Dr. Anton Malevich

Aufgaben zum Thema **Grundbegriffe und Beispiele**

Aufgabe 1.1 Wir betrachten den Code $C \subseteq \mathbb{F}_2^6$ aus Bespiel (1.0) b). Dieser besteht aus den Codewörtern:

000000	101010	010101	111111

a) Erklären Sie, warum C 1-fehlerkorriegierend ist. Wieviel Fehler kann C erkennen?

b) Erklären Sie anhand des Codes C, wie die Fehlererkennung funktioniert.

c) Ist der Code C perfekt?

d) Ist C ein MDS-Code?

Aufgabe 1.2 Wir betrachten den Code $C \subseteq \mathbb{F}_2^5$ aus Bespiel (1.0) c). Dieser besteht aus den Codewörtern:

00000	10110	01101	11011

a) Wieviel Fehler kann C erkennen, wieviel korrigieren?

b) Erklären Sie anhand des Codes C, wie die Fehlerkorrektur funktioniert.

c) Ist der Code C perfekt?

d) Ist C ein MDS-Code?

Aufgabe 1.3 Es sei ein binärer Code $C \subseteq \mathbb{F}_2^7$ gegeben, der aus den folgenden 16 Codewörtern besteht:

0000000	1111111
0001110	1110001
0010111	1101000
0011001	1100110
0100101	1011010
0101011	1010100
0110010	1001101
0111100	1000011

a) Bestimmen Sie die Informationsrate und die Minimaldistanz von C.

b) Ist der Code C perfekt?

c) Ist C ein MDS-Code?

d) Wir nehmen nun an, dass C für Fehlerkorrektur benutzt wird. Es seien drei Codewörter versendet, und die Tupel 0100011, 1100110 und 0000011 erhalten. Was sind laut Maximum-Likelihood-Decodierung die versendeten Codewörter? Unter welcher Voraussetzung sind es tatsächlich die richtigen?

e) Schreiben Sie ein Computerprogramm "ML-Decodierer", das ein beliebiges binäres 7-Tupel zu einem Codewort von C decodiert. (Oder seien Sie in der Lage dies schnell selbst an der Tafel zu tun.)

Aufgabe 1.4 Beweisen Sie,

a) dass es keinen 1-fehlerkorrigierenden Code $C \subseteq \mathbb{F}_2^4$ mit $|C| = 4$ gibt;

b) dass es keinen binären $(7, 2^3, 5)$-Code gibt.

Aufgabe 1.5 Es sei C ein perfekter Code mit $|C| > 1$ und der Minimaldistanz d. Zeigen Sie, dass $d = 2e + 1$ mit $e \in \mathbb{N}_0$ ist (d.h., dass d ungerade ist).

Aufgabe 1.6 Es sei C ein Code der Länge n und der Minimaldistanz d über einem Alphabet K mit q Elementen. Beweisen Sie:

a) Ist die Projektion $\alpha : C \to K^k$ auf vorgegebene k Koordinaten, etwa

$$(c_1, \dots, c_n) \mapsto (c_{i_1}, \dots, c_{i_k}),$$

eine bijektion, so gilt $k \le n - d + 1$. Diese k Koordinaten trennen die Codewörter, d.h. sie bestimmen das Codewort eindeutig.

b) Genau für MDS-Codes ist die Projektion auf beliebige $k = n - d + 1$ Koordinaten bijektiv. Dies erklärt den Begriff MDS, also Maximum Distance Separable.

Aufgabe 1.7 Konstruieren Sie einen binären $(4, 2^3, 2)$-MDS-Code.
Hinweis: Betrachten Sie die Menge aller binären 4-Tupel mit einer geraden Anzahl von Einsen.

Aufgabe# 1.8 Es sei $F = \{0, 1, \dots, q - 1\}$. Für $a, b, \in F$ sei

$$\|a - b\| = \min\{a - b, b - a\},$$

wobei die Addition auf F modulo q zu lesen ist. Sind $u = (u_1, \dots, u_n)$ und $v = (v_1, \dots, v_n) \in \mathbb{F}^n$, so bezeichnen wir mit

$$d_L(u, v) = \sum_{i=1}^{n} \|u_i - v_i\|$$

die Lee-Distanz von u und v. Zeigen Sie:

a) d_L definiert eine translationsinvariante Metrik auf F^n.

b) Ist $q = 2n + 1$ und

$$C = \{(c_1, \dots, c_n) \in \mathbb{F}^n \mid \sum_{i=1}^{n} ic_i \equiv 0 \bmod 2n + 1\}$$

so liefern die Lee-Kugeln vom Radius 1 um die Codeworte $c \in C$ eine disjunkte Überdeckung von F^n. Insbesondere ist C ein perfekter 1-fehlerkorrigierender Code in der Lee-Metrik.

c) Ist $q = 2e^2 + 2e + 1$ mit $e \in \mathbb{N}$, so ist

$$C = \left\{ \big(c, (2e + 1)c\big) \,\middle|\, c \in F \right\} \subseteq F^2$$

ein perfekter e-fehlerkorrigierender Code in der Lee-Metrik.

Hinweise:

zu b) Ist $(a_1, \dots, a_n) \in \mathbb{F}^n$, so betrachte $\sum_{i=1}^{n} ia_i \equiv k \bmod 2n + 1$ mit $-n \le k \le n$, um das Codewort mit Abstand kleiner oder gleich 1 zu finden.

zu c) Zeigen Sie, dass die Minimaldistanz von C größer oder gleich $2e + 1$ ist und dass eine Kugel vom Radius e genau $2e^2 + 2e + 1$ Vektoren enthält.

Aufgaben mit # sind etwas schwieriger und sind speziell für M.Sc. Studierenden gedacht. Diese Aufgaben werden in den Übungen nicht besprochen, sind schriftlich zu bearbeiten und abzugeben.