Verificando Igualdade de Polinômios

Prof. André Vignatti

Dados $F(x)$ e $G(x)$ dois polinômios de grau d dados como:

$$F(x) = (x+1)(x-2)(x+3)(x-4)(x+5)(x-6)$$
$$G(x) = x^6 - 7x^3 + 25$$

Como saber se $F(x) \equiv G(x)$?

- Solução natural em $O(d^2)$.

Considere o seguinte algoritmo aleatorizado:

ALGORITMO VP
1. Escolha $r \in \{1, \ldots, 100d\}$ aleatoriamente.
2. Verifique se $F(r)$ é igual a $G(r)$, em tempo $O(d)$.
3. Se $F(r) = G(r)$ o algoritmo responde SIM;
4. caso contrário, o algoritmo responde NÃO.

VP executa em tempo $O(d)$. Quando erra?

- Erra quando r é raiz de $H(x) = 0$, onde $H(x) = F(x) - G(x)$.

$H(x)$ tem grau $\leq d \implies H(x)$ tem $\leq d$ raízes. Assim, a probabilidade de *VP* errar é:

$$\Pr(\textit{VP errar}) \leq \frac{d}{100d} = \frac{1}{100}$$

Vamos formalizar matematicamente essa conversa.

Definição. Um **espaço de probabilidade discreto** tem 3 componentes:

- Um conjunto Ω, chamado de *espaço amostral*
- O conjunto $\mathcal{F}$ de todos subconjuntos de Ω, cada $E \in \mathcal{F}$ é chamado de *evento*.
- Função de probabilidade $\Pr : \mathcal{F} \to \mathbb{R}^+$

$E \in \mathcal{F}$ é dito ser simples ou elementar se $|E| = 1$

Exemplo. Se $\Omega = \{1, 2, 3\}$ então

$$\mathcal{F} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

$\{1, 2\}$ é um evento, $\{3\}$ é um evento simples, pois $|\{3\}| = 1$.

Definição. Uma *função de probabilidade* é uma função $\Pr : \mathcal{F} \to \mathbb{R}^+$ t.q.

- $\forall E \in \mathcal{F}$ temos $0 \leq \Pr(E) \leq 1$
- $\Pr(\Omega) = 1$
- Para toda seqüência de eventos **disjuntos** $E_1, E_2, \ldots$, temos

$$\Pr(E_1 \cup E_2 \ldots) = \Pr(E_1) + \Pr(E_2) + \ldots$$

Exemplo. Na verificação de polinômios

- $\Omega = \{1, \ldots, 100d\}$
- Cada escolha de $r = i$ é o evento simples $E_i = \{i\}$
- r é escolhido uniformemente $\Rightarrow \Pr(E_i) = \Pr(E_j)$, $\forall i, j$.
- $\Pr(\Omega) = 1 \Rightarrow \Pr(E_i) = \frac{1}{100d}$.

Exemplo. Considere o lance de um dado de 6 lados.

- $\Omega = \{1, \ldots, 6\}$

Exemplo de eventos que podemos considerar

- E' = Evento do dado mostrar número par.
- E'' = Evento do dado mostrar número menor ou igual a 3.
- E''' = Evento do dado mostrar número primo.

Lema. Para eventos E_1 e E_2 temos

$$\Pr(E_1 \cup E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \cap E_2)$$

Demonstração. (Só dar ideia com uma figura) □

Corolário. Para eventos E_1 e E_2 temos

$$\Pr(E_1 \cup E_2) \leq \Pr(E_1) + \Pr(E_2)$$

Lema. Dados eventos $E_1, E_2, \ldots$ temos

$$\Pr(\bigcup_{i \geq 1} E_i) \leq \sum_{i \geq 1} \Pr(E_i)$$

Demonstração. (Exercício: indução) □

Definição. Dois eventos E e F são ditos serem independentes se

$$\Pr(E \cap F) = \Pr(E) \cdot \Pr(F).$$

Suposição computacional: obter um número aleatório gasta $\Theta(1)$.

Como diminuir a probabilidade de erro para $\frac{1}{\text{1bilhão}}$?

- Primeira tentativa: aumentar o espaço amostral
  - Faixa de valores limitada pela precisão da máquina
  - Sorteio do r pode não levar tempo constante!
- Segunda tentativa: executar várias vezes o algoritmo

> ALGORITMO VP_k
> 1. Execute o algoritmo VP k vezes (com reposição).
> 2. Devolve NÃO se em uma das k execuções o VP devolve não;
> 3. caso contrário, devolve SIM.

- Seja E_i o evento do algoritmo escolher raiz de $F(x) - G(x) = 0$ na i-ésima execução de VP.
- Os eventos E_i são mutuamente independentes.
- A probabilidade do algoritmo falhar é:

$$\Pr(E_1 \cap E_2 \cap \ldots \cap E_k) = \Pi_{i=1}^{k} \Pr(E_i) \leq \Pi_{i=1}^{k} \frac{d}{100d} \leq \left(\frac{1}{100}\right)^k$$

> **Filosofando...**
> - Parece errado um algoritmo que pode dar a resposta errada!
>
> **Estamos acostumados com**:
> - algoritmos 100% corretos.
> - otimizar o tempo de execução.
> - sacrificar tempo de execução gastanto menos memória.
>
> Abra sua cabeça! **Porque não pensar em**:
> - algoritmo $<$ 100% corretos?
> - otimizar a corretude?
> - sacrificar tempo de execução aumentando a corretude?