Hinweis zu Aufgabe 16 auf der Webseite der Vorlesung!

z.B $m = 3$, $q = 2$

Hamming-Codes $H = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$

Spaltengröße n

im Falle eines ternären Codes,

also $A = \mathbb{F}_3 = \{0, 1, 2\}$ und $n = 3$

$$\frac{q^m - 1}{q - 1} = \frac{3^3 - 1}{3 - 1} = 13$$

$$H = \left(\begin{array}{ccccccccccc|ccc} 1 & 1 & 1 & 2 & 0 & 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 0 & 0 & 1 \end{array}\right)$$

jedes Element aus $\mathbb{F}_3^3 \setminus \{0\}$ ist Vielfaches einer der Spalten!

(bedenke $2 \cdot 2 = 1$ in $\mathbb{F}_3$)

z.B $2 \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$

Fehlerkorrektur beim binären Hamming-Code

Annahme: es tritt höchstens 1 Fehler auf, d.h. mögliche Fehler sind

$e_1, \ldots, e_n$ (Standardbasisvektoren)

Syndrom von e_i ist gerade die i-te Spalte von H

Decodieren beim binären Hamming-Code:

empfangene Nachricht $w \in H(n,2)$

rechne Syndrom $H \cdot w^T$ aus:

- falls $H \cdot w^T = 0$, so gehen wir davon aus, dass kein Fehler aufgetreten ist
  Information = erste k-Stellen von w
- falls $H \cdot w^T \neq 0$: suche nach, in welcher Spalte i von H das Syndrom auftaucht
  korrigiere die i-te Stelle von w (d.h. berechne $w + e_i$)
  Information = erste k-Stellen von $w + e_i$

Hamming-Codes sind perfekt?

$$\left[\underbrace{\frac{q^m - 1}{q-1}}_{n}, \underbrace{\frac{q^m - 1}{q-1} - m}_{k}, \underbrace{3}_{d} \right]$$

$m = n - k$

Größe des Raums $H(n,q)$ ist q^n

Anzahl der Codewörter q^k

$$|B_1(v)| = 1 + (q-1) \cdot n = 1 + (q-1) \cdot \frac{q^m - 1}{q-1} = q^m$$

$v \in H(n,q)$

$$q^k \cdot |B_1(v)| = q^k \cdot q^m = q^{m+k} = q^n$$

✓

Liste der bekannten perfekten Codes

$[n, k, d]$ — Wortlänge, Dimension des Codes, Mindestabstand

Falls q Primzahlpotenz, so gibt es folgende perfekte Codes:

- der triviale $[n, 0, \infty]$-Code (d.h. nur ein Codewort) $e = n$
- der triviale $[n, n, 1]$-Code (alle Wörter sind Codewörter) $e = 0$

e = Anzahl der korrigierbaren Fehler

- die binären Wiederholungscodes: zu jedem $e \in \mathbb{N}$ ein $[2e+1, 1, 2e+1]$-Code
  (nur die beiden Codewörter $(0, 0, \ldots, 0)$, $(1, 1, \ldots, 1)$)
- die q-ären Hamming-Codes mit Parametern $\left[\frac{q^m - 1}{q-1}, \frac{q^m - 1}{q-1} - m, 3\right]$ $e = 1$
- einige nicht-lineare Codes mit gleichen Parametern wie Hamming-Codes
- den binären Golay-Code: ein $[23, 12, 7]$-Code mit $e = 3$
- den ternären Golay-Code: ein $[11, 6, 5]$-Code mit $e = 2$

Falls q keine Primzahlpotenz ist, weiß man nicht, ob es nicht-triviale perfekte Codes gibt.

Im allgemeinen weiß man nicht viel darüber, was die besten Codes sind.

KAPITEL II : ALGEBRA

Aufgabe 1 Korrektur:

Zeige $U \cap U^\perp \subseteq \{0\}$

also $U \cap U^\perp = \{0\}$

oder $U \cap U^\perp = \emptyset$

§1 Gruppen

Erinnerung an die Definition von Gruppen:

Menge G, zweistellige assoziative Verknüpfung $\circ$

neutrales Element e, d.h. $g \circ e = e \circ g = g$ für alle $g \in G$

Existenz von Inversen, d.h. zu jedem $g \in G$ existiert ein $g^{-1} \in G$ mit

$$g \circ g^{-1} = g^{-1} \circ g = e$$

Neutrales Element und inverse Elemente sind eindeutig bestimmt.

Kommutative oder abelsche Gruppe: falls $\circ$ kommutativ, d.h. $g \circ h = h \circ g$ für alle $g, h \in G$

Schreibweise: $G, \circ, e, g^{-1}$

$G, +, 0, -g$ additive Schreibweise (nur bei kommut. Gruppen)

$G, \cdot, 1, g^{-1}$ multiplikative Schreibweise

Beispiele:

(a) $(\mathbb{Z}, +)$

(b) $(\mathbb{Z}_m, +_m)$ $\quad \mathbb{Z}_m = \{0, 1, \dots, m-1\}$

$x +_m y$ = Rest von $x+y$ bei der Division durch m

$$= \begin{cases} x+y & \text{falls } x+y < m \\ x+y-m & \text{falls } x+y \geq m \end{cases}$$

"Uhrenarithmetik"
"modulo m rechnen"

kommutativ

(c) $(\mathrm{Sym}(M), \circ)$ $\quad \mathrm{Sym}(M)$ = Menge der Bijektionen $M \to M$
"Permutationen von M"

$\circ$ = Verknüpfung von Funktionen

S_n für $\mathrm{Sym}(M)$ mit $|M| = n$

(d) Automorphismengruppen, insbesondere

$GL(n, K)$ = Menge der $(n \times n)$-Matrizen mit Einträgen aus dem Körper K und Determinante $\neq 0$

$\hat{=}$ invertierbare Vektorraumhomomorphismen $K^n \to K^n$

Für $K = \mathbb{F}_q$, dann schreibt man auch $GL(n, q)$

Gruppenoperation = Matrizenmultiplikation

Bem: $GL(n, K) \subseteq \mathrm{Sym}(K^n)$

im allgemeinen nicht kommutativ

S_1, S_2 $GL(1, K)$ sind kommutativ

Def: Eine Abbildung $\varphi: G \to H$, $(G,\cdot)$, $(H,\circ)$ Gruppen, heißt Gruppenhomomorphismus, falls

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2) \quad \text{für alle } g_1, g_2 \in G$$

$$\varphi(e_G) = e_H$$

$$\varphi(g^{-1}) = \varphi(g)^{-1} \quad \text{für alle } g \in G$$

Bemerkung: diese Bedingung folgt aus, die beiden anderen Folge daraus

Bsp:

a) $\mathbb{Z} \to \mathbb{Z}_m$

$x \mapsto$ Rest von x bei der Division durch m

z.B. $m = 12$, $x = 29$, $y = -2$, $x + y = 27$ in $\mathbb{Z}$

"Reste modulo 12": $5 +_{12} 10 = 3$ in $\mathbb{Z}_m$

$x \in \mathbb{Z}$

es gibt eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$r \in \{0, 1, \dots, m-1\}$

und

$x = q \cdot m + r$

r heißt "Rest von x modulo m"

b) Signum ("Vorzeichen"): $S_n \to (\{+1, -1\}, \cdot) \cong \mathbb{Z}_2$

$\sigma \mapsto \operatorname{sg}(\sigma)$

↑ Gruppenisomorphie

"Parität der Anzahl von Transpositionen $\tau_1, \dots, \tau_n$ mit $\sigma = \tau_1 \circ \dots \circ \tau_n$"

$\cdot$	$+1$	-1
$+1$	$+1$	-1
-1	-1	$+1$

$+_2$	0	1
0	0	1
1	1	0

(Zu beweisen: Unabhängigkeit von der Darstellung)

c) Determinante: $\det: GL(n, K) \to (K^\times, \cdot)$

$GL(n, K)$: invertierbare $(n \times n)$-Matrizen über K

$K^\times$: $K \setminus \{0\}$

multiplikative Gruppe des Körpers K

Def: Ein Gruppenhomomorphismus $\varphi: G \to H$ heißt Gruppenisomorphismus, falls φ bijektiv ist und $\varphi^{-1}: H \to G$ auch ein Gruppenhomomorphismus ist.

Bemerkung: gilt stets für bijektive Gruppenhomomorphismen.

Zwei Gruppen G und H heißen isomorph zueinander, $G \cong H$, falls es einen Gruppenisomorphismus $\varphi: G \to H$ gibt.