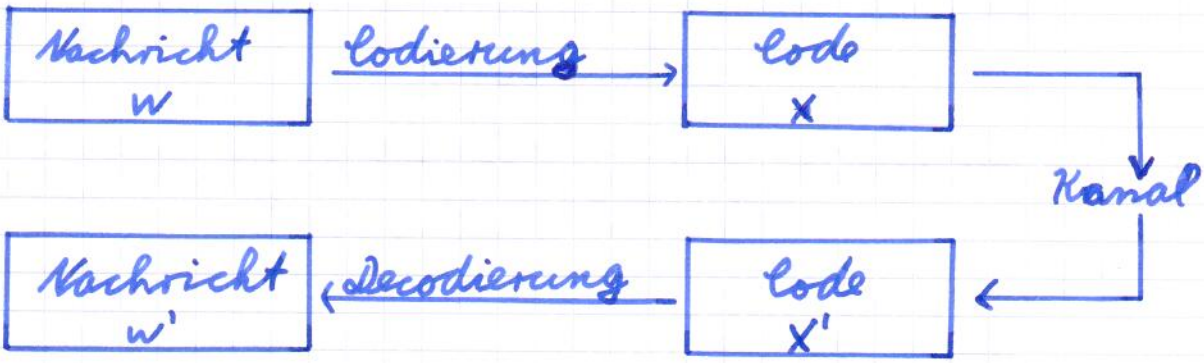
§4 Codierungstheorie

Bemerkung 4.1, Prinzip der Nachrichtenübertragung:
Nachrichten werden vom Sender codiert; die so codierte Mitteilung wird über einen Kanal an den Empfänger geschickt und schließlich von diesem decodiert.

Skizze



Störungen im Kanal können bewirken, dass Nachrichten verfälscht werden. Die Konsequenz in obiger Skizze könnte sein:

$$x \neq x' \text{ und damit auch } w \neq w'.$$

Die Codierungstheorie beschäftigt sich damit, solche Übertragungsfehler zu erkennen und möglichst zu korrigieren. Dabei sollten Codierungen so gestaltet werden, dass sich verschiedene Codewörter „gut genug" - zum Beispiel an mindestens drei Stellen - unterscheiden.

In leichter Abwandlung zur entsprechenden Notation in den Konventionen 3.1 fixieren wir für dieser Kapitel:

Definition 4.2:

Für eine endliche nichtleere Menge A sei

$$A^* := \{\square\} \cup \bigcup_{n=1}^{\infty} A^n .$$

Die Elemente von A^* werden A-Wörter genannt. $\square$ heißt das leere Wort, wir schreiben auch:

$$A^0 = \{\square\} .$$

Die Länge einer Wortes $\tilde{a} \in A^*$ ist gegeben durch

$$l(\tilde{a}) := l, \text{ falls } \tilde{a} \in A^l .$$

Definition 4.3:

Es seien A, B endliche nichtleere Mengen. Ein A-B-Code ist eine injektive Abbildung $c: A \to B^* \setminus \{\square\}$. B heißt das zugrunde liegende Alphabet; die Menge $c(A)$ heißt die Menge der Codewörter von c.

Ist $c: A \to B^* \setminus \{\square\}$ ein A-B-Code, so erweitern wir c auf folgende Weise zu einer Abbildung $c^*: A^* \to B^*$:

$$c^*(\square) := \square ,$$
$$c^*(a_1 \dots a_n) := c(a_1) \dots c(a_n) .$$

Beispiele 4.4:

i) Sei $A \subseteq \mathbb{N}$ endlich und nicht leer sowie

$$B := \{n \in \mathbb{Z} \mid 0 \leq n \leq 9\}.$$

Weiter sei $d: A \to B^* \setminus \{\square\}$ die übliche Dezimaldarstellung, wobei 0 nie Anfangsglied von einem $d(n)$, $n \in A$, ist. Dann ist d ein A-B-Code.

ii) Die Abbildung, die jedem Objekt das zugehörige deutsche Wort über dem „gewöhnlichen" Alphabet zuordnet, ist im Sinne von Definition 4.3 kein Code. Zum Beispiel ist „Tor" ein Wort mehrfacher Bedeutung (sowohl für „Pforte" als auch für „Kurt").

iii) Es sei $A = \{\alpha, \beta, \gamma\}$, $B = \{0, 1\}$ und

$$c(\alpha) := 0, \quad c(\beta) := 1, \quad c(\gamma) := 00.$$

Dann ist c ein A-B-Code, aber die Abbildung c^* ist nicht injektiv. Zum Beispiel ist

$$c^*(\alpha\alpha) = c^*(\gamma) = 00.$$

Definition 4.5:

Ein A-B-Code heißt ein Präfix-Code (oder sofort entzifferbar), falls kein Codewort Präfix - das heißt Anfangsabschnitt - eines anderen ist.

Satz 4.6:

Für jeden Präfix-Code $c: A \to B^* \setminus \{\square\}$ ist neben c auch c^* injektiv.

Beweis:

Wir zeigen durch Induktion nach m:

Zu $b_1 \dots b_m \in c^*(A^*)$ gibt es genau ein $\tilde{a} \in A^*$ mit $c^*(\tilde{a}) = b_1 \dots b_m$.

Für $m = 0$ ist nichts zu zeigen.

Sei nun $m \geq 1$. Weil c ein Präfix-Code ist, gibt es genau ein i mit $1 \leq i \leq m$ und $b_1 \dots b_i \in c(A)$.

Sei $a_1 \in A$ das Element mit $b_1 \dots b_i = c(a_1)$.

Dann ist $b_{i+1} \dots b_m \in c^*(A^*)$; nach Induktionsannahme gibt es also genau ein $\tilde{a}' \in A^*$ mit $b_{i+1} \dots b_m = c^*(\tilde{a}')$. Dann ist $\tilde{a} := a_1 \tilde{a}'$ das eindeutig bestimmte Element in A^* mit $c^*(\tilde{a}) = b_1 \dots b_m$. □

Beispiele:

i) Sind alle Codewörter von c gleich lang, so ist c ein Präfix-Code.

ii) Es sei $A = \{\alpha, \beta, \gamma\}$, $B = \{0, 1\}$ und

$$c(\alpha) := 00, \quad c(\beta) := 01, \quad c(\gamma) := 1.$$

Dann ist c ein Präfix-Code.

Beispielsweise ist

$$00|01|01|00|1|01|00 = c^*(\alpha\beta\beta\alpha\gamma\beta\alpha).$$

Konvention 4.7:

Es sei $c: A \to B^* \setminus \{\square\}$ ein A-B-Code sowie

$$n := \max\{l(c(a)) \mid a \in A\}.$$

Für $1 \leq m \leq n$ und $w \in B^m$ setzen wir

$$F(w) = F_n(w) := \{ww' \mid w' \in B^{n-m}\}.$$

$F_n(w)$ besteht also aus denjenigen B-Wörtern der Längen, die w als Präfix haben.

Lemma 4.8:

Unter der gerade getroffenen Konvention sind folgende Aussagen äquivalent:

(i) $c: A \to B^* \setminus \{\square\}$ ist ein Präfix-Code.

(iii) Für je zwei Elemente $a, a' \in A$ mit $a \neq a'$ sind die Mengen $F(c(a))$ und $F(c(a'))$ disjunkt.

Beweis:

(i) $\Rightarrow$ (iii):

Wir nehmen an, es gebe ein Element $b_1 \dots b_n \in F(c(a)) \cap F(c(a'))$.

Dann gibt es Indizes i, j mit

$$b_1 \dots b_i = c(a), \quad b_1 \dots b_j = c(a').$$

Aus der Injektivität von c auf A und der Annahme $a \neq a'$ folgt: $i \neq j$.

Das widerspricht aber der Voraussetzung, dass c ein Präfix-Code ist.

(iii) $\Rightarrow$ (i):

Seien $a, a' \in A$ mit $a \neq a'$. Aus (iii) folgt dann sofort: $c(a)$ ist kein Präfix von $c(a')$ - und umgekehrt. $\square$

Satz 4.9:

Es seien A, B endliche nichtleere Mengen, es sei $|A| = z$, $|B| = b$, und für jedes $a \in A$ sei $n(a) \in \mathbb{N}$ fixiert. Dann sind die folgenden Aussagen äquivalent:

(i) Es gibt einen Präfix-Code $c: A \to B^* \setminus \{\square\}$ mit
$$l(c(a)) = n(a) \text{ für alle } a \in A.$$

(ii) Es gilt die folgende Kraft'sche Ungleichung:
$$\sum_{a \in A} \frac{1}{b^{n(a)}} \leq 1.$$

Beweis:

(i) $\Rightarrow$ (ii):

Ist c wie in (i), so folgt aus Lemma 4.8, (i) $\Rightarrow$ (ii), dass die Mengen $F(c(a))$ für $a \in A$ paarweise disjunkt sind. Daher folgt:
$$b^n = |B|^n \geq \sum_{a \in A} |F(c(a))| = \sum_{a \in A} b^{n - n(a)}.$$
Division durch b^n liefert die Kraft'sche Ungleichung.

(ii) $\Rightarrow$ (i):

Wir konstruieren den gesuchten Präfix-Code wie folgt:

Wir schreiben $A = \{a_1, \ldots, a_z\}$ und nehmen ohne Einschränkung an:
$$n(a_1) \leq n(a_2) \leq \ldots \leq n(a_z).$$

Sodann wählen wir $c(a_1) \in B^{n(a_1)}$ beliebig.
Ist $1 \leq u < z$, und sind $c(a_1) \in B^{n(a_1)}, \ldots, c(a_u) \in B^{n(a_u)}$ bereits gewählt, so folgt wegen $u < z$ aus der Kraft'schen Ungleichung:

$$\sum_{j=1}^{u} |F(c(a_j))| = \sum_{j=1}^{u} b^{n-n(a_j)} < b^n \cdot \sum_{j=1}^{z} \frac{1}{b^{n(a_j)}} \leq b^n.$$

Es gibt also ein Element $b_1 \ldots b_n \in B^n$, das in keiner der Mengen $F(c(a_j))$ für $1 \leq j \leq u$ liegt.
Setzen wir nun $i := n(a_{u+1})$ und $c(a_{u+1}) = b_1 \ldots b_i$, so folgt zunächst: $\ell(c(a_{u+1})) = i = n(a_{u+1})$.
Ferner gilt laut Konstruktion:

$n(a_j) \leq i$, $b_1 \ldots b_n \notin F(c(a_j))$ für alle j mit $1 \leq j \leq u$.

Das bedeutet, dass kein $c(a_j)$, $1 \leq j \leq u$, Präfix von $c(a_{u+1}) = b_1 \ldots b_i$ ist - und umgekehrt.
Insgesamt folgt somit durch Induktion:
c ist ein Präfix-Code. □

Definition 4.10:

Ein A-B-Code $c: A \to B^* \setminus \{\square\}$ heißt <u>eindeutig entzifferbar</u>, wenn die zugehörige Abbildung $c^*: A^* \to B^*$ injektiv ist.

Bemerkung 4.11:

Nach Satz 4.6 ist jeder Präfix-Code eindeutig entzifferbar. Ebenso ist jeder A-B-Code, in dem kein Codewort <u>Endabschnitt</u> eines anderen ist, eindeutig entzifferbar.

Definition 4.12:

Es sei E eine beliebige nichtleere Menge, und $d: E \times E \to \mathbb{R}_0^+$ sei eine Abbildung. Dann heißt das Paar $M := (E, d)$ ein **metrischer Raum mit der Metrik d**, falls folgende Axiome erfüllt sind:

(M1) $\quad d(x,y) = 0 \Leftrightarrow x = y$.

(M2) $\quad \forall x, y \in E: \quad d(x,y) = d(y,x)$ (Symmetrie).

(M3) $\quad \forall x, y, z \in E: \quad d(x,z) \leq d(x,y) + d(y,z)$.

Die Ungleichung in (M3) heißt **Dreiecksungleichung**.

Definition 4.13:

Sei B eine endliche nichtleere Menge und $n \in \mathbb{N}$. Der **Hamming-Abstand in B^n** ist die Abbildung $h: B^n \times B^n \to \{0, 1, \ldots, n\}$, definiert durch

$$h((x_1, \ldots, x_n), (y_1, \ldots, y_n)) := \#\{i \in \{1, \ldots, n\} : x_i \neq y_i\}.$$

Bemerkung 4.14:

Der Hamming-Abstand h ist eine Metrik auf der Grundmenge B^n.

Definition 4.15:

Sei B endlich und nicht leer, und sei $n \in \mathbb{N}$.

i) Teilmengen C von B^n werden (auch) als **Codes** (genauer: **Block-Codes**) bezeichnet.

ii) Für $x \in B^n$ und $0 \leq e \leq n$ ist die **Hamming-Kugel um x mit Radius e** definiert durch

$$K_e(x) := \{z \in B^n \mid h(x,z) \leq e\}.$$

iii) Sind $x, y \in B^n$, und ist $e := h(x,y)$, so gehe y aus x durch e Abänderungen - oder e Fehler - hervor. Für $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ heißt die Menge $E := \{ j \mid x_j \neq y_j \}$ das Fehler-Muster bei dieser Abänderung.

iv) Ein Block-Code $C \subseteq B^n$ korrigiere bis zu e Fehler, falls für alle $c, d \in C$ mit $c \neq d$ gilt:

$$K_e(c) \cap K_e(d) = \emptyset.$$

v) $C \subseteq B^n$ entdecke bis zu e Fehler, falls gilt:

$$c, d \in C,\ c \neq d \Rightarrow h(c,d) \geq 2 \cdot e.$$

Interpretation:

Für $0 \leq e \leq n$ und $x \in B^n$ besteht $K_e(x)$ aus denjenigen $z \in B^n$, die aus x durch höchstens e Fehler hervorgehen. Korrigiert $C \subseteq B^n$ bis zu e Fehler, so gibt es zu jedem $z \in B^n$ also höchstens ein $x \in C$ mit $h(x,z) \leq e$. Das bedeutet:

Wenn nur Wörter aus C gesendet werden können und dabei maximal e Fehler unterstellt werden, so kann das gesendete Wort $x \in C$ aus dem empfangenen Wort $z \in B^n$ rekonstruiert werden.

C korrigiert genau dann bis zu e Fehler, falls gilt:

$$c, d \in C,\ c \neq d \Rightarrow h(c,d) \geq 2 \cdot e + 1.$$

Ist dagegen $h(c,d) = 2 \cdot e = 2 \cdot h(c,z) = 2 \cdot h(z,d)$ für ein $z \in K_e(c) \cap K_e(d)$, so geht z aus c und aus d jeweils durch e Fehler hervor.

Beispiele 4.16:

Sei jeweils $B = \{0,1\}$ und $k \geq 1$.

i) Sei $n := 3k$ und

$$C := \{(x_1, \ldots, x_n) \in B^n \mid x_i = x_{i+k} = x_{i+2k} \text{ für } 1 \leq i \leq k\}.$$

C heißt der 2-fache Wiederholungscode.

C korrigiert bis zu einem Fehler.

ii) Sei $n := k+1$ und

$$C := \{(x_1, \ldots, x_n) \in B^n \mid x_n \equiv x_1 + \ldots + x_{n-1} \bmod 2\}.$$

C heißt Paritätscode. C entdeckt bis zu einem Fehler, kann ihn aber nicht korrigieren.

iii) Sei $n = 4$, $c := (0,0,0,0)$, $d := (1,1,1,1)$, $C := \{c, d\}$.

Dann entdeckt C bis zu 2 Fehler, kann sie aber nicht korrigieren:

$z := (0,0,1,1)$ kann sowohl aus c als auch aus d durch 2 Fehler hervorgegangen sein.

Satz 4.17 (Die Hamming-Schranke):

Sei $|B| = b$, $n \in \mathbb{N}$, und $C \subseteq B^n$ sei ein bis zu ℓ Fehler korrigierender Code. Dann gilt:

$$|C| \leq b^n \cdot \left(\sum_{k=0}^{\ell} \binom{n}{k} \cdot (b-1)^k \right)^{-1}.$$

Beweis:

Nach Voraussetzung ist $K_\ell(c) \cap K_\ell(d) = \emptyset$ für alle $c, d \in C$ mit $c \neq d$. Für $c \in C$ und $0 \leq k \leq \ell$ gibt es genau $\binom{n}{k} \cdot (b-1)^k$ Wörter in B^n mit Abstand k zu c; also folgt:

$$b^n = |B|^n \geq \Big| \dot{\bigcup_{c \in C}} K_\ell(c) \Big| = \sum_{c \in C} |K_\ell(c)|$$

$$= |C| \cdot \sum_{k=0}^{\ell} \binom{n}{k} \cdot (b-1)^k .$$

Damit folgt auch die Behauptung. □

Bemerkung 4.18:

Für $n \in \mathbb{N}$ mit $n \geq 2$ sind folgende Aussagen äquivalent:

(i) Es gibt einen Körper mit genau n Elementen.

(ii) n ist eine Primzahlpotenz.

Ist $n = p$ selbst eine Primzahl, so ist $\mathbb{Z}/p\cdot\mathbb{Z}$ ein Körper; siehe Aufgabe 23.

Ist $n = p^k$ für $p \in \mathbb{P}$ und $k \geq 2$, so ist $\mathbb{Z}/n\cdot\mathbb{Z}$ aber kein Körper; der Körper mit p^k Elementen hat eine andere Struktur!

Beispiel 4.19:

Ist $K = \{0, 1, a, b\}$ der Körper mit $4 = 2^2$ Elementen - mit neutralem Element 0 bzw. 1 bezüglich der Addition bzw. der Multiplikation, so ergeben sich die folgende Additions- und Multiplikationstabelle:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Bemerkung 4.20 - siehe auch §5, WS 2015/16

Es sei K ein endlicher Körper und $n \in \mathbb{N}$.

i) Für $x = (x_1, \dots, x_n) \in K^n$ und $y = (y_1, \dots, y_n) \in K^n$ setzen wir

$$x + y := (x_1 + y_1, \dots, x_n + y_n).$$

Für $\lambda \in K$ sei ferner

$$\lambda \cdot (x_1, \dots, x_n) := (\lambda \cdot x_1, \dots, \lambda \cdot x_n).$$

ii) Eine Teilmenge V von K^n heißt ein <u>Vektorraum</u>, falls gilt:

(V1) Es ist $0 \in V$.

(V2) Für $x, y \in V$ ist auch $x + y \in V$.

(V3) Für $x \in V$ und $\lambda \in \mathbb{R}$ ist auch $\lambda \cdot x \in V$.

iii) Ähnlich wie für den Grundkörper $\mathbb{R}$ läßt sich zeigen:
Jeder Vektorraum $V \subseteq K^n$ hat eine <u>Basis</u> B mit $|B| \leq n$; das ist eine Teilmenge $B = \{v_1, \dots, v_k\}$ von V mit folgender Eigenschaft:
Zu jedem $v \in V$ existieren eindeutig bestimmte Elemente $\lambda_1, \dots, \lambda_k \in K$ mit

$$v = \sum_{i=1}^{k} \lambda_i \cdot v_i .$$

iv) Je zwei verschiedene Basen B_1, B_2 eines Vektorraums $V \subseteq K^n$ haben gleich viele Elemente.
Ihre gemeinsame Kardinalität heißt die <u>Dimension</u> von V und wird mit $\dim V$ bzw. $\dim_K V$ bezeichnet.

Definition 4.21:

Sei K ein endlicher Körper, und sei $n \in \mathbb{N}$.

i) Jeder Vektorraum $C \subseteq K^n$ wird auch ein *Linearer Code* über K genannt.

Ist $k := \dim_K C$, so heißt C auch ein *(n,k)-Code*.

ii) Die *Distanz* $d(C)$ eines linearen Codes $C \neq \{0\}$ ist gegeben durch

$$d(C) := \min_{\substack{a,b \in C \\ a \neq b}} h(a,b) = \min_{\substack{a,b \in C \\ a \neq b}} h(a-b,0) = \min_{c \in C \setminus \{0\}} w(c),$$

wobei $w(c) := h(c,0)$ ist.

Beispiel:

Es sei $K := \mathbb{Z}/2\mathbb{Z}$, $n \in \mathbb{N}$ beliebig sowie

$$C := \{(0,\dots,0),(1,\dots,1)\} \subseteq K^n.$$

Dann ist C ein $(n,1)$-Code mit $d(C) = n$.

Konventionen 4.22:

Für einen Vektorraum $C \subseteq K^n$ ist der zu C gehörige orthogonale Vektorraum $C^\perp$ gegeben durch

$$C^\perp := \{(u_1,\dots,u_n) \in K^n \mid \sum_{i=1}^{n} u_i \cdot v_i = 0 \text{ für alle } (v_1,\dots,v_n) \in C\}.$$

Dann ist $\dim C + \dim C^\perp = n$.

Sei $k := \dim C$ und $m := n-k$.

Ist M eine Matrix über K mit m Zeilen und n Spalten, deren Zeilen eine Basis von $C^\perp$ bilden, so ist

$$C = \{c \in K^n \mid M \cdot c^T = 0\}.$$

Solch eine Matrix M wird auch *Kontrollmatrix für C* genannt.

Beispiele 4.23:

Wir betrachten $K := \mathbb{Z}/2\mathbb{Z}$.

i) Für

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

erhalten wir den 2-fachen Wiederholungscode

$$C = \{(c_1, c_2, c_3) \in K^3 \mid c_1 = c_2 = c_3\} = \{(0,0,0), (1,1,1)\}.$$

ii) Für

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

erhalten wir den Fano-Code

$$C = \{c \in K^7 \mid M \cdot c^T = 0\}.$$

Satz 4.24:

Sei K ein endlicher Körper und $C \subseteq K^n$ ein (n,k)-Code mit Kontrollmatrix M. Für $d \leq n$ sind dann folgende Aussagen äquivalent:

(i) $d(C) \geq d$.

(ii) Je $d-1$ Spalten von M sind linear unabhängig.

Insbesondere korrigiert C (für $e \leq \frac{n-1}{2}$ genau dann bis zu e Fehler, wenn je $2e$ Spalten von M linear unabhängig sind.

Beweis:

Ist die Äquivalenz von (i) und (ii) bewiesen, so folgt auch die letzte Behauptung mit $d := 2e+1$.

Wir schreiben $M = (v_1 \dots v_n)$ mit Spaltenvektoren $v_1, \dots, v_n \in K^m$.

(i) ⇒ (ii):

Es sei $1 \le i_1 < i_2 < \dots < i_{d-1} \le n$, und es seien $\lambda_{i_1}, \dots, \lambda_{i_{d-1}} \in K$ mit

$$\sum_{j=1}^{d-1} \lambda_{i_j} \cdot v_{i_j} = 0.$$

Definiere $c = (c_1, \dots, c_n) \in C$ durch

$$c_\nu := \begin{cases} \lambda_{i_j}, & \text{falls } \nu = i_j \text{ für passendes } j \\ 0 & \text{sonst.} \end{cases}$$

Dann ist $w(c) \le d-1$, also $c = 0$ nach (i).
Somit ist $\lambda_{i_1} = \dots = \lambda_{i_{d-1}} = 0$; also gilt (ii).

(ii) ⇒ (i):

Es gelte $d(C) < d$, sei also $c = (c_1, \dots, c_n) \in C$ mit $0 < w(c) < d$.
Ist dann $I := \{ i \mid 1 \le i \le n, c_i \neq 0 \}$, so sind die Spalten v_i, $i \in I$, wegen der Beziehung $M \cdot c^T = 0$ linear abhängig.

□

<u>Definition 4.25:</u>

Es sei B eine nichtleere und endliche Menge, und es seien $n, e \in \mathbb{N}$. Ein Code $C \subseteq B^n$ heißt <u>e-perfekt</u>, wenn gilt:

$$B^n = \dot{\bigcup_{c \in C}} K_e(c).$$

Das bedeutet: Zu jedem $x \in B^n$ gibt es <u>genau ein</u> $c \in C$ mit $x \in K_e(c)$.

Beispiel:

Es sei $B = \{0,1\}$, $n = 2e+1 \geq 3$ und

$$C = \{(0,\dots,0),(1,\dots,1)\} \subseteq K^n.$$

Satz 4.26 (siehe auch Satz 4.17):

Es sei B endlich und nicht leer, und es seien $n, e \in \mathbb{N}$. Für einen Code $C \subseteq B^n$ sind dann äquivalent:

(i) C ist e-perfekt.

(ii) C korrigiert bis zu e Fehler, und es gilt:

$$|C| = |B|^n \cdot \left(\sum_{k=0}^{e} \binom{n}{k} \cdot (|B|-1)^k \right)^{-1}.$$

Beweis: Siehe Übung.

Definition 4.27:

Sei K ein Körper mit q Elementen, sei $m \in \mathbb{N}$ und

$$n := \frac{q^m - 1}{q-1} = q^{m-1} + q^{m-2} + \dots + q + 1.$$

Ein Hamming-Code ist ein $(n, n-m)$-Code, der bis zu einem Fehler korrigiert.

Satz 4.28:

Jeder Hamming-Code ist 1-perfekt.

Beweis:

Es seien K, q, m, n wie in Definition 4.27. Ist nun $C \subseteq K^n$ ein Hamming-Code mit $\dim C = n-m$, so folgt:

$$|C| \cdot \sum_{k=0}^{1} \binom{n}{k} \cdot (q-1)^k = q^{n-m} \cdot (1 + n \cdot (q-1))$$
$$= q^{n-m} \cdot q^m = q^n = |K|^n.$$

Damit liefert Satz 4.26, (iii) $\Rightarrow$ (i), die Behauptung. □

Bemerkung 4.29:

Es sei wieder K ein Körper mit q Elementen, sei nun $m \geq 2$ sowie

$$n := \frac{q^m - 1}{q - 1} .$$

Auf $K^m \setminus \{0\}$ betrachten wir folgende Äquivalenzrelation R:

Wir schreiben $v \, R \, w$, falls ein $\lambda \in K \setminus \{0\}$ existiert mit $\lambda \cdot v = w$.

Jede Äquivalenzklasse besitzt $|K \setminus \{0\}| = q - 1$ Elemente; es gibt also genau

$$\frac{|K^m \setminus \{0\}|}{q-1} = \frac{q^m - 1}{q-1} = n$$

Äquivalenzklassen.

Zwei Vektoren $v, w \in K^m \setminus \{0\}$ sind nun genau dann linear unabhängig, wenn sie nicht äquivalent sind. Es gibt also eine Matrix M über K mit n Spalten der Länge m, die paarweise linear unabhängig sind.

Für den $(n, n-m)$-Code

$$C := \{ c \in K^n \mid M \cdot c^T = 0 \}$$

mit Kontrollmatrix M folgt daher aus Satz 4.24:

C ist ein Hamming-Code.

Beispiele 4.30:

i) Für $K = \mathbb{Z}/2\cdot\mathbb{Z}$ ist sowohl der 2-fache Wiederholungscode als auch der Fano-Code - aus den Beispielen 4.23 - ein Hamming-Code.

ii) Sei $K = \mathbb{Z}/3\cdot\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

die Kontrollmatrix M sei - für $m=2$ und $n=4$ - gegeben durch:

$$M = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{1} & \overline{1} & \overline{2} \end{pmatrix}.$$

Der zu M gehörige Hamming-Code ist dann

$$C = \{c \in K^4 \mid M \cdot c^T = 0\}$$

$$= \{(\overline{0},\overline{0},\overline{0},\overline{0}), (\overline{1},\overline{0},\overline{1},\overline{1}), (\overline{2},\overline{0},\overline{2},\overline{2}), (\overline{0},\overline{1},\overline{1},\overline{2}), (\overline{0},\overline{2},\overline{2},\overline{1}),$$
$$(\overline{1},\overline{1},\overline{2},\overline{0}), (\overline{2},\overline{2},\overline{1},\overline{0}), (\overline{1},\overline{2},\overline{0},\overline{2}), (\overline{2},\overline{1},\overline{0},\overline{1})\}.$$

Dies ist ein $(4,2)$-Code.

Definition 4.31:

Es sei K ein endlicher Körper und $C \subseteq K^n$ ein (n,k)-Code über K. Ist $\{g_1, \dots, g_k\}$ eine Basis des Zeilenvektorraumes C, so heißt die $k \times n$-Matrix

$$G := \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$$

eine <u>Generatormatrix</u> für C.

Hat G die Form

$$G = (I_k \; G_1)$$

mit der $k \times k$-Einheitsmatrix I_k und einer Matrix $G_1 \in \mathrm{Mat}_{k\times(n-k)}(K)$, so heißt die Generatormatrix G

systematisch.

Bemerkungen 4.32:

i) Mit obigen Bezeichnungen gilt:

$$C = \{ \sum_{i=1}^{k} w_i \cdot g_i \mid w_i \in K \}.$$

Identifizieren wir die Nachrichten aus C mit den $|K|^k$ Vektoren aus K^k, so codieren wir mittels des Isomorphismus $\Phi: K^k \to C$, gegeben durch

$$\Phi(w_1, \ldots, w_k) := \sum_{i=1}^{k} w_i \cdot g_i .$$

Die Decodierung erfolgt durch Lösung eines Linearen Gleichungssystems.
Liegt eine systematische Generatormatrix zugrunde, so besteht die Nachricht gerade aus den ersten k Symbolen des Codewortes.

ii) Die Generatormatrizen G für einen Code C sind genau die Kontrollmatrizen für $C^{\perp}$.
Ist $G = (I_k \; G_1)$ eine systematische Generator-matrix für C, so ist $H := (-G_1^T \; I_{n-k})$ eine Kontrollmatrix für C.

Definition 4.33:

Die Informationsrate r eines (n, k)-Codes ist gegeben durch

$$r := \frac{k}{n} .$$

Beispiel 4.34:

Sei $n \geq 2$, und sei C der $(n, n-1)$-Code über $\mathbb{Z}/2\cdot\mathbb{Z}$ mit der systematischen Generatormatrix

$$G := \begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{pmatrix} \Big\} \; n-1 \text{ Zeilen}$$

Dann ist

$$C = \{(w_1, \ldots, w_n) \in (\mathbb{Z}/2\cdot\mathbb{Z})^n \mid w_n = w_1 + \ldots + w_{n-1}\}$$

der Paritätscode.

$M := (1 \ldots 1)$ ist die Kontrollmatrix für C, und die Informationsrate ist $r = \frac{n-1}{n}$.

Der zugehörige Duale Code $C^\perp = \{(0, \ldots, 0), (1, \ldots, 1)\}$ hat M als Generatormatrix, G als Kontrollmatrix und Informationsrate $\frac{1}{n}$.

Beispiel 4.35, Die Reed-Solomon-Codes:

Sei $K = \{0, 1, a_1, \ldots, a_{q-2}\}$ „der" Körper mit q Elementen - für eine vorgegebene Primzahlpotenz q.

Für festes $d \in \mathbb{N}$ mit $2 \leq d \leq q+1$ sei

$$M := \begin{pmatrix} 0 & 1 & 1 & 1 & \ldots & 1 \\ \vdots & 0 & 1 & a_1 & \ldots & a_{q-2} \\ & \vdots & \vdots & a_1^2 & \ldots & a_{q-2}^2 \\ & & & \cdot & & \cdot \\ & & & \cdot & & \cdot \\ 0 & & & \cdot & & \cdot \\ 1 & 0 & 1 & a_1^{d-2} & \ldots & a_{q-2}^{d-2} \end{pmatrix}.$$

Die $(d-1)\times(q+1)$-Matrix M hat den Rang $d-1$; genauer sind je $d-1$ Spalten von M linear unabhängig.

Der $(q+1, q+2-d)$-Code C mit Kontrollmatrix M heißt <u>Reed-Solomon-Code</u>.

Weil trivialerweise je d Spalten von M linear abhängig sind, liefert Satz 4.24:

$$d(C) = d.$$

Die Informationsrate $r = r(q,d)$ ist gegeben durch

$$r = \frac{q+2-d}{q+1}.$$

Für festes d ist also $\lim_{q\to\infty} r(q,d) = 1$.