APLICAÇÕES DE ÁLGEBRA LINEAR À COMBINATÓRIA

GABRIEL BUJOKAS (GBUJOKAS@MIT.EDU)

A gente vai discutir algumas das aplicações clássicas de álgebra linear à combinatória. Vamos começar relembrando alguns conceitos básicos que vamos usar.

1. Relembrando álgebra linear

Definição 1. Seja $\mathbb{F}$ um corpo. Um *espaço vetorial* V é um conjunto equipado com uma operação comutativa de soma $(+ : V \times V \to V)$ e multiplicação por escalar $(\cdot : V \times \mathbb{F} \to V)$ compatível com a multiplicação no corpo e distributiva em relação à soma.

Um subconjunto $S \subset V$ *gera* o espaço V se para qualquer $v \in V$, existe $\alpha_v : S \to \mathbb{F}$ de suporte finito (isso é, $\alpha_v(s)$ é 0 para todos menos um número finito de valores de $s \in S$) tal que

$$\sum_{s \in S} \alpha_v(s) s = v$$

Um subconjunto $S \subset V$ é *independente* se $\alpha : S \to \mathbb{F}$ tem suporte finito e

$$\sum_{s \in S} \alpha(s) s = 0$$

então α é identicamente 0.

Um subconjunto S que é gerador e independente é chamado de *base*.

Teorema 1. *Seja $S \subset V$ um subconjunto de um espaço vetorial V. As seguintes condições são equivalentes.*

1. *S é uma base*
2. *S é gerador minimal (isso é, nenhum subconjunto próprio de S é gerador)*
3. *S é independente maximal (isso é, nenhum subconjunto de V propriamente contendo S é independente)*

Além do mais, toda a base de V tem a mesma cardinalidade, chamada dimensão de V.

Examplo 1.1. O exemplo mais básico é $V = \mathbb{F}^n$, com as operaçoes usuais. Observe que $e_i \in \mathbb{F}^n$ definido por

$$(e_i)_j = \delta_{ij}$$

são tais que $\{e_1, e_2, \ldots, e_n\}$ é uma base, e portanto $\dim V = n$.

Um exemplo um pouco mais interessante é o conjunto de polinômios em s variáveis e coeficientes em $\mathbb{F}$, $V = \mathbb{F}[x_1, x_2, \ldots, x_s]$. A soma de polinômios e multiplicação por constantes fazem de V um espaço vetorial. O conjunto de monômios $x_1^{a_1} x_2^{a_2} \ldots x_s^{a_s}$ forma uma base de V, e portanto V tem dimensão infinita. Entretanto, se V' é o conjunto de polinômios homogeneos de grau r, V' é um *subespaço*, com dimensão $\binom{r+s-1}{r}$.

Date: Semana Olimpica - 2010.

Definição 2. Dada uma matriz $M_{n\times m}$, o *posto* de M, denotado por $pt(M)$, é a dimensão do subespaço de $\mathbb{F}^m$ gerado pelas colunas de M.

Teorema 2. *Seja $A_{n\times m}, B_{n\times m}, C_{m\times k}$ matrizes com entradas em $\mathbb{F}$. Portanto,*

- $pt(A) \leq \min(n, m)$
- $pt(A) + pt(B) \geq pt(A + B)$
- $pt(A^T) = pt(A)$
- $pt(AC) \leq pt(A)$

Teorema 3. *Para qualquer matriz $n \times n$ simétrica A, existe uma matriz $n \times n$ U tal que $UU^T = I$ e UAU^t é diagonal. Isso é, podemos escolher n autovetores de A ortogonais. Além do mais, A tem n autovalores (contados com multiplicidade), e soma deles é igual ao traço de A.*

2. Oddtown

Como aquecimento, vejamos uma primeira aplicação.

Teorema 4. *(Berlekamp, 1969) Em Oddtown, existem n pessoas, e m clubes $C_1, \ldots C_m \subset V$. Esses clubes satisfazem:*

(1) *$|C_i|$ é ímpar, para qualquer i.*
(2) *$|C_i \cap C_j|$ é par, para qualquer $i \neq j$.*

Então, $m \leq n$.

Demonstração. Para cada clube i, considere o vetor $c_i \in \{0, 1\}^n$ tal que

$$(c_i)_j = \begin{cases} 1, \text{ se a pessoa } j \text{ faz parte do clube } i \\ 0, \text{caso contrário.} \end{cases}$$

Note que

$$c_i \cdot c_j = |C_i \cap C_j|$$

Portanto, $c_i \cdot c_j$ é par se $i \neq j$, e ímpar se $i = j$. Pensando nos c_i's como vetores em $\mathbb{F}_2^n$, nós temos

$$c_i \cdot c_j = \begin{cases} 1, \text{ se } i = j \\ 0, \text{caso contrário} \end{cases}$$

Isso implica que $c_1, \ldots, c_m$ são linearmente independentes (em $\mathbb{F}_2$). De fato, se existem $\alpha_i \in \mathbb{F}_2$ tais que

$$\alpha_1 c_1 + \alpha_2 c_2 + \ldots + \alpha_m c_m = 0$$

Então, fazendo o produto escalar com c_i, nós concluímos $\alpha_i = 0$.

Finalmente, se m vetores em $\mathbb{F}_2^n$ são linearmente independentes, então

$$m \leq \dim \mathbb{F}_2^n = n$$

□

3. Teorema de Graham-Pollak

Denote por K_n o grafo completo com n vértices.

Questão Qual é o menor valor de m tal que as arestas de K_n possam ser particionadas em m grafos bipartidos completos?

Explicando melhor, seja K_n o grafo completo com vértices $V = \{1, 2, \ldots, n\}$, e seja $E = \binom{V}{2}$ o conjunto de arestas.

Para qualquer $A_k, B_k \subset V$ tal que $A_k \cap B_k = \emptyset$, seja $E(A_k, B_k) = \{\{a, b\} | a \in A_k, b \in B_k\} \subset E$. Seja $m(n)$ o menor valor de m para o qual existem $A_1, B_1, A_2, B_2, \ldots, A_m, B_m \subset V$ tais que

$$\begin{aligned} A_i \cap B_i &= \emptyset, \text{ para todo } i \\ E(A_i, B_i) \cap E(A_j, B_j) &= \emptyset, \text{ para todo } i \neq j \\ \bigcup_i E(A_i, B_i) &= E \end{aligned}$$

Teorema 5. *(Graham-Pollak, 1972)* $m(n) = n - 1$.

Demonstração. É fácil achar um exemplo de partição usando $n-1$ partes [Por que?]. Nós temos que provar $m \geq n-1$. Seja $A_1, B_1, \ldots, A_m, B_m$ qualquer partição de K_n como descrito acima. Seja M_k a matriz $n \times n$ definida por

$$(M_k)_{ij} = \begin{cases} 1, \text{ se } i \in A_k \text{ e } j \in B_k \\ 0, \text{ caso contrário} \end{cases}$$

Seja $M = M_1 + \ldots + M_m$. Podemos reescrever as condições da partição como

$$M + M^T = J - I$$

Note que $pt(M_k) = 1$. Portanto,

$$pt(M) \leq pt(M_1) + pt(M_2) + \ldots + pt(M_m) = m$$

Basta provarmos que $pt(M) \geq n - 1$. Suponha, por contradição, que $pt(M) < n - 1$. Seja $u = (1, 1, \ldots, 1)$. Então, o sistema

$$\begin{aligned} Mx &= 0 \\ ux &= 0 \end{aligned}$$

tem uma solução não nula x. Logo,

$$0 = x^T(M + M^T)x = x^T(J - I)x = -x^T x < 0$$

Contradição. □

Nota 1. Não se conhece nenhuma prova não algébrica desse teorema!

4. Conjuntos de "duas distâncias"

Um conjunto de pontos $S \subset \mathbb{R}^n$ tem "duas distâncias" se existem reais positivos δ_1, δ_2 tais que $d(x, y) = \delta_1$ ou δ_2 para todos $x, y \in S$ distintos. Seja $m(n)$ o maior número de pontos de um conjunto de duas distâncias em $\mathbb{R}^n$. Existe um exemplo com $n(n+1)/2$ pontos [consegue achar?]. O seguinte teorema mostra que esse exemplo não está longe do máximo possível.

Teorema 6. *(Larman-Rogers-Seidel, 1977)* $m(n) \leq (n+1)(n+4)/2$

Demonstração. Sejam $p_1, p_2, \ldots, p_m$ os pontos em S. Seja

$$f_i(x_1, x_2, \ldots, x_n) = (||x - p_i|| - \delta_1^2)(||x - p_i|| - \delta_2^2)$$

É suficiente provar a seguinte proposição.

Proposição 1. *Os polinômios f_i são tais que*

(1) *$f_1, f_2, \ldots, f_m$ são linearmente independentes (em $\mathbb{R}$).*
(2) *$f_1, f_2, \ldots, f_m$ estão contidos em um subespaço S do espaço de polinômios reais em n variáveis, tal que a dimensão de S é menor ou igual a $(n+1)(n+4)/2$.*

Para provar (1), repare que

$$f_i(p_j) = \begin{cases} \delta_1^2\delta_2^2 \neq 0, \text{ se } i = j \\ 0, \text{ se } i \neq j \end{cases}$$

Então $f_1, f_2, \ldots, f_m$ são linearmente independentes, de acordo com o seguinte critério.

Lema 1. *(Critério Diagonal) Sejam $f_1, f_2, \ldots, f_m$ funções $\Omega \to \mathbb{F}$, e $a_1, a_2, \ldots, a_m \in \Omega$ tais que*

$$f_i(a_j) \begin{cases} \neq 0, \text{ se } i = j \\ = 0, \text{ se } i \neq j \end{cases}$$

Então $f_1, f_2, \ldots, f_m$ linearmente independentes sobre $\mathbb{F}$.

Demonstração. Suponha, por contradicção, que existem $\alpha_i \in \mathbb{F}$ tal que

$$\alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_m f_m = 0$$

Substituindo x por a_i, nós temos $\alpha_i f_i(a_i) = 0$, o que implica $\alpha_i = 0$, para todo i. □

Para provar (2), note que f_i, para qualquer i, é uma combinação linear dos seguintes polinômios:

(1) $(\sum x_j^2)^2$
(2) $x_j(\sum_i x_i^2)$, para todo j.
(3) $x_i x_j$, para todo i, j.
(4) x_i, para todo i.
(5) 1

Portanto, o espaço S gerado pelos $1+n+n(n+1)/2+n+1 = (n+1)(n+4)/2$ polinômios acima contém os f_i, o que prova (2). □

5. Hoffman-Singleton

Um grafo G tem cintura g se o menor ciclo contido em G tem tamanho g. Um grafo é r-regular se todos os vértices tem grau r.

Note que um grafo r-regular de cintura 5 tem ao menos $r^2 + 1$ vértices [Por que?]. Chame um grafo G de *r-pequeno* se G é r-regular de cintura 5 e tem exatamente $r^2 + 1$ vértices.

Por exemplo, um ciclo de tamanho 5 é *2-pequeno*. O grafo de Petersen é *3-pequeno*.

Teorema 7. *(Hoffman, Singleton, 1960) Se existe um grafo G r-pequeno, então $r = 2, 3, 7$ ou 57.*

Demonstração. Note que, por G ser pequeno, para qualquer par de vértices v, u distintos e não adjacentes, existe exatamente um vértice w tal que $(v, w), (u, w)$ são arestas [Por que?].

Seja A a matriz de adjacência de G. O observação acima e o fato de que G é r-regular podem ser reescritos como

$$A^2 + A = (r-1)I + J \tag{1}$$

onde J é a matriz $n \times n$ com 1 em todas entradas.

Primeiro, note que $v_1 = (1, 1, \ldots, 1)^T$ é um autovetor de A, com autovalor r. Como A é uma matriz simétrica, ela pode ser diagonalizada por uma matriz ortogonal, isso é, nós podemos escolher outros n-1 autovetores $v_2, v_3, \ldots, v_n$ tal que v_i, v_j são ortogonais para todo i, j. Em particular, $v_i \cdot v_1 = 0$, o que implica $Jv_i = 0$ para $i > 1$. Portanto, multiplicando a relação (1) por v_i, nós obtemos

$$(\lambda_i^2 + \lambda_i)v_i = (r-1)v_i + 0 \tag{2}$$

onde λ_i é o autovalor de v_i. Portanto, os $n-1$ autovalores de A diferentes de $\lambda_1 = r$ satisfazem $\lambda^2 + \lambda - r + 1 = 0$, o que implica que são $\alpha_1 = \frac{\sqrt{4r-3}-1}{2}$ ou $\alpha_2 = \frac{-\sqrt{4r-3}-1}{2}$. Seja r_i o número de autovalores de A iguais a α_i. Nós sabemos que

$$1 + r_1 + r_2 = n$$

Por outro lado, calculando o traço de A, nós descobrimos

$$0 = r - (r_1 + r_2)/2 + \sqrt{4r-3}(r_1 - r_2)/2$$

Juntando as duas equações, e usando $n = r^2 + 1$, nós obtemos

$$0 = 2r - r^2 + s(r_1 - r_2)$$

Onde $s = \sqrt{4r-3}$. Existem dois casos:

Caso 1 O número s é irracional. Portanto, $r_1 = r_2$, e concluímos $r = 2$.

Caso 2 O número s é inteiro. Substituindo, nós obtemos

$$s^4 - 2s^2 + 16s(r_1 - r_2) - 15 = 0$$

O que implica que s divide 15, e portanto $r = 1, 3, 7$, ou 57. □

6. Teorema de Bollobás

Teorema 8. *(Bollobás, 1965) Sejam r, s inteiros positivos, e $A_1, B_1, A_2, B_2, \ldots, A_m, B_m$ conjuntos tais que*

1. $|A_i| = r$ *e* $|B_i| = s$
2. $A_i \cap B_i = \emptyset$
3. $A_i \cap B_j \neq \emptyset$ *se* $i \neq j$

Então, $m \leq \binom{r+s}{s}$.

Demonstração. (Lovász) Um conjunto de pontos em $\mathbb{R}^{r+1}$ está em *posição geral* se nenhum $r+1$ deles estão contidos em um hiperplano de $\mathbb{R}^{r+1}$. Existem infinitos pontos em posição geral em $\mathbb{R}^{r+1}$ (para uma demonstração, veja o exercício 7.8).

Seja $V = (\cup_i A_i) \cup (\cup_i B_i)$ a união de todos A_i, B_i's. Escolha $v : V \to \mathbb{R}^{r+1}$ tal que os vetores na imagem de v estejam em posição geral. Portanto, para cada A_i, os r pontos

$\{v(x), x \in A_i\}$ geram um hiperplano de dimensão r. Seja $a_i \in \mathbb{R}^{r+1}$ um vetor perpendicular a esse plano. Portanto, para qualquer $e \in V$,

$$v(e) \perp a_i \iff e \in A_i$$

(essa é a observação principal, e usa o fato dos $v(e)$ estarem em posição geral).

Considere os polinômios

$$p_i(x) = \prod_{e \in B_i} (x \cdot v(e))$$

Note que

$$p_i(a_j) \begin{cases} \neq 0, \text{ se } i = j \\ = 0, \text{ caso contrário} \end{cases}$$

Pelo critério diagonal (lema 1), os polinômios $p_1, p_2, \ldots, p_m$ são linearmente independentes. Por outro lado, eles são polinômios homogêneos de grau s em $r+1$ variáveis, e portanto elementos de um espaço de dimensão $\binom{r+s}{s}$. □

7. Exercícios

Exercício 7.1. *(Berkelamp)* Em Eventown, existem n pessoas, e uma família $\mathfrak{F}$ de m clubes. Esses clubes satisfazem:

(1) $|C|$ é par, para qualquer $C \in \mathfrak{F}$.
(2) $|C \cap D|$ é par, para qualquer $C, D \in \mathfrak{F}$.

Prove que

(a) A família $\mathfrak{F}$ tem $m \leq 2^{\lfloor n/2 \rfloor}$ clubes.
(b) Se a família $\mathfrak{F}$ tem menos de $2^{\lfloor n/2 \rfloor}$ clubes, então existe um clube C que pode ser adicionado à família sem violar as regras de Eventown.

Exercício 7.2. *(Desigualdade de Fisher)* Seja λ um inteiro positivo, e $\mathfrak{C}$ uma coleção de subconjuntos de um conjunto X, tal que a intersecção de qualquer dois elementos de $\mathfrak{C}$ tem λ elementos. Prove que $|\mathfrak{C}| \leq |X|$.

Exercício 7.3. Para conjuntos disjuntos V_1, V_2, V_3, o grafo tripartido completo com tripartição (V_1, V_2, V_3) tem vértices $V_1 \cup V_2 \cup V_3$, e uv é uma aresta se, e somente se, u e v estão em diferentes V_i's (portanto, o número total de arestas é $|V_1||V_2| + |V_1||V_3| + |V_2||V_3|$). Qual é o valor mínimo de m tal que K_n pode ser particionado em m grafos tripartidos completos?

Exercício 7.4. Um conjunto de pontos $S \subset \mathbb{R}^n$ tem "uma distância" se existe δ tal que $d(x, y) = \delta$ para qualquer $x \neq y \in S$. Prove que um conjunto S em $\mathbb{R}^n$ tem uma distância, então ele contém no máximo $n+1$ pontos. [Dica: Talvez ajude fazer alguma renormalização]

Exercício 7.5. *(Blokhuis, 1981)* Prove que o número máximo de pontos $m(n)$ em um conjunto de duas distâncias em $\mathbb{R}^n$ é menor ou igual à $(n+1)(n+2)/2$. [Dica: Nós mostramos que os m polinômios $f_1, \ldots, f_m$ são linearmente independentes. Mostre que os $m+n+1$ polinômios $f_1, \ldots, f_m, x_1, x_2, \ldots, x_n, 1$ também são linearmente independentes.]

Exercício 7.6. A esfera unitária em $\mathbb{R}^n$ é $S^{n-1} = \{x \in \mathbb{R}^n \text{ tal que } ||x|| = 1\}$. Um conjunto esférico de duas distâncias é um subconjunto de S^{n-1} de duas distâncias. Mostre que o tamanho máximo $m_s(n)$ de tal conjunto satisfaz:

(a) $m_s(n) \geq n(n+1)/2$;

(b) $m_s(n) \leq n(n+3)/2$.

Exercício 7.7. *(Erdös, Sós and Rényi, 1966: O teorema da amizade)* Se G é um grafo tal que qualquer par de vértices tem exatamente um vizinho em comum, então existe um vértice vizinho a todos os outros vértices. [Dica: Suponha por contradição que nenhum vértice é vizinho de todos os outros. Então, mostre que G é regular. Para isso, note que vértices não adjacentes tem o mesmo grau, e que o complemento de G é conexo. Agora, note que $A^2 = J + (r-1)I$, onde A é a matriz de adjacência de G.]

Exercício 7.8. Mostre que qualquer conjunto de pontos da curva $t \to (1, t, t^2, \ldots, t^{n-1})$ estão em posição geral.

Exercício 7.9. *(Prova original do teorema de Bollobás)* Seja A_i, B_i como no teorema de Bollobás. Seja $V = (\cup_i A_i) \cup (\cup_i B_i)$, e $|V| = n$. Seja E_i o conjunto das permutações $\sigma : V \to V$ tal que $\sigma(a) < \sigma(b)$ para qualquer $a \in A_i, b \in B_i$. Mostre que

(1) $|E_i| = n(n-1)\ldots(n-r-s+1)r!s!$
(2) $E_i \cap E_j = \emptyset$ para qualquer $i \neq j$.
(3) Conclua o teorema de Bollobás.

Exercício 7.10. (a) Prove a seguinte generalização do critério diagonal (lema 1):

> **Lema 2.** *(Critério Triangular) Sejam $f_1, f_2, \ldots, f_m$ funções $\Omega \to \mathbb{F}$, e $a_1, a_2, \ldots, a_m \in \Omega$ tais que*
>
> $$f_i(a_j) \begin{cases} \neq 0, \text{ se } i = j \\ = 0, \text{ se } i < j \end{cases}$$
>
> *Então $f_1, f_2, \ldots, f_m$ são linearmente independentes sobre $\mathbb{F}$.*

(b) *(Generalização do teorema de Bollobás)* Use o critério triangular para adaptar a demonstração 6 para provar que a mesma conclusão é válida se relaxarmos a condição 3 para:
(3') $A_i \cap B_j \neq \emptyset$ se $i < j$
(Observação: Não se conhece nenhuma demonstração não algébrica desse teorema)

Exercício 7.11. *(Versão não uniforme de Ray-Chauhuri-Wilson)* Seja $L = \{l_1, l_2, \ldots, l_s\}$ um conjunto de inteiros positivos. Uma família $\mathfrak{F} \subset 2^{[n]}$ é L-intersectante se para qualquer $A \neq B \in \mathfrak{F}$, nós temos $|A \cap B| \in L$. Prove que

$$|\mathfrak{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$$

[Dica: Para cada $A_i \in \mathfrak{F}$, seja $a_i \in \mathbb{R}^n$ tal que a j-ésima entrada é 1, se $j \in A_i$, e 0 caso contrário. Considere os polinômios

$$p_i = \prod_{l_j < |A_i|} (a_i \cdot x - l_j)$$

Seja $\overline{p}_i$ a *multilinearização* de p_i, isso é, o mesmo polinômio com todos os expoentes apagados (por exemplo, a multilinearização de $x^3y^2z + 2x^2$ é $xyz + 2z$). Prove, usando o critério triangular, que $\overline{p}_1, \overline{p}_2, \ldots, \overline{p}_m$ são linearmente independentes.]