Aventuras Combinatórias na Matrix

1. Matrizes e Combinatória: tudo a ver?

Embora não pareça, muitos resultados de Combinatória podem ser demonstrados com o auxílio da Álgebra Linear e vice-versa. O intuito aqui é explorar essa interessante interação entre matrizes e Combinatória.

2. Por que matrizes aparecem na Combinatória?

Essas duas áreas da Matemática, apesar de serem bastante diferentes, têm um ponto de ligação bastante forte: a Combinatória, essencialmente, visa *organizar*. E uma matriz é exatamente uma espécie de tabela, ou seja, é organizada por natureza. Assim, por que as matrizes não podem dar uma mãozinha na Combinatória?

E o melhor é que Álgebra Linear e Combinatória, exatamente por serem duas áreas bem diferentes, quando combinadas nos dão muitos resultados interessantes.

3. Matrizes e grafos: matriz de adjacência e árvores geradoras

Um grafo é um par $(V; E)$ de conjuntos, sendo que $E \subset \big\{\{v_i; v_j\} \mid v_i, v_j \in V, v_i \neq v_j\}\big\}$. Falando de modo mais simples, um grafo consiste de dois conjuntos, um de *vértices* e outro de *arestas*, sendo que obtemos uma aresta é um par de vértices. Normalmente, representamos um grafo com pontos como vértices e uma linha ligando dois pontos para cada aresta correspondente.

Os grafos têm muitas aplicações não só em Matemática, mas principalmente em Computação também. Afinal, muitos problemas podem ser modelados com grafos, como construir a menor rede de estradas que ligam cidades. Note que podemos trocar "estradas" e "cidades" por "roteamento" e "computadores", de modo que a aplicabilidade de grafos a redes de computadores é extremamente vasta.

Então, como um computador reconhece e guarda grafos? Uma maneira (mas não a única) é utilizar matrizes.

A partir daqui, vamos trabalhar somente com grafos com um número finito de vértices.

No que se segue, $n = |V|$ é a quantidade de vértices e $m = |E|$ é a quantidade de arestas.

Definição 3.1. *Matriz de incidência de um grafo é uma matriz $B_{n\times m}$, sendo que associamos a cada linha um vértice e a cada coluna uma aresta. Cada entrada da matriz é definida por*

$$b_{ij} = \begin{cases} 1, & \text{se o vértice } i \text{ está na aresta } j \\ 0, & \text{caso contrário} \end{cases}$$

Definição 3.2. *Matriz de adjacência de um grafo é a matriz $A_{n\times n} = C \cdot C^t$, em que C é obtida de B trocando o sinal de um dos* 1 *em cada coluna.*

Lema 3.1. *A matriz de adjacência A de um grafo é simétrica, com*

$$a_{ij} = \begin{cases} g_i, & \text{se } i = j \\ -1, & \text{se } \{i, j\} \text{ é uma aresta} \\ 0, & \text{caso contrario} \end{cases},$$

sendo g_i o grau do vértice i, isto é, o número de arestas que contêm i.

Demonstração

O elemento a_{ij} da matriz $C \cdot C^t$ é o produto interno das linhas i e j. Observemos que a linha i consiste de 1's e -1's nas colunas correspondentes às arestas que contêm i. O produto interno da linha i com ela mesma

é, considerando ainda que os -1's multiplicam-se com eles mesmos, a quantidade de arestas que contêm o vértice i, ou seja, $a_{ii} = g(i)$.

Considerando que cada coluna só tem duas entradas não nulas, uma igual a 1 e outra, a -1, cada parcela do produto interno de duas linhas distintas i e j só não é nula quando há uma aresta ligando i e j, sendo igual, nesse caso, a $1 \cdot (-1) = -1$. Essa é, se existir, a única parcela não nula, pois há no máximo uma aresta ligando quaiquer dois vértices. Logo, para $i \neq j$, $a_{ij} = -1$ quando $\{i; j\}$ é uma aresta e 0, caso contrário. ∎

Precisamos definir árvores e de alguns fatos sobre elas.

Definição 3.3. *Uma árvore é um grafo conexo (isto é, dados quaisquer dois vértices u e v do grafo, existe um caminho que os liga) e acíclico (isto é, que não contém ciclos).*

Lema 3.2. *Uma árvore tem pelo menos um vértice de grau* 1.

Demonstração

Suponha por absurdo que nenhum vértice da árvore tenha grau 1, ou seja, que tenham grau pelo menos 2. Tome um vértice v e considere um vértice vizinho w (ou seja, ligado a v por uma aresta). Como w tem grau pelo menos 2, existe um vértice $z \neq v$ vizinho de w. Tome z e repita o procedimento, isto é, escolha um vértice diferente de w vizinho de z. Continue a repetir o procedimento. Em algum momento escolheremos um vértice que já foi escolhido antes; nesse momento, fechamos um ciclo. Absurdo. ∎

Lema 3.3. *Uma árvore com n vértices tem $n - 1$ arestas.*

Demonstração

Indução sobre n. Para $n = 1$ não há o que demonstrar; se $n > 1$, suponha que o resultado é válido para $n - 1$ vértices. Tome um vértice de grau 1 (que existe pelo lema anterior) e retire esse vértice e a aresta que sai dele. Temos um vértice a menos ($n - 1$) e uma aresta a menos, e obtemos uma árvore de $n - 1$ vértices e, pela hipótese de indução, n arestas. Recoloque o vértice e a aresta e o resultado segue. ∎

Lema 3.4. *Uma árvore tem pelo menos dois vértices de grau* 1.

Demonstração

Decorre do lema anterior e do fato de que a soma dos graus dos vértices de um grafo é igual ao dobro do número de arestas. Se temos no máximo um vértice de grau 1, a soma dos graus dos n vértices de uma árvore é pelo menos $1 + 2(n - 1) = 2n - 1$, que á maior que o dobro do número de arestas, que é $2(n - 1)$. ∎

Agora, vamos ao resultado principal.

Teorema 3.1. *O número de árvores geradoras que são subgrafos de um grafo com vértices numerados é igual a* $\det M_{ii}$ *para $i = 1, 2, \ldots, n$, sendo M_{ii} a matriz obtida retirando-se a i-ésima linha e a i-ésima coluna.*

Aqui, duas demonstrações. A primeira baseada em Álgebra Linear e a segunda, baseada em técnicas de grafos, ou seja, indução.

Primeira demonstração (Álgebra Linear)

Utilizaremos a fórmula de Binet-Cauchy (que podemos demonstrar, ironicamente, com argumentos combinatórios semelhantes aos da última seção): se $P_{r \times s}$ e $Q_{s \times r}$ são matrizes, então

$$\det(P \cdot Q) = \sum_{\mathcal{Z}} \det P_{\mathcal{Z}} \cdot \det Q_{\mathcal{Z}},$$

em que $P_{\mathcal{Z}}$ é uma submatriz $r \times r$ de P tomando-se as colunas do conjunto $\mathcal{Z}$ e $Q_{\mathcal{Z}}$ é a submatriz de Q tomando-se as r linhas correspondentes do mesmo conjunto $\mathcal{Z}$. A soma é sobre todos os subconjuntos de r elementos de $\{1, 2, \ldots, s\}$.

No nosso caso, sendo $M_{ii} = C_i \cdot C_i^t$, sendo C_i a matriz obtida retirando-se a linha i da matriz de incidência C,

$$\det M_{ii} = \sum_{\mathcal{Z}} \det C_{\mathcal{Z}} \cdot \det C_{\mathcal{Z}}^t = \sum_{\mathcal{Z}} (\det C_{\mathcal{Z}})^2$$

Observe que $\mathcal{Z}$ é um subconjunto de $n-1$ colunas de $\{1, 2, \ldots, m\} \setminus \{i\}$, o que, em termos de grafos, é o mesmo que escolher $n-1$ arestas do grafo correspondente. Afirmamos que $\det C_{\mathcal{Z}} = \pm 1$ quando essas $n-1$ arestas determinam uma árvore no grafo e 0 caso contrário.

Caso as $n-1$ arestas não formem uma árvore (ou seja, não é conexo e acíclico), o grafo resultante não é conexo (o grafo não pode ser conexo e conter um ciclo; se isso acontecesse, teria mais de $n-1$ arestas). Tome uma das componentes conexas do grafo que não contém i. A soma das linhas correspondentes em $C_{\mathcal{Z}}$ é zero, pois essas linhas formam, separadamente, uma matriz de incidência dessa componente conexa unida a uma bloco de zeros. Portanto, nesse caso, $\det C_{\mathcal{Z}} = 0$.

Caso as $n-1$ arestas formem uma árvore, tome um vértice, diferente de i, de grau 1. Troque as linhas da matriz $C_{\mathcal{Z}}$ de modo que esse vértice fique na primeira linha e a aresta que o contém fique na primeira coluna. Note que, na primeira linha, todas as entradas após a primeira coluna são nulas. Tire esse vértice e essa aresta do grafo e repita o procedimento, colocando agora o próximo vértice de grau 1 na segunda linha e a aresta correspondente na segunda coluna. Continue o procedimento até acabarem-se os vértices. Note que obtemos uma matriz triangular superior, cujo determinante é, portanto, ± 1. Como transpor linhas e colunas mantém o determinante a menos de sinal, $\det C_{\mathcal{Z}} = \pm 1$ nesse caso.

Para terminar, vamos ver a identidade

$$\det M_{ii} = \sum_{\mathcal{Z}} (\det C_{\mathcal{Z}})^2$$

com olhos combinatórios: a soma é sobre todos os conjuntos de $n-1$ arestas do grafo, sendo que cada parcela $(\det C_{\mathcal{Z}})^2$ é igual a 1 se as $n-1$ arestas determinam uma árvore e 0, caso contrário; ou seja, cada parcela é um "marcador de árvores". Desse modo, $\det M_{ii}$ é realmente igual ao número de árvores do grafo. ∎

Segunda demonstração (Teoria dos Grafos)

Uma das principais técnicas de demonstração em grafos é indução. Isso ocorre porque grafos, tendo definições tão gerais, tendem a não ter muita estrutura. O que funciona bem para encontrar estrutura em entidades com pouca estrutura? Indução! E muitas dessas induções acabam gerando algoritmos ou vice-versa.

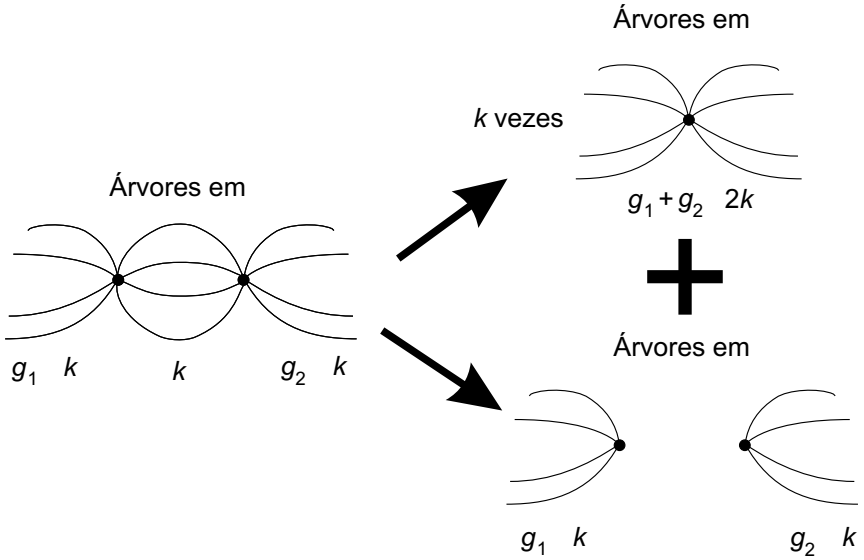
Primeiro, vamos generazilar o problema para *multigrafos*: um *multigrafo* é o mesmo que um grafo, mas com a diferença de que é possível ligar dois vértices com *mais de uma aresta*. A definição de grau continua a mesma: é a quantidade de arestas que contém o vértice. As definições de matriz de incidência e adjacências continuam iguais também: a única diferença é que, na matriz de incidência, se há k arestas ligando i e j, colocamos k colunas com 1 nas linhas i e j. Ao construir a matriz de adjacência A, na hora de designar sinais às arestas, o principal cuidado é de designar a mesma orientação a arestas que ligam os mesmos vértices, de modo que

$$a_{ij} = \begin{cases} g_i, & \text{se } i = j \\ -k, & \text{sendo } k \text{ o número de arestas que ligam } i \text{ e } j \\ 0, & \text{caso contrario} \end{cases},$$

sendo g_i o grau do vértice i.

Vamos provar o resultado generalizado para multigrafos por indução sobre arestas. Quando não há arestas, o resultado é óbvio, dado que a matriz de adjacência é nula. Suponha, agora, que temos um multigrafo e que o resultado é válido para multigrafos com menos arestas. Se todas as arestas contêm i, o resultado é simples de demonstrar e fica como exercício (é só notar que M_{ii}, nesse caso, é uma matriz diagonal). Caso contrário, tome dois vértices v e w, diferentes de i, ligados por $k > 0$ arestas. Classifique as árvores em dois tipos: as que contém uma aresta ligando v e w e as que não contém. A quantidade de árvores do primeiro tipo pode ser calculada *contraindo-se* os vértices v e w, isto é, tomando o grafo com um vértice

u no lugar de v e w, sem as k arestas os ligando, e mantendo as demais arestas, sendo que arestas ligadas a v e w são doravante ligados a u; a quantidade de árvores do segundo tipo pode ser calculada utilizando a hipótese de indução para o grafo obtido deletando-se as k arestas ligando v e w. Para facilitar as contas, vamos supor, sem perda de generalidade, que v e w correspondem à primeira e segunda linhas da matriz M_{ii}.



Note que se a árvore contém uma aresta ligando u e w, podemos escolhê-la de k maneiras; por isso multiplicamos o número de árvores do primeiro tipo por k.

A matriz de adjacência (sem linha e coluna i) que conta árvores do primeiro tipo é

$$X_{n-2\times n-2} = \begin{pmatrix} g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t+\ell_2^t & P \end{pmatrix},$$

sendo g_1 o grau de v, g_2 o grau de w, ℓ_1, ℓ_2, ℓ_1^t e ℓ_2^t respectivamente a primeira linha, a segunda linha, a primeira coluna e a segunda coluna de M_{ii} sem suas duas primeiras entradas e P a submatriz de M_{ii} obtida retirando a primeira e a segunda linhas e a primeira e a segunda colunas de M_{ii}.

A matriz de adjacência (sem linha e coluna i) que conta árvores do segundo tipo é

$$Y_{n-1\times n-1} = \begin{pmatrix} g_1-k & 0 & \ell_1 \\ 0 & g_2-k & \ell_2 \\ \ell_1^t & \ell_2^t & P \end{pmatrix}$$

Assim, temos que provar que

$$\begin{vmatrix} g_1 & -k & \ell_1 \\ -k & g_2 & \ell_2 \\ \ell_1^t & \ell_2^t & P \end{vmatrix} = k \cdot \begin{vmatrix} g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t+\ell_2^t & P \end{vmatrix} + \begin{vmatrix} g_1-k & 0 & \ell_1 \\ 0 & g_2-k & \ell_2 \\ \ell_1^t & \ell_2^t & P \end{vmatrix}$$

Mas isso é só uma conta:

$$
\begin{aligned}
& k \cdot \begin{vmatrix} g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t+\ell_2^t & P \end{vmatrix} + \begin{vmatrix} g_1-k & 0 & \ell_1 \\ 0 & g_2-k & \ell_2 \\ \ell_1^t & \ell_2^t & P \end{vmatrix} \\
= & \begin{vmatrix} k & 0 & 0 \\ g_1-k & g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t & \ell_1^t+\ell_2^t & P \end{vmatrix} + \begin{vmatrix} g_1-k & g_1-k & \ell_1 \\ 0 & g_2-k & \ell_2 \\ \ell_1^t & \ell_1^t+\ell_2^t & P \end{vmatrix} \\
= & \begin{vmatrix} k & 0 & 0 \\ g_1-k & g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t & \ell_1^t+\ell_2^t & P \end{vmatrix} + \begin{vmatrix} g_1-k & g_1-k & \ell_1 \\ g_1-k & g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t & \ell_1^t+\ell_2^t & P \end{vmatrix} \\
= & \begin{vmatrix} g_1-k+k & g_1-k & \ell_1 \\ g_1-k & g_1+g_2-2k & \ell_1+\ell_2 \\ \ell_1^t & \ell_1^t+\ell_2^t & P \end{vmatrix} \\
= & \begin{vmatrix} g_1 & g_1-k & \ell_1 \\ (g_1-k)-g_1 & (g_1+g_2-2k)-(g_1-k) & (\ell_1+\ell_2)-\ell_1 \\ \ell_1^t & \ell_1^t+\ell_2^t & P \end{vmatrix} \\
= & \begin{vmatrix} g_1 & (g_1-k)-g_1 & \ell_1 \\ -k & (g_2-k)-(-k) & \ell_2 \\ \ell_1^t & (\ell_1^t+\ell_2^t)-\ell_1^t & P \end{vmatrix} \\
= & \begin{vmatrix} g_1 & -k & \ell_1 \\ -k & g_2 & \ell_2 \\ \ell_1^t & \ell_2^t & P \end{vmatrix}
\end{aligned}
$$

∎

O interessante é que esse resultado é relacionado com:

3.1. Um problema da vingança olímpica

Problema (Vingança Olímpica). *Seja A uma matriz simétrica tal que a soma de cada linha é zero. Mostre que a diagonal da matriz co-fatora de A possui todas as entradas iguais.*

Obs.: a matriz co-fatora de uma matriz quadrada $A = (a_{ij})$ é igual a $B = (b_{ij})$, onde $b_{ij} = (-1)^{i+j} \det A_{ij}$.

Resolução

A matriz do problema é muito semelhante à matriz de adjacência, não? E as co-fatoras das diagonais correspondem exatamente ao número de árvores! Então, no caso particular em que as entradas da matriz são inteiras, com elementos da diagonal principal não negativos e elementos fora da diagonal principal não positivos.

Como generalizamos? Considere um grafo completo K_n (isto é, um grafo no qual ligamos por uma aresta *todos* os pares de vértices) com tantos vértices quanto a ordem da matriz A. Associe à aresta que liga os vértices $i \neq j$ o número a_{ij}, o que não é problema já que a matriz é simétrica. Por fim, defina o *neograu* do vértice i como o oposto da soma dos números associados a arestas que contêm i.

Por fim, associe a cada subárvore do grafo o produto dos números correspondentes às arestas.

A matriz A é agora uma espécie de matriz de adjacência desse grafo e, utilizando uma demonstração completamente análoga à segunda prova do teorema acima (pode conferir!), resolvemos esse problema. ∎

4. Uma desigualdade útil sobre postos

Um fato bem conhecido da Álgebra Linear é

Lema 4.1. *Seja $p(M)$ o posto da matriz M. Então $p(AB) \leq p(A)$ e $p(AB) \leq B$.*

Podemos usar esse fato para provar algumas desigualdades em Combinatória.

4.1. Posto e block designs

Primeiro, temos que definir block design.

A origem dessa definição vem da Estatística. Um exemplo mostra melhor por quê: suponha que queremos comparar v marcas de café. Para que os testes sejam justos é natural que imponhamos que

(1) Cada pessoa experimenta o mesmo número (digamos, k) de marcas, de modo que cada pessoa tenha o mesmo peso na decisão;

(2) Cada par de marcas é experimentado pela mesma quantidade (digamos, λ) de pessoas, de modo que cada variedade tenha o mesmo tratamento.

Note que quando v é grande, não é prático que todas as pessoas experimentem todas as marcas de café (você já pensou em experimentar, digamos, 2006 marcas de café? É cafeína para deixar de dormir para o resto da vida!).

Definição 4.1. *Seja $S = \{1, 2, \ldots, v\}$. Uma coleção $\mathcal{D}$ de subconjuntos de S é um (v, k, λ)-design se $2 \leq k < v$, cada conjunto de $\mathcal{D}$ tem k elementos e cada par de elementos de S está contido em exatamente λ dos conjuntos de $\mathcal{D}$. Os elementos de $\mathcal{D}$ são chamados blocos.*

Um dos problemas básicos na teoria de block designs é determinar para que valores de v, k e λ existe um (v, k, λ)-design. O próximo lema nos dá uma condição necessária, mas não suficiente.

Lema 4.2. *Seja b a quantidade de conjuntos no (v, k, λ)-design $\mathcal{D}$. Então cada elementos de S pertence a r blocos, sendo $r(k-1) = \lambda(v-1)$. Além disso, $bk = vr$.*

Demonstração

Suponha que um elemento a de S pertence a r_a blocos. Contemos de duas maneiras o número de pares $(\{a, x\}, B)$ em que $a, x \in B$ e $B \in \mathcal{D}$. Contando por B, tal quantidade é $r_a(k-1)$, já que há r_a maneiras de escolher o conjunto B e $k-1$ maneiras de escolher x. Por outro lado, contando por $\{a, x\}$, há $v-1$ escolhas para x e λ conjuntos que contêm ambos x e a, sendo que a quantidade de pares é $\lambda(v-1)$. Portanto $r_a(k-1) = \lambda(v-1)$. Note que r_a não depende de a, portanto, a primeira parte está provada.

A segunda relação é mais uma contagem dupla: agora contamos os pares (x, B), em que $x \in B$ e $B \in \mathcal{D}$. Contando por D, há b escolhas para D e k escolhas para $x \in D$. Logo há bk pares. Contando por x, há v escolhas para x e r escolhas para $D \ni x$. Logo há vr pares e $bk = vr$. ∎

Definimos matriz de incidência também para block designs.

Definição 4.2. *Matriz de adjacência de um (v, k, λ)-design é uma matriz $B = (b_{ij})_{v \times b}$ na qual associamos cada linha a um elemento de S e cada coluna a um bloco, e*

$$b_{ij} = \begin{cases} 1 & \text{se } i \text{ pertence ao bloco } j \\ 0 & \text{caso contrário} \end{cases}$$

Lema 4.3. $B \cdot B^t = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{pmatrix}$.

Demonstração

O elemento a_{ij} do produto é o produto interno das linhas i e j. Se $i = j$, é simplesmente o número de uns na linha i, que é o número de blocos que contêm i, ou seja, r. Se $i \neq j$, é o número de blocos que contêm i e j, ou seja, λ. ∎

Agora usamos um resultado da Álgebra Linear para provar uma desigualdade interessante.

Teorema 4.1. *(Desigualdade de Fisher). Se existe um $(v, k\lambda)$-design então $b \geq v$, ou seja, a quantidade de blocos é maior ou igual à quantidade de elementos de S.*

Em termos de café: precisamos de pelo menos tantos provadores quanto marcas de café.

Demonstração

Observe que o posto da matriz de incidência B (e de sua transposta B^t) é no máximo a menor dimensão de B. Assim, o posto de $B \cdot B^t$ é menor ou igual a ambos v e b.

Calculemos $\det(B \cdot B^t)$:

$$\det(B \cdot B^t) = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{vmatrix} = \begin{vmatrix} r & \lambda - r & \lambda - r & \cdots & \lambda - r \\ \lambda & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & r - \lambda \end{vmatrix}$$

$$= \begin{vmatrix} r + (v-1)\lambda & 0 & 0 & \cdots & 0 \\ \lambda & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & r - \lambda \end{vmatrix} = (r + (v-1)\lambda)(r - \lambda)^{v-1} = rk(r - \lambda)^{v-1}$$

Como $r(k-1) = \lambda(v-1)$ e $k < v$, então $r > \lambda$. Logo $\det(B \cdot B^t)$ não é nulo, ou seja, o posto dessa matriz é v. Logo, pela desigualdade do posto, $p(B \cdot B^t) \leq p(B) \iff v \leq b$. ∎

Designs e matrizes têm muitas relações. Deixamos aqui alguns exercícios para você treinar um pouco.

Exercícios

01. Uma matriz $H_{m \times m}$ cujas entradas são 1 ou -1 é chamada *de Hadamard* quando $H \cdot H^t = mI$, sendo I a identidade. Prove que se $m > 2$ então m é múltiplo de 4.

Dica: prove que podemos supor, sem perda de generalidade, que a primeira linha de H tem todas as entradas iguais a 1; depois, prove que a quantidade de 1's comuns a duas outras linhas quaisquer é $m/4$.

Observação: não se sabe se existem matrizes de Hadamard para todo múltiplo de 4. Conjectura-se que sim.

02. Qual a relação entre essas matrizes e block designs? É a seguinte: prove que existe um matriz de Hadamard de ordem $4n$ se, e somente se, existe uma matriz de Hadamard de ordem n, e que isso equivale a existir um $(4n-1, 2n-1, n-1)$-design.

Dica: a matriz de adjacência; use a matriz de adjacência, Luke.

03. Matrizes de Hadamard induzem códigos corretores de erros. Prove que os vetores correspondentes às linhas de uma matriz H de Hadamard de ordem m e às linhas de $-H$ (troque os -1's por zeros, se preferir) formam um $m/4 - 1$-código corretor de erros, ou seja, que quaisquer dois dos vetores citados acima diferem em pelo menos $m/2$ coordenadas.

04. Planos projetivos finitos induzem um design. Utilizando planos projetivos, prove que se q é uma potência de primo então existe um $(q^2+q+1, q+1, 1)$-design. Usando espaços projetivos, prove que existe um $\left(\frac{q^{m+1}-1}{q-1}, \frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}\right)$-design para m inteiro positivo e q potência de primo.

4.2. Posto e geometrias finitas

Geometrias finitas são aquelas com um número finito de pontos. Por incrível que pareça, essas geometrias têm aplicações interessantes em Teoria da Informação e Criptologia.

Suponha que um conjunto de usuários desejam se comunicar, via um sistema de telefonia. Tal sistema consiste de um conjunto de chaves que satisfazem as seguintes condições:

- Quaisquer dois usuários podem ser ligados diretamente por uma chave;
- Cada chave conecta pelo menos dois usuários;
- Há pelo menos duas chaves (uma chave só ficaria sobrecarregada).

A partir dessas restrições podemos modelar o problema através de *espaços lineares*.

Definição 4.3. *Um espaço linear consiste de um conjunto S de pontos e uma coleção $\mathcal{L}$ de retas (conjuntos de pontos contidos em S) tais que:*

- *Dois pontos quaisquer estão contidos em exatamente uma reta;*
- *Cada reta tem pelo menos dois pontos;*
- *Há pelo menos duas retas.*

Observe que se impusermos que cada ponto esteja contido na mesma quantidade de retas então teríamos um $(v, k, 1)$-design. Pelo teorema da seção anterior, a quantidade de retas é maior ou igual à quantidade de pontos. O fato é que esse resultado também é válido para espaços lineares em geral.

Teorema 4.2. *(Teorema de DeBrujin-Erdős). Num espaço linear, o número de retas é maior ou igual ao número de pontos.*

Demonstração

Defina a matriz de incidência A da mesma maneira que fizemos nas outras seções: sendo v o número de pontos e b o número de retas, A é uma matriz $v \times b$ com pontos como linhas e retas como colunas, sendo

$$a_{ij} = \begin{cases} 1 & \text{se o ponto } i \text{ pertence à reta } j \\ 0 & \text{caso contrário} \end{cases}$$

Calculemos, novamente, $A \cdot A^t$. O produto escalar de uma linha por ela mesma é o número de retas a que o ponto correspondente pertence, e o produto escalar entre duas linhas diferentes é o número de retas que contêm ambas, ou seja, 1.

Além disso, por cada ponto passa pelo menos duas retas. Suponha o contrário, ou seja, que por um ponto P passe somente uma reta. Nesse caso, a reta deve conter todos os pontos do espaço linear, já que por P e outro ponto qualquer passa exatamente uma reta. Mas isso implica o espaço linear ter exatamente uma reta, absurdo. Logo $a_{ii} = x_i + 1$, com $x_i > 0$.

Portanto

$$\det(A\cdot A^t)=\begin{vmatrix} x_1+1 & 1 & 1 & \cdots & 1\\ 1 & x_2+1 & 1 & \cdots & 1\\ 1 & 1 & x_3+1 & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots & \\ 1 & 1 & 1 & \cdots & x_v+1 \end{vmatrix}=\begin{vmatrix} x_1+1 & -x_1 & -x_1 & \cdots & -x_1\\ 1 & x_2 & 0 & \cdots & 0\\ 1 & 0 & x_3 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots & \\ 1 & 0 & 0 & \cdots & x_v \end{vmatrix}$$

$$=x_1x_2x_3\cdots x_v\cdot\begin{vmatrix} 1+\frac{1}{x_1} & -1 & -1 & \cdots & -1\\ \frac{1}{x_2} & 1 & 0 & \cdots & 0\\ \frac{1}{x_3} & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots & \\ \frac{1}{x_v} & 0 & 0 & \cdots & 1 \end{vmatrix}$$

$$=x_1x_2x_3\cdots x_v\cdot\begin{vmatrix} 1+\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}+\cdots+\frac{1}{x_v} & 0 & 0 & \cdots & 0\\ \frac{1}{x_2} & 1 & 0 & \cdots & 0\\ \frac{1}{x_3} & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots & \\ \frac{1}{x_v} & 0 & 0 & \cdots & 1 \end{vmatrix}$$

$$=x_1x_2x_3\cdots x_v\left(1+\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}+\cdots+\frac{1}{x_v}\right)\neq 0,$$

ou seja, o posto de $A\cdot A^t$ é v, que é menor ou igual ao posto de A que, por sua vez, é menor ou igual a b. Logo $v\leq b$. ∎

Exercícios

05. Prove que a igualdade na desigualdade que demonstramos ocorre se, e somente se, temos um plano projetivo ou o conjunto de pontos $S=\{1,2,\ldots,v\}$ com as retas $\{1,i\}$, $2\leq i\leq v$ e $S\setminus\{1\}$. Lembramos que um plano projetivo pode ser definido como um espaço linear que tem as seguintes duas propriedades a mais:

- Duas retas têm sempre interseção não vazia;
- Existem quatro pontos tais que quaisquer três não estão contidos numa mesma reta.

5. Sistemas lineares e decomposição de grafos

O teorema de DeBruijn-Erdős pode ser reescrito em termos de grafos:

Teorema de DeBruijn-Erdős em termos de grafos. *Se decompusermos um grafo completo K_v em b grafos completos diferentes de K_v, tal que toda aresta está em um único grafo completo, então $b\geq v$.*

De fato, é só pensar nos vértices como pontos grafos completos menores como retas! ∎

Um *grafo bipartido completo* $K_{a,b}$ é aquele cujo conjunto de vértices pode ser particionado em duas classes, uma com a vértices e a outra, com b vértices, de modo que dois vértices estão ligados se, e somente se, estão em classes diferentes.

Agora, o nosso problema é decompor um grafo completo em grafos bipartidos completos. Podemos dividir um K_n em $n-1$ grafos bipartidos $K_{1,n-1}$, $K_{1,n-2}$, …, $K_{1,1}$ (tente descobrir como). Será que dá para usar menos grafos bipartidos? A resposta é não.

Teorema 5.1. *Se K_n é decomponível em m subgrafos bipartidos completos então $m\geq n-1$.*

O mais interessante é que não se conhece nenhuma demonstração puramente combinatória para esse teorema; todas usam, de um modo ou de outro, Álgebra Linear.

Demonstração

Suponha que o grafo completo K_n, cujos vértices são $1, 2, \ldots, n$, é decomponível nos grafos bipartidos completos $H_1, H_2, \ldots, H_n$. Sejam A_j e B_j as classes de vértices de H_j.

A idéia deriva de funções geratrizes: associe ao vértice i a variável real x_i e à aresta ligando a e b o produto $x_a \cdot x_b$. Cada grafo bipartido H_j tem $|A_j||B_j|$ arestas (cada vértice de A_j está em $|B_j|$ arestas, uma para cada elemento de B_j), logo a soma das expressões das arestas é

$$\sum_{a \in A_j} x_a \cdot \sum_{b \in B_j} x_b$$

Somando todas as arestas, obtemos

$$\sum_{p<q} x_p x_q = \sum_{j=1}^{m} \left(\sum_{a \in A_j} x_a \cdot \sum_{b \in B_j} x_b \right)$$

Agora, vamos montar um sistema linear que faça com que a soma acima seja zero. Basta fazer, por exemplo, que $\sum_{a \in A_j} x_a = 0$ para $j = 1, 2, \ldots, m$. Obtemos, então $\sum_{p<q} x_p x_q = 0$. Fazemos também a soma de todas as variáveis ser nula, obtendo o sistema homogêneo de n variáveis reais e $m + 1$ equações

$$\left| \begin{array}{rl} x_1 + x_2 + \cdots + x_n = 0 & \\ \displaystyle\sum_{a \in A_j} x_a = 0 & (k = 1, 2, \ldots, m) \end{array} \right.$$

Suponha, por absurdo, que $m < n - 1$, ou seja, $n > m + 1$. Temos mais variáveis que equações, e portanto o sistema acima é indeterminado. Seja, então $(c_1, c_2, \ldots, c_n)$ uma solução não trivial do sistema. Então

$$0 = (c_1 + c_2 + \cdots + c_n)^2 = \sum_{p=1}^{n} c_p^2 + 2 \sum_{p<q} c_p c_q = \sum_{p=1}^{n} c_p^2 > 0,$$

absurdo. ∎

6. Matrizes e caminhos: o problema 6 da OBM-U 2005

O problema 6 da fase final da OBM-U 2005 é

Problema. *Prove que para quaisquer naturais $0 \leq i_1 < i_2 < \ldots < i_k$ e $0 \leq j_1 < j_2 < \ldots < j_k$, a matriz $A = (a_{rs})_{1 \leq r,s \leq k}$ dada por $a_{rs} = \binom{i_r + j_s}{i_r} = \frac{(i_r + j_s)!}{i_r!\, j_s!}$ $(1 \leq r, s \leq k)$ é invertível.*

O incrível é que esse problema tem uma solução combinatória!

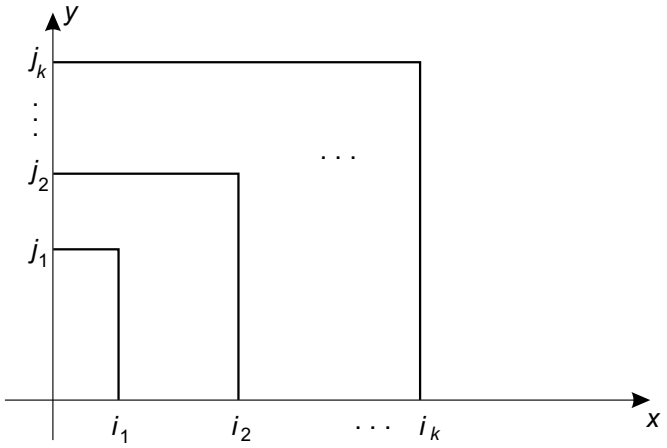
Resolução

Antes, algumas definições.

Considere o reticulado Z^2. Defina *caminho* entre dois pontos P e Q de Z^2 como uma seqüência de pontos do reticulado, cada um igual ao anterior mais $(0, -1)$ ou $(1, 0)$, com o primeiro termo igual a P e o último igual a Q. Defina *sistema de caminhos sem interseção* ligando dois subconjuntos X a Y de Z^2, cada um com n elementos, como um conjunto de n caminhos disjuntos, cada um ligando um ponto de X e um ponto de Y.

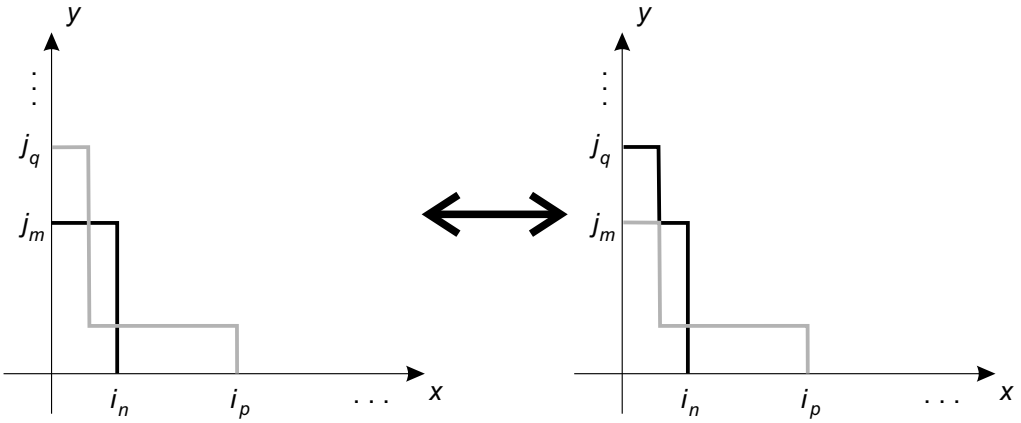
Afirmação. $\det A$ *é igual ao número de sistemas de caminhos sem interseção ligando os conjuntos* $X = \{(0, i_1), (0, i_2), ..., (0, i_k)\}$ *e* $Y = \{(j_1, 0), (j_2, 0), ..., (j_k, 0)\}$.

Note que a partir desse resultado o problema se torna imediato, já que não é difícil achar um sistema de caminhos sem interseção ligando X a Y.



Demonstração da afirmação. Pela definição de determinante, $\det A$ é a soma de $k!$ termos, cada um igual a $\text{sgn}(\sigma) a_{1\sigma(1)}...a_{k\sigma(k)}$, sendo σ uma permutação de $(1, 2, ..., n)$. Considerando que $a_{rs} = \binom{i_r + j_s}{i_r}$, esse termo sem o sinal é igual ao número de maneiras de k caminhos ligarem os pares de pontos $(0, i_n)$ a $(j_{p(n)}, 0)$, intersectando ou não. Em particular, todos os nossos sistemas de caminhos sem interseção estão sendo contados quando σ é a identidade (não é difícil provar que se σ não é a identidade então dois caminhos se intersectam; é só fazer uma figura e usar continuidade). Então os sistemas de caminhos sem interseção aparecem com o sinal positivo no determinante.

Os sistemas de caminhos com alguma interseção se anulam no determinante: considere a interseção que está mais à esquerda (ou seja, com abscissa mínima); caso haja mais de uma, tome a que está mais para baixo (com ordenada mínima). Suponha que a interseção seja entre os caminhos ligando os pares $(0, i_l), (j_m, 0)$ e $(0, i_p), (j_q, 0)$. Esse sistema de caminhos está sendo contado numa parcela do determinante com dois fatores iguais a a_{lm} e a_{pq}. Acontece que podemos obter um sistema de caminhos com os mesmos caminhos, exceto que trocamos os caminhos ligando os pares $(0, i_l), (j_m, 0)$ e $(0, i_p), (j_q, 0)$ pelos que ligam os pares $(0, i_l), (j_q, 0)$ e $(0, i_p), (j_m, 0)$. Mas esse sistema de caminhos está sendo contado numa outra parcela do determinante, que todos os fatores iguais, exceto os termos a_{lm} e a_{pq}, que são substituídos por a_{lq} e a_{pm}. Mas o sinal da permutação está trocado nessa parcela, já que fizemos uma inversão, então esse sistema de caminhos aparece cortado. Note que a escolha dessa inversão não tem ponto fixo e é bijetiva, logo *todos* os caminhos com interseção se anulam no determinante, e o resultado segue, já que tal inversão não se aplica a sistemas de caminhos sem interseção. ∎



7. Referências bibliográficas

[1] Martin Aigner e Günter Ziegler, *As Provas Estão no Livro*, segunda edição traduzida por Marcos Botelho. O nome em inglês do livro é *Proofs From The Book*, e esse é um dos meus livros favoritos. A segunda edição tem diferenças significativas em relação ao primeiro. A primeira demonstração da seção 3, a seção 5 e as idéias da seção 6 (que estão somente na segunda edição!) foram retiradas de lá. Lá tem uma demonstração muito interessante da fórmula de Binet-Cauchy com grafos.

[2] Ian Anderson e Iiro Honkala, *A Short Course In Combinatorial Designs*. Um curso introdutório sobre block designs. Tudo sobre matrizes de Hadamard e a relação de blocks designs com planos projetivos está lá. O arquivo está disponível em `http://users.utu.fi/honkala/designs.ps`

[3] Carlos Shine, *Códigos Corretores de Erros*, aula da VII Semana Olímpica, em janeiro de 2004. O arquivo está disponível em `http://www.obm.org.br/semana/codigos.ps` (se quiser, troque `.ps` por `.pdf`).

[4] Albrecht Beutelspacher e Ute Rosenbaum, *Projective Geometry*. A seção sobre espaços lineares é de lá. A demonstração do teorema de deBruijn-Erdős com posto, contudo, está em [1]. O livro tem um enfoque mais voltado à Teoria da Informação e Criptologia.