Gütekriterien für Code

- Erkennt und korrigiert möglichst viele Fehler (e Stärke)
  (guter Minimalabstand, \(|Be(C)|\) wird groß mit wachsendem \(e\) und \(c\)

- möglichst viele Codewörter (im Verhältnis zur Länge \(n\))
  \(1\) \(\leq\) \(c\), \(n\) fall, \(C\) linear
  (in Packungsproblem: \(Be(C)\) möglichst dicht für \(C = C\))

- Ver- und Entschlüsselung möglichst effektiv (mittelbar \(d\))
  (schnelle Algorithmen sind in der Regel langsamer,
  schneller Algorithmen geben ihrer "Breite der Code, voraus")
  \(c\) ", ursprünglich
Schränken

$q$-äquiv Code $C$ der Länge $n$; Anzahl mögliche Einträge

$|B_r(C)| = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i$

Anzahl der Möglichkeiten für die Stelle, an deren Stelle auftraten

$q=2 \quad |B_r(C)| = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$

Gilbert-Schranke: Gegeben $n, q, d$. Dann gibt es einen (linearen) größten Code der Länge $n$ und vom Minimalabstand $\geq d$ mit

mindestens $q^n / \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i =: c$

$|H(n,q)| \geq |B_{d-1}(C)|$
Beweis: \( C \) Code von Minimalkosten \( d \geq d \), \( |C| < k \)

Dann \( |C| \cdot |B_{d-1}(C)| < q^2 \), also existiert \( \overline{x} \in H(u, q) \) mit
\( d(\overline{x}, \overline{c}) \geq d \) für alle \( \overline{c} \in C \)

Dann ist \( C \cup \{\overline{x}\} \) größter Code von Minimalkosten \( \geq d \).

linearer Fall: \( C \) linearer Code mit \( d \), \( |C| < k \)

\( \text{Fälle: } C' = \langle C, \overline{x} \rangle \) ist Minimalabstand \( \geq d \)

\( \nu/(\nu) \quad \alpha \overline{x} + \beta \overline{c}, \alpha, \beta \in \mathbb{F}_q \), \( \overline{c} \in C \)
\( d(\alpha \overline{x} + \beta \overline{c}, \overline{0}) = ? \quad \begin{array}{ll}
1. \text{Fall} & \alpha = 0 \\
2. \text{Fall} & \alpha \neq 0
\end{array} \\
\begin{array}{ll}
d(\alpha \overline{x} + \beta \overline{c}, \overline{0}) = d(\overline{x}, \frac{\beta \overline{c}}{\alpha}) & \geq d \\
& \text{mit } \overline{c} \in C \quad \text{und } \text{Val}(\Delta)
\end{array} \\
\Rightarrow \text{Minimalabstand von } C' \geq d

\text{Bsp: } q = 2, \mu = 7, d = 3 \quad \text{linearer Schrabe: } 2^7 / \sum_{i=0}^{2} \binom{7}{i} = 128 / (1 + 7 + 27) \geq 4,4

linearer Fall: \( |C| \) linearer, \( |C| \geq 4,4 \)
\( C \) linearer Code \( \text{mit } \mathbb{F}_2^\perp \), \( |C| \leq 2^r \text{ durch } \Rightarrow |C| \geq 8 \)
Hamming-Schranke: Jeder q-ärter Code der Länge $n$ und von Mindestabstand $d$ hat höchstens $q^n / \sum_{i=0}^{\lfloor d/2 \rfloor} \binom{n}{i} (q-1)^i$ Codewörter.

(Beisp: perfekter Code ($=\varnothing$)

Beisp:

a) $q=2$, $n=7$, $d=3$ : $2^7 / (1 + 7) = 16$

b) $q=2$, $n=6$, $2^6 = 64$

$$\binom{6}{0} + \binom{6}{1} + \binom{6}{2} + \ldots$$

= $1 + 6 + 15 + 20 + 15 + 6 + 1$

Einige Teiler von 64:

1 und 64

64

Zugehörige binäre Codes

Lassen alle Elemente von $\mathbb{F}_{11} \times \mathbb{F}_2$ durch Minimalabstand $d$ über;

Lassen nur 1 Codewort

Minimalabstand $\geq d$
Linear Codes

C linearer Code der Dimension k, Wortlänge n, wird beschrieben durch eine *echte* $\begin{pmatrix} k \times n \end{pmatrix}$ Matrix, welche Bilde Basis von $C$ (nicht endlich)

Im Beispiel des $[7,4,3]$-Hamming-Code, $C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

Kodierung: echte Information ist folgende $0 \rightarrow 11$, $1 \rightarrow 12$ in Schritte binärdezimal als Spaltvektor,

$B M_{10} = 1011_2 \rightarrow v_{11} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$

Code von $M$ ist $C^T v_{11} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$. 


Durch Basiswechsel / Skalierung kann man sich erlauben, dass

\[ C \text{ in Form } (I_k | A) \text{ hat } \text{(näherer Übergang in äquivalentem Code)} \]

ist. Gleich Dimension gleiche Minimalabstände.

\( C \) kann auch beschrieben werde durch ein Prüfmatrix \( H \), d.h.

\[ H \cdot \vec{c} = 0 \text{ für alle } \vec{c} \in \text{Kern} (H) \]

und Teile von \( H \) linear unabhängig.

Im Bsp.: \( H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 6 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \)

beachte: \( H \) ist nicht endlich!
\( G \) (\( k \times n \)) - Matrix

\( H \) (\((n-k) \times n\)) - Matrix

\[ G \cdot H^\top = 0 \quad (H \cdot C^\top = 0) \]

Bem.: Umkehrung gilt: 2 Matrizen mit den Eigenschaften

Erstes- und Pfiffmatrix sind k-dimensionaler Code!

\( H \) kann in die Form gebracht werden:

\((-A^\top \mid \text{Id}_{n-k})\)

fallst \( G = (\text{Id}_k \mid A) \)

Dehodierung

Empfange \( \tilde{w} \in \mathbb{F}_q^n \)

\( \tilde{w} \) wird zunächst dekodiert als \( \tilde{c} \in C \) mit \( d(\tilde{c}, \tilde{w}) \leq \frac{d-1}{2} \)

\( \tilde{c} \) "vollständiges Codewort"

d.h.

\[ \tilde{w} = \tilde{c} + \tilde{f} \quad d(\tilde{f}, 0) \leq \frac{d-1}{2} \]

Brechen \( H \cdot \tilde{w} = H \cdot (\tilde{c} + \tilde{f}) = H \cdot \tilde{c} + H \cdot \tilde{f} = \tilde{h} \cdot \tilde{f} \rightarrow \tilde{h} \cdot \tilde{f} \) in Teile

der Syndrom der möglichen Fehler nach-

Falls "Syndrom von \( \tilde{w} \)" 0

\( \tilde{c} = (\text{Id}_k \mid A) \), dann ist die ursprüngliche Information in die erste \( k \)-Stelle von \( \tilde{c} \)
Satz: C linear Code

$C$ hat Minimalabstand $\geq d \iff$ je die Spalten der Primmatrizen sind linear unabhängig.

Sonderfall $d = 3$: kein Spalt ist $0$
keine Spalte ist ein Vielfaches einer anderen

Def.: $C$ Hamming-Code: Mindestabstand $3$, maximal Primmatrizen

d.h. alle Vektoren $\neq 0$ kommen, bis auf ein skalares Vielfaches, als Spalte vor

(all. alle eindeutige Untermenge haben einen Fixpunkt)

Sonderfall $d = 2$: $H$ besteht aus allen Vektoren $\neq 0$ als Spaltenvektor

gegeben $r = n - 2k$, dann ist $n = 2^r - 1$, $k = \dim$ Hamming-Code

Für die Felder von $F$

$l = 3$ : $n = 2^3 - 1 = 7$, $k = 7 - 3 = 4$

$l = 4$ : $n = 2^4 - 1 = 15$, $k = 15 - 4 = 11$
Hamming-Codes sind perfekte Codes vom Minimalabstand 3, d.h. korrigieren einen Fehler.

Für die Dekodierung in Fall $q=2$

Fehler $f = e_i$ Standardbasiselement
Syndrom von $e_i$ ist $i$-te Spalte von $H$

Bem.: Nach Definition von $H$ sind die Spaltenvektoren alle verschieden, d.h. das Syndrom gibt eindeutig an, an welcher Stelle der zu korrigierende Fehler aufgetreten ist.

oder unbedeutend, $i \neq j$, $d(e_i, e_j) = 2$ (bzw. $\leq 2$ in allgemeinem Fall)
also $d(e_i - e_j, 0) = 2$
d.h. $e_i - e_j \notin C$, somit $H(e_i - e_j) \neq 0$
$\implies$ $He_i \neq He_j$ Widerspruch.
Liste aller perfekten quaeren Codes,

- Trivial Code, \([n, 0, n] \quad (n \neq 1 \text{ Vork.}) \quad c = 0\)
- \([n, n, 1] \quad (\text{Nichtcode}) \quad c = 0\)

- Hamming-Code, \(\left[ \frac{q^e - 1}{q - 1}, \frac{q^e - 1}{q - 1} - e, 3 \right] \quad c = 1\)

(einige nicht-lineare Codes mit gleichen Parametern)

- binären Riederholungscode, ungefährer Länge, \([2c+1, 1, e] \quad c = w\)
  (nur 1 Wörter: \(0, 0, \ldots, 0\) \(a, a, \ldots, a\))

- binäre Golay-Code \((q = 2)\) \([23, 12, 7] \quad c = 3\)
  \(q = 3\) \([11, 6, 5] \quad c = 2\)
kein Prinzip, man legt sehr wenig

allgemeines Problem: sehr gute (nicht perfekte) Codes finden

viel offene Frage

Lütkebohmert „Codierungstheorie“ (Vieweg)
Conway, Sloane „Sphere Packings, Lattices and Groups“ (Springer)