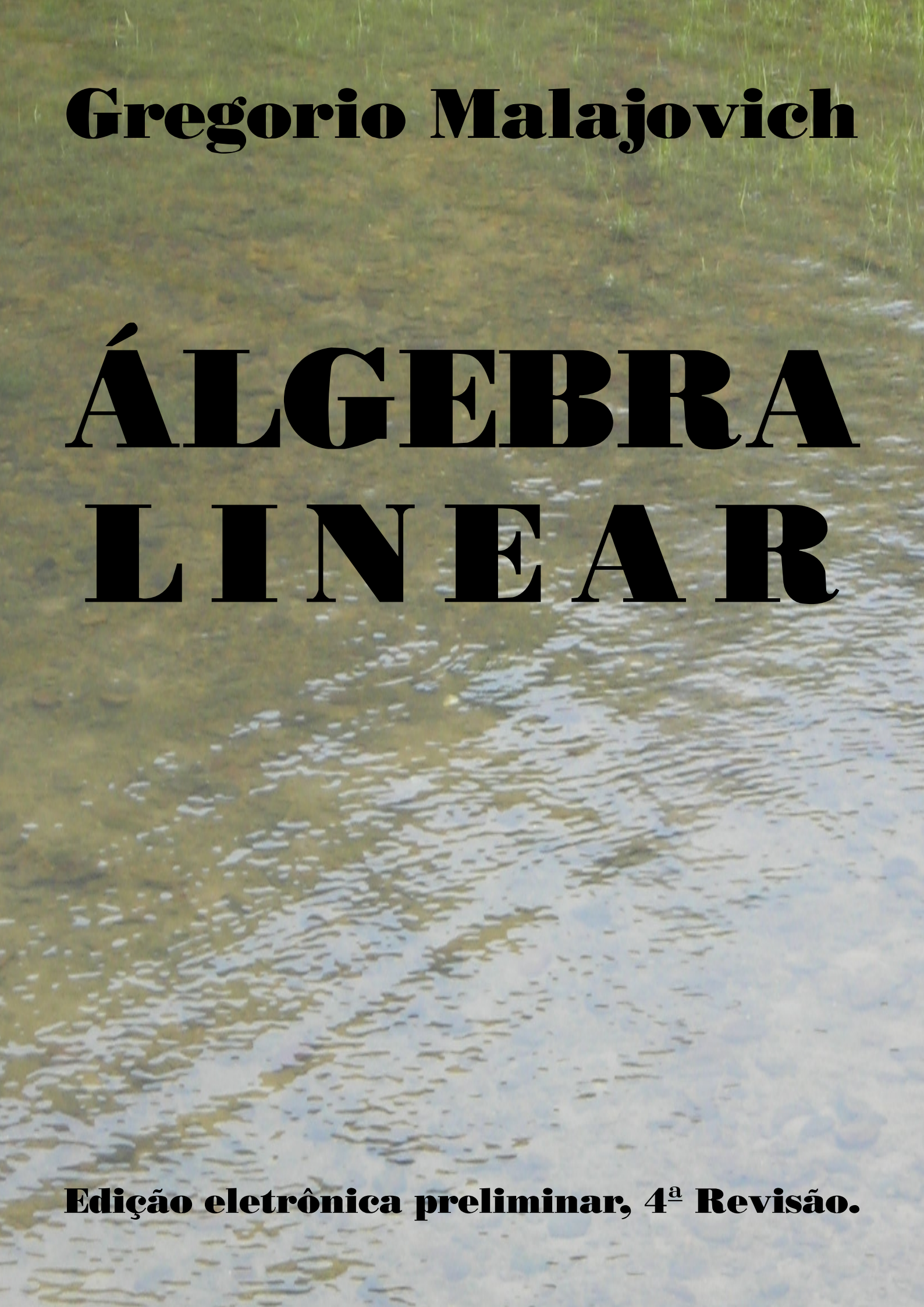




Gregorio Malajovich

ÁLGEBRA LINEAR

Edição eletrônica preliminar, 4ª Revisão.

Álgebra Linear

Gregorio Malajovich

Departamento de Matemática Aplicada, Universidade Federal do Rio de Janeiro.

Versão eletrônica e preliminar, quarta revisão, 3 de maio de 2021.

Prefácio à Edição de 2021



fundamento das tecnologias digitais é a matemática. Quanto mais avançada é uma tecnologia, mais a matemática fica oculta, transparente ao usuário. Este curso se destina à formação de futuros matemáticos, cientistas ou engenheiros-pesquisadores. O conteúdo usual do curso de Álgebra Linear foi reorganizado para contemplar as tecnologias derivadas, como buscas nas redes ou compressão de som e de imagem.

Nossa visão do mundo depende de maneira crucial de conhecimentos matemáticos mais ou menos avançados. Em um mundo dominado pela tecnologia, esses conhecimentos devem ser suficientes para entendê-la. Por isso me recuso a ensinar matemática como uma língua morta. Desta recusa surgiu o presente livro.

Procurei escrever um texto matematicamente completo e rigoroso, mas incentivando o aluno a procurar mais informações na biblioteca e na *internet*. A procura e triagem de informações é parte integrante do processo de aprendizado.

O trabalho individual dos exercícios é outra parte integrante e indispensável. Considero outrossim que estes não devem se constituir em uma lista tediosa e repetitiva de perguntas canônicas. Foram incluídos exercícios teóricos e aplicados (eu pessoalmente não gosto dessa distinção). Para os exercícios aplicados, utilizo o pacote *Julia*, por ser *software* livre e estar disponível em todas as boas distribuições do *GNU linux*.

Ao mesmo tempo, tentei modernizar um pouco o tratamento matemático e o conteúdo geral. A noção de grupo é inevitável. A forma de Jordan (que hoje só serve para se elaborar questões sobre forma de Jordan) pode ser deduzida da forma normal de Schur e a sua prova ficou parcialmente relegada aos exercícios. Já a decomposição em valores singulares é parte essencial do programa.

Tive o cuidado de transpor, na medida do possível, as fronteiras artificiais que ora são erguidas entre diferentes aspectos do mesmo fato matemático. A cultura matemática é unitária, só a incultura é especializada.

Uma característica fundamental da cultura matemática é o convívio com os limites do conhecimento, e com problemas em aberto suficientemente difíceis para motivar grandes programas de pesquisa.

Alguns problemas famosos em aberto podem ser enunciados na linguagem desenvolvida neste livro, mesmo que de modo não absolutamente preciso. Pelas razões expostas acima, decidi incluí-los.

A primeira versão destas notas foi escrita entre 2007 e 2009 e testada em turmas de elite de graduação. O pré-requisito mínimo era um semestre de cursos intensos de matemática, incluindo um primeiro contato com vetores, matrizes, Geometria Analítica e computação científica.

A versão atual foi usada, junto com material extra, para um curso de início de Mestrado ou final de Graduação. Outra possibilidade é usar os capítulos 1 a 17 para um curso regular de Graduação, com uma lista simplificada de exercícios.

Este texto está sendo depurado ao longo do tempo. Ainda acredito existirem bastantes erros, imprecisões e falhas tipográficas. Peço a todos que me os comuniquem em: gregorio@im.ufrj.br.

Agradecimentos: Gostaria de agradecer especialmente às turmas de Matemática Aplicada de 2007 a 2009, que tiveram o infortúnio de estudar com versões preliminares deste texto. Além dos alunos, também ajudaram a corrigir erros no texto: Beatriz Malajovich, Bruno Morier, Cassio Neri, Felipe Acker, Pedro Angelo Fonini, e um *referee* anônimo (em relação a dois dos capítulos, que foram previamente publicados¹). Beatriz Malajovich ajudou também em uma revisão parcial.

Rio de Janeiro, agosto de 2009.

¹Dois dos capítulos deste livro (e mais alguns trechos) foram publicados previamente em Gregorio Malajovich, *Geometria de Algoritmos Numéricos*, Notas em Matemática Aplicada 36, SBMAC, São Carlos, 2008.

Sumário

Prefácio à Edição de 2021	i
Capítulo 1. Espaços lineares, equações afins	1
1. Exemplos de grandezas lineares	1
2. Espaços vetoriais	2
3. Aplicações lineares	4
4. Sistemas de equações: três visões diferentes	5
5. Exercícios	6
Capítulo 2. O espaço $\mathbb{R}^n$ e os fundamentos da geometria	9
1. Pontos e retas em $\mathbb{R}^2$	9
2. A abordagem axiomática	10
3. O axioma das paralelas e a geometria não Euclidiana	12
4. Matrizes e transformações do plano	13
5. Exercícios	14
Capítulo 3. Produto interno	15
1. Definição	15
2. O Teorema de Cauchy-Buniakovskii-Schwarz	16
3. O produto interno. Ângulos, normas	16
4. Aplicações geométricas	17
5. Exercícios	18
Capítulo 4. Solução de equações afins, fatoração LU	21
1. Matrizes triangulares	21
2. Eliminação	22
3. Exemplos onde a eliminação falha	22
4. Exercícios	23
Capítulo 5. Grupos	25
1. Exemplos e definição	25
2. O grupo das permutações de n elementos	26
3. O grupo linear de $\mathbb{R}^n$	28
4. As matrizes de permutação	29
5. Exercícios	30
Capítulo 6. A fatoração PLU	33
1. Ação de grupo	33
2. Pivoteamento	34
3. Interpretação como ação de grupo	34
4. Matrizes não necessariamente quadradas	36
5. Exercícios	37
Capítulo 7. Espaços, subespaços e dimensão	39
1. Sub-espaços	39

2. A imagem de uma matriz	39
3. O núcleo de uma matriz	40
4. Independência linear	40
5. Bases e dimensão	41
6. Dimensão infinita	42
7. Exercícios	42
Capítulo 8. O Teorema do Posto	45
1. Matrizes em forma escada	45
2. Teorema do posto	47
3. Aplicação à matemática discreta	47
4. Exercícios	48
Capítulo 9. Determinante	51
1. Exemplos	51
2. Formas anti-simétricas	52
3. Funções multilineares anti-simétricas	53
4. Multiplicatividade do determinante	55
5. Cofatores	55
6. Volume e área	56
7. Exercícios	57
Capítulo 10. Autovalores e autovetores	61
1. Endomorfismos lineares	61
2. Ação de grupo	62
3. Solução dos exemplos	62
4. Definição	63
5. Autovalores complexos	64
6. Considerações adicionais	65
7. Exercícios	66
Capítulo 11. Mudanças de coordenadas	69
1. Vetores	69
2. Funções lineares	70
3. Transformações lineares	70
4. Funções bilineares	71
5. Exercícios	71
Capítulo 12. Equações diferenciais ordinárias	73
1. O circuito RLC	73
2. O significado dos autovalores complexos	75
3. Exercícios	76
Capítulo 13. O Grupo Ortogonal	79
1. O Grupo Ortogonal	79
2. O grupo Euclidiano	81
3. Como são feitos jogos e animações 3D	82
4. Exercícios	85
Capítulo 14. Projeções e como Aproximar Nuvens de Dados por Mínimos Quadrados	87
1. Projeções ortogonais	87
2. Mínimos quadrados	87
3. Simetrias	89
4. Esparsidade	89

5. Exercícios	92
Capítulo 15. O processo de Gram-Schmidt	93
1. Ortonormalização	93
2. A fatoração QR	93
3. Outra solução para o Problema de Mínimos Quadrados	94
4. Algoritmo para a decomposição QR	94
5. Exercícios	95
Capítulo 16. Matrizes simétricas e o teorema espectral	97
1. Matrizes simétricas e formas bilineares simétricas	97
2. O Teorema Espectral	97
3. Matrizes positivas e positivas definidas	98
4. Aplicação: máximos e mínimos	99
5. Exercícios	100
Capítulo 17. Aplicações lineares e valores singulares	101
1. A decomposição em valores singulares	101
2. Aplicações à mineração de dados	102
3. A pseudo-inversa	103
4. Exercícios	103
Capítulo 18. Covariância e carteiras de investimentos.	105
1. Variáveis aleatórias	105
2. Variáveis aleatórias contínuas	106
3. Covariância	107
4. Estatística multivariada	108
5. Covariância e o Teorema Espectral	109
6. Alocação de ativos	110
7. Exercícios	113
Capítulo 19. Matrizes de Márkov e Processos Estocásticos	115
1. Introdução	115
2. O raio espectral	118
3. Prova do Teorema de Perron-Frobenius	118
4. Processos Estocásticos	119
5. Exercícios	120
Capítulo 20. Grafos e Álgebra Linear	123
1. Introdução à teoria dos grafos	123
2. A Equação do Calor em grafos	124
3. As Leis de Kirchhoff	125
4. Ranqueamento de Page	127
5. Ranqueamento de Kleinberg	130
6. O <i>Hummingbird</i>	131
7. Exercícios	132
Capítulo 21. Álgebra linear com números complexos	135
1. Produto Interno Hermitiano	135
2. Bases ortonormais	136
3. Matrizes Unitárias e Hermitianas Simétricas	136
4. O Teorema Espectral	137
5. A forma normal de Schur	137
6. A exponencial de uma matriz	138
7. A Forma Normal de Jordan	140

8. Estabilidade do <i>Boeing 707</i>	140
9. Exercícios	142
Capítulo 22. Normas de matrizes	145
1. Norma de operador	145
2. Ação de Grupo	146
3. Norma de transformações lineares	148
4. Séries e matrizes	148
5. Exercícios	151
Capítulo 23. Polinômios pérfidos e matrizes mal postas	153
1. Perfídia	153
2. Ponto flutuante	155
3. Condicionamento	156
4. Exercícios	158
Capítulo 24. Processamento de sinais, <i>MP3</i> , <i>JPEG</i> e <i>MPEG</i>	161
1. Sinais sonoros	161
2. A transformada de Fourier	162
3. A base de Haar	164
4. O ouvido humano e a transformada de ondeletas	166
5. O padrão <i>MP3</i> e os CODECs	167
6. Compressão de imagem e de vídeo	169
7. A televisão digital.	170
8. Conclusões	170
9. Exercícios	171
Nota computacional	172
Capítulo 25. Tensores	173
1. Introdução	173
2. Coordenadas	174
3. A decomposição poliádica canônica	175
4. O posto limítrofe	177
5. Trens de tensores e decomposição de Tucker	179
6. Exercícios	180
Capítulo 26. Transformada rápida de Fourier, e como multiplicar números inteiros rápido	181
1. Polinômios e transformada de Fourier.	181
2. Transformada rápida de Fourier	182
3. A multiplicação rápida de polinômios	183
4. A multiplicação rápida de inteiros	184
5. O computador quântico	186
6. Exercícios	187
Apêndice A. Referências comentadas	189
1. Alguns outros livros de Álgebra Linear	189
2. Ferramentas de referência na internet	189
3. Recursos computacionais	190
Apêndice. Índice de Notações	191
Apêndice. Índice Remissivo	193

CAPÍTULO 1

Espaços lineares, equações afins

1. Exemplos de grandezas lineares



Álgebra Linear é a área da Matemática que trata do estudo de grandezas aditivas ou 'lineares', e das relações entre elas. Alguns exemplos de grandezas lineares são:

Velocidades: No mundo descrito pela mecânica clássica, faz sentido somar e subtrair velocidades. Se X e Y são objetos se deslocando em um referencial R , então a velocidade de X em relação a R acrescida da velocidade de Y em relação a X é a velocidade de Y em relação ao referencial R . Se a velocidade de X em relação a R é zero, isso é interpretado como o fato do objeto X estar em repouso no referencial R .

A soma das **forças** exercidas sobre um objeto é chamada de resultante das forças. A segunda Lei de Newton iguala a aceleração desse objeto, vezes a sua massa, à resultante das forças.

Sinais sonoros também podem ser somados. Interpretamos a soma de sinais sonoros como a superposição desses sinais. Gravações antigas têm ruído, que assimilamos a um sinal. Um problema relevante é como 'remasterizar' gravações antigas, subtraindo o ruído. (Ver Capítulo 24)

Ondas na água (Fig.1) podem se sobrepor e produzir diagramas de interferência. A soma corresponde à superposição das ondas.

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.



FIGURA 1. A imagem mostra a superposição de ondas na água, provenientes de duas direções diferentes.

O mesmo fenômeno pode acontecer com sinais luminosos. **Seções do campo eletro-magnético** podem ser somadas e, em certos casos, assimiladas a uma onda. No entanto, a cada ponto do espaço-tempo, precisamos de 6 números para descrever o campo eletro-magnético em um ponto. Já um número basta para descrever a amplitude de uma onda no mar em um ponto.

Na mecânica quântica, a **função de onda** de uma partícula é uma grandeza linear complexa. O quadrado do módulo da função de onda em um ponto costuma ser interpretado como a densidade de probabilidade da “partícula se encontrar nesse ponto”. Diferentemente das ondas no mar, faz sentido físico multiplicar uma função de onda por um número complexo.

Também podemos achar exemplos de grandezas lineares nas atividades humanas. O **estoque** de uma loja ou supermercado é uma grandeza linear. **Metas de produção industrial** assim como os **insumos necessários** são grandezas lineares. **Carteiras de investimento** são grandezas lineares. A soma de duas carteiras corresponde à carteira obtida juntando os ativos.

Uma classe grande de objetos matemáticos se prestam a ser tratados como grandezas lineares. Por exemplo, **polinômios de grau menor ou igual a d** também podem ser somados e subtraídos, e obteremos outros polinômios de grau menor ou igual a d .

Funções a valores reais formam um espaço linear. O mesmo vale para as **funções contínuas**, as **funções diferenciáveis**, as **funções de classe C^k** , etc...

2. Espaços vetoriais

É conveniente definir um objeto matemático que abstrai as principais propriedades das grandezas lineares ou aditivas.

Definição 1.1. Um *espaço vetorial real* $(E, +, \cdot)$ é um conjunto E , com uma operação interna de *soma*

$$\begin{aligned} + : E \times E &\rightarrow E \\ (\mathbf{u}, \mathbf{v}) &\mapsto \mathbf{u} + \mathbf{v} \end{aligned}$$

e uma operação de *multiplicação por um número real*

$$\begin{aligned} \cdot : \mathbb{R} \times E &\rightarrow E \\ (\lambda, \mathbf{u}) &\mapsto \lambda \cdot \mathbf{u} . \end{aligned}$$

Elas devem satisfazer as seguintes propriedades:

- [EV1] Comutatividade da soma: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
- [EV2] Associatividade da soma: $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$.
- [EV3] Elemento neutro para a soma: existe $\mathbf{0} \in E$ tal que, para todo $\mathbf{u} \in E$, $\mathbf{0} + \mathbf{u} = \mathbf{u} + \mathbf{0} = \mathbf{u}$.
- [EV4] Elemento inverso para a soma: para todo $\mathbf{u} \in E$, existe $(-\mathbf{u}) \in E$ tal que $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.
- [EV5] Distributividade da multiplicação em relação à soma vetorial: para todos $\mathbf{u}, \mathbf{v} \in E$, $\lambda \in \mathbb{R}$, $\lambda \cdot (\mathbf{u} + \mathbf{v}) = \lambda \cdot \mathbf{u} + \lambda \cdot \mathbf{v}$.
- [EV6] Distributividade da soma escalar (real) em relação ao produto: para todos $\mathbf{u} \in E$, $\lambda, \mu \in \mathbb{R}$, $(\lambda + \mu) \cdot \mathbf{u} = \lambda \cdot \mathbf{u} + \mu \cdot \mathbf{u}$.
- [EV7] Compatibilidade da multiplicação real e da multiplicação real-vetor: para todos $\mathbf{u} \in E$, $\lambda, \mu \in \mathbb{R}$, $(\lambda\mu) \cdot \mathbf{u} = \lambda \cdot (\mu \cdot \mathbf{u})$.
- [EV8] A identidade da multiplicação por escalar corresponde a identidade da multiplicação real-vetor: para todo $\mathbf{u} \in E$, $1 \cdot \mathbf{u} = \mathbf{u}$.

Aviso: Quando as operações de soma e de multiplicação estiverem claras no contexto, vamos nos referir simplesmente ao 'espaço vetorial' E , entendendo assim não como o conjunto E , mas sim como o espaço vetorial $(E, +, \cdot)$.

Exemplo 1.2. O espaço $(\mathbb{R}, +, \cdot)$, onde $+$ e $\cdot$ são a soma e a multiplicação usuais, é um espaço vetorial real.

Exemplo 1.3. O espaço $(\mathbb{C}, +, \cdot)$, onde $+$ e $\cdot$ são a soma complexa e a multiplicação de um real por um complexo, é também um espaço vetorial real.

Exemplo 1.4. O espaço $(\mathbb{Q}, +, \cdot)$, onde $+$ e $\cdot$ são a soma e a multiplicação usuais, **não** é um espaço vetorial real. Porquê?

Exemplo 1.5. O espaço $(\mathbb{R}^n, +, \cdot)$ é definido como o produto

$$\underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ vezes}}$$

com soma e multiplicação definidas por

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{bmatrix} \quad \text{e} \quad \lambda \cdot \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} \lambda u_1 \\ \lambda u_2 \\ \vdots \\ \lambda u_n \end{bmatrix}.$$

O espaço $(\mathbb{R}^n, +, \cdot)$ é um espaço vetorial real.

Nota: usamos a mesma notação para o conjunto $\mathbb{R}^n$ e para o espaço vetorial $(\mathbb{R}^n, +, \cdot)$. Mas quando nos referimos a pontos do conjunto $\mathbb{R}^n$, escrevemos as coordenadas separadas por vírgulas: $\mathbf{x} = (x_1, \dots, x_n)$. Quando nos referimos a vetores, escrevemos as coordenadas uma em cima da outra. Usaremos também a seguinte notação:

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad \mathbf{e}_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

Definição 1.6. Uma *combinação linear real* dos vetores $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_s \in \mathbb{R}^n$ é um vetor da forma:

$$\mathbf{u} = \lambda_1 \cdot \mathbf{u}_1 + \lambda_2 \cdot \mathbf{u}_2 + \cdots + \lambda_s \cdot \mathbf{u}_s,$$

onde $\lambda_1, \dots, \lambda_s \in \mathbb{R}$.

O seguinte resultado é trivial:

Lema 1.7. *Todo vetor $\mathbf{x} \in \mathbb{R}^n$ se escreve de maneira única como combinação linear dos vetores $\mathbf{e}_i$:*

$$\mathbf{x} = x_1 \cdot \mathbf{e}_1 + x_2 \cdot \mathbf{e}_2 + \cdots + x_n \cdot \mathbf{e}_n.$$

A n -upla de vetores $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ é chamada de *base canônica* de $\mathbb{R}^n$. Os coeficientes x_i são chamados de *coordenadas* do vetor $\mathbf{x}$.

3. Aplicações lineares

A seguir, vamos descrever as aplicações (funções) entre espaços vetoriais, que preservam a estrutura linear.

Definição 1.8. Sejam E e F espaços vetoriais reais. Uma *aplicação linear* (ou *morfismo*) de E em F é uma função

$$\begin{aligned} A : E &\rightarrow F \\ \mathbf{u} &\mapsto A(\mathbf{u}) \end{aligned}$$

tal que $A(\mathbf{u} + \mathbf{v}) = A(\mathbf{u}) + A(\mathbf{v})$, e $A(\lambda \cdot \mathbf{u}) = \lambda \cdot (A\mathbf{u})$.

Uma aplicação linear de um espaço E no mesmo espaço E é chamada de *transformação linear* ou *endomorfismo*.

Exemplo 1.9. A aplicação $(x, y) \mapsto x + 5y$ é linear. As aplicações $(x, y) \mapsto x + 5y + 1$ e $x^2 + 5y$ não são lineares.

Denotamos por $L(E, F)$ o conjunto das aplicações lineares de E em F . Se $A, B \in L(E, F)$ e $\lambda \in \mathbb{R}$, definimos

$$\begin{aligned} A + B : E &\rightarrow F \\ \mathbf{u} &\mapsto A\mathbf{u} + B\mathbf{u} \end{aligned}$$

e

$$\begin{aligned} \lambda \cdot A : E &\rightarrow F \\ \mathbf{u} &\mapsto \lambda \cdot (A\mathbf{u}). \end{aligned}$$

Com essas definições, $L(E, F)$ é um espaço vetorial real.

Lema 1.10. Seja $A \in L(\mathbb{R}^n, \mathbb{R}^m)$. Então existem coeficientes A_{ij} , $1 \leq i \leq m$, $1 \leq j \leq n$, determinados de maneira única e tais que

$$A\mathbf{e}_j = \sum_{i=1}^m A_{ij}\mathbf{e}_i.$$

Representamos a transformação linear $A \in L(\mathbb{R}^n, \mathbb{R}^m)$ pela matriz:

$$A = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & & \vdots \\ A_{m1} & A_{m2} & \dots & A_{mn} \end{bmatrix}.$$

Com essa notação,

$$\begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & & \vdots \\ A_{m1} & A_{m2} & \dots & A_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n A_{1j}x_j \\ \sum_{j=1}^n A_{2j}x_j \\ \vdots \\ \sum_{j=1}^n A_{mj}x_j \end{bmatrix}.$$

Existe outra operação natural entre aplicações lineares: se $A \in L(F, G)$ e $B \in L(E, F)$, então definimos a composta de A e B por:

$$\begin{aligned} A \circ B : E &\rightarrow G \\ \mathbf{u} &\mapsto (A \circ B)(\mathbf{u}) = A(B(\mathbf{u})). \end{aligned}$$

A composta $A \circ B$ é portanto um elemento de $L(E, G)$. Em particular, se $E = F = G$, então A , B e $A \circ B$ são transformações lineares de E .

Lema 1.11. Sejam $A \in L(\mathbb{R}^m, \mathbb{R}^l)$, $B \in L(\mathbb{R}^n, \mathbb{R}^m)$ e $C = A \circ B \in L(\mathbb{R}^n, \mathbb{R}^l)$. Nesse caso, os coeficientes da matriz de C são relacionados aos das matrizes de A e B por:

$$C_{ik} = \sum_{j=1}^m A_{ij} B_{jk}.$$

Em termos matriciais, a fórmula acima define uma operação entre matrizes $l \times m$ e matrizes $m \times n$, conhecida como *multiplicação matricial*.

A transformação linear $I \in L(E, E)$ tal que $I(\mathbf{u}) = \mathbf{u}$ é chamada de transformação *identidade*. Ela tem a propriedade de que $A \circ I = I \circ A = A$ para toda $A \in L(E, E)$. Os coeficientes da identidade $I \in L(\mathbb{R}^n, \mathbb{R}^n)$ são:

$$I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Seja $A \in L(E, F)$. Uma aplicação $B \in L(F, E)$ é uma *inversa à direita* de A se e somente se $A \circ B = I \in L(F, F)$. Uma aplicação $C \in L(F, E)$ é uma *inversa à esquerda* se e somente se $CA = I \in L(E, E)$. Um *isomorfismo linear* é uma aplicação linear $A \in L(E, F)$ com inversa à esquerda e à direita. Quando A é um isomorfismo de E em E , dizemos que A é um *automorfismo linear*.

4. Sistemas de equações: três visões diferentes

Agora consideramos o seguinte problema: os coeficientes $A_{11}, A_{12}, A_{21}, A_{22}$ são dados, assim como os coeficientes b_1 e b_2 . Queremos descrever o conjunto dos reais x_1 e x_2 satisfazendo

$$(1) \quad \begin{cases} A_{11}x_1 + A_{12}x_2 = b_1 \\ A_{21}x_1 + A_{22}x_2 = b_2. \end{cases}$$

Podemos interpretar cada **linha** do sistema (1) como uma reta no plano. Nesse caso, resolver o problema equivale a achar a interseção dessas duas retas. Introduzindo os vetores

$$\mathbf{a}_1 = \begin{bmatrix} A_{11} \\ A_{21} \end{bmatrix}, \mathbf{a}_2 = \begin{bmatrix} A_{12} \\ A_{22} \end{bmatrix} \text{ e } \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix},$$

podemos escrever o sistema acima como

$$x_1 \cdot \mathbf{a}_1 + x_2 \cdot \mathbf{a}_2 = \mathbf{b},$$

de modo que resolver o problema (1) equivale a escrever o vetor $\mathbf{b}$ como combinação linear dos vetores $\mathbf{a}_1$ e $\mathbf{a}_2$, ou seja das **colunas** de A .

Finalmente, podemos considerar a aplicação linear representada pela matriz $A = L(\mathbb{R}^2, \mathbb{R}^2)$ com coeficientes A_{ij} :

$$A\mathbf{x} = \mathbf{b}.$$

Nesse caso, resolver o problema (1) equivale a achar o conjunto das pré-imagens de $\mathbf{b}$ por A .

Assumindo que A_{11} seja diferente de zero, podemos resolver o sistema (1) subtraindo da segunda linha um múltiplo da primeira:

$$(2) \quad \begin{cases} A_{11}x_1 + A_{12}x_2 = b_1 \\ \left(A_{22} - \frac{A_{12}A_{21}}{A_{11}}\right)x_2 = b_2 - \frac{b_1A_{21}}{A_{11}}, \end{cases}$$

e depois resolver para x_2 (se for possível) e para x_1 .

Na interpretação das linhas, substituímos a segunda reta por uma reta horizontal, preservando a interseção. Na interpretação vetorial, substituímos a equação original por

$$x_1(\mathbf{e}_1 A_{11}) + x_2 \mathbf{a}'_2 = \mathbf{b}',$$

onde $\mathbf{a}'_2$ e $\mathbf{b}'$ foram obtidos a partir de $\mathbf{a}_2$ e $\mathbf{b}$ subtraindo um múltiplo conveniente de $\mathbf{e}_2$.

Finalmente, podemos interpretar o sistema (1) como uma composição:

$$\begin{bmatrix} 1 & 0 \\ \frac{A_{21}}{A_{11}} & 1 \end{bmatrix} \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} - \frac{A_{12}A_{21}}{A_{11}} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}.$$

Esta formulação permite resolver o problema (1) com três multiplicações, três divisões e três subtrações:

$$\begin{aligned} t_1 &\leftarrow \frac{A_{21}}{A_{11}}, \\ t_2 &\leftarrow b_2 - b_1 t_1, \\ t_3 &\leftarrow A_{22} - A_{12} t_1, \\ x_2 &\leftarrow \frac{t_2}{t_3}, \\ x_1 &\leftarrow \frac{b_1 - A_{12} x_2}{A_{11}}. \end{aligned}$$

Uma maneira de avaliar o custo ou complexidade de algoritmos numéricos é contar o número de multiplicações e divisões, e ignorar o custo das somas, subtrações e comparações. Esse modelo se justifica pelo fato das multiplicações e divisões serem mais onerosas, tanto para um humano trabalhando no papel quanto para um circuito dedicado¹.

Na última visão apresentada o custo de se resolver (1) é 6. Isso é mais barato do que a famosa *regra de Cramer*,

$$x_1 = \frac{b_1 A_{22} - b_2 A_{12}}{A_{11} A_{22} - A_{21} A_{12}}, \quad x_2 = \frac{A_{11} b_2 - A_{21} b_1}{A_{11} A_{22} - A_{21} A_{12}},$$

que custa 8 (os denominadores são iguais). A regra de Cramer é uma maneira ruim de se resolver sistemas de duas equações a duas incógnitas. Vamos ver no Exercício 9.7 que aplicar a regra de Cramer para sistemas maiores é uma **péssima** ideia.

5. Exercícios

Exercício 1.1. Seja $(E, +, \cdot)$ um espaço vetorial real. Seja E^* o conjunto das aplicações lineares de $(E, +, \cdot)$ em $(\mathbb{R}, +, \cdot)$. Mostre que $(E^*, +, \cdot)$ é um espaço vetorial real.

Exercício 1.2. Sejam $(E, +, \cdot)$ e $(F, +, \cdot)$ espaços vetoriais. Definimos agora um espaço abstrato G como o menor espaço contendo todas as combinações lineares

$$a_1 \otimes u_1 + a_2 \otimes u_2 + \cdots + a_k \otimes u_k,$$

onde $k \in \mathbb{N}_0$, $a_j \in E$, $u_j \in F$, e o símbolo $\otimes$ satisfaz às seguintes regras:

$$(1) \quad (a + b) \otimes u = a \otimes u + b \otimes u$$

¹Antigamente eu afirmava isso também para o computador. Hoje em dia, o custo de transferir informação do processador para a memória pode ser maior do que o de fazer contas. Ainda assim, esse modelo permanece útil quando estamos interessados no custo assintótico, para entradas suficientemente grandes.

- (2) $a \otimes (u + v) = a \otimes u + a \otimes v$
 (3) $(\lambda a) \otimes u = a \otimes (\lambda u)$
 (4) A soma de expressões $a \otimes u$ é comutativa.

Mostre que G é um espaço vetorial, e que não é igual necessariamente a $E \times F$. O espaço G é chamado de *produto tensorial* dos espaços E e F , e denotado por $G = E \otimes F$.

Exercício 1.3. Mostre, para $E = \mathbb{R}^n$ e $F = \mathbb{R}^m$, que $L(E, F) = F \otimes E^*$. Interprete esse resultado em termos de operações com matrizes.

Exercício 1.4. Mostre que o espaço das funções integráveis de $\mathbb{R}$ em $\mathbb{R}$ é um espaço vetorial. Utilize a definição de integral que você viu no curso de Cálculo (ou abra outro livro de Cálculo).

Exercício 1.5. O espaço $L^2(\mathbb{R})$ é o espaço das funções integráveis em $\mathbb{R}$, cujo quadrado também é integrável. Estritamente falando, o espaço $L^2(\mathbb{R})$ é definido usando integral de Lebesgue. Além disso, identifica-se duas funções sempre que a integral do quadrado da diferença se anula. A construção rigorosa deste tipo de integral não é relevante neste livro. Mostre que $L^2(\mathbb{R})$ é um espaço vetorial. Se você quiser, pode resolver o exercício para o espaço de funções deriváveis e a derivada contínua que estão em $L^2(\mathbb{R})$.

Exercício 1.6. Mostre que, se uma aplicação linear $A \in L(E, E)$ tem inversas à esquerda e à direita, então essas inversas são iguais. Deduza que, se A tem inversa à esquerda e à direita, então a inversa é única.

Exercício 1.7. Encontre um exemplo de $A \in L(\mathbb{R}^2, \mathbb{R}^1)$ com duas inversas diferentes à direita e nenhuma inversa à esquerda.

Exercício 1.8 (Multiplicação por blocos). Mostre que, se A, B, C, D, E, F, G, H são matrizes $n \times n$, então:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \begin{bmatrix} AE + BG & AF + BH \\ CE + DG & CF + DH \end{bmatrix}.$$

Exercício 1.9 (Multiplicação de Strassen). Mostre que, se $A, B, C, D, E, F, G, H, J, K, L, M$ são matrizes $n \times n$, e

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \begin{bmatrix} J & K \\ L & M \end{bmatrix},$$

então J, K, L e M podem ser calculadas pela seguinte recorrência (complete os espaços):

$$\begin{aligned} N &= (A + D)(E + H) \\ P &= (C + D)E \\ Q &= A(F - H) \\ R &= D(G - E) \\ S &= (A + B)H \\ T &= (C - A)(E + F) \\ U &= (B - D)(G + H) \\ J &= _ + _ - _ + _ \\ K &= _ + _ \\ L &= _ + _ \\ M &= _ - _ + _ + _. \end{aligned}$$

Exercício 1.10 (Complexidade da multiplicação matricial). Usando a multiplicação de Strassen, mostre que existe um algoritmo para multiplicar matrizes $n \times n$ usando no máximo $(2n)^{\log_2 7}$ multiplicações de números reais. (As somas são de graça).

Problema em aberto N^o 1. Achar ou estimar ω , definido como o menor número real tal que, para todo $\epsilon > 0$, existe um algoritmo para multiplicar matrizes $n \times n$ usando no máximo $n^{\omega+\epsilon}$ multiplicações. O valor de ω não é conhecido. Sabe-se que $\omega \geq 2$. Strassen² mostrou que $\omega \leq \log_2 7 \simeq 2.807 \dots$. Depois do trabalho pioneiro de Strassen (1969), a cota para ω foi reduzida sucessivas vezes³. Hoje a cota $\omega < 2.3728639 \dots$, devida a Le Gall (2014) é a melhor conhecida.

²Volker Strassen: Gaussian elimination is not optimal. *Numerische Mathematik* **13** pp 354-356 (1969).

³Para mais detalhes, ver: Victor Pan, *How to multiply matrices faster*. Lecture Notes in Computer Science **179**, Springer-Verlag, Berlin (1984). Outra referência é o capítulo sobre álgebra linear rápida em: Joachim von zur Gathen e Jürgen Gerhard, *Modern computer algebra*. Second edition. Cambridge University Press, Cambridge (2003).

CAPÍTULO 2

O espaço $\mathbb{R}^n$ e os fundamentos da geometria

1. Pontos e retas em $\mathbb{R}^2$



Euclides de Alexandria escreveu no século 3 AC:

Definições

- I Um *ponto* é aquilo que não tem partes.
- II Uma *linha* é comprimento sem largura.
- III As extremidades de uma linha (segmento) são pontos.
- IV Uma *linha reta* (segmento) é aquilo que está contido entre dois pontos. (...)

Postulados

- I Uma linha reta (segmento) sempre pode ser traçada entre dois pontos.
- II Uma linha finita (segmento) sempre pode ser prolongada até qualquer comprimento finito.

Euclides, Livro I dos *Elementos*.

Por 22 séculos, os Elementos de Euclides garantiam alicerce sólido para a geometria. Nenhuma obra científica foi considerada atual por período tão extenso. Mesmo se não entendemos ao certo o que é um ponto ou um segmento, uma vez admitidas ou *postuladas* as poucas noções fundamentais podemos reconhecer o restante da obra (Teoremas, Proposições, Lemas) como consequência dessas definições e postulados.

Foi apenas durante o século XIX que uma exigência maior de rigor e um escrutínio mais preciso das noções fundamentais tornaram necessária uma intervenção nos fundamentos da geometria. Uma das abordagens modernas consiste em construir um *modelo* para a geometria Euclidiana. É o que vamos fazer a seguir, parcialmente, a partir da noção de números reais e da teoria de conjuntos.

É importante ressaltar que os antigos não conheciam os números reais. Euclides tratava números racionais e comprimentos de maneira diferente, podendo dois comprimentos serem comensuráveis ou não.

Definição 2.1. Um *ponto* do plano é um elemento de $\mathbb{R}^2$. Um ponto do espaço é um elemento de $\mathbb{R}^3$.

Agora que sabemos exatamente o que é um ponto, podemos definir diretamente segmentos de reta por:

Definição 2.2. Um *segmento de reta* no plano é um conjunto da forma

$$[A, B] = \{((1-t)a_1 + tb_1, (1-t)a_2 + tb_2) : 0 \leq t \leq 1\},$$

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.

onde $(a_1, a_2) \neq (b_1, b_2)$. Um *segmento de reta* no espaço é um conjunto da forma

$$[A, B] = \{((1-t)a_1 + tb_1, (1-t)a_2 + tb_2, (1-t)a_3 + tb_3) : 0 \leq t \leq 1\},$$

onde $(a_1, a_2, a_3) \neq (b_1, b_2, b_3)$.

Uma maneira alternativa de escrever a mesma fórmula, utilizando notação vetorial, é:

$$[A, B] = \left\{ \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + t \begin{bmatrix} b_1 - a_1 \\ b_2 - a_2 \end{bmatrix} : t \in [0, 1] \right\},$$

sendo o caso espacial análogo.

O primeiro postulado de Euclides é consequência direta da definição. O segundo postulado segue de uma manipulação algébrica simples, desde que tenhamos uma noção de distância.

Definição 2.3. A distância entre $A = (a_1, a_2)$ e $B = (b_1, b_2)$ é

$$d(A, B) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}.$$

A existência da raiz quadrada decorre do Teorema do Valor Intermediário, que por sua vez depende da construção dos números reais (propriedade do ínfimo).

Definição 2.4. O *círculo* de centro (a_1, a_2) e raio $R > 0$ é o conjunto $\{(x_1, x_2) \in \mathbb{R}^2 : d((x_1, x_2), (a_1, a_2)) = R\}$.

Euclides não define *retas* diretamente, a noção de infinito sendo pouco intuitiva. Ele prefere poder prolongar segmentos infinitamente. Da forma alternativa para definição de segmento, podemos deduzir que os pontos X tais que $[AX]$ prolonga $[AB]$ são aqueles da forma $\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + t \begin{bmatrix} b_1 - a_1 \\ b_2 - a_2 \end{bmatrix}$ com $t > 0$. Similarmente, aqueles tais que $[BX]$ prolonga $[AB]$ são aqueles com $t < 0$. A *equação paramétrica* da reta (AB) é portanto

$$(AB) = \{X : \overrightarrow{AX} = t\overrightarrow{AB} : t \in \mathbb{R}\},$$

onde a notação $\overrightarrow{AX}$ denota $\begin{bmatrix} x_1 - a_1 \\ x_2 - a_2 \end{bmatrix}$.

Essa formulação tem a desvantagem de depender de um parâmetro t . Se dado um ponto $X = (x_1, x_2)$ queremos decidir se $X \in (AB)$, precisamos resolver simultaneamente $(x_1 - a_1) = t(b_1 - a_1)$ e $(x_2 - a_2) = t(b_2 - a_2)$. Isso é possível se e somente se $(b_2 - a_2)(x_1 - a_1) = (b_1 - a_1)(x_2 - a_2)$, ou seja:

$$(b_2 - a_2)x_1 - (b_1 - a_1)x_2 + ((b_2 - a_2)a_1 - (b_1 - a_1)a_2) = 0,$$

que é chamada de *equação implícita* ou *analítica* da reta.

Perguntas: Quais são as equações da forma $Ax_1 + Bx_2 + C = 0$ que representam retas? Quando é que duas equações da forma $Ax_1 + Bx_2 + C = 0$ e $A'x_1 + B'x_2 + C' = 0$ representam a mesma reta?

2. A abordagem axiomática

Outra abordagem moderna para os fundamentos da geometria consiste em explicitar axiomáticamente a relação entre objetos (pontos, retas, círculos, etc...) independente de sua eventual *natureza*, reestruturando assim a apresentação de

Euclides. David Hilbert¹ dividiu os axiomas da geometria em cinco grupos: incidência, ordem, congruência, paralelas, continuidade.

O objetivo desta seção é mostrar por meio de um exemplo o que se entende ou *entendia* como **prova geométrica**. Seguimos a apresentação de Hilbert, mas omitiremos os axiomas relativos à geometria espacial, além dos de congruência e continuidade.

Assume-se a existência de duas classes de objetos. Pontos são denotados por A, B , etc..., e retas por a, b, c , etc... Vamos assumir a existência de uma relação entre pontos e retas. Uma reta pode *conter* um ponto. A relação *conter* satisfaz aos seguintes **axiomas de incidência**:

Axioma 1. *Dados dois pontos distintos A e B , existe uma reta contendo os pontos A e B .*

Axioma 2. *Dados dois pontos distintos A e B , existe no máximo uma reta contendo os pontos A e B .*

Axioma 3. *Existem pelo menos dois pontos contidos em uma reta. Existem pelo menos três pontos não contidos na mesma reta.*

Também postulamos a existência de uma relação, que se aplica a três pontos contidos na mesma reta. É a relação *entre*, que satisfaz aos seguintes axiomas de ordem:

Axioma 4. *Se o ponto B está entre os pontos A e C , então A, B e C são pontos distintos de uma reta, e B está entre C e A .*

Axioma 5. *Para todo par de pontos B e C , existe um ponto A tal que B está entre A e C .*

Axioma 6. *De três pontos, no máximo um deles está entre os outros dois.*

Axioma 7. *Se*

- (1) A, B, C são três pontos não contidos na mesma linha,
- (2) a é uma linha que não contém A, B ou C , e
- (3) A linha a contém um ponto entre A e B ,

então vale uma das seguintes alternativas: a linha a contém um ponto entre A e C , ou a linha a contém um ponto entre B e C .

No caso do item (3), dizemos que a *corta* o segmento AB .

Podemos agora mostrar o Teorema a seguir, a partir dos axiomas acima.

Teorema 2.5. *De cada três pontos A, B e C contidos em uma mesma linha a , e distintos dois a dois, existe um que está entre os dois outros.*

DEMONSTRAÇÃO. (Veja a Fig. 1). Vamos assumir que A não está entre B e C , e que C não está entre A e B . Precisamos mostrar que B está entre A e C .

- (1) Existe um ponto D que não está contido em a . Caso contrário, todos os pontos estariam contidos em a , em contradição ao Axioma 3.
- (2) Pelo Axioma 5, podemos escolher um ponto G tal que D está entre B e G .

¹As notas de Hilbert foram escritas entre 1891 e 1902 e só foram publicadas depois da morte do autor. Traduções para o inglês estão disponíveis: David Hilbert, *Foundations of geometry*, 2ª ed., traduzida da décima edição em alemão por Leo Unger. Open Court, La Salle, Ill (1971).

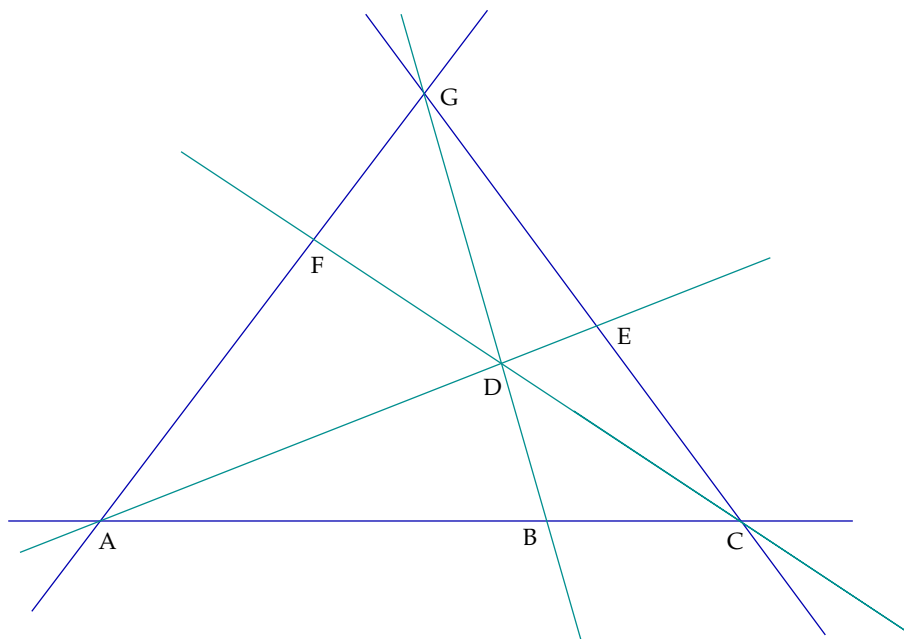


FIGURA 1. Prova do Teorema 2.5.

- (3) Vamos mostrar que a linha (AD) corta o segmento CG em um ponto que chamaremos de E . (A notação (AD) significa a linha contendo A e D . Ela existe devido ao Axioma 1). Para isso, aplicamos o Axioma 7 à tripla B, C, G e à reta (AD) . Deduzimos que (AD) corta o segmento CG ou corta o segmento BC . Mas se tivéssemos um ponto E de (AD) entre B e C , então ele pertenceria às linhas (AD) e $(BC) = (AC) = a$. Pelo Axioma 2, só pode existir uma linha contendo A e E . Logo D está contido em a , contradizendo o item (1).
- (4) A linha (CD) corta o segmento AG em F . (Mesmo argumento, com o Axioma 7 aplicado à tripla B, A, G e à reta (CD)).
- (5) O ponto D está entre A e E . (Axioma 7 aplicado à tripla A, E, G e à reta (CF)).
- (6) O ponto B está entre A e C . (Axioma 7 aplicado à tripla A, E, C e à reta (BG)).

□

3. O axioma das paralelas e a geometria não Euclidiana

Definição 2.6. Duas retas em um mesmo plano são *paralelas* se e somente se elas não têm interseção.

Axioma 8. Se um ponto A não pertence à reta b , então existe uma e uma só reta paralela a b passando por A .

Este é o famoso axioma das paralelas. Ao contrário dos outros axiomas, esse não parece ser absolutamente intuitivo. Por séculos, tentou-se mostrar que ele seria consequência dos outros axiomas.

Por volta de 1823, Nicolai Ivánovich Lobatchevskii assumiu que o axioma era falso, e ao investigar as consequências produziu uma geometria onde todos os outros axiomas eram válidos.

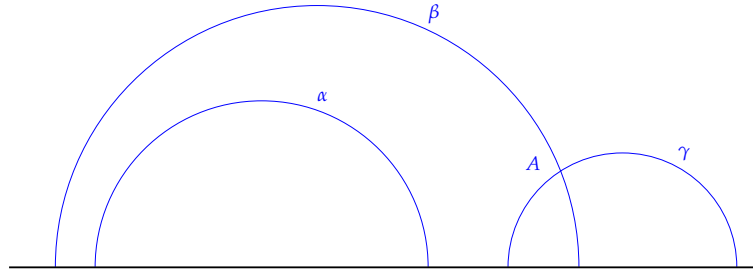


FIGURA 2. Plano de Poincaré: a "reta" α tem mais de uma "paralela" (β e γ) passando pelo ponto A .

Um exemplo de geometria não-Euclidiana é dada pelo *Plano de Poincaré* (Fig. 2). Os pontos desse plano são os elementos $(x, y) \in \mathbb{R} \times \mathbb{R}^+$. As retas são os semicírculos centrados em um ponto do eixo dos x , ao lado das semirretas verticais (semicírculos no infinito). Com essa definição, valem todos os outros axiomas, porém o axioma das paralelas falha.

4. Matrizes e transformações do plano

Definição 2.7. Dois triângulos A, B, C e A', B', C' são similares se e somente se

$$\frac{AB}{A'B'} = \frac{BC}{B'C'} = \frac{CA}{C'A'}.$$

Definição 2.8. Uma *similaridade* f é uma transformação do plano tal que existe um valor fixo $\lambda \in \mathbb{R}^+$ e, para todo par D, E , escrevendo $D' = f(D)$ e $E' = f(E)$, temos:

$$D'E' = \lambda DE.$$

Exemplos de similaridades são rotações, simetrias, homotetias, translações.

Vamos mostrar o seguinte Lema no contexto da geometria analítica (a prova a partir dos axiomas de Hilbert pode ser mais complicada, e exige pelo menos os axiomas de congruência, que não estão enunciados ao longo de texto).

Lema 2.9. Os triângulos A, B, C e A', B', C' são similares se e somente se existe uma similaridade levando A em A' , B em B' e C em C' .

DEMONSTRAÇÃO. Precisamos mostrar duas coisas. A prova da suficiência (o se) é fácil e deixada para o leitor. Para a necessidade (o somente se), vamos construir essa similaridade.

Em primeiro lugar, se $A = A' = O$, e se $AB = A'B'$, então podemos levar (A, B, C) em (A', B', C') por uma rotação ou simetria (verificar). Depois, se $A'B' = \lambda AB$, podemos levar (A, B, C) em (A', B', C') compondo uma rotação ou simetria com a homotetia de coeficiente λ .

Em geral, triângulos não têm um ponto na origem. Mas podemos levar o triângulo (A, B, C) em um triângulo similar com ponto na origem por uma translação. Podemos levar a origem em A' por outra translação. Assim, para levar (A, B, C) em (A', B', C') , podemos compor uma translação, uma rotação ou simetria, e outra translação. A propriedade que estamos utilizando para deduzir o Lema é que a composta de duas similaridades é também uma similaridade. $\square$

Conjuntos G de transformações com essa propriedade (a composta pertence a esse conjunto) e mais duas (a identidade pertence a G , e para toda $g \in G$ a sua inversa $g^{-1} \in G$) são chamados de *grupos*.

A noção de grupo permite unificar o tratamento de todas as *geometrias* (Euclidiana, não-Euclidiana, projetiva) que proliferaram desde o século XIX. Estudam-se objetos geométricos, equiparando-os quando podem ser transformados um no outro por meio de uma transformação do grupo. Isso dá lugar ao moderno conceito de *simetria*.

Por exemplo, na Teoria da Relatividade, leis ou grandezas “físicas” precisam ser invariantes por um certo grupo (de Lorentz ou de Poincaré).

5. Exercícios

Utilize formulações matriciais ou vetoriais sempre que for possível.

Exercício 2.1. Prove (usando geometria analítica) a Proposição I do Livro I dos Elementos: *dado um segmento, é possível construir um triângulo equilátero tendo esse segmento como lado*. Depois, consulte uma tradução dos Elementos. Você acredita na prova de Euclides?

Exercício 2.2. Quais são as equações implícitas da reta (no espaço) passando pelos pontos A e B ?

Exercício 2.3. Quando é que dois conjuntos de equações implícitas em $\mathbb{R}^3$ representam a mesma reta em $\mathbb{R}^3$?

Exercício 2.4. Qual é a equação implícita do plano (no espaço) passando pelos pontos A , B e C ? (Assuma esses pontos não alinhados.)

Exercício 2.5. Quando duas equações representam o mesmo plano?

Exercício 2.6. Prove o Teorema 2.5 utilizando geometria analítica.

Exercício 2.7. Com régua e compasso, ilustre a prova geométrica (axiomática) do Teorema 2.5 no plano de Poincaré.

Exercício 2.8. Mostre a validade dos axiomas de incidência e de ordem no plano $\mathbb{R}^2$.

Exercício 2.9. Verifique a validade do axioma das paralelas 8 no plano $\mathbb{R}^2$.

Exercício 2.10. Verifique a validade do Axioma 6 no Plano de Poincaré.

CAPÍTULO 3

Produto interno

1. Definição



produto interno é uma abstração que permite introduzir noções de comprimento e ângulo em espaços vetoriais. Começamos definindo um exemplo concreto de produto interno, chamado de *produto interno canônico*.

Definição 3.1. O *produto interno canônico* de $\mathbb{R}^n$ é definido por:

$$\begin{aligned} \langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n &\rightarrow \mathbb{R} \\ (u, v) &\mapsto \langle u, v \rangle = \sum_{i=1}^n u_i v_i. \end{aligned}$$

A definição abstrata de um *produto interno* é:

Definição 3.2. Seja E um espaço vetorial real. Um *produto interno* em E é uma função

$$\begin{aligned} \langle \cdot, \cdot \rangle : E \times E &\rightarrow \mathbb{R} \\ (u, v) &\mapsto \langle u, v \rangle \end{aligned}$$

com as seguintes propriedades:

- [PI1] Positividade: para todo u vale $\langle u, u \rangle \geq 0$, com igualdade se e somente se $u = 0$
- [PI2] Simetria: $\langle u, v \rangle = \langle v, u \rangle$
- [PI3] Bilinearidade: $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$.

Verifique que o produto interno canônico de $\mathbb{R}^n$ satisfaz os axiomas acima. Uma vez fixado um produto interno, recuperamos as noções de comprimento e de ângulo.

Em primeiro lugar, definimos a norma ou comprimento de um vetor u como $\|u\| = \sqrt{\langle u, u \rangle}$. Existe uma definição abstrata de norma:

Definição 3.3. Uma *norma* em E é uma função $\|\cdot\|$ de E em $\mathbb{R}$, satisfazendo

- [N1] Positividade: $\|u\| \geq 0$, com igualdade se e somente se $u = 0$
- [N2] Multiplicatividade: $\|\lambda \cdot u\| = |\lambda| \|u\|$
- [N3] Desigualdade triangular: $\|u + v\| \leq \|u\| + \|v\|$.

Está claro que uma norma definida a partir de um produto interno satisfaz as propriedades [N1] e [N2]. A desigualdade triangular depende de um Teorema a ser enunciado, e a prova fica em exercício.

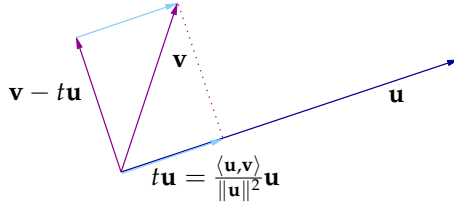


FIGURA 1. Teorema de Cauchy-Buniakovskii-Schwarz

2. O Teorema de Cauchy-Buniakovskii-Schwarz

Teorema 3.4 (Cauchy-Buniakovskii-Schwarz). *Seja E um espaço vetorial real com produto interno $\langle \cdot, \cdot \rangle$ e norma $\|u\|^2 = \langle u, u \rangle$. Então, para todos $u, v \in E$, vale*

$$|\langle u, v \rangle| \leq \|u\| \|v\|.$$

DEMONSTRAÇÃO. Se $u = 0$ então a desigualdade é trivial. Assumimos a partir de agora que $u \neq 0$. Escolhemos $t = \frac{\langle u, v \rangle}{\|u\|^2}$ de modo a ter $u \perp v - tu$, ou seja:

$$\langle u, v - tu \rangle = 0.$$

Decompondo $v = tu + (v - tu)$,

$$\|v\|^2 = t^2 \|u\|^2 + 2\langle u, v - tu \rangle + \|v - tu\|^2 = t^2 \|u\|^2 + \|v - tu\|^2.$$

Obtemos que $t^2 \|u\|^2 \leq \|v\|^2$. Extraíndo as raízes quadradas,

$$|t| \|u\| \leq \|v\|.$$

Substituindo $|t|$ por $\frac{|\langle u, v \rangle|}{\|u\|^2}$ e multiplicando os dois lados por $\|u\|$, deduzimos que

$$|\langle u, v \rangle| \leq \|u\| \|v\|.$$

□

3. O produto interno. Ângulos, normas

Podemos definir o ângulo entre dois vetores pela equação

$$\cos(\widehat{(u, v)}) = \frac{\langle u, v \rangle}{\|u\| \|v\|}.$$

A função $\cos(x)$ é a função cosseno do Cálculo,

$$\cos(x) = 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \cdots.$$

Como a função cosseno tem período 2π , os ângulos são definidos módulo 2π .

Lembremos do cálculo que $\sin(x) = \cos(x - \pi/2)$ tem por expansão de Taylor

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$$

Vamos precisar do seguinte Lema:

Lema 3.5. *Sejam c e s números reais tais que $c^2 + s^2 = 1$. Então, existe $x \in [0, 2\pi)$ tal que $\cos(x) = c$ e $\sin(x) = s$.*

DEMONSTRAÇÃO. A função $\cos(x)$ é contínua, e $\cos(0) = 1$ e $\cos(-\pi) = -1$. Pelo Teorema do valor intermediário, existe x^* em $[-\pi, 0]$ com $\cos(x^*) = c$ (e portanto também $\cos(-x^*) = c$).

Derivando $\cos^2(x) + \sin^2(x)$, deduzimos (usando a diferenciabilidade do seno, do cosseno e o Teorema de Rolle) que $\cos^2(x) + \sin^2(x) \equiv \cos^2(0) + \sin^2(0) \equiv 1$. Na situação do Lema, deduzimos que $\sin(x^*) = \pm\sqrt{1-c^2} = \pm s$, e portanto ou $\sin(x^*) = s$ ou $\sin(-x^*) = s$. $\square$

Um caso particular é o de vetores $\mathbf{u}$ e $\mathbf{v} \in \mathbb{R}^2$ no círculo trigonométrico $u_1^2 + u_2^2 = 1$, $v_1^2 + v_2^2 = 1$. Neste caso,

$$\cos(\widehat{\mathbf{u}, \mathbf{v}}) = u_1 v_1 + u_2 v_2 = \langle \mathbf{u}, \mathbf{e}_1 \rangle \langle \mathbf{v}, \mathbf{e}_1 \rangle + \langle \mathbf{u}, \mathbf{e}_2 \rangle \langle \mathbf{v}, \mathbf{e}_2 \rangle$$

De acordo com o Lema 3.5, podemos escrever $\mathbf{u} = \begin{bmatrix} \cos \alpha \\ \sin \alpha \end{bmatrix}$ e $\mathbf{v} = \begin{bmatrix} \cos \beta \\ \sin \beta \end{bmatrix}$, acabamos de mostrar que

$$\cos(\beta - \alpha) = (\cos \alpha)(\cos \beta) + (\sin \alpha)(\sin \beta).$$

Observação 3.6. Recuperamos acima a fórmula aditiva do cosseno. Essa fórmula pode também ser provada a partir das propriedades da exponencial (lembrando que $e^{it} = \cos(t) + i\sin(t)$). Assim, podemos concluir que a definição de ângulo acima é aditiva:

$$\widehat{\mathbf{u}, \mathbf{v}} = \widehat{\mathbf{e}_1, \mathbf{v}} - \widehat{\mathbf{e}_1, \mathbf{u}} \pmod{2\pi}.$$

Segue-se que para todo $\mathbf{w}$,

$$\widehat{\mathbf{u}, \mathbf{v}} = \widehat{\mathbf{u}, \mathbf{w}} + \widehat{\mathbf{w}, \mathbf{v}} \pmod{2\pi}.$$

Observação 3.7. A definição de ângulo a partir do produto interno é válida em qualquer dimensão. No entanto, a relação $\widehat{\mathbf{u}, \mathbf{w}} = \widehat{\mathbf{u}, \mathbf{v}} + \widehat{\mathbf{v}, \mathbf{w}}$ só vale no plano, ou para vetores $\mathbf{u}, \mathbf{v}, \mathbf{w}$ em um mesmo plano. Em geral, temos apenas que $|\widehat{\mathbf{u}, \mathbf{w}}| \leq |\widehat{\mathbf{u}, \mathbf{v}}| + |\widehat{\mathbf{v}, \mathbf{w}}|$.

De posse da noção de ângulo, podemos definir:

Definição 3.8. Dois vetores $\mathbf{u}, \mathbf{v}$ são ortogonais se e somente se $\langle \mathbf{u}, \mathbf{v} \rangle = 0$. (Em particular, o vetor zero é ortogonal a qualquer vetor).

4. Aplicações geométricas

Um *movimento rígido* ou *isometria* de $\mathbb{R}^n$ é uma transformação

$$\begin{aligned} M: \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ \mathbf{u} &\mapsto M(\mathbf{u}) \end{aligned}$$

que preserva distâncias:

$$\|M(\mathbf{u}) - M(\mathbf{v})\| = \|\mathbf{u} - \mathbf{v}\|.$$

Por exemplo, translações $\mathbf{u} \mapsto \mathbf{u} + \mathbf{w}$ são movimentos rígidos. Todos os movimentos rígidos são similaridades, mas não vale a recíproca.

Proposição 3.9. Se M é um movimento rígido e $M(\mathbf{0}) = \mathbf{0}$, então M é uma transformação linear.

DEMONSTRAÇÃO. Em primeiro lugar, igualando as distâncias entre os pontos $\mathbf{0}$, $\mathbf{u}$ e $\lambda\mathbf{u}$ e o das suas imagens por M , teremos que

$$\begin{aligned}\|M(\mathbf{u})\| &= \|\mathbf{u}\| \\ \|M(\lambda\mathbf{u})\| &= |\lambda|\|\mathbf{u}\| \\ \|M(\lambda\mathbf{u}) - M(\mathbf{u})\| &= \|\lambda\mathbf{u} - \mathbf{u}\|\end{aligned}$$

Segue-se que $M(\mathbf{u})$, $M(\lambda\mathbf{u})$ e $\mathbf{0}$ estão alinhados (porquê?). Disso deduz-se que $M(\lambda\mathbf{u}) = \lambda M(\mathbf{u})$.

Depois, para mostrar que $M(\mathbf{u} + \mathbf{v}) = M(\mathbf{u}) + M(\mathbf{v})$, introduzimos $\mathbf{w} = \frac{1}{2}(\mathbf{u} + \mathbf{v})$. Seja $\nu = \|\mathbf{u} - \mathbf{v}\|$. Então $\|\mathbf{u} - \mathbf{w}\| = \|\mathbf{v} - \mathbf{w}\| = \nu/2$, e teremos que $\|M(\mathbf{u}) - M(\mathbf{v})\| = \nu$ e $\|M(\mathbf{u}) - M(\mathbf{w})\| = \|M(\mathbf{v}) - M(\mathbf{w})\| = \nu/2$. Assim, $M(\mathbf{w}) = \frac{1}{2}(M(\mathbf{u}) + M(\mathbf{v}))$ é o ponto médio do segmento $[M(\mathbf{u}), M(\mathbf{v})]$ e $M(\mathbf{u} + \mathbf{v}) = 2M(\mathbf{w})$. $\square$

Se M é um movimento rígido, a Proposição acima permite definir a transformação linear associada A a M por:

$$\begin{aligned}A: \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ \mathbf{w} &\mapsto A(\mathbf{w}) = M(\mathbf{w}) - M(\mathbf{0})\end{aligned}$$

Deduzimos que M é da forma:

$$M(\mathbf{x}) = \begin{bmatrix} A_{11} & \dots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \dots & A_{nn} \end{bmatrix} \mathbf{x} + M(\mathbf{0})$$

(transformação linear mais translação). A transformação linear A tem uma propriedade adicional, ela preserva normas e produtos internos.

Definição 3.10. Uma matriz A é *ortogonal* se e somente se, para todos $\mathbf{x}$ e $\mathbf{y}$, temos

$$\langle A\mathbf{x}, A\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$$

5. Exercícios

Exercício 3.1. Seja $\mathbf{u}$ um vetor diferente de zero. Mostre diretamente da definição de produto interno que $\mathbf{v}$ pertence à reta $\{\lambda\mathbf{u} : \lambda \in \mathbb{R}\}$ se e somente se $|\langle \mathbf{u}, \mathbf{v} \rangle| = \|\mathbf{u}\|\|\mathbf{v}\|$.

Exercício 3.2. Sejam A e B pontos diferentes do plano. Ache a equação dos pontos equidistantes a A e B . O lugar geométrico desses pontos é chamado de mediatriz do segmento $[A, B]$. Deduzir que a mediatriz de um segmento é sempre uma reta.

Exercício 3.3. Seja $\mathbf{u}$ um vetor diferente de zero em $\mathbb{R}^n$. Ache a equação do hiperplano de vetores ortogonais a $\mathbf{u}$.

Exercício 3.4. A transposta de uma matriz A de tamanho $m \times n$ é a matriz A^T de tamanho $n \times m$ definida por: $(A^T)_{ij} = A_{ji}$.

- Mostre que se $\langle \cdot, \cdot \rangle_{\mathbb{R}^k}$ é o produto interno canônico, então para todos $\mathbf{u} \in \mathbb{R}^n$ e $\mathbf{v} \in \mathbb{R}^m$,

$$\langle A\mathbf{u}, \mathbf{v} \rangle_{\mathbb{R}^m} = \langle \mathbf{u}, A^T \mathbf{v} \rangle_{\mathbb{R}^n}.$$

- Deduza que $(AB)^T = B^T A^T$. Mostre essa fórmula também de maneira direta.
- Deduza que $A \mapsto A^T$ é um isomorfismo de $L(\mathbb{R}^n, \mathbb{R}^m)$ em $L(\mathbb{R}^m, \mathbb{R}^n)$.

Exercício 3.5. Seja $\|u\| = \sqrt{\langle u, u \rangle}$ a norma associada a um produto interno qualquer. Mostre a desigualdade triangular para a norma. Depois, verifique diretamente a desigualdade triangular para a norma associada ao produto interno canônico.

Exercício 3.6. Se uma norma qualquer é dada, e você sabe que essa norma é associada a um produto interno, escreva uma expressão do produto interno em função da norma. Essa fórmula é chamada de *fórmula de polarização*.

Exercício 3.7. Mostre a seguinte igualdade integral, assumindo que f e g são integráveis, e que as duas integrais na parte direita existem:

$$\left(\int_{-\infty}^{\infty} f(x)g(x)dx \right)^2 \leq \left(\int_{-\infty}^{\infty} f(x)^2 dx \right) \left(\int_{-\infty}^{\infty} g(x)^2 dx \right).$$

Exercício 3.8. Para todo $p \geq 1$, definimos uma norma no $\mathbb{R}^n$ por: $\|\mathbf{u}\|_p = \sqrt[p]{\sum_{j=1}^n |u_j|^p}$. No limite, definimos $\|\mathbf{u}\|_{\infty} = \max |u_j|$. Desenhe, para $p = 1, 2, 3, \infty$, o conjunto $\{\mathbf{x} \in \mathbb{R}^2 : \|\mathbf{x}\|_p < 1\}$, também conhecido como *bola unitária*. Mostre que para todo $\mathbf{x}$ e para todo $p \geq 2$,

$$\|\mathbf{x}\|_1 \geq \|\mathbf{x}\|_2 \geq \cdots \|\mathbf{x}\|_p \geq \cdots \geq \|\mathbf{x}\|_{\infty} \geq \frac{1}{n} \|\mathbf{x}\|_1.$$

Exercício 3.9. Mostre que toda norma $\|\cdot\|$ de $\mathbb{R}^n$ é uma função contínua de $\mathbb{R}^n$ em $\mathbb{R}$.

Exercício 3.10. Considere as seguintes definições:

- (1) Um conjunto $\mathcal{B}$ é *convexo* se e somente se, para todos pontos $A, B \in \mathcal{B}$, o segmento $[A, B]$ está contido em $\mathcal{B}$.
- (2) Um conjunto $\mathcal{B}$ é *simétrico* em relação à origem se e somente se, para todo $A \in \mathcal{B}$, $-A \in \mathcal{B}$.
- (3) Um conjunto $\mathcal{B}$ é *limitado* se e somente se existe $R > 0$ tal que, para todo $A = (a_1, \dots, a_n) \in \mathcal{B}$, $\sum |a_i|^2 < R^2$.
- (4) Um conjunto $\mathcal{B}$ é *tem interior* se e somente se existe $r > 0$ tal que, para todo $X = (x_1, \dots, x_n)$ com $\sum x_i^2 < r^2$, temos que $X \in \mathcal{B}$.
- (5) Um conjunto $\mathcal{B}$ é *aberto* se e somente se para todo $B \in \mathcal{B}$, existe um $r > 0$ tal que, para todo $X = (x_1, \dots, x_n)$ com $\sum (x_i - b_i)^2 < r^2$, que $X \in \mathcal{B}$.

Mostre que para todo conjunto $\mathcal{B} \subset \mathbb{R}^n$ aberto, convexo, simétrico em relação à origem, limitado e com volume, podemos definir uma *norma* (abstrata) $\|\cdot\|_{\mathcal{B}}$ tal que $\mathcal{B} = \{\mathbf{X} \in \mathbb{R}^n : \|\mathbf{X}\|_{\mathcal{B}} < 1\}$. Essa norma é chamada de *Norma de Minkovski* associada a $\mathcal{B}$.

CAPÍTULO 4

Solução de equações afins, fatoração LU

1. Matrizes triangulares



Neste capítulo, iniciamos o estudo de algoritmos para resolver sistemas de equações afins:

$$(3) \quad \begin{aligned} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n &= b_1 \\ A_{21}x_1 + A_{22}x_2 + \cdots + A_{2n}x_n &= b_2 \\ &\vdots \\ A_{n1}x_1 + A_{n2}x_2 + \cdots + A_{nn}x_n &= b_n \end{aligned}$$

ou, sob forma matricial,

$$A\mathbf{x} = \mathbf{b}.$$

Estamos assumindo que a matriz A é ‘quadrada’, i.e., tem tantas linhas quanto colunas. Outras hipóteses sobre A podem ser necessárias a seguir.

Existem situações para as quais resolver o sistema (3) é trivial. Vamos analisar primeiro uma dessas situações.

Lema 4.1. *O sistema de equações*

$$\begin{aligned} U_{11}x_1 + U_{12}x_2 + \cdots + U_{1n}x_n &= b_1 \\ U_{22}x_2 + \cdots + U_{2n}x_n &= b_2 \\ &\vdots \\ U_{nn}x_n &= b_n, \end{aligned}$$

onde $U_{ii} \neq 0$ para todo i , pode ser resolvido pela recorrência

$$\begin{aligned} x_n &= \frac{b_n}{U_{nn}}, \\ x_{n-1} &= \frac{b_{n-1} - U_{nn}x_n}{U_{n-1,n-1}}, \\ &\vdots \\ x_j &= \frac{b_j - \sum_{i>j} U_{ji}x_i}{U_{j,j}}, \\ &\vdots \\ x_1 &= \frac{b_1 - \sum_{i>1} U_{1i}x_i}{U_{1,1}}. \end{aligned}$$

Note que o número de multiplicações mais divisões da recorrência acima é $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Do ponto de vista matricial, uma matriz U onde $U_{ij} = 0$ sempre que $i > j$ é chamada de triangular superior:

$$U = \begin{bmatrix} U_{11} & U_{12} & \cdots & U_{1n} \\ & U_{22} & \cdots & U_{2n} \\ & & \ddots & \vdots \\ & & & U_{nn} \end{bmatrix}$$

onde os zeros foram substituídos por espaços. Similarmente, uma matriz L onde $L_{ij} = 0$ sempre que $j > i$ é chamada de triangular inferior.

2. Eliminação

Uma maneira de resolver sistemas de n equações em n variáveis é eliminar as variáveis, uma a uma. Se queremos resolver o sistema

$$(4) \quad \begin{aligned} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n &= b_1 \\ A_{21}x_1 + A_{22}x_2 + \cdots + A_{2n}x_n &= b_2 \\ &\vdots \\ A_{n1}x_1 + A_{n2}x_2 + \cdots + A_{nn}x_n &= b_n \end{aligned}$$

e se A_{11} for diferente de zero, podemos subtrair um múltiplo da primeira equação das equações subsequentes, de maneira a eliminar a variável x_1 :

$$\begin{aligned} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n &= b_1 \\ A_{22} - \frac{A_{12}A_{21}}{A_{11}}x_2 + \cdots + A_{2n} - \frac{A_{1n}A_{21}}{A_{11}}x_n &= b_2 - \frac{b_1A_{21}}{A_{11}} \\ &\vdots \\ A_{n2} - \frac{A_{12}A_{n1}}{A_{11}}x_2 + \cdots + A_{nn} - \frac{A_{1n}A_{n1}}{A_{11}}x_n &= b_n - \frac{b_1A_{n1}}{A_{11}}. \end{aligned}$$

Escrevemos $A_{ij}^{(2)} = A_{ij} - \frac{A_{1j}A_{i1}}{A_{11}}$ e $b_i^{(2)} = b_i - \frac{b_1A_{i1}}{A_{11}}$. Com os novos coeficientes, precisamos resolver:

$$(5) \quad \begin{aligned} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n &= b_1 \\ A_{22}^{(2)}x_2 + \cdots + A_{2n}^{(2)}x_n &= b_2^{(1)} \\ &\vdots \\ A_{n2}^{(2)}x_2 + \cdots + A_{nn}^{(2)}x_n &= b_n^{(1)}. \end{aligned}$$

Você pode (e deve) verificar que toda solução de (4) é uma solução de (5) e reciprocamente. Tentamos agora eliminar x_2, x_3 , etc... sucessivamente. A cada passo, assumimos que $A_{pp}^{(p)} \neq 0$. Sob essa condição, fazemos, para $j > p$:

$$A_{ij}^{(p+1)} = A_{ij}^{(p)} - \frac{A_{pj}^{(p)}A_{ip}^{(p)}}{A_{pp}^{(p)}} \quad \text{e} \quad b_i^{(p+1)} = b_i^{(p)} - \frac{b_p^{(p)}A_{ip}^{(p)}}{A_{pp}^{(p)}}.$$

No final, obtemos um sistema triangular inferior, que sabemos resolver por substituição.

3. Exemplos onde a eliminação falha

Vamos considerar aqui contra-exemplos para o procedimento de eliminação acima.

Exemplo 4.2.

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Neste exemplo, não existe $\mathbf{x}$ tal que $0x_1 + 0x_2 = 1$. O sistema de equações lineares é inconsistente, corresponde (na interpretação *por linhas*) a procurar a interseção de duas retas paralelas.

Exemplo 4.3.

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

Após aplicar eliminação, recaímos no exemplo 4.2. A eliminação pode ser feita mas o sistema de equações continua inconsistente.

Exemplo 4.4.

$$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Agora, o sistema é inconsistente e ainda não conseguimos fazer eliminação.

Exemplo 4.5.

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Agora temos uma infinidade de soluções.

Exemplo 4.6.

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

Neste caso, o procedimento de eliminação não funciona. Mas se trocamos a ordem das linhas, o procedimento funciona e obtemos uma solução única.

Definição 4.7. Uma matriz A de tamanho $n \times n$ é *inversível* se e somente se existe outra matriz B , chamada de *inversa* de A , tal que $AB = I$ e $BA = I$. Escreve-se $B = A^{-1}$.

Se A for inversível, então o sistema

$$A\mathbf{x} = \mathbf{b}$$

tem sempre solução $\mathbf{x} = A^{-1}\mathbf{b}$.

Definição 4.8. Uma *decomposição LU* de A é um par de matrizes L e U , onde L é triangular inferior com $L_{ii} = 1 \forall i$ e U é triangular superior.

Os exemplos acima mostram que nem sempre é possível obter uma decomposição LU de uma matriz. Isso é independente do fato da matriz ser ou não ser inversível. Veremos no Capítulo 6 que a fatoração LU sempre pode ser calculada, para uma matriz obtida permutando as linhas de A . Antes disso porém, precisaremos estudar em mais detalhes o grupo das permutações.

4. Exercícios

Exercício 4.1. Qual é o conjunto de soluções do sistema abaixo?

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}.$$

Exercício 4.2. Qual é o conjunto de soluções do sistema abaixo?

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}.$$

Interprete geometricamente.

Exercício 4.3. Use a formulação matricial para encontrar uma condição necessária e suficiente para duas retas $a_i x + b_i y + c_i = 0$ no plano serem paralelas.

Exercício 4.4. Quantas operações aritméticas são necessárias para resolver $A\mathbf{x} = \mathbf{b}$ por eliminação? Assuma que a solução é única e que o algoritmo de eliminação nunca encontra uma divisão por zero.

Exercício 4.5. Qual é o conjunto das matrizes 2×2 onde o método de eliminação para resolver sistemas de equações falha? Onde ele falha para as duas permutações possíveis das linhas?

Exercício 4.6. Qual é o conjunto das matrizes 2×2 que não admitem decomposição LU?

Exercício 4.7. Qual é o conjunto das matrizes 3×3 onde a eliminação falha? (Escrever a equação do conjunto)

Exercício 4.8. Seja $A = LU$ uma matriz simétrica e inversível. Mostre que $U = DL^T$, onde D é uma matriz diagonal.

Exercício 4.9. Seja $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ uma matriz $2n \times 2n$, sendo cada A_{ij} uma matriz $n \times n$. Explique como fazer a decomposição LU por bloco de A ,

$$A = \begin{bmatrix} L_{11} & 0 \\ L_{21} & L_{22} \end{bmatrix} \begin{bmatrix} U_{11} & U_{12} \\ 0 & U_{22} \end{bmatrix},$$

com L_{11} e L_{22} triangulares inferiores e 1's na diagonal e U_{11} e U_{22} triangulares superiores. Deixe claro sob que condições essa decomposição é possível.

Exercício 4.10. Escreva uma rotina `minhaLU` na linguagem Julia para calcular a fatoração LU de uma matriz arbitrária A . Utilize essa rotina para calcular a fatoração LU de uma matriz aleatória A de tamanho 10×10 ,

[1]: `using(LinearAlgebra)`

[2]: `A=randn(10,10);`

[3]: `minhaLU(A)`

Você também pode digitar exemplos de matrizes para ver o resultado. Tente por exemplo a matriz $\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}$. Compare os resultados com

[4]: `lu(A)`

O que é que Julia fez exatamente?

CAPÍTULO 5

Grupos

1. Exemplos e definição



embremos que uma *bijeção* f entre dois conjuntos S e T é uma função

$$\begin{aligned} f: S &\rightarrow T \\ s &\mapsto f(s) \end{aligned}$$

definida em todo o conjunto S , tal que para todo elemento $t \in T$, existe um e um único $s \in S$ tal que $f(s) = t$.

Queremos estudar o conjunto das bijeções de um conjunto S nele mesmo. Começamos por notar que dadas duas bijeções f e g de S nele mesmo, então a composta $f \circ g$ também é uma bijeção de S nele mesmo. As propriedades do conjunto das bijeções de S em S são abstraídas na seguinte noção:

Definição 5.1. Um *grupo* $(G, \circ)$ é um conjunto G , munido de uma operação interna

$$\begin{aligned} \circ: G \times G &\rightarrow G \\ (a, b) &\mapsto a \circ b \end{aligned}$$

satisfazendo as seguintes propriedades:

- [G1] Associatividade: $a \circ (b \circ c) = (a \circ b) \circ c$
- [G2] Elemento neutro: Existe $e \in G$ tal que, para todo $a \in G$, $a \circ e = e \circ a = a$.
- [G3] Elemento inverso: Para todo $a \in G$, existe $a^{-1} \in G$ tal que $a \circ a^{-1} = a^{-1} \circ a = e$.

Quando não vale a propriedade G3, o conjunto G é chamado de semigrupo. Quando além de G1, G2 e G3, temos sempre que $a \circ b = b \circ a$, o grupo é dito *comutativo*.

Exemplo 5.2. Um movimento rígido de $\mathbb{R}^n$ é uma bijeção

$$\begin{aligned} \mathbf{f}: \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ \mathbf{x} &\mapsto \mathbf{f}(\mathbf{x}) \end{aligned}$$

que preserva a distância Euclidiana:

$$\|\mathbf{f}(\mathbf{x}) - \mathbf{f}(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|.$$

Os movimentos rígidos com a composição também formam um grupo, também conhecido como grupo dos movimentos rígidos ou .

2. O grupo das permutações de n elementos

Seja S um conjunto. Quando existe uma bijeção σ :

$$\begin{array}{ccc} s : \{1, 2, \dots, n\} & \rightarrow & S \\ i & \mapsto & \sigma_i \end{array}$$

dizemos que o conjunto S tem n elementos (ou *cardinalidade* n). O conjunto vazio tem zero elementos. Quando um conjunto tem um número finito de elementos, dizemos que o conjunto é finito. A bijeção s é chamada de *enumeração* do conjunto finito S .

Bijeções de um conjunto finito S nele mesmo são chamadas de *permutações*, e formam um grupo com a composição. Se escolhermos uma enumeração arbitrária para o conjunto S , podemos assimilar permutações σ de S a outras ordenações $\sigma \circ s$. Por isso, para entender o grupo de permutações de um conjunto finito de n elementos basta entender o grupo de permutações do conjunto $\{1, 2, \dots, n\}$.

Chamamos de S_n o grupo das permutações de $\{1, 2, \dots, n\}$, com a operação interna dada pela composição. Nos referimos a S_n como o ‘grupo das permutações de n elementos’.

Definição 5.3. Seja $(G, \circ)$ um grupo. Seja $H \subseteq G$. Dizemos que $(H, \circ)$ é um *subgrupo* de G se e somente se H é um grupo.

Por exemplo, S_{n-1} é subgrupo de S_n . Basta assimilar S_{n-1} ao conjunto de permutações de $\{1, 2, \dots, n\}$ que fixam o elemento n . Podemos descrever cada permutação σ por meio da sua tabela de valores

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Denotamos por e a permutação-identidade e por (ij) , $i \neq j$, a permutação que troca i por j e fixa todos os outros elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \quad (12) = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}.$$

As permutações (ij) são chamadas de *permutações elementares*. Se $i_1, \dots, i_l \in \{1, \dots, n\}$ são distintos dois a dois, definimos a *permutação cíclica* $\sigma = (i_1 i_2 \dots i_l)$ como

$$\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \\ k \mapsto \sigma(k) = \begin{cases} i_{r+1} & \text{se } k = i_r, 1 \leq r < l \\ i_1 & \text{se } k = i_l \\ k & \text{nos outros casos.} \end{cases}$$

Visto que não existe permutação cíclica de ordem 1, podemos usar sem ambiguidade¹ a notação $\sigma(k) = (i_1 i_2 \dots i_l)(k)$. Isso nos leva a escrever a composição de duas ou mais permutações cíclicas sob forma de produto. Por exemplo,

$$((12) \circ (23))(k) = (12)((23)(k)).$$

Omitindo o sinal da composição, teremos:

$$(12)(23) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} = (123)$$

¹Aviso importante, mas apenas para quem lê notas de rodapé: alguns autores escrevem o produto de permutações cíclicas da esquerda para a direita e não da direita para a esquerda como no nosso caso.

enquanto

$$(23)(12) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix} = (132).$$

Vemos assim que o produto de permutações não é comutativo. É fácil ver que toda permutação σ se escreve como um produto de permutações cíclicas de elementos disjuntos, por exemplo

$$(1234)(567)(89)(1011).$$

Para isso, escolhemos um elemento que não seja fixo por σ (por exemplo 1), e produzimos o ciclo $(1 \sigma(1) \sigma(\sigma(1)))$ até voltar ao início. Enquanto houver um elemento não listado e não fixo, continuamos com o mesmo procedimento. Também é fácil ver que qualquer ciclo de comprimento r pode ser quebrado em produto de $r - 1$ permutações elementares, por exemplo

$$(12345) = (12)(23)(34)(45)$$

Lema 5.4. *Toda permutação $\sigma \in S_n$ pode ser escrita como uma composição de no máximo $n - 1$ permutações elementares.*

DEMONSTRAÇÃO. Podemos decompor σ em um produto $\sigma = \sigma_1 \dots \sigma_t$ de permutações cíclicas distintas, cada uma de comprimento relativo $c_1, \dots, c_t$. Como temos n elementos, $c_1 + \dots + c_t \leq n$. Cada σ_i , por sua vez, é um produto de $c_i - 1$ permutações elementares. Assim, σ é um produto de $n - t \leq n - 1$ permutações elementares. $\square$

Chamamos de ordem de uma permutação σ o menor número de permutações elementares necessário para produzir σ . Escrevemos $|\sigma|$ para a ordem de σ . Por exemplo, $|e| = 0$, e $(ij) = 1$. Na decomposição do lema acima, temos claramente $|\sigma| \leq n - t$. Pode-se mostrar por indução que o produto de $c - 1$ permutações elementares permite produzir uma permutação cíclica de no máximo c elementos. Deste modo, se $\sigma \neq e$, $|\sigma| = n - t$ exatamente. Uma permutação σ é *par* se $|\sigma|$ é par, e é *ímpar* se $|\sigma|$ é ímpar. A seguinte propriedade das permutações vai ser usada neste livro:

Lema 5.5. *Se $\sigma_1, \dots, \sigma_k \in S_n$ são permutações elementares, então $\sigma_1 \circ \dots \circ \sigma_k$ é par se e somente se k é par.*

DEMONSTRAÇÃO. Consideramos a seguinte função, que mede o número de ‘ultrapassagens’:

$$\begin{aligned} r: S_n &\rightarrow \mathbb{Z} \\ g &\mapsto r(\sigma) = \sum_{i=2}^n \#\{j < i : \sigma(j) > \sigma(i)\} \end{aligned}$$

Parte 1. Seja $k \in \{1, \dots, n - 1\}$. Seja $p = (k \ k + 1)$. Para toda $\sigma \in S_n$, temos:

$$r(\sigma) - r(\sigma p) = \sum_{i=2}^n \#\{j < i : \sigma(j) > \sigma(i)\} - \sum_{i=2}^n \#\{j < i : (\sigma p)(j) > (\sigma p)(i)\}$$

Os casos onde $\{i, j\} \cap \{k, k + 1\} = \emptyset$ são contados dos dois lados e cancelam. Como estamos contando apenas pares com $i < j$, ficamos com os casos $j = k$ e $j = k + 1$.

$$\begin{aligned} r(\sigma) - r(\sigma p) &= \#\{j < k : \sigma(j) > \sigma(k)\} + \#\{j < k + 1 : \sigma(j) > \sigma(k + 1)\} \\ &\quad - \#\{j < k : \sigma(j) > \sigma(k + 1)\} - \#\{j < k + 1 : \sigma(j) > \sigma(k)\} \\ &= \#\{j < k : \sigma(j) > \sigma(k)\} - \#\{j < k + 1 : \sigma(j) > \sigma(k)\} \\ &\quad + \#\{j < k + 1 : \sigma(j) > \sigma(k + 1)\} - \#\{j < k : \sigma(j) > \sigma(k + 1)\} \\ &= \begin{cases} 1 & \text{Se } \sigma(k) > \sigma(k + 1) \\ -1 & \text{Se } \sigma(k) < \sigma(k + 1) \end{cases} \end{aligned}$$

Logo, $r(\sigma p)$ é par se e somente se $r(\sigma)$ é ímpar.

Parte 2: Toda permutação (ij) pode ser escrita como um produto de um número ímpar de permutações da forma $(k \ k+1)$ (exercício). Logo, $r(\sigma(ij))$ é par se e somente se $r(\sigma)$ é ímpar. $\square$

Definição 5.6. $\{\sigma_1, \dots, \sigma_r\} \subset G$ é um *conjunto gerador* do grupo $(G, \circ)$ se e somente se, todo elemento $g \in G$ é uma composição arbitrária dos σ_i .

A escolha dos geradores é arbitrária. Por exemplo, as permutações elementares são um conjunto gerador de S_n . Mas veremos no exercício 5.1 que $\{p_{i,i+1} : i = 1, \dots, n-1\}$ é também conjunto gerador de S_n .

3. O grupo linear de $\mathbb{R}^n$

Definimos $GL(n)$ como o conjunto de transformações lineares inversíveis de $\mathbb{R}^n$. Se A e B são inversíveis, então $A \circ B$ é inversível, com inversa $B^{-1} \circ A^{-1}$. A identidade é inversível. Se A é inversível, então A^{-1} é inversível e tem inversa A . Logo, $GL(n)$ é um grupo. Esse é um exemplo de grupo não comutativo ! (exercício).

Alguns exemplos de subgrupos são:

- (1) As matrizes diagonais inversíveis.
- (2) As matrizes triangulares inferiores inversíveis.
- (3) As matrizes triangulares superiores ineversíveis.
- (4) As matrizes triangulares inferiores inversíveis com 1's na diagonal.
- (5) As matrizes triangulares superiores inversíveis com 1's na diagonal.
- (6) As transformações lineares associadas a uma isometria (Grupo *ortogonal*).
- (7) As transformações lineares associadas a uma similaridade.

Além desses, vamos definir um subgrupo que pode ser assimilado a S_n . Para isso, definimos duas noções especiais para grupos:

Definição 5.7. Se $(G, \circ)$ e $(H, \circ)$ são grupos, um *homomorfismo* ϕ de G em H é uma função

$$\begin{aligned} \phi: G &\rightarrow H \\ g &\mapsto \phi(g) \end{aligned}$$

tal que $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$ e $\phi(g^{-1}) = \phi(g)^{-1}$. Um homomorfismo que é também uma bijeção é chamado de *isomorfismo*.

Por exemplo, $\chi : S_n \rightarrow (\{-1, +1\}, \cdot)$ definida por $\chi(\sigma) = 1$ sse σ é um produto de um número par de permutações elementares, é um homomorfismo de grupo. Mas χ só é um isomorfismo para $n = 2$.

Como no caso de funções, $\text{Im}\phi = \{\phi(g) : g \in G\}$ é a *imagem* de ϕ , enquanto $\ker \phi = \{g \in G : \phi(g) = e\}$ é chamado de *núcleo* de ϕ . Um subgrupo K de G é *normal* se e somente se, para todos $k \in K$ e $g \in G$, $g^{-1}kg \in K$. Por exemplo, o subgrupo das permutações pares é normal. Um dos Teoremas fundamentais da Teoria de Grupos é o seguinte:

Teorema 5.8 (Isomorfismo de Grupos). Se ϕ é um homomorfismo do grupo $(G, \circ)$ no grupo $(H, \circ)$, então

- (1) A imagem de ϕ é um subgrupo de H .
- (2) O núcleo de ϕ é um subgrupo normal de G .
- (3) O quociente $\frac{G}{\ker \phi}$ é um grupo isomorfo à imagem de ϕ .

DEMONSTRAÇÃO. A prova deste Teorema não é indispensável ao resto do curso.

- (1) Por construção, a imagem de ϕ é um subconjunto de H . Para todos $h_1, h_2 \in \text{Im}\phi$, existem $g_1, g_2 \in G$ tais que $\phi(g_1) = h_1$ e $\phi(g_2) = h_2$. Por definição do homomorfismo, teremos que $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$ e $\phi(g_1^{-1}) = \phi(g_1)^{-1}$. Segue-se que $\text{Im}\phi$ é um subgrupo de H .
- (2) Sejam $g_1, g_2 \in \ker \phi$, então $\phi(g_1) = \phi(g_2) = e$. Por definição do homomorfismo, $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2) = e$ e $\phi(g_1^{-1}) = \phi(g_1)^{-1} = e$. Acabamos de mostrar que se $g_1, g_2 \in \ker \phi$, então $g_1 \circ g_2 \in \ker \phi$ e $g_1^{-1} \in \ker \phi$. Logo $\ker \phi$ é subgrupo de G .

Agora, sejam $g \in \ker \phi$ e $a \in G$ qualquer. Teremos:

$$\phi(a \circ g \circ a^{-1}) = \phi(a) \circ \phi(g) \circ \phi(a)^{-1} = \phi(a) \circ \phi(a)^{-1} = \phi(e) = e.$$

Segue-se que $a \circ g \circ a^{-1} \in \ker \phi$, e $\ker \phi$ é normal.

- (3) Sejam $u, v \in \frac{G}{\ker \phi}$. Como u e v são classes de equivalência, podem ser escritas como

$$u = \{k \circ U \circ k^{-1} : k \in \ker \phi\} \quad \text{e} \quad v = \{k \circ V \circ k^{-1} : k \in \ker \phi\}.$$

(Dizemos que U e V são representantes de u e de v , respectivamente. U e V não são necessariamente únicos). A operação de grupo é:

$$u \circ v = \{k \circ U \circ V \circ k^{-1} : k \in \ker \phi\}$$

Esta operação está bem definida, pois não depende da escolha dos representantes U e V . Se U' e V' são outros representantes, então $U' = k_1 \circ U \circ k_1^{-1}$ e $V' = k_2 \circ V \circ k_2^{-1}$ para $k_1, k_2 \in \ker \phi$. Teremos

$$\phi(k \circ U' \circ V' \circ k^{-1}) = \phi(k \circ k_1 \circ U \circ k_1^{-1} \circ k_2 \circ V \circ k_2^{-1} \circ k^{-1}) = \phi(U \circ V)$$

conforme esperado.

Vamos definir o isomorfismo ψ por

$$\psi(u) = \phi(U).$$

Essa função está bem definida, pois não depende da escolha do representante U de u : se U' é outro representante de u , então $U' = k \circ U \circ k^{-1}$ para algum $k \in \ker \phi$. Logo, $\phi(U') = \phi(U)$.

Também está claro que $\text{Im}\phi = \text{Im}\psi$. Falta demonstrar que ψ é homomorfismo. Para isso, verificamos:

$$\psi(u \circ v) = \phi(U \circ V) = \psi(u) \circ \psi(v)$$

e

$$\psi(u^{-1}) = \phi(U^{-1}) = \phi(U)^{-1} = \psi(u)^{-1}$$

□

4. As matrizes de permutação

Dada uma permutação $\sigma \in S_n$, definimos a *matriz de permutação* P_σ por:

$$(P_\sigma)_{ij} = \begin{cases} 1 & \text{se } i = \sigma(j) \\ 0 & \text{senão.} \end{cases},$$

As linhas dessa matriz são, respectivamente, $e_{\sigma(1)}^T, e_{\sigma(2)}^T, \dots, e_{\sigma(n)}^T$. Também temos:

$$P_\sigma \begin{bmatrix} 1 \\ 2 \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} \sigma(1) \\ \sigma(2) \\ \vdots \\ \sigma(n) \end{bmatrix}$$

Proposição 5.9. A função

$$\begin{aligned} P: S_n &\rightarrow GL(n) \\ \sigma &\mapsto P_\sigma \end{aligned}$$

é um homomorfismo de S_n no grupo multiplicativo das matrizes $n \times n$.

A prova é o Exercício 5.4. Qualquer matriz em $\text{Im}P$ é chamada de matriz de Permutação. Pelo Teorema do Isomorfismo (Teorema 5.8), as matrizes de Permutação formam um grupo multiplicativo, isomorfo a S_n .

5. Exercícios

Exercício 5.1. Mostre que toda permutação elementar é produto de um número ímpar de permutações da forma $(k, k+1)$.

Exercício 5.2. Mostre que as permutações de S_n que fixam n são um subgrupo de S_n .

Exercício 5.3. Mostre que $GL(n)$ não é comutativo para $n > 1$.

Exercício 5.4. Prove a Proposição 5.9.

Exercício 5.5. Mostre que o conjunto das matrizes da forma

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ l_2 & 1 & 0 & \cdots & 0 \\ l_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ l_n & 0 & 0 & \cdots & 1 \end{bmatrix}$$

é um grupo multiplicativo.

Exercício 5.6. Seja G o grupo do exercício acima, e seja $\sigma \in S_n$ tal que $\sigma(1) = 1$. Mostre que para todo $g \in G$, $P_\sigma g P_\sigma^{-1} \in G$.

Exercício 5.7. Mostre o Teorema de Cayley: todo grupo finito de n elementos é isomorfo a um subgrupo de S_n .

Exercício 5.8. O grupo livre de n elementos é o conjunto das palavras formadas por n símbolos e suas inversas. A operação de grupo é a concatenação. Por exemplo, o grupo livre de 2 elementos contém as palavras e (palavra vazia), a , a^{-1} , b , b^{-1} , ab , etc... (Um símbolo não pode ser precedido ou seguido pela sua inversa). Mostre que existe um homomorfismo ϕ do grupo livre de $n-1$ elemento em S_n , com imagem S_n .

Exercício 5.9. Em geral, se G é um grupo, o núcleo de ϕ é chamado de conjunto das *relações* de G . Se tanto G quanto o conjunto das relações forem finitamente gerados, o grupo G é chamado de *finitamente apresentável*. Mostrar que S_n é finitamente apresentável.

Exercício 5.10. O problema da palavra é, dado um grupo finitamente apresentável e uma *palavra* finita (cujas letras são os geradores), decidir se essa palavra representa a identidade do grupo. Escreva um algoritmo para resolver o problema da palavra, para o grupo S_n .

Note-se que nem sempre é possível resolver o problema da palavra.

Teorema (P. S. Novikov², 1952). *Existe um grupo finitamente apresentável, tal que não pode existir um algoritmo decidindo o problema da palavra para esse grupo.*

²Pietr Sergeevich Novikov, On the algorithmic insolvability of the word problem in group theory. *American Mathematical Society Translations*, Ser 2, Vol. 9, pp. 1–122. American Mathematical Society, Providence, R. I., (1958). O original em Russo foi publicado em 1952.

CAPÍTULO 6

A fatoração *PLU*

1. Ação de grupo



Grupos não existem no vazio. A noção de grupo foi desenvolvida para se estudar *transformações* de algum objeto ou conjunto. Isso obriga os grupos a terem as propriedades que têm.

Definição 6.1. Um grupo $(G, \circ)$ age “à esquerda” sobre um conjunto X se e somente se, existe uma função (ação à esquerda)

$$\begin{aligned} a : G \times X &\rightarrow X \\ (g, x) &\mapsto a(g, x) \end{aligned}$$

com as seguintes propriedades:

$$a(g_1, a(g_2, x)) = a(g_1 \circ g_2, x)$$

e

$$a(e, x) = x .$$

Ele age “à direita” sobre um conjunto X se e somente se, existe uma função (ação à direita)

$$\begin{aligned} b : X \times G &\rightarrow X \\ (x, g) &\mapsto b(x, g) \end{aligned}$$

com as seguintes propriedades:

$$b(b(x, g_1), g_2) = b(x, g_1 \circ g_2)$$

e

$$b(x, e) = x .$$

Dessa definição, segue-se que para todo g fixo, $x \mapsto a(g, x)$ é uma bijeção. Quando x é fixo, o conjunto $\{a(g, x) : g \in G\}$ é chamado de *órbita* de x por G . (Mesma definição para ação à direita).

Por exemplo, seja $X = L(n) \times \mathbb{R}^n$ o conjunto de todos os sistemas de equações afins

$$Ax = \mathbf{b} .$$

Então o grupo S_n das permutações de n elementos age sobre X por meio da permutação das linhas:

$$a(\sigma, [A, \mathbf{b}]) = [P_\sigma A, P_\sigma \mathbf{b}]$$

Essa ação deixa invariante o conjunto das soluções do sistema $Ax = \mathbf{b}$.

2. Pivoteamento

O algoritmo de pivoteamento, ou eliminação Gaussiana, é usualmente introduzido assim, como receita de bolo:

Algoritmo de *Eliminação Gaussiana*

Entradas: $n \in \mathbb{N}$, $A \in GL(n)$, $\mathbf{b} \in \mathbb{R}^n$.

Saídas: $\mathbf{x} \in \mathbb{R}^n$ tal que $A\mathbf{x} = \mathbf{b}$, se o sistema tiver solução única. Mensagem de erro, se isso não ocorrer.

- (1) Formar a matriz ampliada $\tilde{A} = [A, \mathbf{b}]$.
- (2) **De** $i = 1$ **até** n , **repetir:**
 - (3) **Se** $\tilde{A}_{ii} = 0$,
 - (4) **Então:**
 - (5) Achar $p \in \{i+1, \dots, n\}$ tal que $\tilde{A}_{pi} \neq 0$. Se tal p não existir, **Mensagem de erro.**
 - (6) Permutar as linhas i e p de $\tilde{A}$.
 - (7) **De** $j = i+1$ **até** n , **repetir:**
 - (8) Subtrair $\frac{\tilde{A}_{ji}}{\tilde{A}_{ii}}$ vezes a i -ésima linha de $\tilde{A}$ da j -ésima linha de $\tilde{A}$.
- (9) Resolver $\tilde{A} \begin{bmatrix} \mathbf{x} \\ -1 \end{bmatrix} = 0$ por substituição.

3. Interpretação como ação de grupo

Teorema 6.2. *Seja A uma matriz $n \times n$. Então existem uma matriz de permutação P , uma matriz triangular inferior L com uns na diagonal, e uma matriz triangular superior tais que*

$$A = PLU.$$

DEMONSTRAÇÃO. Vamos mostrar o Teorema por indução. No caso inicial $n = 1$, podemos fazer $P = 1$, $L = 1$ e $U = A$.

Para o caso geral, vamos assumir que o Teorema vale para matrizes $(n-1) \times (n-1)$. Seja A uma matriz $n \times n$, temos duas possibilidades. Se a primeira coluna de A é uniformemente zero, designamos por A' a submatriz formada retirando a primeira linha e a segunda coluna de A . Em notação por blocos,

$$A = \begin{bmatrix} 0 & A_{12} & \cdots & A_{1n} \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{bmatrix}.$$

Por indução, $A' = P'L'U'$. Temos agora a identidade (por blocos):

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & P' & & \\ 0 & & & \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & L' & & \\ 0 & & & \end{bmatrix} \begin{bmatrix} 0 & A_{12} & \cdots & A_{1n} \\ 0 & & & \\ \vdots & U' & & \\ 0 & & & \end{bmatrix}$$

Chamando as matrizes do lado direito, respectivamente, de P , L e U , verificamos que P é uma matriz de Permutação, L é triangular inferior e U é triangular superior.

Se a primeira coluna de A não é uniformemente zero, então existe uma matriz de permutação P'' tal que $C = (P''A)$ verifica $C_{11} \neq 0$. Logo, podemos definir A' por:

$$P''A = C = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ \frac{C_{21}}{C_{11}} & 1 & \cdots & 0 \\ \vdots & & \ddots & \\ \frac{C_{n1}}{C_{11}} & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ 0 & & & \\ \vdots & A' & & \\ 0 & & & \end{bmatrix}$$

Por indução, podemos fatorar $A' = P'L'U'$. Expandimos $C = P''A$ como:

$$P''A = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ \frac{C_{21}}{C_{11}} & 1 & \cdots & 0 \\ \vdots & & \ddots & \\ \frac{C_{n1}}{C_{11}} & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & P' & & \\ 0 & & & \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & L' & & \\ 0 & & & \end{bmatrix} \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ 0 & & & \\ \vdots & U' & & \\ 0 & & & \end{bmatrix}$$

Temos que resolver a seguinte dificuldade: a fatoração de A obtida não é da forma PLU . Gostaríamos de passar a matriz P para a esquerda. Pelo exercício 5.6 do Capítulo 5, podemos escrever:

$$A = P'' \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & P' & & \\ 0 & & & \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_2 & 1 & \cdots & 0 \\ \vdots & & \ddots & \\ l_n & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & L' & & \\ 0 & & & \end{bmatrix} \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ 0 & & & \\ \vdots & U' & & \\ 0 & & & \end{bmatrix}$$

onde os l_i são uma permutação dos $\frac{C_{n1}}{C_{11}}$, e obtemos a fatoração $A = PLU$ desejada. $\square$

Uma prova mais abstrata pode ser escrita na linguagem da Teoria dos Grupos. Seja L_r o conjunto das matrizes triangulares inferiores, da forma

$$L = \begin{bmatrix} L_1 & 0 \\ L_2 & I_{n-r, n-r} \end{bmatrix}.$$

Lema 6.3. L_r é um subgrupo de $L(n)$.

Seja P_r o grupo das matrizes de permutação que fixam $\mathbf{e}_1, \dots, \mathbf{e}_r$. P_r também é um subgrupo das matrizes de permutação. Temos agora as seguintes cadeias de subgrupos:

$$\{I\} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_{n-1},$$

$$\{I\} = P_n \subset P_{n-1} \subset \cdots \subset P_1 \subset P_0.$$

O procedimento de eliminação Gaussiana permite fatorar

$$l_{n-1}p_{n-2} \cdots p_2l_2p_1l_1p_0A = U,$$

onde $l_j \in L_j$ e $p_j \in P_j$. O exercício 5.6 do Capítulo 5 garante o seguinte resultado:

Lema 6.4. Se $l_j \in L_j$ e $p_j \in P_j$, então $p_j l_j p_{j-1} \in L_j$.

Se assimilamos $GL(n-r)$ ao grupo das matrizes que fixam $\mathbf{e}_1, \dots, \mathbf{e}_r$, então $P_r \subset GL(n-r)$ e teremos um resultado mais geral:

Lema 6.5. Se $l_j \in L_j$ e $x \in GL(n-j)$, então $x l_j x^{-1} \in L_j$.

(Verificar.) De modo geral, chama-se de *estabilizador* de um subgrupo $H \subset G$ o maior subgrupo S de G que torna H normal. Teremos sempre $H \subset S \subset G$. Tanto P_j quanto $GL(n-j)$ são subgrupos do estabilizador de L_j .

Desta maneira, podemos colecionar as permutações à direita, e teremos uma expressão:

$$l'_{n-1} \cdots l'_1 p_{n-2} \cdots p_0 A = U$$

e invertendo, $A = PLU$ como desejado.

4. Matrizes não necessariamente quadradas

Um corolário imediato do Teorema 6.2 é o seguinte:

Corolário 6.5.1. Seja A uma matriz $m \times n$. Então existem uma matriz de permutação P de tamanho $m \times m$, uma matriz triangular inferior L com uns na diagonal e de tamanho $m \times m$, e uma matriz triangular superior U de tamanho $m \times n$ tais que

$$A = PLU.$$

DEMONSTRAÇÃO. Se $n > m$, aplicamos o Teorema 6.2 à submatriz contendo apenas as m primeiras colunas de A . Se $n < m$, completamos a matriz A com zeros, aplicamos o Teorema e retiramos as últimas $m - n$ colunas de U . $\square$

O resultado acima não é satisfatório. Por exemplo, a matriz

$$U = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 3 \end{bmatrix}$$

é triangular superior. Isso não nos ajuda a resolver a equação $U\mathbf{x} = \mathbf{b}$.

Teorema 6.6. Seja A uma matriz $m \times n$. Então existem uma matriz de permutação P de tamanho $m \times m$, uma matriz de permutação P' de tamanho $n \times n$, uma matriz triangular inferior L com uns na diagonal e de tamanho $m \times m$, um inteiro $0 \leq k \leq m$ e uma matriz triangular superior U de tamanho $k \times n$ sem zeros na diagonal tais que

$$A = PL \begin{bmatrix} U \\ 0 \end{bmatrix} P'$$

O algoritmo para calcular essa decomposição é uma adaptação do algoritmo anterior.

Algoritmo de Eliminação Gaussiana com Pivoteamento Completo

Entradas: $n \in \mathbb{N}$, $A \in L(n, m)$.

Saídas: P , P' , L , k e U como no Teorema 6.6.

(1) Fazer $P = I_{m \times m}$, $P' = I_{n \times n}$, $L = I_{n \times n}$.

(2) De $i = 1$ até n , repetir:

- (3) Achar $p \in \{i, \dots, m\}$ e $j \in \{i, n\}$ tal que $|A_{pj}|$ seja maximal. Se $|A_{pj}| = 0$, ir para a linha 6.
- (4) Permutar as linhas i e p de A e de L , e as colunas i e p de P e de L . Permutar as colunas i e j de A e as linhas i e j de P' .
- (5) De $j = i + 1$ até n , Fazer $L_{ji} = \frac{A_{ji}}{A_{ii}}$. Subtrair L_{ji} vezes a i -ésima linha de A da j -ésima linha de A .
- (6) Fazer $k = i$ e U igual às primeiras k linhas de A .

Note que a variável A é modificada durante a execução do algoritmo, mas o produto $PLUP'$ permanece constante e igual ao valor inicial de A .

DEMONSTRAÇÃO DO TEOREMA 6.6. Vamos mostrar que o algoritmo acima produz a fatoração desejada. Note que P e P' são sempre, por construção, matrizes de permutação.

Antes de cada execução da linha (4), a matriz L pertence ao subgrupo L_{i-1} . Em outras palavras, ela é uma matriz triangular superior com uns na diagonal, e as colunas i até n só contêm zeros abaixo da diagonal. A permutação das linhas $i > p$ é um elemento do subgrupo P_{i-1} . Pelo Lema 6.4, as permutações da linha (4) mantêm $L \in L_{i-1}$. Após a execução da linha (5), $L \in L_i$ e o valor de i é incrementado.

Antes de cada execução da linha (3), a submatriz formada das primeiras $i - 1$ colunas de A é triangular superior. O algoritmo só acaba quando as linhas $i + 1$ a m se anularem, ou quando $i = n$. $\square$

5. Exercícios

Exercício 6.1. Verdade ou falso? (Justifique): $P \mapsto P^T$ é um isomorfismo do grupo das matrizes de permutação?

Exercício 6.2. Ache uma fatoração PLU de $A = \begin{bmatrix} 1 & 2 & 3 \\ 6 & 7 & 2 \\ 1 & 1 & -1 \end{bmatrix}$.

Exercício 6.3. Ache uma fatoração PLU de $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$.

Exercício 6.4. A fatoração PLU é única? Ache um exemplo de matriz admitindo duas fatorações diferentes, e um exemplo 2×2 admitindo apenas uma fatoração

Exercício 6.5. Ache todas as fatorações PLU de $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

Exercício 6.6. Usando a fatoração PLU , ache o conjunto das soluções de $Ax = b$, onde $A = \begin{bmatrix} 3 & 1 & 2 \\ 3 & 7 & -1 \\ -6 & 0 & -5 \end{bmatrix}$, e $b = \begin{bmatrix} 1 \\ 4 \\ -1 \end{bmatrix}$.

Exercício 6.7. Mesma pergunta, $b = \begin{bmatrix} 1 \\ 3 \\ -1 \end{bmatrix}$.

Exercício 6.8. Quantas fatorações *PLU* podem existir para uma matriz $n \times n$ inversível?

Exercício 6.9. Usando ainda a fatoração *PLU*, ache uma condição necessária e suficiente para uma matriz A de tamanho 2×2 não ser inversível.

Exercício 6.10. Implemente a fatoração *PLUP'* em linguagem *Julia*. Teste seu programa comparando exemplos, fatorados por *Julia*.

CAPÍTULO 7

Espaços, subespaços e dimensão

1. Sub-espaços



Seja E um espaço vetorial real. Um subespaço F de E é um subconjunto de E que é também um espaço vetorial. Existem essencialmente duas maneiras de se produzir subespaços vetoriais.

O espaço de todas as *combinações lineares* de $\mathbf{u}_1, \dots, \mathbf{u}_s$ é sempre um espaço vetorial, chamado de espaço ‘gerado’ por $\mathbf{u}_1, \dots, \mathbf{u}_s$.

Exemplo 7.1. As matrizes diagonais 2×2 são um espaço vetorial, gerado pelos “vetores” $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ e $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

Exemplo 7.2. Os polinômios da forma $f(x) = a + bx^9 + cx^{10}$ formam um espaço vetorial, gerado pelos “vetores” $1, x^9$ e x^{10} .

O outro procedimento é, dado um espaço vetorial E e um conjunto de equações lineares $L_1, \dots, L_r$ definir F como o espaço de vetores $\mathbf{u}$ tal que $L_1(\mathbf{u}) = \dots = L_r(\mathbf{u}) = 0$.

Exemplo 7.3. As soluções da equação diferencial $\ddot{x}(t) + 2\dot{x}(t) + x(t) = 0$ são um espaço vetorial, definido como o espaço dos “zeros” das equações lineares

$$\left(\left(\frac{\partial^2}{\partial t^2} + 2\frac{\partial}{\partial t} + 1 \right) (x(t)) \right) \Big|_{t=\tau} = 0$$

para todos os valores de $\tau \in \mathbb{R}$.

2. A imagem de uma matriz

Uma maneira mais metódica de se lidar com subespaços vetoriais do $\mathbb{R}^n$ é definir os espaços fundamentais associados a uma matriz. Seja A uma matriz $m \times n$, correspondendo a uma aplicação linear de $\mathbb{R}^n$ em $\mathbb{R}^m$.

Definição 7.4. A *imagem* de A é o espaço

$$\text{Im}(A) = \{A\mathbf{u} : \mathbf{u} \in \mathbb{R}^n\}.$$

Note que $\text{Im}(A) \subset \mathbb{R}^m$. Podemos também ver $\text{Im}(A)$ como o espaço gerado pelas colunas da matriz A .

De maneira análoga, $\text{Im}(A^T)$ é o espaço gerado pelas linhas da matriz A .

3. O núcleo de uma matriz

Definição 7.5. O núcleo de A é o espaço

$$\ker(A) = \{\mathbf{u} : A\mathbf{u} = \mathbf{0}\}$$

Note que o núcleo de A é um subespaço de $\mathbb{R}^m$. Se assumimos o produto interno canônico, podemos mostrar que o núcleo de A é o espaço dos vetores ortogonais a todas as linhas de A (exercício 7.3).

De maneira análoga, o núcleo de A^T é o espaço dos vetores ortogonais a todas as colunas de A . Chamamos o núcleo de A^T de *conúcleo* de A , e escrevemo-lo $\text{coker}(A)$.

4. Independência linear

Lembremos que uma *combinação linear* dos vetores $\mathbf{u}_1, \dots, \mathbf{u}_k \in \mathbb{R}^n$ é uma expressão da forma

$$\lambda_1 \mathbf{u}_1 + \lambda_2 \mathbf{u}_2 + \dots + \lambda_k \mathbf{u}_k = U\lambda$$

onde U é a matriz de colunas $\mathbf{u}_j$ e λ é o vetor de coordenadas λ_j . Quando λ é o vetor zero, dizemos que a combinação linear é *trivial*. O vetor zero é portanto combinação linear trivial para todo conjunto de vetores $\mathbf{u}_1, \dots, \mathbf{u}_k \in \mathbb{R}^n$.

Como o conjunto de todas as combinações lineares de $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k \in \mathbb{R}^n$ é exatamente o subespaço $\text{Im}U \subseteq \mathbb{R}^n$, podemos definir:

Definição 7.6. O subespaço vetorial *gerado* pelos vetores $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k \in \mathbb{R}^n$ é o espaço das combinações lineares de $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$. Chamaremos esse espaço de $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$.

Dado um subespaço vetorial $W \subseteq \mathbb{R}^n$, gostaríamos de representá-lo como $\text{Span}(\mathbf{u}_1, \dots, \mathbf{u}_k)$ para algum conjunto de vetores $\mathbf{u}_1, \dots, \mathbf{u}_k$. Todo vetor $\mathbf{w}$ de W passaria então a ser representado por pelo menos um $\lambda \in \mathbb{R}^k$, por meio da equação $\mathbf{w} = U\lambda$. Para isso basta achar um *conjunto gerador* $\{\mathbf{u}_1, \dots, \mathbf{u}_k\} \subseteq \mathbb{R}^n$ finito.

Mas para garantir a unicidade de λ dado $\mathbf{w}$, vamos precisar de uma condição adicional sobre o conjunto gerador. Precisaremos garantir que nenhum dos vetores $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ seja combinação linear dos outros.

A condição “um dos vetores $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ é combinação linear dos outros” é difícil de escrever literalmente em linguagem matemática. Uma formulação equivalente, mais elegante, é:

Definição 7.7. Os vetores $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k \in \mathbb{R}^n$ são *linearmente dependentes* quando o vetor zero é combinação linear não trivial de $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$.

A negação da condição acima é:

Definição 7.8. Os vetores $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k \in \mathbb{R}^n$ são *linearmente independentes* se e somente se

$$\lambda_1 \mathbf{u}_1 + \lambda_2 \mathbf{u}_2 + \dots + \lambda_k \mathbf{u}_k = \mathbf{0} \implies \lambda = \mathbf{0}$$

Lema 7.9. As colunas de uma matriz U são *linearmente independentes* se e somente se, $\ker U = \{\mathbf{0}\}$.

A prova é um exercício.

5. Bases e dimensão

Seja W um espaço vetorial.

Definição 7.10. Uma *base* do espaço vetorial W é uma d -upla de vetores $(\mathbf{u}_1, \dots, \mathbf{u}_d)$ linearmente independentes, e gerando o espaço W .

Proposição 7.11. Se $(\mathbf{u}_1, \dots, \mathbf{u}_d)$ e $(\mathbf{v}_1, \dots, \mathbf{v}_e)$ são bases de um mesmo espaço W , então $d = e$.

Antes de provar a Proposição 7.11, precisamos de um resultado preliminar:

Lema 7.12. Se A é uma matriz com mais linhas do que colunas, então seu conúcleo tem um vetor $\lambda \neq \mathbf{0}$.

DEMONSTRAÇÃO. Assumimos que A é de tamanho $m \times n$ onde $m > n$. Pelo Corolário 6.5.1, a matriz A admite uma fatoração da forma:

$$A = PLU$$

onde P é uma matriz de permutação, L uma matriz $n \times n$ triangular inferior com 1's na diagonal, e U é uma matriz triangular superior. Em particular, $U_{n+1,j} = 0$ para todo j . A equação $\lambda^T PL = \mathbf{e}_{n+1}$ admite uma solução diferente de zero, já que P e L são inversíveis. Temos então $\lambda^T A = 0$, e portanto $\lambda \in \text{coker} A$. $\square$

Agora voltamos à situação da Proposição 7.11.

Lema 7.13. Se $\mathbf{u}_1, \dots, \mathbf{u}_d$ são vetores linearmente independentes de W e se $\mathbf{v}_1, \dots, \mathbf{v}_e$ geram o espaço W , então $d \leq e$.

DEMONSTRAÇÃO. Assumimos por absurdo que $d > e$. Cada um dos vetores $\mathbf{u}_i$ pertence ao espaço W , e portanto é combinação linear dos $\mathbf{v}_j$. Sejam A_{ij} os coeficientes correspondentes de $\mathbf{u}_i$:

$$\mathbf{u}_i = \sum_{j=1}^e A_{ij} \mathbf{v}_j$$

A matriz A é de tamanho $d \times e$, e tem portanto mais linhas do que colunas. De acordo com o Lema 7.12, existe $\lambda \neq \mathbf{0} \in \mathbb{R}^d$ tal que

$$\lambda^T A = \mathbf{0}$$

Nesse caso,

$$\sum_{i=1}^d \lambda_i \mathbf{u}_i = \sum_{i=1}^d \sum_{j=1}^e \lambda_i A_{ij} \mathbf{v}_j = \sum_{j=1}^e \left(\sum_{i=1}^d \lambda_i A_{ij} \right) \mathbf{v}_j = \sum_{j=1}^e \mathbf{0} = \mathbf{0}$$

o que contradiz a independência linear dos vetores $\mathbf{u}_1, \dots, \mathbf{u}_d$. $\square$

DEMONSTRAÇÃO DA PROPOSIÇÃO 7.11. A prova da Proposição 7.11 é em duas partes. Primeiro, assumimos por absurdo que $d < e$ e aplicamos o Lema 7.13 para obter a contradição. Depois, assumimos que $d > e$ e aplicamos o mesmo Lema, trocando os $\mathbf{u}_i$ pelos $\mathbf{v}_j$, para obter a contradição. $\square$

Definição 7.14. Um espaço vetorial W tem *dimensão* (finita) d quando existe uma base $(\mathbf{u}_1, \dots, \mathbf{u}_d)$ de W . Escrevemos: $d = \dim(W)$.

Pelo que foi visto acima, essa dimensão é única sempre que existir. Por convenção, o espaço $\{0\}$ tem dimensão zero.

Proposição 7.15. Seja W um subespaço vetorial de $\mathbb{R}^n$. Então, W tem dimensão d para algum $d \leq n$.

DEMONSTRAÇÃO. Se $W = \{0\}$ então $d = 0$. Senão, existe pelo menos um vetor $\mathbf{u}_1 \in W$ diferente de zero.

Seja $R \subset \mathbb{N}$ o conjunto dos inteiros r , tais que existem vetores $\mathbf{u}_1, \dots, \mathbf{u}_r$ linearmente independentes em W . Pelo que foi visto acima, $1 \in R$.

Se $r' < r$ e $r \in R$, podemos tomar um subconjunto de r' dos $\mathbf{u}_i$. Os vetores deste subconjunto vão continuar linearmente independente, logo $r' \in R$. Pelo Lema 7.13, $n+1 \notin R$. Logo $R \subseteq \{1, 2, \dots, n\}$. Concluimos que R tem um máximo, que chamamos de d . $\square$

6. Dimensão infinita

O conceito de base ainda faz sentido para espaços vetoriais de dimensão infinita. Por exemplo, seja $\mathcal{P}$ o espaço vetorial real de todos os polinômios na variável x .

É preciso ter o seguinte cuidado: combinações lineares são combinações lineares **finitas**, ou seja combinações lineares de um número finito de 'vetores'. Podemos descrever $\mathcal{P}$ como o espaço das combinações lineares finitas dos vetores

$$1, x, x^2, x^3, \dots$$

Todo polinômio tem um grau, e se o grau for d ele se escreve de maneira única como combinação linear dos vetores $1, x, \dots, x^d$.

Outra base de $\mathcal{P}$ é dada pelos polinômios

$$\binom{x}{k} = \frac{x(x-1) \cdots (x-k+1)}{k!}$$

Observação 7.16. Um conceito diferente de combinação linear será estudado no Capítulo 24 (Ver Observação 24.1).

7. Exercícios

Exercício 7.1. Exiba o núcleo e a imagem de $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

Exercício 7.2. Exiba o núcleo e a imagem de $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$.

Exercício 7.3. Mostre que o núcleo de uma matriz A é o espaço dos vetores ortogonais a todas as linhas de A .

Exercício 7.4. O espaço E é soma direta dos seus subespaços F e G se e somente se todo vetor de E se escreve de maneira única como soma de um vetor de F e de um vetor de G . Mostre que, para toda matriz A de tamanho $m \times n$, $\mathbf{R}^n$ é soma direta dos espaços $\text{Im}(A^T)$ e $\ker(A)$.

Exercício 7.5. Qual é a relação entre $\ker(BA)$ e $\ker(A)$? Entre $\ker(A^T A)$ e $\ker(A)$?

Exercício 7.6. Sejam E e F subespaços vetoriais de $\mathbf{R}^n$. Quando é que $E \cup F$ é um espaço vetorial?

Exercício 7.7. Seja $\mathcal{P}$ o espaço de todos os polinômios de grau até 2 nas variáveis (x, y) . Descreva as equações de todas as cônicas passando pelos pontos $(1, 2)$ e $(1, 3)$, como subespaço de $\mathcal{P}$.

Exercício 7.8. Se E, G e $F = E \oplus G = \{(\mathbf{e}, \mathbf{g}) : \mathbf{e} \in E, \mathbf{g} \in G\}$ são espaços vetoriais, mostre que existe um homomorfismo de $GL(E)$ em $GL(F)$ com núcleo $\{I\}$.

Exercício 7.9. Seja A uma matriz $n \times n$ e seja $\lambda \in \mathbb{R}$. Definimos os dois seguintes conjuntos:

$$E_\lambda = \{\mathbf{u} \in \mathbb{R}^n : A\mathbf{u} = \lambda\mathbf{u}\} \quad \text{e} \quad E_\lambda^* = \{\mathbf{u} \in \mathbb{R}^n : \exists k \geq 0 : (A - \lambda I)^k \mathbf{u} = \mathbf{0}\}.$$

Mostre que E_λ e E_λ^* são espaços vetoriais.

Exercício 7.10. Ache um exemplo de matriz A e de $\lambda \in \mathbb{R}$ tais que $E_\lambda \subsetneq E_\lambda^*$.

Exercício 7.11. Prove o Lema 7.9

Exercício 7.12. Um *isomorfismo linear* é uma itransformação linear inversível, ou seja uma aplicação linear que é também uma bijeção, e cuja inversa é uma aplicação linear. Mostre, usando o Lema 7.9, que dada uma matriz U de tamanho $n \times k$, existem um isomorfismo linear entre $\text{Im} U$ e $\mathbb{R}^k$ se e somente se $\ker U = \{\mathbf{0}\}$.

Exercício 7.13. Se A um isomorfismo linear de $\mathbb{E}$ em $\mathbb{F}$ e seja U subespaço de $\mathbb{E}$ de dimensão finita. Mostrar que U e a sua imagem por A têm a mesma dimensão.

Exercício 7.14. Sejam $(\mathbf{u}_1, \dots, \mathbf{u}_d)$ e $(\mathbf{v}_1, \dots, \mathbf{v}_d)$ bases do espaço W , relacionadas por:

$$\mathbf{v}_j = \sum_{i=1}^d A_{ji} \mathbf{u}_i$$

Um mesmo vetor pode ser escrito como $\mathbf{w} = \sum_{i=1}^d x_i \mathbf{u}_i = \sum_{j=1}^d y_j \mathbf{v}_j$. Qual é a relação entre $\mathbf{x}$ e $\mathbf{y}$?

Exercício 7.15. Agora, seja $\mathbf{h}$ um elemento do espaço dual W (i.e., uma função linear a valores reais). Na base $(\mathbf{v}_1, \dots, \mathbf{v}_d)$, $\mathbf{h}$ se escreve:

$$\mathbf{h}(\sum y_j \mathbf{v}_j) = \sum_{j=1}^d g_j y_j.$$

Escreva $\mathbf{h}$ na base $(\mathbf{u}_1, \dots, \mathbf{u}_d)$. Como variam as coordenadas de $\mathbf{h}$ na nova base?

Exercício 7.16. Ainda na mesma notação, seja $B \in L(W, W)$. Nas coordenadas da base $(\mathbf{u}_1, \dots, \mathbf{u}_d)$, podemos representar B por uma matriz com coordenadas B_{ij} :

$$\sum_{i=1}^d x_i \mathbf{u}_i \mapsto \sum_{i,j=1}^d B_{ij} x_j \mathbf{u}_i.$$

Qual é a matriz correspondente na base $(\mathbf{v}_1, \dots, \mathbf{v}_d)$?

Exercício 7.17. Seja x uma variável real, e $\binom{x}{k}$ a notação do texto. Mostre que, se x for igual a um inteiro $d \geq k$, então $\binom{x}{k} = \binom{d}{k}$.

Exercício 7.18. Verifique que, para todo x real, vale $\binom{x}{k} + \binom{x}{k+1} = \binom{x+1}{k+1}$.

Exercício 7.19. Ache as coordenadas do polinômio x^d na base dos $\binom{x}{k}$.

Exercício 7.20. Seja W um subespaço de $\mathbb{R}^n$. Mostre que qualquer cadeia de inclusões de subespaços

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{r-1} \subsetneq V_r = W$$

é tal que $r \leq n$.

CAPÍTULO 8

O Teorema do Posto

1. Matrizes em forma escada



objetivo desta seção é mostrar o seguinte resultado:

Teorema 8.1 (do posto). *Seja A uma matriz $m \times n$. Então $\dim \operatorname{Im} A = \dim \operatorname{Im} A^T$. Além disso, $\dim(\ker A) + \dim(\operatorname{Im} A^T) = n$.*

O número $\operatorname{Posto}(A) = \dim \operatorname{Im} A = \dim \operatorname{Im} A^T$ é chamado de *posto* da matriz A .

A técnica tradicional para mostrar o Teorema 8.1 é uma variação da eliminação Gaussiana. Embora o Teorema também possa ser obtido a partir do Teorema 6.6, vamos manter a abordagem antiga. Começamos pelo caso fácil

Definição 8.2. Uma matriz E de tamanho $m \times n$ está em *forma escada* se e somente se existem $1 \leq j_1 < j_2 < \dots < j_r$, $r \leq \min(m, n)$, tais que:

- (1) A j_s -ésima coluna de E é o vetor $\mathbf{e}_s$.
- (2) Se $E_{ij} \neq 0$, então $i \leq r$ e $j_i \leq j$.

Exemplo 8.3. A matriz zero, a identidade, as matrizes $\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ e $\begin{bmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ estão em forma escada. As matrizes $\begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ e $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ não estão.

Convenção (só neste capítulo): a base canônica de $\mathbb{R}^m$ será denotada por $(\mathbf{e}_1, \dots, \mathbf{e}_m)$ enquanto a base canônica de $\mathbb{R}^n$ será denotada por $(\mathbf{f}_1, \dots, \mathbf{f}_n)$.

Se uma matriz E está em forma escada, então $(\mathbf{e}_1, \dots, \mathbf{e}_r)$ é uma base do espaço das colunas $\operatorname{Im} E$, enquanto $(\mathbf{f}_{j_1}, \mathbf{f}_{j_2}, \dots, \mathbf{f}_{j_r})$ é uma base do espaço das linhas $\operatorname{Im} E^T$. Logo, a proposição 8.1 vale para matrizes em forma escada, e $r = \operatorname{Posto}(E)$.

Podemos também construir os seguintes vetores, que pertencem ao núcleo de E . Se j não é um dos $j_1, \dots, j_r$, e i é o maior inteiro com $j_i < j$ (pode ser zero), fazemos:

$$\beta_j = \mathbf{f}_j - \sum_{k=1}^i E_{kj} \mathbf{f}_{j_k}$$

Deixamos para os exercícios os seguintes fatos:

Lema 8.4. Os vetores $(\dots \beta_j \dots)_{j \neq j_1, \dots, j_r}$ são uma base do núcleo de E .

Lema 8.5. O conjunto de soluções da equação afim $Ex = \mathbf{b}$ é dado por:

$$\mathcal{S} = \left\{ \sum_{j=1}^r b_s \mathbf{f}_{j_s} + \sum_{j \neq j_1, \dots, j_s} t_j \beta_j : \mathbf{t} \in \mathbb{R}^{n-r} \right\}$$

As variáveis t_j são chamadas de *variáveis livres*. O espaço de soluções $\mathcal{S}$ é um espaço afim de dimensão $n - r$. O Lema 8.4 também implica que $\dim \ker A + \dim \operatorname{Im} A^T = n$.

DEMONSTRAÇÃO DO TEOREMA 8.1. Seja A uma matriz $m \times n$. Vamos mostrar que existe um número finito p de transformações lineares W_k de $\mathbb{R}^n$, tais que

$$W_p W_{p-1} \cdots W_1 A = E$$

onde E está em forma escada. Como vimos no exercício 7.13 do Capítulo anterior, a dimensão de um subespaço e da sua imagem por uma transformação linear inversível são iguais. Assim,

$$\dim \operatorname{Im} A = \dim \operatorname{Im} W_1 A = \cdots = \dim W_p \cdots W_1 A = \dim E.$$

Por outro lado,

$$\operatorname{Im} A^T = \operatorname{Im}(W_1 A)^T = \cdots = \operatorname{Im}(W_p \cdots W_1 A)^T = \operatorname{Im} E^T$$

E disso concluímos que $\dim \operatorname{Im} A = \dim \operatorname{Im} A^T$. Além do que,

$$\ker A = \ker(W_1 A) = \cdots = \ker(W_p \cdots W_1 A) = \ker E.$$

Precisamos construir ainda as transformações W_k .

Hipótese de indução: Existem $W_1, \dots, W_r$ tais que a submatriz composta pelas primeiras r colunas de $A_r = W_r W_{r-1} \cdots W_1 A$ está em forma escada.

A Hipótese vale para $r = 0$. Assumindo que ela vale para um certo $r < n$, consideramos dois casos:

Caso 1: Se a submatriz composta pelas primeiras $r + 1$ colunas de A está em forma escada, fazemos $W_{r+1} = I$.

Caso 2: Existe pelo menos um $(A_r)_{i,r+1} \neq 0$ com $i > r$. Seja P uma permutação trocando a i -ésima e a $r + 1$ -ésima coordenada. Seja $\mathbf{c}$ a $r + 1$ -ésima coluna de $\frac{1}{(PA_r)_{r+1,r+1}} PA_r$, temos que $c_{r+1} = 1$. Seja agora

$$W = \begin{bmatrix} 1 & 0 & \cdots & 0 & -c_1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & -c_2 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & \cdots & 1 & -c_r & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & -c_{r+1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & 0 & \cdots & 0 & -c_{m-1} & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & -c_m & 0 & \cdots & 0 & 1 \end{bmatrix}$$

Então, $W \frac{1}{(PA_r)_{r+1,r+1}} PA_r$ tem as primeiras $r + 1$ colunas em forma escada. $\square$

Observação 8.6. Uma prova alternativa do Teorema acima utiliza a fatoração $A = PL \begin{bmatrix} U \\ 0 \end{bmatrix} P'$ do Teorema 6.6. A matriz $E = \begin{bmatrix} U \\ 0 \end{bmatrix} P'$ está na forma escada, e $E = L^{-1} P^T A$ onde L^{-1} e P^T são transformações lineares inversíveis.

2. Teorema do posto

Definição 8.7. Se W é um subespaço vetorial de $\mathbb{R}^n$, o *complemento ortogonal* de W , denotado por $W^\perp$, é o conjunto dos vetores de $\mathbb{R}^n$ ortogonais a W .

O trabalho difícil desta seção já está feito, falta colher o resultado.

Corolário 8.7.1. *Seja A matriz de tamanho $m \times n$, e de posto r . Então, $n = r + \dim \ker A^T$.*

Isso decorre do Teorema do posto (Teorema 8.1) aplicado à matriz A^T .

Corolário 8.7.2. *Seja A uma matriz de tamanho $m \times n$. Então, $\ker A$ é o complemento ortogonal de $\text{Im} A^T$, e $\text{Im} A^T$ é o complemento ortogonal de $\ker A$.*

DEMONSTRAÇÃO. Começamos pela observação de que, se $\mathbf{u} \in \ker A^T$ e $\mathbf{v} = A\mathbf{w} \in \text{Im} A$, então $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T A\mathbf{w} = 0$ e portanto, $\mathbf{u} \perp \mathbf{v}$.

Segue-se se $\ker A^T \subseteq (\text{Im} A)^\perp$ e que $\text{Im} A \subseteq (\ker A)^\perp$.

Sejam $(\mathbf{u}_1, \dots, \mathbf{u}_{n-r})$ base de $\ker A$ e $(\mathbf{v}_1, \dots, \mathbf{v}_r)$ base de $\text{Im} A^T$. Então $(\mathbf{u}_1, \dots, \mathbf{u}_{n-r}, \mathbf{v}_1, \dots, \mathbf{v}_r)$ são linearmente independentes. Como são n vetores, se eles não gerassem o $\mathbb{R}^n$, haveria $n+1$ vetores linearmente independentes, em contradição com a Proposição 7.11. Logo, $(\mathbf{u}_1, \dots, \mathbf{u}_{n-r}, \mathbf{v}_1, \dots, \mathbf{v}_r)$ é uma base do espaço $\mathbb{R}^n$. $\square$

Temos também a versão “dual” dos Corolários acima:

Corolário 8.7.3. *Seja A uma matriz de tamanho $m \times n$. Então, $\ker A^T$ é o complemento ortogonal de $\text{Im} A$, e $\text{Im} A$ é o complemento ortogonal de $\ker A^T$.*

Outro fato importante é:

Corolário 8.7.4. *Seja $W \subseteq \mathbb{R}^n$ um subespaço vetorial. Então, $(W^\perp)^\perp = W$.*

(Prova nos exercícios).

3. Aplicação à matemática discreta

Definição 8.8. Um *grafo* simples é um par $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ onde $\mathcal{V}$ é um conjunto finito (seus elementos são chamados de *vértices* e $\mathcal{E}$ é um conjunto de pares não ordenados de vértices diferentes (chamados de *arestas*)).

Por exemplo, um mapa rodoviário pode ser representado por um grafo onde as cidades são os vértices e as rodovias são as arestas. Uma rede elétrica pode ser representada como um grafo onde produtores e consumidores são vértices, e as linhas de transmissão são arestas.

Um problema relevante em grafos é saber quantos componentes conexos existem. Um componente conexo é um subgrafo dos vértices atingíveis a partir de um vértice fixo. No caso do mapa rodoviário, estaríamos contando as regiões isoladas das outras.

Outro problema relevante é achar um subgrafo minimal com todas os vértices do problema, e o menor número possível de arestas sem desconectar os componentes conexos.

Teorema 8.9. *O número de componentes conexos de um grafo $\mathcal{G}$, mais o número mínimo de arestas do subgrafo minimal, é igual ao número de vértices.*

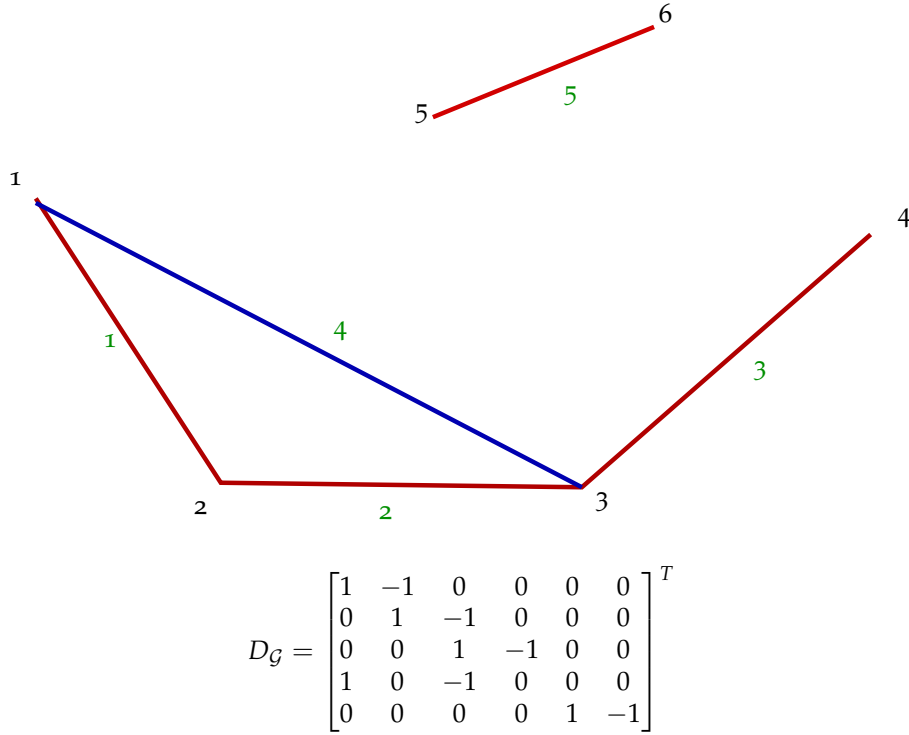


FIGURA 1. Exemplo de grafo e sua matriz de incidência. Os vértices estão numerados em preto, as arestas em verde.

DEMONSTRAÇÃO. A prova é uma consequência direta do Teorema do Posto: para cada aresta $\{u, v\} \in \mathcal{E}$, escolhemos um sentido (ou seja, um dos vértices u, v como sendo o início e o outro como sendo o fim).

A *matriz de incidência* do grafo $\mathcal{G}$ é uma matriz D_G de tamanho $\#\mathcal{V} \times \#\mathcal{E}$, construída assim: associamos um vértice a cada linha e uma aresta a cada coluna de $\mathcal{E}$. Para cada aresta $\{u, v\}$, colocamos $+1$ na posição $(v, \{u, v\})$ e -1 na posição $(u, \{u, v\})$. As outras coordenadas da matriz de incidência são 0.

O número de componentes conexos é então a dimensão do núcleo de D^T . Por outro lado, uma aresta pode ser removida sem desconectar o grafo quando ela é combinação linear de outras arestas. Assim, eliminação Gaussiana em D^T corresponde a retirar arestas sem desconectar nenhum componente do grafo. Concluímos que o número de arestas do subgrafo minimal é exatamente a dimensão de $\text{Im}D$. Agora é só aplicar o Teorema do Posto. $\square$

4. Exercícios

Exercício 8.1. Mostre o Lema 8.4

Exercício 8.2. Mostre o Lema 8.5

Exercício 8.3. Achar a forma escada da matriz $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Exercício 8.4. Achar a forma escada da matriz $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

Exercício 8.5. Mostre que um sistema de equações $A\mathbf{x} = \mathbf{b}$ (com A não necessariamente quadrada) tem solução se e somente se o posto de A é igual ao posto

da *matriz ampliada* $\hat{A} = \begin{bmatrix} A_{11} & \cdots & A_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ A_{m1} & \cdots & A_{mn} & b_m \end{bmatrix}$.

Exercício 8.6. Use forma escada da matriz ampliada para achar a solução geral de

$$\begin{bmatrix} 1 & 7 & 2 & 4 \\ 2 & 1 & 9 & 3 \\ 3 & 8 & 11 & 9 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}.$$

Exercício 8.7. Mesma pergunta, para

$$\begin{bmatrix} 0 & 2 & 0 & 1 \\ 1 & -1 & 2 & 1 \\ 1 & 8 & 1 & 2 \\ 3 & 8 & 5 & 5 \end{bmatrix} \mathbf{x} = \begin{bmatrix} 1 \\ -1 \\ 2 \\ 1 \end{bmatrix}.$$

Exercício 8.8. Mostre que a forma escada de uma matriz A não é única pela ação à esquerda de $GL(m)$, que a cada elemento $B \in GL(m)$ associa: $A \mapsto a(B, A) = BA$.

Exercício 8.9. Seja W um subespaço vetorial de $\mathbb{R}^n$ de dimensão d . Mostre que $W^\perp$ é um subespaço vetorial de $\mathbb{R}^n$, de dimensão $n - d$.

Exercício 8.10. Mostre o Corolário 8.7.4

CAPÍTULO 9

Determinante

1. Exemplos



noção de determinante é historicamente anterior à de matriz. Se queremos resolver o sistema de equações

$$\begin{cases} A_{11}x_1 + A_{12}x_2 = b_1 \\ A_{21}x_1 + A_{22}x_2 = b_2 \end{cases}$$

podemos eliminar a variável x_1 combinando as duas equações. Para isso, multiplicamos a primeira equação por $-A_{21}$ e a segunda por A_{11} . Obtemos:

$$\begin{vmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{vmatrix} x_2 = \begin{vmatrix} A_{11} & b_1 \\ A_{21} & b_2 \end{vmatrix}$$

com a notação $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$. Da mesma maneira, podemos eliminar a segunda variável e obter:

$$\begin{vmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{vmatrix} x_1 = \begin{vmatrix} b_1 & A_{12} \\ b_2 & A_{22} \end{vmatrix}.$$

Ambas equações podem ser resolvidas para todo $\mathbf{b}$ se e somente se a expressão $A_{11}A_{22} - A_{12}A_{21}$ for diferente de zero. O mesmo procedimento pode ser feito para sistemas de três equações em três variáveis. Dado o sistema

$$\begin{cases} A_{11}x_1 + A_{12}x_2 + A_{13}x_3 = b_1 \\ A_{21}x_1 + A_{22}x_2 + A_{23}x_3 = b_2 \\ A_{31}x_1 + A_{32}x_2 + A_{33}x_3 = b_3 \end{cases},$$

eliminamos a variável x_1 de cada conjunto possível de duas equações, obtendo:

$$\begin{cases} \begin{vmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{vmatrix} x_2 + \begin{vmatrix} A_{11} & A_{13} \\ A_{21} & A_{23} \end{vmatrix} x_3 = \begin{vmatrix} A_{11} & b_1 \\ A_{21} & b_2 \end{vmatrix} \\ \begin{vmatrix} A_{21} & A_{22} \\ A_{31} & A_{32} \end{vmatrix} x_2 + \begin{vmatrix} A_{21} & A_{23} \\ A_{31} & A_{33} \end{vmatrix} x_3 = \begin{vmatrix} A_{21} & b_2 \\ A_{31} & b_3 \end{vmatrix} \\ \begin{vmatrix} A_{31} & A_{32} \\ A_{11} & A_{12} \end{vmatrix} x_2 + \begin{vmatrix} A_{31} & A_{33} \\ A_{11} & A_{13} \end{vmatrix} x_3 = \begin{vmatrix} A_{31} & b_3 \\ A_{11} & b_1 \end{vmatrix} \end{cases}.$$

Podemos eliminar a variável x_2 multiplicando cada uma das equações, respectivamente, por A_{32} , A_{12} e A_{22} (conferir !) Obtemos que:

$$\begin{vmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{vmatrix} x_3 = \begin{vmatrix} A_{11} & A_{12} & b_1 \\ A_{21} & A_{22} & b_2 \\ A_{31} & A_{32} & b_3 \end{vmatrix},$$

onde convencionamos que

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - ceg - afh - bdi.$$

(Soma das diagonais diretas, menos soma das antidiagonais). O mesmo método pode ser estendido para dimensões arbitrárias, mas a expressão do “determinante” é bem mais complicada. No caso do determinante 4×4 , aparecem 24 termos. No determinante $n \times n$, aparecem $n!$ termos. Não é verdade portanto que o determinante $n \times n$, $n > 3$ seja a soma das diagonais diretas menos a soma das antidiagonais.

2. Formas anti-simétricas

Definição 9.1. Seja E um espaço vetorial real. Uma função

$$f : \underbrace{E \times E \times \cdots \times E}_{k \text{ vezes}} \rightarrow \mathbb{R}$$

$$(\mathbf{u}_1, \dots, \mathbf{u}_k) \mapsto f(\mathbf{u}_1, \dots, \mathbf{u}_k)$$

é k -linear se e somente se, ela é linear em cada um dos argumentos u_k :

$$\begin{aligned} f(\lambda \mathbf{u}_1 + \mu \mathbf{u}'_1, \mathbf{u}_2, \dots, \mathbf{u}_k) &= \lambda f(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k) + \mu f(\mathbf{u}'_1, \mathbf{u}_2, \dots, \mathbf{u}_k) \\ f(\mathbf{u}_1, \lambda \mathbf{u}_2 + \mu \mathbf{u}'_2, \dots, \mathbf{u}_k) &= \lambda f(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k) + \mu f(\mathbf{u}_1, \mathbf{u}'_2, \dots, \mathbf{u}_k) \\ &\vdots \\ f(\mathbf{u}_1, \mathbf{u}_2, \dots, \lambda \mathbf{u}_k + \mu \mathbf{u}'_k) &= \lambda f(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k) + \mu f(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}'_k) \end{aligned}$$

Por exemplo, se $\langle \cdot, \cdot \rangle$ é um produto interno, a função $f(\mathbf{u}, \mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle$ é 2-linear (dizemos forma ou função *bilinear*). A função $D(\mathbf{u}, \mathbf{v}) = u_1 v_2 - u_2 v_1$ também é uma função bilinear de $\mathbb{R}^2$.

Definição 9.2. Uma função f que é k linear em E é chamada de *forma k -linear simétrica* se ela é invariante por qualquer permutação σ de seus argumentos:

$$f(\mathbf{u}_{\sigma(1)}, \mathbf{u}_{\sigma(2)}, \dots, \mathbf{u}_{\sigma(k)}) = f(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$$

Ela é chamada de *forma k -linear anti-simétrica* ou *alternada* quando ela é invariante por permutações pares, e muda de sinal para permutações ímpares:

$$g(\mathbf{u}_{\sigma(1)}, \mathbf{u}_{\sigma(2)}, \dots, \mathbf{u}_{\sigma(k)}) = (-1)^{|\sigma|} g(\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k)$$

Para verificar simetria ou anti-simetria, basta verificar o comportamento da função quando dois dos argumentos são trocados de lugar, e os outros mantidos. Se o valor não é nunca alterado, a função é simétrica. Se o sinal é trocado sempre, a função é anti-simétrica.

Os determinantes de matrizes 2×2 e 3×3 são funções bilineares (resp. trilineares) nas linhas da matriz, anti-simétricas e que valem 1 na identidade. Vamos utilizar essas propriedades para definir o determinante em dimensão maior.

Teorema 9.3. Existe uma única função $\det : L(\mathbb{R}^n, \mathbb{R}^n) \rightarrow \mathbb{R}$, chamada de determinante de uma matriz, com as seguintes propriedades:

- (1) $\det(A)$ é n -linear nas linhas da matriz A .
- (2) $\det(A)$ é anti-simétrica nas linhas da matriz A .
- (3) $\det(I) = 1$.

A função $\det$ é dada pela fórmula de Leibniz:

$$\det(A) = \sum_{\sigma \in S_n} (-1)^{|\sigma|} A_{1\sigma(1)} A_{2\sigma(2)} \cdots A_{n\sigma(n)}.$$

Corolário 9.3.1. $\det(A) = \det(A^T)$.

DEMONSTRAÇÃO. Vimos que toda permutação σ se escreve como produto de permutações elementares,

$$\sigma = (i_k j_k) \cdots (i_2 j_2)(i_1 j_1)$$

onde escolhemos k minimal, de modo a ter $|\sigma| = k$. A sua inversa é

$$\sigma^{-1} = (i_1 j_1)(i_2 j_2) \cdots (i_k j_k)$$

e portanto $|\sigma^{-1}| = k = |\sigma|$. Deste modo,

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_n} (-1)^{|\sigma|} A_{1\sigma(1)} A_{2\sigma(2)} \cdots A_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} (-1)^{|\sigma^{-1}|} A_{\sigma^{-1}(1)1} A_{\sigma^{-1}(2)1} \cdots A_{\sigma^{-1}(n)n} \\ &= \sum_{\tau \in S_n} (-1)^{|\tau|} A_{\tau(1)1} A_{\tau(2)1} \cdots A_{\tau(n)n} \\ &= \det(A^T) \end{aligned}$$

□

3. Funções multilineares anti-simétricas

O Teorema 9.3 pode ser mostrado diretamente, mas vamos mostra-lo a partir das propriedades do espaço das funções multilineares anti-simétricas.

Lema 9.4. *Seja f uma função k -linear anti-simétrica.*

- (1) Se $\mathbf{u}_i = \mathbf{u}_j$ para algum $i \neq j$, então $f(\mathbf{u}_1, \dots, \mathbf{u}_k) = 0$.
- (2) Se $\mathbf{u}'_j = \mathbf{u}_j + \mathbf{u}_i$ para algum $j \neq i$, então $f(\mathbf{u}_1, \dots, \mathbf{u}_{j-1}, \mathbf{u}'_j, \mathbf{u}_{j+1}, \dots, \mathbf{u}_k) = f(\mathbf{u}_1, \dots, \mathbf{u}_k)$.

DEMONSTRAÇÃO. Para o ítem (1), seja $\sigma = (i j)$ a permutação que troca j com i e preserva os outros elementos. Então,

$$f(\mathbf{u}_{\sigma(1)}, \dots, \mathbf{u}_{\sigma(k)}) = -f(\mathbf{u}_1, \dots, \mathbf{u}_k).$$

Como os dois valores são iguais, $f(\mathbf{u}_1, \dots, \mathbf{u}_k) = 0$. O ítem (2) pode então ser deduzido por linearidade:

$$\begin{aligned} f(\mathbf{u}_1, \dots, \mathbf{u}_{j-1}, \mathbf{u}'_j, \mathbf{u}_{j+1}, \dots, \mathbf{u}_k) &= f(\mathbf{u}_1, \dots, \mathbf{u}_{j-1}, \mathbf{u}_i, \mathbf{u}_{j+1}, \dots, \mathbf{u}_k) + f(\mathbf{u}_1, \dots, \mathbf{u}_k) \\ &= f(\mathbf{u}_1, \dots, \mathbf{u}_k). \end{aligned}$$

□

Vamos chamar de $A^k = A^k(E)$ o espaço das funções k -lineares anti-simétricas em um espaço vetorial E . Em particular, $A^0(E) = \mathbb{R}$ são as funções constantes e

$A^1(E) = E^*$ é o espaço dual de E . No caso $E = \mathbb{R}^n$, havíamos definido a base canônica $(e_1, e_2, \dots, e_n)$ como

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots \quad e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

A base dual é denotada por $(dx_1, dx_2, \dots, dx_n)$ onde $dx_i \in A^1(\mathbb{R}^n) = (\mathbb{R}^n)^*$ é a função $x \mapsto x_i$. Para definir uma base em $A^k(\mathbb{R}^n)$, procedemo em duas etapas. Para todo multi-índice $\mathbf{i} = (i_1, \dots, i_k)$,

$$\begin{aligned} dx_{i_1} \otimes dx_{i_2} \otimes \dots \otimes dx_{i_k} : \mathbb{R}^n \times \dots \times \mathbb{R}^n &\rightarrow \mathbb{R} \\ \mathbf{u}_1, \dots, \mathbf{u}_k &\mapsto (\mathbf{u}_1)_{i_1} (\mathbf{u}_2)_{i_2} \dots (\mathbf{u}_k)_{i_k} \end{aligned}$$

é uma função k -linear em $\mathbb{R}^k$. Uma base para o espaço de todas as funções k -lineares em $\mathbb{R}^k$ é dado pelas funções $dx_{i_1} \otimes dx_{i_2} \otimes \dots \otimes dx_{i_k}$ para todos os multi-índices $\mathbf{i}$ possíveis. Para se obter funções k -lineares anti-simétricas, fazemos a média sobre todas as permutações com peso ± 1 :

$$dx_{i_1} \wedge dx_{i_2} \wedge \dots \wedge dx_{i_k} = \sum_{\sigma \in S_k} (-1)^{|\sigma|} dx_{i_{\sigma(1)}} \otimes dx_{i_{\sigma(2)}} \otimes \dots \otimes dx_{i_{\sigma(k)}}.$$

Por exemplo em $\mathbb{R}^3$,

$$dx_1 \wedge dx_2(\mathbf{u}, \mathbf{v}) = u_1 v_2 - u_2 v_1$$

e

$$dx_1 \wedge dx_2 \wedge dx_3(\mathbf{u}, \mathbf{v}, \mathbf{w}) = u_1 v_2 w_3 + u_2 v_3 w_1 + u_3 v_1 w_2 - u_3 v_2 w_1 - u_1 v_3 w_2 - u_2 v_1 w_3.$$

Note que por força do Lema 9.4, $dx_{i_1} \wedge dx_{i_2} \wedge \dots \wedge dx_{i_k} = 0$ se algum dos índices for repetido.

Lema 9.5. *Seja $0 \leq k \leq n$. Então $(\dots, dx_{i_1} \wedge dx_{i_2} \wedge \dots \wedge dx_{i_k}, \dots)_{1 \leq i_1 < i_2 < \dots < i_k \leq n}$ é uma base de $A^k(\mathbb{R}^n)$.*

DEMONSTRAÇÃO. Seja $f \in A^k(\mathbb{R}^n)$. Sejam $\mathbf{u}_1, \dots, \mathbf{u}_k \in \mathbb{R}^n$ e escrevemos $u_{ij} = (\mathbf{u}_i)_j$. Expandimos por linearidade:

$$f(\mathbf{u}_1, \dots, \mathbf{u}_k) = \sum_{i_1, \dots, i_k=1}^n u_{1i_1} u_{2i_2} \dots u_{ki_k} f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_k}).$$

Como índices repetidos anulam $f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_k})$, podemos assumir os índices diferentes dois a dois. Portanto estamos somando sobre os $1 \leq i_1 < i_2 < \dots < i_n \leq n$ e depois sobre as permutações de $i_1, \dots, i_k$. Como f é anti-simétrica,

$$f(\mathbf{u}_1, \dots, \mathbf{u}_k) = \sum_{1 \leq i_1 < i_2 < \dots < i_n \leq n} \sum_{\sigma \in S_k} (-1)^{|\sigma|} u_{1i_{\sigma(1)}} u_{2i_{\sigma(2)}} \dots u_{ki_{\sigma(k)}} f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_k}).$$

Ou seja,

$$f(\mathbf{u}_1, \dots, \mathbf{u}_k) = \sum_{1 \leq i_1 < i_2 < \dots < i_n \leq n} dx_{i_1} \wedge dx_{i_2} \wedge \dots \wedge dx_{i_k} f(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_k}).$$

Falta verificar a independência linear das $dx_{i_1} \wedge dx_{i_2} \wedge \dots \wedge dx_{i_k}$. Suponha que

$$S = \sum_{1 \leq i_1 < i_2 < \dots < i_n \leq n} f_{\mathbf{i}} dx_{i_1} \wedge dx_{i_2} \wedge \dots \wedge dx_{i_k} = 0$$

com pelo menos um coeficiente $f_{\mathbf{j}} \neq 0$. Então,

$$S(\mathbf{e}_{j_1}, \dots, \mathbf{e}_{j_k}) = f_{\mathbf{j}} \neq 0,$$

contradição. $\square$

Uma consequência imediata é que $\dim A^k(\mathbb{R}^n) = \binom{n}{k}$. Em particular, $\dim A^n(\mathbb{R}^n) =$

1. O Teorema 9.3 segue diretamente do Lema 9.5, sendo a fórmula de Leibniz a forma $dx_1 \wedge dx_2 \wedge \cdots \wedge dx_n$ aplicada às linhas de A .

4. Multiplicatividade do determinante

Teorema 9.6. Se A e B são matrizes de tamanho $n \times n$, então

$$\det(AB) = \det(A) \det(B).$$

Em particular, se A for inversível, $\det(A) \det(A^{-1}) = 1$.

DEMONSTRAÇÃO. Vamos assumir inicialmente que $\det B \neq 0$. Seja $D(A) = \frac{\det(AB)}{\det B}$. Vamos mostrar que a função $D(A)$ é o determinante de A .

- (1) Sejam $\mathbf{a}_1, \dots, \mathbf{a}_n$ as linhas de A , $\mathbf{a}_i = [A_{i1} \ A_{i2} \ \dots \ A_{in}]$. Então as linhas de AB são $\mathbf{a}_1 B, \dots, \mathbf{a}_n B$. Assim,

$$D(AB) = D(\mathbf{a}_1 B, \dots, \mathbf{a}_n B)$$

é linear em cada uma das $\mathbf{a}_i$.

- (2) Pelo mesmo argumento, permutações das linhas de A correspondem a permutações das linhas de AB , e trocam o sinal de $D(AB)$ de acordo com a paridade da permutação. Logo D é anti-simétrica.

- (3) $D(I) = \det(B) / \det(B) = 1$.

Agora, consideramos o caso $\det(B) = 0$. Sejam $\mathbf{b}_1, \dots, \mathbf{b}_n$ as linhas de B . Cada linha de AB pode ser interpretada como uma combinação linear das linhas de B . Por exemplo, a i -ésima linha de AB é

$$[\sum_{j=1}^n A_{ij} \mathbf{b}_j.]$$

Expandindo o determinante de AB como função das linhas de B , recuperamos uma soma onde cada termo se anula. $\square$

Corolário 9.6.1. A é inversível se e somente se $\det(A) \neq 0$.

DEMONSTRAÇÃO. Se A é inversível, temos que $\det(A) \det(A^{-1}) = \det(I) = 1$, logo $\det(A) \neq 0$. Se A não é inversível, então A tem posto $< n$. Pelo Teorema do Posto, o $\dim \text{coker}(A) \geq 1$, e portanto existe $\mathbf{u} \neq 0$ tal que $\mathbf{u}^T A = \mathbf{0}$. Em outras palavras, uma das linhas de A é combinação linear das outras. Usando o Lema 9.4, deduzimos que $\det(A) = 0$. $\square$

Corolário 9.6.2. O determinante é um homomorfismo de $GL(n)$ no grupo multiplicativo dos reais $(\mathbb{R} \setminus \{0\}, \times)$.

DEMONSTRAÇÃO. Pelo corolário anterior, o determinante de qualquer $A \in GL(n)$ é diferente de zero. O Teorema implica que $\det(AB) = \det(A) \det(B)$, e que $\det(A^{-1}) = 1 / \det(A)$. Logo o determinante é um homomorfismo. $\square$

5. Cofatores

Definição 9.7. Seja A uma matriz de tamanho $n \times n$, $n \geq 2$, inversível. Denotamos por A_{ij} a matriz obtida removendo a i -ésima linha e a j -ésima coluna de A . A matriz dos cofatores de A é a matriz C definida por

$$C_{ij} = (-1)^{i+j} \det A_{ij}.$$

Quando $n = 1$, fazemos $C_{11} = 1$.

O determinante pode ser expandido em cofatores, pela fórmula abaixo:

Lema 9.8. *Seja A uma matriz $n \times n$. Seja $1 \leq j \leq n$. Então*

$$\det(A) = \sum_{i=1}^n A_{ij} C_{ij}$$

DEMONSTRAÇÃO. Para cada valor de j , definimos C_{ij} como o fator de A_{ij} em $\det(A)$:

$$C_{ij} = \det \begin{pmatrix} \begin{bmatrix} A_{11} & \dots & A_{1,j-1} & 0 & A_{1,j+1} & \dots & A_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{i-1,1} & \dots & A_{i-1,j-1} & 0 & A_{i-1,j+1} & \dots & A_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ A_{i+1,1} & \dots & A_{i+1,j-1} & 0 & A_{i+1,j+1} & \dots & A_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{n1} & \dots & A_{n,j-1} & 0 & A_{n,j+1} & \dots & A_{nn} \end{bmatrix} \end{pmatrix}.$$

Esta é uma função multilinear simétrica das linhas de $\det A_{ij}$. Quando A_{ij} é a identidade, e pode ser facilmente levada na identidade por $|i - j|$ permutações elementares de suas linhas. Por exemplo, se $i < j$, permutam-se as linhas i e $i + 1$, depois $i + 1$ e $i + 2$, até finalmente $j - 1$ e j . $\square$

Proposição 9.9. *Seja A uma matriz de tamanho $n \times n$ inversível. Então*

$$A^{-1} = \frac{1}{\det(A)} C^T$$

DEMONSTRAÇÃO. Multiplicando C^T por A , obtemos nas coordenadas (i, j) :

$$(C^T A)_{ij} = \sum_{k=1}^n C_{ki} A_{kj}$$

que é o determinante da matriz obtida sobre-escrevendo a j -ésima linha de A sobre a i -ésima linha. Quando $i \neq j$, o determinante é zero. Quando $i = j$, recuperamos o determinante de A . $\square$

Concluimos com a regra de Cramer para dimensão qualquer:

Proposição 9.10. *Seja A uma matriz de tamanho $n \times n$, inversível. Então equação $A\mathbf{x} = \mathbf{b}$ admite como solução única o vetor $\mathbf{x}$ de coordenadas*

$$x_i = \frac{\det(A_i)}{\det(A)},$$

onde A_i é a matriz obtida substituindo a i -ésima coluna de A por $\mathbf{b}$.

DEMONSTRAÇÃO. Expandimos $\mathbf{x} = A^{-1}\mathbf{b}$ pela fórmula dos cofatores:

$$x_i = \frac{1}{\det(A)} \sum_{j=1}^n (A^{-1})_{ij} b_j = \frac{1}{\det(A)} \sum_{j=1}^n C_{ji} b_j = \frac{\det(A_i)}{\det(A)}$$

$\square$

6. Volume e área

A área do paralelogramo $(0, \mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{v}) = \{x\mathbf{u} + y\mathbf{v} : x, y \in [0, 1]\}$ pode ser definida como

$$A((0, \mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{v})) = |\det [\mathbf{u} \quad \mathbf{v}]|.$$

Essa definição tem as seguintes propriedades (usuais da área):

- (1) O quadrado unitário tem área 1.
- (2) $A(0, \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v} + \mathbf{w}, \mathbf{w}) = |A(0, \mathbf{u}, \mathbf{u} + \mathbf{w}, \mathbf{w}) \pm A(0, \mathbf{v}, \mathbf{v} + \mathbf{w}, \mathbf{w})|$, onde o sinal é positivo sse $\mathbf{u}$ e $\mathbf{v}$ estão no mesmo semiplano delimitado pela linha $(0\mathbf{w})$.
- (3) $A(0, \lambda\mathbf{u}, \lambda\mathbf{u} + \mu\mathbf{v}, \mu\mathbf{v}) = |\lambda||\mu|A(0, \mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{v})$

Pode também ser estendida por translação a paralelepípedos quaisquer, e por um processo limite a figuras geométricas usuais (Essa discussão pertence ao curso de Cálculo Infinitesimal).

Uma boa definição de volume é obtida de maneira análoga: O *volume* do paralelepípedo $\{x\mathbf{u} + y\mathbf{v} + z\mathbf{w} : x, y, z \in [0, 1]\}$ é $|\det [\mathbf{u} \ \mathbf{v} \ \mathbf{w}]|$.

Também pode-se definir área orientada (e volume orientado) tirando o valor absoluto da definição:

$$A^{\text{or}}((0, \mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{v})) = \det [\mathbf{u} \ \mathbf{v}].$$

A definição de área orientada é mais elegante !

- (1) O quadrado unitário tem área 1.
- (2) $A^{\text{or}}(0, \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v} + \mathbf{w}, \mathbf{w}) = A^{\text{or}}(0, \mathbf{u}, \mathbf{u} + \mathbf{w}, \mathbf{w}) + A^{\text{or}}(0, \mathbf{v}, \mathbf{v} + \mathbf{w}, \mathbf{w})$.
- (3) $A^{\text{or}}(0, \lambda\mathbf{u}, \lambda\mathbf{u} + \mu\mathbf{v}, \mu\mathbf{v}) = \lambda\mu A^{\text{or}}(0, \mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{v})$

Em geral, podemos definir o volume para paralelotos de qualquer dimensão via determinantes:

$$\text{Vol}(\{A\mathbf{x} : \mathbf{x} \in [0, 1]^n\}) = |\det(A)|$$

$$\text{Vol}^{\text{or}}(\{A\mathbf{x} : \mathbf{x} \in [0, 1]^n\}) = \det(A)$$

Note que se $B \in GL(n)$ e $\mathcal{W} = \{A\mathbf{x} : \mathbf{x} \in [0, 1]^n\}$, teremos sempre

$$\text{Vol}(B\mathcal{W}) = |\det(B)|\text{Vol}(\mathcal{W})$$

e

$$\text{Vol}^{\text{or}}(B\mathcal{W}) = \det(B)\text{Vol}^{\text{or}}(\mathcal{W}).$$

Em geral, vale o seguinte fato:

Teorema 9.11. *Seja $\mathcal{W} \subset \mathbb{R}^n$ um conjunto com volume finito, e seja $B : \mathbb{R}^n \rightarrow \mathbb{R}^n$ uma transformação linear. Então,*

$$\text{Vol}(B\mathcal{W}) = |\det(B)|\text{Vol}(\mathcal{W})$$

e

$$\text{Vol}^{\text{or}}(B\mathcal{W}) = \det(B)\text{Vol}^{\text{or}}(\mathcal{W}).$$

Deixamos a demonstração (e a definição de conjuntos com volume) para o curso de Cálculo.

7. Exercícios

Exercício 9.1. Calcule o determinante de $\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$

Exercício 9.2. Calcule o determinante de $\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 2 & 2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & & 0 \\ n & n & n & \dots & n \end{bmatrix}$

Exercício 9.3. Seja A uma matriz com coeficientes inteiros, inversível e com inversa a coeficientes inteiros. Mostre que $\det(A) = \pm 1$.

Exercício 9.4. Sejam a e b inteiros. Mostre que existem c e d inteiros tais que $\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = 1$, se e somente se a e b são relativamente primos (i.e., $\text{mdc}(a, b) = 1$)

Exercício 9.5. Seja A uma matriz com coeficientes reais, de módulo menor ou igual a H . Mostre que $|\det A| \leq (\sqrt{n}H)^n$.

Exercício 9.6. O simplexo unitário é o conjunto dos pontos $\mathbf{x} \in \mathbb{R}^n$ tais que $0 < x_j < 1$ e $\sum_j x_j < 1$. Mostre que existe uma bijeção linear f levando a região $0 < x_1 < \dots < x_n < 1$ no simplexo unitário, e com $\det f = 1$ (ou seja, preserva volume). Deduza que o simplexo unitário tem volume $1/n!$.

Exercício 9.7. Explique como calcular o determinante usando a fatoração PLU . Quantas multiplicações são necessárias? Compare com a fórmula do Teorema 9.3

Exercício 9.8. Calcule o determinante de

$$\begin{bmatrix} 1 & 2 & -3 & 3 \\ -1 & 2 & 1 & 1 \\ 3 & 2 & -1 & 0 \\ 1 & 1 & 2 & 7 \end{bmatrix}$$

Exercício 9.9. Sejam $a, b, c, d, e, f \in \mathbb{R}$. Defina u, v, w pela expressão:

$$\det \begin{pmatrix} a & d & x \\ b & e & y \\ c & f & z \end{pmatrix} = ux + vy + wz.$$

Isso define o *produto exterior* em $\mathbb{R}^3$,

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} \wedge \begin{bmatrix} d \\ e \\ f \end{bmatrix} = \begin{bmatrix} u \\ v \\ w \end{bmatrix}.$$

Mostre que $\begin{bmatrix} u \\ v \\ w \end{bmatrix}$ é ortogonal aos outros dois vetores. Calcule o seu módulo em função do módulo dos outros dois vetores e do ângulo entre eles.

Exercício 9.10. Sejam $\zeta_1, \dots, \zeta_n \in \mathbb{R}$. A *matriz de Vandermonde* associada aos ζ_i é:

$$V(\zeta_1, \dots, \zeta_n) = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \zeta_1 & \zeta_2 & \dots & \zeta_n \\ \zeta_1^2 & \zeta_2^2 & \dots & \zeta_n^2 \\ \vdots & \vdots & & \vdots \\ \zeta_1^{n-1} & \zeta_2^{n-1} & \dots & \zeta_n^{n-1} \end{bmatrix}$$

Mostre que o determinante da matriz de Vandermonde se anula se e somente se existem $i \neq j$ tais que $\zeta_i = \zeta_j$.

Exercício 9.11. Defina o operador $\wedge : A^k(\mathbb{R}^n) \times A^l(\mathbb{R}^n) \rightarrow A^{k+l}(\mathbb{R}^n)$ compatível com as notações deste capítulo, de maneira a ter associatividade:

$$\omega \wedge (\eta \wedge \phi) = (\omega \wedge \eta) \wedge \phi$$

Problema em aberto N^o 2. O *permanente* de uma matriz A de tamanho $n \times n$ é definido por:

$$\text{Per}(A) = \sum_{\sigma \in S_n} A_{1\sigma(1)} A_{2\sigma(2)} \cdots A_{n\sigma(n)}.$$

Vimos no exercício 9.7 que é possível calcular o determinante de uma matriz $n \times n$ em tempo polinomial em n (ou seja, existem constantes c e d tais que o número de multiplicações é limitado superiormente pelo polinômio cn^d). O problema é: *Mostrar que existem c e d tais que para cada n , o permanente $n \times n$ pode ser calculado em no máximo cn^d operações de soma e multiplicação (vale também utilizar constantes, mas não valem comparações), ou mostrar que tais c e d não podem existir.*

Observação 9.12. O problema acima é equivalente a um problema central em ciência da computação, a hipótese $VP \neq VNP$ de Valiant¹. O modelo de Valiant é um modelo alternativo de computação, e essa conjectura é análoga à famosa conjectura $P \neq NP$.

Problema em aberto N^o 3 (Conjectura do Jacobiano). Seja $F : \mathbb{C}^n \rightarrow \mathbb{C}^n$ um sistema de polinômios (cada coordenada é um polinômio em n variáveis). O *Jacobiano* de F é $\det(DF)$. O Teorema da Função Inversa garante que se $\det(DF(x_0)) \neq 0$, então existe uma inversa de F localmente definida em uma vizinhança de $y_0 = F(x_0)$. Conjectura-se desde 1939 que se $\det(DF)$ é constante $\neq 0$, então F admite uma inversa global G (ou seja, $(F \circ G)(x) \equiv x$, para G definida em $\mathbb{C}^n$). A conjectura também está em aberto no caso real (substituir todos os $\mathbb{C}$ por $\mathbb{R}$).

¹Comentário técnico: a Hipótese de Valiant se refere a $VP \neq VNP$ sobre qualquer corpo e não apenas sobre o corpo dos reais. Isso dito, mostrar a Hipótese de Valiant sobre $\mathbb{R}$ seria um resultado importante. Uma referência geral é: Bürgisser, Clausen e Shokrollahi, *Algebraic Complexity Theory*, Springer Grundlehren der mathematischen Wissenschaften **315**, Berlin, 1997.

CAPÍTULO 10

Autovalores e autovetores

1. Endomorfismos lineares

Nesta seção, consideramos a classe dos endomorfismos ou transformações lineares de $\mathbb{R}^n$. A motivação vem dos exemplos seguintes:

Exemplo 10.1. A sequência de Fibonacci é definida recursivamente por $F_0 = 1, F_1 = 1$ e $F_{i+1} = F_i + F_{i-1}$. Os primeiros termos da sequência são 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, etc... Gostaríamos de resolver a recorrência, ou seja de obter uma fórmula fechada para F_k .

Exemplo 10.2. Gostaríamos de resolver a equação diferencial

$$\ddot{x}(t) - \dot{x}(t) - x(t) = 0$$

para a condição inicial $(x(0), \dot{x}(0)) = (x_0, v_0) = (1, 1)$.

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.

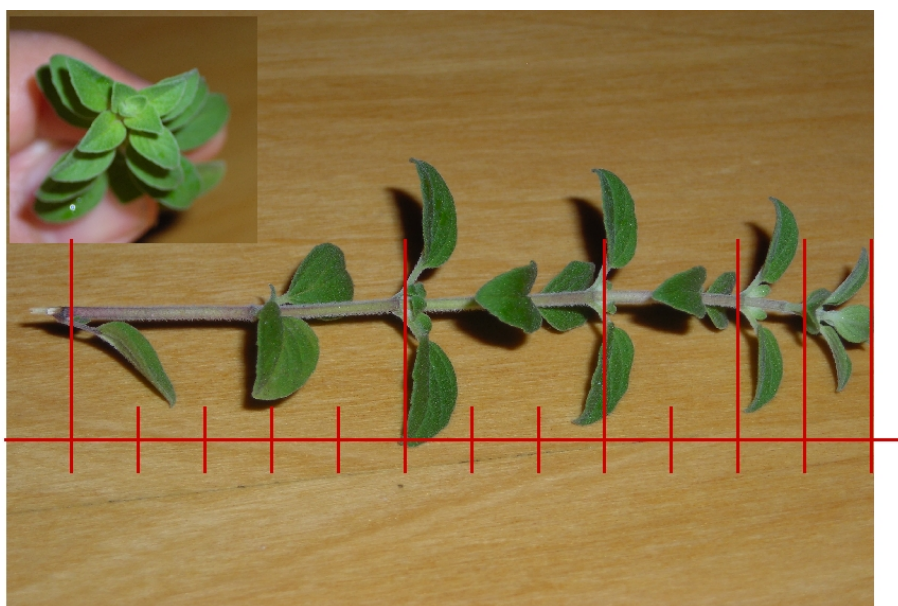


FIGURA 1. A sequência de Fibonacci estaria relacionada ao crescimento das plantas.

Tanto a recorrência quanto a equação diferencial podem ser escritas de forma matricial:

$$\begin{bmatrix} F_i \\ F_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} F_{i-1} \\ F_i \end{bmatrix}$$

e

$$\frac{\partial}{\partial t} \begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix}.$$

Isso nos leva a investigar a transformação linear $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Uma solução geral para a recorrência de Fibonacci seria:

$$\begin{bmatrix} F_i \\ F_{i+1} \end{bmatrix} = A^i \begin{bmatrix} F_0 \\ F_1 \end{bmatrix},$$

Inspirados na solução da equação do decaimento radiativo $\dot{x}(t) = ax(t)$, que é $e^{at}x(0)$, poderíamos escrever formalmente:

$$\begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix} = \left(I + tA + \frac{t^2}{2}A^2 + \frac{t^3}{3!}A^3 + \dots \right) \begin{bmatrix} x_0 \\ v_0 \end{bmatrix}$$

Se a série acima for convergente, e se for possível derivar termo a termo, a expressão acima será uma solução da equação diferencial com a condição inicial dada. Chamaremos essa série de *exponencial* da matriz tA . Mesmo assumindo tudo isso, precisamos ainda de uma fórmula fechada para calcular potências e exponenciais de matrizes.

2. Ação de grupo

O Grupo das transformações lineares inversíveis de $\mathbb{R}^n$ age sobre as transformações lineares por *conjugação*: a cada $X \in GL(\mathbb{R}^n)$, associamos a ação $c_X : A \mapsto XAX^{-1}$. (Verifique que se trata de uma ação de grupo).

Definição 10.3. Duas matrizes A e B de tamanho $n \times n$ são *similares* se e somente se existe uma matriz X inversível de tamanho $n \times n$, tal que $B = XAX^{-1}$.

Em termos abstratos, elas são similares se podem ser levadas uma na outra pela ação do grupo $GL(\mathbb{R}^n)$. Podemos dizer ainda que duas matrizes são similares se e somente se pertencem à mesma órbita dessa ação. Note que se $B = XAX^{-1}$, então

$$B^i = XA^iX^{-1}$$

e

$$\sum_j \frac{1}{j!} B^j = X \left(\sum_j \frac{1}{j!} A^j \right) X^{-1}$$

Uma maneira mais prática de verificar a similaridade de matrizes, se sabemos que X é inversível, é comparar XA com BX .

3. Solução dos exemplos

A matriz $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ é similar a uma matriz diagonal, como podemos verificar da equação seguinte:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix}$$

A solução geral da recorrência de Fibonacci é portanto dada por:

$$\begin{bmatrix} F_i \\ F_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{bmatrix}^i \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Em particular,

$$F_i = \left(\frac{1+\sqrt{5}}{2} \right)^i \frac{5+\sqrt{5}}{10} + \left(\frac{1-\sqrt{5}}{2} \right)^i \frac{5-\sqrt{5}}{10}$$

que é uma solução em forma fechada para a recorrência de Fibonacci.

Já a equação diferencial ordinária admite a solução:

$$\begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} e^{\frac{1+\sqrt{5}}{2}t} & 0 \\ 0 & e^{\frac{1-\sqrt{5}}{2}t} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}^{-1} \begin{bmatrix} x_0 \\ v_0 \end{bmatrix}.$$

Por exemplo, se $x_0 = 1$ e $v_0 = 1$, obtemos a solução:

$$x(t) = \frac{5+\sqrt{5}}{10} e^{\frac{1+\sqrt{5}}{2}t} + \frac{5-\sqrt{5}}{10} e^{\frac{1-\sqrt{5}}{2}t}$$

4. Definição

Definição 10.4. Seja A uma matriz $n \times n$. Um *autovalor* de A é um número (real, complexo) λ tal que a matriz $A - \lambda I$ não seja inversível.

Podemos achar os autovalores resolvendo o polinômio univariado $\det(A - \lambda I) = 0$, chamado de *polinômio característico* da matriz A . O Teorema Fundamental da Álgebra nos garante que esse polinômio tem n raízes complexas, com multiplicidade. Se a matriz A é real, então os coeficientes do polinômio característico são reais, e as raízes são números reais ou pares de números complexos conjugados.

No caso de matrizes de tamanho 2×2 , temos duas possibilidades: ambos os autovalores reais, ou ambos complexos conjugados.

Se λ é um autovalor (real, complexo) de A , um *autovetor* $\mathbf{u}$ (resp. real, complexo) associado a λ é um vetor $\mathbf{u} \neq \mathbf{0}$ (resp. real, complexo) tal que:

$$A\mathbf{u} = \lambda\mathbf{u}$$

Nesta seção, consideramos apenas o caso real. Nesta situação, para todo λ autovalor de A , existe pelo menos um autovetor $\mathbf{u}$ associado. Todo múltiplo $\alpha\mathbf{u}$ com $\alpha \neq 0$ também é autovetor de A .

Lema 10.5. Se uma matriz A de tamanho $n \times n$ admitir n autovalores reais diferentes dois a dois, então existe uma base $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ de $\mathbb{R}^n$ formada de autovetores de A .

DEMONSTRAÇÃO. A prova é por indução, a hipótese de indução em k é que $\mathbf{u}_1, \dots, \mathbf{u}_k$ são linearmente independentes. O caso inicial é fácil: se $k = 1$, sabemos que $\mathbf{u}_1$ é diferente de zero. Logo não existe combinação linear não trivial $x_1\mathbf{u}_1 = \mathbf{0}$.

Admitindo a hipótese de indução para um certo valor k , consideramos por absurdo uma combinação linear não trivial nula de $\mathbf{u}_1, \dots, \mathbf{u}_{k+1}$:

$$x_1\mathbf{u}_1 + \dots + x_k\mathbf{u}_k + x_{k+1}\mathbf{u}_{k+1} = \mathbf{0}.$$

Por indução, $x_k \neq 0$. Multiplicando dos dois lados por $A - \lambda_{k+1}I$, teremos:

$$x_1(\lambda_1 - \lambda_{k+1})\mathbf{u}_1 + \dots + (\lambda_k - \lambda_{k+1})x_k\mathbf{u}_k = \mathbf{0}$$

Como os autovalores são diferentes dois a dois, essa é uma combinação linear não-trivial de $\mathbf{u}_1, \dots, \mathbf{u}_k$. Pela hipótese de indução, ela não pode se anular. Isso estabelece a hipótese para o nível $k + 1$. $\square$

Quando existe uma base $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ de $\mathbb{R}^n$ formada de autovetores de A , dizemos que a matriz A é *diagonalizável real*. O Lema garante que se todos os autovalores são reais e diferentes dois a dois, a matriz é diagonalizável. A identidade é um exemplo de matriz diagonalizável, com autovalores não diferentes dois a dois.

Mas existem matrizes com autovalores reais que não são diagonalizáveis:

Exemplo 10.6. A matriz de Jordan

$$J_n(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ 0 & 0 & \lambda & 1 & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & \lambda & 1 \\ 0 & 0 & \dots & 0 & 0 & \lambda \end{bmatrix}$$

não é diagonalizável. Para ver isso, basta constatar que todos os autovetores são colineares a $\mathbf{e}_1$.

5. Autovalores complexos

A equação diferencial ordinária do exemplo 10.2 é um modelo abstrato, que se afasta sempre da posição de equilíbrio. Para quase qualquer condição inicial, $\lim_{t \rightarrow \infty} x_t = \infty$. Essa equação é dita *instável*.

Se um sistema físico ou um circuito elétrico for modelado pela equação do exemplo 10.2, ele pode quebrar ou queimar, ou a solução $x(t)$ pode atingir valores onde o modelo não é mais adequado. Um exemplo *físico* é a equação do sistema massa-mola amortecido, ou do circuito RLC, que estudaremos em detalhes no Capítulo 12.

Exemplo 10.7. Consideramos a equação diferencial

$$\ddot{x}(t) + \dot{x}(t) + x(t) = 0$$

para a condição inicial $(x(0), \dot{x}(0)) = (x_0, v_0)$.

Sob forma matricial, a equação se escreve:

$$\frac{\partial}{\partial t} \begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix}$$

O polinômio característico é $\lambda^2 + \lambda + 1 = 0$. Os autovalores são os números complexos conjugados

$$\lambda = \frac{-1 + \sqrt{-3}}{2} \quad \bar{\lambda} = \frac{-1 - \sqrt{-3}}{2}.$$

Podemos diagonalizar a matriz $\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ sobre os números complexos:

$$\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \lambda & \bar{\lambda} \end{bmatrix} \begin{bmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \lambda & \bar{\lambda} \end{bmatrix}^{-1}.$$

Se x_0 e v_0 são números reais, então calculamos

$$\begin{bmatrix} 1 & 1 \\ \lambda & \bar{\lambda} \end{bmatrix}^{-1} \begin{bmatrix} x_0 \\ v_0 \end{bmatrix} = \begin{bmatrix} z_0 \\ \bar{z}_0 \end{bmatrix}$$

onde $z_0 = \frac{\bar{\lambda}x_0 - \lambda v_0}{\lambda - \bar{\lambda}}$. A solução da equação é portanto

$$x(t) = z_0 e^{\lambda t} + \bar{z}_0 e^{\bar{\lambda} t}.$$

Podemos reescrever essa fórmula como

$$x(t) = 2\operatorname{re} \left(z_0 e^{\lambda t} \right) = 2\operatorname{re} \left(z_0 e^{\left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)t} \right)$$

Trata-se portanto de uma solução real. Para poder entender o significado desta fórmula, escrevemos z_0 assim: $z_0 = \frac{C}{2} e^{\varphi\sqrt{-1}}$. Então

$$x(t) = C \operatorname{re} \left(e^{-\frac{t}{2} + \left(\frac{\sqrt{3}}{2}t + \varphi\right)\sqrt{-1}} \right) = C e^{-\frac{t}{2}} \cos\left(\frac{\sqrt{3}}{2}t + \varphi\right)$$

As constantes C e φ podem ser achadas diretamente das condições iniciais:

$$x(0) = x_0 = C \cos(\varphi)$$

e derivando $x(t)$ para $t = 0$,

$$v(0) = v_0 = -\frac{x_0}{2} - C \frac{\sqrt{3}}{2} \sin(\varphi)$$

Essas duas equações são equivalentes ao sistema

$$\begin{cases} C \sin(\varphi) &= -\frac{\sqrt{3}}{3}(2v_0 + x_0) \\ C \cos(\varphi) &= x_0 \end{cases}$$

que é facilmente resolvido.

A interpretação dos autovalores complexos em equações diferenciais ordinárias lineares é portanto a seguinte: a parte real corresponde ao coeficiente de crescimento (se positiva) ou decaimento exponencial. A parte imaginária está associada ao comportamento oscilatório da solução. Pode ser assimilada a uma velocidade angular.

6. Considerações adicionais

O Teorema Fundamental da Álgebra nos obriga a considerar autovalores (e portanto também autovetores) complexos.

Definição 10.8. Um *espaço vetorial complexo* $(E, +, \cdot)$ é um conjunto E , com uma operação interna de “soma”:

$$\begin{aligned} + : E \times E &\rightarrow E \\ (\mathbf{u}, \mathbf{v}) &\mapsto \mathbf{u} + \mathbf{v} \end{aligned}$$

e uma operação de multiplicação por um número complexo

$$\begin{aligned} \cdot : \mathbb{C} \times E &\rightarrow E \\ (\lambda, \mathbf{u}) &\mapsto \lambda \cdot \mathbf{u} . \end{aligned}$$

Elas devem satisfazer as propriedades [EV1–EV8] da Definição 1.1, mas com $\lambda, \mu \in \mathbb{C}$.

A definição de subespaço vetorial é idêntica. As definições de *combinação linear*, *independência linear* e *dimensão* são idênticas, mudando apenas o fato de que os coeficientes das combinações lineares são complexos e não apenas reais. Tudo o que foi mencionado nos capítulos anteriores, menos o produto interno, continua valendo com essa e apenas essa modificação. Veremos no Capítulo 21 como adaptar a definição de produto interno a espaços vetoriais complexos.

7. Exercícios

Exercício 10.1. Ache os autovalores e uma base de autovetores para a matriz

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{bmatrix}$$

Exercício 10.2. Para quais valores de t a matriz $\begin{bmatrix} 1 & 2 \\ t & 1 \end{bmatrix}$ possui um autovalor com multiplicidade dois?

Exercício 10.3. Qual é o conjunto de todos os autovetores da matriz $J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$?

Da matriz $J' = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{bmatrix}$?

Exercício 10.4. Dado um polinômio mônico $p(t)$, produza uma matriz (as coordenadas são os coeficientes de p e constantes) cujos autovalores são exatamente as raízes de $p(t) = 0$, com multiplicidade.

Exercício 10.5. Mostre que se uma matriz A admitir um autovalor real λ com $\lambda > 0$, então a equação diferencial ordinária

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t)$$

admite, para alguma condição inicial $\mathbf{x}(0) = \mathbf{x}_0$, uma solução com $\lim_{t \rightarrow \infty} \|\mathbf{x}(t)\| = \infty$.

Exercício 10.6. Mostre que se uma matriz A for diagonalizável sobre os reais, então a exponencial

$$e^A = I + A + \frac{1}{2}A^2 + \cdots + \frac{1}{k!}A^k + \cdots$$

é uma série convergente (para cada coordenada de e^A). Deduza que e^{At} também é convergente. O que acontece no caso complexo?

Exercício 10.7. Ache os autovalores e autovetores complexos da matriz $A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$.

Exercício 10.8. Mostre que para todo $\lambda \in \mathbb{C}$, existe uma matriz real 2×2 com autovalores λ e $\bar{\lambda}$.

Exercício 10.9. Seja $\lambda \in \mathbb{C}$ e seja A uma matriz $n \times n$. O *autoespaço* associado a λ é

$$E_\lambda = \{\mathbf{u} \in \mathbb{C}^n : (A - \lambda I)\mathbf{u} = \mathbf{0}\}$$

O *autoespaço generalizado* associado a λ é

$$E_\lambda^* = \{\mathbf{u} \in \mathbb{C}^n : \exists k \in \mathbb{N} \text{ t.q. } (A - \lambda I)^k \mathbf{u} = \mathbf{0}\}$$

(1) Mostre que E_λ^* é um espaço vetorial *complexo*.

- (2) Mostre que E_λ é um subespaço vetorial *complexo* de E_λ^* , e mostre um exemplo na qual essa inclusão seja estrita.
- (3) Mostre que λ é autovalor de A se e somente se $E_\lambda^* \neq \{0\}$.
- (4) Sejam λ e μ autovalores de A . Verifique que se $E_\lambda^* \cap E_\mu^* = \{0\}$, então $\lambda \neq \mu$.

Exercício 10.10. Seja A uma matriz diagonalizável (sobre os reais ou sobre os complexos) e seja $\mathbf{y}_0$ um vetor dado. Mostre que a equação diferencial ordinária $\dot{\mathbf{y}}(t) = A\mathbf{y}(t)$ tem uma única solução com $\mathbf{y}(0) = \mathbf{y}_0$. Ache essa solução.

CAPÍTULO 11

Mudanças de coordenadas

1. Vetores



e fixamos uma base $(\alpha_1, \dots, \alpha_n)$ para um espaço vetorial E , então cada vetor $\mathbf{v} \in E$ se escreve de maneira única como combinação linear dos α_i 's:

$$(6) \quad \mathbf{v} = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$$

Uma notação usual para isso é:

$$(7) \quad \mathbf{v}_{(\alpha_1, \dots, \alpha_n)} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Quando a base está clara do contexto, o subscrito pode ser omitido. Esse é o caso quando utilizamos, por exemplo, a base canônica $(\mathbf{e}_1, \dots, \mathbf{e}_n)$.

Neste capítulo, consideramos o efeito da escolha da base sobre as coordenadas. Para isso, seja $(\beta_1, \dots, \beta_n)$ uma outra base do espaço E . O mesmo vetor $\mathbf{v}$ se escreve como

$$\mathbf{v} = y_1\beta_1 + y_2\beta_2 + \dots + y_n\beta_n.$$

Como $(\alpha_1, \dots, \alpha_n)$ é base de E , existe uma matriz B tal que cada β_j se escreve da forma

$$\beta_j = B_{1j}\alpha_1 + B_{2j}\alpha_2 + \dots + B_{nj}\alpha_n.$$

Reciprocamente,

$$\alpha_i = A_{1i}\beta_1 + A_{2i}\beta_2 + \dots + A_{ni}\beta_n$$

Verificamos imediatamente que $AB = BA = I$. Substituindo cada α_i em (6) e reagrupando os termos, teremos:

$$y_j = \sum_{i=1}^n A_{ji}x_i$$

Substituindo cada β_j em (7) e reagrupando, o resultado será:

$$x_i = \sum_{j=1}^n B_{ij}y_j$$

Em outras palavras,

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = B \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

ou

$$(8) \quad \mathbf{v}_{(\beta_1, \dots, \beta_n)} = A \mathbf{v}_{(\alpha_1, \dots, \alpha_n)} \quad \text{e} \quad \mathbf{v}_{(\alpha_1, \dots, \alpha_n)} = B \mathbf{v}_{(\beta_1, \dots, \beta_n)}.$$

2. Funções lineares

Agora consideramos uma função linear $\omega : E \rightarrow \mathbb{R}$. Ela pode ser representada por uma matriz de tamanho $1 \times n$ ou *vetor linha*. Dada a base $(\alpha_1, \dots, \alpha_n)$ de E , escrevemos

$$\omega_{(\alpha_1, \dots, \alpha_n)} = [\omega(\alpha_1) \quad \omega(\alpha_2) \quad \dots \quad \omega(\alpha_n)]$$

Com essa notação,

$$\omega(\mathbf{v}) = \omega_{(\alpha_1, \dots, \alpha_n)} \mathbf{v}_{(\alpha_1, \dots, \alpha_n)}.$$

Na base $(\beta_1, \dots, \beta_n)$, teremos também:

$$\omega(\mathbf{v}) = \omega_{(\beta_1, \dots, \beta_n)} \mathbf{v}_{(\beta_1, \dots, \beta_n)}$$

Aplicando a fórmula (8), teremos a seguinte regra de mudança de coordenadas para covetores:

$$(9) \quad \omega_{(\beta_1, \dots, \beta_n)} = \omega_{(\alpha_1, \dots, \alpha_n)} A \quad \text{e} \quad \omega_{(\alpha_1, \dots, \alpha_n)} = \omega_{(\beta_1, \dots, \beta_n)} B.$$

A regra (8) é chamada de mudança contravariante de coordenadas. Vetores são “contravariantes”. A regra (9) é chamada de mudança covariante de coordenadas. Covetores são “covariantes”.

3. Transformações lineares

Agora, seja $V : E \rightarrow E$. Até agora, por termos utilizado apenas a base canônica de $\mathbb{R}^n$, temos tratado aplicações lineares e matrizes como sinônimos. Liberada a escolha da base de E , a situação é diferente. Conforme a escolha da base, a transformação V pode ser *representada* pela matriz $V_{(\alpha_1, \dots, \alpha_n)}$ ou pela matriz $V_{(\beta_1, \dots, \beta_n)}$.

Aplicando o argumento das duas seções precedentes, teremos a seguinte regra de mudança de coordenadas:

$$V_{(\beta_1, \dots, \beta_n)} = B V_{(\alpha_1, \dots, \alpha_n)} A \quad \text{e} \quad V_{(\alpha_1, \dots, \alpha_n)} = A V_{(\beta_1, \dots, \beta_n)} B.$$

Lembrando que A e B são inversas uma da outra, deduzimos que $V_{(\beta_1, \dots, \beta_n)}$ e $V_{(\alpha_1, \dots, \alpha_n)}$ são similares. Essas duas matrizes têm portanto o mesmo determinante e os mesmos autovalores.

Proposição 11.1. *Seja $V : E \rightarrow E$ transformação linear, e seja $((\alpha_1, \dots, \alpha_n))$ base de E . Então, os seguintes objetos não dependem da escolha da base $(\alpha_1, \dots, \alpha_n)$:*

- (1) O determinante de $V_{(\alpha_1, \dots, \alpha_n)}$.
- (2) O polinômio característico de $V_{(\alpha_1, \dots, \alpha_n)}$.
- (3) Os autovalores de $V_{(\alpha_1, \dots, \alpha_n)}$.
- (4) O traço $\text{tr}(V_{(\alpha_1, \dots, \alpha_n)})$, onde $\text{tr}(M) = \sum_{i=1}^n M_{ii}$.
- (5) O posto de $V_{(\alpha_1, \dots, \alpha_n)}$.

Dizemos que esses objetos ou valores são *invariantes* do sistema de coordenadas. **DEMONSTRAÇÃO.** Seja $(\beta_1, \dots, \beta_n)$ uma outra base de E , e sejam A e $B = A^{-1}$ as matrizes de (8) e (9).

(1) Pelo Teorema 9.6,

$$\begin{aligned} \det(V_{(\alpha_1, \dots, \alpha_n)}) &= \det(A) \det(V_{(\beta_1, \dots, \beta_n)}) \det(B) \\ &= \det(V_{(\beta_1, \dots, \beta_n)}) \det(AB) \\ &= \det(V_{(\beta_1, \dots, \beta_n)}) \end{aligned}$$

(2) Pelo mesmo argumento aplicado à transformação $V - \lambda I : E \rightarrow E$, $\mathbf{u} \mapsto V(\mathbf{u}) - \lambda \mathbf{u}$, temos para qualquer λ que:

$$\det(V_{(\alpha_1, \dots, \alpha_n)} - \lambda I) = \det(V_{(\beta_1, \dots, \beta_n)} - \lambda I)$$

Logo, os polinômios característicos são iguais.

- (3) Pelo item precedente, as raízes dos polinômios característicos e as respectivas multilicidades também são iguais.
- (4) O traço é o coeficiente em λ^{n-1} do polinômio característico, logo é invariante.
- (5) O posto é a dimensão da imagem, que é invariante por mudança de base.

□

4. Funções bilineares

Uma função bilinear é uma função $f : E \times E \rightarrow \mathbb{R}$ que é linear em cada um dos dois argumentos. Na base $(\alpha_1, \dots, \alpha_n)$, ela pode ser representada pela matriz

$$F_{(\alpha_1, \dots, \alpha_n)} = \begin{bmatrix} f(\alpha_1, \alpha_1) & f(\alpha_1, \alpha_2) & \dots & f(\alpha_1, \alpha_n) \\ f(\alpha_2, \alpha_1) & f(\alpha_2, \alpha_2) & \dots & f(\alpha_2, \alpha_n) \\ \vdots & \vdots & & \vdots \\ f(\alpha_n, \alpha_1) & f(\alpha_n, \alpha_2) & \dots & f(\alpha_n, \alpha_n) \end{bmatrix}.$$

Se f é simétrica, a matriz é simétrica. Dessa maneira,

$$f(u, v) = u_{(\alpha_1, \dots, \alpha_n)}^T F_{(\alpha_1, \dots, \alpha_n)} v_{(\alpha_1, \dots, \alpha_n)}$$

Agora, a fórmula de mudança de coordenadas é diferente !

$$F_{(\beta_1, \dots, \beta_n)} = A^T F_{(\alpha_1, \dots, \alpha_n)} A \quad \text{e} \quad V_{(\alpha_1, \dots, \alpha_n)} = B^T V_{(\beta_1, \dots, \beta_n)} B.$$

5. Exercícios

Exercício 11.1. Qual é a transformação linear que leva $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ em $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$ e $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ em $\begin{bmatrix} 2 \\ 4 \end{bmatrix}$?

Exercício 11.2. Na base canônica de $\mathbb{R}^2$, a transformação linear T é representada pela matriz $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$. Qual é a matriz de T na base $\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ -2 \end{bmatrix} \right)$?

Exercício 11.3. Uma transformação $A : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ é representada pela matriz identidade na base canônica. Escreva A na base $\left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} -3 \\ 1 \end{bmatrix} \right)$.

Exercício 11.4. Agora consideramos uma aplicação linear $A : \mathbb{R}^2 \rightarrow \mathbb{R}^3$, dada nas bases canônicas respectivas por:

$$A = \begin{bmatrix} 1 & 2 \\ -1 & 3 \\ 0 & 1 \end{bmatrix}.$$

Considere agora o espaço $\mathbb{R}^2$ munido da base $\alpha = \left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right)$ e o espaço $\mathbb{R}^3$ munido da base $\beta = \left(\begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right)$. Escreva a matriz associada a A nas bases α e β .

Exercício 11.5. Mostre que o posto de uma matriz representando uma função bilinear em uma certa base, é invariante da escolha da base.

Exercício 11.6. Se uma matriz M representa uma função bilinear na base canônica, e N representa a mesma função bilinear mas escrita na base α dada pelas colunas da matriz A , qual é a expressão para o determinante de N em função do determinante de M ?

Exercício 11.7. Seja ω uma forma bilinear simétrica do $\mathbb{R}^2$. Mostre que existe uma base de $\mathbb{R}^2$ na qual $\omega(\mathbf{x}, \mathbf{y}) = \sigma_1 x_1 y_1 + \sigma_2 x_2 y_2$, com $\sigma_1, \sigma_2 \in \{-1, 0, 1\}$.

Exercício 11.8. Seja S uma matriz simétrica de tamanho 2×2 (ou seja, $S = S^T$). Mostre que S tem dois autovetores ortogonais.

Exercício 11.9. Seja N uma matriz $n \times n$, nilpotente. Mostre que existe uma base α na qual N se escreve

$$N_\alpha = \begin{bmatrix} J_{r_1} & 0 & \cdots & 0 \\ 0 & J_{r_2} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & J_{r_s} \end{bmatrix}$$

onde $J_1 = [0]$, $J_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $J_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ e, em geral, J_k é a matriz $k \times k$ com $(J_k)_{ij} = 1$ se $j = i + 1$, e todas as outras coordenadas nulas.

Exercício 11.10. Seja G uma função bilinear simétrica positiva definida em $\mathbb{R}^2$, e seja B uma função bilinear simétrica qualquer em $\mathbb{R}^2$. Mostre que existe uma base (α_1, α_2) de $\mathbb{R}^2$ na qual as matrizes representando B e G são diagonais.

CAPÍTULO 12

Equações diferenciais ordinárias

1. O circuito RLC



circuito RLC (Figura 1) é um componente fundamental de varios circuitos eletrônicos, como por exemplo (quando a resistência R é desprezível) o receptor de rádio AM.

O capacitor C é composto de duas placas condutoras paralelas, separadas por uma camada isolante. Cada uma das placas é conectada a um dos eletrodos, por sua vez conectados aos pontos a e c . A carga elétrica assim armazenada (em Coulombs) é igual à diferença de potencial (em Volts) vezes a capacitância C (em Faradays).

A resistência R obedece à Lei de Ohm: a intensidade da corrente (em Ampères) vezes a resistência R (em Ohms) é igual à diferença de potencial entre os eletrodos (em Volts).

A indutância L é uma bobina, e corrente elétrica de intensidade passando por L induz um fluxo magnético na direção do eixo da bobina. A derivada da corrente elétrica induz portanto uma variação no fluxo magnético, que por sua vez induz uma diferença de potencial entre os pontos a e c . A constante de proporcionalidade entre a variação da corrente e a diferença de potencial é chamada de Indutância. A diferença de potencial (em Volts) é igual à derivada da intensidade da corrente (Ampères por segundo) vezes a indutância L (Webers por Ampère).

Seja $x(t)$ a carga do Capacitor C , no tempo t . A intensidade da corrente é por definição a derivada $\dot{x}(t)$ da carga. A diferença de potencial nos eletrodos do resistor é portanto de $C^{-1}x(t) + L\ddot{x}(t)$, e isso é igual a $-R\dot{x}(t)$ pela Lei de Ohm. Vale portanto a equação:

$$L\ddot{x}(t) + R\dot{x}(t) + C^{-1}x(t) = 0,$$

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.

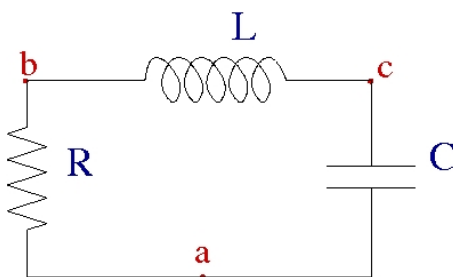


FIGURA 1. Circuito RLC

ou ainda, em termos matriciais,

$$\frac{\partial}{\partial t} \begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\frac{1}{CL} & -\frac{R}{L} \end{bmatrix} \begin{bmatrix} x(t) \\ \dot{x}(t) \end{bmatrix}.$$

Vamos escrever $A = \begin{bmatrix} 0 & 1 \\ -\frac{1}{CL} & -\frac{R}{L} \end{bmatrix}$, o polinômio característico de A é $p_A(\lambda) = \lambda^2 + \frac{R}{L}\lambda + \frac{1}{CL}$. As constantes R , L e C são positivas. Seja $\Delta = \frac{R^2}{L^2} - 4\frac{1}{CL}$. Distiguiremos três casos.

Caso 1: resistência muito grande. Se $R^2 > 4C^{-1}L$, teremos $\Delta > 0$ e haverá dois autovalores reais, $\lambda_1 = -\frac{R}{2L} + \frac{1}{2}\sqrt{\Delta}$ e $\lambda_2 = -\frac{R}{2L} - \frac{1}{2}\sqrt{\Delta}$. Notamos também que $\lambda_2 < \lambda_1 < 0$. A matriz A é diagonalizável real:

$$A = \begin{bmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{bmatrix}^{-1}.$$

Logo, teremos soluções da forma $e^{At} \begin{bmatrix} x(0) \\ \dot{x}(0) \end{bmatrix}$. Se é dada uma condição inicial $x(0) = x_0$ e $\dot{x}(0) = i_0$, podemos achar $x(t)$ da seguinte maneira: sabemos que $x(t)$ é da forma: $x(t) = y_1 e^{\lambda_1 t} + y_2 e^{\lambda_2 t}$, onde:

$$\begin{bmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_0 \\ i_0 \end{bmatrix}$$

Caso 2: resistência $R = 2\sqrt{LC^{-1}}$. Nesse caso $\Delta = 0$ e o autovalor $\lambda = -\frac{R}{2L} = -\sqrt{1/CL}$ terá multiplicidade dois. A matriz A não é diagonalizável! De fato,

$$A - \lambda I = \begin{bmatrix} -\lambda & 1 \\ -\frac{C}{L} & -\frac{R}{L} - \lambda \end{bmatrix} = \begin{bmatrix} -\lambda & 1 \\ -\lambda^2 & \lambda \end{bmatrix}$$

tem núcleo de dimensão 1. Mas podemos constatar que A é similar a uma matriz de Jordan. Como

$$(A - \lambda I) \begin{bmatrix} 1 & \lambda^{-1} \\ \lambda & 2 \end{bmatrix} = \begin{bmatrix} 1 & \lambda^{-1} \\ \lambda & 2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$A \begin{bmatrix} 1 & \lambda^{-1} \\ \lambda & 2 \end{bmatrix} = \begin{bmatrix} 1 & \lambda^{-1} \\ \lambda & 2 \end{bmatrix} \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}.$$

Para calcular a exponencial da matriz de Jordan 2×2 , calculamos primeiro as potências, por indução:

$$\begin{bmatrix} \lambda t & 1 \\ 0 & \lambda t \end{bmatrix}^k = \begin{bmatrix} \lambda^k t^k & k\lambda^{k-1}t^{k-1} \\ 0 & \lambda^k t^k \end{bmatrix}.$$

Somando,

$$\exp \left(\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \right) = \begin{bmatrix} e^{\lambda t} & t e^{\lambda t} \\ 0 & e^{\lambda t} \end{bmatrix}.$$

Procuramos portanto soluções da forma $x(t) = y_1 e^{\lambda t} + y_2 t e^{\lambda t}$, que podemos achar resolvendo o sistema

$$\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_0 \\ i_0 \end{bmatrix}$$

Caso 3: resistência $R < 2\sqrt{LC^{-1}}$. Nesse caso temos um par de autovalores complexos conjugados, $\lambda = -\frac{R}{2L} + \frac{1}{2}\sqrt{\Delta}$ e $\bar{\lambda}$, com $\Delta < 0$. Podemos procurar

soluções da forma $x(t) = y_1 e^{\lambda t} + y_2 e^{\bar{\lambda} t}$, e para que $x(t)$ seja real precisaremos que $y_1 = \bar{y}_2$. Se escrevemos

$$\begin{bmatrix} 1 & 1 \\ \lambda & \bar{\lambda} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_0 \\ i_0 \end{bmatrix}$$

com x_0 e i_0 reais, teremos efetivamente $y_2 = \bar{y}_1$ (Verifique!). Note que também podemos escrever $x(t)$ como combinação linear das funções $e^{-\frac{R}{L}t} \cos(\sqrt{|\Delta|}t)$ e $e^{-\frac{R}{L}t} \sin(\sqrt{|\Delta|}t)$.

2. O significado dos autovalores complexos

Para a discussão que segue, é oportuno introduzir a noção de base em $\mathbb{C}^n$. As definições são idênticas às do caso real:

Definição 12.1. Uma *combinação linear complexa* dos vetores $\mathbf{u}_1, \dots, \mathbf{u}_k$ é uma expressão da forma $\lambda_1 \mathbf{u}_1 + \dots + \lambda_k \mathbf{u}_k$, onde $\lambda_1, \dots, \lambda_k \in \mathbb{C}$. Ela é *trivial* quando $\lambda_1 = \dots = \lambda_k = 0$.

Definição 12.2. Os vetores $(u_1, \dots, u_k)$ são linearmente independentes sobre os complexos se e somente se, não existe combinação linear complexa não-trivial de $u_1, \dots, u_k$ igual a $\mathbf{0}$.

Definição 12.3. Os vetores $u_1, \dots, u_k$ geram o espaço vetorial complexo W se e somente se todo $w \in W$ se escreve como combinação linear complexa dos u_i 's

Definição 12.4. Uma *base* do espaço vetorial complexo W é uma d -upla $(u_1, \dots, u_d)$ de vetores de W , que geram o espaço vetorial complexo W e que são linearmente independentes sobre $\mathbb{C}$.

Duas bases do mesmo espaço vetorial complexo têm sempre o mesmo número de elementos, que é chamado de *dimensão* do espaço vetorial. O Teorema do Posto vale para matrizes complexas. O Determinante para matrizes complexas obedece à mesma fórmula, e uma matriz complexa é inversível se e somente se seu determinante é diferente de zero. O análogo complexo do Lema 10.5 é o seguinte:

Lema 12.5. Se uma matriz A de tamanho $n \times n$ admitir n autovalores complexos diferentes dois a dois, então existe uma base $(\mathbf{u}_1, \dots, \mathbf{u}_n)$ de $\mathbb{C}^n$ formada de autovetores de A .

A prova é exatamente igual à prova do Lema 10.5.

Proposição 12.6. Seja A uma matriz real $n \times n$, com autovalores complexos diferentes dois a dois, que denotamos por $x_1, x_2, \dots, x_r, \lambda_1, \bar{\lambda}_1, \lambda_2, \bar{\lambda}_2, \dots, \lambda_s, \bar{\lambda}_s$, com x_i, a_i e b_i números reais (onde $r + 2s = n$). Escrevemos ainda $\lambda_i = a_i + b_i \sqrt{-1}$. Então a matriz A é similar à matriz:

$$\begin{bmatrix} x_1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & x_r & & & & & & & \\ & & & a_1 & -b_1 & & & & & \\ & & & b_1 & a_1 & & & & & \\ & & & & & a_2 & -b_2 & & & \\ & & & & & b_2 & a_2 & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & a_s & -b_s \\ & & & & & & & & b_s & +a_s \end{bmatrix}$$

e $\exp(At)$, por sua vez, é similar a:

$$\begin{bmatrix} e^{x_1 t} & & & & & \\ & \ddots & & & & \\ & & e^{x_r t} & & & \\ & & & e^{a_1 t} \cos b_1 t & -e^{a_1 t} \sin b_1 t & \\ & & & e^{a_1 t} \sin b_1 t & +e^{a_1 t} \cos b_1 t & \\ & & & & \ddots & \\ & & & & & e^{a_s t} \cos b_s t & -e^{a_s t} \sin b_s t \\ & & & & & e^{a_s t} \sin b_s t & +e^{a_s t} \cos b_s t \end{bmatrix}.$$

DEMONSTRAÇÃO. Em primeiro lugar, existe uma base complexa $\mathbf{u}_1, \dots, \mathbf{u}_n$ de autovetores de A . Multiplicando cada $\mathbf{u}_i$ por um número complexo apropriado, podemos assumir que $\mathbf{u}_1, \dots, \mathbf{u}_r$ são reais e que os vetores restantes são pares de vetores conjugados.

Se $\mathbf{u}$ e $\bar{\mathbf{u}}$ são autovetores associados aos autovalores $\lambda = a + b\sqrt{-1}$ e $\bar{\lambda}$, definimos $\mathbf{v} = (\operatorname{re} \mathbf{u}) = \frac{1}{2}(\mathbf{u} + \bar{\mathbf{u}})$ e $w = (\operatorname{im} \mathbf{u}) = \frac{-\sqrt{-1}}{2}(\mathbf{u} - \bar{\mathbf{u}})$. Temos nesse caso que:

$$A \begin{bmatrix} \mathbf{v} & \bar{\mathbf{v}} \end{bmatrix} = \begin{bmatrix} \mathbf{v} & \bar{\mathbf{v}} \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

O mesmo argumento, aplicado a $e^{\lambda t} = e^{at}(\cos bt + \sqrt{-1} \sin bt)$ e a $e^{\bar{\lambda} t}$ permite obter:

$$A \begin{bmatrix} \mathbf{v} & \bar{\mathbf{v}} \end{bmatrix} = \begin{bmatrix} \mathbf{v} & \bar{\mathbf{v}} \end{bmatrix} e^{at} \begin{bmatrix} \cos bt & -\sin bt \\ \sin bt & \cos bt \end{bmatrix}$$

□

3. Exercícios

Exercício 12.1. Resolva o circuito RC (sem indutância), com condição inicial $q(0) = q_0$.

Exercício 12.2. Consideramos agora que o circuito RLC (Fig 1) está está submetido a um potencial externo dado por $u(t)$ (Por exemplo, podemos acoplar uma antena !). A equação diferencial agora é:

$$(10) \quad \ddot{q}(t) + RL^{-1} \dots q(t) + \frac{1}{LC} q(t) = u(t)$$

e chamamos a equação

$$(11) \quad \ddot{q}(t) + RL^{-1} \dots q(t) + \frac{1}{LC} q(t) = 0$$

de equação homogênea associada. Mostre que o conjunto das soluções de (10) é da forma $q_0(t) + \mathcal{S}$ onde $q_0(t)$ é uma solução particular de (10) e $\mathcal{S}$ é o espaço das soluções da equação homogênea associada (11).

Exercício 12.3. Considere o problema de valor inicial:

$$\begin{cases} \dot{x}(t) &= \lambda x(t) + u(t) \\ x(0) &= 0 \end{cases}$$

onde $x(t)$ e $u(t)$ são funções de $\mathbb{R}$ em $\mathbb{C}$, e $\lambda \in \mathbb{C}$. Mostre que o operador que associa a solução $x(t)$ à “entrada” $u(t)$ é um operador linear.

Exercício 12.4. Ainda para o mesmo problema de valor inicial: Mostre que a solução $x(t)$, se escreve como

$$x(t) = e^{\lambda t} \int_0^t e^{-\lambda s} u(s) ds.$$

Exercício 12.5. Utilize essa expressão no caso de $u(s) = e^{i\operatorname{im}(\lambda)s}$. Interprete o resultado. Como é que o comportamento de $x(t)$ quando $t \rightarrow \infty$ depende de $\operatorname{re}(\lambda)$?

Exercício 12.6. Utilize a análise acima para concluir que a solução de (10) para $u(t) = e^{i\operatorname{im}(\lambda)t}$ permanece limitada quando $t \rightarrow \infty$.

Exercício 12.7. Em geral, costuma-se modelar plantas industriais por equações lineares de primeira ordem da forma:

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t)$$

onde $\mathbf{u}(t)$ é um sinal de entrada (pode ser ruído). Mostre que o operador $\mathbf{u}(t) \mapsto \mathbf{x}(t)$ é linear (Assuma que a solução $\mathbf{x}(t)$ existe e é única).

Exercício 12.8. Mostre que se a matriz A possuir pelo menos um autovalor com parte real estritamente positiva, e B for sobrejetiva, então uma entrada $\mathbf{u}(t)$ infinitesimal pode levar a valores grandes de $\mathbf{x}(t)$ para t suficientemente grande. Nesse caso, a planta é dita *instável*.

Exercício 12.9. Mostre a recíproca, assumindo que A é diagonalizável

Exercício 12.10. Seja $\mathcal{S}$ o espaço de soluções *analíticas em todo* $\mathbb{R}$ de uma equação diferencial linear de ordem n em uma variável:

$$x^{(n)}(t) + a_{n-1}x^{(n-1)}(t) + \cdots + a_0x(t) = 0.$$

O objetivo deste exercício é provar que o espaço vetorial $\mathcal{S}$ tem dimensão $\leq n$. Para isso, dadas $n+1$ funções diferenciáveis $x_i(t)$ de $\mathbb{R}$ em $\mathbb{R}$, defina o *Determinante Wronskiano* de $x_0(t), \dots, x_n(t)$ como:

$$W(t) = \det \begin{pmatrix} x_0(t) & x_1(t) & \cdots & x_n(t) \\ \dot{x}_0(t) & \dot{x}_1(t) & \cdots & \dot{x}_n(t) \\ \vdots & \vdots & & \vdots \\ x_0^{(n)}(t) & x_1^{(n)}(t) & \cdots & x_n^{(n)}(t) \end{pmatrix}$$

Mostre que se $x_1, \dots, x_n \in \mathcal{S}$ então $W(t) \equiv 0$. Deduza que nesse caso, para $t = 0$, as colunas da matriz acima são linearmente dependentes. Deduza, usando séries de Taylor, as funções $x_i(t)$ são linearmente dependentes sobre $\mathbb{R}$.

NOTA: Uma função f é analítica em todo $\mathbb{R}$ quando, para todo $t \in \mathbb{R}$, $f(t) = f(0) + tf'(0) + \cdots + \frac{t^k}{k!}f^{(k)}(t) + \cdots$.

CAPÍTULO 13

O Grupo Ortogonal

1. O Grupo Ortogonal



Consideramos neste capítulo o espaço $\mathbb{R}^n$, munido do produto interno canônico $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^n u_i v_i$. Como vimos no Capítulo 3, O produto interno induz uma norma associada (também chamada de *norma Euclidiana* ou *norma canônica*) dada por $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$.

Definição 13.1. O Grupo Ortogonal de $\mathbb{R}^n$, denotado por $O(n)$, é o subgrupo de todas as $Q \in GL(n)$ que preservam o produto interno canônico:

$$\langle Q\mathbf{u}, Q\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$$

(Verifique que se trata de um subgrupo!).

Exemplo 13.2. O grupo ortogonal de $\mathbb{R}^1$ é $\{-1, 1\}$.

Em particular, se $Q \in O(n)$, teremos sempre:

$$\langle Q\mathbf{e}_i, Q\mathbf{e}_j \rangle = \begin{cases} 1 & \text{Se } i = j, \\ 0 & \text{Se } i \neq j. \end{cases}$$

A recíproca é verdadeira (Exercício 13.5). Dizemos que o conjunto de vetores $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ é *ortonormal* se e somente se eles são ortogonais dois a dois, e têm todos norma 1:

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \begin{cases} 1 & \text{Se } i = j, \\ 0 & \text{Se } i \neq j. \end{cases}$$

Dizemos também que uma base de um espaço é *ortonormal* se e somente se o conjunto de vetores da base é ortonormal.

Um elemento do grupo ortogonal $O(n)$ é uma matriz inversível, com colunas ortonormais. Suas colunas formam portanto uma base ortonormal de $\mathbb{R}^n$. Uma noção mais geral é a de *matriz ortogonal*. Uma matriz de tamanho $m \times n$ é *ortogonal* se as suas colunas são ortonormais (não exigimos mais a inversibilidade). Em particular $m \geq n$. Matricialmente, S é ortogonal se e somente se

$$S^T S = I_n,$$

As seguintes propriedades de elementos do Grupo Ortogonal são consequência direta disso:

Proposição 13.3. Seja $S \in O(n)$. Então,

- (1) A matriz S é inversível, e $S^{-1} = S^T$.
- (2) $\det S = \pm 1$.

(3) Todo autovalor λ de S satisfaz $|\lambda| = 1$.

Os dois primeiros itens são imediatos, e deixamos o terceiro como exercício (Exercício 13.6). Outra propriedade importante de $O(n)$ é que as colunas de qualquer $Q \in O(n)$ formam uma base ortonormal de $\mathbb{R}^n$, e reciprocamente qualquer base ortonormal de $\mathbb{R}^n$ corresponde às colunas de um elemento de $O(n)$.

Agora, vamos tentar escrever todos os elementos de $O(n)$ como produto de matrizes ortogonais mais simples. Isso é análogo a achar os geradores de um grupo finitamente gerado. No entanto, segue-se do Exercício 13.6 que o grupo $O(n)$, $n \geq 2$ não é finitamente gerado.

Proposição 13.4. O grupo ortogonal de $\mathbb{R}^2$ é

$$O(2) = \left\{ \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} : \theta \in [0, 2\pi) \right\} \cup \left\{ \begin{bmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{bmatrix} : \theta \in [0, 2\pi) \right\}.$$

DEMONSTRAÇÃO. Seja $Q \in O(2)$. Como a primeira coluna tem norma um, podemos achar $\theta = \left(\mathbf{e}_1, \begin{bmatrix} Q_{11} \\ Q_{21} \end{bmatrix} \right)$ tal que $\cos \theta = Q_{11}$ e $\sin \theta = Q_{21}$. (Quando $Q_{11} > 0$, $\theta = \arctan Q_{21}/Q_{11}$. Quando $Q_{11} < 0$, $\theta = \pi + \arctan Q_{21}/Q_{11}$. Se $Q_{11} = 0$, $\theta = \pm\pi/2$). Os únicos vetores de norma um ortogonais à primeira coluna são, respectivamente, $\begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix}$ e $\begin{bmatrix} \sin \theta \\ -\cos \theta \end{bmatrix}$. Reciprocamente, todas as matrizes da forma dada no enunciado são ortogonais. $\square$

A Proposição acima mostra que existem dois componentes no grupo $O(2)$: as rotações, de determinante $+1$, e as simetrias, de determinante -1 . Abaixo, investigamos a situação para $n = 3$. O resultado abaixo mostra que, em princípio e esquecendo das forças aerodinâmicas, é possível pilotar um avião apenas com o manche (que tem dois graus de liberdade).

Proposição 13.5. Seja $Q \in O(3)$. Então existem ângulos α, β, γ tais que

$$Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} \cos \beta & -\sin \beta & 0 \\ \sin \beta & \cos \beta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \gamma & -\sin \gamma \\ 0 & \sin \gamma & \cos \gamma \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix}$$

DEMONSTRAÇÃO. Escolhendo $\alpha = \left(\mathbf{e}_1, \begin{bmatrix} Q_{21} \\ Q_{31} \end{bmatrix} \right)$, teremos

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{bmatrix}^T Q = \begin{bmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{33} \\ 0 & R_{32} & R_{33} \end{bmatrix}$$

Fazendo $\beta = \left(\mathbf{e}_1, \begin{bmatrix} R_{11} \\ R_{21} \end{bmatrix} \right)$, teremos agora

$$\begin{bmatrix} \cos \beta & -\sin \beta & 0 \\ \sin \beta & \cos \beta & 0 \\ 0 & 0 & 1 \end{bmatrix}^T \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{bmatrix}^T Q = \begin{bmatrix} 1 & S_{12} & S_{13} \\ 0 & S_{22} & S_{33} \\ 0 & S_{32} & S_{33} \end{bmatrix}.$$

Como a matriz S é ortogonal, deduzimos ainda que $S_{12} = S_{13} = 0$. Finalmente,

escolhendo $\gamma = \left(\mathbf{e}_1, \begin{bmatrix} S_{22} \\ S_{32} \end{bmatrix} \right)$,

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \gamma & -\sin \gamma \\ 0 & \sin \gamma & \cos \gamma \end{bmatrix}^T \begin{bmatrix} \cos \beta & -\sin \beta & 0 \\ \sin \beta & \cos \beta & 0 \\ 0 & 0 & 1 \end{bmatrix}^T \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{bmatrix}^T Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix}$$

□

O processo acima funciona para dimensão n qualquer. Em geral, definimos a *Rotação de Givens* $G_{ij}(\theta)$ por:

$$G_{ij}(\theta) \mathbf{e}_k = \begin{cases} \mathbf{e}_k & \text{Se } k \neq i, j \\ \mathbf{e}_i \cos \theta + \mathbf{e}_j \sin \theta & \text{Se } k = i \\ \mathbf{e}_i \sin \theta - \mathbf{e}_j \cos \theta & \text{Se } k = j. \end{cases}$$

Teorema 13.6. *Seja $Q \in O(n)$. Então existem $\theta_{ij}, 1 \leq i < j \leq n$, tais que:*

$$Q = \begin{bmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & \pm 1 \end{bmatrix} G_{n-1,n}(\theta_{n-1,n}) \times \\ \times G_{n-2,n-1}(\theta_{n-2,n}) G_{n-1,n}(\theta_{n-2,n-1}) \times \cdots \\ \cdots \times G_{1,2}(\theta_{1,2}) \cdots G_{n-2,n-1}(\theta_{1,n-1}) G_{n-1,n}(\theta_{1,n}).$$

Deixamos a prova para o Exercício 13.7.

2. O grupo Euclidiano

Lembremos que um movimento rígido (de $\mathbb{R}^n, n = 2, 3, \dots$) é uma bijeção de $\mathbb{R}^n$ que preserva distâncias. Se $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ é um movimento rígido, então

$$A : \mathbf{u} \rightarrow f(\mathbf{u}) - f(\mathbf{0})$$

é chamada de *transformação linear associada a f* . (Ver Proposição 3.9). A transformação A preserva distâncias, logo preserva ângulos e portanto, $A \in O(n)$.

Uma maneira de representar movimentos rígidos de $\mathbb{R}^3$ é a seguinte: cada ponto (x_1, x_2, x_3) é representado pelo vetor

$$\hat{\mathbf{x}} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ 1 \end{bmatrix}.$$

O movimento rígido $f : \mathbf{x} \mapsto A\mathbf{x} + \mathbf{y}$ é representado por:

$$\hat{f} = \begin{bmatrix} A_{11} & A_{12} & A_{13} & y_1 \\ A_{21} & A_{22} & A_{23} & y_2 \\ A_{31} & A_{32} & A_{33} & y_3 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

onde $\mathbf{y} = f(\mathbf{0})$. Com essa representação,

$$\widehat{f(\mathbf{x})} = \hat{f}\hat{\mathbf{x}}$$

Além disso, se g é outro movimento rígido, $\widehat{f \circ g} = \hat{f}\hat{g}$. Se e denota a identidade $\mathbf{x} \mapsto \mathbf{x}$, teremos ainda $\hat{e} = I$. Nesse sentido, acabamos de descobrir um isomorfismo do grupo de movimentos rígidos de $\mathbb{R}^3$ num subgrupo de $GL(4)$. (isso é chamado de *representação* do grupo de movimentos rígidos).

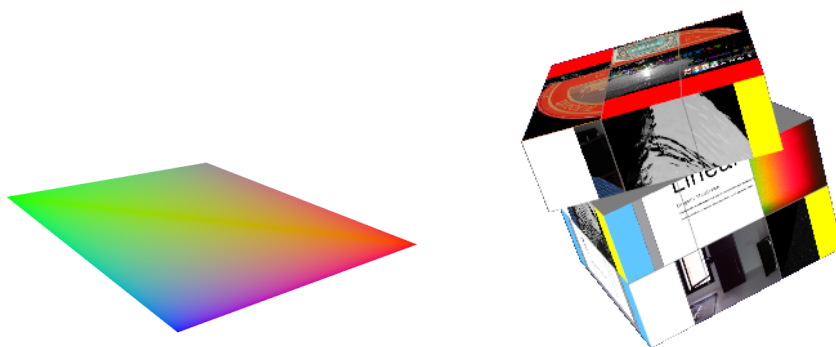


FIGURA 1. Esquerda: simplexo unitário com vértices vermelho, verde, azul e cinza (origem) e cor interpolada entre os pontos. Direita, modelo do cubo mágico com texturas.

3. Como são feitos jogos e animações 3D

Vou tentar explicar abaixo como funciona a perspectiva dos jogos em três dimensões, na qual o jogador está imerso em um ambiente tridimensional. Hoje em dia, programas com gráficos tridimensionais são escritos utilizando uma biblioteca gráfica pronta capaz de tratar perspectiva, iluminação ou texturas. Uma possibilidade é OpenGL, <http://www.opengl.org>. No sistema Linux, sugiro utilizar a interface freeglut, <http://freeglut.sourceforge.net>, para gerenciar janelas e fazer a interface com o OpenGL de maneira intuitiva.

Uma opção mais moderna é a biblioteca Vulkan, <https://www.khronos.org/vulkan/> que permite uma flexibilidade maior, ao preço de tornar a programação bem mais difícil.

Uma parte substancial das operações são feitas por *hardware*, em uma placa gráfica aceleradora ou CUDA, massivamente paralela. Os programas que rodam nessa placa são chamados de *shaders*.

Objetos rígidos são representados em um sistema de coordenadas próprio. Uma estrutura de dados típica é a malha triangular, representada pelas coordenadas dos vértices e por uma triangulação. Vulkan permite que se associe mais informação a um vértice, por exemplo uma cor ou informações sobre uma textura. Por exemplo, o simplexo unitário em $\mathbb{R}^3$ pode ser representado assim:

```

class Vertex {
public:
    alignas(16) glm::vec3 pos;
    alignas(16) glm::vec3 cor;
    ...
};

...
const std::vector<Vertex> vertices = {
    {{0.0f, 0.0f, 0.0f}, {0.5f, 0.5f, 0.5f}},
    {{1.0f, 0.0f, 0.0f}, {1.0f, 0.0f, 0.0f}},
    {{0.0f, 1.0f, 0.0f}, {0.0f, 1.0f, 0.0f}},
    {{0.0f, 0.0f, 1.0f}, {0.0f, 0.0f, 1.0f}}};

const std::vector<uint16_t> triangulos = {
    0, 1, 2,
    0, 2, 3,
    0, 3, 1,
    1, 2, 3};

```

A posição (e orientação) do observador é representada por um movimento rígido f , por sua vez representado pela matriz $\hat{f}$. Esse é o movimento a ser aplicado às coordenadas de um ponto no espaço para obter as suas coordenadas no sistema do observador. Assim, o ponto $x \in \mathbb{R}^3$ é representado pelo ponto $\hat{x} \in \mathbb{R}^4$ e, no sistema de coordenadas do observador, tem coordenadas $\hat{y} = \hat{f}\hat{x}$. Assumindo que o olho do observador está na origem do seu sistema de coordenadas e que a tela está a distância h do observador, o ponto é desenhado na posição $(hy_1/y_3, hy_2/y_3)$ (sistema de coordenadas com origem no centro da tela). A terceira coordenada não é descartada, mas serve para decidir se um ponto está visível ou não. A situação real é mais complicada, porque as coordenadas precisam ser traduzidas em *pixels* e os *pixels* nem sempre são quadrados.

A matriz $\hat{f}$ pode ser armazenada na memória principal ou na memória da placa. Um movimento g aplicado ao observador é equivalente a substituir $\hat{f}$ por $\hat{g}^T \hat{f}$. Objetos articulados ou compostos de varias primitivas (ou da mesma primitiva em posições diferentes) podem ser desenhados substituindo $\hat{f}$ por uma $\hat{f}\tilde{h}$, desenhando uma primitiva, depois recuperando a $\hat{f}$ anterior, etc...

Geralmente, um sólido é representado por uma malha de triângulos, que são passados para a placa gráfica. Os vértices dos triângulos são processados pelo *vertex shader*. Típicamente, os programadores tentam diminuir a necessidade de transferir informação para a placa. Se um objeto é definido por milhares de triângulos, faz sentido manter os vértices na placa e transmitir o movimento rígido e outra informação que varie com o tempo.

A placa pode executar uma variedade limitada de instruções simples, mas de modo massivamente paralelo. Isso permite aplicar por exemplo o movimento rígido aos vértices e eventualmente subdividindo a triangulação.

É possível capturar uma imagem plana, por exemplo uma fotografia, e usar como *textura*, isto é, como imagem a ser parcialmente desenhada nos triângulos do *vertex shader*. Uma vez mapeados três pontos de cada triângulo, o valor da textura nos outros pode ser achado aplicando uma matriz 2×2 e uma translação. Isso é feito no *fragment shader*.

Efeitos como iluminação, ocultação eficiente de linhas e *anti-aliasing* dão lugar a algoritmos específicos, que não vamos discutir aqui. Segue aqui um exemplo simples de *vertex shader*.

```
layout(binding = 0) uniform VarCompartilhada { mat4 matriz; } M;

layout(location = 0) in vec3 Pos;
layout(location = 1) in vec3 Cor;

layout(location = 0) out vec3 fragCor;

void main()
{
    gl_Position = M.matriz*vec4(Pos, 1.0);
    fragCor = Cor;
}
```

Este exemplo aplica uma matriz já guardada na placa a cada vértice que entra (`layout(...) in`) e salva na variável pré-definida `gl_Position`. A saída (`layout(...) out`) é a cor que entrou. Já o *shader* de coloração abaixo interpola entre as cores dos vértices do triângulo (Figura ??):

```
layout(location = 0) in vec3 fragCor;

layout(location = 0) out vec4 Cor;

void main()
{
    Cor=vec4(fragCor,1) ;
}
```

4. Exercícios

Exercício 13.1. Escreva a matriz correspondente à simetria ortogonal de $\mathbb{R}^3$ que leva um vetor $\mathbf{u}$ arbitrário, $\|\mathbf{u}\| = 1$, no vetor $\mathbf{e}_1$. (Aqui e nos próximos exercícios, assuma que $\mathbf{u}$ e $\mathbf{e}_1$ não são colineares.)

Exercício 13.2. Seja $\mathbf{u} \neq \mathbf{0} \in \mathbb{R}^3$. Escreva a matriz de rotação de ângulo $\pi/6$ em torno do vetor $\mathbf{u}$.

Exercício 13.3. Escreva a matriz 4×4 representando a rotação do exercício anterior, seguido da translação pelo vetor $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}^T$.

Exercício 13.4. Ache uma base ortonormal do espaço dos vetores ortogonais a um vetor $\mathbf{u}$ dado.

Exercício 13.5. Seja Q uma matriz inversível, cujas colunas formam um conjunto ortonormal:

$$\langle Q\mathbf{e}_i, Q\mathbf{e}_j \rangle = \begin{cases} 1 & \text{Se } i = j, \\ 0 & \text{Se } i \neq j. \end{cases}$$

Mostre que Q preserva o produto interno.

Exercício 13.6. Seja $Q \in O(n)$. Mostre que todo autovalor de λ satisfaz $|\lambda|^2 = 1$. Mostre que para todo complexo z com $|z| = 1$, existe uma matriz $R \in O(2)$ com autovalores z e $\bar{z}$. Conclua que $O(2)$ não pode ser finitamente gerado.

Exercício 13.7. Mostre o Teorema 13.6. Dica: utilize indução em n .

Exercício 13.8. Mostre que se $Q \in O(n)$, então $|\det(Q)| = 1$. Deduza que o conjunto $O(n)$ não é conexo por caminhos.

Exercício 13.9. Seja $SO(n)$ o conjunto das $Q \in O(n)$ com $\det(Q) = 1$. Mostre que $SO(n)$ é um subgrupo *normal* de $O(n)$.

Exercício 13.10. Uma projeção é uma transformação linear Π tal que $\Pi^2 = \Pi$. Ela é dita *ortogonal* se $\ker \Pi \perp \text{Im} \Pi$. Mostre que se $Q : \mathbb{R}^m \rightarrow \mathbb{R}^n$ é ortogonal, então QQ^T é uma projeção. (Por definição, teremos sempre $m \geq n$. Se $m = n$, verifique que QQ^T é a identidade)

Problema em aberto N° 4. Uma *matriz de Hadamard* é uma matriz $n \times n$ H , com coordenadas ± 1 e $\frac{1}{\sqrt{n}}H \in O(n)$. Por exemplo,

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{e} \quad H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

são matrizes de Hadamard. Matrizes de Hadamard são facilmente construídas para $n = 2^k$. Mostrar que existe (ou não) uma matriz de Hadamard para todo n múltiplo de 4.

CAPÍTULO 14

Projeções e como Aproximar Nuvens de Dados por Mínimos Quadrados

1. Projeções ortogonais



Seja V um subespaço vetorial de $\mathbb{R}^n$, que assumimos munido do produto interno canônico $\langle \cdot, \cdot \rangle$. Um vetor $\mathbf{u}$ é *ortogonal* a V se e somente se, para todo $\mathbf{v} \in V$, $\langle \mathbf{u}, \mathbf{v} \rangle = 0$. O conjunto dos vetores $\mathbf{u}$ ortogonais a V é denotado por $V^\perp$ (Definição 8.7).

Definição 14.1. Uma *projeção* $\pi : \mathbb{R}^n \rightarrow V$ é uma aplicação linear de $\mathbb{R}^n$ em V , tal que para todo $\mathbf{v} \in V$, $\pi(\mathbf{v}) = \mathbf{v}$. Ela é dita *ortogonal* se e somente se $\ker \pi = V^\perp$.

Note (Exercício 14.2) que existe uma e apenas uma projeção ortogonal $\pi : \mathbb{R}^n \rightarrow V$. Se nos for dada uma base ortonormal $(\alpha_1, \dots, \alpha_r)$ de V , construímos a matriz Q de colunas α_j . Essa matriz Q é ortogonal, pois $Q^T Q = I_r$. Por outro lado, $Q Q^T$ fixa V e se anula em $V^\perp$. Logo $\pi = Q Q^T$. Dessa forma, podemos construir Q dada uma base ortonormal de V .

2. Mínimos quadrados

Em ciências experimentais, é necessário interpretar uma amostra de dados em termos de alguma lei ‘física’. Por exemplo, soltamos um objeto (com velocidade inicial zero) de alturas diferentes $h_1, \dots, h_n$ e medimos o tempo da queda. Obtemos intervalos de tempo aproximados $t_1, \dots, t_n$. Esses intervalos foram medidos com uma certa imprecisão, ou erro experimental. Por exemplo,

i	Altura (m)	Tempo (s)
1	1	0.5
2	2	0.6
3	3	0.8

Assumimos certas hipóteses sobre o erro experimental. Uma das hipóteses é que o erro é neutro: a média dos erros em uma mostra arbitrariamente grande tende a zero. Se sabemos *a priori* que $h = \frac{1}{2}gt^2$, podemos tentar avaliar a constante g da seguinte maneira: consideramos o erro experimental como uma função de g .

$$w(g) = \begin{bmatrix} \frac{1}{2}(t_1)^2 \\ \frac{1}{2}(t_2)^2 \\ \frac{1}{2}(t_3)^2 \end{bmatrix} g - \begin{bmatrix} h_1 \\ h_2 \\ h_3 \end{bmatrix}$$

Tentamos então achar o valor de g que minimize $\|w(g)\|^2$. Há três motivos para escolher o quadrado da norma Euclidiana de w . Em primeiro lugar, ela penaliza valores $|w_i|$ muito grandes. Em segundo lugar, o **quadrado** da norma Euclidiana é fácil de calcular e de derivar. Em terceiro lugar, é uma função estritamente convexa, com um mínimo único.

Esse mínimo satisfaz $\frac{\partial \|w(g)\|^2}{\partial g} = 0$. No nosso caso,

$$\frac{\partial \|w(g)\|^2}{\partial g} = 2w(g)^T \begin{bmatrix} \frac{1}{2}(t_1)^2 \\ \frac{1}{2}(t_2)^2 \\ \frac{1}{2}(t_3)^2 \end{bmatrix} \simeq 0,30085g - 2,8900.$$

A solução é a média das medidas $g \simeq 9,6ms^{-2}$, que não está longe do resultado correto ($9.8ms^{-2}$).

Em geral, ensinam-se mínimos quadrados como a melhor maneira de “passar uma reta” por uma nuvem de pontos. Por exemplo, se acreditamos que $b(a) = x_1 + x_2a$ (aqui b é função afim de a), procuramos minimizar o “erro”

$$\left\| \begin{bmatrix} 1 & a_1 \\ 1 & a_2 \\ 1 & a_3 \\ \vdots & \vdots \\ 1 & a_m \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} - \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix} \right\|^2$$

Mas o método é mais geral e não está restrito a ajustar retas. Podemos ajustar funções (“leis físicas”) com vários parâmetros.

Definição 14.2 (Problema de Mínimos Quadrados). É dada uma lei da forma

$$b = x_1a_1 + x_2a_2 + \cdots x_na_n$$

dependendo de n constantes $x_1, \dots, x_n$ a serem determinadas. Logo, b depende de $a_1, \dots, a_n$. O valor de b é medido experimentalmente, para um conjunto de valores de $a_1, \dots, a_n$. A medida obtidas no i -ésimo experimento (de um total de m) é denotadas por y_i , e os valores correspondentes dos b_i 's são denotados por $A_{i1}, \dots, A_{in}$. O problema é achar um vetor x que minimize

$$\|Ax - \mathbf{b}\|^2$$

Se esse vetor não for único, achar o vetor x de menor norma dentre os que minimizam a função acima.

Por exemplo, se queremos uma lei afim $b(t) = x_1 + tx_2$, fazemos $A_{i1} = 1$ e $A_{i2} = t_i$. Se queremos uma lei quadrática $b(t) = x_1 + tx_2 + t^2x_3$, fazemos $A_{i3} = t_i^2$.

Definição 14.3. Um problema de mínimos quadrados é *não-degenerado* se e somente se a matriz A é $m \times n$, $m \geq n$, e tem posto n .

Em geral, $m \gg n$ e a única maneira da matriz A ser degenerada, havendo suficientes experimentos, é uma das variáveis a_i ser combinação linear das outras (e portanto irrelevante).

Proposição 14.4. Dado um problema de mínimos quadrados não degenerado, a solução x satisfaz a equação normal:

$$A^T Ax = A^T \mathbf{b}$$

Como a matriz A tem posto n , a matriz $A^T A$ é inversível, e a equação normal pode ser resolvida por eliminação Gaussiana ou outro algoritmo.

Antes de provar a Proposição 14.4, precisamos de um Lema:

Lema 14.5. *Seja V um subespaço de $\mathbb{R}^m$. Seja π a projeção ortogonal de $\mathbb{R}^m$ em V . Então, para todo $\mathbf{b} \in \mathbb{R}^m$, o ponto proximal a $\mathbf{b}$ em V é $\pi(\mathbf{b})$.*

DEMONSTRAÇÃO. Suponha que o ponto proximal seja $\pi(\mathbf{b}) + \mathbf{z}$, onde $\mathbf{z} \in V$. Nesse caso,

$$\|\pi(\mathbf{b}) + \mathbf{z} - \mathbf{b}\|^2 \leq \|\pi(\mathbf{b}) - \mathbf{b}\|^2$$

Expandindo o primeiro quadrado,

$$\|\mathbf{z}\|^2 + 2\langle \mathbf{z}, \pi(\mathbf{b}) - \mathbf{b} \rangle + \|\pi(\mathbf{b}) - \mathbf{b}\|^2 \leq \|\pi(\mathbf{b}) - \mathbf{b}\|^2$$

Como $\pi(\mathbf{b}) - \mathbf{b} \in \ker \pi \perp \mathbf{z}$, isso é equivalente a:

$$\|\mathbf{z}\|^2 + \|\pi(\mathbf{b}) - \mathbf{b}\|^2 \leq \|\pi(\mathbf{b}) - \mathbf{b}\|^2$$

e deduzimos que $\mathbf{z} = 0$. $\square$

DEMONSTRAÇÃO DA PROPOSIÇÃO 14.4. Seja $V = \text{Im} A$. Seja $\mathbf{x}$ a solução do problema de mínimos quadrados. Ou seja, $A\mathbf{x}$ é o ponto proximal a $\mathbf{b}$ em $V = \text{Im} A$. Pelo Lema, $A\mathbf{x} - \mathbf{b}$ é ortogonal a V . Mas $V^\perp = \ker A^T$. Logo, $(A^T A)\mathbf{x} = A^T \mathbf{b}$.

Reciprocamente, se $\mathbf{x}$ satisfaz a equação normal $(A^T A)\mathbf{x} = A^T \mathbf{b}$, então $A\mathbf{x} - \mathbf{b} \in \ker A^T$, e portanto $\pi(\mathbf{b}) = A\mathbf{x}$. Segue-se que $A\mathbf{x}$ é o ponto proximal a $\mathbf{b}$. $\square$

3. Simetrias

A seguir, resolvemos o seguinte problema. Dados vetores $\mathbf{u} \neq \mathbf{v}$ com $\|\mathbf{u}\| = \|\mathbf{v}\|$, produzir a matriz da simetria ortogonal $H_{\mathbf{u},\mathbf{v}}$ que troca $\mathbf{u}$ com $\mathbf{v}$. Note que $H_{\mathbf{u},\mathbf{v}}(\mathbf{u} - \mathbf{v}) = \mathbf{v} - \mathbf{u}$, e que se $\mathbf{w} \perp \mathbf{u} - \mathbf{v}$ então $H_{\mathbf{u},\mathbf{v}}(\mathbf{w}) = \mathbf{w}$. A projeção ortogonal na linha gerada por $\mathbf{u} - \mathbf{v}$ é dada por:

$$\pi_1 = \frac{1}{\|\mathbf{u} - \mathbf{v}\|^2} (\mathbf{u} - \mathbf{v})(\mathbf{u} - \mathbf{v})^T$$

Logo, a projeção no plano ortogonal a $\mathbf{u} - \mathbf{v}$ é $I - \pi_1$, ou seja:

$$\pi_2 = I - \frac{1}{\|\mathbf{u} - \mathbf{v}\|^2} (\mathbf{u} - \mathbf{v})(\mathbf{u} - \mathbf{v})^T$$

Finalmente, a simetria procurada fixa pontos no plano ortogonal e multiplica por -1 pontos da linha gerada por $\mathbf{u} - \mathbf{v}$. Logo, $H = \pi_2 - 2\pi_1$. Expandindo, obtemos a fórmula

$$H_{\mathbf{u},\mathbf{v}} = I - \frac{2}{\|\mathbf{u} - \mathbf{v}\|^2} (\mathbf{u} - \mathbf{v})(\mathbf{u} - \mathbf{v})^T$$

4. Esparsidade

No início do capítulo, consideramos o problema de minimizar $\|A\mathbf{x} - \mathbf{b}\|$ onde A era uma matriz $m \times n$ de posto máximo com $n \ll m$. Agora vamos considerar o problema de se resolver $A\mathbf{x} = \mathbf{b}$ onde A é de tamanho $m \times n$ com $n \gg m$. Também assumimos para simplificar que A tem posto máximo m . Nesse caso o núcleo de A tem dimensão $n - m > 0$ e a solução não é única. Qual seria a solução mais conveniente? Na formulação clássica, procura-se o vetor de menor energia ou seja de menor norma Euclidiana. É precisamente a solução $\mathbf{x} \perp \ker(A)$.

A abordagem moderna pode ser motivada por problemas de processamento de sinais. As colunas de A representam um conjunto gerador do espaço de sinais,

e qualquer $\mathbf{x}$ com $A\mathbf{x} = \mathbf{b}$ codifica o sinal $\mathbf{b}$. Mas procuramos a codificação mais esparsa, isto é a codificação com o maior número de coordenadas iguais a zero.

Lema 14.6. *Seja A matrix $m \times n$, $m < n$, de posto m . Então existem soluções $\mathbf{x}$ de $A\mathbf{x} - \mathbf{b} = 0$ com pelo menos $n - m$ coordenadas iguais a zero.*

DEMONSTRAÇÃO. A matriz A tem posto m , logo ela admite m colunas linearmente independentes. Seja A' a submatriz formada por essas m colunas, e seja $\mathbf{x}'$ a solução de $A'\mathbf{x}' = \mathbf{b}$. Isso nos permite obter uma solução $\mathbf{x}$ de $A\mathbf{x} = \mathbf{b}$, onde coordenadas de $\mathbf{x}$ correspondendo às colunas de A' recebem a coordenada respectiva de $\mathbf{x}'$ e as outras coordenadas se anulam. $\square$

Obviamente podem existir soluções com mais coordenadas nulas, ou com todas as coordenadas nulas se fizermos $\mathbf{b} = 0$. O conjunto dos 'sinais' $\mathbf{b}$ admitindo uma dessas soluções está contido na união das imagens de A'' para todas as submatrizes de $m - 1$ colunas de A , ou seja em uma união finita de espaços lineares de dimensão $m - 1$.

Definição 14.7. Diremos que uma certa afirmação é válida para um vetor $\mathbf{b}$ em relação a A se para cada valor de A , existe uma união finita de espaços afins tal que a afirmação é verdadeira para $\mathbf{b}$ fora dessa união.

Lema 14.8. *Seja A matrix $m \times n$, $m < n$, de posto m . Seja $\mathbf{b}$ em posição geral em relação a A . Então o menor número possível de coordenadas diferentes de zero para uma solução $\mathbf{x}$ de $A\mathbf{x} - \mathbf{b} = 0$ é exatamente m .*

A prova do Lema é imediata: para cada escolha E de $m - 1$ colunas de A , definimos A_E como a submatriz de A formada apenas pelas colunas em E . A imagem de A_E é $m - 1$ -dimensional. Quando $\mathbf{b}$ não está contido em nenhuma imagem de A_E , então nenhuma solução $\mathbf{x}$ de $A\mathbf{x} = \mathbf{b}$ pode ter mais do que $n - m$ coordenadas nulas. Para achar uma dessas soluções, podemos resolver um problema de otimização:

Proposição 14.9. *Sejam $m < n$. Seja A matrix $m \times n$ de posto m satisfazendo a seguinte propriedade: Para toda submatriz B de A de tamanho $m \times l$, $l > m$, o vetor $[1 \ 1 \ \dots \ 1]^T$ não pertence à imagem de B^T . Seja $\mathbf{b}$ em posição geral em relação a A . Seja X o conjunto das soluções $\mathbf{x}$ de $A\mathbf{x} - \mathbf{b} = 0$ com $\|\mathbf{x}\|_1 = \sum_{j=1}^n |x_j|$ minimal. Então X contém uma solução $\mathbf{x}$ com exatamente m coordenadas diferentes de zero.*

Note que se $[1 \ 1 \ \dots \ 1]^T$ pertencer à imagem de B^T , teremos que

$$\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = B^T \mathbf{y}$$

Se B tiver posto máximo, deduzimos da Proposição 14.4 que $\mathbf{y}$ satisfaz as equações normais:

$$BB^T \mathbf{y} = B \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}.$$

Teremos então a igualdade

$$\begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = B^T (BB^T)^{-1} B \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}.$$

Isso é um sistema de equações polinomiais nos coeficientes de B . As submatrizes B com posto deficiente também satisfazem equações polinomiais (todos os sub-determinantes se anulam). Desta forma, a conclusão da Proposição acima vale para todas as matrizes A que não estão em uma união finita de superfícies definidas por certas equações polinomiais. O conjunto excluído tem volume zero, e nesse sentido a conclusão vale para a maioria das matrizes A , mas não para todas. Na linguagem da geometria algébrica, as condições sobre as submatrizes de A e sobre b estar em posição geral são substituídas por uma única palavra, para A e b *genéricos*.

DEMONSTRAÇÃO DA PROPOSIÇÃO 14.9.

O conjunto dos $\mathbf{x}$ com $A\mathbf{x} - \mathbf{b} = 0$ é não-vazio. O conjunto dos valores $\|\mathbf{x}\|_1$ para $\mathbf{x}$ nesse conjunto é fechado e limitado inferiormente. Como se aprende nos cursos decentes de Cálculo, o ínfimo é atingido. Segue-se que pelo menos um ponto de mínimo é atingido. Seja $\mathbf{x}^*$ uma solução minimizando $\|\mathbf{x}\|_1$.

Podemos reescrever o problema com variáveis positivas: minimizar $\|\mathbf{x}\|_1 + \|\mathbf{y}\|_1$, sujeito a $x_j, y_j \geq 0$ e $A(\mathbf{x} - \mathbf{y}) = 0$. A solução ótima pode ser escrita como $(\mathbf{x}^*, \mathbf{y}^*)$ onde

$$x_j^* y_j^* = 0$$

para todo j . Vamos usar o método dos multiplicadores de Lagrange. Mas previamente vamos reordenar as colunas de A e os valores de $\mathbf{x}, \mathbf{y}$, para ter $x_1^* = \dots = x_k^* = y_1^* = \dots = y_k^* = 0$. Assumimos que todos os outros pares (x_j^*, y_j^*) , $j > k$, são diferentes de $(0, 0)$. Multiplicando por -1 algumas das colunas de A , podemos assumir sem perda de generalidade que $x_{k+1}^*, \dots, x_n^* > 0$ e $\mathbf{y}^* = 0$.

O nosso problema de mínimo era minimizar $f(\mathbf{x}, \mathbf{y}) = \sum x_j + y_j$ sujeito a $x_j, y_j \geq 0$ e $A(\mathbf{x} - \mathbf{y}) = 0$. A derivada de f é o covetor $[1 \dots 1]$. As igualdades que são satisfeitas na solução $(\mathbf{x}^*, \mathbf{y}^*)$ são chamadas de vínculos ativos. A solução do problema está na borda de um conjunto convexo, e os vínculos ativos são as equações que definem localmente essa borda. Neste caso, são $x_1 = \dots = x_k = 0$, $\mathbf{y} = 0$ e $A\mathbf{x} - \mathbf{b}$.

Pelo princípio dos Multiplicadores de Lagrange, quando o mínimo é atingido, a derivada $-Df(\mathbf{x}^*, \mathbf{y}^*)$ é combinação linear das derivadas dos vínculos ativos:

$$[1 \quad \dots \quad 1] + [\mathbf{u} \quad \mathbf{v} \quad \mathbf{w}] \begin{bmatrix} I_k & 0 & 0 \\ 0 & 0 & I_n \\ A_1 & A_2 & -A \end{bmatrix} = 0$$

onde $A = [A_1 A_2]$ com blocos $m \times k$ e $m \times (n - k)$. As condições acima são também chamadas de condições de Karush-Kuhn-Tucker no contexto de otimização. O problema aqui é achar $\mathbf{w}$ tal que as equações correspondentes a $x_{k+1}, \dots, x_n$ sejam satisfeitas. Depois disso os multiplicadores $\mathbf{u}$ e $\mathbf{v}$ são fáceis de serem determinados. Portanto, precisamos ter

$$[1 \quad \dots \quad 1] + \mathbf{w}A_2 = 0.$$

Se $k < n - m$, A_2 é uma submatriz de tamanho $m \times l$ com $l \geq m$ e pela hipótese sobre as submatrizes de A , $\mathbf{w}$ não pode existir. Se $k > n - m$, então $\mathbf{x}^*$ tem mais do que $n - m$ coordenadas nulas, contradição com Lema 14.8. Logo $k = n - m$ e a solução optimal tem exatamente m coordenadas diferentes de zero. $\square$

Problemas de otimização como o apresentado acima são resolvidos por técnicas conhecidas de *programação linear*. A observação de que é possível achar pontos ‘esparcos’ via otimização é um dos fundamentos das técnicas de *compressed sensing*.

5. Exercícios

Exercício 14.1. Quais as implicações do Teorema do Posto (Teorema 8.1) e do Corolário 8.7.4 para os quatro espaços associados a uma projeção ortogonal?

Exercício 14.2. Mostre que existe uma e apenas uma projeção ortogonal em V .

Exercício 14.3. Seja W uma matriz cujas colunas são uma base ortonormal de $V^\perp$. Ache a matriz da projeção ortogonal $\pi : \mathbb{R}^n \rightarrow V$.

Exercício 14.4. Dada uma matriz A , escreva a matriz da projeção ortogonal em $\text{Im}(A)$.

Exercício 14.5. Refaça o exemplo numérico que resultou na equação (?). Imprima, além dos resultados, o erro relativo em cada coordenada. O comando é:

[6]: `(A*x-b) ./ (A*x)`

Verifique que um dos dados tem erro relativo de ordem 8.

Exercício 14.6. Substitua os índices pelo logaritmo e obtenha a aproximação da equação (?). O resultado da previsão, dividido pelo valor real, é a exponencial de $Ax - b$. Qual é o maior erro relativo? O que aconteceu em 1990? Em 2002? Tirando esses casos extremos (explicados por eventos internos ao Brasil), a sua previsão deve estar certa por um fator de 2.

Exercício 14.7. O tempo $T(n)$ utilizado para se calcular autovalores e autovetores de uma matriz aleatória $n \times n$ pode ser medido pelo seguinte comando *octave*:

[8]: `A=randn(n,n)
T0=time();
eigen(A);
T1=time();
T1-T0`

Utilizando mínimos quadrados, aproxime $T(n)$ por um polinômio em n . de grau 4 (faça isso para matrizes com $n > 50$). Qual o maior erro relativo das previsões?

Exercício 14.8. Mesmo problema para matrizes simétricas,

[9]: `A=randn(n,n)
A=A+A';
T0=time();
eigen(A);
T1=time();
T1-T0`

Observação 14.10. Interpretar nuens de dados é um problema extremamente complicado, que admite abordagens diferentes de acordo com a natureza dos dados. Áreas inteiras do conhecimento (como Estatística, Métodos de Interpolação, Teoria do Aprendizado (Learning Theory)) correspondem a diferentes abordagens do problema. No modelo financeiro acima, ignoramos totalmente o caráter aleatório dos índices financeiros utilizados.

CAPÍTULO 15

O processo de Gram-Schmidt

1. Ortonormalização



Seja $\alpha_1, \dots, \alpha_r$ uma base do subespaço $V \subseteq \mathbb{R}^n$. O processo de Gram Schmidt permite construir uma base ortonormal de V a partir dos α_i . O primeiro vetor da nova base é dado por

$$\mathbf{q}_1 = \frac{\alpha_1}{\|\alpha_1\|}$$

O segundo vetor da base é escolhido de forma que $(\mathbf{q}_1, \mathbf{q}_2)$ seja uma base ortonormal do espaço gerado por α_1 e α_2 :

$$\mathbf{q}_2 = \frac{\alpha_2 - \langle \mathbf{q}_1, \alpha_2 \rangle \mathbf{q}_1}{\|\alpha_2 - \langle \mathbf{q}_1, \alpha_2 \rangle \mathbf{q}_1\|}$$

Em geral, para $1 \leq s \leq r$, denotamos por V_s o subespaço gerado por $\alpha_1, \dots, \alpha_s$. Assim,

$$V_1 \subset V_2 \subset \dots \subset V_s = V$$

Escolhemos sempre

$$\mathbf{q}_j = \frac{\alpha_j - \sum_{i=1}^{j-1} \langle \mathbf{q}_i, \alpha_j \rangle \mathbf{q}_i}{\|\alpha_j - \sum_{i=1}^{j-1} \langle \mathbf{q}_i, \alpha_j \rangle \mathbf{q}_i\|}$$

Por indução, $(\mathbf{q}_1, \dots, \mathbf{q}_j)$ é sempre uma base ortonormal de V_j . Assim, concluímos que $(\mathbf{q}_1, \dots, \mathbf{q}_n)$ é base ortonormal de V .

2. A fatoração QR

Agora vamos considerar a versão matricial do procedimento de Gram-Schmidt. Seja A uma matriz $m \times n$ de posto n , $m \geq n$. Chamamos de α_j a j -ésima coluna de A . Utilizando as notações da seção acima, $V = \text{Im}A$.

Podemos escrever cada α_j como uma combinação linear dos $\mathbf{q}_i$. Como $\alpha_j \in V_j$ e $(\mathbf{q}_1, \dots, \mathbf{q}_j)$ é base de V_j , teremos

$$\alpha_j = \sum_{i=1}^j R_{ij} \mathbf{q}_i.$$

Sob forma matricial,

$$A = QR$$

onde Q é ortogonal e R é uma matriz triangular superior, de tamanho $n \times n$.

3. Outra solução para o Problema de Mínimos Quadrados

Voltamos agora ao problema de minimizar $\|Ax - \mathbf{b}\|^2$, onde A é uma matriz $m \times n$. Se soubermos a fatoração QR de A , poderemos escrever:

$$\|Ax - \mathbf{b}\|^2 = \|Q(Rx) - \mathbf{b}\|^2$$

A solução será o vetor $\mathbf{x}$ tal que $Q(Rx) = \pi(\mathbf{b})$, onde $\pi = QQ^T$ é a projeção ortogonal em $\text{Im}A = \text{Im}Q$. Logo, basta resolver $R\mathbf{x} = Q^T\mathbf{b}$.

4. Algoritmo para a decomposição QR

Vimos no capítulo anterior como produzir a matriz de simetria $H_{\mathbf{u},\mathbf{v}} = I - 2\frac{\mathbf{w}\mathbf{w}^T}{\|\mathbf{w}\|^2}$, $\mathbf{w} = \mathbf{u} - \mathbf{v}$ que permuta os vetores $\mathbf{u}$ e $\mathbf{v}$. O método abaixo é atualmente o mais utilizado para calcular decomposições QR. Dada a matriz A , fazemos

$$H_1 = H_{\alpha_1, \mathbf{e}_1}. \text{ Então a matriz } H_1 A \text{ tem por primeira coluna o vetor } \begin{bmatrix} \|\alpha_1\| \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

$$A = \begin{bmatrix} \times & \times & \cdots & \times \\ \times & \times & \cdots & \times \\ \times & \times & \cdots & \times \\ \vdots & \vdots & & \vdots \\ \times & \times & \cdots & \times \end{bmatrix} \quad H_1 A = \begin{bmatrix} \times & \times & \cdots & \times \\ 0 & \times & \cdots & \times \\ 0 & \times & \cdots & \times \\ \vdots & \vdots & & \vdots \\ 0 & \times & \cdots & \times \end{bmatrix}$$

Queremos uma simetria que preserve a primeira coordenada, e que zere parcialmente a segunda coluna de $H_1 A$:

$$H_2 H_1 A = \begin{bmatrix} \times & \times & \cdots & \times \\ 0 & \times & \cdots & \times \\ 0 & 0 & \cdots & \times \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \times \end{bmatrix}.$$

Indutivamente, chamamos de $\mathbf{u}_i$ a i -ésima coluna de $H_{i-1}H_{i-2}\cdots H_1 A$. Seja H_i a

$$\text{simetria permutando } \begin{bmatrix} 0 \\ \vdots \\ 0 \\ (\mathbf{u}_i)_i \\ (\mathbf{u}_i)_{i+1} \\ \vdots \\ (\mathbf{u}_i)_m \end{bmatrix} \text{ com } \mathbf{e}_i. \text{ Essa matriz mantém invariante o espaço}$$

gerado por $\mathbf{e}_1, \dots, \mathbf{e}_{i-1}$. Então, o bloco das primeiras i colunas de $H_i \cdots H_1 A$ será triangular superior. Finalmente,

$$H_n H_{n-1} \cdots H_1 A = \begin{bmatrix} R \\ 0 \end{bmatrix}$$

onde R é um bloco triangular superior de tamanho $n \times n$. Se definimos $Q = H_1 H_2 \cdots H_n$, teremos que

$$A = QR$$

As matrizes H_i são chamadas de *Reflexões de Householder*. A implementação prática desse algoritmo é um pouco mais sutil. A matriz Q não é nunca calculada explicitamente. Apenas as matrizes H_i são guardadas, representadas por um único

vetor (O vetor $\mathbf{w}$ do capítulo anterior). Multiplicar um vetor por H_i equivale a calcular um produto interno, $m - i + 1$ multiplicações e $m - i + 1$ somas. Logo, pode-se multiplicar um vetor por Q a um custo de $\frac{3}{2}(2m - n + 1)n$ operações aritméticas. Se n é bem pequeno, isso é muito mais rápido do que montar a matriz Q .

5. Exercícios

Exercício 15.1. Mostre que para todo i, j , $R_{ij} = \langle \mathbf{q}_i, \mathbf{a}_j \rangle$

Exercício 15.2. Calcule (pelo método de sua escolha) a decomposição QR da matriz $A = \begin{bmatrix} 1 & 2 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$.

Exercício 15.3. Considere a seguinte recorrência. É dada uma matriz A_1 simétrica de tamanho $n \times n$. Indutivamente, $A_i = Q_i R_i$ é a sua decomposição QR (obtida pelo método de Gram-Schmidt). Então fazemos $A_{i+1} = R_i Q_i$. Mostre que as A_i são todas simétricas.

Exercício 15.4. Nas hipóteses do exercício anterior, mostre que os autovalores de A_1 e de A_i são os mesmos.

Exercício 15.5. Ainda nas hipóteses do exercício anterior, se $C = \lim_{i \rightarrow \infty} A_i$ existe A_1 é simétrica, mostre que C é diagonal.

Exercício 15.6. Produza a seguinte matriz simétrica em *Julia*:

[1] : `using(LinearAlgebra)`

[2] : `(T,R)=qr(randn(10,10)); D=diagm(0=>Vector{1.0:10.0}); A=T*D*T';`

Quais são os autovalores de A ? O que é que você observa depois de aplicar 100 vezes a iteração do exercício 15.3?

Exercício 15.7. Considere o espaço E de todos os polinômios reais e uma variável, com o seguinte produto interno:

$$\langle f, g \rangle = \int_{-1}^1 f(x)g(x) \, dx$$

A base $(1, x, x^2, \dots)$ não é ortogonal. Produza numericamente os primeiros 8 elementos de uma base ortonormal. Dica: o oitavo elemento é múltiplo de $429x^7 - 693x^5 + 315x^3 - 35x$. Esses polinômios são conhecidos como *polinômios de Legendre*.

Exercício 15.8. Mesmo exercício, para o produto interno

$$\langle f, g \rangle = \int_{-1}^1 \frac{f(x)g(x)}{\sqrt{1-x^2}} \, dx.$$

O oitavo elemento da base é múltiplo de: $64x^7 - 112x^5 + 56x^3 + 1$. Esses polinômios são chamados de *polinômios de Tchebichev*

Exercício 15.9. Verifique, utilizando fórmulas trigonométricas, que $x \mapsto \cos(n \arccos(x))$ é um polinômio em x .

Exercício 15.10. Mostre que $x \mapsto \cos(n \arccos(x))$ é (a menos de um múltiplo) o $n - 1$ -ésimo polinômio de Tchebichev

CAPÍTULO 16

Matrizes simétricas e o teorema espectral

1. Matrizes simétricas e formas bilineares simétricas



Uma matriz S real de tamanho $n \times n$ é *simétrica* se e somente se $S = S^T$. A uma matriz S real e simétrica, podemos associar uma *forma bilinear simétrica*:

$$\begin{aligned} f: \mathbb{R}^n \times \mathbb{R}^n &\rightarrow \mathbb{R} \\ (\mathbf{u}, \mathbf{v}) &\mapsto f(\mathbf{u}, \mathbf{v}) = \mathbf{u}^T S \mathbf{v} \end{aligned}$$

linear em $\mathbf{u}$, em $\mathbf{v}$ e tal que $f(\mathbf{u}, \mathbf{v}) = f(\mathbf{v}, \mathbf{u})$. Reciprocamente, dada uma forma bilinear simétrica $f = f(\mathbf{u}, \mathbf{v})$, define-se a matriz simétrica S por $S_{ij} = f(\mathbf{e}_i, \mathbf{e}_j)$. Desse ponto de vista, matrizes simétricas e formas bilineares são essencialmente o mesmo objeto.

2. O Teorema Espectral

Vamos mostrar o seguinte resultado para matrizes simétricas:

Teorema 16.1 (Teorema Espectral para matrizes simétricas). *Seja S uma matriz real e simétrica. Então todos os autovalores de S são reais, e existe uma base ortonormal de autovetores reais de S .*

Em termos de formas bilineares, podemos parafrasear o Teorema Espectral assim:

Corolário 16.1.1. *Seja f uma forma bilinear simétrica real. Então existe uma base ortonormal $(\alpha_1, \dots, \alpha_n)$ e existem números reais $\lambda_1, \dots, \lambda_n$ tais que*

$$f(\mathbf{u}, \mathbf{v}) = \sum_i \lambda_i \langle \alpha_i, \mathbf{u} \rangle \langle \alpha_i, \mathbf{v} \rangle$$

Vamos começar provando que os autovalores de uma matriz simétrica são sempre reais.

Lema 16.2. *Seja S uma matriz real e simétrica. Então todo autovalor de S é real.*

Antes de provar o Lema, precisamos introduzir a *transposta Hermitiana*. Se $\mathbf{u}$ é um vetor complexo, escrevemos $\mathbf{u}^H = \bar{\mathbf{u}}^T = [\bar{u}_1, \bar{u}_2, \dots, \bar{u}_n]$. Desse modo, por exemplo, $\|\mathbf{u}\|^2 = \mathbf{u}^H \mathbf{u}$. Da mesma maneira, se A é uma matriz, $A^H = \bar{A}^T$.

DEMONSTRAÇÃO. Assuma que $\mathbf{u} \neq 0$ é um autovetor de S : $S\mathbf{u} = \lambda\mathbf{u}$. Tanto λ com $\mathbf{u}$ podem ser complexos.

Então por um lado

$$\mathbf{u}^H S \mathbf{u} = \mathbf{u}^H (S \mathbf{u}) = \lambda \mathbf{u}^H \mathbf{u} = \lambda \|\mathbf{u}\|^2.$$

Por outro lado,

$$\mathbf{u}^H S \mathbf{u} = (\mathbf{u}^H S) \mathbf{u} = (S \mathbf{u})^H \mathbf{u} = (\lambda \mathbf{u})^H \mathbf{u} = \bar{\lambda} \mathbf{u}^H \mathbf{u} = \bar{\lambda} \|\mathbf{u}\|^2.$$

Como $\mathbf{u} \neq 0$, deduzimos que $\lambda = \bar{\lambda}$, logo $\lambda \in \mathbb{R}$. □

Lema 16.3. *Seja S uma matriz real simétrica. Seja $\mathbf{u}$ um autovetor de S . Então para todo $\mathbf{v} \perp \mathbf{u}$, $S\mathbf{v} \perp \mathbf{u}$*

DEMONSTRAÇÃO.

$$\langle \mathbf{u}, S\mathbf{v} \rangle = \langle S\mathbf{u}, \mathbf{v} \rangle = \lambda \langle \mathbf{u}, \mathbf{v} \rangle = 0$$

□

DEMONSTRAÇÃO DO TEOREMA ESPECTRAL 16.1.

Hipótese de Indução: O Teorema vale para matrizes $n \times n$.

O caso inicial é simples. Se S é de tamanho 1×1 , então existe um único autovalor S associado ao autovetor 1. Assumimos portanto o Teorema provado até o tamanho n .

Seja S uma matriz de tamanho $(n+1) \times (n+1)$. Ela tem pelo menos um autovalor λ_1 real (Lema 16.2), e pelo menos um autovetor $\mathbf{u}_1$ com $\|\mathbf{u}_1\| = 1$. Seja $W = \mathbf{u}_1^\perp$. Seja $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ uma base ortonormal de W . Pelo Lema 16.3, todo vetor de W é levado por S em um vetor de W .

Definimos $T_{ij} = \mathbf{v}_i^T S \mathbf{v}_j$. Então a matriz T é real e simétrica. Por indução, admite uma base ortonormal de autovetores, digamos $(\mathbf{u}_2, \dots, \mathbf{u}_{n+1})$ associados a autovalores reais $\lambda_2, \dots, \lambda_{n+1}$. Temos portanto, para todo $i = 1, \dots, n+1$,

$$S\mathbf{u}_i = \lambda_i \mathbf{u}_i$$

Além disso, como $W = \mathbf{u}_1^\perp$, $(\mathbf{u}_1, \dots, \mathbf{u}_{n+1})$ é base ortonormal de $\mathbb{R}^{n+1}$. □

3. Matrizes positivas e positivas definidas

Definição 16.4. Uma forma bilinear simétrica f em $\mathbb{R}^n$ é

- (1) *positiva*, se e somente se para todo vetor $\mathbf{u} \neq 0$, $f(\mathbf{u}, \mathbf{u}) \geq 0$
- (2) *positiva definida*, se e somente se para todo vetor $\mathbf{u} \neq 0$, $f(\mathbf{u}, \mathbf{u}) > 0$
- (3) *negativa*, se e somente se para todo vetor $\mathbf{u} \neq 0$, $f(\mathbf{u}, \mathbf{u}) \leq 0$
- (4) *negativa definida*, se e somente se para todo vetor $\mathbf{u} \neq 0$, $f(\mathbf{u}, \mathbf{u}) < 0$

A mesma terminologia é utilizada para matrizes simétricas. Por exemplo, uma matriz simétrica S é *positiva definida* se e somente se, para todo vetor $\mathbf{u} \neq 0$, $\mathbf{u}^T S \mathbf{u} > 0$.

Proposição 16.5. *Seja S uma matriz real simétrica. As seguintes afirmações são equivalentes:*

- (1) *A matriz S é positiva definida.*
- (2) *Os autovalores de S são estritamente positivos.*
- (3) *Para todo $k \in \{1, 2, \dots, n\}$, a submatriz principal de tamanho k tem determinante positivo.*
- (4) *A matriz S pode ser fatorada $S = LU$, onde L é triangular inferior com uns na diagonal e U é triangular superior, com $U_{ii} > 0$.*
- (5) *A matriz S pode ser fatorada $S = LDL^T$, onde L é triangular inferior com uns na diagonal e D é diagonal com $D_{ii} > 0$.*

DEMONSTRAÇÃO.

(1) $\Rightarrow$ (2): Assuma que S é positiva definida. Então cada um dos autovetores $\mathbf{u}$ satisfaz $\lambda \|\mathbf{u}\|^2 = \mathbf{u}^T S \mathbf{u} > 0$. Logo $\lambda > 0$ para todos os autovalores.

(2) $\Rightarrow$ (1): Escrevendo $\mathbf{u}$ na base $(\alpha_1, \dots, \alpha_n)$ dos autovetores de S , $\mathbf{u} = x_1 \alpha_1 + \dots + x_n \alpha_n$, deduzimos que $\mathbf{u}^T S \mathbf{u} = \sum x_i^2 \lambda_i > 0$.

(1) $\Rightarrow$ (3): Todas as submatrizes principais são positivas definidas, e seus autovalores são portanto estritamente positivos. O determinante é produto dos autovalores, logo é estritamente positivo.

(3) $\Rightarrow$ (4): Vamos admitir que todos os subdeterminantes principais de S sejam positivos definidos. Podemos obter L e U por eliminação Gaussiana, onde (após k passos) teremos: $U_{11} \dots U_{kk}$ igual ao subdeterminante principal $k \times k$ de S . Por esse motivo $U_{kk} > 0$ e podemos continuar a eliminação Gaussiana.

(4) $\Rightarrow$ (5): Fazemos $D_{ii} = U_{ii}$. Dessa maneira, $S = LD(D^{-1}U)$. Por construção, $M = (D^{-1}U)^T$ é triangular inferior com uns na diagonal. Como S é simétrica, temos que $S = M(DL^T)$ com DL^T triangular superior. Como a fatoração LU é única, $L = M$.

(5) $\Rightarrow$ (1): Assumindo que $S = LDL^T$, teremos sempre

$$\mathbf{u}^T S \mathbf{u} = (L^T \mathbf{u})^T D (L^T \mathbf{u}) > 0.$$

□

4. Aplicação: máximos e mínimos

Se $f : \mathbf{R}^2 \rightarrow \mathbf{R}$ é uma função diferenciável, a sua expansão de Taylor de ordem 2 no ponto $\mathbf{x}$ é dada por:

$$f(\mathbf{x} + \mathbf{h}) = f(\mathbf{x}) + \nabla f(\mathbf{x})\mathbf{h} + \frac{1}{2}\mathbf{h}^T Hf(\mathbf{x})\mathbf{h} + o(\|\mathbf{h}\|^2)$$

onde o Gradiente de f é dado por

$$\nabla f(\mathbf{x}) = \left[\frac{\partial f}{\partial x_1} \quad \frac{\partial f}{\partial x_2} \right]$$

e a Hessiana, ou derivada segunda, é representada pela matriz simétrica

$$Hf(\mathbf{x}) = \begin{bmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} \\ \frac{\partial^2 f}{\partial x_1 \partial x_2} & \frac{\partial^2 f}{\partial x_2^2} \end{bmatrix}$$

Muitos livros de Cálculo contêm sempre o seguinte Teorema, que eu considero um exemplo canônico de mau gosto matemático:

Teorema. Para que um ponto $\mathbf{x}$ seja mínimo local de f , basta que $\nabla f(\mathbf{x}) = 0$ e que, além disso,

$$\frac{\partial^2 f}{\partial x_1^2} > 0 \quad e \quad \frac{\partial^2 f}{\partial x_1^2} \frac{\partial^2 f}{\partial x_2^2} - \frac{\partial^2 f}{\partial x_1 \partial x_2} \frac{\partial^2 f}{\partial x_1 \partial x_2} > 0$$

Esse enunciado obscurece o motivo do Teorema ser verdadeiro. O texto conceitualmente correto é:

Teorema. Para que um ponto $\mathbf{x}$ seja mínimo local de f , basta que $\nabla f(\mathbf{x}) = 0$ e que, além disso, a Hessiana $Hf(\mathbf{x})$ seja positiva definida.

5. Exercícios

Exercício 16.1. Mostre que se S é positiva definida, então existe uma matriz R simétrica positiva definida, conhecida com raiz quadrada de S , tal que $S = R^2$. Ela é única?

Exercício 16.2. Seja $f(x, y) = Ax^2 + 2Bxy + Cy^2 - F$. Qual é o lugar geométrico da curva $f(x, y) = 0$? Existem diversas possibilidades em função da matriz simétrica $\begin{bmatrix} A & B \\ B & C \end{bmatrix}$.

Exercício 16.3. Considere agora a cônica em $\mathbb{R}^n$, de equação $\mathbf{x}^T S \mathbf{x} + \mathbf{v}^T \mathbf{x} - f = 0$. A matriz S é simétrica. Assuma que nenhum dos seus autovalores se anule. Quais são as possibilidades para o lugar geométrico dessa cônica?

Exercício 16.4. Um *cone* é um conjunto $\mathcal{C}$ tal que, se $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ e $\lambda, \mu > 0$, temos sempre $\lambda \mathbf{u} + \mu \mathbf{v} \in \mathcal{C}$. Mostre que o conjunto das matrizes simétricas positivas definidas é um cone.

Exercício 16.5. Descreva todas as matrizes $n \times n$ que são simétricas e ortogonais.

Exercício 16.6. Seja S uma matriz $n \times n$ simétrica. O quociente de Rayleigh é uma função de $\mathbb{R}^n \rightarrow \mathbb{R}$ definida por $Q(\mathbf{x}) = \frac{\mathbf{x}^T S \mathbf{x}}{\mathbf{x}^T \mathbf{x}}$. Sejam $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ os autovalores de S . Mostre que para todo $0 \leq k \leq n-1$, se W é um subespaço de dimensão $k+1$ de $\mathbb{R}^n$, então $\min_{\mathbf{x} \in W} Q(\mathbf{x}) \geq \lambda_{n-k}$.

Exercício 16.7. Mostre que se $f(\mathbf{u}, \mathbf{v})$ é uma forma bilinear simétrica em $\mathbb{R}^n$, então existe uma base $(\alpha_1, \dots, \alpha_n)$ de $\mathbb{R}^n$ na qual f se escreve:

$$f(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^n \sigma_i u_i v_i$$

e $\sigma_i \in \{-1, 0, 1\}$.

Exercício 16.8. Mostre que se A é anti-simétrica, então todo autovalor de A é necessariamente imaginário puro.

Exercício 16.9. Seja G uma matriz simétrica positiva definida, e seja H uma matriz simétrica. Mostre que existe uma base α de $\mathbb{R}^n$ na qual G_α e H_α são ambas diagonais.

Exercício 16.10. Usando *Julia*, gere 10000 matrizes aleatórias 100 por 100 e calcule os autovalores. Plote um histograma dos autovalores. As matrizes aleatórias podem ser geradas por:

[39]: `A=randn(100,100); S=A+A'`

Você deve observar um gráfico em forma de semicírculo. Esse fato é conhecido como *Lei de Wigner*. As matrizes aleatórias que você gerou pertencem a um espaço de probabilidade conhecido como o *Gaussian Orthogonal Ensemble*.

CAPÍTULO 17

Aplicações lineares e valores singulares

1. A decomposição em valores singulares



Seja $A : \mathbb{R}^n \rightarrow \mathbb{R}^m$ uma aplicação linear. Os espaços $\mathbb{R}^n$ e $\mathbb{R}^m$ são munidos do produto interno canônico. Vamos mostrar que existem uma base ortonormal $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ de $\mathbb{R}^n$, e uma base ortonormal $(\mathbf{u}_1, \dots, \mathbf{u}_m)$ de $\mathbb{R}^m$, tais que a matriz $\Sigma = A_{\mathbf{u}, \mathbf{v}}$ associada a A relativa a essas duas bases é diagonal positiva. Podemos escrever esse resultado em forma de fatoração matricial:

Teorema 17.1. *Seja A uma matriz real de tamanho $m \times n$. Então existem $U \in O(m)$, $V \in O(n)$ e Σ diagonal positiva de tamanho $m \times n$, tais que*

$$A = U\Sigma V^T.$$

Além disso, podemos escolher Σ de maneira a que

$$\Sigma_{ij} = \begin{cases} 0 & \text{se } i \neq j \\ \sigma_i & \text{se } i = j, \end{cases}$$

com $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n \geq 0$.

Os números $\sigma_1, \dots, \sigma_n$ são chamados de *valores singulares* da aplicação A . Dependem dos produtos internos utilizados nos espaços $\mathbb{R}^m$ e $\mathbb{R}^n$. Os vetores $\mathbf{u}_i$, ou colunas de U , são chamados de *vetores singulares* à esquerda e os vetores $\mathbf{v}_j$ (colunas de V) de *vetores singulares* à direita.

DEMONSTRAÇÃO. Vamos assumir sem perda de generalidade que $m \geq n$. (Para o caso $m < n$, basta substituir A por A^T). A matriz $A^T A$ é real e simétrica. Pelo Teorema 16.1, ela admite uma base ortonormal $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ de autovetores. Denotamos por λ_i os autovalores de $A^T A$. Para todo $i = 1, \dots, n$, definimos

$$\sigma_i = \|A\mathbf{v}_i\|$$

e assumimos que a base $\mathbf{v}_i$ está ordenada de maneira que $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n$. Seja r o posto de A , então $\sigma_1, \dots, \sigma_r \neq 0$ e para todo $i \in \{1, 2, \dots, r\}$, podemos definir

$$\mathbf{u}_i = \sigma_i^{-1} A\mathbf{v}_i$$

Por construção, $\|\mathbf{u}_i\| = 1$. (Note que isso implica que $\sigma_i^2 = \lambda_i$). Como para todo $i \neq j$, $\mathbf{v}_i(A^T A)\mathbf{v}_j = \lambda_j \mathbf{v}_i^T \mathbf{v}_j = 0$, teremos que $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$ e os $\mathbf{u}_i$ formam um conjunto ortonormal.

Existe uma base $(\mathbf{u}_1, \dots, \mathbf{u}_r, \mathbf{w}_{r+1}, \dots, \mathbf{w}_m)$ de $\mathbb{R}^n$. Aplicando Gram-Schmidt a essa base, obtemos uma base ortonormal $(\mathbf{u}_1, \dots, \mathbf{u}_m)$. Como todo vetor ortogonal à imagem de A pertence ao núcleo de A^T ,

$$A = U \begin{bmatrix} \sigma_1 & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & 0 & \cdots & 0 \\ 0 & 0 & \sigma_3 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \sigma_r \\ 0 & 0 & & & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & & & 0 \end{bmatrix} V^T$$

□

Uma interpretação geométrica é a seguinte. Assuma que A é de tamanho $m \times n$, com $m \geq n$ e posto n). Seja

$$\mathcal{E} = \{A\mathbf{x} : \|\mathbf{x}\| \leq 1\}$$

O conjunto $\mathcal{E}$ é o elipsoide de centro zero, e semieixos $\sigma_i \mathbf{u}_i$.

2. Aplicações à mineração de dados

Em março 2021, foi estimado¹ que existiriam entre 5 e 55 bilhões de páginas indexadas na rede. Um problema fundamental no início da internet era fazer buscas por palavra chave. Para evitar a necessidade de armazenar uma cópia da World Wide Web inteira no site de busca, o seguinte algoritmo foi sugerido para fazer a associação entre páginas e palavras:

Define-se a matriz A , de tamanho $m \times n$, onde m é o número de páginas (11,5 bilhões) e n o número de palavras indexáveis (dicionário, procuras frequentes, etc...). (No início da *Google*, em torno de 24 milhões). (Retiram-se artigos como “o”, “e”, etc...).

A coordenada A_{ij} é o número de ocorrências da j -ésima palavra na i -ésima página. A rede é constantemente vasculhada por programas *rastejadores* (em inglês, *crawlers* ou *bots*, contração de ‘robôs’) que fazem a atualização da matriz.

Com o aumento vertiginoso do conteúdo visível na internet, pode não ser viável (e talvez não seja conveniente hoje) armazenar a matriz A inteira, mesmo de modo esparsa. Uma possibilidade é armazenar uma aproximação de A . Por exemplo, a melhor aproximação de posto k para a matriz A .

Assuma que

$$A = U \begin{bmatrix} \sigma_1 & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & 0 & \cdots & 0 \\ 0 & 0 & \sigma_3 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & \sigma_r \\ 0 & 0 & & & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & & & 0 \end{bmatrix} V^T$$

¹<https://www.worldwidewebsize.com/>

Então prova-se que a melhor aproximação de posto k é

$$A = \begin{bmatrix} \mathbf{u}_1 & \dots & \mathbf{u}_k \end{bmatrix} \begin{bmatrix} \sigma_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_k \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 & \dots & \mathbf{v}_k \end{bmatrix}^T$$

que é um objeto de tamanho $(m + n + 1)k$, bem menor do que mn .

Um algoritmo de compressão similar foi proposto para imagens (A_{ij} seria a intensidade do pixel (i, j)). Mas não parece existir evidência de alguma vantagem em relação aos formatos de compressão usuais, como jpg.

3. A pseudo-inversa

Nem toda matriz é inversível. Mas toda matriz (mesmo sendo quadrada) tem uma pseudo-inversa.

Definição 17.2. Seja A uma matriz real de tamanho $m \times n$. A *pseudo-inversa* de A , denotada por $A^\dagger$, é a matriz de tamanho $n \times m$ dada por:

$$A^\dagger \mathbf{y} = \mathbf{x}$$

onde $A\mathbf{x} = \pi\mathbf{y}$, π denota a projeção ortogonal de $\mathbf{y}$ em $\text{Im}A$, e $\|\mathbf{x}\|$ é minimal sob essas condições. Em particular, $\mathbf{x} \perp \ker A$.

A pseudo-inversa de uma matriz diagonal (por exemplo, $m > n$) é portanto:

$$\begin{bmatrix} \sigma_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & \sigma_n \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{bmatrix}^\dagger = \begin{bmatrix} \rho_1 & \dots & 0 & 0 & \dots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & \dots & \rho_n & 0 & \dots & 0 \end{bmatrix}$$

onde $\rho_j = \sigma_j^{-1}$ quando $\sigma_j \neq 0$, e $\rho_j = 0$ se $\sigma_j = 0$.

A pseudo-inversa de uma matriz quadrada inversível A é sempre $A^\dagger = A^{-1}$.

Outro caso importante é o de matrizes ortogonais. Se Q for ortogonal, da definição de pseudo-inversa concluímos que:

$$Q^\dagger = Q^T \quad \text{e} \quad (Q^T)^\dagger = Q$$

Em geral, se $A = U\Sigma V^T$ é a decomposição em valores singulares de A , $A^\dagger = V\Sigma^\dagger U$ (Exercício 17.6).

Finalmente, podemos escrever a solução geral do problema de mínimos quadrados utilizando a pseudo-inversa: O valor de $\mathbf{x}$ que minimiza $\|A\mathbf{x} - \mathbf{b}\|^2$ com $\|\mathbf{x}\|$ minimal é $\mathbf{x} = A^\dagger \mathbf{b}$.

4. Exercícios

Exercício 17.1. Compare os autovalores e autovetores de $\begin{bmatrix} 0 & A^T \\ A & 0 \end{bmatrix}$ com os valores singulares e vetores singulares de A .

Exercício 17.2. Mostre que para todo vetor $\mathbf{x}$, $\|A\mathbf{x}\| \leq \sigma_1 \|\mathbf{x}\|$, onde σ_1 é o maior valor singular de A .

Exercício 17.3. Se A for sobrejetiva, mostre que $AA^\dagger$ é a identidade. Mostre um exemplo de matriz A não sobrejetiva com $AA^\dagger \neq I$.

Exercício 17.4. Se A for injetiva, mostre que $A^\dagger A$ é a identidade. Mostre um exemplo de matriz A não injetiva com $A^\dagger A \neq I$.

Exercício 17.5. Mostre que se A é uma matriz qualquer, então $A^\dagger A$ é a identidade, ou é uma projeção.

Exercício 17.6. Mostre que se $A = U\Sigma V^T$ é a decomposição em valores singulares de A , $A^\dagger = V\Sigma^\dagger U^T$.

Exercício 17.7. Ache um exemplo onde $(AB)^\dagger \neq B^\dagger A^\dagger$.

Exercício 17.8. Seja A uma matriz $m \times n$, com $m > n$ e valores singulares $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n$. Seja W um subespaço r -dimensional de $\mathbb{R}^n$. Mostre que $\|A|_W\| \geq \sigma_{n-r+1}$.

Exercício 17.9. Descreva o conjunto de todas as triplas (U, Σ, V) tal que $A = U\Sigma V^T$ seja a decomposição em valores singulares de A , para $A = \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$.

Exercício 17.10. Mesmo problema, para $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 1 & 1 \end{bmatrix}$.

CAPÍTULO 18

Covariância e carteiras de investimentos.

1. Variáveis aleatórias



Quando jogamos uma moeda para o alto, não conseguimos prever como é que ela vai cair, se cara para cima ou coroa para cima. Mas podemos tratar o resultado como um *evento aleatório*, e fazer apostas razoáveis.

O exemplo acima introduz uma variável aleatória discreta x (que pode valer, por exemplo, $x = +1$ ou $x = -1$ de acordo com o resultado. A moeda é dita *justa* se a probabilidade do resultado ser $+1$ é de exatamentente $\frac{1}{2}$.

No exemplo acima, seria razoável apostar no resultado $x = +1$, desde que o pagamento (em caso de acerto) seja igual ou maior do que duas vezes a quantia apostada. Para fixar as idéias, vamos supor que a quantia apostada é R\$ 1,00. Digamos que o pagamento em caso de acerto seja $p = 2$. O *retorno* será de px , e o ganho $y = px - 1$. Ocorre que $px - 1$ é uma variável aleatória, que tanto pode valer R\$ 1,00 como R\$ -1,00. O *retorno esperado* é de

$$E(y) = \frac{1}{2} \text{R\$ } 1,00 + \frac{1}{2} \text{R\$ } -1,00 = 0 .$$

Agora vamos supor que dois jogadores repetem esse mesmo jogo por n rodadas. Admitimos que o resultado x_i de cada experimento é independente dos outros. Chamamos de y_i o retorno (para o primeiro jogador) na i -ésima iteração.

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.

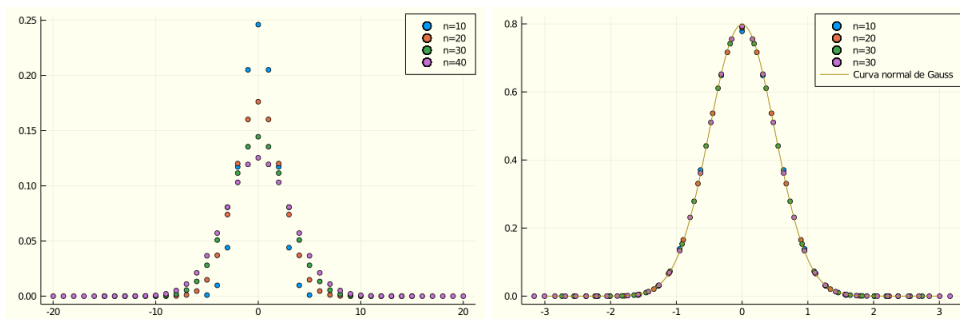


FIGURA 1. Distribuição binomial: à esquerda temos a probabilidade de cada ganho possível para vários valores do número n de rodadas; à direita, distribuições binomiais com média 0 e desvio padrão $\sigma = 1$. O limite é a distribuição normal de Gauss.

Temos que $E(y_i) = 0$. Logo $E(\sum y_i) = 0$. No entanto, também podemos apostar que um dos jogadores vai ficar mais pobre. De fato, a probabilidade do primeiro jogador ganhar exatamente k vezes é dada pela distribuição binomial (Figura 1),

$$\text{Prob}[k = \#\{i : x_i = 1\}] = 2^{-n} \binom{n}{k}$$

A probabilidade de que $|k| > r$ é igual à *probabilidade bicaudal* $2 \sum_{k>r} 2^{-n} \binom{n}{k}$.

Aviso: Os jogos de azar oferecidos em cassinos ou loterias têm sempre retorno esperado negativo para o cliente, e positivo para a banca. Máquinas de video-poker costumam estar viciadas em favor da banca. Por exemplo, no jogo de roleta, o retorno esperado é de no máximo 36/37 devido à introdução do zero. Nos Estados Unidos, existe ainda o 00, o que abaixa o retorno esperado para 35/37.

2. Variáveis aleatórias contínuas

A introdução de variáveis aleatórias contínuas permite introduzir em probabilidade todo o ferramental do cálculo e da álgebra linear (e da análise funcional). Vamos começar com dois exemplos de variáveis aleatórias contínuas.

Exemplo 18.1. A variável x é *uniformemente distribuída* no intervalo $[0, 1]$ se para todos $0 \leq a \leq b \leq 1$,

$$\text{Prob}[x \in [a, b]] = b - a$$

Exemplo 18.2. A variável $x \in \mathbb{R}$ é *normalmente distribuída* com média μ e variância σ^2 se e somente se, para todos $a \leq b \in \mathbb{R}$,

$$\text{Prob}[x \in [a, b]] = \int_a^b \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} dx.$$

É um exercício de cálculo multivariado verificar que $\text{Prob}[x \in (-\infty, +\infty)] = 1$.

No caso acima, a função $\rho(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$ é chamada de *densidade de probabilidade*. Em geral,

Definição 18.3. Seja $\rho(x)$ uma função positiva, e tal que $\int_{-\infty}^{\infty} \rho(x) dx = 1$. Então dizemos que x é uma *variável aleatória* com densidade de probabilidade $\rho(x)$ se e somente se,

$$\text{Prob}[x \in [a, b]] = \int_a^b \rho(x) dx.$$

A *média* ou *esperança matemática* de x é definida por:

$$E(x) = \int_a^b x\rho(x) dx.$$

A *variância* σ^2 de x é a média do quadrado da diferença entre x e $E(x)$:

$$\sigma^2 = E((x - E(x))^2).$$

Chama-se de *desvio padrão* a raiz quadrada σ da variância σ^2 .

Observação 18.4. É possível unificar o tratamento de variáveis aleatórias discretas e contínuas utilizando teoria da medida, ou funções generalizadas. Esses conceitos fazem parte dos cursos de teoria da medida e análise funcional, respectivamente.

Observação 18.5. Até agora tenho tentado explicar como operar com variáveis aleatórias e o conceito de probabilidade, mas não tentei definir o que é uma probabilidade, ou quando é que um evento é *aleatório*. Não existe uma resposta satisfatória a essas perguntas. A maioria dos eventos que tratamos como aleatórios tem uma incerteza associada a uma das seguintes situações:

- (1) Ignorância: Não sabemos prever o resultado de um experimento por falta de embasamento teórico. Por isso, tratamos o resultado como aleatório.
- (2) Falta de informação: Temos um modelo teórico (a mecânica clássica, no caso da moeda) mas não conhecemos as condições iniciais do movimento.
- (3) Conveniência: Mesmo tendo todas as informações relevantes, podemos decidir que é mais conveniente tratar um resultado como aleatório.
- (4) Sensibilidade às condições iniciais: Um modelo pode ser tal que, para prever o resultado de um experimento (por exemplo, o tempo no Rio de Janeiro em um certo dia) sejam necessários dados extremamente precisos, e que a precisão necessária cresça rapidamente em função do intervalo de previsão. Assim, é possível prever o tempo com alguns dias de antecedência, mas aumentar essa antecedência teria um custo proibitivo. A solução é assumir perturbações aleatórias das condições iniciais medidas, e resolver o modelo para um número suficiente de perturbações. O resultado é apresentado como uma ‘probabilidade’ de chuva...
- (5) Adversário: Se existisse um algoritmo para ganhar dinheiro na bolsa de valores acima do mercado, todos utilizariam esse algoritmo. Mas um especulador mais esperto poderia prever a evolução do mercado, se antecipar e ganhar mais dinheiro.
- (6) Complexidade computacional: o custo de prever o próximo número pseudo-aleatório, dados os números pseudo-aleatórios anteriores, é proibitivo.
- (7) Sistema excessivamente complexo: O número de variáveis e as relações entre elas são tão complicadas que não vale a pena fazer uma simulação detalhada.
- (8) Princípio da incerteza de Hessemberg: Não é possível conhecer a posição e o momento de uma partícula simultaneamente. Se medimos a posição, modificamos o momento.
- (9) Interpretação de Copenhagen: A posição de uma partícula não é uma grandeza física fundamental. A grandeza física fundamental é uma função de onda (complexa), e o quadrado do módulo dessa função de onda é a densidade de probabilidade da posição da partícula. Essa é uma das interpretações da mecânica quântica.
- (10) Superposição de caminhos: essa é outra interpretação da mecânica quântica, pela qual uma partícula está naturalmente em uma superposição de estados. O observador também. Quando ocorre a observação, a partícula e o observador ficam em estados *entrelaçados*, e a partícula aparenta ao observador ter assumido um estado definido.

3. Covariância

Agora vamos considerar duas variáveis aleatórias x e y . Elas são ditas *independentes* se o conhecimento do resultado de y em um experimento não nos traz nenhuma informação adicional sobre o valor de x .

Em termos de densidade de probabilidade, o par (x, y) tem uma densidade de probabilidade conjunta $\varphi_{x,y} \geq 0$: Se $\mathcal{D} = [a, b] \times [c, d]$ é um retângulo,

$$\text{Prob}[(x, y) \in \mathcal{D}] = \iint_{(x,y) \in \mathcal{D}} \varphi_{x,y}(x, y) dx dy = \int_a^b \left(\int_c^d \varphi_{x,y}(x, y) dy \right) dx$$

As variáveis x e y são *independentes* se e somente se $\varphi_{x,y}(x, y) = \varphi_x(x)\varphi_y(y)$, onde φ_x e φ_y são positivas e com integral 1 na reta. Nesse caso,

$$\begin{aligned} \text{Prob}[x \in [a, b]] &= \iint_{(x,y) \in [a,b] \times \mathbb{R}} \varphi_{x,y}(x, y) dx dy \\ &= \int_{x \in [a,b]} \varphi_x(x) \left(\int_{y \in \mathbb{R}} \varphi_y(y) dy \right) dx \\ &= \int_{x \in [a,b]} \varphi_x(x) dx \end{aligned}$$

e a mesma coisa para y .

No mundo real, eventos aleatórios nem sempre são independentes. Por exemplo, há dias no qual a bolsa de valores opera em alta e dias no qual a bolsa opera em baixa. Podemos considerar a variação de cada ação como um evento aleatório, mas o desempenho de uma ação está influenciando as outras ações.

Uma maneira de medir a dependência de duas funções aleatórias é definir covariância e correlação linear.

A *covariância* das variáveis aleatórias x e y , de média respectiva $\mu = E(x)$ e $\nu = E(y)$ é

$$C = E((x - \mu)(y - \nu)) .$$

Em particular, a covariância de x com x é igual à variância. Se x e y forem independentes, então a covariância é $C = E((x - \mu)(y - \nu)) = E(x - \mu) = 0$.

Dada uma densidade de probabilidade (por exemplo $\varphi_{x,y}$), podemos definir o produto interno

$$\langle f, g \rangle = \int_{\mathbb{R}^2} f(x, y)g(x, y)\varphi_{x,y}$$

no espaço de todas as funções f de ‘quadrado integrável’, ou seja tais que $E(f(x, y)^2) < \infty$.

Pela estimativa de Cauchy-Buniakovskii-Schwarz,

$$C = \langle x - \mu, y - \nu \rangle \leq \|x - \mu\| \|y - \nu\| .$$

A norma $\|x - \mu\|$ pode ser interpretada como o desvio-padrão de x . Se dividimos a covariância pelos desvios-padrão de x e y , obtemos um índice em $[-1, 1]$

$$\rho = \frac{\langle x - \mu, y - \nu \rangle}{\|x - \mu\| \|y - \nu\|} ,$$

chamado de *correlação linear*.

4. Estatística multivariada

Vamos assumir agora que temos n variáveis aleatórias $x_1, \dots, x_n$, que vamos representar como um vetor aleatório $\mathbf{x} \in \mathbb{R}^n$. Seja $\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^+$ a densidade de probabilidade conjunta das x_i ,

$$1 = \int_{\mathbb{R}^n} \varphi(\mathbf{x}) d\mathbf{x}$$

Se f é uma função em $\mathbb{R}^n$, então a *esperança matemática* de f é

$$E(f) = \int_{\mathbb{R}^n} f(\mathbf{x}) \varphi(\mathbf{x}) d\mathbf{x}$$

A mesma definição se aplica para funções a valores em $\mathbb{R}^m$. Em particular, a *média* de $\mathbf{x}$ é dada por

$$\boldsymbol{\mu} = E(\mathbf{x}) = \int_{\mathbb{R}^n} \mathbf{x} \varphi(\mathbf{x}) d\mathbf{x}$$

onde $\boldsymbol{\mu} \in \mathbb{R}^n$ e a integral é calculada coordenada a coordenada.

Agora gostaríamos de medir quanto é que a variável aleatória $\mathbf{x}$ se afasta da média. Para isso, definimos a *matriz de covariância* C por

$$C_{ij} = E((x_i - \mu_i)(x_j - \mu_j))$$

ou, vetorialmente,

$$C = E((\mathbf{x} - \boldsymbol{\mu})(\mathbf{x} - \boldsymbol{\mu})^T)$$

Por construção, a matriz de covariância é simétrica. No exercício 18.1, você mostrará que ela é positiva. Podemos também definir uma matriz de correlação

$$R = \begin{bmatrix} \frac{1}{\sqrt{C_{11}}} & & \\ & \ddots & \\ & & \frac{1}{\sqrt{C_{nn}}} \end{bmatrix} C \begin{bmatrix} \frac{1}{\sqrt{C_{11}}} & & \\ & \ddots & \\ & & \frac{1}{\sqrt{C_{nn}}} \end{bmatrix}$$

que é também simétrica e positiva. O valor de R_{ij} é a correlação entre x_i e x_j , e pertence ao intervalo $[0, 1]$.

5. Covariância e o Teorema Espectral

Já que a matriz de covariância é simétrica e positiva, podemos fatorá-la como

$$C = Q\Lambda Q^T$$

onde $Q \in O(n)$ é ortogonal e Λ é diagonal e positiva. Se consideramos agora a nova variável aleatória $\mathbf{y} = Q^T \mathbf{x}$, teremos:

$$\begin{aligned} E(\mathbf{y}) &= Q^T E(\mathbf{x}) \\ E((\mathbf{y} - Q^T \boldsymbol{\mu})(\mathbf{y} - Q^T \boldsymbol{\mu})^T) &= E(Q^T (\mathbf{x} - \boldsymbol{\mu})(\mathbf{x} - \boldsymbol{\mu})^T Q) \\ &= Q^T C Q \\ &= \Lambda \end{aligned}$$

Logo, a correlação linear entre y_i e y_j é zero, para $i \neq j$.

Um caso de particular interesse é quando conseguimos medir variáveis aleatórias $\mathbf{x} \in \mathbb{R}^m$, mas postulamos a existência de variáveis *ocultas* $\mathbf{y} \in \mathbb{R}^n$ com uma distribuição dada. Para simplificar as contas, vamos assumir que as variáveis $\mathbf{x}$ tenham média zero. Vamos postular a existência de variáveis $\mathbf{y}$ independentes e Gaussianas, com média zero e variância 1. O modelo é que as variáveis $\mathbf{x}$ são relacionadas com as variáveis $\mathbf{y}$ por meio de:

$$\mathbf{x} = A\mathbf{y}.$$

Dispomos de informações experimentais sobre as variáveis $\mathbf{x}$, mas não sabemos nada sobre A . Por isso, calculamos a matriz de covariância:

$$C = E(\mathbf{x}\mathbf{x}^T) = E(A\mathbf{y}\mathbf{y}^T A^T) = AE(\mathbf{y}\mathbf{y}^T)A^T = AA^T.$$

A solução A para essa equação não é única. Pelo Teorema Espectral, podemos escrever:

$$C = U\Lambda U^T$$

onde U é ortogonal e Λ diagonal (e positiva). Uma solução é portanto:

$$A = \sqrt{\Lambda}U^T.$$

Se os autovalores $\lambda_1 \geq \dots \geq \lambda_n$ decrescerem rapidamente, apenas os primeiros serão relevantes no modelo. Assim, em alguns casos, poderemos escolher $m \ll n$.

6. Alocação de ativos

Fundos de investimento ou de pensão costumam aplicar o dinheiro em uma *carteira de ativos*, que é uma combinação linear de ativos diferentes. O peso de cada ativo na carteira é uma escolha mais ou menos racional, que depende dos objetivos e da natureza do fundo.

Vamos assumir que um fundo investe em uma carteira de n ativos. O valor investido no i -ésimo ativo é proporcional a um peso a_i , onde convençionamos que $\sum a_i = 1$.

Denotamos por x_i a valorização (preço final sobre preço inicial) do i -ésimo ativo em um curto horizonte de tempo (digamos um mês). Então a valorização total da carteira é de $\sum a_i x_i$. Depois desse intervalo, a carteira é eventualmente rebalanceada, possivelmente com pesos diferentes. Mas vamos nos preocupar apenas com o que acontece ao longo de um período.

Ocorre que no início do mês, o valor de cada x_i é desconhecido. O gerente do fundo pode modelar as x_i como variáveis aleatórias, e estimar a esperança matemática $E(x_i)$ utilizando as séries históricas e (talvez) uma *análise qualitativa* ou *fundamentalista*. Se o i -ésimo ativo corresponde às ações de uma empresa, ele pode estimar a valorização futura examinando o balanço da empresa, considerar a conjuntura econômica e tentar prever o lucro da empresa.

Seria tentador achar o ativo com maior valorização esperada x_i e investir todo o dinheiro nesse ativo. Um investidor individual pode fazer isso. Nesse caso, a valorização esperada do fundo será de x_i .

No entanto, em um mês típico, a valorização pode ser muito maior ou muito menor do que x_i . Pode até ocorrer uma desvalorização. Essas oscilações podem ser medidas tomando o desvio padrão de x_i , conhecido no mercado financeiro como *volatilidade*.

Seres humanos não costumam gostar de alta volatilidade nos seus investimentos, principalmente em fundos geridos por outros. Eles estão dispostos a **pagar** por uma volatilidade menor, ou seja a aceitar um lucro esperado menor em troca de uma volatilidade menor.

Os bancos e fundos de investimento vendem o seus fundos como de *baixo risco*, deixando implícito que investimentos como ações são de *alto risco*. Eu estou convencido de que se trata do uso tendencioso da palavra *risco*, e que volatilidade não é risco. Exemplos de risco são o risco de perder o investimento devido a um calote da dívida pública, ou a uma falência fraudulenta de uma empresa, ou de perder todo o capital em investimentos alavancados (ou seja com dinheiro emprestado).

A receita para diminuir a volatilidade é diversificar. O gerente do fundo precisa então decidir como distribuir o dinheiro entre os n ativos disponíveis. Há muitas estratégias para isso, mas vou citar apenas três.

Fundos *ativos* alocam o dinheiro de acordo com decisões individuais do administrador, baseadas em uma análise conjuntural ou econômica. Em geral, apresentam um desempenho de longo prazo menor do que os índices da bolsa, e cobram uma alta taxa de administração.

Fundos *passivos* alocam o dinheiro de acordo com uma certa regra. Uma regra possível é a dos *fundos índice*, onde x_i é proporcional ao peso do i -ésimo ativo em um índice da bolsa (por exemplo, índice BOVESPA, ou IBRX-50). Esses pesos são proporcionais ao capital das empresas ou ao volume de ações negociadas.

Outra possibilidade é usar algum tipo de otimização. A Teoria Moderna de Carteiras ou (*modern portfolio theory*) foi desenvolvida por Harry Markowitz na década de 1950, e lhe valeu o Prêmio em homenagem a Nobel de Economia em 1990. O método de alocação de ativos busca um compromisso entre o retorno esperado

$$\mathbf{a}^T \mu = \sqrt{E(\mathbf{a}^T \mathbf{x})}$$

e a volatilidade

$$\sigma = \mathbf{a}^T (\mathbf{x} - E(\mathbf{x})) = \sqrt{E((\mathbf{a}^T \mathbf{x} - \mu)^2)}$$

Assume-se que a matriz de covariância $C = E(\mathbf{x}\mathbf{x}^T)$ é conhecida (pode ser estimada pela série histórica). Também a média $\mu = E(\mathbf{x})$ precisa ser conhecida de alguma maneira, talvez por uma análise detalhada dos ativos. Podemos escrever, em forma matricial:

$$\mathbf{a}^T (\mathbf{x} - E(\mathbf{x}))^2 = \mathbf{a}^T (\mathbf{x} - E(\mathbf{x})) (\mathbf{x} - E(\mathbf{x}))^T \mathbf{a}$$

Passando à esperança matemática da expressão acima,

$$\sigma^2 = \mathbf{a}^T E((\mathbf{x} - E(\mathbf{x})) (\mathbf{x} - E(\mathbf{x}))^T) \mathbf{a} = \mathbf{a}^T C \mathbf{a}$$

Para entender como diminuir a volatilidade, vamos supor que temos duas carteiras com pesos respectivos $\mathbf{a}_0$ e $\mathbf{a}_1$. Combinamos essas duas carteiras:

$$\mathbf{a}_t = (1 - t)\mathbf{a}_0 + t\mathbf{a}_1$$

onde, assumindo por um instante que não podemos nos alavancar, $t \in [0, 1]$. O retorno esperado e a volatilidade das carteiras é, respectivamente, μ_t e σ_t . Temos facilmente que

$$\mu_t = (1 - t)\mu_0 + t\mu_1.$$

O cálculo da volatilidade é mais complicado:

$$\sigma_t^2 = \mathbf{a}_t^T C \mathbf{a}_t = (1 - t)^2 \sigma_0^2 + t^2 \sigma_1^2 + 2t(1 - t) \mathbf{a}_0^T C \mathbf{a}_1$$

Mais uma vez, aplicamos o Teorema de Cauchy-Buniakovskii-Schwarz. Desta vez, o produto interno é definido por $\langle \mathbf{a}_0, \mathbf{a}_1 \rangle = \mathbf{a}_0^T C \mathbf{a}_1$. Temos que:

$$\langle \mathbf{a}_0, \mathbf{a}_1 \rangle \leq \|\mathbf{a}_0\| \|\mathbf{a}_1\| = \sigma_0 \sigma_1.$$

Logo,

$$\sigma_t^2 \leq (1 - t)^2 \sigma_0^2 + t^2 \sigma_1^2 + 2t(1 - t) \sigma_0 \sigma_1 = ((1 - t)\sigma_0 + t\sigma_1)^2$$

e a volatilidade satisfaz:

$$\sigma_t \leq (1 - t)\sigma_0 + t\sigma_1$$

Acabamos de mostrar o seguinte:

Lema 18.6. A volatilidade $\sigma(\mathbf{a})$ associada a uma alocação de ativos no espaço (afim) de todas as alocações $\mathbf{a} \in \Delta_n = \{\mathbf{a} \in \mathbb{R}^n: a_1, \dots, a_n \geq 0, \sum a_i = 1\}$ é uma função convexa.

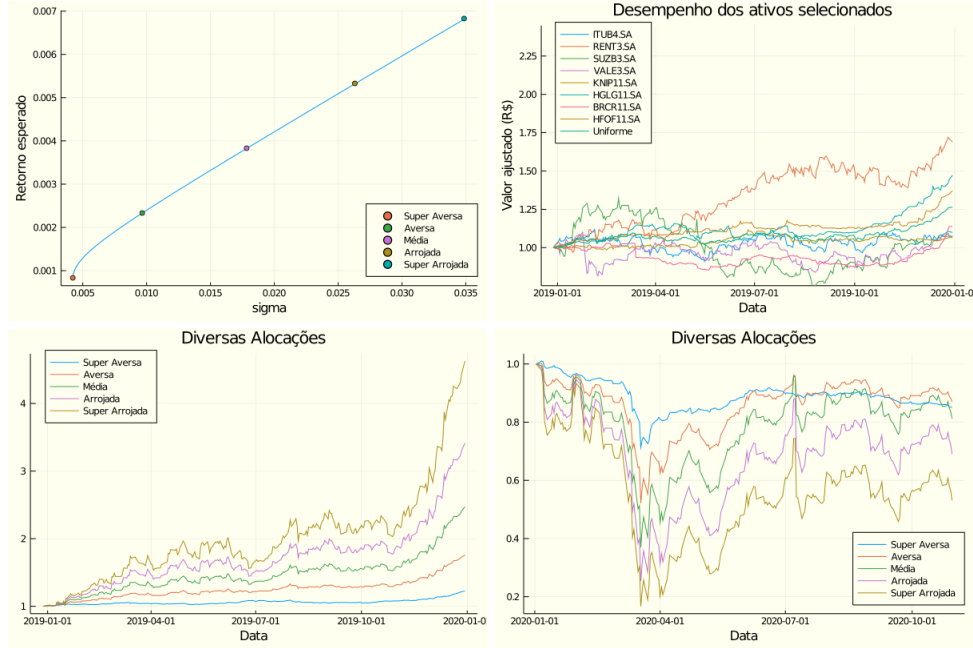


FIGURA 2. Modelo de alocação de ativos de Markowitz. Acima à esquerda, valores de σ e valor esperado para diversos valores de q . À direita, desempenho dos ativos selecionados em 2019. Embaixo, resultados da carteira em um cenário benigno (2019) e em um cenário adverso (2020). Em todos os casos, foram usados os dados de média esperada e covariância de 2019.

O mesmo é verdade para $\{\mathbf{a} \in \mathbb{R}^n : \sum a_i = 1\}$, se permitimos o alavancamento. Como $\sigma \geq 0$, a função σ sempre assume um mínimo em Δ_n (resp. $\mathbb{R}^n$). No caso alavancado ($\mathbb{R}^n$), a forma bilinear simétrica $\mathbf{a} \rightarrow \mathbf{a}^T \mathbf{C} \mathbf{a}$ restrita ao espaço $\sum a_i = 1$ se transforma em um polinômio do segundo grau, convexo. Assumindo $\mathbf{C}$ positiva definida, esse polinômio admite um único mínimo em $\mathbb{R}^n$. Esse é a alocação de menor "risco" (volatilidade) embora possa ser alavancada (alguns $a_i < 0$).

O modelo de Markowitz (Fig. 2) corresponde a minimizar $\sigma^2 - q\mu$, onde $q \geq 0$ é um parâmetro de risco, $q = 0$ sendo o menor risco possível. Nesse caso, é preciso resolver o problema de otimização

$$\begin{aligned} \min \quad & \mathbf{a}^T \mathbf{C} \mathbf{a} - q \mathbf{m}^T \mathbf{a} \\ \text{sujeito a: } & \sum a_i = 1. \end{aligned}$$

Pelo método do Multiplicador de Lagrange, a derivada da função objetivo precisa ser proporcional à derivada da restrição. Se $\mathbf{1}$ é o vetor com todas as coordenadas iguais a 1, resolvemos

$$\begin{bmatrix} 2\mathbf{C} & \mathbf{1} \\ \mathbf{1}^T & 0 \end{bmatrix} \begin{bmatrix} \mathbf{a} \\ \lambda \end{bmatrix} = \begin{bmatrix} \mu \\ 1 \end{bmatrix}.$$

onde λ é o multiplicador de Lagrange. A solução para alocações não alavancadas exige a introdução das restrições $a_i \geq 0$, e é um problema de Otimização.

7. Exercícios

Exercício 18.1. Mostre que a matriz de covariância é positiva. O que significa a matriz de covariância ter um ou mais autovalores nulos ?

Exercício 18.2. Considere que os dados x_i e y_i , $1 \leq i \leq N$, têm média zero e variância 1. Mostre que a correlação linear entre as variáveis y e x é o coeficiente da reta obtida aplicando o método dos mínimos quadrados para $y = t_1 x + t_0$. Calcule o erro de aproximação, em função da correlação.

Exercício 18.3. Agora não assuma hipóteses sobre os dados x_i e y_i , $1 \leq i \leq N$. Calcule o erro da aproximação de mínimos quadrados, em função da correlação e das variâncias.

Exercício 18.4. Sejam $\mathbf{z}_i \in \mathbb{R}^k$, com $1 \leq i \leq N$. Qual é o hiperplano que melhor se ajusta aos dados $\mathbf{z}_i$? Qual é o erro de aproximação ? (Responda em função da matriz de covariância)

Exercício 18.5. Agora sejam $\mathbf{w}_i = D\mathbf{z}_i$ onde os $\mathbf{z}_i$ são os dados do exercício anterior. Qual é a matriz de covariância de $\mathbf{w}$?

Exercício 18.6. Interprete a menor volatilidade possível de uma carteira (modelo de Markowitz) em termos do Teorema Espectral. Alocações podem ser negativas?

Exercício 18.7. Instale o pacote `MarketData` do Julia, e recupere as cotações do índice Dow Jones e (`yahoo("^DJT")`) do índice BOVESPA (`yahoo("^BVSP")`) para o ano passado. Converta os valores do índice BOVESPA para Dólares Americanos, e calcule a correlação entre o retorno diário dessas duas carteiras, ao longo do ano passado.

Exercício 18.8. Mesmo exercício, com o logaritmo do retorno diário.

Exercício 18.9. Com os dados do exercício anterior, resolva o problema de alocação de carteira para diversos valores de q , e simule o resultado.

Exercício 18.10. Suponha que o gerente do fundo tem a possibilidade de manter dinheiro em carteira, ou de tomar dinheiro emprestado. Assuma que a taxa de juros é de 1% ao ano. Assumimos portanto que $\mathbf{a} \in \mathbb{R}^n$ é uma alocação da carteira de ações, com $\sum_{i=1}^n a_i = 1$ e para $i \geq 1$, $a_i \geq 0$. O fundo investe t vezes seu valor na carteira de ações e $1 - t$ em dinheiro (podendo pegar emprestado). Quando $t > 1$, diz-se que o fundo está *alavancado*. Usando os dados do IBOVESPA em reais do exercício acima, calcule o ganho esperado e a volatilidade diária em função de t , μ_0 e do ganho esperado μ_a e da variância σ_a^2 da carteira de ações.

Aviso: fundos com $\sigma > 1$ podem, a qualquer momento, passar a ter um valor negativo. Para evitar ter prejuízo, os bancos e o mercado financeiro em geral exigem uma margem de segurança (garantias). Em geral, são as próprias ações da carteira. Em caso de desvalorização desta, ocorre uma *margin call*: o dono do fundo tem a opção de colocar mais garantias ou ter o fundo liquidado, e eventualmente falir. Para uma análise do lucro esperado desse tipo de fundo, é necessário levar em conta o risco de falência.

CAPÍTULO 19

Matrizes de Márkov e Processos Estocásticos

1. Introdução



Voltamos agora às probabilidades discretas. Assumimos que um sistema pode assumir n estados (numerados de 1 a n). Seja x_t o estado assumido no tempo t . Anteriormente, havíamos considerado variáveis aleatórias independentes ou correlacionadas. Neste capítulo, vamos estudar a situação onde x_{t+1} depende unicamente de x_t . Nesse sentido, o sistema *não tem memória*. Formalmente, usando *probabilidades condicionais*, com $(y_t)_{t \in \mathbb{N}}$ fixa e $(x_t)_{t \in \mathbb{N}}$ aleatória,

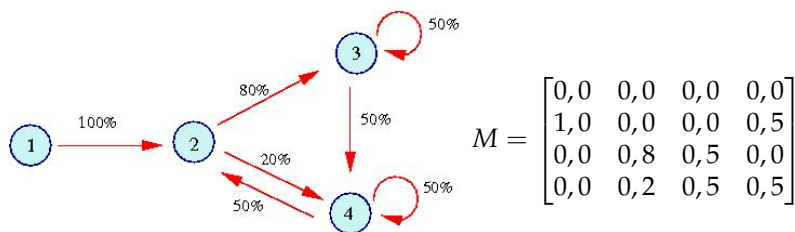
$$\text{Prob}[x_{t+1} = y_{t+1} | x_t = y_t] = \text{Prob}[x_{t+1} = y_{t+1} | x_t = y_t, x_{t-1} = y_{t-1}, \dots, x_1 = y_1]$$

(A primeira dessas probabilidades se lê como a *probabilidade de que o estado de x no tempo $t + 1$ seja y_{t+1} , dado que no tempo t o estado de x era y_t*).

Esse sistema pode ser modelado por um autômato finito (Figura 1), que é um grafo direcionado onde os vértices correspondem aos estados, e as arestas às transições possíveis. A cada aresta, associamos como *peso* a probabilidade da transição respectiva. Assim, os pesos são sempre positivos e a soma dos pesos de arestas saindo de um mesmo vértice é sempre 1. (Admitimos arestas de um estado para ele mesmo).

Exemplo 19.1. Companhias de seguros dividem os motoristas em categorias, por faixa etária, sexo, e antecedentes. A probabilidade de sinistro em motoristas com sinistros anteriores é aparentemente maior, por isso esses motoristas pagam um

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.



1233423333424423344233442333423444244442344234233...

FIGURA 1. Autômato Finito, matriz de transição e mensagem típica.

“prêmio” (valor da anuidade) maior. Quanto maior o período desde a última colisão, menor o prêmio.

A companhia estima a probabilidade de um motorista evoluir de um estado a outro com base nos dados históricos. O valor do prêmio é previsto para equilibrar o balanço da companhia, sem induzir os melhores motoristas a trocar de seguradora.

Exemplo 19.2. Dados transmitidos por um canal discreto costumam ter uma certa estrutura estatística. O mesmo acontece com o discurso humano, onde existe uma probabilidade de uma palavra (ou tipo de palavra) suceder a outra palavra.

Utilizando esse conhecimento, é possível melhorar algoritmos de compressão de dados. O modelo é um autômato probabilista, que serve como *fonte de informação*. A grandeza relevante vai ser o fator esperado de compressão do algoritmo para essa fonte de informação. A figura 1 mostra, além do autômato finito e da matriz de transição, uma mensagem típica.

Escrevemos então a matriz das probabilidades de transição do estado j para o estado i :

$$M_{ij} = \text{Prob}[x_{t+1} = i | x_t = j]$$

Em se tratando de probabilidades, teremos sempre que $M_{ij} \geq 0$ e para todo j , $\sum_i M_{ij} = 1$.

Definição 19.3. Uma *Matriz de Márkov* ou *Matriz Estocástica* é uma matriz quadrada M de tamanho $n \times n$, com $M_{ij} \geq 0$ e, para toda coluna j , $\sum_i M_{ij} = 1$. Ela é *positiva* se e somente se $M_{ij} > 0$ para todos i e j .

Observação 19.4. Em parte da literatura, matrizes de Márkov são definidas como matrizes com coordenadas não-negativas e onde a soma das coordenadas de cada linha é 1. Assim, estamos transpondo a definição, para poder trabalhar com um vetor coluna de probabilidades.

Seja $\mathbf{p}(t)$ o vetor das $p_i(t) = \text{Prob}[x_t = i]$. A partir da probabilidade inicial (que pode ser $\mathbf{e}_j$ se soubermos antecipadamente que $x_0 = j$), podemos calcular a probabilidade no tempo t pela recorrência

$$\mathbf{p}(t+1) = M\mathbf{p}(t)$$

ou ainda, $\mathbf{p}(t) = M^t \mathbf{p}(0)$.

Teorema 19.5 (Perron-Frobenius, caso Markoviano). *Seja M uma matriz de Márkov. Então,*

- (1) *Se λ é autovalor de M , então $|\lambda| \leq 1$*
- (2) *1 é autovalor de M .*
- (3) *Se M for positiva, todo autovalor λ de M diferente de 1 verifica $|\lambda| < 1$.*
- (4) *Existe um autovetor à direita, associado ao autovalor 1, cujas coordenadas são todas não-negativas. Se M for positiva, as coordenadas são positivas.*
- (5) *Se M for positiva, então o autoespaço com autovalor associado 1 tem dimensão 1.*

O autovetor $\mathbf{p}$ associado ao autovalor 1, e tal que $\sum p_i = 1$ e $p_i \geq 0$, é chamado de *estado estacionário*. É o estado limite para quase qualquer valor inicial. Um exemplo de matriz de Márkov onde o estado estacionário não é único é dada pela identidade 2×2 .

Os seguintes Lemas vão ser úteis para a prova do Teorema (que adiamos até o final deste Capítulo).

Lema 19.6. Se $z_1, z_2 \in \mathbb{C}$, então $|z_1 + z_2| \leq |z_1| + |z_2|$. Vale a igualdade se e somente se z_1 e z_2 pertencem a uma mesma semirreta $L_\theta = \{te^{i\theta} : t \in \mathbb{R}, t \geq 0\}$, $\theta \in [0, 2\pi)$.

DEMONSTRAÇÃO. Se $z_1 = z_2 = 0$, o resultado é trivial. Por isso vamos assumir sem perda de generalidade que $z_1 \neq 0$, e $z_1 \in L_\theta$. Logo, $x_1 = e^{-i\theta}z_1 \in \mathbb{R}$ e $x_1 > 0$. Sejam x_2 e y_2 as partes reais (resp. imaginária) de $e^{-i\theta}z_2$. Então $z_2 \in L_\theta$ se e somente se $y_2 = 0$ e $x_2 \geq 0$.

Agora calculamos

$$|z_1 + z_2| = |e^{-i\theta}z_1 + e^{-i\theta}z_2| = |x_1 + x_2 + iy_2| = \left\| \begin{bmatrix} x_1 + x_2 \\ y_2 \end{bmatrix} \right\|$$

e

$$|z_1| + |z_2| = |e^{-i\theta}z_1| + |e^{-i\theta}z_2| = |x_1| + |x_2 + iy_2| = \left\| \begin{bmatrix} x_1 \\ 0 \end{bmatrix} \right\| + \left\| \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \right\|$$

Então a desigualdade triangular implica que $|z_1 + z_2| \leq |z_1| + |z_2|$. Se $z_1, z_2 \in L_\theta$, $|z_1 + z_2| = x_1 + x_2 = |z_1| + |z_2|$. Senão, podem ocorrer dois casos: $y_2 \neq 0$ ou os sinais de x_1 e x_2 são diferentes. Em ambos os casos, a desigualdade triangular é estrita. $\square$

Lema 19.7. Sejam $z_1, \dots, z_m \in \mathbb{C}$. Então $|\sum_{j=1}^m z_j| \leq \sum_{j=1}^m |z_j|$. Vale a igualdade se e somente se os z_i pertencem todos a uma mesma semirreta $L_\theta = \{te^{i\theta} : t \in \mathbb{R}, t \geq 0\}$, $\theta \in [0, 2\pi)$.

DEMONSTRAÇÃO. Utilizamos o Lema anterior (que já nos fornece o caso $m = 2$).

Hipótese de indução: Este Lema vale para um certo valor de m .

Assumindo a hipótese de indução,

$$\left| \sum_{j=1}^{m+1} z_j \right| \left| \left(\sum_{j=1}^m z_j \right) + z_{m+1} \right| \leq \left| \sum_{j=1}^m z_j \right| + |z_{m+1}| \leq \left| \sum_{j=1}^m |z_j| + |z_{m+1}| \right|$$

onde a primeira desigualdade vem do Lema anterior e a segunda desigualdade da hipótese de indução.

Caso os z_j pertençam todos a uma mesma semirreta L_θ , então (ainda pela hipótese de indução) a segunda desigualdade é uma igualdade. Além disso, $\sum_{j=1}^m z_j \in L_\theta$ logo a primeira desigualdade também é uma igualdade.

Caso os z_j não pertençam todos a uma mesma semirreta, assumimos (após reordenar os z_j que z_{m+1} e $\sum_{j=1}^m z_j$ não pertencem à mesma semirreta. Pelo Lema anterior, a primeira desigualdade é estrita. Assim, este lema vale para $m + 1$. $\square$

Lema 19.8. Seja M uma matriz de Márkov e $x \in \mathbb{C}^n$. Se $y = Mx$, então $\sum_i |y_i| \leq \sum_j |x_j|$. Se a matriz M for positiva e duas coordenadas $x_i \neq 0$ e $x_j \neq 0$ de x forem tais que $\frac{x_i}{x_j} \notin \mathbb{R}^+$, então a desigualdade é estrita.

DEMONSTRAÇÃO. Aplicamos o Lema anterior aos números $y_i = M_{ij}x_j$. Teremos sempre que

$$\sum_i |y_i| = \sum_i \left| \sum_j M_{ij}x_j \right| \leq \sum_{ij} M_{ij} |x_j| = \sum_j |x_j|$$

Se ocorrer que $\frac{x_j}{x_k} \notin \mathbb{R}^+$, então y_j e y_k não pertencem à mesma semirreta. Nesse caso, a desigualdade é estrita. $\square$

2. O raio espectral

Definição 19.9. O *raio espectral* de uma matriz A de tamanho $n \times n$ é $\rho(A) = \max |\lambda|$, onde o máximo é tomado entre os autovalores de A .

Proposição 19.10. Se $\rho(A) < 1$, então $\lim_{k \rightarrow \infty} A^k = 0$. Além disso,

$$\lim_{l \rightarrow \infty} \sum_{k \geq l} |(A^k)_{ij}| = 0.$$

Para definir o limite, estamos assimilando matrizes a vetores em $\mathbb{R}^{n^2}$. Note que esse Lema é trivial para matrizes diagonalizáveis. Mas se A é uma matriz qualquer, não podemos assumir que ela seja similar a uma matriz diagonal. Por exemplo, $J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ não é diagonalizável nem sobre os complexos. Mas $J^2 = 0$. Matrizes J tais que $J^k = 0$ para algum k são chamadas de *nilpotentes*. A prova da Proposição 19.10 está adiada para o Capítulo 22 (Página 149).

3. Prova do Teorema de Perron-Frobenius

DEMONSTRAÇÃO.

- (1) Seja $u \neq 0$ um autovetor qualquer de M , com autovalor associado λ :

$$Mu = \lambda u.$$

Pelo Lema 19.8, $|\lambda| \sum |u_i| \leq \sum |u_i|$, o que implica que $|\lambda| \leq 1$.

- (2) Vamos agora verificar que existe um autovalor igual a 1:

$$\begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix} M = \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}.$$

- (3) Se x é um autovetor associado a λ , então

$$Mx = \lambda x.$$

Somando as coordenadas dos dois lados, obtemos que

$$\sum_j x_j = \sum_{ij} M_{ij} x_j = \lambda \sum_j x_j.$$

Assumimos que λ é um autovalor diferente de 1. Logo, $\sum x_j = 0$, e x_n é dependente de $x_1, \dots, x_{n-1}$. Seja W o espaço (complexo) dos vetores x tais que $\sum x_j = 0$. Se $x \neq 0 \in W$, então as suas coordenadas x_j não podem pertencer a uma mesma semirreta em $L_\theta \subset \mathbb{C}$. Como a matriz M é positiva, o mesmo vale para os $M_{ij}x_j$.

Comparando os valores absolutos das coordenadas, temos:

$$|\lambda| \sum |x_j| = \sum_i \left| \sum_j M_{ij} x_j \right|$$

Aplicando o Lema 19.8,

$$|\lambda| \sum |x_j| < \sum_i \sum_j M_{ij} |x_j|$$

e $|\lambda| < 1$.

- (4) seja $p \in \mathbb{R}^n$, com $\sum_i p_i = 1$ e $p_i > 0$. Consideramos a sequência $(p(k))_{k \in \mathbb{N}}$ definida por $p(k) = M^k p$. Vamos mostrar que essa sequência é convergente. Para isso, vamos comparar $q(k) = p(k) - p(k-1)$ com $q(k-1) = p(k-1) - p(k-2)$. Note que $q(k), q(k-1) \in W$. Além disso, $q(k) = Mq(k-1)$. Pela Proposição 19.10 aplicada a $M|_W$, a sequência

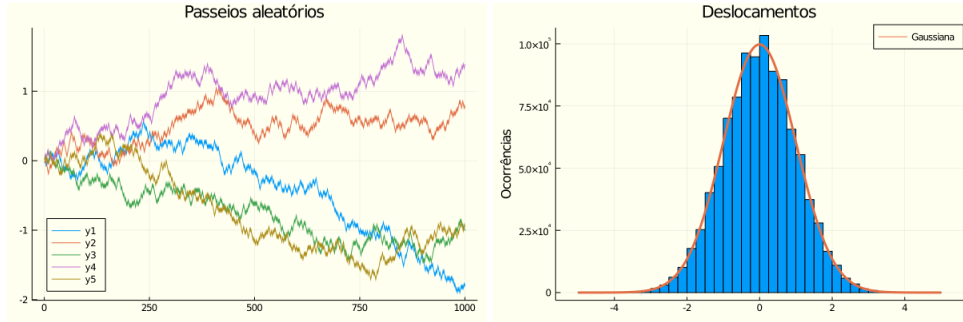


FIGURA 2. Esquerda: passeios aleatórios. Direita: histograma do deslocamento total para $n = 10^6$ passeios, $t = 10^4$. A curva Gaussiana foi multiplicada por n vezes a base dos retângulos, para ter a mesma área.

$(q(k))$ converge para o vetor zero. Além disso, $\sum_{k>1} \|q(k)\|$ também converge para zero. Logo $p(k)$ é convergente. Seja p^* o limite: nesse caso, $Mp^* = p^*$.

- (5) Assumimos a hipótese suplementar de que M é positiva. Sejam p e p' dois autovetores associados ao autovalor 1, tais que $\sum p_i = \sum p'_i = 1$. e seja $q = p - p'$. Então

$$Mq = q.$$

Mas a soma $\sum q_i$ das coordenadas de q é zero, e além disso existem coordenadas com sinais opostos. Pelo Lema 19.8, $\sum q_i < \sum q_i$, o que é uma contradição.

□

4. Processos Estocásticos

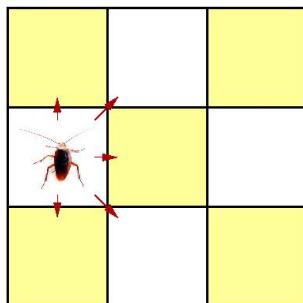
Processos aleatórios “sem memória” são estudados em diversos contextos. Por exemplo, partículas de poeira em suspensão no ar parecem se mover totalmente ao acaso. Um modelo para o movimento da poeira o movimento de uma partícula de poeira, também conhecido como *movimento Browniano*, é por meio da discretização do espaço e do tempo. Variáveis termodinâmicas como a temperatura são explicadas em termos de movimento Browniano.

Vamos supor agora que queremos estudar o movimento de n partículas em uma dimensão. O programa abaixo assume que a cada instante, a partícula pode se deslocar para a esquerda ou para a direita. Note a mudança de escala para $1/\sqrt{t}$, que garante que o desvio-padrão do comprimento é igual a 1.

```
[1]: using LinearAlgebra
      using Plots
```

```
[2]: function passeio(n,t)
      x=rand(-1:2:1,t,n)
      for j=1:(t-1)
          x[j+1,:]=x[j+1,:]+x[j,:]
      end
      return x/sqrt(t)
  end
```

```
[2]: passeio (generic function with 1 method)
```

FIGURA 3. Possíveis deslocamentos da *periplaneta americana*

Passeios aleatórios estão representados na figura 2. O histograma na mesma figura ilustra a convergência da densidade de probabilidade da posição no tempo final para a curva normal de Gauss.

Este é um exemplo de processo Markoviano. A densidade de probabilidade da posição da partícula no tempo t depende linearmente da densidade de probabilidade no tempo $t - 1$, por um operador linear que podemos interpretar como uma matriz de Márkov infinita.

O gráfico da Figura 2(esq) lembra os gráficos do valor de ativos nos mercados financeiros. O modelo de Black-Scholes para precificação de derivativos (que não irei explicar) assume que o logaritmo do valor de um ativo é um processo estocástico, similar a um passeio aleatório. Conhecendo o seu valor no tempo zero, o seu valor no tempo t é uma variável aleatória Gaussiana. O retorno esperado é aproximadamente a média dessa variável, e o desvio-padrão é a chamado de *volatilidade*.

5. Exercícios

Exercício 19.1. Mostre que existe uma matriz de Márkov M não positiva, com M^2 positiva.

Exercício 19.2. Seja M uma matriz duplamente estocástica ($M = M^T$). O que você pode dizer do estado estacionário?

Exercício 19.3. Dê um exemplo de processo Markoviano onde $p(t+1)$ depende de $p(t)$ mas $p(t)$ é independente de $p(t+1)$.

Exercício 19.4. Seja $k \in \mathbb{N}$. Dê um exemplo de matriz A (não necessariamente de Márkov) com raio espectral zero, mas tal que $A^k \neq 0$.

Exercício 19.5. Seja A uma matriz com raio espectral $\rho < 1$. Mostre que para todo $\mathbf{x}$, $\lim_{k \rightarrow \infty} A^k \mathbf{x} = \mathbf{0}$.

Exercício 19.6. Seja A uma matriz com raio espectral $\rho > 1$. Mostre que existe $\mathbf{x}$ tal que $\lim_{k \rightarrow \infty} A^k \mathbf{x} = \infty$. Isso vale para todo $\mathbf{x}$?

Exercício 19.7. Agora seja A uma matriz com raio espectral exatamente igual a 1. O que você pode afirmar sobre $\lim_{k \rightarrow \infty} A^k \mathbf{x}$, em função de $\mathbf{x}$?

Exercício 19.8. Insetos da ordem *blattodea*, quando submetidos a altas temperaturas, se deslocam de maneira aleatória. Considere o seguinte modelo: uma (*periplaneta americana*) se desloca em um tabuleiro 3×3 de maneira aleatória (Figura 3), e de acordo com a seguinte regra: a probabilidade do inseto se deslocar, a cada passo, para uma das casas vizinhas (inclusive na diagonal), é idêntica.

- (1) Represente por graficamente as posições possíveis do inseto e as possíveis transições.
- (2) Construa a matriz de Márkov correspondente.
- (3) Ache o estado estacionário. Mostre que depois de um tempo suficientemente grande, a probabilidade do inseto se encontrar na casa do meio é de $1/5$.

Exercício 19.9. Mostre que se x e y são variáveis aleatórias Gaussianas com média zero e desvio padrão σ , então $x + y$ é uma variável aleatória Gaussiana com desvio padrão $\sigma\sqrt{2}$. Explique o fator de escala de $\sqrt{t}$ no espaço, no programa *passeio.m*.

Exercício 19.10. Modifique o programa do passeio aleatório para uma partícula confinada ao intervalo $[-1, 1]$. Calcule o estado estacionário. Você vai precisar mudar o fator de escala !

CAPÍTULO 20

Grafos e Álgebra Linear

1. Introdução à teoria dos grafos



talvez uma das aplicações mais importantes e menos entendidas da Álgebra Linear sejam os algoritmos de busca na internet. Os conceitos fundamentais são o Teorema Espectral (Teorema 16.1) e a decomposição em valores singulares (ou *svd*, Teorema 17.1). Um curso de Álgebra Linear hoje não estaria completo sem um capítulo sobre redes de computadores e grafos. Lembremos que:

Definição (Definição 8.8). Um *grafo* simples é um par $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ onde $\mathcal{V}$ é um conjunto finito (seus elementos são chamados de *vértices* e $\mathcal{E}$ é um conjunto de pares não ordenados de vértices diferentes (chamados de *arestas*)).

Um *caminho* é uma lista finita de vértices, tais que cada dois vértices consecutivos formam uma aresta. Também podemos representar um caminho pela lista de arestas correspondentes. Um *ciclo* é um caminho onde o último vértice é idêntico ao primeiro vértice.

Exemplo 20.1. A internet (Fig. 1) pode ser modelada por um conjunto (gigantesco mas finito) de computadores (vértices), cada um conectado a um número pequeno de outros computadores. Cada ligação é uma aresta. Um modelo mais realista associaria também a cada aresta, a sua velocidade ou largura de banda.

Exemplo 20.2. A malha rodoviária nacional também pode ser descrita como um conjunto de vértices (localidades), e as arestas correspondem às estradas diretas entre essas localidades.

Exemplo 20.3. Matemáticos costumam escrever artigos em parceria. O *grafo de colaboração* é o grafo cujos vértices correspondem a cada Matemático com artigos publicados, e as arestas à existência de uma colaboração publicada entre eles. A *distância de colaboração* entre dois Matemáticos é a distância entre eles no grafo, e pode ser calculada¹. O *número de Erdős* de um Matemático é a distância de colaboração entre ele e Paul Erdős (1913-1996), que foi aparentemente o mais colaborativo e prolífico dentre os grandes matemáticos do século passado. O *grau* de um vértice é o número de arestas contendo esse vértice. No grafo de colaboração, Paul Erdős tem grau 507.

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.

¹Ver em: amsimpa.br

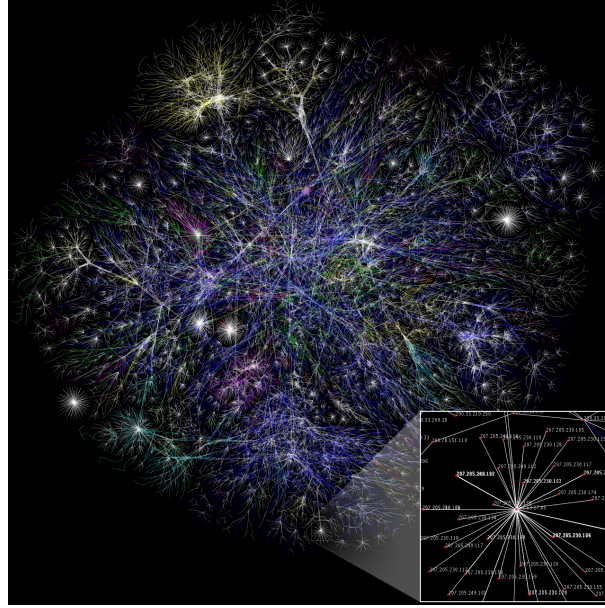


FIGURA 1. Mapa parcial da internet. Imagem publicada por Matt Britt, <http://wikimidia.org>, sob o título *Internet map 1024.jpg*. Copyright © Creative Commons Attribution 2.5 License.

Propriedades métricas e de conexidade de grafos são extremamente importantes. Em uma rede de comunicações, é importante que existam múltiplos caminhos entre dois pontos mas também é crucial que a distância entre dois pontos quaisquer seja pequena.

Isso é uma característica importante de redes de comunicações ou de redes sociais, conhecida como propriedade do “mundo pequeno”.

A internet tem essa propriedade (você podem listar o caminho entre o seu computador e outro computador qualquer usando o comando `tracert`). Uma distância de 30 é incomum. Entre Matemáticos, a distância de colaboração costuma ser bem menor (4 é razoável).

Uma maneira de estudar grafos é introduzir a matriz de adjacência.

Definição 20.4. A *matriz de Adjacência* A_G associada a um grafo simples $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ é a matriz de tamanho $\#\mathcal{V} \times \#\mathcal{V}$ definida por

$$(A_G)_{a,b} = \begin{cases} 1 & \text{Se } \{a,b\} \in \mathcal{E} \\ 0 & \text{Em todos os outros casos} \end{cases}$$

2. A Equação do Calor em grafos

Para se estudar as propriedades de conexidade de grafos do mundo real (em geral com milhares ou milhões de vértices, talvez bilhões) é necessário recorrer a invariantes ‘estatísticos’. Por exemplo, é possível estudar caminhos aleatórios em grafos. Como veremos a seguir, isso está relacionado com a equação do calor.

Seja $\mathcal{G}$ um grafo simples. A *matriz Laplaciana* associada a $\mathcal{G}$ é definida por:

$$\Delta_G = A_G - D_G$$

onde a matriz D_G é diagonal, e $(D_G)_{vv} = \sum_w A_{vw}$ é o *grau* do vértice v (número de arestas incidentes).

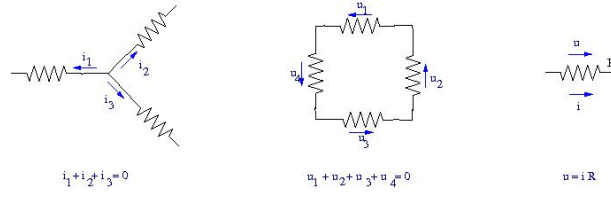


FIGURA 2. Leis de Kirchhoff e de Ohm.

Observação 20.5. Este autor considera que a convenção de sinal para a matriz Laplaciana utilizada por toda a comunidade de grafos está errada, e que a convenção correta é a mostrada acima, que é compatível com a física e as equações do calor e da onda.

A transmissão do calor entre dois compartimentos é proporcional à diferença de temperatura. A equação diferencial do calor em uma barra de metal pode ser obtida discretizando o espaço e o tempo e passando ao limite: $\frac{\partial u(x,t)}{\partial t} = \frac{\partial^2 u(x,t)}{\partial x^2}$. Em uma placa ou barra de metal, a equação é $\frac{\partial u(\mathbf{x},t)}{\partial t} = \Delta_{\mathbf{x}} u(\mathbf{x},t)$.

A equação do calor em grafos é

$$\dot{\mathbf{u}}(t) = \Delta_{\mathcal{H}} \mathbf{u}(t)$$

Essa equação modela um processo de difusão em grafos. Se $\mathcal{H}$ for conexo, $\lim_{t \rightarrow \infty} \mathbf{u}(t)$ existe, e é constante entre vértices conectados por caminhos. Quanto mais rápida (em geral) a convergência, mais bem-conexo é o grafo.

Podemos também considerar o análogo discreto:

$$\mathbf{u}(t+1) = I + \epsilon \Delta_{\mathcal{H}} \mathbf{u}(t)$$

Note que para $\epsilon < 1/(\max(D_{\mathcal{G}})_{vv})$, a matriz $I + \epsilon \Delta_{\mathcal{H}}$ é uma matriz de Márkov! De fato é uma matriz duplamente estocástica, e a distribuição estacionária é $\mathbf{u}_v^* = 1$.

A matriz $\Delta_{\mathcal{H}}$ é simétrica, e pode portanto ser diagonalizada. Seus autovalores são portanto números reais. Como $I + \epsilon \Delta_{\mathcal{H}}$ é estocástica, os autovalores de $\Delta_{\mathcal{H}}$ são menores ou iguais a zero. Sendo $\mathcal{H}$ conexo, o autovalor zero terá multiplicidade 1.

Definição 20.6. O *espectro* de um grafo $\mathcal{H}$ é a lista $0 = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{\#\mathcal{V}}$ dos autovalores de $\Delta_{\mathcal{H}}$.

Pelo Teorema Espectral, a matriz $\Delta_{\mathcal{H}}$ admite uma base ortonormal de autovetores. Isso permite estimar a velocidade de convergência de $u(t)$ por:

$$\|u(t) - u^*\| \leq e^{\lambda_2 t} \|u(0)\|.$$

Quanto mais negativo for λ_2 , mais robusta e eficiente é uma rede de comunicações.

3. As Leis de Kirchhoff

As Leis de Kirchhoff (Fig.2) permitem ‘resolver’ circuitos elétricos com resistências conectadas de maneira arbitrária. Para isso, precisamos representar circuitos elétricos de alguma maneira. Poderíamos utilizar um grafo, mas precisamos ainda de mais informação:

- (1) Precisamos convencionar uma orientação para cada aresta.

(2) Além disso, precisamos conhecer cada uma das resistências.

Um grafo simples onde se especifica uma orientação para cada aresta é chamado de *grafo orientado*. Agora, o conjunto de arestas é um subconjunto $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$, onde, se $(v, w) \in \mathcal{E}$, $(w, v) \notin \mathcal{E}$. Em particular, não existe aresta da forma (v, v) .

Definição 20.7. A *matriz de Incidência* I_G associada a $\mathcal{G}$ é a matriz de tamanho $\#\mathcal{E} \times \#\mathcal{V}$, onde

$$(I_G)_{(a,b),c} = \begin{cases} 1 & \text{Se } b = c \\ -1 & \text{Se } c = a \\ 0 & \text{Em todos os outros casos} \end{cases}$$

Seja $\mathcal{G}$ portanto o grafo orientado de uma malha elétrica, onde a cada aresta (a, b) associamos uma resistência $R_{(a,b)}$. Seja $\mathbf{R} \in \mathbb{R}^{\#\mathcal{E}} \times \mathbb{R} \in \mathbb{R}^{\#\mathcal{E}}$ a matriz diagonal das resistências, $\mathbf{i} \in \mathbb{R}^{\#\mathcal{E}}$ o vetor da corrente em cada aresta e $\mathbf{q} \in \mathbb{R}^{\#\mathcal{V}}$ o vetor de potencial elétrico.

Assumimos que o circuito está em equilíbrio.

Lei de Kirchhoff para a corrente: A corrente elétrica entrando em um vértice é igual à corrente saindo.

Do ponto de vista matricial,

$$I_G^T \mathbf{i} = \mathbf{0}$$

Lei de Kirchhoff para a voltagem A soma de diferenças de potencial entre arestas correspondendo a um ciclo fechado é zero.

O vetor das diferenças de potencial é $\mathbf{u} = I_G \mathbf{q} \in \mathbb{R}^{\#\mathcal{E}}$.

Os caminhos fechados pertencem todos ao núcleo de I_G^T . O que a Segunda Lei afirma é que $\mathbf{u}$ é ortogonal ao núcleo de I_G^T . Isso segue do Teorema do Posto.

Agora aplicamos a **Lei de Ohm:** $u = iR$.

No nosso caso, temos a igualdade matricial $\mathbf{u} = \mathbf{R}\mathbf{i}$. Podemos resolver o circuito:

$$I_G^T \mathbf{R}^{-1} I_G \mathbf{q} = \mathbf{0}.$$

A dimensão do espaço das soluções é $\dim \ker I_G$, que é o número de componentes conexos do grafo. Isso é razoável se o nosso circuito está no equilíbrio.

Agora suponhamos que prescrevemos entrada ou saída de corrente em alguns dos vértices. Teremos agora:

$$I_G^T \mathbf{R}^{-1} I_G \mathbf{q} = \mathbf{j},$$

onde $\mathbf{j}$ corresponde ao intercâmbio de corrente. A matriz $I_G^T \mathbf{R}^{-1} I_G$ é simétrica e pode ser assimilada a um Laplaciano. A Lei de Ohm diz que a derivada da carga em um vértice é igual à soma das diferenças de potencial, ponderadas pela conductância (inversa da resistência). Nesse sentido, a equação acima corresponde também a um processo de difusão. A maneira correta de se definir a matriz de adjacência para um circuito de resistências é como a matriz das conductâncias:

$$(A_G)_{a,b} = \begin{cases} R_{a,b}^{-1} & \text{Se } (a,b) \text{ ou } (b,a) \in \mathcal{E} \\ 0 & \text{Em todos os outros casos} \end{cases}$$

Nesse caso, definimos o grau de a como a soma das conductâncias das arestas incidindo em a . Recuperamos portanto que:

$$I_G^T R^{-1} I_G = A_G - D_G = \Delta_G .$$

4. Ranqueamento de Page

Definição 20.8. Um *digrafo simples* ou *directed simple graph* $\mathcal{G}$ é um par $(\mathcal{V}, \mathcal{E})$ onde $\mathcal{V}$ é um conjunto finito (seus elementos são chamados de *vértices*) e $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. Os elementos de $\mathcal{E}$ são chamados de *arestas*. Arestas de um vértice nele mesmo são permitidas.

Exemplo 20.9. A *world wide web* é modelada por um conjunto de *páginas* (associadas a um endereço *http* ou *uniform resource locator*) (vértices) e um conjunto de ligações orientadas (*links*) entre os vértices.

Exemplo 20.10. O cérebro humano é composto de mais de 100 bilhões de neurônios. Cada neurônio é uma célula com dois prolongamentos (áxil e dendrítico). Cada um desses prolongamentos se ramifica em possivelmente milhares ou dezenas de milhares de extremidades. Potencial elétrico no centro da célula (soma) é transmitido ao prolongamento áxil. Isso afeta o terminal dendrítico de outros neurônios em contato (sinapse), transmitindo assim a informação. A transmissão é unidirecional. Neurônios podem ser ativadores ou inibidores. De qualquer maneira, podemos modelar o fluxo de informação por um digrafo, onde os neurônios são os vértices e as sinapses são as arestas. Um neurônio pode ter mil ou dez mil arestas.

O invariante natural de um digrafo é a matriz de transferência, versão orientada da matriz de adjacência:

$$(T_{\mathcal{G}})_{a,b} = \begin{cases} 1 & \text{Se } (b, a) \in \mathcal{E} \\ 0 & \text{Em todos os outros casos} \end{cases}$$

Essa matriz não é simétrica.

O problema de procura na internet pode ser interpretado como o problema de atribuir um “índice de relevância” para cada página. O sistema de busca precisa mostrar, ordenadas por relevância, as páginas que contêm um certo termo (ou as páginas referidas utilizando esse termo²).

Voltemos ao modelo de grafo orientado para a internet. Vamos supor que um *programa rastreador* (que vamos chamar de *bot*) percorre um grafo orientado $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ escolhendo, a cada vértice, uma aresta aleatória. Para fixar as idéias, vamos considerar apenas o domínio da Figura 3. O *bot* se desloca de maneira aleatória, escolhendo arestas ao acaso.

Quatro domínios disputam a atenção do *bot*, e todos têm uma *bot trap*: uma vez que o bot entrou em uma página, ele não consegue mais sair do subdomínio. Se o bot chega em um vértice sem saída, ele pula para um vértice aleatório. Ainda, poderia ficar preso em um ciclo. Uma solução possível é a seguinte: a cada passo, o bot tem uma probabilidade δ de pular para uma página escolhida de maneira totalmente aleatória.

Larry Page, Sergey Brin e coautores³⁴, então estudantes em Stanford, modelaram a relevância de uma página como o tempo médio que um desses bots ficaria

²Pesquise por exemplo o termo *google bombing*

³Lawrence Page, Sergey Brin, Rajeev Motwani e Terry Winograd, *The PageRank citation ranking: Bringing order to the Web*, Preprint, 1999. <http://dbpubs.stanford.edu:8090/pub/1999-66>

⁴Sergey Brin and Lawrence Page, *The anatomy of a Large-Scale Hypertextual Web Search Engine*, *Computer Networks* 30 pp 107-117, e versão expandida (1998)

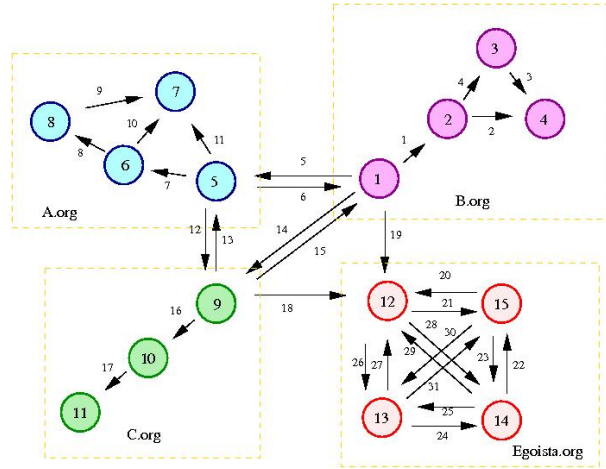


FIGURA 3. Domínio fictício de web.

nessa página. Obviamente é impossível simular isso com um trilhão de bots. Mas o algoritmo que ele desenvolveu, em conjunto com Serguei Brin, permite estimar esse tempo de maneira conveniente.

Para isso, ele modelou o passeio aleatório do bot por um processo de Márkov. Dado um vetor de probabilidade $\mathbf{p}_t$ (que mede a probabilidade do bot se encontrar em cada página, no tempo t), pode-se escrever o vetor $\mathbf{p}_{t+1}$ como $\mathbf{p}_{t+1} = M\mathbf{p}_t$, onde:

$$M = \frac{\delta}{N} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} [1 \quad \dots \quad 1] + (1 - \delta)TD^{-1},$$

N é o número de vértices e D é a matriz diagonal contendo o número de arestas saindo de cada vértice. A Matriz M é uma matriz de Márkov, e portanto $(\mathbf{p}_t)$ converge para um estado estacionário $\mathbf{p}^*$. O índice de relevância da página v é p_v^* .

Os algoritmos que Page e Brin utilizaram se mostraram muito mais eficientes do que os disponíveis para a concorrência (que funcionava como as páginas amarelas, cobrando dos anunciantes). *Google*, o sistema de busca deles, ganhou imediatamente o favor dos usuários da internet. Vamos digitar a matriz de transferência do domínio fictício da Fig. 3:

```
[10]: T = zeros( 15, 15) ;

T[ 1, 2] = 1 ; T[ 2, 4] = 1 ; T[ 3, 4] = 1 ; T[ 2, 3] = 1 ; T[ 1, 5] = 1 ;
T[ 5, 1] = 1 ; T[ 5, 6] = 1 ; T[ 6, 8] = 1 ; T[ 8, 7] = 1 ; T[ 6, 7] = 1 ;
T[ 5, 7] = 1 ; T[ 5, 9] = 1 ; T[ 9, 5] = 1 ; T[ 1, 9] = 1 ; T[ 9, 1] = 1 ;
T[ 9,10] = 1 ; T[10,11] = 1 ; T[ 9,12] = 1 ; T[ 1,12] = 1 ; T[15,12] = 1 ;
T[12,15] = 1 ; T[14,15] = 1 ; T[15,14] = 1 ; T[13,14] = 1 ; T[14,13] = 1 ;
T[12,13] = 1 ; T[13,12] = 1 ; T[12,14] = 1 ; T[14,12] = 1 ; T[15,13] = 1 ;
T[13,15] = 1 ;
T = T'
```

Agora produzimos a matriz M , e iteramos.

```
[11]: delta = 0.15
```

```
[11]: 0.15
```

```
[12]: D=ones(15) '*T
```

Obtemos:

```
[12]: 1×15 Adjoint{Float64,Array{Float64,1}}:
      4.0  2.0  1.0  0.0  4.0  2.0  0.0  1.0  4.0  1.0  0.0  3.0  3.0  3.0  3.0
```

```
[13]: for j=1:15
      if (D[j] == 0) T[:,j] = ones(15,1) ;
      end ;
    end ;
```

```
[14]: D=ones(15) '*T
```

```
[14]: 1×15 Adjoint{Float64,Array{Float64,1}}:
      4.0  2.0  1.0 15.0  4.0  2.0 15.0  1.0  4.0  1.0 15.0  3.0  3.0  3.0  3.0
```

```
[15]: diagm(0=>D')
```

```
[16]: R=ones(15,1)*ones(1,15)/15
      M = delta * R + (1-delta) * T * diagm(0=>((D') .^(-1)))
```

```
[17]: p = ones(15,1)/15 ;
      for k=1:100
        p = M * p ;
      end ;
      p
```

```
[17]: 15×1 Array{Float64,2}:
      0.033144124116458895
      0.026100997741711374
      0.030150795407191195
      0.055778971503303736
      0.033144124116458895
      0.026100997741711374
      0.06282209787805126
      0.030150795407191195
      0.033144124116458895
      0.026100997741711374
      0.041243719447418545
      0.1587617893284052
      0.14778548848464282
      0.14778548848464282
      0.14778548848464282
```

```
[18]: eps=norm(p-M*p)
```

```
[18]: 1.8312633660029008e-16
```

Note que *Egoísta.org* foi quem apresentou os melhores índices de relevância ! O domínio *Egoísta.org* montou uma *fazenda de links*, que aumenta o número de arestas apontando para cada uma das suas páginas.

Os engenhos de busca na internet precisam se atualizar constantemente para combater *Web spam*, práticas desonestas para obter (e vender) mais visibilidade.

O combate ao *Web spam* pode exigir intervenção humana acoplada aos algoritmos⁵, ou reprogramação dos *programas rastejadores* que podem ser instruídos a não frequentar certos domínios.

A maioria dos algoritmos são segredos industriais ou foram patenteados⁶. O resto deste capítulo é baseado em informações de patentes.

5. Ranqueamento de Kleinberg

A matriz de transferência T foi definida assim: $T_{vu} = 1$ se existe uma aresta orientada (u, v) , senão $T_{vu} = 0$. Jon M. Kleinberg⁷ observou o seguinte: $(T^T T)_{u_1 u_2}$ conta o número de vezes que u_1 e u_2 apontam para a mesma página. Isso mede quanto u_1 e u_2 concordam enquanto fontes de referências.

Vamos supor que um engenho de busca atribui peso a_u para a página u enquanto fonte de referência. Quão bom é o vetor de pesos $\mathbf{a}$? Do ponto de vista da página u_1 , uma boa medida é $(T^T \mathbf{a})_{u_1}$. Uma medida de quão consensual é o vetor $\mathbf{a}$ é a norma $\|T^T \mathbf{a}\|$. Kleinberg sugere utilizar o autovetor principal de $T^T T$, que maximiza $\|T^T \mathbf{a}\|$, como peso para as páginas *enquanto fonte de referência*.

Já $(T T^T)_{v_2 v_1}$ conta o número de referências que apontam simultaneamente para v_1 e v_2 . Kleinberg também propõe utilizar o autovetor principal $\mathbf{b}$ de $T T^T$ como peso para as páginas *enquanto conteúdo*. (Ver exercício 20.11 para verificar que podemos escolher $\mathbf{b}$ de tal maneira que $b_u \geq 0$).

Esse algoritmo pode ser interpretado em termos da decomposição em valores singulares (Teorema 17.1). Os vetores $\mathbf{a}$ e $\mathbf{b}$ podem ser escolhidos de tal maneira que $\|\mathbf{a}\| = \|\mathbf{b}\| = 1$. Nesse caso, eles são o vetor singular principal à direita (resp. vetor singular principal à esquerda) de T , e são relacionados por

$$\sigma_1 \mathbf{b} = T \mathbf{a}$$

onde $\sigma_1 = \|T\|_2$ é o valor singular principal.

Os índices de Kleinberg são manipuláveis. Uma página pode obter um alto índice de relevância enquanto fonte apontando para toda a internet.

Para evitar esse tipo de manipulação, podemos substituir a matriz de transferência T pela matriz estocástica M .

Vamos voltar ao nosso exemplo. Uma maneira pouco eficiente de se calcular os vetores singulares é:

```
[19]: (u,sigma,v)=svd(M)
```

```
[20]: sigma
```

```
[20]: 15-element Array{Float64,1}:
 1.1108885716279948
 0.9833453894622696
 0.9232654389529134
 0.8527402231166038
 0.5610403692310317
```

⁵Ver por exemplo: Zoltán Gyöngi, Hector Garcia-Molina e Jan Pedersen, *Combating Web Spam with TrustRank*, Proceedings of the International Conference on Very Large Data Bases 30: 576. <http://www.vldb.org/conf/2004/RS15P3.PDF>.

⁶Algoritmos são objetos matemáticos e portanto não são patenteáveis. No entanto, o departamento de patentes de alguns países aceita objetos matemáticos como parte de um processo industrial.

⁷Jon Michael Kleinberg, *US Patent 6112202: Method and system for identifying authoritative information resources in an environment with content-based links between information resources.*, 1997, 2000

```

0.390362892204572
0.3790670163014063
0.348613722497253
0.30052038200428277
0.28333333333333344
0.28333333333333327
0.22259505340370173
0.06158225120493523
3.303632967362948e-17
4.218853768584729e-18

```

```
[21]: p=u[:,1]; q=v[:,1]; p=p/sum(p); q=q/sum(q) ; [p q]
```

```

[21]: 15×2 Array{Float64,2}:
 0.0408135  0.0413614
 0.027973   0.0726574
 0.0500631  0.102729
 0.137383   0.0540216
 0.0367623  0.0604258
 0.0320242  0.0939687
 0.190207   0.0540216
 0.0591204  0.139113
 0.0408135  0.0413614
 0.027973   0.051422
 0.0628924  0.0540216
 0.0875949  0.0554864
 0.0687932  0.0598031
 0.0687932  0.0598031
 0.0687932  0.0598031

```

Note que a ‘fazenda de links’ da Egoísta.com perdeu a liderança nas buscas ! O algoritmo mais eficiente para se achar autovetores principais (ou vetores singulares principais) é a iteração: Escolher $\mathbf{p}_1$ ao acaso, depois iterar

$$\mathbf{p}_{i+1} = \frac{(M^T M) \mathbf{p}_i}{\|(M^T M) \mathbf{p}_i\|}.$$

A velocidade de convergência é estimada facilmente utilizando o fato de que $M^T M$ é simétrica, e portanto (Teorema 16.1) admite uma base **ortonormal** de autovetores.

Seja $\mathbf{q}$ o autovetor principal de $M^T M$. Vamos escrever:

$$\mathbf{p}_i = x_i \mathbf{q} + \mathbf{r}_i,$$

com $\mathbf{r}_i \perp \mathbf{q}$. Então, a velocidade de convergência pode ser estimada por:

$$\frac{\|\mathbf{r}_{i+1}\|}{x_i + 1} \leq \frac{\lambda_2}{\lambda_1} \frac{\|\mathbf{r}_i\|}{x_i}$$

onde $\lambda_1 \geq \lambda_2 \geq \dots$ são os autovalores de $M^T M$ (e $\lambda_j = \sigma_j^2$).

6. O Hummingbird

Em 2013, a *Google* substituiu sem aviso o seu engenho de busca pelo Hummingbird (beija-flor). Os usuários perceberam que a interface de busca passou a interpretar consultas em linguagem natural. O que apenas especialistas perceberam é que o engenho de busca havia mudado.

Qual foi exatamente a mudança? A *Google* nunca foi clara sobre o *Hummingbird*. A *Alphabet*, conglomerado dono da *Google* e do *YouTube*, depositou uma patente⁸ que parece explicar o funcionamento do engenho.

A matriz de Márkov foi ampliada, introduzindo o conceito de entidade de busca. A entidade de busca pode ser:

- Uma busca feita pelo usuário. O texto é previamente analisado, e algumas buscas podem ser assimiladas a buscas com semântica igual.
- Uma resposta: documento, filme, url ou local geográfico.
- Comerciais. Google vende serviços publicitários que são personalizados para atingir um público alvo.
- Sessões, ou seja listas de buscas feitas em sequência. Podem ser sessões de todos os usuários.
- Tempo e localização geográfica da busca.
- Domínios da internet.

A matriz de Markov do ranqueamento de Page codificava os links de url para url, e continua existindo como uma submatriz de uma matriz bem maior. Mas agora podem existir transições entre outras entidades de busca:

Por exemplo, a probabilidade de transição de uma busca para uma resposta depende dos cliques longos, ou seja da proporção de usuários que depois dessa busca, abriram ou examinaram essa mesma resposta. A probabilidade de transição de um documento para uma busca depende por sua vez de quantos dentre os cliques longos para essa resposta estão associados à busca em questão.

A probabilidade de transição entre uma pergunta e um anúncio publicitário depende da proporção do lucro obtido mostrando esse anúncio em relação ao lucro total obtido depois dessa pergunta. A probabilidade de transição entre um anúncio publicitário e uma busca depende da proporção do lucro obtido com esse anúncio depois da busca, em relação ao lucro total com o anúncio.

A probabilidade de transição de uma sessão para uma pergunta ou documento depende da pergunta ter sido formulada, ou o documento examinado durante a sessão. A probabilidade de transição de uma pergunta ou documento para uma sessão depende da sessão conter essa pergunta ou do documento ter sido examinado.

Existem ainda probabilidades de transição entre tempo/localização geográfica para buscas, e vice-versa, ou entre documentos e domínios. A patente especifica muitas possibilidades em relação aos detalhes finos da matriz de Márkov a ser utilizada.

A partir desse momento, buscas na *Google* passaram a ser enviesadas. Interesses comerciais ou políticos dos anunciantes passam a interferir nos resultados mostrados. Existe também o viés de confirmação: se um usuário procura uma certa opinião, há uma tendência de que ele obtenha como resposta manifestações da mesma opinião.

7. Exercícios

Exercício 20.1. A figura 4 mostra uma “ponte de resistências”. Assuma que o valor de cada resistência é de 1Ω . Sabemos que passa uma corrente de $1A$ entre os pontos a e b . Qual é a diferença de tensão?

⁸Diego Federici, Search entity transition matrix and applications of the transition matrix, US Patent 10,270,791 B1 (2019).

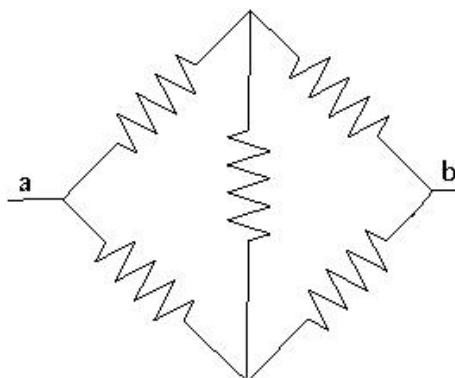


FIGURA 4. Ponte de resistências.

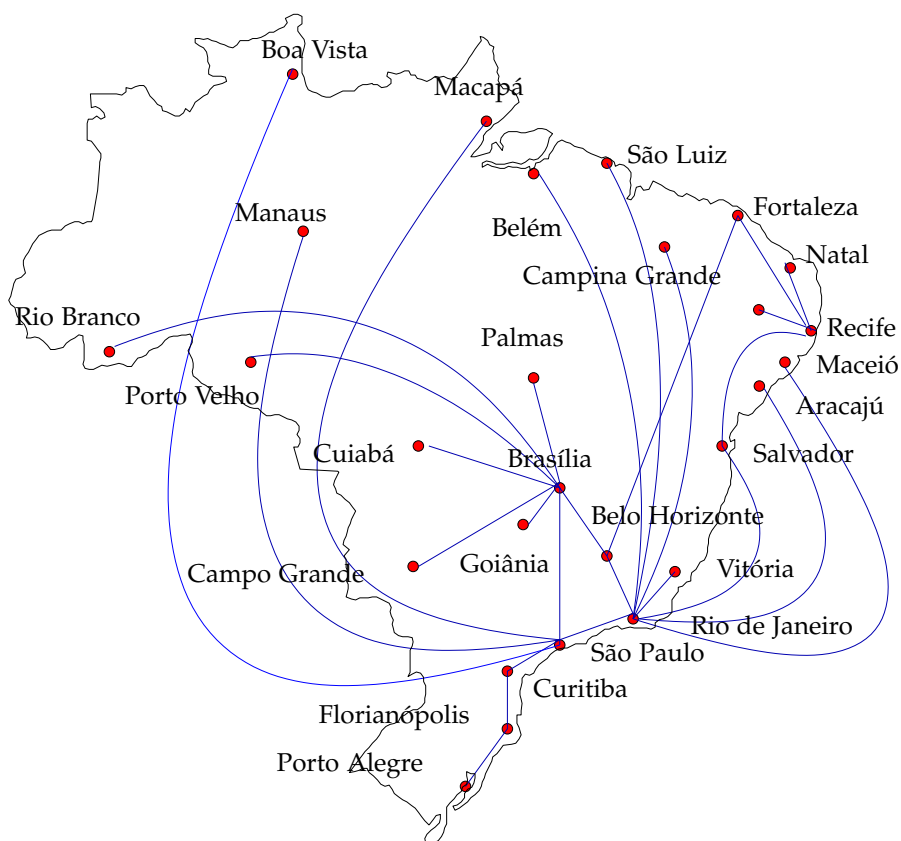


FIGURA 5. Rede Nacional de Pesquisa.

Exercício 20.2. A Figura 5 ilustra o *backbone* da Rede Nacional de Pesquisa (rnp). Escreva a matriz de adjacência. Usando *octave*, escreva o Laplaciano e os dois primeiros autovalores do espectro.

Exercício 20.3. Adapte o algoritmo de Page (PageRank) para ordenar os nodes da rnp por ‘relevância’.

Exercício 20.4. O grafo perfeito K_d de ordem d é o grafo com d vértices, conectados todos com todos. Quais são os autovalores de Δ_{K_d} ?

Exercício 20.5. Considere agora o grafo com d vértices 1 a d , onde j e $j + 1$ estão conectados e d está conectado a 1. Calcule numericamente os autovalores de seu Laplaciano, e trace um gráfico para $d = 100$. Qual foi o segundo autovalor ?

Exercício 20.6. Mesma pergunta, para o grafo cujos vértices são os inteiros entre 2 e 101 e há uma aresta entre $x \neq y$ se e somente se x divide y ou y divide x .

Exercício 20.7. Ainda a mesma pergunta, para uma árvore binária de profundidade 6 (127 vértices).

Exercício 20.8. Mesma pergunta, onde V é o conjunto de vetores em $\mathbb{R}^2$ com coordenadas inteiras entre 1 e n , com vértice entre os vetores a distância 1. Utilize $n = 100$.

Exercício 20.9. Explique qualitativamente os valores de λ_2 obtidos nos exercícios precedentes.

Exercício 20.10. Para a família de grafos do exercício 20.8, calcule numericamente λ_2 em função de n e trace um gráfico. Você pode conjecturar um comportamento assintótico ?

Exercício 20.11. Seja T a matriz de Kleinberg. Seja $\mathbf{b}$ o autovetor principal de TT^T . Use o Teorema de Perron-Frobenius para mostrar que é possível escolher $\mathbf{b}$ com coordenadas não-negativas.

CAPÍTULO 21

Álgebra linear com números complexos



Números complexos são inevitáveis. Autovalores de matrizes reais podem não ser reais, e isso nos obrigou a fazer álgebra linear sobre o corpo dos números complexos.

Os conceitos de independência linear, base, posto, dimensão ou inversibilidade são formalmente equivalentes. Apenas devemos ter em mente que combinações lineares agora são combinações lineares com coeficientes complexos.

A definição do produto interno precisa ser diferente, para que normas (e distâncias) sejam sempre números reais não-negativos. Atrelada à definição do produto interno complexo, vêm o grupo das transformações que preservam esse produto interno e o conceito de matrizes Hermitianas simétricas.

1. Produto Interno Hermitiano

Definição 21.1. O *Produto Interno Hermitiano Canônico* em $\mathbb{C}^n$ é definido por:

$$\langle \mathbf{z}, \mathbf{z}' \rangle_H = \sum_{j=1}^n z_j \bar{z}'_j$$

Podemos assimilar $\mathbb{C}^n$ a $\mathbb{R}^{2n}$ enquanto espaço vetorial *real*. Nesse caso, escrevendo $\mathbf{z} = \mathbf{x} + i\mathbf{y}$, $\mathbf{z}' = \mathbf{x}' + i\mathbf{y}'$, temos:

$$\operatorname{re}(\langle \mathbf{z}, \mathbf{z}' \rangle_H) = \langle \mathbf{x}, \mathbf{x}' \rangle + \langle \mathbf{y}, \mathbf{y}' \rangle$$

Note que podemos definir $\|\mathbf{z}\|^2 = \langle \mathbf{z}, \mathbf{z} \rangle_H = \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2$. Mas $\langle \cdot, \cdot \rangle_H$ é uma função a valores complexos, e pode possuir parte imaginária não nula. Por exemplo, $\left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} i \\ 0 \end{bmatrix} \right\rangle_H = -i$. Se usássemos apenas o produto interno de $\mathbb{R}^{2n}$, os vetores acima (dos quais um é múltiplo do outro) seriam ortogonais. É por essa razão que precisamos da parte imaginária do produto interno Hermitiano. A parte imaginária de $-\langle \cdot, \cdot \rangle_H$ é por vezes chamada de *forma simplética*.

O conceito abstrato de produto interno apresenta uma sutil diferença do caso real: $\langle \cdot, \cdot \rangle_H$ não é propriamente bilinear simétrica, vamos dizer que ela é *sesquimétrica*:

Definição 21.2. Seja E um espaço vetorial sobre o corpo dos números complexos. Uma função $\langle \cdot, \cdot \rangle_H : E \times E \rightarrow \mathbb{C}$ é um *produto interno Hermitiano* se e somente se ela satisfaz:

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.
Copyright © Gregorio Malajovich, 2011, 2021.

[PI1'] Ela é *positiva definida*: $\langle \mathbf{u}, \mathbf{u} \rangle_H \geq 0$, com igualdade se e somente se $\mathbf{u} = 0$.

[PI2'] Ela é *sesquisimétrica*: $\langle \mathbf{u}, \mathbf{v} \rangle_H = \overline{\langle \mathbf{v}, \mathbf{u} \rangle_H}$,

[PI3'] e, para todos $\alpha, \beta \in \mathbb{C}$, $\alpha \mathbf{u} + \beta \mathbf{v}, \mathbf{w} \rangle_H = \alpha \langle \mathbf{u}, \mathbf{w} \rangle_H + \beta \langle \mathbf{v}, \mathbf{w} \rangle_H$

Dado um produto interno Hermitiano, definimos a norma por

$$\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle_H}$$

Essa definição de norma satisfaz as propriedades da Definição 3.3. O conceito de ortogonalidade precisa ser redefinido:

Definição 21.3. Se E é um espaço vetorial complexo com produto interno Hermitiano $\langle \cdot, \cdot \rangle_H$, dizemos que dois vetores $\mathbf{u}$ e $\mathbf{v}$ de E são *ortogonais* se e somente se: $\langle \mathbf{u}, \mathbf{v} \rangle_H = 0$.

2. Bases ortonormais

O processo de Gram-Schmidt é formalmente idêntico ao processo de Gram-Schmidt real. Dada uma base $\alpha_1, \dots, \alpha_n$, podemos produzir uma base ortonormal complexa por:

$$\mathbf{q}_j = \frac{\alpha_j - \sum_{k \leq j} \langle \alpha_j, \mathbf{q}_k \rangle_H \mathbf{q}_k}{\|\alpha_j - \sum_{k \leq j} \langle \alpha_j, \mathbf{q}_k \rangle_H \mathbf{q}_k\|}$$

(verificar).

3. Matrizes Unitárias e Hermitianas Simétricas

A transposta hermitiana de uma matriz A de tamanho $m \times n$ é definida por

$$A^H = \bar{A}^T = \begin{bmatrix} \bar{A}_{11} & \dots & \bar{A}_{m1} \\ \vdots & & \vdots \\ \bar{A}_{1n} & \dots & \bar{A}_{mn} \end{bmatrix}$$

A mesma definição vale para vetores. Se assumimos que $\mathbb{C}^n$ está munido do produto interno canônico,

$$\langle A\mathbf{u}, \mathbf{v} \rangle_H = \mathbf{v}^H A\mathbf{u} = (A^H \mathbf{v})^H \mathbf{u} = \langle \mathbf{u}, A^H \mathbf{v} \rangle_H$$

Definição 21.4. Uma matriz A é *Hermitiana simétrica* se e somente se $A^H = A$. Em particular, a matriz A é quadrada.

Matrizes complexas cujas colunas são ortonormais têm um nome específico:

Definição 21.5. Uma matriz Q é *unitária* se e somente se $Q^H Q = I$.

Assim, podemos representar bases em $\mathbb{C}^n$ ou seus subespaços complexos por matrizes unitárias. O produto de duas matrizes unitárias quadradas ainda é unitário, e a inversa de uma matriz unitária quadrada Q é Q^H .

Definição 21.6. O *Grupo Unitário* $U(n)$ é o grupo das matrizes complexas unitárias de tamanho $n \times n$. A operação de grupo é a multiplicação matricial.

4. O Teorema Espectral

Teorema 21.7 (Teorema Espectral para matrizes Hermitianas). *Seja A uma matriz Hermitiana simétrica. Então os autovalores de A são reais, e A admite uma base ortonormal de autovetores.*

DEMONSTRAÇÃO. Em primeiro lugar, os autovalores são todos reais: se $A\mathbf{u} = \lambda\mathbf{u}$, e $\mathbf{u} \neq 0$, então

$$\lambda\|\mathbf{u}\|^2 = \langle \mathbf{u}, \lambda\mathbf{u} \rangle_H = \langle \mathbf{u}, A\mathbf{u} \rangle_H = \langle A^H \mathbf{u}, \mathbf{u} \rangle_H = \langle A\mathbf{u}, \mathbf{u} \rangle_H = \langle \lambda\mathbf{u}, \mathbf{u} \rangle_H = \bar{\lambda} \langle \mathbf{u}, \mathbf{u} \rangle_H = \bar{\lambda}\|\mathbf{u}\|^2$$

Logo, $\lambda = \bar{\lambda}$ e concluímos que os autovetores são reais.

Em segundo lugar, se $\mathbf{u}$ é um autovetor de A (digamos que $A\mathbf{u} = \lambda\mathbf{u}$) e $\mathbf{v} \perp \mathbf{u}$, então $A\mathbf{v} \perp \mathbf{u}$. De fato,

$$\langle A\mathbf{v}, \mathbf{u} \rangle_H = \langle \mathbf{v}, A\mathbf{u} \rangle_H = \lambda \langle \mathbf{v}, \mathbf{u} \rangle_H = 0.$$

Agora podemos mostrar o Teorema por indução:

Hipótese de Indução: *O Teorema vale em dimensão n .*

O caso inicial é trivial ($n = 1$). Assumindo o Teorema em dimensão n , seja A uma matriz complexa Hermitiana simétrica de tamanho $n + 1$. Ela admite pelo menos um autovetor $\mathbf{u}$, tal que $\|\mathbf{u}\| = 1$ e $A\mathbf{u} = \lambda\mathbf{u}$ para o autovalor $\lambda \in \mathbb{R}$.

Seja $E = \mathbf{u}^\perp$. O operador A leva E em E , e para todo par de vetores de E (digamos $\mathbf{v}$ e $\mathbf{w}$) teremos:

$$\langle A\mathbf{v}, \mathbf{w} \rangle_H = \langle \mathbf{v}, A\mathbf{w} \rangle_H.$$

Ou seja, o operador A restrito a E continua Hermitiano simétrico, e pode ser representado por uma matriz Hermitiana simétrica. Por indução, essa matriz admite uma base ortonormal de autovetores $\mathbf{q}_1, \dots, \mathbf{q}_n$, que são autovetores também de A . Concluimos que $(\mathbf{u}, \mathbf{q}_1, \dots, \mathbf{q}_n)$ é uma base ortonormal de autovetores de A . $\square$

5. A forma normal de Schur

Operadores Hermitianos Simétricos são diagonalizáveis. E matrizes em geral? A matriz de Jordan

$$J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

não é diagonalizável, nem mesmo utilizando números complexos.

Por outro lado, vimos que utilizando álgebra linear sobre os números complexos, conseguimos “diagonalizar” matrizes como

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

Ainda temos dificuldades com matrizes como

$$\begin{bmatrix} \cos \theta & -\sin \theta & 1 & 0 \\ \sin \theta & \cos \theta & 0 & 1 \\ 0 & 0 & \cos \theta & -\sin \theta \\ 0 & 0 & \sin \theta & \cos \theta \end{bmatrix}$$

Essa matriz é similar, sobre os complexos, à matriz:

$$\begin{bmatrix} e^{i\theta} & 0 & 1 & 0 \\ 0 & e^{-i\theta} & 0 & 1 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{-i\theta} \end{bmatrix}$$

Embora não seja diagonal, a matriz acima é triangular superior, o que a torna mais desejável para resolver recorrências e equações diferenciais.

Mas o fato de utilizarmos álgebra linear complexa nos dá mais liberdade. Podemos inclusive exigir que a similaridade seja dada por uma matriz unitária.

Teorema 21.8 (Schur). *Seja A uma matriz (real, complexa) de tamanho $n \times n$. Então existe uma matriz unitária complexa Q tal que*

$$A = QRQ^H$$

onde R é triangular superior, $R_{jj} = \lambda_j$ e $\lambda_1, \dots, \lambda_n$ são os autovalores de A (com multiplicidade).

DEMONSTRAÇÃO. Hipótese de Indução: O Teorema é válido para a dimensão n .

O caso inicial é trivial ($Q = 1$). Vamos agora assumir o Teorema para dimensão n . Seja A uma matriz real ou complexa de tamanho $(n+1) \times (n+1)$. Pelo Teorema Fundamental da Álgebra, A tem pelo menos um autovalor $\lambda \in \mathbb{C}$. Seja $\mathbf{u}$ o autovetor correspondente, com $\|\mathbf{u}\| = 1$, e seja $E = \mathbf{u}^\perp$.

Definimos o operador $B : E \rightarrow E$ por:

$$B(\mathbf{x}) = (I - \mathbf{u}\mathbf{u}^H)A\mathbf{x}$$

onde a matriz $I - \mathbf{u}\mathbf{u}^H$ é a projeção no espaço E . Por indução, existe uma base de E que “triangulariza” B :

$$B = Q_1 R_1 Q_1^H$$

(Onde Q_1 é uma matriz $(n+1) \times n$). Então,

$$A = \begin{bmatrix} \mathbf{u} & Q_1 \end{bmatrix} \begin{bmatrix} \lambda & ? & \dots & ? \\ 0 & R_1 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{u} & Q_1 \end{bmatrix}^H$$

e o Teorema vale para dimensão $n+1$. □

6. A exponencial de uma matriz

Se A é uma matriz quadrada, sua exponencial é definida pela série

$$\exp(A) = I + A + \frac{1}{2!}A^2 + \dots$$

A série acima foi definida por um processo limite. Para mostrar que o limite existe, podemos fazer a seguinte estimativa: Seja σ_1 o maior valor singular de A . Então para todo $\mathbf{u}$, $\|A\mathbf{u}\| \leq \sigma_1 \|\mathbf{u}\|$.

Assim, para todo $\mathbf{u}$, $\|e^A \mathbf{u}\| \leq e^{\sigma_1 \|\mathbf{u}\|} < \infty$. Além disso,

$$\left\| \sum_{k=1}^l \frac{1}{k!} A^k \mathbf{u} \right\| \leq \sum_{k=1}^l \frac{1}{k!} (\sigma_1 \|\mathbf{u}\|)^k$$

e no limite ($\mathbf{u}$ é fixo e $l \rightarrow \infty$) o lado direito é tão pequeno quanto se queira. Substituindo $\mathbf{u}$ por cada um dos vetores canônicos $e_1, \dots, e_n$, recuperamos as coordenadas de e^A . Concluimos disso que a exponencial de matrizes está definida para qualquer matriz A . O argumento acima se estende para matrizes complexas.

Uma motivação para se estudar a exponenciação de matrizes vem de equações diferenciais. O problema de valor inicial

$$\begin{cases} \dot{\mathbf{x}}(t) = A\mathbf{x}(t) \\ \mathbf{x}(0) = \mathbf{x}_0 \end{cases}$$

admite como solução única

$$(12) \quad \mathbf{x}(t) = e^{tA} \mathbf{x}_0.$$

Para se calcular a exponencial de uma matriz tA , é conveniente efetuar primeiro a decomposição de Schur: $A = QRQ^H$, onde Q é unitária e R é triangular superior. Então,

$$e^{tA} = Qe^{tR}Q^H.$$

Isso reduz o nosso problema a calcular a exponencial de uma matriz triangular superior. Vamos supor inicialmente que os autovalores R_{ii} são diferentes dois a dois. Seja $T = e^{tR}$. Valem as seguintes propriedades:

- (1) $T_{ii} = e^{tR_{ii}}$.
- (2) T é triangular superior.
- (3) R e T comutam: $TR = RT$.

Expandindo a coordenada (i, j) da última propriedade, $i \leq j$, temos que:

$$\sum_{k=i}^j T_{ik}R_{kj} = \sum_{k=i}^j R_{ik}T_{kj}.$$

Rearranjando os termos,

$$T_{ij}(R_{ii} - R_{jj}) = \sum_{k=i}^{j-1} T_{ik}R_{kj} - \sum_{k=i+1}^j R_{ik}T_{kj}.$$

Obtemos a expressão:

$$T_{ij} = \frac{\sum_{k=i}^{j-1} T_{ik}R_{kj} - \sum_{k=i+1}^j R_{ik}T_{kj}}{R_{ii} - R_{jj}}$$

Podemos portanto calcular primeiro os T_{ii} , depois os $T_{i,i+1}$, e assim por diante até chegar em $T_{i,n}$.

Se houver igualdade entre os autovalores, é possível substituir o quociente acima pelo limite (que é a derivada em relação a R_{ii}). Para ilustrar isso, escrevemos a exponencial de uma matriz 3×3 :

$$R = \begin{bmatrix} \lambda & R_{12} & R_{13} \\ 0 & \lambda & R_{23} \\ 0 & 0 & \lambda \end{bmatrix} \quad e^{tR} = \begin{bmatrix} e^{t\lambda} & R_{12}te^{t\lambda} & R_{13}te^{t\lambda} + R_{12}R_{23}t^2e^{t\lambda} \\ 0 & e^{t\lambda} & R_{23}te^{t\lambda} \\ 0 & 0 & e^{t\lambda} \end{bmatrix}$$

Concluimos com o seguinte fato sobre equações diferenciais lineares:

Teorema 21.9. *Seja $x(t)$ a solução do problema de valor inicial (12).*

- (1) *Se todos os autovalores de A tiverem parte real estritamente negativa, então para qualquer condição inicial $\mathbf{x}_0$, $\lim_{t \rightarrow \infty} \mathbf{x}(t) = 0$.*
- (2) *Se um dos autovalores de A tiver parte real estritamente positiva, então para qualquer condição inicial $\mathbf{x}_0$ fora de um certo hiperplano, $\lim_{t \rightarrow \infty} \mathbf{x}(t) = \infty$.*

No primeiro caso, o sistema é dito *estável*. Note que mesmo se o sistema for estável, a solução não é necessariamente decrescente (devido aos termos $te^{\lambda t}$ ou maiores).

O cálculo da exponencial de uma matriz qualquer é ainda um desafio tecnológico, e o desenvolvimento de algoritmos e programas de computador é um assunto de pesquisa¹

¹Ver por exemplo Cleve Moler e Charles Van Loan, Nineteen Dubious ways to Compute the Exponential of a Matrix, Twenty-Five Years Later. *Siam review* 45 No. 1, 2003.

7. A Forma Normal de Jordan

Teorema 21.10 (Jordan). *Seja A uma matriz $n \times n$ com autovalores $\lambda_1, \dots, \lambda_u$. Então existe uma base α não necessariamente ortonormal, tal que*

$$(A - \lambda I)_\alpha = \begin{bmatrix} J_{r_1}(\lambda_{t_1}) & 0 & \cdots & 0 \\ 0 & J_{r_2}(\lambda_{t_2}) & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & J_{r_s}(\lambda_{t_s}) \end{bmatrix}.$$

onde $J_1(\lambda) = [\lambda]$, $J_2(\lambda) = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$ e, em geral,

$$J_k(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & & \vdots \\ \vdots & & \ddots & \ddots & \\ 0 & \cdots & & \lambda & 1 \\ 0 & \cdots & & 0 & \lambda \end{bmatrix}$$

DEMONSTRAÇÃO. A prova está essencialmente feita nos exercícios. Lembremos (Ex. 10.9) que os autoespaço generalizados são definidos por:

$$E_\lambda^* = \{\mathbf{u} \in \mathbb{C}^n : \exists k \in \mathbb{N} \text{ t.q. } (A - \lambda I)^k \mathbf{u} = \mathbf{0}\}$$

Você vai mostrar no exercício 21.9 que $\mathbb{C}^n = \oplus E_\lambda^*$. O operador $(A - \lambda I)|_{E_\lambda^*}$ é nilpotente por definição. Assim, pelo exercício 11.9, existe uma base β_λ na qual ele se escreve

$$\left((A - \lambda I)|_{E_\lambda^*}\right)_{\beta} = \begin{bmatrix} J_{r_1}(0) & 0 & \cdots & 0 \\ 0 & J_{r_2}(0) & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & J_{r_s}(0) \end{bmatrix}.$$

Agora basta definir a base α como justaposição das bases β_λ . □

8. Estabilidade do Boeing 707

A seguinte equação é um modelo extremamente simplificado do comportamento de um *Boeing 707-321* voando a uma velocidade 80 ms^{-1} :

$$\dot{\mathbf{x}}(t) = \begin{bmatrix} -0.04600 & 0.10681 & 0.00000 & -0.17122 \\ -0.16759 & -0.51500 & 1.00000 & 0.00642 \\ 0.15431 & -0.54795 & -0.90600 & -0.00152 \\ 0.00000 & 0.00000 & 1.00000 & 0.00000 \end{bmatrix} \mathbf{x}(t) + \begin{bmatrix} 0.16023 & 0.00211 \\ 0.00820 & -0.03025 \\ 0.09174 & -0.75283 \\ 0.00000 & 0.00000 \end{bmatrix} \mathbf{u}(t)$$

$$\mathbf{y}(t) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathbf{x}(t).$$

No modelo acima, $\mathbf{x}(t)$ corresponde aos *estados internos*, $\mathbf{u}(t)$ aos controles do piloto e $\mathbf{y}(t)$ aos *observáveis*, descritos na tabela abaixo:

$x_1 = y_1$	$x_1 + 80ms^{-1}$ é o módulo do vetor Velocidade em relação ao ar.
x_2	Ângulo do eixo do avião com o vetor velocidade.
x_3	Velocidade angular de arfagem
$x_4 = y_2$	Ângulo de arfagem (eixo do avião, em relação ao plano horizontal)
u_1	Impulso do motor
u_2	Ângulo do Profundor

Esse modelo foi obtido de uma demonstração do programa *Octave*². Vamos inicialmente esquecer os controles e observáveis, e investigar a estabilidade do avião.

```
[1]: using(LinearAlgebra)
```

```
[2]: A= [ -0.04600  0.10681  0.00000 -0.17122;
          -0.16759 -0.51500  1.00000  0.00642;
           0.15431 -0.54795 -0.90600 -0.00152;
           0.00000  0.00000  1.00000  0.00000];
```

```
[3]: eigvals(A)
```

```
[3]: 4-element Array{Complex{Float64},1}:
      -0.7159231656462512 - 0.7124445743554908im
      -0.7159231656462512 + 0.7124445743554908im
      -0.017576834353748794 - 0.16899538628694116im
      -0.017576834353748794 + 0.16899538628694116im
```

O avião apresenta dois “modos” de oscilação em torno da equação de equilíbrio. Mas a parte real dos autovalores é negativa, logo $\lim_{t \rightarrow \infty} e^{At} = 0$. No entanto, o segundo modo de oscilação decai muito lentamente. Será que conseguimos inventar um “piloto automático” que torne o avião mais estável? A equação era modelada por:

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t)$$

$$\mathbf{y}(t) = C\mathbf{x}(t)$$

Vamos então realimentar os comandos com o resultado dos observáveis:

$$\mathbf{u}(t) = W\mathbf{y}(t)$$

É nossa responsabilidade escolher a matriz W de maneira adequada. Teremos então:

$$\dot{\mathbf{x}}(t) = (A + BWC)\mathbf{x}(t)$$

Por exemplo, $W = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ permite melhorar um pouco a estabilidade.

```
[6]: W=[-1 0 ;0 1];
      eigvals(A+B*W*C)
```

```
[6]: 4-element Array{Complex{Float64},1}:
      -0.5853255533993076 + 1.0613020101128472im
      -0.5853255533993076 - 1.0613020101128472im
      -0.22828944660069256 + 0.15855706124889934im
      -0.22828944660069256 - 0.15855706124889934im
```

²O modelo era um exemplo do pacote OCST por A. Scottedward Hodel e equipe. Esse pacote não está mais disponível

9. Exercícios

Exercício 21.1. Descreva todas as matrizes unitárias de tamanho 2×2 , em função de quatro parâmetros reais. Por que motivo o conjunto das matrizes unitárias 2×2 pode ser descrito por exatamente quatro parâmetros?

Exercício 21.2. Existe uma maneira rápida de calcular R^k **sem diagonalizar**, onde $k \gg n$ e R é triangular superior $n \times n$ com autovalores diferentes dois a dois?

Exercício 21.3. Implemente um algoritmo de fatoração QR para matrizes complexas 2×2 . Compare seu resultado com o resultado do comando `qr` do *Julia*.

Exercício 21.4. Procure numericamente um controlador W ótimo para o Boeing 707. Explique o seu procedimento.

Exercício 21.5. Seja $C_0^\infty([0, 1])$ o espaço de todas as funções reais infinitamente diferenciáveis do intervalo $[0, 1]$, com $f^{(k)}(0) = f^{(k)}(1) = 0$ para todo $k \geq 0$. É um espaço vetorial real, e admite o produto interno

$$\langle f, g \rangle = \int_0^1 f(x)g(x)dx.$$

O operador $\Delta : f \mapsto \frac{\partial^2 f}{\partial x^2}$ é linear. Não podemos (sem ter uma base para $C_0^\infty([0, 1])$) dizer se esse operador é simétrico. Prove que ele é *autoadjunto*, ou seja que para todas f e g ,

$$\langle \Delta f, g \rangle = \langle f, \Delta g \rangle$$

Exercício 21.6. Seja E um espaço vetorial complexo (possivelmente de dimensão infinita) com produto interno. Mostre que se uma transformação linear autoadjunta $A : E \rightarrow E$ admitir λ como autovalor, então $\lambda \in \mathbb{R}$. Mostre, sob as mesmas hipóteses, que se A admitir dois autovetores associados a autovalores diferentes, então eles são ortogonais.

Exercício 21.7. Matrizes simétricas aleatórias complexas podem ser geradas com:

[24] : `A=randn(100,100); S=A+A'`

Como no exercício 16.10, plote um histograma dos autovalores. A Lei de Wigner também se aplica?

Exercício 21.8. Mostre o Teorema de Cayley-Hamilton: Se $p(\lambda) = \sum_{j=0}^n p_j \lambda^j = \det(A - \lambda I)$ é o polinômio característico de A , então

$$p(A) = \sum_{j=0}^n p_j A^j = 0.$$

Exercício 21.9. Seja A uma matriz (real ou complexa) $n \times n$ e sejam E_λ^* os autoespaços generalizados. Mostre que $\dim E_\lambda^*$ é a multiplicidade de λ no polinômio característico. Deduza do exercício 10.9 que $\mathbb{C}^n = \oplus E_\lambda^*$.

Exercício 21.10. Mostre um contraexemplo para a existência da fatoração de Schur real (ou seja, de que cada matriz real se escreve da forma QRQ^T , com Q ortogonal e R triangular superior real. Mostre, no entanto, que toda matriz real se escreve como QRQ^T , com Q ortogonal e R real ‘triangular superior por blocos’, ou seja da forma:

$$R = \begin{bmatrix} R_{11} & R_{12} \\ 0 & R_{22} \end{bmatrix}$$

com R_{11} real triangular superior e:

$$R_{22} = \begin{bmatrix} a_1 & -b_1 & ? & ? & \cdots & \cdots & ? & ? \\ b_1 & a_1 & ? & ? & \cdots & \cdots & ? & ? \\ 0 & 0 & a_2 & -b_2 & & & \vdots & \vdots \\ 0 & 0 & b_2 & a_2 & & & \vdots & \vdots \\ \vdots & \vdots & & & \ddots & \ddots & ? & ? \\ \vdots & \vdots & & & \ddots & \ddots & ? & ? \\ 0 & 0 & \cdots & \cdots & 0 & 0 & a_k & -b_k \\ 0 & 0 & \cdots & \cdots & 0 & 0 & b_k & a_k \end{bmatrix},$$

e onde o símbolo '?' denota números reais quaisquer.

Problema em aberto N° 5. A função 'zeta' de Riemann é definida por

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$$

para todo número complexo z com $\operatorname{re}(z) > 1$. Ela pode ser estendida de maneira única para uma função 'analítica' de $\mathbb{C} \setminus \{1\}$. (Uma função é analítica se a sua série de Taylor é convergente em uma vizinhança de qualquer ponto).

A função $\zeta(z)$ se anula para $z = -2, -4, -6, \dots$ (são os 'zeros triviais'. Todos os outros zeros de ζ satisfazem $0 < \operatorname{re}(z) < 1$).

A *Hipótese de Riemann* diz que os zeros não-triviais satisfazem todos $\operatorname{re}(z) = 1/2$. Ela implicaria uma série de resultados importantes em teoria dos números.

A Hipótese de Riemann está em aberto desde 1859, e existe uma recompensa de US\$ 1.000.000,00 pela sua elucidação³.

Problema em aberto N° 6. A Hipótese de Riemann é um problema difícilimo. Uma possibilidade de ataque partiu do estudo das propriedades estatísticas dos zeros não-triviais da função ζ . Em 1992, A. Odlyzko descobriu que a separação entre os zeros não-triviais da função ζ pode ser modelada, com precisão surpreendente, pela separação dos autovalores de matrizes aleatórias simétricas complexas.

A definição da separação envolve uma 'normalização' ou transformação não-linear crescente. Nas novas coordenadas, compara-se a probabilidade de que a distância de um autovalor (ou zero) para o k -ésimo consecutivo esteja dentro de um intervalo $[\alpha, \beta]$. As estatísticas obtidas com os zeros da função ζ são (quase) indistinguíveis das obtidas com os autovalores.

A explicação deste fenômeno está totalmente em aberto. Uma explicação pode abrir perspectivas de se interpretar os zeros da função zeta como $z_j = \frac{1}{2} + \lambda_j$ onde os λ_j são autovalores de uma matriz simétrica infinita, e portanto reais.

³www.claymath.org

CAPÍTULO 22

Normas de matrizes



Este capítulo lida com normas de matrizes ou aplicações lineares. O espaço das aplicações lineares de um espaço normado $\mathbb{E}$ em um espaço normado $\mathbb{F}$ tem uma norma “natural”, que iremos definir e utilizar. Para isso, é conveniente lembrar da noção de *supremo* de um conjunto de números reais.

O supremo $\sup \mathcal{X}$, onde $\mathcal{X} \subset \mathbb{R}$, é o menor número real que é maior ou igual a todos os elementos de $\mathcal{X}$. Se $\mathcal{X}$ é limitado superiormente, então o supremo sempre existe. Esse fato segue da construção dos números reais, e é explicado em qualquer bom livro de Cálculo¹.

Quando $\mathcal{X}$ não é limitado superiormente, convencionamos que $\sup \mathcal{X} = \infty$. Vamos também utilizar as seguintes propriedades do supremo: Seja $\mathcal{X} + \mathcal{Y}$ a ‘soma’ dos conjuntos, ou seja o conjunto dos $x + y$ onde $x \in \mathcal{X}$ e $y \in \mathcal{Y}$. Então, $\sup(\mathcal{X} + \mathcal{Y}) \leq \sup \mathcal{X} + \sup \mathcal{Y}$ e, se $r \geq 0$, $\sup(r\mathcal{X}) = r \sup \mathcal{X}$.

1. Norma de operador

Sejam $\mathbb{E} \neq \{0\}$ e $\mathbb{F}$ espaços vetoriais normados, e denotamos por $\|\cdot\|_{\mathbb{E}}$ e $\|\cdot\|_{\mathbb{F}}$ as respectivas normas. Seja A uma aplicação linear de $\mathbb{E}$ em $\mathbb{F}$.

Definição 22.1. A norma de operador de A é

$$\|A\|_{\mathbb{E},\mathbb{F}} = \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}}$$

Quando $\mathbb{E} = \mathbb{R}^n$ e $\mathbb{F} = \mathbb{R}^m$ munidos da norma canônica, escrevemos

$$\|A\|_{\mathbb{E},\mathbb{F}} = \|A\|_2$$

Proposição 22.2. A norma de operador descrita acima satisfaz os axiomas da Definição 3.3

DEMONSTRAÇÃO.

[N1] Positividade: Seja $\mathcal{X} = \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \left\{ \frac{\|A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} \right\}$. Como existe pelo menos um elemento de $\mathcal{X}$ e ele é positivo ou nulo, $\sup \mathcal{X} \geq 0$. Agora vamos supor que $\|A\|_{\mathbb{E},\mathbb{F}} = 0$. Então, para todo $\mathbf{x} \in \mathbb{E}$, teremos $\|A\mathbf{x}\|_{\mathbb{F}} = 0$. Pelo Axioma [N1] da norma $\|\cdot\|_{\mathbb{F}}$, isso implica que $\mathbf{x} = 0$. Como isso vale para todo $\mathbf{x}$, temos que $A \equiv 0$.

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.

Copyright © Gregorio Malajovich, 2011, 2021.

¹Por exemplo: Richard Courant e Fritz John, *Introduction to calculus and analysis*. Vol. I. Reprint of the 1989 edition. Classics in Mathematics, Springer-Verlag, Berlin, 1999.

[N2] Multiplicatividade:

$$\begin{aligned}
\|\lambda A\|_{\mathbb{E}, \mathbb{F}} &= \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|\lambda A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} \\
&= \sup_{0 \neq \mathbf{x} \in \mathbb{E}} |\lambda| \frac{\|A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} \quad \text{pelo Axioma [N2] de } \|\cdot\|_{\mathbb{F}} \\
&= |\lambda| \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}}
\end{aligned}$$

[N3] Desigualdade triangular:

$$\begin{aligned}
\|A + B\|_{\mathbb{E}, \mathbb{F}} &= \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|A\mathbf{x} + B\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} \\
&\leq \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \left(\frac{\|A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} + \frac{\|B\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} \right) \quad \text{pelo Axioma [N3] de } \|\cdot\|_{\mathbb{F}} \\
&\leq \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|A\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} + \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|B\mathbf{x}\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}}
\end{aligned}$$

□

Outra consequência imediata da definição de norma de operador é que, se $A : \mathbb{E} \rightarrow \mathbb{F}$ e $B : \mathbb{F} \rightarrow \mathbb{G}$, então

$$\|B \circ A\| \leq \|B\| \|A\|$$

Observação 22.3. É usual denotar a norma canônica (Euclidiana) de um vetor x por $\|x\|_2$, e é dessa convenção que vem a notação $\|A\|_2$ para a norma do operador A .

Observação 22.4. A norma de operador pode ser infinita. Por exemplo, seja $\mathbb{R}[x]$ o espaço dos polinômios a coeficiente real, de qualquer grau, da variável x . Definimos a norma de $f(x) = \sum_{j=0}^d f_j x^j$ por $\|f(x)\| = \sqrt{\sum_{j=0}^{\infty} f_j^2}$. (Verifique que é uma norma). O operador

$$\begin{aligned}
\frac{\partial}{\partial x} : \mathbb{R}[x] &\rightarrow \mathbb{R}[x] \\
f(x) &\mapsto \frac{\partial}{\partial x} f(x) = \sum_{j=1}^d j f_j x^{j-1}
\end{aligned}$$

tem norma infinita !

2. Ação de Grupo

Vamos supor agora que os espaços $\mathbb{E}$ e $\mathbb{F}$ estão munidos de produto interno, e que as normas $\|\cdot\|_{\mathbb{E}}$ e $\|\cdot\|_{\mathbb{F}}$ são as normas induzidas pelo produto interno:

$$\|\mathbf{x}\|_{\mathbb{E}} = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$$

e mesma coisa para $\mathbb{F}$.

Denotamos por $O(\mathbb{E})$ e $O(\mathbb{F})$ o grupo das transformações lineares *ortogonais* respectivas, ou seja das transformações lineares que preservam o produto interno: $Q \in O(\mathbb{E})$ se e somente se, para todos $\mathbf{x}, \mathbf{y} \in \mathbb{E}$,

$$\langle Q\mathbf{x}, Q\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle.$$

No caso particular $\mathbb{E} = \mathbb{R}^n$ com o produto interno canônico, $O(\mathbb{E})$ é exatamente o grupo das matrizes ortogonais $n \times n$.

Seja $L(\mathbb{E}, \mathbb{F})$ o espaço das aplicações lineares de $\mathbb{E}$ em $\mathbb{F}$. Os grupos $O(\mathbb{E})$ (resp. $O(\mathbb{F})$) agem, resp. à direita e à esquerda, em $L(\mathbb{E}, \mathbb{F})$, por:

$$\begin{aligned} a : L(\mathbb{E}, \mathbb{F}) \times O(\mathbb{E}) &\rightarrow L(\mathbb{E}, \mathbb{F}) \\ A, V &\mapsto a(A, V) = A \circ V \end{aligned}$$

e

$$\begin{aligned} b : O(\mathbb{F}) \times L(\mathbb{E}, \mathbb{F}) &\rightarrow L(\mathbb{E}, \mathbb{F}) \\ U, A &\mapsto b(U, A) = U \circ A \end{aligned}$$

Proposição 22.5. *A norma de operador em $L(\mathbb{E}, \mathbb{F})$ é invariante pelas ações de $O(\mathbb{E})$ e $O(\mathbb{F})$ definidas acima.*

DEMONSTRAÇÃO. Vamos mostrar a proposição apenas para a ação de $O(\mathbb{F})$. A prova para a ação de $O(\mathbb{E})$ é similar.

$$\begin{aligned} \|A \circ V\|_{\mathbb{E}, \mathbb{F}} &= \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|A(V\mathbf{x})\|_{\mathbb{F}}}{\|\mathbf{x}\|_{\mathbb{E}}} \\ &= \sup_{0 \neq \mathbf{x} \in \mathbb{E}} \frac{\|A(V\mathbf{x})\|_{\mathbb{F}}}{\|V\mathbf{x}\|_{\mathbb{E}}} \\ &= \sup_{0 \neq \mathbf{y} \in \mathbb{E}} \frac{\|A\mathbf{y}\|_{\mathbb{F}}}{\|\mathbf{y}\|_{\mathbb{E}}} \end{aligned}$$

□

Proposição 22.6. *Se A é uma matriz $m \times n$, então*

$$\|A\|_2 = \sigma_1$$

onde σ_1 é o valor singular principal de A .

DEMONSTRAÇÃO. No caso particular $\mathbb{E} = \mathbb{R}^n$ e $\mathbb{F} = \mathbb{R}^m$, o Teorema 17.1 (Decomposição em valores singulares) garante que para toda A , existem $U \in O(m)$ e $V \in O(n)$ tais que

$$A = U \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} V^T \quad \text{ou} \quad A = U \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \sigma_m & 0 & \cdots & 0 \end{bmatrix} V^T$$

onde $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_{\min(m,n)}$. Vamos considerar somente o primeiro caso (o outro é idêntico). Pela ação de grupo (Proposição 22.5),

$$\|A\|_2 = \left\| \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \sigma_n \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} V^T \right\|_2$$

Estimamos:

$$\|A\mathbf{x}\| = \sqrt{\sum \sigma_j^2 x_j^2} = \sigma_1 \sqrt{\sum \frac{\sigma_j^2}{\sigma_1^2} x_j^2} \leq \sigma_1 \sqrt{\sum x_j^2} = \sigma_1 \|\mathbf{x}\|.$$

A igualdade é atingida quando $\mathbf{x} = \mathbf{e}_1$. Logo, $\|A\|_2 = \sigma_1$. $\square$

Observação 22.7. Tudo o que fizemos até agora é também válido para espaços vetoriais complexos, com as substituições óbvias: grupos unitários substituem grupos ortogonais e produtos hermitianos substituem o produto interno.

3. Norma de transformações lineares

Vamos agora supor que A é uma transformação inversível de $\mathbf{R}^n$ em $\mathbf{R}^n$. Na seção anterior, a ação de grupo permitia escolher de maneira independente um sistema de coordenadas em $\mathbf{E}$ e outro em $\mathbf{F}$. Desta vez, insistimos para ter o **mesmo** sistema de coordenadas, de maneira a poder iterar a transformação. A ação do grupo ortogonal é portanto por *conjugação*:

$$\begin{aligned} c : GL(\mathbb{R}^n) \times O(n) &\rightarrow GL(\mathbb{R}^n) \\ Q, A &\mapsto c(Q, A) = Q \circ A \circ Q^T \end{aligned}$$

Note que

$$(QAQ^T)^k = \underbrace{(QAQ^T)(QAQ^T) \cdots (QAQ^T)}_{k \text{ vezes}} = QA^kQ^T$$

4. Séries e matrizes

Uma *série* de números reais (ou complexos) é uma soma infinita

$$s = \sum_{i=0}^{\infty} a_i.$$

Ela é dita *convergente* se e somente se a sequência das somas parciais $(s_n)_{n \in \mathbb{N}}$, onde $s_n = \sum_{i=0}^n a_i$, é convergente. A definição formal de convergência é:

$$\exists s^* \text{ tal que } \forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tal que, } n > N \Rightarrow |s_n - s^*| < \epsilon.$$

O valor s^* da série só está definido para séries convergentes.

Uma definição mais forte é a da convergência absoluta: Uma série $s = \sum_{i=0}^{\infty} a_i$ é dita *absolutamente convergente* se $\sum_{i=0}^{\infty} |a_i|$ é convergente. Um bom exercício de ϵ 's e δ 's é mostrar que convergência absoluta implica convergência.

Um exemplo de série absolutamente convergente é a função exponencial:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

Imitando essa definição, definimos a *exponencial* de uma matriz por:

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

Utilizando a noção de norma, a convergência dessa série é fácil de provar. Mas vamos mostrar um resultado mais geral:

Proposição 22.8. Se a série

$$f(x) = \sum_{k=0}^{\infty} c_k x^k$$

é absolutamente convergente para todo $|x| < r$, e se A é uma matriz de raio espectral $\rho(A) < r$, então a série

$$f(A) = \sum_{k=0}^{\infty} c_k A^k$$

é convergente.

A Proposição 22.8 implica, como caso particular, a Proposição 19.10 cuja prova havíamos prometido.

DEMONSTRAÇÃO DA PROPOSIÇÃO 19.10. A série

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

é absolutamente convergente para $|x| < 1$. Da proposição 22.8, deduzimos que quando o raio espectral $\rho(A)$ é menor do que 1, a série

$$(I - A)^{-1} = I + A + A^2 + \dots$$

é absolutamente convergente. Uma consequência imediata é que

$$\lim_{l \rightarrow \infty} \sum_{k \geq l} |(A^k)_{ij}| = 0.$$

Em particular, $\lim_{k \rightarrow \infty} |(A^k)_{ij}| = 0$. Logo, $\lim_{k \rightarrow \infty} A^k = 0$. $\square$

De fato, se A tem autovalores com módulo estritamente menor do que um, todas as séries abaixo são absolutamente convergentes:

$$\begin{aligned} (I - A)^{-1} &= I + A + A^2 + A^3 + \dots \\ (I - A)^{-2} &= I + 2A + 3A^2 + 4A^3 + \dots \\ (I - A)^{-3} &= I + 3A + 6A^2 + 10A^3 + \dots \\ &\vdots \end{aligned}$$

Antes de mostrar a Proposição 22.8, vamos precisar de um resultado sobre séries:

Lema 22.9. Se a série $a(t) = \sum_{i \geq 0} a_i t^i$ é absolutamente convergente para todo $|t| < \epsilon$, então a sua derivada formal $a'(t) = \sum_{i \geq 1} i a_i t^{i-1}$ também é absolutamente convergente na mesma região.

DEMONSTRAÇÃO DA PROPOSIÇÃO 22.9. Seja $|t| < \delta < \epsilon' < \epsilon$. Escolhemos $N \geq 1$ de maneira a que, para todo $i \geq N$

$$i \left(\frac{\delta}{\epsilon'} \right)^{i-1} < 1.$$

Podemos agora escrever $c'(t)$ como:

$$c'(t) = \left(\sum_{1 \leq i < N} i a_i t^{i-1} \right) + \left(\sum_{N \leq i} i a_i t^{i-1} \right)$$

A primeira parcela é finita, e a segunda parcela é absolutamente convergente. Logo, $c'(t)$ é absolutamente convergente. $\square$

DEMONSTRAÇÃO DA PROPOSIÇÃO 22.8.

Ação de grupo: Aplicamos a decomposição de Schur $A = QRQ^H$ onde Q é unitária, e R é triangular superior com os autovalores de A na diagonal.

Se $f(A)$ for convergente,

$$f(A) = Qf(R)Q^H$$

e $f(R)$ será convergente. Reciprocamente, se $f(R)$ for convergente então $f(A)$ será convergente. Assim, basta mostrar a Proposição para $f(R)$.

Caso restrito: Vamos assumir por enquanto que os autovalores de $\lambda_i = R_{ii}$ de R são diferentes 2 a 2. Seja $T = f(R)$. Os termos da diagonal de T são dados por

$$T_{ii} = f(\lambda_i)$$

e portanto são bem-definidos. Considerada como série, T_{ii} é convergente. A idéia agora é produzir uma recorrência para calcular os termos T_{ij} fora da diagonal em tempo finito,

Hipótese de indução em $r = j - i$:

$$(13) \quad T_{ij} = \frac{\sum_{i \leq l < j} T_{il} R_{lj} - \sum_{i < l \leq j} R_{il} T_{lj}}{\lambda_i - \lambda_j}$$

O caso inicial é $r = 1$. Simplesmente escrevemos

$$(R^k)_{i,i+1} = \sum_{l=0}^{k-1} R_{ii}^l R_{i,i+1} R_{i+1,i+1}^{k-l-1} = R_{i,i+1} \frac{R_{ii}^k - R_{i+1,i+1}^k}{R_{ii} - R_{i+1,i+1}}.$$

Assim,

$$T_{i,i+1} = R_{i,i+1} \sum_{k=0}^{\infty} c_k \frac{R_{ii}^k - R_{i+1,i+1}^k}{R_{ii} - R_{i+1,i+1}} = R_{i,i+1} \frac{T_{ii} - T_{i+1,i+1}}{\lambda_i - \lambda_{i+1}}.$$

Logo a hipótese 13 vale para $r = 1$. Assumimos portanto que a hipótese de indução vale até um certo r , e escrevemos:

$$(R^k)_{i,i+r+1} = \sum_{j \in \mathcal{J}(i,k,r)} R_{j_0,j_1} R_{j_1,j_2} \cdots R_{j_{k-1},j_k},$$

onde o somatório é sobre o conjunto $\mathcal{J}(i,k,r)$ de todas as funções $s \mapsto j_s$ não decrescentes de $\{0, \dots, k\}$ em $\{i, \dots, i+r+1\}$ com $j_0 = i$ e $j_k = i+r+1$.

Multiplicando por $R_{ii} - R_{i+r+1,i+r+1} = \lambda_i - \lambda_{i+r+1}$, obtemos:

$$\begin{aligned} (\lambda_i - \lambda_{i+r+1})(R^k)_{i,i+r+1} &= (R_{ii} - R_{i+r+1,i+r+1}) \sum_{j \in \mathcal{J}(i,k,r)} R_{j_0,j_1} R_{j_1,j_2} \cdots R_{j_{k-1},j_k} \\ &= \sum_{j \in \mathcal{J}(i,k,r)} R_{ii} R_{j_0,j_1} R_{j_1,j_2} \cdots R_{j_{k-1},j_k} \\ &\quad - \sum_{j \in \mathcal{J}(i,k,r)} R_{j_0,j_1} R_{j_1,j_2} \cdots R_{j_{k-1},j_k} R_{i+r+1,i+r+1} \\ &= \sum_{i < a \leq i+r+1} R_{a,i+r+1} \sum_{u \in \mathcal{J}(i,k,a-i-1)} R_{u_0,u_1} R_{u_1,u_2} \cdots R_{u_{k-1},u_k} \\ &\quad - \sum_{i \leq b < i+r+1} R_{i,b} \sum_{v \in \mathcal{J}(b,k,r+i-b)} R_{v_0,v_1} R_{v_1,v_2} \cdots R_{v_{k-1},v_k} \\ &= \sum_{i \leq a < i+r+1} R_{a,i+r+1} (R^k)_{i,a} - \sum_{i < b \leq i+r+1} R_{i,b} (R^k)_{b,i+r+1}. \end{aligned}$$

Somando c_k vezes a equação acima para todos os k , recuperamos:

$$(\lambda_i - \lambda_{i+r+1})T_{i,i+r+1} = \sum_{i \leq a < i+r+1} R_{a,i+r+1} T_{i,a} - \sum_{i < b \leq i+r+1} R_{i,b} T_{b,i+r+1},$$

que é equivalente à hipótese (13) para $r + 1$. Isso estabelece a indução.

Extensão ao caso geral ou o poder do Cálculo: Até aqui, supusemos que a matriz R tinha autovalores diferentes dois a dois. Vamos mostrar que quando algum denominador de (13) se anula, é possível interpretar o quociente de (13) como uma derivada.

Para isso, vamos substituir a nossa matriz R (que agora pode ter autovalores iguais) por uma matriz função do tempo:

$$R(t) = R + t \begin{bmatrix} \mu_1 & 0 & \cdots & 0 \\ 0 & \mu_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & \mu_n \end{bmatrix}.$$

Os μ_i são escolhidos para que, se $0 < |t| < \epsilon$, não haja dois $\lambda_i + t\mu_i$ iguais. (Como você faria isso?). Assuma que $\lambda_i = \lambda_{i+1} = \cdots = \lambda_j$. Com $0 < |t| < \epsilon$, temos:

$$(14) \quad T_{ij}(t) = \frac{\sum_{i \leq l < j} T_{il}(t)R_{lj}(t) - \sum_{i < l \leq j} R_{il}(t)T_{lj}(t)}{(\mu_i - \mu_j)t}.$$

Quando $t \rightarrow 0$, o limite do denominador é zero. Assim,

$$T_{ij}(t) = \frac{1}{\mu_i - \mu_j} \frac{\partial}{\partial t} \left(\sum_{i \leq l < j} T_{il}(t)R_{lj}(t) - \sum_{i < l \leq j} R_{il}(t)T_{lj}(t) \right).$$

A expressão entre parênteses é uma série $\sum_{i \geq 0} a_i t^i$ em t , e é absolutamente convergente para todo t com $|t| < \epsilon$ (por indução). Logo (Proposição 22.8) a sua derivada é absolutamente convergente. Além disso, por construção, $\mu_i \neq \mu_j$. $\square$

5. Exercícios

Exercício 22.1. Mostre que existe A tal que $\|A^2\|_2 < \|A\|_2^2$

Exercício 22.2. A *norma de Frobenius* de uma matriz $m \times n$ é definida por: $\|A\|_F = \sqrt{\sum_{i,j} |A_{ij}|^2}$. É a norma Euclidiana se assimilamos A a um vetor de $\mathbb{R}^{mn}$. Mostre que a ação dos grupos $O(\mathbb{R}^m)$ e $O(\mathbb{R}^n)$ definida no capítulo deixa a norma de Frobenius invariante.

Exercício 22.3. Conclua do exercício anterior que

$$\frac{\|A\|_F}{\sqrt{\min(m, n)}} \leq \|A\|_2 \leq \|A\|_F.$$

Mostre exemplos onde a primeira ou a segunda desigualdade são igualdades.

Exercício 22.4. Mostre que a norma de Frobenius não é uma norma de operador.

Exercício 22.5. Mostre para toda matriz $m \times n$, $\|A\|_2 = \|A^T\|_2$.

Exercício 22.6. Escreva $\|A\|_1$ e $\|A\|_\infty$ como funções dos coeficientes de A . Deduza que $\|A\|_1 = \|A^T\|_\infty$.

Exercício 22.7. Seja $\|x\|_\infty = \max |x_i|$ e seja $\|A\|_\infty$ a norma de operador correspondente, onde A é uma matriz $m \times n$. Mostre que

$$\frac{1}{\sqrt{n}} \|A\|_\infty \leq \|A\|_2 \leq \sqrt{m} \|A\|_\infty.$$

Exercício 22.8. Seja $\|x\|_1 = \sum |x_i|$ e seja $\|A\|_1$ a norma de operador correspondente, onde A é uma matriz $m \times n$. Mostre que

$$\frac{1}{\sqrt{m}} \|A\|_\infty \leq \|A\|_2 \leq \sqrt{n} \|A\|_\infty.$$

Exercício 22.9. Seja A uma matriz quadrada e inversível. Mostre que sempre que o termo da direita existir e for positivo,

$$\|A^{-1}\|_2 \leq \frac{1}{1 - \|A - I\|_2} .$$

Exercício 22.10. Seja $\mathcal{P}$ o espaço de todos os polinômios (em qualquer grau). Defina a norma como

$$\|f\|_2 = \sqrt{\sum_0^{\text{grau}(f)} |f_i|^2} .$$

Mostre que a derivação $D : f(x) \mapsto \frac{\partial f(x)}{\partial x}$ tem norma de operador infinita.

CAPÍTULO 23

Polinômios pérfidos e matrizes mal postas

1. Perfídia



polinômio *pérvido* de grau d (também conhecido como polinômio de Pochhammer) é definido por:

$$p_d(x) = (x-1)(x-2) \cdots (x-d)$$

Por exemplo,

$$\begin{aligned} p_{10}(x) = & x^{10} - 55x^9 + 1320x^8 - 18150x^7 + 157773x^6 - 902055x^5 + \\ & + 3416930x^4 - 8409500x^3 + 12753576x^2 - 10628640x + 3628800 \end{aligned}$$

Uma maneira de se resolver polinômios de grau baixo é produzir a *matriz companheira* associada a eles. Se $f(x) = x^d + f_{d-1}x^{d-1} + \cdots + f_1x + f_0$, então a matriz companheira de f é

$$C_f = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & 0 & 1 \\ -f_0 & -f_1 & \cdots & -f_{d-2} & -f_{d-1} \end{bmatrix}$$

A matriz companheira foi construída de maneira a que f fosse o seu polinômio característico (a menos do sinal):

$$\det C_f - \lambda I = (-1)^d f(\lambda).$$

Assim, reduzimos o problema de resolver um polinômio de grau d a outro problema, que é o de achar os autovalores de uma matriz $d \times d$. Existe excelente software numérico para achar autovalores. Vamos aplicar essa idéia ao polinômio pérfido.

```
[1]: using LinearAlgebra
      using Plots
      using Polynomials
```

```
[2]: p=fromroots(1:10)
```

```
[2]: 3628800 - 10628640 · x + 12753576 · x2 - 8409500 · x3 + 3416930 · x4 - 902055 · x5 +
      157773 · x6 - 18150 · x7 + 1320 · x8 - 55 · x9 + x10
```

```
[3]: x=roots(p)
```

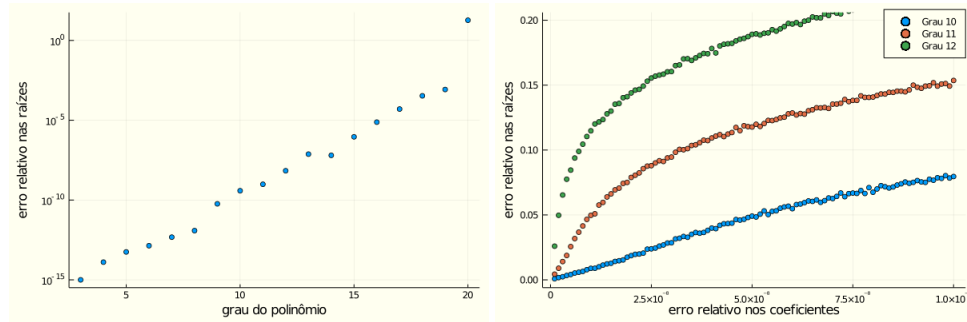


FIGURA 1. Esquerda: erro nas raízes calculadas do polinômio pérfido em função do grau. Direita: erro nas raízes calculadas do polinômio pérfido de grau 10, com perturbações aleatórias dos coeficientes.

```
[3]: 10-element Array{Float64,1}:
 0.999999999999995
 2.000000000000165
 2.999999999983562
 4.000000000107472
 4.99999999494381
 6.000000001506791
 6.99999997320477
 8.00000002751277
 8.9999999849376
10.00000000340687
```

A solução parece quase correta. Mas conhecemos a solução exata, e podemos conferir o erro relativo:

```
[4]: abs.(x-Vector{1.0:10})./abs.(x)
```

```
[4]: 10-element Array{Float64,1}:
 4.9960036108134543e-14
 8.248957072958108e-13
 5.479320700896712e-12
 2.686806332902167e-11
 1.011237316208677e-10
 2.5113185598819673e-10
 3.827890387083582e-10
 3.4390956737236737e-10
 1.6736005177105045e-10
 3.406874782169673e-11
```

Esses valores são grandes para contas em precisão dupla. O erro relativo de cada operação aritmética em precisão dupla é de no máximo $2^{-53} \simeq 10^{-16}$. A acurácia do resultado é discutível. A seguir, vamos ver como o erro relativo nas soluções varia em função do grau do polinômio:

```
[5]: erro=zeros(1,20)
for d=1:20
    p=fromroots(1:d)
    y=roots(p)
    erro[d]=maximum(abs.(y-Vector{1:d})./abs.(y))
end
erro
```

```
[5]: 1x20 Array{Float64,2}:
      0.0  0.0  9.99201e-16  1.28786e-14  ...  0.000338283  0.000843383  18.4336
```

O resultado do experimento aparece na figura 1(esq). Notamos que o erro cresce rapidamente em função do grau. O seguinte experimento mostra que a dificuldade em se resolver polinômios péfidos não é um problema do software ou do algoritmo: vamos introduzir perturbações aleatórias dos coeficientes. O resultado para $d = 10$, $0 < \epsilon \leq 10^{-7}$ com 1000 repetições é mostrado na figura 1(dir). Quando $\epsilon \rightarrow 0$, a derivada do erro nas raízes se aproxima de uma função linear do erro nos coeficientes. O coeficiente diretor dessa reta é chamado de *número de condicionamento* e é um invariante do problema, e é independente do algoritmo utilizado.

```
[17]: function erro_relativo(d::Integer,epsilon)
      p=fromroots(1:d)
      erro_entrada=randn(d+1)*epsilon
      q=Polynomial(coeffs(p).*(ones(d+1)+erro_entrada))
      y=roots(q)
      return maximum(abs.(y-Vector{Complex{Float64}}(1:d))./abs.(y))
    end
```

```
[17]: erro_relativo (generic function with 1 method)
```

```
[18]: function erro_relativo_médio(d::Integer, epsilon, vezes::Integer)
      e=0 ;
      for i=1:vezes
          e+=erro_relativo(d,epsilon)
      end
      return e/vezes
    end
```

```
[18]: erro_relativo_médio (generic function with 1 method)
```

2. Ponto flutuante

Computadores digitais representam números (inteiros ou “reais”) por uma lista finita de zeros e uns (bits). O padrão usual em computadores digitais é o *IEEE-754*(Fig. 2), que prevê um modo de *precisão simples* e um modo de *precisão dupla*. Processadores compatíveis com o padrão Intel (pentium, etc...) possuem ainda um modo de *precisão dupla estendida*.

O padrão *IEEE-754* prevê uma aritmética *corretamente arredondada*, o que quer dizer que o resultado de cada operação aritmética individual é arredondado corretamente para o número representável mais próximo.

Existe uma razão para fazer contas em ponto flutuante e não com precisão absoluta (números inteiros ou racionais). Os coeficientes de números racionais podem dobrar de tamanho (número de bits) a cada multiplicação ou soma. Um fato análogo ocorre com números algébricos, disponíveis em pacotes de álgebra simbólica. Isso torna contas exatas extremamente lentas, o que inviabilizaria o uso de computadores para a maioria dos problemas numéricos.

Entender o sistema de representação *IEEE-754/854* é crucial para quem quer elaborar programas de computador confiáveis. Há relatos de eventos catastróficos relacionados ao mau uso da aritmética¹.

¹<http://www.youtube.com/watch?v=kYUrqdUyEpI>

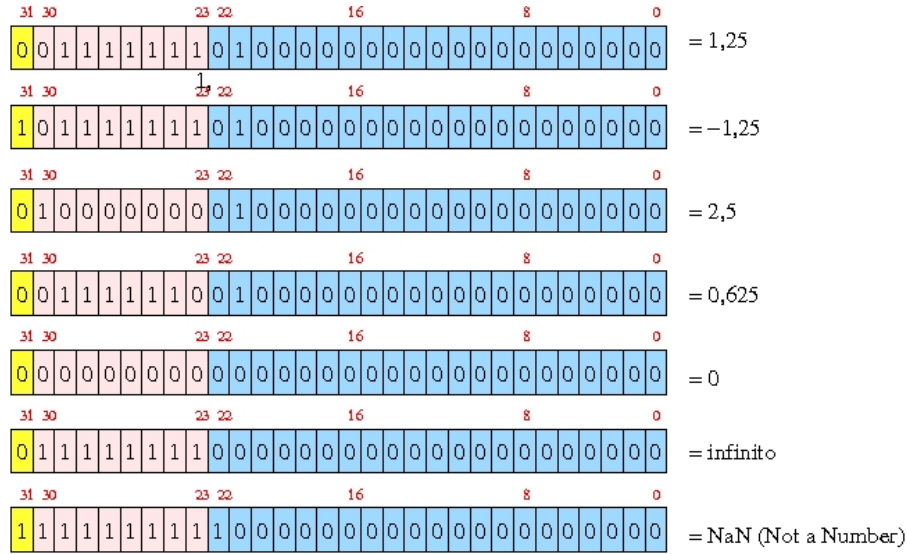


FIGURA 2. Representação de números de precisão simples no formato *IEEE-754*. Um bit é reservado para o sinal (0 positivo, 1 negativo). Oito bits são reservados para o expoente (que é acrescido de 127). Os outros bits são reservados à mantissa (mas um 1 está implícito antes da vírgula). Campos de expoente com valores 0, 254 e 255 indicam valores excepcionais.

Um estudo detalhado da aritmética de ponto flutuante e das implementações dos algoritmos numéricos de álgebra linear escapa (em muito) do escopo deste texto. O objetivo desta discussão é apenas explicar o motivo pelo qual temos que conviver com um erro quase infinitesimal a cada operação aritmética efetuada pelo computador.

Para certos problemas numéricos (como a solução do polinômio pérfido), esses erros numéricos podem se acumular ou ser magnificados ao ponto de inviabilizar as contas.

3. Condicionamento

De maneira geral, podemos assimilar a maioria dos problemas numéricos de dimensão finita ao cálculo de uma função implícita: dado um valor de A , achar $y(A)$ tal que

$$\Phi(A, y(A)) = 0$$

O vetor A representa os coeficientes do problema numérico. Vamos nos referir a A como vetor independentemente de ele representar os coeficientes de uma matriz, de um polinômio ou de outra entidade qualquer.

Estamos assumindo aqui que o vetor dos coeficientes A pertence a algum espaço linear $\mathbb{F}$. (Pode ser que para alguns valores de $A \in \mathbb{F}$, não exista solução associada).

A função Φ caracteriza o tipo de problema.

Exemplo 23.1. Dado um vetor fixo $\mathbf{b} \in \mathbb{R}^n$, e dada uma matriz A real de tamanho $n \times n$, queremos resolver $A\mathbf{y} = \mathbf{b}$. Nesse caso, fazemos $\mathbb{F} = L(n) \simeq \mathbb{R}^{n^2}$ e definimos $\Phi(A, \mathbf{y}) = A\mathbf{y} - \mathbf{b}$.

Exemplo 23.2. Para o problema de autovalores, também fazemos $\mathbb{F} = L(n) \simeq \mathbb{R}^{n^2}$, e definimos

$$\mathbb{F} = L(n) \simeq \mathbb{R}^{n^2} \quad \Phi(A, y) = \det(A - yI)$$

com $y \in \mathbb{C}$. Podemos especificar que queremos todas as soluções.

Para estudar a sensibilidade da solução ao valor dos coeficientes, linearizamos o efeito de uma perturbação infinitesimal: seja $A(t) = A + t\dot{A}$ e seja $y(t)$ solução de $\Phi(A(t), y(t)) = 0$. Derivando para $t = 0$, temos:

$$\frac{\partial \Phi}{\partial A} \dot{A} + \frac{\partial \Phi}{\partial y} \dot{y} = 0$$

Assim,

$$\dot{y} = \left(\frac{\partial \Phi}{\partial y} \right)^{-1} \frac{\partial \Phi}{\partial A} \dot{A}$$

Assumindo que A é conhecido com precisão (relativa) δ , esperamos um erro relativo em y de

$$\frac{\|\dot{y}\|}{\|y\|} \leq \frac{1}{\|\dot{y}\|} \max_{\|\dot{A}\| \leq \delta \|A\|} \left\| \left(\frac{\partial \Phi}{\partial y} \right)^{-1} \frac{\partial \Phi}{\partial A} \dot{A} \right\|$$

Que norma utilizar? No caso de y ser realmente um vetor, faz sentido utilizar a norma Euclidiana. Se A for uma matriz (como nos Exemplos 23.1 e 23.2), ainda faz sentido utilizar a norma de Frobenius e tratar os coeficientes como um vetor.

$$\frac{\|\dot{y}\|}{\|y\|} \leq \frac{\|A\|_F}{\|y\|} \left\| \left(\frac{\partial \Phi}{\partial y} \right)^{-1} \frac{\partial \Phi}{\partial A} \right\|_2 \delta$$

O número

$$\mu_{\Phi}(F, y) = \frac{\|A\|_F}{\|y\|} \left\| \left(\frac{\partial \Phi}{\partial y} \right)^{-1} \frac{\partial \Phi}{\partial A} \right\|_2$$

é chamado de *número de condicionamento*. Vamos calcular o valor do número de condicionamento para o Exemplo 23.1. Começamos por escrever Φ .

$$\begin{aligned} \Phi : L(n) \times \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ (A, \mathbf{y}) &\mapsto A\mathbf{y} - \mathbf{b} \end{aligned}$$

Derivando, obtemos:

$$\begin{aligned} \frac{\partial \Phi}{\partial A}|_{A, \mathbf{y}} : L(n) &\rightarrow \mathbb{R}^n & \frac{\partial \Phi}{\partial \mathbf{y}}|_{A, \mathbf{y}} : \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ \dot{A} &\mapsto \dot{A}\mathbf{y} & \dot{\mathbf{y}} &\mapsto A\dot{\mathbf{y}} \end{aligned}$$

Logo,

$$\begin{aligned} \left(\frac{\partial \Phi}{\partial \mathbf{y}} \right)^{-1} \frac{\partial \Phi}{\partial A} : L(n) &\rightarrow \mathbb{R}^n \\ \dot{A} &\mapsto A^{-1} \dot{A}\mathbf{y} \end{aligned}$$

A norma do operador acima é invariante pelas ações de $O(n)$ à direita e à esquerda de A :

$$\begin{aligned} a : L(n) \times \mathbb{R}^n \times \mathbb{R}^n \times O(n) &\rightarrow L(n) \times \mathbb{R}^n \times \mathbb{R}^n \\ ((A, \mathbf{y}, \mathbf{b}), V) &\mapsto (A \circ V, V^T \mathbf{y}, \mathbf{b}) \end{aligned}$$

e

$$\begin{aligned} b : O(n) \times L(n) \times \mathbb{R}^n \times \mathbb{R}^n &\rightarrow L(n) \times \mathbb{R}^n \times \mathbb{R}^n \\ (U, (A, \mathbf{y}, \mathbf{b})) &\mapsto (U \circ A, \mathbf{y}, U \circ \mathbf{b}) \end{aligned}$$

De acordo com o Teorema da Decomposição em valores singulares (Teorema 17.1), existem U e V tais que:

$$A = U \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \sigma_n \end{bmatrix} V^T$$

com $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n$. Após ação de U^T e V , o operador fica na forma padrão:

$$\left(\frac{\partial \Phi}{\partial \mathbf{y}} \right)^{-1} \frac{\partial \Phi}{\partial A} : L(n) \rightarrow \mathbb{R}^n$$

$$\dot{A} \mapsto \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \sigma_n \end{bmatrix}^{-1} \dot{A} \mathbf{y}$$

Estimamos agora

$$\left\| \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \sigma_n \end{bmatrix}^{-1} \dot{A} \mathbf{y} \right\|_F \leq \sigma_n^{-1} \|\dot{A}\|_2 \|\mathbf{y}\| \leq \sigma_n^{-1} \|\dot{A}\|_F \|\mathbf{y}\|$$

Escolhendo $\dot{A} = \frac{1}{\|\mathbf{y}\|} \mathbf{e}_n \mathbf{y}^T$ (cuja norma de Frobenius é $\|\dot{A}\|_F = 1$), obtemos que a igualdade é estrita. Assim,

$$\mu_\Phi(A, \mathbf{y}) = \|A\|_F \sigma_n^{-1} = \frac{\sqrt{\sum \sigma_j^2}}{\sigma_n}$$

O número de condicionamento é **infinito** se e somente se $\det(A) = 0$. O seguinte resultado interpreta o número de condicionamento como a inversa de uma distância. Multiplicamos A por uma constante conveniente, de maneira a ter $\|A\|_F = 1$. O seguinte Teorema ficar para os exercícios:

Teorema 23.3 (Eckart e Young). *Seja A uma matriz $n \times n$, com $\|A\|_F = 1$. Então*

$$\mu_\Phi(A) = \left(\min_{\det(T)=0} \|T - A\|_F \right)^{-1}$$

4. Exercícios

Exercício 23.1. Baixe uma das versões do programa *paranoia* de W. Kahan (www.netlib.org), e verifique a compatibilidade da aritmética de ponto flutuante do seu computador com o padrão IEEE-754 (tanto para precisão simples quanto para precisão dupla).

Exercício 23.2. Seja A uma matriz 3×3 , inversível, com coeficientes inteiros de valor absoluto não maior do que $H \in \mathbb{N}$. Mostre que o número de condicionamento de A satisfaz:

$$\mu_\Phi(A, \mathbf{y}) \leq 18H^3.$$

Exercício 23.3. Mostre o Teorema de Eckart e Young (Teorema 23.3).

Exercício 23.4. Mostre que o número de condicionamento de um polinômio f de grau d na solução x é $\frac{\|f\| \max(|x|^d, 1)}{|f'(x)|}$.

Exercício 23.5. Deduza do exercício anterior que se o polinômio mônico f tiver coeficientes inteiros de valor absoluto não maior do que $H \in \mathbb{N}$ e x for uma raiz simples, então seu número de condicionamento em x satisfaz

$$\mu(f) \leq (dH)^d \sqrt{d+1}$$

Exercício 23.6. Calcule o número de condicionamento do polinômio pérfido de grau dez.

Exercício 23.7. Introduzindo perturbações aleatórias e pequenas nos coeficientes, estime o condicionamento do ‘controlador’ do exercício 21.4 em função dos coeficientes do modelo do 707.

Exercício 23.8. Mesma pergunta, para o modelo de alocação do exercício 18.9 em função dos lucros esperados e das covariâncias.

Exercício 23.9. O objetivo deste exercício é estudar a dependência dos autovalores de uma matriz simétrica em função dos coeficientes. Para isso, escrevemos:

$$S + t\dot{S} = Q(t)\Lambda(t)Q(t)^T,$$

onde $\dot{S}$ é uma matriz simétrica. Mostre que se os autovalores de S são diferentes dois a dois, então existem $\dot{Q}$ e $\dot{\Lambda}$ únicas tais que

$$\frac{\partial}{\partial t}_{t=0} S + t\dot{S} = \frac{\partial}{\partial t}_{t=0} \left((Q(0) + t\dot{Q})(\Lambda(0) + t\dot{\Lambda})(Q(0) + t\dot{Q})^T \right).$$

Escreva explicitamente $\dot{\Lambda}$ e $\dot{Q}$. Assumindo $\Lambda(t)$ e $Q(t)$ diferenciáveis, o que é que isso implica sobre o condicionamento dos autovalores de uma matriz simétrica? O que acontece com os autovetores?

Nota: a diferenciabilidade de $\Lambda(t)$ e $Q(t)$ segue do Teorema da Função Implícita em várias variáveis, que é mostrado no curso de Cálculo Avançado ou de Análise no $\mathbb{R}^n$.

Exercício 23.10. E

stude numericamente a estabilidade do maior autovalor da matriz identidade I de tamanho 3×3 , quando submetida a uma perturbação simétrica pequena. Mesma pergunta para o maior autovalor da matriz

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

quando submetida a uma perturbação pequena, não necessariamente simétrica. Compare.

CAPÍTULO 24

Processamento de sinais, MP₃, JPEG e MPEG

1. Sinais sonoros



som que ouvimos corresponde a variações de pressão nos nossos tímpanos, que são capturados e transformados em um sinal nervoso no nosso ouvido interno. Podemos capturar um sinal sonoro com um microfone, e o sinal elétrico analógico pode ser gravado, transmitido, reproduzido e retransformado em sinal sonoro.

Hoje em dia preferimos armazenar som sob forma digital. Para isso, o sinal elétrico produzido por um microfone pode ser digitalizado por um conversor analógico-digital. O circuito de áudio dos computadores modernos tem um conversor embutido. É fácil ler o microfone, desde que você esteja com todos os pacotes necessários instalados (ver nota no final deste capítulo).

```
[3]: function grava(segundos::Int64)
    nome=tempname()*".wav"
    run(`arecord -d$segundos -fFLOAT_LE -twav $nome`)
    s=wavread(nome)
    t=SampleBuf(s[1],s[2])
    @printf("Lido sinal com %d canais a %d Hz",nchannels(t),samplerate(t))
    return t
end
```

```
[3]: grava (generic function with 1 method)
```

```
[7]: sinal=grava(10)
```

```
Recording WAVE '/tmp/jl_mZfe3c.wav' : Float 32 bit Little Endian, Rate 8000 Hz, Mono
```

```
Lido sinal com 1 canais a 8000 Hz
```

```
[7]: 80000-frame, 1-channel SampleBuf{Float64, 2}
10.0s sampled at 8000.0Hz
```

Para gravar música em qualidade de CD, precisamos de 44,100 leituras por segundo, vezes dois canais. Para armazenar uma hora de música, precisaríamos armazenar um vetor de $\mathbb{R}^{318 \times 10^6}$. Guardando dois bytes por coordenada, precisaremos de aproximadamente 600 MB, que é o tamanho dos atuais CDs.

Um método de compressão possível (utilizado em redes de telefonia) é aplicar uma escala logarítmica à intensidade do sinal, e armazenar utilizando menos *bits* (por exemplo, 8). Por exemplo, de x é um sinal sonoro, a codificação de x pela

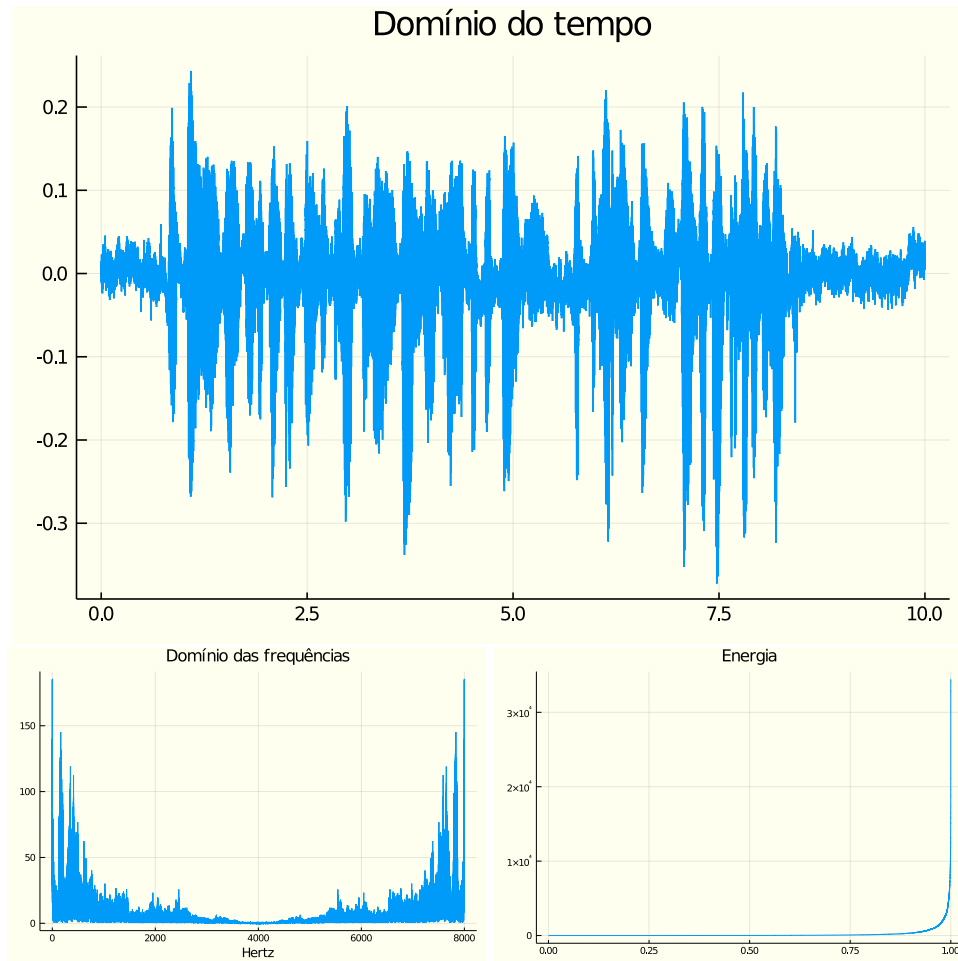


FIGURA 1. Sinal sonoro de 10 segundos. Embaixo: o sinal no domínio da frequência, e a energia (quadrado de cada coordenada) em ordem crescente.

chamada $\mu - law$ ou $u - law$ é definida por:

$$y_i = \frac{\text{sinal}(|x_i|)}{\ln(1 + \mu)} \ln \left(1 + \mu \frac{|x_i|}{\max(|x_j|)} \right)$$

onde $\mu = 255$. Esse método é (apenas) razoável para comunicações telefônicas.

2. A transformada de Fourier

Denotamos por $L^2([0, 1])$ o espaço de todas as funções a valores complexos, definidas para $t \in [0, 1]$, integráveis e com quadrado integrável. Se temos um sinal (função real) f definido no intervalo de tempo $[0, 1]$, podemos considerar ele como um elemento de $L^2([0, 1])$. O produto interno de duas funções f e g em $L^2([0, 1])$ é

$$\langle f, g \rangle = \int_0^1 \bar{f}(t)g(t) dt.$$

Note que esse produto está bem definido em $L^2([0, 1])$. A *transformada de Fourier* de f é definida por:

$$\hat{f}(s) = \int_0^1 f(t) e^{-2\pi i s t} dt$$

para $s \in \mathbb{Z}$. Uma definição equivalente é

$$\hat{f}(s) = \langle t \mapsto e^{-2\pi i s t}, t \mapsto f(t) \rangle .$$

A transformada de Fourier pode ser interpretada como uma aplicação linear de $L^2([0, 1])$ no espaço $l^2(\mathbb{Z})$, que é o espaço de todas as bisequências $(\hat{f}_s)_{s \in \mathbb{Z}}$ a valores complexos com “norma Euclidiana” $\|\hat{f}\| = \sqrt{\sum_{s \in \mathbb{Z}} |\hat{f}_s|^2}$ finita. Esse espaço admite o produto interno

$$\langle \hat{f}_s, \hat{g}_s \rangle = \sum_{s \in \mathbb{Z}} \hat{f}_s \overline{\hat{g}_s} .$$

Prova-se ainda que vale a seguinte fórmula de reconstrução:

$$f(t) = \sum_{s \in \mathbb{Z}} e^{2\pi i s t} \hat{f}(s) .$$

Nesse sentido, diz-se que o conjunto das funções $t \mapsto e^{2\pi i s t}$ é uma *base* do espaço $L^2([0, 1])$.

Observação 24.1. A definição usual de combinação linear, nos textos de Álgebra, costuma ser a da combinação linear finita. Em análise de Fourier ou processamento de sinais, assume-se que uma combinação linear é qualquer soma ou integral, com norma Euclidiana dos coeficientes (ou integral do valor absoluto do módulo da função-coeficiente) limitada.

Note também que

$$\|t \mapsto e^{2\pi i s t}\|^2 = \int_0^1 1 dt = 1$$

e que, para $s_1 \neq s_2$ inteiros,

$$\langle t \mapsto e^{2\pi i s_1 t}, t \mapsto e^{2\pi i s_2 t} \rangle = \int_0^1 e^{2\pi i t(s_2 - s_1)} dt = 0 .$$

Assim, $(t \mapsto e^{2\pi i s t})_{s \in \mathbb{Z}}$ é uma *base ortonormal* do espaço $L^2([0, 1])$.

Observação 24.2. Uma maneira clássica de resolver a equação do calor e a equação da onda é escrever o operador $f(x) \mapsto \frac{\partial^2}{\partial x^2} f(x)$ nessa base ortonormal. Obtemos o operador

$$\hat{f}_s \mapsto -4\pi^2 s^2 \hat{f}_s .$$

Note que esse operador tem norma infinita, e que ele é infinitamente mal condicionado. (Em geral, a derivação é mal condicionada e por isso algoritmos de diferenciação numérica são sempre problemáticos).

Vamos utilizar a base de Fourier como primeira aproximação para processamento de sinais. Mas precisaremos trabalhar com sinais discretos. A *transformada de Fourier discreta*, ou *DFT*, é definida assim: se temos um vetor $\mathbf{f}$ de $\mathbb{R}^N$ ou $\mathbb{C}^N$, o comando produz um vetor $\hat{\mathbf{f}} = \mathcal{F}(\mathbf{f})$ de $\mathbb{C}^N$ onde

$$\begin{aligned} \mathcal{F} : \mathbb{C}^N &\rightarrow \mathbb{C}^N \\ \mathbf{f} &\mapsto \hat{\mathbf{f}} = \mathcal{F}(\mathbf{f}) \text{ onde } \hat{f}_j = \sum_{k=0}^{N-1} f_k e^{-2\pi i j k / N} . \end{aligned}$$

Se o vetor $\mathbf{f}$ é discretização de um sinal de duração T , a j -ésima coordenada de $\hat{f}_j$ corresponde à frequência $\frac{\min(j, N-j)}{T}$. (Ver exercício 24.6). A transformação

linear $\frac{1}{\sqrt{N}}\mathcal{F}$ é uma transformação unitária. Tanto a transformada $\mathcal{F}$ quanto a sua inversa podem ser calculadas de maneira extremamente eficiente.

O ouvido humano consegue perceber frequências entre 20Hz e 20kHz. Se gravamos uma mensagem de 1 segundo com 8000 leituras, então perdemos totalmente as frequências mais altas (Acima de 4kHz). Isso é perceptível na qualidade do sinal, mas não prejudica a sua compreensão. Vamos olhar para o espectro das frequências do sinal (Figure 1). Aparentemente, a norma do sinal está concentrada em algumas poucas coordenadas. Isso pode ser visto ordenando as coordenadas da transformada por valor absoluto, e plotando os quadrados. Deste modo, podemos comprimir o sinal truncando as menores coordenadas, e ainda vamos obter um sinal próximo ao original na métrica L^2 . As seguintes linhas mostram um processo rudimentar de compressão. Dividimos o sinal no tempo em intervalos de 0.2s, para depois aplicar a transformada discreta de Fourier e conservar apenas as coordenadas maiores em valor absoluto.

```
[10]: function comprime_fft(entrada::SampleBuf, quanto::Float64)

    if nchannels(entrada) != 1
        erro("Esta rotina só trabalha com um canal")
    end

    freq=samplerate(entrada)
    h=0.2
    por_quadro=Int(floor(freq*h))
    num_quadros=Int(floor(size(entrada,1)/por_quadro))

    k1=Int(round((por_quadro)*quanto))
    saída=0*entrada

    for quadro=1:num_quadros
        q1=1+(quadro-1)*por_quadro ;
        q2=quadro*por_quadro;

        transformada=fft(entrada[q1:q2,1])
        I=sortperm(abs.(transformada[:,1]),rev=true)
        truncada=0.0*transformada
        for k=1:k1
            truncada[I[k],1]=transformada[I[k],1] ;
        end
        saída[q1:q2,1]=real.(ifft(truncada))
    end
    return saída
end
```

A “remasterização” de gravações antigas é um processo similar. Muitas vezes o chiado corresponde a ruído branco, sem concentração em frequências definidas. A diferença é que não precisamos de uma taxa de compressão constante. Veremos que existem outras técnicas mais modernas de tratamento de sinais, e a escolha exata do algoritmo pode depender também de fatores estéticos ou da música a ser recuperada.

3. A base de Haar

A transformada de Fourier não é a única maneira razoável de se representar um sinal. Uma das grandes desvantagens da transformada de Fourier é que ela

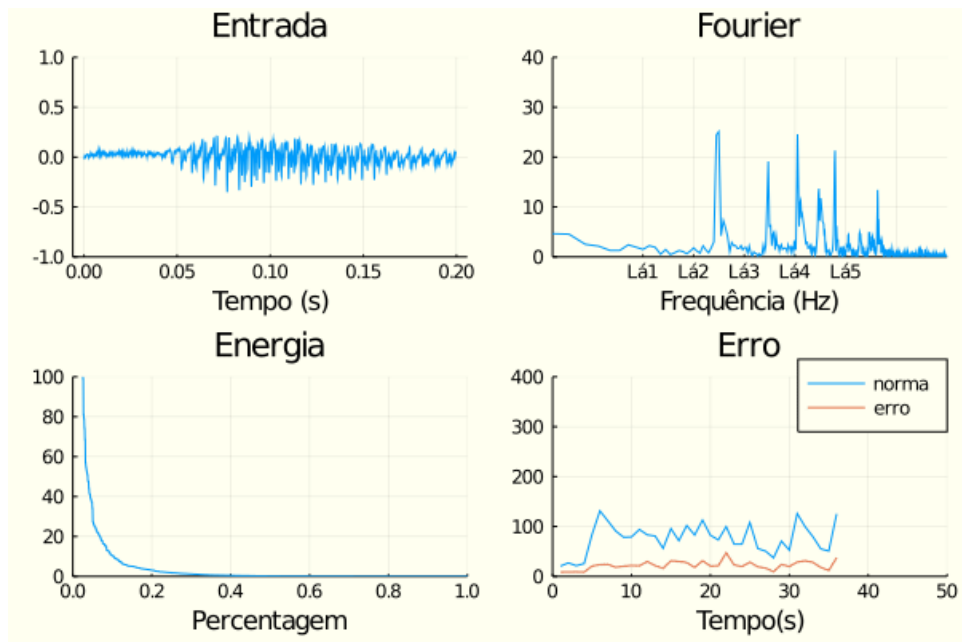


FIGURA 2. Compressão, usando fft, do sinal sonoro previamente gravado (janela de 0.2s).

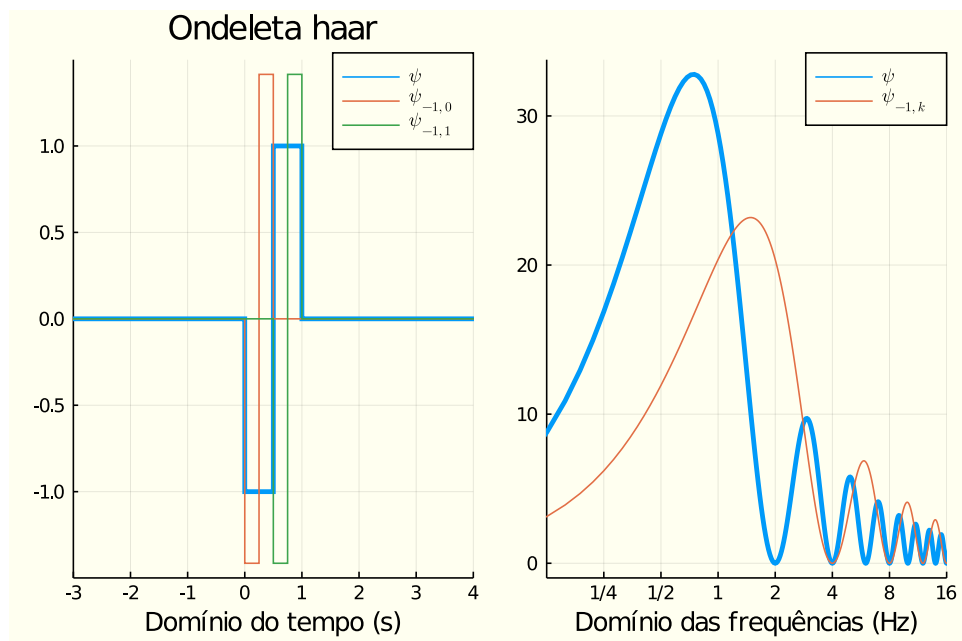


FIGURA 3. Função de Haar, e ondeletas “filhas” .

representa “mal” transientes ou “picos” de um sinal. Isso quer dizer que um transiente, transformado pela transformada de Fourier, não pode facilmente ser comprimido.

Mesmo quando se utiliza a transformada de Fourier de curto prazo, o tamanho da “janela” é fixo, e transientes com duração muito inferior a esse tamanho

serão mal representados. A transformada de Haar é uma maneira razoável de representar sinais com transientes.

A função de Haar (Fig. 3) é definida por:

$$H: \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto H(x) = \begin{cases} 0 & \text{Se } x < 0 \\ 1 & \text{Se } 0 \leq x < 1/2 \\ -1 & \text{Se } 1/2 \leq x < 1 \\ 0 & \text{Se } x > 1. \end{cases}$$

A base de Haar que utilizaremos para representar funções em $L^2([0, 1])$ será composta de dilatações e translações de H . Definimos

$$H_{m,n}(t) = 2^{-m/2} H(2^{-m}t - n)$$

onde $-m \in \mathbb{N}$ e $n = 0, \dots, 2^{-m} - 1$. O fator multiplicativo $2^{-m/2}$ garante que o conjunto das $H_{m,n}$ seja ortonormal. Para geral o espaço $L^2([0, 1])$ inteiro, definiremos ainda $H_{0,0}(t) \equiv 1$. Mostra-se que os H_{mn} formam uma base ortonormal de $L^2([0, 1])$.

A transformada de Haar de uma função real f é definida por:

$$T_{\text{Haar}}f(m, n) = \int_0^1 H_{m,n}(t)f(t) dt.$$

No caso de uma mensagem discreta, é conveniente assumir que o número de leituras é potência de dois. Por exemplo, se temos 8 leituras, a mensagem é um vetor de $\mathbb{R}^8$ e a base de Haar é dada pelas colunas da matriz

$$H_3 = \begin{bmatrix} \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{1}{2} & 0 & \frac{\sqrt{2}}{2} & 0 & 0 & 0 \\ \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{1}{2} & 0 & -\frac{\sqrt{2}}{2} & 0 & 0 & 0 \\ \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{1}{2} & 0 & 0 & \frac{\sqrt{2}}{2} & 0 & 0 \\ \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & -\frac{1}{2} & 0 & 0 & -\frac{\sqrt{2}}{2} & 0 & 0 \\ \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & 0 & \frac{1}{2} & 0 & 0 & \frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & 0 & \frac{1}{2} & 0 & 0 & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & 0 & -\frac{1}{2} & 0 & 0 & 0 & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & 0 & -\frac{1}{2} & 0 & 0 & 0 & -\frac{\sqrt{2}}{2} \end{bmatrix}.$$

As matrizes H_n (ou matrizes de Haar) assim construídas são ortogonais.

4. O ouvido humano e a transformada de ondeletas

A cóclea é o órgão responsável pela audição humana. O sinal sonoro é amplificado mecanicamente no tímpano, e se propaga em meio líquido no interior da cóclea (Ver figura 4).

O órgão de Corti, dentro da cóclea, está recoberto de células ciliares, que fazem a transição para o nervo auditivo. Há dois tipos de células ciliares. As curtas, ou estereocílios, ao se deslocar por força do sinal sonoro, abrem canais iônicos pelos quais estimulam (ou desestimulam) os terminais do nervo auditivo. Por conta desse mecanismo, o sinal nervoso gerado por cada estereocílio é localizado no tempo.

As células ciliares longas ou quinecílios entram em ressonância com o sinal sonoro, amplificando-o. A frequência de vibração dos quinecílios é afetada por sinais nervosos. Assim, o ouvido “sintoniza” as principais frequências recebidas em determinado momento.

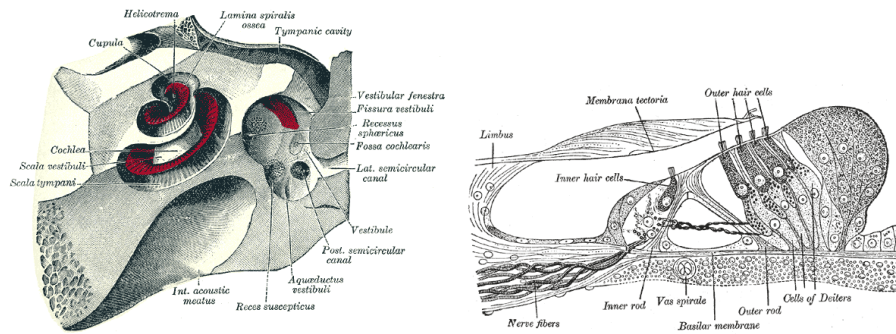


FIGURA 4. Cóclea e órgão de Corti. Wikimedia Commons, Gray923.png, digitalização da *Gray's Anatomy of the Human Body* (1918), domínio público.

Cada seção da cóclea corresponde a uma certa faixa de frequências. Dessa forma, a cóclea já “decompõe” o sinal em frequências, e os quinecílios fazem a sintonia fina.

As bases de ondeletas tentam imitar o processo acima. A compressão por transformada de ondeletas (*wavelets*) trunca exatamente a parte do sinal sonoro que nós não ouvimos. Exemplos de ondeletas-mãe estão ilustrados na figura 5. A base de ondeletas é gerada a partir da ondeleta-mãe da mesma maneira do que a base de Haar:

$$\psi_{m,n}(t) = 2^{-m/2} \psi(2^{-m}t - n) .$$

Existe hoje uma quantidade absurda de bases de ondeletas disponíveis. Em processamento de sinais, utilizam-se “pacotes” de ondeletas, que são conjuntos geradores do espaço das funções (os vetores da “base” não precisam ser linearmente independentes). Essa é uma das motivações para a Proposição ??.

5. O padrão MP3 e os CODECS

O padrão MP3 ou *MPEG-1 Audio Layer 3* está baseado em um modelo psicoacústico. Vimos na seção anterior que os quinecílios no órgão de Corti “sintonizam” as principais frequências do sinal sonoro.

Se o ouvido está sintonizado em uma certa gama de frequências (por exemplo, as utilizadas em uma composição musical), sinais relativamente fracos em frequências vizinhas não encontram ressonância, pois os quinecílios correspondentes estão nas frequências principais. Por isso, deixamos de perceber essa parte do sinal.

A compressão MP3 utiliza esse fato. O sinal é primeiro dividido em pequenos intervalos de tempo, cada um correspondendo a 1152 leituras para cada canal de áudio.

A primeira etapa da codificação é feita pelo chamado *filtro de quadratura poli-fase*. O som em cada intervalo é dividido por frequências em 32 bandas.

Simultaneamente, o som sofre uma transformada de Fourier discreta e é analisado pelo modelo psicoacústico. Esse modelo permite eliminar as frequências não audíveis (escondidas por sinais de maior intensidade em frequências na mesma banda) e realçar sinais que exigem maior resolução no domínio do tempo.

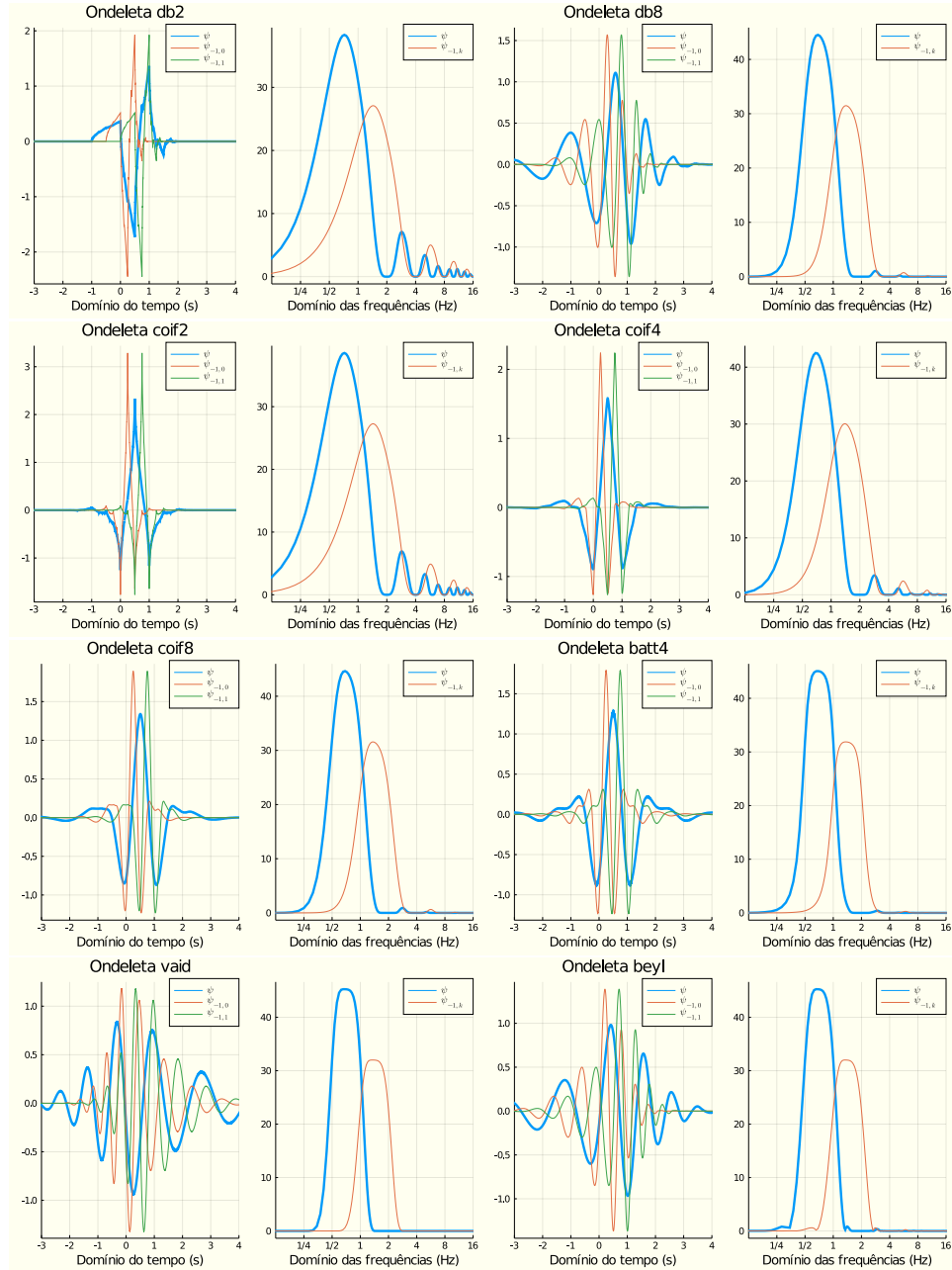


FIGURA 5. Exemplos de ondeletas: Daubechies (db), coiflets(coif), Battle-Lemarie(batt), Vaidyanathan(vaid), Beylkin(beyl).

Mais uma transformada de Fourier (de fato, transformada do cosseno) é aplicada a cada uma das 32 bandas, dividindo cada banda em 18 frequências. Os parâmetros dessa última transformada são fornecidos pelo modelo psicoacústico.

Depois disso, o sinal é discretizado (ainda sob controle do modelo psicoacústico) e os valores discretos são comprimidos pelo código de Huffman (Ver exercícios 24.8–24.10).



FIGURA 6. Enseada de Botafogo, e decomposição no espaço de cores YCbCr. O canal Y é uma média ponderada dos canais R,G e B. Os Canais Cb e Cr (compensation blue e compensation red) essencialmente capturam B-G e R-G.

Os detalhes da codificação são extremamente complicados, e não são definidos pelo padrão MP3. O que o padrão define é a decodificação.

Mais detalhes podem ser encontrados em <http://www.mp3-tech.org>. Em particular, sugiro o artigo de Rassol Raissi, *The theory behind MP3*, Dezembro de 2002.

Existe uma quantidade enorme de padrões de áudio e vídeo disponíveis. Como é impossível escrever um programa capaz de ler todos os padrões existentes, os codificadores/decodificadores (os *codec* infames) podem ser distribuídos a parte. Por exemplo, MP3 e Vorbis são padrões definidos por *codec*.

O padrão MP3 é hoje um padrão industrial dominante. Tem a desvantagem de ser protegido por patentes. O padrão Vorbis tem a vantagem de ser software livre. O algoritmo é aparentemente mais simples, e inclui uma transformada discreta do cosseno e a codificação em separado do “ piso ” e do resíduo. O piso é uma função linear por partes que aproxima o espectro do sinal em um dado intervalo de tempo. O resíduo é a diferença entre o espectro e o piso. Resíduo e espectro são depois truncados e armazenados via código de Huffman (Ex. 24.8–24.10).

6. Compressão de imagem e de vídeo

A compressão de imagens e de vídeos é potencialmente muito mais complicada do que a compressão de áudio.

Por exemplo, a compressão no padrão *JPEG* segue os seguintes passos: em primeiro lugar, as cores são codificadas no espaço de cores *YCbCr* (Figura 6. O olho humano é mais sensível ao lume *Y* do que à cor (representada por *Cr* e *Cb*). Assim, a cor é truncada. A partir deste momento, cada sinal (*Y*, *Cr* e *Cb*) é tratado separadamente.

Cada um dos canais *Y*, *Cr* e *Cb* é dividido em blocos de 8×8 píxeis. Cada bloco é então objeto de uma transformada discreta do cosseno bidimensional.

O resultado é uma descrição de cada bloco por 8×8 “bifrequências”. Nossos olhos são mais sensíveis às baixas do que às altas “frequências”. Por isso, a precisão utilizada para as baixas frequências é muito maior do que a das altas frequências, que são truncadas. Depois disso, o sinal é discretizado e codificado com código de Huffman.

7. A televisão digital.

O padrão *MP4* (aliás *MPEG-4* Parte 14) é na verdade um meta-padrão, com vários *codec* de áudio e vídeo disponíveis. Por exemplo, o *H.264* (também conhecido como *MPEG-4* Parte 10, ou ainda *AVC*) é o *codec* mais popular para a compressão de vídeo, e é usado pelo padrão *ISDB-T* internacional da televisão digital Brasileira. No padrão *H.264*, cada quadro de vídeo (imagem) é dividida em blocos (4×4 , 8×8 ou 16×16 píxeis). O algoritmo básico de codificação é a aplicação de uma transformada discreta do cosseno bidimensional (mesma estratégia do que no *JPEG*), e os resultados são truncados.

Para se obter uma compressão significativamente melhor do que a do *JPEG*, o padrão *H.264* permite codificar cada bloco nos modos *intra* e *inter*. No modo *intra*, cada bloco comprimido é comparado com outros blocos já codificados. Apenas a diferença precisa ser armazenada.

No modo *inter*, o bloco é armazenado como combinação de blocos de quadros já armazenados. Um vetor de deslocamento pode ser utilizado para comprimir objetos em movimento¹. É importante notar que a codificação é um processo muito mais complicado do que a descodificação, e que produzir um código *H.264* otimizado pode demandar recursos computacionais significativos.

8. Conclusões

Assim, vemos que uma das peças fundamentais em processamento de sinais é a aplicação de transformações ortogonais ao espaço de sinais. Transformações ortogonais preservam o produto interno do espaço de sinais (é um *grupo* de transformações que preserva a *geometria* desse espaço). Elas não amplificam ruídos no sinal.

Existem algoritmos extremamente rápidos para calcular as transformações mais usuais (*fft* e assemelhadas, e transformada de ondeletas) em tempo real. Esses algoritmos funcionam como uma decomposição da transformada em transformadas mais simples.

Se escolhermos a base certa, podemos obter uma boa compressão (ou uma boa filtragem) do sinal por meio de uma projeção ortogonal (que também não amplifica ruídos). Aqui descrevemos algumas peças fundamentais. Mas a escolha da base depende de uma boa modelagem do processo acústico ou visual, que é não-linear.

¹Richardson, Iain: Vcodex (página internet) <http://www.vcodex.com>

9. Exercícios

Exercício 24.1. Escreva a matriz de $\mathcal{F}$.

Exercício 24.2. Mostre que $\frac{1}{\sqrt{N}}\mathcal{F}$ é unitária.

Exercício 24.3. Mostre que $\mathcal{F}^2 = -N$

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Exercício 24.4. Mostre que a transformada discreta do cosseno do sinal f é proporcional à transformada discreta de Fourier do sinal

$$g = [0 \ f_1 \ 0 \ f_2 \ 0 \cdots f_T \ 0 \ f_T \ 0 \cdots f_2 \ 0 \ f_1 \ 0] .$$

Exercício 24.5. Dado um sinal f de 2^m leituras, mostre que a sua transformada de Haar pode ser calculada em tempo $O(n)$. Dica: em uma primeira passagem, separe as “altas frequências” $T_{\text{Haar}}f(2^m, n)$ das “baixas frequências”, representadas por um vetor de $\mathbb{R}^{2^{m-1}}$. Continue recursivamente.

Exercício 24.6. No topo da Figura ??

, explique por quê aparecem frequências acima de 500, e por que motivo essa transformada de Fourier parece simétrica.

Exercício 24.7. Reproduza o experimento de compressão de sinal de voz, só que utilizando a base de Haar e não a base de Fourier. Como se comparam o resultados ?

Exercício 24.8. Uma árvore binária é um grafo sem ciclos, com um vértice privilegiado chamado de raiz, e tal que todo vértice tem grau 1 (e nesse caso é chamado de *folha*) ou grau 3.

- Desenhe todas as árvores binárias com 4 folhas
- Seja $\mathbf{p} \in \mathbb{R}^n$ um vetor de probabilidade: $p_i \geq 0$ e $\sum p_i = 1$. Mostre que existe uma árvore binária contendo folhas numeradas 1 a n , e tal que o comprimento do caminho entre a raiz e a i -ésima folha seja menor ou igual do que $\lceil -\log_2 p_i \rceil$. Dica: seja $I_j = \{x : 2^{-j} \leq x < 2^{-j+1}\}$. O que acontece quando no máximo um dos p_i 's está em cada I_j ?

Exercício 24.9. Nas hipóteses do exercício anterior, mostre como associar a todo caminho de comprimento c (saindo da raiz e chegando em uma folha i) uma sequência binária única $s(i)$ de $c(i)$ dígitos, e com a seguinte propriedade:

Se x é uma variável aleatória discreta assumindo o valor i com probabilidade p_i , mostre que $E(c(x)) \leq -\sum p_i \log_2 p_i$. O número da direita é chamado de *entropia* do vetor de probabilidade $\mathbf{p}$.

Exercício 24.10. Mostre como codificar um sinal discreto aleatório $\mathbf{x} \in \{1, \dots, n\}^N$ como uma sequência binária, tal que se $p_i = \text{Prob}[x = i]$, então o valor esperado do tamanho da sequência codificada é menor ou igual do que a entropia de $\mathbf{p}$, vezes o comprimento N da mensagem original. (Assuma o vetor $\mathbf{p}$ conhecido do codificador e do decodificador). O código construído acima é o *código de Huffman* utilizado para compressão de mensagens discretas.

Nota computacional

Os exemplos neste capítulo dependem de alguns pacotes do Julia. Se eles estiverem instalados, podem ser invocados com:

```
[1]: using FileIO
      using LibSndFile
      using SampledSignals
      using LinearAlgebra
      using Plots
      using FFTW
      using Wavelets
      using WAV
      using Printf
      using LaTeXStrings
```

Em caso de erro, é preciso seguir as instruções e instalar os pacotes. A solução que eu apresento para ler o microfone é pouco elegante, mas resolve o problema até os pacotes de audio contarem com uma primitiva correspondente.

CAPÍTULO 25

Tensores



vetores, covetores, endomorfismos e formas bilineares são exemplos de tensores. Tensores de ordem maior aparecem em várias situações. Por exemplo, algoritmos eficientes para a multiplicação matricial dependem de certas propriedades de uma família de tensores de ordem 3. Veremos também aplicações à estatística e à ciência de dados.

1. Introdução

Sejam $\mathbb{E}$ e $\mathbb{F}$ espaços vetoriais reais de dimensão finita. Aprendemos no exercício 1.2 do capítulo 1 que $\mathbb{E} \otimes \mathbb{F}$ é o espaço vetorial gerado por todas as expressões da forma $\mathbf{e} \otimes \mathbf{f}$ onde $\mathbf{e} \in E$, $\mathbf{f} \in F$ e a operação $\otimes$ é bilinear e associativa. Existe também uma definição abstrata.

Definição 25.1. $\mathbb{E} \otimes \mathbb{F}$ e $\pi : E \times F \rightarrow \mathbb{E} \otimes \mathbb{F}$ são o espaço vetorial e a função bilinear com a seguinte propriedade: para toda função bilinear $B : \mathbb{E} \times \mathbb{F} \rightarrow \mathbb{G}$, existe uma única decomposição $B = b \circ \pi$ como abaixo:

$$\begin{array}{ccc} \mathbb{E} \times \mathbb{F} & \xrightarrow{\pi} & \mathbb{E} \otimes \mathbb{F} \\ & \searrow B & \downarrow b \\ & & \mathbb{G} \end{array}$$

O espaço $\mathbb{E} \otimes \mathbb{F}$ pode sempre ser construído, e está definido a menos de um isomorfismo. No caso particular $\mathbb{E} = \mathbb{R}^m$ e $\mathbb{F} = \mathbb{R}^n$, $\mathbb{E} \otimes \mathbb{F} = \mathbb{R}^{mn}$ e podemos representar elementos de $\mathbb{E} \otimes \mathbb{F}$ como matrizes $m \times n$.

Definição 25.2. Seja $\mathbb{E}$ um espaço vetorial real de dimensão finita. Seja $k, l \in \mathbb{N}_0$. Um *tensor* k -contravariante e l -covariante em $\mathbb{E}$ é uma aplicação linear

$$\mathcal{T} : \underbrace{\mathbb{E} \otimes \cdots \otimes \mathbb{E}}_{l \text{ vezes}} \rightarrow \underbrace{\mathbb{E} \otimes \cdots \otimes \mathbb{E}}_{k \text{ vezes}}.$$

Exemplo 25.3. Seja $\Phi : \mathbb{E} \rightarrow \mathbb{E}$ uma função k vezes continuamente diferenciável. Então $D^k \Phi$ é um tensor 1-contravariante, k -covariante.

Exemplo 25.4. A multiplicação matricial

$$\begin{array}{ccc} \mathcal{M}_n : \mathbb{R}^{n^2} \times \mathbb{R}^{n^2} & \rightarrow & \mathbb{R}^{n^2} \\ A, B & \mapsto & D = AB \end{array}$$

é um tensor 1-contravariante, 2-covariante.tensoror.

Exemplo 25.5. O tensor eletromagnético (ou tensor de Faraday) é um tensor 2-covariante (e 0-contravariante) no espaço-tempo.

Exemplo 25.6. Um filme é representado por um certo número N de quadros, com $m \times n$ pixels, e c canais de cores. Ou seja, é um elemento de $\mathbb{R}^{cmnN}$ e é conveniente pensar nele como um elemento de $\mathbb{R}^c \otimes \mathbb{R}^m \otimes \mathbb{R}^n \otimes \mathbb{R}^N$. Tanto para processamento de imagens quanto para compressão de vídeo, a primeira etapa de processamento é uma convolução que pode inclusive produzir um tensor de ordem maior.

2. Coordenadas

Tensores podem ser representados em coordenadas. Se $\mathbf{u}_1, \dots, \mathbf{u}_n$ é uma base de $\mathbb{E}$, podemos escrever

$$\mathcal{T}(\mathbf{u}_{\alpha_1} \otimes \dots \otimes \mathbf{u}_{\alpha_l}) = \sum_{\beta_1, \dots, \beta_l=1}^n \mathcal{T}_{\alpha_1, \dots, \alpha_l}^{\beta_1, \dots, \beta_k} \mathbf{u}_{\beta_1} \otimes \dots \otimes \mathbf{u}_{\beta_k}.$$

Nesse sistema de coordenadas, o tensor $\mathcal{T}$ é representado em coordenadas pelos coeficientes $\mathcal{T}_{\alpha_1, \dots, \alpha_l}^{\beta_1, \dots, \beta_k}$. Os índices contravariantes são escritos encima e os covariantes embaixo. É importante nesse caso entender como mudam as coordenadas em função da base escolhida. Se $\mathbf{v}_1, \dots, \mathbf{v}_n$ é outra base de $\mathcal{E}$, as duas bases se relacionam por

$$\mathbf{v}_\gamma = \sum_{\alpha=1}^n A_{\gamma}^{\alpha} \mathbf{u}_{\alpha} \quad \text{e} \quad \mathbf{u}_{\beta} = \sum_{\delta=1}^n B_{\beta}^{\delta} \mathbf{v}_{\delta}$$

onde A e B são inversas uma da outra, ou seja $\sum_{\gamma=1}^n A_{\gamma}^{\alpha} B_{\delta}^{\gamma} = I_{\delta}^{\alpha}$ e I é a matriz identidade. Para obter a fórmula de mudança de coordenadas substituímos

$$\begin{aligned} \mathcal{T}(\mathbf{v}_{\gamma_1} \otimes \dots \otimes \mathbf{v}_{\gamma_l}) &= \mathcal{T}\left(\bigotimes_{i=1}^l \sum_{\alpha_i=1}^n A_{\gamma_i}^{\alpha_i} \mathbf{u}_{\alpha_i}\right) \\ &= \sum_{\alpha_1, \dots, \alpha_l=1}^n A_{\gamma_1}^{\alpha_1} A_{\gamma_2}^{\alpha_2} \dots A_{\gamma_l}^{\alpha_l} \mathcal{T}(\mathbf{u}_{\alpha_1} \otimes \dots \otimes \mathbf{u}_{\alpha_l}) \\ &= \sum_{\substack{\alpha_1, \dots, \alpha_l=1 \\ \beta_1, \dots, \beta_l=1}}^n A_{\gamma_1}^{\alpha_1} A_{\gamma_2}^{\alpha_2} \dots A_{\gamma_l}^{\alpha_l} \mathcal{T}_{\alpha_1, \dots, \alpha_l}^{\beta_1, \dots, \beta_k} \mathbf{u}_{\beta_1} \otimes \dots \otimes \mathbf{u}_{\beta_k} \\ &= \sum_{\substack{\alpha_1, \dots, \alpha_l=1 \\ \beta_1, \dots, \beta_l=1}}^n \mathcal{T}_{\alpha_1, \dots, \alpha_l}^{\beta_1, \dots, \beta_k} A_{\gamma_1}^{\alpha_1} A_{\gamma_2}^{\alpha_2} \dots A_{\gamma_l}^{\alpha_l} \bigotimes_{j=1}^k \sum_{\delta_j=1}^n B_{\beta_j}^{\delta_j} \mathbf{v}_{\delta_j} \\ &= \sum_{\substack{\alpha_1, \dots, \alpha_l=1 \\ \beta_1, \dots, \beta_l=1 \\ \delta_1, \dots, \delta_k=1}}^n \mathcal{T}_{\alpha_1, \dots, \alpha_l}^{\beta_1, \dots, \beta_k} A_{\gamma_1}^{\alpha_1} \dots A_{\gamma_l}^{\alpha_l} B_{\beta_1}^{\delta_1} \dots B_{\beta_k}^{\delta_k} \mathbf{v}_{\delta_1} \otimes \dots \otimes \mathbf{v}_{\delta_k}. \end{aligned}$$

Finalmente deduzimos que

$$\mathcal{T}_{\gamma_1, \dots, \gamma_l}^{\delta_1, \dots, \delta_k} = \sum_{\substack{\alpha_1, \dots, \alpha_l=1 \\ \beta_1, \dots, \beta_l=1}}^n \mathcal{T}_{\alpha_1, \dots, \alpha_l}^{\beta_1, \dots, \beta_k} A_{\gamma_1}^{\alpha_1} \dots A_{\gamma_l}^{\alpha_l} B_{\beta_1}^{\delta_1} \dots B_{\beta_k}^{\delta_k}$$

que é a lei k -contravariante, l -covariante. Os resultados do Capítulo 11 são casos particulares da fórmula acima.

Vamos introduzir agora duas operações frequentes em tensores. A *contração* de dois tensores $\mathcal{T}_{\beta_1, \dots, \beta_l}^{\alpha_1, \dots, \alpha_k}$ e $\mathcal{S}_{\delta_1, \dots, \delta_o}^{\gamma_1, \dots, \gamma_m}$ em relação aos índices α_k e δ_o é dada por

$$\sum_{i=1}^n \mathcal{T}_{\beta_1, \dots, \beta_l}^{\alpha_1, \dots, \alpha_{k-1}, i} \mathcal{S}_{\delta_1, \dots, \delta_{o-1}, i}^{\gamma_1, \dots, \gamma_m}$$

e corresponde à “multiplicação” de $\mathcal{T}$ e $\mathcal{S}$ em relação aos índices escolhidos. Poderíamos usar qualquer par de índices, desde que um seja contravariante e o outro covariante.

Agora vamos supor que $\mathbf{E}$ tem um produto interno,

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{\alpha, \beta=1}^n g_{\alpha\beta} u^\alpha v^\beta$$

A matriz $g_{\alpha\beta}$ é chamada de métrica de $\mathbf{E}$. É um tensor 2-covariante. A métrica no espaço dual é um tensor 2-contravariante, definido pela matriz inversa $g^{\alpha\beta}$. *Abaixar o índice* de um vetor $\mathbf{u} \in \mathbb{E}$ corresponde a produzir seu dual $\omega = \mathbf{u}^*$ em $\mathbb{E}^*$. Em coordenadas, isso é feito contraindo com a métrica:

$$\omega_\alpha = \sum_{\beta=1}^n g_{\alpha\beta} u^\beta.$$

De maneira análoga, podemos *levantar* o índice de ω se $g^{\alpha,\beta}$ é a matriz inversa a $g_{\alpha,\beta}$:

$$u^\beta = \sum_{\alpha=1}^n g^{\alpha,\beta} \omega_\alpha.$$

Podemos levantar ou abaixar índices de quaisquer tensores.

Exemplo 25.7. O produto interno canônico no espaço de matrizes $m \times n$ é $\langle A, B \rangle = \text{tr}(B^T A) = \sum_{i,j=1}^n A_{ij} B_{ij}$. No caso da multiplicação matricial, abaixar o índice correspondente a D é substituir $\mathcal{M}_n$ pela forma trilinear, também denotada $\mathcal{M}_n$,

$$A, B, C^T \mapsto \langle AB, C^T \rangle = \text{tr}(ABC).$$

3. A decomposição poliádica canônica

Uma das ferramentas clássicas da estatística para analisar nuvens de dados é a decomposição em componentes principais. Era essa a motivação original de Eckart e Young no Teorema 23.3.

Assumimos que os dados estão indexados por dois parâmetros discretos ou modos. Esses dados são codificados em uma matriz A . Por exemplo, N indivíduos foram submetidos a n testes, e A_{ij} é o resultado do teste j no indivíduo i .

Quantas quantidades estamos realmente medindo? Os testes podem medir habilidades ou características do indivíduo que estão relacionadas, ou que são independentes. O modelo estatístico mais simples é de uma única quantidade associada ao indivíduo, ou seja $A_{ij} \simeq u_i v_j$ onde u_i é essa quantidade no indivíduo i , v_j a sensibilidade do teste j a essa quantidade. Esse modelo pede portanto que A possa ser bem aproximada por uma matriz de posto 1.

Um modelo supondo p quantidades pode ser construído a partir da decomposição em valores singulares de A . Se

$$A = U \begin{pmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & \ddots & \\ & & & \sigma_n \\ & & & 0 \\ & & & \vdots \end{pmatrix} V^T,$$

então a melhor aproximação de A em posto p é

$$A_p = U_p \begin{pmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_p \end{pmatrix} V_p^T$$

onde U_p, V_p são as submatrizes de U e V contendo apenas as p primeiras colunas. Se assumimos a existência de p quantidades independentes, a hipótese de mais verossímil é que o indivíduo i mede U_{ik} em relação à k -ésima quantidade, e que o teste j tem sensibilidade $\sigma_k V_{jk}$ à quantidade k .

A partir dos anos 70 do século passado, tentou-se generalizar a decomposição em fatores principais ao caso de 3 ou mais modos. Por exemplo, para analisar os resultados de n testes aplicados em N indivíduos em l ocasiões. Obtemos assim um tensor $\mathcal{A}^{\alpha\beta\gamma}$ correspondendo ao teste β aplicado ao indivíduo α na ocasião γ . Ao contrário da situação anterior, é impossível aproximar

$$\mathcal{A} \simeq \sum_{k=1}^p \sigma_k \mathbf{u}_k \otimes \mathbf{v}_k \otimes \mathbf{w}_k$$

em geral mantendo bases $\mathbf{u}_k, \mathbf{v}_k, \mathbf{w}_k$ ortogonais. Por exemplo,

$$\mathbf{e}_1 \otimes \mathbf{e}_1 \otimes \mathbf{e}_1 + \mathbf{e}_1 \otimes \mathbf{e}_2 \otimes \mathbf{e}_2$$

não admite essa decomposição para $p = 2$ nem pode ser escrito como tensor de posto 1. Mesmo abrindo mão da ortogonalidade das bases, a decomposição para $p = 2$ continua impossível. A possibilidade seguinte, que é pedir apenas que os vetores $\mathbf{u}_k, \mathbf{v}_k$ e $\mathbf{w}_k$ tenham norma 1. Essa decomposição é conhecida como *decomposição poliádica canônica* do tensor (CPD em inglês), ou ainda como decomposição CANDECOMP/PARAFAC. O posto de um tensor $\mathcal{A}$ é o menor inteiro p para o qual exista a decomposição

$$\mathcal{A} = \sum_{k=1}^p \sigma_k \mathbf{u}_k \otimes \mathbf{v}_k \otimes \mathbf{w}_k$$

com $\mathbf{u}_k, \mathbf{v}_k$ e $\mathbf{w}_k$ normalizados e σ_k qualquer. Obter o posto de um tensor ou sua CPD é uma tarefa computacional difícil. Por exemplo, o posto do tensor $\mathcal{M}_2$ é igual a 7, mas temos o seguinte problema em aberto:

Problema em aberto N^o 7. Achar o posto de $\mathcal{M}_n$ para algum $n > 2$.

Finalmente, vamos redefinir o expoente da álgebra linear do Problema em Aberto N^o 1. A discussão sobre a equivalência das duas definições está adiada para os exercícios.

$$\omega = \inf\{\tau : \text{Posto}(\mathcal{M}_n) \in O(n^\tau)\}.$$

4. O posto limítrofe

Você vai mostrar nos exercícios que o posto de matrizes $n \times n$ é uma função semi-contínua inferior. Lembremos que uma função real f é dita semi-contínua inferior em x se e somente se, para todo $\epsilon > 0$, existe uma δ -vizinhança de x onde, para todo y , $f(y) > f(x) - \epsilon$. No caso do posto, por ser uma função discreta, a definição é mais simples: Para toda matriz A , existe $\delta > 0$ tal que se $\|A - B\|_F < \delta$, então $\text{Posto}(B) \geq \text{Posto}(A)$. Para tensores de ordem ≥ 3 , o posto não é mais semi-contínuo inferior.

Exemplo 25.8.

$$T_\epsilon = \frac{1}{\epsilon} ((e_1 - \epsilon e_2) \otimes (e_1 - \epsilon e_2) \otimes (e_1 - \epsilon e_2) - e_1 \otimes e_1 \otimes e_1)$$

tem posto 2 para todo $\epsilon > 0$.

$$\lim_{\epsilon \rightarrow 0} T(\epsilon) = e_2 \otimes e_1 \otimes e_1 + e_1 \otimes e_2 \otimes e_1 + e_1 \otimes e_1 \otimes e_2$$

tem posto 3. O tensor T_ϵ é chamado de *tensor limítrofe* (*border tensor*).

Definição 25.9. O *posto limítrofe* (*border rank*) de um tensor (A) é

$$\underline{\text{Posto}}(A) = \lim_{\delta \rightarrow 0} \inf_{\|B-A\| < \delta} \text{Posto}(B)$$

Por construção, $\underline{\text{Posto}}(A) \leq \text{Posto}(A)$. Surpeendentemente, é possível limitar o expoente da multiplicação matricial em termos do posto limite, não apenas do posto:

Teorema 25.10.

$$\omega = \inf\{\tau : \underline{\text{Posto}}(\mathcal{M}_n) \in O(n^\tau)\}$$

Vamos dar uma idéia da prova do Teorema. Como alguns dos conceitos são mais gerais, seja $\mathcal{T}$ um tensor arbitrário de ordem 3. Interpolamos a definição do posto limite da maneira seguinte: definimos $\text{Posto}_h(\mathcal{T})$ como o menor inteiro r tal que

$$\mathcal{T} = \lim_{\epsilon \rightarrow 0} \epsilon^{-h} \sum_{i=1}^r \mathbf{a}_i(\epsilon) \otimes \mathbf{b}_i(\epsilon) \otimes \mathbf{c}_i(\epsilon)$$

para vetores $\mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i$ dependendo de ϵ de maneira analítica em uma vizinhança da origem. Está claro que se $\underline{\text{Posto}}(\mathcal{T}) \leq \text{Posto}_h(\mathcal{T})$. A recíproca de que existe h tal que $\text{Posto}_h(\mathcal{T}) \leq \underline{\text{Posto}}(\mathcal{T})$ segue de considerações de geometria algébrica que não cabem neste texto. Postulamos essa recíproca para poder provar o Teorema.

Vamos precisar do produto de Kronecker para tensores. Para simplificar, assumimos que $\mathcal{S}$ e $\mathcal{T}$ são tensores de ordem 3 em $\mathbb{R}^m$ e $\mathbb{R}^n$. Então definimos o produto como um tensor de ordem 3 em $\mathbb{R}^{mn}$, com coeficientes

$$(\mathcal{ST})_{\varphi(\alpha_1, \alpha_2) \varphi(\beta_1, \beta_2) \varphi(\gamma_1, \gamma_2)} = \mathcal{S}_{\alpha_1 \beta_1 \gamma_1} \mathcal{T}_{\alpha_2 \beta_2 \gamma_2}$$

onde convencionamos que φ é uma bijeção de $[m] \times [n]$ em $[mn]$. Por exemplo, $(\mathcal{M}_m \mathcal{M}_n)$ é o tensor de multiplicação de matrizes $m \times n$. Deixamos para os exercícios o seguinte Lema:

Lema 25.11. Seja $\mathcal{T}^k$ a k -ésima potência de $\mathcal{T}$ em relação ao produto de Kronecker. Se $\text{Posto}_h(\mathcal{T}) \leq r$, então $\text{Posto}_{kh}(\mathcal{T}^k) \leq r^k$.

Lema 25.12. Se $r = \text{Posto}_h(\mathcal{T})$, então $\text{Posto}(\mathcal{T}) \leq h^2 r$,

DEMONSTRAÇÃO. Por hipótese, podemos escrever

$$\mathcal{T} = \lim_{\epsilon \rightarrow 0} \epsilon^{-h} \sum_{i=1}^r \mathbf{a}_i(\epsilon) \otimes \mathbf{b}_i(\epsilon) \otimes \mathbf{c}_i(\epsilon).$$

O tensor $\mathcal{T}$ é exatamente o termo em ϵ^h de

$$\sum_{i=1}^r \mathbf{a}_i(\epsilon) \otimes \mathbf{b}_i(\epsilon) \otimes \mathbf{c}_i(\epsilon)$$

onde

$$a_i(\epsilon) = a_{i0} + a_{i1}\epsilon + \cdots + a_{ih}\epsilon^h + \cdots$$

e o mesmo vale para $b_i(\epsilon)$ e $c_i(\epsilon)$. Em cada um dos r somandos, o termo em ϵ^h é

$$\sum_{j+k+l=h} a_{ij} \otimes b_{ij} \otimes c_{il}$$

e a soma acima tem no máximo $\binom{h+2}{2}$ termos. Deste modo, o posto de $\mathcal{T}$ é de no máximo $r \binom{h+2}{2} \leq h^2$. $\square$

DEMONSTRAÇÃO DO TEOREMA 25.10. Por hipótese, para todo ϵ , existe uma constante $C = C(\epsilon)$ tal que $\text{Posto}(\mathcal{M}_n) \leq Cn^{\omega+\epsilon}$. Escolhemos $n = n_0$ suficientemente grande, e fixamos $C = C(n_0)$. Sabemos também que $\text{Posto}(\mathcal{M}_n) = \text{Posto}_h(\mathcal{M}_n)$ para algum valor de $h = h(n_0)$. Para cada inteiro N da forma $N = n_0^k$, $\mathcal{M}_N = (\mathcal{M}_{n_0})^k$ e pelo Lema ??,

$$\text{Posto}_{kh}(\mathcal{M}_N) \leq \text{Posto}_h(\mathcal{M}_{n_0})^k \leq C^k n_0^{\omega+\epsilon}.$$

Aplicando agora o Lema ??,

$$\text{Posto}(\mathcal{M}_N) \leq k^2 h^2 C^k n_0^{(\omega+\epsilon)k} = N^{\omega+\delta}$$

onde

$$\delta = \epsilon + \frac{2 \log k}{k \log n_0} + \frac{2 \log h}{k \log n_0} + \frac{\log C}{\log n_0}$$

Escolhemos n_0 suficientemente grande para que $\frac{\log C}{\log n_0} < \epsilon/3$. Para $k \geq k_0$ com k_0 suficientemente grande, as outras duas parcelas ficam menores do que $\epsilon/3$. Deste modo, $\delta \leq 2\epsilon$ e, para todo N da forma $N = n_0^k$ com $k \geq k_0$,

$$\text{Posto}(\mathcal{M}_N) \leq N^{\omega+\delta}$$

Finalmente, precisamos mostrar que $\text{Posto}(\mathcal{M}_n) \leq Cn^{\omega+\delta}$ para todo valor de n . Escolhemos inicialmente uma constante C_0 tal que

$$\text{Posto}(\mathcal{M}_n) \leq C_0 n^{\omega+\delta}$$

para todo $n \leq n_0^{k_0}$. Para todo $k \geq k_0$, se $n_0^k < n \leq n_0^{k+1}$, temos trivialmente que

$$\text{Posto}(\mathcal{M}_n) \leq \text{Posto}(\mathcal{M}_{n_0^{k+1}}) \leq (n_0^k)^{\omega+\delta} n_0^{\omega+\delta}.$$

Escolhemos portanto $C = \max(C_0, n_0^{\omega+\delta})$ e temos sempre

$$\text{Posto}(\mathcal{M}_n) \leq C^{\omega+\delta}$$

para alguma $\delta < 2\epsilon$ e para alguma constante C . $\square$

Nos exercícios, você vai mostrar que:

Corolário 25.12.1. Para todo $n \geq 2$,

$$\omega \leq \frac{\log \text{Posto} \mathcal{M}_n}{\log n}$$

5. Trens de tensores e decomposição de Tucker

A decomposição poliádica canônica não é a única representação possível para tensores. No caso de tensores de ordem grande, as decomposições em trem de tensores ou a decomposição hierárquica de Tucker podem ser mais eficientes.

Vamos supor que $\mathcal{A}$ é um tensor de tamanho $n_1 \times \cdots \times n_k$ e ordem k . Vamos escrever os índices de $\mathcal{A}$ como contravariantes. A decomposição poliádica de $\mathcal{A}$ se escreveria como

$$\mathcal{A}^{i_1 i_2 \dots i_k} = \sum_j (\mathbf{a}_1)_j^{i_1} (\mathbf{a}_2)_j^{i_2} \dots (\mathbf{a}_k)_j^{i_k}$$

para $1 \leq j \leq r$. Podemos truncar essa decomposição para obter uma aproximação, mas não conhecemos uma maneira eficiente de fazer isso.

Uma decomposição em *trem de tensores* é uma decomposição da forma

$$(15) \quad \mathcal{A}^{i_1 i_2 \dots i_k} = \sum_{j_1, \dots, j_{k+1}} (\mathcal{C}_1)_{j_1}^{i_1} (\mathcal{C}_2)_{j_1 j_2}^{i_2} (\mathcal{C}_3)_{j_2 j_3}^{i_3} \dots (\mathcal{C}_k)_{j_{k-1}}^{i_k}$$

Ela pode ser calculada ou aproximada recursivamente. Por exemplo, vamos partir de um tensor $\mathcal{A}^{i_1 i_2 i_3 i_4}$ de tamanho $n_1 \times n_2 \times n_3 \times n_4$. Podemos escrever esse tensor como uma matriz $(n_1 n_2) \times (n_3 n_4)$ ‘baixando’ os dois últimos índices. A decomposição em valores singulares é

$$\mathcal{A}_{i_3 i_4}^{i_1 i_2} = U \Sigma V^T$$

com Σ diagonal de tamanho $\min(i_1 i_2, i_3 i_4)$. e

$$\mathcal{A}^{i_1 i_2 i_3 i_4} = \sum_{j_2} U_{j_2}^{i_1 i_2} W_{j_2}^{i_3 i_4}$$

com $W = (\Sigma V^T)^T$. Depois tratamos U como uma matriz $i_1 \times (i_2 j_2)$ e W como uma matriz $(j_2 i_3) \times i_4$ para obter decomposições

$$U_{j_2}^{i_1 i_2} = \sum_{j_1} (\mathcal{C}_1)_{j_1}^{i_1} (\mathcal{C}_2)_{j_1 j_2}^{i_2}$$

e

$$W_{j_2}^{i_3 i_4} = \sum_{j_3} (\mathcal{C}_3)_{j_2 j_3}^{i_3} (\mathcal{C}_4)_{j_3}^{i_4}$$

obtendo (15). Se o que queremos é aproximar a decomposição podemos truncar, a cada decomposição em valores singulares, os menores valores singulares.

A *decomposição de Tucker* é uma decomposição da forma

$$(16) \quad \mathcal{A}^{i_1 i_2 \dots i_k} = \sum_{j_1, \dots, j_{k+1}} \mathcal{S}^{j_1 j_2 \dots j_k} (U_1)_{j_1}^{i_1} (U_2)_{j_2}^{i_2} (U_3)_{j_3}^{i_3} \dots (U_k)_{j_k}^{i_k}.$$

Uma variante é a *High Order SVD* que usa k decomposições em valores singulares para obter essa aproximação. Para cada $1 \leq r \leq k$, fazemos

$$\mathcal{A}_{i_1 \dots \widehat{i_r} \dots i_k}^{i_r} = U_r \Sigma_r V_r^T.$$

onde assimilamos $\mathcal{A}_{i_1 \dots \widehat{i_r} \dots i_k}^{i_r}$ a uma matriz $n_r \times \prod_{l \neq r} n_l$. O tensor $\mathcal{S}$ faz as partes de valores singulares. Podemos truncar cada matriz Σ_r para obter uma aproximação do tensor $\mathcal{A}$, isso é equivalente a zerar as coordenadas $\mathcal{S}^{j_1 j_2 \dots j_k}$ para j_r alto.

Outra possibilidade para produzir uma decomposição de Tucker ou aproximar tensores é a *decomposição hierárquica de Tucker*. O tensor $\mathcal{S}$ não é mais produzido de maneira explícita. A decomposição é escrita em níveis. No exemplo de ordem 4,

$$\begin{aligned}\mathcal{A}^{i_1 i_2 i_3 i_4} &= \sum_{j_0 k_0} (\mathcal{S}_0)^{j_0 k_0} (\mathcal{T}_1)^{i_1 i_2}_{j_0} (\mathcal{T}_2)^{i_3 i_4}_{k_0} \\ (\mathcal{T}_1)^{i_1 i_2} &= \sum_{j_1 k_1} (\mathcal{S}_1)^{j_1 k_1} \mathcal{U}_{j_1}^{i_1} \mathcal{U}_{k_1}^{i_2} \\ (\mathcal{T}_2)^{i_3 i_4} &= \sum_{j_2 k_2} (\mathcal{S}_2)^{j_2 k_2} \mathcal{U}_{j_2}^{i_3} \mathcal{U}_{k_2}^{i_4}\end{aligned}$$

A aproximação correspondente se escreveria:

$$\begin{aligned}\mathcal{A}^{i_1 i_2 i_3 i_4} &\simeq \sum_{j_0 k_0} (\mathcal{S}_0)^{j_0 k_0} (\mathcal{T}_1)^{i_1 i_2}_{j_0} (\mathcal{T}_2)^{i_3 i_4}_{k_0} \\ (\mathcal{T}_1)^{i_1 i_2} &\simeq \sum_{j_1 k_1} (\mathcal{S}_1)^{j_1 k_1} \mathcal{U}_{j_1}^{i_1} \mathcal{U}_{k_1}^{i_2} \\ (\mathcal{T}_2)^{i_3 i_4} &\simeq \sum_{j_2 k_2} (\mathcal{S}_2)^{j_2 k_2} \mathcal{U}_{j_2}^{i_3} \mathcal{U}_{k_2}^{i_4}\end{aligned}$$

com somas envolvendo menos termos.

6. Exercícios

Exercício 25.1. Mostrar formalmente que o posto de matrizes é uma função semi-continua inferior: qual é o maior valor possível de δ ?

Exercício 25.2. Mostrar com a nova definição de ω , que para todo $\epsilon > 0$, matrizes $n \times n$ podem ser multiplicadas com no máximo $n^{\omega+\epsilon}$ multiplicações. Somas e multiplicações por uma constante são gratuitas, e outras operações não são permitidas.

Exercício 25.3. Mostrar que se, para todo n , existe um algoritmo bilinear para calcular o produto de matrizes $n \times n$ em $O(n^\eta)$ multiplicações, então $\eta \geq \omega$. Um algoritmo bilinear é uma sequência da forma

$$\begin{aligned}d_i &= a_i(A) b_i(B) & i &= 1, \dots, r \\ C_{ij} &= c_{ij}(d_1, \dots, d_r)\end{aligned}$$

com a_i, b_i, c_{ij} funções lineares.

Exercício 25.4. No exercício anterior, mostre que se as a_i, b_i e c_{ij} forem funções afins e $C = AB$ para todos os valores de A e B , então os termos constantes são necessariamente zero.

Exercício 25.5. Mostrar o Lema 25.11.

Exercício 25.6. Mostrar que $\text{Posto}(\mathcal{T}^k) \leq \text{Posto}(\mathcal{T})^k$.

Exercício 25.7. Deduzir o Corolário 25.12.1

Exercício 25.8. Mostre que o tensor $\mathcal{S}^{j_1 \dots j_k}$ da *High order SVD* tem a seguinte propriedade: para cada índice r ,

$$N(r, j_r) = \sqrt{\sum_{j_1, \dots, \hat{j}_r, \dots, j_k} |\mathcal{S}^{j_1, \dots, j_r, \dots, j_k}|^2}$$

é decrescente em j_r .

CAPÍTULO 26

Transformada rápida de Fourier, e como multiplicar números inteiros rápido

1. Polinômios e transformada de Fourier.



Polinômios podem ser representados de várias maneiras. A base canônica (usual) do espaço dos polinômios de grau menor ou igual a d é dada por $(1, x, x^2, \dots, x^d)$. As coordenadas de um polinômio $f(x)$ nessa base são os coeficientes de f :

$$f(x) = \sum_{j=0}^d f_j x^j$$

Se $\alpha_0, \dots, \alpha_d \in \mathbb{C}$ são diferentes dois a dois, podemos reconstruir o polinômio $f(x)$ pelos seus valores nos α_i :

Lema 26.1 (Interpolação de Lagrange).

$$f(x) = \sum_{j=0}^d \left(f(\alpha_j) \prod_{k \neq j} \frac{x - \alpha_k}{\alpha_j - \alpha_k} \right)$$

DEMONSTRAÇÃO. A expressão da direita é um polinômio em x , pois é combinação linear dos polinômios de grau d :

$$h_k(x) = \prod_{j \neq k} \frac{x - \alpha_j}{\alpha_k - \alpha_j}.$$

Os polinômios h_k são chamados de *polinômios interpolantes de Lagrange*. Eles têm a seguinte propriedade:

$$h_l(\alpha_k) = \begin{cases} 1 & \text{se } k = l \\ 0 & \text{se } k \neq l. \end{cases}$$

Logo, para todo $k = 0, 1, \dots, d$, $h(\alpha_k) = f(\alpha_k)$.

É consequência direta do Teorema Fundamental da Álgebra é que, se um polinômio $g(x)$ de grau d se anula em $d + 1$ pontos distintos, então $g(x) \equiv 0$. Já que os dois polinômios $f(x)$ e $h(x)$ assumem valores iguais em $d + 1$ pontos distintos, a diferença é uniformemente nula, e $f(x) \equiv h(x)$. $\square$

Uma escolha possível dos α_k é:

$$\alpha_k = e^{\frac{2\pi ki}{d+1}} = \omega^k.$$

onde $\omega = e^{\frac{2\pi i}{d+1}}$ é a raiz $d + 1$ -ésima primitiva da unidade. Com essa escolha,

$$f(x) = \sum_{k=0}^d f(\omega^k) h_k(x)$$

Os ω^k são $N = d + 1$ pontos igualmente espalhados no círculo unitário complexo, e temos: $\omega^k \omega^l = \omega^{k+l} = \omega^{k+l \bmod N}$. Se consideramos que os coeficientes de f correspondem a uma função discreta $k \mapsto f_k$, a transformada de Fourier discreta de f é exatamente

$$(17) \quad \hat{f}_j = \sum_{k=0}^{N-1} f_k \omega^{-jk} = f(\omega^{-j}) .$$

A fórmula da inversão de Fourier pode ser obtida diretamente. Os polinômios interpolantes de Lagrange são:

$$h_k(x) = \prod_{j \neq k} \frac{x - \omega^j}{\omega^k - \omega^j} = \prod_{j \neq k} \frac{x\omega^k - \omega^{j-k}}{1 - \omega^{j-k}} = \frac{1}{N} \left(1 + \omega^k x + \omega^{2k} x^2 + \dots + \omega^{(N-1)k} x^{N-1} \right)$$

Obtemos portanto diretamente que

$$(18) \quad f_k = \frac{1}{N} \sum_{j=0}^{N-1} f(\omega^j) \omega^{jk}$$

Assim, concluímos que a transformada discreta de Fourier nos coeficientes de um polinômio é equivalente à avaliação nos pontos $1, \omega^{-1}, \dots, \omega^{-N+1}$. Reciprocamente, a transformada discreta inversa de Fourier corresponde ao cálculo do coeficiente do polinômio assumindo valores determinados nos pontos $1, \omega^{-1}, \dots, \omega^{-N+1}$.

2. Transformada rápida de Fourier

As fórmulas da Transformada Discreta de Fourier, assim como estão escritas em (17) e (18) sugerem a realização de $O(N^2)$ operações aritméticas. O algoritmo da Transformada rápida de Fourier (FFT) descrito abaixo permite calcular a transformada e sua inversa de maneira significativamente mais rápida, com $(O(N \log N))$ operações. Esse algoritmo viabiliza o uso da transformada de Fourier e de suas variantes em telecomunicações, onde mensagens precisam ser codificadas e decodificadas em tempo real.

O algoritmo da transformada de Fourier será apresentado de maneira indutiva. Vamos iniciar assumindo por conveniência que $N = 2^k$ seja uma potência de dois. O polinômio $f(x)$ pode ser dividido em uma parte par e uma parte ímpar:

$$\begin{aligned} f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \dots + f_{N-2} x^{N-2} + f_{N-1} x^{N-1} \\ &= \left(f_0 + f_2 x^2 + \dots + f_{N-2} x^{N-2} \right) + \left(f_1 x + f_3 x^3 + \dots + f_{N-1} x^{N-1} \right) \end{aligned}$$

Fazendo, para $j = 0, \dots, 2^{k-1} - 1$,

$$g_j = f_{2j} \quad \text{e} \quad h_j = f_{2j+1},$$

teremos

$$f(x) = g(x^2) + x h(x^2) .$$

Para avaliar f nos $N = 2^k$ pontos $1, \omega^{-1}, \dots, \omega^{-N+1}$, precisamos calcular

$$\hat{f}_j = g(\omega^{-2j}) + \omega^{-j} h(\omega^{-2j}) .$$

Ocorre que $\omega^{-2j} = \omega^{-2j+2^{k-1}}$. Por isso, ao invés de precisarmos de N avaliações de g e de h , precisamos apenas da metade:

$$\hat{f}_j = \hat{g}_{j \bmod 2^{k-1}} + \omega^{-j} \hat{h}_{j \bmod 2^{k-1}},$$

ou ainda:

$$(19) \quad \begin{array}{rclcl} \hat{f}_0 & = & \hat{g}_0 & + & \hat{h}_0 \\ \hat{f}_1 & = & \hat{g}_1 & + & \omega^{-1} \hat{h}_1 \\ \hat{f}_2 & = & \hat{g}_2 & + & \omega^{-2} \hat{h}_2 \\ & \vdots & & & \\ \hat{f}_{2^{k-1}-1} & = & \hat{g}_{2^{k-1}-1} & + & \omega^{-2^{k-1}-1} \hat{h}_{2^{k-1}-1} \\ \hat{f}_{2^{k-1}} & = & \hat{g}_0 & - & \omega^{-1} \hat{h}_0 \\ & \vdots & & & \\ \hat{f}_{2^k-1} & = & \hat{g}_{2^{k-1}-1} & - & \omega^{-2^{k-1}+1} \hat{h}_{2^{k-1}-1}. \end{array}$$

Seja $c(k)$ o custo, em operações aritméticas reais, para calcular a transformada rápida de Fourier de um polinômio de grau $2^k - 1$. Assumimos que ω^{-1} é dada no início, e que o valor de ω^{-2} é repassado para as rotinas calculando $\hat{g}$ e $\hat{h}$. Na k -ésima etapa, temos 2^k somas ou subtrações complexas (duas reais cada) e $2^k - 3$ multiplicações complexas (6 operações reais cada). Temos ainda duas chamadas recursivas de custo $c(k-1)$.

Podemos portanto definir a seguinte recorrência: $c(0) = 0$, $c(1) = 4$ e, em geral,

$$c(k) = 2c(k-1) + 8 \times 2^k - 3$$

Lema 26.2. Se $k \geq 2$, então

$$c(k) = (16k - 15)2^{k-1} + 3$$

Se f é um polinômio de grau d qualquer, a “entrada” tem tamanho $N = d + 1$. Para calcular a transformada rápida de Fourier, podemos completar os coeficientes do polinômio f com zeros, até atingir grau $2^k - 1$, onde $k = \lceil \log_2 N \rceil$. O custo total da transformada será de

$$c(k) \leq (16N + 1) \log_2(N)$$

além do custo de calcular a raiz primitiva da unidade.

Observação 26.3. Existe uma multidão de algoritmos para calcular diretamente a transformada rápida de Fourier usando como base números que não são potência de dois.

3. A multiplicação rápida de polinômios

Se $g(x)$ e $h(x)$ são polinômios de grau d e e respectivamente, o seu produto $f(x) = g(x)h(x)$ tem coeficientes

$$f_k = \sum_{\max(k-d,0) \leq j \leq \min(k,e)} g_{k-j} h_j$$

A operação que leva os coeficientes de $g(x)$ e $h(x)$ nos coeficientes de $f(x)$ é chamada de *convolução*. A convolução de polinômios tem as seguintes propriedades:

- Comutatividade: $\mathbf{f} * \mathbf{g} = \mathbf{g} * \mathbf{f}$
- Associatividade: $(\mathbf{f} * \mathbf{g}) * \mathbf{h} = \mathbf{f} * (\mathbf{g} * \mathbf{h})$

- Elemento neutro multiplicativo: $\mathbf{f} * \mathbf{e}_0 = \mathbf{e}_0 * \mathbf{f}$.
- Distributividade em relação à soma: $\mathbf{f}(\mathbf{g} + \mathbf{h}) = \mathbf{f} * \mathbf{g} + \mathbf{f} * \mathbf{h}$.

As propriedades 1 a 4 implicam que o espaço $(\mathbb{C}[x], +, *)$ de todos os polinômios na variável x , com as operações internas de soma e convolução, é um *anel comutativo com unidade*.

Se $f(x)$, $g(x)$ e $h(x)$ são polinômios de grau menor ou igual a $N - 1$, com $f(x) \equiv g(x)h(x)$ e $\mathbf{f}$, $\mathbf{g}$ e $\mathbf{h}$ são os vetores respectivos dos coeficientes, então temos duas maneiras de calcular $f(x)$ a partir de $g(x)$ e $h(x)$:

Podemos fazer $\mathbf{f} = \mathbf{g} * \mathbf{h}$, ao preço de $O(N^2)$ operações aritméticas. Ou podemos fazer, para cada j ,

$$\hat{f}_j = \hat{g}_j \hat{h}_j,$$

o que custa apenas $O(N)$ operações aritméticas. A transformada de Fourier e a sua inversa custam $O(N \log N)$ iterações, o que torna esse método mais eficiente.

4. A multiplicação rápida de inteiros

A segurança das comunicações eletrônicas depende de uma série de protocolos de criptografia, dos quais o mais famoso é o RSA (inventado por Ron Rivest, Adi Shamir e Leonard Adleman e publicado em 1977). Nesse sistema, cada usuário possui duas chaves. A *chave pública* pode ser publicada livremente. Já a *chave privada* não pode ser divulgada e não deve circular, mesmo criptografada, pela internet. O usuário pode criptografar uma mensagem utilizando a chave pública, e só quem estiver de posse da chave privada consegue decodificá-la. Ele pode também “assinar” uma mensagem com a chave privada, e qualquer um pode conferir a autenticidade se tiver acesso à chave pública do usuário.

O sistema funciona assim: cada usuário gera aleatoriamente dois números primos p e q com suficientes dígitos. Vamos utilizar aritmética inteira módulo $n = pq$. Seja $\lambda = \text{mmc}(p - 1, q - 1)$ e seja $1 < e < \lambda$ um número relativamente primo a λ . Pelo Algoritmo de Euclides estendido, podemos calcular d tal que

$$de + \lambda e' = 1$$

ou, em termos de congruência,

$$de \equiv 1 \pmod{\lambda}.$$

A chave pública é o par (n, e) e a chave privada é o par (n, d) . O algoritmo RSA está baseado no Pequeno Teorema de Fermat:

Teorema (Pequeno Teorema de Fermat). *Seja p primo. Para todo número x entre 0 e $p - 1$, vale a igualdade:*

$$x^p \equiv x \pmod{p}.$$

A prova é deixada em exercício. Uma consequência imediata do Teorema é que:

Lema 26.4. *Nas condições acima, para todo x ,*

$$x^{de} \equiv x \pmod{n}$$

DEMONSTRAÇÃO. Para todo $x \not\equiv 0 \pmod{p}$,

$$x^\lambda \equiv 1 \pmod{p}$$

e

$$x^\lambda \equiv 1 \pmod{q}.$$

Logo, x e n são relativamente primos, e

$$x^\lambda \equiv 1 \pmod{n}.$$

Lembremos que $de \equiv 1 \pmod{\lambda}$. Então existe k tal que $de = k\lambda + 1$. Assim,

$$x^{de} \equiv x^{k\lambda+1} \equiv x \pmod{n}.$$

□

As mensagens a ser codificadas são inicialmente divididas em pacotes, cada um representado por um inteiro entre 0 e $n - 1$. Se x é um pacote, ele é codificado por:

$$y \equiv x^e \pmod{n}.$$

O pacote y é decodificado por:

$$x \equiv y^d \pmod{n}.$$

Da mesma maneira, um pacote pode ser assinado por $z \equiv x^d \pmod{n}$, e a assinatura pode ser verificada por $x \equiv z^e \pmod{n}$.

Quem tiver a capacidade de fatorar o inteiro n pode quebrar o código. O pacote `openssl` no sistema Linux permite gerar as chaves e codificar ou assinar mensagens. Por exemplo, o comando

```
openssl genpkey -algorithm RSA -out priv.pem -pkeyopt rsa_keygen_bits:2048
```

gera um par de chaves pública e privada, guardados em `priv.pem`, com 2048 bits de comprimento. Já o comando

```
openssl rsa -text -in priv.pem
```

permite examinar as chaves. Os campos `publicExponent`, `privateExponent`, `prime1`, `prime2` são respectivamente e , d , p e q , e aparecem em hexadecimal.

A codificação ou decodificação precisa ser processada em tempo real. As chaves públicas e privadas são usadas para estabelecer uma senha compartilhada pelo cliente e pelo servidor, que a partir desse momento usam um sistema ‘simétrico’ de criptografia, muito mais rápido do que a codificação RSA.

O motivo é que a mensagem pode ser uma sessão de *ssh* (secure shell), de *sftp* (secure file transfer protocol) ou uma página de internet segura (protocolo *https*). O computador precisa poder fazer aritmética modular com números extremamente grandes (no exemplo acima, 256 dígitos hexadecimais ou 2048 bits).

A segurança dos esquemas ‘simétricos’ utilizados é independente da segurança do esquema RSA. É concebível que eles possam ser quebrados por outros meios. Para maior segurança, pode ser desejável mudar periodicamente o segredo (por meio de uma nova negociação RSA) ou usar RSA puro.

Sabemos somar, multiplicar e verificar primalidade de maneira eficiente. A hipótese implícita no esquema RSA é que fatorar inteiros é difícil, ou seja que o tempo necessário para fatorar inteiros da forma $n = pq$ seja exponencial no tamanho (número de bits) de n , ou seja linear em n .

Para evitar ataques de um adversário com meios computacionais superiores, vale a pena usar números tão grandes quanto for possível sem afetar a velocidade das comunicações. Aumentar o tamanho de n é a escolha óbvia.

Aritmética rápida de alta precisão ou de inteiros é um assunto vasto, com uma multidão de algoritmos competindo pela preferência de eventuais usuários¹.

Uma das possibilidades (a de melhor complexidade assintótica) é utilizar a FFT (transformada rápida de Fourier). No meu caso, meu “expoente” n pode ser escrito como o valor de um polinômio, avaliado em alguma potência de dois (Por exemplo, $t = 256$:

$$n(t) = 194t^{255} + 123t^{254} + 109t^{253} + \dots$$

O mesmo vale para a mensagem $x(t)$ e para o expoente privado $d(t)$. Para multiplicar dois números $x(t)$ e $y(t)$, basta multiplicar os dois polinômios correspondentes via transformada rápida de Fourier e depois ajustar os coeficientes para estarem entre 0 e $t - 1$. Para calcular o valor de uma expressão $x(t) \bmod n(t)$, é preciso fazer uma divisão com resto. O Algoritmo de Euclides permite fazer isso com multiplicações, somas/subtrações e comparações. Existem algoritmos mais modernos que reduzem o número de comparações necessárias.

O *Openssl* ou Open Security Layer utiliza de fato a multiplicação recursiva de Karatsuba, de complexidade assintótica pior. Em muitos casos, o tamanho das entradas não compensa a utilização do algoritmo assintoticamente mais rápido.

5. O computador quântico

Não existem partículas ou ondas clássicas. A física quântica trata o que se supunha que era uma partícula como uma função de onda complexa, ou ainda como um objeto matemático mais complicado que não vou tentar descrever.

Matéria existe em uma superposição de estados. A observação de um sistema físico corresponderia a um entrelaçamento dos estados do observador e do sistema (isto é **uma** das interpretações da Mecânica Quântica).

Um computador poderia em princípio ser construído para aproveitar a superposição de estados. Essa idéia foi defendida por Richard Feynman e outros autores na década de 1980. O objetivo original seria simular de maneira eficiente processos quânticos.

Uma quantidade impressionante de artigos têm sido escrito sobre algoritmos quânticos, principalmente depois da descoberta da transformada quântica de Fourier e do algoritmo de Shor para fatorização quântica de inteiros.

A mecânica quântica limita as funções que podem ser calculadas por um computador quântico. Essencialmente, apenas transformações unitárias. Mas isso é suficiente para resolver alguns dos problemas assumidos difíceis pelos principais esquemas de criptografia não simétrica.

Vivemos hoje uma corrida tecnológica pela construção de computadores quânticos. A empresa D-Wave tem um dispositivo quântico dedicado que resolve certos problemas de otimização combinatória, talvez utilizando também computadores convencionais. As empresas IBM e Google anunciaram que estão construindo computadores quânticos gerais. Um computador quântico de tamanho suficiente pode quebrar esquemas de criptografia como o RSA. Por enquanto, pode ser suficiente aumentar o tamanho de n . A longo prazo, existe uma área de pesquisa em criptografia pós-quântica.

¹Uma descrição detalhada das principais idéias pode ser encontrada em: Don Knuth, *The Art of Computer Programming Vol. 2 Seminumerical algorithms*. Second edition. Addison-Wesley Publishing Co., Reading, Mass., 1981.

6. Exercícios

É proibido utilizar as rotinas `fft` e `ifft` do Julia ou de outro pacote, salvo para fins de comparação com os seus resultados.

Exercício 26.1. Problema do *hand shaking*: Mostre como dois usuários do sistema RSA podem estabelecer, a distância, um canal seguro (em relação a uma terceira parte que esteja espionando as comunicações). Quais as hipóteses para isso ser possível ?

Exercício 26.2. Mostre a seguinte propriedade da convolução: se D denota a diferenciação em relação a x , vale a regra do produto:

$$D(\mathbf{f} * \mathbf{g}) = (D\mathbf{f}) * \mathbf{g} + \mathbf{f} * (D\mathbf{g}) .$$

Exercício 26.3. Implemente e teste a transformada rápida de Fourier no Julia (apenas para vetores de dimensão 2^k).

Exercício 26.4. Escreva a recorrência para a transformada inversa rápida de Fourier (apenas para vetores de dimensão 2^k).

Exercício 26.5. Se $f(x)$ é um polinômio e $Df(x)$ é a sua derivada em relação a x , qual é a relação entre as transformadas de Fourier de f e de Df ?

Exercício 26.6. Implemente no Julia o algoritmo de multiplicação rápida de inteiros. Cada inteiro será representado por um vetor contendo inteiros entre 0 e 999.999.

Exercício 26.7. Adapte o programa do exercício anterior para calcular os 1000 primeiros dígitos decimais de $\sqrt{2}$. (Utilize iterações de Newton).

Exercício 26.8. Calcule os 1000 primeiros dígitos decimais de π . Utilize (por exemplo) a identidade: $\sin \frac{\pi}{6} = \frac{1}{2}$ e a expansão de Taylor

$$\arcsin(x) = \sum_{n \geq 0} \frac{(2n)!}{4^n (n!)^2 (2n+1)} x^{2n+1},$$

válida para $|x| < 1$.

Exercício 26.9. Plote a transformada de Fourier do vetor cujas coordenadas são as casas decimais das aproximações das duas questões anteriores. Existe alguma periodicidade ?

Exercício 26.10. Mostre o pequeno Teorema de Fermat.

Problema em aberto N° 8. Escrever um algoritmo para calcular a Transformada Discreta de Fourier de um vetor de dimensão N em $T(N)$ operações aritméticas, onde $\lim_{T \rightarrow \infty} \frac{T(N)}{N \log_2(N)} = 0$, ou mostrar que isso não pode ser feito.

Problema em aberto N° 9. Mostrar que não pode existir um algoritmo (determinista, em um computador clássico) para fatorar um inteiro x , com tempo de execução polinomial em $\log_2 x$ (Ou produzir o algoritmo).

APÊNDICE A

Referências comentadas

1. Alguns outros livros de Álgebra Linear

Recomendo sempre aos estudantes que não se limitem à aula ou a um só livro texto.

Não faltam livros de álgebra linear. Começo citando dois que marcaram época. São textos que não descuidam do desenvolvimento rigoroso da matéria, mas sem perder contato com o resto da matemática. Moe Hirsch e Steve Smale¹ apresentam no mesmo livro uma introdução à teoria das equações diferenciais ordinárias e à álgebra linear. Já a Gilbert Strang² produziu um excelente texto para ser utilizado em cursos de Engenharia ou áreas aplicadas. Acredito ser o primeiro dos ‘clássicos’ a abandonar a forma de Jordan em favor de decomposições numericamente estáveis.

Algumas referências canônicas de Álgebra Linear ‘pura’ são os textos de Israel Gel’fand³, Serge Lang⁴, Hoffman e Kunze⁵ ou de Paul Halmos⁶.

2. Ferramentas de referência na internet

A primeira e principal fonte de informação é a **biblioteca** da sua Universidade. Em muitos casos, ela é dividida em bibliotecas setoriais (por exemplo, uma biblioteca de matemática). No entanto, costuma existir uma página de *web* que permite procurar no acervo.

Resultados recentes de matemática aparecem sob forma de artigos. Eles são publicados em periódicos, que podem (ou não) estar disponíveis na sua biblioteca.

De qualquer maneira, os textos costumam estar disponíveis na *internet*. A CAPES (Coordenação de Aperfeiçoamento do Pessoal do Ensino Superior, www.capes.gov.br).

Gregorio Malajovich, *Álgebra Linear*. Versão preliminar, quarta revisão, 3 de maio de 2021.

Copyright © Gregorio Malajovich, 2011, 2021.

¹Morris Hirsch e Stephen Smale, *Differential equations, dynamical systems, and linear algebra*. Pure and Applied Mathematics, Vol. 60. Academic Press New York, 1974. xi+358 pp.

²Gilbert Strang, *Introduction to Linear Algebra*. 3a edição. Wellesley-Cambridge Press, 2003, 2005.

³Israel M. Gel’fand, *Lectures on linear algebra*. With the collaboration of Z. Ya. Shapiro. Translated from the second Russian edition by A. Shenitzer. Reprint of the 1961 translation. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, 1989. vi+185 pp.

⁴Serge Lang, *Linear Algebra* Reprint of the third edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1989. x+285 pp.

⁵Kenneth Hoffman e Ray Kunze, *Linear Algebra*. Second edition. Prentice-Hall, Inc., Englewood Cliffs, N.J. 1971 viii+407 pp.

⁶Paul R. Halmos, *Finite-dimensional vector spaces*. Reprinting of the 1958 second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1974. viii+200 pp.

capes.gov.br) assina uma subscrição *nacional* para os principais periódicos e muitos livros acadêmicos. Essa subscrição inclui as universidades federais e outras com pós-graduação. O ponto de acesso é www.periodicos.capes.gov.br. Para ter acesso à coleção, você precisa se identificar com as credenciais do CAFE (Comunidade Acadêmica Federada), pergunte na sua Universidade.

Resultados ainda mais recentes costumam ser postados no *ArXiv*, www.arxiv.org ou na página dos autores, antes de passar pelo processo de revisão e publicação. Trabalhos divulgados no *ArXiv* não costumam ter sido revisados por *referees* independentes, o que torna o conteúdo dos artigos menos confiável e sujeito a revisões.

As principais ferramentas de busca (autor, título, citações, textual) para artigos ou livros publicados em Matemática são as bases de dados *MathSciNet* <http://www.ams.org/mathscinet/> e *Zentralblatt Math* <http://www.zentralblatt-math.org/zmath/en/>.

3. Recursos computacionais

O principal recurso computacional para matemáticos é a linguagem $\text{\TeX}$ ou $\text{\LaTeX}$ de formatação de textos. Este livro foi datilografado em $\text{\LaTeX}$. Esta linguagem não é um editor de textos. Para obter uma expressão matemática como $\int_0^\infty \frac{1}{x^2} dx$, eu preciso datilografar

```
$\int_{0}^{\infty} \frac{1}{x^2} \mathrm{d}x$.
```

Isso requer um certo aprendizado. Por outro lado, também permite uma formatação profissional do texto sem obrigar o autor a se aprofundar em detalhes tipográficos. O $\text{\TeX}$ (e o $\text{\LaTeX}$) estão disponíveis em qualquer boa distribuição do GNU-Linux. O repositório principal é <http://www.ctan.org/>.

Neste momento, o melhor programa numérico para álgebra linear é a linguagem Julia <https://julialang.org/> disponível livremente. Substitui com vantagem o *Matlab* (pago, <http://www.mathworks.com>) e *Octave* (clone livre do *Matlab*, disponível em qualquer boa distribuição do GNU-Linux e em <http://www.octave.org>).

Os manipuladores de expressões simbólicas mais conhecidos são *Maple* (pago, <http://www.maplesoft.com/>) *Mathematica* (pago, <http://www.wolfram.com/>) e *Maxima* (livre, disponível em qualquer boa distribuição do GNU-Linux e em <http://maxima.sourceforge.net/>).

Índice de Notações

$\mathbb{N}$	- Conjunto dos números naturais $\{1, 2, \dots\}$	
$\mathbb{Z}$	- Conjunto dos números inteiros relativos $\{\dots, -2, -1, 0, 1, 2, \dots\}$	
$\mathbb{Q}$	- Corpo dos números racionais $\frac{p}{q}$, onde $p \in \mathbb{Z}$, $q \in \mathbb{N}$ e $\text{mdc}(p, q) = 1$.	
$\mathbb{R}$	- Corpo dos números reais (Consultar qualquer bom texto de Cálculo)	
$\mathbb{C}$	- Corpo dos números complexos $x + yi$, $x, y \in \mathbb{R}$.	
$\mathbf{e}_j$	- j -ésimo vetor da base canônica de $\mathbb{R}^n$ ou $\mathbb{C}^n$	3
$L(E, F)$	- Espaço das aplicações lineares de E em F	4
$\otimes$	- Produto tensorial	7
$L^2(\mathbb{R})$	- Espaço das funções reais integráveis de quadrado integrável	7
$\langle \cdot, \cdot \rangle$	- Produto interno (canônico ou abstrato)	15
$\ \cdot \ $	- Norma em um espaço vetorial	15
A^T	- Transposta da matriz A , $(A^T)_{ij} = A_{ji}$	18
A^{-1}	- Inversa da matriz A	23
$\circ$	- composição, ou operação interna de grupo	25
S_n	- Grupo das permutações de n elementos	26
$GL(n)$	- Grupo das matrizes $n \times n$ inversíveis	28
$\text{Im}(A)$	- Imagem de uma matriz A	39
$\ker(A)$	- Núcleo de uma matriz A	40
$\det(A)$	- Determinante de uma matriz A	53
$\text{Per}(A)$	- Permanente de uma matriz A	59
$\text{tr}(A)$	- Traço de uma matriz A	70
$O(n)$	- Grupo ortogonal de $\mathbb{R}^n$	79
A^H	- Transposta Hermitiana de A , $(A^H)_{ij} = \bar{A}_{ji}$	97
$A^\dagger$	- Pseudo-inversa da matriz A	103
$\text{Prob}[x \in W]$	- Probabilidade de um evento aleatório $x \in W$	106
$E(x)$	- Valor esperado de uma variável aleatória x	106
$\langle \cdot, \cdot \rangle_H$	- Produto interno Hermitiano	135
$U(n)$	- Grupo Unitário de $\mathbb{C}^n$	136
$\exp(A)$ ou e^A	- Exponencial de uma matriz	138
$\ A\ _{\mathbb{E}, \mathbb{F}}$	- Norma de operador de $A : \mathbb{E} \rightarrow \mathbb{F}$	145
$\ A\ _2$	- Norma de operador em relação à norma canônica de $\mathbb{R}^n$	145
$\ A\ _F$	- Norma de Frobenius de uma matriz A	151

Índice Remissivo

- 3D shooter*, 82
- algoritmo
 - complexidade, 6
 - da transformada rápida de Fourier, 182
 - de compressão de imagens, 103
 - Eliminação Gaussiana, 34
 - de Euclides, 184, 186
 - de Le Gall, 8
 - de Page e Brin, 127
 - de Shor, 186
 - de Strassen, 8
 - para a decomposição QR, 94
 - para achar autovetor principal, 131
 - para o problema da palavra, 31
 - RSA, 184
- anel comutativo com unidade, 184
- aplicação linear, 4
- aritmética
 - corretamente arredondada, 155
 - de alta precisão, 186
- ativo
 - carteira de, 110
 - volatilidade, 110, 120
- autoespaço, 66
 - generalizado, 66
- autômato finito, 116
- automorfismo linear, 5
- autovalor, 63
 - diferentes 2 a 2, 75
- autovetor, 63
- base, 163
 - canônica, 3
 - de autovetores, 75
 - de Haar, 166
 - de ondeletas, 167
 - de wavelets, veja b. de ondeletas
 - ortonormal, 79, 87, 93, 97, 101, 137, 163
- bijecção, 25
- blattodea, 120
- bot*, 102
 - trap*, 127
- Cálculo, 7, 16, 57, 99, 150
 - bom livro de, 145
- CANDECOMP, 176
- chave
 - privada, 184
 - pública, 184
- círculo, 10
- cóclea, 166
- codec*, 169
- código
 - de Huffman, 171
- combinação linear, 3, 39, 40
 - complexa, 75
 - finita, 42
 - trivial, 40, 75
- complemento ortogonal, 47
- composição
 - de aplicações lineares, 4
- compressed sensing, 91
- condições
 - de Karush-Kuhn-Tucker, 91
- cone, 100
- conjunto
 - aberto, 19
 - com interior, 19
 - convexo, 19
 - finito
 - cardinalidade de, 26
 - enumeração de, 26
 - limitado, 19
 - permutação de, 26
 - supremo de, 145
- conucleo, 40
- convolução, 183
- CPD, 176
- crawler*, 102
- criptografia, 184
- decomposição
 - de Schur, 138
 - LU, 23
 - PLU, 34, 36
 - QR, 93
- densidade de probabilidade, 106
- derivativo, 120
- determinante, 52
 - Wronskiano, 77
- DFT, ver *transformada de Fourier discreta*
- digrafo, ver *grafo*
- dimensão, 41, 77
 - complexa, 75
 - infinita, 42
- distância de colaboração, 123

- endomorfismo, **4**
- entropia, **171**
- equação
 - da reta
 - paramétrica, **10**
 - diferencial, **61, 64**
 - do calor, **125**
 - normal, **88**
- espaço vetorial
 - base de, **41**
 - complexo, **65**
 - base de, **75**
 - geradores, **75**
 - conjunto gerador de, **40**
 - definido por geradores, **40**
 - norma em, **15**
 - produto interno em, **15**
 - real, **2**
- esperança matemática
 - esperança matemática, **109**
- estado
 - entrelaçados, **107**
 - estacionário, **116, 128**
 - interno, **140**
 - observável, **140**
 - superposição de, **186**
- evento
 - aleatório, **105, 107**
- fatoração
 - de inteiros, **186, 187**
 - de matrizes, ver *decomposição*
- fazenda de links, **129**
- FFT, ver *transformada rápida de Fourier*
- filtro
 - de quadratura, **167**
- forma
 - bilinear, **52**
 - positiva definida, **136**
 - sesquisimétrica, **135, 136**
 - simétrica, **97**
 - multilinear
 - alternada, **52**
 - anti-simétrica, **52**
 - simétrica, **52**
 - simplética, **135**
- Forma Normal
 - de Jordan, **140**
 - de Schur, **138**
- fórmula
 - de Leibniz, **53**
 - de polarização, **19**
- função
 - de Haar, **166**
 - exponencial, **148**
 - de uma matriz, **62, 66, 148**
 - zeta de Riemann, **143**
- fundo de investimento
 - alavancado, **113**
 - análise fundamentalista, **110**
 - análise qualitativa, **110**
 - ativo, **111**
 - de alto risco, **110**
 - de baixo risco, **110**
 - índice, **111**
 - passivo, **111**
 - risco, **110**
- genérico, **91**
- geometria, **14**
 - Euclidiana, **9**
 - revista por Hilbert, **11**
 - não Euclidiana, **12**
- Google, **128**
- grafo, **47, 123**
 - aresta, **47, 123**
 - de um digrafo, **127**
 - caminho em, **123**
 - ciclo em, **123**
 - de colaboração, **123**
 - digrafo simples, **127**
 - espectro de, **125**
 - orientado, **126**
 - perfeito, **133**
 - vértice, **47, 123**
 - de um digrafo, **127**
 - grau de um, **123, 124**
- grupo, **14, 25**
 - ação
 - por conjugação, **148**
 - ação por conjugação, **62**
 - ação de, **33, 147, 149**
 - comutativo, **25**
 - conjunto de relações, **30**
 - conjunto gerador de, **80**
 - das permutações, **30**
 - de matrizes, **28**
 - de permutações, **26**
 - dos movimentos rígidos, **81**
 - Euclidiano, **25**
 - finitamente apresentável, **30**
 - geradores de, **28**
 - homomorfismo de, **28, 30, 55**
 - isomorfismo de, **28**
 - linear, **28**
 - livre, **30**
 - normal, **36**
 - órbita de, **33, 62**
 - Ortogonal, **79, 148**
 - ortogonal, **28, 80, 146**
 - problema da palavra, **31**
 - representação, ver *representação*
 - representação de, **81**
 - sub, **26, 35**
 - estabilizador de, **36**
 - subG normal, **28**
 - Unitário, **136, 148**
- H.264, **170**
- Hipótes
 - de Riemann, **143**
- homomorfismo
 - imagem de, **28**
 - núcleo de, **28**
- https, **185**
- Hummingbird, **131**

- IEEE-754, 155
- invariante
 - do sistema de coordenadas, 71
- investimento
 - retorno, 105
 - retorno esperado, 105
- isometria, 17
- isomorfismo
 - de grupo, 28
 - linear, 5, 43
- JPEG, 170
- lei
 - de Kirchhoff
 - para a corrente, 126
 - para a voltagem, 126
 - de Ohm, 73, 126
- linha reta
 - do plano Euclidiano, 9
- margin call, 113
- matriz
 - ampliada, 34
 - companheira, 153
 - de adjacência, 124
 - de covariância, 109
 - de Haar, 166
 - de Hadamard, 85
 - de incidência, 48
 - de Jordan, 64, 74
 - de Márkov, 116, 116, 120, 125, 128
 - positiva, 116
 - de permutação, 29, 34, 36
 - de projeção
 - complexa, 138
 - de simetria, 94
 - ortogonal ou de Householder, 89
 - de transição, 116
 - de Vandermonde, 58
 - diagonalizável
 - complexa, 75
 - real, 63, 64, 74
 - dos cofatores, 55
 - em forma escada, 45
 - estocástica, 116
 - exponencial de, 62, 138, 139
 - Hermitiana simétrica, 136, 137
 - Hessiana, 99
 - identidade, 5
 - imagem de, 39
 - incidência, 126
 - inversa, 23
 - inversa à esquerda/direita de, 5
 - inversível, 23
 - Laplaciana, 124
 - nilpotente, 118
 - núcleo de, 40
 - ortogonal, 18, 79, 93
 - pseudo-inversa de, 103
 - raio espectral de, 118, 148
 - simétrica, 72, 97, 97
 - positiva definida, 98
 - similar, 62
 - simétrica
 - negativa, 98
 - negativa definida, 98
 - positiva, 98
 - positiva definida, 98
 - transposta
 - Hermitiana, 97, 136
 - triangular inferior, 22, 34, 36
 - triangular superior, 22, 34, 36, 93
 - unitária, 136, 138
- média
 - de uma variável aleatória, 109
- modelo, 119
 - de Black-Scholes, 120
 - de complexidade, 6
 - estabilidade de um Boeing 707, 140
 - para fonte de informação, 116
 - para passeio na web, 128
 - psicoacústico, 167
- modern portfolio theory, 111
- moeda justa, 105
- morfismo, 4
- movimento Browniano, 119
- movimento rígido, 17
- MP3, 167
- MP4, 170
- MPEG, 167, 170
- multiplicação
 - de matrizes, 5
 - complexidade, 8
 - método de Strassen, 8
- Multiplicadores de Lagrange, 91
- norma, 19
 - de Frobenius, 151
 - de Minkovski, 19
 - Euclidiana ou Canônica, 79
- número de condicionamento, 157
- número de Erdős, 123
- objeto geométrico
 - natureza, 10
- Octave, 141
- OpenGL, 82
- Openssl, 186
- operador
 - autoadjunto, 142
- órgão de Corti, 167
- PageRank, 127
- PARAFAC, 176
- periplaneta americana, 120
- permanente, 59
- permutação
 - cíclica, 26
 - elementar, 26
 - par/ímpar, 27
- plano
 - de Poincaré, 13
- polinômio
 - característico de uma matriz, 63
 - de Lagrange, 181
 - pérfido, 153
- ponto

- do plano, 9
- do plano de Poincaré, 13
- do plano Euclidiano, 9
- posição geral, 90
- posto, 45
 - posto limítrofe, 177
- precisão
 - dupla, 155
 - simples, 155
- probabilidade
 - bicaudal, 106
 - condicional, 115
- problema
 - de mínimos quadrados não-degenerado, 88
- processo
 - de Gram e Schmidt, 93, 95, 102, 136
 - estocástico, 119
 - sem memória, 115
- produto
 - de matrizes, 5
- produto interno
 - abstrato, 15
 - Canônico, 15
 - canônico de $\mathbb{R}^n$, 15
 - Hermitiano, 135
 - canônico, 135
- produto tensorial, 7
- programa
 - rastejador, 102, 127, 130
- projeção, 87
 - ortogonal, 87, 89
- raio espectral
 - ver *matriz*, 1
- reflexão
 - de Householder, 94
- regra
 - de Cramer, 6, 56
- representação
 - de grupo, 4
 - do grupo das transformações lineares, 70
 - do grupo de movimentos rígidos, 83
- reta, 10
 - do plano de Poincaré, 13
 - equação analítica, 10
 - equação implícita, 10
 - paralelas, 12
 - segmento de, 9
- rotação, 80
 - de Givens, 81
- segmento
 - do plano Euclidiano, 9
- sequência
 - convergente, 118
 - de Fibonacci, 61
- série
 - absolutamente convergente, 148, 149
 - convergente, 62, 66, 148, 148
 - de matrizes, 148
 - de números reais, 148
- sftp*, 185
- shader, 82
- simetria
 - em relação a um grupo, 14
 - geométrica, 13, 80
- sistema
 - estável, 139
 - instável, 64
- ssh, 185
- tensor, 173
 - contração, 175
 - da multiplicação matricial, 174
 - decomposição hierárquica, 180
 - decomposição poliádica canônica, 176
 - decomposição de Tucker, 179
 - mudança de coordenadas, 174
 - posto limítrofe, 177
 - trem de, 179
- Teorema
 - da decomposição de Givens, 81
 - da decomposição em valores singulares, 101, 130
 - da decomposição PLU, 34, 36
 - da unicidade do determinante, 52
 - de Cálculo
 - (mau gosto), 99
 - do mínimo local, 99
 - de Cauchy-Buniakovskii-Schwarz, 16
 - de Cayley-Hamilton, 142
 - de Eckart-Young, 158
 - de Novikov (problema da palavra), 31
 - de Perron-Frobenius, 116
 - de Schur, 138
 - do isomorfismo (grupos), 28, 30
 - do posto, 45
 - espectral
 - para matrizes Hermitianas, 137
 - para matrizes simétricas, 97
 - pequeno T. de Fermat, 184, 187
 - relacionando volume e determinante, 57
 - sobre a estabilidade de equações diferenciais, 139
 - sobre o determinante do produto, 55
 - sobre o número de componentes de um grafo, 47
- textura, 83
- transformação
 - de similaridade, 13
 - de um conjunto, 33
 - identidade, 5
 - linear, 4
 - associada, 81
 - ortogonal, 146
- transformada
 - de Fourier, 163
 - discreta, 163, 167, 182
 - do cosseno, 168
 - rápida de Fourier, 182
- url* ou *uniform resource locator*, 127
- valor singular, 101
- variável
 - aleatória, 106

- correlação linear, **108**
- covariância, **108**
- desvio padrão, **106**
- Gaussiana ou normalmente distribuída,
106
- independentes, **107, 108**
- média, **106**
- uniformemente distribuída, **106**
- variância, **106**
- livre, **46**
- vetor
 - complexo
 - ortogonal a outro, **136**
 - conjunto ortonormal, **79**
 - coordenadas de, **3**
 - linearmente dependentes, **40**
 - linearmente independentes, **40**
 - linha, **70**
 - ortogonal a um espaço, **87**
- vetor singular, **101**
- vínculo ativo, **91**
- volume
 - de um paralelepípedo, **57**
- Vulkan, **82**
- Web spam*, **129**
- world wide web*, **102, 127**