Programa Olímpico de Treinamento

Curso de Combinatória – Nível 3

Prof. Carlos Shine

Aula 16

Probabilidades

Probabilidades aparecem em várias situações, tanto em matemática pura como aplicada. Probabilidades aparecem em experimentos que, em princípio, não podem ser previstos com certeza. Parece não fazer sentido tentar prever experimentos incertos, mas é exatamente isso que a probabilidade faz. Vejamos como.

Espaço amostral, evento, probabilidade

Considere um experimento. O conjunto de todos os possíveis resultados desse experimento é o *espaço amostral*. Muitas vezes nos interessamos em algum subconjunto desse espaço amostral. Qualquer subconjunto do espaço amostral é chamado *evento*. Dependendo do conjunto (se ele for discreto ou contínuo), associamos a cada elemento do conjunto um número que descreve frequência relativa, que em conjuntos discretos denominamos *probabilidade* e em conjuntos contínuos denominamos *densidade de probabilidade*. Trabalharemos só com conjunto discretos.

Definição 1. *Dado um espaço amostral S, definimos* probabilidade *como uma função $P\colon \mathcal{P}(S) \to [0,1]$ (ou seja, associamos a cada evento um número) tal que*

1. $P(\emptyset) = 0$ *(a probabilidade de nada acontecer é zero);*
2. $P(S) = 1$ *(a probabilidade de qualquer coisa acontecer é $1 = 100\%$);*
3. *Se $A \cap B = \emptyset$ então $P(A \cup B) = P(A) + P(B)$ (regra do OU para eventos disjuntos).*

Com isso, probabilidade de um evento E pode representar:

1. *chance* de E acontecer;
2. a *frequência* com que E acontece;
3. *informação/incerteza*: se $P(E) = 50\%$, então E é bastante incerto; se $P(E)$ é próximo de 100% então é quase certo que E ocorre; se $P(E)$ é próximo de 0 então é quase certo que E não ocorre.

Quando temos espaços *equiprováveis*, ou seja, cujas probabilidades são iguais para cada elemento do espaço amostral (isso é o mesmo que dizer que cada um tem a mesma chance de ocorrer), a probabilidade pode ser calculada por

$$P(E) = \frac{|E|}{|S|} = \frac{\text{casos favoráveis}}{\text{casos possíveis}}$$

Por causa da simplicidade dessa fórmula, vamos preferir, sempre que possível, trabalhar com espaços equiprováveis. Note que aí precisamos de certa sensibilidade para verificar quando um espaço amostral é equiprovável: caímos, nesse caso, em um problema de *modelagem*, em que há uma preocupação de o modelo matemático ter algum compromisso com a realidade do experimento em questão.

Enfim, ressaltamos que

Evento é subconjunto do espaço amostral.

Parece óbvio? Observe o exemplo a seguir.

Exemplo 1. *Na* Lotomania*, são sorteados* 50 *de* 100 *números. O sorteio consiste em escolher* 20 *dos* 100 *números, sem repetição. Existem um prêmio máximo para quem acerta os* 20 *números entre os seus* 50 *e um prêmio menor para quem não acerta nenhum dos* 20 *números. Calcule a probabilidade de uma aposta ganhar o prêmio máximo e a probabilidade de uma aposta ganhar o prêmio menor.*

Solução: Para o prêmio máximo, há $\binom{100}{50}$ possibilidades, das quais $\binom{50}{20}$ são favoráveis. Então a resposta é

$$\frac{\binom{50}{20}}{\binom{100}{50}},$$

certo?

Errado! Note que $\binom{100}{50}$ é a quantidade de *apostas* possíveis e $\binom{50}{20}$ é a quantidade de *sorteios* contidos nas respostas. Então estamos considerando um conjunto que *não está contido* no espaço amostral.

O que nos induziu ao erro? Foi simplesmente o fato de não termos definido o espaço amostral. Façamos isso agora. Há pelo menos duas possibilidades: *apostas* ou *sorteios*. Resolvamos o problema das duas formas:

- Usando apostas: temos $|S| = \binom{100}{50}$ e as apostas que contêm os vinte números sorteados são em total de $|E| = \binom{20}{20} \cdot \binom{80}{30}$ (escolhemos os 20 números sorteados e mais 30 entre os 80 números restantes para completar a aposta. Com isso, a probabilidade de ganhar o prêmio máximo é

$$\frac{\binom{20}{20} \cdot \binom{80}{30}}{\binom{100}{50}} = \frac{80!\,50!}{30!\,100!}$$

- Usando sorteios: temos $|S| = \binom{100}{20}$ sorteios, dentre os quais $\binom{50}{20}$ estão contidos na aposta. Então a probabilidade é

$$\frac{\binom{50}{20}}{\binom{100}{20}}$$

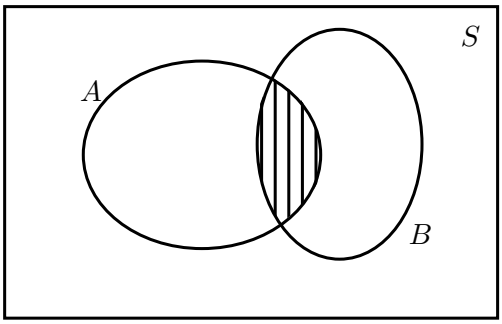
Parece outra resposta, mas não é:

$$\frac{\binom{50}{20}}{\binom{100}{20}} = \frac{50!\,80!}{30!\,100!}$$

A outra probabilidade fica para o leitor (calcule e você talvez terá uma pequena surpresa!).

Probabilidade condicional

Considerando que probabilidade mede *chance* ou *informação*, qualquer informação adicional restringe o espaço amostral e faz com que precisemos recalcular a probabilidade.



Denotamos $P(A|B)$ como a *probabilidade de A sabendo que ocorreu B*. O cálculo em espaços equiprováveis é

$$P(A|B) = \frac{|A \cap B|}{|B|}$$

Podemos usar probabilidades no lugar de cardinalidades:

$$P(A|B) = \frac{|A \cap B|/|S|}{|B|/|S|} = \frac{P(A \cap B)}{P(B)}$$

Em espaços não equiprováveis, usamos a fórmula com probabilidades.

Regra do E

Mexendo um pouco mais com a equação anterior, temos

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \iff P(A \cap B) = P(B) \cdot P(A|B)$$

Esse resultado é conhecido como *regra do E*.

Em muitos casos é possível resolver problemas de probabilidade condicional com a boa e velha fórmula dos espaços equiprováveis, refazendo o espaço amostral.

Exemplo 2. *Qual a probabilidade de obter duas caras no lançamento de três moedas, sabendo que*

(a) uma das moedas deu cara?

(b) a moeda da esquerda deu cara?

Solução:

(a) Representando K para cara e C para coroa, nosso espaço amostral deixa de ter CCC, tendo $2^3 - 1 = 7$ elementos. Desses, três são favoráveis: KKC, KCK, CKK. Então a probabilidade é $\frac{3}{7}$.

(b) Nosso espaço amostral é agora $\{KCC, KCK, KKC, KKK\}$, e dois dos quatro casos são favoráveis, de modo que a probabilidade é $\frac{2}{4} = \frac{1}{2}$.

Nem sempre podemos fazer isso, porém.

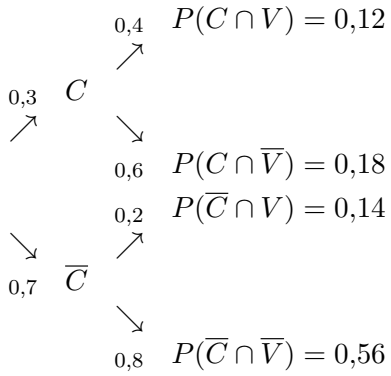
Exemplo 3. *Sabe-se que a chance de chuva no GP Mat de F1 é* 30%*. O piloto Pepe Legal tem* 40% *de chance de vencer caso chova e* 20% *de vencer caso não chova. Sabendo que Pepe Legal venceu, calcule a probabilidade de ter chovido.*

Solução: Sejam C o evento "choveu" e V o evento "Pepe Legal venceu o GP Mat". Temos $P(C) = 30\%$, $P(V|C) = 40\%$ e $P(V|\overline{C}) = 20\%$ ($\overline{C}$ é o *evento complementar* de C; note que, pela regra do OU, $P(C) + P(\overline{C}) = 1 \iff P(\overline{C}) = 1 - P(C)$).

A probabilidade pedida é $P(C|V) = \frac{P(C \cap V)}{P(V)}$. $P(C \cap V)$ é fácil de calcular: $P(C \cap V) = P(C) \cdot P(V|C) = 0{,}3 \cdot 0{,}4 = 0{,}12$. Quanto a $P(V)$, basta notar que Pepe Legal pode vencer com ou sem chuva, com probabilidades $P(V \cap C) = 0{,}12$ e $P(V \cap \overline{C}) = P(\overline{C}) \cdot P(V|\overline{C}) = 0{,}7 \cdot 0{,}2 = 0{,}14$. Logo $P(V) = 0{,}12 + 0{,}14 = 0{,}36$ e a probabilidade pedida é

$$P(V|C) = \frac{0{,}12}{0{,}26} = \frac{6}{13}.$$

Alguns se sentem mais confortáveis com o diagrama de árvore a seguir, que inclui algumas outras probabilidades:



Outros preferem usar uma tabela:

	C	$\overline{C}$	Total
V	$0{,}4 \cdot 0{,}3 = 0{,}12$	$0{,}2 \cdot 0{,}7 = 0{,}14$	0,26
$\overline{V}$	$0{,}6 \cdot 0{,}3 = 0{,}18$	$0{,}8 \cdot 0{,}7 = 0{,}56$	0,74
Total	0,3	0,7	1

Eventos independentes

Se $P(A|B) = P(A)$, dizemos que A e B são *independentes*. Note que isso quer dizer que saber que B ocorre não altera a chance de A ocorre. De certo modo, o evento B é irrelevante para A.

Em termos de proporções, se A e B são independentes, a proporção de A dentro de B se mantém em relação à proporção de A em relação a todo o espaço amostral.

União de eventos: a regra do OU

Quando tivermos eventos $A_1, A_2, \ldots, A_n$ dois a dois disjuntos (nunca acontece dois deles simultaneamente, ou $A_i \cap A_j = \emptyset$ para $i \neq j$), temos

$$P\left(\bigcup_{i=1}^{n} A_i\right) = P(A_1 \cup A_2 \cup \ldots \cup A_n) = P(A_1) + P(A_2) + \cdots + P(A_n) = \sum_{i=1}^{n} P(A_i)$$

Como é de se esperar, a probabilidade também satisfaz o princípio da inclusão-exclusão. Por exemplo,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(B \cap C) - P(C \cap A) + P(A \cap B \cap C)$$

Podemos então obter uma estimativa bacana a partir do princípio da inclusão-exclusão: pode-se mostrar que

Proposição 1. *A probabilidade da união de eventos é menor ou igual à soma das probabilidades dos eventos. Ou seja,*

$$P\left(\bigcup_{i=1}^{n} A_i\right) = P(A_1 \cup A_2 \cup \ldots \cup A_n) \leq P(A_1) + P(A_2) + \cdots + P(A_n) = \sum_{i=1}^{n} P(A_i)$$

Valor esperado e variância

Agora, consideremos um experimento que fornece um número X como resultado. Chamamos X de *variável aleatória*. Estamos interessados em saber a média dos números obtidos quando repetimos o experimento muitas vezes. Tal média é chamada *valor esperado de* X. Como o valor $X = a$ ocorre na fração $P(X = a)$ dos experimentos, o valor esperado de X pode ser dado por

$$E(X) = \sum_{a \in A} P(X = a) \cdot a$$

onde A é o conjunto de todos os valores que X pode assumir.

Não é difícil mostrar que

Proposição 2. *O valor esperado é linear, ou seja,* $E(X+Y) = E(X) + E(Y)$ *e* $E(kX) = kE(X)$ *para* k *constante.*

O princípio da casa dos pombos com médias simplesmente nos diz que

Proposição 3. *Sendo* X *uma variável aleatória. Então* X *assume um valor menor ou igual a* $E(X)$ *e um valor maior ou igual a* $E(X)$*.*

A variância mede o quanto a variável fica distante da média; quanto maior a variância, maior a variabilidade. Temos

$$\text{var}(X) = E((X - E(X))^2 = \sum_{a \in A} P(X = a) \cdot (a - E(X))^2$$

É comum denotarmos $\mu = E(X)$ e $\sigma^2 = \text{var}(X)$ (sim, usamos essa notação, ao quadrado mesmo).

A variância tem as seguintes propriedades:

Proposição 4. *Sendo* X *e* Y *variáveis aleatórias independentes, ou seja,* $P(X = a|Y = b) = P(X = a)$ *para todos* a, b*, temos* $\text{var}(kX) = k^2 \text{var}(X)$*,* $\text{var}(X+Y) = \text{var}(X) + \text{var}(Y)$ *e* $\text{var}(X - Y) = \text{var}(X) + \text{var}(Y)$ *(sim, é estranho assim mesmo).*

A estranheza das duas últimas fórmulas vem da definição de *covariância* $\text{cov}(X, Y)$ entre duas variáveis aleatórias X e Y. Por definição,

$$\text{cov}(X, Y) = E((X - E(X))(Y - E(Y)) = E(XY) - E(X)E(Y)$$

e a variância fica

$$\text{var}(X+Y) = \text{var}(X)+\text{var}(Y)+2\,\text{cov}(X, Y) \text{ e } \text{var}(X-Y) = \text{var}(X)+\text{var}(Y)-2\,\text{cov}(X, Y)$$

É essencialmente quadrado da soma/diferença; só que quando as variáveis são independentes temos $\text{cov}(X, Y) = 0$.

Desigualdades de Markov e Chebyshev

O valor esperado e a variância podem dar boas estimativas sobre a probabilidade.

Teorema 1 (Desigualdade de Markov)**.** *Seja* X *uma variável relacionada a um evento e seja* A *o conjunto dos possíveis valores de* X*. Mostre que*

$$P(X \geq a) \leq \frac{E(X)}{a}$$

Demonstração: Considere a *variável indicadora*

$$I_{X \geq a} = \begin{cases} 1, & \text{se } X \geq a \\ 0, & \text{se } X < a \end{cases}$$

Para cada $X \in A$ temos

$$\begin{aligned} X \geq aI_{X\geq a} &\iff P(X)\cdot X \geq aI_{X\geq a}\cdot P(X) \\ &\implies \sum_{X\in A} P(X)\cdot X \geq a\sum_{X\in A} I_{X\geq a}\cdot P(X) \\ &\iff E(X) \geq a\sum_{X\geq a} P(X) \\ &\iff P(X\geq a) \leq \frac{E(X)}{a} \end{aligned}$$

□

Exemplo 4. *Considere um experimento que gera um número inteiro entre* 0 *e* n*. Mostre que se o valor esperado deste número é menor que* 1*, então a probabilidade do número ser* 0 *é maior que zero, isto é, é possível que o número seja* 0*.*

Solução: Provemos a contrapositiva, ou seja, que se X nunca é zero então $E(X) \geq 1$. Se $P(X=0)=0$, então $P(X\geq 1)=1$ e

$$E(X) = \sum_{a=0}^{n} P(X=a)\cdot a \geq \sum_{a=1}^{n} P(X=a) = 1 - P(X=0) = 1.$$

□

Com um pouco mais de informação, podemos obter alguns resultados um pouco melhores.

Teorema 2 (Desigualdade de Chebyshev)**.** *Seja X uma variável aleatória com média μ e variância σ^2. Para todo real positivo λ,*

$$P(|X-\mu|) \geq \lambda\sigma) \leq \frac{1}{\lambda^2}.$$

Demonstração: Usando a desigualdade de Markov para a variável aleatória $Y = (X-\mu)^2$, temos

$$\begin{aligned} P(Y \geq \lambda^2\sigma^2) \leq \frac{E(Y)}{\lambda^2\sigma^2} &\iff P((X-\mu)^2 \geq \lambda^2\sigma^2) \leq \frac{E((X-\mu)^2)}{\lambda^2\sigma^2} \\ &\iff P(|X-\mu| \geq \lambda\sigma) \leq \frac{\sigma^2}{\lambda^2\sigma^2} = \frac{1}{\lambda^2} \end{aligned}$$

□

Exemplo 5. *Prove que* $P(X=0) \leq \frac{\mathrm{var}(X)}{(E(X))^2}$*.*

Solução: Pela desigualdade de Chebyshev,

$$P(X=0) \leq P\left(|X-\mu| \geq \mu = \frac{\mu}{\sigma}\cdot\sigma\right) \leq \frac{1}{(\mu/\sigma)^2} = \frac{\mathrm{var}(X)}{(E(X))^2}$$

□

O método probabilístico

Muitas vezes queremos demonstrar a existência de algo. Já vimos técnicas que fazem isso, como o princípio da casa dos pombos e continuidade discreta. Mas também podemos utilizar probabilidades, com resultados fantásticos! Usamos a seguinte ideia:

Se $P(A) > 0$ então existe um elemento com a propriedade A.

Como costuma ser difícil mostrar que um número é positivo, costumamos trabalhar com o complementar:

Se $P(\overline{A}) < 1$ então existe um elemento com a propriedade A.

Exemplo 6. *Um torneio de tênis com n participantes (onde todos jogam uma única vez contra todos) tem a propriedade S_k se, para todo conjunto X de k participantes do torneio, existe um participante não pertencente a X que venceu todos os participantes de X. Mostre que para cada k existe um torneio com a propriedade S_k.*

Solução: Estimaremos a probabilidade $P(n)$ de um torneio com n participantes **não** ter a propriedade S_k e mostraremos que existe n tal que $P(n) < 1$ (de modo que a probabilidade de o torneio ter S_k é $1 - P(n) > 0$).

Tomemos um torneio em que a probabilidade de cada tenista vencer cada jogo é $1/2$. Fixemos um conjunto X com k participantes. Este conjunto "estraga" o torneio se todos os $n-k$ demais participantes perde de pelo um participante de X. A probabilidade de isso acontecer é $\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k}$ (por quê?). Como existem $\binom{n}{k}$ conjuntos X's, a probabilidade de um ou mais deles "estragar" o torneio é menor ou igual a $\binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k}$ (ou um estraga ou outro estraga ou...). Logo

$$P(n) < \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} \iff 1 - P(n) > 1 - \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k}$$

Deste modo, basta

$$1 - \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} > 0 \iff \binom{n}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{n-k} < 1$$

Seja $f(m) = \binom{m}{k}\left(1 - \left(\frac{1}{2}\right)^k\right)^{m-k}$. Temos

$$\frac{f(m+1)}{f(m)} = \left(1 - \left(\frac{1}{2}\right)^k\right) \cdot \frac{m+1}{m+1-k} = \left(1 - \left(\frac{1}{2}\right)^k\right) \cdot \frac{1}{1 - \frac{k}{m+1}}$$

Como

$$\left(1 - \left(\frac{1}{2}\right)^k\right) \cdot \frac{1}{1 - \frac{k}{m+1}} < 1 \iff m > k \cdot 2^k - 1,$$

então $\frac{f(m+1)}{f(m)} < 1$ para $m > k \cdot 2^k - 1$, o que implica

$$f(m) < a \cdot c^m, \text{ onde } a = \frac{f(k \cdot 2^k - 1)}{c^{k \cdot 2^k - 1}}$$

Assim, sendo a e c constantes com $0 < c < 1$, e c^m arbitrariamente próximo de 0 quando m é suficientemente grande, temos que existe n tal que $f(n) < 1$. □

Às vezes só ter probabilidade maior do que zero não adianta. Muitas vezes provamos que algo que *quase* tem a propriedade existe e fazemos modificações.

O seguinte resultado foi obtido por Erdős, em 1959. Definimos o *número cromático* de um grafo como o menor número de cores necessárias para pintar os vértices do grafo de modo que não haja dois vértices de mesma cor ligados por uma aresta (sim, isto tem a ver com o teorema das quatro cores!). A *cintura* de um grafo é o número mínimo de vértices dos ciclos contidos no grafo.

Exemplo 7. *Mostre que existe um grafo com número cromático maior que χ e cintura maior que g, para todos χ, g inteiros positivos.*

Solução: Considere um grafo com n vértices e, para cada par de vértices, ligamos uma aresta aleatoria e independentemente com probabilidade p a ser determinada. Seja X o número de ciclos com tamanho no máximo g. A probabilidade de um ciclo ter os vértices $v_1, v_2, \ldots, v_k$, $k \geq 3$, é $(k-1)!p^k/2$ (há $(k-1)!$ permutações circulares, mas pode ser nos dois sentidos). Assim, para $np < 1$,

$$E(X) = \sum_{k=3}^{g} \binom{n}{k} \frac{(k-1)!p^k}{2} < \sum_{k=3}^{g} \frac{(np)^k}{2k} < \frac{1}{2} g (np)^3$$

Em particular, pela desigualdade de Markov, $p_1 = P(X \geq n/2) \leq 2E(X)/n$.

Agora, vamos ao número cromático. Antes precisamos do *número de independência de um grafo* G $\alpha(G)$, que é simplesmente a maior quantidade de vértices tais que não há dois ligados por aresta em G. A quantidade de conjuntos sem arestas é, então, pelo menos $|V(G)|/\alpha(G)$ (todo conjunto sem arestas tem no máximo $\alpha(G)$ elementos), e como pintamos exatamente conjuntos sem arestas, o número cromático é pelo menos $|V(G)|/\alpha(G)$.

Então a ideia é estimar o número de independência α de G. Queremos que ele seja maior ou igual a n/χ. Mas isso é fácil de estimar: a probabilidade de um conjunto com m vértices não ter arestas é $(1-p)^{\binom{m}{2}}$. Então, pela desigualdade da união,

$$p_2 = P(\alpha \geq m) \leq \binom{n}{m} (1-p)^{\binom{m}{2}} < n^m e^{-p\binom{m}{2}} = (n e^{-p(m-1)/2})^m,$$

em que usamos a desigualdade $1 - x < e^{-x}$ para $x > 0$.

Assim, a probabilidade de um grafo ter mais de $n/2$ ciclos "pequenos" ou ter número cromático menor do que χ é no máximo $p_1 + p_2$. Então basta escolher N e p para os quais $p_1 + p_2 < 1$. Vamos fazer melhor: vamos fazer p_1 e p_2 ficarem próximos de zero.

Primeiro, para diminuir $p_1 < \frac{2}{n}\frac{1}{2} g (np)^3 = n^2 p^3 g$, fazemos np pequeno e n grande (por exemplo, $p = n^{-2/3-\epsilon}$ basta, e $p_1 < g/n^{3\epsilon}$, que fica arbitrariamente próximo de zero quando n cresce). Isso faz sentido: é melhor ter poucas arestas para ter menos ciclos.

Vamos a $p_2 < (ne^{-p(m-1)/2})^m$. Vamos escolher m perto de $3\ln n/p$, de modo que $-p(m-1)/2 < -p\ln n/p = -\ln n \implies ne^{-p(m-1)/2} < ne^{-\ln n} = 1$; como o expoente $m \approx 3n^{2/3+\epsilon}\ln n$ fica arbitrariamente grande, p_2 pode ficar arbitrariamente pequeno.

Então, para algum n suficientemente grande, conseguimos um (na verdade, muitos – a maioria!) grafo G com n vértices com no máximo $n/2$ ciclos "pequenos" e α menor que m. O segredo agora é tirar vértices: tiramos um vértice de cada um dos ciclos "pequenos" e obtemos um grafo com pelo menos $n/2$ vértices. A retirada de vértices não aumenta o α, então temos

$$\chi \geq \frac{n/2}{m} = \frac{n/2}{3n^{2/3+\epsilon}\ln n} = \frac{n^{1/3-\epsilon}}{6\ln n}$$

e basta escolher n tal que essa última fração é maior que k, o que é possível pois $n^{1/3-\epsilon}$ cresce bem mais do que $6\ln n$ para $\epsilon < 1/3$. □

Outra ideia é utilizar o princípio da casa dos pombos com médias, ou seja, valor esperado.

Exemplo 8. *Considere um torneio de tênis com n jogadores. Um* caminho hamiltoniano *do torneio é uma sequência de n jogadores distintos i_1, i_2, …, i_n tais que i_1 vence i_2, i_2 vence i_3, …, i_{n-1} vence i_n. Mostre que existe um torneio com pelo menos $n!/2^{n-1}$ caminhos hamiltonianos.*

Solução: Para cada um dos $\binom{n}{2}$ pares de jogadores, jogue uma moeda honesta para decidir quem ganha o jogo. Então, para cada uma das $n!$ permutações dos jogadores, a probabilidade de eles estarem "na ordem certa" na classificação é $1/2^{n-1}$ ($1/2$ para o jogo entre o i-ésimo e o $(i+1)$-ésimo jogadores, $1 \leq i < n$). Assim, como há $n!$ permutações, o valor esperado de caminhos hamiltonianos é $n! \cdot \frac{1}{2^{n-1}}$. Assim, pelo princípio da casa dos pombos com médias, existem torneios com pelo menos $n!/2^{n-1}$ caminhos hamiltonianos. □

Exemplo 9. *(EUA) Sendo $n \geq 2$ inteiro, sejam $x_1, x_2, \ldots, x_n$ reais tais que*

$$x_1 + x_2 + \cdots + x_n = 0 \quad e \quad x_1^2 + x_2^2 + \cdots + x_n^2 = 1.$$

Para cada subconjunto $A \subseteq \{1, 2, \ldots, n\}$, defina

$$S_A = \sum_{i \in A} x_i.$$

(se A é o conjunto vazio, $S_A = 0$.)

Prove que para todo real positivo λ a quantidade de conjuntos A satisfazendo $S_A \geq \lambda$ é no máximo $2^{n-3}/\lambda^2$. Para que valores de $x_1, x_2, \ldots, x_n, \lambda$ ocorre a igualdade?

Solução: Parece um problema de álgebra (e, de certa forma, é), mas tem um pouco de combinatória no meio (a parte da quantidade de conjuntos). Como tem λ^2, a ideia é elevar as somas ao quadrado e somar tudo. Sendo S a soma total de todos os S_A's, somando sobre todos os subconjuntos de $\{1, 2, \ldots, n\}$, temos em S termos do tipo x_k^2, $1 \leq k \leq n$, e do tipo $x_i x_j$, $1 \leq i < j \leq n$. O k do x_k^2 aparece em 2^{n-1} subconjuntos, logo o coeficiente de x_k^2 em S é 2^{n-1}; além disso, os termos $x_i x_j$ aparecem em todo S_A com $i, j \in A$, e

aparece multiplicado por 2. Como há 2^{n-2} tais subconjuntos, o o coeficiente de x_ix_j é $2 \cdot 2^{n-2} = 2^{n-1}$. Logo, utilizando a notação de polinômios simétricos $s_2 = \sum_{1\leq k\leq n} x_k^2$ e $\sigma_2 = \sum_{1\leq i<j\leq n} x_ix_j$ e lembrando que $s_2 = \sigma_1^2 - 2\sigma_2 \iff \sigma_2 = (\sigma_1^2 - s_2)/2$,

$$\begin{aligned} S &= 2^{n-1}\left(\sum_{1\leq k\leq n} x_k^2 + \sum_{1\leq i<j\leq n} x_ix_j\right)^2 = 2^{n-1}(s_2+\sigma_2) \\ &= 2^{n-1}\left(s_2 + \frac{\sigma_1^2 - s_2}{2}\right) = 2^{n-1}\left(1 + \frac{0^2-1}{2}\right) = 2^{n-2} \end{aligned}$$

Mas $S_A + S_{\overline{A}} = 0$, logo os S_A's positivos e negativos vêm aos pares. Somando somente sobre os S_A's positivos, obtemos como total da soma dos quadrados $S/2 = 2^{n-3}$. Agora, somando só sobre os S_A's maiores ou iguais a λ, sendo N a quantidade de tais subconjuntos obtemos

$$2^{n-3} \geq \sum_{S_A\geq\lambda} S_A \geq N\cdot\lambda^2 \implies N \leq \frac{2^{n-3}}{\lambda^2}.$$

A igualdade ocorre quando todos os S_A's têm soma igual a $\pm\lambda$ ou zero. Isso só acontece se tem só um λ e um $-\lambda$ (se tiver mais de um λ, tem um subconjunto com soma 2λ, e não dá certo. Assim, o caso de igualdade ocorre quando $(x_1, x_2, \ldots, x_n) = (\lambda, -\lambda, 0, \ldots, 0)$ e permutações. Substituindo na condição da soma dos quadrados, achamos $\lambda = \sqrt{2}/2$. □

Agora, o que esse problema tem a ver com método probabilístico? Na verdade, o problema é inspirado no método do segundo momento.

Outra solução: Considere variáveis aleatórias independentes V_i, em que $V_i = 2x_i$ com probabilidade $1/2$ e $V_i = 0$ com probabilidade $1/2$. Note que $E(V_i) = \frac{1}{2}\cdot 2x_i + \frac{1}{2}\cdot 0 = x_i$ e $\text{var}(V_i) = \frac{1}{2}(2x_i - x_i)^2 + \frac{1}{2}(0-x_i)^2 = x_i^2$ Então, sendo $V = V_1 + V_2 + \cdots + V_n$,

$$\begin{aligned} E(V) &= E(V_1) + E(V_2) + \cdots + E(V_n) = x_1 + x_2 + \cdots + x_n = 0 \\ \text{var}(V) &= \text{var}(V_1) + \text{var}(V_2) + \cdots + \text{var}(V_n) = x_1^2 + x_2^2 + \cdots + x_n^2 = 1 \end{aligned}$$

Agora, o que representa um valor típico de V? Com probabilidade $(1/2)^n = 1/2^n$, V é igual a $\sum_{i\in A} 2x_i = 2S_A$ para algum $A \subseteq \{1, 2, \ldots, n\}$. Ou seja, V assume cada valor de $2S_A$.

Aplicando a desigualdade de Chebyshev com $\mu = E(V) = 0$ e $\sigma = \sqrt{\text{var}(V)} = 1$, temos

$$P(|V| \geq 2\lambda\cdot 1) \leq \frac{1}{(2\lambda)^2} \iff P(|S_A| \geq \lambda) \leq \frac{1}{4\lambda^2}$$

Mas sabemos que os S_A's positivos e negativos aparecem aos pares, logo

$$P(S_A \geq \lambda) \leq \frac{1}{2}\cdot\frac{1}{4\lambda^2} = \frac{1}{8\lambda^2}$$

Sendo N a quantidade de conjuntos A com $S_A \geq \lambda$, temos

$$\frac{N}{2^n} \leq \frac{1}{8\lambda^2} \iff N \leq \frac{2^{n-3}}{\lambda^2}$$

O caso de igualdade é encontrado como na solução anterior. □

Problemas

1. (OBM) Duas pessoas vão disputar uma partida de par ou ímpar. Elas não gostam do zero e, assim, cada uma coloca 1, 2, 3, 4 ou 5 dedos com igual probabilidade. Calcule a probabilidade de que a pessoa que escolheu par ganhe.

2. (OBM) Uma rifa foi organizada entre os 30 alunos da turma do Pedro. Para tal, 30 bolinhas numeradas de 1 a 30 foram colocadas em uma urna. Uma delas foi, então, retirada da urna. No entanto, a bola caiu no chão e se perdeu e uma segunda bola teve que ser sorteada entre as 29 restantes. Qual a probabilidade de que o número de Pedro tenha sido o sorteado desta segunda vez?

3. (OBM) Dois cubos têm faces pintadas de ocre ou magenta. O primeiro cubo tem cinco faces ocres e uma face magenta. Quando os dois cubos são lançados, a probabilidade de as faces viradas para cima dos dois cubos serem da mesma cor (sim, ocre e magenta são cores!) é 1/2. Quantas faces ocres tem o segundo cubo?

4. (OBM) Uma colônia de amebas tem inicialmente uma ameba amarela e uma ameba vermelha. Todo dia, uma única ameba se divide em duas amebas idênticas. Cada ameba na colônia tem a mesma probabilidade de se dividir, não importando sua idade ou cor. Qual é a probabilidade de que, após 2006 dias, a colônia tenha exatamente uma ameba amarela?

5. (OBM) No programa de auditório Toto Bola, o apresentador Ciço Magallanes dispõe de duas caixas idênticas. Um voluntário da platéia é chamado a participar da seguinte brincadeira: ele recebe dez bolas verdes e dez bolas vermelhas e as distribui nas duas caixas, sem que o apresentador veja, e de modo que em cada caixa haja pelo menos uma bola. Em seguida, o apresentador escolhe uma das caixas e retira uma bola. Se a bola for VERDE, o voluntário ganha um carro. Se for VERMELHA, ele ganha uma banana. A máxima probabilidade que o voluntário tem de ganhar um carro é igual a $\frac{m}{n}$, em que m e n são inteiros positivos primos entre si. Determine o valor de $m + n$.

6. (OBM) Um quadrado de lado 3 é dividido em 9 quadrados de lado unitário, formando um quadriculado. Cada quadrado unitário é pintado de azul ou vermelho. Cada cor tem probabilidade $\frac{1}{2}$ de ser escolhida e a cor de cada quadrado é escolhida independentemente das demais. Qual a probabilidade de obtermos, após colorirmos todos os quadrados unitários, um quadrado de lado 2 pintado inteiramente de uma mesma cor?

7. (OBM) Quantos dados devem ser lançados ao mesmo tempo para maximizar a probabilidade de se obter exatamente um 2?

8. (OBM) Ao jogarmos uma certa quantidade de dados cúbicos com faces numeradas de 1 a 6, a probabilidade de obtermos soma dos pontos 2006 é igual à probabilidade de obtermos soma dos pontos S. Qual é o menor valor possível de S?

9. (OPM) Nos aviões, o cartão de embarque indica, entre outras coisas, o lugar onde o passageiro deve se sentar.

   Murali, o primeiro passageiro a embarcar em um avião, com lugar para 100 pessoas, perdeu seu cartão de embarque, e por isso sentou-se em um assento que escolheu aleatoriamente. Em seguida, cada um dos demais 99 passageiros sentou-se em seu lugar, se este estava livre, ou caso contrário escolheu ao acaso um dos assentos vagos.

   Seja $P(k)$ a probabilidade de o k-ésimo passageiro a embarcar tenha sentado em seu lugar designado.

   a) Calcule $P(2)$, $P(3)$ e $P(4)$.
   b) Encontre uma expressão para $P(k)$, $2 \leq k \leq 100$. Não se esqueça de que você deve justificar sua resposta.

10. (BAMO) São dados n números reais, não todos nulos, cuja soma é 0. Prove que é possível rotular os números em alguma ordem $a_1, a_2, \ldots, a_n$ de modo que

$$a_1a_2 + a_2a_3 + \cdots + a_{n-1}a_n + a_na_1 < 0.$$

11. Sejam A_1, A_2, ..., A_r subconjuntos de $A = \{1; 2; 3; \ldots; n\}$. Colorimos cada elemento de A de azul ou vermelho. Mostre que podemos pintar os elementos de modo que no máximo $\sum_{i=1}^{r} (\frac{1}{2})^{|A_i|-1}$ dos subconjuntos tenha todos os elementos de mesma cor.

12. Prove que é possível pintar cada um dos números 1, 2, 3, ..., n de vermelho ou azul de modo que não exista uma progressão aritmética com $k \geq 3$ elementos pintados da mesma cor quando $n < 2^{k/2}$.

13. Sejam p e q reais não negativos cuja soma é 1 e m e n inteiros não negativos. Prove que

$$(1 - p^m)^n + (1 - q^n)^m \geq 1.$$

14. (Banco da IMO) Seja A um conjunto de n resíduos módulo n^2. Prove que existe um conjunto B de n resíduos módulo n^2 tal que pelo menos metade dos resíduos módulo n^2 pode ser escrito como $a + b$ com $a \in A$ e $b \in B$.

15. (Suécia) Uma cidade tem $3n$ habitantes. Quaisquer duas pessoas na cidade têm um amigo em comum na cidade. Mostre que é possível escolher um grupo de n pessoas da cidade de modo que todas as demais $2n$ pessoas conhecem pelo menos uma das pessoas do grupo.

16. Um conjunto A é dito *livre de somas* se a soma de quaisquer dois elementos (possivelmente iguais) de A não pertence a A. Prove que todo conjunto B de inteiros não nulos tem um subconjunto livre de somas com pelo menos $|B|/3$ elementos.

17. Um conjunto $X = \{x_1, x_2, \ldots, x_k\}$ tem somas distintas se todas as somas

$$\sum_{i \in S} x_i, \quad S \subseteq \{1, 2, \ldots, k\}$$

são distintas.

Seja $f(n)$ o tamanho máximo de um subconjunto de $\{1, 2, \ldots, n\}$ com somas distintas. O exemplo $\{1, 2, 4, \ldots, 2^{\lfloor \log_2 n \rfloor}\}$ mostra que $f(n) \geq 1 + \lfloor \log_2 n \rfloor$. Prove que

$$f(n) < \log_2 n + \frac{1}{2} \log_2 \log_2 n + c,$$

sendo c uma constante. Use o fato de que $2^k > nk \implies k < \log_2 n + \log_2 \log_2 n + c$ para alguma constante c.

Bibliografia

1. N. Alon, J. H. Spencer, P. Erdős, *The Probabilistic Method*, John Wiley & Sons 1992.
2. T. Andreescu e Z. Feng, *102 Combinatorial Problems, From the training of the USA IMO team*, Birkhäuser 2003.
3. R. Boppana, *Unexpected Uses of Probability*. Disponível na Internet, 2005.
4. Diversas listas do professor Po-Shen Loh, disponíveis em

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

Respostas, Dicas e Soluções

1. $\frac{13}{25}$. Faça uma tabela 5×5 com os resultados possíveis.
2. $\frac{1}{30}$. Considere como espaço amostral as possíveis posições do número do Pedro se colocarmos os números em fila, em ordem de sorteio.
3. 3. Com probabilidade condicional sai bem fácil: dada a cor do primeiro dado, a probabilidade nesse caso é sempre 1/2.
4. $\frac{1}{2} \cdot \frac{2}{3} \cdots \frac{2006}{2007} = \frac{1}{2007}$. Use a regra do E.
5. $m = 14$, $n = 19$, probabilidade $\frac{14}{19}$. Seja $P(a, b)$ a probabilidade de o voluntário ganhar o carro no caso em que ele tenha colocado a bolas VERDES e b bolas VERMELHAS na caixa 1. Então, necessariamente haverá $10 - a$ bolas VERDES e $10 - b$ bolas VERMELHAS na caixa 2. Segue que

$$P(a, b) = \frac{1}{2} \cdot \frac{a}{a+b} + \frac{1}{2} \cdot \frac{10-a}{20-a-b}.$$

Podemos supor, sem perda de generalidade, que $a + b \leq 10$, já que as caixas são idênticas. Suponha, ainda, que haja alguma bola VERMELHA na caixa 1. Vejamos o que acontece com essa probabilidade se transferirmos uma bola VERDE da caixa 2 para a caixa 1 e uma bola VERMELHA da caixa 1 para a caixa 2. Ficamos com

$$P(a+1, b-1) = \frac{1}{2} \cdot \frac{a+1}{a+b} + \frac{1}{2} \cdot \frac{9-a}{20-a-b}.$$

Dessa forma,

$$P(a+1,b-1)-P(a,b)=\frac{1}{2}\left(\frac{1}{a+b}-\frac{1}{20-a-b}\right)\geq 0,$$

pois $a+b\leq 10$.

Assim, o voluntário sabe que, enquanto houver bola VERMELHA na caixa que contém menos bolas, a probabilidade pode ser aumentada, bastando, para isto, que ele troque uma das bolas VERMELHAS desta caixa com uma VERDE da outra. Por isso, para maximizarmos a probabilidade, basta considerarmos o caso em que a caixa 1 contém apenas bolas VERDES e a caixa 2 contém o restante das bolas. Teremos

$$P(a,0)=\frac{1}{2}+\frac{1}{2}\cdot\frac{10-a}{20-a}=1-\frac{5}{20-a}.$$

Logo, a probabilidade será máxima quando a for mínimo. Como em cada caixa deve haver pelo menos uma bola, devemos ter $a=1$. Neste caso, a probabilidade é $P(1,0)=1-\frac{5}{19}=\frac{14}{19}$. Segue que $m=14$, $n=19$ e $m+n=33$.

6. $\frac{95}{256}$. Primeiro note que, como não é possível haver um quadrado 2×2 azul e um quadrado 2×2 vermelho ao mesmo tempo, a probabilidade pedida é duas vezes a probabilidade de haver um quadrado 2×2 azul. Há quatro possibilidades para o quadrado 2×2; sendo A_i o conjunto das pinturas contendo o quadrado i, queremos $P(A_1\cup A_2\cup A_3\cup A_4)$. Note que $A_i\cap A_j$ consiste em pintar a região da união dos quadrados correspondentes de azul e escolher as cores das outras casinhas.

7. Cinco ou seis. A probabilidade de se obter exatamente um 2 ao lançar n dados é $f(n)=n\cdot\frac{1}{6}\cdot\left(\frac{5}{6}\right)^{n-1}=\frac{n\cdot 5^{n-1}}{6^n}$. Temos

$$\frac{f(n)}{f(n-1)}>1\iff\frac{5n}{6(n-1)}>1\iff n<6$$

Logo $f(1)<f(2)<\ldots<f(5)=f(6)>f(7)>\ldots$, e o máximo ocorre para $n=5$ ou $n=6$.

8. 339. Sendo n a quantidade de dados, faça uma bijeção entre $(a_1,a_2,\ldots,a_n)$ e $(7-a_1,7-a_2,\ldots,7-a_n)$.

9. a) O mais fácil é trabalhar com o complementar, ou seja, calcular a probabilidade $Q(k)=1-P(k)$ de o k-ésimo passageiro não encontrar o seu lugar livre. Para $k=2$, basta que Murali sente no seu lugar: $Q(2)=\frac{1}{100}$; para $k=3$, ou Murali senta no lugar dele ou Murali senta no lugar do segundo passageiro e o segundo passageiro senta no lugar dele, ou seja, $Q(3)=\frac{1}{100}+\frac{1}{100}\cdot\frac{1}{99}=\frac{1}{99}$; para $k=4$, ou Murali senta no lugar dele, ou no lugar do segundo passageiro e o segundo passageiro no lugar dele, ou no lugar do segundo passageiro, o segundo passageiro senta no lugar do terceiro e o terceiro senta no lugar dele, ou no lugar do terceiro passageiro e o terceiro passageiro senta no lugar dele, ou seja, $Q(4)=\frac{1}{100}+\frac{1}{100}\cdot\frac{1}{99}+\frac{1}{100}\cdot\frac{1}{99}\cdot\frac{1}{98}+\frac{1}{100}\cdot\frac{1}{98}=\frac{1}{98}$. Logo $P(2)=1-Q(2)=\frac{99}{100}$, $P(3)=1-Q(3)=1-\frac{1}{99}=\frac{98}{99}$ e $P(4)=1-Q(4)=1-\frac{1}{98}=\frac{97}{98}$.

b) A probabilidade de alguém até o $k-2$-ésimo passageiro sentar no lugar do k-ésimo passageiro é igual à probabilidade de algum desses passageiros sentar no lugar do $(k-1)$-ésimo passageiro, ou seja, é $Q(k-1)$. Calculemos a probabilidade de o $(k-1)$-ésimo passageiro sentar no lugar do k-ésimo passageiro: para isso é necessário que alguém sente no lugar dele, o que ocorre com probabilidade $Q(k-1)$, e o $(k-1)$-ésimo sente no lugar do k-ésimo passageiro, o que ocorre com probabilidade $\frac{1}{100-(k-2)} = \frac{1}{102-k}$ (ele encontra $100-(k-2)$ lugares livres ao entrar). Logo $Q(k) = Q(k-1) + Q(k-1) \cdot \frac{1}{102-k} = \frac{103-k}{102-k} Q(k-1)$.
Expandindo, obtemos

$$Q(k) = \frac{103-k}{102-k} \cdot \frac{104-k}{103-k} \cdot \frac{105-k}{104-k} \cdot \ldots \cdot Q(2) = \frac{1}{102-k}$$

e $P(k) = 1 - Q(k) = \frac{101-k}{102-k}$.

10. Sejam $x_1, x_2, \ldots, x_n$ os números e considere uma permutação qualquer deles. O valor esperado da soma é

$$\begin{aligned} \frac{1}{n!} \cdot 2(n-2)! \sum_{1 \le i < j \le n} x_i x_j &= \frac{1}{n(n-1)} \left(\left(\sum_{1 \le i \le n} x_i \right)^2 - \sum_{1 \le i \le n} x_i^2 \right) \\ &= \frac{1}{n(n-1)} \sum_{1 \le i \le n} x_i^2 < 0, \end{aligned}$$

então alguma soma é negativa.

11. Pinte cada elemento aleatoriamente, com probabilidade $\frac{1}{2}$ para cada cor. A probabilidade de um subconjunto fixado A_i ter todos os elementos de uma mesma cor é $\frac{2}{2^{|A_i|}} = \left(\frac{1}{2}\right)^{|A_i|-1}$. Então o valor esperado de subconjuntos com elementos de uma mesma cor é a soma das probabilidades, que é $\sum_{i=1}^{r} \left(\frac{1}{2}\right)^{|A_i|-1}$, e existe uma pintura que tem pelo menos essa quantidade de subconjuntos com todos os elementos de uma cor só.

12. Pinte cada elemento aleatoriamente, com probabilidade $\frac{1}{2}$ para cada cor. A probabilidade de uma progressão aritmética $(i, i+r, i+2r, \ldots, i+(k-1)r)$ fixada ter todos os elementos da mesma cor é $2\left(\frac{1}{2}\right)^k = \left(\frac{1}{2}\right)^{k-1}$. Vamos estimar a quantidade de progressões aritméticas contidas em $\{1, 2, \ldots, n\}$. Para isso, basta contar as quantidades de termos iniciais (que é menor do que n) e razões (que é menor do que $n/2$, já que $k \ge 3$). Assim, a quantidade de progressões aritméticas é menor do que $n \cdot n/2 < 2^{k/2} \cdot 2^{k/2-1} = 2^{k-1}$, e o valor esperado de progressões aritméticas monocromáticas é menor do que $2^{k-1} \cdot \frac{1}{2^{k-1}} = 1$, e assim existe uma pintura com quantidade de progressões aritméticas monocromáticas menor do que 1, ou seja, zero.

13. Considere uma tabela $m \times n$. Preencha cada casa da tabela com 0 ou 1 aleatoriamente, com probabilidade p para 0 e q para 1. A probabilidade de ter pelo menos um 1 em

cada coluna é $P(A) = (1-p^m)^n$ e a probabilidade de ter pelo menos um 0 em cada linha é $P(B) = (1-q^n)^m$. Note que ocorre uma coisa ou outra (ou ambas): se uma coluna não tem 1, todas as linhas têm 0; se uma linha não tem 0, todas as colunas têm 1. Então $P(A) + P(B) \geq P(A \cup B) = 1 \implies (1-p^m)^n + (1-q^n)^m \geq 1$.

14. Escolha um conjunto B com n elementos aleatórios de $\mathbb{Z}/(n^2)$, com reposição. Calculemos a probabilidade de um resto fixado r não pertencer a $A+B$: basta que nenhum dos números $r-a$, $a \in A$, pertença a B. Isso ocorre com probabilidade $\left(1-\frac{1}{n}\right)^n$ (a chance de não sortearmos um elemento da forma $r-a$ é $1-\frac{1}{n}$).

    Como $n^n > 2(n-1)^n \iff \left(1-\frac{1}{n}\right)^n < \frac{1}{2}$ para $n \geq 2$, temos que a probabilidade de r não pertencer a $A+B$ é menor do que $\frac{1}{2}$, e o valor esperado de números que não estão em $A+B$ é menor do que $n^2/2$. Logo o valor esperado de números que estão em $A+B$ é maior do que $n^2/2$ e existe um B desejado. De fato, para n grande existe um conjunto B tal que $A+B$ tem pelo menos $n^2\left(1-\frac{1}{e}\right)$ elementos!

15. Chamemos de qualquer grupo que satisfaz as condições do enunciado de *dominante*. Seja p um número em $]0,1[$ a ser determinado. Vamos ver para que valores de p conseguimos um grupo dominante com np elementos, e torcer para que p possa ser pequeno.

    Se alguma pessoa conhece menos de $3np$ pessoas, o problema acaba imediatamente (basta tomar um habitante e seus menos de $3np$ conhecidos). Então vamos supor que todos os graus são maiores ou iguais a np. Parece fácil achar um conjunto dominante pequeno agora que temos tantas arestas. De fato, sorteie np pessoas ao acaso, com repetição. Isso forma um grupo com no máximo np pessoas. A probabilidade de que um vértice qualquer não tenha um conhecido nesse grupo é menor do que $(1-p)^{3np}$ (a probabilidade desse habitante conhecer alguém fixo do grupo é $1-p$). Mas $(1-p)^{3np} \leq (e^{-p})^{3np} = e^{-3np^2}$, e a probabilidade de algum habitante não ter conhecidos no grupo é menor do que $3ne^{-3np^2}$. Basta então fazer $e^{-3np^2} \leq \frac{1}{3n}$; tomando $p = \sqrt{\frac{\ln(3n)}{3}n}$ dá certo, e $3np = \sqrt{3n\ln(3n)}$ é bem menor do que n.

16. A grande ideia é jogar algo sem muito estrutura (como nosso conjunto B) para algo mais estruturado, no caso o conjunto $\mathbb{Z}/(p)$, p primo grande. Se $p = 3k+2$, o conjunto $C = \{k+1, k+2, \ldots, 2k+1\} \subset \mathbb{Z}^*/(p)$ é livre de somas e tem $k+1$ elementos, uma fração $\frac{k+1}{2k+1} > \frac{1}{3}$.

    Quando comparamos duas estruturas, a ideia que vem é tentar cruzá-las, com contagem dupla, por exemplo. $\mathbb{Z}^*/(p)$ tem boa estrutura, e a contagem ajuda a encontrar alguém, mesmo que não haja estrutura em B. O que usamos? O "gira-gira". Multiplique todos os elementos de B por x, $1 \leq x < p$, e reduza módulo p. Nenhum $b \in B$ é 0 módulo p, então aparecem todos os resíduos módulo p em $b\mathbb{Z}^*/(p)$, ou seja, C aparece em todo $b\mathbb{Z}^*/(p)$. Mas, definindo $D_x = xB \pmod p$, sendo $|C| > \frac{1}{3}|\mathbb{Z}^*/(p)|$, a probabilidade de algum elemendo de D pertencer a C é maior do que $\frac{1}{3}$, e portanto o valor esperado de elementos de D_x em C é maior do que $|B|/3$. Então existe um D_t com mais de $|B|/3$ elementos de C, e esse é o subconjunto A que queremos. De

fato, se $a_1, a_2, a_3 \in A$ são tais que $a_1 + a_2 = a_3$ então $ta_1 + ta_2 \equiv ta_3 \pmod{p}$, com $ta_1, ta_2, ta_3 \in C$, absurdo. Logo A é livre de somas.

17. Considere $\{x_1, x_2, \ldots, x_k\}$ com somas distintas e variáveis aleatórias independentes $\epsilon_1, \epsilon_2, \ldots, \epsilon_k$ tais que $P(\epsilon_i = 0) = P(\epsilon_i = 1) = \frac{1}{2}$ e seja $X = \epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_k x_k$ (X é uma soma aleatória). Temos

$$\mu = E(X) = \frac{x_1 + x_2 + \cdots + x_k}{2}$$

e limitamos a variância: sendo $x_i \leq n$,

$$\sigma^2 = \frac{x_1^2 + x_2^2 + \cdots + x_k^2}{4} \leq \frac{n^2 k}{4} \implies \sigma \leq \frac{n\sqrt{k}}{2}$$

Aplicando a desigualdade de Chebyshev, temos

$$P\left(|X - \mu| \leq \frac{\lambda n\sqrt{k}}{2}\right) \leq \lambda^{-2}$$

Tomando complementares obtemos

$$P\left(|X - \mu| > \frac{\lambda n\sqrt{k}}{2}\right) \geq 1 - \frac{1}{\lambda^2}$$

Mas cada soma tem probabilidade 0 ou 2^{-k} de aparecer, já que as somas são distintas. Então

$$P\left(|X - \mu| > \frac{\lambda n\sqrt{k}}{2}\right) \leq 2^{-k}\lambda n\sqrt{k}$$

e portanto

$$2^{-k} n\sqrt{k} \leq 1 - \frac{1}{\lambda^2} \iff n \geq \frac{2^k}{\sqrt{k}} \frac{1 - \lambda^{-2}}{\lambda}.$$

Um pouco de cálculo nos leva ao valor ótimo $\lambda = \sqrt{3}$, e obtemos

$$n \geq \frac{2^{k+1}}{3\sqrt{k}} \iff \log_2 n \geq k + 1 - \frac{1}{2}\log_2 k \implies k \leq \log_2 n + \frac{1}{2}\log_2 \log_2 n + O(1).$$