Aplicações de matrizes no ensino médio

Silvia da Rocha Izidoro Ferreira

Aplicações de matrizes no ensino médio

Silvia da Rocha Izidoro Ferreira

Orientador: **Prof. Dr. Sérgio Henrique Monari Soares**

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Programa de Mestrado Profissional em Matemática. *VERSÃO REVISADA*

USP – São Carlos
Maio de 2013

Ficha catalográfica preparada pela Seção de Tratamento
da Informação da Biblioteca Prof. Achille Bassi – ICMC/USP

F383a

Ferreira, Silvia da Rocha Izidoro
Aplicações de Matrizes no ensino médio / Silvia da Rocha Izidoro Ferreira; orientador Sérgio Henrique Monari Soares. -- São Carlos, 2013.
57 p.

Dissertação (Mestrado – Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2013.

1. Matrizes. 2. Produto de matrizes. 3. Aplicações de matrizes. I. Soares, Sérgio Henrique Monari, orient. II. Título.

Dedico esse trabalho ao
meu esposo, Rovaldo, que
renunciou a seus sonhos
para que eu pudesse viver
os meus, e também à
minha filha, Anna Lívia,
que sem saber me motivava
a continuar.
Meus amores, essa vitória
não é minha, e sim nossa.

Agradecimentos

Agradeço em primeiro lugar a Deus que possibilitou que eu chegasse até aqui, iluminando cada passo, colocando pessoas abençoadas em meu caminho.

Ao meu professor orientador, Sérgio Henrique Monari Soares, por ser um grande mestre, não só pelo seu saber, mas principalmente por sua generosidade e paciência, com que conduziu esse trabalho, a ele minha eterna gratidão e respeito.

A todos os professores do Profmat, USP - São Carlos, em especial à professora coordenadora, Ires, por nos animar nos momentos de angústias e vibrar com nossas vitórias. Obrigada por acreditar em nós.

À minha amiga, Regina Célia Saraiva, a qual possui um imenso coração, que me apoiou nos momentos de desânimo, e não se cansou de ouvir meus desabafos e me fortalecia dizendo que eu era capaz.

Resumo

FERREIRA, S. R. I. Aplicações de matrizes no ensino médio. 2013. 55 f. Dissertação (Mestrado) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2013.

Esta dissertação tem como objetivo salientar a utilidade e importância de cálculos matriciais no ensino médio. Para tanto, foram estudados alguns tópicos que descrevem situações que necessitam de recursos gerados por operações matriciais. Foi observado que esses tópicos apresentam situações que evidenciam a utilidade da multiplicação de matrizes não somente no desenvolvimento teórico, mas também nas aplicações de matrizes, e têm potencial para serem abordados no ensino médio.

Palavras-chave: Matrizes. Produto de matrizes. Aplicação de matrizes.

Abstract

FERREIRA, S. R. I. Applications of matrices in the secondary school. 2013. 55 f. Dissertação (Mestrado) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2013.

The aim is this work is to stress on the use of algebraic operations with matrices in the mathematics teaching for secondary school students. For this purpose, we studied some topics that require algebraic operations with matrices. It was observed that these topics reveal circumstances in which the matrix multiplication is not only useful in the theoretical development but also in the applications. In addition, the studied showed that these themes have potential to be considered in the secondary school.

Key words: Matrices. Matrix multiplication. Application of matrices.

Sumário

Introdução

Matrizes estão presentes no currículo do ensino Médio e o seu ensino é organizado pelo conteúdo:[1]

- Matrizes: significado como tabelas, características e operações.
- A noção de determinante de uma matriz quadrada.
- Resolução e discussão de sistemas lineares: escalonamento.

Matrizes surgem naturalmente em uma variedade de situações e problemas, cuja aplicação vai além da resolução e discussão de sistemas lineares. Diante dessa constatação, a motivação inicial da presente dissertação foi situar a teoria de matrizes como uma linguagem natural para a resolução de certos problemas e oferecer um conjunto de aplicações em diferentes ramos da matemática e outras áreas do saber. Como objetivo específico, pretendemos que esta dissertação forneça um plano de aula sobre um tópico de matrizes que possa ser efetivamente desenvolvido no ensino médio.

Diante dos desafios, a primeira tarefa foi decidir o que estudar. Para tanto, analisamos cuidadosamente o conteúdo da disciplina Álgebra Linear, do ensino superior, onde matrizes são amplamente estudadas, e escolhemos tópicos com maior potencial para aplicação no ensino médio. Para isso, foi levado em consideração a utilização mínima de pré-requisitos e a beleza dos problemas a serem abordados. Tal escolha resultou nos seguintes temas:

1. Aplicações do produto de matrizes.
    - Grafos dirigidos.
    - Criptografia.
    - Cadeias de Markov.

[1] Proposta Curricular do Estado de São Paulo: Matemática - Coord. Maria Inês Fini. - São Paulo: SEE, 2008.

- Genética.

2. Aplicações do determinante.

   - Construção de curvas e superfícies por pontos especificados.
   - Determinante como área ou volume.

Um aspecto que merece destaque é o esforço metodológico que fizemos para desenvolver esses temas utilizando essencialmente o produto de matrizes, não somente nas aplicações, mas também no desenvolvimento teórico. Fizemos desse modo, com o desejo de evidenciar a importância do estudo da operação e também mostrar que a multiplicação de matrizes combinada com o escalonamento produz uma técnica poderosa para estabelecer propriedades e interpretar certos conceitos, tal como fizemos no Capítulo 2 para o determinante.

Capítulo

1

Aplicações do produto de matrizes

Este capítulo é dedicado às aplicações das propriedades aritméticas de matrizes, mais especificamente o produto de matrizes. Seguindo [1, Capítulo 11], estudamos as aplicações em grafos dirigidos, criptografia, cadeias de Markov e genética. Iniciamos relembrando a definição do produto de matrizes.

Definição 1.1. *Sejam $A = (a_{ik})$ e $B = (b_{kj})$ duas matrizes $n \times p$ e $p \times q$, respectivamente. O produto AB é definido como a matriz $C = (c_{ij})$, onde*

$$c_{ij} = a_{i1}b_{1j} + \cdots + a_{ip}b_{pj},$$

para $i = 1, \cdots, n$ e $j = 1, \cdots, q$.

1 Grafos dirigidos

Multiplicação de matrizes é amplamente utilizada na teoria de grafos, um ramo da matemática que se mostra útil para modelagem em diversas situações na ciência de computação, economia e em ciências sociais. Iniciamos introduzindo grafos dirigidos e a relação com matrizes. Nosso objetivo é mostrar como matrizes são empregadas para calcular o número de caminhos de um certo comprimento entre vértices de um grafo.

Definição 1.2. *Um **grafo dirigido** é um conjunto finito de elementos $\{P_1, ..., P_n\}$ junto com uma coleção finita de pares ordenados (P_i, P_j) de elementos distintos deste conjunto, sem*

repetição de pares ordenados. Os elementos do conjunto são chamados ***vértices*** *e os pares ordenados* ***arestas dirigidas*** *do grafo dirigido.*

Dado um grafo dirigido $\{P_1, ..., P_n\}$, a notação $P_i \to P_j$ indica que o elemento P_i está conectado ao elemento P_j. Neste caso, a aresta dirigida (P_i, P_j) pertence ao grafo dirigido. Geometricamente, um grafo dirigido é visualizado representando os vértices como pontos no plano e as arestas dirigidas $P_i \to P_j$ como segmentos de reta ou de arco, desde o vértice P_i até o vértice P_j, com uma seta de P_i para P_j. Se ambos os vértices estão relacionados, isto é, $P_i \to P_j$ e $P_j \to P_i$, é desenhado somente um segmento entre P_i e P_j, mas com setas apontando em sentidos opostos. A Figura 1.1 fornece uma representação geométrica de um grafo dirigido.

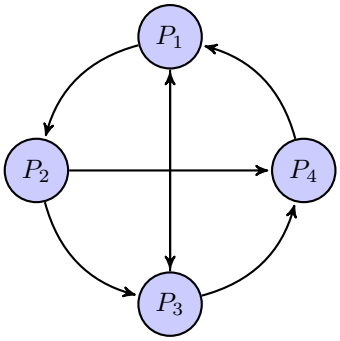


Figura 1.1

A partir de um grafo dirigido de n vértices podemos associá-lo a uma matriz $M = (m_{ij})$ quadrada de ordem n. Tal matriz é denominada **matriz de vértices** do grafo dirigido. Os elementos da matriz M, obedecem à seguinte regra:

$$m_{ij} = \begin{cases} 1, & \text{se } P_i \to P_j, \\ 0, & \text{caso contrário.} \end{cases}$$

Exemplo 1.3. *A matriz de vértices associada ao grafo da Figura 1.1 é dada por*

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Ainda pela Figura 1.1, o vértice P_2 não está conectado diretamente ao vértice P_1. Mas P_2 está conectado a P_4, que por sua vez está concetado a P_1. Escrevemos $P_2 \to P_4 \to P_1$ e chamamos conexão de 2 passos de P_2 para P_1. Similarmente, chamamos $P_2 \to P_4$ conexão de 1 passo, $P_2 \to P_4 \to P_1 \to P_3$ conexão de 3 passos, e assim por diante. O resultado a seguir faz uso do produto de matrizes para encontrar o número de todas as conexões de k passos, $k \in \mathbb{N}$, de um vértice P_i para um vértice P_j de um grafo dirigido qualquer.

Teorema 1.4. *Seja M uma matriz de vértices de um grafo dirigido e seja $m_{ij}^{(k)}$ o elemento (i,j) da matriz M^k. Então $m_{ij}^{(k)}$ é igual ao número de conexões de k passos do vértice P_i para o vértice P_j.*

PROVA: A prova será feita por indução. Para $k = 1$, o número de conexões de 1 passo de um vértice P_i para um vértice P_j é simplesmente m_{ij}. Ou seja, há somente zero ou uma conexão de 1 passo de P_i para P_j. Sendo $m_{ij} = m_{ij}^{(1)}$, o resultado é verdadeiro para $k = 1$.

Suponhamos que o resultado seja verdadeiro para k, isto é, o elemento (i,j) de M^k, $m_{ij}^{(k)}$, é o número de conexões de k passos de P_i para P_j.

Para o número de conexões de $k+1$ passos, consideremos a potência $k+1$ de M. Seja $m_{ij}^{(k+1)}$ o elemento (i,j) de M^{k+1}. Como $M^{k+1} = M^k M$, temos

$$m_{ij}^{(k+1)} = m_{i1}^{(k)} m_{1j} + m_{i2}^{(k)} m_{2j} + \cdots + m_{in}^{(k)} m_{nj}. \tag{1.1}$$

Agora, pela hipótese de indução, se $m_{i1}^{(k)} \neq 0$ e $m_{i1}^{(k)} = 1$, então há uma conexão de k passos de P_i para P_1 seguida por uma conexão de 1 passo de P_1 para P_j, e portanto há uma conexão de $k+1$ passos de P_i para P_j. No entanto, se $m_{i1}^{(k)}$ ou m_{1j} é zero, então uma conexão de P_i para P_j de $k+1$ passos, passando por P_1, não é possível. Assim, uma conexão de P_i para P_j, passando por P_1, é de $k+1$ passos se, e somente se, $m_{i1}^{(k)} m_{1j} \neq 0$. Analogamente, para cada $l = 1, 2, \cdots, n$, uma conexão de P_i para P_j, passando por P_l, é de $k+1$ passos se, e somente se, o termo $m_{il}^{(k)} m_{lj}$, à direita de (1.1), é não nulo; caso contrário o termo é zero e uma tal conexão de $k+1$ passos não é possível. Assim, o lado direito de (1.1) é o número total de conexões de $k+1$ passos de P_i para P_j. Portanto, pelo princípio de indução, o resultado é verdadeiro para todo $k \in \mathbb{N}$. ■

Exemplo 1.5. *Seja A a matriz de vértices de um grafo dirigido dada por*

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Pelo Teorema 1.4, podemos encontrar o número de conexões de 3 passos do vértice P_1 ao vértice P_4 por meio da matriz

$$A^3 = \begin{pmatrix} 2 & 3 & 2 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 2 & 1 & 2 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

Como $m_{14}^{(3)} = 2$, há duas conexões de 3 passos para ir do vértice P_1 ao vértice P_4.

A definição a seguir destaca subconjuntos de um grafo dirigido que possuem seus elementos conectados uns com os outros. Por exemplo, se os vértices representam cidades e $P_i \to P_j$ significa que existe um voo direto de P_i para P_j, então existem voos diretos em ambos sentidos entre as duas cidades quaisquer desse subconjunto.

Definição 1.6. *Um subconjunto de um grafo dirigido é chamado uma panela se as seguintes condições estão satisfeitas:*

(i) O subconjunto contém pelo menos três vértices;

(ii) Para cada par de vértices P_i e P_j no subconjunto, ambos $P_i \to P_j$ e $P_j \to P_i$ são verdadeiros;

(iii) O subconjunto é tão grande quanto possível; ou seja, não há como acrescentar mais nenhum vértice ao subconjunto e ainda satisfazer a condição (ii).

Exemplo 1.7. *O grafo dirigido ilustrado na figura a seguir tem duas panelas:*

$$\{P_1, P_2, P_3, P_4\} \quad e \quad \{P_3, P_4, P_6\}.$$

Este exemplo mostra que um grafo dirigido pode ter várias panelas e que um vértice pode pertencer simultaneamente a mais de uma panela.

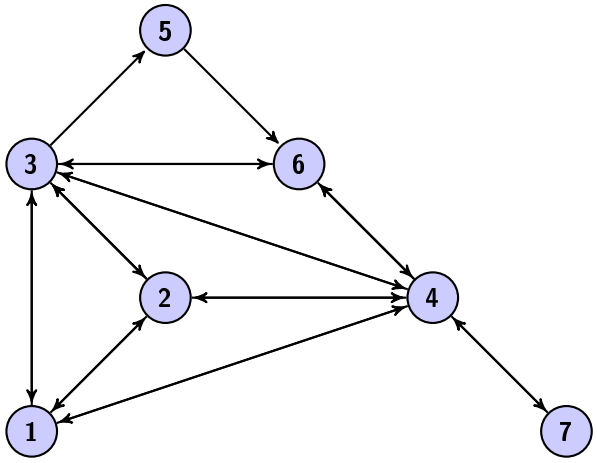
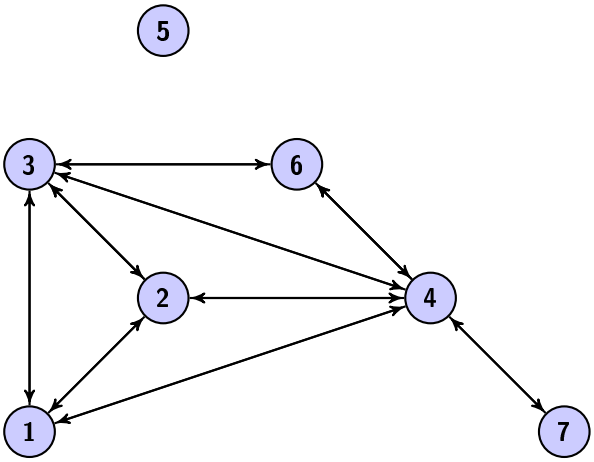


Figura 1.2

Para grafos dirigidos simples, as panelas podem ser encontradas por inspeção. Quando o grafo dirigido é grande, é conveniente definir uma matriz $S = (s_{ij})$ relacionada ao grafo, para então encontrar panelas. Defina

$$s_{ij} = \begin{cases} 1, & \text{se } P_i \leftrightarrow P_j, \\ 0, & \text{caso contrário.} \end{cases}$$

A matriz S determina um grafo dirigido idêntico ao grafo dirigido dado, exceto pelas arestas com somente uma seta que foram eliminadas. Por exemplo, para o grafo dirigido ilustrado pela Figura 1.2, o grafo dirigido que tem S como matriz de vértices é dado pela figura



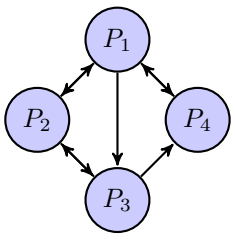
O teorema a seguir utiliza a matriz S e novamente o produto de matrizes para identificar panelas.

Teorema 1.8. *Seja s_{ij}^3 o (i,j)-ésimo elemento de S^3. Então um vértice P_i pertence a uma panela se, e somente se, $s_{ii}^3 \neq 0$.*

Prova: Se $s_{ii}^3 \neq 0$, então existe pelo menos uma conexão de 3 passos de P_i para si mesmo no grafo dirigido modificado por S, digamos, $P_i \to P_j \to P_k \to P_i$. No grafo dirigido modificado, todas as relações dirigidas são bilaterais, de modo que nós também temos as conexões $P_i \leftrightarrow P_j \leftrightarrow P_k \leftrightarrow P_i$. No entanto, isto significa que $\{P_i, P_j, P_k\}$ é ou uma panela ou um subconjunto de uma panela. Em ambos casos, P_i deve pertencer a alguma panela. A afirmação recíproca, que se P_i pertence a alguma panela, então $s_{ii}^3 \neq 0$, segue de maneira análoga. ■

Exemplo 1.9. *Verifique se grafo dirigido dado possui panelas:*

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$



onde M é a matriz de vértices relacionada ao grafo dirigido acima. Assim,

$$S = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad e \quad S^3 = \begin{pmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{pmatrix}.$$

Como $s_{11}^3, s_{22}^3, s_{33}^3, s_{44}^3$ *são todos nulos, segue que esse grafo dirigido não possui panela. Suponha agora um grafo dirigido tendo como matriz de vértices*

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Nesse caso,

$$S = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad e \quad S^3 = \begin{pmatrix} 2 & 4 & 0 & 4 & 3 \\ 4 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 2 & 1 \\ 3 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

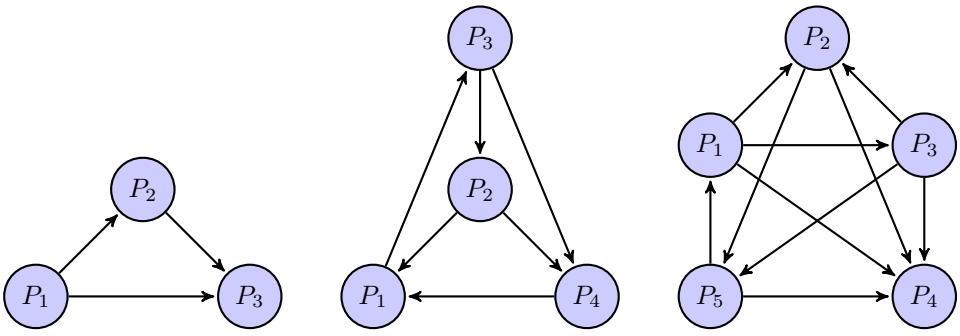
Como $s_{11}^3, s_{22}^3, s_{44}^3$ *são diferentes de zero, segue que* P_1, P_2, P_4 *pertencem a panelas. Como uma panela deve conter pelo menos três vértices, segue que esse grafo dirigido possui apenas uma panela, a saber,* $\{P_1, P_2, P_4\}$.

A próxima definição introduz o conceito de dominância para construir um grafo dirigido.

Definição 1.10. *Um grafo dirigido por dominância é um grafo dirigido de modo que, para qualquer par de vértices distintos* P_i *e* P_j, $P_i \to P_j$ *ou* $P_j \to P_i$, *mas não ambos.*

Exemplo 1.11. *Considere um campeonato com uma divisão de n equipes esportivas em que cada equipe joga exatamente uma vez com cada uma das outras, em que não são permitidos empates, no estilo de rodadas eliminatórias. Se* $P_i \to P_j$ *significa que* P_i *derrota* P_j. *Neste caso, a definição de grafo dirigido por dominância está satisfeita.*

A figura a seguir dá alguns grafos dirigidos por dominância com três, quatro e cinco vértices, respectivamente.



Nestes três grafos dirigidos por dominância, os vértices P_1 do primeiro grafo, os vértices P_1, P_2, P_3 do segundo grafo e P_1, P_3, P_5 do terceiro grafo têm a seguinte propriedade

interessante: de cada um deles existe uma conexão de 1 ou de 2 passos para cada outro vértice do grafo. Num torneio esportivo, estes vértices correspondem às equipes mais "poderosas" que derrotam uma outra equipe, ou derrotam uma equipe que derrota esta outra equipe. O teorema a seguir garante que qualquer grafo dirigido por dominância tem pelo menos um vértice com esta propriedade.

Teorema 1.12. *Em qualquer grafo dirigido por dominância, existe pelo menos um vértice do qual existem conexões de 1 ou 2 passos para qualquer outro vértice.*

PROVA: Considere um vértice com o maior número total de conexões de 1 e de 2 passos para os outros vértices do grafo. Renumerando, se necessário, os vértices, podemos supor que P_1 é um tal vértice. Suponhamos que P_i é um vértice tal que, não existem conexões de 1 ou de 2 passos de P_1 para P_i. Então, em particular, $P_1 \to P_i$ não é verdadeiro, de modo que pela definição de grafo dirigido por dominância, $P_i \to P_1$ é verdadeiro. Suponha agora, que P_k é um vértice tal que $P_1 \to P_k$ é verdadeiro. Então não podemos ter $P_k \to P_i$ pois, neste caso, $P_1 \to P_k \to P_i$ seria uma conexão de 2 passos de P_1 para P_i. Assim, necessariamente, $P_i \to P_k$ é verdadeiro, ou seja, P_i tem uma conexão de 1 passo para todos os vértices para os quais P_1 tem uma conexão de 1 passo. Este vértice P_i então também tem uma conexão de 2 passos para todos os vértices para os quais P_1 tem uma conexão de 2 passos. No entanto, temos adicionalmente que $P_i \to P_1$ é verdadeiro, de modo que P_i tem mais conexões de 1 e de 2 passos a outros vértices de grafo do que P_1. Isto contradiz a maneira pela qual escolhemos P_1, pelo que concluímos que não existe o tal vértice P_i para o qual P_1 não possui conexões de 1 e de 2 passos. ■

A prova anterior mostra que um vértice com o maior número total de conexões de 1 e de 2 passos para os outros vértices do grafo tem a propriedade enunciada no teorema. Uma maneira simples de encontrar tais vértices é utilizar a matriz de vértices M e seu quadrado M^2. A soma das entradas na i-ésima linha de M é o número total de conexões de 1 passo de P_i para os outros vértices e a soma das entradas na i-ésima linha de M^2 é o número total de conexões de 2 passos de P_i para os outros vértices. Consequentemente, a soma das entradas na i-ésima linha de $M + M^2$ é o número total de conexões de 1 e de 2 passos de P_i para os outros vértices. Portanto, uma linha de $M + M^2$ com a maior soma de entradas identifica um vértice com a propriedade enunciada no Teorema 1.12.

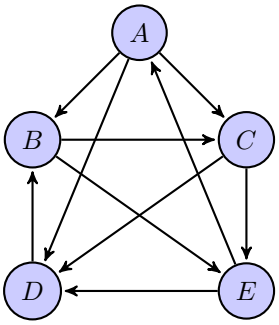
Definição 1.13. *O poder de um vértice num grafo dirigido por dominância é o número total de suas conexões de 1 e de 2 passos para os outros vértices do grafo. Alternativamente, o poder de um vértice P_i é a soma das entradas da i-ésima linha da matriz $A = M + M^2$, onde M é a matriz de vértices do grafo dirigido.*

Exemplo 1.14. *Cinco tenistas jogam entre si uma vez com os seguintes resultados:*

- *A derrota B, C e D.*

- *B derrota C e E.*
- *C derrota D e E.*
- *D derrota B.*
- *E derrota A e D.*

Classifique os cinco tenistas de acordo com o poder dos vértices que lhes correspondem no grafo dirigido por dominância que representa o resultado das partidas.
Resolução. Considere o grafo dirigido cujos vértices correspondem aos tenistas:



Assim representamos a matriz de vértices por M.

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$A = M + M^2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 2 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 \\ 1 & 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 1 & 2 & 0 \end{pmatrix}$$

Somando os elementos das linhas, obtemos:

$$\textit{Linha 1} = 8, \quad \textit{Linha 2} = 5, \quad \textit{Linha 3} = 5, \quad \textit{Linha 4} = 3, \quad \textit{Linha 5} = 6.$$

De acordo com o Teorema 1.12, encontramos a seguinte classificação:

$$A - (\textit{primeiro lugar})$$

$$E - (\textit{segundo lugar})$$

$$B \text{ e } C - (\textit{empatados})$$

$$D - (\textit{último lugar})$$

Fica em primeiro lugar o jogador A, em segundo o E empatados B e C e por último, D. Esta resolução revela um fato interessante: apesar dos tenistas B, C e E terem o mesmo número de vitórias, o que aparentemente poderia indicar um empate entre eles, o tenista E classificou-se em segundo lugar porque ele derrotou o tenista A, o qual corresponde ao vértice de maior poder. Também, em um primeiro momento, poder-se-ia concluir que B supera C na classificação, pois B derrota C. No entanto, há um empate entre eles, pois ambos derrotam E (um vérice com mais poder do que eles), C é derrotado por B, mas B é derrotado por D, que por sua vez foi derrotado por C.

2 Criptografia

Nesta seção discutiremos um método que utiliza operações matriciais combinadas com a aritmética modular para codificar e decodificar mensagens. Veremos como a eliminação gaussiana pode ser usada para quebrar o código de uma mensagem. Para tanto, vamos introduzir os conceitos a serem utilizados.

2.1 Aritmética modular

Definição 1.15. *Sejam a, b e m números inteiros, $m > 0$, dizemos que a é côngruo a b módulo m ($a \equiv b \bmod m$), se m divide $a - b$, ou seja, $a - b$ é múltiplo de m.*

Pelo algoritmo da divisão, dado um inteiro positivo m, qualquer inteiro a é côngruo módulo m a exatamente um dos inteiros $0, 1, 2, \cdots, m-1$. Este inteiro é chamado resíduo de a módulo m.

Isto permite construir uma partição do conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m. Mais precisamente, considere

$$\begin{aligned} [0] &= \{x \in \mathbb{Z}; x \equiv 0 \bmod m\} \\ [1] &= \{x \in \mathbb{Z}; x \equiv 1 \bmod m\} \\ &\vdots \\ [m-1] &= \{x \in \mathbb{Z}; x \equiv m-1 \bmod m\}. \end{aligned}$$

O conjunto $[a] = \{x \in \mathbb{Z}; x \equiv a \bmod m\}$, é chamado de classe residual módulo m do elemento $a \in \mathbb{Z}$. O conjunto de todas as classes residuais módulo m é representada por $\mathbb{Z}_m$. Assim,

$$\mathbb{Z}_m = \{[0], [1], \cdots, [m-1]\}.$$

Observamos que se a é um inteiro não negativo, então seu resíduo módulo m é simplesmente o resto da divisão de a por m. Para um inteiro a arbitrário, o resíduo pode ser encontrado da seguinte forma:

Teorema 1.16. *Dados um número inteiro positivo m e um número inteiro a, seja R o resto da divisão de $|a|$ por m. Então o resíduo r de a é dado por*

$$r = \begin{cases} R, & \text{se } a \geq 0, \\ m - R, & \text{se } a < 0 \text{ e } R \neq 0, \\ 0, & \text{se } a < 0 \text{ e } R = 0. \end{cases}$$

Exemplo 1.17. *Encontre o resíduo módulo 26 de (a) 47, (b) -73.*
Solução (a). A divisão de $|47| = 47$ por 26 dá resto $R = 21$, ou seja, $r = 21$. Assim, $47 \equiv 21$ mod 26.
Solução (b). A divisão de $|-73| = 73$ por 26 dá resto $R = 21$, ou seja, $r = 26 - 21 = 5$. Assim, $-73 \equiv 5$ mod 26.

Em $\mathbb{Z}_m$ definimos as seguintes operações:
Adição: $[a] + [b] = [a + b]$.
Multiplicação: $[a] \cdot [b] = [a \cdot b]$.

Definição 1.18. *Um elemento $[a] \in \mathbb{Z}_m$ é invertível, quando existir $[b] \in \mathbb{Z}_m$ tal que $[a] \cdot [b] = 1$. Neste caso, diremos que $[b]$ é o inverso de $[a]$.*

Exemplo 1.19. *A Tabela 2.1 corresponde a tabela da multiplicação em $\mathbb{Z}_3 = \{[0], [1], [2]\}$.*

$\cdot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Tabela 1.1: Tabela da multiplicação em $\mathbb{Z}_3$.

Exemplo 1.20. *A Tabela 2.2 corresponde a tabela da multiplicação em $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$.*

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Tabela 1.2: Tabela da multiplicação em $\mathbb{Z}_4$.

Observamos que em $\mathbb{Z}_4$ existem dois elementos não nulos cuja multiplicação é nula, a saber, $[2] \neq [0]$, mas $[2] \cdot [2] = [0]$. Note que em $\mathbb{Z}_3$, todo elemento não nulo é invertível. Mas isto não ocorre em todos os $\mathbb{Z}_m$. Por exemplo, em $\mathbb{Z}_4$, vemos que $[2]$ não é invertível. Os elementos invertíveis de $\mathbb{Z}_m$ são caracterizados pela seguinte proposição:

Proposição 1.21. *Um número $[a] \in \mathbb{Z}_m$ é invertível se, e somente se, a e m não têm fatores primos comuns, isto é, $mdc(a, m) = 1$.*

PROVA: Suponha que $[a]$ seja invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a] \cdot [b] = [a \cdot b]$. Logo, $ab \equiv 1 \bmod m$. Consequentemente, $\text{mdc}(a, m) = 1$.

Reciprocamente, se $\text{mdc}(a, m) = 1$, existem naturais b e t tais que $ab - mt = 1$, e assim, [1+mt]=[ab]. Logo,

$$[1] = [1] + [mt] = [1 + mt] = [a \cdot b] = [a] \cdot [b].$$

Portanto, $[a]$ é invertível. ■

Exemplo 1.22. *O número 3 tem um inverso módulo 26, pois $mdc(3, 26) = 1$. Por outro lado, 4 não possui um inverso módulo 26, pois 4 e 26 têm 2 como fator comum.*

Exemplo 1.23. *A tabela abaixo fornece os inversos multiplicativos módulo 26.*

$[a]$	1	3	5	7	9	11	15	17	19	21	23	25
$[a]^{-1}$	1	9	21	15	3	19	7	23	11	5	17	25

Tabela 1.3: *Inversos multiplicativos módulo 26*

Para o que segue, o conceito de matriz invertível módulo m é necessário. Diz-se que uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m, se existir uma matriz B com entradas em $\mathbb{Z}_m$ tal que

$$AB = BA = I,$$

onde I é a matriz identidade. É possível mostrar que a matriz B com essa propriedade é única. Chamamos tal matriz B a inversa de A e denotamos por A^{-1}.

Teorema 1.24. *Uma matriz 2×2 A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, o resíduo de $det(A)$ módulo m tem um inverso multiplicativo módulo m.*

PROVA: Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_m)$ e $det(A) = D = ad - bc \in \mathbb{Z}_m$. Suponhamos que a matriz A possua uma inversa multiplicativa módulo m, isto é, existe uma quadrada A^{-1}, com entrada em A, tal que,

$$AA^{-1} = A^{-1}A = I.$$

Tomando determinantes, obtemos que,

$$det(A)det(A^{-1}) = det(AA^{-1}) = det(I) = 1 \bmod m.$$

Consequentemente $det(A^{-1})$ é o inverso multiplicativo módulo m de $det(A)$.

Reciprocamente, suponhamos que $\text{mdc}(m, D) = 1$. Então, existe $D^{-1} \in \mathbb{Z}_m$, tal que, $DD^{-1} = 1 \bmod m$. É fácil verificar que

$$A^{-1} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix},$$

é a matriz inversa de A. ■

Combinando o Teorema 1.24 com a Proposição 1.21, obtemos o seguinte corolário:

Corolário 1.25. *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, m e o resíduo de $det(A)$ módulo m não tem fatores primos comuns.*

Exemplo 1.26. *Uma matriz quadrada A com entradas em $\mathbb{Z}_{26}$ é invertível módulo 26 se, e somente se, o resíduo de $det(A)$ módulo 26 não é divisível por 2 e 13.*

Exemplo 1.27. *Encontre a inversa de*

$$A = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

Solução: $D = det(A) = 1$. Pelo Exemplo 1.23, $D^{-1} = 1$ mod 26. Assim,

$$A^{-1} = 1 \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix} mod\ 26.$$

2.2 Codificação

O estudo da codificação de mensagens secretas é denominado criptografia. Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não-codificadas são textos comuns e as mensagens são textos cifrados ou criptogramas. O processo de converter um texto comum em cifrado é chamado cifrar ou criptografar, e o processo inverso de converter um texto cifrado em comum é chamado decifrar.

Iremos trabalhar com o sistema poligráfico, que consiste em dividir um texto comum em conjuntos de n letras, e substituí-lo por um conjunto de n letras cifradas. Utilizaremos uma classe de sistemas poligráficos chamados **cifras de Hill**.[1]

No que segue, vamos supor que cada letra de texto comum e de texto cifrado, excetuando o Z, tem um valor numérico que corresponde a sua posição no alfabeto. Damos a Z o valor 0.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

Para cifrar um texto comum usamos o seguinte procedimento:

[1] Lester S. Hill (1891-1961), matemático norte-americano. Estudou no Columbia College (1911) e na Yale University (1926). Lecionou na University of Montana, Princeton University, the University of Maine, Yale University e na Hunter College. Uma das suas notáveis contribuições foi a cifra de Hill. Desenvolveu métodos para detectar erros em códigos numéricos telegráficos.

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Tabela 1.4: Valor numérico de cada letra

1. Escolha uma matriz A, quadrada de ordem 2, com entradas inteiras para efetuar a codificação.

2. Agrupe letras sucessivas do texto comum em pares, adicionando uma letra fictícia para completar o último par se o texto comum possuir um número ímpar de letras, substitua cada letra do texto comum por seu valor numérico, representado na tabela acima.

3. Converta cada par sucessivo p_1p_2 de letras do texto comum em um vetor-coluna $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ e forme o produto Ap. O vetor p será chamado vetor comum e Ap o correspondente vetor cifrado.

4. Converta cada vetor cifrado em seu equivalente alfabético.

Sempre que ocorrer um inteiro maior que 25, ele será substituído pelo resto da divisão deste inteiro por 26. Como o texto comum foi agrupado em pares e criptografado por uma matriz 2×2, dizemos que a cifra de Hill é uma 2-cifra de Hill. É claro que é possível agrupar o texto comum em ternos e criptografar com uma matriz 3×3. Em geral, para uma n-cifra de Hill agrupamos em conjuntos de n letras e codificamos com uma matriz codificadora $n \times n$ de entradas inteiras.

Exemplo 1.28. *Obtenha a cifra de Hill da mensagem "TUDO É POSSÍVEL AO QUE CRÊ", para a matriz codificadora* $\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$.

Solução: Dividindo em blocos de 2, e substituindo seu valor de acordo com a Tabela 1.4, obtemos

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 20 \\ 21 \end{bmatrix} = \begin{bmatrix} 5 \\ 9 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 4 \\ 15 \end{bmatrix} = \begin{bmatrix} 23 \\ 23 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 5 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 15 \\ 19 \end{bmatrix} = \begin{bmatrix} 20 \\ 23 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 19 \\ 9 \end{bmatrix} = \begin{bmatrix} 20 \\ 21 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 22 \\ 5 \end{bmatrix} = \begin{bmatrix} 11 \\ 23 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 12 \\ 1 \end{bmatrix} = \begin{bmatrix} 15 \\ 25 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 15 \\ 17 \end{bmatrix} = \begin{bmatrix} 14 \\ 21 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 21 \\ 5 \end{bmatrix} = \begin{bmatrix} 10 \\ 21 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 3 \\ 18 \end{bmatrix} = \begin{bmatrix} 5 \\ 24 \end{bmatrix} mod 26$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} . \begin{bmatrix} 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 8 \\ 11 \end{bmatrix} mod 26$$

Assim obtemos a cifra de Hill:

$$EIWWAZTWTUKWOYNUJUEXHK$$

Exemplo 1.29. *Decifre a seguinte cifra de Hill que foi criptografada pela matriz do Exemplo 1.27:*

$$NMITRMITRCPEQEOA$$

Solução: para decifrar as cifras de Hill, usamos a inversa mod 26 da matriz codificadora A. Se

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

é um vetor comum, então $c = Ap$ é o correspondente vetor cifrado e $p = A^{-1}c$. Pela Tabela 1.4, o equivalente do texto cifrado é

$$14\,13\,9\,20\,18\,13\,9\,20\,18\,3\,16\,5\,17\,5\,15\,1$$

Para obter os pares de texto comum, façamos os produtos $p = A^{-1}c$ usando a matriz inversa obtida no Exemplo 1.27.

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 14 \\ 13 \end{bmatrix} = \begin{bmatrix} 313 \\ 13 \end{bmatrix} = \begin{bmatrix} 1 \\ 13 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 9 \\ 20 \end{bmatrix} = \begin{bmatrix} 469 \\ 20 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 18 \\ 13 \end{bmatrix} = \begin{bmatrix} 317 \\ 13 \end{bmatrix} = \begin{bmatrix} 5 \\ 13 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 9 \\ 20 \end{bmatrix} = \begin{bmatrix} 469 \\ 20 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 18 \\ 3 \end{bmatrix} = \begin{bmatrix} 87 \\ 3 \end{bmatrix} = \begin{bmatrix} 9 \\ 3 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 16 \\ 5 \end{bmatrix} = \begin{bmatrix} 131 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 17 \\ 5 \end{bmatrix} = \begin{bmatrix} 132 \\ 5 \end{bmatrix} = \begin{bmatrix} 2 \\ 5 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 1 \end{bmatrix} = \begin{bmatrix} 38 \\ 1 \end{bmatrix} = \begin{bmatrix} 12 \\ 1 \end{bmatrix} \ mod\ 26$$

Pela Tabela 1.4, os equivalentes alfabéticos destes vetores são

AM AT EM AT IC AE BE LA

fornencendo a mensagem A MATEMÁTICA É BELA.

2.3 Quebrando uma cifra de Hill

Veremos agora como utilizar a eliminação gaussiana na aritmética modular para decifrar cifras de Hill ao determinar a matriz codificadora. Vamos inicialmente relembrar a eliminação gaussiana usual.

Na próxima definição, uma linha ou coluna não nula em uma matriz significa uma linha ou coluna que contém ao menos uma entrada não nula; o pivô de uma linha corresponde à entrada não nula mais à esquerda em um linha não nula.

Dizemos que uma matriz está na forma escalonada por linhas, quando possui as seguintes propriedades:

1. Todas as linhas não nulas estão acima de qualquer linha constituída só de zeros.
2. Cada pivô de uma linha está em uma coluna à direita do pivô da linha acima dele.
3. Todas as entradas em uma coluna abaixo de um pivô são nulas.

Um matriz está na forma escalonada reduzida por linhas se, além disso, satisfizer

4. O pivô em cada linha não nula é 1.

4. Cada pivô 1 é o único elemento não nulo em sua coluna.

Desse modo, as matrizes escalonadas por linhas possuem uma forma "escada" como indicado a seguir (os símbolos $\bullet$ indicam qualquer número diferente de zero e os asteriscos indicam números arbitrários, incluindo o zero):

$$\begin{bmatrix} 0 & \bullet & * & * & * & * & * \\ 0 & 0 & 0 & \bullet & * & * & * \\ 0 & 0 & 0 & 0 & \bullet & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

O procedimento pelo qual qualquer matriz pode ser levada à forma escalonada, e escalonada reduzida, utiliza as seguintes operações elementares com as linhas da matriz:

I. Trocar a ordem das linhas. $(L_i \leftrightarrow L_j)$

II. Multiplicar uma linha por um número diferente de zero. $(L_i \to kL_i)$

III. Somar um múltiplo de uma linha com uma outra linha. $(L_i \to L_i + kL_j)$

Qualquer matriz pode ser levada à forma escalonada reduzida seguindo os seguintes passos:

1. Se a matriz consiste inteiramente de zeros, não há nada para fazer; ela já está na forma escalonada.

2. Caso contrário, encontre a primeira coluna, vindo da esquerda, que contém um elemento k não nulo, e mova a linha contendo esse elemento ao topo da matriz.

3. Multiple a linha topo por $1/k$ para obter o primeiro pivô.

4. Anule cada elemento abaixo e acima do pivô, subtraindo múltiplos de suas linhas das linhas inferiores e superiores respectivamente.

Isso completa a primeira linha; todas as demais operações por linhas são efetuadas nas demais linhas.

5. Repita os passos 1–4 na matriz formada pelas linhas remanescentes.

Exemplo 1.30. *A primeira matriz abaixo está na forma escalonada, e a segunda, na forma escalonada reduzida, para qual pode ser transformada por meio de operações com as linhas:*

$$\begin{bmatrix} 1 & * & * & * & * \\ 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & * & 0 & * & 0 \\ 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

O procedimento descrito acima quando aplicado à matriz aumentada de um sistema linear é conhecido como método de Gauss ou eliminação gaussiana. Vejamos um exemplo:

Exemplo 1.31. *Resolva o sistema pelo método de Gauss.*

$$\begin{cases} x+y+2z &= 9 \\ 2x+4y-3z &= 1 \\ 3x+6y-5z &= 0 \end{cases}$$

Solução. Associando ao sistema acima a matriz aumentada A, temos

$$A = \left(\begin{array}{ccc|c} 1 & 1 & 2 & 9 \\ 2 & 4 & -3 & 1 \\ 3 & 6 & -5 & 0 \end{array}\right).$$

Somando (-2) vezes à primeira linha à segunda e (-3) vezes a primeira linha a terceira, temos

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 9 \\ 0 & 2 & -7 & -17 \\ 0 & 3 & -11 & -27 \end{array}\right).$$

Somando a segunda linha a (-2) vezes à primeira, e (-3) vezes a segunda linha a 2 vezes a terceira linha, dá

$$\left(\begin{array}{ccc|c} -2 & 0 & -11 & -35 \\ 0 & 2 & -7 & -17 \\ 0 & 0 & -1 & -3 \end{array}\right).$$

Somando (-11) vezes a terceira linha a primeira e (-7) vezes a terceira linha a segunda dá,

$$\left(\begin{array}{ccc|c} -2 & 0 & 0 & -2 \\ 0 & 2 & 0 & 4 \\ 0 & 0 & -1 & -3 \end{array}\right).$$

Multiplicando a primeira linha por $(-\frac{1}{2})$, e a segunda por $\frac{1}{2}$ e a terceira por (-1), e assim obtemos,

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right).$$

Associada a esta matriz na forma reduzida, temos o seguinte sistema equivalente ao sistema original:

$$\begin{cases} x & & & = & 1, \\ & y & & = & 2, \\ & & z & = & 3. \end{cases}$$

Daí, encontramos $x = 1, y = 2$ e $z = 3$.

Exemplo 1.32. *Encontre a inversa da matriz* $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{pmatrix}$.

Queremos reduzir A à matriz identidade por operações sobre linhas e simultaneamente aplicar estas operações a I para produzir A^{-1}. *Para conseguir isto, vamos adjuntar a matriz identidade à direta de A, produzindo uma matriz da forma* $[A\,|\,I]$. *Em seguida, faremos operações com as linhas desta matriz até que o lado esquerdo esteja reduzido a I. Estas operações vão converter o lado direito a* A^{-1}, *de modo que a matriz final terá a forma*

$$[I|A^{-1}] = \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 5 & 3 & 0 & 1 & 0 \\ 1 & 0 & 8 & 0 & 0 & 1 \end{array}\right].$$

Somamos (-2) vezes a primeira linha à segunda e (-1) vez a primeira à terceira

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & -2 & 5 & -1 & 0 & 1 \end{array}\right].$$

Somamos 2 vezes a segunda linha à terceira

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & 0 & -1 & -5 & 2 & 1 \end{array}\right].$$

Multiplicamos a terceira linha por (-1)

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & 0 & 1 & 5 & -2 & -1 \end{array}\right].$$

Somamos 3 vezes a terceira linha à segunda e (-3) vezes a terceira à primeira

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 0 & -14 & 6 & 3 \\ 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 1 & 5 & -2 & -1 \end{array}\right].$$

Somamos (-2) vezes a segunda linha à primeira

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -40 & 16 & 9 \\ 0 & 1 & 0 & 13 & -5 & -3 \\ 0 & 0 & 1 & 5 & -2 & -1 \end{array}\right].$$

E assim obtemos a inversa,

$$A^{-1} = \left[\begin{array}{ccc} -40 & 16 & 9 \\ 13 & -5 & -3 \\ 5 & -2 & -1 \end{array}\right].$$

Os dois exemplos anteriores mostram a importância das operações elementares com as linhas. Acontece que essas operações podem ser realizadas por meio de multiplicações à esquerda por certas matrizes invertíveis.

Definição 1.33. *Uma matriz quadrada E é denominada matriz elementar quando é obtida a partir da matriz identidade mediante uma única operação elementar com linhas. Dizemos que E é do tipo I, II ou III quando a operação elementar com linhas correspondente é do tipo I, II ou III.*

Exemplo 1.34. $E_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, $E_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ *e* $E_3 = \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ *são matrizes elementares do tipo I, II e III respectivamente.*

Observamos que toda matriz elementar E é invertível e sua inversa E^{-1} é a matriz elementar do mesmo tipo obtida da identidade pela operação elementar inversa à que produziu E da identidade.

Exemplo 1.35. *Considere as matrizes elementares*

$$E_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 5 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}.$$

Se uma matriz $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$ *for multiplicada à esquerda por essas matrizes elementares, os resultados serão:*

$$E_1A = \begin{bmatrix} a_{21} & a_{22} & a_{23} \\ a_{11} & a_{12} & a_{13} \end{bmatrix} \quad (L_1 \leftrightarrow L_2)$$

$$E_2A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 5a_{21} & 5a_{22} & 5a_{23} \end{bmatrix} \quad (L_2 \to 5L_2)$$

$$E_3A = \begin{bmatrix} a_{11} + 3a_{12} & a_{12} + 3a_{22} & a_{13} + 3a_{23} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \quad (L_1 \to L_1 + 3L_2)$$

Observe que, em cada caso, E_iA é a matriz obtida de A pela operação que criou E_i a partir da matriz identidade.

O fato observado no exemplo anterior ocorre sempre e exprime o relacionamento entre matrizes elementares e operações com linhas. Isso nos leva a rever o método de eliminação gaussiana para o cálculo de inversas. Como em tal método, suponha que uma série de k operações elementares com as linhas seja aplicada a uma matriz A invertível, e que E_i seja a matriz elementar correspondente à i-ésima operação elementar com as linhas. Portanto, o

passo i da redução por linhas é dado por multiplicação à esquerda por E_i, de modo que a redução se torna

$$A \to E_1A \to E_2E_1A \to \cdots \to E_k \cdots E_2E_1A,$$

ou seja,

$$A \to UA, \quad \text{onde } U = E_k \cdots E_2E_1.$$

Como A é invertível, não é difícil verificar que a matriz reduzida $UA = I$, a matriz identidade, e então $U = A^{-1}$. Assim a redução se torna

$$\left[\begin{array}{c|c} A & B \end{array}\right] \to \left[\begin{array}{c|c} I & A^{-1} \end{array}\right].$$

Este é o algoritmo de inversão de matrizes que foi utilizado no Exemplo 1.32.

Agora estamos prontos para apresentar a técnica para quebrar cifras de Hill codificadas por matrizes invertíveis. Suponhamos que tenhamos algum texto comum e o cifrado correspondente de uma mensagem. O objetivo é determinar a matriz decodificadora da cifra de Hill e consequentemente obter o resto do texto comum da mensagem. O princípio básico da Álgebra Linear que será utilizado é o fato que uma transformação linear fica completamente determinada por seus valores em uma base.

Teorema 1.36. *Sejam $p_1, p_2, ..., p_n$, vetores comuns linearmente independentes e sejam $c_1, c_2, ..., c_n$ os correspondentes vetores cifrados de uma n-cifra de Hill com uma matriz codificadora $n \times n$ invertível A. Se,*

$$P = \begin{bmatrix} p_1^T \\ p_2^T \\ \vdots \\ p_n^T \end{bmatrix}$$

é uma matriz $n \times n$ de vetores-linha $p_1^T, p_2^T, ..., p_n^T$ e se

$$C = \begin{bmatrix} c_1^T \\ c_2^T \\ \vdots \\ c_n^T \end{bmatrix}$$

é a matriz $n \times n$ de vetores-linhas, $c_1^T, c_2^T, ..., c_n^T$, então a sequência de operações elementares sobre linha que reduz C a I, transforma P em $(A^{-1})^T$.

PROVA: Pela definição de P e C, podemos escrever $C = PA^T$. Usando que A invertível e que $p_1, p_2, ..., p_n$ são vetores linearmente independentes, resulta que C é uma matriz invertível. Sejam $E_1, \cdots, E_k$ as matrizes elementares que correspondem às operações elementares com as linhas que reduzem C a I, ou seja, $E_k \cdots E_1C = I$. Substituindo $C = PA^T$, encontramos

$$E_k \cdots E_1PA^T = I,$$

de onde segue que $E_k \cdots E_1 P = (A^{-1})^T$, ou seja, a mesma sequência de operações com as linhas que reduz C a I converte P a $(A^{-1})^T$. ■

Este teorema nos diz que para encontrar a transposta da matriz decodificadora A^{-1} devemos encontrar uma sequência de operações elementares sobre linhas que reduz C a I e então aplicar estas mesmas operações sobre linhas de P.

Exemplo 1.37. *(Quebrando uma cifra de Hill) Foi interceptada a 2-cifra de Hill*

$$IOSBTGXESPXHOPDE$$

Decifre esta mensagem, sabendo que ela principia com a palavra DEAR.
Solução. Pela Tabela 1.4, o equivalente numérico do texto comum conhecido é

D	E	A	R
4	*5*	*1*	*18*

e o correspondente numérico do texto cifrado correspondente é

I	O	S	B
9	*15*	*19*	*2*

de modo que os vetores comuns e correspondentes vetores cifrados são

$$p_1 = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \leftrightarrow c_1 = \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \leftrightarrow c_2 = \begin{bmatrix} 19 \\ 2 \end{bmatrix}.$$

Queremos reduzir $C = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}$ *a* I *por operações elementares sobre linhas e simultaneamente aplicar estas operações a* $P = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix}$ *para obter* $(A^{-1})^T$*, a transposta da matriz decodificadora.*

$$\left[\begin{array}{cc|cc} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{array}\right].$$

Multiplicamos a primeira linha por $9^{-1} = 3$ *mod 26,*

$$\left[\begin{array}{cc|cc} 1 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right].$$

Substituímos 45 *pelo seu resíduo módulo* 26*,*

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right].$$

Somamos -19 *vezes a primeira linha à segunda,*

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{array}\right].$$

Substituímos as entradas da segunda linha pelos seus resíduos módulo 26*,*

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 5 & 7 & 19 \end{array}\right].$$

Multiplicamos a segunda linha por $5^{-1} = 21$*,*

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{array}\right].$$

Somamos -19 *vezes a segunda linha à primeira,*

$$\left[\begin{array}{cc|cc} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{array}\right].$$

Substituímos as entradas da primeira linha pelos seus resíduos módulo 26,

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{array}\right].$$

Assim obtemos, $(A^{-1})^T = \begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix}$*, e portanto a matriz decodificadora é* $A^{-1} = \begin{bmatrix} 1 & 17 \\ 0 & 19 \end{bmatrix}$*.*
Substituindo os equivalentes numéricos de cada letra, temos:

I	*O*	*S*	*B*	*T*	*G*	*X*	*E*	*S*	*P*	*X*	*H*	*O*	*P*	*D*	*E*
9	*15*	*19*	*2*	*20*	*7*	*24*	*5*	*19*	*16*	*24*	*8*	*15*	*16*	*4*	*5*

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 9 \\ 15 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 20 \\ 7 \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 24 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 4 \\ 20 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} . \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 11 \\ 19 \end{bmatrix} \ mod\ 26$$

Assim obtemos o texto:

DEAR IKE SEND TANKS

3 Cadeias de Markov

Suponha que um sistema físico ou matemático esteja sofrendo mudanças tais que a cada momento ele possa ocupar um dentre um número finito de estados, e que a probabilidade de um certo estado ocorrer puder ser predita unicamente a partir do conhecimento do estado do sistema na observação imediatamente anterior, então o processo de mudança de um estado para outro é chamado de uma cadeia ou um processo de Markov[2]

Definição 1.38. *Denotemos por $\{1, 2, ..., k\}$ estados possíveis de uma cadeia de Markov. A probabilidade do sistema estar no estado i em qualquer observação, se na observação imediatamente precedente estava no estado j, é denotado por p_{ij}, e é chamada a probabilidade de transição do estado j ao estado i. A matriz $P = [p_{ij}]$ é chamada de a matriz de transição da cadeia de Markov.*

Por exemplo, em uma cadeia de Markov de três estados, a matriz de transição tem o seguinte formato:

$$\begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix}$$

Nesta matriz, p_{23} é a probabilidade que o sistema vai mudar do estado 3 ao estado 2, p_{12} é a probabilidade que o sistema vai mudar do estado 2 ao estado 1, e assim por diante.

[2]Andrey Andreyevich Markov, Ryazan 1856 - São Petersburgo 1922, matemático russo. Foi quem ajudou a desenvolver a teoria dos processos estocásticos, especialmente aqueles chamados de cadeias de Markov. Com base no estudo de eventos mutualmente independentes, os seus trabalhos tem sido desenvolvidos e amplamente aplicados na biologia e ciências socias. Markov formou-se na Universidade Estatal de São Petersburgo em 1878, onde foi professor em 1886. Seus primeiros trabalhos foram sobre limite de integrais e teoria da aproximação. Depois de 1900 aplicou métodos de frações contínuas, que havia sido iniciada por Pafnuti Tchebychev na teoria da probabilidade. Provou o teorema do limite central. Markov é lembrado pelo seu estudo de cadeias de Markov.

Exemplo 1.39. *Uma locadora de automóveis tem três lojas de atendimento denotadas por 1, 2 e 3. Um cliente pode alugar um carro de qualquer uma das lojas e devolver o mesmo para qualquer uma das três lojas. O gerente nota que os clientes costumam devolver os carros de acordo com as seguintes probabilidades:*

Alugado da loja

1	*2*	*3*	
0,8	*0,3*	*0,2*	*1*
0,1	*0,2*	*0,6*	*2*
0,1	*0,5*	*0,2*	*3*

Devolvido à loja

A matriz

$$\begin{pmatrix} 0,8 & 0,3 & 0,2 \\ 0,1 & 0,2 & 0,6 \\ 0,1 & 0,5 & 0,2 \end{pmatrix}$$

é a matriz de transição do sistema. A partir desta matriz, a probabilidade de um carro alugado na loja 3 ser devolvido na loja 2 é 0,6, a probabilidade de um carro alugado na loja 1 ser devolvido na loja 1 é 0,8, e assim por diante.

As matrizes de transição das cadeias de Markov têm a propriedade que as entradas em qualquer coluna somam 1. E são chamadas de matrizes estocásticas, matrizes de probabilidade ou apenas matrizes de Markov.

Em geral, o estado de um sistema em uma cadeia de Markov não pode ser determinado com certeza numa observação arbitrária. O melhor que pode ser feito é especificar probabilidades para cada um dos estados possíveis. E isso pode ser representado por um vetor-coluna

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},$$

sendo x_1 é a probabilidade que o sistema está no estado 1, x_2 é a probabilidade que ele está no estado 2 e x_3 é a probabilidade que ele está no estado 3.

Definição 1.40. *O vetor-estado de uma observação de uma cadeia de Markov com k estados é um vetor-coluna x cujo i-ésimo componente x_i é a probabilidade do sistema estar naquela observação no i-ésimo estado.*

As entradas em qualquer vetor-estado de uma cadeia de Markov são não-negativas e têm soma 1. E um vetor-coluna que possui essa propriedade é chamado vetor probabilidade.

Teorema 1.41. *Se P é a matriz de transição de uma cadeia de Markov e x_n é o vetor estado na n-ésima observação, então $x_{n+1} = Px_n = P^{n+1}x_0$.*

PROVA: Considere o vetor de estado inicial

$$x_0 = \begin{bmatrix} x_{01} \\ x_{02} \\ \vdots \\ x_{0k} \end{bmatrix}$$

o qual caracteriza a distribuição inicial entre os k estados possíveis, onde x_{0i} é a probabilidade que o sistema esteja no estado i, para $i \in \{1, \cdots, k\}$. Lembrando que p_{ij} é a probabilidade de transição do estado j ao estado i, após uma unidade de tempo a distribuição estará dividida entre os k estados da seguinte forma

$$x_1 = \begin{bmatrix} p_{11}x_{01} + p_{12}x_{02} + \cdots + p_{1k}x_{0k} \\ \vdots \\ p_{k1}x_{01} + p_{k2}x_{02} + \cdots + p_{kk}x_{0k} \end{bmatrix}.$$

Assim, a matriz de estado após uma unidade de tempo é dada pelo produto de matrizes $x_1 = Px_0$.

Como estamos assumindo que em cada unidade de tempo a matriz de transição é a mesma, então após $n+1$ unidades de tempo a distribuição estará dividida entre os k estados segundo a matriz de estado

$$x_{n+1} = Px_n = P^2x_{n-1} = \cdots = P^{n+1}x_0.$$

■

Suponha, dado o vetor-estado x_0 de uma cadeia de Markov em alguma observação inicial. Com o uso do Teorema 1.41, podemos determinar os vetores-estados $x_1, x_2, ..., x_n, ...$ nas observações subsequentes.

Exemplo 1.42. *No Exemplo 1.39, a matriz de transição é*

$$\begin{bmatrix} 0,8 & 0,3 & 0,2 \\ 0,1 & 0,2 & 0,6 \\ 0,1 & 0,5 & 0,2 \end{bmatrix}$$

Se um carro inicialmente é alugado da loja 2, então o vetor estado inicial é $x_0 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$.

Usando este vetor e o Teorema 1.41, obtemos os vetores-estado posteriores $x_n = \begin{bmatrix} x_{n1} \\ x_{n2} \\ x_{n3} \end{bmatrix}$ *listados na tabela a seguir. Os vetores-estado para* $n \geq 11$ *são iguais a* x_{11} *até três casas decimais.*

n	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
x_{n1}	*0*	*0,3*	*0,4*	*0,477*	*0,511*	*0,533*	*0,544*	*0,55*	*0,553*	*0,555*	*0,556*	*0,557*
x_{n2}	*1*	*0,2*	*0,37*	*0,252*	*0,261*	*0,240*	*0,238*	*0,233*	*0,232*	*0,231*	*0,23*	*0,23*
x_{n3}	*0*	*0,5*	*0,23*	*0,271*	*0,228*	*0,227*	*0,219*	*0,217*	*0,215*	*0,214*	*0,214*	*0,213*

Este exemplo revela dois fatos que devem ser observados: 1.) não foi necessário saber por quanto tempo o cliente permaneceu com o carro. Ou seja, em um processo de Markov o tempo entre as observações não precisa ser regular; 2.) os vetores-estado convergem para um vetor fixo à medida que n cresce.

Uma pergunta natural é se os vetores-estado de um sistema de Markov sempre convergem para um vetor fixo. O próximo exemplo mostra que isto não é o caso.

Exemplo 1.43. *Seja*

$$P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad e \quad x_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Como $P^2 = I$ *e* $P^3 = P$, *resulta*

$$x_0 = x_2 = x_4 = \cdots = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad e \quad x_1 = x_3 = x_5 = \cdots = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Este sistema oscila indefinidamente entre dois vetores-estado, e portanto não converge a nenhum vetor fixo.

Entretanto, impondo uma restrição fraca à matriz de transição, mostraremos que o sistema se aproxima de um vetor-estado fixo. Tal condição é dada na próxima definição.

Definição 1.44. *Uma matriz de transição* P *é regular se existe* $N \in \mathbb{N}$ *tal que* P^N *tem todas as entradas positivas. Uma cadeia de Markov que é governada por uma matriz de transição regular é chamada cadeia de Markov regular.*

Lema 1.45 ([3])**.** *Sejam* P *uma matriz* $r \times r$ *de transição regular,* ε *a menor entrada de* P *e* x *um vetor-coluna com* r *componentes. Denote por* M_0 *e* m_0 *as respectivas componentes máxima e mínima de* x. *Denote também por* M_1 *e* m_1 *as respectivas componentes máxima e mínima do vetor* $x^T P$. *Então*

$$M_1 \leq M_0, \quad m_1 \geq m_0 \quad e \quad M_1 - m_1 \leq (1 - 2\varepsilon)(M_0 - m_0).$$

Prova: Seja x' o vetor obtido de x substituindo todas as componentes, exceto a componente m_0, por M_0. Então as respectivas coordenadas desses vetores satisfazem $x_i \leq x'_i$, para $i = 1, \cdots, r$. Usando que P é uma matriz de transição, cada componente de $x'^T P$ é da forma

$$am_0 + (1 - a)M_0 = M_0 - a(M_0 - m_0),$$

onde $a \geq \varepsilon$. Portanto, cada componente de $x'^T P$ é menor ou igual a $M_0 - \varepsilon(M_0 - m_0)$. Mas, $x_i \leq x'_i$ para $i = 1, \cdots, r$. Logo,

$$M_1 \leq M_0 - \varepsilon(M_0 - m_0). \tag{1.2}$$

Se aplicarmos este resultado ao vetor $-x$, obtemos

$$-m_1 \leq m_0 - \varepsilon(-m_0 + M_0). \tag{1.3}$$

Somando (1.2) e (1.3), temos

$$M_1 - m_1 \leq M_0 - m_0 - 2\varepsilon(M_0 - m_0) = (1 - 2\varepsilon)(M_0 - m_0).$$

■

Teorema 1.46 ([3]). *Se P é uma matriz $r \times r$ de transição regular, então*

$$P^n \to Q = \begin{bmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \vdots & \vdots \\ q_k & q_k & \cdots & q_k \end{bmatrix}$$

quando $n \to +\infty$, onde os q_i são números positivos tais que $q_1 + q_2 + \ldots + q_k = 1$.

PROVA: Suponha que P não tenha entradas nulas. Seja ε a menor entrada de P. Seja ρ_j um vetor-coluna com 1 na posição j e 0 nas demais entradas. Sejam M_n e m_n as respectivas máxima e mínima do vetor $\rho_j^T P^n$. Como

$$\rho_j^T P^n = \rho_j^T P^{n-1} P,$$

segue do Lema 1.45 que

$$\begin{cases} M_1 \geq M_2 \geq M_3 \geq \cdots \\ m_1 \leq m_2 \leq m_3 \leq \cdots \\ M_n - m_n \leq (1 - 2\varepsilon)(M_{n-1} - m_{n-1}), \quad \text{para } n \geq 1. \end{cases}$$

Como consequência, M_n e m_n são sequências monótonas limitadas, e portanto convergentes. Seja $d_n = M_n - m_n$. Então

$$d_n \leq (1 - 2\varepsilon)^n d_0 = (1 - 2\varepsilon)^n.$$

Portanto,

$$\lim_{n \to +\infty} d_n = 0$$

e as sequências M_n e m_n convergem para um valor comum. Consequentemente, $\rho_j^T P^n$ tende para um vetor com todas as componentes iguais. Seja q_j esse valor comum. Agora, $\rho_j^T P^n$ é a j-ésima linha de P^n. Assim, a j-ésima linha de P^n tende a um vetor com todas as

componentes iguais a q_j, isto é, P^n tende para uma matriz Q com todas as colunas o mesmo vetor

$$q = \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_r \end{bmatrix}$$

Sendo P uma matriz de transição, qualquer potência P^n também é uma matriz de transição. Desse modo, a soma das entradas de cada coluna de P^n é sempre igual a 1 e o mesmo é verdadeiro para a matriz Q. Isto conclui a demonstração para o caso que P tem todas as entradas positivas.

Considere agora o caso que P é somente regular. Seja N um número natural tal que P^N possui todas as entradas positivas. Seja ε' a menor entrada de P^N. Pela primeira parte da prova,

$$d_{kN} \leq (1 - 2\varepsilon')^k, \quad \text{para } k \geq 1.$$

Portanto, a sequência não-crescente (d_n) possui uma subsequência convergindo para 0. Assim, $d_n \to 0$ quando $n \to +\infty$ e o restante da demonstração é análoga ao caso anterior. ■

Veremos pelo teorema a seguir que qualquer cadeia de Markov regular possui um vetor-estado fixo q, tal que, para qualquer escolha x_0, o vetor $P^n x_0$ converge a q quando $n \to \infty$.

Teorema 1.47. *Se P é uma matriz de transição regular e x é um vetor de probabilidade qualquer, então*

$$P^n x \to \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_k \end{bmatrix} = q$$

quando $n \to +\infty$, onde q é um vetor de probabilidade fixo, independente de n, cujas entradas são todas positivas.

Prova: Pelo Teorema 1.46, $P^n \to Q$ quando $n \to +\infty$. De modo que $P^n x \to Qx = q$ quando $n \to +\infty$. ■

O Teorema anterior estabelece que para uma cadeia de Markov regular, o sistema sempre acaba convergindo para um vetor-estado q fixo. O vetor q é chamado vetor de **estado estacionário** da cadeia de Markov regular. O Teorema a seguir mostra uma maneira de calcular o vetor estacionário.

Teorema 1.48. *O vetor de estado estacionário q de uma matriz de transição regular P é o único vetor de probabilidade que satisfaz a equação $Pq = q$.*

Prova: Considere a identidade matricial $PP^n = P^{n+1}$. Pelo Teorema 1.46, ambas P^n e P^{n+1} convergem para Q quando $n \to +\infty$. Assim, temos que $PQ = Q$. Qualquer uma das colunas desta equação matricial dá $Pq = q$. Para mostrar que q é o único vetor de probabilidade

que satisfaz esta equação, suponha que r é um outro vetor de probabilidade tal que, $Pr = r$. Então também $P^n r = r$ para $n = 1, 2, 3, ...$ Pelo Teorema 1.47, quando $n \to \infty$, resulta $q = r$. ■

O Teorema 1.48, pode ser escrito do seguinte modo: o sistema linear homogêneo

$$(I - P)p = 0$$

tem sempre um único vetor solução q com entradas não negativas satisfazendo $q_1 + \cdots + q_k = 1$.

Exemplo 1.49. *Considere a matriz de transição* $\begin{bmatrix} 0,2 & 0,1 & 0,7 \\ 0,6 & 0,4 & 0,2 \\ 0,2 & 0,5 & 0,1 \end{bmatrix}$. *Encontre seu vetor de estado estacionário.*

Solução. Seja I_3 a matriz identidade e $q = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, tal que, $(I - P)q = 0$.

$$\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0,2 & 0,1 & 0,7 \\ 0,6 & 0,4 & 0,2 \\ 0,2 & 0,5 & 0,1 \end{bmatrix} \right) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 0,8 & -0,1 & -0,7 \\ -0,6 & 0,6 & -0,2 \\ -0,2 & -0,5 & 0,9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

A forma escalonada reduzida por linhas da matriz de coeficientes é:

$$\begin{bmatrix} 1 & 0 & -\frac{22}{21} \\ 0 & 1 & -\frac{29}{21} \\ 0 & 0 & 0 \end{bmatrix}$$

de modo que o sistema linear original é equivalente ao sistema: $x_1 = \frac{22}{21}x_3$ e $x_2 = \frac{29}{21}x_3$. Pondo $x_3 = s$, qualquer solução do sistema linear é da forma,

$$q = s \begin{bmatrix} \frac{22}{21} \\ \frac{29}{21} \\ 1 \end{bmatrix}$$

Mas como $x_1 + x_2 + x_3 = 1$, temos : $x_1 = \frac{11}{36}$, $x_2 = \frac{29}{72}$ e $x_3 = \frac{21}{72}$. Assim, o vetor de estado estacionário deste sitema é:

$$q = \begin{bmatrix} \frac{11}{36} \\ \frac{29}{72} \\ \frac{21}{72} \end{bmatrix}.$$

Exemplo 1.50. *Um país é dividido em três regiões demográficas. Observa-se que, a cada ano,* 5% *dos moradores da região* 1 *mudam para a região* 2 *e* 5% *mudam para a região* 3*. Dos moradores da região* 2*,* 15% *mudam para a região* 1 *e* 10% *mudam para a região* 3*. Finalmente, dos moradores da região* 3*,* 10% *mudam para a região* 1 *e* 5% *mudam para a região* 2*. A longo prazo, qual porcentagem da população mora em cada uma das três regiões?*

Considere a matriz de locomoção de moradores:

$$P = \begin{bmatrix} 90\% & 15\% & 10\% \\ 5\% & 75\% & 5\% \\ 5\% & 10\% & 85\% \end{bmatrix} = \begin{bmatrix} 0,9 & 0,15 & 0,1 \\ 0,05 & 0,75 & 0,05 \\ 0,05 & 0,1 & 0,85 \end{bmatrix}$$

Seja I_3 a matriz identidade e $q = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, tal que, $(I - P)q = 0$. Ou seja,

$$\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0,9 & 0,15 & 0,1 \\ 0,05 & 0,75 & 0,05 \\ 0,05 & 0,1 & 0,85 \end{bmatrix} \right) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 0,1 & -0,15 & -0,1 \\ -0,5 & 0,25 & -0,05 \\ -0,05 & -0,1 & 0,15 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

A forma escalonada reduzida por linhas da matriz de coeficientes é:

$$\begin{bmatrix} 1 & 0 & -\frac{13}{7} \\ 0 & 1 & -\frac{4}{7} \\ 0 & 0 & 0 \end{bmatrix}$$

de modo que o sistema linear original é equivalente ao sistema: $x_1 = \frac{13}{7}x_3$ e $x_2 = \frac{4}{7}x_3$.
Pondo $x_3 = s$, qualquer solução do sistema linear é da forma,

$$q = s. \begin{bmatrix} \frac{13}{7} \\ \frac{4}{7} \\ 1 \end{bmatrix}$$

Mas como $x_1 + x_2 + x_3 = 1$, temos : $x_1 = \frac{13}{24}$, $x_2 = \frac{4}{24}$ e $x_3 = \frac{7}{24}$.
Assim vemos que a longo prazo, terá $54,2\%$ da população na região 1, $16,7\%$ da população na região 2 e $29,1\%$ da população na região 3.

4 Genética

A próxima aplicação ilustra uma situação em que uma cadeia de Markov não é governada por uma matriz regular, mas o comportamento limite de vetores-estado ainda pode ser estudado. O exemplo aborda a propagação de uma característica herdada em sucessivas gerações calculando potências de matrizes. Para tanto, apresentaremos brevemente os pré-requisitos necessários.

Definição 1.51. *Se A é uma matriz $n \times n$, um número λ é chamado um autovalor de A se $Ax = \lambda x$, para algum vetor coluna x não nulo. Tal vetor coluna não nulo x é chamado um autovetor da matriz A associado ao autovalor λ.*

Exemplo 1.52. *Dada a matriz $A = \begin{bmatrix} 5 & -2 \\ 4 & -1 \end{bmatrix}$. Então $\lambda = 3$ é um autovalor de A com autovetor $x = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, já que $x \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $Ax = \begin{bmatrix} 5 & -2 \\ 4 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix} = 3 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 3x$.*

A matriz A do Exemplo 1.52 possui um outro autovalor além de $\lambda = 3$. Para encontrá-lo, observemos um procedimento geral a seguir que funciona para qualquer matriz A de ordem $n \times n$. Por definição, um número λ é um autovalor de A se, e somente se,

$$Ax = \lambda x \quad \text{para algum } x \neq 0.$$

Se I denota a matriz identidade de mesma ordem que A, isso é equivalente a dizer que o sistema linear homogêneo

$$(\lambda I - A)x = 0 \quad \text{possui uma solução não trivial } x \neq 0.$$

Pelo Teorema 2.6 do próximo capítulo, isso acontece se, e somente se, o determinante da matriz dos coeficientes é nulo:

$$|\lambda I - A| = 0.$$

Exemplo 1.53. *Encontre todos os autovalores e autovetores da matriz $A = \begin{bmatrix} 5 & -2 \\ 4 & -1 \end{bmatrix}$.*

Solução. Como $\lambda I - A = \begin{bmatrix} \lambda - 5 & 2 \\ -4 & \lambda + 1 \end{bmatrix}$, temos $|\lambda I - A| = (\lambda - 5)(\lambda + 1) + 8 = (\lambda - 3)(\lambda - 1)$ e, portanto, $\lambda_1 = 3$ e $\lambda_2 = 1$ são os autovalores de A. Observe que $\lambda_1 = 3$ foi o autovalor mencionado no Example 1.52. Para encontrar os autovetores associados a $\lambda_2 = 1$, observe que nesse caso

$$\lambda_2 I - A = \begin{bmatrix} \lambda_2 - 5 & 2 \\ -4 & \lambda_2 + 1 \end{bmatrix} = \begin{bmatrix} -4 & 2 \\ -4 & 2 \end{bmatrix}$$

e as soluções para $(\lambda_2 I - A)x = 0$ são $x = t \begin{bmatrix} 1/2 \\ 1 \end{bmatrix}$ onde t é um número real arbitrário. Portanto, os autovetores x associados a λ_2 são $x = t \begin{bmatrix} 1/2 \\ 1 \end{bmatrix}$ onde $t \neq 0$ é arbitrário. Por

exemplo, para $t = 2$, $x = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ *é um autovetor associado a* λ_2. *Analogamente,* $\lambda_1 = 3$ *dá origem aos autovetores* $x = t \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $t \neq 0$, *que inclui o autovetor mencionado no Exemplo 1.52.*

Definição 1.54. *Uma matriz* $n \times n$ *é uma matriz diagonal se todas as suas entradas, exceto possivelmente as entradas da diagonal principal, são nulas, ou seja, a matriz tem a forma*

$$\begin{bmatrix} \mu_1 & 0 & \cdots & 0 \\ 0 & \mu_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mu_n \end{bmatrix}$$

Definição 1.55. *Uma matriz quadrada* A *é dita diagonalizável se existir uma matriz invertível* P *tal que* $P^{-1}AP$ *é uma matriz diagonal.*

Valendo-se do Exemplo 1.53, consideremos a matriz P cujas colunas são formadas respectivamente por autovetores de A associados a $\lambda_1 = 3$ e $\lambda_2 = 1$, por exemplo,

$$P = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$

Pelo Teorema 2.6 do próximo capítulo, P é invertível e $P^{-1}AP = D$, onde $D = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$, mostrando que a matriz $A = \begin{bmatrix} 5 & -2 \\ 4 & -1 \end{bmatrix}$ é diagonalizável. Isso é de fato um procedimento geral para diagonalizar, quando possível, uma matriz $n \times n$ seguindo os seguintes passos:

1. Encontre os autovalores λ de A.
2. Calcule os autovetores associados a cada um desses autovalores λ, a partir das soluções não triviais do sistema homogêneo $(\lambda I - A)x = 0$.
3. A é diagonalizável se, e somente se, ela possui autovetores $x_1, \cdots, x_n$ tais que a matriz $P = [x_1 x_2 \cdots x_n]$ é invertível.
4. Se A é diagonalizável, $P^{-1}AP$ é uma matriz diagonal, cuja diagonal principal é formada pelos respectivos autovalores associados aos autovetores (colunas de P).

Exemplo 1.56. *Encontre a matriz* P *que diagonaliza* $A = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 \end{bmatrix}$.

Seus autovalores são $\lambda_1 = 1$, $\lambda_2 = \frac{1}{2}$ *e* $\lambda_3 = 0$, *com respectivos autovetores associados* $v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, v_2 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}, v_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$. *Assim,* $P = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{bmatrix}$ *é tal que*

$$P^{-1}AP = D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Um fato notável que devemos observar é sobre o ciclo de potências de matrizes diagonalizáveis. Dada uma matriz quadrada A de ordem $n \times n$ diagonalizável, podemos encontrar uma fórmula explícita para A^k para qualquer que seja o expoente inteiro k. De fato, seja P uma matriz invertível e D uma matriz diagonal tais que $P^{-1}AP = D$, ou equivalentemente

$$A = PDP^{-1}. \tag{1.4}$$

Para $k = 1, 2, \cdots$, usando (1.4), temos

$$\begin{aligned} A^k &= AA\cdots A = (PDP^{-1})(PDP^{-1})\cdots(PDP^{-1}) \\ &= PD(P^{-1}P)DP^{-1}\cdots PDP^{-1} \\ &= PD(I)D(I)\cdots(I)DP^{-1} \\ &= PD\cdots DP^{-1} \\ &= PD^kP^{-1}. \end{aligned}$$

Portanto,

$$A^k = PD^kP^{-1} \quad \text{para } k = 1, 2, \cdots$$

onde

$$D^k = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}^k = \begin{bmatrix} \lambda_1^k & 0 & \cdots & 0 \\ 0 & \lambda_2^k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n^k \end{bmatrix}.$$

Por exemplo, utilizando este fato notável para a matriz A do Exemplo 1.56 encontramos

$$A^n = PD^nP^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \left(\frac{1}{2}\right)^n & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1-\left(\frac{1}{2}\right)^n & 1-\left(\frac{1}{2}\right)^{n-1} \\ 0 & \left(\frac{1}{2}\right)^n & \left(\frac{1}{2}\right)^{n-1} \\ 0 & 0 & 0 \end{bmatrix}.$$

Observa-se com isso que A é uma matriz de transição que não é regular.

4.1 Características Hereditárias

Nesta subseção examinaremos a hereditariedade de características de animais ou plantas. Vamos supor que as características hereditárias sejam governadas por um conjunto de dois genes, denotados por A e a. Pela hereditariedade autossômica, cada indivíduo de cada sexo possui dois destes genes, e os possíveis pares são AA, Aa e aa. Este par de genes é chamado genótipo do indivíduo e determina como o caráter controlado por estes genes se manifesta no indivíduo. Por exemplo, nos humanos a cor dos olhos é definida pela hereditariedade autossômica. Os genótipos AA e Aa têm olhos castanhos e o genótipo aa tem olhos azuis. Neste caso dizemos que o gene A domina o gene a, ou seja, o gene a é recessivo em relação ao gene A. Há também a hereditariedade ligada ao sexo. Neste caso o macho da espécie possui apenas um gene (A ou a) e a fêmea um par de dois genes (AA, Aa ou aa). Nos humanos, o daltonismo, a calvície hereditária, a hemofilia e outros são características controladas por hereditariedade ligada ao sexo. A seguir vamos estudar a maneira pela qual os genes dos pais são transmitidos para seus descendentes no tipo de hereditariedade autossômica. Construíremos modelos matriciais que dão os prováveis genótipos dos descendentes em termos dos genótipos dos pais e usaremos estes modelos para acompanhar a distribuição genotípica de uma população através de sucessivas gerações.

Na hereditariedade autossômica, um indivíduo herda de modo aleatório um par de genes, sendo um de sua mãe e o outro do pai, formando assim seu genótipo. Supondo que um dos pais tenha genótipo Aa, terá igual probabilidade que o descendente herde o gene A ou a daquele genitor. Se um dos pais é do genótipo aa e o outro é do genótipo Aa, o descendente sempre receberá um gene a do genitor aa e receberá, com igual probabilidade, ou um gene A ou um gene a do genitor Aa. Logo, cada descendente terá chances iguais de ser do genótipo Aa ou aa. Abaixo, listamos as probabilidades dos possíveis genótipos dos descendentes para todas as possíveis combinações de genótipos dos pais.

	Genótipo dos pais					
Genótipo do descendente	AA-AA	AA-Aa	AA-aa	Aa-Aa	Aa-aa	aa-aa
AA	1	1/2	0	1/4	0	0
Aa	0	1/2	1	1/2	1/2	0
aa	0	0	0	1/4	1/2	1

Tabela 1.5: Probabilidades dos possíveis genótipos dos descendentes

Exemplo 1.57. *(Distribuição dos genótipos numa população) Suponha que um agricultor tenha uma grande população de plantas consistindo de alguma distribuição de todos os três possíveis genótipos AA, Aa e aa. O agricultor deseja implementar um programa de criação no qual cada planta da população é sempre fertilizada por uma planta do genótipo AA. Deduza*

uma expressão para a distribuição dos três genótipos na população depois de um número qualquer de gerações.

Para $n \in \mathbb{N}$, escrevemos

a_n = fração de plantas do genótipo AA na n- ésima geração;

b_n = fração de plantas do genótipo Aa na n- ésima geração;

c_n = fração de plantas do genótipo aa na n- ésima geração.

Assim, a_0, b_0 e c_0 representam a distribuição inicial dos genótipos. E sabemos que $a_n + b_n + c_n = 1$, para $n = 0, 1, 2, ...$ Como cada planta da população é sempre fertilizada por uma planta do genótipo AA, podemos determinar a distribuição de genótipos em cada geração a partir da distribuição na geração precedente utilizando somente as três primeiras linhas e colunas da Tabela 1.5 para obter as equações:

$$a_n = a_{n-1} + \frac{1}{2}b_{n-1}, \tag{1.5}$$

$$b_n = c_{n-1} + \frac{1}{2}b_{n-1}, \tag{1.6}$$

$$c_n = 0. \tag{1.7}$$

A equação (1.5) representa que todos os descendentes de uma planta do genótipo AA serão do genótipo AA e metade dos descendentes de uma planta do genótipo Aa será do genótipo AA. A equação (1.6) representa que todos os descendentes de uma planta do genótipo aa serão do genótipo Aa e metade dos descendentes de uma planta do genótipo Aa será do genótipo Aa. A equação (1.7) afirma que não haverá descendentes do genótipo aa de uma planta do genótipo AA. As equações (1.5)-(1.7) podem ser escritas em notação matricial como:

$$x_n = Ax_{n-1}, \tag{1.8}$$

onde

$$x_n = \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix}, \quad x_{n-1} = \begin{bmatrix} a_{n-1} \\ b_{n-1} \\ c_{n-1} \end{bmatrix} \quad \text{e} \quad A = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Note que as três colunas da matriz A são iguais às três primeiras colunas da Tabela 1.5. Da equação (1.8) segue que

$$x_n = Ax_{n-1} = A^2x_{n-2} = ... = A^nx_0$$

Pelo Exemplo 1.56, podemos escrever uma expressão explícita para A^n como

$$A^n = PD^nP^{-1} = \begin{bmatrix} 1 & 1-\left(\frac{1}{2}\right)^n & 1-\left(\frac{1}{2}\right)^{n-1} \\ 0 & \left(\frac{1}{2}\right)^n & \left(\frac{1}{2}\right)^{n-1} \\ 0 & 0 & 0 \end{bmatrix}.$$

Segue-se que

$$x^n = PD^nP^{-1}x_0 = \begin{bmatrix} 1 & 1-(\frac{1}{2})^n & 1-(\frac{1}{2})^{n-1} \\ 0 & (\frac{1}{2})^n & (\frac{1}{2})^{n-1} \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ b_0 \\ c_0 \end{bmatrix}$$

ou equivalentemente

$$x^n = \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix} = \begin{bmatrix} a_0 + b_0 + c_0 - (\frac{1}{2})^n b_0 - (\frac{1}{2})^{n-1} c_0 \\ (\frac{1}{2})^n b_0 + (\frac{1}{2})^{n-1} c_0 \\ 0 \end{bmatrix}.$$

Como $a_0 + b_0 + c_0 = 1$, obtemos:

$$\begin{aligned} a_n &= 1 - \left(\frac{1}{2}\right)^n b_0 - \left(\frac{1}{2}\right)^{n-1} c_0 \\ b_n &= \left(\frac{1}{2}\right)^n b_0 + \left(\frac{1}{2}\right)^{n-1} c_0 \\ c_n &= 0 \end{aligned}$$

Estas são as fórmulas explícitas para a fração dos três genótipos na n-ésima geração de plantas em termos das frações de genótipos iniciais. Como $\left(\frac{1}{2}\right)^n$ tende a zero quando n tende ao infinito, temos

$$\begin{aligned} a_n &\to 1, \\ b_n &\to 0. \end{aligned}$$

Note que também $c_n \to 0$ pelo fato de c_n ser uma sequência constante e igual a zero. Isso mostra que no limite todas as plantas da população serão do genótipo AA.

Exemplo 1.58. *Supondo que cada planta da população seja sempre fertilizada por uma planta do seu próprio genótipo em vez de sempre ser fertilizada por uma planta do genótipo AA. Usando a mesma notação do exemplo anterior, teremos:*

$$x^n = A^n . x^0,$$

onde

$$A = \begin{bmatrix} 1 & \frac{1}{4} & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{4} & 1 \end{bmatrix}.$$

Encontramos os autovalores de A, que são: $\lambda_1 = 1$, $\lambda_2 = 1$ e $\lambda_3 = \frac{1}{2}$, e a eles estão associados os autovetores: $v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, $v_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ e $v_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$.

Fazendos os cálculos, obtemos:

$$\begin{aligned} a_n &= a_0 + \frac{1}{2} b_0 - \left(\frac{1}{2}\right)^{n+1} b_0 \\ b_n &= \left(\frac{1}{2}\right)^n b_0 \\ c_n &= c_0 + \frac{1}{2} b_0 - \left(\frac{1}{2}\right)^{n+1} b_0 \end{aligned}$$

Estas são as fórmulas explícitas para a fração dos três genótipos na n-ésima geração de plantas em termos das frações de genótipos iniciais. Como $\left(\frac{1}{2}\right)^n$ tende a zero quando n tende ao infinito, temos

$$\begin{aligned} a_n &\rightarrow a_0 + \frac{1}{2}b_0, \\ b_n &\rightarrow 0, \\ c_n &\rightarrow c_0 + \frac{1}{2}b_0. \end{aligned}$$

Assim fertilizando cada planta com um de seu próprio genótipo produz uma população que no limite contém somente os genótipos AA e aa.

Capítulo

2

Aplicações do determinante

O propósito deste capítulo é apresentar o conceito de determinante e, principalmente, listar as propriedades que todo estudante do ensino médio deveria saber sobre o determinante de uma matriz A:

- detA dá área ou volume;
- A é invertível se, e somente se, detA $\neq 0$;
- det(AB) = detAdetB;
- o modo mais eficiente de calcular detA é usar a redução de A para a forma escalonada.

A apresentação a seguir é baseada na referência [4]. Dada uma matriz quadrada $A = [a_{ij}]$, definimos um número associado à matriz A, chamado determinante. Denotamos detA, det$[a_{ij}]$ ou $|A|$ e escrevemos:

- Determinante de uma matriz 1×1: $|a| = a$
- Determinante de uma matriz 2×2: $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$

• Determinante de uma matriz 3×3:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Para generalizar a definção do determinante para matrizes maiores, usaremos o determinante 2×2 para reescrever o determinante 3×3. Como os termos do determinante 3×3 podem ser agrupados como

$$(a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32}) - (a_{12}a_{21}a_{33} - a_{12}a_{23}a_{31}) + (a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}),$$

temos

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

ou abreviadamente na forma

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}|A_{11}| - a_{12}|A_{12}| + a_{13}|A_{13}|,$$

onde A_{11}, A_{12} e A_{13} são matrizes 2×2 obtidas de A eliminando a primeira linha e uma das três colunas de A. Observamos que é possível desenvolver o determinante usando as outras linhas (ou mesmo as colunas) obtendo o mesmo resultado. Por exemplo, agrupando os termos do determinante 3×3 como

$$-(a_{12}a_{21}a_{33} - a_{13}a_{21}a_{32}) + (a_{11}a_{22}a_{33} - a_{13}a_{22}a_{31}) - (a_{11}a_{23}a_{32} - a_{12}a_{23}a_{31}),$$

obtemos o desenvolvimento do determinante em termos da segunda linha:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = -a_{21}|A_{21}| + a_{22}|A_{22}| - a_{23}|A_{23}|.$$

Podemos dar agora uma definição recursiva do determinante de uma matriz $n \times n$ baseada no determinante de submatrizes $(n-1) \times (n-1)$.

Definição 2.1. *Para $n \geq 2$, o determinante de uma matriz $n \times n$ $A = [a_{ij}]$ é definido por*

$$|A| = a_{i1}|A_{i1}| - a_{i2}|A_{i2}| + \cdots + (-1)^{1+n}a_{in}|A_{in}| = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}|A_{ij}|,$$

onde, para cada $i, j \in \{1, \ldots, n\}$, A_{ij} é a matriz $(n-1) \times (n-1)$ obtida de A eliminando a i-ésima linha e a j-ésima coluna de A.

Observe que na fórmula dada, o determinante foi desenvolvido pela i-ésima linha. Uma fórmula análoga é válida para as colunas. Além disso, pode ser provado que o determinante de uma matriz quadrada é igual ao desenvolvimento ao longo de qualquer linha ou coluna da matriz.

Observe ainda que se uma linha ou coluna de uma matriz quadrada consistir inteiramente de zeros, então o determinante será zero.

Exemplo 2.2. *Dada a matriz*

$$A = \begin{bmatrix} 3 & -7 & 8 & 9 & -6 \\ 0 & 2 & -5 & 7 & 3 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 2 & 4 & -1 \\ 0 & 0 & 0 & -2 & 0 \end{bmatrix},$$

o cálculo do seu determinante é mais oportuno quando desenvolvido pela primeira coluna, pois todos os seus termos são nulos exceto o primeiro. Assim,

$$|A| = 3 \begin{vmatrix} 2 & -5 & 7 & 3 \\ 0 & 1 & 5 & 0 \\ 0 & 2 & 4 & -1 \\ 0 & 0 & -2 & 0 \end{vmatrix}.$$

Expandindo este determinante 4×4 *ao longo da primeira coluna, aproveitando-se das entradas nulas, temos*

$$|A| = 3 \cdot 2 \begin{vmatrix} 1 & 5 & 0 \\ 2 & 4 & -1 \\ 0 & -2 & 0 \end{vmatrix} = 3 \cdot 2 \cdot (-2) = -12,$$

após o cálculo do determinante 3×3 *que ainda resta.*

Um caso particular, mas relevante, é o caso das matrizes triangulares. Uma matriz quadrada é chamada triangular superior se todo elemento abaixo da diagonal principal for igual a zero. Analogamente, uma matriz quadrada é chamada triangular inferior se todo elemento acima da diagonal principal for igual a zero. Uma matriz quadrada é chamada triangular se for triangular superior ou inferior. A matriz do exemplo anterior não é triangular, mas o método usado no cálculo do seu determinante pode ser adaptado para provar o seguinte teorema.

Teorema 2.3. *Se A é uma matriz triangular, então $|A|$ é o produto das entradas da diagonal principal de A.*

O próximo resultado mostra que as operações elementares com as linhas ou colunas têm um efeito simples sobre o determinante.

Teorema 2.4. *Seja A uma matriz $n \times n$ qualquer.*

1. *Se B for obtida de A a partir de A por meio da permutação de duas linhas (colunas) diferentes, então $|B| = -|A|$.*
2. *Se B for obtida de A a partir de A por meio da multiplicação de alguma linha (coluna) de A por um número k, então $|B| = k|A|$.*
3. *Se B for obtida de A a partir de A por meio da adição de um múltiplo de alguma linha (coluna) de A com uma linha (coluna) diferente de A, então $|B| = |A|$.*

É conveniente provar o Teorema 2.4 quando esse é enunciado em termos de operações elementares de matrizes discutidas na Seção 2.3. Chamaremos uma matriz elementar E *uma substituição de linha* se E é obtida da matriz identidade somando um múltiplo de uma linha a uma outra, E é *uma troca* se E é obtida por uma troca de linhas de I e E é *uma escala por r* se E é obtida pelo produto de uma linha de I por um número não nulo r. Com esta terminologia, o Teorema 2.4 pode ser reescrito como:

Se A é uma matriz $n \times n$ qualquer e E é uma matriz $n \times n$ elementar, então

$$|EA| = |E||A|,$$

onde

$$|E| = \begin{cases} 1 & \text{se } E \text{ é uma substituição de linha,} \\ -1 & \text{se } E \text{ é uma troca de linha,} \\ r & \text{se } E \text{ é uma escala por } r. \end{cases}$$

Prova: A prova é por indução em n. Para $n = 2$, a prova é imediata. Suponha o resultado verdadeiro para matrizes $n \times n$ com $n \geq 2$, e provemos que o resultado é verdadeiro para $n+1$. A ação de E envolve duas linhas ou somente uma linha de A. Assim, podemos expandir o determinante de EA ao longo de uma linha não afetada pela ação de E, digamos a linha i. Seja A_{ij} (respectivamente B_{ij}) a matriz obtida eliminando a linha i e a coluna j de E (respectivamente EA). Então as linhas de B_{ij} são obtidas das linhas de A_{ij} pelas mesmas operações elementares que E atua em A. Como estas submatrizes são $n \times n$, a hipótese de indução implica

$$|B_{ij}| = \alpha |A_{ij}|,$$

sendo $\alpha = 1, -1$ ou r, dependendo da natureza de E. Pela definição do determinante (desenvolvido ao longo da linha i), temos

$$\begin{aligned} |EA| &= a_{i1}(-1)^{i+1}|B_{i1}| + \cdots + a_{in}(-1)^{i+n}|B_{in}| \\ &= \alpha a_{i1}(-1)^{i+1}|A_{i1}| + \cdots + \alpha a_{in}(-1)^{i+n}|A_{in}| \\ &= \alpha |A|. \end{aligned}$$

Assim, o teorema é válido para $n+1$. Pelo princípio da indução, o teorema é verdadeiro para todo $n \geq 2$. O teorema é trivialmente verdadeiro para $n = 1$. Portanto, a propriedade é verdadeira para todo n. ■

Exemplo 2.5. *Calcule o determinante de A, onde*

$$A = \begin{bmatrix} 1 & -4 & 2 \\ -2 & 8 & -9 \\ -1 & 7 & 0 \end{bmatrix}.$$

Solução. A estratégia é reduzir A para a forma escalonada e então usar a definição do determinante para uma matriz triangular, cujo valor é o produto das entradas da diagonal principal. As duas primeiras alterações na coluna 1 não mudam o determinante:

$$|A| = \begin{vmatrix} 1 & -4 & 2 \\ -2 & 8 & -9 \\ -1 & 7 & 0 \end{vmatrix} = \begin{vmatrix} 1 & -4 & 2 \\ 0 & 0 & -5 \\ -1 & 7 & 0 \end{vmatrix} = \begin{vmatrix} 1 & -4 & 2 \\ 0 & 0 & -5 \\ 0 & 3 & 2 \end{vmatrix}.$$

Uma troca entre as linhas 2 e 3 troca o sinal do determinante, assim

$$|A| = -\begin{vmatrix} 1 & -4 & 2 \\ 0 & 3 & 2 \\ 0 & 0 & -5 \end{vmatrix} = -(1)3(-5) = 15.$$

A estratégia empregada no exemplo anterior pode revelar uma relação entre determinantes e matrizes invertíveis. Suponha que uma matriz A $n \times n$ tenha sido levada a sua forma escalonada U. Se nesse processo houve r trocas de linhas, então

$$|A| = (-1)^r |U|.$$

Como U está na forma escalonada, ela é uma matriz triangular, e assim o determinante de U é o produto das entradas $u_{11}, \cdots, u_{nn}$ da sua diagonal principal. Se A é invertível, as entradas u_{ii} são todos os pivôs. Caso contrário, pelo menos uma das entradas u_{ii} é zero, e o produto $u_{11} \cdots u_{nn}$ é zero. Assim,

$$|A| = \begin{cases} (-1)^r u_{11} \cdots u_{nn}, & \text{se } A \text{ é invertível,} \\ 0, & \text{se } A \text{ não é invertível.} \end{cases}$$

O próximo teorema é uma consequência dessa fórmula.

Teorema 2.6. *Uma matriz quadrada A é invertível se, e somente se,* $|A| \neq 0$.

Esse teorema possui diversas aplicações e interpretações; mencionaremos apenas uma delas que será sistematicamente utilizada na próxima seção. Trata-se do estudo de sistemas lineares de n equações e n incógnitas:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n &= b_2 \\ \vdots &= \vdots \\ a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n &= b_n \end{cases}$$

o qual pode ser escrito na forma matricial

$$\begin{bmatrix} a_{11} & ... & a_{1n} \\ a_{21} & ... & a_{21} \\ \vdots & & \vdots \\ a_{n1} & ... & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

ou

$$AX = B,$$

onde $A = \begin{bmatrix} a_{11} & ... & a_{1n} \\ a_{21} & ... & a_{21} \\ \vdots & & \vdots \\ a_{n1} & ... & a_{nn} \end{bmatrix}$ é a matriz dos coeficientes, $B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$ é a matriz dos termos independentes e $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ é a matriz das incógnitas. Para esta equação, suponhamos que $|A| \neq 0$ e portanto, que A tenha a inversa A^{-1}. Então, nesse caso, a única solução é dada por $X = A^{-1}B$. No caso particular de $B = 0$, $X = 0$ é sempre uma solução do sistema linear homogêneo $AX = 0$ independente de A ser invertível ou não. No entanto, $AX = 0$ possui uma solução não trivial se, e somente se, $|A| = 0$. Para ver isso, basta observar que quando $|A| = 0$, a forma escalonada de A possui ao menos uma linha com todas as entradas nulas, gerando um sistema linear equivalente ao sistema $AX = 0$ tendo mais incógnitas do que equações, e portanto possui infinitas soluções.

O próximo resultado é sobre determinantes e produtos de matrizes.

Teorema 2.7. *Se A e B são matrizes $n \times n$, então $|AB| = |A||B|$.*

Prova: Se A não é invertível, então a matrizAB também não é invertível Neste caso, $|AB| = |A||B|$, pois ambos os lados dessa igualdade são nulos, e portanto a propriedade é válida. Se A é invertível, então existem matrizes elementares $E_1, \cdots, E_p$ tais que

$$A = E_p E_{p-1} \cdots E_1 \cdot I_n = E_p E_{p-1} \cdots E_1.$$

Pelo Teorema 2.4,

$$\begin{aligned} |AB| &= |E_p E_{p-1} \cdots E_1 \cdot B| = |E_p||E_{p-1} \cdots E_1 \cdot B| = \cdots \\ &= |E_p||E_{p-1}| \cdots |E_1||B| = \cdots = |E_p E_{p-1} \cdots E_1||B| \\ &= |A||B|. \end{aligned}$$

■

1 Construção de curvas e superfícies por pontos especificados

Nesta seção faremos uso de determinantes para construir retas, planos, circunferências e seções cônicas em geral por pontos especificados no plano. O procedimento também é utilizado para construir planos e esferas no espaço passando por pontos fixados.

1.1 Uma reta por dois pontos

Suponha que (x_1, y_1) e (x_2, y_2) sejam dois pontos distintos no plano. Existe uma única reta que passa por estes dois pontos (Figura 2.1). Vamos encontrar a equação dessa reta. Para

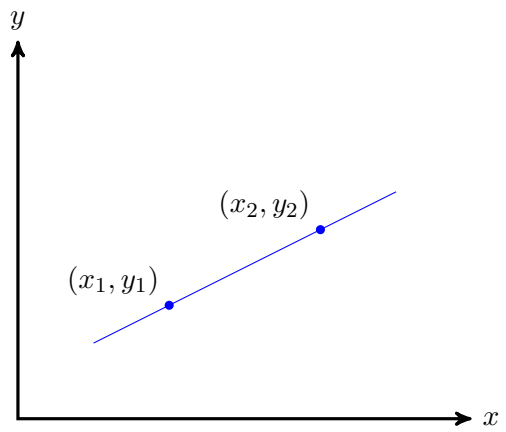


Figura 2.1

um ponto genérico (x, y) pertencer a uma reta, devem existir números c_1, c_2 e c_3 não todos nulos tais que

$$c_1x + c_2y + c_3 = 0.$$

Como os pontos (x_1, y_1) e (x_2, y_2) estão na reta, podemos escrever:

$$\begin{cases} c_1x_1 + c_2y_1 + c_3 &= 0 \\ c_1x_2 + c_2y_2 + c_3 &= 0 \end{cases}$$

Assim, obtemos:

$$\begin{cases} c_1x + c_2y + c_3 &= 0 \\ c_1x_1 + c_2y_1 + c_3 &= 0 \\ c_1x_2 + c_2y_2 + c_3 &= 0 \end{cases}$$

Como c_1, c_2, c_3 não são todos nulos, e este sistema tem solução não trivial, isso implica que o determinante da matriz associada ao sistema deve ser zero. Observe:

$$\begin{vmatrix} x & y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix} = 0.$$

Isto resulta

$$(y_1 - y_2)x - (x_1 - x_2)y + (x_1y_2 - x_2y_1)1 = 0,$$

que é a equação procurada.

Exemplo 2.8. *Encontre a equação da reta que passa pelos pontos* $(2,3), (-1,4)$.
Resolução: fazendo

$$\begin{vmatrix} x & y & 1 \\ 2 & 3 & 1 \\ -1 & 4 & 1 \end{vmatrix} = 0,$$

resulta

$$(3-4)x - (2+1)y + (8+3)1 = 0,$$

ou seja,

$$x + 3y - 11 = 0.$$

1.2 Uma circunferência por três pontos

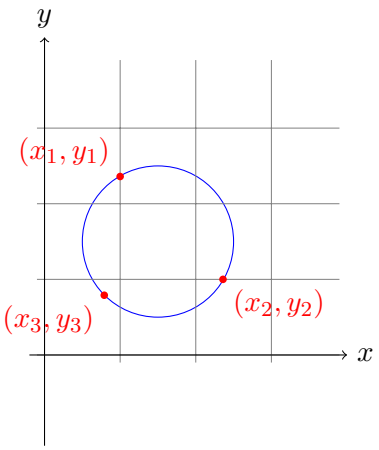


Figura 2.2

Sejam (x_1, y_1), (x_2, y_2) e (x_3, y_3) três pontos distintos e não colineares do plano. Da Geometria Analítica sabemos que existe uma única circunferência que passa por eles (Figura 2.2). Vamos determinar a equação dessa circunferência. Um ponto genérico (x, y) pertence a uma circunferência se existirem números c_1, c_2, c_3 e c_4 não todos nulos tais que

$$c_1(x^2 + y^2) + c_2x + c_3y + c_4 = 0.$$

Como (x_1, y_1), (x_2, y_2) e (x_3, y_3) pertencem a circunferência, temos

$$\begin{cases} c_1(x_1^2 + y_1^2) + c_2x_1 + c_3y_1 + c_4 = 0 \\ c_1(x_2^2 + y_2^2) + c_2x_2 + c_3y_2 + c_4 = 0 \\ c_1(x_3^2 + y_3^2) + c_2x_3 + c_3y_3 + c_4 = 0 \end{cases}$$

Assim, obtemos o seguinte sistema

$$\begin{cases} c_1(x^2+y^2)+c_2x+c_3y+c_4 &= 0 \\ c_1(x_1^2+y_1^2)+c_2x_1+c_3y_1+c_4 &= 0 \\ c_1(x_2^2+y_2^2)+c_2x_2+c_3y_2+c_4 &= 0 \\ c_1(x_3^2+y_3^2)+c_2x_3+c_3y_3+c_4 &= 0 \end{cases}$$

Note que as equações acima formam um sistema linear homogêneo com uma solução não trivial em c_1, c_2, c_3 e c_4. Logo, o determinante é zero, a saber:

$$\begin{vmatrix} x^2+y^2 & x & y & 1 \\ x_1^2+y_1^2 & x_1 & y_1 & 1 \\ x_2^2+y_2^2 & x_2 & y_2 & 1 \\ x_3^2+y_3^2 & x_3 & y_3 & 1 \end{vmatrix} = 0.$$

Exemplo 2.9. *Encontre a equação da circunferência que passa pelos pontos* $(2,6)$, $(2,0)$ *e* $(5,3)$.

Resolução: fazendo

$$\begin{vmatrix} x^2+y^2 & x & y & 1 \\ 4+36 & 2 & 6 & 1 \\ 4+0 & 2 & 0 & 1 \\ 25+9 & 5 & 3 & 1 \end{vmatrix} = 0,$$

encontramos,

$$\begin{vmatrix} x^2+y^2 & x & y & 1 \\ 40 & 2 & 6 & 1 \\ 4 & 2 & 0 & 1 \\ 34 & 5 & 3 & 1 \end{vmatrix} = 0,$$

o que resulta

$$x^2+y^2-4x-6y+4=0,$$

ou equivalentemente

$$(x-2)^2+(y-3)^2=9.$$

1.3 Uma cônica arbitrária por cinco pontos

Como é sabido a equação geral de uma seção cônica arbitrária no plano (parábola, hipérbole ou elípse, ou formas degeneradas destas) é dada por $c_1x^2+c_2xy+c_3y^2+c_4x+c_5y+c_6=0$, com coeficientes c_1, c_2, c_3, c_4, c_5 e c_6 não todos nulos. Dividindo esta equação por um coeficiente que não seja nulo, o número de coeficientes desta equação é reduzido a cinco. Sendo assim, podemos determinar a equação da cônica que passa por cinco pontos, impondo

que o determinante da matriz associada ao respectivo sistema seja nulo, ou seja,

$$\begin{vmatrix} x^2 & xy & y^2 & x & y & 1 \\ x_1^2 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2^2 & x_2y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3^2 & x_3y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4^2 & x_4y_4 & y_4^2 & x_4 & y_4 & 1 \\ x_5^2 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \end{vmatrix} = 0.$$

Resolvendo este determinante obtém-se a equação de uma cônica qualquer.

Exemplo 2.10. *Encontre a equação da seção cônica que passa pelos pontos* $(0,0)$, $(0,-1)$, $(2,0)$, $(2,-5)$ *e* $(4,-1)$.

Resolução: substituindo os valores no determinante anterior, encontramos

$$\begin{vmatrix} x^2 & xy & y^2 & x & y & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & 1 \\ 4 & 0 & 0 & 2 & 0 & 1 \\ 4 & -10 & 25 & 2 & -5 & 1 \\ 16 & -4 & 1 & 4 & -1 & 1 \end{vmatrix} = 0,$$

resultando

$$x^2 + 2xy + y^2 - 2x + y = 0.$$

1.4 Um plano por três pontos

Suponha que (x_1, y_1, z_1), (x_2, y_2, z_2) e (x_3, y_3, z_3) sejam três pontos não colineares no espaço tridimensional. Pela Geometria Analítica, existe um único plano que passa por estes pontos. Vamos determinar a equação deste plano. Um ponto genérico (x, y, z) pertence a um plano se existem números não todos nulos c_1, c_2, c_3 e c_4 tais que $c_1x + c_2y + c_3z + c_4 = 0$. Como (x_1, y_1, z_1), (x_2, y_2, z_2) e (x_3, y_3, z_3) pertencem ao plano, obtemos o seguinte sistema homogêneo

$$\begin{cases} c_1x + c_2y + c_3z + c_4 = 0, \\ c_1x_1 + c_2y_1 + c_3z_1 + c_4 = 0, \\ c_1x_2 + c_2y_2 + c_3z_2 + c_4 = 0, \\ c_1x_3 + c_2y_3 + c_3z_3 + c_4 = 0, \end{cases}$$

o qual possui solução não trivial em c_1, c_2, c_3 e c_4, desde que o determinante da matriz associada seja nulo, ou seja,

$$\begin{vmatrix} x & y & z & 1 \\ x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \end{vmatrix} = 0.$$

Exemplo 2.11. *Encontre a equação do plano do espaço tridimensional que passa pelos pontos,* $(2,3,1)$, $(2,-1,-1)$ *e* $(1,2,1)$.
Resolução: fazendo

$$\begin{vmatrix} x & y & z & 1 \\ 2 & 3 & 1 & 1 \\ 2 & -1 & -1 & 1 \\ 1 & 2 & 1 & 1 \end{vmatrix} = 0,$$

obtemos

$$-x + y - 2z + 1 = 0.$$

1.5 Uma esfera por quatro pontos

A esfera no espaço tridimensional de equação

$$c_1(x^2 + y^2 + z^2) + c_2x + c_3y + c_4z + c_5 = 0$$

que passa por quatro pontos não coplanares (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) e (x_4, y_4, z_4) é dada em forma de determinante

$$\begin{vmatrix} x^2+y^2+z^2 & x & y & z & 1 \\ x_1^2+y_1^2+z_1^2 & x_1 & y_1 & z_1 & 1 \\ x_2^2+y_2^2+z_2^2 & x_2 & y_2 & z_2 & 1 \\ x_3^2+y_3^2+z_3^2 & x_3 & y_3 & z_3 & 1 \\ x_4^2+y_4^2+z_4^2 & x_4 & y_4 & z_4 & 1 \end{vmatrix} = 0.$$

Exemplo 2.12. *A equação da esfera que passa pelos quatro pontos não coplanares* $(0,3,2)$, $(1,-1,1)$, $(2,1,0)$ *e* $(5,1,3)$ *é dada por*

$$\begin{vmatrix} x^2+y^2+z^2 & x & y & z & 1 \\ 13 & 0 & 3 & 2 & 1 \\ 3 & 1 & -1 & 1 & 1 \\ 5 & 2 & 1 & 0 & 1 \\ 35 & 5 & 1 & 3 & 1 \end{vmatrix} = 0.$$

Isto resulta

$$x^2 + y^2 + z^2 - 4x - 2y - 6z + 5 = 0,$$

que na forma canônica é

$$(x-2)^2 + (y-1)^2 + (z-3)^2 = 9.$$

2 Determinantes como área ou volume

O próximo teorema fornece uma interpretação geométrica do determinante como área ou volume.

Teorema 2.13. *1. Suponha que os pontos $A = (a_1, a_2)$, $B = (b_1, b_2)$ e $O = (0, 0)$ não sejam colineares. Então a área do paralelogramo que tem por vértices O, A e B é o valor absoluto do determinante*

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}.$$

2. Suponha que os pontos $A = (a_1, a_2, a_3)$, $B = (b_1, b_2, b_3)$, $C = (c_1, c_2, c_3)$ e $O = (0, 0, 0)$ não sejam coplanares. Então o volume do paralelepípedo que tem por vértices O, A, B e C é o valor absoluto do determinante

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}.$$

Prova: O teorema é obviamente verdadeiro para qualquer matriz diagonal:

$$\left|\det \begin{bmatrix} a_1 & 0 \\ 0 & b_2 \end{bmatrix}\right| = |a_1 b_2| = \text{ área do retângulo (veja Figura 2.3).}$$

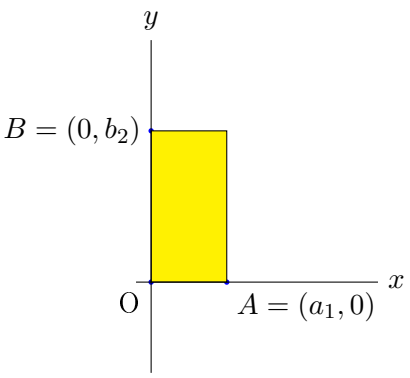


Figura 2.3: Área $= |a_1 b_2|$

É suficiente mostrar que qualquer matriz $M = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}$ pode ser transformada em uma matriz diagonal de modo que nem a área do paralelogramo associado e nem o |detM| sejam alterados. Pelas propriedades do determinante, o valor absoluto do determinante permanece o mesmo quando duas linhas são trocadas ou um múltiplo de uma linha é somada a uma outra linha da matriz. Além disso, essas operações são suficientes para transformar a matriz M em uma matriz diagonal. Portanto, é suficiente provar o seguinte fato geométrico:

Sejam $A = (a_1, b_1)$ e $B = (b_1, b_2)$ pontos distintos da origem $O = (0, 0)$. Então para qualquer número real c, a área do paralelogramo determinado por A e B e O é igual a área do paralelogramo determinado por $A = (a_1, b_1)$, $B + cA = (b_1 + ca_1, b_2 + ca_2)$ e O.

Para provar esta afirmação, vamos supor que A, B e O não sejam colineares, do contrário o paralelogramo é degenerado e tem área zero. Se L é a reta determinada por O e A, então $B + L$ é uma reta que passa por B e é paralela a L e o ponto $B + cA$ pertence a esta reta. (Veja figura abaixo). Os pontos B e $B + cA$ tem a mesma distância a reta L. Portanto os dois paralelogramos na Figura 2.4 têm a mesma área, pois têm a mesma base (o segmento OA). Isto completa a demonstração para o plano.

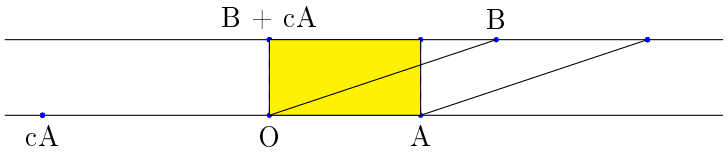


Figura 2.4: Dois paralelogramos de mesma área

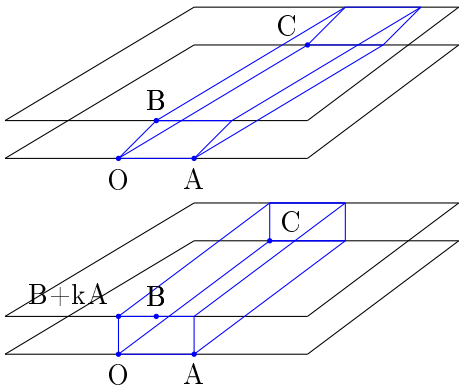


Figura 2.5: Dois paralelepípedos com volumes iguais

A prova para o caso espacial é análoga. O teorema é claramente verdadeiro para uma matriz 3×3 diagonal. E qualquer matriz A 3×3 pode ser transformada em uma matriz diagonal usando operações elementares com as linhas de A sem alterar $|A|$. Assim é suficiente mostrar que essas operações não afetam o volume do paralelepípedo determinado pelas linhas de A. A Figura 2.5 exibe um paralelepípedo com faces inclinadas, cujo volume é a área da base no plano determinado por O, A e C e altura dada pela distância do ponto B ao plano determinado por O, A e C. Qualquer ponto $B + kA$ tem essa mesma distância ao plano determinado por O, A e C. Portanto o volume do paralelepípedo não se altera quando a

matriz

$$\begin{bmatrix} A \\ B \\ C \end{bmatrix}$$

é substituída por

$$\begin{bmatrix} A \\ B + kA \\ C \end{bmatrix}.$$

Como substituições não afetam o volume, a prova está completa.

■

Capítulo

3

Roteiro de uma aula

O professor de matemática tem encontrado grande dificuldade ao trabalhar com alguns conceitos dentro da sala de aula, no que diz respeito a utilidade de tais assuntos. E muitas vezes o aluno é desestimulado, pois desenvolve a matemática de maneira mecânica, sem saber sua real função no cotidiano. Por sua vez o Currículo do Estado de São Paulo visa utilizar elementos de matrizes para organizar e justificar a resolução de situações-problema baseados em contexto do cotidiano, cabe a motivação de criar uma situação-problema que aborde o uso de multiplicação de matrizes.

A proposta desta dissertação é fazer o aluno perceber que multiplicação de matrizes pode ser útil para resolver problemas comuns do dia-a-dia. Assim depois de trabalhar o conceito de produtos de matrizes e a definição de grafos, seria proposto uma situação-problema que consiste em dividir a sala de aula em no máximo 6 equipes, tendo em média 6 alunos por equipe, e cada equipe joga exatamente uma vez com cada uma das outras . Dispondo os alunos, de modo que, todos participem.

Para valorizar essa atividade, e fazer uso da interdisciplinaridade, essa disputa é composta de perguntas e respostas, as quais estão relacionadas a conhecimentos de outras disciplinas. De acordo com os acertos, cria-se uma matriz que mostra a situação de cada equipe com relação às demais.

Na sequência os alunos fazem uso do conceito de grafos dirigidos por dominância, que tem como base a multiplicação de matrizes, para obter a classificação final das equipes.

Essa atividade pode ajudar os alunos a compreenderem a utilidade e importância do produto de matrizes, como também possibilitar que as outras disciplinas se articulem com a matemática.

Referências Bibliográficas

[1] ANTON, H. **Álgebra linear com aplicações**. Tradução de Claus Ivo Doering. 8. ed. Porto Alegre: Bookman, 2001. 572 p.

[2] BOLDRINI, J. L., COSTA, S. I. R., FIGUEIREDO, V. L., WETZLER, H. G. **Álgebra Linear**. 3 ed. São Paulo: Harbra, 1986. 411 p.

[3] KEMENY, J., SNELL, J. **Finite Markov Chains**. New York: Springer Verlag, 1976. 210 p.

[4] LAY, D. **Linear Álgebra and its Applications**. Boston: Addison-Wesley, 2006. 492 p.

[5] NICHOLSON, W. K. **Álgebra Linear**. Tradução técnica Célia Mendes Carvalho Lopes, Leila Maria Vasconcellos Figueiredo, Martha Salerno Monteiro. São Paulo: McGraw-Hill, 2006. 394p.

[6] STRANG, G. **Introduction to linear algebra**. Wellesley: Wellesley-Cambridge Press, 2005. 568 p.