

Escola Politécnica-USP
LARC



Seminário NTT

Resumo

Contents

1	A Dualidade entre Tempo e Frequênci a	2
2	Transformada de Fourier Contínua (CTFT)	2
3	Transformada Discreta de Fourier (DFT)	2
3.1	Definição da IDFT	3
4	A Multiplicação de Polinômios e a Complexidade Computacional	4
5	A Fast Fourier Transform	5
6	Problemas da FFT	7
7	Number Theoretic Transform (NTT)	7
7.1	Fundamentos	7
8	O Isomorfismo via Teorema Chinês dos Restos (CRT)	10
9	Apêndice	10
9.1	Exemplo de convolução circular	10
9.2	Determinição unívoca do polinomio	13

1 A Dualidade entre Tempo e Frequência

A Transformada de Fourier é uma operação matemática que mapeia uma função do domínio do tempo (ou espaço) para o seu domínio dual: a frequência. Essa transição é extremamente útil, pois propriedades que são complexas de analisar no tempo tornam-se claras no espectro de frequências.

Esta ferramenta é um pilar fundamental em diversas áreas do conhecimento:

- **Matemática Pura:** Essencial na Teoria Analítica dos Números e no estudo de Equações Diferenciais Parciais (EDPs).
- **Física Moderna:** É a base matemática do **Princípio da Incerteza de Heisenberg** na Mecânica Quântica, onde a posição e o momento de uma partícula formam um par de variáveis conjugadas de Fourier.
- **Engenharia:** Processamento de sinais, compressão de dados (MP3, JPEG) e telecomunicações.

2 Transformada de Fourier Contínua (CTFT)

Para uma função contínua $g(t)$, a transformada é definida pela integral:

$$\mathcal{F}(f) = \int_{-\infty}^{\infty} g(t)e^{-2\pi ift} dt$$

Elá pode ser entendida como um produto interno (uma projeção) do sinal com todos as frequencias da reta real $\langle g, e^{-2\pi ift} \rangle$, que, devido a ortogonalidade das frequências diferentes e que funções bem comportadas podem ser decompostas em séries de autofunções e^{-ift} , consegue extrair extamente as frequências do sinal. Apesar de sua elegância teórica, a CTFT apresenta desafios para a aplicação prática em sistemas digitais:

1. **Natureza Analítica:** A resolução de integrais impróprias exige uma manipulação simbólica que é difícil de implementar em computadores comuns.
2. **Limite Infinito:** A definição pressupõe que conhecemos o sinal de $-\infty$ a $+\infty$, o que é impossível em cenários reais.
3. **Amostragem Finita:** Na prática, os sinais são capturados de forma discreta (amostras) e por um tempo limitado, o que torna a integral contínua inaplicável.

3 Transformada Discreta de Fourier (DFT)

Para viabilizar o processamento em computadores, utilizamos a **DFT**. Ela opera sobre uma sequência finita de N amostras, mapeando dados discretos no tempo para dados discretos na frequência:

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-i \frac{2\pi}{N} kn}$$

Para $k = 0, 1, \dots, N - 1$.

Diferente da versão contínua, a DFT lida com somatórios e vetores numéricos, permitindo que a teoria de Fourier seja aplicada em qualquer dispositivo digital. Eh possivel provar que a DFT eh um transformacao linear, logo, pode ser representada matricialmente.

Seja $\zeta_N = e^{-i \frac{2\pi}{N}}$. A representação matricial da DFT para $n = 0, 1, \dots, N - 1$ é:

$$\begin{bmatrix} X[0] \\ X[1] \\ \vdots \\ X[N-1] \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N^1 & \zeta_N^2 & \cdots & \zeta_N^{N-1} \\ 1 & \zeta_N^2 & \zeta_N^4 & \cdots & \zeta_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{N-1} & \zeta_N^{2(N-1)} & \cdots & \zeta_N^{(N-1)(N-1)} \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \\ \vdots \\ x[N-1] \end{bmatrix}$$

3.1 Definição da IDFT

A reconstrução do sinal original no domínio do tempo a partir de suas amostras de frequência é realizada pela IDFT:

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k] \zeta_N^{-nk}, \quad n = 0, 1, \dots, N - 1$$

Onde $\zeta_N^{-nk} = e^{i \frac{2\pi}{N} nk}$. Matricialmente, a IDFT é dada por:

$$\begin{bmatrix} x[0] \\ x[1] \\ x[2] \\ \vdots \\ x[N-1] \end{bmatrix} = \frac{1}{N} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_N^{-1} & \zeta_N^{-2} & \cdots & \zeta_N^{-(N-1)} \\ 1 & \zeta_N^{-2} & \zeta_N^{-4} & \cdots & \zeta_N^{-2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{-(N-1)} & \zeta_N^{-2(N-1)} & \cdots & \zeta_N^{-(N-1)(N-1)} \end{bmatrix} \begin{bmatrix} X[0] \\ X[1] \\ X[2] \\ \vdots \\ X[N-1] \end{bmatrix}$$

Percebe-se que nesse caso discreto, a DFT e IDFT atuam como uma matriz mudança de base, saindo da base do tempo e indo para base das raízes unitárias

A DFT pde ser vista de outra óptica, como avaliação de polinomios. Seja

$$a(x) = \sum_{n=0}^{N-1} a_n x^n$$

e tome $\zeta_N = e^{-i \frac{2\pi}{N}}$ seja uma N -ésima raiz primitiva da unidade. Define

$$A_k := a(\zeta_N^k).$$

Então

$$A_k = \sum_{n=0}^{N-1} a_n (\zeta_N^k)^n = \sum_{n=0}^{N-1} a_n \zeta_N^{kn},$$

o que é exatamente a formulação da DFT, para $a_n \equiv x[n]$ e $A_n \equiv X[n]$, oportamente, a IDFT é interpretada como interpolação de polinômios:

Dados os valores $\{A_k\}_{k=0}^{N-1}$, ela reconstrói os coeficientes $\{a_n\}_{n=0}^{N-1}$ do único polinômio de grau $N - 1$ que satisfaz $a(\zeta_N^k) = A_k$ para todo k . Explicitamente,

$$a_n = \frac{1}{N} \sum_{k=0}^{N-1} A_k \zeta_N^{-kn}.$$

Assim, DFT é *avaliar* em raízes da unidade e IDFT é *interpolar* (recuperar os coeficientes) a partir dessas avaliações. (Essa perspectiva baseia-se na determinação unívoca do polinômio de grau $N - 1$ por N pontos veja a seção 9.2 para demonstração desse fato)

4 A Multiplicação de Polinômios e a Complexidade Computacional

Um problema simplificado pela mudança de domínio eh a multiplicacao de polinomios. Tome os polinomios $f(x)$ e $g(x)$ de grau $n - 1$:

$$f(x) = \sum_{i=0}^{N-1} a_i x^i, \quad g(x) = \sum_{j=0}^{N-1} b_j x^j$$

Na abordagem clássica , o produto $h(x) = f(x) \cdot g(x)$ é obtido distribuindo-se cada termo de f sobre todos os termos de g . Este processo resulta em um novo polinômio de grau $2N - 2$:

$$h(x) = \sum_{k=0}^{2N-2} c_k x^k$$

onde $c_k = \sum_{i+j=k} a_i b_j$.

Nesta metodologia, o cálculo de cada coeficiente c_k exige múltiplas operações de produto e soma, resultando em uma complexidade assintótica $O(n^2)$. Para polinômios com grandes volumes de coeficientes, este custo computacional torna o método inviável.

A conexão entre a multiplicação de polinômios e a análise de Fourier vem do fato de que, se $h(x) = f(x)g(x)$, então os coeficientes c_k de h são dados pela **convolução linear** dos coeficientes de f e g :

$$c_k = \sum_{i+j=k} a_i b_j.$$

Neste trabalho, devido ao foco na NTT e ao anel quociente $\mathbb{Z}_p[x]/(x^n - 1)$, trabalhamos com a **convolução circular** (de comprimento n), definida por

$$c_k = \sum_{i=0}^{N-1} a_i b_{(k-i) \bmod n}, \quad k = 0, \dots, N - 1.$$

Teorema da Convolução: a transformada de uma convolução no domínio do tempo (ou espaço) é o produto ponto a ponto (Hadamard) das transformadas no domínio da frequência:

$$\mathcal{F}(f * g) = \mathcal{F}(f) \odot \mathcal{F}(g).$$

Assim, o cálculo custoso da convolução é convertido em um produto ponto a ponto, pois a base de Fourier diagonaliza o operador de convolução (circulante). Com a transformada direta ingênuo o custo ainda é $O(n^2)$, não há ganho da multiplicação clássica de polinômios.

Uma exemplo para o convencimento do leitor foi disposto no apendice 9.1

5 A Fast Fourier Transform

A FFT (Fast Fourier Transform) eh uma maneira de otimizar o calculo da DFT.

O algoritmo da FFT foi redescoberta por Cooley e Tukey em 1965, uma vez que Gauss ja tinha utilzado um algoritmo semelhante para calcular a orbitas de asteroides em 1805.

O algoritmo se baseia em **dividir para conquistar**.

Relembrando

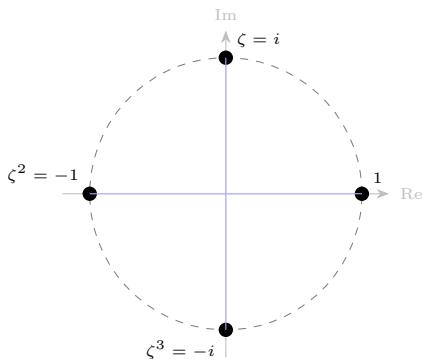
As raízes unitárias possuem propriedades cíclicas e certas simetrias que permitem a economia nos cálculos, vejamos um exemplo.

$$\zeta_4^1 = e^{-i\frac{2\pi}{4}} = e^{-i90^\circ} = -i$$

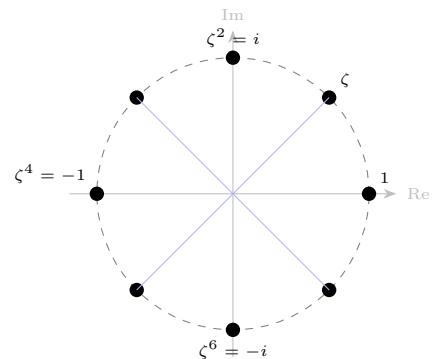
$$\zeta^1 = -i \qquad \zeta^2 = -1$$

$$\zeta^3 = i \qquad \zeta^4 = 1$$

por isso, percebe-se que, a cada 2 "deslocamentos", o valor se torna o oposto, como ilustrado na figura:



(a) 4-ésimas raízes da unidade



(b) 8-ésimas raízes da unidade

Figure 1: Comparação entre as raízes da unidade no plano complexo.

De forma mais geral:

$\zeta_N = e^{\frac{2\pi i}{N}}$, uma raiz N -ésima primitiva da unidade. Então para todo inteiro a ,

$$\zeta_N^{a+\frac{N}{2}} = -\zeta_N^a.$$

Alem de que, pela periodicidade $\zeta_N^{a+N} = \zeta_N^a$.

Para esse caso a DFT eh representada desse modo:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}$$

Voltando a FFT, o algoritmo decompõe uma DFT de tamanho N em duas sub-transformadas de tamanho $N/2$, separando os índices pares e ímpares da sequência original:

$$X[k] = \sum_{m=0}^{\frac{N}{2}-1} x[2m] \zeta_N^{2mk} + \sum_{m=0}^{\frac{N}{2}-1} x[2m+1] \zeta_N^{(2m+1)k}$$

$$\text{Usando } \zeta_N^2 = \zeta_{N/2} : \quad \zeta_N^{2mk} = (\zeta_N^2)^{mk} = \zeta_{N/2}^{mk}$$

$$\begin{aligned} &= \sum_{m=0}^{\frac{N}{2}-1} x[2m] \zeta_{N/2}^{mk} + \zeta_N^k \sum_{m=0}^{\frac{N}{2}-1} x[2m+1] \zeta_{N/2}^{mk} \\ &= E[k] + \zeta_N^k O[k], \quad k = 0, \dots, \frac{N}{2} - 1. \end{aligned}$$

Esta estrutura permite calcular dois valores de saída ($X[k]$ e $X[k + N/2]$) utilizando os mesmos resultados intermediários, através da denominada **operação borboleta** (*butterfly operation*):

1. $X[k] = E[k] + \zeta_N^k O[k]$
2. $X[k + N/2] = E[k] - \zeta_N^k O[k]$

como pode ser visto na imagem

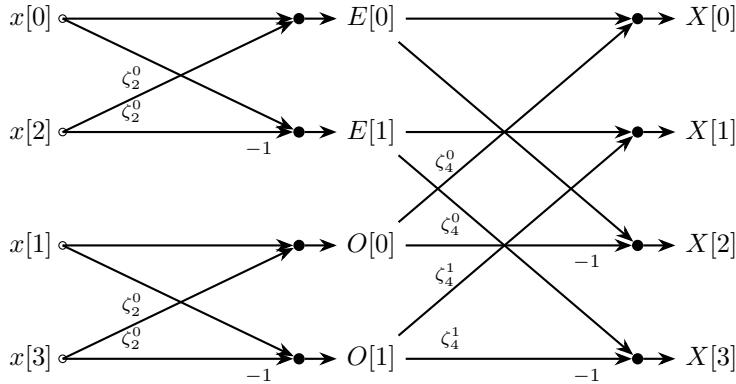


Figure 2: butterfly radix-2

o a implementacao em sage esta no codigo1

Listing 1: Implementação do algoritmo FFT em SageMath

```

1 def fft(a, omega):
2     n = len(a)
3     if n == 1:
4         return a[:]
5
6
7     a_par = fft(a[0::2], omega^2)
8     a_impar = fft(a[1::2], omega^2)
9
10    A = [0] * n
11    w = 1
12    half = n // 2
13    for k in range(half):
14        t = w * a_impar[k]
15        A[k]           = a_par[k] + t
16        A[k + half]   = a_par[k] - t
17        w *= omega
18    return A

```

Desse modo, reduzimos a complexidade da transformada de $O(n^2)$ para $O(n \cdot \log n)$. Por causa disso, podemos utilizar a FFT, junto com o **teorema da convolução**, para multiplicar polinomios em $O(n \cdot \log n)$

6 Problemas da FFT

Um dos problemas da FFT é que ela trabalha com ponto flutuante, o que, para computadores, é um grande problema que pode causar erro de arredondamentos e, assim causar um falha nos esquemas criptográficos. Além disso, o polinômio dobraria de tamanho a cada concatenação e que rapidamente torna-se um problema tanto computacional quanto de armazenamento.

Solução: utilizar uma transformada que utiliza apenas números exatos

7 Number Theoretic Transform (NTT)

7.1 Fundamentos

As propriedades que usamos na FFT — em especial a existência de uma raiz N -ésima da unidade ζ_N e o fato de que suas potências percorrem uniformemente o círculo — têm um análogo perfeito em teoria dos números, dentro de corpos (ou anéis) finitos. Isso não é coincidência: a FFT nada mais é do que a transformada de Fourier no grupo cíclico $\mathbb{Z}/N\mathbb{Z}$, e a mesma construção existe em outros contextos algébricos.

Mais formalmente, se ζ_N é uma raiz N -ésima primitiva da unidade, então o conjunto de todas as N -ésimas raízes

$$\mu_N = \{1, \zeta_N, \zeta_N^2, \dots, \zeta_N^{N-1}\}$$

forma um grupo multiplicativo cíclico de ordem N . Existe um isomorfismo natural de grupos

$$\varphi : \mathbb{Z}/N\mathbb{Z} \rightarrow \mu_N, \quad \varphi([k]) = \zeta_N^k,$$

onde o lado esquerdo usa a soma módulo N e o lado direito usa multiplicação:

$$\varphi([k + \ell]) = \zeta_N^{k+\ell} = \zeta_N^k \zeta_N^\ell = \varphi([k]) \varphi([\ell]).$$

Raiz primitiva Diferente da DFT complexa, onde raízes da unidade sempre existem para qualquer n , a NTT exige que o corpo finito \mathbb{Z}_p suporte a ordem da transformada.

Para que exista uma raiz primitiva n -ésima da unidade em \mathbb{Z}_p , o tamanho da sequência n deve dividir a ordem do grupo multiplicativo do corpo:

$$n \mid (p - 1)$$

Agora, iremos tratar da estrutura aritmética, na qual a NTT ocorre.

Ela é definida da seguinte forma:

$$X[k] = \sum_{n=0}^{N-1} x[n] \omega^{nk} \pmod{p}$$

ou na forma matricial

$$\mathbf{X} = \mathbf{W}_N \mathbf{x}, \quad \mathbf{x} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix},$$

$$\mathbf{W}_N = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix},$$

$$(\mathbf{W}_N)_{k,n} = \omega^{kn}, \quad 0 \leq k, n \leq N - 1,$$

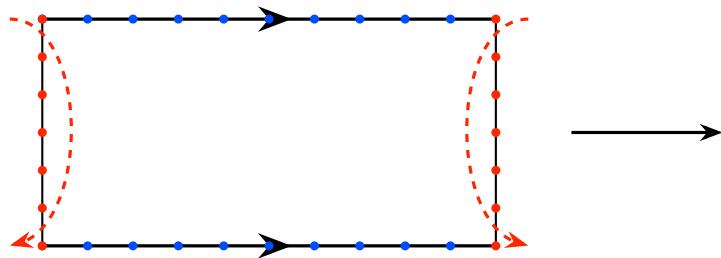
Ela opera no anel quociente

$$R = \mathbb{Z}_p[x]/(x^n - 1)$$

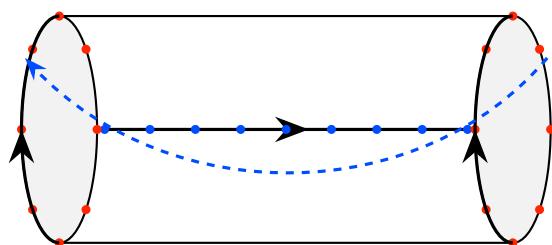
onde $\mathbb{Z}_p[x]$ representa os coeficientes do polinômio mod p e o $(x^n - 1)$ faz com que a cadeia longa de polinômio sobre em si mesma formando um ciclo.

a imagem 3 ilustra a sequência das duas operações visualmente.

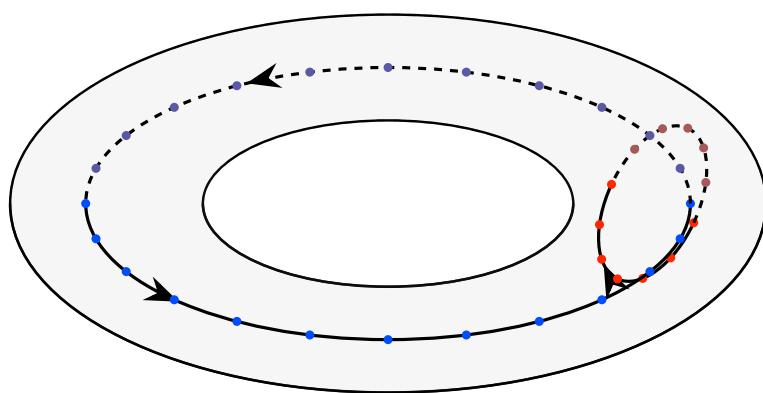
1. Colar lados horizontais (Passo \mathbb{Z}_p)



Obtém-se um cilindro



2. Colar lados verticais (Passo $/(x^n - 1)$)



3. Obtém-se um Toro Discreto

- Direção $/(x^n - 1)$
- Direção \mathbb{Z}_p

Figure 3: representação das transformações

Escolhemos modulo de um primo para que Z_p seja um field, i.e, para que a aritimedita tenha propiedades agradaveis e escolhemos $(x^n - 1)$ para que haja raizes distinta e se preserve as "informacoes" indepentes o que garante que ele possa ser decomposto completamente.

8 O Isomorfismo via Teorema Chinês dos Restos (CRT)

A fundamentação algébrica da NTT reside na decomposição do anel de polinômios. Se ω é uma raiz primitiva n -ésima da unidade no corpo finito \mathbb{Z}_p , o polinômio $x^n - 1$ pode ser fatorado completamente em binômios lineares distintos:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \omega^i)$$

Como cada termo $(x - \omega^i)$ é irreduzível e todos são coprimos entre si, o **Teorema Chinês dos Restos (CRT)** garante a existência de um isomorfismo de anéis:

$$\frac{\mathbb{Z}_p[x]}{(x^n - 1)} \cong \frac{\mathbb{Z}_p[x]}{(x - \omega^0)} \times \frac{\mathbb{Z}_p[x]}{(x - \omega^1)} \times \cdots \times \frac{\mathbb{Z}_p[x]}{(x - \omega^{n-1})}$$

Este isomorfismo é o que permite interpretar a NTT não apenas como uma transformação de vetores, mas como uma mudança de representação.

A comporação computacional dessa ferramentas pode ser vista na tabela a seguir, onde calculou-se os números de Fibonacci.

Algorithm	Fibonacci index
Algoritmo Naive	44
Algoritmo Linear	566'053
Algoritmo FFT	3'145'816
Algoritmo NTT	24'178'839
Algoritmo GMP	238'961'323

fonte: <https://github.com/SheafificationOfG/Fibsonisheaf>

9 Apêndice

9.1 Exemplo de convolução circular

Sejam dois sinais x e y de comprimento $N = 3$:

$$x = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \quad y = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

A frequênci fundamental é a raiz da unidade $\zeta_3 = e^{-i\frac{2\pi}{3}}$. Usaremos a propriedade fundamental:

$$1 + \zeta_3 + \zeta_3^2 = 0 \implies \zeta_3 + \zeta_3^2 = -1$$

Método 1: Convolução no Tempo (Matriz Circulante)

A convolução circular $z = x \circledast y$ equivale à multiplicação de uma matriz circulante C_x pelo vetor y :

$$C_x = \begin{bmatrix} x[0] & x[2] & x[1] \\ x[1] & x[0] & x[2] \\ x[2] & x[1] & x[0] \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}$$

Calculando $z = C_x y$:

$$z = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1(1) + 0 + 2(1) \\ 2(1) + 0 + 0 \\ 0 + 0 + 1(1) \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$$

Método 2: Diagonalização (Domínio da Frequência)

Mostra-se que a mudança de base para a base de Fourier diagonaliza a matriz circulante C_x . Matematicamente, isso significa que C_x pode ser decomposta como

$$C_x = F^{-1} \Lambda_x F$$

onde Λ_x é uma matriz diagonal contendo os coeficientes da DFT de x .

Substituindo essa decomposição na equação original da convolução $z = C_x y$, podemos rearranjar os termos para utilizar a multiplicação na frequência:

$$z = (F^{-1} \Lambda_x F)y = F^{-1} \Lambda_x (Fy) = F^{-1} \Lambda_x Y \quad (1)$$

Dessa forma, o cálculo se resume a obter Y (DFT de y), multiplicar pela matriz diagonal Λ_x e aplicar a inversa (F^{-1}).

Para legitimar que os autovalores de C_x são os coeficientes da DFT de x , resolvemos:

$$\det(C_x - \lambda I) = 0 \implies \det \begin{bmatrix} 1 - \lambda & 0 & 2 \\ 2 & 1 - \lambda & 0 \\ 0 & 2 & 1 - \lambda \end{bmatrix} = 0$$

Expandindo o determinante:

$$(1 - \lambda)^3 + 8 = 0 \implies (1 - \lambda)^3 = -8$$

As raízes para $(1 - \lambda)$ são as três raízes cúbicas de -8 :

$$\begin{aligned} 1 - \lambda_0 &= -2 \implies \lambda_0 = 3 \\ 1 - \lambda_1 &= -2\zeta_3 \implies \lambda_1 = 1 + 2\zeta_3 \\ 1 - \lambda_2 &= -2\zeta_3^2 \implies \lambda_2 = 1 + 2\zeta_3^2 \end{aligned}$$

Estes valores coincidem exatamente com a DFT de x , provando a legitimidade da diagonalização.

Verificação do Autovetor

Verificamos agora se o autovetor v_1 da base de Fourier (coluna de F^{-1}), dado por $v_1 = [1, \zeta_3^2, \zeta_3]^T$, satisfaz $C_x v_1 = \lambda_1 v_1$.

Lado esquerdo ($C_x v_1$):

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ \zeta_3^2 \\ \zeta_3 \end{bmatrix} = \begin{bmatrix} 1 + 2\zeta_3 \\ 2 + \zeta_3^2 \\ 2\zeta_3^2 + \zeta_3 \end{bmatrix}$$

Lado direito ($\lambda_1 v_1$):

$$(1 + 2\zeta_3) \begin{bmatrix} 1 \\ \zeta_3^2 \\ \zeta_3 \end{bmatrix} = \begin{bmatrix} 1 + 2\zeta_3 \\ \zeta_3^2 + 2\zeta_3^3 \\ \zeta_3 + 2\zeta_3^2 \end{bmatrix} = \begin{bmatrix} 1 + 2\zeta_3 \\ 2 + \zeta_3^2 \\ \zeta_3 + 2\zeta_3^2 \end{bmatrix}$$

A igualdade é satisfeita, pensamento analogo é utilizado para mostrar que v_0 e v_2 e tambem são autovetores, confirmando que a base de Fourier é a base natural de C_x .

Representação Matricial da Diagonalização

Primeiro, calculamos os vetores transformados $X = Fx$ e $Y = Fy$:

$$X = \begin{bmatrix} 3 \\ 1 + 2\zeta_3 \\ 1 + 2\zeta_3^2 \end{bmatrix}, \quad Y = \begin{bmatrix} 2 \\ 1 + \zeta_3^2 \\ 1 + \zeta_3 \end{bmatrix}$$

Agora, construímos a matriz diagonal $\Lambda_x = \text{diag}(X)$. A operação de convolução no domínio da frequênciia ($Z = X \cdot Y$), visualizada matricialmente como $Z = \Lambda_x Y$, torna-se:

$$\mathbf{Z} = \underbrace{\begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 + 2\zeta_3 & 0 \\ 0 & 0 & 1 + 2\zeta_3^2 \end{bmatrix}}_{\text{Matriz Diagonal } (\Lambda_x)} \begin{bmatrix} 2 \\ 1 + \zeta_3^2 \\ 1 + \zeta_3 \end{bmatrix}$$

Executando o produto matricial (que equivale ao produto ponto a ponto):

$$\mathbf{Z} = \begin{bmatrix} 3 \cdot 2 \\ (1 + 2\zeta_3)(1 + \zeta_3^2) \\ (1 + 2\zeta_3^2)(1 + \zeta_3) \end{bmatrix} = \begin{bmatrix} 6 \\ 2 + \zeta_3 \\ 2 + \zeta_3^2 \end{bmatrix}$$

*Nota: As simplificações algébricas utilizam $1 + \zeta_3 + \zeta_3^2 = 0$.

Retorno ao Tempo (IDFT)

Finalmente, aplicamos a matriz inversa de Fourier (F^{-1}) para obter z :

$$z = F^{-1}\mathbf{Z} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \zeta_3^{-1} & \zeta_3^{-2} \\ 1 & \zeta_3^{-2} & \zeta_3^{-4} \end{bmatrix} \begin{bmatrix} 6 \\ 2 + \zeta_3 \\ 2 + \zeta_3^2 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$$

Isso confirma numericamente que a base de Fourier diagonalizou a operação.

9.2 Determinação unívoca do polinomio

Theorem 1 (Unicidade via matriz de Vandermonde). *Sejam x_0, \dots, x_{N-1} escalares dois a dois distintos em um corpo \mathbb{K} (e.g., $\mathbb{R}, \mathbb{C}, \mathbb{F}_p$), e sejam $y_0, \dots, y_{N-1} \in \mathbb{K}$. Existe um único polinômio $p(x) = a_0 + a_1x + \dots + a_{N-1}x^{N-1} \in \mathbb{K}[x]$ tal que $p(x_i) = y_i$ para todo $i = 0, \dots, N-1$.*

Proof. Escreva $p(x) = \sum_{k=0}^{N-1} a_k x^k$. Impor as condições $p(x_i) = y_i$ para $i = 0, \dots, N-1$ gera o sistema linear

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{N-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{N-1} & x_{N-1}^2 & \cdots & x_{N-1}^{N-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix}.$$

Denote essa matriz por V (matriz de Vandermonde,i.e. $V_{i,j} = x_i^{j-1}$ para todo os índices i,j), o vetor de coeficientes por a e o vetor de valores por y ; então o sistema é

$$Va = y.$$

O determinante de Vandermonde é dado por

$$\det(V) = \prod_{0 \leq i < j \leq N-1} (x_j - x_i).$$

Como os x_i são dois a dois distintos, temos $x_j - x_i \neq 0$ para $i \neq j$, logo $\det(V) \neq 0$. Portanto, V é invertível e o sistema $Va = y$ tem **solução única**, dada por

$$a = V^{-1}y.$$

Concluímos que existe um único vetor de coeficientes (a_0, \dots, a_{N-1}) , isto é, um **único** polinômio $p(x)$ de grau $\leq N-1$ que interpola os N pontos. \square