Def.: Sei $C \subseteq \mathbb{F}_q^n$ ein $[n,k]$-Code. Der zu C duale Code ist

$$C^\perp = \{ y \in \mathbb{F}_q^n : x^T y = \sum_{i=1}^{n} x_i y_i = 0 \}.$$

Dies ist ein $[n, n-k]$-Code, Falls $C = C^\perp$ gilt, dann heißt C selbst-dual.

Def.: a) Sei $C \subseteq \mathbb{F}_q^n$ ein $[n,k]$-Code. Eine Matrix $G \in \mathbb{F}_q^{k \times n}$ heißt Erzeugermatrix (generator matrix) von C, falls die Zeilen von G den linearen Code C erzeugen / aufspannen.

b) Eine Matrix $H \in \mathbb{F}_q^{(n-k) \times k}$ heißt Kontrollmatrix (parity check matrix) von C, falls $C = \{ x \in \mathbb{F}_q^n : Hx = 0 \} = \operatorname{Kern} H$ gilt.

Lemma $G \in \mathbb{F}_q^{k \times n}$ Erzeugermatrix von C $\Leftrightarrow$ G Kontrollmatrix von $C^\perp$.

Def.: Zwei Code $C, C' \subseteq \mathbb{F}_q^n$ heißen äquivalent, falls

$\exists\, t_1, \dots, t_n \in \mathbb{F}_q \setminus \{0\}$ $\exists\, \sigma \in S_n$, so dass

$$C' = \{ (t_1 x_{\sigma(1)}, \dots, t_n x_{\sigma(n)}) : x \in C \}.$$

Satz Sei $C \subseteq \mathbb{F}_q^n$ ein $[n,k]$-Code.

a) Es gibt einen zu C äquivalenten Code C', der eine Erzeugermatrix in Standardform

$$G = [\, I_k \mid A \,], \quad A \in \mathbb{F}_q^{k \times (n-k)}$$

(I_k: $k \times k$-Einheitsmatrix)

besitzt.

b) Im Fall von a) ist

$$H = [\, -A^T \mid I_{n-k} \,]$$

eine Kontrollmatrix von C'.

Bew.: a) Lineare Algebra

b) $GH = 0$.

Allgemeine Decodierungsprozedur für lineare Codes

Sei $C \subseteq \mathbb{F}_q^n$ ein $[n,k]$-Code, gegeben durch eine Kontrollmatrix $H \in \mathbb{F}_q^{(n-k)\times n}$, d.h.

$$C = \{ x \in \mathbb{F}_q^n : xH^T = 0 \}.$$

Def.: Für $x \in \mathbb{F}_q^n$ ist das **Syndrom** definiert als $xH^T \in \mathbb{F}_q^{(n-k)}$.

Klar: $x \in C \iff xH^T = 0$

Es ist: $xH^T = yH^T \iff x - y \in C$

Finde also $e \in \mathbb{F}_q^n$ mit $xH^T = eH^T$ und minimalem Gewicht $w(e)$. Dann wird x als $x-e$ decodiert.

Aber:

Theorem (Berlekamp, McEliece, van Tilborg) (1978)

Die Berechnung eines solchen e's (ein sog. „Nebenklassenspitzenreiter" (coset leader)) ist NP-vollständig, selbst für $q = 2$.

Bew.: → Seminar Codierungstheorie WS 16/17.

§ 3 Gewichtszähler / Die MacWilliams-Identität

Sei $C \subseteq \mathbb{F}_q^n$ ein linearer Code.

Def.: Definiere

$$A_i = \left| \{ x \in C : w(x) = i \} \right| , \quad i = 0, \dots, n$$

die Anzahl der Codewörter von C vom Gewicht i.
Der **Gewichtszähler** von C (weight enumerator) ist das homogene Polynom

$$W_C(X,Y) = \sum_{i=0}^{n} A_i \, X^{n-i} Y^i .$$

Theorem (MacWilliams, 1963)

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} \, W_C\big(X + (q-1)Y, \; X - Y\big).$$

Bew.: Verwende Orthogonalitätsrelation von Charakteren:

Lemma (Orthogonalitätsrelation)
Sei $(A,+)$ eine endliche abelsche Gruppe. Sei
$\chi : A \to \mathbb{C}^\times = \{ z \in \mathbb{C} : |z| = 1 \}$ ein Charakter von A,