Prof. Dr. Wolfgang Willems
David Lorch
Sebastian Thomas

SS 2009
26.08.2009

Codierungstheorie

Vorlesung 2

(1.12) Singleton-Schranke. $d \leq n - k + 1$.

Beweis. $\pi\colon K^n \to K^{n-d+1}, a \mapsto (a_1, \ldots, a_{n-d+1})$. $\pi|_C\colon C \to K^{n-d+1}$ ist injektiv: Sei $c \in C$ mit $\pi(c) = 0$. Dann folgt $c_1 = \cdots = c_{n-d+1} = 0$, also $\mathrm{wt}(c) \leq d - 1$ und damit $c = 0$. Es folgt $k = \dim C = \dim \pi(C) \leq \dim K^{n-d+1} = n - d + 1$ und damit $d \leq n - k + 1$. □

(1.13) Definition. Ein $[n, k, d]$-Code, für den $d = n - k + 1$ gilt (also die Singleton-Schranke erreicht wird), heißt *MDS-Code* (maximum distance separable code).

(1.14) Hamming-Schranke. Sei C ein $[n, k, d]$-Code über $K = \mathbb{F}_q$. Sei $2e + 1 \leq d$ für $e \in \mathbb{N}_0$. Dann gilt: $(*)$ $q^n \geq q^k \sum_{j=0}^{e} \binom{n}{j}(q-1)^j$ (falls „=“: Kugelpackungsgleichung).
Gleichheit in $(*)$ gilt genau dann, wenn $K^n = \dot{\bigcup}_{c \in C} \mathrm{B}_e(c)$.

Beweis. $e \leq \frac{d-1}{2}$, d.h. $\mathrm{B}_e(c) \cap \mathrm{B}_e(c') = \emptyset$ für $c, c' \in C$ mit $c \neq c'$. $K^n \supseteq \dot{\bigcup}_{c \in C} \mathrm{B}_e(c) \Rightarrow q^n = |K^n| \geq |\dot{\bigcup}_{c \in C} \mathrm{B}_e(c)| = \sum_{c \in C} |\mathrm{B}_e(c)| = |C|\,|\mathrm{B}_r(0)| = q^k \sum_{j=0}^{r} \binom{n}{j}(q-1)^j$. □

(1.15) Definition. $C \leq K^n$ heißt *perfekt*, wenn die Kugelpackungsgleichung gilt.

(1.16) Beispiel. Der binäre $[7, 4, 3]$-Hamming-Code aus (1.6) ist perfekt.

Beweis. $2^7 = 2^4 \cdot 2^3 = 2^4(\binom{7}{0} + \binom{7}{1})$. □

(1.17) Satz (Tietäväinen, van Lint, Zinov'ev, Leont'ev, 1973)**.** Neben den trivialen perfekten Codes

- $\{0\}$ $(d = n)$,
- K^n $(d = 1)$,
- $C = \{(0, \ldots, 0), (1, \ldots, 1)\}$, $n = 2e + 1$, $q = 2$,

gibt es nur die folgenden (nicht-trivialen) perfekten $[n, k, d]$-Codes über $K = \mathbb{F}_q$:

(a) $[\frac{q^l - 1}{q-1}, n - l, 3]$ und q beliebig (Hamming-Codes).

(b) $[23, 12, 7]$, $q = 2$ (binärer Golay-Code).

(c) $[11, 6, 5]$, $q = 3$ (ternärer Golay-Code).

Ohne Beweis. □

V endlich-dimensionaler Vektorraum, d sei eine Metrik auf V. Isometriegruppe von V bzgl. d sind Elemente $A \in \mathrm{GL}(V)$, so dass $d(vA, wA) = d(v, w)$ für alle $v, w \in V$.

(1.18) Lemma. Die Isometriegruppe des Hammingraums (K^n, d) ist die *monomiale Gruppe* $\mathrm{M}(n, K) = \{\mathrm{Diag}(a_1, \ldots, a_n)\mathrm{P}(\pi) \mid \pi \in \mathrm{S}_n, a_i \neq 0\}$.

Beweis. Sei $A = (a_{i,j})$ eine Isometrie auf (K^n, d); $\det A \neq 0$.

$$\mathrm{wt}(uA) = \mathrm{d}(uA, 0) = \mathrm{d}(uA, 0A) = \mathrm{d}(u, 0) = \mathrm{wt}(u).$$

Eine Isometrie erhält die Gewichte. Sei $\mathrm{e}_1, \ldots, \mathrm{e}_n$ die Standardbasis des K^n. $1 = \mathrm{wt}(\mathrm{e}_i) = \mathrm{wt}(\mathrm{e}_i A)$. $\mathrm{e}_i A = a_{i'} e_{i'}$ mit geeigneten $i' \in \{1, \ldots, n\}$, $a_{i'} \neq 0$. Die Abbildung $i \mapsto i'$ ist eine Permutation π, da A Isomorphismus. $A = \mathrm{Diag}(a_1, \ldots, a_n)\mathrm{P}(\pi)$. □

(1.19) Definition. Sei C ein $[n, k, d]$-Code über $K = \mathbb{F}_q$.

(a) $C' = CA$ mit $A \in \mathrm{M}(n, K)$ heißt ein zu C *äquivalenter* Code.

(b) $\mathrm{Aut}(C) = \{A \in \mathrm{M}(n, K) \mid CA = C\}$.

§2 Konstruktion guter Codes

(2.1) Hamming-Codes. Sei $K = \mathbb{F}_q$, $2 \leq k \in \mathbb{N}$. $\mathbb{P}^{k-1}(q) = \{\langle u \rangle \mid 0 \neq u^{\mathrm{T}} \in K^k\}$ (projektiver Raum der Dimension $k-1$).
$|\mathbb{P}^{k-1}(q)| = \frac{q^k-1}{q-1} = n$. Seien $h_1, \ldots, h_n$ Vertreter dieser Geraden. Sei $H = \begin{pmatrix} h_1 & \ldots & h_n \end{pmatrix} \in (K)_{k,n}$. Der Code $C = \{c \in K^n \mid Hc^{\mathrm{T}} = 0\}$ heißt ein *Hamming-Code*.
Länge von C ist n. $\dim C = n - k$. Was ist $\mathrm{d}(C)$? Es ist $\mathrm{d}(C) \geq 2$, da je zwei Spalten linear unabhängig. $\mathrm{d}(C) = 3$, da es 3 linear abhängige Spalten gibt (siehe (1.8)). C ist also ein $[\frac{q^k-1}{q-1}, n-k, 3]$-Code über $\mathbb{F}_q$.
Eine andere Auswahl der Vertreter h_i oder andere Anordnung der h_i in der Matrix H führt zu einem äquivalenten Code im Sinn von (1.19).
C ist perfekt: $3 = d = 2e + 1 \Rightarrow e = 1$.

$$|C| \sum_{j=0}^{e} \binom{n}{j} (q-1)^j = q^{n-k}(1 + \frac{q^k - 1}{q-1}(q-1)) = q^n.$$

(2.2) Plotkin-Konstruktion. Seien C_i $[n_i, k_i, d_i]$-Codes über $K = \mathbb{F}_q$, $i = 1, 2$. Definiere $C = C_1 \propto C_2 = \{(c_1, c_1 + c_2) \mid c_i \in C_i\} \leq K^{2n}$. Dann ist C ein $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$-Code über K.

Beweis. Dimension: Betrachte lineare Abbildung $\alpha \colon C_1 \oplus C_2 \mapsto C = C_1 \propto C_2, (c_1, c_2) \mapsto (c_1, c_1 + c_2)$. α ist bijektiv, also ein Isomorphismus, d.h. $\dim C = \dim(C_1 \oplus C_2) = k_1 + k_2$.
Für $u \in K^n$ setze $\mathrm{Tr}(u) = \{i \mid u_i \neq 0\}$. $|\mathrm{Tr}(u)| = \mathrm{wt}(u)$. $c_i \in C_i$, $\mathrm{wt}(c_1) = |\mathrm{Tr}(c_1)| \geq |\mathrm{Tr}(c_1) \cap \mathrm{Tr}(c_2)|$. Sei $0 \neq c = (c_1, c_1 + c_2) \in C$.

$$\mathrm{wt}(c) = \mathrm{wt}(c_1) + \mathrm{wt}(c_1 + c_2) \geq \mathrm{wt}(c_1) + \mathrm{wt}(c_1) + \mathrm{wt}(c_2) - 2|\mathrm{Tr}(c_1) \cap \mathrm{Tr}(c_2)| \geq \mathrm{wt}(c_2) \geq d_2,$$

falls $c_2 \neq 0$. Sei $c_2 = 0$, $c_1 \neq 0 \Rightarrow$

$$\mathrm{wt}(c) = \mathrm{wt}(c_1, c_1) = 2\mathrm{wt}(c_1) \geq 2d_1.$$

$\mathrm{d}(C) \geq \min\{2d_1, d_2\}$. $\mathrm{wt}(c_1) = d_1$ bzw. $\mathrm{wt}(c_2) = d_2 \Rightarrow$ Minimum wird bei $c = (c_1, c_1)$ bzw. $c = (0, c_2)$. □