Pseudoaleatoriedade

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

Variáveis aleatórias

Definição

Uma variável aleatória é uma função

$$X : \Omega \to S,$$

sendo Ω um espaço amostral de um espaço de probabilidades $(\Omega, \mathbb{P})$ e S uma σ-álgebra (usualmente $\mathbb{R}$).

Variáveis aleatórias

Definição

Uma variável aleatória é uma função

$$X\colon \Omega \to S,$$

sendo Ω um espaço amostral de um espaço de probabilidades $(\Omega, \mathbb{P})$ e S uma σ-álgebra (usualmente $\mathbb{R}$).

Exemplo (Número de lançamentos duma moeda até sair cara)

E. amostral $\Omega = \{(\text{cara}), (\text{coroa}, \text{cara}), (\text{coroa}, \text{coroa}, \text{cara}), \dots\}$

V. aleatória $X\big((\text{cara})\big) = 1,\ X\big((\text{coroa}, \text{cara})\big) = 2,\ X\big((\text{coroa}, \text{coroa}, \text{cara})\big) = 3$

Construção de espaços de probabilidades sobre variáveis aleatórias

Propriedade

Dado um espaço de probabilidades $(\Omega, \mathbb{P})$ *e uma variável aleatória* $X\colon \Omega \to S$, X *induz um espaço de probabilidades* $(\Omega_X, \mathbb{P}_X)$, *em que* $\Omega_X = S$, *e, para todo* $s \in S$,

$$\mathbb{P}_X(s) = \mathbb{P}_X[X = s]$$

Construção de espaços de probabilidades sobre variáveis aleatórias

Propriedade

Dado um espaço de probabilidades $(\Omega, \mathbb{P})$ *e uma variável aleatória* $X : \Omega \to S$, X *induz um espaço de probabilidades* $(\Omega_X, \mathbb{P}_X)$, *em que* $\Omega_X = S$, *e, para todo* $s \in S$,

$$\mathbb{P}_X(s) = \mathbb{P}_X[X = s] = \sum_{\omega \in \Omega} \mathbb{P}_X[X(\omega) = s]$$

Construção de espaços de probabilidades sobre variáveis aleatórias

Propriedade

Dado um espaço de probabilidades $(\Omega, \mathbb{P})$ *e uma variável aleatória* $X \colon \Omega \to S$, X *induz um espaço de probabilidades* $(\Omega_X, \mathbb{P}_X)$, *em que* $\Omega_X = S$, *e, para todo* $s \in S$,

$$\mathbb{P}_X(s) = \mathbb{P}_X[X = s] = \sum_{\omega \in \Omega} \mathbb{P}_X[X(\omega) = s] = \sum_{\omega \in X^{-1}(s)} \mathbb{P}(\omega).$$

Construção de espaços de probabilidades sobre variáveis aleatórias

Propriedade

Dado um espaço de probabilidades $(\Omega, \mathbb{P})$ *e uma variável aleatória* $X \colon \Omega \to S$, X *induz um espaço de probabilidades* $(\Omega_X, \mathbb{P}_X)$, *em que* $\Omega_X = S$, *e, para todo* $s \in S$,

$$\mathbb{P}_X(s) = \mathbb{P}_X[X = s] = \sum_{\omega \in \Omega} \mathbb{P}_X[X(\omega) = s] = \sum_{\omega \in X^{-1}(s)} \mathbb{P}(\omega).$$

Nomenclatura (Distribuição de probabilidades)

$\mathbb{P}_X$ é chamada de distribuição de probabilidades de X sobre S. Se $S = s_1, \ldots, s_m$ for finito, representa-se $\mathbb{P}_X$ por um vetor

$$\pi = (\mathbb{P}_X(s_1), \ldots, \mathbb{P}_X(s_m)).$$

Distribuição uniforme

Definição (Distribuição uniforme)

A distribuição uniforme de X sobre um conjunto finito S é aquela para a qual

$$\mathbb{P}[X = s] = \frac{1}{|S|} \qquad \text{para todo } s \in S.$$

Distribuição uniforme

Definição (Distribuição uniforme)

A distribuição uniforme de X sobre um conjunto finito S é aquela para a qual

$$\mathbb{P}[X = s] = \frac{1}{|S|} \qquad \text{para todo } s \in S.$$

Notação

Se o contradomínio da variável aleatória é finito, costuma-se usar $\mathbf{u}$ para representar a distribuição uniforme.

Máquina de Turing probabilística *offline*

Definição (Máquina de Turing probabilística *offline*)

Uma máquina de Turing probabilística *offline* é uma máquina de Turing determinística que, além da fita de entrada, recebe outra fita, somente de leitura, com m *bits* aleatórios, cada um usado uma só vez.

Máquina de Turing probabilística *offline*

Definição (Máquina de Turing probabilística *offline*)

Uma máquina de Turing probabilística *offline* é uma máquina de Turing determinística que, além da fita de entrada, recebe outra fita, somente de leitura, com m *bits* aleatórios, cada um usado uma só vez.

Exemplo (Teste de primalidade)

O algoritmo de Miller-Rabin usa uma sequencia de *bits* aleatórios para determinar se um número n é primo. Tem complexidade[a] $O(\log^3 n)$.

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

[a] O AKS (determinístico) tem complexidade $O(\log^{12+\epsilon} n)$.

Uma classe de complexidade probabilística

Definição ($\mathcal{BPP}$)

$\mathcal{BPP}$ é o conjunto das linguagens que são decididas por uma máquina de Turing probabilística *offline* com probabilidade de acerto no mínimo $\frac{2}{3}$.

Uma classe de complexidade probabilística

Definição ($\mathcal{BPP}$)

$\mathcal{BPP}$ é o conjunto das linguagens que são decididas por uma máquina de Turing probabilística *offline* com probabilidade de acerto no mínimo $\frac{2}{3}$.

Observação

- $L = \{\langle n \rangle : n \text{ é primo}\} \in \mathcal{BPP}$.
- $\mathcal{P} \subseteq \mathcal{BPP}$, mas ninguém sabe se $\mathcal{BPP} \subseteq \mathcal{P}$.

Uma classe de complexidade probabilística

Definição ($\mathcal{BPP}$)

$\mathcal{BPP}$ é o conjunto das linguagens que são decididas por uma máquina de Turing probabilística *offline* com probabilidade de acerto no mínimo $\frac{2}{3}$.

Observação

- $L = \{\langle n \rangle : n \text{ é primo}\} \in \mathcal{BPP}$.
- $\mathcal{P} \subseteq \mathcal{BPP}$, mas ninguém sabe se $\mathcal{BPP} \subseteq \mathcal{P}$.

Nomenclatura

Uma máquina de Turing $\mathcal{BPP}$ é uma máquina de Turing probabilística *offline* cuja probabilidade de acerto é no mínimo $\frac{2}{3}$.

Iteração de um algoritmo probabilístico

Iterando uma máquina de Turing $\mathcal{BPP}$ k vezes e garantindo a independência entre as sequências de bits aleatórios, a probabilidade de erro no voto da maioria se reduz para no máximo

$$\frac{1}{2^{\Omega(k)}}.$$

Iteração de um algoritmo probabilístico

Iterando uma máquina de Turing $\mathcal{BPP}$ k vezes e garantindo a independência entre as sequências de bits aleatórios, a probabilidade de erro no voto da maioria se reduz para no máximo

$$\frac{1}{2^{\Omega(k)}}.$$

Observação

Note-se que, se a máquina usa m bits aleatórios, precisamos de km bits aleatórios para o procedimento acima.

Algumas normas de vetores

$$\|(x_1, \ldots, x_n)\|_1 = \sum_{j=1}^{n} |x_j|$$ norma de Manhattan

Algumas normas de vetores

$$\|(x_1, \dots, x_n)\|_1 = \sum_{j=1}^{n} |x_j| \qquad \text{norma de Manhattan}$$

$$\|(x_1, \dots, x_n)\|_2 = \sqrt{\sum_{j=1}^{n} x_j^2} \qquad \text{norma euclidiana}$$

Andamento da apresentação

Uma analogia trivial

Observação

Uma sequência de m bits aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$.

Uma analogia trivial

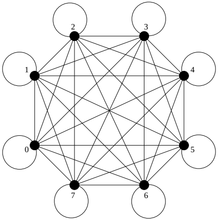
Observação

Uma sequência de m bits aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. 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 probabilidade $\frac{1}{n}$.

Uma analogia trivial

Observação

Uma sequência de m bits aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. 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 probabilidade $\frac{1}{n}$.

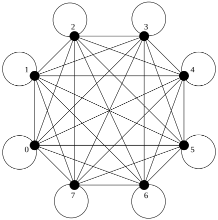


$$v_0, v_1, \ldots, v_k \mapsto R_1, \ldots, R_k$$

Uma analogia trivial

Observação

Uma sequência de m bits aleatórios pode ser entendida como um número em $[0..n-1]$, sendo $n = 2^m$. 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 probabilidade $\frac{1}{n}$.



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

TOTAL km;

Ideia Trocar m por d.

Troca de grafos completos por grafos regulares

G:

- conexo;
- 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 $\frac{1}{2d}$.

Matrizes associadas a G

Definição (Matriz de adjacências)

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

Matrizes associadas a G

Definição (Matriz de adjacências)

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

Observação

Note que, como G possui todos os laços, $\left(A_G\right)_{i,i} = 1$, 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)

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

Passeios aleatórios do ponto de vista probabilístico

Observação

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

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

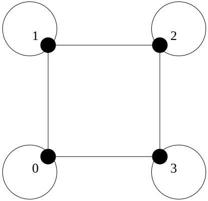
Passeios aleatórios do ponto de vista probabilístico

Observação

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

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

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



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

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

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

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

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

Observação

λ_2 pode ser entendido como uma medida de quão perto de **u** a distribuição $\boldsymbol{\pi}^{(k)}$ 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

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

- 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.
- Passeio aleatório:

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

Um lema importante

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.

Um lema importante

Observação

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

Lema

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

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

O grande teorema

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 (I)

Demonstração

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

Esboço de demonstração (I)

Demonstração

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

Esboço de demonstração (I)

Demonstração

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

Esboço de demonstração (I)

Demonstração

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

Esboço de demonstração (I)

Demonstração

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

Esboço de demonstração (I)

Demonstração

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

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

Esboço de demonstração (I)

Demonstração

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

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

Esboço de demonstração (I)

Demonstração

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

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

Esboço de demonstração (I)

Demonstração

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

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

Esboço de demonstração (I)

Demonstração

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

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

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

Esboço de demonstração (I)

Demonstração

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

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

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

Esboço de demonstração (I)

Demonstração

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

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

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

Esboço de demonstração (I)

Demonstração

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

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

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

Esboço de demonstração (I)

Demonstração

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

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

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

Esboço de demonstração (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 $\left(\frac{1}{5}\right)^{\frac{k}{2}}$.

Esboço de demonstração (II)

Demonstração.

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

Esboço de demonstração (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 (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 (II)

Demonstração.

Indutivamente, dada uma sequência aleatória de "$(\text{bom}, \text{ruim}, \ldots)$" 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 "$(\text{bom}, \text{ruim}, \ldots)$", 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 (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. Para gerar R_1, precisamos de m *bits* aleatórios. Para gerar $R_2, \dots, R_k$, precisamos de $O(tdk) = O(k)$ *bits* aleatórios.

Esboço de demonstração (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. Para gerar R_1, precisamos de m *bits* aleatórios. Para gerar $R_2, \dots, R_k$, precisamos de $O(tdk) = O(k)$ *bits* aleatórios. Portanto, para gerar $R_1, \dots, R_k$, precisamos de $O(m + k)$ bits aleatórios. ♦

Andamento da apresentação

Assimetria de grafos

Definição (Automorfismo)

Um automorfismo sobre um grafo G é um isomorfismo de G em G. É fácil verificar que o conjunto dos automorfismos sobre G, denotado por $\mathrm{Aut}(G)$, forma um grupo de permutações sobre $V(G)$ para a operação usual de composição $\circ$. Dizemos que um grafo G é assimétrico se o grupo $(\mathrm{Aut}(G), \circ)$ é composto apenas pela permutação identidade.

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)

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

Notação

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

Propriedades sobre a translação

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

Propriedade (Translação fraca)

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

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

Propriedades sobre a translação

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

Propriedade (Translação fraca)

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

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

Propriedade (Translação forte)

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

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

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-$2t$)

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

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

Mais propriedades

- 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.

Mais propriedades

- 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.

Mais propriedades

- 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.