Hinweis:
Übungsblatt ist faktisch kopiert;
S.2 ist spätestens morgen im Netz!

Erinnerung: In $H(n,q)$ ist

$$|B_e(v)| = \sum_{i=0}^{e} \binom{n}{i} \cdot (q-1)^i$$

insb. $q=2$: $|B_e(v)| = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{e}$

Bsp: $A = \mathbb{F}_2$, „eigentliche Information": 4 Bits, 1 Fehler soll korrigierbar sein

Methode I: 3fach Wiederholungscode $C_1 \subseteq H(12,2)$

Bijektion zwischen Codewörtern und Codewörtern sind disjunkt

$$C_1 = \{ v \hat{} v \hat{} v \mid v \in \mathbb{F}_2^4 \}$$

$|H(12,2)| = 2^{12} = 4096$

$|C_1| = 16$, $\dim C_1 = 4$

$|B_1(v)| = \binom{12}{0} + \binom{12}{1} = 1 + 12 = 13$

„Korrekturbereich" $16 \cdot 13 = 208$

„$4096 - 208 = 3.888$ Wörter „verschiedener Platz"

Methode II

Man verwendet folgenden Code C_2 in $H(7,2)$:

C_2 ist linearer Code der Dimension 4 mit Mindestabstand 3

$|H(7,2)| = 2^7 = 128$

$|B_1(v)| = \binom{7}{0} + \binom{7}{1} = 8$

benötigter Platz: $16 \cdot 8 = 128$

perfekter Code
kein verschwendeter Platz

Gütekriterien für Codes

- viele korrigierbare Fehler (großer Mindestabstand)
- kompakte Codierung (große Anzahl von Codewörtern bzgl. Wortlänge)

gegensätzlich

- einfache und schnelle Codierung, Decodierung und Fehlerkorrektur

Schranken für Codes

(c) Die Hamming-Schranke

Ein q-närer Code der Länge n mit Mindestabstand $\geq d$ hat höchstens

$$\frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}$$

Codewörter

$q^n = |H(n,q)|$

$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i = |B_{\lfloor \frac{d-1}{2} \rfloor}(v)|$

Ein Code heißt perfekt, falls Gleichheit gilt (bei Mindestabstand d)

Bsp: a) $q = 2, n = 7, d = 3$

Hamming-Schranke $128 / (1+7) = 16$

b) $q = 2, n = 6$

$2^6 = 64$

$\binom{6}{0}$ $\binom{6}{1}$ $\binom{6}{2}$ $\binom{6}{3}$

1 6 15 20 15 6 1

7 nicht ... ein Teiler

22 nicht

1 teilt 64

gesamte Summe = 64

$\rightsquigarrow$ 2 perfekte, aber uninteressante Codes

keine weiteren perfekten Codes!

$\longrightarrow$ Mindestabstand 1, 64 Codewörter

$\longrightarrow$ — " — 6 1 Codewort

(b) Die Gilbert-Schranke

Gegeben q, n, d, dann gibt es einen q-ären Code der Länge n, vom Mindestabstand $\geq d$, mit mindestens $q^n / \sum_{i=0}^{d-1} \binom{n}{i} \cdot (q-1)^i$ Codewörtern.

Wenn q eine Primzahl ist, kann man den Code linear (über $\mathbb{F}_q$) wählen.

Beweis: a) Angenommen C ist ein Code (vom Mindestabstand $\geq d$), der die Gilbert-Schranke nicht erreicht

Dann $\bigcup_{c \in C} B_{d-1}(c) \neq H(n,q)$

Wähle $c' \in H(n,q) \setminus \bigcup_{c \in C} B_{d-1}(c)$. Setze $C' := C \cup \{c'\}$

hat Mindestabstand $\geq d$

Vergrößere sukzessiv Codes, bis die Schranke erreicht ist!

b) Genauso bis zur Wahl von c', aber C soll bereits linear sein (starte mit dem Code $\{0\}$)

Linearer Fall: $C' = \langle C \cup \{c'\} \rangle$

Zu zeige: C' hat Mindestabstand $\geq d$

$v \in C'$, dann ist $v = \alpha \cdot c + \beta \cdot c'$ mit $c \in C$, $\alpha, \beta \in \mathbb{F}_q$

es reicht $d(v, 0) \geq d$ zu zeigen

1. Fall $\beta = 0$ $\quad d(v,0) = d(\alpha \cdot c, 0) \geq d$ nach Annahme an C ($c \in C$)

2. Fall $\beta \neq 0$ $\quad d(v,0) = d(\alpha \cdot c + \beta \cdot c', 0) = d\left(\frac{\alpha}{\beta} \cdot c + c', 0\right) = d\left(c', -\frac{\alpha}{\beta} c\right) \geq d$

C (C hat Wahl von c')

Bsp: $q = 2,\ n = 7,\ d = 3$

Gilbert-Schranke $2^7 / \binom{7}{0} + \binom{7}{1} + \binom{7}{2} = 128 / (1 + 7 + 21) = 128/29 \approx 4.41$

$\rightsquigarrow$ Code mit mindestens 5 Wörtern

Linearer Fall: $|C| = 2^{\dim C}$: linearer Code mit mindestens 8 Wörtern

---

Lineare Codes ($[n,k]$ - Codes mit k = Dimension)

kann beschrieben werden durch eine Erzeugermatrix

$(k \times n)$ - Matrix G, Zeilen der Matrix bilden eine Basis des Codes C

Codierung erfolgt kompatibel mit der Vektorraumstruktur,

d.h. Informationswort $v \in \mathbb{F}_q^k$ wird kodiert durch $v \cdot G$

$$(\underbrace{\ldots\ldots}_{k}) \begin{pmatrix} G \\ \\ \\ n \end{pmatrix} k$$

Nach Basiswechsel kann man annehmen, dass

G die Form $\left(Id_k \mid A \right)$, A: $k \times (n-k)$ - Matrix

In diesem Fall entspricht das Kodieren dem Anhängen von $(n-k)$ Prüfziffern

Im Beispiel des $[7,4,3]$-Hamming-Codes von S. 2 ist

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

Kodieren von $(1,1,0,0)$: $(1,1,0,0) \cdot G = (1,1,0,0,1,1,0)$

Code C = bis auf Transposition Bild (G^T) $\qquad v \cdot G = (G^T \cdot v^T)^T$

(v: Zeilenvektor, v^T: Spaltenvektor)

$k = \dim C = \operatorname{rg}(G^T) = \operatorname{rg}(G)$

= Anzahl der Zeilen von G, da diese linear unabhängig sind!

Eine Prüfmatrix (oder Kontrollmatrix) von C ist eine $((n-k) \times n)$-Matrix H mit $C = \operatorname{Kern}(H)$

Das bedeutet, dass die Zeilen von H linear unabhängig sind

(denn $\dim \text{Bild}(H) + \dim \operatorname{Kern}(H) = n$, $\dim \operatorname{Kern}(H) = k$)

und $H \cdot c^T = 0$ für $c \in C$, also $H \cdot G^T = 0$

($c^T = G^T \cdot v^T$; bzw. $G \cdot H^T = 0$)

Umgekehrt: Ist H eine $(n-k) \times n$-Matrix mit $\operatorname{rg}(H) = n-k$ (d.h. die Zeilen sind linear unabhängig) und $H \cdot G^T = 0$, so ist H eine Prüfmatrix von C, d.h. $C = \operatorname{Kern}(H)$

denn $C \subseteq \operatorname{Kern}(H)$ und $\dim \operatorname{Kern}(H) = k$

$\Rightarrow C = \operatorname{Kern}(H)$

Daraus liest man:

Wenn $C = (Id_k \mid A)$, dann ist $H = (-A^T \mid Id_{n-k})$ eine Prüfmatrix

Im Beispiel ist $H = \left(\begin{array}{ccc|ccc} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{array}\right)$ eine Prüfmatrix.

$-A^T$ $\quad$ Id_{n-k}

Dekodierung: angenommen $w \in H(n,q)$ wird empfangen

Suchen $c \in C$ mit minimalem Abstand zu w

Annahme: es sind höchstens e Übertragungsfehler vorgekommen und Minimalabstand von C ist $\geq 2e+1$

d.h. $w = c + f$ mit $c \in C$ und $d(f,0) \leq e$

c, f eindeutig bestimmt.

Berechne das Syndrom von w, d.i. $H \cdot w^T$

$H \cdot w^T = 0 \Leftrightarrow$ es ist kein Übertragungsfehler passiert!

$H \cdot w^T = H \cdot (c+f)^T = \underbrace{H \cdot c^T}_{=0} + H \cdot f^T = H \cdot f^T$

Falls f, f' zwei mögliche Fehler sind, gilt

$d(f-f', 0) \leq d(f,0) + d(-f', 0) = d(f,0) + d(f',0) \leq e + e < d$

also $f - f' \notin C$, und damit

$0 \neq H \cdot (f-f')^T = H \cdot f^T - H f'^T$, also $H \cdot f^T \neq H \cdot f'^T$

d.h. Verschiedene Fehler haben verschiedene Syndrome!

Decodieren: erstelle Liste aller Syndrome von (möglichen) Fehlern,

rechne $H \cdot w^T$ aus, schaue in der Liste nach und korrigiere an entsprechender Stelle

und lasse Prüfziffern weg.

Satz: Sei C ein linearer Code mit Prüfmatrix H.
Dann hat C genau dann Minimalgewicht $\geq d$,
wenn je $d-1$ Spalten von H linear unabhängig sind.

Beweis: Seien s_i die Spalten von H. Falls $\sum_{i=1}^{n} \lambda_i s_i = 0$, dann heißt dies gerade

$$H \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = 0 \quad \text{d.h.} \quad (\lambda_1, \ldots, \lambda_n) \in C$$

$(s_1 | s_2 | \ldots | s_n)$

Also: Falls m Spalten von H lin. abh. sind, so gibt es einen Vektor in C vom Gewicht m und umgekehrt. ☐

Spezialfall: Minimalgewicht 3: je 2 Spalten der Prüfmatrix sind linear unabhängig

d.h. – keine Spalte ist die Nullspalte
– keine Spalte ist ein Vielfaches einer anderen Spalte

Def: Hamming-Codes sind lineare Codes vom Minimalabstand 3,
bei denen die Prüfmatrix maximale Spaltenanzahl hat, d.h. für jeden Vektorraum $\mathbb{F}_2^r$ der Dimension r gibt es einen Vektor (genau einen!) $\neq 0$, aber als Spalte in der Prüfmatrix steht!

Im Fall $q = 2$: Die Prüfmatrix H besteht aus allen Vektoren $\neq 0$ der Länge $m = n-k$ als Spalten von H

$$|\mathbb{F}_2^m| = 2^m, \quad n = 2^m - 1, \quad m = n-k$$

Dimension des zugehörigen Hamming-Codes ist $2^m - 1 - m$

Im Beispiel: $n = 7$, $k = 4$, $m = 3$

$$4 = 2^3 - 1 - 3$$

Im allgemeinen ist $n = \frac{q^m - 1}{q-1}$, $k = \frac{q^m - 1}{q-1} - m$, $d = 3$

Das gibt perfekte Codes, die einen Fehler korrigieren