Prof. Dr. Wolfgang Willems
David Lorch
Sebastian Thomas

SS 2009
28.08.2009

Codierungstheorie
Vorlesung 4

§3 Dualität

Bekannt: Euklidischer Vektorraum $\mathbb{R}^n$, euklidisches Skalarprodukt: $(x,y) = \sum_{i=1}^n x_i y_i$ (positiv definit: $(x,x) \geq 0$). Dualität: $V \leq \mathbb{R}^n$, $V^\perp$ besteht aus den Vektoren senkrecht auf V. $\dim V = k$, $\dim V^\perp = n-k$, ...

(3.1) Definition. Sei K endlicher Körper. $(\cdot,\cdot)\colon K^n \times K^n \to K$, $(u,v) = \sum_{i=1}^n u_i v_i$. $(\cdot,\cdot)$ ist K-linear in jeder Komponente, also bilinear, symmetrisch, und nicht-ausgeartet, d.h. gilt $(u,v) = 0$ für alle $v \in K^n$, so folgt $u = 0$.

(3.2) Definition. Sei K endlicher Körper.

(a) Ist $C \leq K^n$ ein Code, so heißt $C^\perp = \{v \in K^n \mid (v,c) = 0 \text{ für alle } c \in C\}$ der zu C duale Code. Ist $\dim C = k$, so $\dim C^\perp = n-k$.

(b) C heißt *selbstorthogonal*, falls $C \subseteq C^\perp$. C heißt *selbstdual*, falls $C = C^\perp$. Insbesondere ist dann $\dim C = \frac{n}{2}$.

Achtung: $\operatorname{char} K = p$, $p \mid n$, $0 \neq e = (1,\dots,1)$. $(e,e) = n1_K = 0$. Dies kann in euklidischen Räumen nicht passieren!

(3.3) Lemma. Sei $C = C^\perp$ über $K = \mathbb{F}_q$.

(a) Ist $q = 2$, so gilt $2 \mid \operatorname{wt}(c)$ für alle $c \in C$. (C heißt 2-*dividierbar*.)

(b) Sei $q = 2$ und hat C eine Basis mit $4 \mid \operatorname{wt}(c)$ für alle Basisvektoren c, so ist C 4-dividierbar (d.h. $4 \mid \operatorname{wt}(c)$ für alle $c \in C$).

(c) Ist $q = 3$, so ist C 3-dividierbar.

Beweis. Sei $C \leq K^n$.

(a) $0 = (c,c) = \sum_{i=1}^n c_i^2 = \sum_{\substack{i=1 \\ c_i=1}}^n 1 = \operatorname{wt}(c)1_K \Rightarrow 2 \mid \operatorname{wt}(c)$.

(b) Zu zeigen: $4 \mid \operatorname{wt}(v_1)$, $4 \mid \operatorname{wt}(v_2)$, so $4 \mid \operatorname{wt}(v_1+v_2)$. $\operatorname{wt}(v_1+v_2) = \operatorname{wt}(v_1) + \operatorname{wt}(v_2) - 2|\operatorname{Tr}(v_1) \cap \operatorname{Tr}(v_2)|$, $|\operatorname{Tr}(v_1) \cap \operatorname{Tr}(v_2)|1_K = (v_1,v_2) = 0$. □

(c) Übung.

(3.4) Beispiel.

Sei $K = \mathbb{F}_2$ und C erzeugt von

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

$\dim C = 4$, $C = C^\perp$, da die Zeilen von G paarweise orthogonal aufeinander. $4 \mid \operatorname{wt}(c)$ für c aus Basis, also C 4-dividierbar. C ist ein 4-dividierbarer, selbstdualer $[8,4,4]$-Code, er heißt *erweiterter Hamming-Code*.
Sei C_0 der $[7,4,3]$-Hamming-Code (perfekt). Dann ist C (bis auf Äquivalenz) gleich $C = \{(c_1,\dots,c_7,c_8) \mid (c_1,\dots,c_7) \in C_0, \sum_i c_i = 0\}$ (Anfügen eines Paritätscheckbits).

(3.5) Definition. Sei C ein $[n,k,d]$-Code über K, $A_i := \{c \in C \mid \mathrm{wt}(c) = i\}$. $(A_0, \ldots, A_n)$ *Gewichtsverteilung* von C. Beachte: $A_0 = 1$, $A_1 = A_2 = \cdots = A_{d-1} = 0$. Das Polynom $A(x) = \sum_{i=0}^{n} A_i x^i \in \mathbb{Z}[x]$ heißt *Gewichtspolynom* zu C.

(3.6) Beispiel. Der $[7,4,3]$-Hamming-Code hat das Gewichtspolynom $A(x) = 1+7x^3+7x^4+x^7$. Der erweiterte $[8,4,4]$-Hamming-Code hat das Gewichtspolynom $A(x) = 1 + 14x^4 + x^8$.

(3.7) Definition. Sei $(G, \circ)$ eine endliche abelsche Gruppe. $\chi\colon G \to \mathbb{C}^\times$ heißt ein *Charakter*, falls $\chi(g \circ h) = \chi(g)\chi(h)$ für alle $g, h \in G$. Insbesondere ist $\chi(e) = 1$ für e neutrales Element. χ heißt *trivialer Charakter*, falls $\chi(g) = 1$ für alle $g \in G$.

(3.8) Lemma. Sei χ Charakter der endlichen abelschen Gruppe G. Dann

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{falls } \chi \text{ trivialer Charakter,} \\ 0, & \text{sonst.} \end{cases}$$

Beweis. Sei χ nicht-trivial, also $\chi(h) \neq 1$ für ein geeignetes $h \in G$. Dann impliziert

$$(\sum_{g \in G} \chi(g))\chi(h) = \sum_{g \in G} \chi(g)\chi(h) = \sum_{g \in G} \chi(g \circ h) = \sum_{g \in G} \chi(g)$$

die Behauptung. □

(3.9) Lemma. Sei G endliche abelsche Gruppe, $|G| > 1$. Dann hat G einen nicht-trivialen Charakter.

Beweis.

(a) $G = \mathbb{Z}/n\mathbb{Z}$ ist bzgl. + zyklische Gruppe der Ordnung n. Sei ε primitive n-te komplexe Einheitswurzel. Für $g \in \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ setze $\chi(g) = \varepsilon^g$.

$$\chi(g+h) = \chi(l) = \varepsilon(g+h) = \varepsilon(g)\varepsilon(h) = \chi(g)\chi(h),$$

wobei $g + h = l$ modulo n.

(b) Jede abelsche Gruppe hat Faktorgruppe $\mathbb{Z}/p\mathbb{Z}$ für geeignete Primzahl p, also $G/H \cong \mathbb{Z}/p\mathbb{Z}$ ($G \cong \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$). Definiere nicht-trivialen Charakter ψ auf G/H vermöge (a) durch $\psi(gH) = \varepsilon^g$. Definiere nicht-trivialen Charakter χ auf G durch $\chi(g) = \psi(gH)$ für $g \in G$. □

(3.10) Dualitätssatz von Mac Williams. Sei C ein $[n,k]$-Code über $K = \mathbb{F}_q$ mit Gewichtspolynom $A(x)$. Der duale Code $C^\perp$ habe Gewichtspolynom $A^\perp(x)$. Dann gilt

$$A^\perp(x) = q^{-k}(1 + (q-1)x)^n A(\frac{1-x}{1+(q-1)x}).$$

Beweis. Sei χ ein nicht-trivialer Charakter auf K (additive Gruppe). Für $u \in K^n$ setzen wir

$$g_u(x) = \sum_{v \in K^n} \chi((u,v)) x^{\mathrm{wt}(v)} \in \mathbb{C}[x].$$

Dann

$$\sum_{c \in C} g_c(x) = \sum_{c \in C} \sum_{v \in K^n} \chi((c,v)) x^{\mathrm{wt}(v)} = \sum_{v \in K^n} x^{\mathrm{wt}(c)} f(v)$$

mit $f(v) = \sum_{c \in C} \chi((c,v))$; $c \mapsto \chi((c,v))$ Charakter. Nun ist

$$f(c) = \begin{cases} |C|, & v \in C^\perp, \\ 0, & \text{sonst,} \end{cases}$$

nach (3.8). Dies liefert

$$(*) \qquad \sum_{c \in C} g_c(x) = \sum_{c^\perp \in C^\perp} |C| x^{\mathrm{wt}(c^\perp)} = |C| A^\perp(x).$$

Wir betrachten nun $(*)$ nochmals. Für $c \in C$ gilt

$$\begin{aligned} g_c(x) &= \sum_{v \in K^n} x^{\mathrm{wt}(c)} \chi((c,v)) = \sum_{a \in K^n} x^{\sum_{i=1}^n \mathrm{wt}(a_i)} \chi(\sum_{i=1}^n c_i a_i) = \sum_{a \in K^n} \prod_{i=1}^n x^{\mathrm{wt}(a_i)} \chi(c_i a_i) \\ &= \prod_{i=1}^n \sum_{a_i \in K} x^{\mathrm{wt}(a_i)} \chi(c_i a_i). \end{aligned}$$

Da χ nicht-trivialer Charakter ist, folgt $\sum_{a \in K} \chi(a) = 0$, also $\sum_{a \in K^\times} \chi(a) = -1$.

$$\sum_{a \in K} x^{\mathrm{wt}(a)} \chi(c_i a) = \begin{cases} \sum_{a \in K} x^{\mathrm{wt}(a)} = 1 + (q-1)x, & \text{für } c_i = 0, \\ 1x \sum_{a \in K^\times} \chi(a) = 1 - x, & \text{für } c_i \neq 0. \end{cases}$$

Also

$$g_c(x) = (1-x)^{\mathrm{wt}(c)} (1 + (q-1)x)^{n - \mathrm{wt}(c)}.$$

In $(*)$ einsetzen ergibt

$$\begin{aligned} A^\perp(x) &= |C|^{-1} \sum_{c \in C} g_c(x) = q^{-k} (1 + (q-1)x)^n \sum_{c \in C} (\frac{1-x}{1+(q-1)x})^{\mathrm{wt}(c)} \\ &= q^{-k} (1 + (q-1)x)^n A(\frac{1-x}{1+(q-1)x}). \end{aligned}$$

□