§4 Zwei Anwendungen der FFT

1. Lineare Algebra mit zyklischen Matrizen

Def.: (a) Eine Matrix $C = (c_{ij}) \in K^{n \times n}$ über einem Körper K heißt zyklisch, wenn sie von der Form

$$C = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ \vdots \\ n-1 \end{array} \overset{\begin{array}{cccccc} 0 & 1 & 2 & \dots & n-1 \end{array}}{\begin{bmatrix} c_0 & c_{n-1} & c_{n-2} & \dots & c_1 \\ c_1 & c_0 & c_{n-1} & \dots & c_2 \\ c_2 & c_1 & c_0 & \dots & c_3 \\ & \dots & & & \\ c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_0 \end{bmatrix}} = \left(c_{i-j \bmod n} \right)_{i,j=0,\dots,n-1}$$

(i) (j)

(b) $G = \mathbb{Z}/n\mathbb{Z}$. Sei $c \in \mathbb{C}^G$. Definiere den Faltungsoperator $A_c : \mathbb{C}^G \to \mathbb{C}^G$ durch $A_c f = c * f$

Lemma Darstellungsmatrizen von Faltungsoperatoren $\overset{1-1}{\cong}$ zyklische Matrizen.

Bew.: Der (i,j)-te Eintrag der Darstellungsmatrix von A_c in der δ-Basis ist gleich

$$(A_c \delta_j)(i) = (c * \delta_j)(i) = \sum_{x \in G} c(x)\, \delta_j(i-x) = c(i-j).$$

($\delta_j(i-x) = 1 \Leftrightarrow j = i-x$) ∎

Satz Sei $C \in \mathbb{C}^{n \times n}$ eine zyklische Matrix. Die Eigenwerte von C sind $\hat{c}(0), \dots, \hat{c}(n-1)$, die zugehörigen Eigenvektoren sind $\chi_0, \chi_1, \dots, \chi_{n-1}$.

Bew.: Wähle zu $C \in \mathbb{C}^{n \times n}$ das zugehörige $c \in \mathbb{C}^n$ mit $Cf = A_c f$.

$$\begin{aligned} C\chi_i(j) &= (A_c \chi_i)(j) \\ &= (c * \chi_i)(j) \\ &= \sum_{x \in G} c(x)\, \chi_i(j-x) \\ &= \sum_{x \in G} c(x)\, \chi_i(j)\, \chi_{-i}(x) \\ &= \langle c, \chi_i \rangle\, \chi_i(j) \\ &= \hat{c}(i)\, \chi_i(j). \end{aligned}$$

⊠

Konsequenz Lineare Algebra mit zyklischen Matrizen via FFT

1) Berechnung der Eigenwerte: $O(n \log n)$
2) Matrix-Vektor-Multiplikation: $O(n \log n)$
3) Lösung eines LGS: $O(n \log n)$

Ähnliche Ansätze für Toeplitz- oder Hankelmatrizen möglich.
Toeplitz: $A = (a_{i-j})_{ij}$, Hankel: $A = (a_{i+j})_{ij}$

2. Schnelles Multiplizieren von Polynomen

$$p(x) = \sum_{i=0}^{n-1} p_i x^i \qquad q(x) = \sum_{i=0}^{n-1} q_i x^i \qquad \text{Polynome}$$

$$pq(x) = \sum_{i=0}^{2n-2} \underbrace{\left(\sum_{j=0}^{i} p_j q_{i-j} \right)}_{\text{sieht (fast) aus wie eine Faltung.}} x^i \qquad O(n^2) \text{ Multiplikationen}$$

Idee: Fasse $(p_0, \dots, p_{n-1})$, $(q_0, \dots, q_{n-1})$ als die ersten n Koeffizienten eines Vektors in $\mathbb{C}^G$ mit $G = \mathbb{Z}/m\mathbb{Z}$, $m \geq 2n-1$ auf. Setze die restlichen Koeffizienten gleich Null.

Dann

$$pq(x) = \sum_{i=0}^{m-1} \underbrace{(p * q)(i)}_{\sum_{j=0}^{m-1} p_j q_{i-j}} x^i$$

Da $p * q = \hat{p} \cdot \hat{q}$ gilt und da $(p * q)(i) = \frac{1}{m} \widehat{p * q}(-i)$ ist, kann man $p * q$ mit Hilfe der FFT in Zeit $O(m \log m) = O(n \log n)$ berechnen.

§5 Die lineare Programmierungsschranke von Delsarte

Ziel: Suche obere Schranken für

$$A_q(n,d) = \max\{M : \exists\ (n,M,d)\text{-Code über } \mathbb{F}_q\}.$$

Die LP-Schranke von Delsarte (1973) ist die z. Zt. stärkste allg. obere Schranke.

Beruht auf notwendige Bedingungen an die Autokorrelationsfkt. eines Codes $C \subseteq \mathbb{F}_q^n$.

Def.: Sei $C \subseteq \mathbb{F}_q^n$. Die charakteristische Fkt von C ist

$$1_C : \mathbb{F}_q^n \to \{0,1\}, \quad 1_C(x) = \begin{cases} 1, & \text{falls } x \in C \\ 0, & \text{sonst.} \end{cases}$$

Die Autokorrelationsfkt. von C ist

$$\varphi_C(x) = \frac{1}{q^n}(1_C * \tilde{1}_C)(x),$$

wobei $\tilde{1}_C(x) = 1_C(-x)$, und somit

$$\varphi_C(x) = \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} 1_C(y)\, 1_C(y-x) = \delta(C \cap (x+C)),$$

wobei $\delta(A) = \frac{|A|}{q^n}$ die Dichte einer Menge $A \subseteq \mathbb{F}_q^n$ ist.

Lemma (Eigenschaften der Autokorrelationsfkt.)
Sei $C \subseteq \mathbb{F}_q^n$ ein (n, M, d)-Code. Dann gilt

(a) $\varphi_C(0) = \delta(C)$

(b) $\varphi_C(x) = 0$, für $x \in \mathbb{F}_q^n$ mit $wt(x) \in \{1, \dots, d-1\}$.

(c) Die Matrix $(\varphi_C(x-y))_{x,y \in \mathbb{F}_q^n}$ ist positiv semidefinit

(d) Für $N \in \mathbb{N}$ definiere das Boolean Quadratic Polytope (BQP) durch

$$\mathcal{B}_N = \operatorname{conv}\{vv^T : v \in \{0,1\}^N\}$$

Sei $\sum_{i=1}^{N} \sum_{j=1}^{N} v_{ij} X_{ij} \leq \beta$ eine gültige Ungleichung für $\mathcal{B}_N$, d.h. sie gilt für alle $X \in \mathcal{B}_N$. Dann gilt für alle $x_1, \dots, x_N \in \mathbb{F}_q^n$ die Ungleichung

$$\sum_{i=1}^{N} \sum_{j=1}^{N} v_{ij} \varphi_C(x_i - x_j) \leq \beta.$$

Bew.: (a), (b): ✓