Prof. Dr. Wolfgang Willems
David Lorch
Sebastian Thomas

SS 2009
27.08.2009

Codierungstheorie

Vorlesung 3

(2.3) Die binären Reed-Muller-Codes $\mathrm{RM}(r,m)$**.** Zu $r \in \mathbb{N}_0$, $m \in \mathbb{N}$ mit $0 \le r \le m$ definieren wir binäre Codes $\mathrm{RM}(r,m)$ mit den Parametern $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$. r heißt *Ordnung* des Codes $\mathrm{RM}(r,m)$.
Sei $K = \mathbb{F}_2$.

- $\mathrm{RM}(0,m)$: $[2^m, 1, 2^m]$ Wiederholungscode $\{(0,\dots,0),(1,\dots,1)\}$. Minimaldistanz: m. Dimension: 1.
- $\mathrm{RM}(m,m)$: K^{2^m}. Minimaldistanz: 1. Dimension: 2^m.
- Für $m = 1, 2, \dots$ und $1 \le r \le m-1$ definieren wir $\mathrm{RM}(r,m) = \mathrm{RM}(r,m-1) \propto \mathrm{RM}(r-1,m-1)$.
  Minimaldistanz: $\min\{2d_1, d_2\} = \min\{2 \cdot 2^{m-1-r}, 2^{m-1-(r-1)}\} = 2^{m-r}$.
  Dimension:

$$\begin{aligned}\dim \mathrm{RM}(r,m) &= \sum_{j=0}^{r} \binom{m-1}{j} + \sum_{j=0}^{r-1} \binom{m-1}{j} = 1 + \sum_{j=1}^{r} \left(\binom{m-1}{j} + \binom{m-1}{j-1}\right) = 1 + \sum_{j=1}^{r} \binom{m}{j} \\ &= \sum_{j=0}^{r} \binom{m}{j}.\end{aligned}$$

(2.4) Bemerkung.

(a) RM-Codes spielten zu Anfang der Codierungstheorie eine Rolle in der Praxis.

Mariner Expeditionen (1969–1976): $\mathrm{RM}(1,5)$. Parameter: $[32, 6, 16]$. Konnte $\lfloor \frac{16-1}{2} \rfloor = 7$ Fehler korrigieren. Jeder Pixel eines Bildes entsprach einem Grauton, und diese je einem Codewort. Man hatte $2^6 = 64$ Grautöne für jeden Pixel zur Verfügung.

(b) Es gibt für RM-Codes viele verschiedene Konstruktionsmöglichkeiten: Auswertungscode (Birkhäuser-Buch), Hadamard-Matrizen, ...

(c) RM-Codes über den Primkörpern $K = \mathbb{F}_p$, p Primzahl.

G endliche elementar-abelsche p-Gruppe: $G_1 = \{e^{\frac{2\pi i k}{p}} \mid k \in \{0,\dots,p-1\}\}$ ist zyklische Gruppe der Ordnung p (wird von einem Element erzeugt). $G = G_1 \times \dots \times G_1$ Gruppe (abelsche Gruppe).

$KG = \{\sum_{g\in G} \lambda_g g \mid \lambda_g \in K\}$ Vektorraum über K mit Basis G. KG heißt *Gruppenalgebra*. $\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_g (\lambda_g + \mu_g) g$. $(\sum_g \lambda_g g)(\sum_g \mu_g g) = \sum_g (\sum_{xy=g} \lambda_x \mu_y) g$.
$J = \{\sum_{g\in G} \lambda_g g \mid \sum_g \lambda_g = 0\} \le KG$ Ideal, d.h. $j_1 + j_2 \in J$ für $j_i \in J$, $bja \in J$ für $j \in J$, $a, b \in KG$, denn: $(\sum_g \lambda_g g)h = \sum_g \lambda_g gh = \sum_x \lambda_{xh^{-1}} x \in J$ für alle h. J heißt das *Jacobson-Radikal* von KG.

J ist nilpotent: $J^{m(p-1)+1} = \{\sum j_1 j_2 \dots j_{m(p-1)+1} \mid j_i \in J\} = \{0\}$, denn $(g-1)^p = g^p - 1 = 1 - 1 = 0$.

$KG = J^0 > J > J^2 > \dots > J^{m(p-1)} > J^{m(p-1)+1} = \{0\}$.

$\mathrm{RM}(r,m) = J^{m(p-1)-r} \subseteq KG$.

(2.5) Die Reed-Solomon-Codes RS. Sei $K = \mathbb{F}_q$, $1 \le k \le n \le q$.
$K[x]_{k-1} = \{f \in K[x] \mid \operatorname{grad} f \le k-1\}$ Vektorraum. $\dim K[x]_{k-1} = k$. Sei $\mathcal{M} = \{a_1, \dots, a_n\} \subseteq K$ mit $a_i \ne a_j$ für $i \ne j$.
Code $C := C_{\mathcal{M}} = \{(f(a_1), \dots, f(a_n)) \mid f \in K[x]_{k-1}\} \le K^n$ *Reed-Solomon-Code.*
Was ist die Dimension von C? $\alpha\colon K[x]_{k-1} \to C, f \mapsto c_f = (f(a_1), \dots, f(a_n))$ surjektive lineare Abbildung. α ist auch injektiv, da ein Polynom vom Grad $k-1$ höchstens $k-1$ Nullstellen haben kann (beachte: $k-1 < n$). Also

$\dim C = \dim K[x]_{k-1} = k$. Was ist $\mathrm{d}(C)$? Da grad $f \leq k-1$ hat c_f höchstens $k-1$ Nullen, d.h. $\mathrm{wt}(c_f) \geq n-k+1$.
Singleton: $\mathrm{d}(C) \leq n-k+1$. $\Rightarrow \mathrm{d}(C) \leq n-k+1$. $\mathrm{wt}(c_f) = n-k+1$ für $f = \sum_{i=1}^{k-1}(x-a_i)$.
Parameter des RS-Codes: $[n, k, n-k+1]$. Dies sind MDS-Codes.
Erzeugermatrix:

$$\begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ a_1^2 & \dots & a_n^2 \\ \vdots & & \vdots \\ a_1^{k-1} & \dots & a_n^{k-1} \end{pmatrix}$$

Für die Erzeugermatrix

$$\begin{pmatrix} 1 & \dots & 1 & 0 \\ a_1 & \dots & a_n & 0 \\ a_1^2 & \dots & a_n^2 & 0 \\ \vdots & & \vdots & \vdots \\ a_1^{k-1} & \dots & a_n^{k-1} & 1 \end{pmatrix}$$

erhält man einen $[n+1, k, n-k+2]$-MDS-Code (da je k Spalten linear unabhängig, vgl. Vandermonde-Determinante).

(2.6) Die MDS-Vermutung. Sei $2 \leq k \leq q-1$. Ist C ein $[n,k]$-MDS-Code über $\mathbb{F}_q$, so gilt:

$$n \leq \begin{cases} q+2, & \text{falls } q \text{ gerade}, k = 3 \text{ oder } k = q-1, \\ q+1, & \text{sonst.} \end{cases}$$

(2.7) Beispiel. Sei $K = \mathbb{F}_q = \{a_1, \dots, a_q\}$, $q = 2^l$.
Die Erzeugermatrix

$$\begin{pmatrix} 1 & \dots & 1 & 0 & 0 \\ a_1 & \dots & a_q & 0 & 1 \\ a_1^2 & \dots & a_q^2 & 1 & 0 \end{pmatrix}$$

liefert einen MDS-Code mit Parametern $[q+2, 3, q]$.
Zu testen: alle 3×3-Untermatrizen sind regulär.

- Es ist

  $$\begin{pmatrix} 1 & 1 & 1 \\ a_i & a_j & a_r \\ a_i^2 & a_j^2 & a_r^2 \end{pmatrix}$$

  regulär, da Vandermonde.

- Es ist

  $$\det \begin{pmatrix} 1 & 1 & 0 \\ a_i & a_j & 0 \\ a_i^2 & a_j^2 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 \\ a_i^2 & a_j^2 \end{pmatrix} = a_i^2 - a_j^2 = (a_i - a_j)^2 \neq 0,$$

  da $\mathrm{char}\, K = 2$.

- Es ist

  $$\det \begin{pmatrix} 1 & 1 & 0 \\ a_i & a_j & 1 \\ a_i^2 & a_j^2 & 0 \end{pmatrix} = -\det \begin{pmatrix} 1 & 1 \\ a_i^2 & a_j^2 \end{pmatrix} = a_j^2 - a_i^2 = (a_j - a_i)^2 \neq 0,$$

  da $\mathrm{char}\, K = 2$.

- Es ist

$$\det \begin{pmatrix} 1 & 0 & 0 \\ a_i & 0 & 1 \\ a_i^2 & 1 & 0 \end{pmatrix} = -1.$$

(2.8) Weitere interessante Codes. Binärer perfekter $[23, 12, 7]$-Golay-Code. Ternärer perfekter $[11, 6, 5]$-Golay-Code.
Elferwette Fußballtoto: 11 Spiele; 0, 1, 2. 0 = unentschieden, 1 = Heimsieg, 2 = Auswärtssieg.
Anzahl Tipps: 11 Richtige: $3^{11} = 177147$.
Tippen den ternären Golay-Code: wenigstens 9 Richtige. Tipps: $3^6 = 729$.
Leute mit Fußballverstand: Man wählt eine Bank von 3 Spielen. Für die restlichen 8 Spiele wählt man 2 ternäre $[4, 2, 3]$-Hamming-Codes. Man macht jeweils höchstens 1 Fehler, hat also 9 Richtige (sofern die ersten 3 Spiele richtig getippt sind). Tipps: $3^2 \cdot 3^2 = 81$.