Programa Olímpico de Treinamento

Curso de Combinatória – Nível 3

Prof. Carlos Shine

Aula 21

Aplicações de Álgebra Linear em Combinatória

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.

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.

Matrizes e grafos: matriz de adjacência e árvores geradoras

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

Definição 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 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 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. □

O próximo resultado nos dá uma contagem muito interessante.

Teorema 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. □

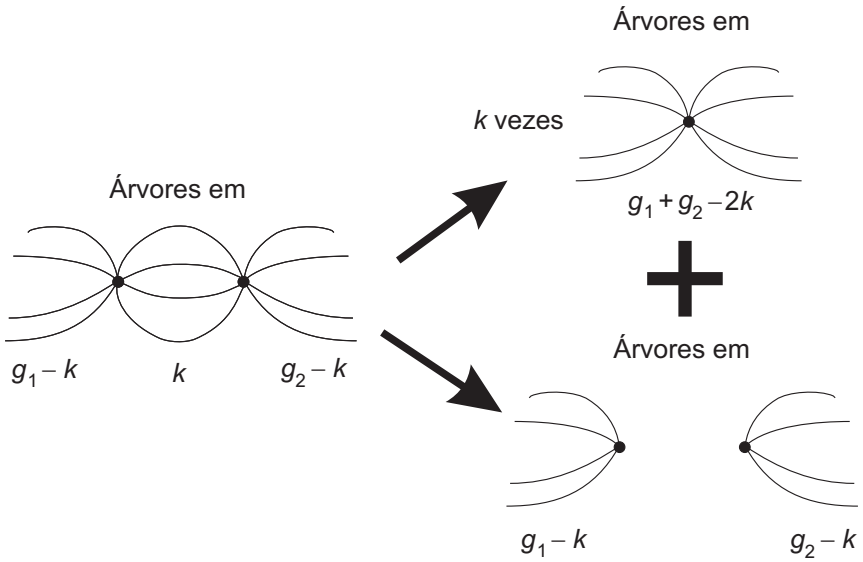
Segunda demonstração (Teoria dos Grafos): Uma das principais técnicas de demonstração em grafos é indução. Isso ocorre porque grafos, tendo definições tão gerais, tendem a não ter muita estrutura. O que funciona bem para encontrar estrutura em entidades com pouca estrutura? Indução! E muitas dessas induções 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

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

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:

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

□

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

Solução: 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. □

Uma desigualdade útil sobre postos

Um fato bem conhecido da Álgebra Linear é

Lema 2. *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.

Posto e design de experimentos

Definimos matriz de incidência também para block designs.

Definição 3. *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 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 2 (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.*

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.

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. *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 3 (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 $v \leq b$. □

Sistemas lineares e decomposição de grafos

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

Teorema 4 (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 $b \geq v$.*

Demonstração: De fato, é só pensar nos vértices como pontos grafos completos menores como retas! □

Lembremos que 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. *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

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

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. □

Exemplo 2. *(OBM-U) 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.*

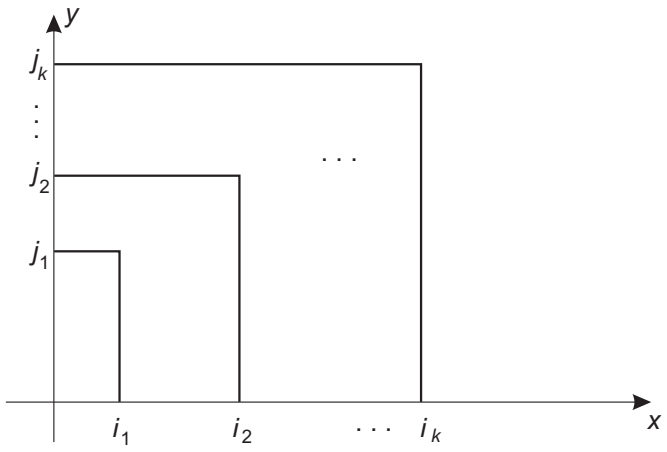
O incrível é que esse problema tem uma solução combinatória!

Solução: Antes, algumas definições.

Considere o reticulado $\mathbb{Z}^2$. 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.

Proposição 1. $\det A$ *é igual ao número de sistemas de caminhos sem interseção ligando os conjuntos* $X = \{(0, i_1), (0, i_2), ..., (0, i_k)\}$ *e* $Y = \{(j_1, 0), (j_2, 0), ..., (j_k, 0)\}$.

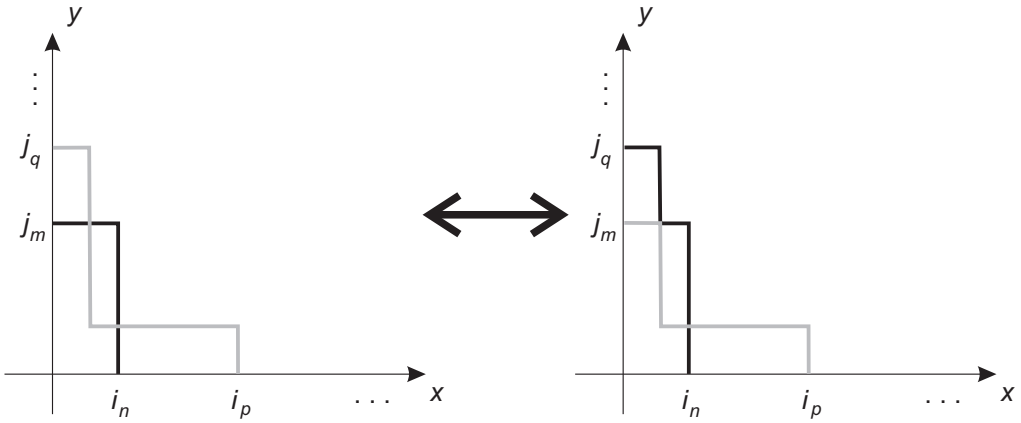
Note que a partir desse resultado o problema se torna imediato, já que não é difícil achar um sistema de caminhos sem interseção ligando X a Y.



Demonstração da afirmação. Pela definição de determinante, $\det A$ é a soma de $k!$ termos, cada um igual a $\text{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{k\sigma(k)}$, sendo σ uma permutação de $(1, 2, \ldots, n)$. 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.



□

Vetores e espaços vetoriais

Um *espaço vetorial sobre um conjunto de escalares* K é um conjunto V, cujos elementos são chamados *vetores*, munido de duas operações, $+$ e $\cdot$, com as seguintes propriedades:

- Para todo $u, v \in V$, $u + v \in V$;
- Para todo $\alpha \in K$ e $v \in V$, $k \cdot V$.

Exemplos típicos de espaços vetoriais são os conjuntos das n-uplas ordenadas $\mathbb{R}^n$. Não há nada de especial em $\mathbb{R}$ exceto pelo fato de ser um corpo. Assim, outro espaço vetorial interessante é $(\mathbb{Z}/(p))^n$ com coordenadas vistas módulo um primo p.

Em combinatória, um caso particular interessante é $(\mathbb{Z}/(2))^n$.

Um conjunto $S = \{v_1, v_2, \ldots, v_k\}$ de vetores pode ser *linearmente dependente* se existirem escalares $a_1, a_2 \ldots, a_k$ tais que

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0;$$

caso contrário, S é *linearmente independente*. Independentemente de ser linearmente dependente ou independente, o conjunto S *gera* o conjunto

$$\langle S \rangle = \{a_1 v_1 + a_2 v_2 + \cdots + a_k v_k, a_1, a_2, \ldots, a_k \in K\}$$

de todas as *combinações lineares* de S.

Conjuntos com as menores quantidades de vetores que geram todo o espaço vetorial V são *bases* de V. Note que bases têm as seguintes propriedades:

- São linearmente independentes;
- Geram V, ou seja, todo vetor de V pode ser escrito como combinação linear dos elementos da base.

Pode-se provar que toda base tem a mesma quantidade de elementos; essa quantidade é chamada *dimensão* de V e é denotada por $\dim V$.

Finalmente, um resultado simples mas extremamente útil: pela definição de base, um conjunto linearmente independente não pode ter mais elementos do que uma base.

Proposição 2. *Seja V um espaço vetorial de dimensão n. Então todo conjunto com $n+1$ ou mais elementos de V é linearmente dependente.* □

Exemplo 3. *(China West) Sejam $A_1, A_2, \ldots, A_{n+1}$ subconjuntos de $\{1, 2, \ldots, n\}$. Prove que existem dois conjuntos disjuntos $I, J \in \{1, 2, \ldots, n+1\}$ tais que*

$$\bigcup_{k \in I} A_k = \bigcup_{k \in J} A_k.$$

Solução: Considere o *vetor característico* de A_i, ou seja, $v_i = (x_1, x_2, \ldots, x_n)$ em que $x_j = 0$ se $j \notin A_i$ e $x_j = 1$ se $j \in A$. Como são $n+1$ vetores em $\mathbb{R}^n$, que tem dimensão n, eles são linearmente independentes, ou seja, existem constantes reais $c_1, c_2, \ldots, c_{n+1}$ tais que

$$\sum_{i=1}^{n+1} c_i v_i = 0$$

Sendo I o conjunto dos índices com c_i positivo e J o conjunto dos c_j's não positivos, temos

$$\sum_{i \in I} |c_i| v_i = \sum_{j \in J} |c_j| v_j$$

Mas $\bigcup_{i \in I} A_i$ é o conjunto das coordenadas da soma do primeiro membro que são diferentes de zero, que deve ser igual ao conjunto das coordenadas da soma do segundo membro que são diferentes de zero, que é $\bigcup_{j \in J} A_j$. □

Problemas

1. 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 1. *Não se sabe se existem matrizes de Hadamard para todo múltiplo de 4. Conjectura-se que sim.*

2. Prove que existe uma matriz de Hadamard de ordem $4n$ se, e somente se, existe um $(4n-1, 2n-1, n-1)$-design.

3. (Suécia) Há 101 vacas em uma fazenda. Quaisquer 100 delas podem ser divididas em dois grupos de 50 vacas de modo que a soma das massas das vacas em cada grupo são iguais. Prove que as 101 vacas têm a mesma massa.

4. (Irã) Seja A um conjunto de vetores de $(\mathbb{Z}/(3))^n$ com a propriedade de que, para quaisquer dois vetores distintos $a, b \in A$, existe uma coordenada i tal que $b_i \equiv a_i + 1 \pmod 3$. Prove que $|A| \leq 2^n$.

5. (Belarus) Considere um tabuleiro 6×6. Cada casa do tabuleiro é pintada de preto ou branco. É permitido escolher qualquer quadrado $t \times t$, $2 \leq t \leq 6$, e inverter todas as cores do quadrado. Você pode fazer isso quantas vezes quiser. É sempre possível fazer com que todo o tabuleiro fique preto?

6. Sejam $A_1, A_2, \ldots, A_r$ subconjuntos distintos de $\{1, 2, \ldots, n\}$ tais que $|A_i|$ é ímpar para todo i e $|A_i \cap A_j|$ é par para todos $i \neq j$. Encontre, em função de n, o maior valor possível de r.

7. Há $2n$ pessoas em uma festa. Cada pessoa tem uma quantidade par de amigos na festa. Prove que existem duas pessoas com uma quantidade par de amigos em comum na festa. Suponha aqui que amizade é uma relação simétrica.

8. Um conjunto T é *par* se $|T|$ é par. Seja n um inteiro positivo par e sejam $S_1, S_2, \ldots, S_n$ subconjuntos pares de $\{1, 2, \ldots, n\}$. Prove que existem $i \neq j$ tais que $|A_i \cap A_j|$ é par.

9. Sejam $A_1, A_2, \ldots, A_n, B_1, B_2, \ldots, B_n$ subconjuntos de $A = \{1, 2, \ldots, n\}$ tais que

   - Para todo conjunto não vazio T de A, existe i tal que $|A_i \cap T|$ é ímpar;
   - Para todos i, j, A_i e B_j têm exatamente um elemento em comum.

   Prove que $B_1 = B_2 = \cdots = B_n$.

10. (Rússia) Em uma festa com n pessoas, para todo grupo de k pessoas, $1 \leq k \leq n$, existe pelo menos uma pessoa, dentro ou fora do grupo, que tem uma quantidade ímpar de amigos no grupo. Prove que n é par.

11. (Vingança Olímpica) **Mediovagio** é um jogo de computador que consiste em um tabuleiro 3×3 no qual cada uma das nove casas é preenchida com um número de 1 a n. Ao clicar-se em uma casa, adiciona-se uma unidade ao número da casa clicada e também ao número de cada uma das casas adjacentes por aresta à casa clicada (a adição dos índices é feita módulo n). Determine para quais valores de n é possível, com um número finito de cliques, chegar a qualquer configuração a partir de uma configuração inicial aleatória.

12. (Moldávia) Existem 22 círculos e 22 pontos no plano tais que cada círculo contém pelo menos 7 pontos e cada ponto pertence a pelo menos 7 círculos?

13. (Vingança Olímpica) Considere n lâmpadas numeradas de 1 a n sobre uma circunferência no sentido horário.

    Seja ξ uma configuração em que $0 \leq \ell \leq n$ lâmpadas quaisquer estão acesas. Um *procedimento batuta* consiste em realizar, simultaneamente, as seguintes operações: para cada uma das ℓ lâmpadas acesas, verificamos a numeração da lâmpada; se i está acesa, um *sinal de alcance* i é enviado por essa lâmpada, e será recebido apenas pelas próximas i lâmpadas que seguem, acesas ou apagadas, também no sentido horário. No final das operações verifica-se, para cada lâmpada, acesa ou não, quantos sinais ela recebeu. Se ela foi atingida por uma quantidade par de sinais, ela permanece no mesmo estado. Caso contrário, ela tem seu estado alterado.

    Sendo Ψ o conjunto de todas as 2^n configurações possíveis, em que $0 \leq \ell \leq n$ lâmpadas quaisquer estão acesas, definimos uma função $f\colon \Psi \to \Psi$ onde, se ξ é uma configuração, então $f(\xi)$ é a configuração obtida após aplicar o procedimento batuta descrito acima.

    Determine todos os valores de n para os quais f é bijetora.

Bibliografia

1. Martin Aigner e Günter Ziegler, *As Provas Estão no Livro*, segunda edição traduzida por Marcos Botelho.

2. Ian Anderson e Iiro Honkala, *A Short Course In Combinatorial Designs*. O arquivo está disponível em `http://users.utu.fi/honkala/designs.ps`

3. Albrecht Beutelspacher e Ute Rosenbaum, *Projective Geometry*.

4. Po-Shen Loh, Notas de aula. Disponíveis em

   `http://www.math.cmu.edu/ ploh/olympiad.shtml`

5. Yufei Zhao, *Algebraic Techniques in Combinatorics*. Disponível em

   `http://yufeizhao.com/olympiad/algcomb.pdf`

Respostas, Dicas e Soluções

1. A entrada a_{ij} de $H \cdot H^t$ é igual ao produto das linhas i e j. Assim, se trocarmos os sinais de toda uma linha de H, $H \cdot H^t$ continua igual a mI. Então podemos supor sem perda de generalidade que todas as entradas da primeira linha são iguais a 1. Agora, para que $a_{1i} = 0$ o produto da linha 1 com a linha i é 0. Portanto as entradas da linha i, $i > 1$, são $m/2$ uns e $m/2$ -1's. Considere agora duas linhas i e j, com $i, j \neq 1$. Sejam U e M o conjunto das posições dos 1's e -1's na linha i, respectivamente. Digamos que x entradas da linha j em U sejam iguais a 1.

Então $m/2-x$ entradas em M são 1, $m/2-x$ entradas em U são -1 e x entradas em M são -1. Para que o produto da linha i com a linha j ser 0, devemos ter $x\cdot 1\cdot 1+(m/2-x)\cdot 1\cdot(-1)+(m/2-x)\cdot(-1)\cdot 1+x\cdot(-1)\cdot(-1)=0 \iff x=m/4$, e portanto m deve ser múltiplo de 4.

2. Como no problema anterior, podemos supor que a primeira linha só tem 1's. Podemos também supor que a primeira coluna só tem 1's também. Tome as $4n-1$ colunas que sobraram como elementos e tome os blocos nas linhas sendo os elementos as colunas com os números 1. Como cada linha tem $2n$ 1's e $2n$ -1's, e eliminamos um 1 de cada linha, cada bloco tem $2n-1$ elementos. Como vimos no problema anterior, duas linhas têm exatamente n 1's em comum, sendo um deles o da coluna eliminada; ou seja, quaisquer dois blocos têm $n-1$ elementos em comum. Da mesma forma, quaisquer dois pontos estão em exatamente $n-1$ blocos.

3. Seja x_i a massa da vaca i, $1\leq i\leq 101$. Montando um sistema de equações indicando as igualdades das massas, obtemos uma matriz A quadrada de ordem 101 com zeros na diagonal principal (eliminamos a vaca i na i-ésima equação) e cada linha tem 50 1's e 50 -1's. Sendo x a matriz coluna com x_i na i-ésima entrada, temos $Ax=0$. Sabemos que o vetor u só com uns como entrada satisfaz a equação. Mostraremos que só múltiplos escalares de u são soluções. Para isso, basta mostrar que o número de variáveis arbitrárias de $Ax=0$ é um, ou seja, que A tem posto 100.

   Para evitar preocupações com sinal, considere a matriz A módulo 2, de modo que $-1\equiv 1 \pmod 2$. Eliminando a última linah e última coluna, obtemos uma matriz $\tilde{A}$ mod 2 com zeros na diagonal principal e 1's nas outras entradas. Como $\tilde{A}^2\equiv I \pmod 2$ (cada linha/coluna tem 99 uns e duas linhas/colunas diferentes têm 98 uns em comum), $\det\tilde{A}^2=1$ é ímpar, e portanto é diferente de zero. Logo $\det\tilde{A}\neq 0$, e o posto de A é pelo menos 100, completando a demonstração.

4. Para cada $a\in A$, considere o polinômio em $(\mathbb{Z}/(3))^n$ $f_a=\prod_{i=1}^n(x_i-a_i-1)$. Note que todos os polinômios da forma $\sum_{S\in\{1,2,\ldots,n\}} a_S\prod_{i\in S}^n x_i$ (dos quais f_a formam um subconjunto) formam um espaço vetorial V sobre $\mathbb{Z}/(3)$. Temos $f_a(b)=0$ para $b\neq a$ e $f_a(a)=(-1)^n\neq 0$. Afirmamos que os f_a's são linearmente independentes. De fato, se $\sum\alpha_a f_a(x)=0$ então substituindo $x=a$ obtemos $\alpha_a=0$. Logo todo α_a é igual a zero, e os f_a's são linearmente independentes. Como a dimensão de V é 2^n (há 2^n produtos $\prod_{i\in S}^n x_i$), a quantidade de f_a's, que é $|A|$, é menor ou igual à dimensão, ou seja, $|A|\leq 2^n$.

5. Há 2^{36} possibilidades de pinturas; o que o problema pede é se é possível gerar todos os possíveis tabuleiros a partir do tabuleiro todo preto (basta reverter as mudanças). A ideia é que o conjunto das operações forma um espaço vetorial S sobre $\mathbb{Z}/(2)$ (de fato, a célula muda tantas vezes quanto for tocada, somando tudo módulo 2), que é um subespaço de $(\mathbb{Z}/(2))^{36}$. Vamos estimar a dimensão de S. Temos 25 quadrados 2×2, e não precisamos dos quadrados 4×4 e 6×6 (basta dividi-los em quadrados 2×2).

Quanto aos quadrados 3×3, considere um quadrado 4×4. Se ativarmos os quatro quadrados 3×3 dentro desse quadrado, só mudamos as quatro casas do canto. Mudando os quatro quadrados 2×2 que têm as duas casas no meio de cada lado, mudamos tudo menos o quadrado do meio. Enfim, mudando o quadrado 2×2 central, mudamos todo o quadrado 4×4; ativando esse mesmo quadrado (com os quatro quadrados 2×2 que o formam), tudo volta ao normal. Isso quer dizer que, tendo os 25 quadrados 2×2 no conjunto, os quatro quadrados 3×3 dentro de qualquer quadrado 4×4 são linearmente dependentes. Com isso, precisamos somente de 7 quadrados 3×3: os quatro de cima e os três da esquerda, exceto o do canto superior esquerdo. Com um argumento análogo, mostramos que precisamos de no máximo 3 quadrados 5×5.

Com isso, são suficientes $25 + 7 + 3 = 35$ quadrados para gerar S. Isso quer dizer que a dimensão de S é no máximo $35 < 36$, o que é insuficiente para gerar todo $(\mathbb{Z}/(2))^{36}$. Ou seja, não é possível obter o quadrado todo preto a partir de qualquer configuração.

6. Transforme cada subconjunto A_i em um vetor de $(\mathbb{Z}/(2))^n$, em que 0 na posição k indica que $k \notin A_i$ e 1 na posição k indica que $k \in A_i$. Coloque os vetores nas linhas de uma matriz A. Então, $A \cdot A^t = I_r$ (o produto de uma linha por si mesma é o número de elementos do conjunto, que é 1 mod 2, e o produto de duas linhas distintas é a quantidade de elementos da interseção, que 0 mod 2), o que quer dizer que A tem posto r. Isso quer dizer que $r \leq n$.

7. Considere o grafo das amizades e seja A a matriz de adjacência desse grafo, ou seja, $a_{ii} = 0$ e $a_{ij} = 1$ quando i e j são amigos e $a_{ij} = 0$ caso contrário. Então $A^2 = B$ em que b_{ii} é o grau do vértice i e b_{ij} é igual à quantidade de amigos comuns de i e j. Suponha por absurdo que, para todo par de pessoas i e j, a quantidade de amigos comuns é ímpar. Então, vendo A^2 mod 2, sendo o grau de cada vértice par, temos $A^2 \equiv J - I \pmod 2$, sendo J a matriz $2n \times 2n$ com todas as entradas iguais a 1 e I a identidade de ordem $2n$. Podemos elevar tudo ao quadrado de novo, obtendo $A^4 \equiv I \pmod 2$ (a quantidade de uns em cada linha é ímpar, e a quantidade de uns comuns em duas linhas diferentes é par). Isso quer dizer que $\det A$ é ímpar. Mas se somarmos todas as linhas de A obtemos um número par em todas as entradas (pois a soma da coluna j é o grau do vértice j), o que quer dizer que $\det A$ é par, absurdo. Logo existem dois vértices i e j com quantidade de amigos comuns par.

8. O problema é essencialmente equivalente ao anterior, considere a matriz A em que a_{ij} é zero se $j \notin S_i$ e um se $j \in S_j$.

9. Considere a matriz A quadrada de ordem n em $\mathbb{Z}/(2)$ em que $a_{ij} = 1$ se $j \in A_i$ e $a_{ij} = 0$ se $j \notin A_i$. A condição $|T \cap A_i|$ ímpar para algum i significa que $Ax \neq 0$ para todo $x \in (\mathbb{Z}/(2))^n$ diferente do nulo, ou seja, $Ax = 0$ só tem a solução trivial, que ocorre se, e somente se, $\det A \neq 0 \pmod 2$. Com isso, sendo x o vetor característico de B_j, temos $Ax = 1$, sendo 1 o vetor só com uns. Mas $Ax = 1$ tem solução única, então $B_i = B_j$ para todo $i \neq j$.

10. Considere a matriz de adjacência A do grafo, como no problema 7. Suponha por absurdo que n é ímpar. Modifique a matriz para a matriz B em que $b_{ij} = a_{ij}$ se $i \leq j$ e $b_{ij} = -a_{ij}$ se $i > j$. Então B é antissimétrica, ou seja, $B^t = -B \implies \det B = (-1)^n \det B^t \iff \det B = -\det B \iff \det B = 0$. Vendo tudo módulo 2, temos $A \equiv B \pmod 2$, ou seja, $\det A \equiv 0 \pmod 2$. Isso quer dizer que existe um conjunto de linhas de A cuja soma só tem componentes pares. Mas isso quer dizer que todos as pessoas da festa conhece uma quantidade par de elementos do conjunto correspondente às linhas, contradição. Logo n é par.

11. Sejam as configurações iniciais e finais, respectivamente,

y_1	y_2	y_3
y_4	y_5	y_6
y_7	y_8	y_9

Inicial

z_1	z_2	z_3
z_4	z_5	z_6
z_7	z_8	z_9

Final

Seja $a_i = z_i - y_i \bmod n$. Sejam x_i o número de clicadas na casa correspondente necessários para obter os valores desejados. Então o problema equivale a provar que o sistema linear

$$\begin{array}{rcccccccccc}
x_1+ & x_2 & + & x_4 & & & & & & = & a_1 \\
x_1+ & x_2+ & x_3 & + & x_5 & & & & & = & a_2 \\
 & x_2+ & x_3 & & + & x_6 & & & & = & a_3 \\
x_1 & & + & x_4+ & x_5 & + & x_7 & & & = & a_4 \\
 & x_2 & + & x_4+ & x_5+ & x_6 & + & x_8 & & = & a_5 \\
 & & x_3 & + & x_5+ & x_6 & & + & x_9 & = & a_6 \\
 & & & x_4 & & + & x_7+ & x_8 & & = & a_7 \\
 & & & & x_5 & + & x_7+ & x_8+ & x_9 & = & a_8 \\
 & & & & & x_6 & + & x_8+ & x_9 & = & a_9
\end{array}$$

sempre admite solução mod n. Mas isso ocorre se, e somente se, o determinante

$$\begin{vmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1
\end{vmatrix} = -7$$

não é divisor de zero mod n.

Deste modo, é sempre possível obter qualquer configuração se, e somente se, n não é múltiplo de 7.

Observação: o sistema

$$\begin{array}{rrrrrrrrrrrrrrrrr}
x_1 + & x_2 & & + & x_4 & & & & & & & & & = & 0 \\
x_1 + & x_2 + & x_3 & & + & x_5 & & & & & & & & = & 0 \\
& x_2 + & x_3 & & & & + & x_6 & & & & & & = & 0 \\
x_1 & & & + & x_4 + & x_5 & & + & x_7 & & & & & = & 0 \\
& x_2 & & + & x_4 + & x_5 + & x_6 & & + & x_8 & & & & = & 0 \\
& & x_3 & & + & x_5 + & x_6 & & & & + & x_9 & = & 0 \\
& & & & x_4 & & & + & x_7 + & x_8 & & & = & 1 \\
& & & & & x_5 & & + & x_7 + & x_8 + & x_9 & = & 0 \\
& & & & & & x_6 & & + & x_8 + & x_9 & = & 0
\end{array}$$

não é possível se n é múltiplo de 7.

12. Primeiro vamos contar a quantidade N de interseções de dois círculos em pontos no conjunto. Temos

$$2 \cdot \binom{22}{2} \geq N \geq 22 \cdot \binom{7}{2}$$

(no lado esquerdo, cada par de círculos se corta em no máximo dois pontos; no lado direito, para cada ponto contamos os pares de círculos a que ele pertence.)

Mas $2 \cdot \binom{22}{2} = 22 \cdot 21 = 22 \cdot \binom{7}{2}$, logo ocorre a igualdade: cada ponto está em *exatamente* 7 círculos e cada par de círculos se corta em pontos do conjunto.

Agora, considere a matriz A, quadrada de ordem 22, em que a entrada a_{ij} é zero se o ponto i não está no círculo j e um se está. Logo $A^2 = 5J + 2I$, em que J é a matriz só com uns e I é a identidade. Isso quer dizer que o determinante de $5J + 2I$ é quadrado perfeito. Mas

$$\begin{vmatrix} 7 & 2 & 2 & \dots & 2 \\ 2 & 7 & 2 & \dots & 2 \\ 2 & 2 & 7 & \dots & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2 & 2 & 2 & \dots & 7 \end{vmatrix} = \begin{vmatrix} 7 & 2 & 2 & \dots & 2 \\ -5 & 5 & 0 & \dots & 0 \\ -5 & 0 & 5 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -5 & 0 & 0 & \dots & 5 \end{vmatrix} = \begin{vmatrix} 7+21\cdot 2 & 2 & 2 & \dots & 2 \\ 0 & 5 & 0 & \dots & 0 \\ 0 & 0 & 5 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 5 \end{vmatrix} = 5^{21} \cdot 49,$$

que não é quadrado perfeito, absurdo.

13. Considere a matriz A, quadrada de ordem n, com entradas em $\mathbb{Z}/(2)$, cuja coluna k tem entradas 1 nas linhas $k+1$, $k+2$, …, $2k$ (tudo módulo n) e 0 caso contrário; isso corresponde às lâmpadas que mudariam. Sendo x um vetor de $(\mathbb{Z}/(2))^n$, o procedimento batuta transforma x em $x + Ax$, ou seja, $f(x) = x + Ax = (A+I)x$. Queremos então saber se f é bijetora, mas como $f\colon (\mathbb{Z}/(2))^n \to (\mathbb{Z}/(2))^n$, basta verificar se f é injetora. Mas $f(x) = f(y) \iff (A+I)x = (A+I)y \iff (A+I)(x-y) = 0$. Então

basta verificar quando $B = A + I$ admite inversa em $\mathbb{Z}/(2)$. Veja alguns exemplos de B:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Quantos uns aparecem na linha i? Temos que contar a quantidade de colunas k em que $k \leq i \leq 2k$ se $k \leq n/2$ ou $k \leq i \leq n$ ou $1 \leq i \leq 2k - n$ se $k > n/2$. Fixemos i. Resolvendo as inequações, obtemos $i/2 \leq k \leq i$ para $k \leq n/2$ ou $k \leq i$ ou $k \geq (n + i)/2$ para $k > n/2$.

Há, então, alguns casos:

- Se $i \leq n/2$, e i é par, temos no primeiro caso $i/2 + 1$ e no segundo caso $n - (n + i)/2 + 1 = n/2 - i/2 + 1$ para n par e $n - (n + i + 1)/2 + 1 = (n - 1)/2 - i/2 + 1$ para n ímpar. Assim, o total é $n/2 + 2$ para n par e $(n - 1)/2 + 2$ para n ímpar.
- Se $i > n/2$, e i é par, temos no primeiro caso $\lfloor n/2 \rfloor - i/2 + 1$ e no segundo caso $i - n/2 + n - (n + i)/2 + 1 = i/2 + 1$ para n par e $i - (n - 1)/2 + n - (n + i + 1)/2 + 1 = i/2 + 1$ para n ímpar. Assim, o total é $\lfloor n/2 \rfloor + 2$ em ambos os casos. Note que, para i par, o total de 1's em cada linha é sempre $\lfloor n/2 \rfloor + 2$.
- Se $i \leq n/2$, e i é ímpar, temos no primeiro caso $(i + 1)/2$ e no segundo caso $n - (n + i + 1)/2 + 1 = n/2 - (i - 1)/2$ para n par e $n - (n + i)/2 + 1 = (n - 1)/2 - (i - 1)/2 + 1$ para n ímpar. O total é $\lfloor n/2 \rfloor + 1$ para n par e $\lfloor n/2 \rfloor + 2$ para n ímpar.
- Se $i > n/2$, e i é par, temos no primeiro caso $\lfloor n/2 \rfloor - (i - 1)/2 + 1$ e no segundo caso $i - n/2 + n - (n + i + 1)/2 + 1 = (i - 1)/2$ para n par e $i - (n - 1)/2 + n - (n + i)/2 + 1 = (i + 1)/2$ para n ímpar. O total é, de novo, $\lfloor n/2 \rfloor + 1$ para n par e $\lfloor n/2 \rfloor + 2$ para n ímpar.
- A única exceção é $i = n$: nesse caso, temos $k = n/2$ se n é par no primeiro caso e $n/2 < k < n$ no segundo caso. No total, $n/2$ para n par e $(n - 1)/2 = \lfloor n/2 \rfloor$ para n ímpar. Em ambos os casos, $\lfloor n/2 \rfloor$.

No final das contas, para n ímpar, a paridade das quantidades de entradas 1 em cada linha é sempre igual. Então, ao somarmos todas as colunas obtemos tudo 1 ou tudo 0; se for tudo 0, o determinante é zero; se for tudo 1, obtemos o resultado igual à penúltima coluna, e o determinante é zero de novo. Com isso, se n é ímpar, f não é bijetora.

Agora, suponha que n é par, ou seja, $n = 2m$. Vamos mostrar que $\det B_{2m} = \det B_m$, em que B_m é a matriz correspondente de dimensão m. Vamos ver a estrutura de A.

Nas colunas ímpares, digamos $2t - 1$, as entradas não nulas são $2t - 1$, $2t$, $2t + 1$, ..., $4t - 2$ módulo $2m$. Note que podemos formar pares $2j - 1, 2j$ de entradas iguais. Além

disso, há uma correspondência direta $2j \bmod 2m \leftrightarrow j \bmod m$. De fato, considerando só as entradas de índice par, temos $t, t+1, \ldots, 2t-1 \bmod m$, ou seja, a linha t de A_m sem o $2t$.

Nas colunas pares, digamos $2t$, as entradas não nulas são $2t$, $2t+1$, $\ldots$, $4t$ módulo $2m$. Os de índice par correspondem a $t, t+1, \ldots, 2t \bmod m$, ou seja, exatamente a linha t de A_m. Os de índice ímpar correspondem a $t+1, t+2, \ldots, 2t \bmod m$, que é a linha t sem a entrada t. Com isso, permutando as linhas e colunas de A_{2m} temos

$$A'_{2m} = \begin{pmatrix} A_m & A_m + K \\ A_m + I & A_m + K \end{pmatrix}$$

em que K é a matriz em que a única entrada na coluna j está na linha $2j \bmod m$.

Temos

$$\det A_{2m} = \begin{vmatrix} A_m & A_m + K \\ I & 0 \end{vmatrix}$$

No caso em que m é ímpar, obtemos $\det A_{2m} = \det(A_m + K)$. Mas K corresponde às linhas da identidade permutadas, então as quantidades de uns continuam com a mesma paridade, ou seja, a soma das colunas ou dá tudo zero ou tudo um. No segundo caso, a última coluna tem tudo um, e então o determinante continua sendo zero.

No caso em que m é par, ou seja, $m = 2\ell$, ao permutarmos as linhas de K obtemos nas entradas pares duas cópias de I_ℓ e nas entradas ímpares, tudo zero. Continuando o determinante, temos

$$\begin{aligned}
\det A_{2m} &= \begin{vmatrix} A_\ell & A_\ell + K' & I & I \\ A_\ell + I & A_\ell + K' & 0 & 0 \\ I & 0 & I & 0 \\ 0 & I & 0 & I \end{vmatrix} = \begin{vmatrix} A_\ell & A_\ell + K' & I & I \\ I & 0 & I & I \\ I & 0 & I & 0 \\ 0 & I & 0 & I \end{vmatrix} \\
&= \begin{vmatrix} A_\ell & A_\ell + K' & I & I \\ 0 & 0 & 0 & I \\ I & 0 & I & 0 \\ 0 & I & 0 & I \end{vmatrix} = \begin{vmatrix} A_\ell & A_\ell + K' & I & I \\ I & 0 & I & 0 \\ 0 & I & 0 & I \\ 0 & 0 & 0 & I \end{vmatrix} = \begin{vmatrix} A_\ell & I & A_\ell + K' & I \\ I & I & 0 & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & I \end{vmatrix} \\
&= \begin{vmatrix} A_\ell + I & I & A_\ell + K' & I \\ 0 & I & 0 & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & I \end{vmatrix} = \det(A_\ell + I)
\end{aligned}$$

Se ℓ é ímpar, novamente temos $\det(A_\ell + I) = 0$, pois de novo a quantidade de uns em cada linha tem a mesma paridade com a última coluna igual a tudo um. Se $\ell = 2q$ é par,

$$\det(A_\ell + I) = \begin{vmatrix} A_q + I & A_q + K \\ A_q + I & A_q + K + I \end{vmatrix} = \begin{vmatrix} A_q + I & A_q + K \\ 0 & I \end{vmatrix} = \det(A_q + I)$$

e continuamos até obtermos um ímpar maior que 1, e nesse caso, o determinante é zero. Assim, o único caso que dá certo é n potência de 2.