TÉCNICA

Acaso e Certezas: A Versatilidade do Método Probabilístico

Carlos Augusto D. Ribeiro, Daniel Vitor C. Vieira e Joice M. Brito

Introdução

O Método Probabilístico trouxe um novo sopro de criatividade para a Matemática lá pelos anos 50, graças à visão inovadora dos matemáticos húngaros Paul Erdős e Alfréd Rényi. Eles, meio que cansados das longas e complexas demonstrações do jeito tradicional, especialmente em áreas como teoria dos números e combinatória, decidiram que era hora de algo diferente. E assim, mergulharam no mundo das probabilidades e estatísticas para dar vida a suas ideias.

Erdős e Rényi foram verdadeiros desbravadores, abraçando a aleatoriedade de sistemas complexos de uma maneira totalmente nova. Em vez de seguir o roteiro tradicional passo a passo, eles jogaram com distribuições de probabilidade e aplicaram teoremas poderosos, como o do Limite Central, para tirar conclusões elegantes mesmo quando tudo parecia incerto.

O coração do método é bastante direto: primeiro, modelar o problema de maneira probabilística, depois mostrar que a propriedade que estamos de olho tem uma chance real de acontecer e, por fim, usar desigualdades famosas, como as de Markov ou Chebyshev, para provar que essa propriedade realmente vem à tona conforme o sistema cresce.

Essa abordagem acabou sendo um verdadeiro achado, ajudando a desvendar problemas antes vistos como impossíveis em várias áreas, desde a teoria dos números até a bioinformática, passando pela física estatística. Por exemplo, Erdős e Rényi usaram essa técnica para descobrir grafos com características que muitos achavam que só existiam na imaginação. Rényi, por sua vez, aplicou esse método para solucionar um dilema sobre números primos que estava sem resposta há mais de meio século.

O sucesso do Método Probabilístico não só abriu portas para novos campos de estudo, como a combinatória probabilística e a teoria dos números analítica, mas também motivou uma nova geração de matemáticos a seguir explorando. Um exemplo é Endre Szemerédi, que levou as ideias ainda mais longe, resolvendo problemas complexos em teoria dos grafos e aritmética.

Apesar de ter sido um pouco controverso no início, hoje o Método Probabilístico é considerado fundamental na matemática contemporânea, continuando a desvendar padrões misteriosos e a estabelecer conexões surpreendentes por todo o universo matemático. Devido a sua versatilidade, hoje vemos o Método Probabilístico ser usado, de maneira direta ou indireta, em áreas como:

- **Teoria dos Números:** O método probabilístico tem sido muito empregado para demonstrar a existência de padrões em propriedades aparentemente aleatórias de números primos, como na estimativa da distribuição de primos feita por Rényi em 1958.
- **Combinatória:** Permite provar a existência de certas configurações combinatórias como emparelhamentos perfeitos, ciclos hamiltonianos, e resolução de identidades envolvendo coeficientes binomiais. Foi crucial para estabelecer novos resultados em teoria extremal de grafos.
- **Teoria dos Grafos:** Ideal para estudar propriedades de grafos aleatórios e probabilísticos. Uti-

lizado para provar bounds em parâmetros como independência, conectividade, coloração e empacotamento de arestas/vértices.

- **Otimização Combinatória:** Técnicas probabilísticas fornecem algoritmos randômicos e aproximados para problemas NP-difíceis de escalonamento, empacotamento, matching e coloring.

- **Processos Estocásticos:** O método probabilístico se aplica no estudo de cadeias de Markov, movimento Browniano, processos de ramificação e percolação.

- **Inferência Estatística:** Estimativas de parâmetros e testes de hipóteses frequentemente envolvem modelagem probabilística. Técnicas como bootstrap e Markov Chain Monte Carlo empregam raciocínio semelhante.

E é esse o objetivo desse artigo: nos lembrar que a Matemática não é só sobre encontrar respostas definitivas, mas também sobre explorar as possibilidades e usar a incerteza para demonstrar certezas. É uma lição sobre como, às vezes, aceitar que não sabemos tudo pode ser exatamente o que precisamos para descobrir algo novo, qualquer que seja a área.

O funcionamento do Método Probabilístico

Como mencionamos na introdução, a beleza do Método Probabilístico reside em sua simplicidade: se uma propriedade tem uma probabilidade não nula de ocorrer, então essa propriedade existe em algum caso concreto. Isso é uma maneira elegante de afirmar a existência de certas configurações sem a necessidade de construí-las passo a passo.

O raciocínio é direto: se a chance de um evento A acontecer é maior que zero, então A tem que se manifestar em algum momento dentro do nosso universo de possibilidades. Demonstrando que $P(A) > 0$, confirmamos a existência de A em alguma instância específica.

O Método Probabilístico, então, se desdobra nos passos a seguir:

- Modelar o problema de forma probabilística, designando distribuições de probabilidade aos componentes do problema.

- Escolher um evento A ligado à característica que queremos demonstrar.

- Calcular a probabilidade $P(A)$, geralmente procurando estabelecer um limite inferior.

- Provar que $P(A) > 0$, muitas vezes recorrendo a desigualdades, como a de Markov.

- Concluir que, devido a $P(A) > 0$, A precisa existir em alguma realização determinística.

Nos exemplos que traremos nas próximas seções, você vai ver essa lógica em ação, ilustrando a aplicabilidade e a eficácia do Método. O artigo se divide então em seis seções principais: Pré-requisitos de Probabilidade, Aplicações em Teoria dos Números, Combinatória, Teoria dos Grafos, Álgebra, e Geometria. Todos os problemas discutidos são acessíveis para estudantes envolvidos em olimpíadas de Matemática do ensino médio. Então, vamos explorar juntos essas ideias fascinantes!

Um pouco de Probabilidade

Um **espaço amostral** Ω é o conjunto de todos os resultados possíveis de um experimento aleatório. Por exemplo, ao lançar uma moeda, temos $\Omega = \{cara, coroa\}$. Este espaço pode ser **finito**, **infinito** ou **enumerável**, dependendo do número de resultados possíveis.

A noção de espaço amostral é crucial para definir a possibilidade de um evento. Um evento é dito possível se puder ocorrer dentro dos resultados do espaço amostral. Por exemplo, "obter cara" é possível ao lançar uma moeda, mas "obter dois" não é, já que não está contido no espaço amostral definido.

Para um espaço amostral finito Ω com n elementos, a **probabilidade** é uma função $P : \Omega \to [0,1]$ que atribui a cada resultado $\omega \in \Omega$ um número real $P(\omega)$, satisfazendo as seguintes condições:

1. $P(\omega) \geq 0$, para todo $\omega \in \Omega$.

2. $\sum_{\omega \in \Omega} P(\omega) = 1$.

Isso indica que as probabilidades são não-negativas e a soma das probabilidades de todos os resultados possíveis é igual a 1.

Em espaços amostrais infinitos, a probabilidade é associada a subconjuntos de Ω através de uma **medida probabilística** μ, que é uma função satisfazendo:

1. $\mu(\emptyset) = 0$.

2. Se $A \subseteq B$, então $\mu(A) \leq \mu(B)$ (monotonia).

3. Se $A_1, A_2, \ldots$ são conjuntos disjuntos, então $\mu(\bigcup A_i) = \sum \mu(A_i)$ (aditividade contável).

4. $\mu(\Omega) = 1$.

Portanto, $\mu(A)$ para um subconjunto $A \subseteq \Omega$ pode ser interpretado como a probabilidade $P(A)$ desse evento.

Dentro deste contexto, introduzimos conceitos como **probabilidade condicional** e **variáveis aleatórias**. A probabilidade condicional de um evento A dado outro evento B com $P(B) > 0$ é expressa como $P(A|B) = \frac{P(A \cap B)}{P(B)}$, representando a probabilidade de A ocorrer sob a condição de B.

Uma **variável aleatória** é uma função que associa um valor numérico a cada resultado de um experimento aleatório, mapeando os resultados de Ω para números reais. Variáveis aleatórias podem ser **discretas** ou **contínuas**, dependendo do tipo de Ω.

A **função de distribuição** ou função de distribuição acumulada (FDA) de uma variável aleatória X, $F_X(x) = P(X \leq x)$, descreve a probabilidade de X assumir um valor menor ou igual a x. Esta função é fundamental para entender a distribuição de probabilidades de variáveis aleatórias, aplicável em diversas distribuições como a Uniforme, Normal, Exponencial, entre outras.

O **valor esperado** $\mathbb{E}[X]$ representa a média ou o "valor médio" de uma variável aleatória X. Para variáveis aleatórias discretas, ele é calculado como:

$$\mathbb{E}[X] = \sum_x xP(X = x).$$

O valor esperado pondera cada resultado possível de X pelo seu peso probabilístico. Por exemplo, o valor esperado ao lançar um dado é 3.5, calculado como a média ponderada de todos os resultados possíveis.

O valor esperado permite resumir o comportamento de uma variável aleatória em um único número, apresentando propriedades importantes como:

1. **Linearidade:** $\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y]$

2. **Multiplicação por constante:** $\mathbb{E}[cX] = c\mathbb{E}[X]$ para qualquer constante c.

3. **Propriedade de não-negatividade:** Se $\mathbb{E}[X] \geq a$, então $P(X \geq a) > 0$.

A **variância**, definida como $\text{Var}[X] = \mathbb{E}[(X - \mathbb{E}[X])^2]$, mede a dispersão dos valores de X em torno de $\mathbb{E}[X]$. Uma alta variância indica que os valores de X estão espalhados longe da média, enquanto uma baixa variância mostra que estão concentrados próximos à média.

Propriedades da variância incluem:

1. $\text{Var}[cX] = c^2\text{Var}[X]$ para qualquer constante c.

2. $\text{Var}[X + Y] = \text{Var}[X] + \text{Var}[Y]$ se X e Y são independentes.

3. $\text{Var}[X] \geq 0$, com igualdade somente se X é constante quase certamente.

A **covariância** $\text{Cov}[X, Y]$ mede a dependência linear entre X e Y, com as propriedades:

1. $\text{Cov}[X, Y] = \text{Cov}[Y, X]$.

2. $\text{Cov}[X, Y] = 0$ se X e Y são independentes.

3. $\text{Cov}[X, X] = \text{Var}[X]$.

Finalmente, as desigualdades de Markov e Chebyshev são ferramentas essenciais:

1. **Desigualdade de Markov:** Para $X \geq 0$, $P(X \geq M) \leq \frac{E(X)}{M}$ para todo $M > 0$.

2. **Desigualdade de Chebyshev:** Para X com média μ e variância σ^2, $P(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2}$ para qualquer $k > 0$.

Agora vamos partir para as aplicações, começando pela Teoria dos Números, e sendo o mais objetivo possível a fim de não tornar a leitura desse artigo massante.

Método Probabilístico e Teoria dos Números

Consideremos $\nu(n)$ como a quantidade de divisores primos distintos p que são divisores de n. Um resultado notável afirma que a maioria esmagadora dos números n possui um número de fatores primos muito próximo a $\ln\ln n$. Esse resultado, originalmente complexo, foi inicialmente demonstrado por Hardy e Ramanujan em 1920. No entanto, uma prova notavelmente simples foi apresentada por Turán em 1934, uma prova que desempenhou um papel crucial no avanço dos métodos probabilísticos na teoria dos números.

Teorema. *Seja $\omega(n) \to \infty$ arbitrariamente devagar. Então o número de x em $1, \ldots, n$ tal que*

$$|\nu(x) - \ln\ln n| > \omega(n)\sqrt{\ln\ln n}$$

é $o(n)$.

Demonstração. Seja x um inteiro escolhido uniformemente ao acaso em $1,\ldots,n$. Para cada primo p, definimos a variável aleatória:

$$X_p = \begin{cases} 1, & \text{se } p \mid x, \\ 0, & \text{caso contrário.} \end{cases}$$

Seja $M = n^{1/10}$ e $X = \sum X_p$, a soma sobre todos os primos $p \le M$. Como nenhum $x \le n$ pode ter mais de 10 divisores primos maiores que M, temos:

$$\nu(x) - 10 \le X \le \nu(x).$$

Logo, grandes desvios em X implicam em desvios assintoticamente similares em $\nu(x)$. Agora, por linearidade do valor esperado:

$$\mathbb{E}[X] = \sum_{p \le M} \mathbb{E}[X_p] = \sum_{p \le M} \frac{1}{p} + O\left(\frac{1}{n}\right) = \ln\ln n + O(1),$$

onde usamos a fórmula assintótica bem conhecida para soma de inversos de primos. Similarmente, pode-se mostrar que:

$$\mathrm{Var}[X] = \ln\ln n + O(1).$$

De fato, para isso, basta usar que

$$\mathrm{Var}[X] = \sum_{p \le M} \mathrm{Var}[X_p] + \sum_{p \ne q} \mathrm{Cov}[X_p, X_q].$$

Como $\mathrm{Var}[X_p] = (1/p)(1-1/p) + O(1/n)$,

$$\sum_{p \le M} \mathrm{Var}[X_p] = \left(\sum_{p \le M} \frac{1}{p}\right) + O(1) = \ln\ln n + O(1).$$

Com p, q primos distintos, $X_p X_q = 1$ se e somente se $p|x$ e $q|x$, o que ocorre se e somente se $pq|x$. Portanto,

$$\begin{aligned} \mathrm{Cov}[X_p, X_q] &= E[X_p X_q] - E[X_p]E[X_q] \\ &= \frac{[n/pq]}{n} - \frac{[n/p]}{n}\frac{[n/q]}{n} \\ &\le \frac{1}{pq} - \left(\frac{1}{p} - \frac{1}{n}\right)\left(\frac{1}{q} - \frac{1}{n}\right) \\ &\le \frac{1}{n}\left(\frac{1}{p} + \frac{1}{q}\right). \end{aligned}$$

Assim,

$$\sum_{p \ne q} \mathrm{Cov}[X_p, X_q] \le \frac{1}{n} \sum_{p \ne q} \left(\frac{1}{p} + \frac{1}{q}\right) \le \frac{2M}{n} \sum \frac{1}{p}.$$

Daí,

$$\sum_{p \ne q} \mathrm{Cov}[X_p, X_q] \le O(n^{-9/10} \ln\ln n) = o(1).$$

E da mesma forma,

$$\sum_{p \ne q} \mathrm{Cov}[X_p, X_q] \ge -o(1).$$

Por fim, a desigualdade de Chebyshev então implica que:

$$P\left[|X - \ln\ln n| > \lambda\sqrt{\ln\ln n}\right] < \frac{1}{\lambda^2} + O(1).$$

Como $|X - \nu| \le 10$, o mesmo vale para $\nu(x)$, completando a prova. □

Na Teoria dos Números, os conjuntos livres de somas são particularmente intrigantes. Eles são definidos de tal maneira que nenhum de seus elementos pode ser obtido pela soma de outros elementos distintos presentes no conjunto. A exploração da existência desses subconjuntos dentro de conjuntos maiores nos permite desvendar aspectos fundamentais da composição aditiva dos números. O teorema apresentado a seguir mergulha nessa questão, destacando a relevância desses conjuntos na compreensão das propriedades numéricas:

Teorema. *Seja $A \subseteq \mathbb{N}$ um conjunto com n elementos. Então existe $B \subseteq A$ livre de somas com mais que $\frac{n}{3}$ elementos.*

Demonstração. Vamos usar aritmética modular para introduzir permutações. Seja $\overline{a}$ o maior elemento de A e seja $p > 2\overline{a}$ um número primo. Dessa forma, para $a, b, c \in A$, temos:

$$a + b = c \Leftrightarrow a + b \equiv c \pmod{p},$$

o que nos permite focar apenas na aritmética modular $\bmod p$, que é mais simples. Suponha, para simplificar, que $p = 3k+2$. Considere o conjunto livre de somas $S = \{k+1, k+2, \ldots, 2k+1\}$ com $k+1$ elementos. Vamos permutar esse conjunto multiplicando seus elementos por algum $x \in \mathbb{Z}/p\mathbb{Z}^*$ escolhido aleatoriamente, pois:

$$xa + xb \equiv xc \pmod{p} \Leftrightarrow a + b \equiv c \pmod{p}.$$

Considere então a variável aleatória:

$$X(x) = |xS \cap A|,$$

onde $xS = \{x(k+1), x(k+2), \ldots, x(2k+1)\}$. Podemos escrever $X = \sum_{a \in A} X_a$, onde:

$$X_a = \begin{cases} 1, & \text{se } a \in xS, \\ 0, & \text{caso contrário.} \end{cases}$$

Note que $\mathbb{E}[X_a] = \mathbb{P}[a \in xS] = \frac{k+1}{3k+1} > \frac{1}{3}$, pois $a \in xS \Leftrightarrow x^{-1}a \in S$. Logo, $\mathbb{E}[X] > \frac{n}{3}$, e existe x tal que $|xS \cap A| > \frac{n}{3}$. Tomando $B = xS \cap A$, obtemos o conjunto livre de somas desejado. □

Método Probabilístico e Combinatória

Considere uma família F de subconjuntos A_i, todos de tamanho $d \geq 2$, de um conjunto finito X. Dizemos que F é *bicolorizável* se existe uma coloração de X com duas cores de forma que ambas as cores aparecem em cada conjunto A_i. É imediato que nem toda família pode ser colorida dessa maneira. Como um exemplo, tome todos os subconjuntos de tamanho d de um conjunto X com $(2d-1)$ elementos. Então qualquer que seja a forma com que bicolorirmos X, deverão existir d elementos que são coloridos da mesma forma. Por outro lado, fica igualmente claro que cada subfamília de uma família bicolorizável de conjuntos com d elementos é bicolorizável. Daí, estamos interessados no menor número $m = m(d)$ para qual existe uma família com m conjuntos que não seja bicolorizável. Expressando de maneira diferente, $m(d)$ é o menor número que garante que cada família com menos de $m(d)$ conjuntos é bicolorizável.

Teorema. *Cada família de no máximo 2^{d-1} conjuntos com d elementos é bicolorizável, isto é, $m(d) > 2^{d-1}$.*

Demonstração. Suponha que F seja uma família de conjuntos de d elementos com no máximo 2^{d-1} conjuntos. Colorize X aleatoriamente com duas cores, sendo todas as colorações igualmente prováveis. Para cada conjunto A pertencente a F, consideremos o evento E_A, que ocorre quando todos os elementos de A são coloridos da mesma forma. Dado que existem exatamente duas possíveis colorações, podemos expressar essa situação de outra forma:

$$P(E_A) = \left(\frac{1}{2}\right)^{d-1}.$$

Daí, com $m = |F| \leq 2^{d-1}$. Note também que os eventos E_A não são adjuntos, isto é,

$$P\left(\bigcup_{A\in F} E_A\right) < \sum_{A\in F} P(E_A) = m\left(\frac{1}{2}\right)^{d-1} \leq 1.$$

Portanto, podemos concluir que existe alguma bicoloração de X sem um conjunto unicolorido e isso é justamente o que procurávamos. □

Para o resultado que segue, uma família F de subconjuntos de $\{1,2...,n\}$ é uma *anticadeia* se nenhum conjunto em F é subconjunto de outro conjunto em F.

Teorema. *(Sperner) Mostre que o tamanho da maior anticadeia de um conjunto com n elementos é*

$$\binom{n}{\lfloor n/2\rfloor}.$$

Demonstração. Inicialmente, vamos provar que se F é uma anticadeia, então

$$\sum_{A\in F} \frac{1}{\binom{n}{|A|}} \leq 1.$$

De fato, seja σ uma permutação aleatoriamente e uniformemente escolhida de $\{1,...,n\}$ e defina o conjunto

$$C_\sigma = \left\{\left\{\sigma(j) : 1 \leq j \leq i\right\} : 0 \leq i \leq n\right\}.$$

É imediato que $\varnothing \in C_\sigma$ e $\{1,...,n\} \in C_\sigma$. Defina uma variável aleatória

$$X = |F \cap C_\sigma|.$$

Decompondo X, obtém-se

$$X = \sum_{A\in F} X_A,$$

onde X_A é a variável aleatória indicadora para $A \in C_\sigma$. Então

$$\mathbb{E}[X_A] = P[A \in C_\sigma] = \frac{1}{\binom{n}{|A|}},$$

já que C_σ contém precisamente um conjunto de tamanho $|A|$, que é distribuído uniformemente entre os conjuntos com $|A|$ elementos. Pela linearidade da expectativa,

$$\mathbb{E}[X] = \sum_{A\in F} \frac{1}{\binom{n}{|A|}}.$$

Para qualquer σ, C_σ forma uma cadeia – pois cada par de conjuntos é comparável. Uma vez que F é uma anticadeia, devemos ter $X = |F \cap C_\sigma| \leq 1$. Assim $\mathbb{E}[X] \leq 1$, o que conclui o que queríamos provar.

Para finalizar, basta notar que a função $\binom{n}{x}$ é maximizada em $x = \lfloor n/2\rfloor$. Logo, usando o fato provado anteriormente, obtemos

$$1 \geq \sum_{A\in F} \frac{1}{\binom{n}{|A|}} \geq \frac{|F|}{\binom{n}{\lfloor n/2\rfloor}}.$$ □

Método Probabilístico e Grafos

Um torneio em um conjunto V de n jogadores é uma orientação $T = (V, E)$ das arestas do grafo completo no conjunto de vértices V. Assim, para cada par distinto de elementos x e y em V, ou (x, y) ou (y, x) está em E, mas não ambos. O nome "torneio" é natural, já que podemos pensar em V como um conjunto de jogadores onde cada par joga uma única partida, e (x, y) está no torneio se e somente se x derrota y. Dizemos que T tem a propriedade S_k se para qualquer conjunto de k jogadores em V, existe um jogador que derrota todos eles. Em outras palavras, dado qualquer grupo de k jogadores, há um que vence cada um deles nas respectivas partidas do torneio. Assim, podemos enunciar o seguinte.

Teorema. *Se* $\binom{n}{k}(1-2^{-k})^{n-k} < 1$, *então existe um torneio com n vértices que possui a propriedade* S_k.

Demonstração. Considere um torneio aleatório no conjunto $V = \{1,2,3,...,n\}$. Para cada subconjunto fixo K de tamanho k de V, seja A_K o evento em que não existe nenhum vértice de K que vença todos os demais membros do mesmo. Claramente, $P(A_k) = (1-2^{-k})^{n-k}$. Isso acontece porque, para cada vértice fixo $v \in V-K$, a probabilidade de que v não vença todos os membros de K é $1-2^{-k}$, e todos esses $n-k$ eventos, correspondentes às várias escolhas possíveis de v, são independentes. Logo, segue que

$$P\left(\bigvee_{K\subset V} A_K\right) \leq \sum_{K\subset V} P(A_K) = \binom{n}{k}(1-2^{-k})^{n-k} < 1.$$

Portanto, com probabilidade positiva, nenhum evento de A_K ocorre, isto é, existe um torneio com n vértices com a propriedade S_k. □

Façamos agora um problema tipicamente olímpico:

Teorema. *(SJSU M179 Midterm) Dados n pontos vermelhos e n pontos azuis, suponha que conectemos pelo menos* n^2-n+1 *pares de cores opostas. Prove que podemos selecionar n segmentos, sem que nenhum par compartilhe uma extremidade.*

Demonstração. Como há um total de n^2 arestas possíveis, ter pelo menos n^2-n+1 arestas significa que praticamente todas as arestas estão presentes. Vamos construir um emparelhamento aleatório entre os dois conjuntos de n vértices, independentemente da existência real de arestas entre eles. Definimos a pontuação desse emparelhamento como o número de pares que estão conectados por uma aresta. Queremos mostrar que existe algum emparelhamento com pontuação n, que será o emparelhamento perfeito desejado.

Sejam $v_1,\ldots,v_n$ os n vértices à esquerda. Para cada um, considere a variável aleatória:

$$X_i = \begin{cases} 1, & \text{se o par com } v_i \text{ tiver uma aresta,} \\ 0, & \text{caso contrário.} \end{cases}$$

A pontuação da configuração é dada por $X = X_1+\cdots+X_n$. Temos que $\mathbb{E}[X_i] = \frac{\text{grau}(v_i)}{n}$, logo

$$\begin{aligned}\mathbb{E}[X] &= \mathbb{E}[X_1]+\cdots+\mathbb{E}[X_n] \\ &= \frac{\text{grau}(v_1)}{n}+\cdots+\frac{\text{grau}(v_n)}{n} \\ &= \frac{n^2-n+1}{n} = n-1+\frac{1}{n}.\end{aligned}$$

Como X assume apenas valores inteiros, existe alguma configuração com $X = n$. Portanto, concluímos a demonstração. □

Método Probabilístico e Álgebra

Os próximos dois resultados são conhecidos como problemas de balanceamento de vetores e mostram que podemos usar o método probabilístico também na Álgebra.

Teorema. *Sejam* $v_1,...,v_n \in \mathbb{R}^n$, *tal que* $|v_i| = 1$ *para todo* $i \in \{1,2,\ldots,n\}$. *Então existem* $\epsilon_1,...,\epsilon_n = \pm 1$ *de modo que:*

$$|\epsilon_1 v_1 + ... + \epsilon_n v_n| \leq \sqrt{n},$$

e também existem $\epsilon_1,...,\epsilon_n = \pm 1$ *de modo que*

$$|\epsilon_1 v_1 + ... + \epsilon_n v_n| \geq \sqrt{n}.$$

Demonstração. Sejam $\epsilon_1,...,\epsilon_n \in \mathbb{R}^n$ selecionados de forma uniforme e independente a partir de $\{-1,+1\}$. Defina:

$$X = |\epsilon_1 v_1 + ... + \epsilon_n v_n|^2.$$

Então

$$X = \sum_{i=1}^{n}\sum_{j=1}^{n} \epsilon_i\epsilon_j v_i \cdot v_j.$$

Por isso,

$$\mathbb{E}[X] = \sum_{i=1}^{n}\sum_{j=1}^{n} v_i \cdot v_j \mathbb{E}\left[\epsilon_i\epsilon_j\right].$$

Quando $i \neq j$ temos $\mathbb{E}\left[\epsilon_i\epsilon_j\right] = \mathbb{E}[\epsilon_i]\mathbb{E}\left[\epsilon_j\right] = 0$, e quando $i = j$ temos $\epsilon_i^2 = 1$ e então $\mathbb{E}\left[\epsilon_i^2\right] = 1$. Assim,

$$\mathbb{E}[X] = \sum_{i=1}^{n} v_i \cdot v_i = n.$$

Portanto, existem valores específicos $\epsilon_1,...,\epsilon_n = \pm 1$ com $X \geq n$ e com $X \leq n$. Tomando as raízes quadradas, obtemos o teorema. □

Nessa mesma ideia, temos o:

Teorema. *Seja* $v_1,...,v_n \in \mathbb{R}^n$, *com todos os* $|v_i| \leq 1$. *Sejam* $p_i,...,p_n \in [0,1]$ *arbitrários e defina* $w = p_1v_1+...+p_nv_n$. *Então existem* $\epsilon_1,...,\epsilon_n \in \{0,1\}$ *de forma que, definindo* $v = a_1v_1+...+a_nv_n$,

$$|w-v| \leq \frac{\sqrt{n}}{2}.$$

Demonstração. Escolha ϵ_i de forma independente com

$$P[\epsilon_i = 1] = p_i, \qquad P[\epsilon_i = 0] = 1-p_i.$$

A escolha aleatória de ϵ_i gera um v aleatório e uma variável aleatória

$$X = |w-v|^2.$$

Fazendo uma expansão

$$X = \left| \sum_{i=1}^{n} (p_i - \epsilon_i) v_i \right|^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} v_i \cdot v_j (p_i - \epsilon_i)(p_j - \epsilon_j),$$

dessa forma

$$\mathbb{E}[X] = \sum_{i=1}^{n} \sum_{j=1}^{n} v_i \cdot v_j \, \mathbb{E}\left[(p_i - \epsilon_i)(p_j - \epsilon_j)\right].$$

Para $i \neq j$,

$$\mathbb{E}\left[(p_i - \epsilon_i)(p_j - \epsilon_j)\right] = \mathbb{E}\left[p_i - \epsilon_i\right] \, \mathbb{E}\left[p_j - \epsilon_j\right] = 0.$$

Para $i = j$,

$$\mathbb{E}\left[(p_i - \epsilon_i)^2\right] = p_i(p_i - 1)^2 + (1 - p_i)p_i^2 = p_i(1 - p_i) \leq \frac{1}{4},$$

$\mathbb{E}\left[(p_i - \epsilon_i)^2\right] = \mathrm{Var}[\epsilon_i]$. Assim,

$$\mathbb{E}[X] = \sum_{i=1}^{n} p_i(1 - p_i)|v_i|^2 \leq \frac{1}{4} \sum_{i=1}^{n} |v_i|^2 \leq \frac{n}{4},$$

e a prova conclui-se como a do teorema anterior. □

Método Probabilístico e Geometria

O exemplo a seguir é uma bela aplicação do método probabilístico na Geometria Plana.

Teorema. *(IMO 1989) Sejam n e k inteiros positivos e seja S um conjunto de n pontos no plano tais que:*

(i) Não existem três pontos de S que sejam colineares, e

(ii) Para qualquer ponto P de S existem pelo menos k pontos de S equidistantes de P.

Prove que:

$$k \leq \frac{1}{2} + \sqrt{2n}.$$

Demonstração. Primeiro, note que a desigualdade pedida é equivalente a:

$$n \geq \binom{k}{2} + 1.$$

Agora, para cada ponto P em S, construímos um círculo centrado em P que contém pelo menos k pontos de S.

Seja d_P o número de círculos que contêm o ponto P. Seja também f_O o número de pontos contidos no círculo definido com centro em O, para cada ponto $O \in S$. Por construção, temos que $f_O \geq k$ para todo $O \in S$.

Como a função binomial $\binom{n}{2}$ é crescente para $n \geq 1$ inteiro, segue que $\binom{f_O}{2} \geq \binom{k}{2}$ para todo $O \in S$. Logo,

$$\mathbb{E}\left[\binom{f}{2}\right] \geq \binom{k}{2},$$

onde o valor esperado é sobre a escolha uniforme do ponto $O \in S$.

Por outro lado, observe que qualquer par de pontos compartilha no máximo 2 círculos, pois caso contrário teríamos 3 círculos com centros em suas bissetrizes perpendiculares, o que violaria as condições do problema. Logo,

$$\sum_{O \in S} \binom{f_O}{2} \leq 2\binom{n}{2},$$

pois o lado esquerdo conta pares de pontos compartilhando algum círculo, enquanto o lado direito limita esse valor por todos os pares possíveis.

Portanto,

$$\binom{k}{2} \leq \mathbb{E}\left[\binom{f}{2}\right] \leq \frac{2}{n}\binom{n}{2} = n - 1,$$

que completa a prova. □

Bibliografia

[1] M. Aigner and G. M. Ziegler. *Proofs from the book*. Springer, Berlin, 1998.

[2] N. Alon and J. H. Spencer. *The probabilistic method*. Wiley, New York, 3 edition, 2000.

[3] B. Bollobás. *Random graphs*. Cambridge University Press, Cambridge, 2 edition, 2001.

[4] Evan Chen. Expected uses of probability. 18 p., 2014.

[5] R. Diestel. *Graph theory*. Springer, Berlin, 5 edition, 2017.

[6] P. Erdős and A. Rényi. On the evolution of random graphs. *Publicationes Mathematicae*, 1950.

[7] P. Erdős and A. Rényi. On random graphs. *Publicationes Mathematicae*, 6:290–297, 1959.

[8] W. Feller. *An introduction to probability theory and its applications*. Wiley, New York, 3 edition, 1968.

[9] F. Harary and E. M. Palmer. *Graphical enumeration*. Academic Press, New York, 1973.

[10] Kiran Kedlaya. Graph theory: Definitions and results. 4 p., 1999.

[11] H. G. Landau and H. J. Landau. *Prime numbers and the Riemann hypothesis*. Cambridge University Press, Cambridge, 2015.

[12] Thiago Landim. Aplicações inesperadas do valor esperado. 10 p., 2020.

[13] Po-Shen Loh. Probabilistic methods in combinatorics. 7 p., 2009.

[14] A. Rényi. On the distribution of primes. *Publicationes Mathematicae*, 1958.

[15] J. Spencer. *Ten lectures on the probabilistic method*. SIAM, Philadelphia, 1994.

Carlos Augusto D. Ribeiro é professor da Universidade Federal do Delta do Parnaíba (UFDPar) desde 2010 e ex-olímpico com premiações na OBM, OCM, Rioplatense, etc. Consciente do impacto positivo que a Olimpíada de Matemática teve em sua vida, hoje contribui com a OBM na promoção de suas olimpíadas, com a ONG Cactus produzindo materiais de treinamento que impactam a vida de dezenas de milhares de alunos da escola pública, bem como com o Projeto CQD com quem tem a alegria de trabalhar ao lado de amigos da época de olimpíada. Viciado em Star Wars, nerd de carteirinha e apaixonado por sua esposa Keivy Lany, se esforça em manter o bom humor quando os seus pets Ahsoka, Yoda, Bombom e Sushi resolvem aprontar.

Maria Joice Machado Brito é natural de Cocal dos Alves, uma cidade pequena no interior do Piauí. Concluiu a graduação em Licenciatura em Matemática pela UFDPAR. Seu interesse pela matemática surgiu durante o ensino médio, graças à participação na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), onde foi medalhista. Atualmente, trabalha em sua cidade natal e busca incentivar os alunos a gostarem de Matemática.

Gosta muito de crianças, de jogos de raciocínio e de competição. Por gostar de crianças, ela já até pensou em fazer pedagogia, mas o que realmente a realiza é resolver questões desafiadoras que envolvam probabilidade. Por isso, pretende fazer um mestrado na área.

Daniel Vitor C. Vieira nasceu em Brasília e está radiante por ter se formado em licenciatura em Matemática pela UFDPar. Atualmente, ele compartilha seu conhecimento ensinando matemática sempre que possível em seu estado que mora, o Maranhão. Daniel tem uma queda pelo estudo da probabilidade e seus campos abstratos, que incluem geometria, teoria dos números e teoria dos grafos. Além disso, é totalmente apaixonado por sua namorada, Liandra, e se esforça ao máximo para fazer com que ela também goste de matemática.