FFT

Pro daná $F = (F(0), F(1), \dots, F(N-1)) \in \mathbb{C}^N$

lze spočítat $\hat{F}(0), \dots, \hat{F}(N-1)$ jako maticové násobení $\hat{F} = F_N F$

... ca $2N^2$ operací

Věta: Pro dané $\omega_N = e^{-\frac{2\pi i}{N}}$ s $N = 2^n$ stačí

$$4 \cdot 2^n \cdot n = 4N \log_2(N) = O(N \log N)$$

operací k výpočtu $\hat{F}$.

Důkaz: Nechť $\#(M)$ je minimální počet operací potřebných k výpočtu $\hat{F}$ na $\mathbb{Z}_M$.

Tvrzení: $\#(2M) \leq 2\#(M) + 8M$, pokud $\omega_{2M} = e^{-\frac{2\pi i}{2M}}$ je dáno

Pak už snadno indukcí ... Pro $N=2$ ... $\#(2) = 4 \leq 8$

$s\ N = 2^{n-1}$: $\#(2N) \leq 2 \cdot 4 \cdot 2^{n-1}(n-1) + 8 \cdot 2^{n-1} = 8n2^{n-1} = 4n2^n$.

Důkaz tvrzení: • $2M$ operací $\to$ výpočet $\omega_{2M}^2, \dots, \omega_{2M}^{2M-1}$

• $F_0(r) := F(2r)$, $F_1(r) := F(2r+1)$ ... jejich Four. transf. v $\#(M)$ operacích

Pak $(0 \leq k \leq 2M-1)$

$$\hat{F}(k) = \sum_{r=0}^{2M-1} F(r)\,\omega_{2M}^{kr} = \sum_{l=0}^{M-1} F(2l)\,\omega_{2M}^{k(2l)} + \sum_{m=0}^{M-1} F(2m+1)\,\omega_{2M}^{k(2m+1)}$$

$$= \sum_{l=0}^{M-1} F_0(l)\,\omega_M^{kl} + \omega_{2M}^{k} \sum_{m=0}^{M-1} F_1(m)\,\omega_M^{km}$$

$$= \hat{F}_0(k) + \omega_{2M}^{k}\,\hat{F}_1(k)$$

... $\hat{F}_0(k) = \hat{F}_0(k-M)$ pro $k \geq M$

Věta: Nechť $A = F_{S^*} \in \mathbb{R}^{m \times N}$, $m = 2s < N$ je horní část Fourierovy matice F_N; $S^* = \{0, 1, \dots, 2s-1\}$. Pak existuje rychlý (= polynomiální) algoritmus, který zrekonstruuje s-řídký $x \in \mathbb{C}^N$ (i.e. $x \in \mathbb{C}^N_s$) $\dots \Sigma_{s,N}$ s měřením $y = Ax \in \mathbb{C}^{2s}$.

Důkaz: • Nejdříve popíšeme algoritmus:

* Vstup: $s, N, y \in \mathbb{C}^{2s}$: $y(j) = \hat{x}(j) = \sum_{k=0}^{N-1} x(k) e^{-2\pi i \frac{jk}{N}}$, $j = 0, \dots, 2s-1$.

* Vyřešíme systém

$$\begin{pmatrix} y(s-1) & y(s-2) & \dots & y(0) \\ y(s) & y(s-1) & \dots & y(1) \\ & & \ddots & \\ y(2s-2) & \dots & & y(s-1) \end{pmatrix} \begin{pmatrix} z(1) \\ z(2) \\ \vdots \\ z(s) \end{pmatrix} = - \begin{pmatrix} y(s) \\ y(s+1) \\ \vdots \\ y(2s-1) \end{pmatrix} \qquad (1)$$

a získáme $z \in \mathbb{C}^s$. Položíme $z(0) = 1$ a $z(k) = 0$ pro $k > s$. $\to z \in \mathbb{C}^N$.

* Položíme $S := (\operatorname{supp} z^\vee)^c$ a dokážeme, že $\#S \le s$ a $\operatorname{supp} x \subset S$.

* Pak už jen vyřešíme $y(j) = \sum_{k \in S} x(k) e^{-\frac{2\pi i jk}{N}}$, $j = 0, 1, \dots, 2s-1$ (2)

Poznámka: • (1) ... $s \times s$ lineární systém ... $O(s^3)$

• hledání $(\operatorname{supp} \check{z})$ ... $O(N \log N)$

• řešení (2) ... $s \times 2s$ systém $O(s^3)$

$\dots \Rightarrow O(s^3 + N \log N)$

• Nestabilní, nerobustní!

Důkaz správnosti algoritmu

- Nechť $\tilde{S} := \operatorname{supp} x$, $s \geq \# \tilde{S}$

  Chceme dokázat, že $(\operatorname{supp} z^{\vee})^c = S \supset \tilde{S} = \operatorname{supp} x$ pro každé

  z $s(1)$ & $z(0) = 1$ & $z(k) = 0, k > s$.

- 1. krok ... dokážeme, že (1) má alespoň 1 řešení & dokážeme větu pokud je toto řešení jediné.

Definujeme $p(t) = \frac{1}{N} \prod_{k \in \tilde{S}} \left(1 - e^{-2\pi i \frac{k}{N}} e^{2\pi i \frac{t}{N}}\right)$, $t \in \{0, 1, \dots, N-1\}$

... $p(t)$ je nula právě tehdy, když $\cancel{}$ $t \in \tilde{S}$ ... $\operatorname{supp} p = \{0, \dots, N-1\} \setminus \tilde{S}$

Tedy $p \cdot x = (p(k) x(k))_{k=0}^{N-1} = \theta$ a $\widehat{p \cdot x} = \hat{p} * \hat{x} = \theta$

- Z def. p: $\hat{p}(0) = 1$:

$$\hat{p}(0) = \sum_{t=0}^{N-1} p(t) = \frac{1}{N} \sum_{t=0}^{N-1} \prod_{k \in \tilde{S}} \left(1 - e^{-\frac{2\pi i k}{N}} \cdot e^{\frac{2\pi i t}{N}}\right)$$

$$= \frac{1}{N} \sum_{t=0}^{N-1} \sum_{S' \subset \tilde{S}} \prod_{l \in S'} \left[(-1) e^{-\frac{2\pi i l}{N}} \cdot e^{\frac{2\pi i t}{N}}\right]$$

$$= \frac{1}{N} \sum_{t=0}^{N-1} \sum_{S' \subset \tilde{S}} (-1)^{\# S'} e^{\frac{2\pi i t}{N} \cdot \# S'} \cdot \exp\left(-\frac{2\pi i}{N} \sum_{l \in S'} l\right)$$

$$= \frac{1}{N} \sum_{S' \subset S} (-1)^{\# S'} \exp\left(-\frac{2\pi i}{N} \sum_{l \in S'} l\right) \underbrace{\sum_{t=0}^{N-1} e^{\frac{2\pi i t}{N} \# S'}}_{= \begin{cases} 0 \dots \# S' \neq 0 \\ N \; \# S' = 0 \end{cases}}$$

$$= \frac{1}{N} (-1)^{0} \cdot 1 \cdot N = 1.$$

- Stejně $\hat{p}(k) = 0$, $k > s$ ... $\operatorname{supp} \hat{p} \subset \{0, 1, \dots, s\}$
- Soustava $\hat{p} * \hat{x} = 0$ dává

$$\hat{p}(0)\hat{x}(s) + \hat{p}(1)\hat{x}(s-1) + \dots + \hat{p}(s)\hat{x}(0) = 0 \quad \dots (\hat{p}*\hat{x})(s) = 0$$
$$\hat{p}(0)\hat{x}(s+1) + \hat{p}(1)\hat{x}(s) + \dots + \hat{p}(s)\hat{x}(1) = 0 \quad (\hat{p}*\hat{x})(s+1) = 0$$
$$\vdots$$
$$\hat{p}(0)\hat{x}(2s-1) + \dots + \hat{p}(s)\hat{x}(s-1) = 0 \quad (\hat{p}*\hat{x})(2s-1) = 0$$

$\Rightarrow \hat{p}$ řeší (1) .... (1) má alespoň jedno řešení!

- Pokud je toto řešení jediné ... tedy $\hat{p} = z$

$\Rightarrow S = (\operatorname{supp} z^\vee)^c = (\operatorname{supp} p)^c = (\{0, 1, \dots, N-1\} \setminus \tilde{S})^c = \tilde{S}$.

- 2. krok ... (1) není jednoznačně řešitelná!

Nechť z řeší (1) & $z(0) = 1$ & $z(k) = 0$ pro $k > s$. Položme $q = z^\vee$

- Pak $\widehat{q \cdot x} = \hat{q} * \hat{x}(j) = 0$ pro $j = s, s+1, \dots, 2s-1$
$= (z * \hat{x})(j)$
- Tedy $q \cdot x$ je s-řídký vektor s s Fourierovskými po sobě jdoucími koeficienty rovnými nule $\boxed{\text{LEMMA}} \Rightarrow q \cdot x \equiv 0$

$\Rightarrow q(j) = 0$ pro $j \in \tilde{S}$

$\tilde{S} = \operatorname{supp} x \subset \{j : q(j) = 0\} = \{j : z^\vee(j) = 0\}$

$= (\operatorname{supp} z^\vee)^c = S$. $\quad \underline{\underline{\# S \le s?}}$