O método probabilístico e algumas aplicações

Lucas Mendes Marques Gonçalves

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

Trabalho de conclusão de curso

Outline

1. O método
   - Definição
   - Um exemplo

2. Dois Problemas
   - Transmissão de dados
   - Grafos aleatórios

Definindo o Método

- É uma maneira de provar teoremas.
- Utilizamos um espaço de probabilidade para provar um teorema de existência
- Confuso ?

Definindo o Método

- É uma maneira de provar teoremas.
- Utilizamos um espaço de probabilidade para provar um teorema de existência
- Confuso ?

No one can be told what the method is ...

- O teorema: Todo grafo contém um subgrafo bipartido com pelo menos $\frac{E(G)}{2}$ arestas
- O espaço de probabilidade.
- Qual a chance de uma determinada aresta sobreviver ?
- Qual a esperança do número de arestas ?
- Como a esperança mostra a existência ?

No one can be told what the method is ...

- O teorema: Todo grafo contém um subgrafo bipartido com pelo menos $\frac{E(G)}{2}$ arestas
- O espaço de probabilidade.
- Qual a chance de uma determinada aresta sobreviver ?
- Qual a esperança do número de arestas ?
- Como a esperança mostra a existência ?

No one can be told what the method is ...

- O teorema: Todo grafo contém um subgrafo bipartido com pelo menos $\frac{E(G)}{2}$ arestas
- O espaço de probabilidade.
- Qual a chance de uma determinada aresta sobreviver ?
- Qual a esperança do número de arestas ?
- Como a esperança mostra a existência ?

No one can be told what the method is ...

- O teorema: Todo grafo contém um subgrafo bipartido com pelo menos $\frac{E(G)}{2}$ arestas
- O espaço de probabilidade.
- Qual a chance de uma determinada aresta sobreviver ?
- Qual a esperança do número de arestas ?
- Como a esperança mostra a existência ?

No one can be told what the method is ...

- O teorema: Todo grafo contém um subgrafo bipartido com pelo menos $\frac{E(G)}{2}$ arestas
- O espaço de probabilidade.
- Qual a chance de uma determinada aresta sobreviver ?
- Qual a esperança do número de arestas ?
- Como a esperança mostra a existência ?

Como a probabilidade nos ajudou ?

- Transformamos um problema global em um problema local
- Pudemos ignorar a extrutura do grafo
- Linearidade da esperança

O problema

- Um canal com p de inversão de bits alta, um único envio
- Um código de correção "ingênuo": repetir n vezes
- Para levar p a zero, levamos R a zero também
- Será que esse tradeoff é necessário ?

O problema

- Um canal com p de inversão de bits alta, um único envio
- Um código de correção ”ingênuo”: repetir n vezes
- Para levar p a zero, levamos R a zero também
- Será que esse tradeoff é necessário ?

O problema

- Um canal com p de inversão de bits alta, um único envio
- Um código de correção "ingênuo": repetir n vezes
- Para levar p a zero, levamos R a zero também
- Será que esse tradeoff é necessário ?

O problema

- Um canal com p de inversão de bits alta, um único envio
- Um código de correção "ingênuo": repetir n vezes
- Para levar p a zero, levamos R a zero também
- Será que esse tradeoff é necessário ?

Quão bom pode ser um código?

Teorema de Shannon

Se aceitamos uma probabilidade p_b de erro por bit, então, conseguimos códigos com rate

$$\frac{C}{1 - H(p_b)}$$

Onde C é uma constante, determinada pela probabilidade de falha do canal e pela distribuição dos dados, e $H(p_b)$ é a entropia binária de p_b (e $0 < H(p_b) \leq 1$)

Observações

- O teorema prova existência, mas não fornece o código
- O teorema, na forma mais geral, dá um limite exato para a capacidade de códigos
- Os códigos podem ter que usar tamanhos de bloco muito grandes
- Há implementações em uso que se aproximam desse limite teórico (LDPC, Turbo Codes)

O problema

- $G(n,p)$, $n \longrightarrow \infty$
- Conter grafos pequenos (H tem tamanho fixo)
- Porque tomamos probabilidade decrescente ?
- H balanceado
- Densidade (ρ) de um grafo

O problema

- $G(n, p)$, $n \to \infty$
- Conter grafos pequenos (H tem tamanho fixo)
- Porque tomamos probabilidade decrescente ?
- H balanceado
- Densidade (ρ) de um grafo

O problema

- $G(n, p)$, $n \to \infty$
- Conter grafos pequenos (H tem tamanho fixo)
- Porque tomamos probabilidade decrescente ?
- H balanceado
- Densidade (ρ) de um grafo

O problema

- $G(n, p)$, $n \to \infty$
- Conter grafos pequenos (H tem tamanho fixo)
- Porque tomamos probabilidade decrescente ?
- H balanceado
- Densidade (ρ) de um grafo

O problema

- $G(n, p)$, $n \to \infty$
- Conter grafos pequenos (H tem tamanho fixo)
- Porque tomamos probabilidade decrescente ?
- H balanceado
- Densidade (ρ) de um grafo

O teorema

Teorema

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:*

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

A prova

- O lado 0
  - $P(X > 0) \leq E(X)$
  - A hipótese de balanceamento
- O lado 1
  - A esperança não é o bastante
  - Desigualdade de Chebychev

A prova

- O lado 0
  - $P(X > 0) \leq E(X)$
  - A hipótese de balanceamento
- O lado 1
  - A esperança não é o bastante
  - Desigualdade de Chebychev

A prova

- O lado 0
  - $P(X > 0) \leq E(X)$
  - A hipótese de balanceamento
- O lado 1
  - A esperança não é o bastante
  - Desigualdade de Chebychev

A prova

- O lado 0
  - $P(X > 0) \leq E(X)$
  - A hipótese de balanceamento
- O lado 1
  - A esperança não é o bastante
  - Desigualdade de Chebychev