Álgebra Linear

Combinatória resolvida com Álgebra

2023

1 Introdução

O objetivo desse material é introduzir certos conceitos de álgebra linear aplicados a problemas de olimpíadas. As provas de cara teorema utilizados nesse material podem ser facilmente encontradas na internet (na Wikipédia, literalmente). Resolvi abster tais provas para evitar entrar em assuntos e conceitos primitivos demais e fugir do foco do material. Faça bom proveito e **SEMPRE** pense antes de ler qualquer dica ou solução.

2 Definições

Definição 1. Dada uma matriz $A_{n\times n}$, dizemos que A^{-1} é sua inversa se $A\times A^{-1} = A^{-1}\times A = I$, onde I é a matriz identidade:

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

Ainda, se B é uma matriz $m\times n$ com entradas $b_{i,j}$ nas casas de coordenadas (i,j), definimos B^t como a matriz $n\times m$ com entradas $b_{j,i}$ nas casas de coordenadas (i,j) e chamamos essa matriz de *matriz transposta de B*.

Definição 2. Dado um inteiro positivo n, definimos $[n] = \{1, 2, \dots, n\}$.

Definição 3. Dado $\sigma : [n] \to [n]$ uma permutação, sua paridade é definida como o número de inversões, i.e, de pares $i < j \in [n]$ tais que $\sigma(i) > \sigma(j)$.

Definição 4. Dada uma matriz n por n dada por $A = (a_{ij})$, definiremos a função determinante como

$$det(A) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{1\le k\le n} a_{k,\sigma(k)},$$

onde $\epsilon(\sigma)$ é 1 se σ é par e -1 caso contrário.

Definição 5. Dado um corpo K, dizemos que V é um espaço vetorial sobre K se:

- V é fechado em soma;
- V é fechado em multiplicação por escalar de K;
- Para qualquer $v \in V$, $1\cdot v = v$;
- A soma e a multiplicação são distributivas;

- A multiplicação é associativa.

(isso é importante)

Definição 6. Se V é um espaço vetorial sobre K, um conjunto de vetores $S \subseteq V$ é linearmente independente se a única combinação linear dos elementos de S igual igual a 0 é a combinação trivial, i.e, se $v_1, v_2, \dots, v_k$ são os elementos de S e $\alpha_1, \alpha_2, \dots, \alpha_k$ são elementos de K tais que

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0,$$

então $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$. Além disso, se o menor conjunto de vetores (por inclusão) que contém S e é um espaço vetorial (chamamos esse de subespaço gerado por S) for V, então dizemos que S é uma base de V e dizemos que a dimensão de V é $|S|$.

Definição 7. O rank-linha de uma matriz A é a dimensão do espaço vetorial gerado pelos vetores formados pelas linhas de A. A definição de rank-coluna é análoga.

3 Teoremas

Teorema 1. Uma matriz quadrada tem inversa se, e somente se, $det(A) \neq 0$.

Teorema 2. Se A e B são matrizes quadradas, então $det(AB) = det(A) \cdot det(B)$. Além disso, $det(A) = det(A^t)$.

Teorema 3. Se somamos a uma coluna uma combinação das outras colunas, o determinante da matriz não muda. O mesmo vale para as linhas.

Teorema 4. Se duas S e T são duas bases de um espaço V, então $|S| = |T|$, i.e, a dimensão de V é única.

Teorema 5. Para todo $n \geq 1$, a dimensão de $\mathbb{R}^n$ é exatamente n, e portanto quaisquer $n+1$ vetores em $\mathbb{R}^n$ são linearmente dependentes.

Teorema 6. Seja $V = \{v_1, v_2, \dots, v_n\}$ um conjunto de vetores de n entradas em um corpo K. Então V é uma base de K^n se, e somente se, o determinante da matriz formada pelos vetores de V não for 0.

Teorema 7. Para qualquer matriz A, o rank-linha é igual ao rank-coluna, e chamamos esse número de $rank(A)$.

Teorema 8. Para matrizes $A_{m\times n}$ e $B_{n\times r}$, sempre vale que $rank(A) \leq \min\{m, n\}$ e que $rank(AB) \leq \min\{rank(A), rank(B)\}$. Além disso, se $rank(A) = n$, então $rank(AB) = rank(B)$ e se $rank(B) = n$, então $rank(AB) = rank(A)$.

Teorema 9. Se v é um vetor e A é uma matriz quadrada com $det(A) \neq 0$, então existe exatamente um vetor w tal que $A \cdot w = v$.

Teorema 10. Se A é uma matriz quadrada com $det(A) = 0$ então existe $v \neq 0$ tal que $Av = 0$.

4 Problemas com Solução

Problema 1. Seja n um inteiro par e sejam $A_1, A_2, \dots, A_n$ subconjuntos distintos de $[n]$, de modo que $|A_i|$ é par para cada i. Mostre que existem i e j tais que $|A_i \cap A_j|$ é par.

Solução. Definimos para cada conjunto A_i o vetor $v_i = (a_{1,i}, a_{2,i}, \ldots, a_{n,i})$, onde o $a_{j,i} = 1$ se $j \in A_i$ e $a_{j,i}$ caso o contrário. Esse é o chamado *vetor de incidência* do conjunto A_i e ele nos "indica" que elementos estão ou não estão em A_i. Definiremos ainda a *matriz de incidência* dos conjuntos como a matriz quadrada

$$A = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

Por último, construiremos a *matriz de adjacência* de A como $M = A \cdot A^t$. Fazendo a multiplicação de matrizes concluímos que

$$M = \begin{pmatrix} |A_1| & |A_1 \cap A_2| & \ldots & |A_1 \cap A_n| \\ |A_2 \cap A_1| & |A_2| & \ldots & |A_2 \cap A_n| \\ \vdots & \vdots & \ddots & \vdots \\ |A_n \cap A_1| & |A_n \cap A_2| & \ldots & |A_n| \end{pmatrix}.$$

Agora, para seguir com o problema, começaremos a analisar o problema em $\mathbb{F}_2$ (inteiros módulo 2). Faz sentido, né? Um problema sobre paridade nos pede para analisar as coisas módulo 2. Suponhamos que toda interseção entre conjuntos é ímpar. Veja que:

$$det(M) = \begin{vmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 0 \end{vmatrix},$$

e, usando que n é par, somando cada coluna na primeira e depois somando a primeira coluna em todas as outras:

$$det(M) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 0 \end{vmatrix} = \begin{vmatrix} 1 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \ldots & 1 \end{vmatrix}$$

onde todas as entradas são 0, exceto a diagonal principal e a primeira coluna. Finalmente, se somamos cada coluna na primeira, concluímos que

$$\begin{vmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{vmatrix} = \left| I \right| = 1.$$

Portanto, temos que $det(A \cdot A^t) = 1$, e como $det(A \cdot A^t) = det(A) \cdot det(A^t) = det(A)^2$, concluímos que $det(A) = 1$. Por outro lado, olhando para A, se somamos cada coluna na primeira, como $|A_i| = 0$, temos que

$$det(A) = \begin{vmatrix} 0 & a_{2,1} & \dots & a_{n,1} \\ 0 & a_{2,2} & \dots & a_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{2,n} & \dots & a_{n,n} \end{vmatrix} = 0,$$

pela definição 4 (todo produto terá um 0). Isso nos dá um absurdo, donde concluímos o problema.■

Problema 2. Seja S um conjunto finito de reais no intervalo $[0, 1]$ de modo que 0 e 1 pertencem a S e cada distância entre elementos aparece ao menos duas vezes entre elementos de S, exceto a distância 1. Prove que S só tem números racionais.

Solução. Esse é um problema bem interessante, e com uma solução mais interessante ainda. A ideia é construirmos uma base finita $B = \{b_1, b_2, \dots, b_m\} \subset \mathbb{R}$ de modo que cada elemento de $s \in S$ pode ser escrito de maneira única como

$$s = \sum_{b \in B} \lambda_{s,b} b,$$

onde cada λ_x é um racional. Veja que podemos fazer isso porque S é finito. Então podemos tomar $B = \emptyset$ e vamos adicionando elemento a elemento em B se ele não puder ser escrito como combinação dos elementos de B com coeficientes racionais. Veja que, se em algum momento adicionamos um b_k e algum elemento $s \in S$ puder ser escrito de ao menos duas vezes, tome o primeiro momento em que isso acontece, digamos

$$\sum_{1 \le i \le k} \lambda_{s,b_i} b_i = s = \sum_{1 \le i \le k} \lambda'_{s,b_i} b_i.$$

Se $\lambda_{s,b_k} = \lambda'_{s,b_k}$, como as combinações são distintas, existe algum $\lambda_{s,b_j} \neq \lambda'_{s,b_j}$, e portanto

$$(\lambda_{s,b_j} - \lambda'_{s,b_j}) b_j = \sum_{1 \le i \le k-1,\ i \neq j} (\lambda_{s,b_i} - \lambda'_{s,b_i}) b_i,$$

o que é um absurdo, pois quando dividimos por $\lambda_{s,b_j} - \lambda'_{s,b_j}$, temos que b_j será combinação linear de coeficientes racionais dos $b_1, b_2, \dots, b_{k-1}$, contradizendo a minimalidade do k.
Se $\lambda_{s,b_k} \neq \lambda'_{s,b_k}$, então de maneira análoga ao caso anterior, provamos que b_k é combinação linear dos $b_1, b_2, \dots, b_{k-1}$. Isso implica, portanto, que o número que "precisaria" do b_k para ser escrito como combinação linear dos b_i's já poderia ter sido escrito antes sem ter o $b_k \in B$. Portanto, $B/\{b_k\}$ consegue escrever de maneira única todos os caras que B estava escrevendo. Assim, garantimos que cada vez que adicionamos alguém, podemos garantir que todos são escritos de maneira única. Como cada elemento novo que adicionamos aumenta em no mínimo 1 a "imagem" de B em S, garantimos que uma hora conseguimos cobrir todos os elementos de S de maneira

única. Esse conjunto B pode ser visto como uma base sobre o conjunto S no corpo $\mathbb{Q}$.
Veja que podemos construir B com $1 \in B$. Seja $b \in B$ um elemento qualquer da base. Tomemos x sendo o maior elemento de S tal que $\lambda_{x,b} = \max\{\lambda_{s,b} \mid s \in S\}$ e seja y o menor elemento de S tal que $\lambda_{x,b} = \max\{\lambda_{s,b} \mid s \in S\}$. Sejam u e v em S tais que $x - y = u - v$, olhando para os coeficientes de b na representação de cada número, temos que

$$\lambda_{x,b} - \lambda_{y,b} = \lambda_{u,b} - \lambda_{v,b},$$

e portanto $\lambda_{x,b} = \lambda_{u,b}$ e $\lambda_{y,b} = \lambda_{v,b}$. Porém, pela maximalidade e minimalidade de x e y, teremos que $x = u$ e $y = v$. Isso implica, então, que $x = 1$ e $y = 0$. Porém, como todos os λ de 1 e 0 são 0, exceto possivelmente pelo que acompanha o $1 \in B$, então todos os λ que acompanham os elementos de $B/\{1\}$ são 0, donde $B = \{1\}$. Isso implica que S só tem números racionais, como queríamos demonstrar. ■

Problema 3. Sejam $a_1, a_2, \ldots, a_{2n+1}$ reais tais que se apagamos qualquer um deles, podemos particionar os $2n$ restantes em dois grupos de n números com soma igual. Prove que todos os reais são iguais.

Solução. Veja que esse enunciado é análogo a existirem $\{\epsilon_{i,j} \mid 1 \leq i, j \leq 2n+1\}$, onde $\epsilon_{i,i} = 0$ e $\epsilon_{i,j} = \pm 1$ para $i \neq j$ tais que o sistema

$$\begin{cases} \epsilon_{1,1}a_1 + \epsilon_{1,2}a_2 + \epsilon_{1,3}a_3 + \cdots + \epsilon_{1,2n+1}a_{2n+1} = 0; \\ \epsilon_{2,1}a_1 + \epsilon_{2,2}a_2 + \epsilon_{2,3}a_3 + \cdots + \epsilon_{2,2n+1}a_{2n+1} = 0; \\ \epsilon_{3,1}a_1 + \epsilon_{3,2}a_2 + \epsilon_{3,3}a_3 + \cdots + \epsilon_{3,2n+1}a_{2n+1} = 0; \\ \vdots \\ \epsilon_{2n+1,1}a_1 + \epsilon_{2n+1,2}a_2 + \epsilon_{2n+1,3}a_3 + \cdots + \epsilon_{2n+1,2n+1}a_{2n+1} = 0, \end{cases}$$

e que $\sum_{1 \leq i \leq 2n+1} \epsilon_{j,i} = 0$. Porém, esse sistema tem infinitas soluções, já que $a_1 = a_2 = \cdots = a_{2n+1} = c$, para qualquer c real é uma solução. Uma forma que temos que nos livrar disso é fixar $a_1 = c$.
Agora, queremos provar que só temos uma solução ao sistema, e como todos iguais é uma solução, isso acabaria o problema. Para isso, provaremos que o sistema

$$\begin{cases} a_1 = c; \\ \epsilon_{2,1}a_1 + \epsilon_{2,2}a_2 + \epsilon_{2,3}a_3 + \cdots + \epsilon_{2,2n+1}a_{2n+1} = 0; \\ \epsilon_{3,1}a_1 + \epsilon_{3,2}a_2 + \epsilon_{3,3}a_3 + \cdots + \epsilon_{3,2n+1}a_{2n+1} = 0; \\ \vdots \\ \epsilon_{2n+1,1}a_1 + \epsilon_{2n+1,2}a_2 + \epsilon_{2n+1,3}a_3 + \cdots + \epsilon_{2n+1,2n+1}a_{2n+1} = 0, \end{cases}$$

tem apenas uma solução. Assim, provaremos que, se

$$A = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ \epsilon_{2,1} & 0 & \epsilon 2, 3 & \dots & \epsilon_{2,2n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \epsilon_{2n+1,1} & \epsilon_{2n+1,2} & \epsilon 2n+1, 3 & \dots & 0 \end{pmatrix},$$

provaremos que $det(A) \neq 0$. Para isso, provaremos que $det(A)$ é ímpar. Como a primeira linha tem 1 e depois só 0, temos que, olhando mód. 2:

$$det(A) = \begin{vmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 0 \end{vmatrix},$$

onde a matriz é $2n \times 2n$. Essa é a mesma matriz do problema 1, e sabemos que o determinante dela é ímpar, donde segue que $det(A)$ é ímpar, e portanto não é zero. Porém, queremos achar uma solução $(a_1, a_2, \dots, a_{2n+1})$ tal que

$$A \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{2n+1} \end{pmatrix} = \begin{pmatrix} c \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\iff \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{2n+1} \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} c \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

donde segue que o vetor $(a_1, a_2, \dots, a_{2n+1}$ é único. Como já vimos, isso conclui o problema. ■

5 Problemas

Problema 1. Sejam $A_1, A_2, \dots, A_{n+1}$ subconjuntos distintos de $[n]$, cada um com 3 elementos. Mostre que existem dois deles cuja interseção tem exatamente 1 elemento.

Problema 2. Seja $n \geq 3$ e A_n e B_n são o conjunto das permutações pares e impares de $[n]$, respectivamente. Mostre que

$$\sum_{\sigma \in A_n} \sum_{1 \leq k \leq n} |i - \sigma(i)| = \sum_{\sigma \in B_n} \sum_{1 \leq k \leq n} |i - \sigma(i)|.$$

Problema 3. Seja n um inteiro positivo. Um tabuleiro $n \times n$ é colorido de preto e branco de forma que podemos escolher um conjunto de colunas $C = \{C_1, C_2, \dots, C_k\}$ de modo que se escolhemos qualquer linhas do tabuleiro, o número de casas brancas dessa linha que pertencem a alguma coluna de C é par. Mostre que podemos escolher um conjunto L de linhas de forma se escolhemos qualquer coluna do tabuleiro, o número de casas brancas nessa coluna que pertencem a alguma linha de L é par.

Problema 4. Sejam $A_1, A_2, \ldots, A_{n+1}$ subconjuntos distintos de $[n]$. Mostre que existem índices $a_1, a_2, \ldots, a_k$ e $b_1, b_2, \ldots, b_j$ tais que

$$A_{a_1} \cup A_{a_2} \cup \cdots \cup A_{a_k} = A_{b_1} \cup A_{b_2} \cup \cdots \cup A_{b_j}.$$

Problema 5. Seja G um grafo completo. Mostre que não é possível particionar G em menos que $n-1$ subgrafos completos bipartidos. (cada aresta pertence a exatamente um subgrafo)

Problema 6. Seja p um número primo. Suponha que os reais $a_1, a_2, \ldots, a_{p+1}$ tenham a propriedade de que, sempre que um deles é deletado, os demais podem ser separados em dois grupos de modo que cada um tenha a mesma média aritmética. Mostre que todos os a_i's são iguais.

Problema 7. Uma cidade possui uma população de n habitantes que adoram formar diferentes clubes. Para limitar o número de clubes, o prefeito da cidade adotou as seguintes regras:

- Todo clube deve ter um número ímpar de membros;
- Quaisquer dois clubes devem ter um número par de membros em comum.

Qual é a quantidade máxima de clubes que pode ser formada?

Problema 8. Num concurso há m candidatos e n juízes, onde $n \geq 3$ é ímpar. Cada candidato é avaliado por cada juiz, podendo ser aprovado ou reprovado. Sabe-se que os julgamentos de cada par de juízes coincidem em no máximo k candidatos. Prove que

$$\frac{k}{m} \geq \frac{n-1}{2n}.$$

Problema 9. Sejam $m > n \geq 2$ inteiros positivos. Sejam $A_1, A_2, \ldots, A_m$ subconjuntos distintos de $[n]$. Mostre que existem índices distintos i e j tais que $|A_i \cap A_j| \neq 1$.

Problema 10. Seja G um grafo com todos os vértices sendo lâmpadas apagadas. Uma operação possível é escolher uma lâmpada e trocar seu estado (acesa $\leftrightarrow$ apagada) e o de todas as lâmpadas vizinhas. Mostre que podemos, em finitas operações, deixar todas as lâmpadas acesas.

Problema 11. Mostre que existe uma função bijetora $f : \mathbb{R} \to \mathbb{R}$ tal que se $x < y < z$, então $f(y) \neq \frac{f(x)+f(z)}{2}$.

Problema 12. Sejam n e k inteiros positivos com $k \leq n$. Em um grupo de n pessoas, cada uma ou sempre fala a verdade ou sempre mente. Arnaldo pode fazer perguntas para quaisquer dessas pessoas desde que essas perguntas sejam do tipo: "No conjunto A, qual a paridade de pessoas que falam de verdade?", onde A é um subconjunto de tamanho k do conjunto das n pessoas. A resposta só pode ser "par" ou "ímpar". Suponha que seja possível determinar, em finitas perguntas, que pessoas mentem e que pessoas falam a verdade. Qual o número mínimo de perguntas necessárias para determinar a confiabilidade de cada pessoa?

6 Referências

- Problems from the book - Titu Andreescu;

- Wikipédia :