

Tópicos de Análise de Algoritmos

Parte destes slides são adaptações de slides
do Prof. Paulo Feofiloff e do Prof. José Coelho de Pina.

Probabilidade e Computação

MU 1.1 e KT 13.1

MU: M. Mitzenmacher e E. Upfal, Probability and Computing, Randomized Algorithms and Probabilistic Analysis, 2005.

Um pouco de probabilidade

$(S, \Pr)$ **espaço de probabilidade**

S = conjunto finito (**eventos elementares**)

$\Pr\{\cdot\}$ = (**distribuição de probabilidades**) função de S
em $[0, 1]$ tal que $\sum_{s \in S} \Pr\{s\} = 1$.

Usa-se $\Pr\{U\}$ como abreviatura de $\sum_{u \in U} \Pr\{u\}$.

Então, para R e $T \subseteq S$ com $R \cap T = \emptyset$,
vale que $\Pr\{R \cup T\} = \Pr\{R\} + \Pr\{T\}$.

Um pouco de probabilidade

$(S, \Pr)$ **espaço de probabilidade**

S = conjunto finito (**eventos elementares**)

$\Pr\{\cdot\}$ = (**distribuição de probabilidades**) função de S
em $[0, 1]$ tal que $\sum_{s \in S} \Pr\{s\} = 1$.

Usa-se $\Pr\{U\}$ como abreviatura de $\sum_{u \in U} \Pr\{u\}$.

Então, para R e $T \subseteq S$ com $R \cap T = \emptyset$,
vale que $\Pr\{R \cup T\} = \Pr\{R\} + \Pr\{T\}$.

Um **evento** é um subconjunto de S .

Mais um pouco de probabilidade

Uma **variável aleatória** é uma função numérica definida sobre os eventos elementares.

Mais um pouco de probabilidade

Uma **variável aleatória** é uma função numérica definida sobre os eventos elementares.

Para uma variável aleatória X :

“ $X = k$ ” é uma abreviatura do evento $\{s \in S : X(s) = k\}$.

Esperança $E[X]$ de uma variável aleatória X

$$E[X] = \sum_{k \in X(S)} k \cdot \Pr\{X = k\} = \sum_{s \in S} X(s) \cdot \Pr\{s\}$$

Mais um pouco de probabilidade

Uma **variável aleatória** é uma função numérica definida sobre os eventos elementares.

Para uma variável aleatória X :

“ $X = k$ ” é uma abreviatura do evento $\{s \in S : X(s) = k\}$.

Esperança $E[X]$ de uma variável aleatória X

$$E[X] = \sum_{k \in X(S)} k \cdot \Pr\{X = k\} = \sum_{s \in S} X(s) \cdot \Pr\{s\}$$

Linearidade da esperança: $E[\alpha X + Y] = \alpha E[X] + E[Y]$

Exemplo

Problema: Dados $(a_0, \dots, a_{d-1})$ e $\{r_1, \dots, r_d\}$,
decidir se o polinômio $F(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$
e o polinômio $G(x) = (x - r_1) \cdots (x - r_d)$ são o mesmo polinômio.

Exemplo

Problema: Dados $(a_0, \dots, a_{d-1})$ e $\{r_1, \dots, r_d\}$,
decidir se o polinômio $F(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$
e o polinômio $G(x) = (x - r_1) \cdots (x - r_d)$ são o mesmo polinômio.

O termo dominante de $F(x)$ e $G(x)$ tem coeficiente 1, e
 $F(x)$ é dado por seus coeficientes enquanto que
 $G(x)$ é dado por suas raízes.

Exemplo

Problema: Dados $(a_0, \dots, a_{d-1})$ e $\{r_1, \dots, r_d\}$, decidir se o polinômio $F(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$ e o polinômio $G(x) = (x - r_1) \cdots (x - r_d)$ são o mesmo polinômio.

O termo dominante de $F(x)$ e $G(x)$ tem coeficiente 1, e $F(x)$ é dado por seus coeficientes enquanto que $G(x)$ é dado por suas raízes.

IGUAIS-1 (A, R, d)

- 1 $t \leftarrow \text{RANDOM}(1, 100d)$
- 2 se $F(t) = G(t)$
- 3 então devolva verdade
- 4 senão devolva falso

Os polinômios F e G são iguais?

IGUAIS-1 (A, R, d)

1 $t \leftarrow \text{RANDOM}(1, 100d)$

2 se $F(t) = G(t)$

3 então devolva verdade

4 senão devolva falso

O que pode acontecer?

Os polinômios F e G são iguais?

IGUAIS-1 (A, R, d)

1 $t \leftarrow \text{RANDOM}(1, 100d)$

2 se $F(t) = G(t)$

3 então devolva verdade

4 senão devolva falso

O que pode acontecer?

Se $F = G$, a resposta está sempre certa.

Os polinômios F e G são iguais?

IGUAIS-1 (A, R, d)

1 $t \leftarrow \text{RANDOM}(1, 100d)$

2 se $F(t) = G(t)$

3 então devolva verdade

4 senão devolva falso

O que pode acontecer?

Se $F = G$, a resposta está sempre certa.

Se $F \neq G$, a resposta pode estar errada.

Os polinômios F e G são iguais?

IGUAIS-1 (A, R, d)

1 $t \leftarrow \text{RANDOM}(1, 100d)$

2 se $F(t) = G(t)$

3 então devolva verdade

4 senão devolva falso

O que pode acontecer?

Se $F = G$, a resposta está sempre certa.

Se $F \neq G$, a resposta pode estar errada.

Erra se $F \neq G$ e t for uma das raízes do polinômio $F - G$.

Com que probabilidade isso acontece?

Os polinômios F e G são iguais?

IGUAIS-1 (A, R, d)

- 1 $t \leftarrow \text{RANDOM}(1, 100d)$
- 2 se $F(t) = G(t)$
- 3 então devolva verdade
- 4 senão devolva falso

O que pode acontecer?

Se $F = G$, a resposta está sempre certa.

Se $F \neq G$, a resposta pode estar errada.

Erra se $F \neq G$ e t for uma das raízes do polinômio $F - G$.

Com que probabilidade isso acontece?

$$\Pr \{\text{resposta errada}\} \leq \frac{d}{100d} = \frac{1}{100}.$$

Algoritmos Monte-Carlo

IGUAIS-1 (A, R, d)

- 1 $t \leftarrow \text{RANDOM}(1, 100d)$
- 2 se $F(t) = G(t)$
- 3 então devolva verdade
- 4 senão devolva falso

Este é um algoritmo Monte-Carlo:
ele pode dar uma resposta errada, ou falhar.

Algoritmos Monte-Carlo

```
IGUAIS-1 ( $A, R, d$ )  
1    $t \leftarrow \text{RANDOM}(1, 100d)$   
2   se  $F(t) = G(t)$   
3       então devolva verdade  
4       senão devolva falso
```

Este é um algoritmo **Monte-Carlo**:
ele pode dar uma resposta errada, ou falhar.

IGUAIS- k : Execute **IGUAIS-1** k vezes, e devolva **verdade**
apenas se todas as execuções devolverem **verdade**.

Algoritmos Monte-Carlo

IGUAIS-1 (A, R, d)

- 1 $t \leftarrow \text{RANDOM}(1, 100d)$
- 2 se $F(t) = G(t)$
- 3 então devolva verdade
- 4 senão devolva falso

Este é um algoritmo **Monte-Carlo**:
ele pode dar uma resposta errada, ou falhar.

IGUAIS- k : Execute IGUAIS-1 k vezes, e devolva verdade apenas se todas as execuções devolverem verdade.

Se as execuções são **independentes**,

$$\Pr \{\text{resposta errada}\} \leq \left(\frac{1}{100}\right)^k.$$

Um pouco de probabilidade

Eventos E e F são independentes se

$$\Pr\{E \cap F\} = \Pr\{E\} \cdot \Pr\{F\}.$$

Um pouco de probabilidade

Eventos E e F são independentes se

$$\Pr\{E \cap F\} = \Pr\{E\} \cdot \Pr\{F\}.$$

Probabilidade condicional:

$$\Pr\{E|F\} = \frac{\Pr\{E \cap F\}}{\Pr\{F\}}.$$

Um pouco de probabilidade

Eventos E e F são independentes se

$$\Pr\{E \cap F\} = \Pr\{E\} \cdot \Pr\{F\}.$$

Probabilidade condicional:

$$\Pr\{E|F\} = \frac{\Pr\{E \cap F\}}{\Pr\{F\}}.$$

Se E e F são independentes,

$$\Pr\{E|F\} = \Pr\{E\}.$$

Problema de contenção

Processos $P_1, \dots, P_n$ querem acessar um mesmo recurso.

Problema de contenção

Processos $P_1, \dots, P_n$ querem acessar um mesmo recurso.

Um acesso por vez. Acessos ocorrem em rodadas.

P_i ganha acesso apenas se for o único na rodada.

Problema de contenção

Processos $P_1, \dots, P_n$ querem acessar um mesmo recurso.

Um acesso por vez. Acessos ocorrem em rodadas.

P_i ganha acesso apenas se for o único na rodada.

(A Ethernet funciona assim.)

Problema de contenção

Processos $P_1, \dots, P_n$ querem acessar um mesmo recurso.

Um acesso por vez. Acessos ocorrem em rodadas.

P_i ganha acesso apenas se for o único na rodada.

(A Ethernet funciona assim.)

Algoritmo da espera aleatória: cada processo P_i acessa na próxima rodada com probabilidade p_i .

Problema de contenção

Processos $P_1, \dots, P_n$ querem acessar um mesmo recurso.

Um acesso por vez. Acessos ocorrem em rodadas.

P_i ganha acesso apenas se for o único na rodada.

(A Ethernet funciona assim.)

Algoritmo da espera aleatória: cada processo P_i acessa na próxima rodada com probabilidade p .

Dá para garantir que todo mundo acessa o recurso?

Problema de contenção

Processos $P_1, \dots, P_n$ querem acessar um mesmo recurso.

Um acesso por vez. Acessos ocorrem em rodadas.

P_i ganha acesso apenas se for o único na rodada.

(A Ethernet funciona assim.)

Algoritmo da espera aleatória: cada processo P_i acessa na próxima rodada com probabilidade p .

Dá para garantir que todo mundo acessa o recurso?

Demora muito?

Problema de contenção

Algoritmo da espera aleatória: cada processo P_i acessa na próxima rodada com probabilidade p .

Eventos interessantes:

$A(i, t)$: P_i tenta acessar no instante t
 $\Pr\{A(i, t)\} = p$

Problema de contenção

Algoritmo da espera aleatória: cada processo P_i acessa na próxima rodada com probabilidade p .

Eventos interessantes:

$A(i, t)$: P_i tenta acessar no instante t

$$\Pr\{A(i, t)\} = p$$

$S(i, t)$: P_i consegue acesso no instante t (sucesso)

$$S(i, t) = A(i, t) \cap \bigcap_{j \neq i} \overline{A(j, t)}$$

Evento $\bar{X}$ é o evento complementar ao evento X .

Problema de contenção

Algoritmo da espera aleatória: cada processo P_i acessa na próxima rodada com probabilidade p .

Eventos interessantes:

$A(i, t)$: P_i tenta acessar no instante t

$$\Pr\{A(i, t)\} = p$$

$S(i, t)$: P_i consegue acesso no instante t (sucesso)

$$S(i, t) = A(i, t) \cap \bigcap_{j \neq i} \overline{A(j, t)}$$

Evento $\bar{X}$ é o evento complementar ao evento X .

Pela independência, $\Pr\{S(i, t)\} = p(1 - p)^{n-1}$.

Gostaríamos de maximizar essa probabilidade.

Probabilidade de sucesso

Para maximizar $\Pr \{S(i, t)\} = p(1 - p)^{n-1}$,
calculamos quando a derivada (em p) se anula:

$$(1 - p)^{n-1} - (n - 1)(1 - p)^{n-2}p = 0$$

que ocorre quando $(1 - p) - (n - 1)p = 0$,
ou seja, quando $p = 1/n$.

Probabilidade de sucesso

Para maximizar $\Pr\{S(i, t)\} = p(1 - p)^{n-1}$,
calculamos quando a derivada (em p) se anula:

$$(1 - p)^{n-1} - (n - 1)(1 - p)^{n-2}p = 0$$

que ocorre quando $(1 - p) - (n - 1)p = 0$,
ou seja, quando $p = 1/n$.

Para tal valor de p , $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1}$.

Probabilidade de sucesso

Para maximizar $\Pr \{S(i, t)\} = p(1 - p)^{n-1}$,
calculamos quando a derivada (em p) se anula:

$$(1 - p)^{n-1} - (n - 1)(1 - p)^{n-2}p = 0$$

que ocorre quando $(1 - p) - (n - 1)p = 0$,
ou seja, quando $p = 1/n$.

Para tal valor de p , $\Pr \{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1}$.

Sabe-se que, para $n \geq 2$,

$$\frac{1}{4} \leq (1 - \frac{1}{n})^n < \frac{1}{e} < (1 - \frac{1}{n})^{n-1} \leq \frac{1}{2}.$$

Breve revisão

Lembre-se que $e^x \geq 1 + x$ para todo x real. (Desigualdade estrita se $x \neq 0$.)

Breve revisão

Lembre-se que $e^x \geq 1 + x$ para todo x real. (Desigualdade estrita se $x \neq 0$.)

Disso deduzimos que

$$e^{-1/n} > 1 - \frac{1}{n} \text{ e portanto } \frac{1}{e} > \left(1 - \frac{1}{n}\right)^n \text{ e}$$

Breve revisão

Lembre-se que $e^x \geq 1 + x$ para todo x real. (Desigualdade estrita se $x \neq 0$.)

Disso deduzimos que

$$e^{-1/n} > 1 - \frac{1}{n} \text{ e portanto } \frac{1}{e} > \left(1 - \frac{1}{n}\right)^n \text{ e}$$

$$e^{1/(n-1)} > 1 + \frac{1}{n-1} = \frac{n}{n-1} \text{ se } n \geq 2 \text{ e portanto}$$

$$e^{-1/(n-1)} < \frac{n-1}{n} = 1 - \frac{1}{n}, \text{ logo } \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1}.$$

Breve revisão

Lembre-se que $e^x \geq 1 + x$ para todo x real. (Desigualdade estrita se $x \neq 0$.)

Disso deduzimos que

$$e^{-1/n} > 1 - \frac{1}{n} \text{ e portanto } \frac{1}{e} > \left(1 - \frac{1}{n}\right)^n \text{ e}$$

$$e^{1/(n-1)} > 1 + \frac{1}{n-1} = \frac{n}{n-1} \text{ se } n \geq 2 \text{ e portanto}$$

$$e^{-1/(n-1)} < \frac{n-1}{n} = 1 - \frac{1}{n}, \text{ logo } \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1}.$$

Ademais,

$$\lim_{n \rightarrow \infty} \left(1 - \frac{1}{n}\right)^n = \frac{1}{e} \quad \left(\text{vai de } \frac{1}{4} \text{ para } \frac{1}{e} \text{ monotonicamente}\right)$$

$$\lim_{n \rightarrow \infty} \left(1 - \frac{1}{n}\right)^{n-1} = \frac{1}{e} \quad \left(\text{vai de } \frac{1}{2} \text{ para } \frac{1}{e} \text{ monotonicamente}\right)$$

Breve revisão

Lembre-se que $e^x \geq 1 + x$ para todo x real. (Desigualdade estrita se $x \neq 0$.)

Disso deduzimos que

$$e^{-1/n} > 1 - \frac{1}{n} \text{ e portanto } \frac{1}{e} > \left(1 - \frac{1}{n}\right)^n \text{ e}$$

$$e^{1/(n-1)} > 1 + \frac{1}{n-1} = \frac{n}{n-1} \text{ se } n \geq 2 \text{ e portanto}$$

$$e^{-1/(n-1)} < \frac{n-1}{n} = 1 - \frac{1}{n}, \text{ logo } \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1}.$$

Ademais,

$$\lim_{n \rightarrow \infty} \left(1 - \frac{1}{n}\right)^n = \frac{1}{e} \quad (\text{vai de } \frac{1}{4} \text{ para } \frac{1}{e} \text{ monotonicamente})$$

$$\lim_{n \rightarrow \infty} \left(1 - \frac{1}{n}\right)^{n-1} = \frac{1}{e} \quad (\text{vai de } \frac{1}{2} \text{ para } \frac{1}{e} \text{ monotonicamente})$$

Logo de fato para $n \geq 2$,

$$\frac{1}{4} \leq \left(1 - \frac{1}{n}\right)^n < \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1} \leq \frac{1}{2}.$$

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1}$.

Sabe-se que, para $n \geq 2$,

$$\frac{1}{4} \leq \left(1 - \frac{1}{n}\right)^n < \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1} \leq \frac{1}{2}.$$

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1}$.

Sabe-se que, para $n \geq 2$,

$$\frac{1}{4} \leq \left(1 - \frac{1}{n}\right)^n < \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1} \leq \frac{1}{2}.$$

Portanto $\frac{1}{en} < \Pr\{S(i, t)\} \leq \frac{1}{2n}$.

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1}$.

Sabe-se que, para $n \geq 2$,

$$\frac{1}{4} \leq \left(1 - \frac{1}{n}\right)^n < \frac{1}{e} < \left(1 - \frac{1}{n}\right)^{n-1} \leq \frac{1}{2}.$$

Portanto $\frac{1}{en} < \Pr\{S(i, t)\} \leq \frac{1}{2n}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

$$\begin{aligned}\Pr\{F(i, t)\} &= \prod_{j=1}^t (1 - \Pr\{S(i, j)\}) \\ &= \left(1 - \frac{1}{n}(1 - \frac{1}{n})^{n-1}\right)^t < \left(1 - \frac{1}{en}\right)^t\end{aligned}$$

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

$$\Pr\{F(i, t)\} = \prod_{j=1}^t (1 - \Pr\{S(i, j)\}) < \left(1 - \frac{1}{en}\right)^t.$$

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

$$\Pr\{F(i, t)\} = \prod_{j=1}^t (1 - \Pr\{S(i, j)\}) < \left(1 - \frac{1}{en}\right)^t.$$

Como $e^x \geq 1 + x$ para todo x real, $e^{-\frac{1}{en}} \geq 1 - \frac{1}{en}$.

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

$$\Pr\{F(i, t)\} = \prod_{j=1}^t (1 - \Pr\{S(i, j)\}) < (1 - \frac{1}{en})^t.$$

Como $e^x \geq 1 + x$ para todo x real, $e^{-\frac{1}{en}} \geq 1 - \frac{1}{en}$.

Assim sendo, para $t = \lceil en \rceil$, $\Pr\{F(i, t)\} < (1 - \frac{1}{en})^{en} \leq \frac{1}{e}$.

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

$$\Pr\{F(i, t)\} = \prod_{j=1}^t (1 - \Pr\{S(i, j)\}) < (1 - \frac{1}{en})^t.$$

Como $e^x \geq 1 + x$ para todo x real, $e^{-\frac{1}{en}} \geq 1 - \frac{1}{en}$.

Assim sendo, para $t = \lceil en \rceil$, $\Pr\{F(i, t)\} < (1 - \frac{1}{en})^{en} \leq \frac{1}{e}$.

E se $t = \lceil en(c \ln n) \rceil$, $\Pr\{F(i, t)\} < (\frac{1}{e})^{c \ln n} = \frac{1}{n^c}$.

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

$$\Pr\{F(i, t)\} = \prod_{j=1}^t (1 - \Pr\{S(i, j)\}) < (1 - \frac{1}{en})^t.$$

Como $e^x \geq 1 + x$ para todo x real, $e^{-\frac{1}{en}} \geq 1 - \frac{1}{en}$.

Assim sendo, para $t = \lceil en \rceil$, $\Pr\{F(i, t)\} < (1 - \frac{1}{en})^{en} \leq \frac{1}{e}$.

E se $t = \lceil en(c \ln n) \rceil$, $\Pr\{F(i, t)\} < (\frac{1}{e})^{c \ln n} = \frac{1}{n^c}$.

Ou seja, para $t = \Theta(n \lg n)$, a probabilidade de um processo não acessar o recurso após t rodadas é polinomialmente pequena.

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

Se $t = \lceil en(c \lg n) \rceil$,

$$\Pr\{F(i, t)\} < \left(\frac{1}{e}\right)^{c \lg n} = \frac{1}{n^c}.$$

Probabilidade de falha

Para $p = 1/n$, $\Pr\{S(i, t)\} = \frac{1}{n}(1 - \frac{1}{n})^{n-1} > \frac{1}{en}$.

$F(i, t)$: P_i não acessa o recurso até o momento t (inclusive)

Se $t = \lceil en(c \lg n) \rceil$,

$$\Pr\{F(i, t)\} < \left(\frac{1}{e}\right)^{c \lg n} = \frac{1}{n^c}.$$

Mais do que isso...

a probabilidade de algum processo falhar é $\Pr\{\cup_i F(i, t)\}$ e

$$\Pr\{\cup_i F(i, t)\} \leq \sum_i \Pr\{F(i, t)\} < n \frac{1}{n^c} = \frac{1}{n^{c-1}}.$$

Protocolo Exponential Backoff

Placa de rede Ethernet: enquanto transmite um pacote por um canal, lê a transmissão, e verifica se o sinal transmitido coincide com o enviado. Caso haja divergência, há **colisão**, ou seja, um outro pacote está sendo transmitido pelo mesmo canal. Neste caso, a placa aborta a transmissão e envia pelo canal um sinal específico que indica colisão.

Algoritmo de exponential backoff:

Transmite e testa colisão.

$c \leftarrow 0$ ▷ número de colisões

Enquanto houver colisão faça

Interrompe a transmissão e envia o sinal de colisão.

$c \leftarrow c + 1$

$k \leftarrow \text{RANDOM}(0, 2^c - 1)$

Retransmite e testa colisão após $k \cdot 51\mu s$.

▷ 51 pode ser trocado por um positivo qualquer