O METODO PROBABILÍSTICO E ALGUMAS APLICAÇÕES

Aluno: Lucas Mendes Marques Gonçalves
Supervisor: Yoshiharu Kohayakawa
Trabalho de conclusão de curso

Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo

1. O método probabilístico

O método probabilístico é um meio para provar teoremas, que tem diversas aplicações em combinatória, álgebra, teoria dos números e computação.
Normalmente, se utiliza o método para provar a existência de determinadas entidades matemáticas, provando que tais entidades ocorrem, com probabilidade positiva, num dado sorteio.
Usualmente, tais provas não fornecem algoritmos eficientes para a construção dessa estrutura (i.e., são provas não construtivas)

2. Dois exemplos

COMO se pode notar, definir o método probabilístico não é muito fácil. Porém, felizmente, há várias provas curtas e bonitas que ilustram bem a idéia por trás do método. Daremos dois exemplos aqui, esperando que serão o bastante para mostrar o poder e a elegância dos argumentos probabilísticos.

2.1 Número de independência

Tomemos um grafo G. Um conjunto de vértices é chamado *independente* se, para todo par de vértices $\{x, y\}$, x e y não são adjacentes. $\alpha(G)$, o chamado *número de independência* de G, é o tamanho do maior conjunto independente de G. Chamamos o grau de um vértice v de δ_v

Teorema 2.1 [1] *Para todo grafo G, temos*

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{1+\delta_v}$$

Prova. Vamos escolher um conjunto independente aleatoriamente em G.

Para isso, tomaremos uma ordenação $<_j$ aleatória dos vértices. Tomaremos o conjunto independente

$$I = \{x \in V(G) / \{x, y\} \in E(G) \rightarrow x <_j y\}$$

Sendo X o tamanho de I, e X_v a variável indicadora do evento $v \in I$, temos que $X = \sum_{v \in G} X_i$. Assim, pela linearidade da esperança, temos que

$$E(X) = \sum_{v \in G} E(X_v) = \sum_{v \in G} P(X_v = 1)$$

Mas, $P(X_v = 1) = \frac{1}{1+\delta_v}$. Assim,

$$E(X) = \sum_{v \in G} \frac{1}{1+\delta_v}$$

Ora, se, em algum espaço amostral, a média do tamanho de I é $\sum_{v \in G} \frac{1}{1+\delta_v}$, então existe I tal que

$$|I| \geq \sum_{v \in G} \frac{1}{1+\delta_v}$$

□

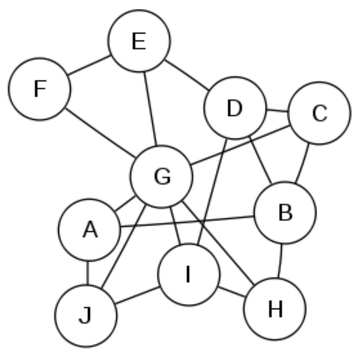

Figura 1: *Tomando a ordenação $a, b, h, j, c, i, f, g, e, d$ temos I=$\{a, f\}$*

2.2 Códigos livres de prefixo

Tomemos, agora, um conjunto F de strings binárias, todas de comprimento finito. Diremos que esse conjunto é *livre de prefixo* se nenhuma string em F é prefixo de outra string em F. Denotemos N_i o número de strings de comprimento i em um tal conjunto.

Teorema 2.2 *Se F é livre de prefixo,*

$$\sum_i \frac{N_i}{2^i} \leq 1$$

Prova. Vamos definir um processo aleatório: Sorteamos uma string aleatória, bit a bit. Se nossa string parcial é alguma string de F, paramos.

A probabilidade de nosso sorteio parar na string $a \in F$, se $|a| = i$ é

$$p_a = \frac{1}{2^i}$$

Note que se F não fosse livre de prefixo, alguns p_a seriam zero. Note também que os eventos são disjuntos, pela definição do processo

A probabilidade p de nosso processo aleatório parar é

$$p = \sum_{a \in F} p_a = \sum_i \frac{N_i}{2^i}$$

Mas p é uma probabilidade. Assim, $p \leq 1$. Por isso,

$$\sum_i \frac{N_i}{2^i} \leq 1$$

□

3. Grafos aleatórios

APLICA-SE o método probabilístico intensamente no estudo de grafos aleatórios.
Vamos explicar aqui uma variação do primeiro problema da área: a determinação de quando um grafo aleatório contem um determinado subgrafo pequeno.
Primeiro, teremos que definir algumas coisas: Nosso modelo de grafo aleatório é $G(n, p)$. Isso quer dizer que estamos tomando grafos de n vértices, e incluindo cada aresta com probabilidade p.
Nosso problema é determinar quando $G(n, p)$ contém um determinado subgrafo H (fixo). Mais precisamente, queremos determinar um comportamento assintótico, ou seja, saber se H surge em G quando n vai a infinito.
Esse problema é trivial se p é fixo (G sempre conterá H quando $n \rightarrow \infty$ se $p > 0$ é fixo). Assim, nos preocuparemos com p que seja função decrescente de n

Definição 3.1 *A densidade de um grafo:* $\rho(H) = e(H)/v(H)$

Definição 3.2 *Um grafo H é dito balanceado se, $\rho(H) \geq \rho(K)$ para todo $K \subseteq H$, e é dito estritamente balanceado se $\rho(H) > \rho(K)$ para todo $K \subset H$, com $K \neq H$*

Definição 3.3 *Dizemos que* $p(n) \gg f(n)$ *se* $\lim_{n \rightarrow \infty} \frac{f(n)}{p(n)} = 0$

Teorema 3.1 [1] *Se H é um grafo balanceado, a função $f(n) = (1/n)^{1/\rho(H)}$ é uma função limiar para a propriedade de G conter H, ou seja:*

$$\begin{cases} \lim_{n \rightarrow \infty} P[H \subset G(n,p)] = 1 & \text{se } p(n) \gg f(n), \\ \lim_{n \rightarrow \infty} P[H \subset G(n,p)] = 0 & \text{se } p(n) \ll f(n). \end{cases}$$

Esse teorema foi provado, com essa restrição de balanceamento, na década de 60. Demoraria até a década de 80 para se provar a seguinte extensão do teorema para grafos quaisquer

Definição 3.4 $m(H) = max_{F \subset H}\ \rho(F)$

Teorema 3.2 [2] *Se H é um grafo qualquer, a função $f(n) = (1/n)^{1/m(H)}$ é uma função limiar para a propriedade de G conter H.*

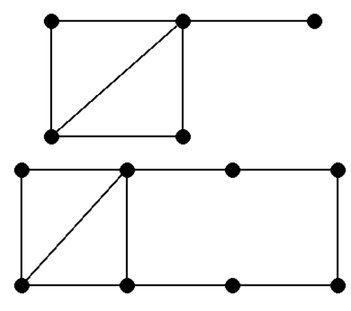

Figura 2: *Um grafo desbalanceado e uma das suas extensões balanceadas*

Há várias maneiras de provar a generalização. Uma das mais curiosas, que estudamos em detalhe, toma H desbalanceado e constrói um F balanceado que contem H, com $m(H) = m(F)$. Quando $G(n, p)$ contém F, obviamente conterá H, e desse fato conseguimos deduzir a afirmação difícil de provar do teorema. (ver [4])

4. Códigos resistentes a erro

SUPONHAMOS que desejamos enviar uma mensagem binária, mas por um canal que não é confiavel (mais precisamente, que inverte um dado bit com probabilidade p).
Certamente podemos aumentar a confiabilidade desse canal, enviando nossas mensagens com mais bits. Podemos, por exemplo, enviar $n \geq 3$ vezes cada bit, e, na decodificação, pegar o valor mais frequente. Conseguimos assim uma probabilidade arbitrariamente baixa de erro, mas nossa velocidade fica sendo $1/n$ da de um canal sem erro.
Podemos, porém, fazer muito melhor do que isso: Podemos reduzir a taxa de transmissão por uma constante, e mesmo assim obter uma probabilidade tão próxima de zero quanto queiramos.

Definição 4.1 *Uma codificação é uma função $f : \{0,1\}^m \rightarrow \{0,1\}^n$ e uma $g : \{0,1\}^n \rightarrow \{0,1\}^m$. Nosso intuito é aplicar f antes do envio e g depois do recebimento. A taxa de transmissão é definida como m/n. Tomando $E = (e_1, \ldots e_n)$ uma string aleatória, com $P(e_1 = 1) = p$ e $P(e_1 = 0) = 1 - p$, definimos a probabilidade de acerto da função como $P_r[g(f(x) + E)] = x$ (usando soma módulo 2, x uniformemente distribuido nas strings de tamanho m)*

Definição 4.2 *A função entropia,*

$$H(p) = -(p \cdot \log_2 p) - (1-p)[\log_2(1-p)]$$

Teorema 4.1 *(de Shannon) Tome $0 < p < \frac{1}{2}$. Para todo $\epsilon > 0$, existe uma codificação tal que a taxa de transmissão é maior que $1 - H(p) - \epsilon$ e a probabilidade de transmissão incorreta é menor que ϵ*

Cumpre enfatizar, porém, que o teorema não nos dá tal codificação, apenas afirma a sua existência (como é usual com teoremas provados pelo método probabilístico). Para prova, ver [1].

5. Conclusão

O intuito desse trabalho foi ter contato com diversas áreas da combinatória e teoria da computação. Para isso, estudamos uma técnica de prova de teoremas, o chamado método probabilístico, e diversos teoremas nos quais se pode utilizar essa técnica. Aqui expomos apenas alguns. Entre os teoremas que não pudemos colocar aqui, vale destacar o estudo de alguns problemas em geometria, pois eles tem aplicações computacionais mais diretas. Também vimos vários outros teoremas interessantes de teoria dos grafos.
Podemos dizer que o intuito foi cumprido. De fato, o estudo do método probabilístico foi um bom meio para conhecer um pouco de diversas áreas de estudo em computação.

Referências

[1] N. Alon and J. Spencer, *The Probabilistic Method*, Wiley-Interscience, 2008.

[2] Janson S., Luczak T., and Rucinski A, *Random graphs*, Wiley, 2000.

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

[4] E. Györi, B. Rothschild, and A. Rucinski, *Every graph is contained in a sparsest possible balanced graph*, Math. Proc. Camb. Phil. Soc. **98** (1985).