduzida como cláusula é o corolário 1.3.7, onde obtemos prefeixes R que podem ser estendidos por um tipo A no caso que todos os prefeixes R' construídos no processo (prévios a R) satisfazem $ER' \leq EA$.

Definição 2.3.4 *Seja ϕ uma fórmula, $\alpha \in SF(\phi)$ e $C \supseteq C(\phi)$. Suponha que α ocorre em ϕ no escopo de quantificadores nas variáveis $v_1 < \dots < v_n$ (na ordem de $\mathcal{V}$). Seja y_1 a primeira variável livre para v_1 em α que não ocorre em C , y_2 a primeira variável livre para v_2 em α que não ocorre em (y_1, C) ; continuando com este procedimento, seja y_n a primeira variável livre para v_n em α que não ocorre em $(y_1, \dots, y_{n-1}, C)$. Definimos o fecho existencial de α em (ϕ, C) como sendo a fórmula*

$$F(\alpha, \phi, C) \equiv_{def} (\exists)(\alpha[y_1/v_1] \dots [y_n/v_n])_D,$$

onde $D = (y_1, \dots, y_n, C)$ é o contexto de α em ϕ, C , denotado por $\mathbf{C}(\alpha, \phi, C)$. Se α não ocorre no escopo de nenhum quantificador em ϕ , então $F(\alpha, \phi, C) \equiv_{def} (\exists)\alpha_C$ e $\mathbf{C}(\alpha, \phi, C) = C$.

Definição 2.3.5 : *Sejam ϕ uma fórmula, C um contexto para ϕ e $T \neq \emptyset$ um conjunto finito de tipos. Definimos a cláusula de extensão direta de ϕ por T (no contexto C) como sendo*

$$ED(\phi, C, T) = \begin{cases} \{\{F(\alpha, \phi, C) \vdash \epsilon(T) : \alpha \in SFE(\phi)\}\} & \text{se } \phi \text{ não é atômica} \\ \{x_{\top}\} & \text{se } \phi \text{ é atômica} \end{cases}.$$

Vemos então que a cláusula de extensão direta de uma fórmula consiste numa única justificativa.

Proposição 2.3.6 : *Seja ϕ uma fórmula, $C \subseteq D$ contextos para ϕ , $T = \text{tipos}(D - C)$ e $\mathcal{I}$ uma interpretação. Se $\mathcal{I}$ satisfaz $ED(\phi, C, T)$, então ϕ é extensível de C para D em $\mathcal{I}$.*

Demonstração: O resultado é claro se ϕ é atômica.

Suponha que ϕ não é atômica; para cada $\psi \in SF(\phi)$, seja $C' = \mathbf{C}(\psi, \phi, C)$, $D' = \mathbf{C}(\psi, \phi, D)$, $|\psi|$ o sub-prefixe de $P_{C'}$ associado a $\llbracket (\psi[\vec{y}/\vec{v}]) \rrbracket_{C'}$ em $\mathcal{I}$, A o prefixe associado a $D - C$ (portanto $P_D = P_C \times A$) e $|\psi|_A$ o sub-prefixe de $P_{D'}$ associado a $\llbracket (\psi[\vec{z}/\vec{v}]) \rrbracket_{D'}$. Por hipótese, se $\psi \in SFE(\phi)$, então $F(\psi, \phi, C) = (\exists)(\psi[\vec{y}/\vec{v}])_{C'}$ e o seguinte

$$(\exists)(\psi[\vec{y}/\vec{v}])_{C'} \vdash \epsilon(T)$$

é válido em $\mathcal{I}$; logo, se $C' = (\vec{x}; \vec{a})$, o lema 2.3.2 nos dá

$$E|\psi| = \llbracket (\exists)(\psi[\vec{y}/\vec{v}])_{C'} \rrbracket_{\vec{a}} \leq \llbracket \epsilon(T) \rrbracket_{\vec{a}} = \llbracket \epsilon(T) \rrbracket \wedge \llbracket \epsilon(\vec{a}) \rrbracket \leq \llbracket \epsilon(T) \rrbracket = EA.$$

Por 1.3.7, $|\phi|$ é extensível por A , i.e., $|\phi|_A = |\phi| \times A$, portanto ϕ é extensível de C para D em $\mathcal{I}$. $\square$

Podemos combinar todas as propriedades de extensão provadas até agora em 1.2.7, 1.3.1, 1.3.4 para definir cláusulas que determinam se uma fórmula é extensível à direita ou à esquerda de um contexto C para outro contexto maior D .

Definição 2.3.7 : Sejam ϕ uma fórmula, C um contexto para ϕ e $T \neq \emptyset$ um conjunto finito de tipos. Definimos as cláusulas $K_D(\phi, C, T)$ e $K_E(\phi, C, T)$ por indução na complexidade de ϕ .

(1) Se ϕ é atômica, então

$$K_D(\phi, C, T) = K_E(\phi, C, T) = ED(\phi, C, T) = \{x_\top\};$$

(2) Se $\phi = \neg\psi$, então

$$K_D(\phi, C, T) = K_E(\psi, C, T) \cup ED(\phi, C, T),$$

$$K_E(\phi, C, T) = \{x \cup \{S_1\} : x \in K_D(\psi, C, T)\} \cup ED(\phi, C, T),$$

onde S_1 denota o seguinte $S_1 : (\epsilon(C) \otimes (\epsilon(C) \wedge \epsilon(T))) \wedge (\exists)\psi_C \vdash \epsilon(C) \wedge \epsilon(T)$;

(3) Se $\phi = \alpha \multimap \beta$, então

$$K_D(\phi, C, T) = \{x \cup y : x \in K_E(\alpha, C, T), y \in K_D(\beta, C, T)\} \cup ED(\phi, C, T),$$

$$K_E(\phi, C, T) = \{x \cup y \cup \{S_2\} : x \in K_D(\alpha, C, T), y \in K_E(\beta, C, T)\} \cup ED(\phi, C, T),$$

onde S_2 denota o seguinte $S_2 : (\epsilon(C) \otimes (\epsilon(C) \wedge \epsilon(T))) \wedge (\exists)\alpha_C \vdash \epsilon(C) \wedge \epsilon(T)$;

(4) Se $\phi = \alpha \otimes \beta$, então

$$K_D(\phi, C, T) = \{x \cup y \cup \{S_3\} : x \in K_D(\alpha, C, T), y \in K_D(\beta, C, T)\} \cup ED(\phi, C, T),$$

$$K_E(\phi, C, T) = \{x \cup y : x \in K_E(\alpha, C, T), y \in K_E(\beta, C, T)\} \cup ED(\phi, C, T),$$

onde S_3 denota o seguinte $S_3 : \epsilon(T) \wedge (\exists)(\alpha \otimes \beta)_C \vdash (\epsilon(T) \wedge (\exists)\alpha_C) \otimes (\epsilon(T) \wedge (\exists)\beta_C)$;

(5) Se $\phi = \alpha \vee \beta$, então

$$K_D(\phi, C, T) = \{x \cup y \cup \{S_4, S_5\} : x \in K_D(\alpha, C, T), y \in K_D(\beta, C, T)\}$$

$$\cup \{x \cup y \cup \{S_6\} : x \in K_D(\alpha, C, T), y \in K_D(\beta, C, T)\}$$

$$\cup \{x \cup y \cup \{S_7, S_8\} : x \in K_D(\alpha, C, T), y \in K_D(\beta, C, T)\} \cup ED(\phi, C, T),$$

$$K_E(\phi, C, T) = \{x \cup y : x \in K_E(\alpha, C, T), y \in K_E(\beta, C, T)\} \cup ED(\phi, C, T),$$

onde S_4, S_5, S_6, S_7 e S_8 denotam os seguintes

$$S_4 : ((\exists)\alpha_C \vee (\exists)\beta_C) \wedge \epsilon(T) \vdash (((\exists)\alpha_C \wedge \epsilon(T)) \vee ((\exists)\beta_C \wedge \epsilon(T))) \otimes ((\exists)\alpha_C \wedge \epsilon(T)),$$

$$S_5 : ((\exists)\alpha_C \vee (\exists)\beta_C) \wedge \epsilon(T) \vdash (((\exists)\alpha_C \wedge \epsilon(T)) \vee ((\exists)\beta_C \wedge \epsilon(T))) \otimes ((\exists)\beta_C \wedge \epsilon(T)),$$

$$S_6 : (\exists)\alpha_C \vee (\exists)\beta_C \vdash \epsilon(T),$$

$$S_7 : (((\exists)\alpha_C \vee (\exists)\beta_C) \wedge \epsilon(C)) \otimes (\exists)\alpha_C \vdash (\exists)\alpha_C \wedge \epsilon(C),$$

$$S_8 : (((\exists)\alpha_C \vee (\exists)\beta_C) \wedge \epsilon(C)) \otimes (\exists)\beta_C \vdash (\exists)\beta_C \wedge \epsilon(C);$$

(6) Se $\phi = \alpha \wedge \beta$, então

$$K_D(\phi, C, T) = \{x \cup y : x \in K_D(\alpha, C, T), y \in K_D(\beta, C, T)\} \cup ED(\phi, C, T),$$

$$K_E(\phi, C, T) = \{x \cup y : x \in K_E(\alpha, C, T), y \in K_E(\beta, C, T)\} \cup ED(\phi, C, T);$$

(7) $\phi = (\forall v)\psi$ ou $\phi = (\exists v)\psi$; se y é a primeira variável livre para v em ψ que não ocorre em C , então

$$K_D(\phi, C, T) = K_D(\psi[y/v], (y, C), T) \cup ED(\phi, C, T),$$

$$K_E(\phi, C, T) = K_E(\psi[y/v], (y, C), T) \cup ED(\phi, C, T).$$

Proposição 2.3.8 : Sejam ϕ uma fórmula, $C = (\vec{x}; \vec{a})$ e $D = ((\vec{x}; \vec{y}); (\vec{a}; \vec{b}))$ contextos para ϕ . Seja $T = \text{tipos}(\vec{y}; \vec{b})$ e $\mathcal{I}$ uma interpretação. Se $\mathcal{I}$ satisfaz $K_D(\phi, C, T)$, então ϕ é extensível à direita de C para D em $\mathcal{I}$. Se $\mathcal{I}$ satisfaz $K_E(\phi, C, T)$, então ϕ é extensível à esquerda de C para D em $\mathcal{I}$.

Demonstração: Se $\mathcal{I}$ satisfaz $ED(\phi, C, T)$, o resultado é consequência da proposição 2.3.6. Se $\mathcal{I}$ não satisfaz $ED(\phi, C, T)$, provaremos o resultado por indução na complexidade k de ϕ . O caso $k = 0$ está claro. Suponha que ϕ tenha complexidade $k + 1$ e que o resultado vale para fórmulas de complexidade $\leq k$.

Seja $|\phi| \subseteq B = P_C$ e $|\phi|_A \subseteq B \times A = P_D$ o prefeixe associado à interpretação de ϕ na estrutura $\mathcal{I}$ nos contextos C e D , respectivamente, com $A = P_{(\vec{y}; \vec{b})}$. Logo, $|\phi|_A = |\phi|(\pi^*)$, onde $\pi : B \times A \rightarrow B$ é a projeção. Suponha que $\mathcal{I}$ satisfaz $K_D(\phi, C, T)$ e seja $x \in K_D(\phi, C, T) - ED(\phi, C, T)$ tal que $\mathcal{I} \models S$ para todo sequente S de x .

Se $\phi = \alpha \rightarrow \beta$, então $x = y \cup z$, com $y \in K_E(\alpha, C, T)$ e $z \in K_D(\beta, C, T)$ e $\mathcal{I}$ satisfaz todos os sequentes de y e z . Logo, $\mathcal{I}$ satisfaz $K_E(\alpha, C, T)$ e $K_D(\beta, C, T)$; a hipótese de indução garante que $|\alpha|_A \subseteq |\alpha| \times A$ e $|\beta|_A \supseteq |\beta| \times A$ e assim 1.2.7(b) nos dá

$$|\phi|_A = |\alpha|_A \rightarrow |\beta|_A \supseteq (|\alpha| \times A) \rightarrow (|\beta| \times A) \supseteq (|\alpha| \rightarrow |\beta|) \times A = |\phi| \times A.$$

Se $\phi = \neg\psi$, então $x \in K_E(\psi, C, T)$, donde $|\psi|_A \subseteq |\psi| \times A$. Assim, como $|\phi| = |\psi| \rightarrow \mathbf{0}$, onde $\mathbf{0}_A = \mathbf{0} \times A$, vale a afirmação pelo caso anterior.

Se $\phi = \alpha \otimes \beta$, então $x = y \cup z \cup \{S_3\}$, com $y \in K_D(\alpha, C, T)$ e $z \in K_D(\beta, C, T)$ e

$$EA \wedge E(|\alpha| \& |\beta|) \leq (EA \wedge E|\alpha|) \& (EA \wedge E|\beta|)$$

donde, por 1.3.1(b.1) e a hipótese de indução,

$$|\phi|_A = |\alpha|_A \& |\beta|_A \supseteq (|\alpha| \times A) \& (|\beta| \times A) = (|\alpha| \& |\beta|) \times A = |\phi| \times A.$$

Se $\phi = \alpha \vee \beta$, então $x = y \cup z \cup \{S_4, S_5\}$, ou $x = y \cup z \cup \{S_6\}$, ou $x = y \cup z \cup \{S_7, S_8\}$, onde $y \in K_D(\alpha, C, T)$ e $z \in K_D(\beta, C, T)$. Logo, pela hipótese de indução, a observação 1.3.4 e o lema 1.3.1,

$$|\phi|_A = |\alpha|_A \vee |\beta|_A \supseteq (|\alpha| \times A) \vee (|\beta| \times A) = (|\alpha| \vee |\beta|) \times A = |\phi| \times A.$$

Se $\phi = \alpha \wedge \beta$, então $x = y \cup z$, com $y \in K_D(\alpha, C, T)$ e $z \in K_D(\beta, C, T)$. Assim, 1.2.7 (d) e a hipótese de indução implicam

$$|\phi|_A = |\alpha|_A \wedge |\beta|_A \supseteq (|\alpha| \times A) \wedge (|\beta| \times A) = (|\alpha| \wedge |\beta|) \times A = |\phi| \times A.$$

Se $\phi = (\mathcal{Q}v)\psi$, então $x \in K_D(\psi[y/v], (y, C), T)$, portanto, pela hipótese de indução e 1.2.7 (e)

$$\begin{aligned} |\phi|_A &= ((\mathcal{Q}b)|\psi[y/v]|)_A = (\mathcal{Q}b)(|\psi[y/v]|_A) \\ &\supseteq (\mathcal{Q}b)(|\psi[y/v]| \times A) = ((\mathcal{Q}b)|\psi[y/v]|) \times A = |\phi| \times A. \end{aligned}$$

Provamos que ϕ é extensível à esquerda de C para D . Suponhamos agora que $\mathcal{I}$ satisfaz $K_E(\phi, C, T)$ e seja $x \in K_E(\phi, C, T) - ED(\phi, C, T)$ tal que todo sequente S de x é válido em $\mathcal{I}$.

Se $\phi = \alpha \multimap \beta$, então $x = y \cup z \cup \{S_2\}$, com $y \in K_D(\alpha, C, T)$ e $z \in K_E(\beta, C, T)$ e

$$(EB \& (EB \wedge EA)) \wedge E|\alpha| \leq EA \wedge EB.$$

Assim, por hipótese de indução,

$$|\alpha|_A \supseteq |\alpha| \times A, \quad |\beta|_A \subseteq |\beta| \times A$$

donde

$$|\alpha|_A \rightarrow |\beta|_A \subseteq (|\alpha| \times A) \rightarrow (|\beta| \times A)$$

e então, por 1.3.4,

$$|\phi|_A = |\alpha|_A \rightarrow |\beta|_A \subseteq (|\alpha| \times A) \rightarrow (|\beta| \times A) = (|\alpha| \rightarrow |\beta|) \times A = |\phi| \times A.$$

O caso em que $\phi = \neg\psi$ é similar ao anterior.

Se $\phi = \alpha * \beta$, tal que $*$ = $\otimes, \vee, \wedge$, então $x = y \cup z$ tal que $y \in K_E(\alpha, C, T)$ e $z \in K_E(\beta, C, T)$. Logo, se $*$ ' é a correspondente operação entre prefeixes (a qual é crescente nas duas coordenadas), então, por 1.2.7 e a hipótese de indução,

$$|\phi|_A = |\alpha|_A *' |\beta|_A \subseteq (|\alpha| \times A) *' (|\beta| \times A) \subseteq (|\alpha| *' |\beta|) \times A = |\phi| \times A.$$

Se $\phi = (\mathcal{Q}v)\psi$, onde $\mathcal{Q} = \forall$ ou $\mathcal{Q} = \exists$, então $x \in K_E(\psi[y/v], (y, C), T)$, donde, por 1.2.7 (e) e hipótese de indução,

$$\begin{aligned} |\phi|_A &= ((\mathcal{Q}b)|\psi[y/v]|)_A = (\mathcal{Q}b)(|\psi[y/v]|_A) \\ &\subseteq (\mathcal{Q}b)(|\psi[y/v]| \times A) = ((\mathcal{Q}b)|\psi[y/v]|) \times A = |\phi| \times A. \end{aligned}$$

Assim, vemos que ϕ é extensível à esquerda de C para D . $\square$

Como a regra $[CUT]$ e as regras de quantificação impõem a redução de tipos, introduzimos a seguinte:

Definição 2.3.9 : Dada uma linguagem $\mathbb{L}$, considere o conjunto $\mathcal{S}(FOR(\mathbb{L}))$ das sequências finitas em $FOR(\mathbb{L})$.

(a) Dada $\Sigma \in S(\text{FOR}(\mathbb{L}))$, definimos

$$\mathbf{Etipos}(\Sigma) \equiv_{\text{def}} \cup \{ \mathbf{Etipos}(\phi) : \phi \text{ ocorre em } \Sigma \}$$

e portanto, $\mathbf{Etipos}(\emptyset) = \emptyset$. Analogamente, definimos $\text{VAR}(\Sigma)$, $\text{CONS}(\Sigma)$ e $C(\Sigma)$. Por outro lado, definimos $K_D(\emptyset, C, T) = \{x_\top\}$ e

$$K_D(\alpha_1, \dots, \alpha_n, C, T) = \{x_1 \cup \dots \cup x_n : x_i \in K_D(\alpha_i, C, T) \ (i = 1, \dots, n)\},$$

onde C é um contexto para todas as α_i . Similarmente definimos $K_E(\Sigma, C, T)$ para $\Sigma \in S(\text{FOR}(\mathbb{L}))$.

(b) Definimos a função de redução como sendo a aplicação $\text{red} : S(\text{FOR}(\mathbb{L})) \rightarrow S(\text{FOR}(\mathbb{L}))$ dada por:

$$\text{red}(\emptyset) = \emptyset;$$

$$\text{red}(\phi; \Gamma) = (\phi; \text{red}(\Gamma)) \quad \text{se } \phi \neq \alpha \otimes \beta;$$

$$\text{red}(\alpha \otimes \beta; \Gamma) = (\text{red}(\alpha); \text{red}(\beta); \text{red}(\Gamma)).$$

Observe que, por *exchange* e idempotência, se $\Gamma = \alpha_1, \dots, \alpha_n$ e $\text{red}(\Gamma) = \beta_1, \dots, \beta_k$, temos que, para todo contexto $C \supseteq C(\Gamma)$,

$$[\Gamma]_C \equiv_{\text{def}} [\alpha_1]_C \& \dots \& [\alpha_n]_C = [\beta_1]_C \& \dots \& [\beta_k]_C.$$

Definição 2.3.10 : Seja $S : \Gamma \vdash \Delta$ um sequente, C o contexto de S e T um conjunto de tipos, com $T \cap \mathbf{tipos}(C) = \emptyset$.

(a) Definimos as cláusulas de extensão de S por T da maneira seguinte:

$$E(S, \emptyset) = \{x_\top\};$$

$$E(S, T) = \{x \cup y : x \in K_E(\text{red}(\Gamma), C, T), y \in K_D(\Delta, C, T)\} \quad (T \neq \emptyset).$$

(b) Definimos as cláusulas de redução de S por T da maneira seguinte:

$$R(S, \emptyset) = \{x_\top\};$$

$$R(S, T) = \{x \cup y \cup \{S_\Gamma\} : x \in K_D(\text{red}(\Gamma), C, T), y \in K_E(\Delta, C, T)\} \quad (T \neq \emptyset, \Gamma \neq \emptyset),$$

onde, se $\text{red}(\Gamma) = \beta_1, \dots, \beta_k$, então S_Γ denota o sequente

$$S_\Gamma : (\exists)(\beta_1 \otimes \dots \otimes \beta_k)_C \vdash ((\exists)(\beta_1)_C \wedge \epsilon(T)) \otimes \dots \otimes ((\exists)(\beta_k)_C \wedge \epsilon(T));$$

$$R(S, T) = \{x \cup \{\epsilon(C) \vdash \epsilon(T)\} : x \in K_E(\Delta, C, T)\} \quad (T \neq \emptyset, \Gamma = \emptyset).$$

Os próximos lemas mostram que as definições das cláusulas de extensão e redução de sequentes funcionam da maneira esperada.

Lema 2.3.11 : Seja $S : \Gamma \vdash \Delta$ um sequente, T um conjunto finito de tipos, $C = (\vec{x}; \vec{a}) = C(S)$, $C_1 = (\vec{y}; \vec{b})$ um contexto tal que $\mathbf{tipos}(C_1) - \mathbf{tipos}(C) = T$ e $C' = ((\vec{x}; \vec{y} - \vec{x}); (\vec{a}; \vec{b} - \vec{a}))$. Se $\mathcal{I}$ é uma interpretação tal que $\mathcal{I} \models S$ e $\mathcal{I}$ satisfaz $E(S, T)$, então $(\mathcal{I}, C') \models S$.

Demonstração: Suponha que $T \neq \emptyset$; seja $(\vec{z}; \vec{c}) \subseteq (\vec{y} - \vec{x}; \vec{b} - \vec{a})$ o máximo contexto tal que $\text{tipos}(\vec{z}; \vec{c}) = T$, e seja $(\vec{w}; \vec{d}) = ((\vec{y} - \vec{x}) - \vec{z}; (\vec{b} - \vec{a}) - \vec{c})$. Logo, $C' = ((\vec{x}; \vec{z}; \vec{w}); (\vec{a}; \vec{c}; \vec{d}))$, sendo que os tipos de $(\vec{w}; \vec{d})$ estão presentes nos tipos de C . Seja $\pi : P_C \times P_{(\vec{z}; \vec{c})} \rightarrow P_C$ a projeção canônica; então, para toda fórmula α tal que $C(\alpha) \subseteq C$, temos que

$$\llbracket \alpha \rrbracket_{(\vec{x}; \vec{z}); (\vec{a}; \vec{c})} = \llbracket \alpha \rrbracket_C(\pi^*).$$

Como $\text{tipos}(\vec{w}; \vec{d}) \subseteq \text{tipos}(C)$, a extensão de $((\vec{x}; \vec{z}); (\vec{a}; \vec{c}))$ para C' é trivial, i.e.,

$$\llbracket \alpha \rrbracket_{C'}(\vec{u}, \vec{v}, \vec{s}) = \llbracket \alpha \rrbracket_{(\vec{x}; \vec{z}); (\vec{a}; \vec{c})}(\vec{u}, \vec{v}) \& E(\vec{s}) = \llbracket \alpha \rrbracket_C(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}).$$

A partir destas observações, vamos provar o resultado. Suponha que $\mathcal{I}$ satisfaz as hipóteses do enunciado.

Se $\Delta = \emptyset$, seja $\Gamma = \alpha_1, \dots, \alpha_n$ e $\text{red}(\Gamma) = \beta_1, \dots, \beta_k$ tal que $\mathcal{I}$ satisfaz $K_E(\text{red}(\Gamma), C, T)$, e considere $F_i = \llbracket \beta_i \rrbracket_C$ e $G_i = \llbracket \beta_i \rrbracket_{C'}$ para $i = 1, \dots, k$. Pela proposição 2.3.8, toda F_i é extensível à esquerda de C para $((\vec{x}; \vec{z}); (\vec{a}; \vec{c}))$. Por outro lado, como $\mathcal{I}$ satisfaz S , então $F_1 \& \dots \& F_k = \mathbf{0}$, donde

$$F_1(\pi^*) \& \dots \& F_k(\pi^*) \leq \pi^*(F_1) \& \dots \& \pi^*(F_k) \leq \pi^*(F_1 \& \dots \& F_k) = \mathbf{0};$$

logo,

$$G_1(\vec{u}, \vec{v}, \vec{s}) \& \dots \& G_k(\vec{u}, \vec{v}, \vec{s}) = F_1(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}) \& \dots \& F_k(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}) = \mathbf{0}.$$

Se $\Delta = \alpha \in \text{FOR}(\mathbb{L})$ e $\Gamma = \emptyset$, então $F = \llbracket \alpha \rrbracket_C = \llbracket V_C(\alpha) \rrbracket_C$; com a mesma notação que acima, a proposição 2.3.8 fornece

$$(1) \quad \pi^*(F) \leq F(\pi^*) = \llbracket \alpha \rrbracket_{(\vec{x}; \vec{z}); (\vec{a}; \vec{c})}.$$

Se $p = \llbracket \epsilon(T) \rrbracket = EP_{(\vec{z}; \vec{c})}$, então

$$(2) \quad \pi^*(F)(\vec{u}, \vec{v}) = (p \wedge \llbracket V_C(\alpha) \rrbracket) \& E(\vec{u}) \& E(\vec{v}).$$

Por indução na complexidade de uma fórmula ϕ , é fácil provar que, se $C \subseteq D$ são dois contextos para ϕ , então

$$(3) \quad \llbracket V_D(\phi) \rrbracket \leq \llbracket V_C(\phi) \rrbracket \wedge \llbracket \epsilon(D) \rrbracket$$

para toda $\mathcal{I}$; assim, dado que $EP_{C'} = p \wedge EP_C$, temos, por (3), (2), (1),

$$\begin{aligned} \llbracket V_{C'}(\alpha) \rrbracket_{C'}(\vec{u}, \vec{v}, \vec{s}) &= \llbracket V_{C'}(\alpha) \rrbracket \& E(\vec{u}) \& E(\vec{v}) \& E(\vec{s}) \\ &\leq (\llbracket V_C(\alpha) \rrbracket \wedge p) \& E(\vec{u}) \& E(\vec{v}) \& E(\vec{s}) = \pi^*(F)(\vec{u}, \vec{v}) \& E(\vec{s}) \\ &\leq F(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}) = \llbracket \alpha \rrbracket_{C'}(\vec{u}, \vec{v}, \vec{s}). \end{aligned}$$

Finalmente, se $\Gamma = \alpha_1, \dots, \alpha_n$, $\Delta = \alpha$ e $\text{red}(\Gamma) = \beta_1, \dots, \beta_k$ tal que $\mathcal{I}$ satisfaz $K_E(\text{red}(\Gamma), C, T)$, sejam

$$F_i = \llbracket \beta_i \rrbracket_C, \quad G_i = \llbracket \beta_i \rrbracket_{C'}, \quad F = \llbracket \alpha \rrbracket_C, \quad G = \llbracket \alpha \rrbracket_{C'}.$$

Como $\mathcal{I} \models S$, então $F_1 \& \dots \& F_k \leq F$. Assim, usando *exchange* e idempotência,

$$\begin{aligned}
G_1(\vec{u}, \vec{v}, \vec{s}) \& \cdots \& G_k(\vec{u}, \vec{v}, \vec{s}) &= (F_1(\pi^*)(\vec{u}, \vec{v}) \& \cdots \& F_k(\pi^*)(\vec{u}, \vec{v})) \& E(\vec{s}) \\
&\leq (\pi^*(F_1)(\vec{u}, \vec{v}) \& \cdots \& \pi^*(F_k)(\vec{u}, \vec{v})) \& E(\vec{s}) \\
&\leq \pi^*(F_1 \& \cdots \& F_k)(\vec{u}, \vec{v}) \& E(\vec{s}) \leq \pi^*(F)(\vec{u}, \vec{v}) \& E(\vec{s}) \\
&\leq F(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}) = G(\vec{u}, \vec{v}, \vec{s}).
\end{aligned}$$

O caso em que $T = \emptyset$, i.e., $(\vec{z}; \vec{c}) = \emptyset$ e π a função identidade, pode ser tratado com um raciocínio análogo. $\square$

Lema 2.3.12 : *Seja $S : \Gamma \vdash \Delta$ um sequente, T um conjunto de tipos, $C = (\vec{x}; \vec{a})$ o contexto de S , $C_1 = (\vec{y}; \vec{b})$ um contexto tal que $\mathbf{tipos}(C_1) - \mathbf{tipos}(C) = T$ e $C' = ((\vec{x}; \vec{y} - \vec{x}); (\vec{a}; \vec{b} - \vec{a}))$. Se $\mathcal{I}$ é uma interpretação tal que $(\mathcal{I}, C') \models S$ e $\mathcal{I}$ satisfaz $R(S, T)$, então S é válido em $\mathcal{I}$.*

Demonstração: Utilizaremos a mesma notação que em 2.3.11; assim,

$$C' = ((\vec{x}; \vec{z}; \vec{w}); (\vec{a}; \vec{c}; \vec{d})), \quad \pi : P_C \times P_{(\vec{z}; \vec{c})} \longrightarrow P_C$$

têm o mesmo significado que em 2.3.11. Se $\Gamma = \alpha_1, \dots, \alpha_n$, $\Delta = \alpha$ e $\mathbf{red}(\Gamma) = \beta_1, \dots, \beta_k$ tal que $\mathcal{I}$ satisfaz $K_D(\mathbf{red}(\Gamma), C, T)$, sejam

$$F_i = \llbracket \beta_i \rrbracket_C, \quad G_i = \llbracket \beta_i \rrbracket_{C'}$$

para todo $i = 1, \dots, k$. Como $\llbracket \epsilon(T) \rrbracket = EP_{(\vec{z}; \vec{c})}$, temos que

$$\begin{aligned}
(1) \quad G_i(\vec{u}, \vec{v}, \vec{s}) &= F_i(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}) \geq \pi^*(F_i)(\vec{u}, \vec{v}) \& E(\vec{s}) \\
&= (EF_i \wedge \llbracket \epsilon(T) \rrbracket) \& F_i(\vec{u}) \& E(\vec{v}) \& E(\vec{s}),
\end{aligned}$$

por hipótese e a proposição 2.3.8. Logo, como $(\mathcal{I}, C') \models S$, temos, por (1), *exchange* e idempotência,

$$\begin{aligned}
(2) \quad \prod_{i=1}^k (EF_i \wedge \llbracket \epsilon(T) \rrbracket) \& (F_1(\vec{u}) \& \cdots \& F_k(\vec{u})) \& E(\vec{v}) \& E(\vec{s}) &= \\
&= \pi^*(F_1)(\vec{u}, \vec{v}) \& E(\vec{s}) \& \cdots \& \pi^*(F_k)(\vec{u}, \vec{v}) \& E(\vec{s}) \leq \\
&\leq G_1(\vec{u}, \vec{v}, \vec{s}) \& \cdots \& G_k(\vec{u}, \vec{v}, \vec{s}) \leq \llbracket \alpha \rrbracket_{C'}(\vec{u}, \vec{v}, \vec{s}) \leq \llbracket \alpha \rrbracket_C(\vec{u}).
\end{aligned}$$

Assim, tomando supremo sobre $\vec{v} \in D_{(\vec{z}; \vec{a}, \vec{c}, \vec{d})}$ e $\vec{s} \in D_{(\vec{w}; \vec{a}, \vec{c}, \vec{d})}$ em (2), obtemos

$$(3) \quad \prod_{i=1}^k (EF_i \wedge \llbracket \epsilon(T) \rrbracket) \& (F_1(\vec{u}) \& \cdots \& F_k(\vec{u})) \& p_1 \& p_2 \leq \llbracket \alpha \rrbracket_C(\vec{u}),$$

onde $p_1 \geq EP_{(\vec{z}; \vec{a}, \vec{c}, \vec{d})}$ e $p_2 \geq EP_{(\vec{w}; \vec{a}, \vec{c}, \vec{d})}$; observe que $p_1, p_2 \geq EP_{C'}$. Como $\mathcal{I} \models S_\Gamma$, temos

$$(4) \quad E(\prod_{i=1}^k F_i) \leq \prod_{i=1}^k (EF_i \wedge \llbracket \epsilon(T) \rrbracket) \leq EP_{C'},$$

pois, para todo $i = 1, \dots, k$,

$$\llbracket (\exists)(\beta_i)_C \wedge \epsilon(T) \rrbracket_{\vec{a}} = \llbracket (\exists)(\beta_i)_C \rrbracket_{\vec{a}} \wedge \llbracket \epsilon(T) \rrbracket_{\vec{a}} = EF_i \wedge EP_{\vec{a}} \wedge \llbracket \epsilon(T) \rrbracket = EF_i \wedge \llbracket \epsilon(T) \rrbracket.$$

Assim, por (3), (4) e [char3], temos que, para todo $\vec{u} \in D_{(\vec{x}; \vec{a}, \vec{c}, \vec{d})}$,

$$F_1(\vec{u}) \& \cdots \& F_k(\vec{u}) \leq \llbracket \alpha \rrbracket_C(\vec{u}).$$

Portanto, se $\vec{x} = x_1, \dots, x_m$, com $x_j \in \mathcal{V}_{t_j}$, então, para todo i, j ,

$$EF_i \wedge [\epsilon(T)] \leq EA_{t_j} \wedge EP_{(\vec{a}; \vec{c}; \vec{d})} = s_j$$

e logo, $EF_i \wedge [\epsilon(T)] \leq \prod_{j=1}^m s_j = s$ para todo i , donde, por (4), $E(\prod_i F_i) \leq s$. Assim, se $\vec{u} = (u_1, \dots, u_m) \in D_{(\vec{x}; \vec{a})}$, $v_j = u_{j|s_j}$, e $\vec{v} = (v_1, \dots, v_m) \in D_{(\vec{x}; \vec{a}; \vec{c}; \vec{d})}$, obtemos

$$(\prod_i F_i)(\vec{u}) = (\prod_i F_i)(\vec{u}) \& s = (\prod_i F_i)(\vec{v}) \leq [\alpha]_C(\vec{v}) = [\alpha]_C(\vec{u}) \& s \leq [\alpha]_C(\vec{u}),$$

donde $\mathcal{I} \models S$. Se $\vec{x} = \emptyset$, a prova acima ainda é válida (considerando $[\alpha]_{\vec{a}}, F_i : \mathbf{1}_{|EP_C} \rightarrow Q$). Uma prova análoga funciona no caso de $\Delta = \emptyset$. Se $\Gamma = \emptyset$ e $\Delta = \alpha$, então, por hipótese, $\mathcal{I} \models (\epsilon(C) \vdash \epsilon(T))$, donde $EP_{C'} = [\epsilon(C)] \wedge [\epsilon(T)] = [\epsilon(C)] = EP_C$. É simples provar, por indução na complexidade de α , que $[V_C(\alpha)] = [V_{C'}(\alpha)]$; logo

$$\begin{aligned} [V_C(\alpha)] \& E(\vec{u}) \& E(\vec{v}) \& E(\vec{s}) &= [V_{C'}(\alpha)] \& E(\vec{u}) \& E(\vec{v}) \& E(\vec{s}) \\ &= [V_{C'}(\alpha)]_{C'}(\vec{u}, \vec{v}, \vec{s}) = [\alpha]_{C'}(\vec{u}, \vec{v}, \vec{s}) = [\alpha]_C(\pi^*)(\vec{u}, \vec{v}) \& E(\vec{s}) \\ &\leq (E[\alpha]_C \wedge [\epsilon(T)]) \& [\alpha]_C(\vec{u}) \& E(\vec{v}) \& E(\vec{s}) \leq [\alpha]_C(\vec{u}) \end{aligned}$$

donde, tomando supremo sobre $\vec{v} \in D_{(\vec{x}; \vec{a}; \vec{c}; \vec{d})}$ e $\vec{s} \in D_{(\vec{w}; \vec{a}; \vec{c}; \vec{d})}$, obtemos

$$[V_C(\alpha)] \& E(\vec{u}) = [V_C(\alpha)] \& E(\vec{u}) \& p_1 \& p_2 \leq [\alpha]_C(\vec{u})$$

para todo $\vec{u} \in D_{(\vec{x}; \vec{a}; \vec{c}; \vec{d})}$ (pois $EP_C = EP_{C'} = r \leq p_1, p_2$). Logo, temos que, para todo $\vec{u} \in D_{(\vec{x}; \vec{a})}$,

$$[V_C(\alpha)] \& E(\vec{u}) = [V_C(\alpha)] \& E(\vec{u}) \& r = [V_C(\alpha)] \& E(\vec{u}|_r) \leq [\alpha]_C(\vec{u}|_r) = [\alpha]_C(\vec{u}) \& r = [\alpha]_C(\vec{u}).$$

O caso em que $T = \emptyset$ está claro. $\square$

Para definir as regras para os quantificadores, estudaremos os casos em que os seguintes

$$(\forall x)\phi(x, \vec{x}) \vdash \phi(x, \vec{x})[\tau/x], \quad \phi(x, \vec{x})[\tau/x] \vdash (\exists x)\phi(x, \vec{x})$$

são válidos, sendo τ um termo arbitrário livre para x em ϕ . Dado o carácter da interpretação de fórmulas, calcular $\phi[\tau/x]$ não é simplesmente calcular $[\phi]$ em $x = [\tau](\vec{u})$ no contexto apropriado, pois a interpretação de $\phi[\tau/x]$ envolve o cálculo de uma imagem inversa, operação que, como já foi provado, não respeita em geral os conectivos; assim, em geral

$$[\phi(x)]_x([\tau(\vec{y})]_{\vec{y}}(\vec{u})) \neq [\phi(\tau(\vec{y}))]_{\vec{y}}(\vec{u}).$$

Mais precisamente, dada uma interpretação $\mathcal{I}$, se $R \subseteq A_x \times B$ denota o prefeixe associado com $[\phi(x, \vec{x})]_{(x, \vec{x}); \vec{a}}$, $B = P_{(\vec{x}; \vec{a})}$ e A_x é o prefeixe interpretando o tipo de x , considere $g = [\tau(\vec{y}; \vec{b})]_{\vec{y}; \vec{b}}$, onde $C(\tau) = (\vec{y}; \vec{b})$. Seja A o prefeixe obtido do contexto $((\vec{y} - \vec{x}); (\vec{b} - \vec{a}))$, C o contexto $((\vec{x}; (\vec{y} - \vec{x})); (\vec{a}; (\vec{b} - \vec{a})))$ e considere os morfismos

$$g_1 = [\tau(\vec{y}; \vec{b})]_C : B \times A \rightarrow A_x, \quad \pi_1 : B \times A \rightarrow B,$$

$$f = \langle g_1, \pi_1 \rangle: B \times A \longrightarrow A_x \times B, \quad \pi: (A_x \times B) \times A \longrightarrow A_x \times B,$$

onde π_1 e π denotam as projeções. Observe que $f(\vec{u}, \vec{v}) = (g_1(\vec{u}, \vec{v}), \vec{u}) = (g(\vec{w}), \vec{u})$, onde $\vec{u}$, $\vec{v}$ e $\vec{w}$ são os parâmetros correspondentes a $\vec{x}$, $\vec{y} - \vec{x}$ e $\vec{y}$, respectivamente (e podemos ter $\vec{y} \cap \vec{x} \neq \emptyset$). Logo, se z é variável nova livre para x em $\phi(x, \vec{x})$,

$$\llbracket \phi(x, \vec{x})[\tau/x] \rrbracket_C \simeq R(f^*), \quad \llbracket \phi(x, \vec{x})[z/x] \rrbracket_{(z,C)} \simeq R(\pi^*),$$

e a expressão correta para avaliar ϕ em τ é então $R(f^*)$. Assim, gostaríamos de ter

$$[R(f^*)](\vec{u}, \vec{v}) = [R(\pi^*)](f((\vec{u}, \vec{v})_{|p \& E(\vec{u}) \& E(\vec{v})}), \vec{v})$$

para todo $\vec{u} \in D_{(\vec{x}; \vec{a}, \vec{b} - \vec{a})}$, $\vec{v} \in D_{(\vec{y} - \vec{x}; \vec{a}, \vec{b} - \vec{a})}$, onde $p = EP_C = EP_C \wedge EA_x$ (por causa de g_1); assim a formulação correta do **Lema de Substituição** é a seguinte:

$$\llbracket \phi[\tau/x] \rrbracket_C(\vec{u}) = \llbracket \phi[z/x] \rrbracket_{(z,C)}(\llbracket \tau \rrbracket_C(\vec{u}), \vec{u})$$

para todo $\vec{u} \in P_C$, onde C é o contexto de $\phi[\tau/x]$ (a variável z é introduzida para permitir que a variável x possa aparecer em τ). Este é exatamente o problema estudado no lema 1.4.17. Assim, adaptando 1.4.14, temos a

Definição 2.3.13 : Seja ϕ uma fórmula, $x_1 < \dots < x_k$ variáveis (na ordem de $\mathcal{V}$), τ_i um termo livre para x_i em ϕ ($i = 1, \dots, k$) e $C \supseteq C(\phi[\vec{\tau}/\vec{x}] \otimes E(\vec{\tau}))$, onde $\vec{\tau}$ denota a sequência $\tau_1, \dots, \tau_k$, $\vec{x}$ denota $x_1, \dots, x_k$, $E(\vec{\tau})$ denota a fórmula $E\tau_1 \otimes \dots \otimes E\tau_k$ e $\phi[\vec{\tau}/\vec{x}]$ é a fórmula obtida de ϕ substituindo simultaneamente todas as ocorrências livres de x_i em ϕ (se houver) pelo termo τ_i ($i = 1, \dots, k$). Seja z_1 a primeira variável livre para x_1 em ϕ que não ocorre em C ; seja z_2 a primeira variável livre para x_2 em ϕ que não ocorre em (z_1, C) ; continuando com este procedimento, seja z_n a primeira variável livre para x_n em ϕ que não ocorre em $(z_1, \dots, z_{n-1}, C)$. Seja $\mathcal{I}$ uma interpretação.

Dizemos que ϕ é consistente (à direita, à esquerda) para $\vec{\tau}, \vec{x}$ em $C, \mathcal{I}$ se satisfaz:

$$\llbracket \phi[\vec{\tau}/\vec{x}] \rrbracket_C(\vec{u}) = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}, C)}(\llbracket \tau_1 \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}), \dots, \llbracket \tau_k \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}), \vec{u})$$

(resp., $\geq$, $\leq$), onde $p = EP_C = EP_{(\vec{z}, C)}$.

Observação 2.3.14 : Com a notação de 2.3.13, considere os contextos

$$C_1 = C((\exists \vec{z})\phi[\vec{z}/\vec{x}]), \quad C_2 = C(\phi[\vec{\tau}/\vec{x}] \otimes E(\vec{\tau})), \quad C \supseteq C_2, \quad C_3 = (\vec{z}; C_1; C - C_2)$$

(observando que $\vec{z}$, C_1 e $C - C_2$ são dois a dois disjuntos, pois as variáveis em $\vec{z}$ são novas). Dada uma interpretação $\mathcal{I}$, considere os prefixos

$$A = P_{C(\vec{\tau}) - C_1}, \quad B = P_{C_1; C - C_2}, \quad P = P_{\vec{z}}.$$

Então $P_C = B \times A$, $\alpha = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C_3}$ é um esquema em $P \times B$ na estrutura $\mathcal{I}$ e

$$g = \langle \llbracket \tau_1 \rrbracket_C, \dots, \llbracket \tau_k \rrbracket_C \rangle: B \times A \longrightarrow P.$$

Portanto, considerando

$$\pi_1 : B \times A \longrightarrow B, \quad \pi : (P \times B) \times A \longrightarrow P \times B, \quad f = \langle g, \pi_1 \rangle : B \times A \longrightarrow P \times B,$$

onde π_1 e π denotam projeções, as definições implicam que

$$\llbracket \phi[\vec{\tau}/\vec{x}] \rrbracket_C = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C_3}(f^*), \quad \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z};C)} = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C_3}(\pi^*).$$

É imediato das definições que ϕ é consistente (à direita, à esquerda) para $\vec{\tau}, \vec{x}$ em $C, \mathcal{I}$ sse o esquema α satisfaz $[S =]$ (resp., $[S D]$, $[S E]$) na estrutura $\mathcal{I}$ para $f = \langle g, \pi_1 \rangle$ (definição 1.4.14), fixados domínios $D = D_C \in DF(B \times A)$ e $D' = D_{(\vec{z};\vec{a})} \times D \in DF(P \times B \times A)$, onde $C = (\vec{w}; \vec{a})$. $\square$

Podemos formular as cláusulas correspondentes às condições suficientes de consistência 1.4.15 da maneira seguinte:

Definição 2.3.15 : *Sejam ϕ , $\vec{\tau}$, $\vec{x}$, $\vec{z}$ e $C = (\vec{w}; \vec{a})$ como na definição 2.3.13. Considere os conjuntos finitos*

$$\text{disj}(\phi) = \{\alpha \vee \beta : \alpha \vee \beta \in SF(\phi)\},$$

$$\text{disj}_1(\phi) = \{\alpha \vee \beta : \alpha \vee \beta \in SF(\delta), \delta \multimap \gamma \in SF(\phi)\}.$$

(i) *Dada $\alpha \vee \beta \in SF(\phi)$, seja $\vec{u} = (\vec{z} - \vec{x}; \vec{x})$, $C' = ((\vec{u}; \vec{w} - \vec{u}); \vec{a})$ o contexto obtido de C , $\vec{x}$, $\vec{z}$, e considere $\mathbf{C}(\alpha \vee \beta, \phi, C') = (\vec{y}, C')$. Definimos a seguinte cláusula:*

$$T(\alpha \vee \beta, (\vec{\tau}; \vec{x}), \phi, C) = \{\{T_1\}, \{T_2, T_3, T_4, T_5\}\},$$

onde

$$\begin{aligned} T_1 &: (\exists)(\alpha[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)} \vee (\exists)(\beta[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)} \\ &\quad \vdash (\exists)(\alpha[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)} \vee (\exists)(\beta[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)}, \\ T_2 &: (\exists)(\beta[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)} \otimes (\exists)(\alpha[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)} \vdash (\exists)(\alpha[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)}, \\ T_3 &: (\exists)(\alpha[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)} \otimes (\exists)(\beta[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)} \vdash (\exists)(\beta[\vec{y}/\vec{v}][\vec{\tau}/\vec{x}])_{(\vec{y},C)}, \\ T_4 &: (\exists)(\beta[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)} \otimes (\exists)(\alpha[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)} \vdash (\exists)(\alpha[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)}, \\ T_5 &: (\exists)(\alpha[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)} \otimes (\exists)(\beta[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)} \vdash (\exists)(\beta[\vec{y}/\vec{v}][\vec{z}/\vec{x}])_{(\vec{y};\vec{z},C)}. \end{aligned}$$

(ii) *Definimos a seguinte cláusula:*

$$C_=(\phi, (\vec{\tau}; \vec{x}), C) = \{\bigcup_{i=1}^r x_i : x_i \in T(\alpha_i \vee \beta_i, (\vec{\tau}; \vec{x}), \phi, C) \ (i = 1, \dots, r)\}$$

se $\text{disj}(\phi) = \{\alpha_i \vee \beta_i : i \leq r\}$, ou $C_=(\phi, (\vec{\tau}; \vec{x}), C) = \{x_\top\}$ se $\text{disj}(\phi) = \emptyset$.

(iii) *Definimos a cláusula*

$$C_E(\phi, (\vec{\tau}; \vec{x}), C) = \{\bigcup_{i=1}^r x_i : x_i \in T(\alpha_i \vee \beta_i, (\vec{\tau}; \vec{x}), \phi, C) \ (i = 1, \dots, r)\}$$

se $\text{disj}_1(\phi) = \{\alpha_i \vee \beta_i : i \leq r\}$, ou $C_E(\phi, (\vec{\tau}; \vec{x}), C) = \{x_\top\}$ se $\text{disj}_1(\phi) = \emptyset$.

(iv) Definimos por indução na complexidade de ϕ a cláusula $C_D(\phi, (\vec{\tau}; \vec{x}), C)$, como se segue :

(1) Se ϕ é atômica, então $C_D(\phi, (\vec{\tau}; \vec{x}), C) = \{x_\top\}$;

(2) Se $\phi = \alpha * \beta$, com $*$ = $\wedge, \otimes$, então

$$C_D(\phi, (\vec{\tau}; \vec{x}), C) = \{x \cup y : x \in C_D(\alpha, (\vec{\tau}; \vec{x}), C), y \in C_D(\beta, (\vec{\tau}; \vec{x}), C)\} \cup C_=(\phi, (\vec{\tau}; \vec{x}), C);$$

(3) Se $\phi = \alpha \multimap \beta$, então

$$C_D(\phi, (\vec{\tau}; \vec{x}), C) = \{x \cup y : x \in C_E(\alpha, (\vec{\tau}; \vec{x}), C), y \in C_D(\beta, (\vec{\tau}; \vec{x}), C)\} \cup C_=(\phi, (\vec{\tau}; \vec{x}), C);$$

(4) Se $\phi = \neg\psi$, então

$$C_D(\phi, (\vec{\tau}; \vec{x}), C) = C_E(\psi, (\vec{\tau}; \vec{x}), C) \cup C_=(\phi, (\vec{\tau}; \vec{x}), C);$$

(5) Se $\phi = \alpha \vee \beta$, então

$$C_D(\phi, (\vec{\tau}; \vec{x}), C) = \{x \cup y \cup z : x \in C_D(\alpha, (\vec{\tau}; \vec{x}), C), y \in C_D(\beta, (\vec{\tau}; \vec{x}), C), \\ z \in T(\alpha \vee \beta, (\vec{\tau}; \vec{x}), \alpha \vee \beta, C)\} \cup C_=(\phi, (\vec{\tau}; \vec{x}), C);$$

(6) Se $\phi = (Qv)\psi$, com $Q = \forall, \exists$, seja y a primeira livre para v em ψ que não ocorre em $\vec{x}$ nem em C ; então

$$C_D(\phi, (\vec{\tau}; \vec{x}), C) = C_D(\psi[y/v], (y, \vec{\tau}; y, \vec{x}), C) \cup C_=(\phi, (\vec{\tau}; \vec{x}), C).$$

Lema 2.3.16 : Com a notação da observação 2.3.14, seja $\mathcal{I}$ uma interpretação.

(1) Se $\mathcal{I}$ satisfaz $C_=(\phi, (\vec{\tau}; \vec{x}), C)$, então $\llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C_3} \in C_=(f)$ na estrutura $\mathcal{I}$ (definição 1.4.15) para $f = \langle \llbracket \tau_1 \rrbracket_C, \dots, \llbracket \tau_k \rrbracket_C, \pi_1 \rangle$, fixados os domínios D e D' .

(2) O mesmo resultado vale para $C_E(\phi, (\vec{\tau}; \vec{x}), C)$ e $C_D(\phi, (\vec{\tau}; \vec{x}), C)$.

Demonstração: Imediata a partir das definições e a observação 2.3.14. $\square$

Corolário 2.3.17 : Sejam $\phi, \vec{\tau}, \vec{x}$ e C como na definição 2.3.13 e $\mathcal{I}$ uma interpretação.

Se $\mathcal{I}$ satisfaz $C_=(\phi, (\vec{\tau}; \vec{x}), C)$, então ϕ é consistente para $\vec{\tau}, \vec{x}$ em $C, \mathcal{I}$. O mesmo resultado vale à direita e à esquerda.

Demonstração: É imediata a partir do lema 2.3.16, do lema 1.4.17 e da observação 2.3.14. $\square$

2.4 O Cálculo (QPC)

Nesta seção definiremos um cálculo de primeira ordem, indicado por (QPC), tendo a discussão anterior como parâmetro. (QPC) será parecido com o cálculo linear intuicionista com igualdade

discutido no Apêndice I, o que não deve surpreender, dada a relação entre lógica linear e quantais. Uma particularidade do cálculo, mencionada anteriormente, é que cada regra $\mathcal{R}$ (junto com o axioma de substituição) terá associada uma cláusula, denotada $\text{clau}(\mathcal{R})$, de maneira que, para poder aplicar a regra, será necessário provar todos os sequentes de alguma justificativa de $\text{clau}(\mathcal{R})$.

Definição 2.4.1 *Sejam ϕ, ψ, α fórmulas, Γ, Δ, Θ sequências finitas (eventualmente vazias) de fórmulas, $\tau, \kappa, \rho, \tau_i, \kappa_i$ termos ($i = 1, \dots, n$), f um símbolo de função (de aridade n) e s, t tipos.*

O cálculo (QPC) consiste dos seguintes axiomas e regras :

Axiomas:

$$[EX] \quad (\exists x_1)Ex_1 \wedge \dots \wedge (\exists x_n)Ex_n \vdash (\exists x)Ex$$

para cada símbolo funcional $f : t_1 \times \dots \times t_n \rightarrow t$ na linguagem, com $x_i \in \mathcal{V}_{t_i}$ ($i = 1, \dots, n$) e $x \in \mathcal{V}_t$.

$$[CH1.0] \quad \phi_C \vdash V_C(\phi) \quad (C(\phi) \subseteq C)$$

$$[CH1.1] \quad \phi \vdash \phi \otimes (E\tau_1 \otimes \dots \otimes E\tau_k)$$

$$[CH3] \quad \phi[y/x], \phi \vdash \phi \quad (y \text{ livre para } x \text{ em } \phi)$$

$$[AX1] \quad \Gamma \vdash \top$$

$$[AX2] \quad \phi \vdash \phi \otimes \phi$$

$$[AX3] \quad \phi, \Gamma \vdash \phi$$

$$[AX4] \quad \Gamma, \neg\phi \vdash \neg\phi$$

$$[AX5] \quad \Gamma, \phi \multimap \psi \vdash \phi \multimap \psi$$

$$[E1] \quad E\tau \vdash (\tau = \tau)$$

$$[E2] \quad (\tau = \tau) \vdash E\tau$$

$$[E3] \quad (\tau = \kappa) \vdash (\kappa = \tau)$$

$$[E4] \quad (\tau = \kappa), (\kappa = \rho) \vdash (\tau = \rho)$$

$$[E5] \quad \Gamma, (\tau = \kappa) \vdash (\tau = \kappa)$$

$$[E6] \quad (\tau_1 = \kappa_1), \dots, (\tau_n = \kappa_n) \vdash (f(\tau_1, \dots, \tau_n) = f(\kappa_1, \dots, \kappa_n))$$

$$[SUBS] \quad \phi[\vec{\tau}/\vec{x}], (\tau_1 = \kappa_1), \dots, (\tau_n = \kappa_n) \vdash \phi[\vec{\kappa}/\vec{x}]$$

onde $\vec{\tau} = \tau_1, \dots, \tau_n$, $\vec{\kappa} = \kappa_1, \dots, \kappa_n$, $\vec{x} = x_1, \dots, x_n$, e τ_i e κ_i são termos livres para x_i em ϕ .

$$\text{clau}([SUBS]) = \{y_1 \cup y_2 : y_1 \in C_E(\phi, (\vec{\tau}; \vec{x}), C), y_2 \in C_D(\phi, (\vec{\kappa}; \vec{x}), C)\}$$

onde $C = C(\phi[\vec{\tau}/\vec{x}] \otimes E(\vec{\tau}) \otimes E(\vec{\kappa}))$.

Regras estruturais:

$$[CUT] \quad \frac{S_1 : \Gamma \vdash \Phi \quad S_2 : \Sigma, \Phi, \Delta \vdash \Theta}{S_3 : \Sigma, \Gamma', \Delta \vdash \Theta}$$

onde $\Gamma' = \Gamma$ se $\Gamma \neq \emptyset$, ou $\Gamma' = V_C(\phi)$ se $\Gamma = \emptyset$, $\Phi = \phi$ e C é o contexto de ϕ .

$$\text{clau}([CUT]) = \{y_1 \cup y_2 \cup y_3 : y_1 \in E(S_1, T_1), y_2 \in E(S_2, T_2), y_3 \in R(S_3, T_3)\},$$

onde $T_1 = \text{Etipos}(S_2) - \text{Etipos}(S_1)$, $T_2 = \text{Etipos}(S_1) - \text{Etipos}(S_2)$ e $T_3 = \text{Etipos}(\Phi) - \text{Etipos}(S_3)$.

$$[WR] \quad \frac{S_1 : \Gamma \vdash}{S_2 : \Gamma \vdash \phi}$$

$$[WL] \quad \frac{S_1 : \Gamma \vdash}{S_3 : \phi, \Gamma \vdash}$$

com $\Gamma \neq \emptyset$.

$$\text{clau}([WR]) = \text{clau}([WL]) = E(S_1, T),$$

onde $T = \text{Etipos}(\phi) - \text{Etipos}(\Gamma)$.

Regras de quantificação: Para estas regras, o termo τ e a variável y são livres para x em ϕ .

$$[\forall L] \quad \frac{S_1 : \Gamma, \phi[\tau/x], \Delta \vdash \Theta}{S_2 : \Gamma, (\forall x)\phi, \Delta \vdash \Theta}$$

– se $\tau \in \mathcal{V}$, temos

$$\text{clau}([\forall L]) = \{y_1 \cup y_2 : y_1 \in E(S_1, T_1), y_2 \in R(S_2, T_2)\};$$

– se $\tau \notin \mathcal{V}$, temos

$$\text{clau}([\forall L]) = \{y_1 \cup y_2 \cup y_3 : y_1 \in E(S_1, T_1), y_2 \in R(S_2, T_2), y_3 \in C_D(\phi, (\tau; x), C)\},$$

onde $T_1 = \text{tipos}(\tau) - \text{Etipos}(S_1)$, $T_2 = \text{tipos}(\tau) - \text{Etipos}(S_2)$, $C = C(\Gamma, \phi[\tau/x] \otimes E\tau, \Delta, \Theta)$.

$$[\forall R] \quad \frac{S_1 : \Gamma \vdash \phi[y/x]}{S_2 : \Gamma \vdash (\forall x)\phi}$$

onde y não ocorre livre em S_2 , com as cláusulas:

– se $\Gamma \neq \emptyset$,

$$\text{clau}([\forall R]) = \{y_1 \cup y_2 : y_1 \in E(S_1, T_1), y_2 \in R(S_2, T_2)\};$$

– se $\Gamma = \emptyset$, $\text{clau}([\forall R]) = E(S_1, T_1)$,

onde $T_1 = \text{tipos}(y) - \text{Etipos}(S_1)$, $T_2 = \text{tipos}(y) - \text{Etipos}(S_2)$.

$$[\exists L] \quad \frac{S_1 : \Gamma, \phi[y/x], \Delta \vdash \Theta}{S_2 : \Gamma, (\exists x)\phi, \Delta \vdash \Theta}$$

onde y não ocorre livre em S_2 , com as cláusulas:

– se $\Gamma, \Delta, \Theta \neq \emptyset$, temos

$$\text{clau}([\exists L]) = \{y_1 \cup y_2 : y_1 \in E(S_1, T_1), y_2 \in R(S_2, T_2)\};$$

– se $\Gamma, \Delta, \Theta = \emptyset$, temos $\text{clau}([\exists L]) = E(S_1, T_1)$,

onde $T_1 = \text{tipos}(y) - \text{Etipos}(S_1)$ e $T_2 = \text{tipos}(y) - \text{Etipos}(S_2)$.

$$[\exists R] \quad \frac{S_1 : \Gamma \vdash \phi[\tau/x]}{S_2 : \Gamma \vdash (\exists x)\phi}$$

– se $\tau \in \mathcal{V}$ e $\Gamma \neq \emptyset$, temos a cláusula

$$\text{clau}([\exists R]) = \{y_1 \cup y_2 : y_1 \in E(S_1, T_1), y_2 \in R(S_2, T_2)\};$$

– se $\tau \in \mathcal{V}$ e $\Gamma = \emptyset$, temos a cláusula

$$\text{clau}([\exists R]) = \{y_1 \cup y_2 \cup \{\epsilon(C_1) \vdash \epsilon(C_2)\} : y_1 \in E(S_1, T_1), y_2 \in K_E((\exists x)\phi, C_3, T_2,)\};$$

– se $\tau \notin \mathcal{V}$, $\Gamma \neq \emptyset$, temos

$$\text{clau}([\exists R]) = \{y_1 \cup y_2 \cup y_3 : y_1 \in E(S_1, T_1), y_2 \in R(S_2, T_2), y_3 \in C_E(\phi, (\tau; x), C)\};$$

– se $\tau \notin \mathcal{V}, \Gamma = \emptyset$, temos

$$\text{clau}([\exists R]) = \{y_1 \cup y_2 \cup y_3 \cup \{\epsilon(C_1) \vdash \epsilon(C_2)\} : y_1 \in E(S_1, T_1), y_2 \in K_E((\exists x)\phi, C_3, T_2), \\ y_3 \in C_E(\phi, (\tau; x), C)\},$$

onde $T_1 = \mathbf{tipos}(\tau) - \mathbf{Etipos}(S_1)$, $T_2 = \mathbf{tipos}(\tau) - \mathbf{Etipos}(S_2)$, $C = C(\Gamma, \phi[\tau/x] \otimes E\tau)$, z é a primeira variável livre para x em ϕ que não ocorre em C , $C_1 = C(\phi[z/x] \otimes Ez)$, $C_2 = C(\phi[\tau/x] \otimes E\tau)$ e $C_3 = C((\exists x)\phi)$.

Regras para os Conectivos:

$$[\otimes R] \quad \frac{S_1 : \Gamma \vdash \phi \quad S_2 : \Delta \vdash \psi}{S_3 : \Gamma', \Delta' \vdash \phi \otimes \psi},$$

onde $\Gamma', \Delta' = \Gamma, \Delta$ se $\Gamma \neq \emptyset \neq \Delta$, ou se $\Gamma, \Delta = \emptyset$; $\Gamma' = V_C(\phi)$ e $\Delta' = \Delta$ se $\Gamma = \emptyset \neq \Delta$, onde C é o contexto de ϕ ; $\Delta' = V_D(\psi)$ e $\Gamma' = \Gamma$ se $\Delta = \emptyset \neq \Gamma$, onde D é o contexto de ψ .

$$\text{clau}([\otimes R]) = \{x \cup y : x \in E(S_1, T_1), y \in E(S_2, T_2)\},$$

onde $T_1 = \mathbf{Etipos}(S_2) - \mathbf{Etipos}(S_1)$ e $T_2 = \mathbf{Etipos}(S_1) - \mathbf{Etipos}(S_2)$.

$$[\otimes L] \quad \frac{\Gamma, \phi, \psi, \Delta \vdash \Theta}{\Gamma, \phi \otimes \psi, \Delta \vdash \Theta}$$

$$[\wedge R] \quad \frac{S_1 : \Gamma \vdash \phi \quad S_2 : \Gamma \vdash \psi}{S_3 : \Gamma \vdash \phi \wedge \psi}$$

$$\text{clau}([\wedge R]) = \{x \cup y : x \in E(S_1, T_1), y \in E(S_2, T_2)\},$$

onde $T_1 = \mathbf{Etipos}(\psi) - \mathbf{Etipos}(S_1)$ e $T_2 = \mathbf{Etipos}(\phi) - \mathbf{Etipos}(S_2)$.

$$[\wedge L1] \quad \frac{S_1 : \Gamma, \phi, \Delta \vdash \Theta}{S_2 : \Gamma, \phi \wedge \psi, \Delta \vdash \Theta}$$

$$[\wedge L2] \quad \frac{S_3 : \Gamma, \psi, \Delta \vdash \Theta}{S_4 : \Gamma, \phi \wedge \psi, \Delta \vdash \Theta}$$

$$\text{clau}([\wedge L1]) = E(S_1, T_1); \quad \text{clau}([\wedge L2]) = E(S_3, T_2),$$

onde $T_1 = \mathbf{Etipos}(\psi) - \mathbf{Etipos}(S_1)$ e $T_2 = \mathbf{Etipos}(\phi) - \mathbf{Etipos}(S_3)$.

$$[\vee L1] \quad \frac{S_1 : \Gamma, \phi \vdash \Theta \quad S_2 : \Gamma, \psi \vdash \Theta}{S_3 : \Gamma, \phi \vee \psi \vdash \Theta}$$

$$\text{clau}([\vee L1]) = \{x \cup y : x \in E(S_1, T_1), y \in E(S_2, T_2)\},$$

onde $T_1 = \mathbf{Etipos}(\psi) - \mathbf{Etipos}(S_1)$ e $T_2 = \mathbf{Etipos}(\phi) - \mathbf{Etipos}(S_2)$.

$$[\vee L2] \quad \frac{S_1 : \phi, \alpha \vdash \Theta \quad S_2 : \psi, \alpha \vdash \Theta}{S_3 : \phi \vee \psi, \alpha \vdash \Theta}$$

$$\text{clau}([\vee L2]) = \{x \cup y \cup \{S\} : x \in E(S_1, T_1), y \in E(S_2, T_2)\},$$

com $T_1 = \mathbf{Etipos}(\psi) - \mathbf{Etipos}(S_1)$, $T_2 = \mathbf{Etipos}(\phi) - \mathbf{Etipos}(S_2)$, $C = C(S_3)$ e S é o sequente

$$S : ((\exists)\phi_C \vee (\exists)\psi_C) \otimes ((\exists)(\phi \otimes \alpha)_C \vee (\exists)(\psi \otimes \alpha)_C) \vdash (\exists)(\phi \otimes \alpha)_C \vee (\exists)(\psi \otimes \alpha)_C.$$

$$[\vee R1] \quad \frac{S_1 : \Gamma \vdash \phi}{S_2 : \Gamma' \vdash \phi \vee \psi} \quad [\vee R2] \quad \frac{S_3 : \Gamma \vdash \psi}{S_4 : \Gamma' \vdash \phi \vee \psi},$$

onde, em $[\vee R1]$, $\Gamma' = \Gamma$, se $\Gamma \neq \emptyset$, ou $\Gamma' = V_C(\phi)$ se $\Gamma = \emptyset$, sendo C o contexto de ϕ ; em $[\vee R2]$, $\Gamma' = \Gamma$, se $\Gamma \neq \emptyset$, ou $\Gamma' = V_D(\psi)$ se $\Gamma = \emptyset$, sendo D o contexto de ψ .

$$\text{clau}([\vee R1]) = E(S_1, T_1); \quad \text{clau}([\vee R2]) = E(S_3, T_2),$$

com $T_1 = \mathbf{Etipos}(\psi) - \mathbf{Etipos}(S_1)$, $T_2 = \mathbf{Etipos}(\phi) - \mathbf{Etipos}(S_3)$.

$$[\neg O L] \quad \frac{S_1 : \Gamma \vdash \phi \quad S_2 : \Sigma, \psi, \Delta \vdash \Theta}{S_3 : \Sigma, \Gamma', \phi \neg \psi, \Delta \vdash \Theta}$$

onde $\Gamma' = \Gamma$, se $\Gamma \neq \emptyset$ e $\Gamma' = V_C(\phi)$ se $\Gamma = \emptyset$ (sendo C o contexto de ϕ).

$$\text{clau}([\neg O L]) = \{x \cup y : x \in E(S_1, T_1), y \in E(S_2, T_2)\},$$

com $T_1 = \mathbf{Etipos}(S_2) - \mathbf{Etipos}(S_1)$ e $T_2 = \mathbf{Etipos}(S_1) - \mathbf{Etipos}(S_2)$.

$$[\neg O R] \quad \frac{\phi, \Gamma \vdash \psi}{\Gamma \vdash \phi \neg \psi}$$

$$[\neg R] \quad \frac{\phi, \Gamma \vdash}{\Gamma \vdash \neg \phi}$$

$$[\neg L] \quad \frac{\Gamma \vdash \phi}{\Gamma', \neg \phi \vdash}$$

onde $\Gamma' = \Gamma$, se $\Gamma \neq \emptyset$, ou $\Gamma' = V_C(\phi)$ se $\Gamma = \emptyset$, C o contexto de ϕ .

A exigência de justificativas $y_1 \in E(S_1, T_1)$ nas regras de quantificação é que permite quantificar corretamente sobre variáveis que não ocorrem livres na fórmula (e é por isso que em $[\forall L]$ e $[\exists R]$, escrevemos $\phi[\tau/x] \otimes E\tau$ no lugar de $\phi[\tau/x]$); assim, se $x \in VAR(\phi)$, então $T_1 = \emptyset$ e $y_1 = x_\top$, a justificativa trivial. Na regra $[\exists R]$, se $\Gamma \neq \emptyset$, então exigimos uma justificativa $y_2 \in R(S_2, T_2)$; observe que, se $\Gamma = \emptyset$, então toda $y_2 \in R(S_2, T_2)$ é da forma $z_2 \cup \{\epsilon((\exists x)\phi) \vdash \epsilon(T_2)\}$, com $z_2 \in K_E((\exists x)\phi, C_3, T_2)$, logo, o sequente $\epsilon((\exists x)\phi) \vdash \epsilon(T_2)$ foi substituído, na cláusula da regra pelo sequente $\epsilon(C_1) \vdash \epsilon(T_2)$ para $\Gamma = \emptyset$. A razão é que a validade do primeiro sequente implica a validade do segundo, mas a recíproca não é necessariamente verdadeira.

Com relação à regra de substituição, o axioma é enunciado para toda fórmula, no lugar de ser postulado para as fórmulas atômicas. Uma vez que definamos a noção de prova em (QPC) , é possível provar que, a partir dos axiomas

$$[SA] \quad \psi[\vec{\tau}/\vec{x}], (\vec{\tau} = \vec{\kappa}) \vdash \psi[\vec{\kappa}/\vec{x}] \quad (\psi \in ELF(\mathbb{L}))$$

onde $(\vec{\tau} = \vec{\kappa})$ denota a fórmula $(\tau_1 = \kappa_1) \otimes \cdots \otimes (\tau_k = \kappa_k)$, obtemos, por indução na complexidade de ϕ , a propriedade de substituição, se alguma justificativa em $\text{clau}([SUBS])$ é demonstrável e se ϕ não utiliza a disjunção. Se $\phi = \alpha \vee \beta$ e $x \in C_E(\phi, (\vec{\tau}; \vec{x}), C)$, então, por definição,

$x \in C_E(\alpha, (\vec{\tau}; \vec{x}), C) \cap C_E(\beta, (\vec{\tau}; \vec{x}), C)$ e analogamente para C_D ; logo, se uma interpretação $\mathcal{I}$ satisfaz **clau**([SUBS]) para $\phi = \alpha \vee \beta$, temos que

$$F_1(x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \leq F_2(x), \quad G_1(x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \leq G_2(x),$$

onde F_1 e F_2 representam as funções características associadas a $\alpha[\vec{\tau}/\vec{x}]$ e $\alpha[\vec{\kappa}/\vec{x}]$ no contexto C , respectivamente; afirmações análogas valem em relação à G_1 e G_2 para β ; f e g denotam os morfismos obtidos pela interpretação de $\vec{\tau}$ e $\vec{\kappa}$ (junto com as projeções) em C , enquanto p é o extent de P_C . Como o domínio das funções é o mesmo, deduzimos que

$$F_1(x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \leq [F_2 \vee G_2](x),$$

$$G_1(x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \leq [F_2 \vee G_2](x),$$

e conseqüentemente

$$(*) \quad F_1(x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \vee G_1(x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \leq [F_2 \vee G_2](x).$$

Para deduzir nos modelos o resultado desejado,

$$[F_1 \vee G_1](x) \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})] \leq [F_2 \vee G_2](x),$$

(o qual é verdadeiro) a partir de (*), deveríamos provar que $(F_1 \vee G_1) \& F = F_1 \& F \vee G_1 \& F$, onde $F(x) = p \& [f(x|_{p \& Ex}) = g(x|_{p \& Ex})]$, ou equivalentemente (Teorema 1.1.17(b)),

$$(**) \quad (EF_1 \vee EG_1) \& (E(F_1 \& F) \vee E(G_1 \& F)) = E(F_1 \& F) \vee E(G_1 \& F).$$

Em 2.4.3 vamos dar um exemplo em que esta última propriedade não é verdadeira; logo, será necessário postular a regra de substituição para toda fórmula ϕ (deve ser observado que, se $\vec{\tau}$ e $\vec{\kappa}$ são seqüências de variáveis, então a propriedade (**)) sempre é satisfeita; logo, numa linguagem sem constantes nem funções, a substituição pode ser obtida a partir das fórmulas atômicas).

Observação 2.4.2 : Seja QS um quantal simples. Se A é um prefeixe sobre QS e $x, y \in |A|$ tais que $[x = y] \neq 0$, então $[x = y] = Ex \& [x = y] = Ex$. Logo, a igualdade $[x = y]$ toma o valor 0 ou Ex para todo x, y . Com relação à restrição, se $x \neq *$ e $p \neq 0$, então $E(x|_p) = p \& Ex = p$, portanto $E : |A| \rightarrow EA^\leftarrow$ é uma aplicação sobrejetora. Por outro lado, uma função $f : A \rightarrow B$ é um morfismo sse satisfaz: para todo x, y , $[x = y] = Ex$ implica que $[fx = fy] = Ex$. Finalmente, as funções características $F : A \rightarrow QS$ são aplicações satisfazendo:

$$F(*) = 0; \quad F(x) \neq 0, [x = y] = Ex \text{ implica } F(x) = F(y) \leq EA \quad \forall x, y \neq *;$$

$$F(x), F(y) \neq 0 \text{ implica } F(x) = F(y) \leq EA \quad \forall x, y \neq *. \quad \square$$

Exemplo 2.4.3 : A partir da observação 2.4.2, vamos a dar um contraexemplo para a propriedade (**)) definida acima. Considere as cópias disjuntas de $\mathbf{1} \in Psh(QS)$

$$A_1 = \{x_p : p \in QS\}, \quad A_2 = \{y_p : p \in QS\}, \quad A_3 = \{z_p : p \in QS\},$$

e seja $|A| = A_1 \sqcup A_2 \sqcup A_3$ (identificando $x_0 = y_0 = z_0 \equiv_{def} *$) o prefeixe coproduto, i.e.,

$$[x_p = x_q] = [y_p = y_q] = [z_p = z_q] = p \& q,$$

$$[x_p = y_q] = [x_p = z_q] = [y_p = z_q] = 0,$$

$$(x_p)_{|q} = x_{q \& p}, \quad (y_p)_{|q} = y_{q \& p}, \quad (z_p)_{|q} = z_{q \& p} \quad \forall p, q \in QS.$$

Sejam $f, g : A \rightarrow A$ os morfismos dados por

$$f(x_p) = f(y_p) = x_p; \quad f(z_p) = y_p \quad \forall p \in QS; \quad g = id_A.$$

Temos $[f(x_p) = g(x_p)] = p$ para todo $p \in QS$, bem como $[f(x) = g(x)] = 0$ para todo $x \in A_2 \sqcup A_3$.

Sejam $a, b \in QS$ não nulos tais que $b \not\leq a$ e considere as funções características

$$F_\alpha(x) = \begin{cases} 0 & \text{se } x = * \\ a & \text{se } x \neq * \end{cases}; \quad F_\beta(x) = \begin{cases} 0 & \text{se } x \in A_1 \sqcup A_3 \\ b & \text{se } x \in A_2 \text{ e } x \neq y_0 \end{cases}.$$

Finalmente, seja $F_1 = f^*F_\alpha$, $G_1 = f^*F_\beta$, $F_2 = g^*F_\alpha = F_\alpha$ e $G_2 = g^*F_\beta = F_\beta$; assim, $F_\phi = F_\alpha \vee F_\beta \in C_E(f) \cap C_D(g)$. Por outro lado,

$$F_1(x_p) = F_\alpha(f(x_p)) = F_\alpha(x_p) = a;$$

$$G_1(x_p) = F_\beta(f(x_p)) = F_\beta(x_p) = 0; \quad G_1(z_p) = F_\beta(f(z_p)) = F_\beta(y_p) = b \quad \forall p \neq 0.$$

Temos

$$F_1(x_p) \& [f(x_p) = g(x_p)] = a, \quad G_1(x_p) \& [f(x_p) = g(x_p)] = 0 \quad \forall p \neq 0,$$

e então, como $F(x) = \top \& [f(x) \& g(x)]$, obtemos

$$(EF_1 \vee EG_1) \& (E(F_1 \& F) \vee E(G_1 \& F)) = (a \vee b) \& (a \vee 0) = a \vee b \neq a = E(F_1 \& F) \vee E(G_1 \& F),$$

contrariando (**). $\square$

Finalmente, devemos observar que as cláusulas de extensão $E(S_1, T_1)$ exigidas nas regras são indispensáveis para garantir a corretude das deduções. Para as regras de *weakening* $[WL]$ e $[WR]$, daremos o

Exemplo 2.4.4 : Sejam $Q = QS$ e A, B, S e T como no contraexemplo dado no lema 1.2.7 (b). Assim, temos que

$$S \rightarrow T = 0_B, \quad (S \times A) \rightarrow (T \times A) = B \times A \not\leq (S \rightarrow T) \times A = 0_{B \times A}.$$

Logo, para $R \subseteq B \times A$, com $0_{B \times A} \neq R \neq B \times A$, as duas condições

$$(S \times A) \rightarrow (T \times A) \subseteq R, \quad R \& ((S \times A) \rightarrow (T \times A)) = 0_{B \times A}$$

são falsas. Este é também um bom exemplo para ver que a operação de imagem inversa satisfaz:

$$\phi = \psi \text{ (como funções características) não implica necessariamente que } \phi(f^*) = \psi(f^*).$$

De fato, $\phi = h_S \rightarrow h_T$, $\psi \equiv 0$ e $f = \pi : B \times A \rightarrow B$ são um contraexemplo da igualdade $\phi(f^*) = \psi(f^*)$. A explicação é que a operação de imagem inversa $\phi(f^*)$ é computada a partir da estrutura de ϕ como esquema e não a partir dos valores de ϕ como função. $\square$

2.5 Teorema de Corretude

Introduziremos agora a noção de prova em (QPC) e demonstraremos que a lógica é correta, i.e., se um sequente S é demonstrável em (QPC) , então S é válido.

Definição 2.5.1 *Seja S um sequente e L um conjunto de sequentes. Uma prova de S a partir de L em (QPC) consiste numa sequência finita de sequentes $S_1, \dots, S_n = S$ tal que, para todo $i \leq n$, temos que alguma das seguintes condições é satisfeita:*

- (1) $S_i \in L$;
- (2) S_i é uma instância particular de um axioma diferente de $[SUBS]$;
- (3) S_i é derivado de sequentes anteriores mediante a aplicação de uma regra de inferência que não possui uma cláusula;
- (4) S_i é uma instância de $[SUBS]$ e existe alguma justificativa $x \in \text{clau}([SUBS])$ tal que, se $S' \in x$ e $S' \neq (\vdash \top)$, então $S' = S_j$ para algum $j < i$;
- (5) S_i é obtido de sequentes anteriores mediante a aplicação de uma regra $\mathcal{R}$ e existe $x \in \text{clau}(\mathcal{R})$ tal que, se $S' \in x$, $S' \neq (\vdash \top)$, então $S' = S_j$ para algum $j < i$.

Se S admite uma prova P em (QPC) a partir de L , então S é demonstrável em (QPC) a partir de L .

Se $L = \emptyset$, dizemos que P é uma prova de S (em (QPC)) e que S é demonstrável em (QPC) .

O resultado principal a ser provado nesta seção é o seguinte:

Teorema 2.5.2 : *Seja L um conjunto de sequentes e S um sequente. Se S é demonstrável em (QPC) a partir de L , então S é válido em toda interpretação $\mathcal{I}$ que satisfaz os sequentes de L utilizados numa prova de S .*

Em particular, quando $L = \emptyset$, temos o fundamental

Teorema 2.5.3 : *(Corretude) Seja S um sequente. Se S é demonstrável em (QPC) , então S é válido.*

A demonstração do teorema 2.5.2 é consequência de uma série de lemas, que garantem que as regras e os axiomas são corretos, que passaremos a provar.

Lema 2.5.4 : *A regra $[CUT]$ é correta, i.e.: dada uma instância particular de $[CUT]$, se $\mathcal{I}$ é uma interpretação tal que $\mathcal{I} \models S_1$, $\mathcal{I} \models S_2$ e $\mathcal{I}$ satisfaz $\text{clau}([CUT])$, então $\mathcal{I} \models S_3$.*

Demonstração: Sejam C , C' e D os contextos de S_1 , S_2 e S_3 , respectivamente, D' o contexto obtido de C e C' (eliminando as repetições de variáveis e constantes) e $\mathcal{I}$ uma interpretação nas

hipóteses da enunciado, i.e., $\mathcal{I} \models S_1$, $\mathcal{I} \models S_2$ e existe $x = y_1 \cup y_2 \cup y_3$ em $\mathbf{clau}([CUT])$ tal que $\mathcal{I}$ satisfaz todos os seguintes em y_1, y_2, y_3 .

Se $\Phi = \emptyset$, então $D' = D$ e $\llbracket \Gamma \rrbracket_{D'} = \llbracket \Gamma \rrbracket_D = 0$ (pois $(\mathcal{I}, D') \models S_1$), logo

$$0 = \llbracket \Sigma \rrbracket_D \& 0 \& \llbracket \Delta \rrbracket_D = \llbracket \Sigma, \Gamma, \Delta \rrbracket_D \leq \llbracket \Theta \rrbracket_D$$

donde $\mathcal{I} \models S_3$.

Se $\Phi = \phi$, então, dado que $\mathcal{I}$ satisfaz $E(S_1, T_1)$ e $E(S_2, T_2)$, obtemos, pelo lema 2.3.11 (com $C_1 = C'$ e $C_1 = C$, respectivamente),

$$(*) \quad (\mathcal{I}, D') \models S_1, \quad (\mathcal{I}, D') \models S_2.$$

Se $\Gamma = \emptyset$, então S_3 é da forma $\Sigma, V_C(\phi), \Delta \vdash \Theta$. Por (*), temos que $(\mathcal{I}, D') \models S_3$, pois

$$\llbracket \phi \rrbracket_{D'} = \llbracket V_{D'}(\phi) \rrbracket_{D'} = \llbracket V_C(\phi) \rrbracket_{D'}, \quad \llbracket \Sigma \rrbracket_{D'} \& \llbracket \phi \rrbracket_{D'} \& \llbracket \Delta \rrbracket_{D'} \leq \llbracket \Theta \rrbracket_{D'}.$$

Como $\mathcal{I}$ satisfaz $R(S_3, T_3)$, o lema 2.3.12 (com $C_1 = C$), fornece $\mathcal{I} \models S_3$.

Finalmente, se $\Gamma = \alpha_1, \dots, \alpha_n \neq \emptyset$, então, sejam

$$F = \llbracket \alpha_1 \rrbracket_{D'} \& \dots \& \llbracket \alpha_n \rrbracket_{D'}, \quad G = \llbracket \phi \rrbracket_{D'}.$$

Por (*), temos que

$$F \leq G, \quad \llbracket \Sigma \rrbracket_{D'} \& G \& \llbracket \Delta \rrbracket_{D'} \leq \llbracket \Theta \rrbracket_{D'}$$

donde $\llbracket \Sigma \rrbracket_{D'} \& F \& \llbracket \Delta \rrbracket_{D'} \leq \llbracket \Theta \rrbracket_{D'}$, pela transitividade da relação $\leq$ e por ser $\&$ crescente nas duas coordenadas (observe que, se Σ ou Δ são vazios, o resultado continua valendo, pois eles são simplesmente omitidos). Assim, $(\mathcal{I}, D') \models S_3$; como $\mathcal{I}$ satisfaz $R(S_3, T_3)$, 2.3.12 (com $C_1 = C(\phi)$) garante que $\mathcal{I} \models S_3$. $\square$

Lema 2.5.5 : *As regras de weakening são corretas, i.e., se $\mathcal{I}$ é uma interpretação satisfazendo S_1 e $\mathbf{clau}([WR]) = \mathbf{clau}([WL])$, então $\mathcal{I} \models S_2$ e $\mathcal{I} \models S_3$.*

Demonstração: Seja $\mathcal{I}$ uma interpretação nas condições do enunciado e $C = C(\Gamma, \phi)$.

Por hipótese, $(\mathcal{I}, C) \models (\Gamma \vdash)$, pois $\mathcal{I}$ satisfaz $E(S_1, T)$, portanto $\llbracket \Gamma \rrbracket_C = 0$, provando o resultado. $\square$

Lema 2.5.6 : *As regras de quantificação são corretas, i.e.: para cada uma das regras, dada uma instância particular $\mathcal{R}$ da regra, se $\mathcal{I}$ é uma interpretação tal que $\mathcal{I} \models S_1$ e que satisfaz $\mathbf{clau}(\mathcal{R})$, então $\mathcal{I} \models S_2$.*

Demonstração: Ao longo da prova, $\mathcal{I}$ denotará uma interpretação nas condições do enunciado.

$[\forall L]$: Seja $C = (\vec{x}; \vec{a})$ o contexto de $\Gamma, (\forall x)\phi, \Delta, \Theta$ e C' o contexto de $\Gamma, \phi[\tau/x] \otimes E\tau, \Delta, \Theta$.

Se $\tau \notin \mathcal{V}$, sejam $\vec{y}$ e $\vec{b}$ as variáveis e constantes de τ diferentes das $\vec{x}$ e das $\vec{a}$, respectivamente; então, $C' = ((\vec{x}; \vec{y}); (\vec{a}; \vec{b}))$. Considere os prefeixes $B = P_C$ e $A = P_{(\vec{y}; \vec{b})}$ determinados pelos contextos $(\vec{x}; \vec{a})$ e $(\vec{y}; \vec{b})$ em $\mathcal{I}$, respectivamente. Sejam A_t o prefeixe interpretando o tipo t de x em $\mathcal{I}$, $z \in \mathcal{V}_t$ uma variável nova, livre para x em ϕ e $p = EP_{C'} = EP_{(z, C')} \leq EP_{(\vec{a}; \vec{b})} = q$. Como $\mathcal{I}$ satisfaz $C_D(\phi, (\tau; x), C')$, o corolário 2.3.17 fornece

$$\llbracket \phi[\tau/x] \rrbracket_{C'}(\vec{u}; \vec{v}) \geq \llbracket \phi[z/x] \rrbracket_{(z, C')}(\llbracket \tau \rrbracket_{C'}((\vec{u}; \vec{v})_{|p \& E(\vec{u}) \& E(\vec{v})}), \vec{u}, \vec{v})$$

para todo $(\vec{u}, \vec{v}) \in D_{C'}$. Assim, se $v = \llbracket \tau \rrbracket_{C'}((\vec{u}; \vec{v})_{|p \& E(\vec{u}) \& E(\vec{v})}) \in |(A_t)_{|EA_t \wedge q}|$, temos $Ev = p \& E(\vec{u}) \& E(\vec{v})$; logo

$$\begin{aligned} \llbracket (\forall x)\phi \rrbracket_{C'}(\vec{u}, \vec{v}) &\leq (Ev \rightarrow_l \llbracket \phi[z/x] \rrbracket_{(z, C')}(v, \vec{u}, \vec{v})) \& p \& E(\vec{u}) \& E(\vec{v}) \\ &\leq \llbracket \phi[z/x] \rrbracket_{(z, C')}(v, \vec{u}, \vec{v}) \leq \llbracket \phi[\tau/x] \rrbracket_{C'}(\vec{u}; \vec{v}). \end{aligned}$$

Se $\tau = y \in \mathcal{V}$ e $y \in \vec{x}$, temos que $\vec{x} = (y; \vec{w})$, e $C' = C = ((y; \vec{w}); \vec{a})$, donde

$$\llbracket (\forall x)\phi \rrbracket_{C'}(v; \vec{u}) = \llbracket (\forall x)\phi \rrbracket_{\vec{w}, \vec{a}}(\vec{u}) \& Ev \leq \llbracket \phi[y/x] \rrbracket_{C'}(v; \vec{u}).$$

Se $y \notin \vec{x}$, então $C' = ((y; \vec{x}); \vec{a})$ e $C = (\vec{x}; \vec{a})$, e portanto para todo $(v, \vec{u}) \in D_{C'}$ vale

$$\llbracket (\forall x)\phi \rrbracket_{C'}(v; \vec{u}) = \llbracket (\forall x)\phi \rrbracket_C(\vec{u}) \& Ev \leq \llbracket \phi[y/x] \rrbracket_{C'}(v; \vec{u}).$$

Assim, provamos que, para todo termo τ nas hipóteses do enunciado, $\llbracket (\forall x)\phi \rrbracket_{C'} \leq \llbracket \phi[\tau/x] \rrbracket_{C'}$. Já que $\mathcal{I}$ satisfaz $E(S_1, T_1)$, temos que $(\mathcal{I}, C') \models (\Gamma, \phi[\tau/x], \Delta \vdash \Theta)$ e então

$$\llbracket \Gamma \rrbracket_{C'} \& \llbracket (\forall x)\phi \rrbracket_{C'} \& \llbracket \Delta \rrbracket_{C'} \leq \llbracket \Gamma \rrbracket_{C'} \& \llbracket \phi[\tau/x] \rrbracket_{C'} \& \llbracket \Delta \rrbracket_{C'} \leq \llbracket \Theta \rrbracket_{C'}.$$

Segue que $(\mathcal{I}, C') \models S_2$, com S_2 o sequente $\Gamma, (\forall x)\phi, \Delta \vdash \Theta$; mesmo que Γ , Δ ou Θ seja vazio, a última afirmação é ainda verdadeira. Portanto, dado que $\mathcal{I}$ satisfaz $R(S_2, T_2)$, o lema 2.3.12 (com $C_1 = C(\tau) - C$), mostra que $\mathcal{I} \models S$.

$[\forall R]$: Seja $C = (\vec{x}; \vec{a})$ o contexto de $\Gamma, (\forall x)\phi$; se $\Gamma = \alpha_1, \dots, \alpha_n \neq \emptyset$ então, pela hipótese da regra, y não ocorre em C e $\mathcal{I}$ satisfaz $E(S_1, T_1)$, donde $(\mathcal{I}, (y, C)) \models (\Gamma \vdash \phi[y/x])$ e

$$\llbracket \alpha_1 \rrbracket_{(y; C)} \& \dots \& \llbracket \alpha_n \rrbracket_{(y; C)} \leq \llbracket \phi[y/x] \rrbracket_{(y; C)}.$$

Como $\mathcal{I}$ satisfaz $R(S_2, T_2)$ então, se $t \in \text{tipos}(C)$ (onde $y \in \mathcal{V}_t$) ou, caso contrário, pela prova de 2.3.12, temos que, para todo $(v, \vec{u}) \in D_{(y, C)}$,

$$\llbracket \llbracket \alpha_1 \rrbracket_C \& \dots \& \llbracket \alpha_n \rrbracket_C \rrbracket(\vec{u}) \& Ev \leq \llbracket \alpha_1 \rrbracket_{(y; C)}(v, \vec{u}) \& \dots \& \llbracket \alpha_n \rrbracket_{(y; C)}(v, \vec{u}) \leq \llbracket \phi[y/x] \rrbracket_{(y; C)}(v, \vec{u}),$$

portanto

$$\llbracket \llbracket \alpha_1 \rrbracket_C \& \dots \& \llbracket \alpha_n \rrbracket_C \rrbracket(\vec{u}) \leq Ev \rightarrow_l \llbracket \phi[y/x] \rrbracket_{(y; C)}(v, \vec{u})$$

para todo $v \in |(A_t)_{|EA_t \wedge p}|$, onde $p = EP_{\vec{a}}$; assim, $\llbracket \Gamma \rrbracket_C \leq \llbracket (\forall x)\phi \rrbracket_C$.

No caso $\Gamma = \emptyset$, como $(\mathcal{I}, (y, C)) \models (\vdash \phi[y/x])$, teremos

$$\begin{aligned} \llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}) &= \llbracket V_{(y,C)}(\phi[y/x]) \rrbracket_{(y,C)}(v, \vec{u}) = \llbracket V_C((\forall x)\phi) \rrbracket_{(y,C)}(v, \vec{u}) \\ &= \llbracket V_{(y,C)}((\forall x)\phi) \rrbracket \& E(\vec{u}) \& Ev = \llbracket V_C((\forall x)\phi) \rrbracket \& E(\vec{u}) \& Ev \\ &= \llbracket V_C((\forall x)\phi) \rrbracket_C(\vec{u}) \& Ev, \end{aligned}$$

e portanto

$$\llbracket V_C((\forall x)\phi) \rrbracket_C(\vec{u}) \leq Ev \rightarrow_l \llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}),$$

donde

$$\llbracket V_C((\forall x)\phi) \rrbracket_C \leq \llbracket (\forall x)\phi \rrbracket_C.$$

$[\exists L]$: Sejam $C = (\vec{x}; \vec{a})$ e (y, C) os contextos de $\Gamma, (\exists x)\phi, \Delta, \Theta$ e de $\Gamma, \phi[y/x] \otimes Ey, \Delta, \Theta$, respectivamente, e t o tipo de y .

Se $\Gamma, \Delta, \Theta \neq \emptyset$, suponha que $t \notin \mathbf{tipos}(C)$; então $\mathcal{I}$ satisfaz $R(S_2, \{t\})$. Como na prova do lema 2.3.12, $\llbracket \Theta \rrbracket_{(y,C)}(v, \vec{u}) \leq \llbracket \Theta \rrbracket_C(\vec{u})$ e

$$(*) \quad \llbracket \Gamma \rrbracket_C(\vec{u}) \& \llbracket (\exists x)\phi \rrbracket_C(\vec{u}) \& \llbracket \Delta \rrbracket_C(\vec{u}) \& Ev \leq \llbracket \Gamma \rrbracket_{(y,C)}(v, \vec{u}) \& \llbracket (\exists x)\phi \rrbracket_C(\vec{u}) \& Ev \& \llbracket \Delta \rrbracket_{(y,C)}(v, \vec{u}),$$

pois $\llbracket (\exists x)\phi \rrbracket_{(y,C)}(v, \vec{u}) = \llbracket (\exists x)\phi \rrbracket_C(\vec{u}) \& Ev$. Já que $\llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}) \leq \llbracket (\exists x)\phi \rrbracket_C(\vec{u}) \& Ev$, temos que

$$\llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}) = \llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}) \& \llbracket (\exists x)\phi \rrbracket_C(\vec{u}) \& Ev,$$

e então, multiplicando $(*)$ à direita (se $\Gamma \neq \emptyset$) ou à esquerda (se $\Gamma = \emptyset$) por $\llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u})$, obtemos que

$$\begin{aligned} \llbracket \Gamma \rrbracket_C(\vec{u}) \& \llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}) \& \llbracket \Delta \rrbracket_C(\vec{u}) &\leq \llbracket \Gamma \rrbracket_{(y,C)}(v, \vec{u}) \& \llbracket \phi[y/x] \rrbracket_{(y,C)}(v, \vec{u}) \& \llbracket \Delta \rrbracket_{(y,C)}(v, \vec{u}) \\ &\leq \llbracket \Theta \rrbracket_{(y,C)}(v, \vec{u}) \leq \llbracket \Theta \rrbracket_C(\vec{u}) \end{aligned}$$

para todo $(v, \vec{u}) \in D_{(y,C)}$, pois $(\mathcal{I}, (y, C)) \models (\Gamma, \phi[y/x]; \Delta \vdash \Theta)$, por hipótese. Logo, tomando supremo sobre $v \in |(A_t)_p|$ (onde $p = EA_t \wedge EP_a$), obtemos que

$$\llbracket \Gamma \rrbracket_C \& \llbracket (\exists x)\phi \rrbracket_C \& \llbracket \Delta \rrbracket_C \leq \llbracket \Theta \rrbracket_C.$$

Se $t \in \mathbf{tipos}(C)$ então $\llbracket \Gamma \rrbracket_{(y,C)}(v, \vec{u}) = \llbracket \Gamma \rrbracket_C(\vec{u}) \& Ev$, com o mesmo valendo para Δ e Θ . Assim, o mesmo argumento que acima pode ser usado para tratar este caso.

Se $\Gamma, \Delta, \Theta = \emptyset$, então $\llbracket \phi[y/x] \rrbracket_{(y,C)} = \mathbf{0}$, pois $(\mathcal{I}, (y, C)) \models (\phi[y/x] \vdash)$, por hipótese, donde

$$\llbracket (\exists x)\phi \rrbracket_C(\vec{u}) = \bigvee_{v \in |(A_t)_p|} \llbracket \phi[y/x] \rrbracket_{(y,C)}(v_p, \vec{u}) = \mathbf{0}.$$

$[\exists R]$: Seja $C = (\vec{x}; \vec{a})$ o contexto de $\Gamma, (\exists x)\phi$ e C' o contexto de $\Gamma, \phi[\tau/x] \otimes E\tau$.

Se $\tau \notin \mathcal{V}$, sejam $(\vec{y}; \vec{b})$ as variáveis e constantes de τ não presentes em C , assim, $C' = ((\vec{x}; \vec{y}); (\vec{a}; \vec{b}))$.

Pelo corolário 2.3.17, analogamente ao caso $[\forall L]$, provamos que

$$\llbracket \phi[\tau/x] \rrbracket_{C'}(\vec{u}) \leq \llbracket \phi[z/x] \rrbracket_{(z,C')}(\llbracket \tau \rrbracket_{C'}(\vec{u}_{|p \& E(\vec{u})}), \vec{u}) \leq \llbracket (\exists x)\phi \rrbracket_{C'}(\vec{u}).$$

Se $\tau = y \in \mathcal{V}_t$, suponha que $y \in \vec{x}$; nesse caso, $C = ((y; \vec{w}); \vec{a}) = C'$; se $P = (A_t)_{|EA_t \wedge EP_{\vec{a}}}$,

$$\begin{aligned} \llbracket (\exists x)\phi \rrbracket_{C'}(v; \vec{u}) &= \llbracket (\exists x)\phi \rrbracket_{\vec{w}; \vec{a}}(\vec{u}) \& Ev = (\bigvee_{u \in |P|} \llbracket \phi[y/x] \rrbracket_{C'}(u; \vec{u})) \& Ev \\ &\geq \llbracket \phi[y/x] \rrbracket_{C'}(v; \vec{u}) \& Ev = \llbracket \phi[y/x] \rrbracket_{C'}(v; \vec{u}). \end{aligned}$$

Por outro lado, se $\tau = y \notin \vec{x}$, então $C' = ((y; \vec{x}); \vec{a})$ e $C = (\vec{x}; \vec{a})$, portanto, com P como acima,

$$\llbracket \phi[y/x] \rrbracket_{C'}(v; \vec{u}) \leq \bigvee_{u \in |P|} \llbracket \phi[y/x] \rrbracket_{C'}(u; \vec{u}) = \llbracket (\exists x)\phi \rrbracket_C(\vec{u})$$

relação que multiplicada à direita por Ev fornece

$$\llbracket \phi[y/x] \rrbracket_{C'}(v; \vec{u}) \leq \llbracket (\exists x)\phi \rrbracket_C(\vec{u}) \& Ev = \llbracket (\exists x)\phi \rrbracket_{C'}(v; \vec{u}).$$

Provamos assim que, para todo termo τ nas hipóteses do enunciado, $\llbracket \phi[\tau/x] \rrbracket_{C'} \leq \llbracket (\exists x)\phi \rrbracket_{C'}$.

Como $(\mathcal{I}, C') \models (\Gamma \vdash \phi[\tau/x])$, temos dois casos a discutir :

i) se $\Gamma \neq \emptyset$, então,

$$\llbracket \Gamma \rrbracket_{C'}(\vec{u}) \leq \llbracket \phi[\tau/x] \rrbracket_{C'}(\vec{u}) \leq \llbracket (\exists x)\phi \rrbracket_{C'}(\vec{u}),$$

i.e., $(\mathcal{I}, C') \models (\Gamma \vdash (\exists x)\phi)$. Já que $\mathcal{I}$ satisfaz $R(S_2, T_2)$, o lema 2.3.12 (com $C_1 = C(\tau) - C$) garante que $\mathcal{I} \models (\Gamma \vdash (\exists x)\phi)$.

ii) Se $\Gamma = \emptyset$, seja $C'' = (z, C)$, onde $z \in V_t$ é nova e livre para x em ϕ ; logo, dado que $\mathcal{I} \models (\epsilon(C'') \vdash \epsilon(C'))$, então $EP_{C''} \leq EP_{C'}$. Por outro lado, a existência do termo τ exige $EP_{C''} \geq EP_{C'}$, donde $EP_{C''} = EP_{C'}$. Por indução na complexidade de ϕ , é fácil provar que $\llbracket V_{(z,C)}(\phi[z/x]) \rrbracket = \llbracket V_{C'}(\phi[\tau/x]) \rrbracket$. Assim, pelo lema 2.2.12 e o fato que $\mathcal{I}$ satisfaz $K_E((\exists x)\phi, C, T_2)$, devemos ter que, para todo $(\vec{v}, \vec{u}) \in D_{C'}$,

$$\begin{aligned} \llbracket V_{C'}(\phi[\tau/x]) \rrbracket \& E(\vec{v}) \& E(\vec{u}) &= \llbracket V_{C'}(\phi[\tau/x]) \rrbracket_{C'}(\vec{v}, \vec{u}) = \llbracket \phi[\tau/x] \rrbracket_{C'}(\vec{v}, \vec{u}) \\ &\leq \llbracket (\exists x)\phi \rrbracket_{C'}(\vec{v}, \vec{u}) \leq \llbracket (\exists x)\phi \rrbracket_C(\vec{v}) \& E(\vec{u}) \leq \llbracket V_C((\exists x)\phi) \rrbracket \& E(\vec{v}) \& E(\vec{u}) \\ &= \llbracket V_{(z,C)}(\phi[z/x]) \rrbracket \& E(\vec{v}) \& E(\vec{u}) = \llbracket V_{C'}(\phi[\tau/x]) \rrbracket \& E(\vec{v}) \& E(\vec{u}). \end{aligned}$$

Assim,

$$\llbracket (\exists x)\phi \rrbracket_C(\vec{v}) \& E(\vec{u}) = \llbracket V_C((\exists x)\phi) \rrbracket \& E(\vec{v}) \& E(\vec{u}) = \llbracket V_C((\exists x)\phi) \rrbracket_C(\vec{v}) \& E(\vec{u})$$

donde, tomando supremo sobre $\vec{u} \in D_{(\vec{y}; \vec{a}, \vec{b})}$, obtemos

$$\llbracket (\exists x)\phi \rrbracket_C(\vec{v}) \& p = \llbracket V_C((\exists x)\phi) \rrbracket_C(\vec{v}) \& p$$

para todo $\vec{v} \in D_{(\vec{x}; \vec{a}, \vec{b})}$, onde $p \geq EP_{(\vec{y}; \vec{a}, \vec{b})} \geq EP_{C'}$. Por outro lado,

$$E\llbracket (\exists x)\phi \rrbracket_C \leq EP_{C''} = EP_{C'} \leq p, \quad E\llbracket V_C((\exists x)\phi) \rrbracket_C \leq EP_{C''} = EP_{C'} \leq p,$$

e então

$$\llbracket (\exists x)\phi \rrbracket_C(\vec{v}) = \llbracket V_C((\exists x)\phi) \rrbracket_C(\vec{v})$$

para todo $\vec{v} \in D_{(\vec{x}; \vec{a}, \vec{b})}$. Seja então $\vec{v} \in D_C$; como $\vec{w} = \vec{v}|_{EP_{C'}} \in D_{(\vec{x}; \vec{a}, \vec{b})}$, teremos

$$\begin{aligned} \llbracket (\exists x)\phi \rrbracket_C(\vec{v}) &= \llbracket (\exists x)\phi \rrbracket_C(\vec{v}) \& EP_{C'} = \llbracket (\exists x)\phi \rrbracket_C(\vec{w}) \\ &= \llbracket V_C((\exists x)\phi) \rrbracket_C(\vec{w}) = \llbracket V_C((\exists x)\phi) \rrbracket_C(\vec{v}) \& EP_{C'} = \llbracket V_C((\exists x)\phi) \rrbracket_C(\vec{v}), \end{aligned}$$

completando a prova. $\square$

Lema 2.5.7 : *O axioma de substituição é correto, i.e., dada uma instância particular S de $[SUBS]$, se $\mathcal{I}$ é uma interpretação que satisfaz $\text{clau}([SUBS])$, então $\mathcal{I} \models S$.*

Demonstração: Seja S uma instância de $[SUBS]$,

$$S : \phi[\vec{\tau}/\vec{x}], (\tau_1 = \kappa_1), \dots, (\tau_n = \kappa_n) \vdash \phi[\vec{\kappa}/\vec{x}],$$

e seja $\mathcal{I}$ uma interpretação nas condições do enunciado. Seja z_i como na definição 2.3.13 ($i = 1, \dots, n$), $\vec{z} = z_1, \dots, z_n$, $E(\vec{z}) = Ez_1 \otimes \dots \otimes Ez_n$, $C' = ((\vec{z}; \vec{y}); \vec{a})$ o contexto de $\phi[\vec{z}/\vec{x}] \otimes E(\vec{z})$ e $\vec{w}$, $\vec{c}$ as variáveis e constantes de $\vec{\tau}$, $\vec{\kappa}$ não presentes em $C_1 = (\vec{y}; \vec{a})$; logo, $C = ((\vec{y}; \vec{w}); (\vec{a}; \vec{c}))$ é o contexto de S . Sejam $A = P_{(\vec{w}; \vec{c})}$, $B = P_{C_1}$, $P = \prod_i A_{t_i}$ e

$$f_i = \llbracket \tau_i \rrbracket_C : B \times A \longrightarrow A_{t_i}, \quad g_i = \llbracket \kappa_i \rrbracket_C : B \times A \longrightarrow A_{t_i},$$

$$\pi_1 : B \times A \longrightarrow B, \quad f = \langle f_1, \dots, f_n, \pi_1 \rangle, \quad g = \langle g_1, \dots, g_n, \pi_1 \rangle : B \times A \longrightarrow P \times B,$$

$$\pi : P \times B \times A \longrightarrow P \times B.$$

Observe que $f(\vec{u}, \vec{v}) = (\llbracket \tau_1 \rrbracket_C(\vec{u}, \vec{v}), \dots, \llbracket \tau_n \rrbracket_C(\vec{u}, \vec{v}), \vec{u})$ e analogamente para g . Logo, temos que

$$\llbracket \phi[\vec{\tau}/\vec{x}] \rrbracket_C = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C'}(f^*), \quad \llbracket \phi[\vec{\kappa}/\vec{x}] \rrbracket_C = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C'}(g^*), \quad \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}; C)} = \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{C'}(\pi^*).$$

Como $\mathcal{I}$ satisfaz $C_E(\phi, (\vec{\tau}; \vec{x}), C)$ e $C_D(\phi, (\vec{\kappa}; \vec{x}), C)$, o corolário 2.3.17 fornece

$$\llbracket \phi[\vec{\tau}/\vec{x}] \rrbracket_C(\vec{u}, \vec{v}) \leq \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}; C)}(f((\vec{u}, \vec{v})|_{p \& E(\vec{u}) \& E(\vec{v})}), \vec{v}),$$

$$\llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}; C)}(g((\vec{u}, \vec{v})|_{p \& E(\vec{u}) \& E(\vec{v})}), \vec{v}) \leq \llbracket \phi[\vec{\kappa}/\vec{x}] \rrbracket_C(\vec{u}, \vec{v}),$$

onde $p = EP_C = EA \wedge EB = EA \wedge EB \wedge EP$. Por outro lado,

$$\llbracket (\tau_i = \kappa_i) \rrbracket_C(\vec{u}, \vec{v}) = p \& [f_i((\vec{u}, \vec{v})|_{p \& E(\vec{u}) \& E(\vec{v})}) = g_i((\vec{u}, \vec{v})|_{p \& E(\vec{u}) \& E(\vec{v})})]$$

para todo $i = 1, \dots, n$. Portanto, fixando $(\vec{u}, \vec{v}) \in D_C$, se

$$r_i = f_i((\vec{u}, \vec{v})|_{p \& E(\vec{u}) \& E(\vec{v})}), \quad s_i = g_i((\vec{u}, \vec{v})|_{p \& E(\vec{u}) \& E(\vec{v})})$$

($i = 1, \dots, n$), $\vec{r} = (r_1, \dots, r_n)$ e $\vec{s} = (s_1, \dots, s_n)$, então, por $[char2]$ para $\llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}; C)}$, temos que

$$\begin{aligned} \llbracket \phi[\vec{\tau}/\vec{x}] \rrbracket_C(\vec{u}, \vec{v}) \& \llbracket (\tau_1 = \kappa_1) \rrbracket_C(\vec{u}, \vec{v}) \& \dots \& \llbracket (\tau_n = \kappa_n) \rrbracket_C(\vec{u}, \vec{v}) \\ &\leq \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}; C)}(\vec{r}, \vec{u}, \vec{v}) \& [\vec{r} = \vec{s}] \& [\vec{u} = \vec{u}] \& [\vec{v} = \vec{v}] \\ &\leq \llbracket \phi[\vec{z}/\vec{x}] \rrbracket_{(\vec{z}; C)}(\vec{s}, \vec{u}, \vec{v}) \leq \llbracket \phi[\vec{\kappa}/\vec{x}] \rrbracket_C(\vec{u}, \vec{v}), \end{aligned}$$

mostrando que $\mathcal{I} \models S$. $\square$

Lema 2.5.8 : *Os axiomas de (QPC) são válidos.*

Demonstração: Fixemos uma interpretação $\mathcal{I}$ para $\mathbb{L}$.

[EX]: Como o contexto do sequente é vazio, a interpretação do lado esquerdo do sequente produz

$$EA_{t_1} \wedge \cdots \wedge EA_{t_n}$$

enquanto o lado direito produz EA_t ; pela cláusula (ii)-(a) da definição de interpretação, a declaração de $f : t_1 \times \cdots \times t_n \rightarrow t$ obriga que $\mathcal{I}$ satisfaça

$$EA_{t_1} \wedge \cdots \wedge EA_{t_n} \leq EA_t,$$

mostrando que o axioma é válido em $\mathcal{I}$.

[CH1.0]: É uma consequência imediata do corolário 2.2.13.

[CH1.1]: Seja $C = (\vec{x}; \vec{a})$ o contexto do sequente e $p = EP_C$. Para todo $i = 1, \dots, n$, se τ_i é do tipo t_i , então

$$\llbracket E\tau_i \rrbracket_C(\vec{u}) = (p \wedge EA_{t_i}) \& EA_{t_i} \& E(\llbracket \tau_i \rrbracket_C(\vec{u}_{p \& E(\vec{u})})) = p \& E(\vec{u})$$

pois $p \leq EA_{t_i}$. Assim, por [char1] e idempotência, temos que

$$\llbracket \phi \rrbracket_C(\vec{u}) = \llbracket \phi \rrbracket_C(\vec{u}) \& p \& E(\vec{u}) = \llbracket \phi \otimes (E\tau_1 \otimes \cdots \otimes E\tau_n) \rrbracket_C(\vec{u}).$$

[CH3]: Suponha que $y \notin VAR(\phi)$; seja $(x, C) = C(\phi)$, $(y, C) = C(\phi[y/x])$ e (x, y, C) o contexto de $\phi[y/x]$, ϕ (pois y é livre para $x \in VAR(\phi)$ em ϕ). Sejam

$$F = \llbracket \phi \rrbracket_{(x,C)} = \llbracket \phi[y/x] \rrbracket_{(y,C)}, \quad F_1 = \llbracket \phi \rrbracket_{(x,y,C)}, \quad G_1 = \llbracket \phi[y/x] \rrbracket_{(x,y,C)}.$$

Então,

$$F_1(u, v; \vec{u}) = F(u; \vec{u}) \& Ev, \quad G_1(u, v; \vec{u}) = F(v; \vec{u}) \& Eu = F_1(v, u; \vec{u}),$$

e [char3] aplicada a F_1 fornece

$$G_1(u, v; \vec{u}) \& F_1(u, v; \vec{u}) = F_1(v, u; \vec{u}) \& F_1(u, v; \vec{u}) \leq EF_1 \& F_1(u, v; \vec{u}) = F_1(u, v; \vec{u}).$$

Se $y \in VAR(\phi)$, então $C(\phi) = (x, y, C)$ e $C(\phi[y/x]) = (y, C)$; logo, se $F_1 = \llbracket \phi \rrbracket_{C(\phi)}$ e $G_1 = \llbracket \phi[y/x] \rrbracket_{C(\phi)}$, então $G_1(u, v; \vec{u}) = F_1(v, v; \vec{u}) \& Eu$, e o resultado é consequência de que [char3] vale para F_1 .

[AX1]: Se $\Gamma = \emptyset$, então $\llbracket \top \rrbracket = \top = \llbracket V_\emptyset(\top) \rrbracket$. Se $\Gamma = \alpha_1, \dots, \alpha_n \neq \emptyset$, seja $C = (\vec{x}; \vec{a})$ o contexto de Γ e $p = EP_C$. Se $\vec{x} = \emptyset$, então

$$\llbracket \alpha_1 \rrbracket_{\vec{a}} \& \cdots \& \llbracket \alpha_n \rrbracket_{\vec{a}} \leq p = \llbracket \top \rrbracket_{\vec{a}}.$$

Se $\vec{x} \neq \emptyset$, então, por [char1],

$$\llbracket \alpha_1 \rrbracket_C(\vec{u}) \& \cdots \& \llbracket \alpha_n \rrbracket_C(\vec{u}) \leq p \& E(\vec{u}) = \llbracket \top \rrbracket_C(\vec{u}).$$

[AX2]: Vem imediatamente da idempotência de Q .

[AX3]: Vem do fato que Q é right-sided.

[AX4], [AX5], [E5]: Se $\Gamma = \emptyset$, o resultado é trivial. Se $\Gamma \neq \emptyset$, seja C o contexto do sequente em [AX5], $p = EP_C$, e $F = \llbracket \phi \multimap \psi \rrbracket_C$. Por definição, $F(\vec{u}) = p \& F(\vec{u})$, portanto

$$\llbracket \Gamma \rrbracket_C(\vec{u}) \& F(\vec{u}) \leq p \& F(\vec{u}) = F(\vec{u}).$$

A prova de [AX4] e [E5] é similar.

[E1], [E2]: Seja t o tipo de τ , $C = C(\tau)$ e $p = EP_C \leq EA_t$; então

$$\begin{aligned} \llbracket (\tau = \tau) \rrbracket_C(\vec{u}) &= p \& \llbracket \tau \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}) = \llbracket \tau \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}) \\ &= p \& E(\llbracket \tau \rrbracket_C(\vec{u}_{|p \& E(\vec{u})})) = \llbracket E\tau \rrbracket_C(\vec{u}). \end{aligned}$$

[E3]: Seja $C = C((\tau = \kappa))$, $p = EP_C$, $\vec{u} \in D_C$ e $\vec{w} = \vec{u}_{|p \& E(\vec{u})}$; então

$$\begin{aligned} \llbracket (\tau = \kappa) \rrbracket_C(\vec{u}) &= p \& \llbracket \tau \rrbracket_C(\vec{w}) = \llbracket \kappa \rrbracket_C(\vec{w}) \\ &= p \& \llbracket \kappa \rrbracket_C(\vec{w}) = \llbracket \tau \rrbracket_C(\vec{w}) = \llbracket (\kappa = \tau) \rrbracket_C(\vec{u}). \end{aligned}$$

[E4]: Seja C o contexto do sequente, $p = EP_C$, $\vec{u} \in D_C$ e $\vec{w} = \vec{u}_{|p \& E(\vec{u})}$; então

$$\begin{aligned} \llbracket (\tau = \kappa) \rrbracket_C(\vec{u}) \& \llbracket (\kappa = \rho) \rrbracket_C(\vec{u}) &= p \& \llbracket \tau \rrbracket_C(\vec{w}) = \llbracket \kappa \rrbracket_C(\vec{w}) \& p \& \llbracket \kappa \rrbracket_C(\vec{w}) = \llbracket \rho \rrbracket_C(\vec{w}) \\ &\leq p \& \llbracket \tau \rrbracket_C(\vec{w}) = \llbracket \rho \rrbracket_C(\vec{w}) = \llbracket (\tau = \rho) \rrbracket_C(\vec{u}). \end{aligned}$$

[E6]: Sejam t_i os tipos de τ_i, κ_i ($i = 1, \dots, n$), $f : t_1 \times \dots \times t_n \rightarrow t$, C o contexto do sequente e $p = EP_C$. Sejam

$$x_i = \llbracket \tau_i \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}), \quad y_i = \llbracket \kappa_i \rrbracket_C(\vec{u}_{|p \& E(\vec{u})})$$

para $i = 1, \dots, n$, logo

$$\llbracket f(\tau_1, \dots, \tau_n) \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}) = f^{\mathcal{I}}(x_1, \dots, x_n), \quad \llbracket f(\kappa_1, \dots, \kappa_n) \rrbracket_C(\vec{u}_{|p \& E(\vec{u})}) = f^{\mathcal{I}}(y_1, \dots, y_n).$$

Assim, por [mor2] para $f^{\mathcal{I}}$,

$$[x_1 = y_1] \& \dots \& [x_n = y_n] \leq [f^{\mathcal{I}}(x_1, \dots, x_n) = f^{\mathcal{I}}(y_1, \dots, y_n)]$$

donde, multiplicando à esquerda por p ambos membros da desigualdade,

$$\llbracket (\tau_1 = \kappa_1) \rrbracket_C \& \dots \& \llbracket (\tau_n = \kappa_n) \rrbracket_C(\vec{u}) \leq \llbracket (f(\tau_1, \dots, \tau_n) = f(\kappa_1, \dots, \kappa_n)) \rrbracket_C(\vec{u}). \quad \square$$

Lema 2.5.9 : *As regras para os conectivos são corretas, i.e.: para cada instância de cada regra introduzida em 2.4.1, se $\mathcal{I}$ é uma interpretação satisfazendo o antecedente da regra, bem como as (eventuais) cláusulas da regra, então $\mathcal{I}$ satisfaz o consequente da regra.*

Demonstração: Seja $\mathcal{I}$ uma interpretação nas condições do enunciado.

$[\otimes R]$: Sejam C e C' os contextos de $\Gamma \vdash \phi$ e $\Delta \vdash \psi$, respectivamente. Como $\mathcal{I} \models (\Gamma \vdash \phi)$ e $\mathcal{I}$ satisfaz $E(S_1, T_1)$ então $(\mathcal{I}, C'') \models (\Gamma \vdash \phi)$, onde C'' é o contexto obtido de C e C' ; analogamente, $(\mathcal{I}, C'') \models (\Delta \vdash \psi)$.

Se $\Gamma \neq \emptyset \neq \Delta$, então

$$[\Gamma]_{C''} \leq [\phi]_{C''}, \quad [\Delta]_{C''} \leq [\psi]_{C''}$$

donde

$$[\Gamma]_{C''} \& [\Delta]_{C''} \leq [\phi]_{C''} \& [\psi]_{C''}.$$

Se $\Gamma = \emptyset = \Delta$, então

$$[\phi]_{C''} = [V_{C''}(\phi)]_{C''}, \quad [\psi]_{C''} = [V_{C''}(\psi)]_{C''}$$

e logo

$$[\phi \otimes \psi]_{C''} = [\phi]_{C''} \& [\psi]_{C''} = [V_{C''}(\phi)]_{C''} \& [V_{C''}(\psi)]_{C''} = [V_{C''}(\phi \otimes \psi)]_{C''}.$$

Se $\Gamma = \emptyset \neq \Delta$, então

$$[\phi]_{C''} = [V_{C''}(\phi)]_{C''}, \quad [\Delta]_{C''} \leq [\psi]_{C''},$$

portanto

$$\begin{aligned} [\Gamma']_{C''} \& [\Delta]_{C''} &= [V_C(\phi)]_{C''} \& [\Delta]_{C''} \\ &= [V_{C''}(\phi)]_{C''} \& [\Delta]_{C''} \leq [\phi]_{C''} \& [\psi]_{C''}. \end{aligned}$$

Se $\Gamma \neq \emptyset = \Delta$, a prova é similar.

$[\otimes L]$: Vale pela definição de interpretação.

As regras restantes são provadas analogamente a $[\otimes R]$; elas funcionam, porque os sequentes podem ser estendidos e porque as regras dos conectivos descrevem as propriedades das operações que os interpretam; assim, em $[\wedge R]$, com a notação de acima,

$$[\Gamma]_{C''} \leq [\phi]_{C''}, \quad [\Gamma]_{C''} \leq [\psi]_{C''}$$

implica que

$$[\Gamma]_{C''} \leq [\phi]_{C''} \wedge [\psi]_{C''} = [\phi \wedge \psi]_{C''}.$$

A regra $[\vee L1]$ vale por causa da estrutura de right-quantal das funções características:

$$[\Gamma]_{C''} \& [\phi]_{C''} \leq [\Theta]_{C''}, \quad [\Gamma]_{C''} \& [\psi]_{C''} \leq [\Theta]_{C''}$$

implica que

$$[\Gamma]_{C''} \& ([\phi]_{C''} \vee [\psi]_{C''}) = [\Gamma]_{C''} \& [\phi]_{C''} \vee [\Gamma]_{C''} \& [\psi]_{C''} \leq [\Theta]_{C''}.$$

A regra $[\vee L2]$ é válida, pois $\mathcal{I} \models S$, por hipótese; logo, se

$$F = [\phi]_{C''}, \quad G = [\psi]_{C''}, \quad H = [\alpha]_{C''},$$

então $E(F \& H) \vee E(G \& H) \in (EF \vee EG) \downarrow$, portanto (Teorema 1.1.17(b))

$$(F \vee G) \& H = (F \& H) \vee (G \& H) \leq \llbracket \Theta \rrbracket_{C''}.$$

Em $[-\circ R]$, se $\Gamma = \emptyset$, então

$$\llbracket \phi \rrbracket_{C''} \leq \llbracket \psi \rrbracket_{C''}$$

donde

$$\llbracket \phi - \circ \psi \rrbracket_{C''}(\vec{u}) = EP_{C''} \& E(\vec{u}) = \llbracket V_{C''}(\phi - \circ \psi) \rrbracket_{C''}(\vec{u}).$$

Em $[-\circ L]$, se $\Gamma = \emptyset$, temos

$$\llbracket \phi \rrbracket_{C''} = \llbracket V_{C''}(\phi) \rrbracket_{C''}$$

$$\llbracket \Sigma \rrbracket_{C''} \& \llbracket \psi \rrbracket_{C''} \& \llbracket \Delta \rrbracket_{C''} \leq \llbracket \Theta \rrbracket_{C''}$$

e então, como $\llbracket V_{C''}(\phi) \rrbracket_{C''} = \llbracket V_C(\phi) \rrbracket_{C''}$,

$$\llbracket \Sigma \rrbracket_{C''} \& \llbracket V_C(\phi) \rrbracket_{C''} \& (\llbracket \phi \rrbracket_{C''} \rightarrow \llbracket \psi \rrbracket_{C''}) \& \llbracket \Delta \rrbracket_{C''} \leq \llbracket \Theta \rrbracket_{C''}. \quad \square$$

Demonstração do teorema 2.5.2 : Por indução no comprimento mínimo k de uma prova de S em (QPC) a partir de L .

Se $k = 1$, suponha que S é uma instância de um axioma (no caso de $[SUBS]$, temos que $x_{\top} \in \text{clau}([SUBS])$); portanto, como já foi provado em 2.5.7 e 2.5.8, S é válido em toda interpretação $\mathcal{I}$. Se $S \in L$, então S é válido em $\mathcal{I}$, por hipótese.

Suponha o resultado verdadeiro para todo sequente S' que admite uma prova de comprimento $\leq k$, para $1 \leq k$ a partir de L (hipótese de indução) e seja S com prova P de comprimento mínimo $k + 1$ a partir de L .

Assim, S é o resultado da aplicação de alguma regra, ou do axioma $[SUBS]$, obtido a partir de sequentes anteriores $S_1, \dots, S_n$ em P . Assim, se $\mathcal{I}$ é uma interpretação nas hipóteses do enunciado, então $\mathcal{I} \models S_i$ para todo i , pela hipótese de indução. Portanto, pela correte de cada uma das regras e do axioma $[SUBS]$, temos que $\mathcal{I} \models S$. $\square$

Claro que o Teorema de Correte de 2.5.3 é uma consequência imediata de 2.5.2, com $L = \emptyset$.

Na prática, as provas em (QPC) são realizadas da maneira seguinte: iniciada a partir de axiomas (no caso de $[SUBS]$, $x_{\top} \in \text{clau}([SUBS])$), pode prosseguir se pudermos utilizar regra sem cláusulas ou que contém a justificativa trivial.

Em um ponto da prova, precisamos aplicar uma regra (ou o axioma $[SUBS]$) com uma cláusula que não contém $x_{\top}$. Pela definição 2.5.1, devemos parar a prova e tentar provar, uma a uma, as justificativas da cláusula; se conseguirmos provar todos os sequentes de alguma justificativa x , devemos colocar as provas dos sequentes de x antes de aplicar a regra ou axioma. É claro que o processo de provar esses sequentes terá as mesmas características, i.e., precisaremos eventualmente provar justificativas para aplicar as regras; essas justificativas podem levar a provar novas justificativas, etc.; portanto, vemos que toda prova vêm munida de um repertório de provas paralelas,

as quais devem ser recolocadas antes do ponto em que foram requisitadas. Porém, devemos observar que nem sempre provamos sequentes auxiliares para aplicar uma regra; na regra $[CUT]$ (um exemplo típico), para conferir $E(S, T)$, onde $S = (\Gamma \vdash \phi)$, devemos provar alguma justificativa de $K_E(\alpha, C, T)$ para toda fórmula α de $\text{red}(\Gamma)$; mas, se α não utiliza o conectivo $\rightarrow$ nem a negação $\neg$, então é simples verificar por indução na complexidade de α que $x_\top \in K_E(\alpha, C, T)$ para todo C, T . Dessa maneira, se nenhuma fórmula de Γ utiliza $\rightarrow$ nem $\neg$, então $x_\top \in K_E(\text{red}(\Gamma), C, T)$. Da mesma maneira, se ϕ não utiliza $\vee$ nem $\neg$ nem $\otimes$ e, para toda subfórmula $\alpha \rightarrow \beta$, α não utiliza o conectivo $\rightarrow$, então $x_\top \in K_D(\phi, C, T)$, donde $x_\top \in E(S, T)$. Assim, em certos casos, as condições de extensão ou redução exigidas na cláusula de uma regra podem ser verificadas mediante inspeção sintática, sem precisar de uma prova auxiliar. Para representar a dinâmica do processo de provas em (QPC) , introduzimos uma outra noção de prova, chamada de prova aberta, que resultará equivalente à noção em 2.5.1.

Definição 2.5.10 : *Seja L um conjunto de sequentes e S um sequente. Uma prova aberta de S em (QPC) (a partir de L) é uma estrutura P da forma*

$$\begin{array}{ccccccc} S_1, \dots, S_{i_1}, & S_{i_1+1}, \dots, S_{i_2}, & S_{i_2+1}, \dots, S_{i_k}, & S_{i_k+1}, \dots, S_m = S \\ [P_1^1] & [P_1^2] & \dots & [P_1^k] \\ \vdots & \vdots & & \vdots \\ [P_{n_1}^1] & [P_{n_2}^2] & \dots & [P_{n_k}^k] \end{array}$$

onde os S_j são sequentes e os (eventuais) $[P_l^h]$ são provas abertas em (QPC) de sequentes R_l^h efetuadas na ordem $[P_1^1], \dots, [P_{n_1}^1], [P_1^2], \dots, [P_{n_k}^k]$, sendo que cada $[P_l^h]$ é realizada a partir de (eventualmente) sequentes em $[P_r^s]$ (com $s < h$) ou em $[P_r^h]$ (com $r < l$) ou sequentes S_j , com $j \leq i_h$, ou sequentes em L . Além disso, cada S_r é um axioma (no caso de $[SUBS]$, utilizando a justificativa trivial), ou $S_r \in L$, ou é deduzido de sequentes S_j (com $j < r$) e (eventualmente) R_l^h (com $i_h < r$) por uma regra de inferência $\mathcal{R}$ (ou pelo axioma $[SUBS]$), de maneira que, se a instância de $\mathcal{R}$ ou $[SUBS]$ possui uma cláusula CL que não contém a justificativa trivial, então existe $x \in CL$ tal que todos os sequentes $\neq (\vdash \top)$ de x ocorrem entre os sequentes S_j e R_l^h .

Observe que uma prova aberta sem provas abertas auxiliares $[P_l^h]$ é uma prova de S em (QPC) (a partir de L). Se $L = \emptyset$, então P é uma prova aberta de S em (QPC) .

Dada uma prova aberta P de S a partir de L , definimos a largura de P , denotada por $L(P)$, como sendo:

$$\begin{aligned} L(P) &= 0, & \text{se } P \text{ não utiliza provas } [P_l^h]; \\ L(P) &= \text{Max}\{L(P_l^h) : l = 1, \dots, n_h, h = 1, \dots, k\} + 1 & \text{em caso contrário.} \end{aligned}$$

Proposição 2.5.11 : *Seja S um sequente e L um conjunto de sequentes. Então, S é demonstrável em (QPC) a partir de L se e somente se S admite uma prova aberta P em (QPC) a partir de L .*

Demonstração: É suficiente mostrar que se S admite uma prova aberta, então admite uma prova. Iremos proceder por indução na largura mínima de uma prova aberta P , mostrando que P pode ser transformada numa prova P' de S em (QPC) a partir de L .

Se $L(P) = 0$, então a prova aberta é uma prova em (QPC) a partir de L .

Suponha que para todo sequente S que admite uma prova aberta P a partir de L com $L(P) \leq N$ ($0 \leq N$), podemos transformar P numa prova P' de S em (QPC) a partir de L . Seja S com uma prova aberta P a partir de L de largura $N + 1$. Assim, P é da forma

$$\begin{array}{cccc} S_1, \dots, S_{i_1}, & S_{i_1+1}, \dots, S_{i_2}, & S_{i_2+1}, \dots, S_{i_k}, & S_{i_k+1}, \dots, S_m = S \\ [P_1^1] & [P_1^2] & \dots & [P_1^k] \\ \vdots & \vdots & & \vdots \\ [P_{n_1}^1] & [P_{n_2}^2] & \dots & [P_{n_k}^k] \end{array}$$

onde $L(P_l^h) \leq N$; logo, pela hipótese de indução, P_1^1 pode ser transformada numa prova Q_1^1 de R_1^1 em (QPC) a partir de L . Assim, temos que Q_1^1 é uma sequência $T_1, \dots, T_{m_1} = R_1^1$ que pode ser colocada a continuação de S_{i_1} , e então a sequência

$$S_1, \dots, S_{i_1}, T_1, \dots, T_{m_1} = R_1^1$$

é uma prova de R_1^1 em (QPC) a partir de L . Usando novamente a hipótese de indução para P_j^1 , com $j > 1$, colocamos a continuação as sequências Q_j^1 , com $j = 2, \dots, n_1$, e continuamos com a sequência original, obtendo uma prova em (QPC)

$$S_1, \dots, S_{i_1}, R_1, \dots, R_{j_1}, S_{i_1+1}, \dots, S_{i_2}$$

de S_{i_2} a partir de L . Repetimos o processo para as provas P_l^h , com $l = 1, \dots, n_h$, e $h = 2, \dots, k$, obtendo finalmente uma prova P' de S em (QPC) a partir de L . $\square$

2.6 Teoremas Básicos em (QPC)

Uma técnica de prova fundamental em (QPC) consiste em combinar os axiomas $[CH1.1]$ e $[AX3]$, junto com a regra $[CUT]$; desta maneira, por $[AX3]$ ou $[CH1.1]$, partimos de sequentes da forma $\phi_C \vdash \phi$ ou $\phi \vdash \phi_C$ no lugar de $\phi \vdash \phi$, onde C é um contexto para todas as fórmulas envolvidas na prova. Esta técnica será utilizada na proposição 2.6.4. A notação $\alpha \sim \beta$ indica que as fórmulas α e β são equivalentes em (QPC) , i.e., os sequentes

$$\alpha \vdash \beta, \quad \beta \vdash \alpha$$

são ambos demonstráveis em (QPC) .

Lema 2.6.1 : Seja ϕ uma fórmula, C um contexto para ϕ e $\epsilon(C)$ o extant de C .

(a) O sequente $V_C(\phi) \vdash \epsilon(C)$ é demonstrável.

(b) O sequente $\phi_C \vdash \epsilon(C)$ é demonstrável.

Demonstração: (a) Por indução na complexidade de ϕ .

Se ϕ é atômica, então $V_C(\phi) = \epsilon(C)$ e o resultado é consequência de $[AX3]$.

Suponha o resultado verdadeiro para ϕ de complexidade $\leq k$ e seja ϕ de complexidade $k + 1$.

Se $\phi = \neg\alpha$ ou $\phi = \alpha \multimap \beta$, está claro que $V_C(\phi) = \epsilon(C)$.

Se $\phi = \alpha \wedge \beta$, então $V_C(\phi) = V_C(\alpha) \wedge V_C(\beta)$ e portanto, já que $\mathbf{Etipos}(V_C(\phi)) = \emptyset = \mathbf{Etipos}(\epsilon(C))$ para toda ϕ e $\epsilon(C)$, podemos escrever

$$\frac{\frac{V_C(\alpha) \vdash V_C(\alpha)}{V_C(\alpha) \wedge V_C(\beta) \vdash V_C(\alpha)} [\wedge L1] \quad V_C(\alpha) \vdash \epsilon(C) (HI)}{V_C(\alpha) \wedge V_C(\beta) \vdash \epsilon(C)} [CUT] .$$

Se $\phi = \alpha \otimes \beta$, então $V_C(\phi) = V_C(\alpha) \otimes V_C(\beta)$ e então

$$\frac{\frac{V_C(\alpha), V_C(\beta) \vdash V_C(\alpha)}{V_C(\alpha) \otimes V_C(\beta) \vdash V_C(\alpha)} [\otimes L] \quad V_C(\alpha) \vdash \epsilon(C) (HI)}{V_C(\alpha) \otimes V_C(\beta) \vdash \epsilon(C)} [CUT] .$$

Se $\phi = \alpha \vee \beta$, então $V_C(\phi) = V_C(\alpha) \vee V_C(\beta)$ e então

$$\frac{V_C(\alpha) \vdash \epsilon(C) \quad V_C(\beta) \vdash \epsilon(C)}{V_C(\alpha) \vee V_C(\beta) \vdash \epsilon(C)} [\vee L1] .$$

Se $\phi = (Qv)\alpha$, com $Q = \forall, \exists$ e $v \in \mathcal{V}_t$, então $V_C(\phi) = V_{(z,C)}(\alpha[z/v])$, onde z é livre para v em α e não ocorre em C . Seja $\epsilon(z, C)$ o extant de (z, C) . Se $t \in T = \mathbf{tipos}(C)$, então $\epsilon(z, C) = \epsilon(C)$ e então, por hipótese de indução, $V_{(z,C)}(\alpha[z/v]) \vdash \epsilon(C)$ é demonstrável. Se $t \notin T$, então $\epsilon(z, C) \sim (\exists v_0^t) Ev_0^t \wedge \epsilon(C)$ e temos

$$\frac{V_{(z,C)}(\alpha[z/v]) \vdash (\exists v_0^t) Ev_0^t \wedge \epsilon(C) (HI) \quad \frac{\epsilon(C) \vdash \epsilon(C)}{(\exists v_0^t) Ev_0^t \wedge \epsilon(C) \vdash \epsilon(C)} [\wedge L2]}{V_{(z,C)}(\alpha[z/v]) \vdash \epsilon(C)} [CUT] .$$

(b) Usando (a), temos

$$\frac{\phi_C \vdash V_C(\phi) [CH1.0] \quad V_C(\phi) \vdash \epsilon(C)}{\phi_C \vdash \epsilon(C)} [CUT]$$

onde a aplicação do $[CUT]$ é válida, pois $x_\top \in E((V_C(\phi) \vdash \epsilon(C)), T)$ para todo T , em virtude da sua sintaxe. $\square$

Corolário 2.6.2 : Seja $\phi = (Q_1 v_1) \cdots (Q_n v_n) \alpha$ uma fórmula, com $Q_i = \forall$ ou $Q_i = \exists$ ($i = 1, \dots, n$) e C um contexto para ϕ . Então, todos os sequentes da justificativa da cláusula $ED(\phi, C, T)$ são demonstráveis em (QPC) , onde T é o conjunto dos tipos das v_i . Além disso, o sequente $(\exists)\phi_C \vdash \epsilon(T)$ é demonstrável.

Demonstração: Seja $C = (\vec{x}; \vec{a})$, e considere as $n + 1$ subfórmulas de ϕ

$$\phi_i = (\mathcal{Q}_i v_i) \cdots (\mathcal{Q}_n v_n) \alpha \quad (i = 1, \dots, n), \quad \phi_{n+1} = \alpha.$$

Seja $C_1 = C$, $C_i = (\vec{z}_i, C) = \mathbf{C}(\phi_i, \phi, C)$ ($i = 2, \dots, n + 1$) e

$$(\phi_i[\vec{z}_i/\vec{w}_i])_{C_i} = \phi_i[\vec{z}_i/\vec{w}_i] \otimes \varphi_i, \quad \psi_i = F(\phi_i, \phi, C) = (\exists)(\phi_i[\vec{z}_i/\vec{w}_i] \otimes \varphi_i)$$

para $i = 1, \dots, n + 1$. Logo, $(\psi_i)_{\vec{a}} = \psi_i$ e

$$V_{\vec{a}}(\psi_i) = V_{C_i}((\phi_i[\vec{z}_i/\vec{w}_i])_{C_i}) = V_{(\vec{z}_{n+1}, C)}(\alpha[\vec{z}_{n+1}/\vec{w}_{n+1}]) \otimes V_{C_i}(\varphi_i),$$

por causa do seguinte

Fato: Seja ϕ uma fórmula, $C \supseteq C((\exists v)\phi)$, x, y livres para v em ϕ , $x \neq y$, tal que x, y não ocorrem em C . Então,

$$V_{(x,C)}(\phi[x/v]) = V_{(y,C)}(\phi[y/v]) = V_{(x,y,C)}(\phi[x/v]).$$

A prova do **Fato**, por indução na complexidade de ϕ , é imediata.

Se $\epsilon(T')$ é o extent de $(\vec{z}_{n+1}, C)$, então $\epsilon(T') \vdash \epsilon(T)$ é demonstrável, portanto, por 2.6.1 (a),

$$\frac{\frac{V_{C'}(\alpha'), V_{C_i}(\varphi_i) \vdash V_{C'}(\alpha')}{V_{C'}(\alpha') \otimes V_{C_i}(\varphi_i) \vdash V_{C'}(\alpha')} \quad \frac{V_{C'}(\alpha') \vdash \epsilon(T') \quad \epsilon(T') \vdash \epsilon(T)}{V_{C'}(\alpha') \vdash \epsilon(T)}}{V_{C'}(\alpha') \otimes V_{C_i}(\varphi_i) \vdash \epsilon(T)}$$

onde $\alpha' \equiv_{def} \alpha[\vec{z}_{n+1}/\vec{w}_{n+1}]$ e $C' = (\vec{z}_{n+1}, C)$; assim

$$\frac{(\psi_i)_{\vec{a}} \vdash V_{\vec{a}}(\psi_i) \quad V_{\vec{a}}(\psi_i) \vdash \epsilon(T)}{(\psi_i)_{\vec{a}} \vdash \epsilon(T)},$$

i.e., $\psi_i \vdash \epsilon(T)$ é demonstrável para $i = 1, \dots, n + 1$. Se $\beta \in SFE(\alpha)$, considere

$$D = \mathbf{C}(\beta, \phi, C) = (\vec{z}, C), \quad \delta = F(\beta, \phi, C) = (\exists)(\beta[\vec{z}/\vec{w}])_D.$$

Portanto, o **Fato** garante

$$(*) \quad (\beta[\vec{z}/\vec{w}])_D = \beta[\vec{z}/\vec{w}] \otimes \psi, \quad V_{\vec{a}}((\exists)\beta[\vec{z}/\vec{w}])_D = V_D(\beta[\vec{z}/\vec{w}]) \otimes V_D(\psi)$$

e então podemos escrever

$$\frac{\frac{V_D(\beta[\vec{z}/\vec{w}]), V_D(\psi) \vdash V_D(\beta[\vec{z}/\vec{w}])}{V_D(\beta[\vec{z}/\vec{w}]) \otimes V_D(\psi) \vdash V_D(\beta[\vec{z}/\vec{w}])} \quad \frac{V_D(\beta[\vec{z}/\vec{w}]) \vdash \epsilon(D) \quad \epsilon(D) \vdash \epsilon(T)}{V_D(\beta[\vec{z}/\vec{w}]) \vdash \epsilon(T)}}{(**) \quad V_D(\beta[\vec{z}/\vec{w}]) \otimes V_D(\psi) \vdash \epsilon(T)}.$$

Finalmente, observemos que $\delta = \delta_{\vec{a}}$; logo, por [CH1.0], (*) e (**), temos

$$\frac{\delta \vdash V_D(\beta[\vec{z}/\vec{w}]) \otimes V_D(\psi) \quad V_D(\beta[\vec{z}/\vec{w}]) \otimes V_D(\psi) \vdash \epsilon(T)}{\delta \vdash \epsilon(T)},$$

onde a aplicação da regra $[CUT]$ é válida, pois $x_\top \in E((V_C(\phi) \vdash \epsilon(T)), T')$ para todo ϕ, C, T, T' , como foi observado na prova de 2.6.1(b). $\square$

Provaremos agora propriedades básicas dos quantificadores, estabelecendo, por exemplo, que a ordem de quantificação (para quantificadores da mesma classe) é irrelevante, assim como a variável quantificada.

Lema 2.6.3 : *Sejam ϕ, ψ fórmulas e x, y, z variáveis diferentes.*

- (a) *Se $x \in VAR(\phi)$ e $y \notin VAR(\phi)$ é livre para x em ϕ , então $(\forall x)\phi \sim (\forall y)\phi[y/x]$;*
- (b) *Se $x \in VAR(\phi)$ e $y \notin VAR(\phi)$ é livre para x em ϕ , então $(\exists x)\phi \sim (\exists y)\phi[y/x]$;*
- (c) *Se $x \in VAR(\phi)$, o sequente $(\forall x)\phi \vdash (\exists x)\phi$ é demonstrável;*
- (d) *Se $x, z \in VAR(\phi)$, então $(\forall x)(\forall z)\phi \sim (\forall z)(\forall x)\phi$;*
- (e) *Se $x, z \in VAR(\phi)$, então $(\exists x)(\exists z)\phi \sim (\exists z)(\exists x)\phi$;*
- (f) *Se $x \in VAR(\phi) \cap VAR(\psi)$ e $\phi \vdash \psi$ é demonstrável, então os seguintes*

$$(\forall x)\phi \vdash (\forall x)\psi, \quad (\exists x)\phi \vdash (\exists x)\psi$$

são demonstráveis. Em particular, se $x \in VAR(\phi)$,

$$(\forall x)\phi \sim (\forall x)(\phi \otimes Ex), \quad (\exists x)\phi \sim (\exists x)(\phi \otimes Ex);$$

- (g) *Se $C \supseteq C(\phi, \psi)$, então os seguintes sequentes são demonstráveis:*

$$(\exists)(\phi_C \otimes \psi_C) \vdash ((\exists)\phi_C) \otimes ((\exists)\psi_C);$$

$$(\exists)(\phi_C \wedge \psi_C) \vdash ((\exists)\phi_C) \wedge ((\exists)\psi_C);$$

$$(\exists)(\phi_C \vee \psi_C) \vdash ((\exists)\phi_C) \vee ((\exists)\psi_C); \quad ((\exists)\phi_C) \vee ((\exists)\psi_C) \vdash (\exists)(\phi_C \vee \psi_C).$$

Demonstração: (a) Temos a seguinte prova

$$\frac{\frac{\phi[y/x][y/y] \vdash \phi[y/x]}{(\forall y)\phi[y/x] \vdash \phi[y/x]} [\forall L]}{(\forall y)\phi[y/x] \vdash (\forall x)\phi} [\forall R]$$

onde a aplicação de $[\forall L]$ é permitida, pois $x_\top \in \mathbf{clau}([\forall L])$ (se $x \in VAR(\phi)$). A aplicação da regra $[\forall R]$ é permitida pois, se o tipo t de x não está presente em $C = C((\forall y)\phi[y/x], (\forall x)\phi)$, então podemos provar (como no corolário 2.6.2) todos os sequentes da justificativa y_1 de $ED((\forall y)\phi[y/x], C, \{t\})$ e da justificativa y_2 de $ED((\forall x)\phi, C, \{t\})$, assim como o sequente

$$(\exists)(\forall y)\phi[y/x] \vdash (\exists v_0^t)Ev_0^t,$$

e portanto

$$S : \quad (\exists)(\forall y)\phi[y/x] \vdash (\exists)(\forall y)\phi[y/x] \wedge (\exists v_0^t)Ev_0^t.$$

Assim, obtemos todos os sequentes de $y_1 \cup y_2 \cup \{S\} \in R(((\forall y)\phi[y/x] \vdash (\forall x)\phi), \{t\})$. Analogamente, provamos

$$(\forall x)\phi \vdash (\forall y)\phi[y/x].$$

(b) Considere a seguinte prova

$$\frac{\frac{\phi[y/x][y/y] \vdash \phi[y/x]}{\phi[y/x][y/y] \vdash (\exists x)\phi} [\exists R]}{(\exists y)\phi[y/x] \vdash (\exists x)\phi} [\exists L]$$

onde as considerações são as mesmas que no item anterior.

(c) Temos a seguinte prova

$$\frac{\frac{\phi[x/x] \vdash \phi[x/x]}{\phi[x/x] \vdash (\exists x)\phi} [\exists R]}{(\forall x)\phi \vdash (\exists x)\phi} [\exists L]$$

com as mesmas justificativas que nos itens anteriores.

(d) Temos a seguinte dedução

$$\frac{\frac{\frac{\phi[x/x][z/z] \vdash \phi[z/z][x/x]}{(\forall z)\phi[x/x] \vdash \phi[z/z][x/x]} [\forall L]}{(\forall x)(\forall z)\phi \vdash \phi[z/z][x/x]} [\forall L]}{(\forall x)(\forall z)\phi \vdash (\forall x)\phi[z/z]} [\forall R]}{(\forall x)(\forall z)\phi \vdash (\forall z)(\forall x)\phi} [\forall R]$$

com as mesma justificativas que nos itens precedentes.

(e) Idêntico a (d).

(f) São generalizações de (a) e (b), respectivamente e as provas são idênticas.

(g) Considere a prova seguinte:

$$\frac{\frac{\frac{\phi_C \vdash \phi_C}{\phi_C \vdash (\exists)\phi_C} \quad \frac{\psi_C \vdash \psi_C}{\psi_C \vdash (\exists)\psi_C}}{\phi_C, \psi_C \vdash ((\exists)\phi_C) \otimes ((\exists)\psi_C)} \quad \cdot}{\phi_C \otimes \psi_C \vdash ((\exists)\phi_C) \otimes ((\exists)\psi_C)}{(\exists)(\phi_C \otimes \psi_C) \vdash ((\exists)\phi_C) \otimes ((\exists)\psi_C)}$$

As aplicações de $[\exists L]$ são válidas, pelo corolário 2.6.2. Da mesma maneira, provamos:

$$\frac{\frac{\frac{\phi_C \vdash (\exists)\phi_C}{\phi_C \wedge \psi_C \vdash (\exists)\phi_C} \quad \frac{\psi_C \vdash (\exists)\psi_C}{\phi_C \wedge \psi_C \vdash (\exists)\psi_C}}{\phi_C \wedge \psi_C \vdash (\exists)\phi_C \wedge (\exists)\psi_C} \quad ,}{(\exists)(\phi_C \wedge \psi_C) \vdash (\exists)\phi_C \wedge (\exists)\psi_C}$$

$$\frac{\frac{\frac{\phi_C \vdash \phi_C}{\phi_C \vdash \phi_C \vee \psi_C} \quad \frac{\psi_C \vdash \psi_C}{\psi_C \vdash \phi_C \vee \psi_C}}{(\exists)\phi_C \vdash (\exists)(\phi_C \vee \psi_C)} \quad \frac{\psi_C \vdash \psi_C}{(\exists)\psi_C \vdash (\exists)(\phi_C \vee \psi_C)} \quad ,}{((\exists)\phi_C) \vee ((\exists)\psi_C) \vdash (\exists)(\phi_C \vee \psi_C)}$$

$$\frac{\frac{\phi_C \vdash (\exists)\phi_C}{\phi_C \vdash ((\exists)\phi_C) \vee ((\exists)\psi_C)} \quad \frac{\psi_C \vdash (\exists)\psi_C}{\psi_C \vdash ((\exists)\phi_C) \vee ((\exists)\psi_C)}}{\phi_C \vee \psi_C \vdash ((\exists)\phi_C) \vee ((\exists)\psi_C)} \quad . \quad \square$$

$$\frac{}{(\exists)(\phi_C \vee \psi_C) \vdash ((\exists)\phi_C) \vee ((\exists)\psi_C)}$$

Na próxima proposição coletamos algumas propriedades básicas dos conectivos, tais como associatividade, distributividade de $\otimes$ à esquerda de $\vee$ e à direita de $\wedge$, assim como uma versão sintática da regra de *exchange*, a qual é provada reproduzindo os passos da demonstração desta propriedade para os quantais RSI.

Proposição 2.6.4 : *Sejam $\alpha, \beta, \gamma, \alpha_1, \dots, \alpha_n$ fórmulas e τ, κ termos em $\mathbb{L}$. Em (QPC) valem as seguintes propriedades :*

- (1) *Os conectivos $\otimes, \wedge$ e $\vee$ são associativos. Em particular, $\alpha * (\beta * \gamma) \sim (\alpha * \beta) * \gamma$, onde $*$ = $\otimes, \wedge, \vee$.*
- (2) *Se $\alpha \vdash \beta$ é demonstrável, então $\alpha \sim \alpha \otimes \beta$.*
- (3) *$\alpha \otimes (\beta \vee \gamma) \sim \alpha \otimes \beta \vee \alpha \otimes \gamma$.*
- (4) *$\overbrace{\alpha, \dots, \alpha}^{n \text{ vezes}} \vdash \beta$ é demonstrável se e somente se $\alpha \vdash \beta$ é demonstrável.*
- (5) *O sequente $\alpha_1 \wedge \dots \wedge \alpha_n \vdash \alpha_1 \otimes \dots \otimes \alpha_n$ é demonstrável.*
- (6) *$\alpha_1, \dots, \alpha_n \vdash \alpha$ é demonstrável se e somente se $\alpha_1 \otimes \dots \otimes \alpha_n \vdash \alpha$ é demonstrável.*
- (7) *$\alpha_1 \otimes \dots \otimes \alpha_n \sim \alpha_1 \otimes (\top \otimes \alpha_2) \otimes \dots \otimes (\top \otimes \alpha_n)$.*
- (8) *$\alpha \otimes \beta \sim \alpha \wedge (\top \otimes \beta)$.*
- (9) *$(\alpha \wedge \beta) \otimes \gamma \sim \alpha \otimes \gamma \wedge \beta \otimes \gamma$.*
- (10) *$(\top \otimes \alpha_1) \otimes \dots \otimes (\top \otimes \alpha_n) \sim (\top \otimes \alpha_1) \wedge \dots \wedge (\top \otimes \alpha_n)$.*
- (11) *$\alpha_1 \wedge \dots \wedge \alpha_n \sim \alpha_{\sigma(1)} \wedge \dots \wedge \alpha_{\sigma(n)}$ para toda permutação σ de $\{1, \dots, n\}$.*
- (12) *$(\top \otimes \alpha_1) \otimes \dots \otimes (\top \otimes \alpha_n) \sim (\top \otimes \alpha_{\sigma(1)}) \otimes \dots \otimes (\top \otimes \alpha_{\sigma(n)})$ para toda permutação σ de $\{1, \dots, n\}$.*
- (13) *Em (QPC) vale a regra de **exchange** sintático:*

$$[ES] \quad \text{se } \alpha, \alpha_1, \dots, \alpha_n \vdash \beta \text{ é demonstrável, então } \alpha, \alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)} \vdash \beta \text{ é demonstrável,}$$

onde σ é uma permutação de $\{1, \dots, n\}$.
- (14) *$(\alpha_1)_C \otimes \dots \otimes (\alpha_n)_C \sim (\alpha_1 \otimes \dots \otimes \alpha_n)_C$ para todo $C \supseteq C(\alpha_1, \dots, \alpha_n)$.*
- (15) *Seja α tal que $\Gamma, \alpha \vdash \alpha$ é demonstrável para todo Γ . Se $C \supseteq C(\alpha)$, então $\Gamma, \alpha_C \vdash \alpha_C$ é demonstrável para todo Γ .*
- (16) *Seja α tal que $\Gamma, \alpha \vdash \alpha$ é demonstrável para todo Γ . Então, $\beta \otimes \alpha \sim \beta \wedge \alpha$ para todo β .*
- (17) *O sequente $\Gamma, E\tau \vdash E\tau$ é demonstrável para todo Γ .*
- (18) *O sequente $E_s\tau \vdash E_t\kappa$ é demonstrável.*

(19) Seja α tal que $\Gamma, \alpha \vdash \alpha$ é demonstrável para todo Γ . Então, para qualquer β e Γ , o sequente $\Gamma, \alpha \otimes \beta \vdash \alpha \otimes \beta$ é demonstrável.

(20) Seja α tal que $\Gamma, \alpha \vdash \alpha$ é demonstrável para todo Γ . Se $\alpha_1, \dots, \alpha_n \vdash \alpha$ é demonstrável, então $\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)} \vdash \alpha$ é demonstrável para toda permutação σ de $\{1, \dots, n\}$.

(21) O sequente $\alpha, \alpha \multimap \beta \vdash \beta$ é demonstrável. Logo, $\alpha, \Gamma \vdash \beta$ é demonstrável se e somente se $\Gamma \vdash \alpha \multimap \beta$ é demonstrável.

(22) Se $\alpha, \beta \vdash \quad$ é demonstrável, então $\beta, \alpha \vdash \quad$ é demonstrável. Logo, os sequentes $\neg \alpha, \alpha \vdash \quad$ e $\alpha \vdash \neg \neg \alpha$ são demonstráveis, e $\neg \alpha \sim \neg \neg \neg \alpha$.

(23) $\alpha, \Gamma \vdash \quad$ é demonstrável se e somente se $\Gamma \vdash \neg \alpha$ é demonstrável.

(24) O sequente $\neg(\alpha \vee \beta) \vdash \neg \alpha \wedge \neg \beta$ é demonstrável.

(25) O sequente $\neg \alpha \vee \neg \beta \vdash \neg(\alpha \wedge \beta)$ é demonstrável.

(26) Temos que $\alpha \multimap (\beta \multimap \gamma) \sim (\beta \otimes \alpha) \multimap \gamma$.

Demonstração:

(1) Seja $C = C(\alpha, \beta, \gamma)$. Por $[AX3]$ e $[\otimes L]$ temos

$$\alpha_C \vdash \alpha, \quad \beta_C \vdash \beta, \quad \gamma_C \vdash \gamma,$$

e então, por $[\otimes R]$, obtemos

$$\frac{\frac{\alpha_C \vdash \alpha \quad \beta_C \vdash \beta}{\alpha_C, \beta_C \vdash \alpha \otimes \beta} \quad \gamma_C \vdash \gamma}{\alpha_C, \beta_C, \gamma_C \vdash (\alpha \otimes \beta) \otimes \gamma},$$

pois os tipos dos sequentes são os mesmos. De $[CH1.1]$ e $[CUT]$ vem

$$\frac{\alpha \vdash \alpha_C \quad \alpha_C, \beta_C, \gamma_C \vdash (\alpha \otimes \beta) \otimes \gamma}{\alpha, \beta_C, \gamma_C \vdash (\alpha \otimes \beta) \otimes \gamma},$$

pois os contextos dos sequentes coincidem. Eliminando β_C e γ_C da mesma maneira, obtemos

$$\frac{\alpha, \beta, \gamma \vdash (\alpha \otimes \beta) \otimes \gamma}{\alpha \otimes (\beta \otimes \gamma) \vdash (\alpha \otimes \beta) \otimes \gamma}.$$

A prova do sequente $(\alpha \otimes \beta) \otimes \gamma \vdash \alpha \otimes (\beta \otimes \gamma)$ é análoga.

Com relação ao conectivo $\wedge$, provamos:

$$\frac{\frac{\alpha \vdash \alpha_C}{\alpha \wedge (\beta \wedge \gamma) \vdash \alpha_C} \quad \alpha_C \vdash \alpha}{\alpha \wedge (\beta \wedge \gamma) \vdash \alpha}.$$

Da mesma maneira, obtemos

$$\alpha \wedge (\beta \wedge \gamma) \vdash \beta \quad \alpha \wedge (\beta \wedge \gamma) \vdash \gamma,$$

donde, por $[\wedge R]$,

$$\alpha \wedge (\beta \wedge \gamma) \vdash (\alpha \wedge \beta) \wedge \gamma.$$

A prova de $(\alpha \wedge \beta) \wedge \gamma \vdash \alpha \wedge (\beta \wedge \gamma)$ é análoga.

Finalmente,

$$\frac{\frac{\frac{\alpha_C \vdash \alpha}{\alpha_C \vdash \alpha \vee \beta}}{\alpha_C \vdash (\alpha \vee \beta) \vee \gamma}}{\alpha \vdash (\alpha \vee \beta) \vee \gamma}$$

Da mesma maneira, são provados

$$\beta \vdash (\alpha \vee \beta) \vee \gamma, \quad \gamma \vdash (\alpha \vee \beta) \vee \gamma$$

donde obtemos, por $[\vee L1]$,

$$\alpha \vee (\beta \vee \gamma) \vdash (\alpha \vee \beta) \vee \gamma.$$

O sequente $(\alpha \vee \beta) \vee \gamma \vdash \alpha \vee (\beta \vee \gamma)$ é provado analogamente.

(2) Seja $C = C(\alpha, \beta)$ e assumamos que $\alpha \vdash \beta$ é demonstrável. Assim:

$$\begin{array}{c} \vdots \\ \frac{\frac{\frac{\alpha_C \vdash \alpha \quad \alpha \vdash \beta}{\alpha_C \vdash \beta}}{\alpha_C, \alpha_C \vdash \alpha \otimes \beta}}{\frac{(\alpha_C) \otimes (\alpha_C) \vdash \alpha \otimes \beta}}{\alpha_C \vdash \alpha \otimes \beta}} \quad \alpha_C \vdash \alpha \quad \alpha_C \vdash \beta \quad \alpha_C \vdash (\alpha_C) \otimes (\alpha_C) \quad \alpha \vdash \alpha_C \\ \hline \alpha \vdash \alpha \otimes \beta \end{array}$$

Por outro lado, por $[AX3]$ e $[\otimes L]$, sempre temos (sem precisar de $\alpha \vdash \beta$) o sequente

$$\frac{\alpha, \beta \vdash \alpha}{\alpha \otimes \beta \vdash \alpha}.$$

(3) Seja $C = C(\alpha, \beta, \gamma)$. Temos

$$\frac{\frac{\alpha \vdash \alpha_C \quad \beta \vdash \beta_C \quad \frac{\alpha_C \vdash \alpha \quad \frac{\beta_C \vdash \beta}{\beta_C \vdash \beta \vee \gamma}}{\alpha_C, \beta_C \vdash \alpha \otimes (\beta \vee \gamma)}}{\alpha, \beta \vdash \alpha \otimes (\beta \vee \gamma)}}{\alpha \otimes \beta \vdash \alpha \otimes (\beta \vee \gamma)}$$

Analogamente, provamos o sequente $\alpha \otimes \gamma \vdash \alpha \otimes (\beta \vee \gamma)$; portanto obtemos

$$\frac{\alpha \otimes \beta \vdash \alpha \otimes (\beta \vee \gamma) \quad \alpha \otimes \gamma \vdash \alpha \otimes (\beta \vee \gamma)}{(\alpha \otimes \beta) \vee (\alpha \otimes \gamma) \vdash \alpha \otimes (\beta \vee \gamma)}.$$

Por outro lado, podemos escrever

$$\frac{\alpha \vdash \alpha_C \quad \beta \vdash \beta_C \quad \frac{\frac{\alpha_C \vdash \alpha \quad \beta_C \vdash \beta}{\alpha_C, \beta_C \vdash \alpha \otimes \beta}}{\alpha_C, \beta_C \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma)}}{\alpha, \beta \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma)};$$

analogamente, provamos o sequente $\alpha, \gamma \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma)$; assim, obtemos

$$\frac{\frac{\alpha, \beta \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma) \quad \alpha, \gamma \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma)}{\alpha, \beta \vee \gamma \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma)}}{\alpha \otimes (\beta \vee \gamma) \vdash (\alpha \otimes \beta) \vee (\alpha \otimes \gamma)} .$$

(4) Suponha que $n = k + 2 \geq 2$; seja $C = C(\alpha, \beta)$ e $\Gamma = \overbrace{\alpha, \dots, \alpha}^{k \text{ vezes}}$ (eventualmente, $\Gamma = \emptyset$). Assim assumindo que $\Gamma, \alpha, \alpha \vdash \beta$ é demonstrável, obtemos:

$$\begin{array}{c} \vdots \\ \frac{\frac{\Gamma, \alpha, \alpha \vdash \beta \quad \alpha_C \vdash \alpha}{\Gamma, \alpha_C, \alpha_C \vdash \beta} \quad \alpha_C \vdash \alpha_C \otimes \alpha_C \quad \alpha \vdash \alpha_C}{\Gamma, \alpha_C \otimes \alpha_C \vdash \beta} \\ \hline \Gamma, \alpha_C \vdash \beta \\ \hline \Gamma, \alpha \vdash \beta \end{array} ,$$

eliminando uma cópia de α . Repetindo o processo k vezes, provamos $\alpha \vdash \beta$. Reciprocamente, se $\alpha \vdash \beta$ é demonstrável, $n = k + 2 \geq 2$, e Γ é como acima, temos

$$\begin{array}{c} \vdots \\ \frac{\frac{\alpha \vdash \beta \quad \alpha, \alpha_C, \Gamma \vdash \alpha}{\alpha, \alpha_C, \Gamma \vdash \beta} \quad \alpha \vdash \alpha_C}{\alpha, \alpha, \Gamma \vdash \beta} . \end{array}$$

(5) Seja $C = C(\alpha_1, \dots, \alpha_n)$, $\alpha \equiv_{def} \alpha_1 \wedge \dots \wedge \alpha_n$ e $\beta \equiv_{def} \alpha_1 \otimes \dots \otimes \alpha_n$, associados de maneira arbitrária com relação aos parênteses. Então

$$\frac{\frac{\frac{\alpha_i \vdash (\alpha_i)_C}{\alpha \vdash (\alpha_i)_C} \quad (\alpha_i)_C \vdash \alpha_i}{\alpha \vdash \alpha_i}}{\alpha, \dots, \alpha \vdash \beta} ,$$

e o resultado segue de (4).

(6) Seja $C = C(\alpha_1, \dots, \alpha_n, \alpha)$ e $\beta = \alpha_1 \otimes \dots \otimes \alpha_n$ (associados de maneira arbitrária). Claramente,

$$\begin{array}{c} \vdots \\ \frac{\alpha_1, \dots, \alpha_n \vdash \alpha}{\beta \vdash \alpha} , \end{array}$$

por $[\otimes L]$. Suponha agora que $\beta \vdash \alpha$ é demonstrável. Então, para $i = 1, \dots, n$, obtemos:

$$\frac{\frac{\frac{(\alpha_i)_C \vdash \alpha_i}{(\alpha_1)_C, \dots, (\alpha_n)_C \vdash \beta} \quad \beta \vdash \alpha}{(\alpha_1)_C, \dots, (\alpha_n)_C \vdash \alpha}}{\alpha_1, \dots, \alpha_n \vdash \alpha} .$$

(7) Seja $C = C(\alpha_1, \dots, \alpha_n)$ e considere

$$\alpha = ((\alpha_1 \otimes \top) \otimes \dots \otimes (\alpha_{n-1} \otimes \top)) \otimes \alpha_n, \quad \beta = \alpha_1 \otimes ((\top \otimes \alpha_2) \otimes \dots \otimes (\top \otimes \alpha_n)).$$

Por (1), temos que $\alpha \sim \beta$. Logo, para $i = 1, \dots, n - 1$, podemos escrever

$$\frac{\frac{\frac{(\alpha_i)_C \vdash \alpha_i \quad (\alpha_i)_C \vdash \top}{(\alpha_i)_C, (\alpha_i)_C \vdash \alpha_i \otimes \top}}{(\alpha_i)_C \otimes (\alpha_i)_C \vdash \alpha_i \otimes \top} \quad (\alpha_i)_C \vdash (\alpha_i)_C \otimes (\alpha_i)_C \quad (\alpha_n)_C \vdash \alpha_n \quad \alpha \vdash \beta}{(\alpha_i)_C \vdash \alpha_i \otimes \top} \quad \frac{(\alpha_1)_C, \dots, (\alpha_n)_C \vdash \alpha}{(\alpha_1)_C, \dots, (\alpha_n)_C \vdash \beta}$$

Logo, de $\alpha_i \vdash (\alpha_i)_C$ ($i = 1, \dots, n$), provamos, por $[CUT]$ e $[\otimes L]$, o sequente $\alpha_1 \otimes \dots \otimes \alpha_n \vdash \beta$. Por outro lado, se $(\alpha_i)_C = \alpha_i \otimes \phi_i$, então

$$\frac{\alpha_i, \phi_i, \top \vdash \alpha_i}{(\alpha_i)_C \otimes \top \vdash \alpha_i}$$

para $i = 1, \dots, n - 1$. Logo, se $\gamma = \alpha_1 \otimes \dots \otimes \alpha_n$ e $i < n$, obtemos, por (6),

$$\frac{\frac{\frac{(\alpha_i)_C \otimes \top \vdash \alpha_i \quad (\alpha_n)_C \vdash \alpha_n}{(\alpha_1)_C \otimes \top, \dots, (\alpha_{n-1})_C \otimes \top, (\alpha_n)_C \vdash \gamma}}{((\alpha_1)_C \otimes \top) \otimes \dots \otimes ((\alpha_{n-1})_C \otimes \top) \otimes (\alpha_n)_C \vdash \gamma} \quad \alpha_i \vdash (\alpha_i)_C \quad \alpha_n \vdash (\alpha_n)_C}{(\alpha_1)_C, \top, \dots, (\alpha_{n-1})_C, \top, (\alpha_n)_C \vdash \gamma} \quad \frac{\alpha_1, \top, \dots, \alpha_{n-1}, \top, \alpha_n \vdash \gamma}{\alpha_1 \otimes (\top \otimes \alpha_2) \otimes \dots \otimes (\top \otimes \alpha_n) \vdash \gamma}$$

(8) Seja $C = C(\alpha, \beta)$. Logo:

$$\frac{\frac{\frac{\alpha_C \vdash \alpha \quad \alpha, \beta_C \vdash \alpha}{\alpha_C, \beta_C \vdash \alpha} \quad \frac{\alpha_C \vdash \top \quad \beta_C \vdash \beta}{\alpha_C, \beta_C \vdash \top \otimes \beta} \quad \alpha \vdash \alpha_C \quad \beta \vdash \beta_C}{\alpha_C, \beta_C \vdash \alpha \wedge (\top \otimes \beta)} \quad \frac{\alpha, \beta \vdash \alpha \wedge (\top \otimes \beta)}{\alpha \otimes \beta \vdash \alpha \wedge (\top \otimes \beta)}$$

Por outro lado, de (5) e (7), obtemos

$$\frac{\alpha \wedge (\top \otimes \beta) \vdash \alpha \otimes (\top \otimes \beta) \quad \alpha \otimes (\top \otimes \beta) \vdash \alpha \otimes \beta}{\alpha \wedge (\top \otimes \beta) \vdash \alpha \otimes \beta}$$

(9) Seja $C = C(\alpha, \beta, \gamma)$. Então

$$\frac{\frac{\frac{\alpha_C \vdash \alpha}{\alpha_C \wedge \beta_C \vdash \alpha} \quad \gamma_C \vdash \gamma}{\alpha_C \wedge \beta_C, \gamma_C \vdash \alpha \otimes \gamma} \quad \gamma \vdash \gamma_C \quad \frac{\frac{\alpha \vdash \alpha_C}{\alpha \wedge \beta \vdash \alpha_C} \quad \frac{\beta \vdash \beta_C}{\alpha \wedge \beta \vdash \beta_C}}{\alpha \wedge \beta \vdash \alpha_C \wedge \beta_C}}{\alpha \wedge \beta, \gamma \vdash \alpha \otimes \gamma} \quad \frac{\alpha \wedge \beta, \gamma \vdash \alpha \otimes \gamma}{(\alpha \wedge \beta) \otimes \gamma \vdash \alpha \otimes \gamma}$$

Da mesma maneira, provamos $(\alpha \wedge \beta) \otimes \gamma \vdash \beta \otimes \gamma$; logo

$$\frac{(\alpha \wedge \beta) \otimes \gamma \vdash \alpha \otimes \gamma \quad (\alpha \wedge \beta) \otimes \gamma \vdash \beta \otimes \gamma}{(\alpha \wedge \beta) \otimes \gamma \vdash (\alpha \otimes \gamma) \wedge (\beta \otimes \gamma)}$$

Por outro lado, temos

$$\frac{\frac{\frac{\alpha_C, \gamma_C \vdash \alpha_C}{\alpha_C, \gamma_C \vdash \alpha} \quad \alpha_C \vdash \alpha}{\alpha_C, \gamma_C \vdash \alpha \wedge (\top \otimes \gamma)} \quad \frac{\alpha_C \vdash \top \quad \gamma_C \vdash \gamma}{\alpha_C, \gamma_C \vdash \top \otimes \gamma}}{\alpha_C \otimes \gamma_C \vdash \alpha \wedge (\top \otimes \gamma)} \quad \frac{}{(\alpha_C \otimes \gamma_C) \wedge (\beta_C \otimes \gamma_C) \vdash \alpha \wedge (\top \otimes \gamma)}$$

Da mesma maneira, provamos $(\alpha_C \otimes \gamma_C) \wedge (\beta_C \otimes \gamma_C) \vdash \beta \wedge (\top \otimes \gamma)$; assim

$$\frac{(\alpha_C \otimes \gamma_C) \wedge (\beta_C \otimes \gamma_C) \vdash \alpha \wedge (\top \otimes \gamma) \quad (\alpha_C \otimes \gamma_C) \wedge (\beta_C \otimes \gamma_C) \vdash \beta \wedge (\top \otimes \gamma)}{(*) \quad (\alpha_C \otimes \gamma_C) \wedge (\beta_C \otimes \gamma_C) \vdash (\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma))}$$

Além disso, temos

$$\frac{\frac{\frac{\alpha \vdash \alpha_C \quad \gamma \vdash \gamma_C}{\alpha, \gamma \vdash \alpha_C \otimes \gamma_C}}{\alpha \otimes \gamma \vdash \alpha_C \otimes \gamma_C}}{(\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash \alpha_C \otimes \gamma_C} \quad ;$$

da mesma maneira, obtemos $(\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash \beta_C \otimes \gamma_C$; então

$$\frac{(\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash \alpha_C \otimes \gamma_C \quad (\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash \beta_C \otimes \gamma_C}{(\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash (\alpha_C \otimes \gamma_C) \wedge (\beta_C \otimes \gamma_C)}$$

Aplicando [CUT] com (*), deduzimos

$$(**) \quad (\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash (\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma)) \quad .$$

Finalmente, com as mesmas técnicas usadas até agora, podemos provar os seguintes

$$(\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma)) \vdash \alpha \wedge \beta, \quad (\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma)) \vdash \top \otimes \gamma \quad ,$$

e então, por [$\wedge R$], obtemos

$$(\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma)) \vdash (\alpha \wedge \beta) \wedge (\top \otimes \gamma).$$

Assim, de (8) vem

$$\frac{(\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma)) \vdash (\alpha \wedge \beta) \wedge (\top \otimes \gamma) \quad (\alpha \wedge \beta) \wedge (\top \otimes \gamma) \vdash (\alpha \wedge \beta) \otimes \gamma}{(\alpha \wedge (\top \otimes \gamma)) \wedge (\beta \wedge (\top \otimes \gamma)) \vdash (\alpha \wedge \beta) \otimes \gamma} \quad ,$$

e então, aplicando [CUT] com (**), deduzimos finalmente

$$(\alpha \otimes \gamma) \wedge (\beta \otimes \gamma) \vdash (\alpha \wedge \beta) \otimes \gamma.$$

(10) Por (5), prova-se o seguinte $(\top \otimes \alpha_1) \wedge \cdots \wedge (\top \otimes \alpha_n) \vdash (\top \otimes \alpha_1) \otimes \cdots \otimes (\top \otimes \alpha_n)$. Por outro lado, provaremos o seguinte

$$\top \otimes \alpha_1, \dots, \top \otimes \alpha_n \vdash \top \otimes \alpha_i$$

para todo $i = 1, \dots, n$. Se $i = 1$, a prova é imediata. Seja $i > 1$ fixo e considere

$$\Gamma = \top, (\alpha_1)_C, \top, \alpha_2, \dots, \top, \alpha_{i-1}, \top; \quad \Delta = \top, \alpha_{i+1}, \dots, \top, \alpha_n.$$

Então

$$\begin{array}{c}
\frac{\Gamma \vdash \top \quad \frac{(\alpha_i)_C, \Delta \vdash (\alpha_i)_C \quad (\alpha_i)_C \vdash \alpha_i}{(\alpha_i)_C, \Delta \vdash \alpha_i}}{\Gamma, (\alpha_i)_C, \Delta \vdash \top \otimes \alpha_i} \quad \alpha_1 \vdash (\alpha_1)_C \quad \alpha_i \vdash (\alpha_i)_C \\
\hline
\frac{\top, (\alpha_1)_C, \top \otimes \alpha_2, \dots, \top \otimes \alpha_{i-1}, \top, (\alpha_i)_C, \top \otimes \alpha_{i+1}, \dots, \top \otimes \alpha_n \vdash \top \otimes \alpha_i}{\top \otimes \alpha_1, \top \otimes \alpha_2, \dots, \top \otimes \alpha_{i-1}, \top \otimes \alpha_i, \top \otimes \alpha_{i+1}, \dots, \top \otimes \alpha_n \vdash \top \otimes \alpha_i}
\end{array}$$

e o resultado segue de $[\otimes L]$ e $[\wedge R]$.

(11) Seja $C = C(\alpha_1, \dots, \alpha_n)$ e σ uma permutação de $\{1, \dots, n\}$. Como antes, é simples provar o seguinte

$$\alpha_1 \wedge \dots \wedge \alpha_n \vdash (\alpha_1)_C \wedge \dots \wedge (\alpha_n)_C.$$

Assim, para $i = 1, \dots, n$, teremos

$$\begin{array}{c}
\frac{(\alpha_i)_C \vdash \alpha_i}{(\alpha_1)_C \wedge \dots \wedge (\alpha_n)_C \vdash \alpha_i} \quad \alpha_1 \wedge \dots \wedge \alpha_n \vdash (\alpha_1)_C \wedge \dots \wedge (\alpha_n)_C \\
\hline
\frac{(\alpha_1)_C \wedge \dots \wedge (\alpha_n)_C \vdash \alpha_{\sigma(1)} \wedge \dots \wedge \alpha_{\sigma(n)}}{\alpha_1 \wedge \dots \wedge \alpha_n \vdash \alpha_{\sigma(1)} \wedge \dots \wedge \alpha_{\sigma(n)}}
\end{array}$$

(12) É imediata a partir de (10) e (11) (os contextos dos seguintes são idênticos).

(13) Seja $C = C(\alpha, \alpha_1, \dots, \alpha_n, \beta)$ e σ uma permutação de $\{1, \dots, n\}$. Suponha que o seguinte $\alpha, \alpha_1, \dots, \alpha_n \vdash \beta$ é demonstrável e seja $\gamma = (\top \otimes (\alpha_1)_C) \otimes (\top \otimes \alpha_2) \otimes \dots \otimes (\top \otimes \alpha_n)$. De (7) vem

$$\begin{array}{c}
\vdots \\
\frac{\alpha, \alpha_1, \dots, \alpha_n \vdash \beta \quad (\alpha_1)_C \vdash \alpha_1}{\alpha, (\alpha_1)_C, \alpha_2, \dots, \alpha_n \vdash \beta} \quad \alpha \otimes \gamma \vdash \alpha \otimes (\alpha_1)_C \otimes \alpha_2 \otimes \dots \otimes \alpha_n \\
\hline
\frac{\alpha \otimes (\alpha_1)_C \otimes \alpha_2 \otimes \dots \otimes \alpha_n \vdash \beta}{(*) \quad \alpha \otimes \gamma \vdash \beta}
\end{array}$$

Por (12), se $i = \sigma^{-1}(1)$ e $\delta = (\top \otimes \alpha_{\sigma(1)}) \otimes \dots \otimes (\top \otimes (\alpha_{\sigma(i)})_C) \otimes \dots \otimes (\top \otimes \alpha_{\sigma(n)})$, então $\delta \sim \gamma$. Logo, por (*) e (6),

$$\begin{array}{c}
\frac{\alpha_C \vdash \alpha \quad \delta \vdash \gamma}{\alpha_C, \delta \vdash \alpha \otimes \gamma} \quad \alpha \otimes \gamma \vdash \beta \\
\hline
\frac{\alpha_C, \delta \vdash \beta}{\alpha_C \otimes \delta \vdash \beta} \\
\hline
\alpha_C, \top \otimes \alpha_{\sigma(1)}, \dots, \top \otimes (\alpha_{\sigma(i)})_C, \dots, \top \otimes \alpha_{\sigma(n)} \vdash \beta
\end{array}$$

Por (1), podemos escrever

$$\frac{\top \otimes \alpha_{\sigma(i)} \vdash (\top \otimes \alpha_{\sigma(i)})_C \quad (\top \otimes \alpha_{\sigma(i)})_C \vdash \top \otimes (\alpha_{\sigma(i)})_C}{\top \otimes \alpha_{\sigma(i)} \vdash \top \otimes (\alpha_{\sigma(i)})_C}$$

e então, obtemos

$$\begin{array}{c}
\frac{\alpha_C, \top \otimes \alpha_{\sigma(1)}, \dots, \top \otimes (\alpha_{\sigma(i)})_C, \dots, \top \otimes \alpha_{\sigma(n)} \vdash \beta \quad \top \otimes \alpha_{\sigma(i)} \vdash \top \otimes (\alpha_{\sigma(i)})_C}{\alpha_C, \top \otimes \alpha_{\sigma(1)}, \dots, \top \otimes \alpha_{\sigma(n)} \vdash \beta} \\
\hline
(**) \quad \alpha_C \otimes (\top \otimes \alpha_{\sigma(1)}) \otimes \dots \otimes (\top \otimes \alpha_{\sigma(n)}) \vdash \beta
\end{array}$$

Como (7) implica o seguinte

$$\alpha_C \otimes \alpha_{\sigma(1)} \otimes \cdots \otimes \alpha_{\sigma(n)} \vdash \alpha_C \otimes (\top \otimes \alpha_{\sigma(1)}) \otimes \cdots \otimes (\top \otimes \alpha_{\sigma(n)}),$$

[*CUT*] com (**), fornece $\alpha_C \otimes \alpha_{\sigma(1)} \otimes \cdots \otimes \alpha_{\sigma(n)} \vdash \beta$. Assim, de (6) vem

$$\frac{\frac{\alpha_C \otimes \alpha_{\sigma(1)} \otimes \cdots \otimes \alpha_{\sigma(n)} \vdash \beta}{\alpha_C, \alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)} \vdash \beta} \quad \alpha \vdash \alpha_C}{\alpha, \alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)} \vdash \beta}.$$

(14) Seja $C \supseteq C(\alpha_1, \dots, \alpha_n)$, $\alpha = \alpha_1 \otimes \cdots \otimes \alpha_n$, $\beta = (\alpha_1)_C \otimes \cdots \otimes (\alpha_n)_C$ e $\alpha_C = \alpha \otimes \phi$. Se $i = 2, \dots, n$, então, [*ES*] nos fornece

$$\frac{\frac{\frac{(\alpha_1)_C, \phi \vdash (\alpha_1)_C \quad \alpha_i \vdash (\alpha_i)_C}{(\alpha_1)_C, \phi, \alpha_2, \dots, \alpha_n \vdash \beta} \quad \alpha_1 \vdash (\alpha_1)_C}{\alpha_1, \phi, \alpha_2, \dots, \alpha_n \vdash \beta}}{\alpha_1, \dots, \alpha_n, \phi \vdash \beta} \quad \alpha \otimes \phi \vdash \beta.$$

Por outro lado, para $i = 1, \dots, n$, temos

$$\frac{\frac{(\alpha_i)_C \vdash \alpha_i}{(\alpha_1)_C, \dots, (\alpha_n)_C \vdash \alpha} \quad \alpha \vdash \alpha_C}{(\alpha_1)_C, \dots, (\alpha_n)_C \vdash \alpha_C} \quad \beta \vdash \alpha_C.$$

(15) Seja $C \supseteq C(\alpha)$, $\Gamma \neq \emptyset$ e $D = C(\Gamma, \alpha_C) \supseteq C$. De [*AX3*], (6), [*ES*] e [*⊗L*], obtemos o seguinte $\alpha_D \vdash \alpha_C$. Assim, se $\alpha_C = \alpha \otimes \phi$, então, por [*ES*], podemos escrever

$$\frac{\frac{\frac{\Gamma, \phi, \alpha \vdash \alpha \quad \alpha \vdash \alpha_D}{\Gamma, \phi, \alpha \vdash \alpha_D} \quad \alpha_D \vdash \alpha_C}{\Gamma, \alpha, \phi \vdash \alpha_D}}{\Gamma, \alpha_C \vdash \alpha_D} \quad \Gamma, \alpha_C \vdash \alpha_C.$$

(16) Por (5), temos $\beta \wedge \alpha \vdash \beta \otimes \alpha$. Por outro lado, o sequente $\beta, \alpha \vdash \alpha$ é demonstrável, por hipótese. Logo, podemos escrever

$$\frac{\frac{\beta, \alpha \vdash \beta \quad \beta, \alpha \vdash \alpha}{\beta, \alpha \vdash \beta \wedge \alpha}}{\beta \otimes \alpha \vdash \beta \wedge \alpha}.$$

(17) Observe que se T é um conjunto finito de tipos, então

$$x_T \in E((E\tau \vdash (\tau = \tau)), T) \cap E(((\tau = \tau) \vdash E\tau), T).$$

Portanto, temos

$$\frac{\frac{E\tau \vdash (\tau = \tau) \quad \Gamma, (\tau = \tau) \vdash (\tau = \tau)}{\Gamma, E\tau \vdash (\tau = \tau)} \quad (\tau = \tau) \vdash E\tau}{\Gamma, E\tau \vdash E\tau}.$$

(18) Segue imediatamente de (17) e [CH1.1] :

$$\frac{\frac{E_s\tau, E_t\kappa \vdash E_t\kappa}{E_s\tau \otimes E_t\kappa \vdash E_t\kappa} \quad E_s\tau \vdash E_s\tau \otimes E_t\kappa}{E_s\tau \vdash E_t\kappa}.$$

(19) Seja $C = C(\Gamma, \alpha, \beta)$ e $\alpha_C = \alpha \otimes \phi$. De [ES] vem

$$\frac{\frac{\frac{\Gamma, \phi, \alpha \vdash \alpha}{\Gamma, \alpha, \phi \vdash \alpha}}{\Gamma, \alpha_C \vdash \alpha} \quad \beta_C \vdash \beta \quad \alpha \vdash \alpha_C \quad \beta \vdash \beta_C}{\Gamma, \alpha_C, \beta_C \vdash \alpha \otimes \beta} \quad \frac{\Gamma, \alpha_C, \beta_C \vdash \alpha \otimes \beta}{\Gamma, \alpha \otimes \beta \vdash \alpha \otimes \beta}.$$

(20) Seja $C = C(\alpha_1, \dots, \alpha_n)$, $i = \sigma^{-1}(1)$, e $\beta = \alpha_{\sigma(1)} \otimes \dots \otimes (\alpha_{\sigma(i)})_C \otimes \dots \otimes \alpha_{\sigma(n)}$. De (15) e [ES] obtemos

$$\begin{array}{c} \vdots \\ \frac{\frac{\alpha_1, \dots, \alpha_n \vdash \alpha \quad \alpha \vdash \alpha_C \quad (\alpha_1)_C \vdash \alpha_1}{(\alpha_1)_C, \alpha_2, \dots, \alpha_n \vdash \alpha_C} \quad \top \vdash \top \quad \top \otimes \alpha_C \vdash \alpha_C \quad \alpha_C \vdash \alpha}{\top, (\alpha_1)_C, \alpha_2, \dots, \alpha_n \vdash \top \otimes \alpha_C} \\ \frac{\top, (\alpha_1)_C, \alpha_2, \dots, \alpha_n \vdash \top \otimes \alpha_C}{\top, (\alpha_1)_C, \alpha_2, \dots, \alpha_n \vdash \alpha} \\ \frac{\top, (\alpha_1)_C, \alpha_2, \dots, \alpha_n \vdash \alpha}{\top, \alpha_{\sigma(1)}, \dots, (\alpha_{\sigma(i)})_C, \dots, \alpha_{\sigma(n)} \vdash \alpha} \end{array}.$$

Desta maneira, por $[\otimes L]$ e (6), lembrando que $\beta \vdash \top \otimes \beta$ é demonstrável, obtemos:

$$\frac{\frac{\beta \vdash \top \otimes \beta \quad \top \otimes \beta \vdash \alpha}{\beta \vdash \alpha} \quad \alpha_{\sigma(i)} \vdash (\alpha_{\sigma(i)})_C}{\alpha_{\sigma(1)}, \dots, (\alpha_{\sigma(i)})_C, \dots, \alpha_{\sigma(n)} \vdash \alpha} \quad \frac{\alpha_{\sigma(1)}, \dots, (\alpha_{\sigma(i)})_C, \dots, \alpha_{\sigma(n)} \vdash \alpha}{\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)} \vdash \alpha}.$$

(21) Seja $C = C(\alpha, \beta)$. Então

$$\frac{\frac{\frac{\alpha_C \vdash \alpha \quad \beta \vdash \beta_C}{\alpha_C, \alpha \multimap \beta \vdash \beta_C} \quad \beta_C \vdash \beta}{\alpha_C, \alpha \multimap \beta \vdash \beta} \quad \alpha \vdash \alpha_C}{\alpha, \alpha \multimap \beta \vdash \beta}.$$

Agora, suponha que $\Gamma \vdash \alpha \multimap \beta$ é demonstrável e seja $D = C(\Gamma, \alpha, \beta)$. Se $\Gamma \neq \emptyset$, então, da mesma maneira que acima, obtemos o sequente $\alpha_D, \alpha \multimap \beta \vdash \beta$. Assim, podemos escrever

$$\begin{array}{c}
\vdots \\
\frac{\Gamma \vdash \alpha \multimap \beta \quad \alpha_D, \alpha \multimap \beta \vdash \beta}{\alpha_D, \Gamma \vdash \beta} \quad \alpha \vdash \alpha_D \\
\hline
\alpha, \Gamma \vdash \beta
\end{array}$$

Por outro lado, se $\Gamma = \emptyset$, então $D = C$ e $V_C(\alpha \multimap \beta) = \epsilon(C)$. Logo, por 2.6.1 (b), o sequente $\alpha_C \vdash V_C(\alpha \multimap \beta)$ é demonstrável; então (2) fornece o sequente $\alpha_C \vdash \alpha_C \otimes V_C(\alpha \multimap \beta)$. Assim, podemos escrever

$$\begin{array}{c}
\vdots \\
\frac{\vdash \alpha \multimap \beta \quad \alpha_C, \alpha \multimap \beta \vdash \beta}{\alpha_C, V_C(\alpha \multimap \beta) \vdash \beta} \quad \alpha_C \vdash \alpha_C \otimes V_C(\alpha \multimap \beta) \quad \alpha \vdash \alpha_C \\
\hline
\alpha_C \otimes V_C(\alpha \multimap \beta) \vdash \beta \\
\hline
\alpha_C \vdash \beta \\
\hline
\alpha \vdash \beta
\end{array}$$

Reciprocamente, se $\alpha, \Gamma \vdash \beta$ é demonstrável, então deduzimos $\Gamma \vdash \alpha \multimap \beta$ por $[\multimap R]$.

(22) Suponha que $\alpha, \beta \vdash$ é demonstrável e seja $C = C(\alpha, \beta)$. De $[WL]$ e $[ES]$ vem

$$\begin{array}{c}
\vdots \\
\frac{\alpha, \beta \vdash \quad \beta_C \vdash \beta}{\alpha, \beta_C \vdash} \quad \beta_C \vdash \beta_C \otimes \beta_C \quad \beta \vdash \beta_C \\
\hline
\beta_C, \alpha, \beta_C \vdash \\
\hline
\beta_C \otimes \beta_C, \alpha \vdash \\
\hline
\beta_C, \alpha \vdash \\
\hline
\beta, \alpha \vdash
\end{array}$$

Como $\alpha \vdash \alpha$ é demonstrável, $[\neg L]$ implica $\alpha, \neg \alpha \vdash$. Da prova acima, obtemos $\neg \alpha, \alpha \vdash$, e então, por $[\neg R]$, deduzimos $\alpha \vdash \neg \neg \alpha$ (em particular, $\neg \alpha \vdash \neg \neg \neg \alpha$). Dai, por $[\neg L]$ e $[\neg R]$, deduzimos $\alpha, \neg \neg \neg \alpha \vdash$ e $\neg \neg \neg \alpha \vdash \neg \alpha$.

(23) Suponha que o sequente $\Gamma \vdash \neg \alpha$ é demonstrável e seja $C = C(\Gamma, \alpha)$. Se $\Gamma \neq \emptyset$, então

$$\begin{array}{c}
\vdots \\
\frac{\Gamma \vdash \neg \alpha \quad \frac{\alpha_C \vdash \alpha}{\alpha_C, \neg \alpha \vdash}}{\alpha_C, \Gamma \vdash} \quad \alpha \vdash \alpha_C \\
\hline
\alpha, \Gamma \vdash
\end{array}$$

Se $\Gamma = \emptyset$, então $C = C(\alpha)$, $V_C(\neg \alpha) = \epsilon(C)$ e $\alpha \vdash V_C(\neg \alpha)$ é demonstrável, por 2.6.1(b). Portanto, por (2), $\alpha \vdash \alpha \otimes V_C(\neg \alpha)$ é demonstrável e podemos escrever

$$\begin{array}{c}
\vdots \\
\frac{\frac{\frac{\vdash \neg \alpha \quad \alpha, \neg \alpha \vdash}{\alpha, V_C(\neg \alpha) \vdash}}{\alpha \otimes V_C(\neg \alpha) \vdash}}{\alpha \vdash} \quad \alpha \vdash \alpha \otimes V_C(\neg \alpha)
\end{array}$$

Reciprocamente, por $[\neg R]$, de $\alpha \vdash$ obtemos $\vdash \neg \alpha$.

(24) Seja $C = C(\alpha, \beta)$. Então

$$\begin{array}{c}
\frac{\frac{\frac{\alpha_C \vdash \alpha}{\alpha_C \vdash \alpha \vee \beta}}{\alpha_C, \neg(\alpha \vee \beta) \vdash}}{\alpha, \neg(\alpha \vee \beta) \vdash} \quad \alpha \vdash \alpha_C \\
\hline
\neg(\alpha \vee \beta) \vdash \neg \alpha
\end{array}$$

Da mesma maneira, provamos o sequente $\neg(\alpha \vee \beta) \vdash \neg \beta$, terminando a prova aplicando $[\wedge R]$.

(25) Seja $C = C(\alpha, \beta)$. Então

$$\begin{array}{c}
\frac{\frac{\frac{\alpha \vdash \alpha_C}{\alpha \wedge \beta \vdash \alpha_C}}{\alpha \wedge \beta \vdash \alpha}}{\alpha \wedge \beta, \neg \alpha \vdash} \quad \alpha_C \vdash \alpha \\
\hline
\neg \alpha \vdash \neg(\alpha \wedge \beta)
\end{array}$$

Analogamente, provamos $\neg \beta \vdash \neg(\alpha \wedge \beta)$, e o resultado segue aplicando $[\vee L1]$

(26) Por (21), (6) e $[\neg \circ R]$ podemos escrever

$$\begin{array}{c}
\frac{\frac{\frac{\alpha, \alpha \neg \circ (\beta \neg \circ \gamma) \vdash \beta \neg \circ \gamma}{\beta, \alpha, \alpha \neg \circ (\beta \neg \circ \gamma) \vdash \gamma}}{\beta \otimes \alpha, \alpha \neg \circ (\beta \neg \circ \gamma) \vdash \gamma}}{\alpha \neg \circ (\beta \neg \circ \gamma) \vdash \beta \otimes \alpha \neg \circ \gamma} \\
\frac{\frac{\frac{\beta \otimes \alpha, \beta \otimes \alpha \neg \circ \gamma \vdash \gamma}{\beta, \alpha, \beta \otimes \alpha \neg \circ \gamma \vdash \gamma}}{\alpha, \beta \otimes \alpha \neg \circ \gamma \vdash \beta \neg \circ \gamma}}{\beta \otimes \alpha \neg \circ \gamma \vdash \alpha \neg \circ (\beta \neg \circ \gamma)} \quad . \quad \square
\end{array}$$

Corolário 2.6.5 : *Sejam ϕ uma fórmula, $x, y, z \in \mathcal{V}_t$ e τ termo do tipo t , livre para x em ϕ .*

(a) *Se y é livre para x em ϕ , $C \supseteq C(\phi[y/x] \otimes Ey)$ e z é uma variável livre para x em ϕ que não ocorre em C , então o sequente*

$$(\exists)(\phi[z/x])_{(z,C)} \vdash (\exists)(\phi[y/x])_C$$

é demonstrável. Portanto, se $\text{disj}(\phi) = \{\alpha_i \vee \beta_i : 1 \leq i \leq n\}$ e T_1^i denota o sequente T_1 da definição 2.3.15 (i) correspondente a $\alpha_i \vee \beta_i$ ($i = 1, \dots, n$), então todos os sequentes da justificativa

$$y_1 = \{T_1^i : 1 \leq i \leq n\} \in C_=(\phi, (y; x), C)$$

são demonstráveis para toda ϕ tal que y é livre para x .

(b) Se $x \in VAR(\phi)$ e todos os seqüentes de alguma justificativa de $C_E(\phi, (\tau; x), C(\phi[\tau/x]))$ são demonstráveis, então o seqüente

$$[S \exists] \quad \phi[\tau/x] \vdash (\exists x)\phi$$

é demonstrável. Em particular, o seqüente

$$\phi \vdash (\exists x)\phi$$

é demonstrável para toda ϕ tal que $x \in VAR(\phi)$.

(c) Se $x \in VAR(\phi)$ e todos os seqüentes de alguma justificativa de $C_D(\phi, (\tau; x), C(\phi[\tau/x]))$ são demonstráveis, então

$$[S \forall] \quad (\forall x)\phi \vdash \phi[\tau/x]$$

é demonstrável. Em particular, o seqüente

$$(\forall x)\phi \vdash \phi$$

é demonstrável para toda ϕ tal que $x \in VAR(\phi)$.

(d) Seja $\vec{a} = a_1, \dots, a_n$ uma seqüência finita de constantes diferentes que não ocorrem em ϕ e $E\vec{a} = Ea_1 \otimes \dots \otimes a_n$. Então,

$$(\exists)(\phi \otimes E\vec{a}) \sim ((\exists)\phi) \otimes E\vec{a}.$$

Demonstração: (a) Suponha que $x \notin VAR(\phi)$ e seja $C = (y, \vec{x}; \vec{a})$; logo, $\phi[z/x] = \phi = \phi[y/x]$. Portanto, por $[AX3]$, $[ES]$ e 2.6.4 (6), obtemos:

$$\frac{\frac{\phi_{(z,C)} \vdash \phi_C}{(\exists y)(\exists \vec{x})\phi_{(z,C)} \vdash (\exists)\phi_C}}{(\exists z)(\exists y)(\exists \vec{x})\phi_{(z,C)} \vdash (\exists)\phi_C}.$$

A primeira inferência sai de 2.6.3(f). A última aplicação de $[\exists L]$ é válida, pois, por 2.6.2, podemos provar todos os seqüentes de uma justificativa de $R((\exists)\phi_{(z,C)} \vdash (\exists)\phi_C, \text{tipos}(z))$. Se $x \in VAR(\phi)$, então, por $[ES]$ e 2.6.4 (6), obtemos que

$$((\phi[z/x])_{(z,C)})[y/z] \sim (\phi[y/x])_C \otimes Ey,$$

logo

$$\frac{((\phi[z/x])_{(z,C)})[y/z] \vdash (\phi[y/x])_C \otimes Ey \quad (\phi[y/x])_C \otimes Ey \vdash (\phi[y/x])_C[y/y]}{((\phi[z/x])_{(z,C)})[y/z] \vdash (\phi[y/x])_C[y/y]},$$

pois os tipos coincidem. Assim, aplicamos $[\exists R]$ em y e depois $[\exists L]$ em z , obtendo

$$(\exists z)(\phi[z/x])_{(z,C)} \vdash (\exists y)(\phi[y/x])_C$$

e então, aplicando $[\exists L]$ em y (por 2.6.2), deduzimos

$$(\exists y)(\exists z)(\phi[z/x])_{(z,C)} \vdash (\exists y)(\phi[y/x])_C.$$

Logo, aplicando 2.6.3 (f) nas outras variáveis, obtemos

$$(\exists)(\phi[z/x])_{(z,C)} \vdash (\exists)(\phi[y/x])_C.$$

Provaremos agora os seguintes T_1^i . Assim, se $\alpha \vee \beta \in SF(\phi)$ e $D = \mathbf{C}(\alpha \vee \beta, \phi, C)$, então, pela primeira parte, obtemos:

$$\frac{(\exists)(\alpha[\vec{y}/\vec{v}][z/x])_{(z,D)} \vdash (\exists)(\alpha[\vec{y}/\vec{v}][y/x])_D \quad [\vee R1]}{(\exists)(\alpha[\vec{y}/\vec{v}][z/x])_{(z,D)} \vdash (\exists)(\alpha[\vec{y}/\vec{v}][y/x])_D \vee (\exists)(\beta[\vec{y}/\vec{v}][y/x])_D},$$

e analogamente para β . Finalmente, por $[\vee L1]$,

$$(\exists)(\alpha[\vec{y}/\vec{v}][z/x])_{(z,D)} \vee (\exists)(\beta[\vec{y}/\vec{v}][z/x])_{(z,D)} \vdash (\exists)(\alpha[\vec{y}/\vec{v}][y/x])_D \vee (\exists)(\beta[\vec{y}/\vec{v}][y/x])_D.$$

Os itens (b), (c) são imediatos a partir das regras de quantificação e da hipótese:

$$\frac{\phi[\tau/x] \vdash \phi[\tau/x] \quad [\exists R]}{\phi[\tau/x] \vdash (\exists x)\phi}, \quad \frac{\phi[\tau/x] \vdash \phi[\tau/x] \quad [\forall L]}{(\forall x)\phi \vdash \phi[\tau/x]}.$$

(d) A proposição 2.6.3(f) fornece

$$\frac{\frac{\phi \vdash \phi \otimes E\vec{a}}{(\exists)\phi \vdash (\exists)(\phi \otimes E\vec{a})} \quad (\exists)\phi, E\vec{a} \vdash (\exists)\phi}{(\exists)\phi, E\vec{a} \vdash (\exists)(\phi \otimes E\vec{a})}.$$

Por outro lado, pela proposição 2.6.4(17) e (19), temos que o sequente $\Gamma, E\vec{a} \vdash E\vec{a}$ é demonstrável para todo Γ . Então, podemos escrever

$$\frac{\phi, E\vec{a} \vdash E\vec{a}}{\phi \otimes E\vec{a} \vdash E\vec{a}}, \quad \frac{\phi \otimes E\vec{a} \vdash E\vec{a}}{(\exists)(\phi \otimes E\vec{a}) \vdash E\vec{a}}$$

onde as aplicações de $[\exists L]$ são válidas, pelo corolário 2.6.2 e pelo fato de termos $x_\top \in K_E(E\vec{a}, C, T)$ para todo T, C . Por outro lado, da proposição 2.6.3(f) vem

$$\frac{\frac{\phi \otimes E\vec{a} \vdash \phi}{(\exists)(\phi \otimes E\vec{a}) \vdash (\exists)\phi} \quad (\exists)(\phi \otimes E\vec{a}) \vdash E\vec{a}}{(\exists)(\phi \otimes E\vec{a}) \vdash ((\exists)\phi) \wedge E\vec{a}} \quad ((\exists)\phi) \wedge E\vec{a} \vdash ((\exists)\phi) \otimes E\vec{a}$$

encerrando a prova. $\square$

2.7 O Cálculo (QPC1) para Extents Constantes

Nesta seção discutiremos um caso particular importante do cálculo (QPC), que consiste em assumir o axioma $(\exists x)E_s x \vdash (\exists y)E_t y$ para todos os tipos s, t da linguagem. Isto implica que, nos

modelos de prefeixes ou feixes, todos os tipos têm o mesmo extent p , donde $\llbracket V_C(\phi) \rrbracket = p$ para todo C, ϕ . O cálculo resultante, indicado por (QPC1), será aplicado para provar o teorema de Kaplansky em $Sh(Q)$ no último capítulo. O resultado principal que obtemos a partir da hipótese de igualdade dos extents é a

Proposição 2.7.1 : *Suponha que os axiomas $(\exists v_0^s)E_s v_0^s \vdash (\exists v_0^t)E_t v_0^t$, $s, t \in TIPOS$, sejam adicionados à (QPC). Sejam $\phi, \beta_1, \dots, \beta_k$ fórmulas, T um conjunto finito de tipos e C um contexto. Então:*

(1) *Todos os seqüentes da justificativa de $ED(\phi, C, T)$ são demonstráveis em (QPC) para todo $C \supseteq C(\phi)$.*

(2) *O seqüente*

$$(\exists)(\beta_1 \otimes \dots \otimes \beta_k)_C \vdash ((\exists)(\beta_1)_C \wedge \epsilon(T)) \otimes \dots \otimes ((\exists)(\beta_k)_C \wedge \epsilon(T))$$

é demonstrável em (QPC) para todo $C \supseteq C(\beta_1, \dots, \beta_k)$.

(3) *Para todo seqüente S , existem justificativas $x \in E(S, T)$ e $y \in R(S, T)$ tal que todos os seqüentes em x e y são demonstráveis em (QPC)*

Demonstração: (1) Seja $C = (\vec{x}; \vec{a})$. Então, $V_a((\exists)\phi_C) = V_C(\phi_C)$ e os axiomas implicam que $\epsilon(C) \sim \epsilon(T)$. Portanto,

$$\frac{\frac{(\exists)\phi_C \vdash V_C(\phi_C) \quad V_C(\phi_C) \vdash \epsilon(C)}{(\exists)\phi_C \vdash \epsilon(C)} \quad \epsilon(C) \vdash \epsilon(T)}{(\exists)\phi_C \vdash \epsilon(T)}.$$

A prova acima vale para toda $\phi, C \supseteq C(\phi)$ e T finito, donde segue-se o resultado.

(2) Definimos a seguinte notação :

$$\begin{aligned} \prod \beta_i)_C &\equiv_{def} (\beta_1 \otimes \dots \otimes \beta_k)_C, & \prod (\beta_i)_C &\equiv_{def} (\beta_1)_C \otimes \dots \otimes (\beta_k)_C, \\ \prod (\exists)(\beta_i)_C &\equiv_{def} (\exists)(\beta_1)_C \otimes \dots \otimes (\exists)(\beta_k)_C, \\ \prod ((\exists)(\beta_i)_C \wedge \epsilon(T)) &\equiv_{def} ((\exists)(\beta_1)_C \wedge \epsilon(T)) \otimes \dots \otimes ((\exists)(\beta_k)_C \wedge \epsilon(T)). \end{aligned}$$

Assim, fixado $1 \leq i \leq k$, obtemos, pelos lemas 2.6.3(f) e 2.6.3(g),

$$\frac{\frac{(\prod \beta_i)_C \vdash \prod (\beta_i)_C}{(\exists)(\prod \beta_i)_C \vdash (\exists) \prod (\beta_i)_C} \quad (\exists) \prod (\beta_i)_C \vdash \prod (\exists)(\beta_i)_C}{(*) \quad (\exists)(\prod \beta_i)_C \vdash \prod (\exists)(\beta_i)_C}.$$

Por outro lado, pelo item (1), obtemos

$$\frac{(\exists)(\beta_i)_C \vdash (\exists)(\beta_i)_C \quad (\exists)(\beta_i)_C \vdash \epsilon(T)}{(\exists)(\beta_i)_C \vdash (\exists)(\beta_i)_C \wedge \epsilon(T)}$$

para todo i . Portanto, por $[\otimes R]$ e $[\otimes L]$, deduzimos

$$(**) \quad \prod (\exists)(\beta_i)_C \vdash \prod ((\exists)(\beta_i)_C \wedge \epsilon(T)).$$

Assim, por $[CUT]$ aplicado a $(*)$ e $(**)$, temos

$$(\exists)(\prod \beta_i)_C \vdash \prod ((\exists)(\beta_i)_C \wedge \epsilon(T)).$$

(3) Seja $S : \Gamma \vdash \Delta$ um sequente, e T um conjunto finito de tipos. Pelo item (1), temos que existe uma cláusula em $E(S, T)$ tal que todos os sequentes de x são demonstráveis. Por outro lado, (2) assegura que, se $\text{red}(\Gamma) = \beta_1, \dots, \beta_k$, então o sequente S_Γ da definição 2.3.10 é demonstrável. Se $\Gamma = \emptyset$, está claro que os axiomas implicam que o sequente $\epsilon(C) \vdash \epsilon(T)$ é demonstrável. $\square$

A partir deste resultado, vemos que as justificativas nas cláusulas da forma $E(S, T)$, $R(S, T)$ ou $K_E((\exists)\phi, C, T)$ podem ser eliminadas, pois elas são sempre satisfeitas nas hipóteses atuais. Porém, devemos observar que o sequente S na cláusula de $[\forall L2]$ não pode ser omitido pois, como vimos no exemplo 2.4.3, ele nem sempre é válido, mesmo quando temos um só tipo. Da mesma maneira, os sequentes das cláusulas $C_D(\phi, (\vec{\tau}; \vec{x}), C)$ ou $C_E(\phi, (\vec{\tau}, \vec{x}), C)$ no axioma $[SUBS]$ e nas regras de quantificação devem permanecer, pois a sua interpretação envolve a imagem inversa de morfismos (diferentes em geral da projeção), que têm um comportamento imprevisível. Podemos então dar a

Definição 2.7.2 : *O cálculo (QPC1) é definido a partir de (QPC), introduzindo os axiomas da forma $(\exists v_0^t)E_t v_0^t \vdash (\exists v_0^s)E_s v_0^s$ para todos os tipos s, t , eliminando as cláusulas nas regras dos conectivos (com exceção de $[\forall L2]$), nas regras estruturais e nas regras $[\forall R]$ e $[\exists L]$. Por outro lado, mantemos as seguintes cláusulas:*

$$\text{clau}([\forall L]) = C_D(\phi, (\tau; x), C) \quad \text{se } \tau \notin \mathcal{V};$$

$$\text{clau}([\exists R]) = C_E(\phi, (\tau; x), C) \quad \text{se } \tau \notin \mathcal{V};$$

$$\text{clau}([\forall L2]) = \{\{S\}\}$$

(assumindo em cada caso a notação da definição 2.4.1). A cláusula do axioma $[SUBS]$ permanece inalterada. A noção de prova em (QPC1) é a mesma que em (QPC) (definição 2.5.1).

A partir da proposição 2.7.1 e o teorema 2.5.2, obtemos o

Teorema 2.7.3 : *(Corretude de (QPC1)) Seja S um sequente, e L um conjunto de sequentes. Suponha que S é demonstrável em (QPC1) a partir de L . Se $\mathcal{I}$ é uma interpretação satisfazendo os sequentes de L e tal que todos os tipos em $\mathcal{I}$ têm extents iguais, então S é válido em $\mathcal{I}$.*

Estruturas Algébricas em $\text{Psh}(\mathbf{Q})$

Neste capítulo estudaremos algumas aplicações do cálculo (QPC) e do teorema 2.5.2. Na primeira seção estudaremos relações binárias, mostrando que os axiomas standard sobre ordens parciais e relações de equivalência (entre outros) funcionam no contexto de quantais. Na segunda seção, discutiremos a axiomatização de algumas estruturas algébricas; em particular, veremos que, como acontece com feixes sobre $\mathbf{cHa}$, a noção de corpo não tem uma axiomatização única em feixes sobre quantais. Finalmente, definiremos os números naturais em $\text{Sh}(\mathbf{Q})$, a partir dos quais poderemos definir os inteiros e os racionais. O feixe dos números naturais satisfaz um princípio de indução que permitirá realizar provas por indução em (QPC) e ($QPC1$).

3.1 Relações Binárias

Proposição 3.1.1 : *Seja A um prefeixe, h_R a interpretação de um predicado $\langle R, 2, t, t \rangle$ e $|R|$ o domínio do sub-prefeixe fechado de $A \times A$ associado com h_R por uma interpretação $\mathcal{I}$. Considere os axiomas :*

- [sim] $\vdash \forall w \forall v (R(w, v) \multimap R(v, w))$
- [ref] $\vdash \forall w R(w, w)$
- [anti] $\vdash \forall w \forall v (R(w, v) \wedge R(v, w) \multimap (w = v))$
- [tran] $\vdash \forall w \forall v \forall u (R(w, v) \wedge R(v, u) \multimap R(w, u))$
- [asim] $\vdash \forall w \forall v (R(w, v) \multimap \neg R(v, w))$

Então:

- (i) $\mathcal{I} \models [\text{sim}]$ sse para todo $a, b \in |A|$, $(a, b) \in |R|$ implica $(b, a) \in |R|$;
- (ii) $\mathcal{I} \models [\text{ref}]$ sse para todo $a \in |A|$, $(a, a) \in |R|$;
- (iii) $\mathcal{I} \models [\text{anti}]$ sse para todo $a, b \in |A|$, $(a, b) \in |R|$ e $(b, a) \in |R|$ implica $a = b$;
- (iv) $\mathcal{I} \models [\text{tran}]$ sse para todo $a, b, c \in |A|$, $(a, b) \in |R|$ e $(b, c) \in |R|$ implica $(a, c) \in |R|$;
- (v) $\mathcal{I} \models [\text{asim}]$ sse para todo $a, b \in |A|$, $(a, b) \in |R|$ e $(b, a) \in |R|$ implica então $a = * = b$,

onde $*$ representa a única seção sobre $\mathbf{0}$ de A .

Demonstração: (i) $\mathcal{I} \models [sim]$ sse

$$\llbracket \forall w \forall v (R(w, v) \multimap R(v, w)) \rrbracket = EA$$

sse

$$EA \leq \bigwedge_{a \in |A|} (Ea \rightarrow_l \llbracket \forall v (R(w, v) \multimap R(v, w)) \rrbracket_w(a))$$

sse para todo $a \in |A|$

$$EA \& Ea \leq \llbracket \forall v (R(w, v) \multimap R(v, w)) \rrbracket_w(a)$$

sse para todo $a \in |A|$

$$EA \& Ea \leq \bigwedge_{b \in |A|} (Eb \rightarrow_l \llbracket (R(w, v) \multimap R(v, w)) \rrbracket_{(w,v)}(a, b))$$

sse para todo a, b

$$EA \& Ea \& Eb \leq \llbracket (R(w, v) \multimap R(v, w)) \rrbracket_{(w,v)}(a, b)$$

sse para todo a, b

$$EA \& Ea \& Eb \leq h_R(a, b) \rightarrow h_R(b, a)$$

sse para todo a, b , $h_R(a, b) \leq h_R(b, a)$, pois $Ch(A, 2)$ é um right-quantal RSI. Assim

$$\mathcal{I} \models [sim] \text{ sse } h_R(a, b) = h_R(b, a), \forall a, b \in |A|.$$

Se $h_R(a, b) = h_R(b, a)$ para todo a, b e $(a, b) \in |R|$, então,

$$Ea = Eb \leq h_R(a, b) = h_R(b, a)$$

de onde $(b, a) \in |R|$.

Reciprocamente, suponha que $|R|$ satisfaz:

$$\text{para todo } a, b \in |A|, \text{ se } (a, b) \in |R| \text{ então } (b, a) \in |R|,$$

e sejam $(a, b) \in |A| \times |A|$ e $p = h_R(a, b) \leq EA$; então,

$$\begin{aligned} E(a|_p) &= h_R(a, b) \& Ea = h_R(a, b) = h_R(a, b) \& Eb = E(b|_p) \\ &= h_R(a, b) \& p = h_R(a|_p, b|_p) \end{aligned}$$

mostrando que $(a|_p, b|_p) \in |R|$. Portanto, $(b|_p, a|_p) \in |R|$ e então

$$h_R(a, b) = E(b|_p) = E(a|_p) \leq h_R(b|_p, a|_p) = h_R(b, a) \& p \leq h_R(b, a)$$

provando que $[sim]$ é válido em $\mathcal{I}$.

(ii) $\mathcal{I} \models [ref]$ sse para todo $a \in |A|$,

$$(1) \quad EA \& Ea \leq h_R(a, a) .$$

Se $\mathcal{I}$ é modelo de $[ref]$ e $a \in |A|$, (1) implica

$$Ea \leq EA \& Ea \leq h_R(a, a),$$

de onde $(a, a) \in |R|$. Reciprocamente, seja $\mathcal{I}$ uma interpretação tal que $(a, a) \in |R|$ para todo $a \in |A|$. Então,

$$Ea \leq h_R(a, a) \leq Eh_R$$

para todo $a \in |A|$, de onde

$$EA = \bigvee_{a \in |A|} Ea \leq Eh_R,$$

e portanto

$$EA \& Ea \leq EA \& h_R(a, a) \leq Eh_R \& h_R(a, a) = h_R(a, a),$$

i.e., $[ref]$ é válido em $\mathcal{I}$.

(iii) $\mathcal{I} \models [anti]$ sse para todo $a, b \in |A|$,

$$EA \& Ea \& Eb \leq (h_R(a, b) \wedge h_R(b, a)) \rightarrow (EA \& [a = b])$$

sse, para todo $a, b \in |A|$,

$$(2) \quad h_R(a, b) \wedge h_R(b, a) \leq EA \& [a = b].$$

Seja $\mathcal{I}$ um modelo de $[anti]$ e sejam $a, b \in |A|$ tais que $(a, b), (b, a) \in |R|$. Então,

$$Ea = Eb \leq h_R(a, b) \quad \text{e} \quad Eb = Ea \leq h_R(b, a)$$

portanto, por (2),

$$Ea = Eb \leq h_R(a, b) \wedge h_R(b, a) \leq EA \& [a = b].$$

Multiplicando a última relação à esquerda por Ea , temos

$$Ea = Ea \& Ea \leq Ea \& (EA \& [a = b]) = Ea \& [a = b] = [a = b] \leq Ea,$$

i.e., $Ea = Eb = [a = b]$ e $[EXT]$ acarreta $a = b$.

Reciprocamente, seja $\mathcal{I}$ uma interpretação tal que, para todo $a, b \in A$,

$$(a, b) \in |R| \quad \text{e} \quad (b, a) \in |R| \quad \text{implica} \quad a = b.$$

Sejam $(a, b) \in |A| \times |A|$ e $p = h_R(a, b) \wedge h_R(b, a) \leq EA$. Então,

$$(a_{|p}, b_{|p}) \in |R| \quad \text{e} \quad (b_{|p}, a_{|p}) \in |R|$$

o que garante $a_{|p} = b_{|p}$; portanto

$$p = E(a_{|p}) = [a_{|p} = b_{|p}] = p \& [a = b] \& p \leq EA \& [a = b]$$

o que prova (2) e que $[anti]$ é válida em $\mathcal{I}$.

(iv) $\mathcal{I} \models [tran]$ sse para todo $a, b, c \in |A|$,

$$EA \& Ea \& Eb \& Ec \leq (h_R(a, b) \& Ec \wedge h_R(b, c) \& Ea) \rightarrow h_R(a, c) \& Eb$$

sse para todo $a, b, c \in |A|$

$$(3) \quad h_R(a, b) \& Ec \wedge h_R(b, c) \& Ea \leq h_R(a, c).$$

Seja $\mathcal{I}$ um modelo de $[tran]$ e sejam $(a, b) \in |R|$, $(b, c) \in |R|$. Então,

$$Ea = Eb = Ec \leq h_R(a, b) \& Ec \text{ e } Ea = Eb = Ec \leq h_R(b, c) \& Ea,$$

de onde, por (3), concluimos

$$Ea = Ec \leq h_R(a, b) \& Ec \wedge h_R(b, c) \& Ea \leq h_R(a, c),$$

i.e., $(a, c) \in |R|$.

Reciprocamente, seja $\mathcal{I}$ uma estrutura satisfazendo, para todo $a, b, c \in |A|$,

$$(a, b) \in |R| \text{ e } (b, c) \in |R| \text{ implica } (a, c) \in |R|.$$

Sejam $a, b, c \in |A|$ e $p = h_R(a, b) \& Ec \wedge h_R(b, c) \& Ea \leq EA$; temos que

$$E(a|_p) = p \& Ea = p = p \& Eb = E(b|_p) \leq h_R(a, b) \& p = h_R(a|_p, b|_p),$$

de onde $(a|_p, b|_p) \in |R|$. Analogamente $(b|_p, c|_p) \in |R|$; assim $(a|_p, c|_p) \in |R|$ e então

$$p = E(a|_p) = E(c|_p) \leq h_R(a|_p, c|_p) = h_R(a, c) \& p \leq h_R(a, c)$$

o que prova (3) e que $\mathcal{I}$ é um modelo de $[tran]$.

(v) $\mathcal{I} \models [asim]$ sse para todo $a, b \in |A|$,

$$EA \& Ea \& Eb \leq h_R(a, b) \rightarrow (h_R(b, a) \rightarrow \mathbf{0})$$

sse para todo a, b

$$h_R(a, b) \leq h_R(b, a) \rightarrow \mathbf{0}$$

sse para todo a, b

$$(4) \quad h_R(b, a) \& h_R(a, b) = \mathbf{0}.$$

Seja $\mathcal{I}$ um modelo de $[asim]$ e $(a, b) \in |R|$; então

$$Ea = Eb \leq h_R(a, b)$$

que multiplicada à esquerda por $h_R(b, a)$, fornece

$$h_R(b, a) = h_R(b, a) \& Ea \leq h_R(b, a) \& h_R(a, b) = \mathbf{0},$$

de onde $h_R(b, a) = 0$. Assim, se $(b, a) \in |R|$, então

$$Ea = Eb \leq h_R(b, a) = 0$$

e portanto $a = * = b$.

Reciprocamente, seja $\mathcal{I}$ uma estrutura tal que

$$(a, b) \in |R| \text{ e } (b, a) \in |R| \text{ implica } a = * = b.$$

Sejam $a, b \in |A|$ e $p = h_R(a, b) \wedge h_R(b, a) = h_R(b, a) \& h_R(a, b) \leq EA$. Como

$$(a|_p, b|_p) \in |R| \text{ e } (b|_p, a|_p) \in |R|,$$

então $a|_p = * = b|_p$, de onde

$$h_R(b, a) \& h_R(a, b) = p = p \& Ea = E(a|_p) = 0$$

provando (4) e que $\mathcal{I}$ é modelo de $[asim]$. $\square$

Podemos observar que a caracterização axiomática de relação de equivalência corresponde à definição encontrada em [MS] (pags. 18 e 72). De fato, se h é a função característica associada numa interpretação dada com um predicado satisfazendo os axiomas $[ref]$, $[sim]$, $[tran]$, então $Eh = EA$ (por $[ref]$) e portanto

$$(EA \& Ex \& Ey) \& h(x, y) = Eh \& h(x, y) \& Ex \& Ey = h(x, y),$$

mostrando que h é uma função característica two-sided, definindo em consequência um sub-prefeixe 2-fechado (Proposição 1.1.32(b)). Por outro lado, temos o seguinte:

Definição 3.1.2 (MS) : *Seja A um Q -set. Uma relação de equivalência em A é uma função 2-característica $\theta : |A| \times |A| \rightarrow Q$ satisfazendo para todo $x, y, z \in |A|$:*

$$[eqr\ 1] \quad [x = y] \leq \theta(x, y);$$

$$[eqr\ 2] \quad \top \& \theta(x, y) = \top \& \theta(y, x);$$

$$[eqr\ 3] \quad \theta(x, y) \& \theta(y, z) \leq \theta(x, z).$$

Se θ é uma equivalência em A , temos que

$$\hat{x\theta y} \text{ sse } Ex = Ey = \theta(x, y)$$

é uma relação de equivalência em $|A|$, que permite definir o Q -set extensional

$$|A/\theta| = \{x/\theta : x \in |A|\}, \quad [x/\theta = y/\theta] = \theta(x, y),$$

onde x/θ denota a classe de equivalência de $x \in |A|$. Se A é um prefeixe, então A/θ é um prefeixe com a restrição dada por $(x/\theta)|_p = (x|_p)/\theta$ para todo $p \leq EA = EA/\theta$.

Dada uma função 2-característica $\theta : |A| \times |A| \rightarrow Q$, então θ é uma relação de equivalência se e somente se a função característica associada $h(x, y) = EA \& \theta(x, y)$ satisfaz, para todo $x, y, z \in |A|$:

$$EA \& [x = y] \leq h(x, y); \quad h(x, y) = h(y, x); \quad h(x, y) \& h(y, z) \leq h(x, z).$$

Proposição 3.1.3 : *Seja θ uma relação de equivalência num prefeixe A . Então, a função característica associada a θ , $h(x, y) = EA\&\theta(x, y)$, satisfaz os axiomas $[ref]$, $[sim]$ e $[tran]$ da proposição 3.1.1. Reciprocamente, se h é uma função característica satisfazendo $[ref]$, $[sim]$ e $[tran]$, então a função 2-característica associada $\theta(x, y) = Ex\&Ey\&h(x, y)$ é uma relação de equivalência.*

Demonstração: Seja θ uma relação de equivalência e $h(x, y) = Ex\&Ey\&\theta(x, y)$ a função característica associada. Pela definição 3.1.2, temos $EA\&Ex \leq h(x, x)$ para todo $x \in |A|$. A prova da proposição 3.1.1 mostra que h satisfaz $[ref]$. Por outro lado, para todo $x, y \in |A|$, temos que $h(x, y) = h(y, x)$, donde h satisfaz $[sim]$, pela prova de 3.1.1. Finalmente, para todo $x, y, z \in |A|$, temos que

$$h(x, y)\&Ez \wedge h(y, z)\&Ex = h(x, y)\&h(y, z) \leq h(x, z),$$

e h satisfaz $[tran]$, pela prova de 3.1.1.

Reciprocamente, se h é uma função característica two-sided satisfazendo $[ref]$, $[sim]$, $[tran]$, então h satisfaz

$$EA\&Ex \leq h(x, x); \quad h(x, y) = h(y, x); \quad h(x, y)\&h(y, z) \leq h(x, z)$$

para todo $x, y, z \in |A|$. Logo, para todo $x, y \in |A|$, obtemos

$$EA\&[x = y] = EA\&Ey\&[y = x]\&[y = y] \leq h(y, y)\&[y = x]\&[y = y] \leq h(x, y). \quad \square$$

Mostraremos agora que os axiomas usuais caracterizam, em $Sh(Q)$, a noção de relação funcional.

Definição 3.1.4 : (i) *Sejam A e B feixes e $f : A \longrightarrow B$ um morfismo. O gráfico de f é o sub-feixe*

$$G_f = \{(a, b) \in A \times B : b = f(a)\}.$$

(ii) *Sejam A e B feixes, com $EA \leq EB$ e $R \subseteq A \times B$ um sub-feixe. Dizemos que R é uma relação funcional se R é o gráfico de um único morfismo $f : A \longrightarrow B$, i.e.,*

$$(a, b) \in |R| \text{ sse } f(a) = b.$$

Proposição 3.1.5 : *Seja $\langle R, 2, s, t \rangle$ um símbolo de predicado, e considere os axiomas seguintes:*

$$[RF1] \quad \vdash (\forall x)(\exists y)R(x, y);$$

$$[RF2] \quad \vdash (\forall x)(\forall y)(\forall z)(R(x, y) \wedge R(x, z) \multimap (y = z)).$$

Então, uma interpretação de feixes $\mathcal{I}$ tal que $EA_s \leq EA_t$ satisfaz $[RF1]$, $[RF2]$ sse o sub-feixe $|R| \subseteq |A_s \times A_t|$ associado com h_R é uma relação funcional.

Demonstração: Seja $\mathcal{I}$ uma interpretação de feixes, com $A = A_s$, $B = A_t$, $EA \leq EB$; então, $\mathcal{I} \models [RF1]$ se e somente se para todo $a \in |A|$,

$$(1) \quad E(a|_{EA}) = EA\&Ea = \bigvee_{b \in |B|} h_R(a, b).$$

Por outro lado, $\mathcal{I} \models [RF2]$ sse para todo $a \in |A|$ e $b, c \in |B|$,

$$EA \& Ea \& Eb \& Ec \leq (h_R(a, b) \& Ec \wedge h_R(a, c) \& Eb) \rightarrow (EA \& [b = c] \& Ea)$$

se e somente se

$$h_R(a, b) \& Ec \wedge h_R(a, c) \& Eb \leq EA \& [b = c]$$

se e somente se

$$(2) \quad \text{se } (a, b) \in |R| \text{ e } (a, c) \in |R| \text{ então } b = c.$$

Com efeito, suponha que $\mathcal{I} \models [RF2]$ e sejam $(a, b), (a, c) \in |R|$; então, $Ea = Eb \leq h_R(a, b)$, $Ea = Ec \leq h_R(a, c)$ e temos

$$Eb = Ec \leq h_R(a, b) \& Ec \wedge h_R(a, c) \& Eb \leq EA \& [b = c].$$

Multiplicando à esquerda por $Eb = Ea \leq EA$, obtemos

$$Eb = Ec \leq Eb \& EA \& [b = c] = Eb \& [b = c] = [b = c] \leq Eb$$

e extensionalidade garante que $b = c$. Reciprocamente, se (2) é verdadeira em $\mathcal{I}$, sejam $a \in |A|$, $b, c \in |B|$ e $p = h_R(a, b) \& Ec \wedge h_R(a, c) \& Eb$; então

$$E(a|_p) = E(b|_p) = p \leq h_R(a, b) \& p = h_R(a|_p, b|_p)$$

nos dá $(a|_p, b|_p) \in |R|$; analogamente, provamos $(a|_p, c|_p) \in |R|$. Por (2), $b|_p = c|_p$ e então

$$E(b|_p) = E(c|_p) = p = [b|_p = c|_p] = p \& [b = c] \leq EA \& [b = c]$$

mostrando que $\mathcal{I} \models [RF2]$.

Suponha agora que $\mathcal{I}$ satisfaz $[RF1]$, $[RF2]$. Para $a \in |A|$ fixado, seja $\tilde{a} = a|_{EA}$ e considere o conjunto $\mathcal{S} = \{b|_{h_R(a, b)} : b \in |B|\} \subseteq |B|$. Note que se $s = b|_{h_R(a, b)} \in \mathcal{S}$, então $Es = h_R(a, b)$. Provaremos que o conjunto de seções $\mathcal{S}$ é compatível. Sejam então $s = b|_{h_R(a, b)}$ e $s' = b'|_{h_R(a, b')}$ em $\mathcal{S}$. Então

$$s|_{Es \& Es'} = (b|_{h_R(a, b)})|_{h_R(a, b) \& h_R(a, b')} = b|_{h_R(a, b) \& h_R(a, b')}$$

enquanto que

$$s'|_{Es \& Es'} = (b'|_{h_R(a, b')})|_{h_R(a, b) \& h_R(a, b')} = b'|_{h_R(a, b) \& h_R(a, b')}.$$

Considere agora

$$x = (a|_{h_R(a, b) \& h_R(a, b')}, b|_{h_R(a, b) \& h_R(a, b')}), \quad y = (a|_{h_R(a, b) \& h_R(a, b')}, b'|_{h_R(a, b) \& h_R(a, b')}).$$

Lembrando que, para toda função característica h , vale a relação $h(\vec{x}) \& h(\vec{y}) = h(\vec{x}) \wedge h(\vec{y}) = h(\vec{y}) \& h(\vec{x})$, temos que $x, y \in |R|$. Assim, por (2),

$$b|_{h_R(a, b) \& h_R(a, b')} = b'|_{h_R(a, b) \& h_R(a, b')},$$

isto é, $s_{|Es \& Es'} = s'_{|Es \& Es'}$ e assim $\mathcal{S}$ é de fato compatível. Como B é um feixe, existe $\tilde{b} \in |B|$ tal que

$$E\tilde{b} = \bigvee_{b \in |B|} h_R(a, b) = E\tilde{a}, \quad \tilde{b}_{|h_R(a, b)} = b_{|h_R(a, b)} \quad \text{para todo } b \in |B|.$$

Mas então $(\tilde{a}, \tilde{b}) \in |R|$; de fato,

$$\begin{aligned} E\tilde{a} &= E\tilde{b} = \bigvee_{b \in |B|} h_R(a, b) = \bigvee_{b \in |B|} h_R(\tilde{a}, b_{|h_R(a, b)}) \\ &= \bigvee_{b \in |B|} h_R(\tilde{a}, \tilde{b}_{|h_R(a, b)}) = h_R(\tilde{a}, \tilde{b}_{|q}) = h_R(\tilde{a}, \tilde{b}) \end{aligned}$$

onde $q = \bigvee_{b \in |B|} h_R(a, b) = E\tilde{b}$, pela proposição 1.1.31(c). Observe que, por (1), tomando supremo sobre $a \in |A|$, temos que $E|R| = EA$. Assim, $Ea \leq E|R|$ e então

$$(a, \tilde{b}_{|Ea}) = (\tilde{a}, \tilde{b})_{|Ea} \in |R|.$$

Acabamos de definir uma aplicação $f : A \longrightarrow B$, $a \mapsto \tilde{b}_{|Ea}$ (f é função, pois $\tilde{b}$ é único). Vamos provar que f é um morfismo. Dado $a \in |A|$, então

$$Ea = Ea \& (EA \& Ea) = E(\tilde{b}_{|Ea}) = Ef(a).$$

Sejam $a, a' \in |A|$ e considere a função característica

$$h : |B| \times |B| \longrightarrow Q, \quad h(x, y) = EA \& [x = y]$$

(h satisfaz $[char1]$, pois $EA \leq EB$). Seja $\tilde{a} = a_{|EA}$ e $\tilde{b} \in |B|$ tal que $\tilde{b}_{|Ea} = f(a)$. Logo,

$$h_R(\tilde{a}, \tilde{b}) = EA \& Ea = h_R(a, \tilde{b}) = \bigvee_{b \in |B|} h_R(a, b) = E\tilde{b}.$$

Considere $\tilde{c}$ tal que $f(a') = \tilde{c}_{|Ea'}$ e $\tilde{a}' = a'_{|EA}$. A proposição 1.1.31(c) e a construção de $\tilde{b}$, fornecem

$$\begin{aligned} [\tilde{b} = \tilde{c}] &= E\tilde{b} \& [\tilde{b} = \tilde{c}] = EA \& E\tilde{b} \& [\tilde{b} = \tilde{c}] = EA \& [\tilde{b} = \tilde{c}] \\ &= h(\tilde{b}, \tilde{c}) = h(\tilde{b}_{|E\tilde{b}}, \tilde{c}) = h(\tilde{b}_{|h_R(a, \tilde{b})}, \tilde{c}) = \bigvee_b h(\tilde{b}_{|h_R(a, b)}, \tilde{c}) \\ &= \bigvee_b h(b_{|h_R(a, b)}, \tilde{c}) \geq h(\tilde{c}_{|h_R(a, \tilde{c})}, \tilde{c}) = EA \& h_R(a, \tilde{c}) \& [\tilde{c} = \tilde{c}] = h_R(a, \tilde{c}) \end{aligned}$$

pois $EA = E|R|$. Assim, dado que $h_R(x, y) \& h_R(x', y') \leq h_R(x', y')$ para todo x, x', y, y' , temos

$$\begin{aligned} [\tilde{a} = \tilde{a}'] &= EA \& Ea \& [a = a'] \& EA \& Ea' = h_R(a, \tilde{b}) \& [a = a'] \& h_R(a', \tilde{c}) \\ &= h_R(a, \tilde{b}) \& h_R(a', \tilde{c}) \& [a' = a] \leq h_R(a', \tilde{c}) \& [a' = a] \leq h_R(a, \tilde{c}) \leq [\tilde{b} = \tilde{c}]. \end{aligned}$$

Multiplicando à esquerda por Ea e à direita por Ea' , obtemos

$$[a = a'] = Ea \& [\tilde{a} = \tilde{a}'] \& Ea' \leq Ea \& [\tilde{b} = \tilde{c}] \& Ea' = [\tilde{b}_{|Ea} = \tilde{c}_{|Ea'}] = [f(a) = f(a')],$$

mostrando que f é um morfismo tal que $|R| = G_f$. Reciprocamente, suponha que $\mathcal{I}$ é uma interpretação tal que para algum morfismo $f : A \longrightarrow B$, temos que $|R| = G_f$. Então

$$|R| = \{(a, fa) : a \in |A|\}$$

mostrando que $E|R| = EA$. Seja $a \in |A|$; como $(a, fa) \in |R|$, teremos

$$EA \& Ea \leq EA \& h_R(a, fa) = E|R| \& h_R(a, fa) = h_R(a, fa) \leq \bigvee_b h_R(a, b) \leq EA \& Ea$$

provando (1) e que $\mathcal{I} \models [RF1]$. Por outro lado, a condição (2) é claramente verdadeira e portanto $\mathcal{I} \models [RF2]$. $\square$

3.2 Estruturas Algébricas em $Psh(Q)$

Estudaremos agora alguns conceitos algébricos básicos na linguagem de (QPC) , definindo estruturas tais como anel e módulo em $Psh(Q)$. Discutiremos também a noção de corpo, que admite diversas axiomatizações não equivalentes, como acontece no caso de feixes sobre uma álgebra de Heyting completa. Para melhor interpretar o conteúdo semântico dos axiomas em $Psh(Q)$, introduziremos a noção de fibra de um prefeixe sobre Q . Começamos lembrando a noção de ponto num quantal introduzida em [BvB1] (consultar também [Ros]).

Definição 3.2.1 (Ros) : *Seja Q um quantal RSI.*

(i) Um ponto de Q é uma aplicação $\alpha \rightarrow 2$ (onde $2 = \{0, \top\}$ com a única estrutura de quantal RSI, $a \& b = \top$ sse $a = \top = b$) satisfazendo:

$$[P1] \quad \alpha(\top) = \top;$$

$$[P2] \quad \alpha(p \& q) \geq \alpha(p) \& \alpha(q);$$

$$[P3] \quad \alpha(\bigvee S) = \bigvee \{\alpha(s) : s \in S\}; \text{ em particular, } \alpha(0) = 0.$$

O conjunto dos pontos de Q será denotado por $\mathcal{P}(Q)$. Um ponto é estrito se em [P2] vale a igualdade.

(ii) Um elemento $p \in Q$ é primo se satisfaz: $p \neq \top$ e $a \& b \leq p$ implica $a \leq p$ ou $b \leq p$. Os elementos maximais são sempre primos (pois Q é RSI).

(iii) Dizemos que Q tem suficientes pontos (estritos, resp.) se, dados $a \neq b \in Q$, existe um ponto (estrito, resp.) α tal que $\alpha(a) \neq \alpha(b)$.

Proposição 3.2.2 (Ros) : (1) *Existe uma bijeção entre os pontos de Q e os elementos primos de Q . Esta bijeção leva os pontos estritos nos primos two-sided de Q .*

(2) *Q tem suficientes pontos sse, para todo $a \in Q$,*

$$a = \bigwedge \{p \in Q : a \leq p, p \text{ primo}\}.$$

(3) *Se Q tem suficientes pontos estritos, então Q é uma cHa.*

Um exemplo importante de quantal RSI com suficientes pontos é o quantal $Q = \text{Rid } \mathcal{A}$ dos ideais à direita, fechados em norma, de uma álgebra C^* (Proposição 5.3.1 em [Ros]). Com a noção de ponto num quantal, vamos adaptar [Mir1] para definir a noção de fibra em prefeixes sobre quantais.

Seja A um prefeixe sobre Q e α um ponto de Q . Seja $V_\alpha = \{p \in Q : \alpha(p) = \top\}$ o conjunto das vizinhanças de α . Observe que V_α satisfaz:

- (1) $p, q \in V_\alpha \Rightarrow p \& q, q \& p \in V_\alpha$;
- (2) $p \in V_\alpha, p \leq q \Rightarrow q \in V_\alpha$.

Considere $X_\alpha = \bigsqcup_{p \in V_\alpha} A(p)$, e defina a relação seguinte em X_α^2 : $x \sim y$ sse $[x = y] \in V_\alpha$. Então $\sim$ é uma relação de equivalência. Com efeito, é claro que $x \sim x$, para todo $x \in A(Ex)$. Se $x \sim y$, então $\alpha(Ex) = \alpha(Ey) = \alpha([x = y]) = \top$ e então

$$\alpha([y = x]) = \alpha(Ey \& [x = y]) \geq \alpha(Ey) \& \alpha([x = y]) = \top,$$

mostrando que $y \sim x$. Finalmente, se $x \sim y$ e $y \sim z$, então

$$\top = \alpha([x = y]) \& \alpha([y = z]) \leq \alpha([x = y] \& [y = z]) \leq \alpha([x = z]),$$

e assim $\sim$ é, de fato, uma relação de equivalência.

Definição 3.2.3 *Seja A um prefeixe sobre Q e α um ponto de Q . Definimos a fibra de A em α como sendo*

$$A_\alpha = X_\alpha / \sim = \{\bar{x} : \alpha(Ex) = \top\}, \quad \bar{x} = \{y : \alpha([y = x]) = \top\}.$$

A classe $\bar{x}$ de x em A_α será chamada de germe de x em α .

Da mesma maneira que nos prefeixes sobre um espaço topológico ([Mir1]), temos o seguinte:

Lema 3.2.4 *Dado um ponto α e A_α a fibra do prefeixe A em α , defina a seguinte família de aplicações:*

$$\phi_p : A(p) \longrightarrow A_\alpha, \quad x \mapsto \bar{x} \quad \text{para todo } p \in V_\alpha.$$

Então,

- (1) Para todo $p, q \in V_\alpha$, se $q \& p = q$ e $x \in A(p)$, então $\phi_p(x) = \phi_q(x|_q)$.
- (2) Seja D um conjunto e $\psi_p : A(p) \longrightarrow D$ uma família de funções indexadas por $p \in V_\alpha$ satisfazendo (1), i.e.: para todo $p, q \in V_\alpha$, com $q \& p = q$ e $x \in A(p)$, temos que $\psi_p(x) = \psi_q(x|_q)$. Então existe uma única função $F : A_\alpha \longrightarrow D$ tal que $F \circ \phi_p = \psi_p$, para todo $p \in V_\alpha$.
- (3) $A_\alpha = \bigcup_{p \in V_\alpha} \text{Im } \phi_p$.
- (4) Seja $S \subseteq |A|$ finito tal que $r = \bigwedge \{Es : s \in S\} \in V_\alpha$ e seja $p = r \& \prod \{[s = t] : s, t \in S\}$. As seguintes condições são equivalentes:

- (i) Para todo $s, t \in S$, $\bar{s} = \bar{t}$;
- (ii) Existe $q \in V_\alpha \cap r \downarrow$ tal que, para todo $s, t \in S$, $s|_q = t|_q$;
- (iii) $p \in V_\alpha$.

Demonstração: (1) Sejam $p, q \in V_\alpha$ com $q \& p = q$; dado $x \in A(p)$, então

$$\alpha([x|_q = x]) = \alpha(q \& p) = \alpha(q) = \top,$$

mostrando que $x \sim x|_q$.

(2) Defina a aplicação

$$F : A_\alpha \longrightarrow D, \quad F(\bar{x}) = \psi_p(x).$$

Se F estiver bem definida, então é a única função que satisfaz o requerido pela conclusão. Vamos provar que F é bem definida. Com efeito, suponha que $x \sim y$, onde $p = Ex$, $q = Ey$. Então, $\alpha([x = y]) = \top$ e $[x = y] \& Ex = [x = y] = [x = y] \& Ey$, donde

$$\psi_p(x) = \psi_{[x=y]}(x|_{[x=y]}) = \psi_{[x=y]}(y|_{[x=y]}) = \psi_q(y).$$

(3) É óbvio.

(4) (i) $\Rightarrow$ (ii): Considere $q = p \in r \downarrow$; por (i), temos que

$$\alpha(q) \geq \alpha(r) \& \prod \{ \alpha([s = t]) : s, t \in S \} = \top,$$

donde $q \in V_\alpha$. Por outro lado, para todo $s, t \in S$,

$$s|_q = s|_{q \& [s=t]} = (s|_{[s=t]})|_q = (t|_{[s=t]})|_q = t|_q.$$

(ii) $\Rightarrow$ (iii): Para q nas condições de (ii), sejam $s, t \in S$ e considere $q(s, t) = Es \& Et \& q$; então, $q = r \& q(s, t)$, com $q(s, t) \in (Es \& Et) \downarrow$ e

$$s|_{q(s,t)} = (s|_q)|_{Es \& Et} = (t|_q)|_{Es \& Et} = t|_{q(s,t)},$$

donde $q(s, t) \leq [s = t]$; assim

$$q = r \& \prod \{ q(s, t) : s, t \in S \} \leq r \& \prod \{ [s = t] : s, t \in S \} = p.$$

Como $q \in V_\alpha$, concluímos que $p \in V_\alpha$.

(iii) $\Rightarrow$ (i): Temos que

$$\top = \alpha(r \& \prod \{ [s = t] : s, t \in S \}) \leq \alpha(Es \& [s = t]) = \alpha([s = t])$$

para todo $s, t \in S$; o resultado é agora imediato. $\square$

Vamos agora definir a noção de grupo em $Psh(Q)$.

Proposição 3.2.5 *Considere uma linguagem $\mathbb{L}$ com um tipo t , uma constante $c \in C_t$ e símbolos de função $< f, t, t, t >$, $< g, t, t >$; a notação utilizada para os termos $f(x, y)$ e $g(x)$ será $x \cdot y$ e x^{-1} , respectivamente. Defina uma teoria em (QPC) pelos seguintes axiomas :*

$$[A] \quad \vdash (\forall x)(\forall y)(\forall z)(x \cdot (y \cdot z) = (x \cdot y) \cdot z);$$

$$[N] \quad \vdash (\forall x)((x \cdot c = x) \wedge (c \cdot x = x));$$

$$[I] \quad \vdash (\forall x)((x \cdot x^{-1} = c) \wedge (x^{-1} \cdot x = c)).$$

Então, uma interpretação $\mathcal{I}$ satisfaz os axiomas $[A], [N], [I]$ se e somente se existem morfismos $\cdot : A_t \times A_t \rightarrow A_t$, $i : A_t \rightarrow A_t$ e uma seção global $1 \in A_t(EA)$ tal que $A_t(p)$, com as operações induzidas pela restrição dos morfismos acima, é um grupo com elemento neutro $1|_p$ e inverso $x^{-1} = i(x)$. Mais ainda, $A_t(p)$ é abeliano para todo p se e somente se $\mathcal{I}$ satisfaz o axioma

$$[C] \quad \vdash (\forall x)(\forall y)(x \cdot y = y \cdot x).$$

Demonstração: Seja $\mathcal{I}$ uma interpretação, $G = A_t$, $1 = c^{\mathcal{I}}$, $\cdot = f^{\mathcal{I}}$, e $i = g^{\mathcal{I}}$. Então, $\mathcal{I} \models [A]$ se e somente se, para todo $x, y, z \in |G|$

$$p = EG\&[x|_p \cdot (y|_p \cdot z|_p) = (x|_p \cdot y|_p) \cdot z|_p],$$

onde $p = EG\&Ex\&Ey\&Ez$, se e somente se, para todo $x, y, z \in |G|$

$$x|_p \cdot (y|_p \cdot z|_p) = (x|_p \cdot y|_p) \cdot z|_p.$$

Por outro lado, $\mathcal{I} \models [N]$ se e somente se, para todo $x \in |G|$

$$p = EG\&[x|_p \cdot 1|_p = x|_p] \wedge EG\&[1|_p \cdot x|_p = x|_p],$$

onde $p = EG\&Ex$, se e somente se, para todo $x \in |G|$

$$[x \cdot 1|_{Ex} = x] = Ex = [1|_{Ex} \cdot x = x],$$

se e somente se, para todo $x \in |G|$

$$x \cdot 1|_{Ex} = x = 1|_{Ex} \cdot x.$$

Analogamente, $\mathcal{I} \models [I]$ se e somente se, para todo $x \in |G|$,

$$p = EG\&[x|_p \cdot i(x|_p) = 1|_p] \wedge EG\&[i(x|_p) \cdot x|_p = 1|_p],$$

onde $p = EG\&Ex$, se e somente se, para todo $x \in |G|$,

$$[x \cdot i(x) = 1|_{Ex}] = Ex = [i(x) \cdot x = 1|_{Ex}],$$

se e somente se, para todo $x \in |G|$,

$$x \cdot i(x) = 1|_{Ex} = i(x) \cdot x.$$

Finalmente, $\mathcal{I} \models [C]$ se e somente se, para todo $x, y \in |G|$,

$$p = EG\&[x|_p \cdot y|_p = y|_p \cdot x|_p],$$

onde $p = EG\&Ex\&Ey$, se e somente se, para todo $x, y \in |G|$,

$$x|_p \cdot y|_p = y|_p \cdot x|_p,$$

se e somente se $G(p)$ é abeliano para todo p . $\square$

Definição 3.2.6 : Um prefeire G sobre Q é um grupo se ele é modelo dos axiomas $[A]$, $[N]$, $[I]$. Dizemos que G é abeliano se, adicionalmente, satisfaz o axioma $[C]$.

De maneira inteiramente análoga, os axiomas usuais de anel e módulo serão as bases para definir os conceitos correspondentes em $Psh(Q)$.

Definição 3.2.7 Considere uma linguagem $\mathbb{L}_M$ com dois tipos s, t , constantes $0_s, 1_s \in \mathcal{C}_s$, $0_t \in \mathcal{C}_t$ e símbolos de função

$$+, \cdot : s \times s \longrightarrow s, \quad i : s \longrightarrow s, \quad \tilde{+} : t \times t \longrightarrow t, \quad j : t \longrightarrow t, \quad \star : s \times t \longrightarrow t.$$

(a) Um anel (com identidade) em $Psh(Q)$ é um modelo A dos seguintes axiomas em $\mathbb{L}_M$:

- [A1] $\vdash (\forall a)(\forall b)(\forall c)(a + (b + c) = (a + b) + c);$
- [A2] $\vdash (\forall a)(a + 0_s = a);$
- [A3] $\vdash (\forall a)(a + i(a) = 0_s);$
- [A4] $\vdash (\forall a)(\forall b)(a + b = b + a);$
- [A5] $\vdash (\forall a)(\forall b)(\forall c)(a \cdot (b \cdot c) = (a \cdot b) \cdot c);$
- [A6] $\vdash (\forall a)((a \cdot 1_s = a) \wedge (1_s \cdot a = a));$
- [A7] $\vdash (\forall a)(\forall b)(\forall c)((a \cdot (b + c) = a \cdot b + a \cdot c) \wedge ((a + b) \cdot c = a \cdot c + b \cdot c));$
- [A8] $\vdash \neg(1_s = 0_s).$

Dizemos que A é comutativo se satisfaz o axioma

$$[A9] \quad (\forall a)(\forall b)(a \cdot b = b \cdot a).$$

Os inversíveis de A são os elementos do sub-prefeire fechado $U(A)$ determinado pela fórmula

$$a \in U(s) \equiv_{def} (\exists b)((a \cdot b = 1_s) \wedge (b \cdot a = 1_s)).$$

Dizemos que um anel comutativo A é um domínio de integridade se satisfaz o seguinte

$$[DI] \quad \vdash (\forall a)(\forall b)((a \cdot b = 0_s) \otimes \neg(b = 0_s) \multimap (a = 0_s)) .$$

Dizemos que A é um anel local se satisfaz o seguinte

$$[AL] \quad \vdash (\forall a)(x \in U(s) \vee (1 - a) \in U(s)) .$$

(b) Dado um anel A , definimos um módulo (à esquerda) sobre A como sendo um prefeire M que satisfaz os seguintes axiomas (onde $M = A_t$) :

- [M1] $\vdash (\forall x)(\forall y)(\forall z)(x \tilde{+} (y \tilde{+} x) = (x \tilde{+} y) \tilde{+} z);$
- [M2] $\vdash (\forall x)(x \tilde{+} 0_t = x);$
- [M3] $\vdash (\forall x)(x \tilde{+} j(x) = 0_t);$
- [M4] $\vdash (\forall x)(\forall y)(x \tilde{+} y = y \tilde{+} x);$

$$[M5] \quad \vdash (\forall a)(\forall x)(\forall y)(a \star (x \tilde{+} y) = (a \star x) \tilde{+} (a \star y));$$

$$[M6] \quad \vdash (\forall a)(\forall b)(\forall x)(a \star (b \star x) = (a \cdot b) \star x);$$

$$[M7] \quad \vdash (\forall a)(\forall b)(\forall x)((a + b) \star x = a \star x \tilde{+} b \star x);$$

$$[M8] \quad \vdash (\forall x)(1_s \star x = x).$$

Como no caso dos axiomas de grupo, temos

Proposição 3.2.8 *Um prefeixe A é um anel se e somente se existem morfismos $+, \cdot : A \times A \rightarrow A$, $i : A \rightarrow A$, juntamente com seções globais $0, 1 \in A(EA)$ com $[0 = 1] = \mathbf{0}$, tal que $A(p)$ com as operações induzidas pela restrição dos morfismos a $A(p)$ é um anel com identidade $1_p \neq 0_p$ (se $p \neq \mathbf{0}$). Além disso, $x \in U(A)(p)$ se e somente se x é inversível no anel $A(p)$. Por outro lado, M é um módulo sobre A se e somente se $M(p)$ é um módulo sobre o anel $A(p)$ para todo $p \leq EA \wedge EM$.*

Observe que, se A é um anel, então, para cada ponto α de Q tal que $\alpha(EA) = \top$, a fibra A_α de A em α é um anel, com as definições:

$$\bar{x} \cdot \bar{y} \equiv_{def} \overline{x|_{EA \& Ex \& Ey} \cdot y|_{EA \& Ex \& Ey}}, \quad 1 = \bar{1};$$

$$\bar{x} + \bar{y} \equiv_{def} \overline{x|_{EA \& Ex \& Ey} + y|_{EA \& Ex \& Ey}}, \quad 0 = \bar{0}.$$

Além disso, $1 \neq 0$, pois, caso contrário, $\mathbf{0} = [1 = 0] \in V_\alpha$ e então $\alpha(\mathbf{0}) = \top$, o que contradiz a definição de ponto. Da mesma maneira, a fibra M_α de um módulo M sobre A tem estrutura de A_α -módulo para todo ponto α tal que $\alpha(EA \wedge EM) = \top$, com a operação

$$\bar{x} \star \bar{m} \equiv_{def} \overline{x|_p \star m|_p},$$

onde $p = (EA \wedge EM) \& Ex \& Em$.

Lema 3.2.9 *Seja A um anel em $Psh(Q)$ e considere o sub-prefeixe fechado $R \subseteq A$ obtido de interpretar a fórmula*

$$\phi_1(x) \equiv_{def} \neg(x \in U(s)) \multimap (x = 0_s).$$

Então,

(i) $a \in |R|$ se e somente se satisfaz:

$$\forall p \leq EA (\forall q \leq p (q \& Ea \neq \mathbf{0} \Rightarrow a|_q \notin U(A)(q \& Ea)) \Rightarrow a|_p = 0_{p \& Ea}).$$

(ii) Se Q tem suficientes pontos, então $a \in |R|$ se e somente se satisfaz:

$$\forall p \leq EA (\forall \alpha \in \mathcal{P}(Q) (\alpha(p \& Ea) = \top \Rightarrow \overline{a|_p} \notin U(A_\alpha)) \Rightarrow a|_p = 0_{p \& Ea}).$$

Demonstração: Temos que, $a \in |R|$ se e somente se $Ea \leq \llbracket \phi_1 \rrbracket_{(x; 0_s)}(a)$, se e somente se

$$(*) \quad EA \& ((\bigvee_{b \in |A|} EA \& [a|_r \cdot b|_r = 1] \& [b|_r \cdot a|_r = 1]) \rightarrow_r \mathbf{0}) \& Ea \leq EA \& [a = 0]$$

onde $r = EA \& Ea \& Eb$.

(i) Seja $a \in |R|$ e $p \leq EA$ tal que $a|_q \notin U(A)(q \& Ea)$, para todo $q \leq p$ que satisfaz $q \& Ea \neq 0$. Iremos provar que

$$r(b) = [a|_{p \& Ea \& Eb} \cdot b|_{p \& Ea \& Eb} = 1] \& [b|_{p \& Ea \& Eb} \cdot a|_{p \& Ea \& Eb} = 1] = 0 \quad \text{para todo } b \in |A|.$$

Com efeito, observe que

$$\begin{aligned} r(b) &= p \& r(b) = [a|_{p \& Ea \& Eb} \cdot b|_{p \& Ea \& Eb} = 1] \wedge [b|_{p \& Ea \& Eb} \cdot a|_{p \& Ea \& Eb} = 1] \\ &= s(b) \wedge t(b) = s(b) \& t(b) = t(b) \& s(b), \end{aligned}$$

logo, se $r(b) \neq 0$, então $s(b) \neq 0 \neq t(b)$. Se existir $b \in |A|$ tal que $r(b) \neq 0$, então

$$a|_{s(b)} \cdot b|_{s(b)} = (a|_{p \& Ea \& Eb} \cdot b|_{p \& Ea \& Eb})|_{s(b)} = 1|_{s(b)},$$

logo, restringindo a $t(b)$, obtemos que $a|_{r(b)} \cdot b|_{r(b)} = 1|_{r(b)}$; por simetria, temos também que $b|_{r(b)} \cdot a|_{r(b)} = 1|_{r(b)}$. Logo, $a|_{r(b)} \in U(A)(r(b) \& Ea)$, com $0 < r(b) \& Ea = r(b) \leq p$, o que contradiz a hipótese sobre p . Isto mostra que $r(b) = 0$ para todo $b \in |A|$, portanto $EA \& r(b) = 0$ para todo b . Observe agora que, como $EA \& [0 = 0] = EA$, então $0 \in |R|$, donde $ER = EA$. Assim, $a|_p \in |R|$, e então, por (*),

$$EA \& p \& Ea = EA \& \top \& p \& Ea = EA \& ((\bigvee_b EA \& r(b)) \rightarrow_r 0) \& Ea|_p \leq EA \& [a|_p = 0],$$

relação que multiplicada à esquerda por $p \& Ea$, fornece $a|_p = 0|_{p \& Ea}$.

Reciprocamente, seja $a \in |A|$ tal que, para todo $p \leq EA$, se $a|_p \neq 0|_{p \& Ea}$, então existe $q \leq p$ tal que $q \& Ea \neq 0$ e $a|_q \in U(A)(q \& Ea)$. Considere

$$f(b) = [a|_{EA \& Ea \& Eb} \cdot b|_{EA \& Ea \& Eb} = 1] \& [b|_{EA \& Ea \& Eb} \cdot a|_{EA \& Ea \& Eb} = 1] \quad \text{para todo } b \in |A|,$$

$$h(a) = EA \& Ea \& ((\bigvee_b EA \& f(b)) \rightarrow_r 0) = \bigvee \{ EA \& Ea \& c : EA \& f(b) \& c = 0 \ \forall b \in |A| \}.$$

Vamos provar então que, se $EA \& f(b) \& c = 0$ para todo b , então

$$x = a|_{EA \& Ea \& c} = 0|_{EA \& Ea \& c} = y.$$

Com efeito, se $x \neq y$, então, por hipótese, existe $p \leq EA \& Ea \& c$ tal que $p = p \& Ea \neq 0$ e $a|_p \in U(A)(p)$. Seja então $b \in A(p)$ tal que $a|_p \cdot b = 1|_p = b \cdot a|_p$. Então

$$0 = EA \& f(b) \& c = EA \& Ea \& [a|_p \cdot b = 1] \& [b \cdot a|_p = 1] \& c = EA \& Ea \& p \& c = (EA \& Ea \& c) \& p,$$

e portanto $p = p \& (EA \& Ea \& c) = 0$, uma contradição. Como $x = y$, temos

$$EA \& Ea \& c \leq \bigvee \{ s \in (EA \& Ea) \downarrow : a|_s = 0|_s \} = [a|_{EA} = 0] = EA \& [a = 0],$$

mostrando que $h(a) \leq EA \& [a = 0]$ e que $a \in |R|$.

(ii) Observe que, dados $p, q \in Q$, sempre temos $p \& (p \& q \rightarrow_r 0) \leq p \& (q \rightarrow_r 0)$ (de fato, vale a igualdade). Com efeito, dado que $p \& q = 0$ implica $q \& p = 0$ para todo p, q , então

$$\begin{aligned}
p \& (p \& q \rightarrow_r \mathbf{0}) &= p \& \bigvee \{c : (p \& q) \& c = \mathbf{0}\} = p \& \bigvee \{p \& c : (p \& c) \& q = \mathbf{0}\} \\
&= p \& \bigvee \{p \& c : q \& (p \& c) = \mathbf{0}\} \leq p \& \bigvee \{c : q \& c = \mathbf{0}\} = p \& (q \rightarrow_r \mathbf{0}).
\end{aligned}$$

Seja então $a \in |R|$ e considere $p \leq EA$ tal que, para todo ponto α onde $\alpha(p \& Ea) = \top$, o elemento $\overline{a|_p}$ não é inversível no anel A_α e suponha que $a|_p \neq 0|_{p \& Ea}$. Logo, $[a|_p = 0] < p \& Ea$ e então existe um ponto α tal que $\alpha([a|_p = 0]) = \mathbf{0}$ e $\alpha(p \& Ea) = \top$, pois Q tem suficientes pontos. Pela observação acima, seja $q = \bigvee_b EA \& f(b)$ (com $f(b)$ como no item (i)); assim, dado que $a \in |R|$, temos

$$p \& Ea \& ((\bigvee_b p \& f(b)) \rightarrow_r \mathbf{0}) \leq p \& EA \& Ea \& (q \rightarrow_r \mathbf{0}) \leq p \& EA \& [a = 0] = [a|_p = 0].$$

Aplicando α e lembrando que $\alpha(p \& Ea) = \top$,

$$\mathbf{0} = \alpha([a|_p = 0]) \geq \alpha(p \& Ea \& (r \rightarrow_r \mathbf{0})) \geq \alpha(p \& Ea) \& \alpha(r \rightarrow_r \mathbf{0}) \geq \alpha(r \rightarrow_r \mathbf{0}),$$

donde $\alpha(r \rightarrow_r \mathbf{0}) = \mathbf{0}$, com $r = \bigvee_b p \& f(b)$. Suponha que $r \neq \mathbf{0}$; então, existe um ponto β tal que $\beta(r) = \top$, pois Q tem suficientes pontos. Portanto, existe $b \in |A|$ tal que $\top = \beta(p \& f(b)) \leq \beta(p \& Ea)$ e então, com a notação de (i), dado que $p \& f(b) = r(b) = s(b) \wedge t(b)$, temos $\beta(s(b)) = \top = \beta(t(b))$, isto é, $\overline{a|_p}$ é inversível em A_β , uma contradição. Logo, devemos ter que $r = \mathbf{0}$ e então

$$\mathbf{0} = \alpha(r \rightarrow_r \mathbf{0}) = \alpha(\mathbf{0} \rightarrow_r \mathbf{0}) = \alpha(\top) = \top,$$

uma contradição. Isto prova que $a|_p = 0|_{p \& Ea}$.

Reciprocamente, seja a tal que, para todo $p \leq EA$, se para todo ponto α (onde $\alpha(p \& Ea) = \top$) temos que $\overline{a|_p} \notin U(A_\alpha)$, então $a|_p = 0|_{p \& Ea}$. Seja $c \in Q$ tal que

$$EA \& f(b) \& c = f(b) \& c = \mathbf{0} \quad \text{para todo } b \in |A|.$$

Suponha que $a|_{EA \& Ea \& c} \neq 0|_{EA \& Ea \& c}$; então existe um ponto α tal que $\alpha(EA \& Ea \& c) = \top$ e $\overline{a|_{EA \& Ea \& c}} \in U(A_\alpha)$. Seja $b \in |A|$ tal que $\bar{b}$ é o inverso de $\overline{a|_{EA \& Ea \& c}}$ em $U(A_\alpha)$. Então

$$\alpha(EA \& f(b) \& c) = \alpha(EA \& c \& f(b)) = \top,$$

o que contradiz a hipótese sobre c . Portanto, $a|_{EA \& Ea \& c} = 0|_{EA \& Ea \& c}$ e então $EA \& Ea \& c \leq [a|_{EA} = 0]$, donde

$$EA \& Ea \& ((\bigvee_b f(b)) \rightarrow_r \mathbf{0}) = \bigvee \{EA \& Ea \& c : f(b) \& c = \mathbf{0} \ \forall b \in |A|\} \leq [a|_{EA} = 0],$$

i.e., $a \in |R|$. $\square$

Lema 3.2.10 *O axioma de anel local é equivalente (na presença dos axiomas de anel) ao seguinte axioma:*

$$[AL1] \quad \vdash (\forall x \in A)(\forall y \in A)((x + y \in U(s)) \rightarrow (x \in U(s) \vee (y \in U(s)))).$$

Demonstração: Claramente, $[AL1]$ implica $[AL]$. Com efeito, considerando a fórmula sem disjunções $\phi(z) \equiv_{def} z \in U(s) \equiv_{def} (\exists y)((yz = 1) \wedge (zy = 1))$, $[SUBS]$ fornece

$$(z \in U(s))[^1/z], (x + (1 - x) = 1) \vdash x + (1 - x) \in U(s),$$

isto é, $(1 \in U(s)) \otimes (x + (1 - x) = 1) \vdash x + (1 - x) \in U(s)$. Por outro lado, podemos escrever

$$\frac{\frac{(\exists x)Ex \vdash 1 \in U(s) \quad (\exists x)Ex \vdash (x + (1 - x) = 1)}{(\exists x)Ex \otimes (\exists x)Ex \vdash (1 \in U(s)) \otimes (x + (1 - x) = 1)} \quad (\exists x)Ex \vdash (\exists x)Ex \otimes (\exists x)Ex}{(\exists x)Ex \vdash (1 \in U(s)) \otimes (x + (1 - x) = 1)}$$

e então, por $[CUT]$, provamos $(\exists x)Ex \vdash x + (1 - x) \in U(s)$. Logo, de

$$x + (1 - x) \in U(s) \vdash (x \in U(s)) \vee (1 - x \in U(s))$$

(obtido de $[AL1]$) deduzimos

$$\frac{(\exists x)Ex \vdash (x \in U(s)) \vee (1 - x \in U(s))}{(\exists x)Ex \vdash (\forall x)((x \in U(s)) \vee (1 - x \in U(s)))},$$

que é um axioma equivalente a $[AL]$, pois $(\exists x)Ex \sim V_1((\forall x)((x \in U(s)) \vee (1 - x \in U(s))))$. Por outro lado, é fácil provar que

$$xy \in U(s), x \in U(s) \vdash y \in U(s).$$

Com efeito:

$$\frac{\frac{\frac{(z(xy) = 1), (z(xy) = (zx)y) \vdash ((zx)y = 1) \quad (\exists x)Ex \vdash (z(xy) = (zx)y)}{(z(xy) = 1) \otimes (\exists x)Ex \vdash ((zx)y = 1)}}{(z(xy) = 1) \vdash ((zx)y = 1)}}{((xy)z = 1) \wedge (z(xy) = 1) \vdash ((zx)y = 1)}}{((xy)z = 1) \wedge (z(xy) = 1), (x \in U(s)) \vdash ((zx)y = 1)}$$

Da mesma maneira, manipulando as equações utilizando as regras da igualdade, provamos:

$$\frac{\frac{\frac{((xy)z = 1), (wx = 1) \vdash (yz = w) \quad (yz = w), (wx = 1) \vdash (y(zx) = 1)}{((xy)z = 1), (wx = 1) \vdash (y(zx) = 1)}}{((xy)z = 1) \wedge (z(xy) = 1), (wx = 1) \wedge (xw = 1) \vdash (y(zx) = 1)}}{((xy)z = 1) \wedge (z(xy) = 1), (x \in U(s)) \vdash (y(zx) = 1)},$$

donde obtemos

$$\frac{((xy)z = 1) \wedge (z(xy) = 1), (x \in U(s)) \vdash (y(zx) = 1) \wedge ((zx)y = 1)}{(xy \in U(s)), (x \in U(s)) \vdash (y \in U(s))}.$$

Assim, pela proposição 2.6.4 (20), temos

$$\begin{aligned} & ((x + y)z = 1) \wedge (z(x + y) = 1), zx \in U(s), zy \in U(s) \vdash y \in U(s), \\ & ((x + y)z = 1) \wedge (z(x + y) = 1), 1 - zx \in U(s), zy \in U(s) \vdash y \in U(s), \\ & ((x + y)z = 1) \wedge (z(x + y) = 1), zx \in U(s), 1 - zy \in U(s) \vdash x \in U(s) \end{aligned}$$

e então, nos três casos, por $[\vee R1], [\vee R2]$, provamos $(x \in U(s)) \vee (y \in U(s))$. Finalmente, temos que

$$\begin{aligned} & (z(x+y) = 1) \vdash ((1-zx)(1-zy) = zxzy), \\ & (w(1-zx) = 1), ((1-zx)(1-zy) = zxzy) \vdash (wzxzy = 1-zy), \end{aligned}$$

donde, aplicando $[CUT]$ nos dois sequentes acima, obtemos

$$(w(1-zx) = 1), (z(x+y) = 1) \vdash (wzxzy = 1-zy).$$

Logo, de

$$(v(1-zy) = 1), (wzxzy = 1-zy) \vdash ((vwzxz)y = 1)$$

obtemos, por $[CUT]$ e pela proposição 2.6.4(20),

$$\frac{(v(1-zy) = 1), (w(1-zx) = 1), (z(x+y) = 1) \vdash ((vwzxz)y = 1)}{(z(x+y) = 1), (w(1-zx) = 1), (v(1-zy) = 1) \vdash ((vwzxz)y = 1)} \quad (*).$$

Por outro lado, de

$$(z(x+y) = 1) \vdash ((1-zy)(1-zx) = zyzx)$$

provamos analogamente que

$$(z(x+y) = 1), ((x+y)z = 1), ((1-zx)w = 1), ((1-zy)v = 1) \vdash (y(zxwvz) = 1) \quad (**).$$

Agora, temos que

$$\exists b(by = 1), \exists c(yz = 1) \vdash y \in U(s) \quad (***)$$

e então, de $(*)$, $(**)$ e $(***)$ obtemos

$$((x+y)z = 1) \wedge (z(x+y) = 1), 1-zx \in U(s), 1-zy \in U(s) \vdash y \in U(s).$$

Assim, de $[\vee L]$ vem

$$\Gamma \vdash (x \in U(s)) \vee (y \in U(s))$$

onde Γ é a sequência

$$((x+y)z = 1) \wedge (z(x+y) = 1), (zx \in U(s)) \vee (1-zx \in U(s)), (zy \in U(s)) \vee (1-zy \in U(s)).$$

O resultado segue agora de $[AL]$. $\square$

Vamos finalizar esta seção estudando o conceito de corpo. Os três axiomas usuais, classicamente equivalentes, são os seguintes:

$$\begin{aligned} [CORP1] \quad & \vdash (\forall x)((x = 0) \vee (x \in U(s))); \\ [CORP2] \quad & \vdash (\forall x)(\neg(x = 0) \multimap (x \in U(s))); \\ [CORP3] \quad & \vdash (\forall x)(\neg(x \in U(s)) \multimap (x = 0)). \end{aligned}$$

Estes axiomas não são intuicionisticamente equivalentes, mas o primeiro implica os outros dois e cada um deles implica o axioma $[DI]$ ($[Mul1]$). Vamos provar que em (QPC) a situação é a mesma.

Proposição 3.2.11 *Na presença dos axiomas de anel, temos que [CORP1] implica [CORP2] e [CORP3]. Além disso, [CORPi] implica [DI] (para $i = 1, 2, 3$).*

Demonstração: [CORP1] $\Rightarrow$ [CORP2]: Por 2.6.4(3), temos que

$$\neg(x = 0), (x = 0) \vee (x \in U(s)) \vdash \neg(x = 0) \otimes (x = 0) \vee \neg(x = 0) \otimes (x \in U(s)).$$

Além disso, por 2.6.4(22) e [WR], temos

$$\frac{\neg(x = 0) \otimes (x = 0) \vdash \neg(x = 0) \otimes (x \in U(s)) \quad \neg(x = 0) \otimes (x \in U(s)) \vdash \neg(x = 0) \otimes (x \in U(s))}{\neg(x = 0) \otimes (x = 0) \vee \neg(x = 0) \otimes (x \in U(s)) \vdash \neg(x = 0) \otimes (x \in U(s))}$$

e então, por [CUT], deduzimos

$$\neg(x = 0), (x = 0) \vee (x \in U(s)) \vdash \neg(x = 0) \otimes (x \in U(s)).$$

Por outro lado, de 2.6.4(19) e (16) obtemos

$$\frac{\frac{\neg(x = 0), (xy = 1) \otimes (yx = 1) \vdash (xy = 1) \otimes (yx = 1)}{\neg(x = 0), (xy = 1) \wedge (yx = 1) \vdash (xy = 1) \wedge (yx = 1)}}{\neg(x = 0) \otimes (x \in U(s)) \vdash x \in U(s)},$$

e assim, deduzimos

$$\frac{\frac{\neg(x = 0), (x = 0) \vee (x \in U(s)) \vdash x \in U(s)}{(x = 0) \vee (x \in U(s)) \vdash \neg(x = 0) \multimap (x \in U(s))}}{(\forall x)((x = 0) \vee (x \in U(s))) \vdash (\forall x)(\neg(x = 0) \multimap (x \in U(s)))}.$$

[CORP1] $\Rightarrow$ [CORP3]: Pela proposição 2.6.4(3), temos

$$\neg(x \in U(s)), (x = 0) \vee (x \in U(s)) \vdash \neg(x \in U(s)) \otimes (x = 0) \vee \neg(x \in U(s)) \otimes (x \in U(s)).$$

Por outro lado, por 2.6.4(22), [WR] e [VL1], podemos escrever

$$\neg(x \in U(s)) \otimes (x = 0) \vee \neg(x \in U(s)) \otimes (x \in U(s)) \vdash \neg(x \in U(s)) \otimes (x = 0),$$

e assim, obtemos

$$\frac{\frac{\frac{\neg(x \in U(s)), (x = 0) \vee (x \in U(s)) \vdash \neg(x \in U(s)) \otimes (x = 0) \quad \neg(x \in U(s)) \otimes (x = 0) \vdash (x = 0)}{\neg(x \in U(s)), (x = 0) \vee (x \in U(s)) \vdash (x = 0)}}{(x = 0) \vee (x \in U(s)) \vdash \neg(x \in U(s)) \multimap (x = 0)}}{(\forall x)((x = 0) \vee (x \in U(s))) \vdash (\forall x)(\neg(x \in U(s)) \multimap (x = 0))}.$$

[CORP2] $\Rightarrow$ [DI]: Por 2.6.5(c), 2.6.4(21) e [CORP2], obtemos

$$\frac{\frac{\vdash (\forall x)(\neg(x = 0) \multimap (x \in U(s))) \quad (\forall x)(\neg(x = 0) \multimap (x \in U(s))) \vdash \neg(y = 0) \multimap (y \in U(s))}{(\exists x)Ex \vdash \neg(y = 0) \multimap (y \in U(s))}}{\neg(y = 0), (\exists x)Ex \vdash y \in U(s)}}{\neg(y = 0) \vdash y \in U(s)},$$

e assim, deduzimos

$$\frac{\frac{(xy = 0) \vdash (xy = 0) \quad \neg(y = 0) \vdash y \in U(s)}{(xy = 0), \neg(y = 0) \vdash (xy = 0) \otimes (y \in U(s))}}{(*) \quad (xy = 0) \otimes \neg(y = 0) \vdash (xy = 0) \otimes (y \in U(s))}.$$

A partir dos axiomas de anel e do axioma [E6], é simples provar o seguinte

$$(xy = 0), (yz = 1) \vdash (x = 0);$$

logo, por (*), obtemos:

$$\frac{\frac{\frac{(xy = 0), (yz = 1) \vdash (x = 0)}{(xy = 0), (yz = 1) \wedge (zy = 1) \vdash (x = 0)} \quad (xy = 0) \otimes \neg(y = 0) \vdash (xy = 0) \otimes (y \in U(s))}{(xy = 0), y \in U(s) \vdash (x = 0)}}{(xy = 0) \otimes (y \in U(s)) \vdash (x = 0)} \\ \hline (xy = 0) \otimes \neg(y = 0) \vdash (x = 0) \\ \hline \vdash (\forall x)(\forall y)((xy = 0) \otimes \neg(y = 0) \multimap (x = 0))$$

[CORP3] $\Rightarrow$ [DI]: Pelos axiomas de anel e [E6], temos

$$\frac{\frac{\frac{(zx = 1), (xy = 0) \vdash (y = 0)}{x \in U(s), (xy = 0) \vdash (y = 0)} \quad \neg(y = 0) \vdash \neg(y = 0) \quad (y = 0) \otimes \neg(y = 0) \vdash}{x \in U(s), (xy = 0), \neg(y = 0) \vdash (y = 0) \otimes \neg(y = 0)}}{x \in U(s), (xy = 0), \neg(y = 0) \vdash} \\ \hline (xy = 0), \neg(y = 0) \vdash \neg(x \in U(s))$$

Finalmente, de [CORP3] e 2.6.4(21) vem

$$\frac{\frac{\frac{(xy = 0), \neg(y = 0) \vdash \neg(x \in U(s)) \quad \neg(x \in U(s)) \vdash (x = 0)}{(xy = 0), \neg(y = 0) \vdash (x = 0)}}{\vdash (xy = 0) \otimes \neg(y = 0) \multimap (x = 0)}}{\vdash (\forall x)(\forall y)((xy = 0) \otimes \neg(y = 0) \multimap (x = 0))} \quad \square$$

Observação 3.2.12 : Dado um anel A em $Sh(Q)$, o anel $A(p)$ (para $p \neq 0$) não vai ser, em geral, um corpo. Com efeito, se $a \in U(A)(p)$ e $b \in A(p)$ é o seu inverso, então $a \cdot b = 1_p$, donde, restringindo por $[a = 0]$, obtemos $a_{|[a=0]} \cdot b_{|[a=0]} = 1_{|[a=0]}$ e então

$$\begin{aligned} [a = 0] &= [a_{|[a=0]} = 0_{|[a=0]}] \& [b_{|[a=0]} = b_{|[a=0]}] \leq [a_{|[a=0]} \cdot b_{|[a=0]} = 0_{|[a=0]} \cdot b_{|[a=0]}] \\ &= [1_{|[a=0]} = 0_{|[a=0]}] = [a = 0] \& [1 = 0] = [a = 0] \& \mathbf{0} = \mathbf{0}. \end{aligned}$$

Assim, $U(A)(p) \subseteq \{a \in A(p) : [a = 0] = \mathbf{0}\} \equiv_{def} I(A)(p)$. É claro que $I(A)$ é um sub-feixe de A , com extent EA (pois $1 \in |I(A)|$) e tal que $I(A)(p) \subseteq A(p) - \{0_p\}$ para $p \neq \mathbf{0}$, pois $[0_p = 0] = p \& [0 = 0] = p \& EA = p \neq \mathbf{0}$.

Na realidade, $I(A)$ é o feixe que interpreta a fórmula $\neg(x = 0_s)$. Com efeito, se $R \subseteq A$ é o sub-feixe obtido de interpretar $\neg(x = 0_s)$, então $a \in |R|$ se e somente se

$$Ea \leq EA \& Ea \& (EA \& [a = 0] \rightarrow_r \mathbf{0})$$

se e somente se (multiplicando à esquerda por Ea ou EA , respectivamente)

$$Ea \leq Ea \& ([a = 0] \rightarrow_r \mathbf{0}),$$

pois $p \& (p \& q \rightarrow_r 0) = p \& (q \rightarrow_r 0)$ para todo $p, q \in Q$. Assim, é claro que $|I(A)| \subseteq |R|$. Por outro lado, se $a \in |R|$, então $a_{|[a=0]} \in |R|$, donde

$$[a = 0] = E(a_{|[a=0]}) \leq [a = 0] \& ([a_{|[a=0]} = 0] \rightarrow_r 0) = [a = 0] \& ([a = 0] \rightarrow_r 0) = 0.$$

Deve-se observar que, em geral, $a \neq 0_{|p}$ não implica que, para todo $0 < q \in p \downarrow$, $a_{|q} \neq 0_{|q}$; logo $U(A)(p) \neq A(p) - \{0_{|p}\}$. Assim, o máximo valor que podemos obter para $U(A)(p)$ é $I(A)(p)$. $\square$

Proposição 3.2.13 *Seja A um anel em $Sh(Q)$.*

(a) *A satisfaz [CORP2] se e somente se $U(A) = I(A)$.*

(b) *Se A satisfaz [CORP1], então A_α é um corpo para todo ponto α de Q tal que $\alpha(EA) = \top$.*

(c) *Se Q tem suficientes pontos, então A satisfaz [CORP1] se e somente se A_α é um corpo para todo ponto α tal que $\alpha(EA) = \top$.*

Demonstração: (a) Seja A um anel, e $h_1, h_2 : |A| \rightarrow Q$ as funções características associadas às fórmulas $\neg(x = 0)$ e $x \in U$, respectivamente. Portanto, h_1 e h_2 definem $I(A)$ e $U(A)$, respectivamente, e $h_2 \leq h_1$, pela observação 3.2.12. Assim, temos que A é um modelo de [CORP2] sse $h_1 \leq h_2$ sse $h_1 = h_2$ sse $U(A) = I(A)$.

(b) Seja A um anel; A satisfaz [CORP1] se e somente se, para todo $a \in |A|$,

$$(**) \quad EA \& Ea = \bigvee_b EA \& [a_{|p} \cdot b_{|p} = 1] \& [b_{|p} \cdot a_{|p} = 1] \vee EA \& [a = 0]$$

onde $p = EA \& Ea \& Eb$, pois, se

$$k(a) = \bigvee_b EA \& [a_{|p} \cdot b_{|p} = 1] \& [b_{|p} \cdot a_{|p} = 1], \quad h(a) = EA \& [a = 0],$$

então $Ek = EA = h(0)$; logo,

$$[k \vee h](a) = (Ek \vee Eh) \& (k(a) \vee h(a)) = EA \& (k(a) \vee h(a)) = k(a) \vee h(a).$$

Suponha agora que A satisfaz [CORP1] e seja $a \in |A|$; multiplicando (**) à esquerda por Ea , obtemos

$$(***) \quad Ea = \bigvee_b [a_{|p} \cdot b_{|p} = 1] \& [b_{|p} \cdot a_{|p} = 1] \vee [a = 0],$$

onde $p = Ea \& Eb$. Seja α um ponto e $a \in |A|$ tal que $\alpha(Ea) = \top$, $\alpha([a = 0]) = 0$, isto é, escolhemos $\bar{a} \in A_\alpha$ não nulo. Logo, por (***), temos que existe $b \in |A|$ tal que

$$\top = \alpha([a_{|p} \cdot b_{|p} = 1] \& [b_{|p} \cdot a_{|p} = 1]) = \alpha([a_{|p} \cdot b_{|p} = 1] \wedge [b_{|p} \cdot a_{|p} = 1]),$$

donde obtemos que $\bar{a} \cdot \bar{b} = 1 = \bar{b} \cdot \bar{a}$, isto é, $\bar{a}$ é inversível.

(c) Suponha que Q tem suficientes pontos e seja A um anel tal que a fibra A_α de A em α é um corpo, para todo ponto α tal que $\alpha(EA) = \top$. Suponha que existe $a \in |A|$ tal que

$$r = \bigvee_b [a_{|p} \cdot b_{|p} = 1] \& [b_{|p} \cdot a_{|p} = 1] \vee EA \& [a = 0] < EA \& Ea,$$

onde $p = EA \& Ea \& Eb$. Então, existe um ponto α tal que $\alpha(r) = \mathbf{0}$ e $\alpha(EA \& Ea) = \top$; concluímos que $\alpha([a]_{EA} = 0]) = \mathbf{0}$ e então $\overline{a]_{EA}} \in A_\alpha$ é não nulo. Portanto, existe $b \in |A|$ tal que

$$\alpha([a]_p \cdot b]_p = 1]) = \top = \alpha([b]_p \cdot a]_p = 1]),$$

donde

$$\alpha([a]_p \cdot b]_p = 1]) \& [b]_p \cdot a]_p = 1]) \geq \alpha([a]_p \cdot b]_p = 1]) \& \alpha([b]_p \cdot a]_p = 1]) = \top$$

e então

$$\alpha(\bigvee_b [a]_p \cdot b]_p = 1]) \& [b]_p \cdot a]_p = 1]) = \top,$$

o que contradiz a escolha de α . Logo, A satisfaz $(**)$ do item (b) para todo $a \in |A|$, i.e., A satisfaz $[CORP1]$. $\square$

Não há em $Sh(Q)$ uma única noção de corpo, pois os axiomas $[CORPi]$ produzem diferentes estruturas; não podemos dizer que uma noção é melhor do que a outra, pois cada situação pode exigir um axioma específico, da mesma forma que acontece com o caso intuicionista ([Mull]), sendo possível a existência de outros axiomas diferentes, apropriados para resolver um problema dado.

3.3 Naturais, Inteiros e Racionais em $Sh(Q)$

Para finalizar o capítulo, definiremos os objetos número natural $\tilde{\mathbb{N}}$, número inteiro $\tilde{\mathbb{Z}}$ e número racional $\tilde{\mathbb{Q}}$ em $Sh(Q)$. Provaremos também um princípio de indução. Preliminarmente, estabelecemos algumas propriedades gerais de feixes e prefeixes que serão de utilidade.

Lema 3.3.1 : (a) Sejam A e B prefeixes sobre Q e $f : A \longrightarrow B$ um morfismo.

(a.1) f é uma bijeção sse f é um isomorfismo.

(a.2) $[a = b] = [fa = fb]$ para todo $a, b \in |A|$ e f é sobrejetora sse f é um isomorfismo.

(a.3) Se A é feixe, $EA = EB$ e f é épico e mônico, então f é bijetora, portanto um isomorfismo.

(b) Sejam A e B Q -sets extensionais e $f : A \longrightarrow B$ um morfismo satisfazendo $[x = y] = [fx = fy]$, para todo $x, y \in |A|$.

(b.1) A é prefeixe sse $f(A)$ é prefeixe; neste caso, se B é prefeixe, então $f(A)$ é sub-prefeixe de B e $f : A \longrightarrow f(A)$ é um isomorfismo de prefeixes.

(b.2) A é feixe sse $f(A)$ é feixe; neste caso, se B é feixe, então $f(A)$ é sub-feixe de B e $f : A \longrightarrow f(A)$ é um isomorfismo de feixes.

(c) Sejam A e B prefeixes e $S \subseteq |A|$ um conjunto denso de seções. Então, para toda função característica $h : |A| \times \prod_{i=1}^n |A_i| \longrightarrow Q$, temos que

$$[(\forall a)h](\vec{x}) = (EA \wedge \bigwedge_i EA_i \wedge \bigwedge_{s \in S} (Es \rightarrow_l h(s, \vec{x}))) \& E\vec{x}, \quad [(\exists a)h](\vec{x}) = \bigvee_{s \in S} h(s, \vec{x})$$

para todo $\vec{x} \in \prod_i |A_i|$.

Demonstração: (a.1) Se f é isomorfismo, então é claramente bijetora. Reciprocamente, se f é bijetora, seja $g : |B| \rightarrow |A|$ a função inversa de f . Dado $b \in |B|$, então $b = f(a)$ para $a = g(b)$, portanto $Eb = Ef(a) = Ea = Eg(b)$. Se $b, b' \in |B|$ com $b = f(a)$, $b' = f(a')$, então, por 1.1.15,

$$[b = b'] = [fa = fa'] = [a = a'] = [gb = gb'],$$

portanto g é morfismo, inverso de f .

(a.2) É uma consequência de (a.1) e do lema 1.1.15.

(a.3) Pelo lema 1.1.15, a aplicação f é injetora. Seja $b \in |B|$ e considere o conjunto de seções $S = \{a_{|[b=f(a)]} : a \in |A|\} \subseteq |A|$. Dado que $EA = EB$, S está bem definido. Provaremos que S é compatível. Com efeito, observando que $E(a_{|[b=f(a)]}) = [b = f(a)]$ e $[a = c] = [f(a) = f(c)]$ para todo $a, c \in |A|$, então o lema 1.1.5(a) fornece

$$\begin{aligned} [a_{|[b=f(a)]} = c_{|[b=f(c)]}] &= [b = f(a)] \& [a = c] \& [b = f(c)] \\ &= ([b = f(a)] \& [f(a) = f(c)]) \& [b = f(c)] \\ &= ([b = f(a)] \& [b = f(c)]) \& [b = f(c)] \\ &= [b = f(a)] \& [b = f(c)] = E(a_{|[b=f(a)]}) \& E(c_{|[b=f(c)]}). \end{aligned}$$

Como A é um feixe e f épico, existe $x \in |A|$ tal que

$$Ex = \bigvee_{a \in |A|} [b = f(a)] = Eb, \quad x_{|[b=f(a)]} = a_{|[b=f(a)]} \quad \forall a \in |A|.$$

Portanto, para todo $a \in |A|$, obtemos

$$f(x)_{|[b=f(a)]} = f(x_{|[b=f(a)]}) = f(a_{|[b=f(a)]}) = f(a)_{|[b=f(a)]} = b_{|[b=f(a)]}$$

e então, por $[EXT]$,

$$[b = f(a)] = [f(x)_{|[b=f(a)]} = b_{|[b=f(a)]}] = [b = f(a)] \& [f(x) = b]$$

para todo $a \in |A|$. Logo,

$$Eb = \bigvee_{a \in |A|} [b = f(a)] = \bigvee_{a \in |A|} ([b = f(a)] \& [f(x) = b]) = Eb \& [f(x) = b] = [f(x) = b]$$

donde, por $[EXT]$, obtemos que $f(x) = b$ e f é sobrejetora. Por (a.1), f é um isomorfismo.

(b.1) Suponha que A é um prefeixe tal que a igualdade gerada pela restrição de acordo com $[*]$, na seção 1 do capítulo 2 coincide com a igualdade original. Observe que f é injetora, pelo lema 1.1.9(a); logo, para todo $x \in f(A)$ e $p \leq EA = Ef(A)$, definimos $x|_p \equiv_{def} f(f^{-1}(x)|_p)$. É fácil ver que a restrição satisfaz a condição $[R]$ (seção 1 capítulo 2), logo $f(A)$ é um prefeixe. Além disso, se B possui uma restrição $*_{!}$ compatível com a igualdade original, então, $[EXT]$ em B implica que $f(a)|_p = f(a)|_p$ para todo $p \leq Ef(A)$. Reciprocamente, se $f(A)$ é prefeixe, então $a|_p \equiv_{def} f^{-1}(f(a)|_p)$, $a \in |A|$ e $p \leq EA$, define uma estrutura de prefeixe em A compatível com a estrutura original de Q -set. Desta maneira, por (a.1), temos que $f : A \rightarrow f(A)$ é um isomorfismo de prefeixes.

(b.2) É fácil ver que $S \subseteq |A|$ é compatível em A sse $f(S)$ é compatível em $f(A)$ (e em B).

(c) Seja $g(\vec{x}) = (EA \wedge \bigwedge_i EA_i \wedge \bigwedge_{s \in S} (Es \rightarrow_l h(s, \vec{x}))) \& E\vec{x}$ para todo $\vec{x} \in \prod_i |A_i|$. Então, é claro que $[(\forall a)h](\vec{x}) \leq g(\vec{x})$ para todo $\vec{x}$, pois $S \subseteq |A|$. Por outro lado, seja $\vec{x} \in \prod_i |A_i|$, $a \in |A|$ e $t \in S$; então

$$\begin{aligned} g(\vec{x}) \& [t = a] &\leq (\bigwedge_{s \in S} (Es \rightarrow_l h(s, \vec{x}))) \& [t = a] \& E\vec{x} \\ &\leq (Et \rightarrow_l h(t, \vec{x})) \& Et \& [t = a] \& E\vec{x} \leq h(t, \vec{x}) \& [t = a] \& [\vec{x} = \vec{x}] \leq h(a, \vec{x}) \end{aligned}$$

para $t \in S$; portanto

$$g(\vec{x}) \& Ea = g(\vec{x}) \& \bigvee_{t \in S} [a = t] = \bigvee_{t \in S} (g(\vec{x}) \& [t = a]) \leq h(a, \vec{x})$$

para todo $a \in |A|$, donde $g(\vec{x}) \leq [(\forall a)h](\vec{x})$ para $\vec{x} \in \prod_i |A_i|$. Por outro lado,

$$\begin{aligned} h(a, \vec{x}) &= h(a, \vec{x}) \& Ea \& E\vec{x} = h(a, \vec{x}) \& (\bigvee_{t \in S} [a = t]) \& E\vec{x} \\ &= \bigvee_{t \in S} (h(a, \vec{x}) \& [a = t] \& [\vec{x} = \vec{x}]) \leq \bigvee_{t \in S} h(t, \vec{x}) \end{aligned}$$

para $a \in |A|$ e $\vec{x} \in \prod_i |A_i|$; como $S \subseteq |A|$,

$$[(\exists a)h](\vec{x}) = \bigvee_{a \in |A|} h(a, \vec{x}) \leq \bigvee_{t \in S} h(t, \vec{x}) \leq \bigvee_{a \in |A|} h(a, \vec{x}) = [(\exists a)h](\vec{x}). \quad \square$$

Definição 3.3.2 : Um objeto indutivo em $Sh(Q)$ consiste de uma tripla $\langle A, f, a_0 \rangle$ tal que A é um feixe sobre Q com $EA = \top$, $f : A \rightarrow A$ é um morfismo de feixes e $a_0 \in A(\top)$.

Um morfismo de objetos indutivos $\langle A, f, a_0 \rangle \xrightarrow{h} \langle B, g, b_0 \rangle$ é um morfismo de feixes $h : A \rightarrow B$ tal que $h(a_0) = b_0$ e $g \circ h = h \circ f$. Os objetos indutivos formam uma categoria (com a composição em $Sh(Q)$), indicada por **(Ind)**. O objeto número natural em $Sh(Q)$ é o objeto inicial em **(Ind)**, denotado $\langle \tilde{IN}, \text{succ}, \tilde{0} \rangle$ (ou simplesmente $\tilde{IN}$). $\tilde{IN}$ é caracterizado pela seguinte propriedade :

Para todo objeto indutivo $\langle A, f, a_0 \rangle$, existe um único morfismo de feixes $h : \tilde{IN} \rightarrow A$, tal que $h(\tilde{0}) = a_0$ e $f \circ h = h \circ \text{succ}$.

Provaremos abaixo que $\mathcal{C}_{IN}$, o feixe constante sobre IN (exemplo 1.1.21(3)), é o objeto número natural em $Sh(Q)$. Lembremos que, por definição,

$$\mathcal{C}_{IN}(p) = \{ IN \xrightarrow{f} p \downarrow : \forall n, m (n \neq m \Rightarrow f(n) \& f(m) = \mathbf{0}), p = \bigvee_n f(n) \},$$

$$|\mathcal{C}_{IN}| = \bigcup_p \mathcal{C}_{IN}(p) \times \{p\}, \quad [(f, p) = (g, q)] = \bigvee_n f(n) \& g(n),$$

$$(f, p)|_r = (r \& f, r \& p), \quad [r \& f](n) = r \& f(n),$$

donde $EC_{IN} = \top$, sendo que o conjunto $\mathcal{N} = \{\tilde{n} : n \in IN\}$, dado por

$$\tilde{n}(m) = \begin{cases} \top & \text{se } m = n \\ \mathbf{0} & \text{se } m \neq n \end{cases}$$

é denso em $\mathcal{C}_{\mathbb{N}}$; para $f \in \tilde{IN}(p)$,

$$[(f, p) = (\tilde{n}, \top)] = \bigvee_m f(m) \& \tilde{n}(m) = f(n).$$

Considere agora $\tilde{IN} = C_{\mathbb{N}}$ e

$$\text{succ} : |\tilde{IN}| \longrightarrow |\tilde{IN}|, \quad \text{succ}(f)(0) = \mathbf{0}, \quad \text{succ}(f)(n+1) = f(n).$$

Vamos provar que $f \in \tilde{IN}(p)$ implica $\text{succ}(f) \in \tilde{IN}(p)$. De fato,

$$\text{succ}(f)(0) \& \text{succ}(f)(m) = \mathbf{0} \& \text{succ}(f)(m) = \mathbf{0} = \text{succ}(f)(m) \& \text{succ}(f)(0),$$

$$\text{succ}(f)(n+1) \& \text{succ}(f)(m+1) = f(n) \& f(m) = \mathbf{0} \quad \text{se } n+1 \neq m+1$$

Por outro lado, $p = \bigvee_n f(n) = \bigvee_n \text{succ}(f)(n)$. Observe que $\text{succ}(\tilde{n}) = (n+1)^\sim$. Logo,

$$[(f, p) = (g, q)] = \bigvee_n f(n) \& g(n) = \bigvee_n \text{succ}(f)(n) \& \text{succ}(g)(n) = [\text{succ}(f, p) = \text{succ}(g, q)]$$

mostrando que succ é um morfismo mônico em $Sh(Q)$.

Dado um objeto indutivo $\langle A, \varphi, a_0 \rangle$, defina

$$\psi_0 : \mathcal{N} \longrightarrow |A|, \quad \psi_0(\tilde{0}) = a_0, \quad \psi_0(\tilde{n}) = \varphi^n(a_0) \text{ se } n > 0.$$

Assim, $E(\psi_0(\tilde{n})) = \top = E\tilde{n}$ para todo n . Além disso, se $n \neq m$,

$$[(\tilde{n}, \top) = (\tilde{m}, \top)] = \mathbf{0} \leq [\psi_0(\tilde{n}) = \psi_0(\tilde{m})].$$

Logo, pela proposição 1.1.23(b), existe um único morfismo de feixes

$$\psi : \tilde{IN} \longrightarrow A, \quad \psi|_{\mathcal{N}} = \psi_0$$

onde $\psi(f, p)$ é o join a_f em A do conjunto compatível de seções

$$S_f = \{\psi_0(\tilde{n})|_{f(0)} : n \in \mathbb{N}\} = \{a_0|_{f(0)}\} \cup \{\varphi^n(a_0)|_{f(n)} : n \geq 1\} \subseteq |A|.$$

Por definição, $\psi(\tilde{0}) = a_0$. Vamos provar que $\varphi \circ \psi = \psi \circ \text{succ}$. Observe que, em geral, se $S \subseteq |A|$ é um conjunto compatível de seções num feixe A e $\varphi : A \longrightarrow B$ é um morfismo de feixes, então $\varphi(S) \subseteq |B|$ é compatível; além disso se $a \in |A|$ é o join de S , então $\varphi(a) \in |B|$ é o join de $\varphi(S)$. Assim, $\varphi(\psi(f, p))$ é o join de

$$\varphi(S_f) = \{\varphi(a_0)|_{f(0)}\} \cup \{\varphi(\varphi^n(a_0)|_{f(n)}) : n \geq 1\} = \{\varphi^{n+1}(a_0)|_{f(n)} : n \in \mathbb{N}\}.$$

Seja $(g, p) = \text{succ}(f, p)$. Como $g(0) = \mathbf{0}$, temos que

$$S_g = \{a_0|_{g(0)}\} \cup \{\varphi^n(a_0)|_{g(n)} : n \geq 1\} = \{*\} \cup \{\varphi^n(a_0)|_{f(n-1)} : n \geq 1\} = \{*\} \cup \varphi(S_f)$$

e então $\psi(\text{succ}(f, p)) = \varphi(\psi(f, p))$ (pois o join de um conjunto compatível S de seções coincide com o join do conjunto compatível $S \cup \{*\}$). Por outro lado, se $\psi' : \tilde{IN} \longrightarrow A$ satisfaz $\varphi \circ \psi' = \psi' \circ \text{succ}$ e $\psi'(\tilde{0}) = a_0$, então $\psi'|_{\mathcal{N}} = \psi_0 = \psi|_{\mathcal{N}}$ e a unicidade de ψ implica $\psi' = \psi$. Acabamos de provar a

Proposição 3.3.3 : O objeto $\langle \tilde{IN}, \text{succ}, \tilde{0} \rangle$ definido acima é o objeto número natural em $Sh(Q)$.

$\tilde{IN}$ satisfaz o seguinte princípio de indução:

Proposição 3.3.4 : Seja $S \subseteq \tilde{IN}$ um subfeixe e $p = ES$. São equivalentes:

- (i) $\tilde{0}_p \in |S|$; $\text{succ}(S) \subseteq S$;
- (ii) $S = \tilde{IN}_p$.

Demonstração: Observe que para $n \in \tilde{IN}$, $\tilde{n}_p(m) = p$ se $m = n$ e $\tilde{n}_p(m) = \mathbf{0}$, se $m \neq n$. Por outro lado, se escrevemos $\mathcal{N}_p = \{\tilde{n}_p : n \in \tilde{IN}\}$, então, para todo (f, q) ,

$$[(\tilde{n}_p, p) = (f, q)] = \bigvee_m \tilde{n}_p(m) \& f(m) = p \& f(n),$$

donde

$$\begin{aligned} cl(\mathcal{N}_p) &= \{(f, q) \in |\tilde{IN}_p| : q \leq \bigvee_n [(\tilde{n}_p, p) = (f, q)]\} \\ &= \{(f, q) \in |\tilde{IN}_p| : q \leq \bigvee_n p \& f(n) = p \& q\} = |\tilde{IN}_p|. \end{aligned}$$

Assim, se $S \subseteq \tilde{IN}_p$ satisfaz (i), então $\mathcal{N}_p \subseteq |S|$, donde $|\tilde{IN}_p| = cl(\mathcal{N}_p) \subseteq |S|$. A recíproca é óbvia. $\square$

A contraparte sintáctica de 3.3.4 é a

Proposição 3.3.5 : Seja $\mathbb{L}$ uma linguagem, $t \in TIPOS$, $s : t \rightarrow t \in \mathcal{F}$, $a_0 \in \mathcal{C}_t$, $x \in \mathcal{V}_t$, e $\phi \in FOR(\mathbb{L})$ tal que $x \in VAR(\phi)$. Sejam $C = C(\phi[a_0/x])$, $C' = (x; C)$ e $\mathcal{I}$ uma interpretação de feixes tal que $A_t = \tilde{IN}$, $a_0^{\mathcal{I}} = \tilde{0}$, e $s^{\mathcal{I}} = \text{succ}$. Então, o seguinte

$$[ind] \quad \phi[a_0/x] \otimes (\forall x)(\phi \multimap \phi[s(x)/x]) \vdash (\forall x)\phi$$

é válido em $\mathcal{I}$, se $\mathcal{I}$ satisfaz

$$\text{clau}([ind]) = \{y_1 \cup y_2 : y_1 \in C_E(\phi, (a_0; x), C), y_2 \in C_E(\phi, (s(x); x), C')\}.$$

Demonstração: Seja $C = (\vec{x}; a_0, \vec{a}) = C(\phi[a_0/x])$ o contexto de $[ind]$, $p = EP_C$ e $F = \llbracket \phi \rrbracket_{(x; C)}$. Vamos provar primeiro que

$$G(\vec{u}) = \llbracket \phi[a_0/x] \rrbracket_C(\vec{u}) \& \llbracket (\forall x)(\phi \multimap \phi[s(x)/x]) \rrbracket_C(\vec{u}) \leq \bigwedge_n (E\tilde{n}_p \rightarrow_l F(\tilde{n}_p, \vec{u})).$$

Para todo $u \in \tilde{IN}_p$ e $\vec{u} \in D_C$ temos, por hipótese,

$$(*) \quad \llbracket \phi[a_0/x] \rrbracket_C(\vec{u}) \leq F(\tilde{0}_p, \vec{u}),$$

$$(**) \quad \llbracket \phi^{[s(x)/x]} \rrbracket_{(x;C)}(u, \vec{u}) \leq F(\text{succ}(u), \vec{u}).$$

Observe que $E\tilde{n}_{|p} = p$ para todo $n \in \mathbb{N}$. Assim, por (*), temos que

$$G(\vec{u}) \& p = G(\vec{u}) \leq F(\tilde{0}_{|p}, \vec{u}) \& \llbracket (\forall x)(\phi \multimap \phi^{[s(x)/x]}) \rrbracket_C(\vec{u}) \leq F(\tilde{0}_{|p}, \vec{u}),$$

donde $G(\vec{u}) \leq E\tilde{0}_{|p} \rightarrow_l F(\tilde{0}_{|p}, \vec{u})$. Suponha que, para todo $k \leq n$ (com $n \geq 0$), temos

$$G(\vec{u}) \leq E\tilde{k}_{|p} \rightarrow_l F(\tilde{k}_{|p}, \vec{u})$$

para todo $\vec{u}$, i.e., $G(\vec{u}) \leq F(\tilde{k}_{|p}, \vec{u})$. Como $a \rightarrow_r b \leq a \rightarrow_r c$ e $a \rightarrow_l b \leq a \rightarrow_l c$ para todo $a, b, c \in Q$ tal que $b \leq c$, então temos, por hipótese de indução e por (**),

$$\begin{aligned} G(\vec{u}) \& p &= G(\vec{u}) \& G(\vec{u}) \& E\tilde{n}_{|p} \\ &\leq F(\tilde{n}_{|p}, \vec{u}) \& (E\tilde{n}_{|p} \rightarrow_l (F(\tilde{n}_{|p}, \vec{u}) \rightarrow_r F((\text{succ}(\tilde{n}))_{|p}, \vec{u}))) \& E\tilde{n}_{|p} \\ &\leq F((\text{succ}(\tilde{n}))_{|p}, \vec{u}). \end{aligned}$$

Assim, $G(\vec{u}) \leq \bigwedge_n (E\tilde{n}_{|p} \rightarrow_l F(\tilde{n}_{|p}, \vec{u}))$ para todo $\vec{u} \in D_C$ e então

$$G(\vec{u}) \leq (p \wedge \bigwedge_n (E\tilde{n}_{|p} \rightarrow_l F(\tilde{n}_{|p}, \vec{u}))) \& E\vec{u} = \llbracket (\forall x)\phi \rrbracket_C(\vec{u}),$$

pelo lema 3.3.1 (c) e a definição de interpretação. $\square$

Vamos agora definir a soma em $\tilde{\mathbb{N}}$. Considere a aplicação

$$+_0 : \mathcal{N} \times \mathcal{N} \longrightarrow |\tilde{\mathbb{N}}|, \quad \tilde{n} +_0 \tilde{m} = (n + m)^\sim.$$

Temos que $\mathcal{N} \times \mathcal{N}$ é denso em $\tilde{\mathbb{N}} \times \tilde{\mathbb{N}}$. Com efeito, dado $(f, g) \in |\tilde{\mathbb{N}} \times \tilde{\mathbb{N}}|$,

$$[(f, g) = (\tilde{n}, \tilde{m})] = [f = \tilde{n}] \& [g = \tilde{m}] = f(n) \& f(m)$$

e então

$$E(f, g) = (\bigvee_n f(n)) \& (\bigvee_m g(m)) = \bigvee_{(n,m)} f(n) \& g(m) = \bigvee_{(n,m)} [(f, g) = (\tilde{n}, \tilde{m})].$$

Por outro lado, a aplicação $+_0$ é tal que $E(\tilde{n} +_0 \tilde{m}) = \top = E\tilde{n} = E\tilde{m}$, e, dado que, para todo $n, m, r, s \in \mathbb{N}$, $n = r$ e $m = s$ implica $n + m = r + s$, então

$$[(\tilde{n}, \tilde{m}) = (\tilde{r}, \tilde{s})] = [\tilde{n} = \tilde{r}] \& [\tilde{m} = \tilde{s}] \leq [(n + m)^\sim = (r + s)^\sim].$$

Logo, pela proposição 1.1.23(b), $+_0$ tem uma única extensão a um morfismo $+: \tilde{\mathbb{N}} \times \tilde{\mathbb{N}} \longrightarrow \tilde{\mathbb{N}}$ dado, para $(f, g) \in |\tilde{\mathbb{N}} \times \tilde{\mathbb{N}}|$, pelo join do conjunto compatível de seções

$$T_{(f,g)} = \{((n + m)^\sim)_{|f(n) \& g(m)} : n, m \in \mathbb{N}\}.$$

Assim, para todo $n, m, r \in \mathbb{N}$, temos

$$f(n) \& g(m) \& (f + g)(r) = (f + g)_{|f(n) \& g(m)}(r)$$

$$= ((n+m)^\sim)_{|f(n)\&g(m)}(r) = f(n)\&g(m)\&(n+m)^\sim(r),$$

e então, tomando supremo sobre n, m (com r fixo), obtemos

$$(f+g)(r) = p\&(f+g)(r) = \bigvee \{f(n)\&g(m) : n+m=r\},$$

pois $(f+g)(r) \in p\downarrow$. Agora, fixado r , temos que existem $r+1$ pares $(n, m) \in \mathbb{N}^2$ tais que $n+m=r$, a saber:

$$(r, 0), (r-1, 1), \dots, (r/2, r/2), (r/2-1, r/2+1), \dots, (0, r) \quad \text{se } r \text{ é par,}$$

$$(r, 0), (r-1, 1), \dots, ((r+1)/2, (r-1)/2), ((r-1)/2, (r+1)/2), \dots, (0, r) \quad \text{se } r \text{ é ímpar.}$$

Assim, determinamos uma forma explícita para a soma $(f+g)$:

$$\begin{aligned} (f+g)(r) &= \\ &= \begin{cases} f(r)\&g(0) \vee \dots \vee f(r/2)\&g(r/2) \vee f(r/2-1)\&g(r/2+1) \vee \dots \vee f(0)\&g(r) \\ f(r)\&g(0) \vee \dots \vee f((r+1)/2)\&g((r-1)/2) \vee f((r-1)/2)\&g((r+1)/2) \vee \dots \vee f(0)\&g(r) \end{cases} \end{aligned}$$

se r é par ou ímpar, respectivamente.

Assim, temos que para todo $f \in \tilde{IN}(Ef)$, $f + \tilde{1}_{|Ef} = \text{succ}(f)$. Com efeito,

$$(f + \tilde{1}_{|Ef})(0) = f(0)\&Ef\&\tilde{1}(0) = 0, \quad (f + \tilde{1}_{|Ef})(r+1) = f(r)\&Ef\&\tilde{1}(1) = f(r).$$

Temos ainda que $f+g = g+f$; de fato, $f(n), g(m) \in p\downarrow$, e então

$$f(n)\&g(m) = f(n) \wedge g(m) = g(m)\&f(n) \quad \text{para todo } n, m \in \mathbb{N}.$$

O passo seguinte é definir o feixe dos inteiros $\tilde{\mathbb{Z}}$. Primeiro de tudo, precisamos do seguinte resultado:

Lema 3.3.6 : Se $f, g, h \in \tilde{IN}(p)$, então $f+g = h+g$ implica $f=h$.

Demonstração: Se $(f+g) = k = (h+g)$, temos que $f_0\&g_0 = k_0 = h_0\&g_0$; logo

$$f_0\&g_0 = (f_0\&g_0)\&(h_0\&g_0) = (f_0\&h_0)\&g_0.$$

Suponha que, para todo $m \leq n$ (com $0 \leq n$ fixo), temos $f_0\&g_m = (f_0\&h_0)\&g_m$. Por hipótese,

$$f_{n+1}\&g_0 \vee \dots \vee f_0\&g_{n+1} = k_{n+1} = h_{n+1}\&g_0 \vee \dots \vee h_0\&g_{n+1}$$

que multiplicada à direita por f_0 fornece

$$f_{n+1}\&g_0\&f_0 \vee \dots \vee f_0\&g_{n+1}\&f_0 = h_{n+1}\&g_0\&f_0 \vee \dots \vee h_0\&g_{n+1}\&f_0.$$

Todos os termos do lado esquerdo (com exceção de $f_0\&g_{n+1}\&f_0 = f_0\&g_{n+1}$), desaparecem, pois $f_r\&f_s = 0$ se $r \neq s$. No lado direito, temos por hipótese de indução e para $i > 0$,

$$h_i \& g_{n+1-i} \& f_0 = h_i \& f_0 \& g_{n+1-i} = h_i \& f_0 \& h_0 \& g_{n+1-i} = h_i \& h_0 \& f_0 \& g_{n+1-i} = 0$$

pois $h_r \& h_s = 0$ se $r \neq s$. Para $i = 0$, obtemos $h_0 \& g_{n+1} \& f_0 = (h_0 \& f_0) \& g_{n+1}$, e portanto

$$f_0 \& g_{n+1} = (h_0 \& f_0) \& g_{n+1}.$$

Mostramos que, para todo n , $f_0 \& g_n = (h_0 \& f_0) \& g_n$; tomando supremo sobre n , obtemos $f_0 = h_0 \& f_0 \leq h_0$. Analogamente, de k_1 e por indução (usando agora f_1) provamos que para todo n , $f_1 \& g_n = (h_1 \& f_1) \& g_n$ e conseqüentemente, $f_1 = h_1 \& f_1 \leq h_1$. Com o mesmo método, provamos que $f_n \leq h_n$ para todo n . Como o argumento é simétrico em relação a f, h , concluímos que $f = h$, como desejado. $\square$

Definimos em $|\tilde{N} \times \tilde{N}|^2$ a relação seguinte: $(f, g) \sim (f', g')$ sse $Ef = Ef'$ e $f + g' = f' + g$. Claramente, a relação é reflexiva e simétrica. Para a transitividade, suponha que $(f, g) \sim (f', g')$, $(f', g') \sim (f'', g'')$. Então, $(f + g'') + g' = (f'' + g) + g'$, e portanto $f + g'' = f'' + g$.

Observe que a relação $\sim$ poderia ser definida “internamente” da maneira seguinte: considere a aplicação

$$\theta : |\tilde{N} \times \tilde{N}|^2 \longrightarrow Q, \quad \theta((f, g), (f', g')) = [f|_{Ef \& Ef'} + g'|_{Ef \& Ef'} = f'|_{Ef \& Ef'} + g|_{Ef \& Ef'}].$$

Como $+$ é um morfismo, por [eq 1], [eq 2], temos que θ satisfaz as condições da definição 3.1.2; a condição de transitividade [eqr 3] é consequência do lema 3.3.6. Com efeito, para todo $g \in \tilde{N}(p)$, o morfismo

$$\varphi_g : \tilde{N}|_p \longrightarrow \tilde{N}, \quad \varphi_g(f) = f + g|_{Ef}$$

é injetor, portanto $[f + g = f' + g] = [f = f']$ para $f, g, f' \in \tilde{N}(p)$. A partir das propriedades [eqr 1], [eqr 2], [eqr 3] e $Ef \& Ef' \& \theta((f, g), (f', g')) = \theta((f, g), (f', g'))$, é simples verificar que θ é 2-característica. Assim, definimos a relação de equivalência

$$(f, g) \hat{\theta} (f', g') \text{ sse } Ef = Ef' = \theta((f, g), (f', g')),$$

obtendo o prefeixe $(\tilde{N} \times \tilde{N})/\theta$. Por [EXT] temos que $(f, g) \hat{\theta} (f', g') \text{ sse } (f, g) \sim (f', g')$, portanto as relações coincidem. A função θ pode ser obtida interpretando a fórmula

$$P(x, y, x', y') \equiv_{def} (x + y' = x' + y)$$

onde $x, y, x', y' \in \mathcal{V}_t$, $+: t \times t \longrightarrow t$, via $A_t = \tilde{N}$ e com $+$ sendo interpretado pela soma em $\tilde{N}$.

Definimos então $|\hat{\mathbb{Z}}| \equiv_{def} |\tilde{N} \times \tilde{N}|/\sim = |(\tilde{N} \times \tilde{N})/\theta|$. Vamos mostrar que $\hat{\mathbb{Z}}$ é naturalmente isomorfo ao feixe constante sobre $\mathbb{Z}$, $\mathcal{C}_{\mathbb{Z}} \equiv_{def} \hat{\mathbb{Z}}$.

A soma em $\hat{\mathbb{Z}}$ é definida de maneira análoga a $\tilde{N}$, i.e.,

$$(\alpha + \beta)(r) = \bigvee \{ \alpha_n \& \beta_m : n, m \in \mathbb{Z}, n + m = r \} \quad \text{para todo } r \in \mathbb{Z}$$

obtida estendendo a aplicação

$$+_0 : \mathcal{Z} \times \mathcal{Z} \longrightarrow |\mathbb{Z}|, \quad \tilde{z} +_0 \tilde{w} = (z + w)^\sim,$$

onde $\mathcal{Z} = \{\tilde{z} : z \in \mathbb{Z}\} \subseteq |\tilde{\mathbb{Z}}|$ é a cópia densa de $\mathbb{Z}$ em $\tilde{\mathbb{Z}}$.

Assim, $+: \tilde{\mathbb{Z}} \times \tilde{\mathbb{Z}} \rightarrow \tilde{\mathbb{Z}}$ é morfismo de feixes tal que $f + g = g + f$ e $f + \tilde{0}_{|Ef} = f$. Considere agora as aplicações

$$\tilde{\alpha}: \tilde{N} \rightarrow \tilde{\mathbb{Z}}, \quad \tilde{\alpha}(f) = \alpha_f: \mathbb{Z} \rightarrow Ef \downarrow, \quad \alpha_f(n) = f_n \text{ se } n \geq 0, \alpha_f(n) = 0 \text{ se } n < 0,$$

$$-\tilde{\alpha}: \tilde{N} \rightarrow \tilde{\mathbb{Z}}, \quad -\tilde{\alpha}(f) = -\alpha_f: \mathbb{Z} \rightarrow Ef \downarrow, \quad -\alpha_f(n) = f_{-n} \text{ se } n \leq 0, -\alpha_f(n) = 0 \text{ se } n > 0.$$

É fácil ver que $\alpha_f + -\alpha_f = \tilde{0}_{|Ef}$ (aqui, $\tilde{0} \in \tilde{\mathbb{Z}}(\top)$); por outro lado, $\tilde{\alpha}$ e $-\tilde{\alpha}$ são morfismos injetores de feixes e $\alpha_f + \alpha_g = \alpha_{f+g}$. Defina agora a aplicação

$$\varphi: |\hat{\mathbb{Z}}| \rightarrow |\tilde{\mathbb{Z}}|, \quad \varphi(\overline{(f, g)}) = \alpha_f + -\alpha_g,$$

onde $\overline{(f, g)}$ denota a classe de equivalência de (f, g) em $\hat{\mathbb{Z}}$. Assim, temos que

$$\varphi(\overline{(f, g)})(n) = \bigvee_{r \geq 0} f(r+n) \& g(r) \quad \text{se } n \geq 0,$$

$$\varphi(\overline{(f, g)})(n) = \bigvee_{r \geq 0} f(r) \& g(r-n) \quad \text{se } n < 0.$$

Lema 3.3.7 : *A aplicação φ é bem definida, i.e., se $(f, g) \sim (f', g')$ então $\alpha_f + -\alpha_g = \alpha_{f'} + -\alpha_{g'}$.*

Demonstração: Suponha que $f + g' = f' + g$; então,

$$\alpha_f + \alpha_{g'} = \alpha_{f+g'} = \alpha_{f'+g} = \alpha_{f'} + \alpha_g$$

donde, somando $-\alpha_g + -\alpha_{g'}$, obtemos o resultado desejado. $\square$

Mostraremos agora que φ é bijeção. É fácil ver que φ é injetora: com efeito, $\alpha_f + -\alpha_g = \alpha_{f'} + -\alpha_{g'}$ implica, somando $\alpha_g + \alpha_{g'}$, que

$$\alpha_{f+g'} = \alpha_f + \alpha_{g'} = \alpha_{f'} + \alpha_g = \alpha_{f'+g}.$$

Como $\tilde{\alpha}$ é injetora, temos que $f + g' = f' + g$.

Lema 3.3.8 : *A aplicação φ é sobrejetora.*

Demonstração: Seja $\beta \in \tilde{\mathbb{Z}}(p)$ e defina as seguintes sequências $(f_n), (g_n)$ em $p \downarrow$:

$$g_0 = f_0 = \beta_0;$$

$$\text{para } j \geq 1, \text{ seja } i(j) = \text{Min}\{n : g_n \text{ não foi ainda definido}\};$$

$$\text{então, } g_{i(j)} = \beta_j = f_{i(j)+j}, \quad f_{i(j)} = \beta_{-j} = g_{i(j)+j}.$$

Assim, temos o seguinte:

$$g_0 = \beta_0 = f_0;$$

$$\begin{aligned}
g_1 &= \beta_1 = f_2; & f_1 &= \beta_{-1} = g_2; \\
g_3 &= \beta_2 = f_5; & f_3 &= \beta_{-2} = g_5; \\
g_4 &= \beta_3 = f_7; & f_4 &= \beta_{-3} = g_7; \\
g_6 &= \beta_4 = f_{10}; & f_6 &= \beta_{-4} = g_{10}; \\
g_8 &= \beta_5 = f_{13}; & f_8 &= \beta_{-5} = g_{13}
\end{aligned}$$

Fato: As sequências (f_n) e (g_n) estão bem definidas.

Prova do Fato: Vamos provar por indução que, para todo $j \geq 1$, se g_h foi definido (até o passo $j - 1$), então $h < i(j) + j$. Com efeito, se $j = 1$, então $i(j) = 1 > 0$. Suponha a afirmação verdadeira para $j \leq k$, com $k \geq 1$ fixo; assim, no final do passo k , $i(k) + k$ é o maior índice n para o qual g_n foi definido, pela hipótese de indução. Após definir $g_{i(k+1)}$, o maior índice n tal que g_n já foi definido é $\text{Max}\{i(k) + k, i(k + 1)\}$. Como $i(k + 1) > i(k)$, pois $i(k)$ foi escolhido mínimo, temos $i(k + 1) + k + 1 > i(k) + k$ e $i(k + 1) + k + 1 > i(k + 1)$. Assim, $i(k + 1) + k + 1 > n$. Concluimos que em cada passo j , $g(i(j) + j)$ recebe um valor pela primeira (portanto, única) vez, provando o **Fato**.

Temos então duas funções $f, g : \mathbb{N} \rightarrow Q$ (é claro que, para todo n , existe j suficientemente grande tal que g_n é definido; analogamente para f_n). Por outro lado, é também claro que $\text{Im } f = \text{Im } \beta = \text{Im } g$, portanto $\bigvee_n f_n = p = \bigvee_n g_n$ e $f_n \& f_m = 0 = g_n \& g_m$ se $n \neq m$, mostrando que $f, g \in \tilde{\mathbb{N}}(p)$. Pela definição das sequências,

$$\beta_n = f_{i(n)+n} \& g_{i(n)} = (\alpha_f + -\alpha_g)(n) \quad \text{se } n \geq 0,$$

$$\beta_n = f_{i(-n)} \& g_{i(-n)-n} = (\alpha_f + -\alpha_g)(n) \quad \text{se } n < 0,$$

o que prova $\alpha_f + -\alpha_g = \beta$ e que φ é sobrejetora. $\square$

Se consideramos em $\hat{\mathbb{Z}}$ a estrutura de prefeixe induzida por θ , obtemos o seguinte:

$$[\varphi(\overline{(f, g)}) = \varphi(\overline{(f', g')})]$$

$$\begin{aligned}
&= [\alpha_f + -\alpha_g = \alpha_{f'} + -\alpha_{g'}] \\
&= \bigvee \{p \in (Ef \& Ef') \downarrow : (\alpha_f)_{|p} + (-\alpha_g)_{|p} = (\alpha_{f'})_{|p} + (-\alpha_{g'})_{|p}\} \\
&= \bigvee \{p \in (Ef \& Ef') \downarrow : \alpha_{f_{|p}} + -\alpha_{g_{|p}} = \alpha_{f'_{|p}} + -\alpha_{g'_{|p}}\} \\
&= \bigvee \{p \in (Ef \& Ef') \downarrow : \alpha_{f_{|p}} + \alpha_{g'_{|p}} = \alpha_{f'_{|p}} + \alpha_{g_{|p}}\} \\
&= \bigvee \{p \in (Ef \& Ef') \downarrow : \alpha_{f_{|p}+g'_{|p}} = \alpha_{f'_{|p}+g_{|p}}\} \\
&= \bigvee \{p \in (Ef \& Ef') \downarrow : f_{|p} + g'_{|p} = f'_{|p} + g_{|p}\} \\
&= \bigvee \{p \in (Ef \& Ef') \downarrow : (f_{|Ef \& Ef'} + g'_{|Ef \& Ef'})_{|p} = (f'_{|Ef \& Ef'} + g_{|Ef \& Ef'})_{|p}\} \\
&= [f_{|Ef \& Ef'} + g'_{|Ef \& Ef'} = f'_{|Ef \& Ef'} + g_{|Ef \& Ef'}] \\
&= \theta((f, g), (f', g')) = [\overline{(f, g)} = \overline{(f', g')}]
\end{aligned}$$

Como φ é sobrejetora, o lema 3.3.1(b.2) garante que $\hat{\mathbb{Z}}$ é isomorfo a $\tilde{\mathbb{Z}}$ via φ . Note que, por definição, a restrição em $\hat{\mathbb{Z}}$ é simplesmente a restrição no representante da classe: $\overline{(f, g)}|_p = \overline{(f|_p, g|_p)}$.

Uma vez de posse dos inteiros, podemos definir, da maneira usual, os racionais em $Sh(Q)$, $\tilde{\mathcal{Q}}$. Para isso, devemos primeiro caracterizar o feixe dos números naturais positivos, $\tilde{N}_+$. Seja $\tilde{N}_+$ o feixe correspondente à interpretação da fórmula $(\exists y)(x = s(y))$. Então,

$$\begin{aligned} |\tilde{N}_+| &= tcl(\text{succ}(\tilde{N})) = \{f \in |\tilde{N}| : Ef = \bigvee_g [f = \text{succ}(g)]\} \\ &= \{f \in |\tilde{N}| : Ef = \bigvee_g \bigvee_{n>0} f_n \& g_{n-1}\}. \end{aligned}$$

Note que se $f \in |\tilde{N}_+|$, então

$$f_0 = Ef \& f_0 = (\bigvee_g \bigvee_{n>0} f_n \& g_{n-1}) \& f_0 = \bigvee_g \bigvee_{n>0} f_n \& f_0 \& g_{n-1} = \mathbf{0}.$$

Por outro lado, se $f \in |\tilde{N}|$ é tal que $f_0 = \mathbf{0}$, então $f = \text{succ}(g)$, onde $g_n \equiv_{def} f_{n+1}$ para todo n . Assim,

$$|\tilde{N}_+| = \{f \in |\tilde{N}| : f_0 = \mathbf{0}\} = |\text{succ}(\tilde{N})|.$$

Podemos observar que $\tilde{N}_+$ é também caracterizado pela fórmula $\neg(x = 0)$. De fato, lembrando a observação 3.2.12, obtemos que $\llbracket \neg(x = 0) \rrbracket_{(x;0)} = |I(A)| = |\tilde{N}_+|$.

Por outro lado, o seguinte

$$\vdash (\forall x)((x = 0) \vee (\exists y)(x = s(y)))$$

é válido. Com efeito, $E(\top \& [f = \tilde{0}]) = \top$ e o lema 3.3.1 (c) fornecem

$$\begin{aligned} \llbracket (x = 0) \vee (\exists y)(x = s(y)) \rrbracket_{(x;0)}(f) &= \top \& (\top \& [f = \tilde{0}]) \vee \top \& \bigvee_n [f = \text{succ}(\tilde{n})] \\ &= \top \& (f_0 \vee \bigvee_{n>0} f_n) = \top \& Ef. \end{aligned}$$

O produto em $\tilde{\mathbb{Z}}$ é definido a partir da aplicação

$$\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \tilde{\mathbb{Z}}, \quad \tilde{n} \cdot \tilde{m} = (nm)^\sim,$$

analogamente à definição da soma em $\tilde{\mathbb{Z}}$. Assim, existe um único morfismo, $\cdot : \tilde{\mathbb{Z}} \times \tilde{\mathbb{Z}} \longrightarrow \tilde{\mathbb{Z}}$, indicado por $\alpha \cdot \beta$, que é o join do conjunto compatível $\{(nm)^\sim\}_{\alpha_n \& \beta_m} : n, m \in \mathbb{Z}\}$. Portanto, prova-se facilmente que

$$(\alpha \cdot \beta)(r) = \bigvee \{\alpha_n \& \beta_m : n, m \in \mathbb{Z}, nm = r\}.$$

Por outro lado, é fácil ver que para $\alpha, \beta, \gamma \in |\tilde{\mathbb{Z}}|$ e $r \in \mathbb{N}$,

$$((\alpha \cdot \beta) \cdot \gamma)(r) = \bigvee \{\alpha_u \& \beta_v \& \gamma_w : u, v, w \in \mathbb{Z}, uvw = r\} = (\alpha \cdot (\beta \cdot \gamma))(r).$$

É claro que o produto é comutativo. O seguinte resultado é necessário para definir a relação de equivalência que define os números racionais:

Lema 3.3.9 : Sejam $\alpha, \beta, \gamma \in \tilde{\mathbb{Z}}(p)$, tal que $\gamma_0 = 0$. Então, $\alpha \cdot \gamma = \beta \cdot \gamma$ implica $\alpha = \beta$. Em particular, o resultado vale para $\gamma = \alpha_f$, com $f \in |\tilde{\mathbb{N}}_+|$.

Demonstração: Como $\gamma_0 = 0$, temos que

$$\begin{aligned}\alpha_0 &= p \& \gamma_0 \vee \alpha_0 \& p = \vee_n \alpha_n \& \gamma_0 \vee \vee_m \alpha_0 \& \gamma_m = (\alpha \cdot \gamma)_0 \\ &= (\beta \cdot \gamma)_0 = \vee_n \beta_n \& \gamma_0 \vee \vee_m \beta_0 \& \gamma_m = p \& \gamma_0 \vee \beta_0 \& p = \beta_0.\end{aligned}$$

Seja $k \in \mathbb{Z}$ não nulo; então, para todo $n \in \mathbb{Z}$ não nulo,

$$\begin{aligned}\alpha_k \& \gamma_n &= \vee \{ \alpha_r \& \gamma_s \& \gamma_n : rs = kn \} = (\alpha \cdot \gamma)_{kn} \& \gamma_n \\ &= (\beta \cdot \gamma)_{kn} \& \gamma_n = \vee \{ \beta_r \& \gamma_s \& \gamma_n : rs = kn \} = \beta_k \& \gamma_n,\end{aligned}$$

i.e., $\alpha_k \& \gamma_n = \beta_k \& \gamma_n$ para todo $k, n \neq 0$. Assim, tomando supremo sobre n , obtemos

$$\alpha_k = \alpha_k \& p = \vee \{ \alpha_k \& \gamma_n : n \neq 0 \} = \vee \{ \beta_k \& \gamma_n : n \neq 0 \} = \beta_k \& p = \beta_k$$

para todo $k \neq 0$ e portanto, $\alpha = \beta$. $\square$

Agora definimos uma relação em $|\tilde{\mathbb{Z}} \times \tilde{\mathbb{N}}_+|^2$ pela condição: $(\beta, f) \sim (\gamma, g)$ sse $E\beta = E\gamma$ e $\beta \cdot \alpha_g = \gamma \cdot \alpha_f$. Pelo lema 3.3.9, a relação é transitiva, sendo claramente simétrica e reflexiva.

Como no caso da definição de $\hat{\mathbb{Z}}$, podemos internalizar a relação $\sim$ definindo a equivalência

$$\theta : |\tilde{\mathbb{Z}} \times \tilde{\mathbb{N}}_+|^2 \longrightarrow Q, \quad \theta((\beta, f), (\gamma, g)) = [\beta]_{E\beta \& E\gamma} \cdot (\alpha_g)_{|E\beta \& E\gamma} = \gamma_{|E\beta \& E\gamma} \cdot (\alpha_f)_{|E\beta \& E\gamma},$$

obtida pela interpretação da fórmula

$$Q(x, y, x', y') \equiv_{def} (x \cdot y' = x' \cdot y)$$

com x, x' de tipo $\tilde{\mathbb{Z}}$ e y, y' de tipo $\tilde{\mathbb{N}}_+$. Assim,

$$(\beta, f) \sim (\gamma, g) \text{ se e somente se } (\beta, f) \hat{\theta}(\gamma, g).$$

Considere então $|\hat{Q}| = |\tilde{\mathbb{Z}} \times \tilde{\mathbb{N}}_+|/\sim = |(\tilde{\mathbb{Z}} \times \tilde{\mathbb{N}}_+)/\theta|$; provaremos que $\hat{Q}$ é isomorfo a $\tilde{Q}$, o feixe constante sobre Q ; além disso, a estrutura de prefeixe herdada de $\tilde{Q}$ coincidirá com a herdada da relação de equivalência $\sim$, exatamente como aconteceu com os inteiros. Primeiro de tudo, vamos considerar

$$\begin{aligned}Q &= \{q_i : i \in \mathbb{N}\}, \quad q_i = p_i/n_i, \quad q_0 = 0/1, \quad p_i, n_i \in \mathbb{Z}, \\ &n_i > 0 \text{ se } i > 0, \quad mdc(n_i, p_i) = 1, \quad q_i \neq q_j \text{ se } i \neq j.\end{aligned}$$

Da mesma maneira em que foram definidas as operações em $\tilde{\mathbb{N}}$ e $\tilde{\mathbb{Z}}$, o morfismo produto em $\tilde{Q}$ vem dado por

$$\cdot : \tilde{Q} \times \tilde{Q} \longrightarrow \tilde{Q}, \quad (\phi \cdot \psi)(r) = \vee_{pq=r} \phi_p \& \psi_q.$$

sendo associativo e comutativo. Considere as imersões de $\tilde{\mathbb{Z}}$ e $\tilde{\mathbb{N}}_+$ em $\tilde{Q}$ dadas por:

$$\tilde{\phi} : \tilde{\mathbb{Z}} \longrightarrow \tilde{Q}, \quad \tilde{\phi}(\alpha) = \phi_\alpha : Q \longrightarrow E\alpha \downarrow,$$

$$\begin{aligned}\phi_\alpha(p/1) &= \alpha_p, & \phi_\alpha(p/n) &= \mathbf{0} \text{ se } n > 1; \\ \tilde{\psi}: \tilde{IN}_+ &\longrightarrow \tilde{Q}, & \tilde{\psi}(f) &= \psi_f: Q \longrightarrow Ef \downarrow, \\ \psi_f(1/n) &= f_n, & \psi_f(p/n) &= \mathbf{0} \text{ se } p \neq 1.\end{aligned}$$

É fácil ver que $\tilde{\phi}, \tilde{\psi}$ são morfismos injetores de feixes. Por outro lado,

$$\begin{aligned}(\phi_\alpha \cdot \phi_\beta)(p/1) &= \bigvee_{rs=p/1} \phi_\alpha(r) \& \phi_\beta(s) = \bigvee_{n,m \in \mathbb{Z}, nm=p} \alpha_n \& \beta_m \\ &= (\alpha \cdot \beta)(p) = \phi_{\alpha \cdot \beta}(p/1),\end{aligned}$$

$$(\phi_\alpha \cdot \phi_\beta)(p/n) = \bigvee_{rs=p/n} \phi_\alpha(r) \& \phi_\beta(s) = \mathbf{0} = \phi_{\alpha \cdot \beta}(p/n)$$

se $n > 1$, pois $r/1 \cdot s/1 \neq p/n$ para $r, s \in \mathbb{Z}$; assim, $\phi_\alpha \cdot \phi_\beta = \phi_{\alpha \cdot \beta}$. Finalmente,

$$(\phi_{\alpha_f} \cdot \psi_f)(1/1) = \bigvee_{rs=1/1} \phi_{\alpha_f}(r) \& \psi_f(s) = \bigvee_{n>0} \phi_{\alpha_f}(n/1) \& \psi_f(1/n) = \bigvee_{n>0} f_n = Ef,$$

enquanto que

$$\begin{aligned}(\phi_{\alpha_f} \cdot \psi_f)(p/n) &= \bigvee_{rs=p/n} \phi_{\alpha_f}(r) \& \psi_f(s) \\ &= \bigvee_{m>0} \phi_{\alpha_f}(mp/1) \& \psi_f(1/mn) = \bigvee_{m>0} f(mp) \& f(mn) = \mathbf{0}\end{aligned}$$

se $p/n \neq 1$, portanto $\phi_{\alpha_f} \cdot \psi_f = \tilde{1}_{|Ef}$, o neutro do produto em $\tilde{Q}(Ef)$. Com estas observações, podemos definir a aplicação

$$\varphi: \hat{Q} \longrightarrow \tilde{Q}, \quad \varphi(\overline{(\beta, f)}) = \phi_\beta \cdot \psi_f.$$

φ está bem definida: se $(\beta, f) \sim (\gamma, g)$, então $\beta \cdot \alpha_g = \gamma \cdot \alpha_f$, donde

$$\phi_\beta \cdot \phi_{\alpha_g} = \phi_{\beta \cdot \alpha_g} = \phi_{\gamma \cdot \alpha_f} = \phi_\gamma \cdot \phi_{\alpha_f}$$

que multiplicada por $\psi_f \cdot \psi_g$ fornece $\phi_\beta \cdot \psi_f = \phi_\gamma \cdot \psi_g$. Como $\tilde{\phi}$ injetora, φ é injetora. Para ver que φ é sobrejetora, seja $\phi \in \tilde{Q}(p)$; defina $\alpha_0 = f_1 = \phi_0$, $f_0 = \mathbf{0}$ e considere

$$m_i = \text{Min}\{m > 0 : \alpha(mp_i), f(mn_i) \text{ não foram ainda definidos}\} \quad (i \geq 1);$$

$$\alpha(m_i p_i) = \phi(p_i/n_i) = f(m_i n_i).$$

Finalmente, para os $n \in \mathbb{Z}$ tais que α_n não recebeu um valor pela definição acima, definimos $\alpha_n = \mathbf{0}$. Analogamente, definimos $f_m = \mathbf{0}$ para todos os $m > 1$ tais que f_m não recebeu um valor. Assim, é claro que $\alpha \in \tilde{\mathbb{Z}}(p)$ e $f \in \tilde{IN}_+(p)$. Por outro lado,

$$(\phi_\alpha \cdot \psi_f)(0) = \bigvee_{n>0} \alpha_0 \& f_n = \alpha_0 \& p = \phi_0;$$

$$(\phi_\alpha \cdot \psi_f)(p_i/n_i) = \bigvee_{m>0} \alpha(mp_i) \& f(mn_i).$$

Se existem m, j tais que $(mp_i, mn_i) = (m_j p_j, m_j n_j)$, então $p_i/n_i = (mp_i)/(mn_i) = (m_j p_j)/(m_j n_j) = p_j/n_j$, donde $j = i$ e $m = m_i$. Logo,

$$(\phi_\alpha \cdot \psi_f)(p_i/n_i) = \alpha(m_i p_i) \& f(m_i n_i) = \phi(p_i/n_i)$$

e então $\varphi(\overline{(\alpha, f)}) = \phi$, portanto φ é bijetora. Por outro lado, considerando em $\hat{\mathcal{Q}}$ a estrutura de prefeixe induzida por θ , temos

$$\begin{aligned} [\varphi(\overline{(\beta, f)}) = \varphi(\overline{(\gamma, g)})] &= [\phi_\beta \cdot \psi_f = \phi_\gamma \cdot \psi_g] \\ &= \bigvee \{p \in (E\beta \& E\gamma) \downarrow : \phi_{\beta|_p} \cdot \psi_{f|_p} = \phi_{\gamma|_p} \cdot \psi_{g|_p}\} \\ &= \bigvee \{p \in (E\beta \& E\gamma) \downarrow : \phi_{\beta|_p} \cdot \phi_{\alpha_{(g|_p)}} = \phi_{\gamma|_p} \cdot \phi_{\alpha_{(f|_p)}}\} \\ &= \bigvee \{p \in (E\beta \& E\gamma) \downarrow : \beta|_p \cdot (\alpha_g)|_p = \gamma|_p \cdot (\alpha_f)|_p\} \\ &= [\beta|_{E\beta \& E\gamma} \cdot (\alpha_g)|_{E\beta \& E\gamma} = \gamma|_{E\beta \& E\gamma} \cdot (\alpha_f)|_{E\beta \& E\gamma}] \\ &= \theta((\beta, f), (\gamma, g)) = [\overline{(\beta, f)} = \overline{(\gamma, g)}]. \end{aligned}$$

Pelo lema 3.3.1(b.2), $\hat{\mathcal{Q}}$ é um feixe isomorfo a $\tilde{\mathcal{Q}}$ via φ . Por definição, temos que $(\overline{(\alpha, f)})|_p = \overline{(\alpha|_p, f|_p)}$.

Finalmente, provamos o seguinte:

Proposição 3.3.10 (1) O objeto $\tilde{\mathbb{Z}}$ é um domínio de integridade em $Sh(Q)$.

(2) O objeto $\tilde{\mathcal{Q}}$ é um anel comutativo em $Sh(Q)$ que satisfaz o axioma $[CORP1]$.

Demonstração: (1) É claro que $\tilde{\mathbb{Z}}$ é um anel comutativo com a soma e o produto definidos anteriormente. Por outro lado, um anel comutativo A é um modelo de $[DI]$ se e somente se, para todo $x, y \in |A|$

$$[x|_{Ex \& Ey} \cdot y|_{Ex \& Ey} = 0] \& ([y = 0] \& Ex \rightarrow_r 0) \leq [x = 0].$$

Em $\tilde{\mathbb{Z}}$, a condição acima tem a forma

$$E\alpha \& E\beta \& (\alpha_0 \vee \beta_0) \& (\beta_0 \& E\alpha \rightarrow_r 0) \leq \alpha_0,$$

a qual é verdadeira para todo $\alpha, \beta \in |\tilde{\mathbb{Z}}|$, pois

$$\begin{aligned} E\alpha \& E\beta \& (\alpha_0 \vee \beta_0) \& (\beta_0 \& E\alpha \rightarrow_r 0) &= \\ &= (E\alpha \& E\beta \& \alpha_0 \& (\beta_0 \& E\alpha \rightarrow_r 0)) \vee (E\alpha \& E\beta \& (\beta_0 \& E\alpha) \& (\beta_0 \& E\alpha \rightarrow_r 0)) \\ &= E\alpha \& E\beta \& \alpha_0 \& (\beta_0 \& E\alpha \rightarrow_r 0) \leq E\alpha \& \alpha_0 = \alpha_0. \end{aligned}$$

(2) É imediato que $\tilde{\mathcal{Q}}$ é um anel comutativo com as operações de soma e produto. Por outro lado, um anel A é um modelo de $[CORP1]$ se e somente se, para todo $x \in |A|$,

$$(*) \quad Ex = [x = 0] \vee \bigvee_{y \in |A|} [x|_{Ex \& Ey} \cdot y|_{Ex \& Ey} = 1] \& [y|_{Ex \& Ey} \cdot x|_{Ex \& Ey} = 1].$$

Pelo lema 3.3.1 (c), basta verificar a condição (*) num conjunto denso de seções; assim, em $\tilde{\mathcal{Q}}$, basta verificar

$$(**) \quad \top = \tilde{r}_0 \vee \bigvee_s (\tilde{r} \cdot \tilde{s})(1)$$

para todo $r \in \mathcal{Q}$, onde $\tilde{r}, \tilde{s} \in \mathcal{Q}$, a cópia densa de $\mathcal{Q}$ em $\tilde{\mathcal{Q}}$. Agora, observe que, se $0 \neq r = p_i/n_i \in \mathcal{Q}$, então

$$s = \begin{cases} n_i/p_i & \text{se } p_i > 0 \\ (-n_i)/(-p_i) & \text{se } p_i < 0 \end{cases}$$

é um elemento de $\mathcal{Q}$, pois n_i e p_i não tem divisores comuns. Logo, temos que $rs = 1$ e

$$\top = \tilde{r}(r) \& \tilde{s}(s) \leq \vee \{ \tilde{r}(r') \& \tilde{s}(s') : r's' = 1 \} = (\tilde{r} \cdot \tilde{s})(1).$$

Além disso, $\top = \tilde{0}_0$, portanto a condição (**) é satisfeita para todo $r \in \mathcal{Q}$, concluindo a prova. $\square$

Módulos Projetivos sobre Anéis Locais em $\text{Sh}(\mathcal{Q})$

O principal resultado deste capítulo é o

Teorema 4.2.2 : *Em $\text{Sh}(\mathcal{Q})$, todo módulo projetivo finitamente gerado sobre um anel local é livre.*

O Teorema 4.2.2 generaliza, para o contexto de feixes sobre quantais RSI, o trabalho de C. Mulvey ([Mul1]), que por sua vez estende para a lógica intuicionista um resultado clássico de I. Kaplansky ([Kap]).

Além da importância que o resultado tem *per se*, devemos destacar que, no caso intuicionista, o resultado tem como corolário um importante teorema de R. Swan, que caracteriza os módulos projetivos finitamente gerados sobre $C(X)$, com X um espaço topológico compacto. Assim, a representação de uma álgebra C^* não comutativa com identidade $\mathcal{A}$ como as seções globais de um feixe sobre $\text{Sh}(\text{Rid } \mathcal{A})$ pode produzir um resultado análogo no contexto não comutativo.

4.1 Definições e Resultados Preliminares

Por simplicidade, identificaremos os nomes dos tipos da linguagem $\mathbb{L}$ com os nomes dos feixes que os interpretam; assim, o tipo destinado a ser interpretado pelo anel local A será denotado por A , o tipo para o módulo P sobre A será escrito como P , etc. Fixado o anel A , indicaremos por $\tilde{I}N$ o objeto $\tilde{I}N|_{EA}$. Começamos definindo uma linguagem $\mathbb{L}$ (que permanecerá fixada ao longo do capítulo) contendo os seguintes tipos:

$$\mathcal{T} = \{A, P, \tilde{I}N, A^{\tilde{I}N}, P^{\tilde{I}N}, (A^{\tilde{I}N})^{\tilde{I}N}, (P^{\tilde{I}N})^{\tilde{I}N}, ((A^{\tilde{I}N})^{\tilde{I}N})^{\tilde{I}N}, (A^{\tilde{I}N})^{(A^{\tilde{I}N})}, P^P, (A^{\tilde{I}N})^P, P^{(A^{\tilde{I}N})}\}.$$

Para $A, B \in \mathcal{T}$ tais que $B^A \in \mathcal{T}$, vamos incluir em $\mathbb{L}$ a função de cálculo num ponto $\text{ev} : B^A \times A \rightarrow B$ de maneira que, se ϕ e x são variáveis do tipo B^A e A , respectivamente, o termo $\text{ev}(\phi, x)$ será denotado por $\phi(x)$; se $A = \tilde{I}N$, então poderemos escrever ϕ_i para denotar $\phi(i)$, enquanto a_{ij} denotará $a(i)(j)$ para a do tipo $(B^{\tilde{I}N})^{\tilde{I}N}$.

Indicaremos por Mod a teoria consistindo dos seguintes axiomas :

- Os axiomas da aritmética para $\tilde{N}$;
- O axioma de indução;
- Os axiomas de anel para A e de A -módulo (à esquerda) para P ;
- Os axiomas de definição das operações nos módulos $M^{\tilde{N}}$ (i.e., ponto a ponto) para $M \in \mathcal{M}$, com

$$\mathcal{M} = \{A, A^{\tilde{N}}, (A^{\tilde{N}})^{\tilde{N}}, P, P^{\tilde{N}}\}.$$

Se $\mathcal{I}$ é uma interpretação, $\mathcal{I} \models Mod$ significa que $\mathcal{I}$ é modelo da teoria Mod .

Definimos em $\tilde{N} \times \tilde{N}$ a relação de ordem $f \leq g$ dada pela fórmula

$$n \leq m \equiv_{def} (\exists k)(n + k = m).$$

Analogamente, definimos $f < g$ pela fórmula

$$n < m \equiv_{def} (\exists k)(\neg(k = 0) \wedge (n + k = m)).$$

Lema 4.1.1 : *A relação $R(n, m) \equiv_{def} n \leq m$ é uma relação de ordem, i.e., R é reflexiva, antisimétrica e transitiva. A relação $S(n, m) \equiv_{def} n < m$ é uma relação de ordem estrita, i.e., S é assimétrica e transitiva. Além disso, para $f, g \in \tilde{N}$ temos*

a) $f \leq g$ sse $Ef = Eg$ e existe h tal que $Ef = Eh$ e $f + h = g$. Em particular, $\tilde{n} \leq \tilde{m}$ sse $n \leq m$.

b) $f < g$ sse $Ef = Eg$ e existe h tal que $Ef = Eh$, $h \neq \tilde{0}_{Ef}$ e $f + h = g$. Em particular, $\tilde{n} < \tilde{m}$ sse $n < m$.

Demonstração: Lembrando que $\tilde{N}$ denota o feixe $\tilde{N}_{|EA}$, temos que

$$f \leq g \text{ sse } Ef = Eg \leq \bigvee_h EA \& [f_{|Ef \& Eh} + h_{|Ef \& Eh} = g].$$

Seja $R \subseteq \tilde{N}^2$ o feixe correspondente à interpretação de $R(n, m)$; como $(\tilde{n}, \tilde{n}) \in |R|$ para todo n , temos $ER = EA$. Considere a função característica $F : |R| \times |\tilde{N}| \rightarrow Q$ dada por $F((f, g), h) = EA \& [f_{|Ef \& Eh} + h_{|Ef \& Eh} = g]$. Pelo lema 3.3.6, F é uma relação funcional, i.e., se R_F é o feixe associado com F , temos o seguinte:

$$((f, g), h), ((f, g), h') \in |R_F| \text{ implica } h = h'; \quad ER \& E(f, g) = \bigvee_h F((f, g), h).$$

Portanto, pela prova da proposição 3.1.5, temos que $(f, g) \in |R|$ sse existe um único $h \in |\tilde{N}|$ tal que $Eh = Ef = Eg$ e $f + h = g$. Por outro lado, é fácil provar que $h + h' = \tilde{0}_{|Eh}$ implica que $h = h' = \tilde{0}_{|Eh}$. É agora imediato que a conclusão vale para R . A prova para a relação S é similar, utilizando a função característica

$$F_1 : |S| \times |\tilde{N}| \rightarrow Q, \quad F_1((f, g), h) = (EA \& Ef \& Eh \& (EA \& Ef \& h_0 \rightarrow_r 0)) \wedge F((f, g), h). \quad \square$$

Se B é um tipo, então $B^{\tilde{N}}$ é o tipo das sequências em B . Assim, uma sequência num feixe B é um morfismo $f : \tilde{N}_{|EB \& p} \rightarrow B$, sendo então caracterizada pela sequência $(f(\tilde{n}_{|EB \& p}))_{n \in \mathbb{N}}$, isto é, as sequências em B correspondem com sequências no sentido usual. Observe que, para todo feixe B e $x \in |B|$ fixo, a proposição 1.1.23 garante que existe um único morfismo

$$f : \tilde{N}_{|EB \& Ex} \rightarrow B \quad \text{tal que} \quad f(\tilde{n}_{|EB \& Ex}) = x_{|EB} \quad \forall n \in \mathbb{N};$$

assim, $(f, Ex) \in B^{\tilde{N}_{|EB}}(Ex)$. Segue que

$$EB^{\tilde{N}_{|EB}} = EB. \quad (*)$$

Antes das definições formais de módulo projetivo finitamente gerado em $Sh(Q)$, iremos desenvolver algumas propriedades algébricas fundamentais de cálculo em módulos em $Sh(Q)$. Para evitar complicações desnecessárias, vamos trabalhar com hipóteses adicionais sobre os extents dos tipos envolvidos. Apresentaremos agora uma justificativa heurística para estas hipóteses, que estão verificadas pela conceituação rigorosa dada na definição 4.2.1.

Se A é um anel, um módulo (à esquerda) P sobre A é **projetivo** se é somando direto de um A -módulo livre, isto é, se existe um conjunto I , juntamente com homomorfismos de A -módulos

$$A^I \xrightleftharpoons[\psi]{\phi} P,$$

tal que $\phi \circ \psi = Id_P$. P é finitamente gerado quando I é finito. Assim, mesmo no caso de $Sh(Q)$, podemos supor que $EA = EP$; a existência dos morfismos

$$\phi : A^{\tilde{N}_{|EA}} \rightarrow P, \quad \psi : P \rightarrow A^{\tilde{N}_{|EA}},$$

garante, juntamente com a fórmula (*) acima, que $EA = EA^{\tilde{N}_{|EA}} = EP$ e $E((A^{\tilde{N}})^P) = E(P^{(A^{\tilde{N}})}) = EA = EP$. Desta maneira, temos que

$$E(A^{\tilde{N}}) = E((A^{\tilde{N}})^{\tilde{N}}) = E(((A^{\tilde{N}})^{\tilde{N}})^{\tilde{N}}) = E(P^{\tilde{N}}) = E((P^{\tilde{N}})^{\tilde{N}}) = EA = EP.$$

Além disso, os morfismos identidade implicam que $E((A^{\tilde{N}})^{(A^{\tilde{N}})}) = E(P^P) = EA = EP$.

Uma consequência importante destas hipóteses naturais em relação ao problema que desejamos atacar é que **todos os tipos considerados têm o mesmo extent**. Consequentemente, podemos utilizar em nossas deduções formais o cálculo ($QPC1$), correspondente a (QPC) quando todos os tipos tem mesmo extent.

A expressão EA denotará toda fórmula da forma $(\exists x)Ex$, $x \in \mathcal{V}$; note que temos $\phi \sim \phi \otimes EA$ para toda fórmula ϕ . Por outro lado, as variáveis do tipo B^A satisfazem a seguinte propriedade:

Lema 4.1.2 : *Sejam v, w variáveis do tipo B^A , para A, B tipos tais que $B^A \in \mathcal{T}$.*

(a) *Para toda interpretação $\mathcal{I}$, temos que*

$$\llbracket (v = w) \rrbracket_{(v, w)} \leq \llbracket (\forall x)(v(x) = w(x)) \rrbracket_{(v, w)}.$$

(b) Se $\mathcal{I}$ é uma interpretação tal que existe $S \subseteq A(EA)$ denso em A , então

$$\llbracket (v = w) \rrbracket_{(v,w)} = \llbracket (\forall x)(v(x) = w(x)) \rrbracket_{(v,w)}.$$

Demonstração: (a) Seja $\mathcal{I}$ uma interpretação. Como $E(B^A) = EA$, temos que

$$\begin{aligned} \llbracket (v = w) \rrbracket_{(v,w)}((f, p), (g, q)) &= EA \& [(f, p) = (g, q)] \\ &= EA \& \forall \{r \in (p \& q) \downarrow : f(x) = g(x) \ \forall x \in A_{|EA \& r} \}, \end{aligned}$$

enquanto que

$$\llbracket (\forall x)(v(x) = w(x)) \rrbracket_{(v,w)}((f, p), (g, q)) = (EA \wedge \bigwedge_{x \in |A|} (Ex \rightarrow_l [f(x_{|EA \& p \& q}) = g(x_{|EA \& p \& q})])) \& p \& q.$$

Seja $r \in (p \& q) \downarrow$ tal que $f(x) = g(x)$ em $A_{|EA \& r}$ e considere $s = EA \& r \& Ex$, para $x \in |A|$ fixo. De $x_{|EA \& r \& Ex} = x_{|EA \& r} \in |A_{|EA \& r}|$, obtemos

$$f(x|_s) = f(x_{|EA \& r \& Ex}) = f(x_{|EA \& r}) = g(x_{|EA \& r}) = g(x|_s)$$

e então

$$s \leq \forall \{t \in (EA \& p \& q \& Ex) \downarrow : f(x|_t) = g(x|_t)\} = [f(x_{|EA \& p \& q}) = g(x_{|EA \& p \& q})].$$

Assim, provamos que $EA \& r \leq \bigwedge_{x \in |A|} (Ex \rightarrow_l [f(x_{|EA \& p \& q}) = g(x_{|EA \& p \& q})])$, donde segue-se o resultado.

(b) Seja $S \subseteq A(EA)$ denso em A . Da propriedade geral

$$(a \wedge \bigwedge_i (a \rightarrow_l a_i)) \& b \leq a \& \bigwedge_i (a \rightarrow_l a_i) \& a \& b = a \& b \& (a \rightarrow_l (\bigwedge_i a_i)) \& a \leq a \& b \& \bigwedge_i a_i$$

para $a, b, a_i \in Q$ ($i \in I$), da densidade de S em A e de $Ex = EA$, para todo $x \in S$, deduzimos que

$$\begin{aligned} \llbracket (\forall x)(v(x) = w(x)) \rrbracket_{(v,w)}((f, p), (g, q)) &= (EA \wedge \bigwedge_{x \in S} (EA \rightarrow_l [a_x = b_x])) \& p \& q \\ &\leq EA \& p \& q \& \bigwedge_{x \in S} [a_x = b_x] = EA \& t, \end{aligned}$$

onde $t = p \& q \& \bigwedge_{x \in S} [a_x = b_x]$, $a_x = f(x_{|EA \& p \& q})$ e $b_x = g(x_{|EA \& p \& q})$ para todo $x \in S$. Logo, $t \in (p \& q) \downarrow$ é tal que $t \leq p \& q \& [a_x = b_x]$ para todo $x \in S$; portanto

$$t = t \& p \& q \& [a_x = b_x] = t \& [a_x = b_x]$$

para todo $x \in S$, pois $t = t \& p \& q$. Assim,

$$f(x_{|EA \& t}) = ((a_x)_{|[a_x = b_x]})_{|EA \& t} = ((b_x)_{|[a_x = b_x]})_{|EA \& t} = g(x_{|EA \& t})$$

para todo $x \in S$. Como $S_{|EA \& u} = \{x_{|EA \& u} : x \in S\}$ é denso em $A_{|EA \& u}$ para todo u , temos

$$\begin{aligned} \llbracket (v = w) \rrbracket_{(v,w)}((f, p), (g, q)) &= EA \& \forall \{u \in (p \& q) \downarrow : f(x_{|EA \& u}) = g(x_{|EA \& u}) \ \forall x \in S\} \\ &\geq EA \& t \geq \llbracket (\forall x)(v(x) = w(x)) \rrbracket_{(v,w)}((f, p), (g, q)) \end{aligned}$$

donde segue-se o resultado. $\square$

Corolário 4.1.3 : Para toda interpretação tal que $\mathcal{I} \models \text{Mod}$,

$$\llbracket (a = b) \rrbracket_{(a,b)} = \llbracket (\forall n)(a_n = b_n) \rrbracket_{(a,b)}$$

onde a, b variáveis do tipo $B^{\tilde{N}}$, com B um tipo tal que $B^{\tilde{N}} \in \mathcal{T}$.

Demonstração: Aplicamos o lema 4.1.2(b), com $S = \{\tilde{n}_{|EA} : n \in \mathbb{N}\} \subseteq \tilde{N}_{|EA}(EA)$. $\square$

O corolário anterior permite a incorporação na teoria dos axiomas-sequentes

$$[IG1] \quad (a = b) \vdash (\forall n)(a_n = b_n), \quad [IG2] \quad (\forall n)(a_n = b_n) \vdash (a = b),$$

para a, b do tipo $M^{\tilde{N}}$, com $M \in \mathcal{M}$. Para simplificar a notação, usaremos símbolos de somatórias finitas para sequências num módulo $M \in \mathcal{M}$. Como $EA = EM$ para todo $M \in \mathcal{M}$, o seguinte lema garante a existência dos morfismos correspondentes:

Lema 4.1.4 : Seja M um módulo em $Sh(Q)$. Então, existe um único morfismo

$$\varphi : M^{\tilde{N}_{|EM}} \times \tilde{N}_{|EM} \times \tilde{N}_{|EM} \longrightarrow M \text{ tal que}$$

$$\varphi((f, p), \tilde{n}_{|p}, \tilde{m}_{|p}) = 0_{|p} \quad \text{se } n \geq m, (f, p) \in |M^{\tilde{N}_{|EM}}|,$$

$$\varphi((f, p), \tilde{n}_{|p}, (\tilde{m} + \tilde{1})_{|p}) = f(\tilde{n}_{|p}) + \cdots + f(\tilde{m}_{|p}) \quad \text{se } n \leq m, (f, p) \in |M^{\tilde{N}_{|EM}}|.$$

Para $((f, p), a, b) \in |M^{\tilde{N}_{|EM}} \times \tilde{N}_{|EM} \times \tilde{N}_{|EM}|$, escreveremos $\varphi((f, p), a, b) = \sum_{i=a}^b f_i$.

Demonstração: Dado que, para todo feixe B , o conjunto de seções

$$S = \{(a, \tilde{n}_{|Ea}, \tilde{m}_{|Ea}) : a \in |B|, n, m \in \mathbb{N}\} \subseteq |B \times \tilde{N}_{|EB} \times \tilde{N}_{|EB}|$$

é denso, basta provar, pela proposição 1.1.23(b), que φ satisfaz $[MOR1]$ e $[MOR2]$ sobre S . A validade da propriedade $[MOR1]$ é imediata a partir da definição. Sejam então $x = ((f, p), \tilde{n}_{|p}, \tilde{m}_{|p})$ e $y = ((g, q), \tilde{n}'_{|q}, \tilde{m}'_{|q})$ em S . Como $[x = y] = [(f, p) = (g, q)]$ se $(n, m) = (n', m')$, e 0 caso contrário, podemos assumir que $n = n'$ e $m = m'$. Assim,

$$[x = y] = \bigvee \{r \in (p \& q) \downarrow : f(\tilde{k}_{|r}) = g(\tilde{k}_{|r}) \quad \forall k \in \mathbb{N}\}$$

enquanto que, se $n < m$, temos

$$[\varphi(x) = \varphi(y)] = \bigvee \{r \in (p \& q) \downarrow : f(\tilde{n}_{|r}) + \cdots + f((m-1)_{|r}) = g(\tilde{n}_{|r}) + \cdots + g((m-1)_{|r})\}$$

e $[\varphi(x) = \varphi(y)] = \bigvee \{r \in (p \& q) \downarrow : 0_{|r} = 0_{|r}\} = p \& q$, caso $n \geq m$. Segue imediatamente das definições que $[x = y] \leq [\varphi(x) = \varphi(y)]$, como desejado. $\square$

Para $M \in \mathcal{M}$, definimos o símbolo de função $\text{sum} : M^{\tilde{N}} \times \tilde{N} \times \tilde{N} \longrightarrow M$, pelos axiomas

$$[SUM 1] \quad \vdash \forall n \forall m (m \leq n \rightarrow (\text{sum}(a, n, m) = 0))$$

$$[SUM 2] \quad \vdash \forall n \forall m (n \leq m \rightarrow (\text{sum}(a, n, m+1) = \text{sum}(a, n, m) + a(m))).$$

Lema 4.1.5 : Se $\mathcal{I} \models \text{Mod}$, então $\mathcal{I} \models [\text{SUM } i] \ (i = 1, 2)$ sse $\text{sum}^{\mathcal{I}}$ coincide com o morfismo de somatória definido em 4.1.4.

Demonstração: Basta provar que $\text{sum}^{\mathcal{I}}$ coincide com o morfismo φ do lema 4.1.4 no conjunto denso S . Mas isto é imediato a partir da definição de interpretação, das propriedades de $\tilde{N}$ e da propriedade $[\text{EXT}]$. $\square$

Uma sequência a num módulo M é finita se satisfizer a fórmula $\forall m (n \leq m \rightarrow (a_m = 0))$, para algum $n \in \tilde{N}$. Se a é do tipo $A^{\tilde{N}}$ e z é do tipo $M^{\tilde{N}}$, onde $M \in \mathcal{M}$, então $a.z$ é do tipo $M^{\tilde{N}}$; portanto $\text{sum}(a.z, n, m)$ é do tipo M , representando $\sum_{i=n}^m a_i z_i$. O produto $\cdot : A^{\tilde{N}} \times M^{\tilde{N}} \rightarrow M^{\tilde{N}}$ acima mencionado é dado pelo axioma

$$[\text{PROD}] \quad \vdash (\forall n)((a.z)(n) = a(n).z(n))$$

o qual é validado pelo seguinte

Lema 4.1.6 : Se A é um anel e M um módulo em $\text{Sh}(Q)$ tal que $EA = EM$, então existe um único morfismo

$$\varphi : A^{\tilde{N}|EA} \times M^{\tilde{N}|EA} \rightarrow M^{\tilde{N}|EA} \quad \text{tal que} \quad \varphi((a, p), (f, p))(\tilde{n}|_p) = a(\tilde{n}|_p).f(\tilde{n}|_p) \quad \forall n \in \mathbb{N}.$$

Demonstração: Por 1.1.23(b) e pelo teorema 1.1.22, basta definir

$$\varphi_0 : S \rightarrow M, \quad \varphi_0((a, p), (f, p), \tilde{n}|_p) = a(\tilde{n}|_p).f(\tilde{n}|_p) \quad \forall n \in \mathbb{N}$$

satisfazendo $[\text{MOR1}]$ e $[\text{MOR2}]$, pois

$$S = \{(x, \tilde{n}|_{Ex}) : x \in |A^{\tilde{N}|EA} \times M^{\tilde{N}|EA}|, n \in \mathbb{N}\} \subseteq |A^{\tilde{N}|EA} \times M^{\tilde{N}|EA} \times \tilde{N}|_{EA}|$$

é denso. A verificação da propriedade $[\text{MOR1}]$ é imediata. Sejam $x = ((a, p), (f, p), \tilde{n}|_p)$ e $y = ((b, q), (g, q), \tilde{n}|_q)$ em S (o caso em que as coordenadas em $\tilde{N}$ de x e y diferem é trivial). Então,

$$[x = y] = \bigvee \{r \& s : r, s \in (p \& q) \downarrow, a(\tilde{m}|_r) = b(\tilde{m}|_s), f(\tilde{m}|_r) = g(\tilde{m}|_s) \quad \forall m \in \mathbb{N}\}.$$

Assim, $r \& s = s \& r \in (p \& q) \downarrow$ é tal que $a(\tilde{n}|_{r \& s}) = b(\tilde{n}|_{r \& s})$ e $f(\tilde{n}|_{r \& s}) = g(\tilde{n}|_{r \& s})$; portanto, $a(\tilde{n}|_{r \& s}).f(\tilde{n}|_{r \& s}) = b(\tilde{n}|_{r \& s}).g(\tilde{n}|_{r \& s})$ e então

$$r \& s \leq \bigvee \{t \in (p \& q) \downarrow : a(\tilde{n}|_t).f(\tilde{n}|_t) = b(\tilde{n}|_t).g(\tilde{n}|_t)\} = [a(\tilde{n}|_p).f(\tilde{n}|_p) = b(\tilde{n}|_q).g(\tilde{n}|_q)],$$

completando a prova. $\square$

O axioma $[\text{PROD}]$ de fato descreve o produto 4.1.6 nos modelos :

Lema 4.1.7 : Se $\mathcal{I} \models \text{Mod}$ e $M \in \mathcal{M}$, então $\mathcal{I} \models [\text{PROD}]$ sse a interpretação em $\mathcal{I}$ do produto coincide com o morfismo definido em 4.1.6.

Para poder somar uma sequência $z \in (M^{\tilde{N}})^{\tilde{N}}$ em relação a um índice específico, precisamos de uma operação de “transposição”, de maneira que $\sum_{i=n}^m z_{ij}$ seja o termo $\text{sum}(z_j^t, n, m)$, i.e., $\sum_{i=n}^m z_{ji}^t$, onde $z^t \in (M^{\tilde{N}})^{\tilde{N}}$ denota a transposta de z . Isto é implementado por uma função $t : (M^{\tilde{N}})^{\tilde{N}} \rightarrow (M^{\tilde{N}})^{\tilde{N}}$ definida por

$$\vdash (\forall z \in (M^{\tilde{N}})^{\tilde{N}})(\forall i \in \tilde{N})(\forall j \in \tilde{N})(t(z)(i)(j) = z(j)(i)).$$

A interpretação de t é a óbvia e é claro que existe o morfismo correspondente nos modelos. Da mesma maneira, são utilizados outros produtos $(\cdot : A^{\tilde{N}} \times M \rightarrow M^{\tilde{N}}, (a.v)_n = a_n.v, \text{ etc.})$ para, formalmente, executar passos algébricos como os seguintes:

$$\sum_{j=0}^k \left(\sum_{i=0}^k a_i d_{ji} \right) \sum_{h=0}^n c_{hj} u_h = \sum_{i=0}^k a_i \left(\sum_{h=0}^n \left(\sum_{j=0}^k d_{ji} c_{hj} \right) u_h \right) + \sum_{h=k}^n \left(\sum_{i=0}^k \left(\sum_{j=0}^k a_i d_{ji} c_{hj} \right) \right) u_h$$

onde $c, d \in (A^{\tilde{N}})^{\tilde{N}}$, $a \in A^{\tilde{N}}$, e $u \in M^{\tilde{N}}$. A validade da fórmula acima envolve a validade de propriedades básicas das somatórias, as quais podem ser provadas facilmente na teoria dada. Como um exemplo, provaremos que a ordem das somatórias pode ser trocada.

Lema 4.1.8 : *Seja a variável do tipo $M^{\tilde{N}}$, M um módulo. O seguinte sequente é provável na teoria Mod :*

$$(\forall j)(a_j = 0) \vdash (\forall k)(\text{sum}(a, 0, k) = 0).$$

Demonstração: Por indução (interna) em k . Seja $\phi(k) \equiv_{def} (\text{sum}(a, 0, k) = 0)$; pela definição de somatória,

$$\frac{(\forall j)(a_j = 0) \vdash EA \quad EA \vdash \phi(0)}{(\forall j)(a_j = 0) \vdash \phi(0)}.$$

Por outro lado, por [E6], obtemos

$$\frac{\frac{\phi(k) \vdash \phi(k) \quad (\forall j)(a_j = 0) \vdash (a_k = 0)}{\phi(k), (\forall j)(a_j = 0) \vdash \phi(k) \otimes (a_k = 0)} \quad \phi(k) \otimes (a_k = 0) \vdash (\text{sum}(a, 0, k) + a_k = 0)}{\phi(k), (\forall j)(a_j = 0) \vdash (\text{sum}(a, 0, k) + a_k = 0)}$$

Além disso, como $EA \vdash (\text{sum}(a, 0, k+1) = \text{sum}(a, 0, k) + a_k)$, então

$$\begin{aligned} & \phi(k), (\forall j)(a_j = 0), EA \vdash (0 = \text{sum}(a, 0, k) + a_k) \otimes (\text{sum}(a, 0, k) + a_k = \text{sum}(a, 0, k+1)), \\ & (0 = \text{sum}(a, 0, k) + a_k) \otimes (\text{sum}(a, 0, k) + a_k = \text{sum}(a, 0, k+1)) \vdash \phi(k+1), \end{aligned}$$

e então deduzimos $\phi(k), (\forall j)(a_j = 0) \vdash \phi(k+1)$ e em seguida $(\forall j)(a_j = 0) \vdash (\forall k)(\phi(k) \rightarrow \phi(k+1))$. Isto prova $(\forall j)(a_j = 0) \vdash \phi(0) \otimes (\forall k)(\phi(k) \rightarrow \phi(k+1))$; o resultado é agora consequência do axioma de indução, pois ϕ não tem disjunções. $\square$

Lema 4.1.9 : *Seja M um módulo e a, b, c variáveis de tipo $(M^{\tilde{N}})^{\tilde{N}}$. Sejam i, j, k, n variáveis de tipo $\tilde{N}$. Considere as seguintes fórmulas :*

$$\alpha \equiv_{def} (\forall i)(\forall k)(b_{ki} = \mathbf{sum}(a_i, 0, k)), \quad \beta \equiv_{def} (\forall n)(\forall j)(c_{nj} = \mathbf{sum}(a_j^t, 0, n))$$

$$\phi(n) \equiv_{def} (\forall k)(\mathbf{sum}(b_k, 0, n) = \mathbf{sum}(c_n, 0, k)).$$

Então, o sequente $\alpha, \beta \vdash (\forall n)\phi(n)$ é provável em Mod . Portanto

$$\vdash (\forall a)(\forall b)(\forall c)(\alpha \otimes \beta \multimap (\forall n)\phi(n))$$

é provável em Mod , i.e., $\sum_{i=0}^n (\sum_{j=0}^k a_{ij}) = \sum_{j=0}^k (\sum_{i=0}^n a_{ij})$ para todo a .

Demonstração: Por indução (interna) em n . Pela definição de $\mathbf{sum}$, temos

$$EA \vdash \mathbf{sum}(b_k, 0, 0) = 0, \quad EA \vdash \mathbf{sum}(a_j^t, 0, 0) = 0,$$

para todo k e para todo j ; o lema 4.1.8 implica

$$\frac{\beta \vdash (\forall j)(c_{0j} = 0)}{\beta \vdash (\forall k)(\mathbf{sum}(c_0, 0, k) = 0)},$$

onde provamos $\alpha, \beta \vdash \phi(0)$. Por outro lado, temos

$$(1) \quad \alpha \vdash \mathbf{sum}(b_k, 0, n+1) = \mathbf{sum}(b_k, 0, n) + \mathbf{sum}(a_n, 0, k)$$

para todo k , enquanto que, para todo j , obtemos

$$\beta \vdash c_{n+1j} = (c_n + a_n)(j).$$

Consequentemente, para todo k , vale

$$(2) \quad \beta \vdash \mathbf{sum}(c_{n+1}, 0, k) = \mathbf{sum}(c_n, 0, k) + \mathbf{sum}(a_n, 0, k).$$

De (1) e (2), deduzimos

$$\phi(n), \alpha, \beta \vdash \phi(n+1)$$

onde

$$\alpha, \beta \vdash (\forall n)(\phi(n) \multimap \phi(n+1))$$

e então

$$\alpha, \beta \vdash \phi(0) \otimes (\forall n)(\phi(n) \multimap \phi(n+1)),$$

finalizando a prova pelo axioma de indução, pois ϕ não tem disjunções. $\square$

Para todo $n \in \tilde{N}$, o módulo A^n é definido pela fórmula $a \in A^n \equiv_{def} \forall m(n \leq m \multimap (a_m = 0_A))$, i.e., A^n consiste das sequências finitas em A de comprimento n . Se n é “standard”, então podemos identificar A^n com $\prod_{i=1}^n A$, como provaremos abaixo.

Lema 4.1.10 : Para uma interpretação $\mathcal{I}$ satisfazendo Mod , suponha que

$$\llbracket a \in A^n \rrbracket_{(a,n;0_A)} = \llbracket \forall m(n \leq m \multimap (a_m = 0_A)) \rrbracket_{(a,n;0_A)} = F : |A^{\tilde{N}|_{EA}}| \times |\tilde{N}|_{EA} \longrightarrow Q.$$

Então, para $n \geq 0$,

$$G_n : |A^{\tilde{N}|_{EA}}| \longrightarrow Q, \quad G_n((f, p)) = F((f, p), \tilde{n}|_p)$$

é uma função característica, tal que

i) Se $n > 0$, o sub-feixe $S_n \subseteq A^{\tilde{N}|_{EA}}$ associado é

$$S_n = \{(f, p) \in |A^{\tilde{N}|_{EA}}| : f(\tilde{m}|_p) = 0|_p \ \forall m \geq n\} \simeq \prod_{i=1}^n A.$$

Além disso, S_n é também o sub-feixe associado a $\llbracket a \in A^{s^n(0)} \rrbracket_{(a; 0_A; 0)}$.

ii) Se $n = 0$, então $|S_0| \simeq \{0|_p : p \leq EA\}$ é o sub-feixe associado com $\llbracket a \in A^0 \rrbracket_{(a; 0_A; 0)}$.

Demonstração: Seja $T \subseteq A^{\tilde{N}|_{EA}} \times \tilde{N}|_{EA}$ o sub-feixe associado a F . Para todo $x = ((f, p), \tilde{n}|_p) \in |A^{\tilde{N}|_{EA}} \times \tilde{N}|_{EA}|$, temos que $x \in |T|$ sse

$$p \leq \bigwedge_{m \in \mathbb{N}} (EA \rightarrow_l ((\bigvee_{r \in \mathbb{N}} EA \& [(n+r)|_{EA \& p} = \tilde{m}]) \rightarrow_r EA \& [f(\tilde{m}|_{EA \& p}) = 0])),$$

sse, para todo $m \in \mathbb{N}$,

$$\bigvee_r [(n+r)|_p = \tilde{m}|_p] \leq [f(\tilde{m}|_p) = 0|_p].$$

Assim, observando que $\bigvee_r [(n+r)|_p = \tilde{m}|_p] = p$ sse $m \geq n$ e $\bigvee_r [(n+r)|_p = \tilde{m}|_p] = \mathbf{0}$ sse $m < n$, temos que, para todo $m \geq n$,

$$p = [f(\tilde{m}|_p) = 0|_p] = Ef(\tilde{m}|_p) = E(0|_p)$$

donde, por $[EXT]$, obtemos que $f(\tilde{m}|_p) = 0|_p$. Reciprocamente, $f(\tilde{m}|_p) = 0|_p$ para todo $m \geq n$ implica que $((f, p), \tilde{n}|_p) \in |T|$ e então

$$|T| = \{((f, p), \tilde{n}|_p) : f(\tilde{m}|_p) = 0|_p \ \forall m \geq n\}.$$

Em particular, $|S_n| = \{(f, p) \in |A^{\tilde{N}|_{EA}}| : f(\tilde{m}|_p) = 0|_p \ \forall m \geq n\}$. Considere agora $n > 0$ e

$$\varphi : \prod_{i=1}^n A \longrightarrow A^{\tilde{N}|_{EA}}, \quad \varphi(a_0, \dots, a_{n-1}) = (f, p) \quad \text{com } p = Ea_0 = \dots = Ea_{n-1},$$

onde $f : \tilde{N}|_{EA \& p} \longrightarrow A$ é o único morfismo satisfazendo

$$f(\tilde{m}|_{EA \& p}) = a_m|_{EA} \text{ se } m < n, \quad f(\tilde{m}|_{EA \& p}) = 0|_{EA \& p} \text{ se } m \geq n.$$

A existência de f é garantida pela proposição 1.1.23 (b), pois $\mathcal{N}|_{EA \& p} = \{\tilde{m}|_{EA \& p} : m \in \mathbb{N}\}$ é uma cópia densa de $\tilde{N}$ em $\tilde{N}|_{EA \& p}$. Vamos provar que φ é injetora. Com efeito, dados $\vec{a}, \vec{b} \in |\prod_{i=1}^n A|$, então $\varphi(\vec{a}) = (f, p) = \varphi(\vec{b})$ implica $a_m|_{EA} = b_m|_{EA}$ para todo $m < n$, donde

$$a_m = (a_m|_{EA})|_p = (b_m|_{EA})|_p = b_m \quad \forall m < n$$

e então $\vec{a} = \vec{b}$. Pelos lemas 1.1.15 e 3.3.1 (b.2), a aplicação $\varphi : \prod_{i=1}^n A \longrightarrow \varphi(\prod_{i=1}^n A)$ é um isomorfismo de feixes, sendo fácil verificar que

$$|\varphi(\prod_{i=1}^n A)| = \{(f, p) : f(\tilde{m}|_p) = 0|_p \ \forall m \geq n\} = |S_n|.$$

Está claro que S_n é o sub-feixe associado à interpretação da fórmula $a \in A^{s^n(0)}$, para $n > 0$. Se $n = 0$, então

$$|S_0| = \{(f, p) : f(\tilde{m}_{|p}) = 0_{|p} \ \forall m \geq 0\} \simeq \{0_{|p} : p \leq EA\}$$

via $(f, p) \mapsto 0_{|p}$, onde S_0 é o objeto definido pela interpretação da fórmula $a \in A^0$. $\square$

Observe que $\varphi_{|(\prod_{i=1}^n A)(p)} : (\prod_{i=1}^n A)(p) \rightarrow S_n(p)$ é um isomorfismo de $A(p)$ -módulos para todo $p \leq EA$.

A identificação de S_n com $\prod_{i=1}^n A$ do lema 4.1.10 é um caso particular da identificação de $B^{\tilde{IN}_{|EB}}$ com $\prod_{n \in IN} B$ para todo feixe B , como mostra o

Lema 4.1.11 : *Seja B um feixe. Então, a aplicação*

$$\psi : B^{\tilde{IN}_{|EB}} \rightarrow \prod_{n \in IN} B, \quad \psi((f, p)) = (f(\tilde{n}_{|p}))_{n \in IN}$$

é um isomorfismo de feixes extendendo a identificação de S_n com $\prod_{i=1}^n B$ do lema 4.1.10.

Demonstração: Como f é um morfismo, temos $Ef(\tilde{n}_{|p}) = E\tilde{n}_{|p} = p = E(f, p)$ para todo n , mostrando que ψ está bem definida. Se $\psi((f, p)) = \psi((g, q))$, então, não só $p = q$, como também f e g coincidem num conjunto denso; assim, $f = g$ e ψ é injetora. Por outro lado, por 1.1.23(b), uma sequência $x = (x_n)_{n \in IN}$ em $\prod_{n \in IN} B$ determina um único morfismo $f : \tilde{IN}_{|EB \& Ex} \rightarrow B$ satisfazendo $f(\tilde{n}_{|EB \& Ex}) = x_{n|EB}$, tal que $\psi((f, Ex)) = x$. Pelo lema 3.3.1 (a.1), ψ é um isomorfismo que estende o isomorfismo descrito em 4.1.10. $\square$

Dizemos que uma sequência finita y do tipo $M^{\tilde{IN}}$ gera o módulo M se satisfaz

$$gera_M(y, n) \equiv_{def} (\forall b \in M)(\exists a \in A^{\tilde{IN}})(\sum_{i=0}^n a_i y_i = b),$$

onde n é o comprimento de y . A sequência y é linearmente independente se satisfizer

$$li_M(y, n) \equiv_{def} (\forall a \in A^{\tilde{IN}})((\sum_{i=0}^n a_i y_i = 0) \rightarrow \forall i (i < n \rightarrow (a_i = 0))).$$

Logo, y é uma base finita de M se é linearmente independente e gera M , i.e., satisfaz a fórmula

$$base_M(y, n) \equiv_{def} gera_M(y, n) \wedge li_M(y, n).$$

Dizemos que M é finitamente gerado se satisfizer

$$FG_M \equiv_{def} (\exists n \in \tilde{IN})(\exists y \in M^{\tilde{IN}}) gera_M(y, n),$$

e M admite uma base finita, ou é livre com base finita se satisfizer

$$FBAS_M \equiv_{def} (\exists n \in \tilde{IN})(\exists y \in M^{\tilde{IN}}) base_M(y, n).$$

Poderemos indicar por $P = \langle x_i : 1 \leq i \leq n-1 \rangle$ ou ainda $P = \langle x_1, \dots, x_{n-1} \rangle$, que P satisfaz $gera_P(x, n) \wedge (x_0 = 0)$. A notação $P = \langle \langle x_i : i \leq n-1 \rangle \rangle$ indica que $base_P(x, n)$. Para uma fórmula $M(x, \vec{x})$, com x do tipo P , dizemos que $M(x, \vec{x})$ é um sub-módulo de P se satisfaz os axiomas de módulo para cada sequência $\vec{x}$ de parâmetros, i.e., os seguintes

$$\begin{aligned} EA \vdash M(0_P, \vec{x}); \quad & M(x, \vec{x}), M(y, \vec{x}) \vdash M(x+y, \vec{x}); \\ M(x, \vec{x}) \vdash M(j(x), \vec{x}); \quad & M(x, \vec{x}) \vdash M(a \star x, \vec{x}) \end{aligned}$$

são prováveis. Podemos adaptar as definições anteriores para um sub-módulo $M(x, \vec{x})$. Assim, teremos

$$gera_M(y, n, \vec{x}) \equiv_{def} (\forall m < n) M(y_m, \vec{x}) \wedge (\forall b \in P) (M(b, \vec{x}) \rightarrow (\exists a \in A^{\tilde{N}}) (\sum_{i=0}^n a_i y_i = b)),$$

$$base_M(y, n, \vec{x}) \equiv_{def} gera_M(y, n, \vec{x}) \wedge li_P(y, n),$$

$$FG_M(\vec{x}) \equiv_{def} (\exists n \in \tilde{N}) (\exists y \in P^{\tilde{N}}) gera_M(y, n, \vec{x}),$$

$$FBAS_M(\vec{x}) \equiv_{def} (\exists n \in \tilde{N}) (\exists y \in P^{\tilde{N}}) base_M(y, n, \vec{x}).$$

Para A^n , poderemos escrever $base(u, A^n)$ para indicar que a sequência u é base do sub-módulo A^n de $A^{\tilde{N}}$. A notação $M = \langle x_i : 1 \leq i \leq n-1 \rangle$ ou $M = \langle \langle x_i : 1 \leq i \leq n-1 \rangle \rangle$ também pode ser utilizada para $M(x, \vec{x})$. Por outro lado, a notação $P_1 = M_1 \oplus P_2$ indica a fórmula

$$\begin{aligned} & (\forall x) (P_1(x, \vec{x}) \rightarrow (\exists y) (\exists z) \delta(x, y, z)) \wedge \\ & \wedge (\forall x) (P_1(x, \vec{x}) \rightarrow (\forall y) (\forall z) (\forall y') (\forall z') (\delta(x, y, z) \otimes \delta(x, y', z') \rightarrow (y = y') \wedge (z = z'))), \\ & \delta(x, y, z) \equiv_{def} M_1(y, \vec{y}) \otimes P_2(z, \vec{z}) \otimes (x = y + z), \end{aligned}$$

para os sub-módulos $M_1(y, \vec{y}), P_1(x, \vec{x}), P_2(z, \vec{z})$ de P .

Introduzimos um símbolo de constante e , de tipo $((A^{\tilde{N}})^{\tilde{N}})^{\tilde{N}}$, que será interpretado, para cada $n \in \tilde{N}$, como a base canônica e^n de A^n . e é definido pelos seguintes axiomas :

$$\begin{aligned} [BC1] \quad & \vdash (\forall n) (\forall m) (m < n \rightarrow (e^n(m)(m) = 1)), \\ [BC2] \quad & \vdash (\forall n) (\forall m) (\forall r) ((m < n) \otimes (\neg(m = r)) \rightarrow (e^n(m)(r) = 0)), \\ [BC3] \quad & \vdash (\forall n) (\forall m) (\forall r) (m \geq n \rightarrow (e^n(m)(r) = 0)), \end{aligned}$$

onde e^n denota o termo $e(n)$ para todo $n \in \tilde{N}$. A existência de um modelo é garantida pelo seguinte resultado, cuja prova é similar à do lema 4.1.6.

Lema 4.1.12 : *Seja A um anel em $Sh(Q)$ e $B = \tilde{N}|_{EA}$. Então, existe um único elemento $bc \in ((A^B)^B)^B(EA)$ satisfazendo:*

$$\begin{aligned} bc(\tilde{n}|_{EA})(\tilde{m}|_{EA})(\tilde{m}|_{EA}) &= 1_A \quad \forall m < n, \\ bc(\tilde{n}|_{EA})(\tilde{m}|_{EA})(\tilde{r}|_{EA}) &= 0_A \quad \forall m < n, \quad \forall r \neq m, \\ bc(\tilde{n}|_{EA})(\tilde{m}|_{EA})(\tilde{r}|_{EA}) &= 0_A \quad \forall m \geq n, \quad \forall r \in \tilde{N}. \end{aligned}$$

Observe que se $n, m \in \mathbb{N}$, com $m \geq n$, então $\mathbf{bc}(\tilde{n}_{|EA})(\tilde{m}_{|EA}) \equiv 0_A$, logo $\mathbf{bc}(\tilde{n}_{|EA}) = (e^n, EA) \simeq (e_0^n, \dots, e_{n-1}^n) \in |\prod_{i=1}^n A^B|$, pelo lema 4.1.10. Por outro lado, para todo $i < n$, $e_i^n(\tilde{r}_{|EA}) = 0_A$ para todo $r \geq n$ e então $e_i^n \in |\prod_{i=1}^n A|$, pelo lema 4.1.10, dado por $e_i^n = (0_A, \dots, 1_A, \dots, 0_A)$, onde 1_A está na posição $i + 1$, para $i = 0, \dots, n - 1$. A sequência finita $e^n = (e_0^n, \dots, e_{n-1}^n)$ será chamada de base canônica de $A^n = \prod_{i=1}^n A$. Como antes, podemos provar a correspondência entre sintaxe e semântica:

Lema 4.1.13 : *Se $\mathcal{I} \models \text{Mod}$, então, $\mathcal{I} \models [BC\ i]$ ($i = 1, 2, 3$) sse $e^{\mathcal{I}}$ coincide com o elemento $\mathbf{bc}$ definido no lema 4.1.12. Em particular, $(e^{\mathcal{I}})(\tilde{n}_{|EA})$ pode ser identificado com a base canônica e^n de $\prod_{i=1}^n A$ para todo $n \in \mathbb{N}$.*

As propriedades formais da base e^n são as esperadas, provando que A^n tem base para todo n “standard” (o mesmo resultado vale para todo $n \in \tilde{\mathbb{N}}$).

Lema 4.1.14 : *Sejam $n < m \in \mathbb{N}$ e considere os termos $s^n(0)$, $s^m(0)$ (denotados por n e m). Seja x uma variável de tipo $M^{\tilde{\mathbb{N}}}$, com M módulo e y variável de tipo $A^{\tilde{\mathbb{N}}}$.*

- (a) *O seguinte $EA \vdash \sum_{i=n}^m x_i = x_n + \dots + x_{m-1}$ é provável em Mod .*
- (b) *Para $n > 0$, o seguinte $y \in A^n \vdash (y = \sum_{i=0}^n y_i e_i^n)$ é provável em Mod .*

Demonstração: (a) Óbvio, a partir dos axiomas.

(b) A parte (a), a definição da soma em $A^{\tilde{\mathbb{N}}}$ e os axiomas $[IG1]$, $[BC1]$ e $[BC2]$ fornecem

$$\begin{aligned} EA \vdash (\sum_{i=0}^n y_i e_i^n)(j) &= (y_0 e_0^n + \dots + y_{n-1} e_{n-1}^n)(j) \\ EA \vdash (y_0 e_0^n + \dots + y_{n-1} e_{n-1}^n)(j) &= (y_0 e_0^n)(j) + \dots + (y_{n-1} e_{n-1}^n)(j) \\ j < n \vdash (y_0 e_0^n)(j) + \dots + (y_{n-1} e_{n-1}^n)(j) &= y_j \\ j < n \vdash (\sum_{i=0}^n y_i e_i^n)(j) &= y_j, \end{aligned}$$

enquanto que $[BC2]$ acarreta

$$j \geq n \vdash (y_0 e_0^n)(j) + \dots + (y_{n-1} e_{n-1}^n)(j) = 0.$$

Logo, $j \geq n \vdash (\sum_{i=0}^n y_i e_i^n)(j) = 0$; pela proposição 2.6.4(20) podemos escrever

$$\frac{y \in A^n, j < n \vdash y_j = (\sum_{i=0}^n y_i e_i^n)(j) \quad y \in A^n, j \geq n \vdash y_j = (\sum_{i=0}^n y_i e_i^n)(j)}{y \in A^n, (j < n) \vee (j \geq n) \vdash y_j = (\sum_{i=0}^n y_i e_i^n)(j)}.$$

Como $EA \vdash (j < n) \vee (j \geq n)$ é um teorema da teoria de $\tilde{\mathbb{N}}$, temos

$$\frac{y \in A^n \vdash y_j = (\sum_{i=0}^n y_i e_i^n)(j)}{y \in A^n \vdash (\forall j)(y_j = (\sum_{i=0}^n y_i e_i^n)(j))}$$

que, juntamente com $[IG2]$, implica o resultado desejado. $\square$

Uma variável de tipo M^N , com M e N módulos, é dita um morfismo de módulos se satisfaz a

fórmula

$$Hom_{N,M}(f) \equiv_{def} (\forall x \in N)(\forall y \in N)(f(x+y) = fx + fy) \wedge (\forall x \in N)(\forall a \in A)(f(ax) = af(x)).$$

Introduzimos na linguagem os símbolos de função $\circ : M^B \times B^C \longrightarrow M^C$, definidos pelos axiomas

$$\vdash (\forall g \in M^B)(\forall f \in B^C)(\forall c \in C)((g \circ f)(c) = g(f(c))).$$

Temos que, na teoria Mod , $\mathcal{I}$ é um modelo do sequente acima se e somente se $\circ^{\mathcal{I}}(g, f) = g \circ f$. Assim, se a é do tipo $B^{\tilde{N}}$ e b é do tipo M^B , então $b \circ a$ é uma sequência em M . Seja $P_1(x, \vec{x})$ uma fórmula com x de tipo P – denotando um sub-módulo de P – e ϕ, ψ variáveis do tipo $P^{(A^{\tilde{N}})}$ e $(A^{\tilde{N}})^P$, respectivamente. Introduzimos as seguintes abreviações :

$$Im \phi \subseteq P_1 \equiv_{def} (\forall z) P_1(\phi(z), \vec{x}),$$

$$Im \psi \subseteq A^n \equiv_{def} (\forall x)(\psi(x) \in A^n),$$

$$(\phi \circ (\psi|_{P_1}) = id_{P_1}) \equiv_{def} (\forall x)(P_1(x, \vec{x}) \rightarrow (\phi(\psi(x)) = x)),$$

$$A^n \xrightarrow[\psi]{\phi} P_1 \equiv_{def} Hom_{A^{\tilde{N}}P}(\phi) \wedge Hom_{PA^{\tilde{N}}}(\psi) \wedge (Im \phi \subseteq P_1) \wedge (Im \psi \subseteq A^n) \wedge (\phi \circ (\psi|_{P_1}) = id_{P_1}).$$

Lema 4.1.15 : *Seja $P_1(x) \equiv_{def} (x = x)$. Então, na teoria Mod temos*

$$gera_{P_1}(y, n) \sim gera_P(y, n), \quad FBAS_{P_1} \sim FBAS_P, \quad (\phi \circ (\psi|_{P_1}) = id_{P_1}) \sim (\forall x)(\phi(\psi(x)) = x).$$

Demonstração: Dado que todos os tipos têm o mesmo extent, então $EA \vdash (\tau = \tau)$ é provável para todo termo τ . Portanto, de

$$(b = b), (b = b) \rightarrow (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b) \vdash (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b)$$

e $(m < n) \rightarrow (y_m = y_m) \vdash (b = b)$, obtemos, por $[CUT]$,

$$(m < n) \rightarrow (y_m = y_m), (b = b) \rightarrow (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b) \vdash (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b)$$

donde, aplicando as regras de quantificação na ordem certa, deduzimos $gera_{P_1}(y, n) \vdash gera_P(y, n)$.

Por outro lado, temos

$$\frac{\frac{(b = b), (\sum_{i=0}^n a_i y_i = b) \vdash (\sum_{i=0}^n a_i y_i = b)}{(b = b), (\sum_{i=0}^n a_i y_i = b) \vdash (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b)}}{(b = b), (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b) \vdash (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b)}$$

$$(\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b) \vdash (\forall b)((b = b) \rightarrow (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b))$$

e, de $EA \vdash (y_m = y_m)$, obtemos

$$\frac{m < n, (\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b) \vdash (y_m = y_m)}{(\exists a \in A^{\tilde{N}})(\sum_{i=0}^n a_i y_i = b) \vdash (\forall m < n)(y_m = y_m)}$$

donde deduzimos $gera_P(y, n) \vdash gera_{P_1}(y, n)$; portanto, $FBAS_{P_1} \sim FBAS_P$. As outras afirmações do enunciado podem ser verificadas de forma análoga. $\square$

A prova do teorema 4.2.2 requer a manipulação de sistemas de equações lineares (e, consequentemente, de matrizes) no anel local A , que não é necessariamente comutativo. Logo, precisamos definir as operações elementares de linha e a multiplicação de matrizes da maneira apropriada para os nossos fins.

Definição 4.1.16 : *Seja A um anel. Dadas $\mathbf{a} = (a_{ij})$ e $\mathbf{b} = (b_{jk})$ matrizes em $A^{n \times m}$ e $A^{m \times r}$, respectivamente, definimos o produto $\mathbf{a} \cdot \mathbf{b} \in A^{n \times r}$ da maneira seguinte:*

$$(\mathbf{a} \cdot \mathbf{b})_{ik} \equiv_{def} \sum_{j=1}^m b_{jk} a_{ij} \quad (1 \leq i \leq n, 1 \leq k \leq r).$$

Este produto é associativo e a matriz identidade Id_n é o seu neutro. Por outro lado, um sistema de equações lineares em A da forma

$$\sum_{j=1}^n x_j a_{ij} = b_i \quad (1 \leq i \leq n)$$

pode ser escrito na notação matricial usual: $\mathbf{a} \cdot \mathbf{x} = \mathbf{b}$.

Definição 4.1.17 : *Seja $\mathbf{a} \in A^{n \times n}$. O resultado de aplicar uma operação elementar (de linha) sobre $\mathbf{a}$ é uma matriz $\mathbf{b}$, obtida de $\mathbf{a}$ substituindo a linha L_i de $\mathbf{a}$ por $L_i + L_j \lambda$ para algum par $1 \leq i \neq j \leq n$, $\lambda \in A$, ou então uma matriz $\mathbf{c}$ obtida de $\mathbf{a}$ substituindo a linha L_i de $\mathbf{a}$ por $L_i \lambda$ para algum $1 \leq i \leq n$ e algum λ inversível em A . Se E é uma operação elementar, $E(\mathbf{a})$ denota a matriz obtida pela aplicação de E à $\mathbf{a}$.*

Observação 4.1.18 : Se E é uma operação elementar de linha, é fácil provar que para toda matriz $\mathbf{a} \in A^{n \times n}$ temos

$$E(\mathbf{a}) = E(Id_n) \cdot \mathbf{a};$$

além disso, se E é a operação $L_i \longleftrightarrow L_i + L_j \lambda$, então a operação $\overline{E} : L_i \longleftrightarrow L_i + L_j(-\lambda)$ produz: $\overline{E}(Id_n) = E(Id_n)^{-1}$, onde a inversa é com relação ao produto definido em 4.1.16. Analogamente, se $E : L_i \longleftrightarrow L_i \lambda$, então $\overline{E} : L_i \longleftrightarrow L_i(\lambda^{-1})$ produz $\overline{E}(Id_n) = E(Id_n)^{-1}$. Isto permite aplicar um método usual de cálculo da matriz inversa: suponha que, dada uma matriz $\mathbf{a} \in A^{n \times n}$, achamos uma sequência de operações elementares $E_1, \dots, E_N$ tais que

$$E_N(Id_n) \cdots E_1(Id_n) \cdot \mathbf{a} = E_N(\cdots (E_1(\mathbf{a})) \cdots) = Id_n.$$

Multiplicando à esquerda por $E_1(Id_n)^{-1} \cdots E_N(Id_n)^{-1}$, obtemos

$$\mathbf{a} = E_1(Id_n)^{-1} \cdots E_N(Id_n)^{-1},$$

donde, multiplicando à direita por $E_N(Id_n) \cdots E_1(Id_n)$, temos que

$$\mathbf{a} \cdot E_N(Id_n) \cdots E_1(Id_n) = Id_n,$$

isto é, a matriz $E_N(Id_n) \cdots E_1(Id_n) = E_N(\cdots (E_1(Id_n)) \cdots)$ é a inversa de $\mathbf{a}$. $\square$

Com estas definições, provaremos o lema 4.1.19, de fundamental importância para a demonstração do teorema 4.2.2. Na prova de 4.1.19 utilizaremos uma sequência finita $\Delta = \delta_1, \dots, \delta_r$ de sentenças, tais que $\llbracket \delta_i \rrbracket = EA$. As sentenças δ_i correspondem às definições que usualmente são feitas numa prova, tais como a introdução de novas variáveis, ou mudanças de variáveis. Dado que as δ_i são válidas com valor EA , então a prova de um sequente $\Gamma, \Delta \vdash \phi$ implica a validade do sequente $\Gamma \vdash \phi$, que é o sequente objetivo. Assim, dizemos que uma sentença δ como as indicadas acima é uma hipótese válida.

Lema 4.1.19 : *Se $n \in \mathbb{N}$ é não nulo, denotaremos por n o termo*

$$s^n(0) \equiv_{def} \overbrace{s(\dots s(0) \dots)}^{n \text{ vezes}}.$$

Então, o seguinte sequente é provável na teoria de anel local (junto com os axiomas da aritmética):

$$(\forall i < n)(\sum_{j=0}^n a_j c_{ij} = a_i), \Delta \vdash \alpha_0 \vee \dots \vee \alpha_{n-1} \vee \beta$$

onde, para cada $0 \leq j \leq n-2$, temos

$$\alpha_j \equiv_{def} \forall b((\forall i < j)(b_i = a_i) \otimes (\forall j \leq i \leq n-2)(b_i = a_{i+1}) \rightarrow (\exists \lambda)(a_j = \sum_{i=0}^{n-1} b_i \lambda_i)),$$

$$\alpha_{n-1} \equiv_{def} (\exists \lambda)(a_{n-1} = \sum_{i=0}^{n-1} a_i \lambda_i),$$

$$\beta \equiv_{def} (\exists d)((\forall i, j < n)(\neg(i = j) \rightarrow ((\sum_{k=0}^n c_{kj} d_{ik} = 0) \wedge (\sum_{k=0}^n d_{kj} c_{ik} = 0))) \wedge$$

$$\wedge (\forall i < n)((\sum_{k=0}^n c_{ki} d_{ik} = 1) \wedge (\sum_{k=0}^n d_{ki} c_{ik} = 1))),$$

e Δ consiste de hipóteses válidas. Aqui, a, b, λ são do tipo $A^{\tilde{N}}$ e c, d são do tipo $(A^{\tilde{N}})^{\tilde{N}}$.

Observação: As fórmulas α_j estão indicando que a_j pode ser escrito como uma combinação linear à direita dos a_i ($i \neq j$), enquanto que β expressa que a matriz c_{ij} tem inversa d_{ij} .

Demonstração: Para realizar a prova em (QPC1), utilizaremos as seguintes variáveis auxiliares:

$$c^1, \dots, c^{n-1}, d^0, \dots, d^{2n-1} \text{ variáveis do tipo } (A^{\tilde{N}})^{\tilde{N}};$$

$$a^1, \dots, a^{n-1}, \lambda^0, \dots, \lambda^{n-1} \text{ variáveis do tipo } A^{\tilde{N}};$$

$$z^0, \dots, z^{n-1} \text{ variáveis do tipo } A.$$

Considere $\gamma \equiv_{def} (\forall i < n)(\sum_{j=0}^n a_j c_{ij} = a_i)$ e $\alpha \equiv_{def} \alpha_0 \vee \dots \vee \alpha_{n-1} \vee \beta$. Por simples manipulação de equações, temos que

$$\gamma, 1 - c_{00} \in U, \delta_0 \vdash \alpha_0,$$

onde $\delta_0 \equiv_{def} (\forall c)(\forall z^0)(\exists \lambda^0)\delta'_0(c, z^0, \lambda^0)$ e

$$\delta'_0(c, z^0, \lambda^0) \equiv_{def} (\lambda_0^0 = \tau_0(c, z^0)) \otimes \cdots \otimes (\lambda_{n-2}^0 = \tau_{n-2}(c, z^0)),$$

sendo que os termos τ_i descrevem as coordenadas de a_0 em função de $a_1, \dots, a_{n-1}$; assim, podemos escrever

$$\frac{\frac{(\forall 0 \leq i \leq n-2)(b_i = a_{i+1}), \gamma, ((1 - c_{00})z^0 = 1), \delta'_0(c, z^0, \lambda^0) \vdash (a_0 = \sum_{i=0}^{n-1} b_i \lambda_i)[\lambda^0/\lambda]}{(\forall 0 \leq i \leq n-2)(b_i = a_{i+1}), \gamma, ((1 - c_{00})z^0 = 1), \delta'_0(c, z^0, \lambda^0) \vdash (\exists \lambda)(a_0 = \sum_{i=0}^{n-1} b_i \lambda_i)}}{(\forall 0 \leq i \leq n-2)(b_i = a_{i+1}), \gamma, ((1 - c_{00})z^0 = 1), \delta_0 \vdash (\exists \lambda)(a_0 = \sum_{i=0}^{n-1} b_i \lambda_i)} \quad \gamma, 1 - c_{00} \in U, \delta_0 \vdash \alpha_0$$

Por outro lado, a hipótese $c_{00} \in U$ permite definir a matriz c^1 obtida de c zerando os coeficientes c_{j0} para $1 \leq j \leq n-1$ e redefinindo o sistema de equações γ , i.e.: sejam

$$\sigma_1 \equiv_{def} (a_0^1 = a_0) \otimes (\forall 1 \leq i \leq n-1)(a_i^1 = a_i - a_0 z^0 c_{i0}),$$

$$\beta_1 \equiv_{def} (\forall j \leq n-1)(c_{0j}^1 = c_{0j}) \otimes (\forall 1 \leq i \leq n-1)(\forall j \leq n-1)(c_{ij}^1 = c_{ij} - c_{0j} z^0 c_{i0}),$$

$$\gamma_1 \equiv_{def} (\forall i \leq n-1)(\sum_{j=0}^n a_j c_{ij}^1 = a_i^1).$$

A regras da igualdade, juntamente com os axiomas algébricos e aritméticos, fornecem

$$\gamma, (c_{00} z^0 = 1) \wedge (z^0 c_{00} = 1), \sigma_1, \beta_1 \vdash \gamma_1,$$

$$\gamma_1, 1 - c_{11}^1 \in U, \sigma_1, \beta_1, \delta_1 \vdash \alpha_1,$$

onde $\delta_1 = (\forall c)(\forall c^1)(\forall z^0)(\forall z^1)(\exists \lambda^1)\delta'_1(c, c^1, z^0, z^1, \lambda^1)$ é construído como δ_0 . Se assumimos que c_{11}^1 é inversível, podemos agora definir uma nova matriz c^2 obtida de c^1 zerando os coeficientes c_{j1}^1 para $2 \leq j \leq n-1$, obtendo um novo sistema de equações:

$$\sigma_2 \equiv_{def} (a_0^2 = a_0) \otimes (a_1^2 = a_1^1) \otimes (\forall 2 \leq i \leq n-1)(a_i^2 = a_i^1 - a_1^1 z^1 c_{i1}^1),$$

$$\beta_2 \equiv_{def} (\forall j \leq n-1)(c_{0j}^2 = c_{0j}) \otimes (\forall j \leq n-1)(c_{1j}^2 = c_{1j}^1) \otimes (\forall 2 \leq i \leq n-1)(\forall j \leq n-1)(c_{ij}^2 = c_{ij}^1 - c_{1j}^1 z^1 c_{i1}^1),$$

$$\gamma_2 \equiv_{def} (\forall i \leq n-1)(\sum_{j=0}^n a_j c_{ij}^2 = a_i^2).$$

Desta maneira, provamos

$$\gamma_1, (c_{11}^1 z^1 = 1) \wedge (z^1 c_{11}^1 = 1), \sigma_1, \sigma_2, \beta_1, \beta_2 \vdash \gamma_2,$$

$$\gamma_2, 1 - c_{22}^2 \in U, \sigma_1, \sigma_2, \beta_1, \beta_2, \delta_2 \vdash \alpha_2.$$

Por exemplo, se $n = 3$, teremos:

$$\gamma, ((1 - c_{00})z^0 = 1) \vdash (a_0 = a_1 c_{01} z^0 + a_2 c_{02} z^0),$$

$$\gamma_1, (1 - c_{11}^1)z^1 = 1, \sigma_1, \beta_1 \vdash (a_1 = a_0 z^0 c_{10} + a_2 c_{12}^1 z^1),$$

$$\gamma_2, 1 - c_{22}^2 \in U, \sigma_1, \sigma_2, \beta_1, \beta_2 \vdash (a_2 = a_0 z^0 c_{20} + a_1 z^1 c_{21}^1).$$

O último sequente mostra que δ'_i pode, eventualmente, não depender de c^i e z^i . Continuando com este procedimento, no passo $n - 1$ definimos

$$\begin{aligned}\sigma_{n-1} &\equiv_{def} (a_0^{n-1} = a_0) \otimes (a_1^{n-1} = a_1^1) \otimes \dots \\ &\quad \dots \otimes (a_{n-2}^{n-1} = a_{n-2}^{n-2}) \otimes (a_{n-1}^{n-1} = a_{n-1}^{n-2} - a_{n-2}^{n-2} z^{n-2} c_{n-1}^{n-2} c_{n-2}), \\ \beta_{n-1} &\equiv_{def} (\forall j \leq n-1) (c_{0j}^{n-1} = c_{0j}) \otimes (\forall j \leq n-1) (c_{1j}^{n-1} = c_{1j}^1) \otimes \dots \\ &\quad \dots \otimes (\forall j \leq n-1) (c_{n-2j}^{n-1} = c_{n-2j}^{n-2}) \otimes (\forall j \leq n-1) (c_{n-1j}^{n-1} = c_{n-1j}^{n-2} - c_{n-2j}^{n-2} z^{n-2} c_{n-1}^{n-2} c_{n-2}), \\ \gamma_{n-1} &\equiv_{def} (\forall i \leq n-1) (\sum_{j=0}^n a_j c_{ij}^{n-1} = a_i^{n-1}),\end{aligned}$$

provando os seguintes

$$\gamma_i, (c_{ii}^i z^i = 1) \wedge (z^i c_{ii}^i = 1), \sigma_1, \dots, \sigma_{i+1}, \beta_1, \dots, \beta_{i+1} \vdash \gamma_{i+1} \quad 1 \leq i \leq n-2,$$

$$\gamma_i, 1 - c_{ii}^i \in U, \sigma_1, \dots, \sigma_i, \beta_1, \dots, \beta_i, \delta_i \vdash \alpha_i \quad 1 \leq i \leq n-1,$$

onde $\delta_i \equiv_{def} (\forall)(\exists \lambda^i) \delta'_i(c, c^1, \dots, c^i, z^0, \dots, z^i, \lambda^i)$. Logo, definindo as sequências

$$\Sigma_0 \equiv_{def} (c_{00} z^0 = 1) \wedge (z^0 c_{00} = 1), \quad \Sigma'_0 \equiv_{def} c_{00} \in U,$$

$$\Sigma_i \equiv_{def} (c_{00} z^0 = 1) \wedge (z^0 c_{00} = 1), (c_{11}^1 z^1 = 1) \wedge (z^1 c_{11}^1 = 1), \dots, (c_{ii}^i z^i = 1) \wedge (z^i c_{ii}^i = 1),$$

$$\Sigma'_i \equiv_{def} c_{00} \in U, c_{11}^1 \in U, \dots, c_{ii}^i \in U,$$

$$\Delta_i \equiv_{def} \sigma_1, \beta_1, \dots, \sigma_i, \beta_i,$$

$$\Delta'_i \equiv_{def} (\forall)(\exists a^1) \sigma_1, (\forall)(\exists c^1) \beta_1, \dots, (\forall)(\exists a^i) \sigma_i, (\forall)(\exists c^i) \beta_i$$

para $i = 1, \dots, n-1$, [CUT] nos fornece

$$\gamma, 1 - c_{00} \in U, \delta_0 \vdash \alpha_0,$$

$$\gamma, \Sigma_{i-1}, \Delta_i, 1 - c_{ii}^i \in U, \delta_i \vdash \alpha_i \quad 1 \leq i \leq n-1.$$

Logo, por [VR1] e [VR2], obtemos

$$\gamma, 1 - c_{00} \in U, \delta_0 \vdash \alpha \quad (*),$$

$$\gamma, \Sigma_{i-1}, \Delta_i, 1 - c_{ii}^i \in U, \delta_0, \dots, \delta_{n-1} \vdash \alpha \quad 1 \leq i \leq n-1,$$

donde, aplicando as regras [VL] e [EL] na ordem apropriada, provamos

$$\gamma, \Sigma'_{i-1}, \Delta'_i, 1 - c_{ii}^i \in U, \delta_0, \dots, \delta_{n-1} \vdash \alpha \quad 1 \leq i \leq n-1 \quad (**).$$

Para terminar a prova falta resolver o caso Σ_{n-1} , i.e., todos os elementos da diagonal da matriz c^{n-1} são inversíveis. Neste caso, construiremos uma inversa para a matriz c , provando β . Observe que a matriz c^1 é obtida de c a partir das $n-1$ operações elementares de linha

$$L_i \longleftrightarrow L_i + L_0(-z^0 c_{i0}) \quad i = 1, \dots, n-1;$$

a matriz c^2 é obtida de c^1 aplicando as $n - 2$ operações

$$L_i \longleftrightarrow L_i + L_1(-z^1 c_{i1}^1) \quad i = 2, \dots, n - 1;$$

finalmente, c^{n-1} é obtida de c^{n-2} aplicando a operação

$$L_{n-1} \longleftrightarrow L_{n-1} + L_{n-2}(-z^{n-2} c_{n-1, n-2}^{n-2}).$$

Desta maneira, a matriz c^{n-1} tem, por hipótese, todos os elementos da diagonal inversíveis, enquanto todos os elementos embaixo da diagonal são nulos. Assim, é simples ver que as operações elementares

$$L_i \longleftrightarrow L_i + L_{n-1}(-z^{n-1} c_{i, n-1}^{n-1}) \quad i = 0, \dots, n - 2;$$

$$L_i \longleftrightarrow L_i + L_{n-2}(-z^{n-2} c_{i, n-2}^{n-1}) \quad i = 0, \dots, n - 3;$$

$\vdots$

$$L_0 \longleftrightarrow L_0 + L_1(-z^1 c_{01}^{n-1})$$

aplicadas a c^{n-1} produzem uma matriz diagonal com $c_{00}, c_{11}, \dots, c_{n-1, n-1}^{n-1}$ na diagonal. Por fim, a sequência de n operações

$$L_i \longleftrightarrow L_i z^i \quad i = 0, \dots, n - 1$$

levam à matriz identidade. Pela observação 4.1.18, as n^2 operações descritas acima aplicadas na matriz identidade produzem a inversa de c . Para implementar isto na lógica definimos uma sequência de matrizes $d^0, \dots, d^{2n-1}$, com d^0 igual à matriz identidade, codificando as $2n-1$ sequências de operações descritas acima. Portanto, definimos

$$\theta_0 \equiv_{def} (\forall i \leq n - 1)(d_{ii}^0 = 1) \otimes (\forall i \leq n - 1)(\forall j \leq n - 1)(\neg(i = j) \multimap (d_{ij}^0 = 0)),$$

$$\theta_1 \equiv_{def} (\forall j \leq n - 1)(d_{0j}^1 = d_{0j}) \otimes (\forall 1 \leq i \leq n - 1)(\forall j \leq n - 1)(d_{ij}^1 = d_{ij} - d_{0j} z^0 c_{i0}),$$

$$\theta_2 \equiv_{def} (\forall j \leq n - 1)(d_{0j}^2 = d_{0j}) \otimes (\forall j \leq n - 1)(d_{1j}^2 = d_{1j}^1) \otimes (\forall 2 \leq i \leq n - 1)(\forall j \leq n - 1)(d_{ij}^2 = d_{ij}^1 - d_{1j}^1 z^1 c_{i1}^1),$$

e analogamente para as outras sequências de operações elementares. Assim, se

$$\Theta \equiv_{def} \theta_0, \dots, \theta_{2n-1}, \quad \Theta' \equiv_{def} (\exists d^0) \theta_0, (\forall)(\exists d^1) \theta_1, \dots, (\forall)(\exists d^{2n-1}) \theta_{2n-1}$$

então, como d^{2n-1} é a inversa de c , teremos

$$\frac{\gamma, \Sigma_{n-1}, \beta_1, \dots, \beta_{n-1}, \Theta \vdash \beta}{\gamma, \Sigma_{n-1}, \beta_1, \dots, \beta_{n-1}, \Theta \vdash \alpha} \\ \frac{\gamma, \Sigma'_{n-1}, (\forall)(\exists c^1) \beta_1, \dots, (\forall)(\exists c^{n-1}) \beta_{n-1}, \Theta' \vdash \alpha}{\gamma, \Sigma'_{n-1}, (\forall)(\exists c^1) \beta_1, \dots, (\forall)(\exists c^{n-1}) \beta_{n-1}, \Theta' \vdash \alpha}$$

Por exemplo, se $n = 2$, obtemos a inversa d^3 de c , dada por

$$d^3 = \begin{bmatrix} z^0 + z^0 c_{10} z^1 c_{01} z^0 & -z^1 c_{01} z^0 \\ -z^0 c_{10} z^1 & z^1 \end{bmatrix}.$$

Seja finalmente Δ a sequência

$$\Delta \equiv_{def} \Theta', \Delta'_{n-1}, \delta_0, \dots, \delta_{n-1}.$$

Assim, utilizando (**), obtemos

$$\frac{\gamma, \Delta, \Sigma'_{n-1} \vdash \alpha \quad \gamma, \Delta, \Sigma'_{n-2}, 1 - c_{n-1}^{n-1} \in U \vdash \alpha}{\gamma, \Delta, \Sigma'_{n-2}, (c_{n-1}^{n-1} \in U) \vee (1 - c_{n-1}^{n-1} \in U) \vdash \alpha}.$$

Como A é um anel local, concluímos $\gamma, \Delta, \Sigma'_{n-2} \vdash \alpha$.

Reiterando o processo (e usando o sequente (*) no último passo), provamos então $\gamma, \Delta \vdash \alpha$, onde Δ consiste claramente em hipóteses válidas. $\square$

4.2 O Teorema de Kaplansky em $Sh(Q)$

Estamos agora em condições de provar o teorema de Kaplansky em $Sh(Q)$. Primeiro de tudo, devemos dar uma definição precisa de módulo projetivo na linguagem de primeira ordem $\mathbb{L}$.

Definição 4.2.1 *Seja P um módulo em $Sh(Q)$. Dizemos que P é projetivo finitamente gerado se é um modelo do sequente $\vdash PFG_P$, onde PFG_P denota a fórmula*

$$(\exists n)(\exists y)(\exists \phi)(\exists \psi)(Hom_{A^{\tilde{N}}, P}(\phi) \wedge Hom_{P, A^{\tilde{N}}}(\psi) \wedge (\forall x)(\phi(\psi(x)) = x) \wedge (Im \psi \subseteq A^n) \wedge gera_P(y, n))$$

ou, equivalentemente, considerando $P_1(x) \equiv_{def} (x = x)$, P satisfaz

$$\vdash (\exists n)(\exists y)(\exists \phi)(\exists \psi)((A^n \xrightleftharpoons[\psi]{\phi} P_1) \wedge gera_{P_1}(y, n)).$$

Teorema 4.2.2 : *Em $Sh(Q)$, todo módulo projetivo finitamente gerado sobre um anel local é livre com base finita, i.e., P é um modelo do sequente $\vdash FBAS_P$.*

Sejam

$$\phi : \mathcal{A}^{\tilde{N}|EA} \longrightarrow P, \quad \psi : P \longrightarrow \mathcal{A}^{\tilde{N}|EA}$$

os morfismos que testemunham o fato de que P é projetivo. A existência dos morfismos ϕ e ψ garante que todos os tipos considerados em $\mathbb{L}$ têm o mesmo extent. Assim, o nosso objetivo é provar que o sequente $PFG_P \vdash FBAS_P$ é válido. Para isso, para cada termo da forma $s^m(0)$, escrito como m , provaremos, em $(QPC1)$, o sequente $S(m) : \Gamma_{(m)}, \Delta_{(m)} \vdash FBAS_P$, onde

$$\Gamma_{(m)} : Hom_{A^{\tilde{N}}, P}(\phi), Hom_{P, A^{\tilde{N}}}(\psi), (\forall x)(\phi(\psi(x)) = x), (Im \psi \subseteq A^m), gera_P(y, m)$$

e onde $\Delta_{(m)}$ é uma sequência finita de hipóteses válidas, que codifica mudança de variáveis e definições de funções auxiliares.

Note que uma vez que os sequentes $S(m)$ estejam provados para todo $m \geq 0$, completamos a prova do teorema 4.2.2 da forma seguinte :

A proposição 2.6.4(5), a regra $[\exists L]$, o teorema de corretude e o fato de termos $\llbracket \Delta_{(m)} \rrbracket = EA$, fornece

$$\llbracket \alpha_P[s^m(0)/n] \rrbracket \leq \llbracket FBAS_P \rrbracket, \quad \llbracket \alpha_P[0/n] \rrbracket \leq \llbracket FBAS_P \rrbracket$$

para todo $m \geq 1$, onde α_P é a fórmula $PF\bar{G}_P$ sem a quantificação em n , i.e., $(\exists n)\alpha_P(n) = PF\bar{G}_P$.

Como α_P não utiliza disjunções, temos

$$\llbracket \alpha_P[s^m(0)/n] \rrbracket = \llbracket \alpha_P(n) \rrbracket_n(\tilde{m}), \quad \llbracket \alpha_P[0/n] \rrbracket = \llbracket \alpha_P(n) \rrbracket_n(\tilde{0})$$

para todo $m \geq 1$; então

$$\llbracket \alpha_P(n) \rrbracket_n(\tilde{m}) \leq \llbracket FBAS_P \rrbracket$$

para todo $m \in \mathbb{N}$. Finalmente, pelo lema 3.3.1(c), obtemos

$$\llbracket PF\bar{G}_P \rrbracket = \llbracket (\exists n)\alpha_P(n) \rrbracket = \bigvee_{m \in \mathbb{N}} \llbracket \alpha_P(n) \rrbracket_n(\tilde{m}) \leq \llbracket FBAS_P \rrbracket.$$

A prova dos sequentes $S(m)$ será realizada por recursão em m . Fixado $n > 0$, considere os seguintes passos de dedução: partindo de Γ , dado por

$$A^n \xrightarrow[\psi_1]{\phi_1} P_1, \quad P_1 = \langle x_0, \dots, x_{n-1} \rangle, \quad base(\mathbf{e}^n, A^n), \quad \psi_1(x_0) = \sum_{i=0}^n a_i \mathbf{e}_i^n, \quad (\forall j < n)(\psi_1(\phi_1(\mathbf{e}_j^n)) = \sum_{i=0}^n c_{ij}^1 \mathbf{e}_i^n)$$

onde $P_1(x) \equiv_{def} (x = x)$, deduzimos $x_0 = \sum_{i=0}^n a_i \phi_1(\mathbf{e}_i^n)$ e portanto

$$\sum_{i=0}^n a_i \mathbf{e}_i^n = \psi_1(x_0) = \sum_{j=0}^n a_j \psi_1(\phi_1(\mathbf{e}_j^n)) = \sum_{i=0}^n \left(\sum_{j=0}^n a_j c_{ij}^1 \right) \mathbf{e}_i^n$$

donde, pelo fato de $\mathbf{e}^n$ ser base, obtemos

$$(\forall i < n) \left(\sum_{j=0}^n a_j c_{ij}^1 = a_i \right).$$

Pelo lema 4.1.19, deduzimos (acrescentando as hipóteses válidas Δ)

$$\alpha \equiv_{def} \alpha_0 \vee \dots \vee \alpha_{n-1} \vee \beta,$$

$$\alpha_j \equiv_{def} \forall b((\forall i < j)(b_i = a_i) \otimes (\forall j \leq i \leq n-2)(b_i = a_{i+1}) \rightarrow (\exists \lambda)(a_j = \sum_{i=0}^{n-1} b_i \lambda_i)) \quad (0 \leq j \leq n-2),$$

$$\alpha_{n-1} \equiv_{def} (\exists \lambda)(a_{n-1} = \sum_{i=0}^{n-1} a_i \lambda_i),$$

$$\beta \equiv_{def} (\exists d^1)((\forall i, j < n)(\neg(i = j) \rightarrow ((\sum_{k=0}^n c_{kj}^1 d_{ik}^1 = 0) \wedge (\sum_{k=0}^n d_{kj}^1 c_{ik}^1 = 0))) \wedge$$

$$\wedge (\forall i < n)((\sum_{k=0}^n c_{ki}^1 d_{ik}^1 = 1) \wedge (\sum_{k=0}^n d_{ki}^1 c_{ik}^1 = 1))).$$

O objetivo é provar os seguintes

$$\Gamma, \Delta_j, \alpha_j \vdash FBAS_{P_1} \quad (0 \leq j \leq n-1),$$

$$\Gamma, \Delta_n, \beta \vdash FBAS_{P_1}$$

onde Δ_j são seqüências de hipóteses válidas; logo, por $[\forall L1]$ e o lema 4.1.19, se $\Delta_{(n)} = \Delta, \Delta_0, \dots, \Delta_n$, provaremos

$$\frac{\Gamma, \Delta_{(n)}, \alpha \vdash FBAS_P \quad \Gamma, \Delta_{(n)} \vdash \alpha}{\Gamma, \Delta_{(n)} \vdash FBAS_{P_1}}.$$

Portanto, aplicando $[\exists L]$, teremos provado

$$\boxed{\begin{array}{l} A^n \xrightarrow[\psi_1]{\phi_1} P_1, P_1 = \langle x_0, \dots, x_{n-1} \rangle, base(e^n, A^n), \Delta_{(n)}, \\ (\exists a)(\psi_1(x_0) = \sum_{i=0}^n a_i e_i^n), (\exists c^1)(\forall j < n)(\psi_1(\phi_1(e_j^n)) = \sum_{i=0}^n c_{ij}^1 e_i^n) \end{array}} \vdash FBAS_{P_1}$$

e então, dado que

$$base(e^n, A^n) \vdash (\exists a)(\psi_1(x_0) = \sum_{i=0}^n a_i e_i^n) \otimes (\exists c^1)(\forall j < n)(\psi_1(\phi_1(e_j^n)) = \sum_{i=0}^n c_{ij}^1 e_i^n),$$

obteremos

$$A^n \xrightarrow[\psi_1]{\phi_1} P_1, P_1 = \langle x_0, \dots, x_{n-1} \rangle, base(e^n, A^n), \Delta_{(n)} \vdash FBAS_{P_1}.$$

Finalmente, de $EA \vdash base(e^n, A^n)$, vem

$$A^n \xrightarrow[\psi_1]{\phi_1} P_1, P_1 = \langle x_0, \dots, x_{n-1} \rangle, \Delta_{(n)} \vdash FBAS_{P_1}$$

e então o lema 4.1.15 fornece $\Gamma_{(n)}, \Delta_{(n)} \vdash FBAS_P$.

A prova está portanto reduzida à verificação do sequente $\Gamma, \Delta_{(n)}, \alpha \vdash FBAS_{P_1}$. Para provar o sequente $\Gamma, \Delta_j, \alpha_j \vdash FBAS_{P_1}$ (para $j \leq n-1$), provaremos primeiro o seguinte:

$$\boxed{\begin{array}{l} \Gamma, \Delta_j^1, (\forall i < j)(b_i = a_i), (\forall j \leq i \leq n-2)(b_i = a_{i+1}), (a_j = \sum_{i=0}^{n-1} b_i \lambda_i), \\ (\forall i < j)(u_i^1 = e_i^n + \lambda_i e_j^n), (\forall j \leq i \leq n-2)(u_i^1 = e_{i+1}^n + \lambda_i e_j^n), (u_{n-1}^1 = e_j^n) \end{array}} \vdash FBAS_{P_1} \quad (*).$$

Com isto, podemos aplicar $[\exists L]$ a u^1 e $[\forall L]$ a λ , obtendo

$$\Gamma, \Delta_j^1, (\forall i < j)(b_i = a_i), (\forall j \leq i \leq n-2)(b_i = a_{i+1}), (a_j = \sum_{i=0}^{n-1} b_i \lambda_i), \delta_1 \vdash FBAS_{P_1},$$

onde

$$\delta_1 \equiv_{def} (\forall \lambda)(\exists u^1)((\forall i < j)(u_i^1 = e_i^n + \lambda_i e_j^n) \otimes (\forall j \leq i \leq n-2)(u_i^1 = e_{i+1}^n + \lambda_i e_j^n) \otimes (u_{n-1}^1 = e_j^n));$$

a regra $[\exists L]$ aplicada ao sequente anterior, em relação a λ , fornece

$$\Gamma, \Delta_j^1, (\forall i < j)(b_i = a_i), (\forall j \leq i \leq n-2)(b_i = a_{i+1}), (\exists \lambda)(a_j = \sum_{i=0}^{n-1} b_i \lambda_i), \delta_1 \vdash FBAS_{P_1}.$$

Por outro lado,

$$(\forall i < j)(b_i = a_i), (\forall j \leq i \leq n-2)(b_i = a_{i+1}), \alpha_j \vdash (\exists \lambda)(a_j = \sum_{i=0}^{n-1} b_i \lambda_i),$$

que implica

$$\Gamma, \Delta_j^1, \alpha_j, (\forall i < j)(b_i = a_i), (\forall j \leq i \leq n-2)(b_i = a_{i+1}), \delta_1 \vdash FBAS_{P_1};$$

agora, as regras $[\otimes L]$, $[\exists L]$ em relação a b e a regra $[\forall L]$ em relação a a nos dá

$$\Gamma, \Delta_j^1, \alpha_j, \delta_2, \delta_1 \vdash FBAS_{P_1},$$

onde $\Delta_j \equiv_{def} \Delta_j^1, \delta_1, \delta_2$, com

$$\delta_2 \equiv_{def} (\forall a)(\exists b)((\forall i < j)(b_i = a_i) \otimes (\forall j \leq i \leq n-2)(b_i = a_{i+1})).$$

A prova de $\Gamma, \Delta_{n-1}, \alpha_{n-1} \vdash FBAS_{P_1}$ será análoga, só que neste caso não é necessário definir os b_i . Para provar $(*)$, observemos que, partindo de

$$\begin{aligned} & base(\mathbf{e}^n, A^n), \psi_1(x_0) = \sum_{i=0}^n a_i \mathbf{e}_i^n, \\ & (\forall i < j)(b_i = a_i), (\forall j \leq i \leq n-2)(b_i = a_{i+1}), (a_j = \sum_{i=0}^{n-1} b_i \lambda_i), \\ & (\forall i < j)(u_i^1 = \mathbf{e}_i^n + \lambda_i \mathbf{e}_j^n), (\forall j \leq i \leq n-2)(u_i^1 = \mathbf{e}_{i+1}^n + \lambda_i \mathbf{e}_j^n), (u_{n-1}^1 = \mathbf{e}_j^n), \end{aligned}$$

provamos $base(u^1, A^n) \otimes (\psi_1(x_0) = \sum_{i=0}^{n-1} b_i u_i^1)$. Logo, podemos recomeçar a prova a partir de Γ_1 , dado por

$$\begin{aligned} & A^n \xrightleftharpoons[\psi_1]{\phi_1} P_1, P_1 = \langle x_0, \dots, x_{n-1} \rangle, base(u^1, A^n), \\ & \psi_1(x_0) = \sum_{i=0}^{n-1} a_i^1 u_i^1, (\forall j < n)(\psi_1 \phi_1(u_j^1) = \sum_{i=0}^n c_{ij}^2 u_i^1) \end{aligned}$$

em cada um dos n nós correspondentes à hipótese α_j . Por outro lado, assumindo β , vamos provar depois (lema 4.2.3) que $P_1 = \langle \phi_1(u_i) : i \leq n-1 \rangle$, obtendo portanto

$$\Gamma, \beta \vdash FBAS_{P_1}.$$

Continuando com este processo a partir dos n nós Γ_1 (onde agora vamos deixar pendentes os nós β), vamos poder escrever $\psi_1(x_0) = a'u'_0$ em alguma base $(u'_i)_{i=0}^n$ de A^n . Pelo lema 4.2.4 a ser provado depois, teremos que $\{\phi_1(u'_0)\}$ é linearmente independente, ou $x_0 = 0$. Nos dois casos, provaremos (lemas 4.2.8 e 4.2.7, respectivamente)

$$P_1 = M_1 \oplus P_2, FBAS_{M_1}, P_2 = \langle z_i : i \leq n-2 \rangle, A^{n-1} \xrightleftharpoons[\psi_2]{\phi_2} P_2,$$

recomeçando a prova num nível de complexidade estritamente menor. Os nós pendentes β vão gerar (como provaremos no lema 4.2.6) os nós

$$P_1 = M_1 \oplus P_2, FBAS_{M_1}, P_2 = \langle z_i : i \leq n-k-1 \rangle, A^{n-k} \xrightleftharpoons[\psi_2]{\phi_2} P_2$$

recomeçando a prova nesses nós com complexidade estritamente menor. Podemos definir o seguinte esquema, para visualizar a árvore de demonstração; as fórmulas α_j serão escritas, por simplicidade, como $a_j^k = \sum_{i \neq j} a_i^k \lambda_i$, enquanto que as β serão escritas como $d^k \cdot c^k = Id_{n-k+1} = c^k \cdot d^k$.

Esquema da prova: No nível 0, temos o seguinte nó:

$$A^n \xrightleftharpoons[\psi_1]{\phi_1} P_1, P_1 = \langle x_0, \dots, x_{n-1} \rangle, base(e^n, A^n), \psi_1(x_0) = \sum_{i=0}^n a_i e_i^n, \psi_1(\phi_1(e_j^n)) = \sum_{i=0}^n c_{ij}^1 e_i^n;$$

isto gera no nível 1 os seguintes $n+1$ nós:

$a_0 = \sum_{i \neq 0} a_i \lambda_i$ $base(u^1, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-1} a_i^1 u_i^1$ $\psi_1(\phi_1(u_j^1)) = \sum_{i=0}^n c_{ij}^2 u_i^1$	$\dots$	$a_{n-1} = \sum_{i \neq n-1} a_i \lambda_i$ $base(u^1, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-1} a_i^1 u_i^1$ $\psi_1(\phi_1(u_j^1)) = \sum_{i=0}^n c_{ij}^2 u_i^1$
---	---------	---

$A^n \xrightleftharpoons[\psi_1]{\phi_1} P_1$ $base(e^n, A^n)$ $d^1 \cdot c^1 = Id_n = c^1 \cdot d^1$ $\psi_1(\phi_1(e_j^n)) = \sum_{i=0}^n c_{ij}^1 e_i^n$

O último nó produz (lema 4.2.3) $P_1 = \langle \phi_1(e_0^n), \dots, \phi_1(e_{n-1}^n) \rangle$, sendo os $\phi_1(e_i^n)$ linearmente independentes, portanto obtemos que P_1 é livre, terminando o ramo.

Cada um dos n primeiros nós

$a_r = \sum_{i \neq r} a_i \lambda_i$ $base(u^1, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-1} a_i^1 u_i^1$ $\psi_1(\phi_1(u_j^1)) = \sum_{i=0}^n c_{ij}^2 u_i^1$

produzem, no nível 2, os seguintes n nós:

$a_0^1 = \sum_{i \neq 0} a_i^1 \lambda_i^1$ $base(u^2, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-2} a_i^2 u_i^2$ $\psi_1(\phi_1(u_j^2)) = \sum_{i=0}^n c_{ij}^3 u_i^2$	$\dots$	$a_{n-2}^1 = \sum_{i \neq n-2} a_i^1 \lambda_i^1$ $base(u^2, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-2} a_i^2 u_i^2$ $\psi_1(\phi_1(u_j^2)) = \sum_{i=0}^n c_{ij}^3 u_i^2$	$A^n \xrightleftharpoons[\psi_1]{\phi_1} P_1$ $base(u^1, A^n)$ $d^2 \cdot c^2 = Id_{n-1} = c^2 \cdot d^2$ $\psi_1(\phi_1(u_j^1)) = \sum_{i=0}^n c_{ij}^2 u_i^1$
---	---------	---	---

Cada um dos primeiros $n - 1$ nós da forma

$a_r^1 = \sum_{i \neq r} a_i^1 \lambda_i^1$ $base(u^2, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-2} a_i^2 u_i^2$ $\psi_1(\phi_1(u_j^2)) = \sum_{i=0}^n c_{ij}^3 u_i^2$

gera no nível 3 os seguintes $n - 1$ nós:

$a_0^2 = \sum_{i \neq 0} a_i^2 \lambda_i^2$ $base(u^3, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-3} a_i^3 u_i^3$ $\psi_1(\phi_1(u_j^3)) = \sum_{i=0}^n c_{ij}^4 u_i^3$	$\dots$	$a_{n-3}^2 = \sum_{i \neq n-3} a_i^2 \lambda_i^2$ $base(u^3, A^n)$ $\psi_1(x_0) = \sum_{i=0}^{n-3} a_i^3 u_i^3$ $\psi_1(\phi_1(u_j^3)) = \sum_{i=0}^n c_{ij}^4 u_i^3$	$A^n \xrightleftharpoons[\psi_1]{\phi_1} P_1$ $base(u^2, A^n)$ $d^3 \cdot c^3 = Id_{n-2} = c^3 \cdot d^3$ $\psi_1(\phi_1(u_j^2)) = \sum_{i=0}^n c_{ij}^3 u_i^2$
---	---------	---	---

Continuamos desta maneira até chegar ao nível $n - 1$, onde vamos ter nós da forma

$a_0^{n-2} = a_1^{n-2} \lambda_1^{n-2}$ $base(u^{n-1}, A^n)$ $\psi_1(x_0) = a_0^{n-1} u_0^{n-1}$ $\psi_1(\phi_1(u_j^{n-1})) = \sum_{i=0}^n c_{ij}^n u_i^{n-1}$	$a_1^{n-2} = a_0^{n-2} \lambda_0^{n-2}$ $base(u^{n-1}, A^n)$ $\psi_1(x_0) = a_0^{n-1} u_0^{n-1}$ $\psi_1(\phi_1(u_j^{n-1})) = \sum_{i=0}^n c_{ij}^n u_i^{n-1}$	$A^n \begin{smallmatrix} \xrightarrow{\phi_1} \\ \xleftarrow{\psi_1} \end{smallmatrix} P_1$ $base(u^{n-2}, A^n)$ $d^{n-1} \cdot c^{n-1} = Id_2 = c^{n-1} \cdot d^{n-1}$ $\psi_1(\phi_1(u_j^{n-2})) = \sum_{i=0}^n c_{ij}^{n-1} u_i^{n-2}$
--	--	---

Finalmente, cada um dos nós da forma

$a_r^{n-2} = a_i^{n-2} \lambda_i^{n-2}$ $base(u^{n-1}, A^n)$ $\psi_1(x_0) = a_0^{n-1} u_0^{n-1}$ $\psi_1(\phi_1(u_j^{n-1})) = \sum_{i=0}^n c_{ij}^n u_i^{n-1}$	$(i \neq r)$
--	--------------

gera no nível n os dois nós (lema 4.2.4)

$\{\phi_1(u_0^{n-1})\}$ linearmente independente	$x_0 = 0$
--	-----------

No primeiro caso, obtemos (lema 4.2.8)

$P_1 = \langle\langle \phi_1(u_0^{n-1}) \rangle\rangle \oplus P_2$ $P_2 = \langle z_i : i \leq n-2 \rangle$ $A^{n-1} \begin{smallmatrix} \xrightarrow{\phi_2} \\ \xleftarrow{\psi_2} \end{smallmatrix} P_2$	$;$
---	-----

no segundo caso, deduzimos (lema 4.2.7)

$$P_1 = \langle x_i : 1 \leq i \leq n-1 \rangle$$

$$A^{n-1} \xrightleftharpoons[\psi_2]{\phi_2} P_1$$

Os nós β pendentes são da forma

$$A^n \xrightleftharpoons[\psi_1]{\phi_1} P_1$$

$$base(u^{n-k}, A^n)$$

$$(2 \leq k \leq n-1),$$

$$d^{n-k+1} \cdot c^{n-k+1} = Id_k = c^{n-k+1} \cdot d^{n-k+1}$$

$$\psi_1(\phi_1(u_j^{n-k})) = \sum_{i=0}^n c_{ij}^{n-k+1} u_i^{n-k}$$

deduzindo então (lema 4.2.6)

$$P_1 = \langle \phi_1(u_i^{n-k}) : i \leq k-1 \rangle \oplus P_2$$

$$P_2 = \langle z_i : i \leq n-k-1 \rangle$$

$$A^{n-k} \xrightleftharpoons[\psi_2]{\phi_2} P_2$$

Reiniciamos portanto o processo em cada um dos nós, a partir de

$$A^{n-k} \xrightleftharpoons[\psi_2]{\phi_2} P_2, P_1 = M_1 \oplus P_2, FBAS_{M_1},$$

$$P_2 = \langle z_i : i \leq n-k-1 \rangle, base(u, A^{n-k})$$

onde M_1 pode ser eventualmente o módulo nulo ($x = 0$). Finalmente, só resta verificar os nós finais da prova, i.e., o caso $n-k=1$. Genericamente, são nós Θ da forma

$$A \xrightleftharpoons[\psi]{\phi} P_i, P_1 = M \oplus P_i, base_M(y, r, \vec{x}), P_i = \langle v \rangle,$$

$$\forall x \exists \lambda (\phi(x) = \lambda v), \phi(\psi(v)) = v, base(e, A)$$

para algum $0 \leq r \leq n - 1$. De $\psi(v) = ae$ obtemos $v = a\phi(e)$, que juntamente com $\psi(\phi(e)) = ce$, implica $ae = \psi(v) = a\psi(\phi(e)) = (ac)e$, donde $a = ac$. Geramos assim dois nós:

$$\Theta, (\psi(v) = ae), (\psi(\phi(e)) = ce), c \in U,$$

$$\Theta, (\psi(v) = ae), (\psi(\phi(e)) = ce), 1 - c \in U.$$

No primeiro caso, temos que $\phi(e)$ é linearmente independente (lema 4.2.4) e portanto $P_1 = M \oplus \langle \phi(e) \rangle$ é livre com $1 \leq r + 1 \leq n$ geradores linearmente independentes. No segundo caso, $a(1 - c) = 0$ implica $a = 0$ e $v = 0$, mostrando que $P_1 = M$ livre com $0 \leq r \leq n - 1$ geradores linearmente independentes. Assim, temos

$$\Theta, (\psi(v) = ae), (\psi(\phi(e)) = ce), (c \in U) \vee (1 - c \in U) \vdash FBAS_{P_1};$$

como A é um anel local, deduzimos

$$\Theta, (\psi(v) = ae), (\psi(\phi(e)) = ce) \vdash FBAS_{P_1};$$

agora $[\exists L]$ fornece

$$\Theta, \exists a(\psi(v) = ae), \exists c(\psi(\phi(e)) = ce) \vdash FBAS_{P_1}.$$

Este último sequente e $base(e, A) \vdash \exists a(\psi(v) = ae) \otimes \exists c(\psi(\phi(e)) = ce)$ implicam $\Theta \vdash FBAS_{P_1}$. Utilizando o lema 4.1.19 subimos na árvore eliminando as disjunções α , provando o sequente no primeiro nível,

$$\Gamma, \Delta_j, \alpha_j \vdash FBAS_{P_1}.$$

Como visto acima, isto nos dá

$$A \overset{\phi_1}{\underset{\psi_1}{\rightleftarrows}} P_1, P_1 = \langle x_0, \dots, x_{n-1} \rangle, \Delta_{(n)} \vdash FBAS_{P_1}.$$

como desejado.

Vamos agora demonstrar os lemas necessários para completar a prova.

Lema 4.2.3 : *Seja $P_1(x, \vec{x})$ um sub-módulo de P . Então o sequente*

$$\boxed{\begin{array}{l} A \overset{\phi}{\underset{\psi}{\rightleftarrows}} P_1, base(u, A^n), \\ (\forall j \leq n - 1)(\psi(\phi(u_j)) = \sum_{i=0}^n c_{ij}u_i), d \cdot c = Id_n = c \cdot d \end{array}} \vdash P_1 = \langle \phi(u_i) \rangle_{i=0}^{n-1}$$

é provável.

Demonstração: Dado que os tipos envolvidos na prova têm o mesmo extent, não será necessário tomar nenhuma providência com relação à aplicação das regras de inferência. Seja então Γ a sequência de hipóteses do sequente a ser provado. Então

$$\Gamma, (\psi(x) = \sum_{i=0}^n \lambda_i u_i), P_1(x, \vec{x}) \vdash (x = \sum_{i=0}^n \lambda_i \phi(u_i))$$

donde, pela proposição 2.6.4 (20), obtemos

$$P_1(x, \vec{x}), \Gamma, (\psi(x) = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \sum_{i=0}^n \lambda_i \phi(u_i)).$$

Aplicando $[-\circ R]$ e $[\forall R]$, deduzimos $\Gamma \vdash \text{gera}_{P_1}(\phi \circ u, n, \vec{x})$. Para provar a independência linear dos geradores, partimos de

$$\Gamma, (\sum_{j=0}^n \lambda_j \phi(u_j) = 0) \vdash (\sum_{i=0}^n (\sum_{j=0}^n \lambda_j c_{ij}) u_i = 0);$$

lembrando que os u_i 's são linearmente independentes, obtemos

$$\Gamma, (\sum_{j=0}^n \lambda_j \phi(u_j) = 0) \vdash (\forall i \leq n-1) (\sum_{j=0}^n \lambda_j c_{ij} = 0).$$

Logo, por $[E6]$, multiplicando por d_{ki} , com $k \leq n-1$, temos que

$$\Gamma, (\sum_{j=0}^n \lambda_j \phi(u_j) = 0) \vdash (\forall i \leq n-1) (\sum_{j=0}^n \lambda_j c_{ij} d_{ki} = 0),$$

donde, somando sobre os i e permutando a ordem das somatórias, obtemos

$$\begin{aligned} \Gamma, (\sum_{j=0}^n \lambda_j \phi(u_j) = 0) &\vdash (\sum_{j=0}^n \lambda_j (\sum_{i=0}^n c_{ij} d_{ki}) = 0), \\ \Gamma, (\sum_{j=0}^n \lambda_j \phi(u_j) = 0) &\vdash (\sum_{j=0}^n \lambda_j (\sum_{i=0}^n c_{ij} d_{ki}) = \lambda_k), \end{aligned}$$

e assim

$$\Gamma, (\sum_{j=0}^n \lambda_j \phi(u_j) = 0) \vdash \lambda = 0. \quad \square$$

Lema 4.2.4 : *Seja $P_1(x, \vec{x})$ um sub-módulo de P e seja Γ a seguinte sequência de fórmulas:*

$$A^n \xrightleftharpoons[\psi]{\phi} P_1, \text{base}(u, A^n), P_1(x_0, \vec{x}), (\psi(x_0) = au_0), (\psi(\phi(u_0)) = \sum_{i=0}^n c_{i0} u_i).$$

Então os seguintes

$$\Gamma, c_{00} \in U \vdash li_P(\phi \circ u, 1) \quad e \quad \Gamma, 1 - c_{00} \in U \vdash (x_0 = 0)$$

são prováveis.

Demonstração: Podemos escrever

$$\frac{\Gamma \vdash (x_0 = a\phi(u_0))}{\Gamma \vdash (au_0 = ac_{00}u_0 + \sum_{i=1}^n ac_{i0}u_i)};$$

como os (u_i) 's são linearmente independentes, obtemos $\Gamma \vdash (a = ac_{00})$. Logo:

$$\frac{\frac{\Gamma, (c_{00}z = 1), (b\phi(u_0) = 0) \vdash (b\psi(\phi(u_0)) = 0)}{\Gamma, (c_{00}z = 1), (b\phi(u_0) = 0) \vdash (bc_{00}u_0 + \sum_{i=1}^n bc_{i0}u_i = 0)}}{\Gamma, (c_{00}z = 1), (b\phi(u_0) = 0) \vdash (bc_{00} = 0)}$$

portanto, pela proposição 2.6.4 (20), deduzimos

$$\frac{\frac{\Gamma, (c_{00}z = 1), (b\phi(u_0) = 0) \vdash (b = 0)}{(b\phi(u_0) = 0), \Gamma, (c_{00}z = 1) \vdash (b = 0)}}{\Gamma, c_{00} \in U \vdash (\forall b)((b\phi(u_0) = 0) \multimap (b = 0))}.$$

Por outro lado:

$$\Gamma, (a = ac_{00}) \vdash (a(1 - c_{00}) = 0),$$

e então

$$\frac{\Gamma, 1 - c_{00} \in U \vdash (a = 0)}{\Gamma, 1 - c_{00} \in U \vdash (x_0 = 0)}. \quad \square$$

Observação 4.2.5 : Pela descrição dada anteriormente da árvore da prova, vemos que as bases (u_i^k) de A^m (para $m \leq n$) são obtidas da base canônica por combinações lineares (que dependem do ramo). Assim, no nível 1, temos que a base (u_i^1) do ramo j é da forma

$$\begin{aligned} u_i^1 &= \mathbf{e}_i^m + \lambda_i \mathbf{e}_j^m \quad (0 \leq i < j); \\ u_i^1 &= \mathbf{e}_{i+1}^m + \lambda_i \mathbf{e}_j^m \quad (j \leq i \leq m-2); \\ u_{m-1}^1 &= \mathbf{e}_j^m \end{aligned}$$

de maneira que para todo $x \in A^m$ pode ser provado (na lógica) que

$$\begin{aligned} x &= x_0 u_0^1 + \cdots + x_{j-1} u_{j-1}^1 + x_{j+1} u_j^1 + \cdots + x_{m-1} u_{m-2}^1 + b u_{m-1}^1, \\ b &= x_j - (x_0 \lambda_0 + \cdots + x_{j-1} \lambda_{j-1} + x_{j+1} \lambda_j + \cdots + x_{m-1} \lambda_{m-2}). \end{aligned}$$

No nível 2, no ramo $h > j$, a base u_i^2 obtida é da forma

$$\begin{aligned} u_i^2 &= u_i^1 + \lambda_i^1 u_h^1 = \mathbf{e}_i^m + (\lambda_i + \lambda_i^1 \lambda_h) \mathbf{e}_j^m + \lambda_i^1 \mathbf{e}_{h+1}^m \quad (0 \leq i < j); \\ u_i^2 &= u_i^1 + \lambda_i^1 u_h^1 = \mathbf{e}_{i+1}^m + (\lambda_i + \lambda_i^1 \lambda_h) \mathbf{e}_j^m + \lambda_i^1 \mathbf{e}_{h+1}^m \quad (j \leq i < h); \\ u_i^2 &= u_{i+1}^1 + \lambda_i^1 u_h^1 = \mathbf{e}_{i+2}^m + (\lambda_{i+1} + \lambda_i^1 \lambda_h) \mathbf{e}_j^m + \lambda_i^1 \mathbf{e}_{h+1}^m \quad (h \leq i \leq m-2); \\ u_{m-2}^2 &= u_h^1 = \mathbf{e}_{h+1}^m + \lambda_h \mathbf{e}_j^m; \\ u_{m-1}^2 &= u_{m-1}^1 = \mathbf{e}_j^m, \end{aligned}$$

e então pode ser provado (na lógica) que todo $x \in A^m$ se escreve na base (u_i^2) como

$$x = (x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_h, x_{h+2}, \dots, x_{m-1}, a, b)$$

onde

$$a = x_{h+1} - (x_0 \lambda_0^1 + \cdots + x_{j-1} \lambda_{j-1}^1 + x_{j+1} \lambda_j^1 + \cdots + x_h \lambda_{h-1}^1 + x_{h+2} \lambda_h^1 + \cdots + x_{m-1} \lambda_{m-3}^1),$$

$$b = x_j - (x_0\lambda_0 + \cdots + x_{j-1}\lambda_{j-1} + x_{j+1}\lambda_j + \cdots + x_{m-1}\lambda_{m-2}).$$

Os casos em que $h = j$ e $h < j$ são tratados similarmente. Isto significa que, em cada ramo, contamos com termos $\tau_i(x, \vec{\lambda})$ ($i = 0, \dots, m-1$) descrevendo as coordenadas de x na base u^k de A^m , assim como uma fórmula $\gamma(e, u^k, \vec{\lambda})$ descrevendo u^k em função da base canônica e^m de A^m , onde $\vec{\lambda}$ denota uma sequência finita de variáveis do tipo $A^{\tilde{N}}$. Claro que $\tau_i(x, \vec{\lambda})$ e $\gamma(e, u, \vec{\lambda})$ dependem de cada ramo em particular. Esta informação será utilizada na prova. $\square$

Lema 4.2.6 : *Dada um sub-módulo $P_1(x, \vec{x})$ de P , considere as seguintes hipóteses Γ :*

$$\begin{aligned} & A^n \xrightarrow[\psi]{\phi} P_1, \wedge_{i=1}^s \text{Hom}_{PP}(\bar{\pi}_i), \text{base}(u, A^n), \\ & \text{base}(e^{n-k}, A^{n-k}), P_1 = \langle z_i : i \leq n-1 \rangle, \\ & (\forall j \leq n-1)(\psi(\phi(u_j))) = \sum_{i=0}^n c_{ij}u_i, c \cdot d = id_k = d \cdot c, \end{aligned}$$

onde $k \leq n$ e $\bar{\pi}_i$ é uma variável do tipo P^P ($i = 1, \dots, s$). Suponha que P_1 é definido pela fórmula

$$P_1(x, \bar{\pi}_1, \dots, \bar{\pi}_s) \equiv_{\text{def}} (x = x) \wedge (\bar{\pi}_1(x) = x) \wedge \cdots \wedge (\bar{\pi}_s(x) = x),$$

ou $P_1(x) \equiv_{\text{def}} (x = x)$ (em cujo caso, não temos a hipótese $\wedge_{i=1}^s \text{Hom}_{PP}(\bar{\pi}_i)$). Suponha que u é obtida da base canônica e^n após finitas aplicações do processo descrito na observação 4.2.5, codificadas numa fórmula $\gamma(e, u, \vec{\lambda})$ e sejam $\tau_i(x, \vec{\lambda})$ os termos descrevendo as coordenadas de x na base u ($i = 0, \dots, n-1$). Considere Δ formado por $\gamma(e, u, \vec{\lambda})$, junto com as seguintes definições:

$$(\forall x \in A^{\tilde{N}})((\pi_0(x) = \tau_0(x, \vec{\lambda})) \wedge \cdots \wedge (\pi_{n-1}(x) = \tau_{n-1}(x, \vec{\lambda})) \wedge (\forall i \geq n)(\pi_i(x) = 0)),$$

$$(\forall x \in A^{\tilde{N}})(\tilde{\pi}(x) = \sum_{i=k}^n \pi_i(x)e_{i-k}^{n-k}),$$

$$(\forall x \in P)(\bar{\pi}(x) = x - \sum_{j=0}^k (\sum_{i=0}^k \pi_i(\psi(x))d_{ji})\phi(u_j)),$$

$$\psi' = \tilde{\pi} \circ \psi \circ \bar{\pi},$$

$$(\forall x \in A^{\tilde{N}})(\phi'(x) = \sum_{i=0}^{n-k} x_i \bar{\pi} \phi(u_{i+k})),$$

onde π é do tipo $(A^{\tilde{N}})^{(A^{\tilde{N}})}$ e $\pi_i(x)$ denota o termo $\pi(x)(i)$ para $i \in \tilde{N}$ e $x \in A^{\tilde{N}}$. Seja $P_2(x, \vec{y})$ a fórmula

$$P_2(x, \bar{\pi}_1, \dots, \bar{\pi}_s, \bar{\pi}) \equiv_{\text{def}} P_1(x, \bar{\pi}_1, \dots, \bar{\pi}_s) \wedge (\bar{\pi}(x) = x)$$

ou $P_2(x, \bar{\pi}) \equiv_{\text{def}} (x = x) \wedge (\bar{\pi}(x) = x)$, segundo a forma de P_1 . Então, P_2 é um sub-módulo de P e os seguintes sequentes são prováveis:

$$(1) \quad \Gamma, \Delta \vdash \text{Hom}_{A^{\tilde{N}}A^{\tilde{N}}}(\pi) \wedge (\text{Im}(\pi) \subseteq A^n);$$

- (2) $\Gamma, \Delta \vdash Hom_{A^{\tilde{N}} A^{\tilde{N}}}(\tilde{\pi}) \wedge (Im(\tilde{\pi}) \subseteq A^{n-k});$
- (3) $\Gamma, \Delta \vdash Hom_{PP}(\bar{\pi});$
- (4) $\Gamma, \Delta \vdash Hom_{PA^{\tilde{N}}}(\psi') \wedge (Im(\psi') \subseteq A^{n-k});$
- (5) $\Gamma, \Delta \vdash Hom_{A^{\tilde{N}} P}(\phi');$
- (6) $\Gamma, \Delta \vdash (\forall x)(\bar{\pi}(\bar{\pi}(x)) = \bar{\pi}(x));$
- (7) $\Gamma, \Delta, (\bar{\pi}(x) = x), (x = \sum_{i=0}^k \lambda_i \phi(u_i)) \vdash (x = 0);$
- (8) $\Gamma, \Delta \vdash li_P(\phi \circ u, k);$
- (9) $\Gamma, \Delta \vdash P = \langle\langle \phi(u_i) : i \leq k-1 \rangle\rangle \oplus \{x : \bar{\pi}(x) = x\};$
- (10) $\Gamma, \Delta, P_2(x, \vec{y}) \vdash (\exists \lambda)(x = \sum_{i=k}^n \lambda_i \bar{\pi} \phi(u_i));$
- (11) $\Gamma, \Delta, (x = \sum_{i=k}^n \lambda_i \bar{\pi} \phi(u_i)) \vdash P_2(x, \vec{y});$
- (12) $\Gamma, \Delta \vdash \phi' \circ (\psi'_{|P_2}) = id_{P_2};$
- (13) $\Gamma, \Delta \vdash Im \phi' \subseteq P_2;$
- (14) $\Gamma, \Delta \vdash P_1 = \langle\langle \phi(u_i) : i \leq k-1 \rangle\rangle \oplus P_2;$
- (15) $\Gamma, \Delta, P = M_1 \oplus P_1 \vdash P = (M_1 \oplus \langle\langle \phi(u_i) : i \leq k-1 \rangle\rangle) \oplus P_2.$

Demonstração: As propriedades (1)-(5) são imediatas.

(6) : Por definição, temos que

$$\Gamma, \Delta \vdash (\bar{\pi}(\bar{\pi}x) = \bar{\pi}x - \sum_{j=0}^k (\sum_{i=0}^k \pi_i(\psi(\bar{\pi}x)) d_{ji}) \phi(u_j)) \quad (*).$$

Por outro lado, se a_i denota $\pi_i(\psi(x))$ ($i \leq n-1$), podemos escrever

$$\frac{\frac{\Gamma, \Delta \vdash \psi(\bar{\pi}x) = \psi x - \sum_{j=0}^k (\sum_{i=0}^k a_i d_{ji}) \sum_{h=0}^n c_{hj} u_h}{\Gamma, \Delta \vdash \psi(\bar{\pi}x) = \psi x - \sum_{i=0}^k a_i (\sum_{h=0}^k (\sum_{j=0}^k d_{ji} c_{hj}) u_h) - \sum_{h=k}^n (\sum_{i=0}^k (\sum_{j=0}^k a_i d_{ji} c_{hj})) u_h}}{\Gamma, \Delta \vdash \psi(\bar{\pi}x) = \psi x - \sum_{i=0}^k a_i u_i - \sum_{h=k}^n (\sum_{i=0}^k (\sum_{j=0}^k a_i d_{ji} c_{hj})) u_h} \\ \hline \Gamma, \Delta \vdash \psi(\bar{\pi}x) = \sum_{h=k}^n (a_h - \sum_{i=0}^k (\sum_{j=0}^k a_i d_{ji} c_{hj})) u_h$$

pois

$$\Gamma, \Delta \vdash (\psi x = \sum_{i=0}^n \pi_i(\psi(x)) u_i).$$

Assim, temos que

$$\frac{\frac{\Gamma, \Delta \vdash (\forall i \leq k-1) (\pi_i(\psi(\bar{\pi}x)) = 0)}{\Gamma, \Delta \vdash (\forall j \leq k-1) (\sum_{i=0}^k \pi_i(\psi(\bar{\pi}x)) d_{ji} = 0)}}{\Gamma, \Delta \vdash \sum_{j=0}^k (\sum_{i=0}^k \pi_i(\psi(\bar{\pi}x)) d_{ji}) \phi(u_j) = 0}$$

e o resultado segue de (*).

(7) : Observe que

$$\Gamma, \Delta, (x = \sum_{j=0}^k \lambda_j \phi(u_j)) \vdash (\psi x = \sum_{i=0}^n (\sum_{j=0}^k \lambda_j c_{ij}) u_i).$$

Como

$$\Gamma, \Delta \vdash (\psi x = \sum_{i=0}^n \pi_i(\psi(x)) u_i),$$

obtemos

$$\Gamma, \Delta, (x = \sum_{j=0}^k \lambda_j \phi(u_j)) \vdash (\forall i \leq k-1) (\sum_{j=0}^k \lambda_j c_{ij} = \pi_i(\psi(x))).$$

Mas, pela prova de (6) acima,

$$\Gamma, \Delta, (x = \bar{\pi}x) \vdash (\forall i \leq k-1) (\pi_i(\psi(x)) = 0)$$

e então

$$\frac{\frac{\Gamma, \Delta, x = \bar{\pi}x, x = \sum_{j=0}^k \lambda_j \phi(u_j) \vdash (\forall i \leq k-1) (\sum_{j=0}^k \lambda_j c_{ij} = 0)}{\Gamma, \Delta, x = \bar{\pi}x, x = \sum_{j=0}^k \lambda_j \phi(u_j) \vdash \sum_{i=0}^k (\sum_{j=0}^k \lambda_j c_{ij}) = 0}}{\frac{\Gamma, \Delta, x = \bar{\pi}x, x = \sum_{j=0}^k \lambda_j \phi(u_j) \vdash (\forall h \leq k-1) (\sum_{i=0}^k (\sum_{j=0}^k \lambda_j c_{ij} d_{hi}) = 0)}{\Gamma, \Delta, x = \bar{\pi}x, x = \sum_{j=0}^k \lambda_j \phi(u_j) \vdash (\forall h \leq k-1) (\lambda_h = 0)}} ,$$

completando a prova de (7).

(8) : A prova é análoga à do lema 4.2.3.

(9) : Queremos provar

$$\Gamma, \Delta \vdash (\forall x)(\exists y)(\exists z)\delta(x, y, z) \wedge (\forall x)(\forall y)(\forall z)(\forall y')(\forall z')(\delta(x, y, z) \otimes \delta(x, y', z') \multimap (y = y') \wedge (z = z')),$$

$$\delta(x, y, z) \equiv_{def} (\bar{\pi}y = y) \otimes (\exists \lambda)(z = \sum_{i=0}^k \lambda_i \phi(u_i)) \otimes (x = y + z).$$

Para provar a primeira parte, temos que

$$\frac{x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j) \vdash ((x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j)) \otimes (\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j))) [a/\lambda]}{x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j) \vdash (\exists \lambda)((x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j)) \otimes (\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j)))} (*) .$$

Como

$$\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j) \vdash (\exists \lambda)(\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j)),$$

de $[\otimes R]$ e $[\otimes L]$ vem

$$\begin{aligned} & (x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j)) \otimes (\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j)) \\ & \vdash (x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j)) \otimes (\exists \lambda)(\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j)) \end{aligned}$$

Aplicando $[\exists L]$ com relação a λ e depois $[CUT]$ com $(*)$ acima, teremos

$$x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j) \vdash (x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j)) \otimes (\exists \lambda)(\sum_{j=0}^k a_j \phi(u_j) = \sum_{j=0}^k \lambda_j \phi(u_j)) \quad (**).$$

Fazendo $a_j \equiv_{def} \sum_{i=0}^k \pi_i(\psi(x))d_{ji}$, temos

$$\Gamma, \Delta \vdash (x = \bar{\pi}x + \sum_{j=0}^k a_j \phi(u_j))$$

e então, $[CUT]$ e $(**)$ fornecem

$$\Gamma, \Delta \vdash (x = y + z) \otimes (\exists \lambda)(z = \sum_{j=0}^k \lambda_j \phi(u_j)) [\sum a_j \phi(u_j) / z] [\bar{\pi}x / y].$$

Por (6), temos que

$$\Gamma, \Delta \vdash \bar{\pi}(\bar{\pi}x) = \bar{\pi}x$$

portanto, a regra $[\otimes R]$, a proposição 2.6.4 (13) e as regras de quantificação nos fornecem

$$\frac{\Gamma, \Delta \vdash (\bar{\pi}y = y) \otimes (\exists \lambda)(z = \sum_{j=0}^k \lambda_j \phi(u_j)) \otimes (x = y + z) [\sum a_j \phi(u_j) / z] [\bar{\pi}x / y]}{\Gamma, \Delta \vdash (\forall x)(\exists y)(\exists z)((\bar{\pi}y = y) \otimes (\exists \lambda)(z = \sum_{j=0}^k \lambda_j \phi(u_j)) \otimes (x = y + z))}.$$

Para provar a unicidade da decomposição, partimos de

$$(\exists \lambda)(z = \sum_{i=0}^k \lambda_i \phi(u_i)), (\exists \lambda')(z' = \sum_{i=0}^k \lambda'_i \phi(u_i)) \vdash (\exists \lambda'')(z' - z = \sum_{i=0}^k \lambda''_i \phi(u_i)).$$

Além disso, $[SUBS]$ garante que

$$\frac{(\exists \lambda'')(z' - z = \sum_{i=0}^k \lambda''_i \phi(u_i)), (y - y' = z' - z) \vdash (\exists \lambda'')(y - y' = \sum_{i=0}^k \lambda''_i \phi(u_i))}{\bar{\pi}(y - y') = y - y', (\exists \lambda'')(z' - z = \sum_{i=0}^k \lambda''_i \phi(u_i)), (y - y' = z' - z) \vdash \sigma}$$

onde $\sigma \equiv_{def} (\bar{\pi}(y - y') = y - y') \otimes (\exists \lambda'')(y - y' = \sum_{i=0}^k \lambda''_i \phi(u_i))$. Por (7), temos

$$\Gamma, \Delta, \sigma \vdash (y - y' = 0)$$

e então, pela proposição 2.6.4 (20), obtemos

$$(\bar{\pi}(y - y') = y - y'), (\exists \lambda'')(z' - z = \sum_{i=0}^k \lambda''_i \phi(u_i)), (y - y' = z' - z), \Gamma, \Delta \vdash (y - y' = 0).$$

Por outro lado, temos que

$$(y - y' = 0), (y - y' = z' - z) \vdash (z' - z = 0),$$

$$(y - y' = 0) \vdash (y = y'), \quad (z' - z = 0) \vdash (z = z'),$$

donde

$$\bar{\pi}(y - y') = y - y', (\exists \lambda'')(z' - z = \sum_{i=0}^k \lambda''_i \phi(u_i)), (y - y' = z' - z), \Gamma, \Delta \vdash (y = y') \wedge (z = z').$$

Finalmente, de

$$(x = y + z), (x = y' + z') \vdash (y - y' = z' - z),$$

$$(\bar{\pi}y = y), (\bar{\pi}y' = y'), Hom_{PP}(\bar{\pi}) \vdash (\bar{\pi}(y - y') = y - y')$$

provamos

$$\delta(x, y, z), \delta(x, y', z'), \Gamma, \Delta \vdash (y = y') \wedge (z = z'),$$

e o resultado segue das regras $[\otimes L]$, $[-\circ R]$ e $[\forall R]$.

(10) : Pela prova de (6),

$$\Gamma, \Delta, (\bar{\pi}x = x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (\psi x = \sum_{i=k}^n \lambda_i u_i).$$

Por outro lado,

$$\Gamma, \Delta, P_1(x) \vdash (\phi(\psi(x)) = x)$$

e então obtemos

$$\Gamma, \Delta, P_2(x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \sum_{i=k}^n \lambda_i \phi(u_i)).$$

Dado que

$$(\bar{\pi}x = x), (x = \sum_{i=k}^n \lambda_i \phi(u_i)), Hom_{PP}(\bar{\pi}) \vdash (x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i)),$$

então

$$\frac{\Gamma, \Delta, P_2(x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i))}{\Gamma, \Delta, P_2(x), (\exists \lambda)(\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (\exists \lambda)(x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i))}$$

donde segue-se o resultado, pois

$$\Gamma, \Delta \vdash (\exists \lambda)(\psi x = \sum_{i=0}^n \lambda_i u_i).$$

(11) : Dado que $Im \phi \subseteq P_1$ e que P_1 satisfaz $\Gamma, P_1(x), P_1(y) \vdash P_1(x + y)$, então, pela definição de $\bar{\pi}$, prova-se que

$$\Gamma, \Delta, P_1(x) \vdash P_1(\bar{\pi}x).$$

Logo,

$$\Gamma, \Delta, (x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i)) \vdash P_1(x) \quad (*).$$

Por outro lado,

$$\Gamma, \Delta, (x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i)) \vdash (x = \bar{\pi}(\sum_{i=k}^n \lambda_i \phi(u_i)))$$

e então, por (6),

$$\Gamma, \Delta, (x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i)) \vdash (\bar{\pi}x = x),$$

portanto, por (*), obtemos

$$\Gamma, \Delta, (x = \sum_{i=k}^n \lambda_i \bar{\pi}\phi(u_i)) \vdash P_2(x).$$

(12) : Temos que

$$\Gamma, \Delta, (\bar{\pi}x = x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (\psi' x = \sum_{i=k}^n \lambda_i e_{i-k}^{n-k})$$

e então

$$\Gamma, \Delta, (\bar{\pi}x = x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (\phi' \psi' x = \sum_{i=k}^n \lambda_i \bar{\pi} \phi u_i) \quad (*).$$

Por outro lado, pela prova de (10),

$$\Gamma, \Delta, P_2(x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \sum_{i=k}^n \lambda_i \bar{\pi} \phi u_i),$$

donde segue-se, por (*) e pela proposição 2.6.4 (20),

$$\frac{\frac{\frac{\Gamma, \Delta, P_2(x), (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \phi' \psi' x)}{P_2(x), \Gamma, \Delta, (\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \phi' \psi' x)}}{P_2(x), \Gamma, \Delta, (\exists \lambda)(\psi x = \sum_{i=0}^n \lambda_i u_i) \vdash (x = \phi' \psi' x)}}{\frac{P_2(x), \Gamma, \Delta \vdash (x = \phi' \psi' x)}{\Gamma, \Delta \vdash (\forall x)(P_2(x) \multimap (x = \phi' \psi' x))}}$$

como desejado.

(13) : Por definição,

$$\Gamma, \Delta, (x = \sum_{i=0}^k \lambda_i e_i^{n-k}) \vdash (\phi' x = \sum_{i=k}^n \lambda_{i-k} \bar{\pi} \phi(u_i)).$$

Logo, por (11),

$$\frac{\frac{\frac{\Gamma, \Delta, (x = \sum_{i=0}^k \lambda_i e_i^{n-k}) \vdash P_2(\phi' x)}{\Gamma, \Delta, (\exists \lambda)(x = \sum_{i=0}^k \lambda_i e_i^{n-k}) \vdash P_2(\phi' x)}}{\Gamma, \Delta \vdash P_2(\phi' x)}}{\Gamma, \Delta \vdash (\forall x) P_2(\phi' x)}$$

como queríamos provar.

(14) : Da definição de P_2 vem

$$\Gamma, \Delta, P_1(x), (x = y + z), (\bar{\pi}y = y), (z = \sum_{i=0}^k \lambda_i \phi(u_i)) \vdash P_2(y)$$

(pois $y = x - z$, e vale $P_1(x), P_1(z)$). Logo,

$$\Gamma, \Delta, P_1(x), (x = y + z), (\bar{\pi}y = y), (z = \sum_{i=0}^k \lambda_i \phi(u_i)) \vdash (x = y + z) \otimes P_2(y) \otimes (\exists \lambda)(z = \sum_{i=0}^k \lambda_i \phi(u_i))$$

e então, por (9) e $[\exists R]$, obtemos

$$\Gamma, \Delta, P_1(x) \vdash (\exists y)(\exists z)((x = y + z) \otimes P_2(y) \otimes (\exists \lambda)(z = \sum_{i=0}^k \lambda_i \phi(u_i)))$$

como queríamos provar.

(15) : É uma consequência imediata de (14). $\square$

Lema 4.2.7 : Com a notação do lema 4.2.6, considere as seguintes hipóteses Γ :

$$\begin{aligned} & A^n \xrightarrow[\psi]{\phi} P_1, \text{ base}(u, A^n), \\ & \text{base}(\mathbf{e}^{n-1}, A^{n-1}), P_1 = \langle z_i : i \leq n-1 \rangle, \\ & (z_0 = 0), (\forall j \leq n-1)(\phi(u_j) = \sum_{i=1}^n b_{ji} z_i). \end{aligned}$$

Considere Δ formado por $\gamma(\mathbf{e}, u, \vec{\lambda})$ (a definição de u a partir de $\mathbf{e}^n$) junto com as seguintes definições:

$$\begin{aligned} & (\forall x \in A^{\tilde{N}})((\pi_0(x) = \tau_0(x, \vec{\lambda})) \wedge \cdots \wedge (\pi_{n-1}(x) = \tau_{n-1}(x, \vec{\lambda})) \wedge (\forall i \geq n)(\pi_i(x) = 0)), \\ & (\forall x \in P)(\psi'(x) = \sum_{i=0}^{n-1} (\sum_{j=0}^n \pi_j(\psi(x)) b_{j \ i+1}) \mathbf{e}_i^{n-1}), \\ & (\forall x \in A^{\tilde{N}})(\phi'(x) = \sum_{i=0}^{n-1} x_i z_{i+1})). \end{aligned}$$

Então, os seguintes sequentes são prováveis:

- (1) $\Gamma, \Delta \vdash \text{Hom}_{PA^{\tilde{N}}}(\psi') \wedge (\text{Im}(\psi') \subseteq A^{n-1});$
- (2) $\Gamma, \Delta \vdash \text{Hom}_{A^{\tilde{N}}P}(\phi');$
- (3) $\Gamma, \Delta \vdash \phi' \circ (\psi'_{|P_1}) = \text{id}_{P_1};$
- (4) $\Gamma, \Delta \vdash \text{Im } \phi' \subseteq P_1.$

Demonstração: As propriedades (1) e (2) são óbvias.

(3) : Temos que

$$\frac{\Gamma, \Delta \vdash \psi x = \sum_{j=0}^n \pi_j(\psi(x)) u_j}{\Gamma, \Delta, P_1(x) \vdash x = \sum_{j=0}^n \pi_j(\psi(x)) \phi(u_j)}.$$

Por outro lado,

$$\frac{\frac{\Gamma, \Delta \vdash \phi' \psi' x = \sum_{i=0}^{n-1} (\sum_{j=0}^n \pi_j(\psi(x)) b_{j \ i+1}) z_{i+1}}{\Gamma, \Delta \vdash \phi' \psi' x = \sum_{j=0}^n \pi_j(\psi(x)) (\sum_{i=0}^{n-1} b_{j \ i+1} z_{i+1})}}{\Gamma, \Delta \vdash \phi' \psi' x = \sum_{j=0}^n \pi_j(\psi(x)) \phi(u_j)}$$

donde segue-se o resultado.

(4) : Imediato, pela definição de ϕ' . $\square$

Lema 4.2.8 : Com a notação do lema 4.2.6, considere as seguintes hipóteses Γ :

$$\begin{aligned} & A^n \xrightarrow[\psi]{\phi} P_1, \wedge_{i=1}^s \text{Hom}_{PP}(\pi_i), \text{ base}(u, A^n), \\ & \text{base}(\mathbf{e}^{n-1}, A^{n-1}), P_1 = \langle z_i : i \leq n-1 \rangle, \end{aligned}$$

$$\psi(\phi(u_0)) = \sum_{i=0}^n c_{i0}u_i, \quad (c_{00}w_0 = 1 \wedge w_0c_{00} = 1).$$

Suponha que P_1 é definido pela fórmula

$$P_1(x, \bar{\pi}_1, \dots, \bar{\pi}_s) \equiv_{def} (x = x) \wedge (\bar{\pi}_1(x) = x) \wedge \dots \wedge (\bar{\pi}_s(x) = x),$$

ou $P_1(x) \equiv_{def} (x = x)$ (em cujo caso, não temos a hipótese $\bigwedge_{i=1}^s Hom_{PP}(\bar{\pi}_i)$). Considere Δ formado por $\gamma(\mathbf{e}, u, \vec{\lambda})$ (definindo u a partir de $\mathbf{e}^n$) junto com as seguintes definições:

$$(\forall x \in A^{\tilde{N}})((\pi_0(x) = \tau_0(x, \vec{\lambda})) \wedge \dots \wedge (\pi_{n-1}(x) = \tau_{n-1}(x, \vec{\lambda})) \wedge (\forall i \geq n)(\pi_i(x) = 0)),$$

$$(\forall x \in A^{\tilde{N}})(\tilde{\pi}(x) = \sum_{i=1}^n \pi_i(x) \mathbf{e}_{i-1}^{n-1}),$$

$$(\forall x \in P)(\bar{\pi}(x) = x - \pi_0(\psi(x))w_0\phi(u_0)),$$

$$\psi' = \tilde{\pi} \circ \psi \circ \bar{\pi},$$

$$(\forall x \in A^{\tilde{N}})(\phi'(x) = \sum_{i=0}^{n-1} x_i \bar{\pi} \phi(u_{i+1})).$$

Seja $P_2(x, \vec{y})$ a fórmula

$$P_2(x, \bar{\pi}_1, \dots, \bar{\pi}_s, \bar{\pi}) \equiv_{def} P_1(x, \bar{\pi}_1, \dots, \bar{\pi}_s) \wedge (\bar{\pi}(x) = x)$$

ou $P_2(x, \bar{\pi}) \equiv_{def} (x = x) \wedge (\bar{\pi}(x) = x)$, segundo a forma de P_1 . Então, P_2 é um sub-módulo de P e os seguintes sequentes são prováveis:

- (1) $\Gamma, \Delta \vdash Hom_{PA^{\tilde{N}}}(\psi') \wedge (Im(\psi') \subseteq A^{n-1});$
- (2) $\Gamma, \Delta \vdash Hom_{A^{\tilde{N}}P}(\phi');$
- (3) $\Gamma, \Delta \vdash li_P(\phi \circ u, 1);$
- (4) $\Gamma, \Delta \vdash P = \langle\langle \phi(u_0) \rangle\rangle \oplus \{x : \bar{\pi}(x) = x\};$
- (5) $\Gamma, \Delta, P_2(x, \vec{y}) \vdash (\exists \lambda)(x = \sum_{i=1}^n \lambda_i \bar{\pi} \phi(u_i));$
- (6) $\Gamma, \Delta, (x = \sum_{i=1}^n \lambda_i \bar{\pi} \phi(u_i)) \vdash P_2(x, \vec{y});$
- (7) $\Gamma, \Delta \vdash \phi' \circ (\psi'_{|P_2}) = id_{P_2};$
- (8) $\Gamma, \Delta \vdash Im \phi' \subseteq P_2;$
- (9) $\Gamma, \Delta \vdash P_1 = \langle\langle \phi(u_0) \rangle\rangle \oplus P_2;$
- (10) $\Gamma, \Delta, P = M_1 \oplus P_1 \vdash P = (M_1 \oplus \langle\langle \phi(u_0) \rangle\rangle) \oplus P_2.$

Demonstração: Isto é um caso particular do lema 4.2.6 com $k = 1$. $\square$

Finalmente, devemos fazer duas observações com relação à finalização da prova. No lema 4.2.6, temos a sequência de definições Δ formada por $\gamma(\mathbf{e}, u, \vec{\lambda})$, junto com

$$\sigma(\pi, \vec{\lambda}) \equiv_{def} (\forall x \in A^{\tilde{N}})((\pi_0(x) = \tau_0(x, \vec{\lambda})) \wedge \dots \wedge (\pi_{n-1}(x) = \tau_{n-1}(x, \vec{\lambda})) \wedge (\forall i \geq n)(\pi_i(x) = 0)),$$

$$\begin{aligned}
\theta_1(\pi, \mathbf{e}, \tilde{\pi}) &\equiv_{def} (\forall x \in A^{\tilde{N}})(\tilde{\pi}(x) = \sum_{i=k}^n \pi_i(x) \mathbf{e}_{i-k}^{n-k}), \\
\theta_2(\pi, d, \phi, u, \bar{\pi}) &\equiv_{def} (\forall x \in P)(\bar{\pi}(x) = x - \sum_{j=0}^k (\sum_{i=0}^k \pi_i(\psi(x)) d_{ji}) \phi(u_j)), \\
\theta_3(\tilde{\pi}, \psi, \bar{\pi}, \psi') &\equiv_{def} (\psi' = \tilde{\pi} \circ \psi \circ \bar{\pi}), \\
\theta_4(u, \phi, \bar{\pi}, \phi') &\equiv_{def} (\forall x \in A^{\tilde{N}})(\phi'(x) = \sum_{i=0}^{n-k} x_i \bar{\pi} \phi(u_{i+k})).
\end{aligned}$$

que deve ser quantificada, para obter hipóteses válidas. Para isso, uma vez que provamos (utilizando eventualmente uma sequência adicional Σ de sentenças válidas)

$$\Gamma, \Delta, \Sigma \vdash FBAS_{P_1}$$

aplicamos as regras de quantificação, obtendo:

$$\begin{array}{l}
\Gamma, \gamma(\mathbf{e}, u, \vec{\lambda}), \sigma(\pi), \theta_1(\pi, \mathbf{e}, \tilde{\pi}), \theta_2(\pi, d, \phi, u, \bar{\pi}), \\
(\forall \tilde{\pi})(\forall \psi)(\forall \bar{\pi})(\exists \psi') \theta_3(\tilde{\pi}, \psi, \bar{\pi}, \psi'), \\
(\forall u)(\forall \phi)(\forall \bar{\pi})(\exists \phi') \theta_4(u, \phi, \bar{\pi}, \phi'), \Sigma
\end{array} \vdash FBAS_{P_1}$$

e depois

$$\begin{array}{l}
\Gamma, \gamma(\mathbf{e}, u, \vec{\lambda}), \sigma(\pi), (\forall \pi)(\exists \tilde{\pi}) \theta_1(\pi, \mathbf{e}, \tilde{\pi}), \\
(\forall u)(\forall d)(\forall \pi)(\forall \phi)(\exists \bar{\pi}) \theta_2(\pi, d, \phi, u, \bar{\pi}), \\
(\forall \tilde{\pi})(\forall \psi)(\forall \bar{\pi})(\exists \psi') \theta_3(\tilde{\pi}, \psi, \bar{\pi}, \psi'), \\
(\forall u)(\forall \phi)(\forall \bar{\pi})(\exists \phi') \theta_4(u, \phi, \bar{\pi}, \phi'), \Sigma
\end{array} \vdash FBAS_{P_1}$$

e finalmente

$$\begin{aligned}
&\Gamma, (\forall \vec{\lambda})(\exists u)\gamma(\mathbf{e}, u, \vec{\lambda}), (\exists \pi)\sigma(\pi), (\forall \pi)(\exists \tilde{\pi})\theta_1(\pi, \mathbf{e}, \tilde{\pi}), \\
&(\forall u)(\forall d)(\forall \pi)(\forall \phi)(\exists \bar{\pi})\theta_2(\pi, d, \phi, u, \bar{\pi}), \\
&(\forall \tilde{\pi})(\forall \psi)(\forall \bar{\pi})(\exists \psi')\theta_3(\tilde{\pi}, \psi, \bar{\pi}, \psi'), \\
&(\forall u)(\forall \phi)(\forall \bar{\pi})(\exists \phi')\theta_4(u, \phi, \bar{\pi}, \phi'), \Sigma
\end{aligned}$$

$\vdash FBAS_{P_1}$

obtendo claramente hipóteses válidas. O mesmo tipo de raciocínio é aplicado nos lemas 4.2.7 e 4.2.8.

Por último, devemos ressaltar que o módulo nulo ($x = 0$) é livre, com base $\{z_i : i < 0\}$ para z a sequência vazia em P (a qual é finita). Com efeito, suponha que M é dado pela fórmula $M(x) \equiv_{def} (x = 0)$. Os seguintes

$$EA \vdash (\forall i < 0)M(z_i), \quad EA \vdash (\forall x)(M(x) \rightarrow (\exists \lambda)(x = \sum_{i=0}^0 \lambda_i z_i)),$$

$$(\sum_{i=0}^0 \lambda_i z_i = 0) \vdash (\forall i < 0)(\lambda_i = 0)$$

são prováveis, por causa do sequente válido $i < 0 \vdash$. Logo, temos que

$$EA \vdash (\forall i < 0)M(z_i) \wedge gera_M(z, 0) \wedge li_M(z, 0),$$

portanto obtemos $EA \vdash (\exists z \in P^{\tilde{N}})((\forall i < 0)M(z_i) \wedge base_M(z, 0))$.

Isto completa a prova do Teorema 4.2.2. $\square$

Observação 4.2.9 : Na prova do teorema, foram feitas algumas demonstrações por indução interna a partir de fórmulas $\phi(x)$ **sem disjunções**, sendo portanto válidas. Para permitir provas por indução em geral, deveríamos modificar a definição de prova 2.5.1, adicionando o item seguinte:

(6) O sequente S_i é uma instância de $[ind]$, de maneira que existe uma justificativa x em **clau** $([ind])$ tal que para todo sequente S' em x diferente de $\vdash \top$ temos que $S' = S_j$ para algum $j < i$. $\square$

Bibliografia

- [Ak1] C.A. Akemann, The General Stone-Weierstrass Problem, *Journal of Functional Analysis* 4 (1969), 277-294.
- [Ak2] C.A. Akemann, Left Ideal Structure of C^* -Algebras, *Journal of Functional Analysis* 6 (1970), 305-317.
- [Ak3] C.A. Akemann, A Gelfand Representation Theory for C^* -Algebras, *Pacific Journal of Mathematics*, Vol. 39, No. 1 (1971), 1-11.
- [BBC] U. Berni, F. Borceaux, R. Cruciani, A Theory of Quantal Sets, *J. of Pure and Applied Algebra* 62 (1989), 123-136.
- [BC1] F. Borceaux, R. Cruciani, Sheaves on a Quantale, *Cahiers de Topologie et Géom. Diff. Cat.* vol. XXXIV-3 (1993), 209-228.
- [BC2] F. Borceaux, R. Cruciani, A Generic Representation Theorem for Non-commutative Rings, *J. of Algebra* 167 (1994), 291-308.
- [BvB1] F. Borceaux, G. van den Bossche, Quantales and their Sheaves, *Order* 3 (1986), 61-87.
- [BvB2] F. Borceaux, G. van den Bossche, An Essay on Noncommutative Topology, *Topology and its Applications* 31 (1989), 203-223.
- [BvB3] F. Borceaux, G. van den Bossche, A Generic Sheaf Representation for Rings, *Lecture Notes in Mathematics* 1488 (1991), 30-42.
- [BvdBR] F. Borceaux, G. van den Bossche, J. Rosický, Quantales and C^* -algebras, a appearer no *Jour. of London Math. Soc.*
- [BG] C. Brown, D. Gurr, A Representation Theorem for Quantales, *Journal of Pure and Applied Algebra* 85 (1993), 27-42.
- [BS] J.L. Bell, A.B. Slomson, **Models and Ultraproducts: An Introduction** (1971), North-Holland, Amsterdam.

- [BvN] G. Birkhoff, J. von Neumann, The Logic of Quantum Mechanics, *Annals of Mathematics* 37, No. 4 (1936), 823-843.
- [Dix] J. Dixmier, **Les C^* -algèbres et leurs Représentations** (1964), Gauthiers-Villars, Paris.
- [FS] M.P. Fourman, D.S. Scott, Sheaves and Logic, *Lecture Notes in Mathematics* 753 (1979), 302-401.
- [Gir] J.Y. Girard, Linear Logic, *Theoretical Computer Science* 50 (1987), 1-102.
- [G1] J.Y. Girard, Towards a Geometry of Interaction, *Contemporary Mathematics* 92 (1989), 69-108.
- [Gi1] R. Giles, Foundations for Quantum Mechanics, *Journal of Mathematical Physics*, Vol. 11, No. 7 (1970), 2139-2160.
- [GK] R. Giles, H. Kummer, A Non-Commutative Generalization of Topology, *Indiana University Mathematics Journal*, Vol. 21, No. 1 (1971), 91-102.
- [Hof] K.H. Hofmann, Representation of Algebras by Continuous Sections, *Bull. of the A.M.S.* 78, No. 3 (1972).
- [Joh] P. Johnstone, **Stone Spaces** (1982), Cambridge University Press, Cambridge.
- [Kap] I. Kaplansky, Projective Modules, *Annals of Mathematics* 68 (1958), 372-377.
- [Law] F.W. Lawvere, Quantifiers and Sheaves, *Actes de Congres International des Maths.*, Nice (1970), 329-334.
- [MR] M. Makkai, G.E. Reyes, **First-Order Categorical Logic**, *Lecture Notes in Mathematics* 611 (1977).
- [Mir] F. Miraglia, **Sheaves and Logic**, preprint.
- [MS] F. Miraglia, U. Solitro, Sheaves Over Right Sided Idempotent Quantales, *Équipe de Logique Mathématique, Paris VII* (1992), a appear no *Journal of the IGPL (Interest Group in Pure and Applied Logics)*, 87 p., 1997.
- [MP1] C.J. Mulvey, J.W. Pelletier, A Quantisation of the calculus of Relations, *Can. Math. Soc. Conference Proceeding* 13 (1992), 345-360.

- [MP2] C.J.Mulvey, J.W. Pelletier, On the Quantisation of Points, preprint.
- [Mul1] C.J. Mulvey, Intuitionistic Algebra and Representations of Rings, *Memoirs of the American Mathematical Society* 148 (1974), 3-57.
- [Mu2] C.J. Mulvey, &, *Suppl. Rend. Circ. Mat. Palermo Ser. II*, 12 (1986), 99-104.
- [Naw] M. Nawaz, *Quantales: Quantal sets*, Thesis (1985), Sussex University.
- [Pel] J.W. Pelletier, *von Neumann Algebras and Hilbert Quantales*, a appearer no *Applied Categorical Structures*.
- [PR] J.W. Pelletier, J. Rosický, *Simple Involutive Quantales*, York University, Report no. 96-02.
- [Ros] K.I. Rosenthal, **Quantales and their Applications**, Pitman Research Notes in Math., vol. 234, Longman Scientific & Technical, Essex, UK (1990).
- [Sco] D.S. Scott, *Identity and Existence in Intuitionistic Logic*, *Lecture Notes in Mathematics* 753 (1979), 660-696.
- [Urs] A. Ursini, *Semantical Investigations of Linear Logic*, *Università di Siena, Rapp. Mat.* no. 291 (1995).
- [vdB] G. van den Bossche, *Quantaloids and Non-Commutative Ring Representations*, *Applied Categorical Structures* 3 (1995), 305-320.
- [WD] M. Ward, R.P. Dilworth, *Residuated Lattices*, *Trans. Amer. Math. Soc.* 45 (1939), 335-354.
- [Yet] D. Yetter, *Quantales and (Noncommutative) Linear Logic*, *Journal of Symbolic Logic* 55 (1990), 41-64.

Equality in Linear Logic

EQUALITY IN LINEAR LOGIC

Marcelo E. Coniglio

Francisco Miraglia

Instituto de Matemática e Estatística da Universidade de São Paulo

1 Quantales

In this section we introduce the basic definitions and results of the theory of quantales (a good reference is [Ros]). Quantales were introduced by Mulvey ([Mul]) as an algebraic tool for studying representations of non-commutative C^* -algebras. Informally, a quantale is a complete lattice Q equipped with a product distributive over arbitrary sup's. The importance of quantales for Linear Logic is revealed in Yetter's work ([Yet]), who proved that semantics of classical linear logic is given by a class of quantales, named Girard quantales, which coincides with Girard's phase semantics. An analogous result is obtained for a sort of non-commutative linear logic, as well as intuitionistic linear logic without negation, which suggest that the utilisation of the theory of quantales (or even weaker structures, such that $*$ -autonomous posets) might be fruitful in studying the semantic of several variants of linear logic.

As usual, we denote the order in a lattice by $\leq$, while $\vee$ and $\wedge$ denote the operations of sup and inf, respectively. We write $\top$ for the largest element in a lattice and $\mathbf{0}$ for its smallest element.

Definition 1.1 A *quantale* is a complete lattice Q with an associative binary operation $\otimes : Q \times Q \longrightarrow Q$, which distributes on the right and on the left of arbitrary sup's, i.e.:

$$[Q1] \quad a \otimes (b \otimes c) = (a \otimes b) \otimes c, \text{ for every } a, b, c \in Q$$

$$[Q2] \quad a \otimes (\vee_{i \in I} a_i) = \vee_{i \in I} (a \otimes a_i), \quad (\vee_{i \in I} a_i) \otimes a = \vee_{i \in I} (a_i \otimes a)$$

A quantale Q is *unital* if it has an element $\mathbf{1} \in Q$ such that $a \otimes \mathbf{1} = \mathbf{1} \otimes a = a$, for every $a \in Q$. A quantale Q is *commutative* if $a \otimes b = b \otimes a$, for every $a, b \in Q$.

A *morphism of quantales* is an operator between quantales which preserves $\otimes$ and arbitrary sup's.

It's easily seen that the above axioms imply that $\otimes$ is increasing in both coordinates, that is

$$\text{If } a \leq b \text{ then, } \forall c \in Q, \quad a \otimes c \leq b \otimes c \quad \text{and} \quad c \otimes a \leq c \otimes b$$

We register a classic result:

Proposition 1.2 The endomorphisms $a \otimes \cdot, \cdot \otimes a : Q \longrightarrow Q$ have right adjoints, denoted by $a \rightarrow_r \cdot$ and $a \rightarrow_l \cdot$, respectively. Thus,

$$a \otimes c \leq b \text{ iff } c \leq a \rightarrow_r b \quad c \otimes a \leq b \text{ iff } c \leq a \rightarrow_l b$$

and consequently

$$a \rightarrow_r b = \bigvee \{c \in Q : a \otimes c \leq b\} \quad a \rightarrow_l b = \bigvee \{c \in Q : c \otimes a \leq b\}.$$

Definition 1.3 Let Q be a quantale. A map $j : Q \rightarrow Q$ is said to be a

a) quantic nucleus if it satisfies

$$\begin{array}{ll} [NQ1] & a \leq b \text{ implies } j(a) \leq j(b) \\ [NQ2] & a \leq j(a) \\ [NQ3] & j(j(a)) = j(a) \\ [NQ4] & j(a) \otimes j(b) \leq j(a \otimes b) \end{array}$$

b) quantic conucleus if it satisfies :

$$\begin{array}{ll} [CNQ1] & a \leq b \text{ implies } g(a) \leq g(b) \\ [CNQ2] & g(a) \leq a \\ [CNQ3] & g(g(a)) = g(a) \\ [CNQ4] & g(a) \otimes g(b) \leq g(a \otimes b) \end{array}$$

Quantic nuclei and conuclei are important, because they determine the quocients and subobjects in the category of quantales.

Definition 1.4 Let Q be a quantale. A subset $S \subseteq Q$ is a subquantale of Q if it is closed under $\otimes$ and arbitrary sup's.

Proposition 1.5 [Ros] : (a) If $Q \xrightarrow{j} Q$ is a quantic nucleus, then $Q_j = \{x \in Q : j(x) = x\}$ is a quantale where the operations $\otimes^j$, $\bigvee^j$ and $\bigwedge^j$ in Q_j are given by :

$$a \otimes^j b = j(a \otimes b) \quad \bigvee_{i \in I}^j a_i = j(\bigvee_{i \in I} a_i) \quad \bigwedge_{i \in I}^j a_i = \bigwedge_{i \in I} a_i.$$

Moreover, the map $j : Q \rightarrow Q_j$ given by $a \mapsto j(a)$, is a surjective morphism of quantales. Further, every surjective morphism of quantales can be represented in this form.

(b) If $Q \xrightarrow{g} Q$ is a quantic conucleus, then $Q_g = \{x \in Q : g(x) = x\}$ is a subquantale where, with notation as in (a), $\bigwedge_{i \in I}^g a_i = g(\bigwedge_{i \in I} a_i)$. Moreover, every subquantale is of this form, i.e.,

if $S \subseteq Q$ is a subquantale, then there exists a quantic conucleus g in Q such that $S = Q_g$.

Definition 1.6 An element $\perp \in Q$ is dualizing if:

$$(a \rightarrow_r \perp) \rightarrow_l \perp = a = (a \rightarrow_l \perp) \rightarrow_r \perp, \text{ for every } a \in Q.$$

An element $s \in Q$ is cyclic if:

$$a \rightarrow_r s = a \rightarrow_l s, \text{ for every } a \in Q.$$

Proposition 1.7 [Yet] : Let Q be a quantale and $s, \perp$ be elements of Q .

a) $s \in Q$ is cyclic iff for all $a_1, \dots, a_n$ in Q ,

$$a_1 \otimes \cdots \otimes a_n \leq s \text{ implies } a_{\pi(1)} \otimes a_{\pi(2)} \otimes \cdots \otimes a_{\pi(n)} \leq s,$$

for all cyclic permutations π of $\{1, \dots, n\}$.

b) If $\perp \in Q$ is dualizing, then Q is unital and we have :

$$\mathbf{1} = \perp \rightarrow_r \perp = \perp \rightarrow_l \perp.$$

Definition 1.8 A Girard quantale is a quantale which has a cyclic dualizing element $\perp$. The operator $\cdot \rightarrow_l \perp = \cdot \rightarrow_r \perp \equiv_{def} \cdot \rightarrow \perp$ is called linear negation, and we write $a^\perp = a \rightarrow \perp$ (note that $\mathbf{1} = \perp^\perp$, $\perp = \mathbf{1}^\perp$, and $a = a^{\perp\perp}$).

Next proposition is of frequent use when computing in a Girard quantale.

Proposition 1.9 [Ros] : Let Q be a Girard quantale with a cyclic dualizing element $\perp$ and let $a, b \in Q$. Then:

$$\begin{array}{ll} (1) \ a \rightarrow_l b = (a \otimes b^\perp)^\perp & (2) \ a \rightarrow_r b = (b^\perp \otimes a)^\perp \\ (3) \ a \otimes b = (a \rightarrow_l b^\perp)^\perp & (4) \ b \otimes a = (a \rightarrow_r b^\perp)^\perp \\ (5) \ a \rightarrow_r b = b^\perp \rightarrow_l a^\perp & (6) \ a \rightarrow_l b = b^\perp \rightarrow_r a^\perp \end{array}$$

Proposition 1.10 [Yet] : Let Q be an unital quantale and $s \in Q$ cyclic. Then, $j : Q \rightarrow Q$, given by $j(a) = (a \rightarrow s) \rightarrow s$ is a quantic nucleus, and $Q_j = \{a \in Q : j(a) = a\}$ is a Girard quantale, where $\perp = s \in Q_j$.

Example 1.11 : The Phase Quantales (Girard)

Let $(M, \cdot, 1)$ be a monoid. We define $A \cdot B = \{a \cdot b : a \in A, b \in B\} \ \forall A, B \subseteq M$. Let $\perp \subseteq M$ be such that $a \cdot b \in \perp$ implies $b \cdot a \in \perp$ (for example, $\perp$ can be a semiprime ideal or the complement of a prime ideal of M).

Thus, $\mathcal{P}(M)$ is a quantale with the product defined above, and with sup's e inf's calculated as unions ($\cup$) and intersections ($\cap$). In fact, it's an unital quantale, where $\mathbf{1} = \{1\}$ and $\perp$ is cyclic. Then, by proposition 1.10, $\mathcal{P}(M)_j$ is a Girard's quantale containing $\perp$. Their elements are called facts, and we have:

$$A \otimes B = (A \cdot B)^{\perp\perp}$$

$$\bigvee_{i \in I} A_i = (\bigcup_{i \in I} A_i)^{\perp\perp}; \text{ in particular, } A \vee B = (A \cup B)^{\perp\perp} \equiv_{def} A \oplus B,$$

$$\bigwedge_{i \in I} A_i = \bigcap_{i \in I} A_i; \text{ in particular, } A \wedge B = A \cap B \equiv_{def} A \& B.$$

The next result tells us that every Girard quantale is of this form.

Proposition 1.12 [Ros] : If Q is a Girard's quantale, then Q is isomorphic to a phase quantale.

We are now going to relate the exponentials treated by Yetter ([Yet]) and Avron ([Avr]) with certain concepts in the theory of quantales.

Definition 1.13 [Yet] : An open modality in a quantale Q is a map $\mu : Q \longrightarrow Q$ satisfying:

$$\begin{aligned} [M1] \quad & \mu(a) \leq a & [M2] \quad & a \leq b \text{ implies } \mu(a) \leq \mu(b) \\ [M3] \quad & \mu(\mu(a)) = \mu(a) & [M4] \quad & \mu(\mu(a) \otimes \mu(b)) = \mu(a) \otimes \mu(b). \end{aligned}$$

An open modality μ is said to be

- central if $b \otimes \mu(a) = \mu(a) \otimes b$ for every $a, b \in Q$.
- idempotent if $\mu(a) \otimes \mu(a) = \mu(a)$ for every $a \in Q$.
- weak if Q is unital, $\mu(1) = 1$, and $\mu(a) \leq 1$ for every $a \in Q$.

Let $M(Q) = \{\mu : \mu \text{ is an open modality in } Q\}$, partially ordered by pointwise order.

Proposition 1.14 [Yet] : Let Q be a quantale (resp. unital quantale). Then, there exists an unique maximal open modality in Q central (resp. central, idempotent and weak) denoted by c_m (resp. $!_m$) given by:

$$c_m(x) = \bigvee \{a \in Q : a \leq x, a \in Z(Q)\}$$

$$!_m(x) = \bigvee \{a \in Q : a \leq x \wedge 1, a = a \otimes a, a \in Z(Q)\},$$

where $Z(Q) = \{a \in Q : a \otimes b = b \otimes a, \text{ for every } b \in Q\}$.

Definition 1.15 [Avr] : Let Q be an unital quantale. A map $B : Q \longrightarrow Q$ is a modal operation if it satisfies, for all $x, y \in Q$:

$$\begin{aligned} [B1] \quad & B(1) = 1 & [B2] \quad & B(x) \leq x \\ [B3] \quad & B(B(x)) = B(x) & [B4] \quad & B(x) \otimes B(y) = B(x \wedge y). \end{aligned}$$

Proposition 1.16 Let Q be a quantale, and $\mu : Q \longrightarrow Q$ a map.

- (i) μ is an open modality iff μ is a quantic conucleus.
- (ii) If Q is unital, then μ is an open, idempotent and weak modality iff μ is a modal operation.

Proof: (i) We must prove that $[M4]$ is equivalent to $[CNQ4]$. Let μ be an open modality. Because $\mu(a) \otimes \mu(b) \leq a \otimes b$, we get $\mu(a) \otimes \mu(b) = \mu(\mu(a) \otimes \mu(b)) \leq \mu(a \otimes b)$.

Conversely, if μ is a quantic conucleus, then

$$\mu(a) \otimes \mu(b) = \mu(\mu(a)) \otimes \mu(\mu(b)) \leq \mu(\mu(a) \otimes \mu(b)) \leq \mu(a \otimes b).$$

(ii) Assume that μ is an open, weak and idempotent modality. Then, it clearly satisfies conditions $[B1]$, $[B2]$, $[B3]$. Because $\mu(a) \leq a$ and $\mu(b) \leq 1$, we get $\mu(a) \otimes \mu(b) \leq a \otimes 1 = a$. Similarly, $\mu(a) \otimes \mu(b) \leq b$ and therefore, $\mu(a) \otimes \mu(b) \leq a \wedge b$. Thus, $\mu(a) \otimes \mu(b) = \mu(\mu(a) \otimes \mu(b)) \leq \mu(a \wedge b)$.

Now, since μ is increasing and $a \wedge b \leq a, b$, then $\mu(a \wedge b) \leq \mu(a), \mu(b)$. Thus,

$$\mu(a \wedge b) = \mu(a \wedge b) \otimes \mu(a \wedge b) \leq \mu(a) \otimes \mu(b),$$

and so μ satisfies $[B4]$.

Conversely, if μ is a modal operation, then $[M1]$ is just $[B2]$; $[M3]$ is $[B3]$, while $[M4]$ is equivalent to $[CNQ4]$, in the presence of $[M1], [M2], [M3]$, by item (i) above.

Condition $[M2]$ is item (5) of Lemma 4.2 in [Avr] and μ satisfies $[CNQ4]$ by item 8 of Lemma 4.2 in [Avr]. It follows from items 4 and 1 in that same Lemma, that $\mu(x) \leq 1$ for every $x \in Q$. Thus, $[B1]$ yields that μ is weak. $\square$

Definition 1.17 A frame (or Complete Heyting algebra) is a quantale where $\otimes = \wedge$.

Definition 1.18 Let Q be a quantale and let $\top$ be the maximum of Q . We say that $x \in Q$ is

- a) right-sided (in Q) if $x \otimes \top \leq x$; b) left-sided (in Q) if $\top \otimes x \leq x$;
- c) two-sided (in Q) if it is right and left sided in Q . d) idempotent if $x \otimes x = x$

Proposition 1.19 [Ros] : Let Q be a quantale, and g a quantic conucleus in Q . Are equivalent:

- (a) Q_g is a frame. (b) $g(a) \otimes g(b) = g(a \wedge b)$.
- (c) every $x \in Q_g$ is idempotent and two-sided (in Q_g).

Definition 1.20 A map g satisfying the conditions above is called a localic conucleus and Q_g is called a localic subquantale.

Since open, weak idempotent modalities are localic conuclei μ such that $\mu(1) = 1$, we have

Corollary 1.21 Let Q be an unital quantale, and let μ be an open, weak and idempotent modality. Then, Q_μ is a frame.

Thus, the fixed points of the interpretation of the modality ! (of course) lie in a localic subquantale (complete Heyting algebra) of any quantale in which linear logic is interpreted.

2 Linear Calculus with Equality

In this section we discuss the laws for a binary predicate representing equality. The goal is to define a reflexive, symmetric and transitive predicate satisfying the substitution (Leibnitz's) rule for the class of all formulas. We may assume, just as in Classical Logic (CL), that we have substitution for atomic formulas. With this model in mind, we shall define a prototype of a linear calculus with equality, called (LLE_1) . Our formulation will use sequents in Linear Logic (LL). Analogously, we will set down a calculus with equality for the $(MALL)$ fragment, i.e., the fragment without exponentials, indicated by (LLE_0) . Starting from the property of substitution for elementary formulas, we prove that $(\cdot = \cdot)$ must be ≤ 1 , idempotent in $(MALL)$ and open in the general case.

Definition 2.1 A first order linear language with equality $\mathbb{L}$ consists in a countable set of predicate symbols $\mathcal{P} = \{P_n : n \in \omega\} \cup \{ = \}$ (where " $=$ " is binary), a countable set of variables $V = \{v_n : n \in \omega\}$, together with the symbols:

$$1, \perp, \top, 0, \perp^\perp, \vee, \wedge, \oplus, \&, \otimes, \sqcup, !, ?.$$

Definition 2.2 The formulas of $\mathbb{L}$, $FOR(\mathbb{L})$, are defined recursively:

[F1] $1, \perp, \top, 0 \in FOR(\mathbb{L})$.

[F2] If $P \in \mathcal{P}$ is a predicate of arity n and $x_1, \dots, x_n$ are variables, then

$$P(x_1, \dots, x_n) \text{ and } P(x_1, \dots, x_n)^\perp \in FOR(\mathbb{L}).$$

[F3] if $F, G \in FOR(\mathbb{L})$ then $F \otimes G, F \sqcup G, F \& G, F \oplus G \in FOR(\mathbb{L})$

[F4] if $F \in FOR(\mathbb{L})$, then $!F, ?F \in FOR(\mathbb{L})$.

[F5] if $F \in FOR(\mathbb{L})$ and $x \in V$, then $\wedge x.F$ and $\vee x.F \in FOR(\mathbb{L})$.

Every occurrence of a variable x in a formula F is free except in a subformula of the type $\wedge x.G$ or $\vee x.G$ (which are bounded occurrences). We shall write

$ELF(\mathbb{L}) = \{P(x_1, \dots, x_n) : P \in \mathcal{P} - \{ = \}, x_i \in V\}$, the set of elementary formulas and

$ELF^+(\mathbb{L}) = ELF(\mathbb{L}) \cup \{(x = y) : x, y \in V\}$, the extended set of elementary formulas.

Definition 2.3 The syntactic linear negation is a map $\perp : FOR(\mathbb{L}) \longrightarrow FOR(\mathbb{L})$ given by the usual rules:

[NL1] $\perp(1) = \perp, \perp(\perp) = 1, \perp(0) = \top, \perp(\top) = 0$

[NL2] $\perp(P(x_1, \dots, x_n)) = P(x_1, \dots, x_n)^\perp, \perp((x = y)) = (x = y)^\perp,$

$\perp(P(x_1, \dots, x_n)^\perp) = P(x_1, \dots, x_n), \perp((x = y)^\perp) = (x = y)$

(here, $P(x_1, \dots, x_n) \in ELF(\mathbb{L})$)

[NL3] $\perp(F \otimes G) = \perp(F) \sqcup \perp(G), \perp(F \sqcup G) = \perp(F) \otimes \perp(G),$

$\perp(F \& G) = \perp(F) \oplus \perp(G), \perp(F \oplus G) = \perp(F) \& \perp(G)$

[NL4] $\perp(!F) = ?\perp(F), \perp(?F) = !\perp(F)$

[NL5] $\perp(\wedge x.F) = \vee x.\perp(F), \perp(\vee x.F) = \wedge x.\perp(F)$

We write $\perp(F) = F^\perp$; clearly $F = F^{\perp\perp}$ for every $F \in FOR(\mathbb{L})$.

Definition 2.4 Let A a formula; we define $A[y/x]$ to be the formula obtained from A by replacing all bound occurrences of y by z , where z is the first variable (in the natural order of V) not occurring in A , and then replacing all free occurrences of variable x by y .

Definition 2.5 (Girard) The calculus (LL) for first order commutative linear logic is defined by the axioms and rules below (here, A, B denote formulas, and Γ, Δ denote multisets of formulas):

$$[AX1] \quad \vdash A^\perp, A \quad [AX2] \quad \vdash \top, \Gamma \quad [AX3] \quad \vdash 1$$

$$[CUT] \quad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}$$

$$[EXCH] \quad \text{If } \Delta \text{ is a permutation of } \Gamma, \text{ then } \frac{\vdash \Gamma}{\vdash \Delta}$$

$$[\&] \quad \frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \& B, \Gamma}$$

$$[\oplus 1] \quad \frac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma} \quad [\oplus 2] \quad \frac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma}$$

$$[\perp] \quad \text{If } \Gamma \text{ is not empty, then } \frac{\vdash \Gamma}{\vdash \perp, \Gamma}$$

$$[\otimes] \quad \frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \quad [\sqcup] \quad \frac{\vdash A, B, \Gamma}{\vdash A \sqcup B, \Gamma}$$

$$[dereliction] \quad \frac{\vdash A, \Gamma}{\vdash ?A, \Gamma} \quad [weakening] \quad \frac{\vdash \Gamma}{\vdash ?A, \Gamma}$$

$$[contraction] \quad \frac{\vdash ?A, ?A, \Gamma}{\vdash ?A, \Gamma} \quad [!] \quad \frac{\vdash A, ?\Gamma}{\vdash !A, ?\Gamma}$$

$$[\vee] \quad \frac{\vdash A[y/x], \Gamma}{\vdash \vee x.A, \Gamma} \quad [\wedge] \quad \text{If } x \text{ is not free in } \Gamma, \text{ then } \frac{\vdash A, \Gamma}{\vdash \wedge x.A, \Gamma}$$

We can consider as defined connectives the linear implication and the linear equivalence, given by:

$$(A \multimap B) \equiv_{def} (A^\perp \sqcup B) = (A \otimes B^\perp)^\perp \quad (A \multimap\multimap B) \equiv_{def} (A \multimap B) \& (B \multimap A).$$

Definition 2.6 The linear calculus with equality (LLE_0) for the (MALL) fragment of (LL) is defined by adding the axioms below to those in the preceding definition :

$$[R=] : \vdash (x = x); \quad [S=] : \vdash (x = y)^\perp, (y = x); \quad [T=] : \vdash (x = y)^\perp, (y = z)^\perp, (x = z).$$

$$[SUBST] : \vdash (x_1 = y_1)^\perp, \dots, (x_n = y_n)^\perp, F(x_1, \dots, x_n)^\perp, F(x_1 \setminus y_1, \dots, x_n \setminus y_n),$$

where $F(x_1, \dots, x_n)$ denotes an elementary formula with (eventually) $x_1, \dots, x_n$ free and $F(x_1 \setminus y_1, \dots, x_n \setminus y_n)$ is obtained from $F(x_1, \dots, x_n)$ by replacing some occurrences of x_i (which are not in the scope of a y_i -quantifier) by y_i .

$$[I=] : \vdash (x = y)^\perp, (x = y) \otimes (x = y) \quad [\leq 1] : \vdash (x = y)^\perp, 1$$

Definition 2.7 The linear calculus with equality (LLE_1) for (LL) is defined by adding, besides the axioms $[R=]$, $[S=]$, $[T=]$, $[SUBST]$ the following rule

$$[! =] : \vdash (x = y)^\perp, !(x = y)$$

Obviously, all the rules (with exception of $[R =]$) could be formulated as linear implications, for example $[T =]$ could be stated as

$$\vdash (x = y) \otimes (y = z) \multimap (x = z)$$

We have as well that (LLE_1) is equivalent to the calculus obtained from (LLE_1) by replacing $[S =]$ and $[! =]$ by the rule:

$$[S! =] \quad \vdash (x = y)^\perp, !(y = x)$$

3 Semantics

In this section we develop interpretations for the calculi described above. It will be necessary to extend the definitions in [Yet] so that the axioms involving equality are verified.

Definition 3.1 An interpretation of a language $\mathbb{L}$ is a triple $\langle \mathcal{A}, \mathcal{V}, |\cdot|_{\mathcal{A}} \rangle$ where

- $\mathcal{A}$ is an algebra for the theory with constants $\mathbf{1}, \perp, \top, \mathbf{0}$;
- a set of unary operations $\{\perp, !, ?\}$ (the interpretation of the modalities);
- binary operations $\otimes, \sqcup, \&, \oplus$, and infinitary operations $\bigvee$ and $\bigwedge$;
- $\mathcal{V} \subseteq \mathcal{A}$, the set of valids elements; and
- $|\cdot|_{\mathcal{A}} : ELF^+(\mathbb{L}) \longrightarrow \mathcal{A}$ is a map.

It is straightforward to see that there exists a (unique) extension of $|\cdot|_{\mathcal{A}}$ to $FOR(\mathbb{L})$, also denoted by $|\cdot|_{\mathcal{A}}$. When there is no risk of confusion, we write $|\cdot|$ for $|\cdot|_{\mathcal{A}}$.

Definition 3.2 A semantics for $\mathbb{L}$ is a class of interpretations. A semantics is sound (with respect to a linear calculus P) if:

$\vdash A_1, \dots, A_n$ is provable in P implies $|A_1| \sqcup \dots \sqcup |A_n| \in \mathcal{V}$ for every $\langle \mathcal{A}, \mathcal{V}, |\cdot|_{\mathcal{A}} \rangle$ in the semantics.

A semantics for $\mathbb{L}$ is complete (with respect to P) if:

$|F|_{\mathcal{A}} \in \mathcal{V}$, for every $\langle \mathcal{A}, \mathcal{V}, |\cdot|_{\mathcal{A}} \rangle$ in the semantics, implies $\vdash F$ is provable in P .

Definition 3.3 An interpretation of quantales for $\mathbb{L}$ is a Girard quantale Q , together with an assignement $! \mapsto \mu \in M(Q)$ and a map $|\cdot|_Q : ELF^+(\mathbb{L}) \longrightarrow Q$, where $\mathcal{V} = \{ a \in Q : a \geq 1 \}$ such that

- $\forall a, b \in Q, a \sqcup b \equiv_{def} (a^\perp \otimes b^\perp)^\perp$ and $?a \equiv_{def} (\mu(a^\perp))^\perp$;
- We interpret $\bigwedge x.A$ and $\bigvee x.A$ as $\bigwedge_{y \in V} |A[y/x]|_Q$ and $\bigvee_{y \in V} |A[y/x]|_Q$, respectively.

Recall that $M(Q)$ is the lattice of open modalities in Q (Definition 1.13).

Definition 3.4 The semantics of quantales for (commutative) Linear Logic with equality is the class of interpretation of quantales for $\mathbb{L}$ such that:

[S1] Q is commutative. [S2] $\mu \equiv_{def} !$ is idempotent and weak.

[S3] $|\cdot|_Q : ELF^+(\mathbb{L}) \longrightarrow Q$ satisfies:

(a) For the Calculus (LLE_0):

[= 1]: $|x = x| \geq \mathbf{1}$; [= 2]: $|x = y| \otimes |y = z| \leq |x = z|$; [= 3]: $|x = y| = |y = x|$;

[= 4]: $|x_1 = y_1| \otimes \cdots \otimes |x_n = y_n| \otimes |F(x_1, \dots, x_n)| \leq |F(x_1 \wr y_1, \dots, x_n \wr y_n)|$

(same notation as $[SUBST]$);

[= 5]: $|x = y| \leq |x = y| \otimes |x = y|$; [= 6]: $|x = y| \leq \mathbf{1}$

(b) For the Calculus (LLE_1), conditions [= 5] and [= 6] are replaced by the stronger :

[= 7]: $|x = y| \leq !|x = y|$.

The next result shows that it is always possible to define a map $|\cdot|_Q$ satisfying the above conditions.

Proposition 3.5 If $|\cdot|_Q : ELF(\mathbb{L}) \longrightarrow Q$ is a map, then it can be extended to $ELF^+(\mathbb{L})$ satisfying, in the ($MALL$) case, conditions [= 1], ..., [= 6] and, in the general case, conditions [= 1], ..., [= 4], [= 7].

Proof: Let's begin by the general case, in which $! \in M(Q)$ is idempotent and weak.

Let $|\cdot|_Q : ELF(\mathbb{L}) \longrightarrow Q$ be a map, and let $x, y \in V$, $x \neq y$. Define $A_{x,y}$ and $B_{x,y}$ as:

$$A_{x,y} = \{F \in ELF(\mathbb{L}) : \text{neither } x \text{ nor } y \text{ occur in } F\}$$

$$B_{x,y} = \{F \in ELF(\mathbb{L}) : x \text{ or } y \text{ occur in } F\}$$

In $B_{x,y}$ consider the relation:

$$F \sim G \quad \text{iff} \quad G \text{ is obtained from } F \text{ by replacing some occurrences of } x \text{ by } y \text{ and/or some occurrences of } y \text{ by } x.$$

For example, $P(x, z, y) \sim P(x, z, x) \sim P(y, z, y) \sim P(y, z, x)$. Clearly, $\sim$ is an equivalence relation. Now define,

$$T_{x,y} = \bigwedge \{|F|_Q \rightarrow |G|_Q : F, G \in B_{x,y}, F \sim G\}.$$

Fact 1: If $|\cdot|_Q$ satisfies [= 7] and [= 3], then it satisfies [= 4] iff $|x = y| \leq T_{x,y}$ for $x \neq y$.

To see this, assume that $F, G \in B_{x,y}$, $F \sim G$. Note that there is $H \in ELF(\mathbb{L})$ such that $H = F(x \wr y)$, $G = H(y \wr x)$.

Since $!$ is idempotent, [= 7] implies [= 5] and so, by [= 3], [= 4] and [= 5] we have that $|x = y| \otimes |F| \leq |H|$; thus,

$$|x = y| \otimes |F| \leq |x = y| \otimes (|x = y| \otimes |F|) \leq |x = y| \otimes |H| \leq |G|.$$

Therefore, $|x = y| \leq |F| \rightarrow |G|$, proving that $|x = y| \leq T_{x,y}$.

Conversely, suppose that $|x = y| \leq T_{x,y}$ for $x \neq y$. Then, if $F \in \bigcup_{i=1}^n B_{x_i, y_i}$,

$$|x_n = y_n| \leq |F(x_1, \dots, x_n)| \rightarrow |F(x_1, \dots, x_{n-1}, x_n \wr y_n)|$$

and therefore, $|x_n = y_n| \otimes |F(x_1, \dots, x_n)| \leq |F(x_1, \dots, x_{n-1}, x_n \wr y_n)|$. Analogously,

$$\begin{aligned} |x_{n-1} = y_{n-1}| \otimes (|x_n = y_n| \otimes |F(x_1, \dots, x_n)|) &\leq |x_{n-1} = y_{n-1}| \otimes |F(x_1, \dots, x_{n-1}, x_n \wr y_n)| \\ &\leq |F(x_1, \dots, x_{n-2}, x_{n-1} \wr y_{n-1}, x_n \wr y_n)|. \end{aligned}$$

We may proceed by induction to get:

$$|x_1 = y_1| \otimes \dots \otimes |x_n = y_n| \otimes |F(x_1, \dots, x_n)| \leq |F(x_1 \wr y_1, \dots, x_n \wr y_n)|,$$

as desired.

If $F \in \bigcap_{i=1}^n A_{x_i, y_i}$ then, since $[= 7]$ implies $[= 6]$, we have:

$$|x_1 = y_1| \otimes \dots \otimes |x_n = y_n| \otimes |F| \leq (\mathbf{1} \otimes \dots \otimes \mathbf{1}) \otimes |F| = |F|,$$

showing that $[= 4]$ is valid and proving Fact 1.

By induction, define a map $|\cdot|$ as follows: for $x, y \in V, x \neq y$, set

$$|x = y|_0 = T_{x,y};$$

$$|x = y|_{n+1} = \bigwedge_{z \neq x, y} (|x = z|_n \leftrightarrow |y = z|_n) \text{ (} a \leftrightarrow b \text{ means } (a \rightarrow b) \wedge (b \rightarrow a) \text{)};$$

$$|x = y|_\infty = !(\bigwedge_{n \in \mathbb{N}} |x = y|_n); \text{ finally, set } |x = x|_\infty = \mathbf{1}.$$

Fact 2: $|\cdot|_\infty$ satisfies the properties required for the full logic.

In fact: condition $[= 1]$ is clear, while $[= 3]$ is verified because it's true for $|x = y|_n$, for all $n \in \omega$.

Since $|x = y|_\infty = !|x = y|_\infty$, $[= 7]$ is satisfied (the case $x = y$ is valid too, because $!\mathbf{1} = \mathbf{1}$). Observe that, for every $n \geq 0$ and $z \neq x, y$:

$$|x = y|_{n+1} \otimes |x = z|_n \leq |y = z|_n \text{ and therefore,}$$

$$|x = y|_\infty \otimes |x = z|_\infty \leq |x = y|_{n+1} \otimes |x = z|_n \leq |y = z|_n \text{ for every } n \geq 0. \text{ Thus,}$$

$$|x = y|_\infty \otimes |x = z|_\infty \leq \bigwedge_{n \in \mathbb{N}} |y = z|_n; \text{ now } [= 7] \text{ and } [M4] \text{ yield } [= 2].$$

Since $|x = y|_\infty \leq |x = y|_0 = T_{x,y}$, Fact 1 guarantees that $|\cdot|_\infty$ satisfies $[= 4]$.

For the (MALL) fragment, it's enough to take $! = !_m$ (see Proposition 1.14) in the above computations. $\square$

Discussion 3.6 Are requirements $[= 5], [= 6]$ (resp. $[= 7]$) too strong ?

The motivation for them is, starting with substitution for elementary formulas, to have substitution for every formula. Obviously, they are sufficient, but indeed, **they are also necessary**. To see this, note that, if $a = |x = y|$, $b = |P(x)|$ and $c = |P(x \wr y)|$, then we must have that $a \otimes b \leq c$ and $a \otimes c \leq b$, (i.e. $a \leq (b \leftrightarrow c)$) must imply $a \otimes !b \leq !c$ (and, of course, that $a \otimes !c \leq !b$). Since $\mathbf{1}$ is a formula, we must also have $a = a \otimes \mathbf{1} \leq \mathbf{1}$. The critical cases are $\otimes$ and $!$. We have

Lemma 3.7 Let Q be a Girard Quantale and let a be an element of Q such that $a \leq \mathbf{1}$.

(a) Are equivalent:

(i) $\forall b, c, d \in Q, \quad a \leq (b \leftrightarrow c), a \leq (d \leftrightarrow e) \quad \text{implies} \quad a \leq ((b \otimes d) \leftrightarrow (c \otimes e)).$

(ii) $a \leq a \otimes a$

(b) Assume that $! \in M(Q)$ is idempotent and weak. Are equivalent:

(i) $\forall b, c \in Q, \quad a \leq (b \leftrightarrow c) \quad \text{implies} \quad a \leq (!b \leftrightarrow !c).$

(ii) $a = !a$

(c) $\forall b, c \in Q, \quad a \leq (b \leftrightarrow c) \quad \text{implies} \quad a \leq (b^\perp \leftrightarrow c^\perp).$

Proof: (a) (i) $\Rightarrow$ (ii) : since $a \leq 1$, then $a \leq (1 \leftrightarrow a)$ and so $a \leq ((1 \otimes 1) \leftrightarrow (a \otimes a))$; thus, $a = a \otimes (1 \otimes 1) \leq a \otimes a$.

(i) $\Leftarrow$ (ii) : If $a \leq (b \leftrightarrow c), a \leq (d \leftrightarrow e)$, then we have $a \otimes b \leq c$ and $a \otimes d \leq e$, and so $a \otimes (b \otimes d) \leq (a \otimes a) \otimes (b \otimes d) = (a \otimes b) \otimes (a \otimes d) \leq c \otimes e$. Analogously, $a \otimes (c \otimes e) \leq b \otimes d$.

(b) (i) $\Rightarrow$ (ii) : since $a \leq 1$ and $!1 = 1$, then $a \leq (1 \leftrightarrow a)$ and therefore $a \leq (1 \leftrightarrow !a)$; thus, $a = a \otimes 1 \leq !a \leq a$.

(i) $\Leftarrow$ (ii) : suppose that $a \leq (b \leftrightarrow c)$; thus, $a \otimes b \leq c$ and then $a \otimes !b \leq a \otimes b \leq c$. Thus, by [M4], we have $a \otimes !b = !a \otimes !b = !(a \otimes !b) = !(a \otimes !b) \leq !c$. Analogously, we can prove that $a \otimes !c \leq !b$.

(c) Since Q is commutative, then $(x \rightarrow y) = (y^\perp \rightarrow x^\perp)$, by Proposition 1.9. $\square$

We can now show that we have substitution for every formula:

Proposition 3.8 Let $|\cdot| : ELF(\mathbb{L}) \longrightarrow Q$ satisfying $[= 1] - [= 6]$ ($[= 1] - [= 4], [= 7]$ resp.). Then, the extension to $FOR(\mathbb{L})$ verifies:

$$|x_1 = y_1| \otimes \cdots \otimes |x_n = y_n| \otimes |\phi(x_1, \dots, x_n)| \leq |\phi(x_1 \wr y_1, \dots, x_n \wr y_n)|$$

where $\phi(x_1, \dots, x_n) \in FOR(\mathbb{L})$ has (eventually) free occurrences of variables $x_1, \dots, x_n$, and $\phi(x_1 \wr y_1, \dots, x_n \wr y_n)$ is obtained from $\phi(x_1, \dots, x_n)$ by replacing some occurrences of x_i (not in the scope of a y_i -quantifier) by y_i .

Proof: By induction in the complexity of ϕ . As a first step, we have two cases to consider.

i) $\phi \in ELF^+(\mathbb{L})$. It's true by $[= 2], [= 3], [= 4]$ and $[= 6]$ (or $[= 7]$ and $!$ weak).

ii) $\phi \in \{1, \perp, \top, 0\}$. It's true by $[= 6]$ (or $[= 7]$ and $!$ weak).

To proceed with the induction, assume that substitution holds true for every φ with complexity $\leq k$ and let ϕ be a formula with complexity $k + 1$. We have the following cases:

a) $\phi = \alpha \otimes \beta$. It's immediate from $[= 5]$ (common to both systems) and lemma 3.7.

b) $\phi = \alpha^\perp$. Since $|\alpha^\perp| = |\alpha|^\perp$, the conclusion follows from Lemma 3.7.

c) $\phi = \bigwedge x. \alpha(x_1, \dots, x_n, x)$. Given $z \in V$, we have:

$$\begin{aligned} \bigotimes_{i=1}^n |x_i = y_i| \otimes \bigwedge_{y \in V} |\alpha(x_1, \dots, x_n, x)[y/x]| &\leq \bigotimes_{i=1}^n |x_i = y_i| \otimes |\alpha(x_1, \dots, x_n, x)[z/x]| \\ &\leq |\alpha(x_1 \wr y_1, \dots, x_n \wr y_n, x)[z/x]|, \quad \text{and then} \end{aligned}$$

$$\otimes_{i=1}^n |x_i = y_i| \otimes \wedge_{y \in V} |\alpha(x_1, \dots, x_n, x)[y/x]| \leq \wedge_{y \in V} |\alpha(x_1 \wr y_1, \dots, x_n \wr y_n, x)[y/x]|.$$

d) $\phi = \alpha \& \beta$. Similar to c).

e) (full logic) $\phi = !\alpha$. It follows from $[= 7]$ and Lemma 3.7.

Since the other connectives are defined by duality, the proof is complete. $\square$

Now, we shall extend the results in [Yet] to the calculus with equality.

Theorem 3.9 (Soundness) *The semantics of quantales for commutative Linear Logic with equality is sound with respect to the given calculus.*

Proof: We prove the validity of the new axioms (for the others rules, consult [Yet]). Define $|\vdash A_1, \dots, A_n| = |A_1 \sqcup \dots \sqcup A_n|$. By observing that, for every $a, b \in Q$, $a \leq b$ iff $a^\perp \sqcup b \geq \mathbf{1}$, the validity of each axiom is guaranteed by $[= 1] - [= 6]$ (resp. $[= 1] - [= 4], [= 7]$). $\square$

Theorem 3.10 (Completeness) *The semantic of quantales for commutative Linear Logic with equality is complete with respect to the given calculus.*

Proof: The proof is an extension of the proofs by [Yet] and [Gir]. Let M_1 be the set of finite sequence of formulas in $\mathbb{L}$; M_1 is a monoid with the operation of concatenation (and identity the null sequence). Let M be the (commutative) monoid obtained by identifying sequences which are distinct only by a permutation of their elements. Just as in example 1.11, $\mathcal{P}(M)$ is a commutative quantale and we set $\perp = \{\Gamma : \vdash \Gamma \text{ is provable}\} \in \mathcal{P}(M)$.

Since M is commutative, $\perp$ is cyclic and so we can consider the phase quantale $Q = \mathcal{P}(M)_j$, where $j : \mathcal{P}(M) \rightarrow \mathcal{P}(M)$ is given by $j(A) = (A \rightarrow \perp) \rightarrow \perp$.

Let $Pr : FOR(\mathbb{L}) \rightarrow \mathcal{P}(M)$ defined by:

$$Pr(A) = \{\Gamma : \vdash A, \Gamma \text{ is provable}\}.$$

By theorem 3.4 in [Yet], Pr factors through Q , i.e., $Pr(FOR(\mathbb{L})) = Q$.

Let $|\cdot| = Pr|_{ELF^+(\mathbb{L})}$; clearly, the unique extension of $|\cdot|$ to $FOR(\mathbb{L})$ is Pr , once we have defined in Q the open, weak and idempotent modality $!$ as:

$$!(x) = \vee \{Pr(!A) : Pr(A) \leq x\}.$$

Fact: $!\mathbf{1} = \mathbf{1}$ (where, by definition, $\mathbf{1} = \bigwedge \{Pr(A) : \vdash A \text{ is provable}\}$).

To see this, Let $\Gamma \in Pr(!\mathbf{1})$; thus, $\vdash !\mathbf{1}, \Gamma$ (i.e., $\vdash (? \perp)^\perp, \Gamma$) is provable and let $A \in FOR(\mathbb{L})$ be such that $\vdash A$ is provable. Then:

$$\begin{array}{c} \vdots \\ \vdash A \\ \hline \vdash A, \perp \quad \vdots \\ \vdash A, ?\perp \quad \vdash (? \perp)^\perp, \Gamma \\ \hline \vdash A, \Gamma \end{array}$$

i.e., $\Gamma \in Pr(A)$, and so $Pr(!\mathbf{1}) \leq \bigwedge \{Pr(A) : \vdash A \text{ is provable}\} = \mathbf{1}$.

Thus, $Pr(!1) \leq \bigvee \{Pr(!A) : Pr(!A) \leq 1\} = !1$. In fact, equality holds because $\vdash !1$ is provable, and so $1 \leq Pr(!1) \leq !1 \leq 1$, i.e. $1 = !1$.

We shall now show that $|\cdot|$ satisfies the required properties. Since $\vdash (x = x)$ is provable, $1 \leq Pr((x = x)) = |x = x|$. This verifies $[= 1]$.

To prove $[= 2]$, let $\Gamma\Delta \in |x = y| \cdot |y = z|$. Then we have:

$$\begin{array}{c} \vdots \\ \vdash (x = y), \Gamma \qquad \vdash (x = y)^\perp, (y = z)^\perp, (x = z) \qquad \vdots \\ \hline \vdash (y = z)^\perp, (x = z), \Gamma \qquad \vdash (y = z), \Delta \\ \hline \vdash (x = z), \Gamma, \Delta \end{array}$$

i.e., $\Gamma\Delta \in |x = z|$. Thus, $|x = y| \cdot |y = z| \leq |x = z|$ and so

$$|x = y| \otimes |y = z| = (|x = y| \cdot |y = z|)^{\perp\perp} \leq |x = z|.$$

To prove $[= 3]$, let $\Gamma \in |x = y|$. We have:

$$\begin{array}{c} \vdots \\ \vdash (x = y), \Gamma \qquad \vdash (x = y)^\perp, (y = x) \\ \hline \vdash (y = x), \Gamma \end{array}$$

i.e., $\Gamma \in |y = x|$ and thus $|x = y| \leq |y = x|$.

Properties $[= 4]$, $[= 5]$, $[= 6]$, $[= 7]$ are verified in a similar way. This shows that we have an interpretation of quantales such that $|A| \geq 1$ iff $\vdash A$ is provable, completing the proof. $\square$

4 Generalisations of the Calculus

There are alternatives to the treatment of equality given above, using the exponentials of Linear Logic. For example, instead of requiring $(\cdot = \cdot)$ to be open, we could establish that its characteristic properties be valid in the interior of $(\cdot = \cdot)$. Thus, we define the calculus $(P_!)$ by the axioms:

$$[R!] \vdash !(x = x) \quad [S!] \vdash !(x = y) \multimap !(y = x) \quad [T!] \vdash !(x = y) \otimes !(y = z) \multimap !(x = z)$$

For every predicate symbol P ,

$$[SUBS!] \vdash !(x_1 = y_1) \otimes \cdots \otimes !(x_n = y_n) \otimes P(x_1, \dots, x_n) \multimap P(x_1 \wr y_1, \dots, x_n \wr y_n)$$

Clearly, we have substitution for every formula, and we can say that $!(x = y)$ has the behaviour of a linear equality. An even weaker form of substitution can be defined as follows :

$$\vdash !(x_1 = y_1) \otimes \cdots \otimes !(x_n = y_n) \otimes !P(x_1, \dots, x_n) \multimap !P(x_1 \wr y_1, \dots, x_n \wr y_n)$$

or, even

$$\vdash !(x_1 = y_1) \otimes \cdots \otimes !(x_n = y_n) \otimes !P(x_1, \dots, x_n) \multimap ?P(x_1 \wr y_1, \dots, x_n \wr y_n).$$

We can modify each axiom combining the modal operators in all possible ways. It is straightforward to verify that (incorporating id , the identity operation on formulas), there are only seven modal operations obtained by successive applications of $\{!, ?\}$, namely, the set

$$\mathcal{M} = \{!, !?, !, !?, !?, ?, id\}$$

fig. 1

with it's natural lattice structure (see figure 1). This is in complete analogy with Kuratowski's problem, in which we can prove that, given a topological space X and $A \subseteq X$, there are only 14 distinct sets that can be obtained from A by combinations of taking complements and closure (in our case, we do not consider modalities of the form $m'(x) = m(x)^\perp$ with $m \in \mathcal{M}$). Starting with this, we can define a general scheme to create a linear calculus with equality.

Definition 4.1 Let $(m_i)_{i=1}^{10}$ be a sequence in $\mathcal{M}$. A linear calculus with equality $P((m_i))$ is defined by the following axioms:

$$[R] \quad \vdash m_1(x = x) \quad [S] \quad \vdash m_2(x = y) \multimap m_3(y = x)$$

$$[T] \quad \vdash m_4(m_5(x = y) \otimes m_5(y = z)) \multimap m_6(x = z)$$

For each predicate symbol P , the axiom

$$[SUBS] \quad \vdash m_7((\otimes_{i=1}^n m_8(x_i = y_i)) \otimes m_9(P(x_1, \dots, x_n))) \multimap m_{10}(P(x_1 \wr y_1, \dots, x_n \wr y_n)).$$

Remarks 4.2 (a) If $m_3 \leq m_2$, then $[S]$ implies that, for $m_3 \leq r, s \leq m_2$, $r(x = y)$, $s(x = y)$, $r(y = x)$ and $s(y = x)$ are all equivalent.

(b) If $m_1 = id$ or $m_1 = !$, then $\vdash m(x = x)$ is provable for every $m \in \mathcal{M}$.

(c) If $m_7 = id$, $m_8 \in \{!, !?, !?! \}$ and $m_9 \geq m_{10}$, then substitution holds for every formula ϕ built up from formulas of the form $m_9(P)$, where $P \in ELF(\mathbb{L})$.

(d) For each $m_i \in \{!, !?, !?! \}$, we have $m(\otimes_{i=1}^n m_i(A_i)) = m!(\otimes_{i=1}^n m_i(A_i))$.

Examples 4.3 (a) The system (LLE_1) of section 2 is obtained by the assignment

$$m_3 = ! \quad \text{and} \quad m_i = id, \text{ for every } i \neq 3.$$

(b) If we set

$$m_1 = m_2 = m_3 = m_5 = m_6 = m_8 = ! \quad \text{and} \quad m_4 = m_7 = m_9 = m_{10} = id,$$

we get the system (P_1) , in which "equality" is the interior of $(\cdot = \cdot)$. This system satisfies substitution for every formula.

(c) If we set

$$m_1 = m_2 = m_5 = m_6 = m_8 = ?, \quad m_4 = m_7 = m_9 = m_{10} = id \quad \text{and} \quad m_3 = !?$$

then we have a system in which "equality" corresponds to the closure of $(\cdot = \cdot)$; from $[S]$ will follows that that $!(\cdot = \cdot)$ is "clopen". This system satisfies the substitution rule for every formula.

(d) By considering

$$m_1 = m_3 = m_6 = m_{10} = ?! \quad m_2 = m_5 = m_8 = m_9 = !?! \quad \text{and} \quad m_4 = m_7 = !? \text{ or } !?!$$

we get a system containing a translation of the classical theory of equality inside (LL), to be studied in next section.

(e) Another translation of classical equality in (LL) can be obtained by considering the assignment

$$m_1 = id, m_2 = m_4 = m_5 = m_7 = m_8 = m_9 = ? \quad \text{and} \quad m_3 = m_6 = m_{10} = !.$$

Now, we would like to identify the classes of equivalent calculi. Instead of doing a complete classification of the possible calculi, we present quantale theoretic techniques that are useful in deciding this problem. We start with reflexivity ([R]) :

Proposition 4.4 *Let Q be a Girard's quantale, and let $x \in Q$. Then:*

(a) *Are equivalent:*

$$(i) ?x \geq 1 \quad (ii) !?x \geq 1 \quad (iii) ?!x \geq 1$$

(b) *Are equivalent:*

$$(i) x \geq 1 \quad (ii) !x \geq 1$$

(c) *Are equivalent:*

$$(i) ?!x \geq 1 \quad (ii) !?!x \geq 1$$

Proof: (a): If $?x \geq 1$, then $!x \geq !1 = 1$. If $!x \geq 1$, then $?!x \geq ?1 \geq 1$. Finally, $?!x \geq 1$ implies $?x \geq 1$, because $? \geq ?!?$.

(b) comes directly from $!1 = 1$, while (c) is consequence of (b). $\square$

Thus, introducing the notation $r \equiv s$ to denote that calculi obtained with $m_1 = r$ and $m_1 = s$ are equivalent, we have:

$$(a) ? \equiv !? \equiv ?!? \quad (b) id \equiv ! \quad (c) ?! \equiv !?!$$

and so there are only three non equivalent possibilities for [R].

With respect to axiom [S], consider $\mathcal{M}_1 = \{?, !?, !?! \} = \{?m : m \in \mathcal{M}\}$, together with $\mathcal{M}_2 = \{!, !?, !?! \} = \{!m : m \in \mathcal{M}\}$. Write $(r, s) \equiv (r', s')$ to denote that calculi obtained with $m_2 = r$, $m_3 = s$ and $m_2 = r'$, $m_3 = s'$ are equivalent. Then we have:

Proposition 4.5 (a) *If $m_3 \in \mathcal{M}_1$, then:*

$$(i) (!, m_3) \equiv (!!, m_3) \equiv (!!!, m_3) \quad (ii) (!?, m_3) \equiv (!?! , m_3) \quad (iii) (id, m_3) \equiv (?, m_3)$$

(b) *If $m_2 \in \mathcal{M}_2$, then:*

$$(i) (m_2, ?) \equiv (m_2, !?) \equiv (m_2, ?!?) \quad (ii) (m_2, ?!) \equiv (m_2, !?!) \quad (iii) (m_2, id) \equiv (m_2, !)$$

Therefore, there are only 26 non equivalent cases for [S]:

$$(1): (!, !?) \equiv (!, ?!) \equiv (!, ?) \equiv (!!, ?!) \equiv (!!, ?!?) \equiv (!!, !?) \equiv (!!, ?) \equiv (!!, ?)$$

$$\begin{aligned}
(2): (!?, !?) &\equiv (!?, !?) \equiv (!?, ?) \equiv (!?, !?) \equiv (!?, ?) \\
(3): (!, !?) &\equiv (!?, !?) \equiv (!, !?) \equiv (!, !?) \equiv (!?, !?) \\
(4): (id, ?) &\equiv (?, ?) \quad (5): (!?, !?) \equiv (!?, !?) \equiv (!?, !?) \quad (6): (id, !?) \equiv (?, !?) \\
(7): (id, !?) &\equiv (?, !?) \quad (8): (!, id) \equiv (!, !) \quad (9): (!?, !) \equiv (!?, id) \\
(10): (!?, !) &\equiv (!?, id) \quad (11): (id, id) \\
(12): (id, !) &\quad (13): (id, !?) \quad (14): (id, !?) \quad (15): (?, id) \quad (16): (?, !?) \\
(17): (?, !?) &\quad (18): (?, !) \quad (19): (!?, id) \quad (20): (!?, !?) \quad (21): (!?, !?) \\
(22): (!?, !) &\quad (23): (!?, id) \quad (24): (!?, !?) \quad (25): (!?, !?) \quad (26): (!?, !)
\end{aligned}$$

For transitivity ($[T]$), we shall write $(r, s, t) \equiv (r', s', t')$ when calculi obtained with $m_4 = r$, $m_5 = s$, $m_6 = t$ and $m_4 = r'$, $m_5 = s'$, $m_6 = t'$ are equivalent. Then we have:

Proposition 4.6 *If $m_5 \in \mathcal{M}_2$, then:*

- (i) *If $m_6 \in \mathcal{M}_1$, then $(r, m_5, m_6) \equiv (s, m_5, m_6)$ for every $r, s \in \mathcal{M}$*
- (ii) *$(r, m_5, ?) \equiv (s, m_5, ?) \equiv (id, m_5, !?) \equiv (!, m_5, !?) \equiv (!?, m_5, !?) \equiv (!?, m_5, !?) \equiv (t, m_5, !?) \equiv (u, m_5, !?)$ for every $r, s, t, u \in \mathcal{M}$.*
- (iii) *$(r, m_5, !?) \equiv (s, m_5, !?) \equiv (id, m_5, !?) \equiv (!, m_5, !?) \equiv (!?, m_5, !?) \equiv (!?, m_5, !?)$ for every $r, s \in \mathcal{M}$.*

The results above imply that, for $m_5 \in \mathcal{M}_2$ fixed, we have only 8 possibilities for pairs (m_4, m_6) (in contrast with 26 possibles ones), where the numbers refer to the pairs described above.

$$\begin{aligned}
[1] : (1) &\equiv (2) \equiv (4) \equiv (7) \equiv (13) & [2] : (3) &\equiv (5) \equiv (6) \equiv (14) \\
[3] : (8) &\equiv (11) \equiv (12) & [4] : (9) &\equiv (10) & [5] : (15) &\equiv (19) \equiv (23) \\
[6] : (16) &\equiv (20) \equiv (24) & [7] : (17) &\equiv (21) \equiv (25) & [8] : (18) &\equiv (22) \equiv (26)
\end{aligned}$$

With respect to substitution, if we fix $m_8, m_9 \in \mathcal{M}_2$, then there are again, for pairs (m_7, m_{10}) , only the 8 cases above. Thus, these are the non equivalent calculi that can be constructed with the exponentials, satisfying the usual rules of equality. We register that this corresponds to only 8% of the original universe of possible calculi.

5 Interpreting Classical Equality in Linear Logic with Equality

It is well known that the exponentials of linear logic (LL) are important in interpreting intuitionistic logic (IL) and classical logic (CL) inside LL . For each of these logics, we have two translations, one of them based in the fact that every (commutative) Girard's quantale contains a frame (complete Heyting algebra) (corollary 1.21) and a complete Boolean algebra:

$$\mathcal{H} = \{!x : x \in Q\} \quad \text{and} \quad \mathcal{B} = \{?!x : x \in Q\},$$

respectively. Operations and constants in each of these algebras are given by :

(H). For the frame $\mathcal{H}$:

$$\begin{aligned} 0_{\mathcal{H}} &= 0, \top_{\mathcal{H}} = 1, & (x \wedge_{\mathcal{H}} y) &= (x \otimes y) = !(x \wedge y), & (x \vee_{\mathcal{H}} y) &= (x \vee y); \\ (x \Rightarrow y) &= !(x \rightarrow y), & \neg x &= (x \Rightarrow 0_{\mathcal{H}}) = !(x \rightarrow 0), \\ \wedge_{\mathcal{H}} S &= !\wedge S, & \vee_{\mathcal{H}} S &= \vee S. \end{aligned}$$

(B). For the complete Boolean algebra $\mathcal{B}$:

$$\begin{aligned} 0_{\mathcal{B}} &= \perp, \top_{\mathcal{B}} = ?1, & (x \wedge_{\mathcal{B}} y) &= ?(!x \otimes !y) = ?!(x \wedge y), & (x \vee_{\mathcal{B}} y) &= (x \sqcup y) = (x^{\perp} \otimes y^{\perp})^{\perp}; \\ (x \Rightarrow y) &= (!x \rightarrow y), & \neg x &= (x \Rightarrow 0_{\mathcal{B}}) = (!x \rightarrow \perp) = ?(x^{\perp}); \\ \wedge_{\mathcal{B}} S &= ?!\wedge S, & \vee_{\mathcal{B}} S &= ?\vee\{!x : x \in S\}. \end{aligned}$$

Thus, we can interpret $A \in FOR(IL)$ as $A^i \in FOR(\mathbb{L})$ by the rules:

$A^i = !A$ if A is atomic; proceed by induction on complexity using the operations in (H) to define A^i for all intuitionistic formulas (here, $FOR(IL)$ denote the set of intuitionistic formulas).

For classical logic, we have our first translation :

(*) $A^c = ?!A$ if A is atomic; then proceed by induction on complexity, using the rules in (B).

Thus, if we assume two-hand sequents for (LL) , we have ([Gir]):

$A_1, \dots, A_n \vdash_{IL} A$ is provable in intuitionistic logic iff $(A_1)^i, \dots, (A_n)^i \vdash A^i$ is provable in LL ,

and

$(1^{st}T) : A_1, \dots, A_n \vdash_{CL} A$ is provable in classical logic iff $!(A_1)^c, \dots, !(A_n)^c \vdash A^c$ is provable in LL .

Another interpretation for classical logic is constructed from polarities for formulas. Thus, given a sequent for classical logic $\Gamma \vdash_{CL} \Delta$, we'll say that occurrences of formulas $A \in \Gamma$ are positive (denoted by pA) and occurrences of formulas $B \in \Delta$ are negative (denoted by nA). We have the following rules of a second translation (**):

$$\begin{aligned} pA &= A = nA \text{ if } A \text{ is atomic.} \\ p(\neg A) &= (nA)^{\perp}, n(\neg A) = (pA)^{\perp}, \\ p(A \vee B) &= p(A) \oplus p(B), n(A \vee B) = !n(A) \sqcup !n(B), \\ p(A \wedge B) &= ?p(A) \otimes ?p(B), n(A \wedge B) = n(A) \& n(B), \\ p(A \Rightarrow B) &= n(A)^{\perp} \oplus p(B), n(A \Rightarrow B) = ?p(A) - \circ !n(B), \\ p((\forall x)A) &= \wedge x. ?p(A), n((\forall x)A) = \wedge x. n(A), \\ p((\exists x)A) &= \vee x. p(A), n((\exists x)A) = \vee x. !n(A). \end{aligned}$$

With this definition, we have ([Gir]):

(**) $A_1, \dots, A_k \vdash_{CL} A$ is provable in (CL) iff $!n(A_1), \dots, !n(A_k) \vdash ?p(A)$ is provable in (LL) .

We now turn to the question of determining a linear theory of equality such that, given a classical theory of, its translation into linear logic defines a linear theory contained in the original linear theory of equality.

For this, we need to relate the deduction of a sequent in (LL) from a set of sequent-axioms and the deduction of a formula from a multiset of hypothesis (in the left-hand side of the sequent), called external and internal relations of consequence (respectively) by [Avr].

Definition 5.1 Let $A \in FOR(\mathbb{L})$ with exactly $x_1, \dots, x_n$ as free variables. The universal closure of A , denoted by $\bigwedge A$ is the formula obtained from A by quantifying universally all the free variables of A , i.e., $\bigwedge A = \bigwedge x_1 \cdots \bigwedge x_n. A$. Analogously, we define $\bigvee A$, the existencial closure of A .

It is straightforward to prove next result:

Proposition 5.2 Let $A_1, \dots, A_n$ be formulas, $B = !\bigwedge A_1 \& \cdots \& !\bigwedge A_n$, and Δ a multiset of formulas. Are equivalent:

- (i) $\vdash \Delta$ is provable from the sequent-axioms $\vdash A_1, \dots, \vdash A_n$;
- (ii) there exists $k \geq 0$ such that $\underbrace{B, \dots, B}_{k \text{ times}} \vdash \Delta$ is provable;
- (iii) $!\bigwedge A_1, \dots, !\bigwedge A_n \vdash \Delta$ is provable.

Now, assume that $\mathcal{A}$ is the set of axioms (without free variables) of a theory of (CL) in a language without functional symbols. It follows from Proposition 5.2 that if $A_1, \dots, A_n \in \mathcal{A}$ and A is a formula, then the following are equivalent, for the first translation $(*)$ of CL into LL :

- (i) $A_1, \dots, A_n \vdash_{CL} A$;
- (ii) $!(A_1)^c, \dots, !(A_n)^c \vdash A^c$ is provable in (LL) ;
- (iii) There is a proof of $\vdash A^c$ from the axioms $\vdash (A_1)^c, \dots, \vdash (A_n)^c$ (recall that the A_i 's have no free variables).

Thus, to each axiom $A \in \mathcal{A}$ of a classical theory, corresponds a sequent-axiom $\vdash A^c$ in (LL) . Similarly, for the second translation $(**)$, it can be seen that to each axiom $A \in \mathcal{A}$, there corresponds a sequent-axiom $\vdash n(A)$.

Now assume that $\mathcal{A}$ defines the classical theory of equality. Thus, $\mathcal{A}$ consists in the following axioms:

- $(\forall x)(x = x)$;
- $(\forall x)(\forall y)((x = y) \Rightarrow (y = x))$;
- $(\forall x)(\forall y)(\forall z)((x = y) \wedge (y = z) \Rightarrow (x = z))$;
- $(\forall x_1)(\forall y_1) \dots (\forall x_n)(\forall y_n)((x_1 = y_1) \wedge \cdots \wedge (x_n = y_n) \wedge P(x_1, \dots, x_n) \Rightarrow P(x_1 \wr y_1, \dots, x_n \wr y_n))$
(where P varies over every predicate symbol of arity n of the language).

For the first translation $(*)$, we get a calculus (E_1) with the following axioms:

- [R1] $\vdash ?!\bigwedge x ?!(x = x)$ [S1] $\vdash ?!\bigwedge x ?!\bigwedge y (!?(x = y) \multimap ?!(y = x))$
- [T1] $\vdash ?!\bigwedge x ?!\bigwedge y ?!\bigwedge z (!?(x = y) \otimes !?(y = z)) \multimap ?!(x = z)$
- [SUBST1] If P is a n -ary predicate symbol of the language
 $\vdash ?!\bigwedge x_1 ?!\bigwedge y_1 \cdots ?!\bigwedge x_n ?!\bigwedge y_n (!?(x_1 = y_1) \otimes \cdots \otimes !?(x_n = y_n) \otimes !?P(x_1, \dots, x_n))$
 $\multimap ?!P(x_1 \wr y_1, \dots, x_n \wr y_n))$

For the second translation (**), we get a calculus (E_2) with the following axioms:

$$[R2] \quad \vdash \wedge x (x = x) \quad [S2] \quad \vdash \wedge x \wedge y (? (x = y) \multimap ! (y = x))$$

$$[T2] \quad \vdash \wedge x \wedge y \wedge z (? (? (x = y) \otimes ? (y = z)) \multimap ! (x = z))$$

[SUBST2] If P is a n -ary predicate symbol in the language

$$\vdash \wedge x_1 \wedge y_1 \cdots \wedge x_n \wedge y_n (? (? (x_1 = y_1) \otimes \cdots \otimes ? (x_n = y_n) \otimes ? P(x_1, \dots, x_n)) \multimap ! P(x_1 \wr y_1, \dots, x_n \wr y_n)).$$

Consider the linear theory (P_1) determined by the axioms:

$$[LR1] \quad \vdash ?!(x = x) \quad [LS1] \quad \vdash ?!(x = y) \multimap ?!(y = x)$$

$$[LT1] \quad \vdash ?!(x = y) \otimes ?!(y = z) \multimap ?!(x = z)$$

$$[LSUBST1] \quad \vdash ?!(x_1 = y_1) \otimes \cdots \otimes ?!(x_n = y_n) \otimes ?!P(x_1, \dots, x_n) \multimap ?!P(x_1 \wr y_1, \dots, x_n \wr y_n).$$

Clearly, (P_1) contains (E_1) (because every axiom in (E_1) is deducible in (P_1), using the equivalences of last section) and we have that (P_1) defines a linear theory of equality in the sense of section 4.

Similarly, define the theory (P_2) by the axioms:

$$[LR2] \quad \vdash (x = x) \quad [LS2] \quad \vdash ?(x = y) \multimap ! (y = x)$$

$$[LT2] \quad \vdash ?(? (x = y) \otimes ? (y = z)) \multimap ! (x = z)$$

$$[LSUBST2] \quad \vdash ?(? (x_1 = y_1) \otimes \cdots \otimes ? (x_n = y_n) \otimes ? P(x_1, \dots, x_n)) \multimap ! P(x_1 \wr y_1, \dots, x_n \wr y_n).$$

We can reformulate (P_2) as:

$$[LR2'] \quad \vdash (x = x) \quad [LS2'] \quad \vdash (x = y) \multimap (y = x)$$

$$[LT2'] \quad \vdash (x = y) \otimes (y = z) \multimap (x = z)$$

$$[LSUBST2'] \quad \vdash ?((x_1 = y_1) \otimes \cdots \otimes (x_n = y_n) \otimes ? P(x_1, \dots, x_n)) \multimap ! P(x_1 \wr y_1, \dots, x_n \wr y_n)$$

$$[? \leq!] \quad \vdash ?(x = y) \multimap ! (x = y).$$

It is straightforward to check that (P_2) and (E_2) are equivalents. In fact, (P_2) is the strongest (and therefore more restricted as far as semantics is concerned) of the calculi already defined.

6 Equality and intuitionistic Linear Logic

In this section we shall study how to recover classical logic and intuitionistic logic from a linear calculus without exponentials, as well as analyse another extensions of the relationship between linear logic and quantales. Our basic system is (commutative) first order intuitionistic linear logic, from now on denoted by (LLI). The appropriate semantics will turn out to be furnished by commutative unital quantales. Similarly, the semantics for non-commutative first order intuitionistic linear shall be proven to be given by unital quantales. From this, it will be seen that, adding appropriate axioms, we can recover intuitionistic logic, classical logic and classical linear logic. Thus, an intuitionistic linear theory of equality provides an intuitionistic theory of equality, a classical theory of equality, and a classical linear theory of equality, simultaneously. The most natural candidate is system (LLE_0), the simplest already defined.

We define a sequent calculus for (commutative) first-order intuitionistic linear logic without

negation, simply by extending the system in [GiLa] and then proving soundness and completeness for this system.

Definition 6.1 The language $\mathbb{L}_i$ for commutative first-order intuitionistic linear logic consist of a countable set of predicate symbols, $\mathcal{P} = \{P_n : n \in \omega\}$, a countable set of variables $V = \{v_n : n \in \omega\}$, the symbols $\otimes, \multimap, \&, \oplus, \vee, \wedge$ and the same rules as in Definition 2.2 for the formation of the set of formulas $FOR(\mathbb{L}_i)$. For $A \in FOR(\mathbb{L}_i)$ and $x, y \in V$, $A[y/x]$ is as in Definition 2.4.

Definition 6.2 The calculus (LLI) for commutative first order intuitionistic linear logic consist in the following rules and axioms (A, B, C denote formulas, and Γ, Δ denote multisets of formulas):

$$\begin{array}{ll}
[AX1] \quad A \vdash A & [AX2] \quad \Gamma \vdash \top \\
[AX3] \quad \vdash 1 & [AX4] \quad \Gamma, 0 \vdash A \\
\\
[CUT] \quad \frac{\Gamma \vdash A \quad A, \Delta \vdash B}{\Gamma, \Delta \vdash B} & [EXCH] \quad \frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, B, A, \Delta \vdash C} \\
\\
[1L] \quad \frac{\Gamma \vdash A}{1, \Gamma \vdash A} & [\otimes R] \quad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} & [\otimes L] \quad \frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} \\
\\
[\&R] \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \& B} & [\&1] \quad \frac{\Gamma, A \vdash C}{\Gamma, A \& B \vdash C} & [\&2] \quad \frac{\Gamma, B \vdash C}{\Gamma, A \& B \vdash C} \\
\\
[\oplus L] \quad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \oplus B \vdash C} & [\oplus 1] \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} & [\oplus 2] \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B} \\
\\
[\multimap R] \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B} & [\multimap L] \quad \frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C} \\
\\
[\vee R] \quad \frac{\Gamma \vdash A[y/x]}{\Gamma \vdash \vee x.A} & [\vee L] \quad \frac{\Gamma, A \vdash B}{\Gamma, \vee x.A \vdash B} \quad \text{if } x \text{ not occurs free in } \Gamma, B \\
\\
[\wedge L] \quad \frac{\Gamma, A[y/x] \vdash B}{\Gamma, \wedge x.A \vdash B} & [\wedge R] \quad \frac{\Gamma \vdash A}{\Gamma \vdash \wedge x.A} \quad \text{if } x \text{ not occurs free in } \Gamma
\end{array}$$

Definition 6.3 An interpretation of quantales for (LLI) is a commutative unital quantale $(Q, \vee, *, 1)$ and a map $|\cdot|_Q : FOR(\mathbb{L}_i) \rightarrow Q$ satisfying:

1. $|0| = 0, |1| = 1, |\top| = \top$.
2. $|A \otimes B| = |A| * |B|, |A \multimap B| = |A| \rightarrow |B|$.
3. $|A \& B| = |A| \wedge |B|, |A \oplus B| = |A| \vee |B|$.
4. $|\wedge x.A| = \bigwedge_{y \in VAR(\mathbb{L}_i)} |A[y/x]|, |\vee x.A| = \bigvee_{y \in VAR(\mathbb{L}_i)} |A[y/x]|$.

We say that $A \in FOR(\mathbb{L}_i)$ is valid in Q if $|A|_Q \geq 1$.

A sequent $\Gamma \vdash A$ is valid in Q if $|\Gamma|_Q \leq |A|_Q$, where

$$|\Gamma|_Q = \begin{cases} 1 & \text{if } \Gamma = \emptyset \\ \bigotimes_{i=1}^n |A_i|_Q & \text{if } \Gamma = A_1, \dots, A_n \end{cases}$$

Before stating and proving soundness we establish the following simple

Lemma 6.4 *Let Q be a quantale. Then, $a \otimes 0 = 0 \otimes a = 0$ for every $a \in Q$.*

Proof: $0 \leq a \rightarrow_r 0$ implies $a \otimes 0 \leq 0$; $0 \leq a \rightarrow_l 0$ implies $0 \otimes a \leq 0$. $\square$

Theorem 6.5 (Soundness) *If $\Gamma \vdash A$ is provable in (LLI), then it is valid in every interpretation of quantales, i.e., $|\Gamma|_Q \leq |A|_Q$ for every unital quantale Q .*

Proof: By induction on least length n of a proof of $\Gamma \vdash A$.

Let Q be a quantale. If $n = 1$, [AX1], [AX2] and [AX3] are immediate, while [AX4] is a consequence of Lemma 6.4.

Assume the thesis holds for all sequents with a proof of length $\leq n$ ($n \geq 1$ fixed) and let $\Lambda \vdash D$ be a sequent admitting a proof of minimum length $n + 1$. We discuss the last rule applied in the proof of $\Lambda \vdash D$:

[CUT]: We have $|\Gamma| \leq |A|$ and $|A| * |\Delta| \leq |B|$ by the induction hypothesis; thus, $|\Gamma| * |\Delta| \leq |A| * |\Delta| \leq |B|$.

The passage through the rules [EXCH] and [1L] follow from the fact that Q is commutative and that **1** is the unit of Q .

[$\otimes R$]: $|\Gamma| \leq |A|$ and $|\Delta| \leq |B|$ (induction hypothesis) yield, then $|\Gamma| * |\Delta| \leq |A| * |B|$.

[$\otimes L$]: This works by definition of interpretation.

[$\& R$]: By induction, $|\Gamma| \leq |A|$ and $|\Gamma| \leq |B|$, and so $|\Gamma| \leq |A| \wedge |B|$.

[$\& 1$] and [$\& 2$]: We have $|\Gamma| * |A| \leq |C|$ (induction hypothesis); thus

$$|\Gamma| * (|A| \wedge |B|) \leq |\Gamma| * |A| \leq |C|.$$

The other rule is similar.

[$\oplus L$], [$\oplus 1$], [$\oplus 2$]: Same argument as in $\&$, using $\vee$ in place of $\wedge$.

[$\rightarrow R$]: Induction yields $|\Gamma| * |A| \leq |B|$; thus, by adjointness $|\Gamma| \leq |A| \rightarrow |B|$.

[$\rightarrow L$]: The induction hypothesis yields $|\Gamma| \leq |A|$ and $|\Delta| * |B| \leq |C|$. Thus,

$$(|A| \rightarrow |B|) * |\Gamma| * |\Delta| \leq (|A| \rightarrow |B|) * |A| * |\Delta| \leq |B| * |\Delta| \leq |C|.$$

[$\vee R$]: By induction, there is a variable y such that $|\Gamma| \leq |A[y/x]|$; but then

$$|\Gamma| \leq |A[y/x]| \leq \vee_y |A[y/x]|.$$

We now state a Fact whose proof is routine:

Fact: If $\Gamma, A \vdash B$ is provable in n steps and x is not free in either Γ or B , then $\Gamma, A[y/x] \vdash B$ is provable in n steps for every $y \in V$.

[$\vee L$]: Suppose that last rule applied was [$\vee L$]. Since x is not free in Γ, B , by induction and the Fact above, we may assume that $|\Gamma| * |A[y/x]| \leq |B|$, for every $y \in V$.

Thus, $|A[y/x]| \leq |\Gamma| \rightarrow |B|$ for every $y \in V$ and so $|\vee x A| = \vee_y |A[y/x]| \leq |\Gamma| \rightarrow |B|$, i.e. $|\Gamma| * |\vee x A| \leq |B|$.

$[\wedge L]$: This is treated just as $[\vee R]$, above.

$[\wedge R]$: Suppose that last rule applied was $[\wedge R]$. Since x is not free in Γ , induction and the Fact above allow us to assume that $|\Gamma| \leq |A[y/x]|$, for every $y \in V$. It is then clear that $|\Gamma| \leq \wedge_y |A[y/x]|$, ending the proof. $\square$

Before we prove completeness, we need a general result about quantales (generalizing an analogous result about Heyting algebras in [Mir]).

Definition 6.6 An autonomous poset is a partially ordered set P with a binary associative operation $\otimes$ such that the endomorphisms $a \otimes \cdot$ and $\cdot \otimes a$ have right adjoints, denoted by $a \rightarrow_r \cdot$ and $a \rightarrow_l \cdot$, respectively.

A $[\otimes, \vee]$ -autonomous lattice L is an autonomous poset where L is a lattice and such that $\otimes$ is distributive for all $\vee$'s which exists in L , i.e., if $S \subseteq L$ such that $\vee S$ exists in L , then, for every $a \in L$, $\vee_{s \in S}(a \otimes s)$ and $\vee_{s \in S}(s \otimes a)$ exists in L , and we have that $\vee_{s \in S}(a \otimes s) = a \otimes (\vee S)$, $\vee_{s \in S}(s \otimes a) = (\vee S) \otimes a$.

If S, T are subsets of L , define

$$S \cdot T = \{a \otimes b : a \in S \text{ and } b \in T\}.$$

Definition 6.7 Let L be a lattice and $I \subseteq L$ an ideal (i.e., if $x \in I$ and $y \leq x$ then $y \in I$; if $x, y \in I$ then $x \vee y \in I$). We say that I is complete if it satisfies:

$$\text{if } S \subseteq I \text{ such that } \vee_L S \text{ exists, then } \vee_L S \in I.$$

Since an arbitrary meet of complete ideals is again a complete ideal,

$CI(L) = \{I \subseteq L : I \text{ is a complete ideal in } L\}$, is a complete lattice ordered by inclusion, and containing, for each $a \in L$,

$$a^\leftarrow = \{x \in L : x \leq a\}.$$

If $a \in L$ and $S \subseteq L$ is a subset of L , define

$$a \rightarrow_r S \equiv_{\text{def}} \bigcup_{c \in S} (a \rightarrow_r c)^\leftarrow \quad \text{and} \quad a \rightarrow_l S \equiv_{\text{def}} \bigcup_{c \in S} (a \rightarrow_l c)^\leftarrow.$$

Lemma 6.8 Let L be a $[\otimes, \vee]$ -autonomous lattice. Then

(a) If $a \in L$ and $I \in CI(L)$, then $a \rightarrow_r I$ and $a \rightarrow_l I$ are in $CI(L)$.

(b) For every $S, T \subseteq L$ and $K \in CI(L)$, we have

$$S \cdot T \subseteq K \quad \text{iff} \quad S \subseteq \bigcap_{a \in T} (a \rightarrow_l K) \quad \text{iff} \quad T \subseteq \bigcap_{a \in S} (a \rightarrow_r K).$$

Proof:(a) If $x \in a \rightarrow_r I$, then there is $c \in I$ such that $x \leq a \rightarrow_r c$; thus, if $y \leq x$ then $y \leq a \rightarrow_r c$ and therefore $y \in a \rightarrow_r I$.

If $x, y \in a \rightarrow_r I$, then there are $c, d \in I$ such that $x \leq a \rightarrow_r c$, and $y \leq a \rightarrow_r d$; therefore

$$x \vee y \leq (a \rightarrow_r c) \vee (a \rightarrow_r d) \leq a \rightarrow_r (c \vee d),$$

yields $x \vee y \in a \rightarrow_r I$, because $c \vee d \in I$.

Let $S \subseteq a \rightarrow_r I$ be such that $c = \vee_L S$ exists. For every $s \in S$ there is $c_s \in I$ such that $s \leq a \rightarrow_r c_s$, i.e., $a \otimes s \leq c_s$. Since I is an ideal, $a \otimes s \in I$, for all $s \in S$. Then,

$$a \otimes c = a \otimes \bigvee_{s \in S} s = \bigvee_{s \in S} a \otimes s \in I,$$

because I is complete. But this means that $c \in a \rightarrow_r I$. A similar computation will prove that $a \rightarrow_l I \in CI(L)$.

(b) Let $x \in S$ and $a \in T$ and assume that $S \cdot T \subseteq K$; since $x \otimes a = c \in K$, then $x \leq a \rightarrow_l c$ and thus $x \in a \rightarrow_l K$, for every $a \in T$.

Now, suppose that $S \subseteq \bigcap_{a \in T} (a \rightarrow_l K)$, $x \in S$ and $a \in T$; since $x \in a \rightarrow_l K$, there is $c \in K$ such that $x \leq a \rightarrow_l c$, i.e. $x \otimes a \leq c$. Since K is an ideal, we get $x \otimes a \in K$. The other equivalence can be handled similarly. $\square$

Theorem 6.9 (*The completion of a $[\otimes, \vee]$ -autonomous lattice*)

Let L be a $[\otimes, \vee]$ -autonomous lattice with $\mathbf{0}, \top$. Then, there exists a quantale Q and an injective map $\phi: L \rightarrow Q$ such that

1. $\phi(\mathbf{0}) = \mathbf{0}$, $\phi(\top) = \top$. Moreover, ϕ preserves all $\vee$'s and $\wedge$'s existing in L , i.e., if $\bigvee_{i \in I} a_i$ and $\bigwedge_{j \in J} b_j$ exists in L , then

$$\phi(\bigvee_{i \in I} a_i) = \bigvee_{i \in I} \phi(a_i) \quad \text{and} \quad \phi(\bigwedge_{j \in J} b_j) = \bigwedge_{j \in J} \phi(b_j).$$

2. For all $a, b \in L$,

$$(i) \phi(a \otimes b) = \phi(a) \otimes \phi(b)$$

$$(ii) \phi(a \rightarrow_r b) = \phi(a) \rightarrow_r \phi(b) \quad \text{and} \quad \phi(a \rightarrow_l b) = \phi(a) \rightarrow_l \phi(b).$$

3. If $a \otimes b = b \otimes a$ for every $a, b \in L$, then Q is commutative.

4. If L is unital, i.e., there is $\mathbf{1} \in L$ such that $a \otimes \mathbf{1} = a = \mathbf{1} \otimes a$, $\forall a \in L$, then Q is unital and $\phi(\mathbf{1}) = \mathbf{1}_Q$.

5. If in addition, L has a cyclic dualizing element $\perp$, then Q is a Girard quantale and $\phi(\perp) = \perp$.

Proof: Set $Q = CI(L)$ and define in Q the operation

$$(I) \quad I * J \equiv_{\text{def}} \bigcap \{K \in Q : K \supseteq I \cdot J\}.$$

Clearly $*$ is increasing in both variables. By Lemma 6.8, $\cdot * I$ and $I * \cdot$ have right adjoints $I \rightarrow_r J$ and $I \rightarrow_l J$, given by

$$\bigcap_{a \in I} (a \rightarrow_r J) \quad \text{and} \quad \bigcap_{a \in I} (a \rightarrow_l J),$$

respectively. Thus, $\forall I, J \in Q$,

$$(II) \quad I * J \subseteq K \quad \text{iff} \quad I \subseteq J \rightarrow_l K \quad \text{iff} \quad J \subseteq I \rightarrow_r K.$$

Formulas (I) and (II) will be of constant use. To show that $*$ is associative, we need

Fact 1 : Let $I, J, K \in Q$. Then

$$\mathcal{A} = \{H \in Q : H \supseteq (I * J) \cdot K\} = \{H \in Q : H \supseteq I \cdot (J * K)\} = \mathcal{B}.$$

Proof of Fact 1 : We have, using Lemma 6.8, the following sequence of implications

$$H \supseteq (I * J) \cdot K \Rightarrow H \supseteq (I \cdot J) \cdot K = I \cdot (J \cdot K) \Rightarrow J \cdot K \subseteq I \rightarrow_r H \Rightarrow J * K \subseteq I \rightarrow_r H.$$

The last term implies $H \supseteq I \cdot (J * K)$ and $\mathcal{A} \subseteq \mathcal{B}$. Similar reasoning yields $\mathcal{B} \subseteq \mathcal{A}$.

It follows directly from the Fact that $*$ is associative. We now must show that $*$ distributes

over suprema.

Let $I \in Q$ and $\{I_\alpha\}_{\alpha \in A} \subseteq Q$; we shall prove that $I * \bigvee I_\alpha = \bigvee(I * I_\alpha)$. Observe that $\bigvee I_\alpha = \bigcap \{H \in Q : H \supseteq \bigcup_\alpha I_\alpha\}$, as well as that $\bigvee(I * I_\alpha) \subseteq I * \bigvee I_\alpha$ is always true. Now, we have the following sequence of implications

$$\begin{aligned} K \supseteq \bigcup(I * I_\alpha) &\Rightarrow K \supseteq I * I_\alpha, \forall \alpha \in A \Rightarrow I_\alpha \subseteq I \rightarrow_r K, \forall \alpha \in A \Rightarrow \bigcup I_\alpha \subseteq I \rightarrow_r K \Rightarrow \\ &\Rightarrow \bigvee I_\alpha \subseteq I \rightarrow_r K \Rightarrow I * \bigvee I_\alpha \subseteq K, \end{aligned}$$

and so $I * \bigvee I_\alpha \subseteq \bigvee(I * I_\alpha)$. Right distributivity is similar and so Q is indeed a quantale.

Before defining the map ϕ , we state

Fact 2 : For $a, b \in Q$

- (i) $a^\leftarrow \rightarrow_r b^\leftarrow = (a \rightarrow_r b)^\leftarrow$ and $a^\leftarrow \rightarrow_l b^\leftarrow = (a \rightarrow_l b)^\leftarrow$.
- (ii) If $S \subseteq L$ is such that $a = \bigvee S$ exists in L , then $\bigvee_{s \in S} s^\leftarrow = a^\leftarrow$.
- (iii) If $S \subseteq L$ such that $a = \bigwedge S$ exists in L , then $a^\leftarrow = \bigwedge_{s \in S} s^\leftarrow = \bigcap_{s \in S} s^\leftarrow$.
- (iv) $a^\leftarrow * b^\leftarrow = (a \otimes b)^\leftarrow$.

Proof of Fact 2 : (i) Let $K \in Q$ be such that $a^\leftarrow * K \subseteq b^\leftarrow$; for $x \in K$, we have $a \otimes x \leq b$ and so, $x \leq a \rightarrow_r b$. Thus, $K \subseteq (a \rightarrow_r b)^\leftarrow$, proving that $a^\leftarrow \rightarrow_r b^\leftarrow \subseteq (a \rightarrow_r b)^\leftarrow$.

For the reverse inclusion, consider $x \leq a$ and $y \leq a \rightarrow_r b$; then $x \otimes y \leq a \otimes (a \rightarrow_r b) \leq b$ and so $a^\leftarrow \cdot (a \rightarrow_r b)^\leftarrow \subseteq b^\leftarrow$, i.e., $a^\leftarrow * (a \rightarrow_r b)^\leftarrow \subseteq b^\leftarrow$. This last relation implies $(a \rightarrow_r b)^\leftarrow \subseteq a^\leftarrow \rightarrow_r b^\leftarrow$, as needed. For the operation $\rightarrow_l$, the argument is similar.

- (ii) If $\bigvee S = a$, then $s^\leftarrow \subseteq a^\leftarrow$ for every $s \in S$, and so it is clear that $\bigvee_{s \in S} s^\leftarrow \subseteq a^\leftarrow$.

If $H \supseteq \bigcup_{s \in S} s^\leftarrow$, since H is complete, it follows that $a \in H$.

- (iii) Is similar to (ii).

- (iv) If $x \leq a$, $y \leq b$ then $x \otimes y \leq a \otimes b$ implies $a^\leftarrow \cdot b^\leftarrow \subseteq (a \otimes b)^\leftarrow$. Thus, $a^\leftarrow * b^\leftarrow \subseteq (a \otimes b)^\leftarrow$.

Now, if $H \supseteq a^\leftarrow \cdot b^\leftarrow$ then $a \otimes b \in H$ and we get $(a \otimes b)^\leftarrow \subseteq H$. By the definition of $*$ (formula (I)), this yields $(a \otimes b)^\leftarrow \subseteq a^\leftarrow * b^\leftarrow$, as desired. This ends the proof of Fact 2.

We now define

$$\phi : L \longrightarrow Q \quad \text{by} \quad \phi(a) = a^\leftarrow.$$

Clearly ϕ is injective and, by Fact 2.(ii) and (iii), preserves all existing $\bigvee$'s and $\bigwedge$'s in L . Furthermore, $\phi(0) = \{0\}$ (the smallest complete ideal in L) and $\phi(1) = L = \top_Q$. The preservation of the others operations is guaranteed by Fact 2.(i) and (iv). This shows that ϕ has the properties in items 1 and 2 of the statement.

It is quite clear from the definition of $*$ (see (I), above) that Q will be commutative if $*$ is commutative in L . Moreover, if L is unital, straightforward computation will show that $\phi(1) = 1^\leftarrow$ is the unit of Q .

(d) Let $\perp \in L$ be a cyclic dualizing element in L . Clearly $\perp^\leftarrow \in Q$ is cyclic and therefore $Q_j = \{I \in Q : j(I) = I\}$ is a Girard quantale, where $j : Q \longrightarrow Q$ given by $j(I) = (I \rightarrow \perp^\leftarrow) \rightarrow \perp^\leftarrow$ (Proposition 1.10). Moreover, $a^\leftarrow \in Q_j$, for every $a \in L$. Thus, the map $j \circ \phi : L \longrightarrow Q_j$ is an embedding of L in a Girard quantale, with all the required properties. $\square$

We can now prove

Theorem 6.10 (Completeness) *If $|\Gamma|_Q \leq |A|_Q$ for all interpretations in quantales Q , then $\Gamma \vdash A$ is provable in (LLI) .*

Proof: Our method will be to show that the Lindenbaum algebra L of (LLI) can be embedded in a commutative unital quantale Q , such that $|\Gamma|_Q \leq |A|_Q$ iff $\Gamma \vdash A$ is provable.

Define in $FOR(\mathbb{L}_i)$ the relation:

$$A \sim B \quad \text{iff} \quad A \vdash B \quad \text{and} \quad B \vdash A \text{ are provable.}$$

It is easily seen that $\sim$ is an equivalence relation. Its equivalence classes shall be denoted by $A/\sim$.

Let L be the set of equivalence classes, i.e., $L = \{A/\sim : A \in FOR(\mathbb{L}_i)\}$. In L , define the relation:

$$A/\sim \leq B/\sim \quad \text{iff} \quad A \vdash B \text{ is provable in } (LLI).$$

By $[CUT]$, $\leq$ is a partial order in L . Moreover, for formulas A, B in LLI , we have

Fact 1 : If A, B are formulas in (LLI) , then

1. $(A \& B)/\sim = (A/\sim) \wedge (B/\sim)$ and $(A \oplus B)/\sim = (A/\sim) \vee (B/\sim)$.
2. $\bigwedge_{y \in V} (A[y/x]/\sim) = (\bigwedge x.A)/\sim$ and $\bigvee_{y \in V} (A[y/x]/\sim) = (\bigvee x.A)/\sim$.
3. $0 = 0/\sim$ and $1 = 1/\sim$.

Proof of Fact 1 : All these equalities can be read off the corresponding rules of the calculus. We do the first one in each of items 1. and 2. in some detail, just naming the rules that should be used for the other cases.

1. From $[AX1]$, $[\&1]$ and $[\&]$ we get $A \& B \vdash A, B$ and so $(A \& B)/\sim \leq A/\sim$, $(A \& B)/\sim \leq B/\sim$. On the other hand, if $C \vdash A$ and $C \vdash B$, then $[\&R]$ yields $C \vdash A \& B$. This means that

$$C/\sim \leq A/\sim, C/\sim \leq B/\sim \Rightarrow C/\sim \leq (A \& B)/\sim,$$

proving that $(A \& B)/\sim = (A/\sim) \wedge (B/\sim)$ in L .

Similarly, $[AX1]$, $[\oplus1]$, $[\oplus2]$ and $[\oplus L]$ will yield $(A \oplus B)/\sim = (A/\sim) \vee (B/\sim)$.

2. By $[AX1]$ and $[\wedge L]$, $(\bigwedge x.A)/\sim \leq A[y/x]/\sim$, for every $y \in V$.

If $B/\sim \leq A[y/x]/\sim$, for every y , let z be a variable not occurring in B . Then, $B/\sim \leq A[z/x]/\sim$ and so $[\wedge R]$ yields $B/\sim \leq (\bigwedge x.A)/\sim$. This proves that $\bigwedge_{y \in V} (A[y/x]/\sim) = (\bigwedge x.A)/\sim$.

For the existential quantifier, the reasoning is the same, using $[AX1]$, $[\vee R]$ and $[\vee L]$.

3. This follows directly from $[AX2]$ and $[AX4]$, ending the proof of Fact 1.

Define in L a binary operation $*$ by :

$$(A/\sim) * (B/\sim) \equiv_{def} (A \otimes B)/\sim.$$

Clearly, $*$ is well defined, is associative, commutative, increasing in both variables and $1/\sim$ is the unit. We have

Fact 2 : With the operation $*$ defined above, L is a $[\otimes, \vee]$ autonomous lattice.

Proof of Fact 2 : It remains to be shown that $*$ has right adjoints and distributes over the suprema existing in L .

If A, B, C are formulas in (LLI) , then

(+) $A \otimes B \vdash C$ is provable iff $A, B \vdash C$ is provable iff $A \vdash B \multimap C$ is provable.

To see this, note that $[\otimes R]$ yields $\frac{A \vdash A \quad B \vdash B}{A, B \vdash A \otimes B}$

Thus if $A \otimes B \vdash C$ is provable, $[CUT]$ implies that $A, B \vdash C$ is provable.

The converse comes directly from $[\otimes L]$ as $\frac{A, B \vdash C}{A \otimes B \vdash C}$.

From $[\multimap R]$ we get $\frac{A, B \vdash C}{A \vdash B \multimap C}$.

To show that the last clause in (+) implies the second, first note that $B, B \multimap C \vdash C$ is provable, because we can use $[\multimap R]$ as $\frac{B \vdash B \quad C \vdash C}{B, B \multimap C \vdash C}$.

Thus, the provability of $A \vdash B \multimap C$ and $B, B \multimap C \vdash C$ and $[CUT]$ yield that of $A, B \vdash C$.

It is clear from (+) that $(A \multimap \cdot)/\sim$ is the right adjoint to $A/\sim * \cdot = \cdot * A/\sim$ in L .

To show that $*$ distributes over the sup's in L , let $S \subseteq L$ be such that there is $A/\sim \in L$ satisfying $A/\sim = \bigvee_L S$. Fix $B/\sim \in L$. Since $*$ is increasing, $(B/\sim) * (X/\sim) \leq (B/\sim) * (A/\sim)$, for every $X/\sim \in S$.

Let $F/\sim \in L$ such that $(B/\sim) * (X/\sim) \leq F/\sim$, for every $X/\sim \in S$. By (+) we have that, for $X/\sim$ in S ,

$$B \otimes X \vdash F \text{ is provable iff } X \vdash (B \multimap F) \text{ is provable,}$$

$\forall X/\sim \in S$; taking sup's, we get $A \vdash (B \multimap F)$ is provable. Thus, $B \otimes A \vdash F$ is provable, and so $(B/\sim) * (A/\sim) \leq F/\sim$. But this means that $\bigvee_{X/\sim \in S} ((B/\sim) * (X/\sim))$ exists in L , and it's equal to $(B/\sim) * \bigvee_L S$, ending the proof of Fact 2.

Therefore, L is a commutative $[\otimes, \bigvee]$ -autonomous lattice and by theorem 6.9 it has a completion $\phi : L \rightarrow Q$, where Q is an unital commutative quantale. Moreover, ϕ preserves $\otimes$, $\multimap$, $\mathbf{0}$, $\top$, $\mathbf{1}$ and all existing $\bigvee$'s and $\bigwedge$'s in L . Consequently, if X, Y are formulas in (LLI) we have

$$\phi(X/\sim) \leq \phi(Y/\sim) \quad \text{iff} \quad X/\sim \leq Y/\sim.$$

It follows from these preservation properties that the map $|\cdot|_Q : FOR(\mathbb{L}_i) \rightarrow Q$ given by $|A|_Q = \phi(A/\sim)$ is an interpretation of quantales such that $|\Gamma| \leq |A|$ iff $\Gamma \vdash A$ is provable, as required to complete the proof of the Theorem. $\square$

Before we give logical applications of the preceding results, we need to investigate when is it that a quantale becomes a frame. From Lemma 6.4 comes :

Corollary 6.11 *Let Q be a quantale. If Q has a largest localic subquantale L , then*

$$L = I(Q) = \{a \in Q : a^2 = a\}.$$

Proof : We must have $L \subseteq I(Q)$ because every $x \in L$ is idempotent (proposition 1.19).

For $a \in I(Q)$, set $L_a = \{0, a\}$. By Lemma 6.4, L_a is closed under $\otimes$; it is clearly closed under arbitrary $\vee$'s, and so L_a is a subquantale of Q . Since a is idempotent, it follows that L_a is localic. Thus, $L_a \subseteq L$, i.e., $a \in L$, and therefore $I(Q) \subseteq L$. $\square$

The next result is a correction of Theorem 3.4.1 in [Ros], which is false as it stands. In fact, the usual quantale of phases of Linear Logic is a counterexample to that result.

Proposition 6.12 *Let Q be a quantale. Are equivalent:*

- (1) Q has a largest localic subquantale .
- (2) $I(Q)$ is a localic subquantale of Q .
- (3) For all every $a, b \in I(Q)$, $a \otimes b = b \otimes a \leq a \wedge b$ ($\wedge$ in Q or in $I(Q)$).

Proof. (1) $\Rightarrow$ (2) comes from Corollary 6.11, while (2) $\Rightarrow$ (3) is immediate.

(3) $\Rightarrow$ (1) : Because $I(Q)$ is commutative, it is closed under $\otimes$. To show that $I(Q)$ is closed under sup's, let $\{a_i\}_{i \in I} \subseteq I(Q)$. Then:

$$(*) \quad \bigvee_{i \in I} a_i = \bigvee_{i \in I} (a_i \otimes a_i) \leq \bigvee_{i, j \in I} (a_i \otimes a_j) = (\bigvee_{i \in I} a_i) \otimes (\bigvee_{j \in I} a_j);$$

$$(**) \quad (\bigvee_{i \in I} a_i) \otimes (\bigvee_{j \in I} a_j) = \bigvee_{i \in I} (\bigvee_{j \in I} (a_i \otimes a_j)) \leq \bigvee_{i \in I} a_i,$$

because $a_i \otimes a_j \leq a_i$ for every $j \in I$. From (*) and (**) it follows that $\bigvee_{i \in I} a_i$ is idempotent and so $I(Q)$ is a subquantale of Q .

To show that $I(Q)$ is localic, observe that it follows from 3. that $a \otimes b \leq a$, for every $b \in I(Q)$. Thus, $\forall a \in I(Q)$,

$$a \otimes \bigvee I(Q) = \bigvee_{b \in I(Q)} (a \otimes b) \leq a \quad \text{and} \quad (\bigvee I(Q)) \otimes a \leq a,$$

which shows that all elements of $I(Q)$ are idempotent and two-sided in $I(Q)$. Now, Proposition 1.19 guarantees that $I(Q)$ is localic. If $L \subseteq Q$ is a localic subquantale then every $x \in L$ is idempotent (Proposition 1.19) and so $L \subseteq I(Q)$. $\square$

Thus, in a commutative Girard quantale Q , $I(Q) \cap \mathbf{1}^\leftarrow$ is the **largest frame** contained in $\mathbf{1}^\leftarrow$. From the point of view of Logic, we have a privileged localic subquantale, that corresponds to intuitionistic Logic. However, the situation is quite different in the non commutative case : in general, a Girard quantale will not have a largest localic subquantale. If one considers Proposition 1.14, one realizes the importance of commutativity : there is a largest interpretation for ! in a Girard's quantale Q , corresponding to the largest among frames L satisfying

- (i) $L \subseteq Z(Q)$ (ii) $L \subseteq \mathbf{1}^\leftarrow = \{x \in Q : x \leq \mathbf{1}\}$

In fact, $Q_! = I(Q) \cap Z(Q) \cap \mathbf{1}^\leftarrow$, where $Z(Q)$ is the center of Q .

The quantale theoretic setting will be helpful in finding axioms that, when added to various systems of Linear Logic, produce classical intuitionism and classical logic. We have the simple (compare with proposition 1.19),

Lemma 6.13 *Let L be a complete lattice and $*$: $L \times L \longrightarrow L$ a binary operation on L . Are equivalent:*

- (i) $*$ = $\wedge$.
- (ii) (a) $x * x = x$ for every $x \in L$.

- (b) $x * \top \leq x, \top * x \leq x$ for every $x \in L$.
- (c) $*$ is increasing in both variables.

Proof: (i) $\Rightarrow$ (ii) is clear.

(ii) $\Rightarrow$ (i) : We have $a * b \leq a * \top \leq a; a * b \leq \top * b \leq b$ and therefore, $a * b \leq a \wedge b$.

On the other hand, since $*$ is increasing $a \wedge b = (a \wedge b) * (a \wedge b) \leq a * b$. $\square$

An analogous (and dual) result holds for the operation $\vee$. From the preceding results we get

Corollary 6.14 *Let Q be a quantale. Are equivalent:*

- (i) Q is a frame, i.e., $\otimes = \wedge$.
- (ii) every $x \in Q$ is idempotent and two-sided. $\square$

This Corollary and the completeness Theorem 6.10 yield

Proposition 6.15 (a) *The system (LI) obtained from (LLI) by adding the axioms*

$$[ID1] \quad \vdash A \otimes A \multimap A \quad [ID2] \quad \vdash A \multimap A \otimes A \quad [2S] \quad \vdash A \otimes \top \multimap A$$

determines intuitionistic logic, and therefore if we add to (LI) the axiom

$$[\neg\neg] \quad (A \multimap 0) \multimap 0 \vdash A$$

we get classical logic, where 1 is equivalent to $\top$ and $1 \multimap 0$ is equivalent to 0 .

Thus, adding the axioms [ID1], [ID2], [2S] and $[R=], [S=], [T=], [SUBST], [\leq 1]$ (see section 2) to (LLI) we obtain a intuitionistic theory of equality, which becomes first order classical logic with equality upon the addition of $[\neg\neg]$.

(b) *The system (MALL1) obtained from (LLI) by adding the constant formula $\perp$ to the language and the axiom*

$$[\neg\neg'] \quad (A \multimap \perp) \multimap \perp \vdash A,$$

is equivalent with (MALL) in the following sense:

$$\vdash A \text{ is provable in (MALL)} \quad \text{iff} \quad \vdash A \text{ is provable in (MALL1),}$$

where $A^\perp$ and $A \sqcup B$ are interpreted as $A \multimap \perp$ and $((A \multimap \perp) \otimes (B \multimap \perp)) \multimap \perp$, respectively. Thus, adding $\perp$ to the language we have that

(LLI) + the axioms $[\neg\neg'], [R=], [S=], [T=], [SUBST], [I=], [\leq 1]$ is equivalent to (LLE₀),

where (LLE₀) is described in Definition 2.6.

(c) *Adding [ID1], [ID2] and [2S] to (MALL1) produces classical logic, where 1 is equivalent to $\top$, and 0 is equivalent to $\perp$. $\square$*

Remark 6.16 *The possibility of obtaining (MALL) from (LLI) in part (b) appears in [Dos] proved by a different method : one interprets $A \multimap B$, $A \& B$ and $\bigwedge x.A$ as $(A \otimes (B \multimap \perp)) \multimap \perp$, $((A \multimap \perp) \oplus (B \multimap \perp)) \multimap \perp$ and $(\bigvee x.(A \multimap \perp)) \multimap \perp$, respectively, together with the interpretation for $\sqcup$ maked in (b).*

Since $(a \otimes b) \rightarrow c = a \rightarrow (b \rightarrow c)$ and $b = \mathbf{1} \rightarrow b$, in every unital commutative quantale, it can be shown that his interpretation of linear implication is equivalent to adding $[\neg\neg']$ to (LLI) to obtain $(MALL)$ (translations for $\&$ and $\wedge$ are derived and a consequence of the ones given).

As a matter of fact, we can extend this result to non-commutative intuitionistic linear logic, simply by observing that each rule of (LLI) determines an algebraic property of the Lindenbaum algebra of the calculus. For a general unital quantale, we need two implications, $\multimap_l$ and $\multimap_r$, to discard the exchange rule $[EXCH]$, as well as to modify the rules in order to describe the properties of each operation. We can define a linear calculus which describes unital quantales, essentially the same as in [Abr].

Definition 6.17 *The calculus $(NCLLI)$ for noncommutative first-order linear intuitionistic logic consist in the following rules and axioms:*

$$\begin{array}{ll}
[AX1] \quad A \vdash A & [AX2] \quad \Gamma \vdash \top \\
[AX3] \quad \vdash \mathbf{1} & [AX4] \quad \Gamma, \mathbf{0}, \Delta \vdash A \\
[CUT] \quad \frac{\Gamma \vdash A \quad \Sigma, A, \Delta \vdash B}{\Sigma, \Gamma, \Delta \vdash B} & [1L] \quad \frac{\Gamma, \Delta \vdash A}{\Gamma, \mathbf{1}, \Delta \vdash A} \\
[\otimes R] \quad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} & [\otimes L] \quad \frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, A \otimes B, \Delta \vdash C} \\
[\& R] \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \& B} & [\oplus L] \quad \frac{\Gamma, A, \Delta \vdash C \quad \Gamma, B, \Delta \vdash C}{\Gamma, A \oplus B, \Delta \vdash C} \\
[\& L1] \quad \frac{\Gamma, A, \Delta \vdash C}{\Gamma, A \& B, \Delta \vdash C} & [\& L2] \quad \frac{\Gamma, B, \Delta \vdash C}{\Gamma, A \& B, \Delta \vdash C} \\
[\oplus R1] \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} & [\oplus R2] \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B} \\
[\multimap_l L] \quad \frac{\Gamma \vdash A \quad \Sigma, B, \Delta \vdash C}{\Sigma, A \multimap_l B, \Gamma, \Delta \vdash C} & [\multimap_l R] \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap_l B} \\
[\multimap_r L] \quad \frac{\Gamma \vdash A \quad \Sigma, B, \Delta \vdash C}{\Sigma, \Gamma, A \multimap_r B, \Delta \vdash C} & [\multimap_r R] \quad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap_r B} \\
[\vee R] \quad \frac{\Gamma \vdash A[y/x]}{\Gamma \vdash \vee x.A} & [\vee L] \quad \text{If } x \text{ is not free in } \Gamma, \Delta, B \text{ then } \frac{\Gamma, A, \Delta \vdash B}{\Gamma, \vee x.A, \Delta \vdash B} \\
[\wedge L] \quad \frac{\Gamma, A[y/x], \Delta \vdash B}{\Gamma, \wedge x.A, \Delta \vdash B} & [\wedge R] \quad \text{If } x \text{ is not free in } \Gamma \text{ then } \frac{\Gamma \vdash A}{\Gamma \vdash \wedge x.A}
\end{array}$$

With the same method employed in Theorems 6.5 and 6.10, Theorem 6.9 yields that unital quantales are a complete and sound class of models for $(NCLLI)$:

Theorem 6.18 : *(Completeness and Soundness for $(NCLLI)$)*

A sequent $\Gamma \vdash A$ is provable in $[NCLLI]$ iff $\Gamma \vdash A$ is valid in every interpretations of quantales.

References

- [Abr] V.M. Abrusci, Non-commutative Intuitionistic Linear Logic, *Zeitschr. f. math. Logik und Grundlagen d. Math.* 36 (1990), 297-318.
- [Avr] A. Avron, The Semantics and Proof Theory of Linear Logic, *Theoretical Computer Science* 57 (1988), 161-184.
- [BrGu] C. Brown and D. Gurr, A Representation Theorem for Quantales, *Journal of Pure and Applied Algebra* 85 (1993), 27-42.
- [Dos] K. Dosen, Nonmodal Classical Linear Predicate Logic is a Fragment of Intuitionistic Linear Logic, *Theoretical Computer Science* 102 (1992), 207-214.
- [Gir] J.Y. Girard, Linear Logic, *Theoretical Computer Science* 50 (1987), 1-102.
- [GiLa] J.Y. Girard and Y. Lafont, Linear Logic and Lazy Computation, *Lectures Notes in Computer Science* 250 (Springer, 1987), 52-66.
- [Mir] F. Miraglia, **Sheaves and Logic**, preprint.
- [Ros] K. Rosenthal, **Quantales and their Applications**, Pitman Research Notes in Mathematics Series, vol. 234 (Longman, Harlow, 1990).
- [Yet] D. Yetter, Quantales and (Noncommutative) Linear Logic, *Journal of Symbolic Logic* 55 (1990), 41-64.

M.E. Coniglio
Instituto de Matemática e Estatística
Universidade de São Paulo
Caixa Postal 66.281 - Cep 05315-970
S.Paulo, S.P. Brasil
e-mail : conigli@ime.usp.br

F. Miraglia
Instituto de Matemática e Estatística
Universidade de São Paulo
Caixa Postal 66.281 - Cep 05315-970
S.Paulo, S.P. Brasil
e-mail : miraglia@ime.usp.br or
miraglia@jussieu.logique.fr