Métodos Probabilísticos e Algébricos em Combinatória

Domingos Dellamonica Jr.
Orientador: Yoshiharu Kohayakawa

1 de junho de 2004

Resumo

Este é um projeto de iniciação científica cuja finalidade é estudar métodos probabilísticos e algébricos na resolução de problemas combinatórios.

O conteúdo será distribuído em seções, onde cada método será discutido com exemplos encontrados na bibliografia e referências de estudo. Além de descrições e exemplos relacionados, alguns problemas selecionados serão resolvidos.

Acreditamos que a resolução de tais problemas é essencial para a absorção do conteúdo estudado e servirá de exemplo aos leitores.

Para compreender o texto é necessário algum conhecimento de probabilidade, álgebra linear e teoria dos grafos.

Sumário

1 Método Probabilístico

1.1 O Método Básico

O Método Probabilístico tem como finalidade demonstrar que uma estrutura com certas propriedades existe. Para isso, um espaço de probabilidade adequado é definido e deve-se demonstrar que as propriedades desejadas aparecem em um elemento deste espaço com probabilidade positiva.

Ao longo do texto este conceito ficará mais claro, especialmente a partir dos muitos exemplos que serão detalhados a seguir.

Um exemplo simples de aplicação do método é na obtenção de cotas para os *Números de Ramsey*. O número $R(k,l)$ é o menor inteiro n tal que em qualquer coloração das arestas do grafo completo com n vértices, K_n, usando-se duas cores (vermelho e azul, por exemplo) sempre existe um grafo K_k vermelho ou um K_l azul. Ramsey (1930) mostrou que $R(k,l)$ é finito para quaisquer k e l.

Vamos usar o método para encontrar um limitante inferior para $R(k,k)$.

Se $\binom{n}{k}2^{1-\binom{k}{2}} < 1$ *então* $R(k,k) > n$.

Dem. Considere uma coloração das arestas de K_n com as cores vermelho e azul, onde cada aresta é colorida independentemente com igual probabilidade para ambas as cores.
Para qualquer conjunto R fixado com k vértices, seja A_R o evento em que o sub-grafo induzido por R é *monocromático* (todas as arestas tem a mesma cor).

Cada aresta é pintada independentemente e há 2 opções de cores, portanto

$$\Pr[A_R] = 2 \times 2^{-\binom{k}{2}}.$$

Como há $\binom{n}{k}$ possíveis escolhas para R, a probabilidade de pelo menos um dos eventos A_R ocorrer é limitada superiormente por

$$\binom{n}{k}2^{1-\binom{k}{2}} < 1.$$

Então, com probabilidade positiva, nenhum evento A_R ocorre. Isso significa que existe uma 2-coloração das arestas de K_n sem um K_k monocromático, ou seja, $R(k,k) > n$.

Corolário: $R(k,k) > 2^{k/2}$ *para todo* $k \geq 3$.
Quando $k \geq 3$, se tomarmos $n = \lfloor 2^{k/2} \rfloor$, então

$$\binom{n}{k} 2^{1-\binom{k}{2}} = \frac{n(n-1)\cdots(n-k+1)}{k!} 2^{1+(k-k^2)/2} < \frac{2^{1+k/2}}{k!} \times \frac{n^k}{2^{k^2/2}} < 1,$$

portanto $R(k,k) > 2^{k/2}$ para todo $k \geq 3$.

1.1.1 Teorema de Erdős-Ko-Rado

Este teorema é um clássico da *Teoria Extremal dos Conjuntos*. A demonstração que daremos utiliza o Método Probabilístico, é bem concisa e serve de exemplo do poder do Método.

Uma família de conjuntos $\mathcal{F}$ é dita intersectante se $A, B \in \mathcal{F}$ implica $A \cap B \neq \emptyset$. Suponha $n \geq 2k$ e seja $\mathcal{F}$ uma família de k-conjuntos contidos em $\{0, 1, \ldots, n-1\}$. O Teorema de Erdős-Ko-Rado nos diz que $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

Lema. *Para* $0 \leq s \leq n-1$, *defina* $A_s = \{s, s+1, \ldots, s+k-1\}$, *onde a adição é módulo* n. *A família intersectante* $\mathcal{F}$ *possui no máximo* k *conjuntos da forma* A_s.

Dem. Suponha que $A_i \in \mathcal{F}$. Há exatamente $2k-2$ conjuntos da forma A_s que têm intersecção não vazia com A_i. Podemos arranjar esses $2k-2$ conjuntos em $k-1$ pares de conjuntos disjuntos. Fica claro que $\mathcal{F}$ pode conter no máximo um elemento de cada par, provando o lema.

Sejam σ uma permutação de $\{0, 1, \ldots, n-1\}$ e $i \in \{0, 1, \ldots, n-1\}$ escolhidos aleatoriamente, uniformemente e independentemente. Defina $A = \{\sigma(i), \sigma(i+1), \ldots, \sigma(i+k-1)\}$, com adição módulo n.

Pelo lema, temos que, para qualquer permutação σ tomada, há no máximo k dentre os n conjuntos da forma $\{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$ em $\mathcal{F}$. Portanto, $\Pr[A \in \mathcal{F}] \leq k/n$.

Um pouco de reflexão mostra que isso é equivalente a escolher A aleatoriamente entre todos os k-conjuntos de $\{0, 1, \ldots, n-1\}$. Sendo assim,

$$\frac{k}{n} \geq \Pr[A \in \mathcal{F}] = \frac{|\mathcal{F}|}{\binom{n}{k}}, \text{ e então}$$

$$|\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}.$$

1.1.2 Desbalanceando Luzes

TODO: (Esta parte deve estar mais conectada, preciso inserir as motivações para o que está sendo calculado, apresentar a análise assintótica a partir da identidade combinatória e chegar no resultado final do livro.)

Seja S_n uma variável aleatória correspondente a soma de n variáveis aleatórias uniformes em $\{-1, 1\}$. Vamos demonstrar que

$$E[|S_n|] = n2^{1-n}\binom{n-1}{\lfloor (n-1)/2 \rfloor}. \tag{1}$$

Por simetria, verificamos que para cada soma dessas n variáveis resultando num inteiro i existe uma soma resultando $-i$. Além disso, só existem somas nulas caso n seja par.

Uma soma com exatamente i elementos positivos ($n/2 < i \leq n$) tem soma positiva $i - (n - i) = 2i - n > 0$.

Como cada soma tem probabilidade 2^{-n} de ser escolhida e existem $\binom{n}{i}$ somas com exatamente i elementos positivos, vemos que

$$E[|S_n|] = 2^{-n} \times 2 \sum_{n/2<i\leq n} \binom{n}{i}(2i - n). \tag{2}$$

Para verificarmos a proposição, nos resta mostrar que

$$k\binom{k-1}{\lfloor (k-1)/2 \rfloor} = \sum_{k/2<i\leq k} \binom{k}{i}(2i - k). \tag{3}$$

Por inspeção, verificamos que a identidade acima está correta para $k = 1, 2$. Suponha que esta também seja verdadeira para $2 \leq k \leq n$.

Definimos $J_n = \{j : n/2 < j \leq n\}$.
Vamos utilizar a identidade $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$ [†] nesta demonstração.

[†]Esta identidade vale mesmo quando o índice inferior é negativo ou maior que n, assumindo que $\binom{n}{p} = 0$ quando $p < 0$ ou $p > n$.

Queremos provar a identidade (3) para $k = n+1$, ou seja, precisamos obter

$$S = \sum_{i \in J_{n+1}} \binom{n+1}{i}(2i - n - 1).$$

Aplicando a identidade acima, temos

$$S = \sum_{i \in J_{n+1}} \left(\binom{n}{i} + \binom{n}{i-1} \right)(2i - n - 1),$$

onde o somatório pode ser quebrado em duas somas,

$$S_1 = \sum_{i \in J_{n+1}} \binom{n}{i}(2i - n) - \sum_{i \in J_{n+1}} \binom{n}{i},$$

$$S_2 = \sum_{i \in J_{n+1}} \binom{n}{i-1}(2(i-1) - n) + \sum_{i \in J_{n+1}} \binom{n}{i-1}.$$

Vamos analisar o caso n par e o caso n ímpar separadamente:

1. Quando $n = 2m$, $J_n = \{m+1, \ldots, 2m\}$ e $J_{n+1} = J_n \cup \{2m+1\}$.
   Como $\binom{2m}{2m+1} = 0$, temos

   $$S_1 = \sum_{i \in J_n} \binom{n}{i}(2i - n) - \sum_{i \in J_n} \binom{n}{i}, \text{ e}$$

   $$S_2 = \sum_{i \in J_n} \binom{n}{i}(2i - n) + \sum_{i \in J_n} \binom{n}{i} + \binom{n}{n/2}$$

   pois quando $i = m+1$ o termo $\binom{n}{i-1}(2i - n - 2)$ se anula.
   Restaurando a soma, obtemos

   $$S = S_1 + S_2 = 2\sum_{i \in J_n} \binom{n}{i}(2i - n) + \binom{n}{n/2}.$$

   A hipótese de indução nos garante que

   $$\sum_{i \in J_n} \binom{n}{i}(2i - n) = n\binom{n-1}{\lfloor (n-1)/2 \rfloor} = 2m\binom{2m-1}{m-1}.$$

Com algumas manipulações algébricas simples chegamos a

$$S = (2m+1)\binom{2m}{m} = (n+1)\binom{n}{\lfloor n/2 \rfloor},$$

que é exatamente a identidade desejada.

2. O caso n ímpar é análogo ao caso par. Diferenças sutis aparecem na manipulação dos índices dos somatórios.

A identidade (3) segue por indução para todo $n \geq 1$ e assim obtemos a fórmula fechada (1) para $E[|S_n|]$.

1.2 Linearidade da Esperança

Em todo o texto, se X é uma variável aleatória, $\Pr[X = i]$ é a probabilidade de X assumir o valor i. Para variáveis contínuas isso não faz sentido já que a probabilidade uma variável contínua assumir um valor específico é sempre 0.

Caso X seja uma variável aleatória contínua, definimos $f(x)$ como a função de densidade de probabilidade de X, de modo que

$$\Pr[a \leq X \leq b] = \int_a^b f(x)dx.$$

Definimos o conceito de **Esperança** de uma variável aleatória X como

$$E[X] = \sum_{i=-\infty}^{\infty} i \times \Pr[X = i] \text{ , no caso discreto e}$$

$$E[X] = \int_{-\infty}^{\infty} xf(x)dx \text{ , no caso contínuo.}$$

Uma propriedade muito útil da Esperança é que se $X_1, X_2, \ldots, X_n$ são variáveis aleatórias, $c_1, \ldots, c_n$ são constantes e a variável aleatória $X = c_1X_1 + \cdots + c_nX_n$, então $E[X] = c_1E[X_1] + \ldots c_nE[X_n]$.

O grande poder desta propriedade é que não é exigido absolutamente nada sobre as variáveis $X_1, \ldots, X_n$, elas podem ser dependentes, de distribuições completamente diferentes e o resultado continua valendo.

Vamos agora dar um exemplo do uso da Linearidade da Esperança:
Seja $G = (V, E)$ um grafo com n vértices e e arestas. Então G contém um sub-grafo bipartido com pelo menos $e/2$ arestas.

Dem. Seja $T \subset V$ um subconjunto aleatório formado escolhendo-se independentemente elementos de V, com probabilidade $1/2$ de estarem em T. Defina $B = V - T$, dizemos que uma aresta $\{x, y\}$ cruza as partes B e T se exatamente um elemento de $\{x, y\}$ está em T. Seja X o número de arestas que cruzam as partes. Podemos decompor

$$X = \sum_{\{x,y\} \in E} X_{xy},$$

onde X_{xy} é a variável aleatória indicadora para o evento em que a aresta $\{x, y\}$ cruza as partes. Mas então

$$E[X_{xy}] = \Pr[x \in B, y \in T] + \Pr[x \in T, y \in B],$$

como os eventos são independentes,

$$E[X_{xy}] = \Pr[x \in B] \Pr[y \in T] + \Pr[x \in T] \Pr[y \in B] = 1/2.$$

Pela Linearidade da Esperança, $E[X] = \sum_{\{x,y\} \in E} E[X_{xy}] = e/2$. Sendo assim, para alguma escolha de T, devemos ter $X \geq e/2$.

Para essa escolha de T, elimine as arestas que não cruzam as partes. Tome o grafo formado como um sub-grafo bipartido de G com pelo menos $e/2$ arestas.

1.2.1 Partição de Grafo - Problema Resolvido

Este problema foi retirado de *TODO: (fazer uma ref. bibliográfica aqui)*.
Problema: *Seja $G = (V, E)$ um grafo com n vértices de grau mínimo $d > 10$. Mostre que há uma partição de V em dois conjuntos disjuntos A e B tal que $|A| = O(\frac{n \log(d)}{d})$, e todo vértice de B tem ao menos um vizinho em A e ao menos um vizinho em B.*

Considere como espaço de probabilidade (uniforme) todas as partições possíveis com $|A| = \lceil n \log(d)/d \rceil$. Defina $p = |A|/n$.

Dado um elemento $x \in V$, definimos $d(x)$ como o grau de x.
Se x é um vértice e todo vizinho de x está em B, dizemos que x é do *tipo 1*. Se todo

vizinho de x está em A, dizemos que x é do *tipo 2*.

Sendo assim,

$$\begin{aligned}\Pr[x \text{ é do tipo 1}] &= \frac{|B|}{n}\frac{|B|-1}{n-1}\cdots\frac{|B|-d(x)+1}{n-d(x)+1} < \left(\frac{|B|}{n}\right)^{d(x)} = \\ &= (1-p)^{d(x)} \leq (1-p)^d \leq e^{-pd} \leq e^{-\log(d)} = 1/d,\end{aligned} \tag{4}$$

$$\begin{aligned}\Pr[x \text{ é do tipo 2}] &= \frac{|A|}{n}\frac{|A|-1}{n-1}\cdots\frac{|A|-d(x)+1}{n-d(x)+1} < \left(\frac{|A|}{n}\right)^{d(x)} = \\ &= p^{d(x)} \leq p^d.\end{aligned} \tag{5}$$

Em (4), estamos usando a desigualdade $1 + x \leq e^x$, que vale para todo x real. Nas passagens $(1-p)^{d(x)} \leq (1-p)^d$ e $p^{d(x)} \leq p^d$, usamos que $0 < p < 1-p < 1$ e $d(x) \geq d$, pois d é o grau mínimo do grafo.
Como $p = |A|/n \geq \log(d)/d$, temos $pd \geq \log(d)$ e, portanto, $-pd \leq -\log(d)$. Logo $e^{-pd} \leq e^{-\log(d)}$.

Defina X como uma variável aleatória que indica quantos vértices são do tipo 1 e, analogamente, defina Y como uma variável aleatória que indica quantos vértices são do tipo 2. A partir de (4) e (5), obtemos $E[X] \leq n/d$ e $E[Y] \leq np^d$.

Pela Linearidade da Esperança, temos

$$E[X+Y] \leq n(1/d + p^d).$$

Portanto, existe uma partição de V em partes A e B, com $|A| = pn$, de forma que há x elementos de tipo 1 e y elementos de tipo 2, com

$$x + y \leq n(1/d + p^d). \tag{6}$$

Mova todos os elementos de tipo 1 que estejam em B para A (no máximo x elementos).

Se $u \in B$ é um elemento de tipo 2, temos duas situações possíveis:

(i) todo vizinho $v \in B$ de u, que não é de tipo 2, possui um vizinho em B que **não** é de tipo 2;

(ii) existe um vizinho $v \in B$ de u, que não é de tipo 2, cujos vizinhos em B são **todos** de tipo 2.

No primeiro caso, se movermos u para A, estaremos reduzindo o conjunto dos elementos de tipo 2 (u e todos os seus vizinhos de tipo 2 deixarão de sê-lo). Fazendo essa movimentação, nenhum elemento passa a ser do tipo 2 se já não era antes. Também não transformamos nenhum vértice em um elemento de tipo 1, pois todos os vizinhos de u (os vértices que poderiam ser afetados pela movimentação) têm vizinhos em B.

No segundo caso, se movermos o vizinho v para A, u deixará de ser tipo 2 (todo vizinho de v que seja de tipo 2 deixará de sê-lo). Também não transformamos vértices em elementos do tipo 1 ou tipo 2 neste caso.

Podemos, através de sucessivas movimentações, eliminar todos elementos de tipo 2. Para que isso ocorra, teremos de mover no máximo y elementos de B para A .

Após tais movimentações, a partição não terá elementos de tipo 1 ou 2 e, portanto, todo vértice em B terá ao menos um vizinho em A e ao menos um vizinho em B. A partir da inequação (6), temos $|A| \leq pn + n(1/d + p^d)$.

É simples ver que $1/d + p^d < 2/d < p$ para $d > 10$ e, portanto, $|A| \leq 2pn$, ou seja, $|A| = O(\frac{n \log(d)}{d})$, como queríamos.

1.2.2 Médias Aritméticas - Problema Resolvido

O problema a seguir foi parte da prova da IMO (International Math Olympiad) de 1981. Provaremos uma generalização deste utilizando o método probabilístico (esta prova é uma adaptação de uma proposta de solução no livro *TODO: ref.*).

Problema: *Seja $1 \leq r \leq n$ e considere todos os subconjuntos de $\{1, 2, \ldots, n\}$ com r elementos. Cada um desses subconjuntos tem um elemento mínimo. Seja $F(n, r)$ a média aritmética desses elementos mínimos; prove que*

$$F(n, r) = \frac{n+1}{r+1}.$$

Seja $k \leq r$, todo subconjunto de $\{1, 2, \ldots, n\}$ com r elementos tem um k'ésimo menor, defina $F(n, r, k)$ como a média aritmética de tais elementos. Fica claro que $F(n, r) = F(n, r, 1)$.

Se definirmos X como o k'ésimo menor elemento de um r-conjunto de $\{1, 2, \ldots, n\}$ sorteado aleatoriamente e uniformemente, teremos $E[X] = F(n, r, k)$.

Vamos montar um experimento aleatório que é simples de analisar e mostrar que este experimento é equivalente a selecionar um r-conjunto de $\{1, 2, \ldots, n\}$ uniformemente.

Considere uma circunferência de comprimento $n + 1$ com $n + 1$ pontos igualmente espaçados marcados (não diferenciados). Escolha aleatoriamente $r + 1$ pontos destes marcados. Suponha que $C_1, \ldots, C_{r+1}$ sejam variáveis aleatórias correspondentes aos tamanhos dos arcos formados pelos intervalos entre dois pontos escolhidos consecutivos.

Como $E[C_1 + \cdots + C_{r+1}] = n + 1$ e, por simetria, $E[C_1] = E[C_2] = \cdots = E[C_{r+1}]$, pela Linearidade da Esperança, temos

$$E[C_1 + \cdots + C_{r+1}] = (r + 1)E[C_1], \text{ portanto } E[C_1] = (n + 1)/(r + 1).$$

Quebre a circunferência no $(r + 1)$'ésimo ponto escolhido e estique para formar uma linha. Os pontos que estavam marcados na circunferência agora recebem uma numeração nesta linha, ao $(r + 1)$'ésimo ponto escolhido associamos 0 e, caminhando no sentido horário, por exemplo, numeramos sequencialmente os pontos marcados.

Note para uma escolha dos $r + 1$ pontos na circunferência, temos uma escolha de r pontos em $\{1, 2, \ldots, n\}$. Também verificamos que, para qualquer escolha de r pontos em $\{1, 2, \ldots, n\}$, podemos selecionar um ponto marcado arbitrário da circunferência e escolher os demais pontos a partir desse primeiro no sentido horário (o primeiro ponto selecionado realmente não faz diferença pois os pontos na circunferência não são numerados).

Temos então um mapa um-para-um entre os eventos nos dois espaços de probabilidade. Como ambos são uniformes, a esperança do k'ésimo menor elemento de um r-conjunto de $\{1, 2, \ldots, n\}$ escolhido de forma uniforme é equivalente a esperança do tamanho dos k segmentos consecutivos a partir do $(r+1)$'ésimo ponto escolhido. Mas essa esperança é precisamente $k(n + 1)/(r + 1)$, como queríamos.

1.3 Conjuntos Livres de Somas

Dizemos que um conjunto S é livre de somas quando não existem $a, b, c \in S$, tais que $a + b = c$. Vamos apresentar um teorema, provado por Erdős em 1965.

TEOREMA: *Todo conjunto $B = \{b_1, \ldots, b_n\}$ de inteiros não nulos contém um subconjunto A, livre de somas, de tamanho $|A| > n/3$.*

Dem.: Seja $p = 3k + 2$ um primo satisfazendo $p > 2\max_{1 \leq i \leq n} |b_i|$ e defina $C = \{k + 1, k + 2, \ldots, 2k + 1\} \subset \mathbb{Z}_p$. Veja que C é livre de somas em $\mathbb{Z}_p$ e que

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

Escolha um elemento aleatório x, de $\mathbb{Z}_p^*$, conforme uma distribuição uniforme. Defina $d_i = xb_i \mod p$, $1 \leq i \leq n$. Note que como p é primo e $b_i \not\equiv 0 \pmod p$, $\varphi_i(x) = xb_i$ é uma função bijetiva e, portanto, $\Pr[d_i \in C] = |C|/(p-1) > 1/3$. O número esperado de elementos b_i tais que $d_i \in C$ é maior que $n/3$. Logo, existe um $x \in \mathbb{Z}_p^*$ e $A \subset B$ de cardinalidade $|A| > n/3$ tal que $xy \mod p \in C$ para todo $y \in A$. Mas A é livre de somas, pois se $a_1, a_2, a_3 \in A$ são tais que $a_1 + a_2 = a_3$, então $xa_1 + xa_2 \equiv xa_3 \pmod p$, o que contradiz o fato de que C é livre de somas.

Vamos mostrar que tal teorema pode ser generalizado. É simples ver que se B é um conjunto de n números racionais, podemos multiplicar todos os elementos do conjunto por um inteiro k, que cancela todos os denominadores, ou seja, $kB = \{kx \mid x \in B\}$ é um conjunto de n inteiros. Pelo teorema acima, existe $A \subset kB$, com $|A| > n/3$, livre de somas. Mas então, $(1/k)A \subset B$ é livre de somas e tem tamanho maior que $n/3$.

Podemos ir além e provar tal teorema para um conjunto de n números reais. Faremos isso em 2.2, onde serão abordadas técnicas de álgebra linear aplicadas a problemas combinatórios.

2 Técnicas de Álgebra

texto...

2.1 Conhecimentos Necessários de Álgebra Linear

texto...

2.2 Conjuntos Livres de Somas - Problema Resolvido

Este problema foi proposto no livro *Probabilistic Method* e é uma generalização do teorema visto em 1.3. Queremos mostrar que *todo conjunto $B = \{b_1, \ldots, b_n\}$ de reais não*

nulos contém um subconjunto A, livre de somas, de tamanho $|A| > n/3$.

Seja $B = \{b_1, \ldots, b_n\}$ um conjunto de n números reais. Sejam $x_1, \ldots, x_n$, variáveis. Para cada $1 \leq i, j, k \leq n$ com $b_i + b_j = b_k$, adicione a equação $x_i + x_j - x_k = 0$ a um sistema de equações lineares. Se não existem i, j, k dessa forma, então B é livre de somas e o enunciado é satisfeito.

Caso o sistema tenha pelo menos uma equação, podemos definir uma matriz $\mathbf{T}$, correspondente ao sistema linear homogêneo formado. Note que as entradas de $\mathbf{T}$ são elementos de $\{0, 1, -1\}$, que são racionais.

Denotamos $\ker(\mathbf{T}) = \{\mathbf{x} \mid \mathbf{Tx} = \mathbf{0}\}$ (alguns autores definem o núcleo de uma transformação linear $\mathbf{T}$ como $\mathrm{Null}(\mathbf{T})$). Como $\mathbf{b} = (b_1, \ldots, b_n)$ é solução do sistema por definição, $\mathbf{b} \in \ker(\mathbf{T})$, ou seja, $\ker(\mathbf{T}) \neq \emptyset$ e, portanto, deve haver uma base de $\ker(\mathbf{T})$ com vetores de coordenadas racionais (pois $\mathbf{T}$ tem coordenadas racionais).

Seja $\mathbf{u} \in \ker(\mathbf{T}) \cap \mathbb{Q}^n$ com o menor número de coordenadas repetidas, ou seja, $\#\{(i, j) \mid u_i = u_j\}$ é mínimo. Vamos mostrar que $\mathbf{u}$ não tem coordenadas repetidas.

Suponha que $u_i = u_j$. Existe um vetor $\mathbf{v} \in \ker(\mathbf{T}) \cap \mathbb{Q}^n$ com $v_i \neq v_j$. Caso contrário, todos os vetores da base de $\ker(\mathbf{T})$ teriam as coordenadas i e j iguais, mas como $\mathbf{b}$ é uma combinação linear dos vetores de tal base (com coeficientes reais), teríamos $b_i = b_j$, o que é absurdo.

Vamos mostrar que para algum $\lambda \in \mathbb{Q}^*$, $\mathbf{u} + \lambda\mathbf{v}$ tem estritamente menos coordenadas repetidas que $\mathbf{u}$. Para isso, veja que

$$u_i + \lambda v_i \neq u_j + \lambda v_j.$$

Além disso, $u_k + \lambda v_k = u_l + \lambda v_l$ somente se $u_k - u_l = \lambda(v_k - v_l)$. Então, ou $u_k - u_l = v_k - v_l = 0$, ou

$$\lambda = \frac{u_k - u_l}{v_k - v_l}.$$

Como há um número finito de pares (k, l), os valores que λ não pode assumir formam um conjunto finito e, portanto, para infinitos valores de λ, $\mathbf{u} + \lambda\mathbf{v}$ possui menos coordenadas repetidas que $\mathbf{u}$, o que contradiz a definição de $\mathbf{u}$.

Para concluir a demonstração, tome $U = \{u_1, \ldots, u_n\}$, que é um conjunto de n números racionais. Pelo teorema 1.3, existe $U' \subset U$, de cardinalidade $|U'| > n/3$, livre de somas. Mas se $U' = \{u_{i_1}, \ldots, u_{i_r}\}$, o conjunto $A = \{b_{i_1}, \ldots, b_{i_r}\} \subset B$ deve ser livre de somas.

2.3 Caso de Igualdade do Teorema de Erdős-Ko-Rado

Esta é uma adaptação de um paper de Peter J. Cameron [1] apresentando uma demonstração para um dos principais resultados da Teoria Extremal de Conjuntos.

O teorema de Erdős-Ko-Rado já foi demonstrado na seção 1.1.1 usando o método probabilístico. Agora daremos uma demonstração diferente e caracaterizaremos o caso de igualdade do teorema.

2.3.1 Algumas Definições

Um automorfismo num grafo $G = (V, E)$ é uma função $f : V \mapsto V$, bijetora, que preserva arestas, ou seja, $(u, v) \in E$, $(f(u), f(v)) \in E$.
Um grafo G é dito vértice-transitivo se, para quaisquer vértices x e y de G, exista um automorfismo g com $g(x) = y$.
Se X é um conjunto de vértices e g uma função definida para todo elemento de X, convencionamos que $X^g = \{g(x) : x \in X\}$.

2.3.2 Lema sobre Grafos Vértice-Transitivos

Seja $G = (X, E)$ um grafo vértice-transitivo. Seja $Y \subset X$ tal que todo clique em Y tem tamanho máximo $|Y|/m$. Então, qualquer clique em G tem tamanho máximo $|X|/m$. Um clique C atingindo tal limite satisfaz $|C^g \cap Y| = |Y|/m$ para todo automorfismo g de G.

Demonstração Seja N a ordem do grupo de automorfismos de G. Dados $x, y \in X$, o número de automorfismos satisfazendo $g(x) = y$ é $N/|X|$.
Note que para todo $z \in X$ existe um automorfismo π, com $\pi(y) = z$. Sendo assim, se $\sigma_1, \sigma_2, \ldots, \sigma_r$ são tais que $\sigma_i(x) = y, i = 1, \ldots, r$, então $\pi\sigma_i(x) = z, i = 1, \ldots, r$ são r automorfismos distintos (teoria dos Grupos) que levam x a z. Por simetria, vemos que o número de automorfismos que levam x a qualquer elemento de X deve ser o mesmo, $N/|X|$.

Suponha que C seja um clique no grafo. Vamos agora contar os pares x, g onde x é um vértice em C e g um automorfismo tal que $g(x) \in Y$. Há $|C|$ escolhas para o vértice x e $N/|X|$ possíveis automorfismos g com $g(x) = y$ para todo $y \in Y$. O número de pares é, portanto, $|C||Y|N/|X|$.

[1] Obtido na Web em `http://www.maths.qmw.ac.uk/~pjc/comb/`.

Podemos contar os mesmos pares por outra perspectiva. Para cada um dos N automorfismos g, há no máximo $|Y|/m$ escolhas para $x \in X$. Para esta afirmação, veja que C^g é um clique e, como qualquer clique em Y tem tamanho máximo $|Y|/m$, $|C^g \cap Y| \leq |Y|/m$. Como g é uma bijeção, há no máximo $|Y|/m$ escolhas para $x \in X$.

Sendo assim, $|C||Y|N/|X| \leq N|Y|/m$. Simplificando, temos $|C| \leq |X|/m$, como no lema. Para o caso de um clique satisfazendo o limite, devemos ter $N|Y|/m$ pares x, g e, como vimos, isso só é possível se, para todo automorfismo g, tivermos $|C^g \cap Y| = |Y|/m$.

2.3.3 Demonstrando o Teorema

Seja $n \geq 2k$. Uma família intersectante de k-conjuntos de um n-conjunto tem cardinalidade máxima $\binom{n-1}{k-1}$.

Demonstração Considere o grafo $G = (X, E)$ cujos vértices são todos os k-conjuntos de um n-conjunto e as arestas ligam conjuntos que tem intersecção não vazia.

O grafo G é vértice-transitivo pois qualquer permutação do n-conjunto serve de automorfismo. Resta-nos mostrar que há uma família Y, de k-conjuntos, com $|Y| = n$, tal que qualquer subfamília intersectante de Y tem tamanho no máximo k. Se este é o caso, teremos encontrado um subconjunto de vértices do grafo que não possui nenhum clique (uma família intersectante é um clique) de tamanho maior que $(k/n)|Y|$. Pelo Lema, qualquer clique em G teria no máximo $(k/n)|X| = (k/n)\binom{n}{k} = \binom{n-1}{k-1}$ vértices.

Para facilitar a demonstração, tomaremos $\mathbb{Z}_n$ como n-conjunto, mas o resultado valerá para qualquer n-conjunto.

Considere $Y = \{Y_i = \{i, i+1, \ldots, i+k-1\} : i \in \mathbb{Z}_n\}$. Vamos mostrar que em tal conjunto, não podemos escolher mais que k conjuntos intersectantes.

Fixe um conjunto escolhido inicialmente, digamos Y_0. Como $n \geq 2k$, qualquer conjunto de Y que intercepte Y_0 deve ter como intersecção uma seqüência de inteiros módulo n. Sendo assim, todos os conjuntos que interceptam Y_0 são $\{Y_{1-k}, \ldots, Y_{-1}, Y_1, \ldots, Y_{k-1}\}$.

Veja que os pares $\{(Y_{1-k}, Y_1), (Y_{2-k}, Y_2), \ldots, (Y_{-1}, Y_{k-1})\}$ são formados por conjuntos disjuntos. Portanto, no máximo podemos escolher um elemento de cada par para formar uma família intersectante, ou seja, no máximo $k-1$ desses conjuntos podem, junto

com Y_0, formar uma família intersectante.

Além disso, caso $n > 2k$, é possível ver que a única maneira de conseguir k conjuntos intersectantes em Y é tomando conjuntos consecutivos, pois (Y_{i-k}, Y_{i+1}) e (Y_i, Y_{i+1-k}), $i = 1, \ldots, k-2$, também formam pares disjuntos.
Dessa forma, se escolhermos Y_1, não poderemos escolher Y_{2-k}, devemos tomar Y_2, analogamente, não podemos escolher Y_{3-k} e devemos tomar $Y_3 \ldots$ A situação é a mesma se escolhermos primeiro Y_{1-k}.

2.3.4 Caso de Igualdade

Para $n = 2k$, podemos particionar todos os k-conjuntos em pares disjuntos. Tome um elemento de cada par e teremos uma família intersectante de tamanho

$$\frac{1}{2}\binom{2k}{k} = \frac{(2k)!}{2(k!)^2} = \frac{(2k-1)!}{k!(k-1)!} = \binom{2k-1}{k-1} = \binom{n-1}{k-1}.$$

Para $n > 2k$, mostraremos que as únicas famílias intersectantes atingindo o tamanho máximo são do tipo $\mathcal{F}_j = \{S \subset \mathbb{Z}_n : |S| = k, j \in S\}$. No caso anterior, existe um número muito grande de famílias intersectantes possíveis (com tamanho máximo) e apenas n famílias do tipo $\mathcal{F}_j$, ou seja, a grande maioria das famílias não é do tipo $\mathcal{F}_j$.

Seja $\mathcal{F}$ uma família intersectante de tamanho máximo. Vamos começar com duas observações:

1. Suponha que existam x e y tais que todo k-conjunto contendo x e não contendo y pertence a $\mathcal{F}$. Então $\mathcal{F}$ consiste de todos os k-conjuntos contendo x. Para ver isso, suponha que $L \in \mathcal{F}$ não contenha x, então existe um k-conjunto K, com $L \cap K = \emptyset$ que contem x mas não y (pois $|\mathbb{Z}_n - L| = n - k > k$), mas é impossível termos $K, L \in \mathcal{F}$.

2. Há dois k-conjuntos, K, K', com $|K \cap K'| = k-1$, com $K \in \mathcal{F}$ e $K' \notin \mathcal{F}$. Suponha que isso não seja verdade e sejam $\{a_i\}_{i=1}^n = \mathbb{Z}_n$ e $K_1 = \{a_1, \ldots, a_k\} \in \mathcal{F}$.
Devemos ter $K_2 = \{a_2, \ldots, a_{k+1}\}$ em $\mathcal{F}$ pois $|K_1 \cap K_2| = k-1$. Continuando dessa mesma forma obteremos $K_{k+1} = \{a_{k+1}, \ldots a_{2k}\} \in \mathcal{F}$, mas $K_1 \cap K_{k+1} = \emptyset$.

Tome K, K' como em (2) e, sem perda de generalidade, assuma que $K = \{0, \ldots, k-1\}$ e $K' = \{1, \ldots, k\}$. Por (1), podemos tomar $K'' \notin \mathcal{F}$ com $0 \in K''$ e $k \notin K''$, e também podemos assumir sem perda de generalidade que $K'' = \{l-k, \ldots, 0, 1, \ldots, l-1\}$, com $1 \leq l < k$.

Pela caracterização de igualdade do lema, devemos ter k conjuntos intersectantes em Y e, como vimos acima, isso ocorre somente se tomarmos k conjuntos consecutivos. Mas $Y_0 = K \in \mathcal{F}, Y_1 = K' \notin \mathcal{F}, Y_{l-k} = K'' \notin \mathcal{F}$, ou seja, é impossível tomar k conjuntos intersectantes em Y.