Exercícios

Prof. André Vignatti

Exercício 1. Jogamos uma moeda não viciada dez vezes. Encontre a probabilidade dos seguintes eventos:

(a) O número de caras e o número de coroas serem iguais.

(b) Há mais caras que coroas.

(c) a i-ésima jogada e a $(11 - i)$-ésima jogada são iguais, para $i = 1, \ldots, 5$.

Exercício 2. Dados números inteiros x, y, N denotamos por $x \equiv y \bmod N$ o fato de N dividir $x - y$. Por exemplo, $253 \equiv 13 \bmod 60$ pois $253 - 13$ é múltiplo de 60. Com base nesta definição, o *Pequeno Teorema de Fermat* é enunciado como:

Teorema 1. Se N é um número primo, então para todo $1 \leq a < N$,

$$a^{N-1} \equiv 1 \bmod N$$

O Pequeno Teorema de Fermat pode ser usado diretamente para obter o seguinte algoritmo:

Algoritmo primo(N)
- Escolha aleatoriamente um inteiro $a < N$
- **se** a^{N-1} *mod* $N = 1$ **então retorna** SIM
- **senão retorna** NÃO

(a) Reescreva o enunciado do Pequeno Teorema de Fermat usando a *contrapositiva* da implicação (dada uma implicação $a \Rightarrow b$, a contrapositiva é $\overline{b} \Rightarrow \overline{a}$. Ambas implicações são equivalentes do ponto de vista da lógica).

(b) Qual o problema com a corretude do algoritmo acima? (Dica: releia com atenção o pequeno teorema de Fermat. Ler sua contrapositiva pode ajudar também)

(c) Considere o seguinte teorema:

Teorema 2. [1] Se N não é primo, então $a^{N-1} \equiv 1 \bmod N$ para no máximo $(N-1)/2$ valores de $a < N$.

Qual a probabilidade do algoritmo acima retornar SIM quando N é primo? Qual a probabilidade do algoritmo acima retornar SIM quando N não é primo?

[1] Esse teorema é verdadeiro para *quase* todos os números, com exceção dos *números de Carmichael*, que são números raros. Mais informações em CLRS, Cap. 31

Exercício 3. Considere o seguinte teorema:

Teorema 3 (Teorema de Lagrange dos números primos)**.** Seja $\pi(n)$ o número de primos $\leq n$. Então

$$\lim_{n \to \infty} \frac{\pi(n)}{n / \ln n} = 1.$$

(a) Dado um número inteiro aleatoriamente escolhido, qual a probabilidade deste número ser primo? Qual a probabilidade de não ser?

(b) Dados 2 números inteiros aleatoriamente escolhidos, qual a probabilidade de nenhum deles ser primo? E para k números?

(c) Quantos números aleatórios deve-se obter para que, com probabilidade maior ou igual a $1 - 1/n$, pelo menos um seja primo? (Dica: será útil a desigualdade $(1 - 1/x)^x \leq 1/e$)

Exercício 4. Uma dada função *hash* $h : \mathbb{N} \to [1..n]$ mapeia *aleatoriamente* para $[1..n]$.

(a) Qual a probabilidade de k números serem mapeados na mesma posição?

(b) Qual a probabilidade de k números serem mapeados em posições distintas?

Exercício 5. Considere um algoritmo aleatorizado que tem *sucesso* (ou seja, devolve a resposta correta) com probabilidade $\frac{2}{3}$.

(a) Qual a probabilidade de *falha* do algoritmo? Explique.

(b) Suponha que o algoritmo foi executado k vezes. Qual a probabilidade de *todas* as execuções falharem? Explique.

(c) Quantas execuções devem ser feitas para que a probabilidade de falha seja no máximo $\frac{1}{n}$? Explique.