Pseudoaleatoriedade e Semialeatoriedade

Leandro Miranda Zatesko
leandro@inf.ufpr.br
ORIENTADOR: Jair Donadelli Jr.

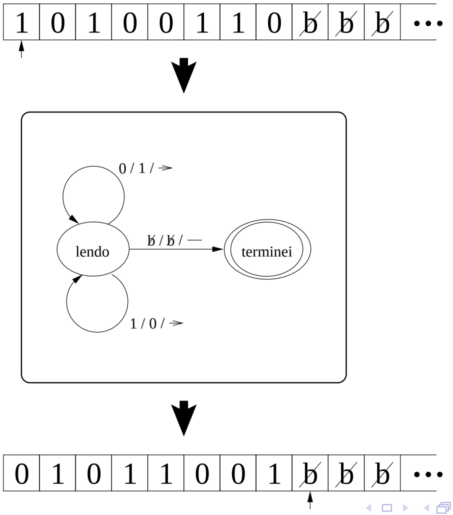
Grupo de Pesquisa em Algoritmos

25 de novembro de 2009

Sumário

Andamento da apresentação

Máquinas de Turing



Nomenclaturas sobre máquinas de Turing

Nomenclatura (Tempo)

O tempo de uma execução de uma máquina de Turing é o número de transições que ocorrem durante toda aquela execução.

Nomenclaturas sobre máquinas de Turing

Nomenclatura (Tempo)

O tempo de uma execução de uma máquina de Turing é o número de transições que ocorrem durante toda aquela execução.

Nomenclatura (Máquina de Turing polinomialmente executável)

Uma máquina de Turing polinomialmente executável é uma máquina de Turing que pode ser executada em tempo polinomial no tamanho da entrada.

Nomenclaturas sobre máquinas de Turing

Nomenclatura (Tempo)

O tempo de uma execução de uma máquina de Turing é o número de transições que ocorrem durante toda aquela execução.

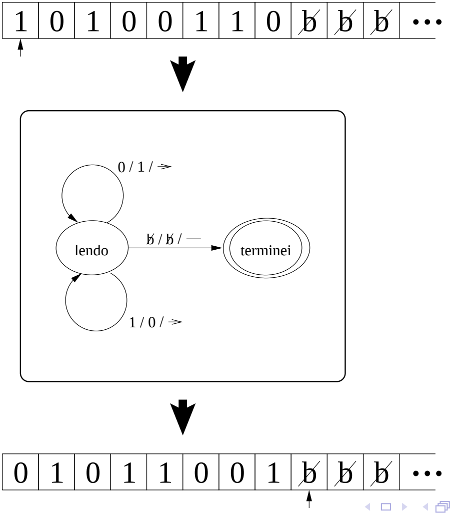
Nomenclatura (Máquina de Turing polinomialmente executável)

Uma máquina de Turing polinomialmente executável é uma máquina de Turing que pode ser executada em tempo polinomial no tamanho da entrada.

Nomenclatura (Determinismo das máquinas de Turing)

Dizemos que uma máquina de Turing é determinística, porque, para uma mesma entrada, obtemos sempre o mesmo comportamento da máquina.

Máquinas de Turing probabilísticas *offline*



Primalidade

Exemplo (Teste de primalidade)

O algoritmo de Miller-Rabin usa uma sequencia de *m bits* aleatórios para determinar se um número *n* é primo.

- n primo $\Longrightarrow MR(n) = \texttt{primo}$ sempre.
- n composto $\Longrightarrow MR(n) = \texttt{primo}$ com probabilidade menor que $\frac{1}{4}$.

Primalidade

Exemplo (Teste de primalidade)

O algoritmo de Miller-Rabin usa uma sequencia de *m bits* aleatórios para determinar se um número *n* é primo.

- n primo $\implies MR(n) = \texttt{primo}$ sempre.
- n composto $\implies MR(n) = \texttt{primo}$ com probabilidade menor que $\frac{1}{4}$.

$$\mathbb{P}[\text{Miller-Rabin errar para um número menor que } L] < 1\left(\frac{\pi(L)}{L}\right) + \frac{1}{4}\left(1 - \frac{\pi(L)}{L}\right).$$

Primalidade

Exemplo (Teste de primalidade)

O algoritmo de Miller-Rabin usa uma sequencia de *m bits* aleatórios para determinar se um número *n* é primo.

- n primo $\implies MR(n) = \texttt{primo}$ sempre.
- n composto $\implies MR(n) = \texttt{primo}$ com probabilidade menor que $\frac{1}{4}$.

$$\mathbb{P}[\text{Miller-Rabin errar para um número menor que } L] < 1\left(\frac{\pi(L)}{L}\right) + \frac{1}{4}\left(1 - \frac{\pi(L)}{L}\right).$$

Teorema (Teorema dos números primos)

$$\pi(L) \sim \frac{L}{\ln L}.$$

Primalidade

Exemplo (Teste de primalidade)

O algoritmo de Miller-Rabin usa uma sequencia de *m bits* aleatórios para determinar se um número *n* é primo.

- n primo $\implies MR(n) = \texttt{primo}$ sempre.
- n composto $\implies MR(n) = \texttt{primo}$ com probabilidade menor que $\frac{1}{4}$.

$$\mathbb{P}[\text{Miller-Rabin errar para um número menor que } L] < 1\left(\frac{\pi(L)}{L}\right) + \frac{1}{4}\left(1 - \frac{\pi(L)}{L}\right).$$

Teorema (Teorema dos números primos)

$$\pi(L) \sim \frac{L}{\ln L}.$$

$$\mathbb{P}[\text{Miller-Rabin errar}] < \frac{1}{4}.$$

Iteração do teste de primalidade de Miller-Rabin

Iterando o algoritmo k vezes e garantindo a independência entre as sequências de *bits* aleatórios, a probabilidade de erro no voto da maioria fica menor que

$$\left(\frac{1}{4}\right)^k.$$

Iteração do teste de primalidade de Miller-Rabin

Iterando o algoritmo k vezes e garantindo a independência entre as sequências de *bits* aleatórios, a probabilidade de erro no voto da maioria fica menor que

$$\left(\frac{1}{4}\right)^k.$$

Observação

Precisamos de km *bits* aleatórios para o procedimento acima. A Pseudoaleatoriedade trata sobre como gerar k sequências de m *bits* a partir de menos que km *bits* aleatórios, de modo que todos "pareçam" aleatórios. Tal processo é chamado de "reciclagem de *bits* aleatórios".

Andamento da apresentação

Variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

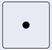
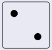
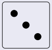
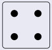
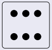
Seja $S = \{\text{PAR}, \text{ÍMPAR}\}$.

Ω

Variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

Seja $S = \{\text{PAR}, \text{ÍMPAR}\}$.

Ω						
$\Omega \to [0,1]$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

Variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

Seja $S = \{\text{PAR}, \text{ÍMPAR}\}$.

Ω						
$\Omega \to [0,1]$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$
$X : \Omega \to S$	PAR	ÍMPAR	PAR	ÍMPAR	PAR	ÍMPAR

Construção de espaços de probabilidades sobre variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

$\Omega_X = S$ PAR ÍMPAR

Construção de espaços de probabilidades sobre variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

$\Omega_X = S$ PAR ÍMPAR

$\mathbb{P}_X = S \rightarrow [0, 1]$

Construção de espaços de probabilidades sobre variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

PAR ÍMPAR

$\Omega_X = S$

$\mathbb{P}_X = S \to [0, 1] \quad \mathbb{P}(2) + \mathbb{P}(4) + \mathbb{P}(6) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$

Construção de espaços de probabilidades sobre variáveis aleatórias

Experimento (Paridade do resultado dum lançamento dum dado)

	PAR	ÍMPAR
$\Omega_X = S$		
$\mathbb{P}_X = S \to [0,1]$	$\mathbb{P}(2) + \mathbb{P}(4) + \mathbb{P}(6) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$	$\frac{1}{2}$

Um exemplo de distribuição de probabilidades

Exemplo (Distribuição uniforme)

$$\mathbf{u} = \Bigl(\overbrace{\frac{1}{|S|}, \frac{1}{|S|}, \ldots, \frac{1}{|S|}}^{|S| \text{ posições}}\Bigr).$$

Andamento da apresentação

Uma analogia imediata

Observação

Uma sequência de m *bits* aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. Por exemplo, $1010 \mapsto 10$.

Uma analogia imediata

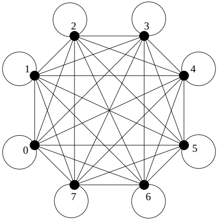
Observação

Uma sequência de m *bits* aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. Por exemplo, $1010 \mapsto 10$. Assim, já que as k sequências $R_1, \ldots, R_k$ são independentes, estando na j-ésima sequência (ou j-ésimo número) e indo para a $(j+1)$-ésima, temos n possibilidades, cada uma com $\mathbb{P} = \frac{1}{n}$.

Uma analogia imediata

Observação

Uma sequência de m *bits* aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. Por exemplo, $1010 \mapsto 10$. Assim, já que as k sequências $R_1, \ldots, R_k$ são independentes, estando na j-ésima sequência (ou j-ésimo número) e indo para a $(j+1)$-ésima, temos n possibilidades, cada uma com $\mathbb{P} = \frac{1}{n}$.

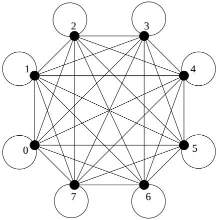


$$v_0, v_1, \ldots, v_k \mapsto R_1, \ldots, R_k$$

Uma analogia imediata

Observação

Uma sequência de m *bits* aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. Por exemplo, $1010 \mapsto 10$. Assim, já que as k sequências $R_1, \ldots, R_k$ são independentes, estando na j-ésima sequência (ou j-ésimo número) e indo para a $(j+1)$-ésima, temos n possibilidades, cada uma com $\mathbb{P} = \frac{1}{n}$.



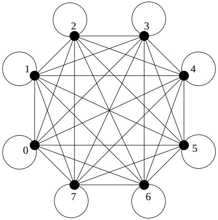
$$v_0, v_1, \ldots, v_k \mapsto R_1, \ldots, R_k$$

TOTAL km;

Uma analogia imediata

Observação

Uma sequência de m *bits* aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. Por exemplo, $1010 \mapsto 10$. Assim, já que as k sequências $R_1, \ldots, R_k$ são independentes, estando na j-ésima sequência (ou j-ésimo número) e indo para a $(j+1)$-ésima, temos n possibilidades, cada uma com $\mathbb{P} = \frac{1}{n}$.



$v_0, v_1, \ldots, v_k \mapsto R_1, \ldots, R_k$

TOTAL km;

Ideia Trocar m por d.

Troca de grafos completos por grafos regulares

G:

- conexo;

Troca de grafos completos por grafos regulares

G:

- conexo;
- com $n = 2^m$ vértices;

Troca de grafos completos por grafos regulares

G:

- conexo;
- com $n = 2^m$ vértices;
- bipartido;

Troca de grafos completos por grafos regulares

G:

- conexo;
- com $n = 2^m$ vértices;
- bipartido;
- d-regular;

Troca de grafos completos por grafos regulares

G:

- conexo;
- com $n = 2^m$ vértices;
- bipartido;
- d-regular;
- com todos os laços (d não conta laços);

Troca de grafos completos por grafos regulares

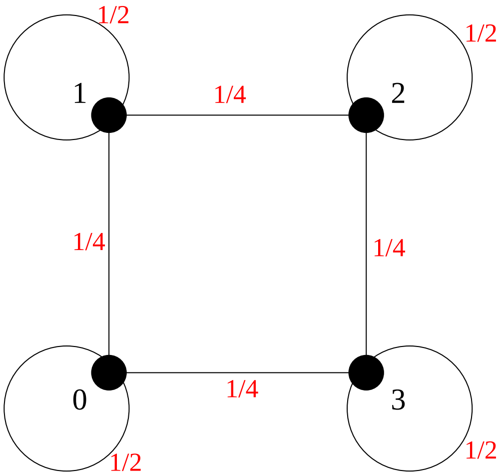
G:

- conexo;
- com $n = 2^m$ vértices;
- bipartido;
- d-regular;
- com todos os laços (d não conta laços);
- com a seguinte distribuição de probabilidades para as arestas:

  laço $\frac{1}{2}$;

  outras arestas $\frac{1}{2d}$.

Exemplo de grafo regular



Matrizes associadas a G

Definição (Matriz de adjacências)

$$(A_G)_{i,j} = \begin{cases} 1, & \text{se } i \text{ é adjacente a } j; \\ 0, & \text{caso contrário.} \end{cases}$$

Matrizes associadas a G

Definição (Matriz de adjacências)

$$(A_G)_{i,j} = \begin{cases} 1, & \text{se } i \text{ é adjacente a } j; \\ 0, & \text{caso contrário.} \end{cases}$$

Observação

Note que, como G possui todos os laços, $(A_G)_{i,i} = 1$, para todo i.

Matrizes associadas a G

Definição (Matriz de adjacências)

$$(A_G)_{i,j} = \begin{cases} 1, & \text{se } i \text{ é adjacente a } j; \\ 0, & \text{caso contrário.} \end{cases}$$

Observação

Note que, como G possui todos os laços, $(A_G)_{i,i} = 1$, para todo i.

Definição (Matriz de transição da cadeia de Markov)

$$(P_G)_{i,j} = \begin{cases} \frac{1}{2}, & \text{se } i = j; \\ \frac{1}{2d}, & \text{se } i \text{ é adjacente a } j, \text{ mas } i \neq j; \\ 0, & \text{caso contrário.} \end{cases}$$

Passeios aleatórios do ponto de vista probabilístico

Observação

O passeio aleatório em G pode ser entendido como uma sequência de distribuições de probabilidade.

$$\pi^{(0)} = \text{distribuição de probabilidades inicial;}$$
$$\pi^{(k)} = (\mathrm{P}_G)^k \left(\pi^{(0)}\right)^\top.$$

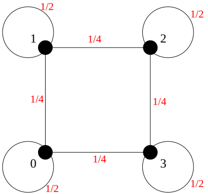
Passeios aleatórios do ponto de vista probabilístico

Observação

O passeio aleatório em G pode ser entendido como uma sequência de distribuições de probabilidade.

$$\pi^{(0)} = \text{distribuição de probabilidades inicial;}$$
$$\pi^{(k)} = (\mathrm{P}_G)^k \left(\pi^{(0)}\right)^\top.$$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} & 0 \\ 0 & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{2} \end{pmatrix}$$



$$(1, 0, 0, 0)$$
$$\left(\tfrac{1}{2}, \tfrac{1}{4}, 0, \tfrac{1}{4}\right)$$
$$\left(\tfrac{3}{8}, \tfrac{1}{4}, \tfrac{1}{8}, \tfrac{1}{4}\right)$$

Autovalores de P

Teorema

P *é simétrica e, portanto, diagonalizável, seus autovalores* $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ *são reais, e*

$$1 = \lambda_1 > \lambda_2 \geqslant \cdots \geqslant \lambda_n \geqslant 0.$$

Autovalores de P

Teorema

P é simétrica e, portanto, diagonalizável, seus autovalores $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ são reais, e

$$1 = \lambda_1 > \lambda_2 \geqslant \cdots \geqslant \lambda_n \geqslant 0.$$

Teorema

$$\|\pi^{(k)} - u\|_2 \leqslant \lambda_2^k.$$

Autovalores de P

Teorema

P *é simétrica e, portanto, diagonalizável, seus autovalores* $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ *são reais, e*

$$1 = \lambda_1 > \lambda_2 \geqslant \cdots \geqslant \lambda_n \geqslant 0.$$

Teorema

$$\|\pi^{(k)} - u\|_2 \leqslant \lambda_2^k.$$

Observação

λ_2 pode ser entendido como uma medida de quão perto de **u** a distribuição $\pi^{(k)}$ é. Quanto menor o λ_2, mais próximo.

Grafos expansores

Definição (Grafo expansor)

Um grafo bipartido conexo $H = (X \cup Y, E)$ é (n, d, c)-expansor se:

1. $X = Y = \frac{n}{2}$;
2. H é d-regular;
3. para todo $W \subseteq X$,

$$|\{(w, y)\colon w \in W\}| \leqslant \left(1 + c\left(1 - \frac{2|W|}{n}\right)\right)|W|.$$

Autovalores de A_G

Teorema

A_G *é simétrica e, portanto, diagonalizável, seus autovalores* $\mu_1 \geqslant \cdots \geqslant \mu_n$ *são reais, e*

$$\mu_1 = -\mu_n = d$$

Autovalores de A_G

Teorema

A_G é simétrica e, portanto, diagonalizável, seus autovalores $\mu_1 \geqslant \cdots \geqslant \mu_n$ são reais, e

$$\mu_1 = -\mu_n = d$$

Notação

μ denota o 2º maior autovalor distinto de A_G. Note-se que não necessariamente $\mu = \mu_2$.

Algumas propriedades dos grafos expansores

Definição (Discrepância dos grafos expansores)

Sendo $A \subseteq X$ e $B \subseteq Y$,

$$\mathrm{D}(A, B) = \left| |E(A, B)| - \frac{2d|A||B|}{n} \right|.$$

Algumas propriedades dos grafos expansores

Definição (Discrepância dos grafos expansores)

Sendo $A \subseteq X$ e $B \subseteq Y$,

$$\mathrm{D}(A, B) = \left| |E(A, B)| - \frac{2d|A||B|}{n} \right|.$$

Teorema

$$\mathrm{D}(A, B) = |\mu| \sqrt{|A||B|}.$$

Ideia do algoritmo

- F é o conjunto das sequências de *bits* que fazem a máquina falhar. Assumimos que $F < \frac{n}{100}$, $n = 2^m$ e

$$\mathrm{F}_{i,j} = \begin{cases} 1, & \text{se } i = j \text{ e } i \in F; \\ 0, & \text{caso contrário.} \end{cases}$$

Ideia do algoritmo

- F é o conjunto das sequências de *bits* que fazem a máquina falhar. Assumimos que $F < \frac{n}{100}$, $n = 2^m$ e

$$\mathrm{F}_{i,j} = \begin{cases} 1, & \text{se } i = j \text{ e } i \in F; \\ 0, & \text{caso contrário.} \end{cases}$$

- G é um (n, d, c)-expansor com adição de laços.

Ideia do algoritmo

- F é o conjunto das sequências de *bits* que fazem a máquina falhar. Assumimos que $F < \frac{n}{100}$, $n = 2^m$ e

$$\mathrm{F}_{i,j} = \begin{cases} 1, & \text{se } i = j \text{ e } i \in F; \\ 0, & \text{caso contrário.} \end{cases}$$

- G é um (n, d, c)-expansor com adição de laços.
- t é um natural tal que $\lambda_2^t < \frac{1}{10}$.

Ideia do algoritmo

- F é o conjunto das sequências de *bits* que fazem a máquina falhar. Assumimos que $F < \frac{n}{100}$, $n = 2^m$ e

$$\mathsf{F}_{i,j} = \begin{cases} 1, & \text{se } i = j \text{ e } i \in F; \\ 0, & \text{caso contrário.} \end{cases}$$

- G é um (n, d, c)-expansor com adição de laços.
- t é um natural tal que $\lambda_2^t < \frac{1}{10}$.
- R_1 é um vértice aleatório de G (escolhido uniformemente).

Ideia do algoritmo

- F é o conjunto das sequências de *bits* que fazem a máquina falhar. Assumimos que $F < \frac{n}{100}$, $n = 2^m$ e

$$\mathrm{F}_{i,j} = \begin{cases} 1, & \text{se } i = j \text{ e } i \in F; \\ 0, & \text{caso contrário.} \end{cases}$$

- G é um (n, d, c)-expansor com adição de laços.
- t é um natural tal que $\lambda_2^t < \frac{1}{10}$.
- R_1 é um vértice aleatório de G (escolhido uniformemente).
- Passeio aleatório:

$$R_1 \xrightarrow{t\ \text{passos}} R_2 \xrightarrow{t\text{passos}} R_3 \rightarrow \cdots \rightarrow R_k.$$

Cálculo da probabilidade total de falha

Observação

Dada uma distribuição de probabilides π sobre os vértices de G, $\|\mathsf{F}\pi^\top\|_1$ representa a probabilidade de uma sequência de *bits* escolhida aleatoriamente com distribuição π estar em F.

Cálculo da probabilidade total de falha

Observação

Dada uma distribuição de probabilides π sobre os vértices de G, $\|F\pi^\top\|_1$ representa a probabilidade de uma sequência de *bits* escolhida aleatoriamente com distribuição π estar em F.

$$\left\| \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{3} \\ \frac{1}{6} \\ \frac{1}{3} \\ \frac{1}{6} \end{pmatrix} \right\|_1 = \left\| \begin{pmatrix} \frac{1}{3} \\ 0 \\ \frac{1}{3} \\ 0 \end{pmatrix} \right\|_1 = \frac{2}{3}.$$

O grande teorema

Lema

Para todo vetor $\mathbf{x}$ *do* $\mathbb{R}^n$,

$$\|\mathsf{F}(\mathsf{P}_G)^t\mathbf{x}^\top\|_2 \leqslant \frac{1}{5}\|x\|_2 \qquad e \qquad \|(\mathbf{I}-\mathsf{F})(\mathsf{P}_G)^t\mathbf{x}^\top\|_2 \leqslant \|x\|_2.$$

Teorema

Dada uma máquina $\mathcal{BPP}$ *que usa* m *bits aleatórios por rodada, consegue-se uma probabilidade de erro do voto da maioria no máximo* $\frac{1}{2^k}$ *utilizando* $O(m+k)$ *bits aleatórios e* $O(k)$ *rodadas.*

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1$

Esboço de demonstração do teorema (I)

Demonstração.

$$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_2$$

Esboço de demonstração do teorema (I)

Demonstração.

$$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)^\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)^\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2$$

Esboço de demonstração do teorema (I)

Demonstração.

$$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right)$$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathsf{F}(\mathsf{P}_G)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_1$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)^\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)^\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathsf{F}\left(\mathsf{P}_G\right)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)^\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\left(\mathsf{P}_G\right)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)^\top}\|_2$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)^\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)^\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathsf{F}\left(\mathsf{P}_G\right)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)^\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\left(\mathsf{P}_G\right)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)^\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)^\top}\|_2$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathsf{F}(\mathsf{P}_G)^t(\mathsf{I}-\mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}(\mathsf{P}_G)^t(\mathsf{I}-\mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathsf{I}-\mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\sqrt{n\left(\frac{1}{n^2}\right)} = \frac{\sqrt{n}}{5}\left(\frac{1}{\sqrt{n}}\right)$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathsf{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathsf{F}\left(\mathsf{P}_G\right)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathsf{F}\left(\mathsf{P}_G\right)^t(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathsf{I} - \mathsf{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\sqrt{n\left(\frac{1}{n^2}\right)} = \frac{\sqrt{n}}{5}\left(\frac{1}{\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \in F] = \|\mathsf{F}\left(\mathsf{P}_G\right)^t\mathsf{F}\boldsymbol{\pi}^{(0)\top}\|_1$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathrm{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathrm{F}(\mathrm{P}_G)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}(\mathrm{P}_G)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\sqrt{n\left(\frac{1}{n^2}\right)} = \frac{\sqrt{n}}{5}\left(\frac{1}{\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \in F] = \|\mathrm{F}(\mathrm{P}_G)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}(\mathrm{P}_G)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathrm{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathrm{F}(\mathrm{P}_G)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}(\mathrm{P}_G)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\sqrt{n\left(\frac{1}{n^2}\right)} = \frac{\sqrt{n}}{5}\left(\frac{1}{\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \in F] = \|\mathrm{F}(\mathrm{P}_G)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}(\mathrm{P}_G)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathrm{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathrm{F}(\mathrm{P}_G)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}(\mathrm{P}_G)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\sqrt{n\left(\frac{1}{n^2}\right)} = \frac{\sqrt{n}}{5}\left(\frac{1}{\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \in F] = \|\mathrm{F}(\mathrm{P}_G)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}(\mathrm{P}_G)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\left(\frac{1}{10\sqrt{n}}\right)$

Esboço de demonstração do teorema (I)

Demonstração.

$\mathbb{P}[R_1 \in F] = \|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 = \sqrt{n}\|\mathrm{F}\mathbf{u}^\top\|_2 \leqslant \sqrt{n}\sqrt{\frac{n}{100}\left(\frac{1}{n^2}\right)} = \sqrt{n}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \notin F] = \|\mathrm{F}\left(\mathrm{P}_G\right)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}\left(\mathrm{P}_G\right)^t(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|(\mathrm{I}-\mathrm{F})\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\sqrt{n\left(\frac{1}{n^2}\right)} = \frac{\sqrt{n}}{5}\left(\frac{1}{\sqrt{n}}\right) \leqslant \frac{1}{5}$.

$\mathbb{P}[R_2 \in F | R_1 \in F] = \|\mathrm{F}\left(\mathrm{P}_G\right)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_1 \leqslant \sqrt{n}\|\mathrm{F}\left(\mathrm{P}_G\right)^t\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\|\mathrm{F}\boldsymbol{\pi}^{(0)\top}\|_2 \leqslant \frac{\sqrt{n}}{5}\left(\frac{1}{10\sqrt{n}}\right) \leqslant \frac{1}{50} \leqslant \frac{1}{5}$.

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "$(\text{bom}, \text{ruim}, \dots)$" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \dots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "$(\text{bom}, \text{ruim}, \dots)$" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \dots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Como há 2^k possíveis arranjos "$(\text{bom}, \text{ruim}, \dots)$", a probabilidade de $(R_1, \dots, R_k)$ conter no mínimo $\frac{k}{2}$ "ruins" é no máximo $2^k\left(\frac{1}{5}\right)^{\frac{k}{2}}$.

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "(bom, ruim, ...)" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \ldots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Como há 2^k possíveis arranjos "(bom, ruim, ...)", a probabilidade de $(R_1, \ldots, R_k)$ conter no mínimo $\frac{k}{2}$ "ruins" é no máximo $2^k\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Logo, a probabilidade de erro no voto da maioria é no máximo

$$\left(\frac{2}{\sqrt{5}}\right)^k.$$

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "$(\text{bom}, \text{ruim}, \dots)$" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \dots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Como há 2^k possíveis arranjos "$(\text{bom}, \text{ruim}, \dots)$", a probabilidade de $(R_1, \dots, R_k)$ conter no mínimo $\frac{k}{2}$ "ruins" é no máximo $2^k\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Logo, a probabilidade de erro no voto da maioria é no máximo

$$\left(\frac{2}{\sqrt{5}}\right)^k.$$

Sendo c tal que $\left(\frac{2}{\sqrt{5}}\right)^c \leqslant \frac{1}{2}$, rode a máquina $k' = ck = O(k)$ vezes.

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "(bom, ruim, ...)" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \ldots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Como há 2^k possíveis arranjos "(bom, ruim, ...)", a probabilidade de $(R_1, \ldots, R_k)$ conter no mínimo $\frac{k}{2}$ "ruins" é no máximo $2^k\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Logo, a probabilidade de erro no voto da maioria é no máximo

$$\left(\frac{2}{\sqrt{5}}\right)^k.$$

Sendo c tal que $\left(\frac{2}{\sqrt{5}}\right)^c \leqslant \frac{1}{2}$, rode a máquina $k' = ck = O(k)$ vezes. Para gerar R_1, precisamos de m *bits* aleatórios.

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "(bom, ruim, ...)" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \ldots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Como há 2^k possíveis arranjos "(bom, ruim, ...)", a probabilidade de $(R_1, \ldots, R_k)$ conter no mínimo $\frac{k}{2}$ "ruins" é no máximo $2^k\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Logo, a probabilidade de erro no voto da maioria é no máximo

$$\left(\frac{2}{\sqrt{5}}\right)^k.$$

Sendo c tal que $\left(\frac{2}{\sqrt{5}}\right)^c \leqslant \frac{1}{2}$, rode a máquina $k' = ck = O(k)$ vezes. Para gerar R_1, precisamos de m *bits* aleatórios. Para gerar $R_2, \ldots, R_k$, precisamos de $O(tdk) = O(k)$ *bits* aleatórios.

Esboço de demonstração do teorema (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "(bom, ruim, ...)" com no mínimo $\frac{k}{2}$ "ruins", a probabilidade de $(R_1, \ldots, R_k)$ casar com essa sequência é no máximo $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Como há 2^k possíveis arranjos "(bom, ruim, ...)", a probabilidade de $(R_1, \ldots, R_k)$ conter no mínimo $\frac{k}{2}$ "ruins" é no máximo $2^k\left(\frac{1}{5}\right)^{\frac{k}{2}}$.Logo, a probabilidade de erro no voto da maioria é no máximo

$$\left(\frac{2}{\sqrt{5}}\right)^k.$$

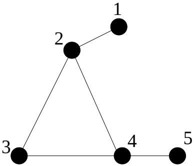
Sendo c tal que $\left(\frac{2}{\sqrt{5}}\right)^c \leqslant \frac{1}{2}$, rode a máquina $k' = ck = O(k)$ vezes. Para gerar R_1, precisamos de m *bits* aleatórios. Para gerar $R_2, \ldots, R_k$, precisamos de $O(tdk) = O(k)$ *bits* aleatórios. Portanto, para gerar $R_1, \ldots, R_k$, precisamos de $O(m + k)$ *bits* aleatórios. ♦

Andamento da apresentação

Assimetria de grafos

Definição (Grafo assimétrico)

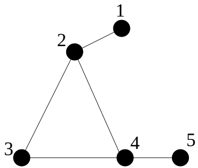
Dizemos que um grafo G é assimétrico se o único automorfismo possível sobre G é a identidade.



Assimetria de grafos

Definição (Grafo assimétrico)

Dizemos que um grafo G é assimétrico se o único automorfismo possível sobre G é a identidade.

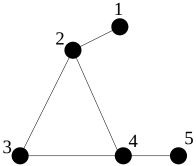


$$\begin{aligned} 1 &\mapsto 5 \\ 2 &\mapsto 4 \\ 3 &\mapsto 3 \\ 4 &\mapsto 2 \\ 5 &\mapsto 1 \end{aligned}$$

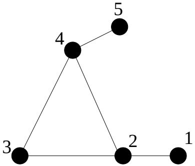
Assimetria de grafos

Definição (Grafo assimétrico)

Dizemos que um grafo G é assimétrico se o único automorfismo possível sobre G é a identidade.



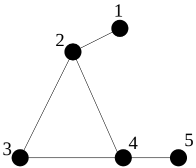
$$\begin{aligned} 1 &\mapsto 5 \\ 2 &\mapsto 4 \\ 3 &\mapsto 3 \\ 4 &\mapsto 2 \\ 5 &\mapsto 1 \end{aligned}$$



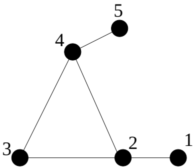
Assimetria de grafos

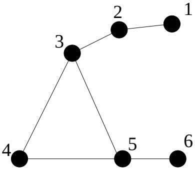
Definição (Grafo assimétrico)

Dizemos que um grafo G é assimétrico se o único automorfismo possível sobre G é a identidade.



$$\begin{aligned} 1 &\mapsto 5 \\ 2 &\mapsto 4 \\ 3 &\mapsto 3 \\ 4 &\mapsto 2 \\ 5 &\mapsto 1 \end{aligned}$$





Observação

A probabilidade de um grafo com n vértices tomado aleatoriamente ser assimétrico tende a 1 quando n tende ao infinito.

Assimetria de grafos

Definição (Semialeatoriedade para subconjuntos do $\mathbb{Z}_n$)

Diz-se que um subconjunto S do $\mathbb{Z}_n$ é semialeatório quando S satisfaz alguma — e, por conseguinte, cada uma[a] — das propriedades listadas a seguir.

[a] As propriedades são todas equivalentes.

Notações preliminares

Dado um subconjunto S de $\mathbb{Z}_n$:

Definição (Caracter, função característica ou função indicatória)

É a função $\chi_S\colon \mathbb{Z} \to \{0,1\}$ tal que $\chi_S(z) = 0$, se $z \notin S$, e $\chi_S(z) = 1$, caso contrário.

Notações preliminares

Dado um subconjunto S de $\mathbb{Z}_n$:

Definição (Caracter, função característica ou função indicatória)

É a função $\chi_S \colon \mathbb{Z} \to \{0,1\}$ tal que $\chi_S(z) = 0$, se $z \notin S$, e $\chi_S(z) = 1$, caso contrário.

Definição (Translado de S por x)

$S + x = \{s + x \colon s \in S\}$.

Notações preliminares

Dado um subconjunto S de $\mathbb{Z}_n$:

Definição (Caracter, função característica ou função indicatória)

É a função $\chi_S \colon \mathbb{Z} \to \{0, 1\}$ tal que $\chi_S(z) = 0$, se $z \notin S$, e $\chi_S(z) = 1$, caso contrário.

Definição (Translado de S por x)

$S + x = \{s + x \colon s \in S\}$.

Definição (Grafo associado a S)

$G_S = \big(\mathbb{Z}_n, \{\{i, j\} : i + j \in S\}\big)$.

Notações preliminares

Dado um subconjunto S de $\mathbb{Z}_n$:

Definição (Caracter, função característica ou função indicatória)

É a função $\chi_S\colon \mathbb{Z} \to \{0,1\}$ tal que $\chi_S(z) = 0$, se $z \notin S$, e $\chi_S(z) = 1$, caso contrário.

Definição (Translado de S por x)

$S + x = \{s + x\colon s \in S\}$.

Definição (Grafo associado a S)

$G_S = \big(\mathbb{Z}_n, \{\{i,j\} : i + j \in S\}\big)$.

Notação

$(\tilde{\forall} x \in X)\,(p(x)) \iff |\{x \in X\colon p(x)\}| = |X| - o(|X|)$.

Propriedades sobre a translação

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade . . . se. . .

Propriedade (Translação fraca)

Para quase todo $x \in \mathbb{Z}_n$,

$$|S \cap (S + x)| = \frac{|S|^2}{n} + o(n).$$

Propriedades sobre a translação

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ... se...

Propriedade (Translação fraca)

Para quase todo $x \in \mathbb{Z}_n$,

$$|S \cap (S + x)| = \frac{|S|^2}{n} + o(n).$$

Propriedade (Translação forte)

Para todo subconjunto T de $\mathbb{Z}_n$ e quase todo x em $\mathbb{Z}_n$,

$$|S \cap (T + x)| = \frac{|S||T|}{n} + o(n).$$

Propriedades sobre o padrão

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade . . . se. . .

Propriedade (Padrão-2)

Para quase todo $u_1, u_2 \in \mathbb{Z}_n$,

$$\sum_{s \in S} \chi_S(x + u_1)\chi_S(x + u_2) = \frac{|S|^2}{n} + o(n).$$

Propriedades sobre o padrão

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ... se...

Propriedade (Padrão-2)

Para quase todo $u_1, u_2 \in \mathbb{Z}_n$,

$$\sum_{s \in S} \chi_S(x + u_1)\chi_S(x + u_2) = \frac{|S|^2}{n} + o(n).$$

Propriedade (Padrão-k)

Para quase todo $u_1, \ldots, u_k \in \mathbb{Z}_n$,

$$\sum_{s \in S} \prod_{j=1}^{k} \chi_S(x + u_j) = \frac{|S|^k}{n^{k-1}} + o(n).$$

Propriedades sobre a representação

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ...se...

Propriedade (Representação-2)

Para quase todo $x \in \mathbb{Z}_n$,

$$\sum_{\substack{u_1, u_2 \in S \\ u_1 + u_2 = x}} \chi_S(u_1)\chi_S(u_2) = \frac{|S|^2}{n} + o(n).$$

Propriedades sobre a representação

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ... se...

Propriedade (Representação-2)

Para quase todo $x \in \mathbb{Z}_n$,

$$\sum_{\substack{u_1, u_2 \in S \\ u_1 + u_2 = x}} \chi_S(u_1)\chi_S(u_2) = \frac{|S|^2}{n} + o(n).$$

Propriedade (Representação-k)

Para quase todo $x \in \mathbb{Z}_n$,

$$\sum_{\substack{u_1, \ldots, u_k \in S \\ \sum_{\ell=1}^{k} u_j = x}} \prod_{j=1}^{k} \chi_S(u_j) = \frac{|S|^k}{n^{k-1}} + o(n).$$

Mais propriedades

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ...se...

Propriedade (Soma exponencial)

Para todo $j \in \mathbb{Z}_n \setminus \{0\}$,

$$\sum_{x \in S} \chi_S(x) \mathrm{e}^{\frac{2\pi \mathrm{i} j x}{n}} = o(n).$$

Mais propriedades

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade . . . se. . .

Propriedade (Soma exponencial)

Para todo $j \in \mathbb{Z}_n \setminus \{0\}$,

$$\sum_{x \in S} \chi_S(x) \mathrm{e}^{\frac{2\pi \mathrm{i} j x}{n}} = o(n).$$

Propriedade (Grafo semialeatório)

G_S *é semialeatório.*

Mais propriedades ainda

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ...se...

Propriedade (Ciclo-2t)

$$\sum_{x_1,\ldots,x_{2t}} \chi_S(x_1+x_2)\chi_S(x_2+x_3)\cdots\chi_S(x_{2t-1}+x_{2t})\chi_S(x_{2t}+x_1)$$
$$= s^{2t} + o\big((n^{2t}\big).$$

Mais propriedades ainda

Um subconjunto $S \subseteq \mathbb{Z}_n$ tem a propriedade ...se...

Propriedade (Ciclo-$2t$)

$$\sum_{x_1,\dots,x_{2t}} \chi_S(x_1+x_2)\chi_S(x_2+x_3)\cdots\chi_S(x_{2t-1}+x_{2t})\chi_S(x_{2t}+x_1) = s^{2t} + o\big((n^{2t}\big).$$

Propriedade (Densidade relativa)

Para todo subconjunto T de $\mathbb{Z}_n$,

$$\sum_{x,y \in S} \chi_T(x)\chi_T(y)\chi_S(x+y) = \frac{|S||T|^2}{n} + o(n^2).$$

Andamento da apresentação

O que aprendemos neste seminário

- A pseudoaleatoriedade trata sobre como, a partir de algumas sequências aleatórias, gerar outras sequências, de modo que o conjunto de todas as sequências se comporte quase como se fosse verdadeiramente aleatório para a distribuição uniforme.

O que aprendemos neste seminário

- A pseudoaleatoriedade trata sobre como, a partir de algumas sequências aleatórias, gerar outras sequências, de modo que o conjunto de todas as sequências se comporte quase como se fosse verdadeiramente aleatório para a distribuição uniforme.
- Vimos que, dada uma máquina $\mathcal{BPP}$ que usa m *bits* aleatórios por rodada, consegue-se uma probabilidade de erro do voto da maioria no máximo $\frac{1}{2^k}$ utilizando $O(m+k)$ *bits* aleatórios e $O(k)$ rodadas.

O que aprendemos neste seminário

- A pseudoaleatoriedade trata sobre como, a partir de algumas sequências aleatórias, gerar outras sequências, de modo que o conjunto de todas as sequências se comporte quase como se fosse verdadeiramente aleatório para a distribuição uniforme.
- Vimos que, dada uma máquina $\mathcal{BPP}$ que usa m *bits* aleatórios por rodada, consegue-se uma probabilidade de erro do voto da maioria no máximo $\frac{1}{2^k}$ utilizando $O(m+k)$ *bits* aleatórios e $O(k)$ rodadas.
- A semialeatoriedade busca definir propriedades equivalentes que sirvam para garantir a representatividade de um elemento de uma classe, de acordo com aquilo que é esperado que um elemento realmente aleatório daquela classe tenha.

Referências

B. Chazelle.
The Discrepancy Method: Randomness and Complexity.
Cambridge University Press, 2000.
Capítulo 9: Pseudorandomness.

F. R. K. Chung and R. L. Graham.
Quasi-random subsets of $\mathbb{Z}_n$.
Journal of Combinatorial Theory, pages 64–86, 1992.

F. R. K. Chung, R. L. Graham, and R. M. Wilson.
Quasi-random graphs.
Proc. Natl. Acad. Sci., 85:969–970, 1988.

Se te parece que sabes e entendes bem muitas coisas, lembra-te que é muito mais o que ignoras.

(Imitação de Cristo)