Kapitel 3 Schranken für Codes

§ 1 Elementare Schranken

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

Satz (Hamming-Schranke)

$$A_q(n,d) \leq q^n \Big/ \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i$$

Satz (Singleton-Schranke)

$$A_q(n,d) \leq q^{n-d+1}$$

Satz (Gilbert-Varshamov-Schranke)

$$A_q(n,d) \geq q^n \Big/ \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i.$$

Bew.: Sei $C \subseteq \mathbb{F}_q^n$ ein maximaler (n, M, d)-Code.
D.h. für alle $x \in \mathbb{F}_q^n$ gibt es ein $c \in C$ mit $d(x,c) \leq d-1$. I.a.W. die Hamming-Kugeln vom

Radius $d-1$, deren Mittelpunkte die Codewörter $c \in C$ sind, überdecken ganz $\mathbb{F}_q^n$. Also folgt die Beh.

$$M \cdot \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^n. \qquad \boxtimes$$

Satz (Plotkin - Schranke)

Sei $\Theta = 1 - \frac{1}{q}$. Für $d > \Theta n$ gilt

$$A_q(n,d) \leq \frac{d}{d - \Theta n}.$$

Bew.: Schreibe $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$. Sei $C = \{c_1, \dots, c_M\}$ ein (n, M, d) - Code. Dann gilt

einerseits

$$\sum_{i \neq j} d(c_i, c_j) \geq d\, M(M-1)$$

und andererseits

$$\sum_{i \neq j} d(c_i, c_j) = \sum_{i \neq j} \sum_{k=1}^{n} \underbrace{d(c_{i,k}, c_{j,k})}_{\in \{0,1\}}.$$

Für festes $k \in \{1, \dots, n\}$ gilt mit $m_\tau = \{i : c_{i,k} = \alpha_\tau\}$, $\tau = 1, \dots, q$

$$\sum_{i \neq j} d(c_{i,k}, c_{j,k}) = \sum_{r=1}^{q} m_r (M - m_r)$$

$$= M \sum_{r=1}^{q} m_r - \sum_{r=1}^{q} m_r^2$$

$$= M^2 - \sum_{r=1}^{q} m_r^2 .$$

Cauchy - Schwarz liefert

$$\left(\sum_{r=1}^{q} m_r \right)^2 \leq q \sum_{r=1}^{q} m_r^2$$

Also

$$\sum_{i \neq j} d(c_{i,k}, c_{j,k}) \leq M^2 - \frac{1}{q} \left(\sum_{r=1}^{q} m_r \right)^2$$

$$= M^2 - \frac{1}{q} M^2 = \theta M^2 .$$

Zusammen

$$d M(M-1) \leq n \theta M^2$$

Also, falls $d > n\theta$

$$M \leq \frac{n}{d - \theta n} .$$

$\boxtimes$

§2 Diskrete Fourier Transformation

Hier: Betrachte Gruppe $G = \mathbb{Z}/n\mathbb{Z}$

(allgemeine Theorie für G = endl. abelsche Gruppe
→ VL MPDM)

Def.: $\mathbb{C}^G = \{ f : G \to \mathbb{C} \}$

= Komplexwertige Fkt. auf G

= Vektoren, indiziert durch G.

ist $|G|$-dimensionaler $\mathbb{C}$-VR mit Skalarprodukt

$$\langle f, g \rangle = \sum_{x \in G} f(x)\, \overline{g(x)}, \qquad f, g \in \mathbb{C}^G.$$

Ausgezeichnete Basis: Deltafunktionen = Standardbasisvektoren

$\delta_x \in \mathbb{C}^G$, $x \in G$

$$\delta_x(y) = \begin{cases} 1, & \text{falls } y = x \\ 0, & \text{sonst.} \end{cases}$$

$[\delta_x = e_x.]$ Deltafunktionen sind eine Orthonormalbasis von $\mathbb{C}^G$.

Def.: Seien $f, g \in \mathbb{C}^G$. Die **Faltung** ("convolution") $f * g \in \mathbb{C}^G$ ist definiert als

$$(f*g)(x) = \sum_{y \in G} f(y)\, g(x-y), \qquad x \in G.$$

Lemma (i) $f * g = g * f$

(ii) $f * (g * h) = (f * g) * h$.

(iii) $\delta_x * \delta_y = \delta_{x+y}$

(iv) $(f * \delta_x)(y) = f(y-x)$

Bew.: direktes Nachrechnen, z.B.

$$(iv)\quad (f*\delta_x)(y) = \sum_{a \in G} f(a)\, \underbrace{\delta_x(y-a)}_{= \begin{cases} 1, & x = y-a \\ 0, & \text{sonst} \end{cases}}$$

$$x = y-a \iff a = y-x. \qquad \boxtimes$$

Zweite ausgezeichnete Basis: Charaktere = Exponentialfkt.

Def.: Seien $a, x \in G$. Definiere $\chi_a \in \mathbb{C}^G$ durch

$$\chi_a(x) = e^{\frac{2\pi i\, a \cdot x}{n}}.$$