(c): Es gilt

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

$$= \frac{1}{q^n} \sum_{z \in \mathbb{F}_q^n} 1_C(z-y)\, 1_C(z-x),$$

$$= \frac{1}{q^n} \sum_{z \in \mathbb{F}_q^n} 1_{y+C}(z)\, 1_{x+C}(z)$$

d.h.

$$\left(\varphi_C(x-y)\right)_{xy} = \left(\langle 1_{x+C}, 1_{y+C} \rangle \right)$$

ist eine Gram-Matrix des Skalarprodukts

$$\langle f, g \rangle = \frac{1}{q^n} \sum_{z \in \mathbb{F}_q^n} f(z)\, g(z).$$

(d) Es gilt

$$\sum_{i=1}^{N} \sum_{j=1}^{N} V_{ij}\, \varphi_C(x_i - x_j) = \frac{1}{q^n} \sum_{z \in \mathbb{F}_q^n} \overbrace{\sum_{i=1}^{N} \sum_{j=1}^{N} V_{ij}\, 1_{x_i+C}(z)\, 1_{x_j+C}(z)}^{\leq \beta \text{, weil } \left(1_{x_i+C}(z) 1_{x_j+C}(z)\right)_{ij} \in \mathcal{B}_N}$$

$$\leq \beta.$$

$\boxtimes$

(e) $\sum_{x \in \mathbb{F}_q^n} \sum_{y \in \mathbb{F}_q^n} \varphi(x-y) = |C|^2.$

Bew.: (e)

$$\sum_{x \in \mathbb{F}_q^n} \sum_{y \in \mathbb{F}_q^n} \varphi(x-y) = \sum_x \sum_y \frac{1}{q^n} \sum_z 1_C(z) 1_C(z+x-y)$$

$$= \frac{1}{q^n} \sum_z \sum_{x,y} 1_C(z+y) 1_C(z+x)$$

$$= \sum_{x,y} 1_C(x) 1_C(y)$$

$$= \Big(\sum_x 1_C(x) \Big)^2$$

$$= |C|^2. \qquad \boxtimes$$

<u>Lemma</u> Das folgende semidefinite Optimierungsproblem liefert eine obere Schranke für $A_q(n,d)$:

$$A_q(n,d) \leq \max \langle J, X \rangle$$
$$X \in S_{\succeq 0}^{\mathbb{F}_q^n}$$
$$\langle I, X \rangle = 1$$
$$X_{xy} = 0 \quad \text{falls } w(x-y) \in \{1, \dots, d-1\},$$

dabei ist $\langle A, B \rangle = \mathrm{Tr}(AB) = \sum_i \sum_j A_{ij} B_{ij}$, $J = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{bmatrix}$,

$I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

Bew.: folgt unmittelbar aus (a), (b), (c), (e). ⊠

Bem.: (i) Das Optimierungsproblem ist ein Bsp. für die Thetafkt. von Lovász (→ VL Konvexe Optimierung)

(ii) Es hat exponentielle Größe. Ziel: Vereinfache zu einem linearen Programm mit linearer Größe.

(iii) Schnellkurs: Konische Optimierung

Sei E ein euklidischer Vektorraum mit Skalarprodukt $\langle x,y\rangle$.
Sei $K \subseteq E$ ein ordentlicher konvexer Kegel, d.h. K ist abgeschlossen, voll-dimensional, spitz ($K \cap (-K) = \{0\}$).
Der zu K duale Kegel $K^* = \{y \in E : \langle x,y\rangle \geq 0 \ \forall x \in K\}$ ist ebenfalls ordentlich.

gegeben: $c \in E$, $a_1, \dots, a_m \in E$, $\beta_1, \dots, \beta_m \in \mathbb{R}$.

primales konisches Programm:

$$p^* = \sup \langle c, x\rangle$$
$$x \in K$$
$$\langle a_j, x\rangle = \beta_j, \quad j = 1, \dots, m$$

duales konisches Programm:

$$d^* = \inf \sum_{j=1}^m \beta_j y_j$$
$$\sum y_j a_j - c \in K^*$$

Satz (a) (schwache Dualität)

$$p^* \leq d^*$$

(b) (starke Dualität)

Ang. primalen & dualen konische Programm haben zulässige Lösungen, die im Inneren von K bzw. K^* liegen, dann ist $p^* = d^*$; sup = max, inf = min.

(c) Für die Kegel $K = \mathbb{R}^n_{\geq 0}$ (nichtnegativer Orthant / LP) oder $K = S^n_{\geq 0}$ (semidefinite Matrizen (SDP)), kann man konische Programme effizient lösen. (→ Ellipsoid-Methode, Innere-Punkt-Methode)

Bew.: nur (a) ist einfach:

$$\sum_j \beta_j y_j - \langle c, x\rangle = \sum_j \langle a_j, x\rangle y_j - \langle c, x\rangle$$

$$= \langle \underbrace{\sum_j a_j y_j - c}_{\in K^*}, \underbrace{x}_{\in K} \rangle \geq 0.$$

(b), (c): → VL OR, Konvexe Optimierung. $\boxtimes$

Zurück zu

$$A_q(n,d) \leq \max \langle J, X \rangle$$
$$X \in S^{\mathbb{F}_q^n}_{\geq 0}$$
$$\langle I, X \rangle = 1$$
$$X_{xy} = 0 \,, \quad \text{falls } w(x-y) \in \{1, \ldots, d-1\}$$

<u>1. Schritt</u>: Transformiere / Vereinfache: SDP $\to$ LP

<u>Vereinfachung der Notation</u>: Sei ab jetzt $q = p$ prim.

Wähle Gruppe: $G = (\mathbb{Z}/p\mathbb{Z})^n$. DFT funktioniert wie bisher. Charaktere sind für $x, y \in G$

$$\chi_x(y) = e^{\frac{2\pi i\, x\cdot y}{p}} \,, \quad \text{mit } x \cdot y = \sum_{i=1}^{p} x_i y_i \mod p.$$

Eine Matrix $A \in \mathbb{C}^{G \times G}$ heißt G-zyklisch, falls $\exists\, a \in \mathbb{C}^G$ mit $A_{xy} = a_{x-y}$.

Eigenwerte von A sind $\hat{a}(x) = \langle a, \chi_x \rangle$.

Zugehörige Eigenvektoren sind χ_x.

D.h. $\boxed{A_{xy} = \frac{1}{|G|} \sum_z \hat{a}(z)\, \chi_z(x-y).}$

<u>Idee</u>: Verwende $\hat{a}(z)$ als Optimierungsvariablen

Dann

- $A \in S^{\mathbb{F}_p^n}_{\geq 0} \iff \hat{a}(z) \geq 0$ für $z \in \mathbb{F}_p^n$.

- $$\langle J, A \rangle = \sum_{x,y} \frac{1}{p^n} \sum_z \hat{a}(z)\, \chi_z(x-y)$$

$$= \frac{1}{p^n} \sum_z \hat{a}(z) \sum_{x,y} \chi_z(x)\, \chi_z(-y)$$

$$= \frac{1}{p^n} \sum_z \hat{a}(z) \underbrace{\Big(\sum_x \chi_z(x)\Big)}_{= \begin{cases} p^n, & \text{falls } z=0 \\ 0, & \text{sonst} \end{cases}} \underbrace{\Big(\sum_y \chi_z(-y)\Big)}_{= \begin{cases} p^n, & \text{falls } z=0 \\ 0, & \text{sonst} \end{cases}}$$

$$= p^n \ \hat{a}(0).$$

- $$\langle I, A \rangle = \sum_x \frac{1}{p^n} \sum_z \hat{a}(z)\, \underbrace{\chi_z(x-x)}_{=1}$$

$$= \sum_z \hat{a}(z)$$

Zusammen:

$$A_p(n,d) \leq \max \ p^n \hat{a}(0)$$
$$\hat{a}(z) \geq 0, \quad z \in \mathbb{F}_p^n$$
$$\sum_z \hat{a}(z) = 1$$
$$\sum_z \hat{a}(z)\, \chi_z(x-y) = 0, \quad \text{falls } w(x-y) \in \{1, \dots, d-1\}.$$