II Codes II

→ Kanalcodierung:
sichere Übertragung mit Fehlerkorrektur

Code C: $C \subseteq S^n$, S Menge, meistens $S = \mathbb{Z}_q$, $\mathbb{Z}_2$

Hammingabstand: $d(a,b) = |\{i \mid a_i \neq b_i\}|$

C ist e-fehlerkorrigierend: $d(C) \geq 2e+1 \quad \forall a,b \in C$
e-fehlererkennend: $\geq e+1$

$d(C) := \min\{d(a,b) \mid a,b \in C\}$ Distanz

- Code C mit $d := d(C)$ kann
$$|C| \leq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}$$ Elemente haben.
- e-fehlerkorrigierender Code hat höchstens
$$|C| \leq \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i} (q-1)^i}$$ Elemente
(Hammingschranke)

Def: Gleichheit in Hammingschranke
$\rightsquigarrow$: C ist e-perfekt oder perfekt

Bsp. Face-Ebene → A 11.4. für $q=2$

$S = \mathbb{Z}_2$, $C \subseteq S^n$ → können $a \in C$ als Menge
$I_a := \{i \mid a_i = 1\} \subseteq [n]$ auffassen.

→ Code entspricht Mengenfamilie $\mathcal{F} \subseteq 2^{[n]}$

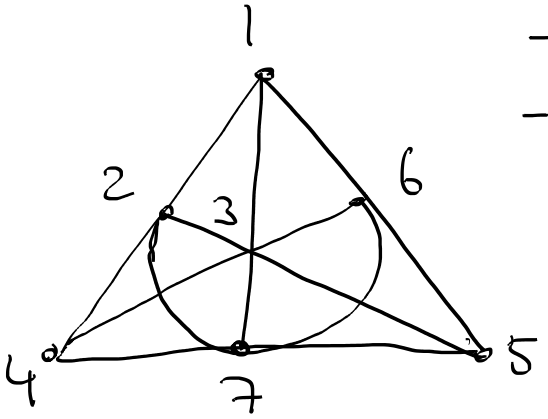
→ $d(a,b) = |I_a \Delta I_b|$

$\mathcal{F}$ ist e-perfekt $\Leftrightarrow$ $|A \Delta B| \geq 2e+1$

$$|\mathcal{F}| = \frac{2^4}{\sum_{i=0}^{e} \binom{4}{i}}$$

Fano-Ebene zu $q=2$: $n=7$ Punkte

$n=7$ Geraden



→ je zwei schneiden sich in einem Punkt

→ jede Gerade enthält 3 Punkte.

Schon: $\mathcal{F} = \{\emptyset\} \cup \{\text{Geraden}\} \cup \{\text{Komplemente von Geraden}\}$

Als Elemente von $\mathbb{Z}_2^7$:

$\emptyset$	0 0 0 0 0 0 0	1 1 1 1 1 1 1
124	1 1 0 1 0 0 0	0 0 1 0 1 1 1
137	1 0 1 0 0 0 1	0 1 0 1 1 1 0
156	1 0 0 0 1 1 0	0 1 1 1 0 0 1
235	0 1 1 0 1 0 0	1 0 0 1 0 1 1
267	0 1 0 0 0 1 1	1 0 1 1 1 0 0
346	0 0 1 1 0 1 0	1 1 0 0 1 0 1
457	0 0 0 1 1 0 1	1 1 1 0 0 1 0

→ $|A \Delta B| \geq 3 \Rightarrow e = 1$

$$|\mathcal{F}| = (1+7) \cdot 2 = \frac{2^7}{1+7}$$

$\Rightarrow \mathcal{F}$ ist ein 1-perfekter Code.

Def: $C \subseteq S^n$ heißt *linear*, wenn $S = \mathbb{Z}_q$ und für alle $x, y \in C$, $\lambda \in S$

$$x+y \in C, \quad \lambda x \in C$$

$\Leftrightarrow$ C ist linearer Unterraum von $\mathbb{Z}_q^n$

Sei $k = \dim C$ und $d = d(C)$

Dann ist C ein q-$[n,k,d]$-Code

Für $q = 2$: binärer $[n,k,d]$-Code

$\frac{n}{k}$ ist die Coderate

Bsp: Der Code zur Fanoebene ist ein 2-$[7,4,3]$-Code

Def C linear, $a \in C$

$$w(a) := |\{i \mid a_i \neq 0\}| \quad \text{Gewicht von } a$$

Sei $a, b \in C$, $a \neq b$

$\rightarrow$ $a_i \neq b_i \Leftrightarrow a_i - b_i \neq 0$

$\Rightarrow d(a,b) = w(a-b)$

linear $\Rightarrow d(a,b) = d(a-b, 0)$ und $a-b \in C$

Damit folgt:

Bsp: C linear, dann $d(C) = \min(w(a) \mid a \in C)$

Def C lineaer Code.
Das zu C duale Code ist:

$$C^\perp := \{a \in \mathbb{Z}_q^n \mid \langle a,b\rangle = 0 \ \forall\, b \in C\}$$

$\Rightarrow$ $C^\perp$ ist das orth. Komplement von C in $\mathbb{Z}_q^n$.

$C^\perp$ ist $[n, n-k, d']$-Code für ein d'

C ist ein lineaer Unterraum von $\mathbb{Z}_q^n$

$\rightarrow$ C hat eine Basis $g_1, \dots, g_k$

Def Die Matrix G mit Zeilen g_i heißt
Erzeuger- oder Generatormatrix von C

$\rightarrow$ $C = \{\lambda G \mid \lambda \in \mathbb{Z}_q^k\}$

$\rightarrow$ G ist nicht eindeutig.

Def Eine Erzeugermatrix H von $C^\perp$ heißt
Kontrollmatrix von C

$\rightarrow$ $a \in C \iff Hc = 0$

Satz C lineaer Code mit $k = \dim C$ und
Kontrollmatrix H. Dann

$d(C) \geq d \iff$ je $d-1$ Spalten von H sind
linear unabhängig

Satz H hat $< d$ lin. abhängige Spalten
$\Leftrightarrow$ es gibt $a \in C$ mit $< d$ Einträgen $\neq 0$ und $Ha = 0$
$\Leftrightarrow$ es gibt $a \in C$ mit $w(a) < d$. ∎

Korr C $[n, k, d]$-Code, dann $d \leq n - k + 1$

Satz $H \in \mathbb{Z}_q^{r}$ hat höchstens r lin. unabhängige Vektoren
$\Rightarrow d - 1 \leq r = n - k$ ∎

Bsp. $S = \mathbb{Z}_q^{r}$

Wähle zu jedem eindimensionalen Untervektorraum einen Erzeuger
$\rightarrow$ je zwei solche Erzeuger sind lin. unabh.
$\Rightarrow$ es gibt $n := \frac{q^r - 1}{q - 1}$ solche

Setze: H Matrix mit diesen Spalten
$\rightarrow$ H ist $(r \times n)$-Matrix

$\rightarrow$ Fasse H als Kontrollmatrix eines Codes C auf.

Mit $k = n - r$: $\dim C = k$

$\rightarrow$ nach Satz $d(C) \geq 2 + 1 = 3$

Außerdem: $|C| = q^k = q^{n-r} = \frac{q^n}{q^r} = \frac{q^n}{1 + \frac{q^r - 1}{q-1}(q-1)} = \frac{q^n}{1 + n(q-1)}$

$\Rightarrow C$ ist 1-perfekt

- $q=2, r=2$

  $H = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, $C = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$

- $q=2, r=3$ $\exists$ Hamcode

Def: Diese Codes heißen Hammingcodes

→ wie viel codiert / decodiert:

- C $[n,k,d]$-Code über $\mathbb{Z}_q$, e-fehlerkorrigierend
  → G Generatormatrix
  → Nachrichten $\hat{=}$ $\mathbb{Z}_q^k$, q^k viele
  → Codieren: $w \in \mathbb{Z}_q^k \to Gw \in C$

- decodieren:

  a gesendet, b empfangen,

  Dann: $d(a,b) \leq e$, $d(b,x) > e$ $\forall x \in C, x \neq a$

  → Liste des Codewörter durchsuchen

  besser: H Kontrollmatrix

  $s: \mathbb{Z}_2^n \to \mathbb{Z}_2^r$, $r = n-k$

  $a \mapsto Ha$

  Dann: $b = a + x$ und $s(b) = s(a)$

  und zu $y \in \mathrm{im}(s)$ gibt es eindeutiges $x \in \mathbb{Z}_2^n$ mit $s(x) = y$, $w(x) \leq e$.

→ können Liste dieser x aufstellen

→ Syndrome

Damit zu b suche Syndrom x mit

$S(b) = S(x)$

→ das gesuchte Codewort ist $a = b - x$