Codierungstheorie Vorlesung 5

(3.11) Ausblick. Sei C ein binärer selbstdualer 4-dividierbarer $[n, \frac{n}{2}, d]$ -Code.
 MALLOWS und SLOANE: $d \leq 4 \lfloor \frac{n}{24} \rfloor + 4$ (Invariantentheorie). C heißt *extremal*, falls Gleichheit gilt.
 GLEASON: Ist C extremal, dann $8 \mid n$.
 ZHANG: Ist C extremal, so $n \leq 3928$.
 Beispiel: erweiterter $[8, 4, 4]$ -Hamming-Code, erweiterter $[24, 12, 8]$ -Golay-Code, $[48, 24, 12]$ -QR-Code.
 Frage: Gibt es einen extremalen $[72, 36, 16]$ -Code? Offen seit ungefähr 35 Jahren (SLOANE 1973).
 Das Beste, was wir können ist $n = 136$.

(3.12) Bemerkung. Selbstduale Codes haben Beziehungen zu vielen Gebieten der Mathematik: Gruppentheorie, Invariantentheorie, endliche Geometrie, ...
 Erweiterter $[24, 12, 8]$ -Golay-Code. Automorphismengruppe: M_{24} Mathieu-Gruppe. Zugeordnetes Gitter: Leech-Gitter. Automorphismengruppe des Leech-Gitters: C_1 Conway-Gruppe.
 Definition: Ein *Steiner-System* $S(t, k, n)$ besteht aus einer Menge $\mathcal{P}$ von n Punkten, einer Menge $\mathcal{B}$ von k -elementigen Teilmengen von $\mathcal{P}$, *Blöcke*, und beliebige t Elemente aus $\mathcal{P}$ liegen in genau einem Block.
 Fano-Ebene: $|\mathcal{P}| = n = 7$, Block = Gerade, $k = 3$, $t = 2$, definiert ein $S(2, 3, 7)$ -Steinersystem (gehört zum $[7, 4, 3]$ -Hamming-Code).
 Problem: Bisher sind keine Steinersysteme für $t > 5$ bekannt.
 Satz: Gibt es einen selbstdualen $[2d, d, d]$ -Code mit $A_{d+1} = 0$. Dann gibt es ein $S(d-1, d, 2d)$ -Steinersystem.

§4 Der Peterson-Gorenstein-Zierler-Decoder für BCH-Codes

Sei $K = \mathbb{F}_q$, $K \leq \mathbb{F}_{q^m} = E$. $a_1, \dots, a_n \in E$, $a_i \neq a_j$ für $i \neq j$. $v_1, \dots, v_n \in E$, $v_i \neq 0$ für alle i .

$$H = \begin{pmatrix} v_1 & \dots & v_n \\ a_1 v_1 & \dots & a_n v_n \\ a_1^2 v_1 & \dots & a_n^2 v_n \\ \vdots & & \vdots \\ a_1^{d-2} v_1 & \dots & a_n^{d-2} v_n \end{pmatrix}$$

Vandermonde-Matrix.
 Sei $C \leq K^n$ der durch H als Kontrollmatrix gegebene Code. Ist $K = E$, so ist H bis auf Äquivalenz ein RS-Code, d.h. ist Erzeugermatrix vom Dualcode eines RS-Codes. Der Duale eines RS-Codes ist ein RS-Code. C heißt BCH-Code (BOSE, RAY-CHANDERI, HOQUENGHENI). Die Minimaldistanz von C ist $\geq d$.
 Wir können mit C wenigstens bis zu $\lfloor \frac{d-1}{2} \rfloor$ Fehler korrigieren.

(4.1) Definition. Sei $c \in C$, sei $\tilde{c} = c + f$ mit Fehlervektor f mit $\text{wt}(f) \leq \lfloor \frac{d-1}{2} \rfloor$.

- (a) $s^T = H\tilde{c}^T = Hc^T + Hf^T = Hf^T$ *Syndrom*.
- (b) $F = \text{Tr}(f) = \{i_1, \dots, i_t\}$ *Fehlerpositionen*.
- (c) $\sigma(x) = \prod_{l \in F} (1 - a_l x) = \sigma_0 + \sigma_1 x + \dots + \sigma_t x^t \in E[x]$ *Fehlerortungspolynom*.
 $l \in F \Leftrightarrow \sigma(a_l^{-1}) = 0$.

(4.2) Lemma.

- (a) $s_i = \sum_{l \in F} a_l^{i-1} v_l f_l$ ($i = 1, \dots, d-1$).

(b) $s_i = -\sum_{j=1}^t \sigma_j s_{i-j}$ ($i = t+1, \dots, d-1$) (lineare Rekursionsgleichung).

Beweis.

(a) $\sum_{j=0}^t \sigma_j s_{i-j} = \sum_{j=0}^t \sigma_j (\sum_{l \in F} a_l^{i-j-1} v_l f_l) = \sum_{l \in F} a_l^{i-1} v_l f_l (\sum_{j=0}^t \sigma_j a_l^{-j}) = \sum_{l \in F} a_l^{i-1} v_l f_l \sigma(a_l^{-1}) = 0.$ $\square$

(4.3) Bemerkung. Angenommen, wir kennen $\sigma(x)$ (Fehlerortungspolynom). Dann können wir den Fehler f aus (4.2)(a) berechnen durch

$$\begin{pmatrix} v_{i_1} & \dots & v_{i_t} \\ a_{i_1} v_{i_1} & \dots & a_{i_t} v_{i_t} \\ a_{i_1}^2 v_{i_1} & \dots & a_{i_t}^2 v_{i_t} \\ \vdots & & \vdots \\ a_{i_1}^{t-1} v_{i_1} & \dots & a_{i_t}^{t-1} v_{i_t} \end{pmatrix} \begin{pmatrix} f_{i_1} \\ \vdots \\ f_{i_t} \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_t \end{pmatrix}.$$

Zum Decodieren benötigen wir nur $\sigma(x)$.

(4.4) Lemma. Sei $\eta(x) = 1 + \eta_1 x + \dots + \eta_t x^t \in E[t]$ mit $s_i = -\sum_{j=1}^t \eta_j s_{i-j}$ für $i \in \{t+1, \dots, d-1\}$ (Bedingung in (4.2)(b)). Dann ist $\eta(x) = \sigma(x)$.

Beweis. $0 = \sum_{j=0}^t \eta_j s_{i-j}$ wie in (4.2)(b) $\stackrel{=}{=} \sum_{l \in F} a_l^{i-1} v_l f_l \eta(a_l^{-1})$ für $i \in \{t+1, \dots, d-1\}$. Gleichungssystem mit Koeffizientenmatrix $(a_l^{i-1} v_l)_{\substack{i \in \{t+1, \dots, d-1\} \\ l \in \{1, \dots, t\}}}$. Gleichungen: $d-1-t \geq 2t-t = t$. $\Rightarrow$ Kann $\eta(a_l^{-1}) = 0$ ausrechnen, d.h. $\eta = \sigma$. $\square$

Sei $1 \leq r \leq \lfloor \frac{d-1}{2} \rfloor$.

$$S_r = \begin{pmatrix} s_1 & \dots & s_r \\ s_2 & \dots & s_{r+1} \\ \vdots & & \vdots \\ s_r & \dots & s_{2r-1} \end{pmatrix}.$$

Die ersten t Gleichungen in (4.2)(b) besagen:

$$S_t \begin{pmatrix} \sigma_t \\ \vdots \\ \sigma_1 \end{pmatrix} = - \begin{pmatrix} s_{t+1} \\ \vdots \\ s_{2t} \end{pmatrix}.$$

Wir können $\sigma(t)$ eindeutig bestimmen, wenn S_t regulär ist.

(4.5) Lemma. S_t ist eine reguläre Matrix.

Beweis. $S_t = ABC^T$ (alles $t \times t$ -Matrizen). $A = (a_{h,k})$, $B = (b_{h,k})$, $C = (c_{h,k})$, mit $a_{h,k} = a_{i_k}^{h-1} v_{i_k}$ (Vandermonde-Matrix), $b_{h,k} = \delta_{h,k} f_{i_k}$ (reguläre Diagonalmatrix), $c_{h,k} = a_{i_k}^{h-1}$ (Vandermonde-Matrix). $\square$

Unbekannt ist noch $t = |F|$.

(4.6) Satz. Sei $e = \lfloor \frac{d-1}{2} \rfloor$. Dann ist $t = |F| = \text{rg } S_e$ und S_r für $t < r \leq e$ ist singulär.

Beweis.

$$S_e = \begin{pmatrix} s_1 & \dots & s_e \\ s_2 & \dots & s_{e+1} \\ \vdots & & \vdots \\ s_e & \dots & s_{2e-1} \end{pmatrix}.$$

Wegen (4.5) sind die ersten t Spalten linear unabhängig, also $\text{rg } S_e \geq t$. Sei $t < r \leq e$. Die Gleichungen in (4.2)(b) besagen, dass die r -te Spalte von S_e linear abhängig ist von den vorherigen, d.h. $\text{rg } S_e = t$. $\square$

(4.7) Decodieralgorithmus. c gesendet, $\tilde{c} = c + f$ empfangen (mit $\text{wt}(f) \leq \frac{d-1}{2}$).

- (a) Berechne das Syndrom $s^T = H\tilde{c}^T$. Ist $s = 0$, so ist $c = \tilde{c}$.
- (b) Bestimme $t = \max\{r \in \{1, \dots, \lfloor \frac{d-1}{2} \rfloor \mid \det S_r \neq 0\}$. Sind alle Determinanten gleich 0, so Fehlermeldung und Stop.
- (c) Bestimme $\sigma(x)$ aus

$$S_t \begin{pmatrix} \sigma_t \\ \vdots \\ \sigma_1 \end{pmatrix} = - \begin{pmatrix} s_{t+1} \\ \vdots \\ s_{2t} \end{pmatrix}.$$

- (d) Bestimme die Nullstellen von $\sigma(x)$. Liefert $F = \{i_1, \dots, i_t\}$.
- (e) Berechne f aus

$$\begin{pmatrix} v_{i_1} & \dots & v_{i_t} \\ a_{i_1} v_{i_1} & \dots & a_{i_t} v_{i_t} \\ a_{i_1}^2 v_{i_1} & \dots & a_{i_t}^2 v_{i_t} \\ \vdots & & \vdots \\ a_{i_1}^{t-1} v_{i_1} & \dots & a_{i_t}^{t-1} v_{i_t} \end{pmatrix} \begin{pmatrix} f_{i_1} \\ \vdots \\ f_{i_t} \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_t \end{pmatrix}.$$

- (f) Setze $c = \tilde{c} - f$.

(4.8) Bemerkung. Es gibt andere (effizientere) Decodierverfahren.

- Berlekamp-Massey-Algorithmus.
- Euklidischer Algorithmus.