Transformada Rápida de Fourier em Programação Competitiva

Luis Gustavo Bitencourt Almeida
Orientador José Coelho de Pina

Instituto de Matemática e Estatística, Universidade de São Paulo

Introdução

- Jean-Baptiste Joseph Fourier foi um matemático e físico francês que viveu entre 1768 e 1830. Séries e a transformadas de Fourier são resultados de seu trabalho no estudo de transferência de calor.
- Polinômios são usados em vários contextos para representar objetos e modelar fenômenos. Aqui serão usados para abordar a transformada rápida de Fourier.
- Operações em polinômios são importantes. A multiplicação de dois polinômios se feita de maneira clássica consome tempo $O(n^2)$. A transformada rápida de Fourier é um algoritmo proposto por Cooley e Tukey que resolve este problema e muito outros.

Polinômios

Um polinômio é uma expressão formada por coeficientes e variáveis envolvendo somente as operações de adição, subtração, multiplicação e exponenciação das variáveis por inteiros não negativos. Neste texto trataremos de polinômios com apenas uma variável. Isto é, um polinômio é uma função da forma

$$A(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} = \sum_{k=0}^{n-1} a_k x^k$$

O grau de um polinômio é o maior expoente de suas variáveis. Os valores a_k são os *coeficientes do polinômio*, em geral são valores reais.

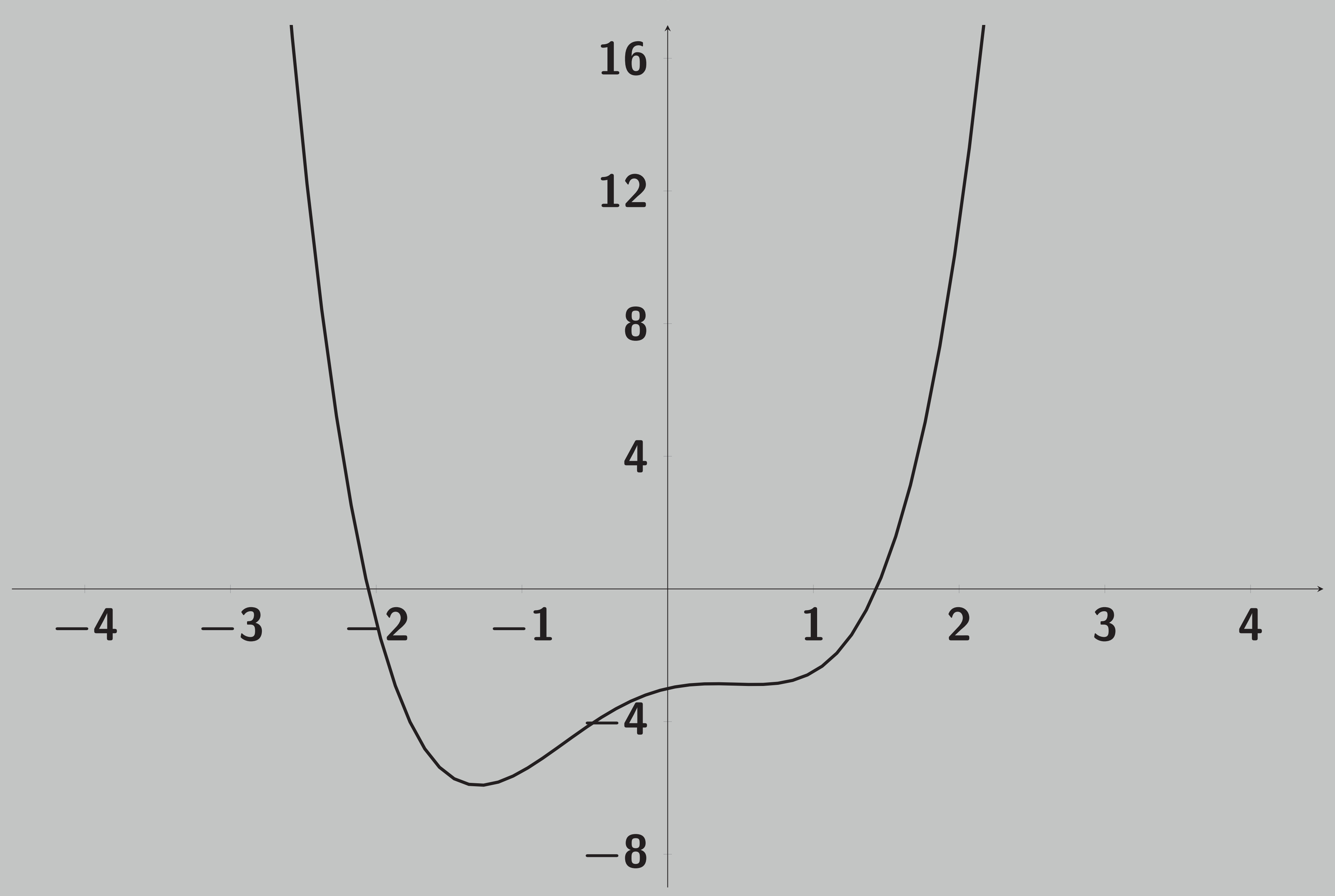

Figura 1: Gráfico do polinômio $A(x) = x^4 + 0.5x^3 - 2x^2 + x - 3$.

Representação de polinômios

- Como visto acima, um polinômio $A(x)$ pode ser determinado por seus coeficientes a_k. Isto é, um vetor $a = \langle a_0, a_1, \ldots, n-1\rangle$ determina o polinômio $a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$. O vetor a é dito vetor de coeficientes de $A(x)$.
- Podemos determinar unicamente os coeficientes de $A(x)$ a partir da lista de pontos $\{(x_0, y_0), (x_1, y_1), \ldots, (x_{n-1}, y_{n-1})\}$ tal que $y_k = A(x_k)$ para $k = 0, 1, \ldots, n-1$ e $x_i \neq x_j$. Está é a representação por pontos (*point-value*) de um polinômio.

Operações

Existem pelo menos três operações elementares envolvendo polinômios. São elas: valoração, adição e multiplicação. A primeira associa a um polinômio e um valor tipicamente real ou complexo, um outro valor real ou complexo. As outras duas associam dois polinômios a um terceiro polinômio. A tabela a seguir resume o consumo de tempo dos algoritmos padrões para realizar cada operação.

	Representação	
Operação	coeficientes	pontos
Valoração	$O(n)$	$O(n^2)$
Adição	$O(n)$	$O(n)$
Multiplicação	$O(n^2)$	$O(n)$

Raízes da unidade

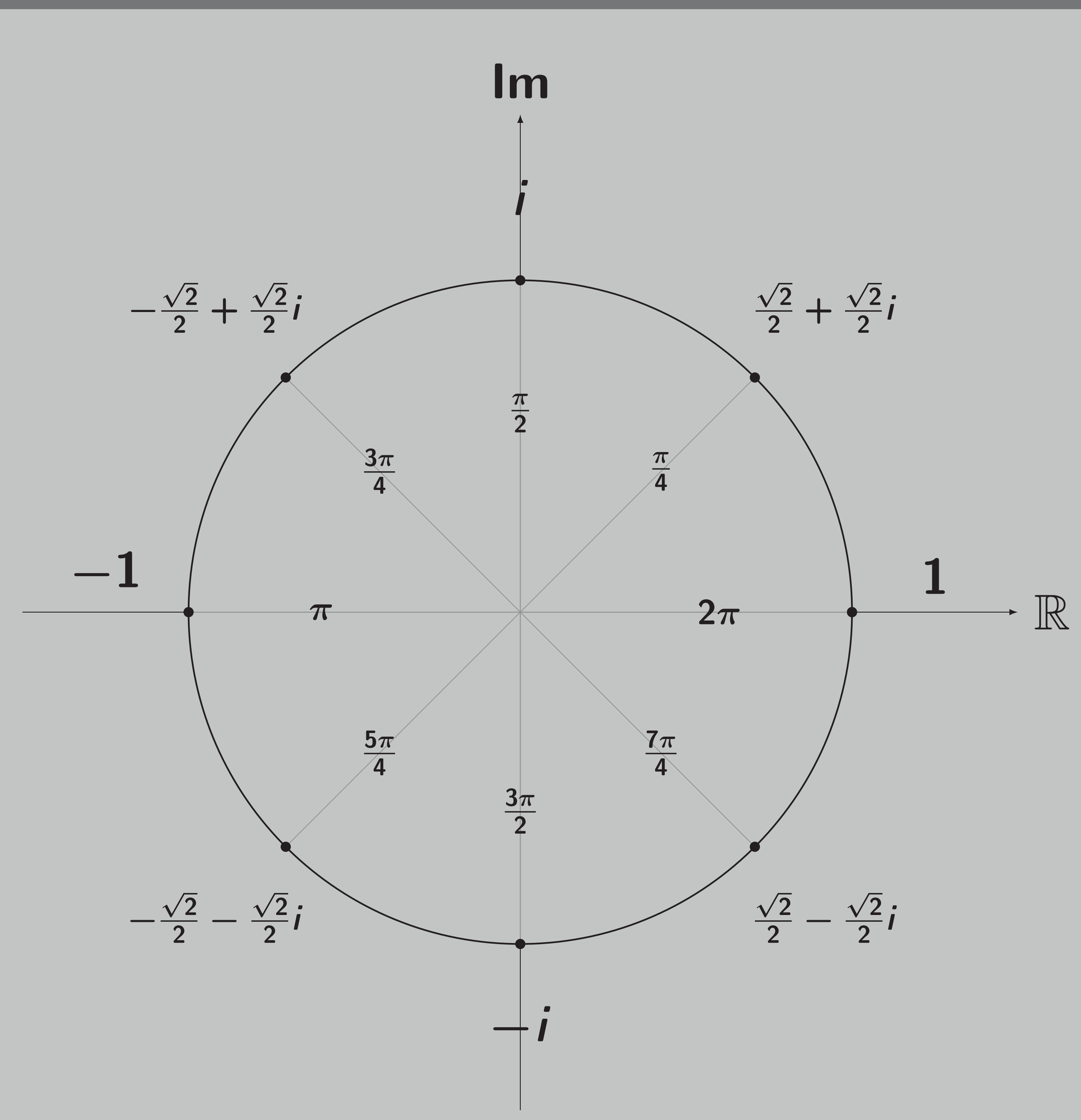

Figura 2: Círculo unitário do plano complexo e as raízes oitavas da unidade.

As n raízes complexas da unidade são definidas por $\omega_n^k = e^{2\pi ik/n}$ para $k = 0, 1, \ldots, n-1$. A raiz $\omega_n = e^{2\pi i/n}$ é dita principal enésima raiz da unidade.
A raízes da unidade também podem ser obtidas em um corpo finito $\mathbb{Z}_p^*$ para p primo.
Os algoritmos da transformada de Fourier se baseiam fortemente nas propriedades das raízes da unidade.

Transformada discreta de Fourier

A transformada de Fourier de n valores é dita discreta se os valores são igualmente espaçados. Queremos calcular o polinômio $A(x)$ nas n raízes n-ésimas da unidade $\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1}$.
O vetor $y = (A(\omega_n^0), A(\omega_n^1), \ldots, A(\omega_n^{n-1}))$ é dito DFT (*Discrete Fourier Transform*) do polinômio $A(x)$. O algoritmo para calcular o DFT é de divisão e conquista. Na divisão, separa o polinômio $A(x)$ em

$$A^{[0]}(x) = a_0 + a_2x + a_4x^2 + \cdots + a_{n-2}x^{n/2-1},$$
$$A^{[1]}(x) = a_1 + a_3x + a_5x^2 + \cdots + a_{n-1}x^{n/2-1}$$

e combina a resposta desses polinômios menores com

$$A(x) = A^{[0]}(x^2) + xA^{[1]}(x^2)$$

Inversa da transformada discreta

Estamos interessados em calcular o seguinte produto de matrizes

$$\begin{bmatrix} 1 & \omega_0 & \omega_0^2 & \cdots & \omega_0^{n-1} \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \omega_2^2 & \cdots & \omega_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_{n-1} & \omega_{n-1}^2 & \cdots & \omega_{n-1}^{n-1} \end{bmatrix}^{-1} \cdot \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{n-1} \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

Essa é a matriz de Vandermonde V e tem como inversa sua conjugada complexa $\overline{V}$. Logo, para recuperar os coeficientes do vetor de um DFT basta computar o mesmo algoritmo usando os pontos $\overline{\omega}$

Multiplicação rápida de polinômios

Ao calcular o DFT de um polinômio $A(x)$ obtemos sua representação por pontos. Sendo assim, podemos computar o produto de dois polinômios neste formato em tempo linear. Deste modo, para multiplicar dois polinômios no formato de coeficientes basta tomar o DFT de ambos, multiplicá-los na representação por pontos e voltar para o formato de coeficientes usando o IDFT.

Informações

A monografia está disponível com muito mais detalhes em
`https://linux.ime.usp.br/~lgbitencourt/mac0499/`

luis.bitencourt.almeida@usp.br