Prosem Kodierungstheorie 14.6.21

§ 9 Perfekte Codes (lin & nicht lin!)

Def: C q-närer (ggf. lin) Code (ggf. über $\mathbb{F}_q$)

Min'dist ↙

$d(C) = 2t+1$ (t-fehlerkorrigierend)

Länge n (ggf. $C \leq \mathbb{F}_q^n$ ein UVR)

C heißt perfekt, falls:

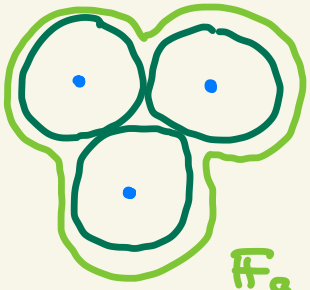
C ist ein $(n, M, 2t+1)$-Code

(n: Länge, M: $|C|$, $2t+1$: $d(C)$ Min'dist)

und

$$M\left(1 + (q-1)n + (q-1)^2\binom{n}{2} + \ldots + (q-1)^t\binom{n}{t}\right) = q^n$$

⊛



„Sphere-packing"-Bedingung

(≤ gilt immer)

$$\mathbb{F}_q^n = \bigcup_{x \in C} S(x,t)$$

$S(x,t) = \{y \mid d(x,y) \leq t\}$

- „beste Codes" für feste $n, d = 2t+1$
- ⇝ Design-Theorie, (Automorphismen-) Gruppen

Klassifikationsprobleme

Golay ~ 1949

1) welche $(n, M, d)_q$ (für perfekte Codes)?

2) welche Codes (bis auf Äquivalenz)?

⇝ Thm 9.5 (van Lint, Tietäväinen 1973):

vollst Antwort für

q Primzahlpotenz

Bem

(1) „triviale perfekte Codes"

(i) binärer Wiederholungscode

$\{\underbrace{0\dots0}_{n}, \underbrace{1\dots1}_{n}\}$ $\quad n = 2t+1$

2) ein $[n, 1, n]$-Code über $\mathbb{F}_2$

$$\left(2^1 \cdot \left(1 + n + \binom{n}{2} + \dots + \binom{n}{\frac{n-1}{2}} \right) \overset{\checkmark}{=} 2^n \right)$$

$$= \frac{1}{2}(1+1)^n = 2^{n-1}$$

?? (ii) nur ein Elmt, für $d(C) = 2n+1$ per Def...

$$1 \cdot \left(\underbrace{1 + \dots + (q-1)^n}_{(1+(q-1))^n} \right) = q^n$$

ein $[n, 0, ?]$-Code über $\mathbb{F}_q$

(iii) ganz $\mathbb{F}_q^n$ ⇝ ein $[n, n, 1]$-Code über $\mathbb{F}_q$

$(q^w \cdot 1 \overset{\checkmark}{=} q^w)$

$1 = 2 \cdot 0 + 1$ ($k = 0$)

(2) q-näre Hamming-Codes $Ham(r, q)$

ein $[n, n-r, 3]$-Code über $\mathbb{F}_q$

$r \geq 2$

q Primzahlpotenz

$\downarrow$

$(n, M, d) =$

$\left(\frac{q^r - 1}{q-1}, q^{n-r}, 3 \right)$

zB: • $r = 2, q = 2$ $(3, 2^1, 3)$-Code

mit Prüfmatrix

$$H = \left(\begin{array}{c|cc} 1 & 1 & 0 \\ 1 & 0 & 1 \end{array} \right)$$

(I_2)

und Erz'matrix (transponieren)

$$G = \left(\begin{array}{c|cc} 1 & 1 & 1 \end{array} \right)$$

(I_1)

• $r = 3, q = 2$ $\rightsquigarrow$ $(7, 2^4, 3)$-Code

$H = \ldots$ $G = \ldots$

$\left(q^{n-r} \left(1 + (q-1) \underbrace{\frac{q^r - 1}{q-1}}_{n} \right) = q^{n-r} \cdot q^r \overset{\checkmark}{=} q^n \right)$

§ Wie kann man (neue) perfekte Codes finden?

1. Schritt suche Lösungen (n, M, d) ($d = 2t+1$) für ⊛ !

Golay (1949): zusätzlich zu den bereits bekannten Parametern:

$(23, 2^{12}, 7)$, $(90, 2^{78}, 5)$ $q=2$

$(11, 3^6, 5)$ $q=3$

G_{23} über $\mathbb{F}_2$ — G_{11} über $\mathbb{F}_3$ — keine Codes

ein nicht-ein

Thm 9.2 bzw 9.7

ex keine (perfekte) binären Codes für die Parameter $(90, 2^{78}, 5)$!

Bew (für ein Situation):

zeige: es ex kein $[90, 78, \underbrace{5}_{=2\cdot 2+1}]$-Code über $\mathbb{F}_2$.

$\left(2^{78} \cdot \left(\underbrace{1 + 90 + \binom{90}{2}}_{91 + 45\cdot 89 = 4096} \right) = 2^{78} \cdot 2^{12} = 2^{90} \checkmark \right)$

WA: $H \in \mathrm{Mat}_{12,90}(\mathbb{F}_2)$ Prüfmatrix für solch ein C

$= (H_1 \mid \dots \mid H_{90})$ $H_i \in \mathbb{F}_2^{12}$

$d(C) = 5 \xrightarrow{(8.4)} H_i, H_j, H_k, H_\ell$ für $i<j<k<\ell$

$\mathbb{F}_2$-Linearkombinationen

$\rightsquigarrow \quad X = \{0\} \cup \{H_1, \dots, H_{90}\}$

$\cup \{H_i + H_j \mid i<j\}$

$|X| = 1 + 90 + \binom{90}{2} = 2^{12}$

$\rightarrow \quad X = \mathbb{F}_2^{12}$

sing.: $\#\{v \in X \mid w(v) \equiv_2 0\}$

$= \#\{v \in X \mid w(v) \equiv_2 1\} = \boxed{2^{11}}$

andererseits: $m = \#\{i \mid w(H_i) \equiv_2 1\}$

$90 - m = \#\{i \mid w(H_i) \equiv_2 0\}$

$\overset{\S 2}{\rightsquigarrow} \quad w(H_i + H_j) \equiv_2 w(H_i) + w(H_j)$

$\#\{v \in X \mid w(v) \equiv_2 1\} = m + m(90-m)$

$= \boxed{m(91-m)}$

$\rightarrow \quad 2^{11} = \underbrace{m}_{\text{2-er Potenzen, sing.} \equiv_2 0} (91-m)$ ↯ //

§ Der binäre Golay $[23, 12, 7]$-Code über $\mathbb{F}_2$

(ein zyklischer Code) (Golay 1949)

Bem (§2):

ex $[23, 12, 7]$-Code C $\Leftrightarrow$ ex $[24, 12, 8]$-Code $\hat{C}$

→ Prüfziffer hinzufügen

← gerade Koord streichen

Thm 9.3 G_{24} $(= \hat{G}_{23})$ mit Erz'matrix $(I_{12} \mid A)$

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & & & & & & & & & & & \\ \vdots & & & & & & & & & & & \\ 1 & & & & & & & & & & & \\ 1 & & & & & & & & & & & \end{pmatrix} \in \mathrm{Mat}_{12}(\mathbb{F}_2)$$

$\in \mathbb{F}_2^{11}$

= zyklischen Vertauschungen von

ist ein lin $[24, 12, 8]$-Code ✓ ✓ ↑ ?? über $\mathbb{F}_2$.

dann:

Lem 1: $G_{24}^{\perp} = G_{24}$ selbstdual ✓

Lem 2: $(A \mid I_{12})$ auch Erz-Matrix für G_{24}

$(A^t \mid I_{12})$ Prüfmatrix, damit Erz'matrix für $G_{24}^{\perp} = G_{24}$

Lem 3: $\forall\, v \in G_{24}: \; 4 \mid w(v)$

per Induktion ✓

Lem 4: kein $v \in G_{24}$ hat $w(v) = 4$

$v = (\underbrace{L}_{x_1 \dots x_{12}} \mid \underbrace{R}_{x_{13} \dots x_{24}})$ WA: $w(v) = 4$

$w(v) = w(L) + w(R)$

0	4
1	3
2	2
(3	1)
(4	0)

nur $v = 0$ ✓
v teile in A ✓
Summe beider Zeilen ✓
fallen weg wegen Signum, kein 2

//

Konstr von G_{23} aus G_{24}: streiche bel Koord

(perfekt :

$$2^{12}\left(1 + 23 + \binom{23}{2} + \binom{23}{3}\right)$$

$$= 2^{12} \cdot 2^{11} = 2^{23} \quad \checkmark)$$

Ähnlich: $G_{12} \rightsquigarrow G_{11}$ über $\mathbb{F}_3$

Erzeugermatrix $(I_6 \mid A)$

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 & 2 & 1 \end{pmatrix} \in \mathrm{Mat}_6(\mathbb{F}_3)$$

$\rightsquigarrow$ $[12, 6, 6]$-Code

... Thm 9.5 :

nicht-trivialer perfekter q-närer Code C &

q Primzahlpotenz

⇝ C ein (n, M, d)-Code mit Parametern

wie für → $Ham(r, q)$ oder

G_{23} oder G_{11}

scheinbar viele neue Codes ...

↳ keine weiteren Codes

Thm 9.12 ex kein 6-närer $(7, 6^5, 3)$-Code

$t=1$

$(6^5 \cdot (1 + 5 \cdot 7) = 6^5 \cdot 6^2 = 6^7 \checkmark)$

↳ wie Hamming...

Bew: WA C solch ein Code über $\mathbb{Z}_6 = \{1, \dots, 6\}$

$|C| = 6^5$ $\quad d(C) = 3$

⇝ Streichen der letzten 2 Koord

inj Abb $C \to \mathbb{Z}_6^5$

autom surj

jew 6^5 Elemente

⇝ C enthält 6^2 Elemente v mit 111 ...

Streiche bei diesen die ersten drei Koord

⇝ $(4, 6^2, \geq 3)$-Code D

wende das gleiche Arg erneut an:

2 Koord streichen ⇝

$36 = 6^2$ per versch Elemente in $\mathbb{Z}_6^2$

$(i\ j\ k\ \ell) \in D \rightarrow$ Offiziere

- Rang i
- Regiment j
- Reihe k
- Position (Spalte) ℓ

Lösung zu Eulers 36-Offiziere-Problem hat aber gar keine Lösung! (1782)

da zueinander orthogonale lateinische Quadrate

Beweis: 3 statt 6

1	2	3
2	3	1
3	1	2

Rang

$\perp$ orth

1	2	3
3	1	2
2	3	1

Regiment

//