

Hamming-Geometrie der Bitvektoren

$\mathbb{B} = \{0, 1\}$ mit den Operationen

- ▶ \wedge = Konjunktion ("und")
- ▶ \vee = Disjunktion ("oder")
- ▶ \neg oder $\bar{}$ = Negation ("nicht")

ist die zweielementige *boolesche Algebra*.

- ▶ $(\mathbb{B}, \oplus, 0)$ mit $\oplus = \text{EXOR}$ ist eine kommutative Gruppe.
- ▶ $(\mathbb{B}, \oplus, \wedge, 0, 1)$ ist ein Ring (*boolescher Ring*) und ein Körper (\mathbb{F}_2).

$\mathbb{B}^n = \{0, 1\}^n$: Bitvektoren $\mathbf{a} = (a_1, a_2, \dots, a_n)$ der Länge n
 \mathbb{B}^n mit den speziellen Elementen $\mathbf{0} = (0, 0, \dots, 0)$, $\mathbf{1} = (1, 1, \dots, 1)$
 und den komponentenweisen Operationen

- ▶ \wedge = Konjunktion ("und")
- ▶ \vee = Disjunktion ("oder")
- ▶ $\bar{}$ = Negation ("nicht")

ist eine *boolesche Algebra* mit 2^n Elementen.

- ▶ $(\mathbb{B}^n, \oplus, \mathbf{0})$ mit komponentenweisem $\oplus = \text{EXOR}$ ist eine kommutative Gruppe. (NB. $\bar{\mathbf{a}} = \mathbf{a} \oplus \mathbf{1}$).
- ▶ $(\mathbb{B}^n, \oplus, \wedge, \mathbf{0}, \mathbf{1})$ ist ein Ring (*boolescher Ring*) und ein Vektorraum der Dimension n über dem Körper \mathbb{F}_2 .
- ▶ Standardbasis: $\mathbf{e}^k = (0, 0, \dots, 0, 1_k, 0, \dots, 0)$ ($1 \leq k \leq n$).

- ▶ Für $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{B}^n$ bezeichnet $\|\mathbf{a}\|$ die Anzahl der Komponenten $a_i = 1$ in \mathbf{a} (HAMMING-Gewicht).
- ▶ Für $\mathbf{a}, \mathbf{b} \in \mathbb{B}^n$ bezeichnet

$$d(\mathbf{a}, \mathbf{b}) = \|\mathbf{a} \oplus \mathbf{b}\| = \|\mathbf{a}\| + \|\mathbf{b}\| - 2 \cdot \|\mathbf{a} \wedge \mathbf{b}\|$$

den HAMMING-Abstand.

- ▶ Die Funktion

$$d : \mathbb{B}^n \times \mathbb{B}^n \rightarrow \{0, 1, 2, \dots, n\} : (\mathbf{a}, \mathbf{b}) \mapsto d(\mathbf{a}, \mathbf{b})$$

ist eine *Metrik* auf \mathbb{B}^n , d.h. es gilt für $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{B}^n$:

$$d(\mathbf{a}, \mathbf{b}) = 0 \Leftrightarrow \mathbf{a} = \mathbf{b}$$

$$d(\mathbf{a}, \mathbf{b}) = d(\mathbf{b}, \mathbf{a})$$

$$d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}) \geq d(\mathbf{a}, \mathbf{c})$$

Translationsinvarianz: $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{a} \oplus \mathbf{c}, \mathbf{b} \oplus \mathbf{c})$

- ▶ $\mathbb{B}_k^n = \{\mathbf{a} \in \mathbb{B}^n; \|\mathbf{a}\| = k\}$ ($0 \leq k \leq n$)
- ▶ $\#\mathbb{B}_k^n = \binom{n}{k}$
- ▶ $\mathbb{B}_{\leq k}^n = \{\mathbf{a} \in \mathbb{B}^n; \|\mathbf{a}\| \leq k\}$ ($0 \leq k \leq n$)
 HAMMING-Kugel vom Radius k um den Nullvektor
- ▶ $S_k(\mathbf{a}) = \mathbf{a} \oplus \mathbb{B}_{\leq k}^n$
 HAMMING-Kugel vom Radius k um den Vektor \mathbf{a}
- ▶ $V(n, k) = \#\mathbb{B}_{\leq k}^n = \sum_{j=0}^k \binom{n}{j}$
 Volumen einer HAMMING-Kugel vom Radius k .
- ▶ $d(\mathbf{a}, \mathbf{b}) > k \Leftrightarrow \mathbf{b} \notin S_k(\mathbf{a}) \Leftrightarrow \mathbf{a} \notin S_k(\mathbf{b})$
- ▶ $d(\mathbf{a}, \mathbf{b}) > 2k \Leftrightarrow S_k(\mathbf{a}) \cap S_k(\mathbf{b}) = \emptyset$

Abschätzung des Kugelvolumens

Sei $0 \leq \lambda \leq 1/2$, also $\frac{\lambda}{1-\lambda} \leq 1$. Aus

$$\left[\frac{\lambda}{1-\lambda} \right]^k \geq \left[\frac{\lambda}{1-\lambda} \right]^{\lfloor \lambda n \rfloor} \quad (0 \leq k \leq \lfloor \lambda n \rfloor)$$

und mit Verwendung der Binomialformel folgt

$$V(n, \lambda n) \leq \lambda^{-\lfloor \lambda n \rfloor} (1-\lambda)^{\lfloor \lambda n \rfloor - n} \leq 2^{n \cdot H(\lambda)}$$

Zusammen mit der Abschätzung für $\binom{n}{\lfloor \lambda n \rfloor}$ ergibt sich

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log V(n, \lambda n) = H(\lambda)$$

Diskreter gedächtnisfreier stationärer Kanal

► Daten

- Inputalphabet $A = \{a_1, a_2, \dots, a_m\}$
- Outputalphabet $B = \{b_1, b_2, \dots, b_n\}$
- Kanalmatrix $P = (p_{i,j}; 1 \leq i \leq m, 1 \leq j \leq n)$ mit $p_{i,j} \geq 0$ ($1 \leq i \leq m, 1 \leq j \leq n$) und $\sum_{1 \leq j \leq n} p_{i,j} = 1$ (stochastische Matrix)

- Funktionsweise: wird $a_i \in A$ gesendet, so wird $b_j \in B$ empfangen mit Wahrscheinlichkeit

$$P(b_j | a_i) = p_{i,j} \quad (1 \leq i \leq m, 1 \leq j \leq n)$$

- für $N \geq 1$: wird $\mathbf{u} = (u_1, u_2, \dots, u_N) \in A^N$ gesendet, so wird $\mathbf{v} = (v_1, v_2, \dots, v_N) \in B^N$ empfangen mit Wahrscheinlichkeit

$$P(\mathbf{v} | \mathbf{u}) = \prod_{1 \leq k \leq N} P(v_k | u_k) = P(v_1 | u_1) \cdot P(v_2 | u_2) \cdots P(v_N | u_N)$$

Beispiele

- Binärer symmetrischer Kanal BSC_p
 $A = B = \mathbb{B} = \{0, 1\}$, $0 < p < 1$

$$P = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

- Binärer Kanal mit Löschung $A = \mathbb{B} = \{0, 1\}$, $B = \mathbb{B} \cup \{*\}$, $0 < \varepsilon < 1$

$$P = \begin{bmatrix} 1-\varepsilon & 0 & \varepsilon \\ 0 & 1-\varepsilon & \varepsilon \end{bmatrix}$$

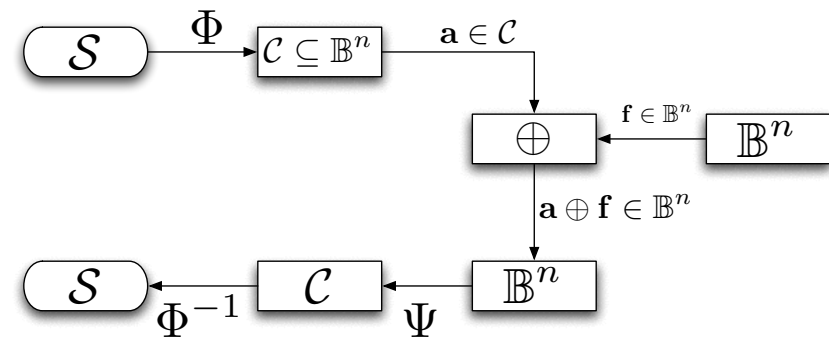


Abbildung: Informationsübertragung über einen gestörten Kanal

Nachrichtenübertragung mit BSC

- ▶ Quelle (source): $\mathcal{Q} = (S, \pi)$, wobei S Alphabet und $\pi = (\pi_s)_{s \in S}$ Wahrscheinlichkeitsverteilung auf S .
- ▶ Codierung: injektive Abbildung $\Phi : S \rightarrow \mathbb{B}^n$
 $\mathcal{C} = \Phi(\mathbb{B}^n)$: der durch Φ definierte Code
- ▶ Kanalmodell: die Wahrscheinlichkeit, beim Senden von $\mathbf{a} \in \mathbb{B}^n$ den Vektor $\mathbf{b} \in \mathbb{B}^n$ zu empfangen, d.h. dass der Fehler $\mathbf{f} = \mathbf{a} \oplus \mathbf{b}$ auftritt, ist

$$P(\mathbf{b} | \mathbf{a}) = \text{bin}_{n,p}(\mathbf{f}) = p^{|\mathbf{f}|} (1-p)^{n-|\mathbf{f}|}$$

- ▶ Der Empfänger ist bestrebt, aus der Kenntnis des empfangenen $\mathbf{b} \in \mathbb{B}^n$ das mit grösster Wahrscheinlichkeit gesendete $\mathbf{a} \in \mathcal{C}$ zu ermitteln.

- ▶ Unter der Annahme, dass alle $\mathbf{a} \in \mathcal{C}$ mit gleicher Wahrscheinlichkeit gesendet werden, d.h. $\pi(s) = 1/|S|$ für alle $s \in S$, muss man $\mathbf{a} \in \mathcal{C}$ bestimmen, für das $P(\mathbf{b} | \mathbf{a})$ maximal wird. (*maximum likelihood Decodierung*)
- ▶ Für $0 < p < 1/2$ gilt

$$0 \leq j \leq k \leq n \Rightarrow p^j (1-p)^{n-j} \geq p^k (1-p)^{n-k}$$

- ▶ Daraus ergibt sich das Prinzip der *minimum distance* Decodierung:

$\Psi : \mathbb{B}^n \rightarrow \mathcal{C} : \mathbf{b} \mapsto \mathbf{a} \in \mathcal{C}$ für das $d(\mathbf{a}, \mathbf{b}) = \|\mathbf{a} \oplus \mathbf{b}\|$ minimal ist

Ein solches $\mathbf{a} \in \mathcal{C}$ muss nicht eindeutig bestimmt sein!

Beispiel (1)

- ▶ Quelle $S = \{s_1, s_2, \dots, s_8\}$, $\pi_s = \frac{1}{8}$ ($1 \leq s \leq 8$)
- ▶ Codierung Φ_1

s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
↓	↓	↓	↓	↓	↓	↓	↓
000	100	010	001	110	101	011	111

- ▶ Inputalphabet für den BSC_p ist $\Phi_1(S) = \mathcal{C}_1 = \mathbb{B}^3$
- ▶ Decodierung $\Psi_1(a_1 a_2 a_3) = a_1 a_2 a_3$, d.h. $\Psi_1 = id_{\mathbb{B}^3}$
- ▶ Die Wahrscheinlichkeit fehlerfreier Übertragung eines $(a_1 a_2 a_3) \in \mathbb{C}$ ist $(1-p)^3$. N Nachrichten werden mit Wahrscheinlichkeit $(1-p)^{3N}$ korrekt übertragen und decodiert.
- ▶ Es werden keine Fehler erkannt oder korrigiert

Beispiel (2)

- ▶ Quelle $S = \{s_1, s_2, \dots, s_8\}$, $\pi_s = \frac{1}{8}$ ($1 \leq s \leq 8$)
- ▶ Codierung Φ_2

s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
↓	↓	↓	↓	↓	↓	↓	↓
0000	1001	0101	0011	1100	1010	0110	1111

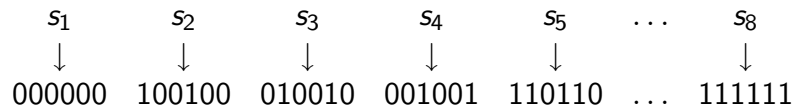
- ▶ Inputalphabet für den BSC_p ist $\Phi(S) = \mathcal{C}_2 = \{\mathbf{a} \in \mathbb{B}^4; \|\mathbf{a}\| \text{ gerade}\}$
- ▶ Decodierung

$$\Psi_2(a_1 a_2 a_3 a_4) = \begin{cases} a_1 a_2 a_3 & \text{falls } \|a_1 a_2 a_3 a_4\| \text{ gerade} \\ \text{error} & \text{falls } \|a_1 a_2 a_3 a_4\| \text{ ungerade} \end{cases}$$

- ▶ $a_1 a_2 a_3 a_4 \in \mathbb{C}$ wird mit Wahrscheinlichkeit $(1-p)^4$ fehlerfrei übertragen, mit W.keit $4p(1-p)^3$ tritt ein 1-Bit-Fehler auf.
- ▶ 1-Bit-Fehler werden erkannt, aber nicht korrigiert.

Beispiel (3)

- ▶ Quelle $S = \{s_1, s_2, \dots, s_8\}$, $\pi_s = \frac{1}{8}$ ($1 \leq s \leq 8$)
- ▶ Codierung Φ_3



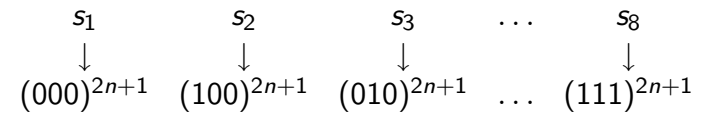
- ▶ Inputalphabet für den BSC_p ist $\Phi_3(S) = \mathcal{C}_3 \subset \mathbb{B}^6$
- ▶ Decodierung

$$\Psi_3(a_1 a_2 a_3 a_4 a_5 a_6) = \begin{cases} a_1 a_2 a_3 & \text{falls } a_1 a_2 a_3 = a_4 a_5 a_6 \\ \text{error} & \text{falls } a_1 a_2 a_3 \neq a_4 a_5 a_6 \end{cases}$$

- ▶ Es werden viele Fehler erkannt, aber sie können nicht korrigiert werden.

Beispiel (4)

- ▶ Quelle $S = \{s_1, s_2, \dots, s_8\}$, $\pi_s = \frac{1}{8}$ ($1 \leq s \leq 8$)
- ▶ Codierung Φ_4



- ▶ Inputalphabet für den BSC_p ist $\Phi_4(S) = \mathcal{C}_4 \subset \mathbb{B}^{6n+3}$
- ▶ Decodierung

$$\Psi_4(a_1 a_2 \dots a_{6n+3}) = \begin{cases} abc & \text{falls } \geq n+1 \text{ Dreierblöcke} = abc \\ \text{error} & \text{sonst} \end{cases}$$

- ▶ Es werden alle Fehler mit Gewicht $\leq 2n$ erkannt. Alle Fehler mit Gewicht $\leq n$ können korrigiert werden.

Codes

- ▶ Ein (binärer Block)-Code der Länge n ist eine Teilmenge $\mathcal{C} \subseteq \mathbb{B}^n$.
- ▶ Die *Minimaldistanz* von \mathcal{C} ist

$$d_{\min}(\mathcal{C}) = \min_{\substack{\mathbf{a}, \mathbf{b} \in \mathcal{C} \\ \mathbf{a} \neq \mathbf{b}}} d(\mathbf{a}, \mathbf{b})$$

- ▶ Die *Coderate* von \mathcal{C} ist

$$R(\mathcal{C}) = \frac{1}{n} \cdot \log \#\mathcal{C}$$

- ▶ \mathcal{C} ist ein (n, K, d) -Code, falls $\mathcal{C} \subseteq \mathbb{B}^n$, $\#\mathcal{C} = K$ und $d_{\min}(\mathcal{C}) = d$.

- ▶ Ein (n, K, d) -Code kann e Fehler *erkennen*, falls $e < d$ ist, d.h. falls

$$\forall \mathbf{a} \in \mathcal{C} : S_e(\mathbf{a}) \cap \mathcal{C} = \{\mathbf{a}\}$$

- ▶ Ein (n, K, d) -Code kann e Fehler *korrigieren*, falls $2e < d$ ist, d.h. falls

$$\forall \mathbf{a}, \mathbf{b} \in \mathcal{C} \text{ mit } \mathbf{a} \neq \mathbf{b} : S_e(\mathbf{a}) \cap S_e(\mathbf{b}) = \emptyset$$

- ▶ Für einen e Fehler korrigierenden (n, K, d) -Code gilt die *Kugelpackungsschranke*:

$$K \cdot V(n, e) \leq 2^n, \text{ d.h. } R(\mathcal{C}) + H\left(\frac{e}{n}\right) \leq 1$$

- ▶ Gesucht sind Codes mit hoher Rate und grosser Minimaldistanz: das sind antagonistische Anforderungen!
- ▶ $A(n, d)$: maximales K für das ein (n, K, d) -Code existiert.

Beispiele

- ▶ $d_{\min}(C_1) = 1, R(C_1) = 1$
- ▶ $d_{\min}(C_2) = 2, R(C_2) = \frac{3}{4}$
- ▶ $d_{\min}(C_3) = 2, R(C_3) = \frac{1}{2}$
- ▶ $d_{\min}(C_4) = 2n + 1, R(C_4) = \frac{1}{2n+1}$

- ▶ $A(n, 1) = 2^n, A(n, n) = 2$
- ▶ $A(n, 2) = 2^{n-1}$
- ▶ $A(3, 3) = 2, A(4, 3) = 2, A(5, 3) = 5, A(7, 3) = 16$
- ▶ $A(n, 2t + 1) \leq \frac{2^n}{V(n,t)}$ (HAMMING)
- ▶ $A(n, d) \leq 2^{n-d+1}$ (SINGLETON)
- ▶ $A(n, d) \geq \frac{2^n}{V(n,d-1)}$ (GILBERT-VARSHAMOV)

Lineare Codes

- ▶ (binärer) *linearer* Code der Länge $n =$ linearer Teilraum $C \subseteq \mathbb{B}^n$.
NB: hier gilt
linearer Teilraum = Untergruppe = \oplus -abg. Teilmenge ($\neq \emptyset$)
- ▶ Hat C die Dimension $\dim C = k$, so gilt $\#C = 2^k$.
Die Coderate ist dann $R(C) = \frac{k}{n}$.
- ▶ Für lineare Codes C gilt immer

$$d_{\min}(C) = \min_{\mathbf{0} \neq \mathbf{a} \in C} \|\mathbf{a}\|$$

Man spricht deshalb vom *Minimalgewicht*.

- ▶ Ein linearer Code $C \subseteq \mathbb{B}^n$ mit $\dim C = k$ und Minimalgewicht $d_{\min}(C) = d$ wird als $[n, k, d]$ -Code bezeichnet.

Es gibt zwei wesentliche Möglichkeiten, lineare Codes $C \subseteq \mathbb{B}^n$ zu beschreiben:

- ▶ mittels *Generatoren*, d.h. durch Angabe einer *Basis* $\mathbf{g}^1, \mathbf{g}^2, \dots, \mathbf{g}^k$ von C , also durch eine *Generatormatrix*

$$G = \begin{bmatrix} \mathbf{g}^1 \\ \mathbf{g}^2 \\ \vdots \\ \mathbf{g}^k \end{bmatrix}$$

d.h. es gilt $\forall \mathbf{c} \in \mathbb{B}^n$:

$$\mathbf{c} \in C \iff \exists \mathbf{x} \in \mathbb{B}^k : \mathbf{c} = \mathbf{x} \cdot G$$

- ▶ Da die Basis eines Vektorraumes nicht eindeutig bestimmt ist, gibt es auch immer mehrere Generatormatrizen zu einem linearen Code.

- ▶ mittels *Akzeptoren*, d.h. durch Angabe einer *Basis* $\mathbf{h}^1, \mathbf{h}^2, \dots, \mathbf{h}^{n-k}$ des zu C orthogonalen Teilraumes

$$C^\perp = \{\mathbf{b} \in \mathbb{B}^n : \forall \mathbf{c} \in C : \mathbf{b} \cdot \mathbf{c}^t = 0\},$$

also durch eine *Kontrollmatrix*

$$H = \begin{bmatrix} \mathbf{h}^1 \\ \mathbf{h}^2 \\ \vdots \\ \mathbf{h}^{n-k} \end{bmatrix}$$

d.h. es gilt $\forall \mathbf{c} \in \mathbb{B}^n$:

$$\mathbf{c} \in C \iff H \cdot \mathbf{c}^t = \mathbf{0}^t$$

- ▶ Da die Basis eines Vektorraumes nicht eindeutig bestimmt ist, gibt es auch immer mehrere Kontrollmatrizen zu einem linearen Code.

Beispiel

- Ein Code $\mathcal{C} \subseteq \mathbb{B}^4$ der Dimension 2 sei gegeben durch die Generatormatrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

oder – gleichwertig – durch die Kontrollmatrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Der Code enthält die 4 Vektoren

0000, 1010, 0111, 1101

Sein Minimalgewicht und der Minimalabstand sind $d_{\min}(\mathcal{C}) = 2$.

Beispiel

- Ein Code $\mathcal{C} \subseteq \mathbb{B}^4$ der Dimension 3 sei gegeben durch die Generatormatrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

oder – gleichwertig – durch die Kontrollmatrix

$$H = [1 \ 1 \ 1 \ 1]$$

Der Code enthält die $2^3 = 8$ Vektoren aus \mathbb{B}^4 mit geradem Gewicht.

0000, 1001, 0101, 0011, 1100, 1010, 0110, 1111

Sein Minimalgewicht und der Minimalabstand sind $d_{\min}(\mathcal{C}) = 2$.

- Systematische Codierung

- Bezeichnet $E_k \in \mathbb{B}^{k \times k}$ die Einheitsmatrix und ist $A \in \mathbb{B}^{k \times (n-k)}$ eine Matrix, so hat der von

$$G = [E_k \mid A]$$

erzeugte lineare $[n, k]$ -Code die Kontrollmatrix

$$H = [A^t \mid E_{n-k}]$$

- Bei der Codierung

$$\mathbb{B}^k \rightarrow \mathcal{C} : \mathbf{x} \mapsto \mathbf{x} \cdot G = [\mathbf{x} \mid \mathbf{x} \cdot A]$$

ist die ursprüngliche Nachricht \mathbf{x} im Codewort sichtbar!

Codierung und Decodierung linearer Codes

- \mathcal{C} linearer $[n, k, d]$ -Code mit Generatormatrix G und Kontrollmatrix H .
- Quelle $S = \mathbb{B}^k$
- Codierung mittels linearer Transformation

$$\Phi : \mathbb{B}^k \rightarrow \mathbb{B}^n : \mathbf{x} \mapsto \mathbf{c} = \mathbf{x} \cdot G$$

- Tritt bei Übertragung Fehler $\mathbf{f} \in \mathbb{B}^n$ auf, d.h. wird $\mathbf{b} = \mathbf{c} \oplus \mathbf{f}$ empfangen, so gilt wegen $H \cdot \mathbf{c}^t = \mathbf{0}^t$ und Linearität:

$$\mathbf{s}^t = H \cdot \mathbf{b}^t = H \cdot \mathbf{c}^t \oplus H \cdot \mathbf{f}^t = H \cdot \mathbf{f}^t$$

d.h. empfangener Vektor \mathbf{b} und Fehlervektor \mathbf{f} haben das gleiche *Syndrom* \mathbf{s}^t .

- Codevektoren sind Vektoren mit Syndrom $\mathbf{0}^t$.

Syndromdecodierung

- ▶ Mit den genannten Daten G, H, \mathbf{b} :
 - ▶ berechne das Syndrom $\mathbf{s}^t = H \cdot \mathbf{b}^t$ des empfangenen Vektors \mathbf{b}
 - ▶ bestimme unter den Vektoren $\mathbf{b} \oplus \mathcal{C}$ mit dem gleichen Syndrom \mathbf{s}^t einen Vektor \mathbf{a} mit minimalem Gewicht (der mutmassliche Fehlervektor)
 - ▶ $\Psi(\mathbf{b}) = \mathbf{b} \oplus \mathbf{a} \in \mathcal{C}$
- ▶ Algebraisch gesprochen ist die Menge $\mathbf{b} \oplus \mathcal{C}$ eine *Nebenklasse* (coset) der Untergruppe \mathcal{C} von \mathbf{B}^n . Einen Vektor von minimalem Gewicht (nicht notwendigerweise eindeutig) in einer solchen Klasse nennt man einen *Führer* der Nebenklasse (coset leader). Man spricht deshalb auch von coset-leader Decodierung. Für "kleine" Codes kann man effizient mit coset-leader Tabellen (Syndromtabellen) arbeiten, d.h. Tabelle mit (Fehler)Vektor minimalen Gewichts zu jedem möglichen Syndrom.

Zur Komplexität der linearen Decodierung

- ▶ Die beiden folgenden Probleme sind NP-vollständig:
 - ▶ (LD – linear decoding)
Gegeben: eine Kontrollmatrix $H \in \mathbb{B}^{m \times n}$, ein (Syndrom)Vektor $\mathbf{s} \in \mathbb{B}^m$ und eine Zahl $w \in \mathbb{N}$.
 - Gibt es einen Vektor $\mathbf{x} \in \mathbb{B}^n$ mit $H \cdot \mathbf{x}^t = \mathbf{s}^t$ und $\|\mathbf{x}\| \leq w$?
 - ▶ (EMD – exact minimum distance)
Gegeben: eine Kontrollmatrix $H \in \mathbb{B}^{m \times n}$ und eine Zahl $w \in \mathbb{N}$.
 - Gibt es einen Vektor $\mathbf{x} \in \mathbb{B}^n$ mit $H \cdot \mathbf{x}^t = \mathbf{0}^t$ und $\|\mathbf{x}\| = w$?
- ▶ E.R. BERLEKAMP, R.J. McELIECE, H.C.A. VAN TILBURG, *On the inherent intractability of certain coding problems*, IEEE Transactions on Information Theory 24 (1978).

Der [7, 4, 3]-Hamming Code

- ▶ In \mathbb{B}^7 werden folgende Vektoren ausgezeichnet

$\mathbf{g}^0 = \mathbf{1}^7 = 1111111$	$\mathbf{h}^0 = \mathbf{0}^7 = 0000000$
$\mathbf{g}^1 = \bigoplus_{i \in \{1,2,4\}} \mathbf{e}^i = 1101000$	$\mathbf{h}^1 = \bigoplus_{i \in \{3,5,6,7\}} \mathbf{e}^i = 0010111$
$\mathbf{g}^2 = \bigoplus_{i \in \{2,3,5\}} \mathbf{e}^i = 0110100$	$\mathbf{h}^2 = \bigoplus_{i \in \{4,6,7,1\}} \mathbf{e}^i = 1001011$
$\mathbf{g}^3 = \bigoplus_{i \in \{3,4,6\}} \mathbf{e}^i = 0011010$	$\mathbf{h}^3 = \bigoplus_{i \in \{5,7,1,2\}} \mathbf{e}^i = 1100101$
$\mathbf{g}^4 = \bigoplus_{i \in \{4,5,7\}} \mathbf{e}^i = 0001101$	$\mathbf{h}^4 = \bigoplus_{i \in \{6,1,2,3\}} \mathbf{e}^i = 1110010$
$\mathbf{g}^5 = \bigoplus_{i \in \{5,6,1\}} \mathbf{e}^i = 1000110$	$\mathbf{h}^5 = \bigoplus_{i \in \{7,2,3,4\}} \mathbf{e}^i = 0111001$
$\mathbf{g}^6 = \bigoplus_{i \in \{6,7,2\}} \mathbf{e}^i = 0100011$	$\mathbf{h}^6 = \bigoplus_{i \in \{1,3,4,5\}} \mathbf{e}^i = 1011100$
$\mathbf{g}^7 = \bigoplus_{i \in \{7,1,3\}} \mathbf{e}^i = 1010001$	$\mathbf{h}^7 = \bigoplus_{i \in \{2,4,5,6\}} \mathbf{e}^i = 0101110$

Beachte: $\mathbf{h}^i = \mathbf{g}^i \oplus \mathbf{1}^7$ ($0 \leq i \leq k$)

Die FANO-Ebene PG(2,2)

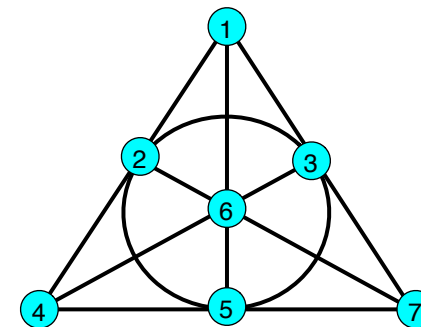


Abbildung: FANO-Ebene

- ▶ Eine *endliche projektive Ebene* besteht aus einer endlichen Menge von Punkten und einer endlichen Menge von Geraden und einer Inzidenzrelation ("liegt auf") zwischen Punkten und wobei gilt:
 - ▶ Je zwei Punkte liegen auf genau einer gemeinsamen Geraden
 - ▶ Je zwei Geraden schneiden sich in genau einem Punkt
 - ▶ Es gibt vier Punkte, so dass je drei von ihnen nicht auf einer Geraden liegen
- ▶ Zu einer endlichen projektiven Ebene gibt es eine Zahl n , die *Ordnung*, so dass gilt:
 - ▶ Jede Gerade enthält genau $n + 1$ Punkte
 - ▶ Jeder Punkt liegt auf $n + 1$ Geraden
 - ▶ Es gibt insgesamt $n^2 + n + 1$ Punkte
 - ▶ Es gibt insgesamt $n^2 + n + 1$ Geraden
- ▶ Die FANO-Ebene ist eine (sogar die einzige) projektive Ebene der Ordnung 2, also die kleinstmögliche projektive Ebene.

Zur Geometrie der FANO-Ebene

- ▶ Die FANO-Ebene enthält sieben Punkte $\{1, 2, \dots, 7\}$ und sieben Geraden $\{g^1, g^2, \dots, g^7\}$, wobei

$$g^k = \{k, k + 1, k + 3\} \pmod{7} \quad (1 \leq k \leq 7)$$

- ▶ Die drei Geraden, die durch den Punkt k gehen, sind g^k, g^{k+4}, g^{k+6} ($1 \leq k \leq 7$). Es gilt also

$$g^k \oplus g^{k+4} \oplus g^{k+6} = 1^7$$

- ▶ Sind g^i und g^j zwei Geraden, so haben diese genau einen Schnittpunkt ℓ und es gibt noch genau eine weitere Gerade g^k , die ℓ enthält. Also ist $g^i \oplus g^j \oplus g^k = 1^7$ und somit

$$g^i \oplus g^j = g^k \oplus 1^7 = h^k$$

- ▶ $\mathcal{H} := \{h^i; 0 \leq i \leq 7\}$, $\mathcal{G} := \mathcal{H} \cup \{g^i; 0 \leq i \leq 7\}$
- ▶ Fundamentale Beobachtung (FANO-Ebene!):
Zu jedem Paar (i, j) mit $0 \leq i, j \leq 7$ gibt es ein k mit $0 \leq k \leq 7$ mit : $g^i \oplus g^j = h^k$
- ▶ Folgerung: \mathcal{G} und \mathcal{H} sind unter \oplus abgeschlossen, also lineare Codes der Länge 7, denn

$$\begin{aligned} g^i \oplus g^j &= h^k \\ g^i \oplus h^j &= g^i \oplus g^j \oplus 1^7 = h^k \oplus 1^7 = g^k \\ h^i \oplus h^j &= g^i \oplus 1^7 \oplus g^j \oplus 1^7 = h^k \end{aligned}$$

- ▶ \mathcal{G} und \mathcal{H} sind lineare Teilräume von \mathbb{B}^7 ,
 $\dim \mathcal{G} = 4$, $\dim \mathcal{H} = 3$.
- ▶ \mathcal{G} ist der [7, 4, 3]-HAMMING-Code, \mathcal{H} der dazu *duale* [7, 3, 4]-Code.

- ▶ Nachweis der Orthogonalität von \mathcal{G} und \mathcal{H}

Mit $g^i \oplus h^j = g^k$ (wie vorher) gilt:

- ▶ wegen $\|g^i\|, \|g^k\| \in \{3, 7\}$ und $\|h^j\| \in \{0, 4\}$ und

$$\|g^k\| = \|g^i \oplus h^j\| = \|g^i\| + \|h^j\| - 2 \cdot \|g^i \wedge h^j\|$$

gilt $\|g^i \wedge h^j\| \equiv 0 \pmod{2}$, also $h^j \cdot (g^i)^t = 0$

- ▶ wegen $\|h^i\|, \|h^j\|, \|h^k\| \in \{0, 4\}$ und

$$\|h^k\| = \|h^i \oplus h^j\| = \|h^i\| + \|h^j\| - 2 \cdot \|h^i \wedge h^j\|$$

gilt $\|h^i \wedge h^j\| \equiv 0 \pmod{2}$, also $h^j \cdot (h^i)^t = 0$

- ▶

- ▶ Je 4 linear unabhängige Vektoren aus \mathcal{G} bilden eine Basis und können für eine Generatormatrix genommen werden, z.B.

$$G = \begin{pmatrix} \mathbf{g}^1 \\ \mathbf{g}^2 \\ \mathbf{g}^3 \\ \mathbf{g}^4 \end{pmatrix} = \begin{pmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{pmatrix}$$

- ▶ Je 3 linear-unabhängige Vektoren aus \mathcal{H} bilden eine Basis und können für eine Kontrollmatrix genommen werden, z.B.

$$H = \begin{pmatrix} \mathbf{h}^1 \\ \mathbf{h}^2 \\ \mathbf{h}^3 \end{pmatrix} = \begin{pmatrix} 0010111 \\ 1001011 \\ 1100101 \end{pmatrix}$$

Beachte: die Spalten von H enthalten jeden Vektor $\neq \mathbf{0}^3$ aus \mathbb{B}^3 genau einmal!

Eine interessante Eigenschaft

- ▶ Wegen $d_{\min}(\mathcal{G}) = 3$ ist der [7, 4, 3]-HAMMING-Code 1-Fehler-korrigierend, die HAMMING-Kugeln vom Radius 1

$$\mathbf{c} \oplus \mathbb{B}_{\leq 1}^7 \quad (\mathbf{c} \in \mathcal{G})$$

sind paarweise disjunkt.

- ▶ Jede dieser HAMMING-Kugeln enthält genau $V(7, 1) = 8$ Elemente

$$\mathbf{c} \text{ und } \mathbf{c} \oplus \mathbf{e}^i \quad (1 \leq i \leq 7)$$

- ▶ Wegen

$$\#\mathcal{G} \cdot V(7, 1) = 2^4 \cdot 8 = 2^7 = \#\mathbb{B}^7$$

bilden diese HAMMING-Kugeln eine *Zerlegung* von \mathbb{B}^7 . Man sagt: der [7, 4, 3]-HAMMING-Code ist ein *perfekter* Code.

- ▶ Perfekte Codes sind extrem selten!

- ▶ Sei $r > 0$ und $n = 2^r - 1$. Sei H eine $r \times n$ -Matrix, die alle Elemente von \mathbb{B}^r ($\neq \mathbf{0}^r$) als Spaltenvektoren enthält.
- ▶ Die Matrix H hat den Rang r , kann also als Kontrollmatrix eines Codes \mathcal{G} der Länge n und der Dimension $\dim \mathcal{G} = n - r = 2^r - r - 1$ aufgefasst werden.
- ▶ Da je zwei Spalten von H linear-unabhängig sind, enthält \mathcal{G} keine Vektoren vom Gewicht 1 oder 2. Also gilt $d_{\min}(\mathcal{G}) \geq 3$, d.h. der Code \mathcal{G} ist 1-Fehler-korrigierend.
- ▶ Wegen

$$\#\mathcal{G} \cdot V(n, 1) = 2^{n-r} \cdot (n + 1) = 2^n$$

bilden die HAMMING-Kugeln vom Radius 1 um die Codevektoren eine Zerlegung von \mathbb{B}^n , es gilt also $d_{\min}(\mathcal{G}) = 3$ und der Code ist perfekt.

- ▶ Dieser $[2^r - 1, 2^r - r - 1, 3]$ -Code heisst (binärer) HAMMING-Code der Ordnung r .

Zur Decodierung der HAMMING Codes

- ▶ H Kontrollmatrix des $[2^r - 1, 2^r - r - 1, 3]$ -HAMMING Codes der Ordnung r .
- ▶ Die Spalten von H sind genau die Vektoren $\neq \mathbf{0}$ aus \mathbb{B}^r . Zu jedem $\mathbf{b} \in \mathbb{B}^{2^r-1}$ gibt es also genau ein $1 \leq i \leq 2^r - 1$ mit $H \cdot \mathbf{b}^t = H \cdot \mathbf{e}^i$, d.h. das Syndrom ist die i -te Spalte der Matrix H . Dann ist \mathbf{e}^i der gesuchte coset leader!
- ▶ Decodierung
 - ▶ empfangen $\mathbf{b} \in \mathbb{B}^{2^r-1}$ und berechne das Syndrom $\mathbf{s} = H \cdot \mathbf{b}^t$
 - ▶ $\Psi(\mathbf{b}) = \mathbf{b} \oplus \mathbf{e}^i$, wobei \mathbf{s} die i -te Spalte von H ist.
- ▶ R.W. HAMMING, *Error detecting and error correcting codes*, Bell Systems Technical Journal, 29 (1950).

Reed-Muller Codes

- Die Abbildung

$$\rho_n : \mathbb{B}^{2^n} \equiv \mathbb{B}^n \times \mathbb{B}^n \rightarrow \mathbb{B}^{2^n} : (\mathbf{a}, \mathbf{b}) \mapsto (\mathbf{a} \oplus \mathbf{b}, \mathbf{b})$$

ist linear und invertierbar ($\rho_n \circ \rho_n = id$, also $\rho^{-1} = \rho$).

- $A \subseteq \mathbb{B}^{2^n}$ linear unabhängig $\Rightarrow \rho_n(A) \subseteq \mathbb{B}^{2^n}$ linear unabhängig
- A Basis von $\mathbb{B}^{2^n} \Rightarrow \rho_n(A)$ Basis von \mathbb{B}^{2^n}
- $A, B \subseteq \mathbb{B}^n$ linear unabhängig \Rightarrow

$$\rho_n(A \times \mathbf{0}^n \cup \mathbf{0}^n \times B) = \{(\mathbf{a}, \mathbf{0}^n); \mathbf{a} \in A\} \cup \{(\mathbf{b}, \mathbf{b}); \mathbf{b} \in B\} \subseteq \mathbb{B}^{2^n}$$

linear unabhängig

- A, B Basen von $\mathbb{B}^n \Rightarrow \rho_n(A \times \mathbf{0}^n \cup \mathbf{0}^n \times B)$ Basis von \mathbb{B}^{2^n}

- Für $m = 0, 1, 2, \dots$ werden Basen \mathcal{G}_m von \mathbb{B}^n mit $n = 2^m$ definiert:

- $\mathcal{G}_0 = \{\mathbf{1}^1\}$
- $\mathcal{G}_{m+1} = \rho_n(\mathcal{G}_m \times \mathbf{0}^n) \uplus \rho_n(\mathbf{0}^n \times \mathcal{G}_m)$
 $= \{(\mathbf{a}, \mathbf{0}^n); \mathbf{a} \in \mathcal{G}_m\} \cup \{(\mathbf{a}, \mathbf{a}); \mathbf{a} \in \mathcal{G}_m\}$

- Eigenschaften:

- $\#\mathcal{G}_m = 2^m$
 - Für alle $\mathbf{a} \in \mathcal{G}_m$ ist $\|\mathbf{a}\| = 2^r$ für ein $r \in \{0, 1, 2, \dots, m\}$
 - Sei $\mathcal{G}_{m,r} = \{\mathbf{a} \in \mathcal{G}_m; \|\mathbf{a}\| = 2^{m-r}\}$.
- Dann gilt $\mathcal{G}_{m,0} = \{\mathbf{1}^n\}$ ($m \geq 0$) und

$$\mathcal{G}_{m+1,r+1} = \rho_n(\mathcal{G}_{m,r} \times \mathbf{0}^n) \uplus \rho_n(\mathbf{0}^n \times \mathcal{G}_{m,r+1}) \quad (0 \leq r \leq m)$$

also insbesondere

$$\#\mathcal{G}_{m+1,r+1} = \#\mathcal{G}_{m,r} + \#\mathcal{G}_{m,r+1} \quad (0 \leq r \leq m)$$

und daher (per Induktion)

$$\#\mathcal{G}_{m,r} = \binom{m}{r} \quad (0 \leq r \leq m)$$

- Der (binäre) REED-MULLER Code $\mathcal{RM}_{m,r}$ der Länge $n = 2^m$ und der Ordnung r ($0 \leq r \leq m$) ist der von

$$\mathcal{G}_{m,0} \cup \mathcal{G}_{m,1} \cup \dots \cup \mathcal{G}_{m,r}$$

erzeugte lineare Teilraum von \mathbb{B}^n .

- Eigenschaften

- Inklusion als Teilräume

$$\{\mathbf{0}^n, \mathbf{1}^n\} = \mathcal{RM}_{m,0} \subset \mathcal{RM}_{m,1} \subset \mathcal{RM}_{m,2} \subset \dots \subset \mathcal{RM}_{m,m} = \mathbb{B}^n$$

- rekursive Darstellung

$$\mathcal{RM}_{m+1,r+1} = \rho_n(\mathcal{RM}_{m,r} \times \mathcal{RM}_{m,r+1})$$

- Dimension

$$\dim(\mathcal{RM}_{m,r}) = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r} = V(m, r)$$

- Minimalabstand: $d_{\min}(\mathcal{RM}_{m,r}) = 2^{m-r}$

Beispiele:

- $\mathcal{G}_{0,0} = \{1\}$
- $\mathcal{G}_{1,0} = \{11\}$
 $\mathcal{G}_{1,1} = \{10\}$
- $\mathcal{G}_{2,0} = \{1111\}$
 $\mathcal{G}_{2,1} = \{1100, 1010\}$
 $\mathcal{G}_{2,2} = \{1000\}$
- $\mathcal{G}_{3,0} = \{11111111\}$
 $\mathcal{G}_{3,1} = \{11110000, 11001100, 10101010\}$
 $\mathcal{G}_{3,2} = \{11000000, 10100000, 10001000\}$
 $\mathcal{G}_{3,3} = \{10000000\}$

Alternative Beschreibung der REED-MULLER Basisvektoren
Für $n = 2^m$ werden Vektoren $\mathbf{v}^1, \dots, \mathbf{v}^m$ definiert

$$\begin{aligned} \mathbf{v}^1 &= \mathbf{1}^{2^{m-1}} \mathbf{0}^{2^{m-1}} \\ \mathbf{v}^2 &= \mathbf{1}^{2^{m-2}} \mathbf{0}^{2^{m-2}} \mathbf{1}^{2^{m-2}} \mathbf{0}^{2^{m-2}} \\ &\dots \\ \mathbf{v}^k &= \left(\mathbf{1}^{2^{m-k}} \mathbf{0}^{2^{m-k}} \right)^{2^{r-1}} \\ &\dots \\ \mathbf{v}^m &= (\mathbf{10})^{2^{m-1}} \end{aligned}$$

Für $1 \leq r \leq m$ besteht $\mathcal{G}_{m,r}$ aus den Vektoren $\bigwedge_{i \in A} \mathbf{v}^i$, wobei A r -elementige Teilmenge von $\{1, 2, \dots, m\}$ ist.

Andere Formulierung dieser Beschreibung:

- ▶ Es seien X_1, X_2, \dots, X_m boolesche Variable.
Jede Variable definiert eine (lineare) Funktion

$$X_k : \mathbb{B}^m \rightarrow \mathbb{B} : \mathbf{b} = (b_1, b_2, \dots, b_m) \mapsto b_k \quad (1 \leq k \leq m)$$

- ▶ Für jeden Bitvektor $\mathbf{c} = (c_1, c_2, \dots, c_m) \in \mathbb{B}^m$ definiert das boolesche Monom $X_{\mathbf{c}} = \bigwedge_{c_i=1} X_i$ eine Funktion:

$$X_{\mathbf{c}} : \mathbb{B}^m \rightarrow \mathbb{B} : \mathbf{b} = (b_1, b_2, \dots, b_m) \mapsto \bigwedge_{c_k=1} b_k$$

$$\text{d.h. } X_{\mathbf{c}}(\mathbf{b}) = 1 \iff \mathbf{c} \leq \mathbf{b}$$

- ▶ Ein boolesches Polynom ist eine Summe von Monomen, also durch eine Abbildung $p : \mathbb{B}^m \rightarrow \mathbb{B}$ gegeben. Dies definiert eine Funktion

$$X_p : \mathbb{B}^m \rightarrow \mathbb{B} : \mathbf{b} \mapsto \bigoplus_{p(\mathbf{c})=1} X_{\mathbf{c}}(\mathbf{b})$$

- ▶ Zu jeder booleschen Funktion $f : \mathbb{B}^m \rightarrow \mathbb{B}$ gibt es genau ein boolesches Polynom X_p , das diese Funktion darstellt:

$$\forall \mathbf{b} \in \mathbb{B} : f(\mathbf{b}) = X_p(\mathbf{b})$$

(Ring-Normalform von booleschen Funktionen).

- ▶ Der REED-MULLER Code $\mathcal{RM}_{m,r}$ besteht genau aus den Werte-Vektoren

$$\mathbf{v}_p = (X_p(\mathbf{b}))_{\mathbf{b} \in \mathbb{B}^m}$$

wo p ein boolesches Polynom vom Grad $\leq r$ ist.

Zum Minimalabstand (Beweis durch Induktion)

- ▶ $d_{\min}(\mathcal{RM}_{n+1,r+1}) \leq 2^{m-r}$
 - ▶ Ist $\mathbf{a} \in \mathcal{RM}_{m,r}$ mit $\|\mathbf{a}\| = 2^{m-r}$, so ist $(\mathbf{a}, \mathbf{0}^n) \in \mathcal{RM}_{m+1,r+1}$ mit $\|(\mathbf{a}, \mathbf{0}^n)\| = 2^{m-r} = 2^{(m+1)-(r+1)}$
 - ▶ Ist $\mathbf{a} \in \mathcal{RM}_{m,r+1}$ mit $\|\mathbf{a}\| = 2^{m-r-1}$, so ist $(\mathbf{a}, \mathbf{a}) \in \mathcal{RM}_{m+1,r+1}$ mit $\|(\mathbf{a}, \mathbf{a})\| = 2 \cdot 2^{m-r-1} = 2^{(m+1)-(r+1)}$
- ▶ $d_{\min}(\mathcal{RM}_{m+1,r+1}) \geq 2^{m-r}$
Für $\mathbf{w} = (\mathbf{u} \oplus \mathbf{v}, \mathbf{v}) \in \mathcal{RM}_{m+1,r+1}$ mit $\mathbf{u} \in \mathcal{RM}_{m,r}$, $\mathbf{v} \in \mathcal{RM}_{m,r+1}$ und mit $\mathbf{w} \neq \mathbf{0}^{2n}$ gilt
 - ▶ $\mathbf{v} = \mathbf{0}^n \Rightarrow \mathbf{u} \neq \mathbf{0}^n$, also $\|\mathbf{w}\| = \|(\mathbf{u}, \mathbf{0}^n)\| = \|\mathbf{u}\| \geq 2^{m-r}$
 - ▶ $\mathbf{u} = \mathbf{0}^n \Rightarrow \mathbf{v} \neq \mathbf{0}^n$, also $\|\mathbf{w}\| = \|(\mathbf{v}, \mathbf{v})\| = 2 \cdot \|\mathbf{v}\| \geq 2 \cdot 2^{m-r-1} = 2^{m-r}$
 - ▶ $\mathbf{u} \neq \mathbf{0}^n \neq \mathbf{v}$ und $\mathbf{u} = \mathbf{v} \Rightarrow \mathbf{w} = (\mathbf{0}^n, \mathbf{v})$ und $\mathbf{v} \in \mathcal{RM}_{m,r}$, also $\|\mathbf{w}\| = \|\mathbf{v}\| \geq 2^{m-r}$
 - ▶ $\mathbf{u} \neq \mathbf{0}^n \neq \mathbf{v}$ und $\mathbf{u} \neq \mathbf{v} \Rightarrow \mathbf{u} \oplus \mathbf{v} \in \mathcal{RM}_{m,r+1}$, also $\|\mathbf{w}\| = \|\mathbf{u} \oplus \mathbf{v}\| + \|\mathbf{v}\| \geq 2 \cdot 2^{m-r-1} = 2^{m-r}$

Bemerkungen: Die REED-MULLER Codes

- ▶ gehen zurück auf die Arbeiten
 - ▶ I.S. REED, *A Class of Multiple Error Correcting Codes and the Decoding Scheme*, IRE Transactions Inform. Theory (1954).
 - ▶ D.E. MULLER, *Application of Boolean Algebra to Switching Circuit Design*, IRE Transactions Electronic Computing (1954).
- ▶ lassen sich elegant und effizient mit *majority logic* decodieren – dank enger Beziehung zu geometrischen Konfigurationen (diskrete euklidische und projektive Geometrie).
- ▶ gehören, neben den HAMMING und den GOLAY Codes, zu frühesten interessanten und nützlichen linearen Codes.
- ▶ fanden breite Beachtung dank ihrer Verwendung in Projekten des NASA (1969–1976), z.B. der [32, 6, 16]-Code $\mathcal{RM}_{5,1}$ im MARINER-Projekt. → E.C. POSNER, *Combinatorial Structures in Planetary Reconnaissance*, in: H.B. MANN (ed.), *Error Correcting Codes*, Wiley (1968).

Zyklische Codes

- ▶ Ein (binärer) linearer $[n, k, d]$ Code $\mathcal{C} \subseteq \mathbb{B}^n$ ist *zyklisch*, wenn er mit jedem Codewort auch dessen zyklische shifts enthält:

$$\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathcal{C} \Rightarrow (a_2, a_3, \dots, a_n, a_1) \in \mathcal{C}$$

- ▶ Die meisten der praktisch verwendeten Blockcodes sind zyklische Codes (z.B. HAMMING Codes, GOLAY Codes, verkürzte REED-MULLER Codes, BCH Codes, REED-SOLOMON Codes)
- ▶ Zyklische Codes lassen sich elegant mit Mitteln der *Polynomarithmetik* beschreiben, untersuchen und implementieren (→ lineare Schieberegister)
- ▶ Effiziente Codierungsalgorithmen benutzen lineare Schieberegister; effiziente Decodierung beruht auf Polynomarithmetik (euklidischer Algorithmus!)
- ▶ sehr lange zyklische Codes sind nicht besonders gut im Sinne der asymptotische Schranken, bessere Codes (z.B. GOPPA Codes) erfordern aber einen viel höheren mathematischen Aufwand!

- ▶ $A(n, d)$: maximales K , für das ein (n, K, d) -Code existiert
- ▶ obere Schranke (PLOTKIN-Schranke)

$$A(n, d) \leq \frac{2d}{2d - n} \quad \text{für } 2d > n$$

- ▶ Beweis: für einen (n, K, d) -Code \mathcal{C} gilt

$$d \cdot \frac{K(K-1)}{2} \leq \frac{1}{2} \sum_{\mathbf{a}, \mathbf{b} \in \mathcal{C}} d(\mathbf{a}, \mathbf{b}) \leq n \cdot \max_{1 \leq k \leq K} k \cdot (K-k) = n \cdot \frac{K^2}{4}$$

- ▶ untere Schranke (GILBERT-VARSHAMOV-Schranke)

$$A(n, d) \geq \frac{2^n}{V(n, d-1)}$$

- ▶ Beweis: Ist \mathcal{C} ein (n, K, d) -Code, so gilt wegen der Maximalität von K :

$$\mathbb{B}^n \subseteq \bigcup_{\mathbf{a} \in \mathcal{C}} S_{d-1}(\mathbf{a})$$

Asymptotische Aussagen

- ▶ Sei $0 \leq \delta \leq 1$ und $R(\delta)$ die maximale Rate, die asymptotisch für Codes der Länge n mit relativer Minimaldistanz $\delta = d/n$ erreicht werden kann. D.h.

$$R(\delta) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log A(n, \delta \cdot n)$$

Dann gilt

- ▶ (PLOTKIN)

$$R(\delta) \begin{cases} \leq 1 - 2 \cdot \delta & \text{falls } 0 \leq \delta \leq 1/2 \\ = 0 & \text{falls } 1/2 \leq \delta \leq 1 \end{cases}$$

- ▶ (GILBERT-VARSHAMOV)

$$R(\delta) \geq 1 - H(\delta) \quad (0 \leq \delta \leq 1/2)$$

Beweis der asymptotischen PLOTKIN-Schranke

- ▶ Ist \mathcal{C} ein (n, K, d) -Code, so kann man daraus für $r = 1, 2, \dots$ einen $(n - r, K_r, d)$ -Code \mathcal{C}_r konstruieren mit $K_r \geq K/2^r$.
- ▶ Für $n - r = 2d - 2$ erhält man nach PLOTKIN:

$$\frac{K}{2^r} \leq \#\mathcal{C}_r \leq \frac{2d}{2d - (n - r)} = d, \text{ also } K \leq d \cdot 2^r$$

- ▶ Daraus folgt mit $d = \delta \cdot n$

$$\begin{aligned} R(\delta) &\leq \limsup_{n \rightarrow \infty} \frac{1}{n} \cdot \log(\delta \cdot n \cdot 2^{n-2\delta \cdot n+2}) \\ &= \lim_{n \rightarrow \infty} \left(\frac{\log \delta}{n} + \frac{\log n}{n} + 1 - 2\delta + \frac{2}{n} \right) \\ &= 1 - 2\delta \end{aligned}$$

Beweis der asymptotischen GILBERT-VARSHAMOV-Schranke

- ▶ Aus der asymptotischen Abschätzung des Volumens von HAMMING-Kugeln folgt sofort:

$$\begin{aligned} R(\delta) &\geq \limsup_{n \rightarrow \infty} \frac{1}{n} \cdot \log \frac{2^n}{V(n, \delta \cdot n)} \\ &= 1 - \lim_{n \rightarrow \infty} \frac{1}{n} \cdot \log V(n, \delta \cdot n) \\ &= 1 - H(\delta) \end{aligned}$$

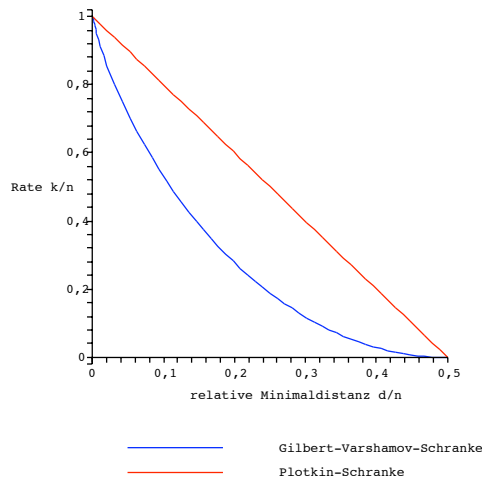


Abbildung: Asymptotische Schranken für Codes

- ▶ Es gibt neben der GILBERT-VARSHAMOV-Schranke und der PLOTKIN-Schranke noch viele weitere Schranken, vor allem obere (HAMMING, ELIAS, McELIECE, ...).
- ▶ Die GILBERT-VARSHAMOV-Schranke war von 1952 bis 1982 die beste bekannte untere Schranke! Erst dann gelang es TSFASMAN, VLADUT, ZINK mit Hilfe von GOPPA-Codes (1977 erfunden) Codes zu konstruieren, welche die GILBERT-VARSHAMOV-Schranke übertreffen.
- ▶ Literatur
 - ▶ D. WELSH, *Codes and Cryptography*, Oxford UP (1988).
 - ▶ F.J. MACWILLIAMS, N. J.A. SLOANE, *The Theory of Error-Correcting Codes*, Elsevier (1997).