Codierungstheorie – SS 2017 **Blatt 2**

Dr. Anton Malevich

Aufgaben zum Thema **Lineare Codes**

Aufgabe 2.1 Ein nicht perfekter binärer Code.

a) Konstruieren Sie einen $[8, 4, 4]$-Code $C = C_1 \propto C_2$ (siehe Aufgabe 2.5a), wobei C_1 der $[4, 3, 2]$-Code ist, der aus aller Wörter des geraden Gewichts besteht, und C_2 der $[4, 1, 4]$-Wiederholungscode ist.

b) Geben Sie eine Kontrollmatrix H des Codes C an und konstruieren Sie die Liste aller Syndrome und Nebenklassenanführer.

c) Realisieren Sie die Syndrom-Decodierung für den Code C (mit dem Rechner oder an der Tafel). Welche Fehler von Gewicht > 1 kann der Code C eindeutig korrigieren, welche "zweideutig", etc.?

Aufgabe 2.2 Wir wollen einen linearen Code konstruieren, der es uns erlaubt, die 26 Buchstaben des lateinischen Alphabets zu übertragen, und der zwei Fehler korrigieren kann. Um die 26 Buchstaben codieren zu können, konstruieren wir einen binären Code C_2 der Dimension 5, einen ternären Code C_3 der Dimension 3 oder einen quinären Code C_5 der Dimension 2 (wir sind zur Not auch bereit, einen Buchstaben zu opfern).

Um zwei Fehler korrigieren zu können, muss die Minimaldistanz des Codes mindestens 5 sein. Die kleinste Länge n, die das erlaubt, ist $n = 13$ für C_2, $n = 8$ für C_3 und $n = 6$ für C_5. (Warum gibt es keinen $[n, 5, 5]_2$-Code mit $n \leq 11$ sowie keinen $[n, 3, 5]_3$-Code mit $n \leq 7$?) Wir nehmen nun an, C_2 ist der $[13, 5, 5]_2$-Code, C_3 — der $[8, 3, 5]_3$-Code und C_5 — der $[6, 2, 5]_5$-Code.

a) Erklären Sie, wie das Codieren und das Decodieren der Nachrichten für C_2, C_3 und C_5 funktioniert.

b) Angenommen, es liegt ein q-när symmetrischer Kanal mit Symbolfehlerwahrscheinlichkeit $p = 0.1$ vor. Wie hoch ist in jedem einzelnen Fall die Wahrscheinlichkeit, dass bei der Übertragung eines zufälligen Codewortes mindestens drei Fehler passieren.

c) Spekulieren Sie, welcher der drei Codes am effizientesten ist. Beachten Sie dabei Faktoren wie Geschwindigkeit der Decodierung, Wahrscheinlichkeit einer falschen Decodierung, Preis der Übertragung, etc.

Aufgabe 2.3 Nicht binäre Codes, die einen Fehler korrigieren.

a) Konstruieren Sie einen $[4, 2, 3]_3$-Code C_1 über $\mathbb{F}_3$ ($\mathrm{Ham}_3(2)$ oder Aufgabe 2.4c) und einen $[5, 3, 3]_5$-Reed-Solomon-Code C_2 über $\mathbb{F}_5$ (Aufgabe 2.4a)

b) Geben Sie Kontrollmatrizen H_1 und H_2 für die Codes C_1 und C_2 an und konstruieren Sie jeweils die Liste aller Syndrome und Nebenklassenanführer.

c) Realisieren Sie die Syndrom-Decodierung für die Codes C_1 und C_2 (mit dem Rechner oder an der Tafel).

Aufgabe 2.4 Es sei $C = C_M$ ein $[n, k, n-k+1]$-Reed-Solomon-Code zur n-elementigen Menge $M = \{a_1, \ldots, a_n\} \subseteq K$. Zeigen Sie:

a) Die Matrix G ist eine Erzeugermatrix für C:

$$G = \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ a_1^2 & \cdots & a_n^2 \\ \vdots & & \vdots \\ a_1^{k-1} & \cdots & a_n^{k-1} \end{pmatrix} \qquad \text{(Vandermonde-Matrix).}$$

b) Es gilt

$$\det \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ a_1^2 & \cdots & a_n^2 \\ \vdots & & \vdots \\ a_1^{n-1} & \cdots & a_n^{n-1} \end{pmatrix} \neq 0 \qquad \text{(Vandermonde-Determinante).}$$

c) Die Matrix

$$G = \begin{pmatrix} 1 & \cdots & 1 & 0 \\ a_1 & \cdots & a_n & 0 \\ a_1^2 & \cdots & a_n^2 & 0 \\ \vdots & & \vdots & \vdots \\ a_1^{k-1} & \cdots & a_n^{k-1} & 1 \end{pmatrix}$$

ist Erzeugermatrix eines $[n+1, k, n-k+2]$-MDS-Codes.

Aufgabe 2.5 Sei $K = \mathbb{F}_2$.

a) (Plotkin-Konstruktion) Für $i = 1, 2$ seien $[n, k_i, d_i]$-Codes C_i über K gegeben. Zeigen Sie, dass

$$C = C_1 \propto C_2 = \{\, (c_1, c_1 + c_2) \,|\, c_i \in C_i \} \leq K^{2n}$$

ein $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$-Code ist. (*Hinweis:* Benutzen Sie Aufgabe 2.6b)

b$^{\#}$) Für $m \in \mathbb{N}$ sei $\mathrm{RM}(0, m)$ der $[2^m, 1, 2^m]$-Wiederholungscode und $\mathrm{RM}(m, m) = K^{2^m}$. Für $1 \leq r \leq m-1$ definieren wir rekursiv

$$\mathrm{RM}(r, m) = \mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1).$$

Beweisen Sie, dass $\mathrm{RM}(r, m)$ ein $[2^m, \sum_{j=0}^{r} \binom{m}{j}, 2^{m-r}]$-Code ist. (Die so konstruierten Codes sind äquivalent zu den Reed-Muller-Codes; daher die gleiche Bezeichnung.)

Aufgabe 2.6 Sei K ein Körper. Für $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in K^n$ bezeichne

$$x \star y = (x_1 y_1, \ldots, x_n y_n).$$

Sei nun $K = \mathbb{F}_2$. Beweisen Sie, dass für alle $x, y \in K^n$ gilt

a) $\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\,\mathrm{wt}(x \star y)$,

b) $\mathrm{wt}(x + y) \geq \mathrm{wt}(x) - \mathrm{wt}(y)$,

c$^{\#}$) $\mathrm{wt}(x + z) + \mathrm{wt}(y + z) + \mathrm{wt}(x + y + z) \geq 2\,\mathrm{wt}(x + y + x \star y) - \mathrm{wt}(z)$.

d$^{\#}$) Ist $K = \mathbb{F}_3$, so gilt $\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - f(x \star y)$, wobei $f(u) = b + 2c$ ist, falls der Vektor $u = (u_1, \ldots, u_n)$ genau a Nullen, b Einsen und c Zweien hat.

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