# Zusatzaufgaben

**Ein Ausflug in die Codierungstheorie** (20 Zusatzpunkte)**.** Die Problemstellung für fehlerkorrigierende Codes ist die folgende: *Alice* sendet *Bob* eine Nachricht über einen *Kanal*. Wie kann Bob erkennen, ob die empfangene Nachricht die von Alice gesendete ist, und wie kann er mögliche Fehler korrigieren?
Um dieses Problem zu lösen, wird ein Code benutzt. Es bezeichne $E$ die Codierungsabbildung und $D$ die Decodierungsabbildung. Dann ist die Situation wie folgt:

$$\boxed{\text{Originalnachricht}} \xrightarrow{E} \boxed{\text{codierte Nachricht}} \to \boxed{\text{empfangene Nachricht}} \xrightarrow{D} \boxed{\text{decodierte Nachricht}}$$

Unser Alphabet ist $\{0,1\}$, aufgefaßt als Elemente des Körpers mit zwei Elementen $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$. Unser Beispielcode heißt $(7,4)$-Hammingcode. Dieser Code ist ein Blockcode, d. h., er codiert sukzessive eine feste Anzahl von $k$ Buchstaben zu einem Wort der Länge $n$. Im Fall des $(7,4)$-Hammingcodes ist $n = 7$ und $k = 4$, die Informationsrate ist $\frac{k}{n} = \frac{4}{7}$.
Die Codierungsabbildung ist also eine Abbildung $\mathbb{F}_2^4 \to \mathbb{F}_2^7$. Der Hammingcode ist linear, die Codierung eines Wortes $w = (w_1, w_2, w_3, w_4)$ ist gegeben durch Multiplikation mit einer Matrix

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix}.$$

(a) Diese Codierungsvorschrift ist so formuliert, dass die Anzahlen von Einsen im codierten Wort an den Stellen $(1,2,4,7)$, $(2,3,4,6)$ und $(1,3,4,5)$ jeweils gerade ist. Beweisen Sie dies, indem Sie zeigen, dass das Bild der Codierungsabbildung in $\mathbb{F}_2^7$ durch die Gleichungen

$$\begin{cases} x_1 + x_2 \quad + x_4 \quad + x_7 = 0 \\ \quad x_2 + x_3 + x_4 \quad + x_6 \quad = 0 \\ x_1 \quad + x_3 + x_4 + x_5 \quad = 0 \end{cases} \tag{$*$}$$

beschrieben wird.

(b) Für einen allgemeinen linearen Code über dem Alphabet $\{0,1\}$ ist das *Hamminggewicht* $w(y)$ eines codierten Wortes $y = (y_1, \ldots, y_n)$ gleich der Anzahl der Einsen des Wortes. Fasst man also das Alphabet $\{0,1\}$ als Teilmenge der ganzen Zahlen auf, so gilt $w(y) = \sum_{i=1}^n y_i$. Die *Hammingdistanz* zweier Worte ist das Gewicht der Differenz der beiden Worte in $\mathbb{F}_2^n$, d.h. $d(x,y) = w(x-y)$.
Das *minimale Gewicht* eines Codes ist das minimale Hamminggewicht eines Wortes $w \neq 0$ im Bild der Codierungsabbildung, der *minimale Abstand* eines Codes ist die minimale Hammingdistanz zweier Worte im Bild der Codierungsabbildung. Zeigen Sie mit dem Wissen, dass das Bild der Codierungsabbildung eines linearen Codes ein Untervektorraum ist, dass der minimale Abstand eines Codes gleich dem minimalen Gewicht des Codes ist.

(c) Ermitteln Sie den minimalen Abstand des $(7,4)$-Hammingcodes. Wieviele Fehler kann man also bemerken, wieviele kann man noch korrigieren?

(d) Schlüpfen Sie nun in die Rolle von Alice. Codieren Sie sieben verschiedene Worte $w^{(i)} = (w_1^{(i)}, \ldots, w_4^{(i)}) \in \mathbb{F}_2^4$, $i \in \{1, \ldots, 7\}$, Ihrer Wahl mit dem $(7,4)$-Hammingcode zu $y^{(i)} = (y_1^{(i)}, \ldots, y_7^{(i)}) \in \mathbb{F}_2^7$. Simulieren Sie dann einen Übertragungsfehler jeweils an einer anderen Stelle, d. h., betrachten Sie die Worte

$$\bar{y}^{(i)} = (y_1^{(i)}, \ldots, y_{i-1}^{(i)}, y_i^{(i)} + 1, y_{i+1}^{(i)}, \ldots, y_7^{(i)})$$

Multiplizieren Sie schließlich die übertragenen Worte mit der Matrix des obigen Gleichungssystems $(*)$. Das Ergebnis ist jeweils ein Vektor $e^{(i)} = (e_1^{(i)}, e_2^{(i)}, e_3^{(i)}) \in \mathbb{F}_2^3$. Berechnen Sie in $\mathbb{Z}$ jeweils die Werte $e(i) := e_1^{(i)} \cdot 2^2 + e_2^{(i)} \cdot 2^1 + e_3^{(i)} \cdot 2^0$. Finden Sie die Vertauschung der Zeilen der Codierungsmatrix, sodass die mit der entsprechend veränderten Matrix des Gleichungssystems berechneten Werte $e(i)$ jeweils die Stelle des Übertragungsfehlers angeben.

**Der projektive Raum** (20 Zusatzpunkte)**.** Wir wollen in dieser Aufgabe eine Erweiterung der bekannten ebenen Geometrie vornehmen. Das Ziel wird es sein, einen Raum zu konstruieren, in dem sich zwei Geraden *immer* in einem Punkt schneiden, d. h., es gibt dort keine Fallunterscheidungen der Art: zwei Geraden sind parallel/nicht parallel.

(a) Sei $V$ ein endlichdimensionaler Vektorraum über dem Körper $k$. Dann führen wir auf der Menge $V \setminus \{0\}$ die folgende Relation ein: Vektoren $v, w \in V$ heißen äquivalent, geschrieben $v \sim w$, falls es ein Element $\lambda \in k \setminus \{0\}$ gibt, so dass $\lambda v = w$ ist. Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist. Wir bezeichnen mit $\widehat{\mathbb{P}}(V)$ die Menge der Äquivalenzklassen von $V$ bezüglich $\sim$. Dann existiert die kanonische Restklassenprojektion

$$\pi : V \setminus \{0\} \to \widehat{\mathbb{P}}(V)$$

welche einem Vektor $v \in V \setminus \{0\}$ seine Äquivalenzklasse zuordnet.

(b) Sei $V$ genauso wie in (a). Dann sei

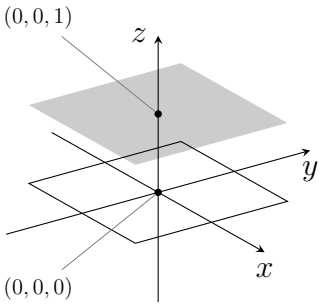
$$\widetilde{\mathbb{P}}(V) := \{U \subset V \mid \dim(U) = 1\}$$

die Menge aller eindimensionalen Untervektorräume von $V$. Zeigen Sie, dass es eine Bijektion zwischen den Mengen $\widetilde{\mathbb{P}}(V)$ und $\widehat{\mathbb{P}}(V)$ gibt, die wir deshalb einheitlich mit $\mathbb{P}(V)$ bezeichnen können und den *projektiven Raum von* $V$ nennen.

(c) Wir wählen nun speziell $V = k^n$ als Vektorraum über $k$. Wir bezeichnen mit $\mathbb{P}_k^n$ den projektiven Raum $\mathbb{P}(k^{n+1})$. Man nennt $\mathbb{P}_k^n$ den *$n$-dimensionalen projektiven Raum über $k$*. Wir führen auf $\mathbb{P}_k^n$ die folgenden Koordinaten ein: Ein Element $p \in \mathbb{P}_k^n$ ist nach (a) eine Äquivalenzklasse von Punkten aus $k^{n+1} \setminus \{0\}$. Sei $x = (x_0, \ldots, x_n)$ ein Vertreter (d. h. ein Element) dieser Klasse. Dann schreibt man den Punkt $p$ als $p = (x_0 : \ldots : x_n)$. Dies sind die *homogenen* Koordinaten von $p$. Diese sind also nur bis auf Multiplikation mit einem von Null verschiedenen Skalar definiert. Entscheiden Sie bei den folgenden Gleichheiten (welche in $\mathbb{P}_k^n$ gelten sollen), ob sie richtig oder falsch sind (mit Begründung):

$$\begin{array}{rclcrcl} (1:2:3) & = & (3:6:9) \in \mathbb{P}^2_{\mathbb{R}}, & \qquad & (1:0) & = & (0:1) \in \mathbb{P}^1_{\mathbb{R}}, \\ (1:2:3) & = & (2:3:4) \in \mathbb{P}^2_{\mathbb{R}}, & & (2:10:4) & = & (0:0:0) \in \mathbb{P}^2_{\mathbb{R}}. \end{array}$$

(d) Nun betrachten wir die injektive lineare Abbildung $j : \mathbb{R}^2 \to \mathbb{R}^3$. $(x, y) \mapsto (x, y, 1)$. Stellt man sich $\mathbb{R}^2$ als Ebene und $\mathbb{R}^3$ als uns umgebenden Raum vor, so ist das Bild dieser Abbildung die rechts grau dargestellte Ebene. Sei jetzt $i : \mathbb{R}^2 \to \mathbb{P}^2_{\mathbb{R}}$ die Komposition von $j$ mit der kanonischen Abbildung $\pi$, also $i = \pi \circ j$. Zeige, dass $i$ injektiv, aber nicht surjektiv ist.




(e) Die folgenden Mengen $U$ und $V$ sind Teilmengen von $\mathbb{R}^3$. Beschreiben Sie (möglichst geometrisch) die Mengen $\pi^{-1}(\pi(U))$ und $\pi^{-1}(\pi(V))$, wobei $\pi$ die kanonische Abbildung $\pi : \mathbb{R}^3 \setminus \{0\} \to \mathbb{P}^2_{\mathbb{R}}$ ist.

(i) $U := \{(a, b, c) \in \mathbb{R}^3 \mid 2a + 3b = 5, c = 1\}$
(ii) $V := \{(a, b, c) \in \mathbb{R}^3 \mid a^2 + b^2 = 9, c = 1\}$

(f) Sei $V \subset W$ ein zweidimensionaler Untervektorraum eines $k$-Vektorraums $W$. Dann nennen wir das Bild $\pi(V)$ unter der kanonischen Projektion $\pi$ eine *projektive Gerade* in $\mathbb{P}(W)$. Zeigen Sie, dass zwei projektive Geraden immer einen Schnittpunkt besitzen.

(g) Sei $L$ eine projektive Gerade in $\mathbb{P}^2_{\mathbb{R}}$. Zeigen Sie, dass das Urbild $i^{-1}(L)$ entweder leer oder eine Gerade in $\mathbb{R}^2$ ist.

(h) Zeigen Sie, dass es für jede Gerade $l \subset \mathbb{R}^2$ genau eine projektive Gerade $l^{\mathbb{P}} \subset \mathbb{P}^2_{\mathbb{R}}$ gibt, so dass $i^{-1}(l^{\mathbb{P}}) = l$ ist. Finden Sie einen Punkt (dieser heißt unendlich ferner Punkt) $p \in \mathbb{P}^2_{\mathbb{R}}$, so dass $p \in l^{\mathbb{P}} \setminus i(l)$ gilt.

(i) Wir betrachten die beiden Paare von Geraden $g_1$, $g_2$ und $h_1$, $h_2$ aus $\mathbb{R}^2$, gegeben durch die folgenden Gleichungen:

$$g_1 = \{(a, b) \mid a + 3b = 5\}, \qquad g_2 = \{(a, b) \mid 4a + 5b = 10\},$$
$$h_1 = \{(a, b) \mid 3a + 5b = 2\}, \qquad h_2 = \{(a, b) \mid 9a + 15b = 4\}.$$

Bestimmen Sie (auch geometrisch) $g_1^{\mathbb{P}} \cap g_2^{\mathbb{P}}$ und $h_1^{\mathbb{P}} \cap h_2^{\mathbb{P}}$ .

Alle Informationen zur Vorlesung (Termine, Aufgabenblätter, etc.) sind unter

`https://www.tu-chemnitz.de/mathematik/algebra/LinAlg1-WS1920/linalg1.php`

zu finden.

**Abgabe bis 07.01.2020 in der Übung.**