Análise de Algoritmos

Gabarito da Terceira Prova

Análise de Algoritmos Algébricos e Noções de Teoria de Complexidade

Instituto de Ciências Exatas, Universidade de Brasília
17 de junho de 2009
Prof. Mauricio Ayala-Rincón

Algoritmos Algébricos

1. (40 pontos) O algoritmo de Karatsuba para multiplicação de polinômios está baseado num aprimoramento da multiplicação de polinômios lineares:

$$(ax+b)(cx+d) = acx^2 + (ad+cb)x + bd$$

Os coeficientes do polinômio resultante podem ser computados da seguinte maneira:

$$\text{compute primeiro } \ ac \quad \text{e} \quad bd \quad \text{e} \quad u = (a+b)(c+d)$$

logo, o coeficiente da parte linear pode ser computado como:

$$u - ac - bd$$

Para a computação direta (definicional) desta multiplicação de polinômios, precisamos quatro multiplicações e uma adição. Com o mecanismo proposto, precisamos unicamente três multiplicações e quatro adições.

O mecanismo estende-se para polinômios de maior grau como segue.

Suponha $\boldsymbol{n = 2^k}$ e sejam f e g polinômios de grau $n-1$. f e g podem-se decompor como segue

$$f = F_1 x^{n/2} + F_0 \quad \text{e} \quad g = G_1 x^{n/2} + G_0$$

onde F_i e G_i, $i = 0, 1$, são polinômios de graus adequados ($\leq n/2 - 1$).

fg pode-se, então, expressar como

$$fg = F_1 G_1 x^n + (F_0 G_1 + F_1 G_0) x^{n/2} + F_0 G_0$$

Neste ponto, utiliza-se o mecanismo acima descrito, recursivamente.

O **algoritmo de Karatsuba** para multiplicação de polinômios é então descrito com os quatro passos apresentados na tabela embaixo.

Passo 1:	Se $n = 1$ retorne $f \cdot g \in \mathbb{R}$;
Passo 2:	seja $f = F_1 x^{n/2} + F_0$ e $g = G_1 x^{n/2} + G_0$, com F_1, F_0, G_1, G_0 polinômios de grau $< n/2$;
Passo 3:	compute F_0G_0, F_1G_1 e $(F_0 + F_1)(G_0 + G_1)$ recursivamente;
Passo 4:	retorne $F_1G_1x^n + ((F_0 + F_1)(G_0 + G_1) - F_0G_0 - F_1G_1)x^{n/2} + F_0G_0$.

Tabela 1: Algoritmo de Karatsuba para multiplicação de polinômios

(a) (10 pontos) **Explique brevemente (máximo 30 palavras)** por que a relação de recurrência para o trabalho realizado pelo algoritmo de Karatsuba é da forma:

$$T(n) = \begin{cases} 1, & n = 1 \\ 3T(n/2) + 4n, & n > 1 \end{cases}$$

R/ Para $n = 1$, multiplicam-se polinômios de grau zero com uma multiplicação: $T(1) = 1$. Para $n > 1$, realizam-se três chamadas recursivas para polinômios de grau $n/2 - 1$, o que explica o fator $3T(n/2)$. Adicionalmente, realizam-se quatro sumas de polinômios, o que explica o fator $4n$.

(b) (30 pontos) **Calcule** $T(n)$. Suponha que $\boldsymbol{n = 2^k}$, para algum $k \in \mathbb{N}$.
R/

$$\begin{aligned} T(n) &= 3^k T(\frac{n}{2^k}) + \sum_{i=0}^{k-1} 3^i (4\frac{n}{2^i}) \\ &= 3^k + 4n \sum_{i=0}^{k-1} (\frac{3}{2})^i \\ &= 3^k + 4n(\frac{(3/2)^k - 1}{(3/2) - 1}) \\ &= 3^k + 8n((\frac{3}{2})^k - 1) \\ &= 3^k + 8\,3^k - 8n \\ &= 9\,3^k - 8n \\ &= 9n^{log_2 3} - 8n \\ &\in \Theta(n^{log_2 3}) \end{aligned}$$

2. (40 pontos) A transformação discreta de Fourier (DFT) é um operador que transforma um n-vetor $A = (a_0, \ldots, a_{n-1})^t$ no campo $\mathbb{C}$, no n-vetor

$$F_n \times A$$

sendo F_n a $n \times n$-matriz definida com base na n-raiz primitiva da unidade principal,

ω, como segue:

$$F_n := \begin{pmatrix} \omega^0 & \omega^0 & \dots & \omega^0 \\ \omega^0 & \omega^1 & \dots & \omega^{n-1} \\ \omega^0 & \omega^2 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & & \vdots \\ \omega^0 & \omega^{n-1} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

Dessa forma, $F_n \times A$ corresponde ao vetor de avaliações do polinômio $P_A = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$ nas n n-raízes da unidade $\omega^0, \omega, \omega^2, \ldots \omega^{n-1}$:

$$F_n \times A = (\ P_A(\omega^0), P_A(\omega), P_A(\omega^2), \ldots, P_A(\omega^{n-1})\ )^t$$

A computação direta (definicional) desse operador realiza n^2 multiplicações e $n(n-1)$ adições em $\mathbb{C}$, mas mecanismos mais eficientes, como a transformação rápida de Fourier (FFT), permitem computações sub-quadráticas.

Em particular, FFT está baseada em propriedades das n n-raízes complexas e no fato de que, para n par o polinômio P_A pode ser avaliado em x e em $-x$ como

$$P_A(\pm x) = P_A^{par}(x^2) \pm x P_A^{impar}(x^2)$$

onde

$$P_A^{par}(z) = a_0 + a_2 z + \ldots + a_{n-2} z^{n/2-1} \quad \text{e} \quad P_A^{impar}(z) = a_1 + a_3 z + \ldots + a_{n-1} z^{n/2-1}$$

Para n par, as propriedades utilizadas das n n-raízes da unidade $\omega, \omega^2, \ldots \omega^n$ são as seguintes:

$$\omega^{n/2+1} = -\omega;\ \omega^{n/2+2} = -\omega^2;\ \ldots\ \omega^n = -\omega^{n/2} (= 1)$$

e

$$(\omega^{n/2+1})^2 = (\omega)^2 = \omega^2;\ (\omega^{n/2+2})^2 = (\omega^2)^2 = \omega^4;\ \ldots\ (\omega^n)^2 = (\omega^{n/2})^2 = \omega^{2n} (= 1)$$

Dessa maneira, $F_n \times A$, ou equivalentemente a avaliação do polinômio P_A nas n-raízes $\omega, \omega^2, \ldots, \omega^n$, pode ser realizado avaliando os polinômios P_A^{par} e P_A^{impar} nas $n/2$-raízes da unidade $\omega^2, \omega^4, \ldots, \omega^{2n}$, ou equivalentemente computando $F_{n/2} \times A_{par}$ e $F_{n/2} \times A_{impar}$, onde A_{par} e A_{impar} são os $n/2$-vetores de componentes pares e ímpares de A, respectivamente. Finalmente, obtém-se:

$$\begin{aligned} P_A(\pm\omega) &= P_A^{par}(\omega^2) \pm \omega P_A^{impar}(\omega^2) \\ P_A(\pm\omega^2) &= P_A^{par}(\omega^4) \pm \omega^2 P_A^{impar}(\omega^4) \\ &\vdots \\ P_A(\pm\omega^{n/2}) &= P_A^{par}(\omega^n) \pm \omega^{n/2} P_A^{impar}(\omega^n) \end{aligned}$$

Assim, para computar $F_n \times A$ computa-se $F_{n/2} \times A_{par}$ e $F_{n/2} \times A_{impar}$, sendo que estes últimos são computados recursivamente, o que implica uma equação de recurrência para o número de multiplicações entre complexos, M, da seguinte forma

$$M(n) = \begin{cases} 0, & n = 1 \\ 2M(n/2) + n/2, & n > 1 \end{cases}$$

(a) (10 pontos) **Explique brevemente (máximo 30 palavras)** por que a relação de recurrência para o trabalho realizado é dessa forma.

R/ Para $n = 1$, avalia-se um polinômio de grau zero em um: $M(1) = 0$. Para $n > 1$, realizam-se duas chamadas recursivas para DFT de tamanho $n/2$. Os valores obtidos são combinados com $n/2$ operações.

(b) (30 pontos) **Calcule** $M(n)$. Suponha que $\boldsymbol{n = 2^k}$, para algum $k \in \mathbb{N}$.

R/

$$\begin{aligned} M(n) &= 2^k M(\frac{n}{2^k}) + \sum_{i=0}^{k-1} 2^i (\frac{n}{2^{i+1}}) \\ &= 2^k\, 0 + \sum_{i=0}^{k-1} \frac{n}{2} \\ &= \frac{n}{2} k \\ &\in \Theta(n\, log_2 n) \end{aligned}$$

Noções de Teoria de Complexidade

3. (20 pontos) Seja Π um problema de decisão $\mathcal{NP}$-completo. **Demonstre** que se $\Pi \in \mathcal{P}$, então $\mathcal{NP} \subseteq \mathcal{P}$.

Siga o seguinte roteiro.

(a) (10 pontos) Seja $\Gamma \in \mathcal{NP}$. **Justifique brevemente (máximo dez palavras)** porque decidir qualquer instância x para o problema Γ se pode reduzir polinomialmente a decidir uma instância $T(x)$, obtida com algum mecanismo de transformação T, para o problema Π.

R/ Como Π é $\mathcal{NP}$-completo e $\Gamma \in \mathcal{NP}$, $\Gamma \leq_{\mathcal{P}} \Pi$ via T. Assim, respostas para x em Γ correspondem a respostas para $T(x)$ em Π.

(b) (10 pontos) Supondo que T pode ser computada com um algoritmo $\mathcal{A}_T$, polinomialmente limitado por um polinômio p, e que Π pode ser decidido por um algoritmo $\mathcal{A}_\Pi$, polinomialmente limitado por um polinômio q (veja a figura), **demostre** que qualquer entrada x do problema Γ pode ser decidida em tempo limitado polinomialmente.

Indique explicitamente qual o polinômio que limita o algoritmo de decisão para Γ, indicado na figura como $\mathcal{A}_\Gamma$.

R/ A computação de $\mathcal{A}_T$ com entrada x está limitada por $p(|x|)$. Por outra parte, como $T(x)$ é computada em tempo limitado por $p(|x|)$, $|T(x)| \leq p(|x|)$. Dessa forma, a computação de $\mathcal{A}_\Pi$ com entrada $T(x)$ estará limitada por $q(p(|x|)$. Em total, temos que $\mathcal{A}_\Gamma$ com entrada x estará limitada por $p(|x|) + q(p(|x|)$. Sempre que composição e suma de polinômios é um polinômio, temos que Γ pode ser decidida em tempo limitada pelo polinômio

$$p(n) + q(p(n))$$

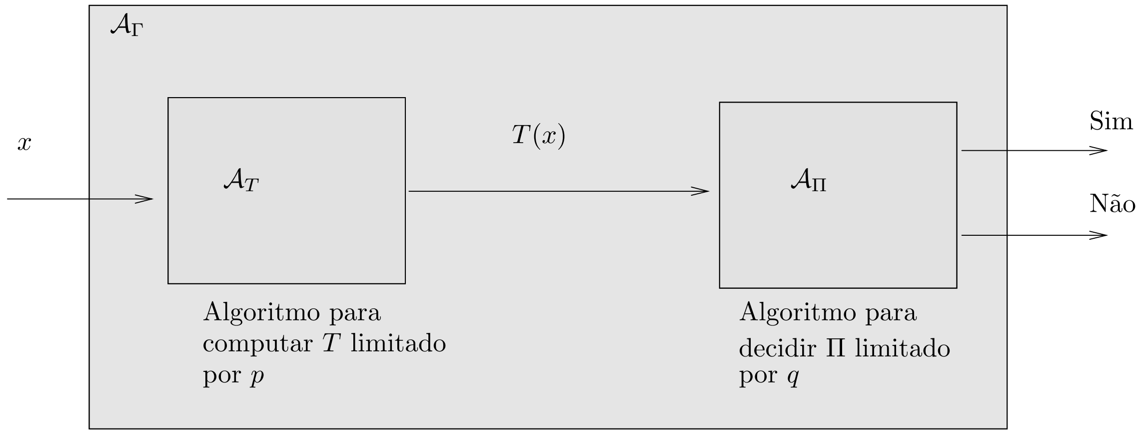

Figura 1: Algoritmo de decisão $\mathcal{A}_\Gamma$ para o problema Γ