Kodierungstheorie

Frühjahrssemester 2010

Mannheim

Claus Hertling

18. Mai 2010

Inhaltsverzeichnis

1 Einführung

Kodierungstheorie = die Theorie fehlerkorrigierender Codes.

Anwendungen: bei Nachrichtenübertragungen aller Art, insbesondere bei der Übertragung von Satellitenbildern, beim Telefonieren, im CD-Spieler.

Forschung: an den Universitäten, bei den großen amerikanischen Telefongesellschaften, bei der NASA, bei Philips (CD-Spielern).

Einordnung: Grenzgebiet zwischen Algebra, Informatik und Stochastik; vor allem Algebra. Bezüge zu Zahlentheorie, Gruppentheorie, algebraischer Geometrie, Kryptographie und Informationstheorie.

Die Situation: Ein Sender hat Informationen, gegeben in Form von Wörtern über einem endlichen Alphabet. Er möchte sie einem Empfänger über einen Kanal senden. Im Kanal können aber durch Rauschen einzelne Buchstaben des gesendeten Textes verändert werden. Der Empfänger möchte aus dem empfangenen Wort das gesendete Wort rekonstruieren. Das klappt, falls nur wenig Fehler aufgetreten sind und falls nur ein erlaubtes Wort dem empfangenen Wort hinreichend ähnlich sieht.

Ein Code: ordnet jedem der Wörter des Senders ein neues Wort (i.a. länger) zu, so daß der Abstand zwischen je zwei möglichen neuen Wörtern hinreichend groß ist, um sie auch bei mehreren Fehlern unterscheiden zu können.

Das endliche Alphabet: in dieser Vorlesung ist es immer ein endlicher Körper. "Erinnerung" (Diskussion und Beweis in Kapitel 6):

Es gibt einen endlichen Körper mit $q \in \mathbb{N}$ Elementen

$$\iff q = p^e \text{ mit } p \text{ Primzahl und } e \in \mathbb{N}.$$

Zu solchem q gibt es genau einen Körper. Er heißt $\mathbb{F}_q$.

Beispiele: Für $e = 1$ und $q = p$ Primzahl ist $\mathbb{F}_q = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \{0, 1, \cdots, p-1\}$. Damit kann man gut rechnen. Der Körper $\mathbb{F}_2 = \{0, 1\}$ ist der kleinste und - in der Kodierungstheorie - der wichtigste. Es gibt keinen Körper mit einem Element, da jeder Körper ein 0-Element und ein 1-Element haben muss, die voneinander verschieden sein müssen.

Beispiel 1.1 1969 hat eine Mariner-Sonde schwarz-weiße Bilder vom Mars zur Erde gesandt. Über ein Bild wurde ein feines Raster gelegt, jedem Gitterpunkt wurde eine Zahl zwischen 0 und 63 zugeordnet, die die Helligkeit im Punkt beschreibt. Mit einer Bijektion $\{0, 1, \cdots, 63\} \to \mathbb{F}_2^6$ bekam man Wörter der Länge 6 über dem Alphabet $\mathbb{F}_2$.
Die Kodierung dieser Wörter bestand aus einer sorgfältig gewählten injektiven Abbildung f: $\mathbb{F}_2^6 \to \mathbb{F}_2^{32}$, d.h. man ordnet jedem Wort der Länge 6 ein Wort der Länge 32 über $\mathbb{F}_2$ zu.
Diese Wörter der Länge 32 wurden vom Mars zur Erde gesandt.
Die Menge $C = \text{Bild}(f) \subset \mathbb{F}_2^{32}$ hat die Eigenschaft: je zwei Wörter in C unterscheiden sich in mindestens 16 der 32 Stellen.
Daher konnte der Empfänger das gesendete Wort rekonstruieren, wenn höchstens 7 Fehler bei der Übertragung aufgetreten waren. Diese Rekonstruktion und danach f^{-1} waren die Dekodierung des empfangenen Wortes.
C ist eine Nebenklasse des Reed-Muller-Codes R(1,5) (Definition und Diskussion in Kapitel 5.

Lemma/Definition 1.2 *Sei $\mathbb{F}_q$ ein endlicher Körper, $n \in \mathbb{N} = \{1, 2, 3 \cdots\}$.*

(a) (Definition) Das Gewicht $w(x)$ eines Wortes $x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$ ist

$$w(x) = \#(i \mid x_i \neq 0).$$

Also $w : \mathbb{F}_q^n \to \{0, 1, ..., n\}$.

(b) (Definition) Der Hamming-Abstand $d_H(x, y)$ zwischen zwei Worten x und $y \in \mathbb{F}_q^n$ ist

$$d_H(x, y) = w(x - y).$$

(c) (Lemma, Beweis leicht) Die Abb. $d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{Z}_{\geq 0}$ ist eine Metrik, d.h.

1. $d_H(x, y) = d_H(y, x)$,
2. $d_H(x, y) \geq 0 \quad \text{und} \quad d_H(x, y) = 0 \Longleftrightarrow x = y$,
3. $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$.

Definition 1.3 Sei $\mathbb{F}_q$ ein endlicher Körper und $n \in \mathbb{N}$.

(a) Eine Teilmenge $C \subset \mathbb{F}_q^n$ mit $|C| \geq 2$ heißt Code oder Block-Code. Die Elemente von C sind die Codewörter. [Sie haben alle die gleiche Länge, daher "Block-Code"].

(b) Der minimale Hamming-Abstand eines Codes $C \subset \mathbb{F}_q^n$ ist

$$d(C) = \min\,(d_H(x, y) \mid x, y \in C, x \neq y).$$

(c) Falls für ein $t \in \mathbb{N}$ $d(C) \geq 2t+1$ ist, so ist der Code C t-fehlerkorrigierend. Hier wird angenommen, dass der Empfänger nach der Methode "maximum likelihood" dekodiert, d.h. zu einem empfangenen Wort $y \in \mathbb{F}_q^n$ wählt der Empfänger ein $x \in C$, so dass $d_H(x,y)$ minimal ist.

Bei $d_H(x,y) \leq t$ und $d(C) \geq 2t+1$ ist x eindeutig. Unter der (optimistischen) Annahme, dass $\leq t$ Fehler aufgetreten sind, kann der Empfänger dann schließen, dass der Sender das Wort x gesandt hat.

(d) Ist $M = |C|$ die Anzahl der Elemente von $C \subset \mathbb{F}_q^n$ und $d = d(C)$, so nennt man C einen (n, M, d)-Code oder einen (n, M)-Code.

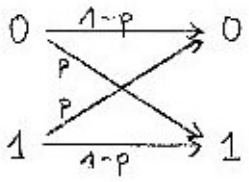
(e) Die Informationsrate eines (n, M)-Codes $C \subset \mathbb{F}_q^n$ ist die Zahl $R = \frac{log_q\ M}{n}$ [also $0 < R < 1$]. Falls $C \cong \mathbb{F}_q^k$ ist, ist $M = q^k$ und $R = \frac{k}{n}$.

(f) Ein Code heißt binär, falls $q = 2$ ist.

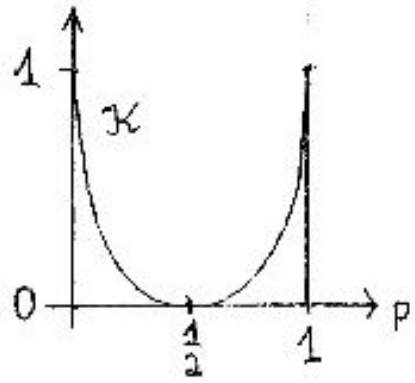
Beispiel 1.4 Der Code der Mariner-Sonde ist ein binärer $(32, 2^6 = 64, 16)$-Code mit $R = \frac{6}{32}$.

Man kann (natürlich) Codes konstruieren, bei denen die Wahrscheinlichkeit, ein Wort nicht rekonstruieren zu können, beliebig klein wird, wenn man beliebig kleine Informationsrate in Kauf nimmt. Aber es geht besser, mit nicht kleiner Informationsrate, Satz 1.7!

Definition 1.5 (a) Ein Kanal, der nur die Buchstaben 0 und 1 ($\in \mathbb{F}_2$) überträgt, heißt binärer symmetrischer Kanal, wenn er in beiden Fällen mit derselben Wahrscheinlichkeit $0 \leq p \leq 1$ den Buchstaben ändert, also einen Fehler macht (meistens $p \ll 1$).



(b) Die Kapazität eines binären symmetrischen Kanals ist $\kappa := 1 + p\ log_2\ p + (1-p)\ log_2(1-p)$.



Definition 1.6 Die Fehlerwahrscheinlichkeit $P(C)$ eines Codes $C \subset \mathbb{F}_q^n$ ist

$$P(C) = \frac{1}{|C|} \sum_{x \in C} P_{Fehler}(x),$$

wobei $P_{Fehler}(x)$ die Wahrscheinlichkeit dafür ist, dass x beim Übertragen so verfälscht wird, dass das empfangene Wort falsch dekodiert wird.

Satz 1.7 *(Spezialfall des "Channel coding theorem" von Shannon 1948, Beginn der Kodierungstheorie.)*
Gegeben sei ein binärer symmetrischer Kanal mit $p \neq \frac{1}{2}$, *also* $0 < \kappa \leq 1$.
Es gilt:

$\forall\ \epsilon > 0\ \ \forall\ R_0$ *mit* $0 < R_0 < \kappa\ \exists\ n \in \mathbb{N}$ *und* $\exists$ *Code* $C \subset \mathbb{F}_2^n$,

so dass die Informationsrate $R(C) = \frac{log_2\ |C|}{n} \geq R_0$ *ist (aber* $R(C) < \kappa$*)und die Fehlerwahrscheinlichkeit* $P(C) < \epsilon$ *ist.*

Bemerkungen 1.8

a) Beweis hier nicht. Der Beweis benutzt Methoden der Wahrscheinlichkeitstheorie und ist nicht konstruktiv.

b) Satz: Es gibt keine Folge $(C_k)_{k \in \mathbb{N}}$ von Codes $C_k \subset F_2^{n_k}$ mit $R(C_k) > \kappa\ \forall\ k$ und mit $P(C_k) \to 0$ für $k \to \infty$.

c) Bei $\epsilon \to 0$ geht $n \to \infty$ in Theorem 1.7.

d) Es ist schwer, Folgen $(C_k)_{k \in \mathbb{N}}$ von Codes $C_k \subset F_2^{n_k}$ zu konstruieren mit $R(C_K) \geq R_0\ \forall\ k$ und $P(C_K) \to 0$ für $k \to \infty$.

e) Es ist besonders schwer, wenn man Codes C_K mit viel Struktur wünscht, die leicht zu kodieren und dekodieren sind.

Bemerkungen 1.9 Man wünscht sich Codes $C \subset \mathbb{F}_q^n$ mit folgenden schwer unter einen Hut zu bringenden Eigenschaften:

(α) hohe Informationsrate $R(C) = \frac{log_q|C|}{n}$;

(β) kleine Fehlerwahrscheinlichkeit $P(C)$;

(γ) (verwandt mit (β)) großer minimaler Hamming-Abstand $d(C) = min\ (d_H(x,y) \mid x,y \in C, x \neq y)$;

(δ) leicht und schnell zu kodieren, d.h. eine leicht zu handhabende bijektive Abbildung $f : \{\text{zu kodierende Wörter}\} \longrightarrow C \subset \mathbb{F}_q^n$;

(ϵ) leicht und schnell zu dekodieren.

Zu (ϵ): Einen guten Algorithmus zum Dekodieren zu finden ist oft schwierig und immer von großer praktischer Bedeutung.

2 Lineare Codes, Hamming-Codes

Definition 2.1 Sei $\mathbb{F}_q$ ein endlicher Körper und $n \in \mathbb{N}$.

(a) Ein Code $C \subset \mathbb{F}_q^n$ heißt linearer Code, falls $C \subset \mathbb{F}_q^n$ ein Untervektorraum ist.

(b) Ein linearer Code $C \subset \mathbb{F}_q^n$ mit $\dim C = k$ heißt $[n,k]$-Code oder $[n,k,d]$-Code, mit $d = d(c) =$ der minimale Hamming-Abstand.

(c) **Notation:** $\mathbb{F}_q^n = M(1 \times n, \mathbb{F}_q)$, d.h. die Elemente von $\mathbb{F}_q^n$ werden als Zeilenvektoren aufgefasst.

(d) Sei $C \subset \mathbb{F}_q^n$ ein linearer Code der Dimension k.

Eine Matrix $G \in M(k \times n, \mathbb{F}_q)$ heißt Erzeugermatrix von C, falls die Zeilen von G eine Vektorraumbasis von C bilden.

Bemerkung: Dann ist $C = \{a \cdot G \mid a \in \mathbb{F}_q^k\}$. Und dann ist die Abbildung

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ a & \longmapsto & a \cdot G \end{array}$$

eine sehr einfache Kodierungsregel.

(e) Sei $C \subset \mathbb{F}_q^n$ ein linearer Code der Dimension k.

Eine Matrix $H \in M(n-k) \times n, \mathbb{F}_q)$ heißt Kontrollmatrix von C, falls $C = \{x \in \mathbb{F}_q^n \mid H \cdot x^t = 0\}$.

(f) Zwei Codes $C_1 \subset \mathbb{F}_q^n$ und $C_2 \subset \mathbb{F}_q^n$ (nicht notwendig linear) heißen äquivalent, falls es eine Permutation $\sigma \in S_n$ gibt mit

$$\begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n, \quad (x_1, \cdots, x_n) \longmapsto (x_{\sigma(1)}, \cdots, x_{\sigma(n))}) \\ \bigcup & & \bigcup \\ C_1 & \longrightarrow & C_2 \end{array}$$

Beispiel 2.2 Der folgende Code ist für $k = 5$ und $n = 6$ der älteste benutzte Code. Sei

$$q = 2,\ n \in \mathbb{N}_{\geq 2},\ k = n - 1.$$

Sei

$$C := \{(x_1, \cdots, x_n) \in \mathbb{F}_2^n \mid \sum_{i=1}^{n} x_i = 0 \text{ in } \mathcal{F}_2\}.$$

Es ist $k := \dim C = n - 1$, denn man hat genau eine Relation, die Relation $\sum_{i=1}^n x_i = 0$. Eine Erzeugermatrix ist

$$G = \begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{pmatrix}.$$

Eine (hier sogar die) Kontrollmatrix ist

$$H = (1, \cdots, 1), \qquad \text{denn } H \cdot x^t = \sum_{i=1}^{n} x_i.$$

Diese Kontrollmatrix heißt parity check-Matrix.
Es ist $d(C) = 2$. Der Code C ist ein $[n, n-1, 2]$-Code.
$d(C) = 2 \Rightarrow$ der Code kann keine Fehler korrigieren, er kann bloß einzelne Fehler erkennen.
Die bijektive Abbildung

$$\begin{array}{rcl} f : \mathbb{F}_q^{n-1} & \to & C \subset \mathbb{F}_q^n \\ x = (x_1, \cdots, x_{n-1}) & \longmapsto & x \cdot G = (x_1, \cdots x_{n-1}, \sum_{i=1}^{n-1} x_i) \end{array}$$

fügt zu $(x_1, \cdots, x_{n-1})$ einen parity check-Eintrag x_n hinzu, so dass $\sum_{i=1}^{n} x_i = 0$ (in $\mathbb{F}_2$) ist. Diese Abbildung kann man hier als Kodierung deuten.

Lemma 2.3 *Sei $C \subset \mathbb{F}_q^n$ ein linearer $[n, k, d]$-Code.*

(a) $d = min\ (w(x) \mid x \in C - \{0\})$.

(b) Es gibt einen zu C äquivalenten linearen Code $\widetilde{C} \subset \mathbb{F}_q^n$ mit einer Erzeugermatrix $\widetilde{G}$ in "Standardform", d.h. von der Gestalt

$$\widetilde{G} = (\mathbb{1}_k, \widetilde{P}) \text{ mit } \mathbb{1}_k = k \times k\text{-Einheitsmatrix},$$
$$\widetilde{P} \in M(k \times (n-k), \mathbb{F}_q).$$

(c) (Definition) C selbst habe eine Erzeugermatrix $G = (\mathbb{1}_k, P)$ in Standardform. Bei $x = (x_1, \cdots, x_n) \in C$ heißen die Einträge $(x_1, \cdots, x_k)$ Informationssymbole und die Einträge $(x_{k+1} \cdots, x_n)$ Kontrollsymbole oder parity-check-Einträge (in Verallgemeinerung von Beispiel 2.2).
Es ist $(x_1, \cdots, x_n) = (x_1, \cdots, x_k) \cdot G$.

(d) C selbst habe eine Erzeugermatrix $G = (\mathbb{1}_k, P)$ in Standardform. Dann ist $H = (-P^t, \mathbb{1}_{n-k})$ eine Kontrollmatrix.

(e) Für jede Kontrollmatrix $\widetilde{H}$ von C gilt rang $\widetilde{H} = n - k$.

(f) (Nochmal Beispiel 2.2) In Beispiel 2.2 war

$$C = \begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{pmatrix}$$

in Standardform mit

$$P = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

Dort ist

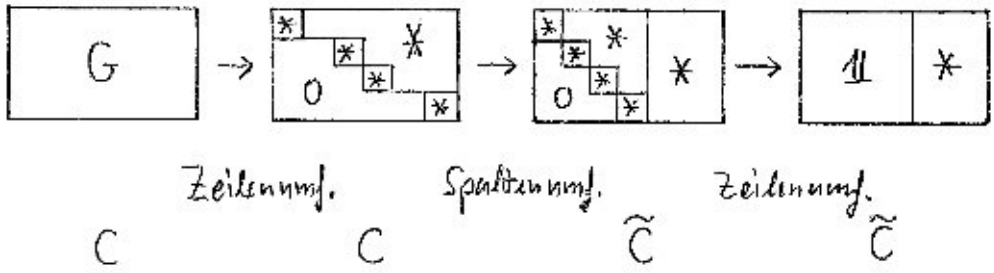
$$H = (-1, \cdots, -1, 1) = (1, \cdots, 1, 1),$$

da in $\mathbb{F}_2 \quad 1 = -1$ *ist.*

Beweis:

(a) Nach Definition von $d(C)$ gibt es Wörter x und $\widetilde{x} \in C$ mit $d(C) = d_H(x, \widetilde{x})$. C ist linear, also $x - \widetilde{x} \in C$, also $d(C) = d_H(x, \widetilde{x}) = w(x - \widetilde{x})$.

(b) Man kommt in vier Schritten von G zu $\widetilde{G}$: Man startet mit einer beliebigen Erzeugermatrix G; man wendet den Gauß-Algorithmus an; man vertauscht Spalten, so dass alle Treppenstufen vorne stehen; man wählt eine neue Basis, so dass vorne die Einheitsmatrix $\mathbb{1}_k$ steht:



(c) o.k.

(d) nach (e).

(e) $C = \{x \in \mathbb{F}_q^n \mid \widetilde{H} \cdot x^t = 0\}$,
aus der Theorie der linearen Gleichungssysteme folgt

$$\dim C = k \Longleftrightarrow \operatorname{rang} \widetilde{H} = n - k.$$

(d)

$$H \cdot G^t = (-P^t, \mathbb{1}_{n-k}) \cdot \begin{pmatrix} \mathbb{1}_k \\ P^t \end{pmatrix} = -P^t + P^t = 0,$$

also $H \cdot x^t = 0$ für alle $x \in C$, also ist H Teil einer Kontrollmatrix.
$\operatorname{rang} H = n - k$ und (e) $\Longrightarrow$ H Kontrollmatrix.

(f) o.k. □

Beispiel 2.4 (Hamming-Codes)
Wähle einen endlichen Körper $\mathbb{F}_q$ und $r \in \mathbb{N}_{\geq 2}$.
Die Menge $\mathbb{F}_q^* := \mathbb{F}_q - \{0\}$ operiert auf $\mathbb{F}_q^r - \{0\}$, nämlich durch Einschränkung der skalaren Multiplikation des $\mathbb{F}_q$-Vektorraums $\mathbb{F}_q^r$. Die Orbits dieser Operation sind die 1-dimensionalen Unterräume ohne 0 von $\mathbb{F}_q^r$. Die Menge aller Orbits ist

$$\begin{aligned}(\mathbb{F}_q^r - \{0\})/\mathbb{F}_q^* &\cong \{1-\text{dim Unterräume von } \mathbb{F}_q^r \text{ ohne } 0\} \\ &\overset{1:1}{\sim} \{1-\text{dim Unterräume von } \mathbb{F}_q^r\}.\end{aligned}$$

Sie hat

$$(q^r - 1)/(q-1) = q^{r-1} + q^{r-2} + ... + q + 1 =: n$$

Elemente.
Wegen $q^j > 1$ für $j > 0$ ist $n > r$.
Man kann eine Matrix $H \in M(r \times n, \mathbb{F}_q)$ wählen, so dass ihre Spalten Erzeuger der 1-dimensionalen Unterräume von $M(r \times 1, \mathbb{F}_q) \cong \mathbb{F}_q^r$ sind,

$$H = \left(\left| \right| \left| \right| \left| \right| \ .... \ \left| \right| \right)$$

bzw. äquivalent: so dass je zwei Spalten linear unabhängig sind.
Bemerkung: Und n ist maximal mit dieser Eigenschaft.
Es ist rang $H = r$, denn zu jeder Basis von $M(r \times 1, \mathbb{F}_q)$ enthält H skalare Vielfache aller Basisvektoren.

Der lineare Code $C = \{x \in \mathbb{F}_q^n \mid H \cdot x^t = 0\}$ mit Kontrollmatrix H heißt Hamming-Code.

Beispiel:

$$q = 2,\ r = 3,\ n = \frac{2^3 - 1}{2 - 1} = 7,$$

es ist $\mathbb{F}_2^* = \{1\}$, und $(\mathbb{F}_2^r - \{0\})/\mathbb{F}_2^* \sim \mathbb{F}_2^r - \{0\}$, also kann man H wählen als

$$\begin{aligned}H &= \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \\ &= \text{ eine Liste aller Elemente von } M(r \times 1, \mathbb{F}_2) - \{0\}.\end{aligned}$$

Nach Lemma 2.3 (e) kann man G wählen als

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right).$$

Lemma 2.5 *(Fortsetzung von Beispiel 2.4)*
Der Hamming-Code C ist ein $[n, n-r, 3]$-Code, also 1-fehlerkorrigierend.

Beweis:
$\dim C = n - r$ wegen $\operatorname{rang} H = r$ und Lemma 2.3 (e).

$d(C) \geq 3$: Je zwei Spalten von H sind linear unabhängig, und daher gilt

$$x \in C - \{0\} \overset{\text{Def von } H}{\Longleftrightarrow} H \cdot x^t = 0,\ x \neq 0 \overset{!}{\Longrightarrow} w(x) \geq 3.$$

Mit Lemma 2.3 (a) folgt $d(C) \geq 3$.

$d(C) \leq 3$: Für $x \in C$ sei

$$B_1(x) := \{y \in \mathbb{F}_q^n \mid d_H(x, y) \leq 1\}$$

Es ist

$$\mid B_1(x) \mid = 1 + n \cdot (q-1) = q^r.$$

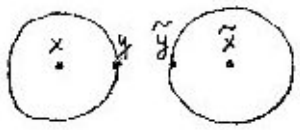
Wegen $d \geq 3$ ist $\dot{\bigcup}_{x \in C} B_1(x)$ Vereinigung disjunkter Bälle. Daher ist

$$\mid \dot{\bigcup_{x \in C}} B_1(x) \mid = q^r \cdot q^{n-r} = q^n = |\mathbb{F}_q^n|,$$

also ist

$$\mathbb{F}_q^n = \dot{\bigcup_{x \in C}} B_1(x) \qquad (*).$$

Sei nun $x \in C$ beliebig. Zu $y \in B_1(x) - \{x\}$ kann man ein $\widetilde{y} \notin B_1(x)$ mit $d_H(y, \widetilde{y}) = 1$ wählen. Dazu gibt es wegen $(*)$ ein eindeutiges $\widetilde{x} \in C$ mit $\widetilde{y} \in B_1(\widetilde{x})$.



Es ist $x \neq \widetilde{x}$ und

$$d_H(x, \widetilde{x}) \leq 1 + 1 + 1 = 3.$$

□

Bemerkungen 2.6 (Fortsetzung von Beispiel 2.4)
(i) $(*)$ sagt:

$$\forall\ y \in \mathbb{F}_q^n \quad \exists!\ x \in C \quad \text{ mit } d_H(x, y) \leq 1$$

Daher gibt die maximum-likelihood-Dekodierung [zu einem empfangenen Wort $y \in \mathbb{F}_q^n$ wähle ein $x \in C$ mit $d_H(x, y)$ minimal] hier eindeutige Worte [$\forall\ y \in \mathbb{F}_q^n \quad \exists!\ x \in C \quad$ mit $d_H(x, y)$ minimal.]

Wunderbarerweise ist sie auch einfach auszuführen:
Gegeben sei ein "empfangenes Wort" $y \in \mathbb{F}_q^n$.

1. Fall, $H \cdot y^t = 0 \Longrightarrow y \in C$: Fertig.

2. Fall, $H \cdot y^t \neq 0$: Dann ist $H \cdot y^t \in M(r \times 1, \mathbb{F}_q)\{0\}$. Dann gibt es ein eindeutiges $i \in \{1, \cdots, n\}$ und ein eindeutiges $\lambda \in \mathbb{F}_q - \{0\}$ mit

$$H \cdot y^t = \lambda \cdot (\text{i-te Spalte von H}) = \lambda \cdot H \cdot e_i^t.$$

$x := y - \lambda \cdot e_i$ erfüllt $x \in C$ und $d_H(x, y) = 1$

(ii) Die Hamming-Codes für festes $q, r, n = \frac{q^r-1}{q-1}$ sind fast äquivalent:
Änderung der Reihenfolge der Spalten von H führt zu einem äquivalenten Code (Def. 2.1 (f)).
Es bleibt die Freiheit, Spalten von H durch Multiplikation mit einem Skalar zu ändern. Das ist die Freiheit der Automorphismen

$$\begin{array}{rcll} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n & \\ x & \longrightarrow & x \cdot y^t & \text{für } y \in (\mathbb{F}_q - \{0\})^n. \end{array}$$

Im Fall $q = 2$ hat man diese Freiheit nicht, denn $\mathbb{F}_2 - \{0\} = \{1\}$. Im Fall $q = 2$ sind die Hamming-Codes zu festem q, r alle äquivalent.

(iii) Die Hamming-Codes sind leicht zu dekodieren, und für großes n ist die Informationsrate $R(C) = \frac{n-r}{n}$ schön hoch.
Aber: Für großes n ist die Eigenschaft "1-fehlerkorrigierend" zu schlecht, so dass die Codes dann unbrauchbar werden.

Lemma 2.7 *(Syndrom-Dekodierung)*
Die folgende Dekodierungsmethode für lineare Codes ist eine maximum-likelihood-Dekodierung. Sie ist brauchbar bei hoher Informationsrate.

Gegeben seien ein linearer $[n, k, d]$-Code $C \subset \mathbb{F}_q^n$ und eine Kontrollmatrix $H \in M((n-k) \times n, \mathbb{F}_q)$.
Die Abbildung

$$\mathbb{F}_q^n \longrightarrow M((n-k) \times 1, \mathbb{F}_q),\ y \longrightarrow H \cdot y^{tr},$$

induziert eine Bijektion

$$\mathbb{F}_q^n / C \longrightarrow M((n-k) \times 1, \mathbb{F}_q),\ y + C \longmapsto H \cdot y^{tr}.$$

Hier ist $\mathbb{F}_q^n / C$ die Menge der Nebenklassen $y + C = \{y + x \mid x \in C\}$ von C in $\mathbb{F}_q^n$. Diese Bijektion ist sogar ein Vektorraumisomorphismus.
Zu jeder Nebenklasse $y + C$ wählt man ein $e \in y + C$ mit minimalem Gewicht $w(e)$. So ein e heißt Nebenklassenführer ("coset leader").

Man hält die Bijektion

$$\beta : M((n-k) \times 1, \mathbb{F}_q) \to \{\text{Nebenklassenführer}\},$$

die man aus aus folgenden Bijektionen erhält, in einer Tabelle fest:

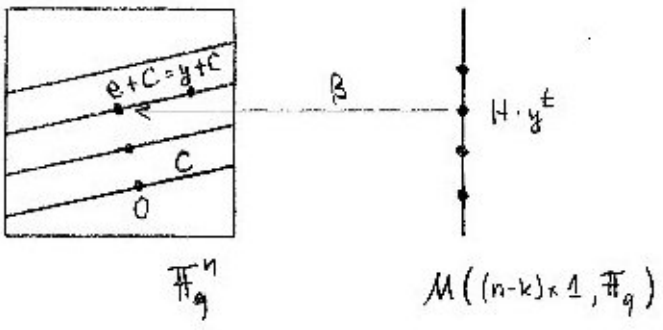
$$\begin{array}{rll} \{\text{Nebenklassenführer}\} \longrightarrow & \mathbb{F}_q^n/C & \longrightarrow M((n-k) \times 1, \mathbb{F}_q) \\ e \longrightarrow & e + C & \\ & y + C & \longrightarrow H \cdot y^{tr}. \end{array}$$

Ein empfangenes Wort $y \in \mathbb{F}_q^n$ wird dekodiert als

$$x := y - \beta(H \cdot y^{tr}).$$

$H \cdot y^{tr}$ heißt Syndrom von y. Daher "Syndrom-Dekodierung".

Beweis:



$e := \beta((H \cdot y^t)^t)$ ist in $y + C$, daher ist $x = y - e \in C$.

Wegen w(e) minimal ist $d_H(x, y) = w(e) \leq d_H(\widetilde{x}, y) \ \ \forall\, \widetilde{x} \in C$

$\Longrightarrow$ Es handelt sich um eine maximum-likelihood-Dekodierung.

Bei $R(C) = \frac{k}{n}$ hoch ist sie brauchbar, denn dann ist $|\mathbb{F}_q^{n-k}| = q^{n-k}$ klein und die Tabelle zu β klein. □

Beispiel 2.8 (zur Syndrom-Dekodierung) (a) Lemma 2.7 im Fall eines Hamming-Codes $C \subset \mathbb{F}_q^n$, $n = \frac{q^r-1}{q-1}$:

$$\begin{array}{rl} & \text{Nebenklassenführer von } y + C \\ = & \begin{cases} \lambda \cdot e_i \text{ mit } H \cdot y^{tr} = H \cdot (\lambda \cdot e_i)^{tr} & \text{falls } H \cdot y^{tr} \neq 0 \\ 0 & \text{falls } H \cdot y^{tr} = 0 \end{cases} \end{array}$$

$$\begin{array}{rlcll} y \in & \mathbb{F}_q^n & & & \\ & \downarrow & & & \\ & \mathbb{F}_q^n/C & \xrightarrow{\cong} & M(r \times 1, \mathbb{F}_q) & \xrightarrow{\beta} \{\text{Nebenklassenführer}\} \\ & [y] & \mapsto & H \cdot y^{tr} & \mapsto (\text{Nebenklassenführer von } y + C) \end{array}$$

(b) In Beispiel 8.4 wird ein binärer $[63, 51, 5]$-Code konstruiert werden. Dann ist

$$|\mathbb{F}_q^{n-k}| = 2^{63-51} = 2^{12} = 4096, \qquad |C| = 2^{51} \sim 2 \cdot 10^{15}.$$

Ohne Beweis:
63 Nebenklassen haben Nebenklassenführer mit $w = 1$.
1953 Nebenklassen haben Nebenklassenführer mit $w = 2$.
In beiden Fällen sind die Nebenklassenführer wegen $d = 5$ eindeutig.

Hier ist es sinnvoll, nur unvollständig zu dekodieren:
Bei $H \cdot y^t \notin$ (Bild in $\mathbb{F}_q^{n-k}$ von den 63 + 1953 Nebenklassen) sucht man kein x, sondern man sagt nur "≥ 3 Fehler".

Definition/Lemma 2.9 *Sei $C \subset \mathbb{F}_q^n$ ein linearer [n,k,d]-Code.*

(a) (Definition) Der duale Code $C^\perp$ ist $C^\perp := \{y \in \mathbb{F}_q^n \mid x \cdot y^t = 0 \; \forall x \in C\}$.

(b) (Lemma) $C^\perp$ ist ein linearer [n,n-k,?]-Code.

(c) (Lemma) Sind G und H eine Erzeugermatrix und eine Kontrollmatrix von C, so sind H und G eine Erzeugermatrix und eine Kontrollmatrix von C.

(d) $(C^\perp)^\perp = C$.

(e) (Definition) C heißt selbstdual, falls $C = C^\perp$.

Beweis: (a) und (e) OK.

(b) und (c) $C^\perp = \{y \in \mathbb{F}_q^n \mid G \cdot y^t = 0\}$, $\quad \operatorname{rang} G = \dim C = k$,
also ist $\dim C^\perp = n - k$, und G ist eine Kontrollmatrix von $C^\perp$.

Die Zeilen von H sind Elemente von $C^\perp$. Wegen $\dim C^\perp = n-k$ und $\operatorname{rang} H = n - k$ (Lemma 2.3 (e)) bilden die Zeilen von H eine Basis von $C^\perp$. Also ist H eine Erzeugermatrix von $C^\perp$.

(d) folgt aus c). □

Beispiele 2.10 (i) Der duale Code $C^\perp$ zum Code $C = \{(x_1, \cdots, x_n) \in \mathbb{F}_2^n \mid \sum_{i=1}^n x_i = 0\}$ in Beispiel 2.2 ist

$$C^\perp = \{(0, \cdots, 0), (1, \cdots, 1)\} \subset \mathbb{F}_2^n,$$

ein $[n, 1, n]$-Code, da $H = (1, \cdots, 1)$ ist.

(ii) (Kapitel 4 und 5, Beweis später in der Vorlesung oder Übung)

Sei C ein Hamming-Code über $\mathbb{F}_2$ und $\overline{C}$ der erweiterte Code aus Definition 2.11 unten. Dann ist $\overline{C}^\perp$ äquivalent zum Standard-Hadamard-Code $\mathcal{C}(H_{2^r}^{(st)})$ (Definition 4.6 und Satz 4.7) mit

$$\mathcal{C}(H_{2^r}^{(st)}) = \mathcal{R}(1, r) = \text{ ein Reed-Muller-Code (nach Satz 5.4).}$$

Definition/Lemma 2.11 *Sei $C \subset \mathbb{F}_q^n$ ein linearer [n,k,d]-Code.*
Der (mittels Paritätsregel) erweiterte Code $\overline{C} \subset \mathbb{F}_q^{n+1}$ ist definiert durch

$$\overline{C} := \{x_1, \cdots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1} \mid (x_1, \cdots, x_n) \in C, \sum_{i=1}^{n+1} x_i = 0\}.$$

Es ist ein [n+1, k, d($\overline{C}$)]-Code mit $d+1 \geq d(\overline{C}) \geq d$.

Im Fall $q = 2$ und d ungerade ist $d(\overline{C}) = d + 1$.

Beweis: $\overline{C}$ ist ein linearer Code: Additiv:

$$\begin{aligned} & (x_1, \cdots, x_n, x_{n+1}),\ (y_1, \cdots, y_n, y_{n+1}) \in \overline{C} \\ \Longrightarrow\ & 0 = \sum_{i=1}^{n+1} x_i + \sum_{i=1}^{n+1} y_1 = \sum_{i=1}^{n+1} (x_i + y_i) \\ \Longrightarrow\ & (x_1, \cdots, x_n, x_{n+1}) + (y_1, \cdots, y_n, y_{n+1}) \in \overline{C}. \end{aligned}$$

Invariant unter skalarer Multiplikation:

$$\begin{aligned} & \lambda \in \mathbb{F}_q,\ (x_1, \cdots, x_n, x_{n+1}) \in \overline{C} \\ \Longrightarrow\ & 0 = \lambda \cdot \sum_{i=1}^{n+1} x_i = \sum_{i=1}^{n+1} \lambda x_i \\ \Longrightarrow\ & (\lambda x_1, \cdots, \lambda x_{n+1}) \in \overline{C} \end{aligned}$$

$\dim \overline{C} = \dim C = k$: ok, da x_{n+1} eindeutig ist für jedes $(x_1, \ldots, x_n) \in C$.
$d + 1 \geq d(\overline{C}) \geq d$: $\overline{C}$ entsteht aus C, indem an jedes Wort ein Buchstabe angehängt wird.
Im Fall $q = 2$ und d ungerade ist für $(x_1, \ldots, x_n)$ mit $w((x_1, \ldots, x_n)) = d$ der neue Eintrag $x_{n+1} \neq 0$, also $w(x_1, \cdots, x_n, x_{n+1}) = d + 1$. □

3 Perfekte Codes

Definition 3.1 Ein (nicht notwendig linearer) Code $C \subset \mathbb{F}_q^n$ heißt perfekt, falls es ein $e \in \mathbb{N}$ gibt, so dass

$$\forall\ y \in \mathbb{F}_q^n \quad \exists \text{ eindeutiges } x \in C \text{ mit } d_H(x,y) \leq e.$$

Bemerkungen 3.2 (i) Dann ist $d(C) = 2e+1$, und die maximum likelihood-Dekodierung hat eindeutige Werte.

(ii) Dann ist $\mathbb{F}_q^n$ die disjunkte Vereinigung der "Bälle"

$$B_e(x) := \{y \in \mathbb{F}_q^n \mid d_H(x,y) \leq e\},$$

$$\mathbb{F}_q^n = \dot{\bigcup}_{x \in C} B_e(x).$$

Wegen

$$|B_e(x)| = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i$$

impliziert das

$$|C| \cdot \left(\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \right) = |\mathbb{F}_q^n| = q^n.$$

(iii) Es scheinen nur folgende Lösungen der Bedingung

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i \quad \text{teilt} \quad q^n$$

bekannt zu sein (vgl. MacWilliams/Sloane 1977: es sind auf jeden Fall die einzigen mit $n, q, e \leq 1000$):

(α) q, n beliebig, $e = 0$:

$$\sum_{i=0}^{0} \binom{n}{i} (q-1)^i = 1 = q^0 \mid q^n.$$

(β) q, n beliebig, $e = n$:

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i = (1 + (q-1))^n = q^n \mid q^n.$$

(γ) $q = 2, n = 2m+1$ (ungerade), $e = m$:

$$\sum_{i=0}^{m} \binom{n}{i} 1^i = \frac{1}{2} \sum_{i=0}^{n} \binom{n}{i} = \frac{1}{2} \cdot (1+1)^n = 2^{n-1} \mid 2^n$$

(δ) q beliebig, $n = \frac{q^r-1}{q-1}, e = 1$:

$$1 + n(q-1) = q^r \mid q^n \qquad \text{(Hamming)}.$$

(ϵ) $q = 2,\ n = 23,\ e = 3$:

$$1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11} \mid 2^{23}.$$

(ζ) $q = 3,\ n = 11,\ e = 2$:

$$1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 4 = 243 = 3^5 \mid 3^{11}.$$

(η) $q = 2,\ n = 90,\ e = 2$:

$$1 + \binom{90}{1} + \binom{90}{2} = 4096 = 2^{12} \mid 2^{90}.$$

Definition 3.3 Ein Code $\widetilde{C} \subset \mathbb{F}_q^n$ entsteht aus einem Code $C \subset \mathbb{F}_q^n$ durch Verschiebung, falls ein $y \in \mathbb{F}_q^n$ existiert mit $\widetilde{C} = y + C$.

Satz 3.4 *(Hier fast ohne Beweis; harte Einzelresultate; vgl. Lütkebohmert, van Lint)*

(a) Der einzige perfekte Code zu (α) ist

$$C = \mathbb{F}_q^n \subset \mathbb{F}_q^n, \qquad \text{ein } [n, n, 1]\text{-Code}.$$

(b) In Definition 1.3 (a) war für Codes $|C| \geq 2$ gefordert. Wenn man jetzt auch $|C| = 1$ zulässt, gehören zu (β) alle Codes $C \subset \mathbb{F}_q^n$ mit $|C| = 1$, also bis auf Verschiebung nur der lineare Code $C = \{0\} \subset \mathbb{F}_q^n$, ein $[n, 0, d$ nicht definiert$]$*-Code.*

(c) Die einzigen perfekten Codes zu (γ) sind, bis auf Verschiebung, die sogenannten Wiederholungscodes:

$$C = \{(0, \cdots, 0), (1, \cdots, 1)\} \subset \mathbb{F}_2^{2m+1}$$

(zwei Wörter, die möglichst weit voneinander entfernt stehen).

C ist ein $[n, 1, n]$-Code.

(d) Die einzigen linearen perfekten Codes zu (δ) sind die Hamming-Codes:

$$[n, n-r, 3]\text{-Codes}.$$

(e) Bis auf Äquivalenz (Definition 2.1 (f)) und Verschiebung gibt es nur einen perfekten Code zu (ϵ)*, den binären Golay-Code* $\mathcal{G}_{23}$*, ein* $[23, 12, 7]$*-Code.*

(f) Bis auf Äquivalenz und Verschiebung gibt es nur einen perfekten Code zu (ζ)*, den ternären Golay-Code* $\mathcal{G}_{11}$*, ein* $[11, 6, 5]$*-Code.*

(g) Zu (η) *gibt es keinen perfekten Code.*

(h) (a)-(f) geben eine vollständige Liste aller linearen perfekten Codes.

(i) Die einzigen perfekten Codes außer denen in (a)-(f) sind nichtlineare Codes mit den Daten wie in (δ)*, also* $e = 1$*,* $n = \frac{q^r-1}{q-1}$ *(wie bei den Hamming-Codes).*

(j) Es gibt solche Codes, die nicht durch Verschiebung aus den Hamming-Codes entstehen. Aber ihre vollständige Klassifikation ist ein (noch immer) offenes Problem.

Beweisteile:
(a)–(c) Klar.
Zu (d): Hamming-Codes sind perfekt mit $e = 1$, wegen Bemerkung 2.6 (i). □

Bemerkung 3.5 G_{23} wurde in einer Voyager-Sonde benutzt. Er hat reiche Bezüge zu finiter Geometrie und endlichen Gruppen.

Sloane/MacWilliams: "der wichtigste aller Codes, aus praktischen und theoretischen Gründen."

Golay hatte erst (ϵ) und (ζ) gefunden, dann $\mathcal{G}_{23}$ und $\mathcal{G}_{11}$.

4 Hadamard-Codes

Definition 4.1 Eine $n \times n$ Matrix $H = (h_{ij})$ heißt Hadamard-Matrix, falls alle $h_{ij} \in \{-1, 1\}$ sind und falls $H \cdot H^t = n \cdot \mathbb{1}_n$ ist.

Bemerkungen/Beispiele 4.2 (i) Bei $h_{ij} \in \{\pm 1\}$ erfüllt jede Zeile von H automatisch

$$(h_{i1}, \cdots, h_{in}) \cdot \begin{pmatrix} h_{i1} \\ \vdots \\ h_{in} \end{pmatrix} = n.$$

Die Bedingung $H \cdot H^t = n \cdot \mathbb{1}_n$ sagt deshalb nur, dass verschiedene Zeilen von H orthogonal sind. Wegen $h_{ij} \in \{\pm 1\}$ ist das äquivalent dazu, dass verschiedene Zeilen sich an genau $\frac{n}{2}$ Stellen unterscheiden.

(ii) Die Matrizen

$$H_1^{(st)} := (1) \quad \text{und} \quad H_2^{(st)} := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

sind Hadamard-Matrizen (der obere Index (st) steht für "Standard").

(iii) **Definition:** Das Tensorprodukt zweier Matrizen

$$A = (a_{ij}) \in M(n \times n, \mathbb{C}) \qquad \text{und} \qquad B \in M(m \times m, \mathbb{C})$$

(statt $\mathbb{C}$ kann man irgendeinen kommutativen Ring nehmen) ist

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{1n}B \\ \vdots & \vdots \\ a_{n1}B & a_{nn}B \end{pmatrix} \in M(nm \times nm, \mathbb{C}).$$

Es ist im allgemeinen nicht symmetrisch, aber assoziativ,

$$(A \otimes B) \otimes C = A \otimes (B \otimes C)$$

(Beweis: Übung), und es erfüllt bei

$$C \in M(n \times n, \mathbb{C}), \quad D \in M(m \times m, \mathbb{C}),$$

$$(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$$

(Beweis: Übung).

(iv) **Behauptung:** Sind H und $\widetilde{H}$ Hadamard-Matrizen, so ist auch $H \otimes \widetilde{H}$ eine Hadamard-Matrix.

Beweis: (a) Die Einträge von $H \otimes \widetilde{H}$ sind offenbar in $\{\pm 1\}$.

(b) Verschiedene Zeilen von $H \otimes \widetilde{H}$ sind orthogonal:

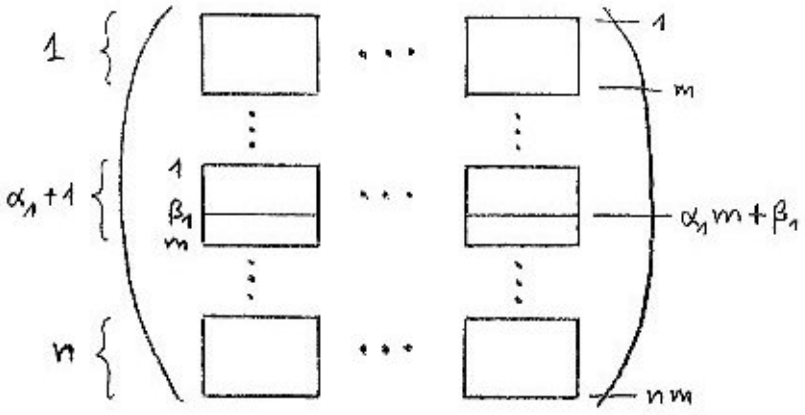
Betrachte die $(\alpha_1 m + \beta_1)$-te Zeile und die $(\alpha_2 m + \beta_2)$-te Zeile mit $0 \leq \alpha_j < n$, $1 \leq \beta_j \leq m$ und $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$.

$(\alpha_1 m + \beta_1)$-te Zeile:

$$z_1 := (a_{\alpha_1+1,1} \cdot (b_{\beta_1,1}, \cdots, b_{\beta_1,m}), \cdots, a_{\alpha_1+1,n} \cdot (b_{\beta_1,1}, \cdots, b_{\beta_1,m}))$$

$(\alpha_2 m + \beta_2)$-te Zeile:

$$z_2 := (a_{\alpha_2+1,1} \cdot (b_{\beta_2,1}, \cdots, b_{\beta_2,m}), \cdots, a_{\alpha_2+1,n} \cdot (b_{\beta_2,1}, \cdots, b_{\beta_2,m})).$$



<u>1. Fall, $\beta_1 \neq \beta_2$:</u>

$$(b_{\beta_1,1}, \cdots, b_{\beta_1,m}) \cdot \begin{pmatrix} b_{\beta_2,1} \\ \vdots \\ b_{\beta_2,m} \end{pmatrix} = 0, \quad \text{also } z_1 \cdot z_2^t = 0.$$

<u>2. Fall, $\beta_1 = \beta_2,\ \alpha_1 \neq \alpha_2$:</u>

$$(a_{\alpha_1+1,1,\cdots,}a_{\alpha_1+1,n}) \cdot \begin{pmatrix} a_{\alpha_2+1,1} \\ \vdots \\ a_{\alpha_2+1,n} \end{pmatrix} = 0, \quad (b_{\beta_1,1}, \cdots, b_{\beta_1,m}) \cdot \begin{pmatrix} b_{\beta_1,1} \\ \vdots \\ b_{\beta_1,m} \end{pmatrix} = m,$$

$$\text{also } z_1 \cdot z_2^t = (a_{\alpha_1+1,1,\cdots,}a_{\alpha_1+1,n}) \cdot m \cdot \begin{pmatrix} a_{\alpha_2+1,1} \\ \vdots \\ a_{\alpha_2+1,n} \end{pmatrix} = 0.$$

(v) Daher sind die induktiv definierten $2^n \times 2^n$-Matrizen

$$H_{2^n}^{(st)} := H_2^{(st)} \otimes H_{2^{n-1}}^{(st)} = \begin{pmatrix} H_{2^{n-1}}^{(st)} & H_{2^{n-1}}^{(st)} \\ H_{2^{n-1}}^{(st)} & -H_{2^{n-1}}^{(st)} \end{pmatrix}$$

auch Hadamard-Matrizen. Die ersten Beispiele:

$$H_4^{(st)} = \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right), \quad H_8^{(st)} = \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & \\ 1 & -1 & 1 & -1 & \\ 1 & 1 & -1 & -1 & \text{dito} \\ 1 & -1 & -1 & 1 & \\ \hline \multicolumn{4}{c|}{\text{dito}} & -\text{dito} \end{array}\right)$$

Wegen der Assoziativität ist

$$\begin{aligned} H_{2^n}^{(st)} &= H_2^{(st)} \otimes (H_2^{(st)} \otimes (\cdots \otimes H_2^{(st)}) \cdots)) \\ &= H_2^{(st)} \otimes \cdots \otimes H_2^{(st)} = H_{2^{n-1}}^{(st)} \otimes H_2^{(st)}. \end{aligned}$$

(vi) Aus einer Hadamard-Matrix erhält man wieder Hadamard-Matrizen, wenn man Spalten oder Zeilen vertauscht oder wenn man Spalten oder Zeilen mit (-1) multipliziert.

Daher kann man aus jeder Hadamard-Matrix eine neue konstruieren, die nur $+1$ in der 1. Spalte und 1.Zeile hat.

Definition: Solche Hadamard-Matrizen heißen normalisiert.

Die $H_{2^n}^{(st)}$ sind normalisiert.

(vii) Abgesehen von den $H_{2^n}^{(st)}$ ist es schwierig, Hadamard-Matrizen zu konstruieren.

Lemma 4.3 *Sei H eine $n \times n$-Hadamard-Matrix. Dann ist $n \in \{1, 2\}$, oder 4 teilt n.*

Beweis: Sei $n \geq 3$. Wegen Bemerkung 4.2 (vi) kann man annehmen, dass die ersten 3 Zeilen von H so aussehen:

$$\begin{array}{cccc} 1-1 & 1-1 & 1-1 & 1-1 \\ 1-1 & 1-1 & (-1)-(-1) & (-1)-(-1) \\ 1-1 & (-1)-(-1) & 1-1 & (-1)-(-1), \end{array}$$

mit vier Blöcken der Längen i, j, k, l, mit $i + j + k + l = n$.
Die Zeilen von H sind paarweise orthogonal. Das gibt im Fall

$$\begin{aligned} &\text{1. \& 2. Zeile:} \quad 0 = i + j - k - l \quad (A) \\ &\text{1. \& 3. Zeile:} \quad 0 = i - j + k - l \quad (B) \end{aligned}$$

2. & 3. Zeile: $0 = i - j - k + l \quad (C)$

$(A) + (B) \Longrightarrow i = l, \quad$ mit $(A) \Longrightarrow j = k,$
mit $(C) \Longrightarrow i = j = k = l.$
Also $n = 4 \cdot i, \quad \Longrightarrow \quad n$ ist durch 4 teilbar. □

Bemerkung 4.4 Warum kann man das Argument von Lemma 4.3 nicht erweitern auf 4 Zeilen und $8|n$?

In Lemma 4.3: 4 Variablen i, j, k, l; 3 Zeilen orthogonal, also $\binom{3}{2} = 3$ Gleichungen; ausrechnen $\Longrightarrow i = j = k = l \Longrightarrow n = i + j + k + l = 4i \Longrightarrow 4|n$.

Im allgemeinen Fall von k Zeilen: 2^{k-1} Variablen und $\binom{k}{2}$ Gleichungen,

Für $k \geq 4$ ist $\binom{k}{2} < 2^{k-1} - 1$, also hat man nicht $2^{k-1} - 1$ Gleichungen, also kann man nicht auf $i = j = k = l = \cdots$ schließen.

Vermutung 4.5 *Für alle $n \in \mathbb{N}$, die durch 4 teilbar sind, gibt es $n \times n$-Hadamard-Matrizen.*
Der erste offene Fall (?) ist $n = 268$. Schon der Fall $n = 12$ ist nichttrivial.

Definition 4.6 Sei $n \geq 2$. Aus einer $n \times n$-Hadamard-Matrix H erhält man folgendermaßen einen Hadamard-Code $\mathcal{C}(H) \subset \mathbb{F}_2^n$:

Zuerst ersetzt man in allen Einträgen von $H \quad 1$ durch $0 \in \mathbb{F}_2$ und (-1) durch $1 \in \mathbb{F}_2$ und nennt die neue Matrix

$$A(H) \in M(n \times n, \mathbb{F}_2).$$

Dann ist der Code

$$\mathcal{C}(H) = \{\text{Zeilen von } A(H)\} \cup \big((1, \ldots, 1) + \{\text{Zeilen von } A(H)\}\big).$$

Offenbar ist $|\mathcal{C}(H)| = 2n$.
Notation: $e := (1, \ldots, 1) \in \mathbb{F}_2^n$.

Satz 4.7 *(a) $\mathcal{C}(H)$ ist ein $(n, 2n, \frac{n}{2})$-Code*

[n = Wortlänge, $2n = |\mathcal{C}(H)|$, $\frac{n}{2} = d(\mathcal{C}(H))$].

[Es ist nicht behauptet, dass $\mathcal{C}(H)$ ein linearer Code ist.]

Man hat eine präzise Aussage über die Hamming-Abstände:

Für alle $x \in \mathcal{C}(H)$ gilt:

$$d_H(x, x) = 0, \qquad d_H(x, x + e) = n,$$
$$\forall\ y \in \mathcal{C}(H) - \{x, x + e\} \text{ ist } d_H(x, y) = \tfrac{n}{2}.$$

(b) Bemerkung: $d(\mathcal{C}(H)) = \frac{n}{2}$ *ist schön groß, aber die Informationsrate*

$$R(\mathcal{C}(H)) = \frac{\log_2(2n)}{n}$$

ist sehr klein für großes n*.*

(c) Sei $n = 2^m \geq 2$*. Der Standard-Hamming-Code* $\mathcal{C}(H_{2^m}^{(st)})$ *ist ein* <u>*linearer*</u> $[2^m, m+1, 2^{m-1}]$*-Code* $\quad$ *[*$m+1 = \log_2 |\mathcal{C}(H_{2^m}^{(st)})$*].*

Beweis:
(a) 4.2 (i): Verschiedene Zeilen von $A(H)$ unterscheiden sich an genau $\frac{n}{2}$ Stellen. Daher gilt

$$x \in \{\text{Zeilen von } A(H)\} \Longrightarrow x + e \notin \{\text{Zeilen von } A(H)\}.$$

Daher ist $|\mathcal{C}(H)| = 2n$.
Die Aussagen zu den Hamming-Abständen folgen auch sofort aus 4.2 (i).

(b) Klar.

(c) Wegen (a) ist nur zu zeigen ist, dass $\mathcal{C}(H_{2^m}^{(st)})$ ein linearer Code ist.

Behauptung: Die Menge $\{\text{Zeilen von } A(H_{2^m}^{(st)})\} \subset \mathbb{F}_2^n$ ist ein Untervektorraum von $\mathbb{F}_2^n$ der Dimension m.

Beweis: Mit Induktion nach m.
<u>$m = 1$</u>:

$$A(H_{2^1}^{(st)}) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Die Menge $\{(0,0),(0,1)\} \subset \mathbb{F}_2^2$ ist ein Untervektorraum der Dimension 1.

<u>$m \to m+1$</u>:

$$\begin{aligned} H_{2^{m+1}}^{(st)} &= H_2^{(st)} \otimes H_{2^m}^{(st)} = \begin{pmatrix} H_{2^m}^{(st)} & H_{2^m}^{(st)} \\ H_{2^m}^{(st)} & -H_{2^m}^{(st)} \end{pmatrix}, \\ \{\text{Zeilen von } A(H_{2^{m+1}}^{(st)})\} &= \{(x,x) \mid x \text{ Zeile von } A(H_{2^m}^{(st)})\} \\ &\cup \{(x, e+x) \mid x \text{ Zeile von } A(H_{2^m}^{(st)})\}. \\ &\subset \mathbb{F}_2^{2^{m+1}}. \end{aligned}$$

(i) Diese Teilmenge ist invariant unter skalarer Multiplikation mit $\mathbb{F}_2$:
Wegen $\mathbb{F}_2 = \{0,1\}$ reicht es zu zeigen, dass diese Teilmenge die 0 enthält.
Das tut sie, denn die Matrix $H_{2^{m+1}}^{(st)}$ ist normalisiert (4.2 (vi)), also ist ihre erste Zeile gleich $(1,...,1)$, also ist $(0,...,0) = 0 \in \mathbb{F}_2^{2^{m+1}}$ in der Menge $\{\text{Zeilen von } A(H_{2^{m+1}}^{(st)})\}$.

(ii) Diese Teilmenge ist invariant unter Addition:

$$\begin{aligned}(x,x)+(y,y) &= (x+y,x+y),\\ (x,x)+(y,e+y) &= (x+y,e+x+y),\\ (x,e+x)+(y,e+y) &= (x+y,x+y)\end{aligned}$$

Induktionsannahme $\Longrightarrow x+y$ ist eine Zeile von $A(H_{2^m}^{(st)})$
$\Longrightarrow (x+y,x+y)$ und $(x+y,e+x+y)$ sind Zeilen von $A(H_{2^{m+1}}^{(st)})$.

(i) und (ii) geben den Induktionsschritt. Die Behauptung ist bewiesen. ($\square$)

Folgerung:

$$\mathcal{C}(H_{2^m}^{(st)}) = \{\text{Zeilen von } A(H_{2^m}^{(st)})\} \cup \ (e + \{\text{Zeilen von } A(H_{2^m}^{(st)})\})$$

ist ein Untervektorraum von $\mathbb{F}_2^{2^m}$ der Dimension $m+1$.

Beweis: Nach (a) ist das eine Menge mit 2^{m+1} Elementen.
Invariant unter skalarer Multiplikation: $0 \in \mathcal{C}(H_{2^m}^{(st)})$ wegen (i). Gleiches Argument wie in (i).
Additiv: Seien $x, y \in \{\text{Zeilen von } A(H_{2^m}^{(st)})\}$.
Nach der Behauptung ist dann $x+y \in \{\text{Zeilen von } A(H_{2^m}^{(st)})\}$.
Es ist auch $x+y = (e+x)+(e+y)$.
Es folgt auch $(e+x)+y = x+(e+y) \in e + \{\text{Zeilen von } A(H_{2^m}^{(st)})\}$. $\square$

Bemerkungen 4.8 (a) Die Mariner-Mission 1969 bestand aus 2 Raumfahrzeugen.

Mariner 6 startete am 24.02.1969 von der Erde und erreichte am 30.07.1969 einen Abstand von 2130 Meilen vom Äquator des Mars.

Mariner 7 startete am 27.03.1969 von der Erde und erreichte am 04.08.1969 einen Abstand von 2131 Meilen vom Äquator des Mars.

Zusammen sandten sie 201 schwarz-weiße Bilder zur Erde, jedes aus zahlreichen Pixeln mit Helligkeitsstufen von 0 bis 63.

Die Bilder wurden mit einer Nebenklasse des Codes $\mathcal{C}(H_{2^5}^{(st)})$ (= der Reed-Muller-Code $\mathcal{R}(1,5)$, siehe Kapitel 5, Satz 5.4) kodiert.

(b) "Coding-Gain":

Es gibt eine Größe "SNR" = "Signal to noise ratio" = $\frac{E_b}{\sigma^2}$,

E_b = aufgewandte Energie pro gesendetem Bit,

σ = Varianz des störenden "weißen Rauschens" im Kanal.

Damit ein Code nützlich ist, muss

$$\text{SNR(mit Kodierung)} < \text{SNR(ohne Kodierung)}$$

sein. [Je kleiner das SNR ist, desto besser]. Dann heißt

$$10 \cdot log_{10} \left(\frac{\text{SNR(ohne Kodierung)}}{\text{SNR(mit Kodierung)}} \right)$$

coding gain, mit der Einheit "dB".

(c) Schätzung für die Raumfahrt Ende der 60er Jahre:

1 dB coding gain $\approx$ 1.000.000 \$

Schätzung 1998:

1 dB coding gain $\approx$ 80.000.000 \$

Auf der Galileo- Mission (Hubble-Teleskop) hat nur Kodierung die Mission gerettet und den Verlust von 10^9 \$ verhindern können.

Definition 4.9 Ein Code $C \subset \mathbb{F}_q^n$ heißt kommafrei vom Index $r \in \mathbb{N}$, falls

$$\forall\, x, y, z \in C\ \forall\, k \in \{2, \cdots, n\} \quad d_H((x_k, x_{k+1}, \cdots, x_n, y_1, \cdots, y_{k-1}), z) \geq r$$

ist.

Bemerkungen 4.10 (a) Ist ein Code kommafrei und treten pro Wort $< r$ Fehler auf, so kann der Empfänger, falls bei der Übertragung die Information verlorengegangen ist, wo Wörter anfangen und enden, aus dem empfangenen Wort-Bandwurm rekonstruieren, wo die Wörter anfangen und enden und welche Wörter gesendet wurden.

(b) Bei der Mariner-Mission 1969 wurde als Code die Nebenklasse $n_{69} + \mathcal{C}(H_{2^5}^{(st)})$ gewählt mit

$$n_{69} = (1000\ 1101\ 1101\ 0100\ 0010\ 0101\ 1001\ 1111) \in \mathbb{F}_2^{32}.$$

Sie ist kommafrei vom Index 6.

$\mathcal{C}(H_{2^5}^{(st)})$ hat auch 32 Nebenklassen, die kommafrei vom Index 7 sind, allerdings keine von einem Index ≥ 8. Jede Nebenklasse hat 64 Elemente $= 64$ Repräsentanten, da $|\mathcal{C}(H_{2^5}^{(st)})| = 2 \cdot 32 = 64$ ist.

Also existieren $64 \cdot 32$ Elemente von $\mathbb{F}_2^{32}$, mit denen man von $\mathcal{C}(H_{2^5}^{(st)})$ zu einer der 32 Nebenklasse, die kommafrei von Index 7 sind, übergehen könnte.

Aber gegenüber allen diesen Elementen hat n_{69} einen entscheidenden Vorteil, der dazu geführt hat, dass es allen diesen Elementen v vorgezogen wurde: In einem Sinn, der hier nicht präzisiert wird, kann man es schneller erzeugen und besser damit arbeiten als mit allen $64 \cdot 32$ Elementen der Nebenklassen vom Index 7.

Kodieren und Dekodieren der Codes $\mathcal{C}(H_{2^m}^{(st)})$

Das läßt sich effizient durchführen, aufgrund schöner Eigenschaften von $H_{2^m}^{(st)}$. Angewandt wurden die Verfahren bei den Mariner '69 Sonden.

Satz/Definition 4.11 *(a) (Definition) Induktiv über $m \in \mathbb{N}$ werden Matrizen $G_m \in M(m \times 2^m, \mathbb{F}_2)$ definiert durch*

$$\begin{aligned} G_1 &:= (0\ 1), \\ G_{m+1} : &= \left(\begin{array}{c|c} 0\cdots 0 & 1\cdots 1 \\ \hline G_m & G_m \end{array}\right). \end{aligned}$$

Also ist zum Beispiel

$$G_2 := \left(\begin{array}{cc|cc} 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \end{array}\right),$$

$$G_3 := \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right),$$

$$G_4 := \left(\begin{array}{cccccccc|cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

(b) Die Spalten von G_m sind die Zahlen $0, 1, \ldots, 2^m - 1$ binär geschrieben, d.h. bei $j \in \{0, 1, \ldots, 2^m - 1\}$ und $j = \sum_{k=1}^{m} j_k \cdot 2^{k-1}$ ist

$$\begin{pmatrix} j_m \\ \vdots \\ j_1 \end{pmatrix} = (j+1)\text{-te Spalte von } G_m.$$

(c)

$$G_m^t \cdot G_m = A(H_{2^m}^{(st)}).$$

Beweis:
(a) ok.

(b) Beweis mit Induktion: Klar.

(c) Beweis mit Induktion nach m:

$\underline{m = 1}$: $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = A(\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}) = A(H_2^{(st)})$.

$\underline{m \longrightarrow m+1}$:

$$
\begin{aligned}
G_{m+1}^{tr} \cdot G_{m+1} &= \left(\begin{array}{c|c} 0 & \\ \vdots & G_m^{tr} \\ 0 & \\ \hline 1 & \\ \vdots & G_m^{tr} \\ 1 & \end{array}\right) \cdot \left(\begin{array}{c|c} 0\cdots 0 & 1\cdots 1 \\ \hline G_m & G_m \end{array}\right) \\
&= \left(\begin{array}{c|c} \mathbf{0}\cdot\mathbf{0} + G_m^t \cdot G_m & \mathbf{0}\cdot\mathbb{1} + G_m^t \cdot G_m \\ \hline \mathbb{1}\cdot\mathbf{0} + G_m^t \cdot G_m & \begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}\begin{pmatrix}1 & \cdots & 1\end{pmatrix} + G_m^t \cdot G_m \end{array}\right) \\
&= \left(\begin{array}{c|c} A(H_{2^m}^{(st)}) & A(H_{2^m}^{(st)}) \\ \hline A(H_{2^m}^{(st)}) & \begin{pmatrix}1\cdots 1\\ 1\cdots 1\end{pmatrix} + A(H_{2^m}^{(st)}) \end{array}\right) \\
&= A\left(\begin{array}{c|c} H_{2^m}^{(st)} & H_{2^m}^{(st)} \\ \hline H_{2^m}^{(st)} & -H_{2^m}^{(st)} \end{array}\right) \\
&= A(H_2^{(st)} \otimes H_{2^m}^{(st)}) \\
&= A(H_{2^{m+1}}^{(st)}) \qquad \square
\end{aligned}
$$

Bemerkung 4.12 Drei Beschreibungen der $H_{2^m}^{(st)}$:

1) Bemerkung 4.2 (v): Induktive Definition, $\quad H_{2^m}^{(st)} := H_2^{(st)} \otimes H_{2^{m-1}}^{(st)}$.

2) Satz 4.11 (c), $\quad G_m^t \cdot G_m = A(H_{2^m}^{(st)})$,
   mit $A : \{1, -1\} \to \mathbb{F}_2, 1 \mapsto 0, -1 \mapsto 1$.

3) Satz 4.16 (b), $\quad H_{2^m}^{(st)} = M_{2^m}^{(1)} \cdot M_{2^m}^{(2)} \cdot \ldots \cdot M_{2^m}^{(m)}$.

   1) $\longrightarrow$ $H_{2^m}^{(st)}$ Hadamard-Matrix, $\mathcal{C}(H_{2^m}^{(st)})$ linearer Code (Satz 4.7 (c)).
   2) $\longrightarrow$ schöne Erzeugermatrix, schnelles Kodieren (Korollar 4.13).
   3) $\longrightarrow$ schnelles Dekodieren (Lemma 4.14 und Satz 4.16): Entscheidend für die Wahl von $\mathcal{C}(H_{32}^{(st)})$ bei den Mariner '69 Sonden.

Korollar 4.13 *(Kodieren des Codes $\mathcal{C}(H_{2^m}^{(st)})$)*

(a) Sei $j \in \{0, 1, 2, \ldots, 2^{m+1} - 1\}$). Die $(j+1)$-te Zeile der Matrix

$$\begin{pmatrix} A(H_{2^m}^{(st)}) \\ A(-H_{2^m}^{(st)}) \end{pmatrix}$$

ist

$$(j_{m+1}, j_m, \ldots, j_2, j_1) \cdot \begin{pmatrix} 1 \cdots 1 \\ G_m \end{pmatrix},$$

bei $j = \sum_{k=1}^{m+1} j_k \cdot 2^{k-1}, \qquad (j_{m+1}, \ldots, j_2, j_1) \in \mathbb{F}_2^{m+1}$.

Bemerkung: $\{\text{Zeilen dieser Matrix}\} = \mathcal{C}(H_{2^m}^{(st)})$.

(b) Eine Erzeugermatrix (nicht in Standardform $(\mathbb{1}, P)$, aber trotzdem schön) des Codes $\mathcal{C}(H_{2^m}^{(st)})$ ist

$$G_m^{erz} := \begin{pmatrix} 1 \cdots 1 \\ G_m \end{pmatrix} \in M((m+1) \times 2^m, \mathbb{F}_2).$$

(c) (Kodierung) Die Kodierungsabbildung $\mathbb{F}_2^{m+1} \to \mathcal{C}(H_{2^m}^{(st)})$ ist daher einfach die Abbildung

$$(j_{m+1}, \ldots, j_1) \longrightarrow (j_{m+1} \cdots j_1) \cdot G_m^{erz}.$$

Bemerkung: Für die Realisierung der Binärdarstellung $(j_{m+1}, \ldots, j_2, j_1) \in \mathbb{F}_2^{m+1}$ einer Zahl $j \in \{0, 1, \ldots, 2^{m+1} - 1\})$ braucht man bloß einen Digitalzähler. Er durchläuft dann die Spalten von G_{m+1}.

Beweis: (a)+(b) Für $0 \leq j \leq 2^m - 1$ folgt (a) aus Satz 4.11 (b)+(c), für $2^m \leq j \leq 2^{m+1} - 1$ ist es dann auch klar.
Daher erzeugen die Zeilen von G_m^{erz} den linearen Code $\mathcal{C}(H_{2^m}^{(st)})$.
G_m^{erz} ist eine Erzeugermatrix, denn

$$|\{\text{Zeilen von } G_m^{erz}\}| = m + 1 = \dim \mathcal{C}(H_{2^m}^{(st)}).$$

(c) klar. □

Lemma 4.14 *(Dekodieren der Codes $\mathcal{C}(H_{2^m}^{(st)})$)*

(a) (Definition) Für $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ sei

$$A^{-1}(x) := (A^{-1}(x_1), \ldots, A^{-1}(x_n)) \in M(1 \times n, \{1, -1\})$$

mit $A^{-1} : \mathbb{F}_2 \to \{1, -1\}, 0 \mapsto 1, 1 \mapsto -1$.

(b) (Dekodieren) Wird ein Wort $x \in \mathcal{C}(H_{2^m}^{(st)})$ gesendet und ein Wort $y = x + c \in \mathbb{F}_2^{2^m}$ empfangen mit

$c \in \mathbb{F}_2^{2^m}, w(c) \leq 2^{m-2} - 1 \quad (\approx \frac{1}{4} \cdot 2^m = \frac{1}{4}$ *der Länge von* $x)$,

so ist x durch die Eigenschaft eindeutig bestimmt, dass es das einzige Wort in $\mathcal{C}(H_{2^m}^{(st)})$ mit $A^{-1}(x) \cdot A^{-1}(y)^{tr} \geq 2^{m-1} + 2$ ist. Genauer gilt:

$$\begin{aligned} A^{-1}(x) \cdot A^{-1}(y)^{tr} &\geq 2^{m-1} + 2 \\ A^{-1}(e+x) \cdot A^{-1}(y)^{tr} &= (-A^{-1}(x)) \cdot A^{-1}(y)^{tr} \leq -(2^{m-1} + 2), \\ |A^{-1}(z) \cdot A^{-1}(y)^{tr}| &\leq 2^{m-1} - 2 \quad \text{für alle } z \in \mathcal{C}(H_{2^m}^{(st)}) - \{x, e+x\}. \end{aligned}$$

Die Zuordnung $y \mapsto x$ ist die maximum likelihood-Dekodierung, falls $w(c) \leq 2^{m-2} - 1$, d.h. falls die Anzahl der Fehler $\leq 2^{m-2} - 1$ war.

Beweis: (a) Definition.

(b) Im fehlerfreien Fall $x = y$ ist $A^{-1}(x)A^{-1}(y)^{tr} = 2^m$. Jeder Fehler erniedrigt die Summe um 2, also

$$A^{-1}(x) \cdot A^{-1}(x+c)^{tr} = 2^m - 2 \cdot w(c) \geq 2^{m-2} + 2.$$

Wegen $A^{-1}(x+e) = -A^{-1}(x)$ ist

$$A^{-1}(e+x) \cdot A^{-1}(y)^{tr} = (-A^{-1}(x)) \cdot A^{-1}(y)^{tr} \leq -(2^{m-1} + 2).$$

Für $z \in \mathcal{C}(H_{2^m}^{(st)})$ ist

$$A^{-1}(z) \cdot A^{-1}(x)^{tr} = 0,$$

daher ist

$$\begin{aligned} |A^{-1}(z) \cdot A^{-1}(x+c)| &= |\text{Eine Summe mit } w \text{ Summanden, jeder } \in \{\pm 2\}| \\ &\leq 2 \cdot w(c) \leq 2^{m-1} - 2. \end{aligned}$$

□

Bemerkung 4.15 Zur Dekodierung in Lemma 4.14 (b) muss man die Produkte aller Zeilen von $H_{2^m}^{(st)}$ mit $A^{-1}(y)^{tr}$ testen, also muss man die Abbildung

$$A^{-1}(y)^{tr} \longmapsto H_{2^m}^{(st)} \cdot A^{-1}(y)^{tr}, \quad M(2^m \times 1, \{1, -1\}) \longmapsto M(2^m \times 1, \mathbb{Z})$$

durchführen. Sie heißt Hadamard-Transformation.
Satz 4.16 zeigt, wie man sie schnell ausführen kann. Satz 4.16 wurde von Green (Mitarbeiter am JPL = Jet Propulsion Laboratory) gefunden und in der "Green machine" zum Dekodieren der Signale von den Mariner '69-Sonden implementiert.
Ein allgemeineres Rezept, ausgehend von einer "schnellen Fourier-Transformation für endliche abelsche Gruppen" wurde von Welsh (unabhängig) entwickelt.

Satz 4.16 *(Schnelle Hadamard-Transformation)*

(a) (Definition) Für $m \geq 1$ und $i = 1, 2, \ldots, m$ sei

$$M_{2^m}^{(i)} := \mathbb{1}_{2^{m-i}} \otimes H_2^{(st)} \otimes \mathbb{1}_{2^{i-1}} \in M(2^m \times 2^m, \{0, 1, -1\}),$$

wobei $\mathbb{1}_k$ die $k \times k$-Einheitsmatrix ist. Zum Beispiel ist

$$\begin{aligned}
M_{2^m}^{(m)} &= \left(\begin{array}{c|c} \mathbb{1}_{2^{m-1}} & \mathbb{1}_{2^{m-1}} \\ \hline \mathbb{1}_{2^{m-1}} & -\mathbb{1}_{2^{m-1}} \end{array}\right), \\
M_{2^m}^{(m-1)} &= \left(\begin{array}{cc|cc} \mathbb{1}_{2^{m-2}} & \mathbb{1}_{2^{m-2}} & & \\ \mathbb{1}_{2^{m-2}} & -\mathbb{1}_{2^{m-2}} & & \\ \hline & & \mathbb{1}_{2^{m-2}} & \mathbb{1}_{2^{m-2}} \\ & & \mathbb{1}_{2^{m-2}} & -\mathbb{1}_{2^{m-2}} \end{array}\right), \\
M_{2^m}^{(1)} &= \begin{pmatrix} H_2^{(st)} & & \\ & \ddots & \\ & & H_2^{(st)} \end{pmatrix}.
\end{aligned}$$

Bei jedem $M_{2^m}^{(i)}$ sind pro Spalte zwei Einträge in $\{1, -1\}$ und alle anderen Einträge gleich 0.

(b)

$$H_{2^m}^{(st)} = M_{2^m}^{(1)} \cdot \ldots \cdot M_{2^m}^{(m)}.$$

(c) Multipliziert man $A^{-1}(y)^{tr} \in M(2^m \times 1, \{1, -1\})$ von rechts direkt an $H_{2^m}^{(st)}$, so muss man sehr oft 2 Zahlen addieren, nämlich $(2^m - 1) \cdot 2^m$ mal ($2^m - 1$ = Anzahl der Additionen pro Zeile, 2^m = Anzahl der Zeilen).

Nutzt man (b), so geht es viel schneller, wegen der vielen Nullen. Man muss nur $m \cdot 2^m$ mal 2 Zahlen addieren (m = Anzahl der Matrizen, 2^m = Anzahl der Zeilen).

[Die Multiplikationen werden hier ignoriert.]

Beweis: (a) Definition.

(b) Beweis via Induktion.

$\underline{m = 1:}$ $\quad M_2^{(1)} = H_2^{(st)}$.

$\underline{m \to m+1:}$ Es ist $\mathbb{1}_{ab} = \mathbb{1}_a \otimes 1_b$. Für $1 \leq i \leq m$ ist

$$\begin{aligned}
M_{2^{m+1}}^{(i)} &= \mathbb{1}_{2^{m+1-i}} \otimes H_2^{(st)} \otimes \mathbb{1}_{2^{i-1}} \\
&\overset{\otimes \text{ ass.}}{=} \mathbb{1}_2 \otimes (\mathbb{1}_{2^{m-i}} \otimes H_2^{(st)} \otimes \mathbb{1}_{2^{i-1}}) \\
&= \mathbb{1}_2 \otimes M_{2^m}^{(i)}, \\
M_{2^{m+1}}^{(m+1)} &= H_2^{(st)} \otimes \mathbb{1}_{2^m},
\end{aligned}$$

Mit der Regel $(A \otimes B)(C \otimes D) = (A \cdot C) \otimes (B \cdot D)$ von 4.2 (iii) m mal angewandt erhält man

$$\begin{aligned} M_{2^{m+1}}^{(1)} \cdot \ldots \cdot M_{2^{m+1}}^{(m+1)} &= (\mathbb{1}_2 \cdot \ldots \cdot \mathbb{1}_2 \cdot H_2^{(st)}) \otimes (M_{2^m}^{(1)} \cdot \ldots \cdot M_{2^m}^{(m)} \cdot \mathbb{1}_{2^m}) \\ &= H_2^{(st)} \otimes (M_{2^m}^{(1)} \cdot \ldots \cdot M_{2^m}^{(m)}) \\ &= H_2^{(st)} \otimes H_{2^m}^{(st)} = H_{2^{m+1}}^{(st)} \end{aligned}$$

(c) Klar. □

Bemerkung 4.17 Der Vorteil an Schnelligkeit $\frac{2^m-1}{m}$ beim Dekodieren wächst schnell mit m. Aber die Informationsrate

$$\frac{\dim \mathcal{C}(H_{2^m}^{(st)})}{2^m} = \frac{m+1}{2^m}$$

fällt schnell mit m. Bei der Mariner '69 Mission war offenbar $m = 5$ der beste Kompromiß.

5 Reed-Muller-Codes

Bemerkung 5.1 Die Reed-Muller-Codes sind Verallgemeinerungen der Codes $\mathcal{C}(H_{2^m}^{(st)})$. Auch die Dekodierungsmethode in Lemma 4.14 (b) verallgemeinert sich.
Es gibt (mindestens) zwei Beschreibungen der Reed-Muller-Codes: Eine konkrete kommt gleich. Eine andere kommt am Ende von Kapitel 5 als Nachtrag. Sie ist scheinbar elegant, aber sie gibt wenig Kontrolle und Einsicht in die Reed-Muller-Codes.

Lemma 5.2 *Sei* $m \in \mathbb{N}$.
(a) Die Menge $\mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ *ist ein* $\mathbb{F}_2$*-Vektorraum und als solcher kanonisch isomorph zu* $\mathbb{F}_2^{2^m}$*: zuerst beachte man die Bijektion*

$$\begin{array}{rcl} \{0,1,...,2^m-1\} & \longrightarrow & \mathbb{F}_2^m \\ j = \sum_{k=1}^{m} j_k \cdot 2^{k-1} & \longmapsto & (j_m,...,j_1), \end{array}$$

es ist die Binärdarstellung der Zahlen $0,1,...,2^m-1$.
Daraus erhält man die folgenden Bijektionen,

$$\begin{array}{ccccc} \mathrm{Abb}(\mathbb{F}_2^m,\mathbb{F}_2) & \longrightarrow & \mathrm{Abb}(\{0,1,\ldots,2^m-1\},\mathbb{F}_2) & \longrightarrow & \mathbb{F}_2^{2^m} \\ (\widetilde{f}:\mathbb{F}_2^m\to\mathbb{F}_2) & \longmapsto & (f:\{0,1,...,2^m-1\}\to\mathbb{F}_2) & \longmapsto & (f(0),f(1),\ldots,f(2^m-1)) \\ & & \text{mit } f(j)=\widetilde{f}((j_m,...,j_1)) & & \end{array}$$

Sie sind $\mathbb{F}_2$*-Vektorraumisomorphismen.*
Daher hat der $\mathbb{F}_2$*-Vektorraum* $\mathrm{Abb}(\mathbb{F}_2^m,\mathbb{F}_2)$ *die Dimension* 2^m.

(b) (Definition) Für $k \in \{1,2,...,m\}$ *ist* $z_k \in \mathrm{Abb}(\mathbb{F}_2^m,\mathbb{F}_2)$ *die* k*-te Koordinatenfunktion*

$$z_k : \mathbb{F}_2^m \to \mathbb{F}_2, \quad (j_m,...,j_1) \mapsto j_{m+1-k}.$$

(Lemma)

$$z_k^2 = z_k.$$

(c)

$$\mathrm{Abb}(\mathbb{F}_2^m,\mathbb{F}_2) = \{\text{Polynome in } z_1,...,z_m\}.$$

Vorsicht: Hier sind $z_1,...,z_m$ *keine Variablen, sondern die oben gewählten Funktionen, mit der Relation* $z_k^2 = z_k$.
Eine $\mathbb{F}_2$*-Vektorraumbasis bilden die* 2^m *Monome* $z_{i_1}\cdot...\cdot z_{i_l}$ *mit* $0 \le l \le m$ *und* $i_1 < ... < i_l$ *(im Fall* $l=0$ *ist das Monom* $:=1$*).*

Beweis: (a) Dass die genannten Abbildungen bijektiv sind, ist klar.

Erinnerung an die Vektorraumstruktur auf $\mathrm{Abb}(X,K)$ mit $X =$ eine beliebige Menge und $K =$ ein Körper:

für $\lambda \in K,\ f \in \mathrm{Abb}(X, K),\ x \in X$ ist $(\lambda \cdot f)(x) := \lambda \cdot f(x)$,
für $f_1, f_2 \in \mathrm{Abb}(X, K),\ x \in X$ ist $(f_1 + f_2)(x) := f_1(x) + f_2(x)$,
also werden skalare Multiplikation und Addition über die Werte definiert.

Auch bei $\mathbb{F}_2^{2^m}$ werden skalare Multiplikation und Addition über die Werte definiert. Also ist die zweite Abbildung ein Vektorraumisomorphismus.
Die erste ist es sowieso.

(b) $z_k^2 = z_k$ gilt, denn die Werte sind in $\mathbb{F}_2$, und $0^2 = 0, 1^2 = 1$.

(c) Der Beweis hat sieben Schritte, zuerst eine Definition, dann lauter elementare Beobachtungen.

(i) **Definition:** Für $s \in \mathbb{F}_2^m$ ist $f_s \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ definiert durch

$$f_s := \prod_{k=1}^{m} (z_k + s_k + 1).$$

(ii) f_s erfüllt $f_s(t) = \begin{cases} 1 & \text{für } t = s, \\ 0 & \text{für } t \in \mathbb{F}_2^m - \{s\}. \end{cases}$

(iii) Jede Funktion $f \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ lässt sich als Linearkombination der f_s schreiben, nämlich

$$f = \sum_{s \in \mathbb{F}_2^m} f(s) \cdot f_s.$$

(iv) (Nicht relevant für das Folgende) Die f_s, $s \in \mathbb{F}_2^m$, sind ein Erzeugendensystem des $\mathbb{F}_2$-Vektorraums $\mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$. Ihre Anzahl ist gleich seiner Dimension, gleich 2^m. Also sind sie eine Basis.

(v) Die f_s sind schreibbar als Polynome in den z_k. Daher sind alle Elemente von $\mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ schreibbar als Polynome in den z_k.

(vi) Vorsicht: Hier werden nicht Polynome in abstrakten Variablen betrachtet, sondern in den Funktionen $z_1, ..., z_m$. Wegen (b) $z_k^2 = z_k$ können verschiedene Polynome die gleiche Abbildung in $\mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ geben.

Insbesondere lässt sich wegen (b) $z_k^2 = z_k$ jedes Monom auf ein Monom der Gestalt

$$z_{i_1} \cdot ... \cdot z_{i_l} \text{ mit } 0 \leq l \leq m \text{ und } i_1 < ... < i_l$$

reduzieren. Daher bilden diese Monome ein Erzeugendensystem des $\mathbb{F}_2$-Vektorraums $\mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$.

(vii) Wegen

$$\begin{aligned} |\{\text{diese Monome}\}| &= |\{\{i_1,...,i_l\} \mid 0 \le l \le m, i_1 < ... < i_l\}| \\ &= |\text{Potenzmenge von } \{1,...,m\}| \\ &= 2^m = \dim \text{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \end{aligned}$$

bilden sie eine Basis.

□

Definition 5.3 Sei $m \in \mathbb{N}$ und $r \in \{-1, 0, 1, ..., m\}$.
Der Reed-Muller-Code $\mathcal{R}(r,m) \subset \mathbb{F}_2^{2^m}$ ist definiert durch

$$\begin{array}{ccc} \{\text{Polynome in } z_1,...,z_m \text{ vom Grad} \le r\} & \subset & \text{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \\ \text{induzierte } \downarrow \text{ Bijektion} & & \text{Bijektion } \downarrow \text{ von 5.2 (a)} \\ \mathcal{R}(r,m) & \subset & \mathbb{F}_2^{2^m} \end{array}$$

Im Folgenden werden mit Hilfe der Bijektion von Lemma 5.2 (a) die Mengen $\text{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ und $\mathbb{F}_2^{2^m}$ identifiziert.

Satz 5.4

$$\mathcal{R}(1,m) = \mathcal{C}(H_{2^m}^{(st)}).$$

Also "sind" $1, z_1, ..., z_m$ eine $\mathbb{F}_2$-Basis von $\mathcal{C}(H_{2^m}^{(st)})$, insbesondere sind sie in $\mathcal{C}(H_{2^m}^{(st)})$. Tatsächlich "ist" z_k die k-te Zeile der Matrix G_m.

Erinnnerung: Nach 4.13 (b) ist $G_m^{erz} = \binom{1...1}{G_m}$ eine Erzeugermatrix von $\mathcal{C}(H_{2^m}^{(st)})$. Seine Zeilen "sind" also genau die Elemente $1, z_1, ..., z_m$ (in dieser Reihenfolge).

Beweis: Das Polynom 1 gibt bei der Identifikation von $\text{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ und $\mathbb{F}_2^{2^m}$ die Zeile $(1, ..., 1)$.
Es reicht daher zu zeigen, dass z_k die k-te Zeile von G_m ist.
Erinnerung an 4.11 (a):

$$G_1 := (0\ 1) \quad , \quad G_{m+1} := \left(\begin{array}{c|c} 0\ldots0 & 1\ldots1 \\ \hline G_m & G_m \end{array}\right),$$

$$\text{also zum Beispiel } G_2 = \left(\begin{array}{c|c} 00 & 11 \\ \hline 01 & 01 \end{array}\right) \quad , \quad G_3 = \left(\begin{array}{c|c} 0000 & 1111 \\ \hline 0011 & 0011 \\ 0101 & 0101 \end{array}\right)$$

Erinnerung an 4.11 (b) und 5.2 (b): Sei $j \in \{0, 1, ..., 2^m - 1\}$, $j = \sum_{k=1}^m j_k \cdot 2^{k-1}$, also ist $(j_m, ..., j_1)$ die Binärdarstellung von j.

Die $(j+1)$-te Spalte von G_m ist $\begin{pmatrix} j_m \\ \vdots \\ j_1 \end{pmatrix}$.

Unter den kanonischen Bijektionen hat man daher

$$\begin{aligned} k\text{-te Zeile von } G_m &\sim \text{die Abbildung in } \mathrm{Abb}(\{0,1,...,2^m-1\},\mathbb{F}_2) \text{ mit} \\ & \quad j \mapsto j_{m+1-k} \\ &\sim \text{die Abbildung } z_k \end{aligned}$$

□

Satz 5.5 *a)*

$$\begin{aligned} \mathcal{R}(-1,m) &= \{(0,\ldots,0)\}\text{“}=''\{0\} = \{\text{Polynom } 0\}, \\ \mathcal{R}(0,m) &= \{(0,\ldots,0),(1,\ldots,1)\}\text{“}=''\{\text{Polynome 0 und 1}\}, \\ \mathcal{R}(m,m) &= \mathbb{F}_2^{2^m}\text{“}=''\mathit{Abb}(\mathbb{F}_2^m,\mathbb{F}_2) = \{\text{alle Polynome}\}. \end{aligned}$$

b) $\mathcal{R}(r,m)$ ist ein linearer Code, ein $[2^m, \binom{m}{0}+\binom{m}{1}+\cdots+\binom{m}{r}, 2^{m-r}]$- Code. (Erinnerung: [Wortlänge, Dimension, minimaler Hamming-Abstand].)

Beweis:
(a) $\mathcal{R}(-1,m) = \{0\}$: Das einzige Polynom vom Grad ≤ -1 ist das Nullpolynom.
$\mathcal{R}(0,m) = \{0,1\}$: Die einzigen Polynome vom Grad ≤ 0 sind die konstanten Polynome 0 und 1.
$\mathcal{R}(m,m) = \mathrm{Abb}(\mathbb{F}_2^m,\mathbb{F}_2)$: Jede Abbildung ist Linearkombination der Monome $z_{i_1}\cdot ...z_{i_l}$ mit $0 \leq l \leq m$.

(b) Linearität des Codes: ok.
Wortlänge $= 2^m$: ok.
Dimension $= \binom{m}{0}+\binom{m}{1}+\cdots+\binom{m}{r}$:
Für ein festes l mit $0 \leq l \leq m$ gilt

$$\begin{aligned} & |\{\text{Monome } z_{i_1}\cdot ...\cdot z_{i_l} \text{ mit } i_1 < ... < i_l\}| \\ = \; & |\{\text{Teilmengen von}\{1,...,m\} \text{ mit } l \text{ Elementen }\}| = \binom{m}{l}. \end{aligned}$$

Die $z_{i_1}\cdot ...\cdot z_{i_l}$ mit $0 \leq l \leq r$ und $i_1 < ... < i_l$ sind eine Basis von $\mathcal{R}(r,m)$.
$d(\mathcal{R}(r,m)) = 2^{m-r}$:

$$d(\mathcal{R}(r,m)) \overset{\text{linear}}{=} \min(w(f) \mid f \text{ Polynom vom Grad } \leq r).$$

Betrachte $f = z_{i_1}\cdot ...\cdot z_{i_r}$ mit $i_1 < ... < i_r$.

$$w(f) = |\{x \in \mathbb{F}_2^m \mid f(x) = 1\}| = |\{x \in \mathbb{F}_2^m \mid x_{i_1} = ... = x_{i_r} = 1\}| = 2^{m-r},$$

also ist $d(\mathcal{R}(r,m)) \leq 2^{m-r}$.

1. Beweis von $d(\mathcal{R}(r,m)) \geq 2^{m-r}$: In den Bemerkungen 5.6 (iv)–(vii), trickreich. Dieselben Tricks werden auch für die Dekodierung in Satz 5.7 gebraucht.

2. Beweis von $d(\mathcal{R}(r,m)) \geq 2^{m-r}$: Am Ende von Kapitel 5 in Bemerkung 5.12, eleganter. □

Notationen/Bemerkungen 5.6 Sei $m \in \mathbb{N}$.
(i)–(iii) sind Notationen,
(iv)–(vii) ist der 1. Beweis von $d(\mathcal{R}(r,m)) \geq 2^{m-r}$,
(viii)–(x) sind Vorbereitungen für Satz 5.7 (=Dekodierung).

(i) Sei $f \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$. Der Träger = Support von f ist

$$\mathrm{supp}(f) := \{x \in \mathbb{F}_2^m \mid f(x) = 1\}.$$

Wegen

$$f(x) = \begin{cases} 1 & x \in \mathrm{supp}(f) \\ 0 & x \notin \mathrm{supp}(f) \end{cases}$$

bestimmt $\mathrm{supp}(f)$ die Abbildung f. Es ist

$$w(f) = |\mathrm{supp}(f)|.$$

(ii) $M := \{1, ..., m\}$.
Sei $I \subset M$, $\quad I^c := M - I$ ($c \sim$ complementary set).
Sei $s \in \mathbb{F}_2^m, s = (s_1, \ldots s_m)$. Definiere das Polynom

$$P_{I,s} := \prod_{i \in I} (z_i + s_i + 1) \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2).$$

Es ist

$$P_{I,(1,\ldots,1)} = \prod_{i \in I} z_i$$

ein Monom. Es ist

$$\begin{aligned} \mathrm{supp}\, P_{I,s} &= \{x \in \mathbb{F}_2^m \mid P_{I,s}(x) = 1\} \\ &= \{x \in \mathbb{F}_2^m \mid \forall\ i \in I\ x_i = s_i\} \\ &= \{\text{die } x \in \mathbb{F}_2^m, \text{ die auf } I \text{ so aussehen wie } s\}. \end{aligned}$$

(iii)

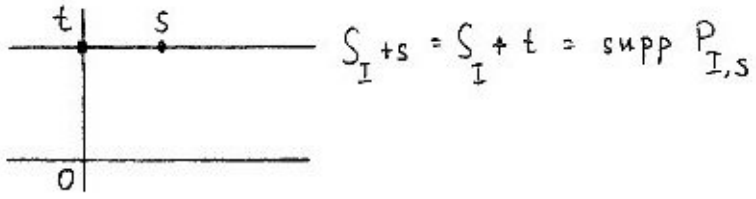
$$S_I := \mathrm{supp}\, P_{I,0} = \{x \in \mathbb{F}_2^m \mid \forall\ i \in I\ x_i = 0\}$$

ist ein Untervektorraum der Dimension $m - |I|$ von $\mathbb{F}_2^m$. Es ist

$$\mathrm{supp}\, P_{I,s} = S_I + s = \{x + s \mid x \in S_I\},$$

also ist $\operatorname{supp} P_{I,s}$ ein affiner Unterraum der Dimension $m - |I|$ von $\mathbb{F}_2^m$.
Es ist

$$\begin{aligned} P_{I,s} = P_{I,t} &\iff \operatorname{supp} P_{I,s} = \operatorname{supp} P_{I,t} \\ &\iff S_I + s = S_I + t \\ &\iff s \text{ und } t \text{ sehen auf } I \text{ gleich aus ,} \\ &\quad \text{d.h. } \forall\ i \in I\ s_i = t_i \\ &\iff s - t \in S_I \\ &\iff t \in S_I + s. \end{aligned}$$



Es gilt: Bei I und s wie oben gibt es ein eindeutiges $t \in S_{I^c}$ mit $P_{I,s} = P_{I,t}$, nämlich

$$t_i = \begin{cases} s_i & \text{für } i \in I \\ 0 & \text{für } i \notin I \end{cases}$$

Es gilt

$$\mathbb{F}_2^m = \dot{\bigcup}_{t \in S_{I^c}} (S_I + t).$$

(iv) Seien $I, J \subset M$ und $s, t \in \mathbb{F}_2^m$.

$$\begin{aligned} \operatorname{supp}(P_{I,s} \cdot P_{J,t}) &= \{x \in \mathbb{F}_2^m \mid P_{I,s}(x) \cdot P_{J,t}(x) = 1\} \\ &= \{x \in \mathbb{F}_2^m \mid P_{I,s}(x) = 1 = P_{J,t}(x)\} \\ &= \operatorname{supp} P_{I,s} \cap \operatorname{supp} P_{J,t} \\ &= (S_I + s) \cap (S_J + t). \end{aligned}$$

1. Fall, $= \emptyset$: Das gilt dann, wenn $\exists\ i \in I \cap J$ mit $s_i \neq t_i$.

2. Fall, $\neq \emptyset$: Das gilt dann, wenn $\forall i \in I \cap J\ s_i = t_i$. Dann gibt es ein $r \in (S_I + s) \cap (S_J + t)$, und dann ist

$$\operatorname{supp}(P_{I,s} \cdot P_{J,t}) = S_I \cap S_J + r = S_{I \cup J} + r.$$

Es ist

$$|\operatorname{supp}(P_{I,s} \cdot P_{J,t})| = \begin{cases} 0 & \text{im 1. Fall,} \\ 2^{m-|I \cup J|} & \text{im 2. Fall.} \end{cases}$$

(v) **Behauptung:** Seien $I, J \subset M$ mit $|I| \leq |J|$ und $s, t \in \mathbb{F}_2^m$. Dann gilt

$$|(S_I + s) \cap (S_{J^c} + t)| \begin{cases} = 1 & \text{falls } I = J, \\ \text{gerade} & \text{sonst.} \end{cases}$$

Beweis: Fall $I = J$:

$$(S_I + s) \cap (S_{I^c} + t) = \{\widetilde{t}\} \quad \text{mit} \quad \begin{array}{l} \widetilde{t}_i = s_i \text{ für } i \in I, \\ \widetilde{t}_i = t_i \text{ für } i \notin I. \end{array}$$

Fall $I \neq J$ und $(S_I + s) \cap (S_{J^c} + t) = \emptyset$: Dann ist $|...| = 0$ gerade.
Fall $I \neq J$ und $(S_I + s) \cap (S_{J^c} + t) \neq \emptyset$: Dann ist nach (iv)

$$|(S_I + s) \cap (S_{J^c} + t)| = 2^{m-|I \cup J^c|}.$$

Wegen $I \neq J$ und $|I| \leq |J|$ ist $I \cup J^c \subsetneq M$ und $|I \cup J^c| < m$. Also ist dann $2^{m-|I\cup J^c}$ gerade. □

(vi) Seien $f_1, ..., f_l \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$, sei $T \subset \mathbb{F}_2^m$.
Behauptung:

$$|\operatorname{supp}(f_1 + ... + f_l) \cap T| \equiv \sum_{i=1}^{l} |\operatorname{supp}(f_i) \cap T| \qquad \text{mod } 2.$$

Beweis: 1. Reduktion: Es reicht, $l = 2$ zu betrachten, denn dann folgt der allgemeine Fall induktiv.
2. Reduktion: Es reicht, eine Menge $T = \{t\}$ zu betrachten.

$$\begin{array}{rl} & |\operatorname{supp}(f_1 + f_2) \cap \{t\}| \equiv 1 \qquad \text{mod } 2 \\ \iff & t \in \operatorname{supp}(f_1 + f_2) \\ \iff & (f_1 + f_2)(t) = 1 \\ \iff & (f_1(t) = 0 \text{ und } f_2(t) = 1) \text{ oder } (f_1(t) = 1 \text{ und } f_2(t) = 0) \\ \iff & \displaystyle\sum_{i=1}^{2} |\operatorname{supp}(f_i) \cap \{t\}| \equiv 1 \qquad \text{mod } 2. \end{array}$$

□

(vii) Sei $J \subset M$, $r := |J| \geq 0$. Dann ist

$$P_{J,(1,...,1)} = \prod_{j \in J} z_j$$

ein Monom (im Fall $J = \emptyset$ ist es gleich 1) mit

$$\begin{array}{rcl} \operatorname{supp} P_{J,(1,...,1)} & = & S_J + (1, ..., 1), \\ \text{also } w(P_{J,(1,...,1)}) & = & |S_J + (1, ..., 1)| = 2^{m-r}. \end{array}$$

Betrachte nun ein "gestörtes" Polynom

$$f = P_{J,(1,...,1)} + \sum_{I \subset M,\ |I| \leq r,\ I \neq J} m_I \cdot P_{I,(1,...,1)}$$

mit beliebigen $m_I \in \{0,1\}$. Das Polynom f hat Grad r (nicht Grad $< r$), weil es das Monom $P_{J,(1,\ldots,1)}$ enthält.

Behauptung 1:

$$w(f) \stackrel{(i)}{=} |\operatorname{supp}(f)| \stackrel{!}{\geq} 2^{m-r}.$$

Beweis:

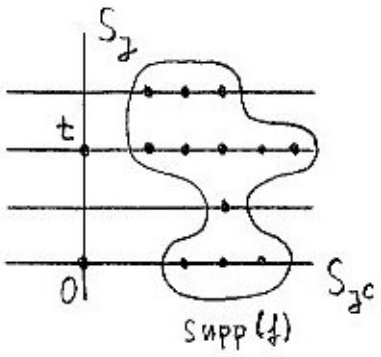
$$\begin{aligned} \mathbb{F}_2^m &= \dot{\bigcup}_{t \in S_J} (S_{J^c} + t), \\ \operatorname{supp}(f) &= \dot{\bigcup}_{t \in S_J} \operatorname{supp}(f) \cap (S_{J^c} + t). \end{aligned}$$

Mit der Behauptung 2 unten folgt nun

$$|\operatorname{supp}(f)| \geq \sum_{t \in S_J} 1 = |S_J| = 2^{m-r}.$$

□

Behauptung 2: Für alle $t \in S_J$ ist $\operatorname{supp}(f) \cap (S_{J^c} + t) \neq \emptyset$, und es ist sogar $|\operatorname{supp}(f) \cap (S_{J^c} + t)|$ ungerade (aber oben wird nur $|...| \geq 1$ gebraucht).



Beweis: Wegen (vi) und (v) ist modulo 2

$$\begin{aligned} |\operatorname{supp}(f) \cap (S_{J^c} + t)| &\equiv |\operatorname{supp}(P_{J,(1,\ldots,1)}) \cap (S_{J^c+t})| \\ &\quad + \sum_{I \subset M,\ |I| \leq r,\ I \neq J,\ m_I = 1} |\operatorname{supp}(P_{I,(1,\ldots,1)}) \cap (S_{J^c+t})| \\ &\equiv 1 + \sum_{I \subset M,\ |I| \leq r,\ I \neq J,\ m_I = 1} 0 \\ &\equiv 1 \mod 2. \end{aligned}$$

□

Jedes Polynom $f \in \mathcal{R}(r,m) - \{0\}$ kann man als ein gestörtes Polynom (mit $\deg(f)$ statt r) interpretieren. Aus der Behauptung 1 folgt

$$w(f) = |\operatorname{supp}(f)| \geq 2^{m-|\deg(f)|} \geq 2^{m-r}.$$

Also ist $d(\mathcal{R}(r,m)) \geq 2^{m-r}$. Der 1. Beweis von Satz 5.5 (b) ist fertig.

(viii) Definiere eine Paarung

$$\begin{aligned} \prec,\succ \quad &: \quad \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \times \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \to \mathbb{F}_2 \\ \prec f, g \succ \quad &:= \quad \sum_{x \in \mathbb{F}_2^m} f(x) \cdot g(x) \in \mathbb{F}_2 \\ \text{Beobachtung:} \qquad &\overset{!}{=} \quad (|\operatorname{supp}(f \cdot g)| \mod 2) \in \mathbb{F}_2. \end{aligned}$$

Daraus und aus (iv) und (v) folgt die nächste Behauptung.

Behauptung: Seien $I, J \subset M$ mit $|I| \leq |J|$, und seien $s, t \in \mathbb{F}_2^m$. Dann ist

$$\prec P_{I,s}, P_{J^c,t} \succ = \begin{cases} 1 & \text{für } I = J, \\ 0 & \text{sonst.} \end{cases}$$

(ix) Sei $r \in \{0, 1, \ldots, m\}$ und

$$f = \sum_{I \subset M,\ |I| \leq r} m_I \cdot P_{I,(1,\ldots,1)} \in \mathcal{R}(r,m) \qquad (\text{mit } m_I \in \mathbb{F}_2 \text{ beliebig}).$$

Dann gilt für $J \subset M$ mit $|J| = r$ und für beliebiges $t \in \mathbb{F}_2^m$

$$\prec f, P_{J^c,t} \succ = \sum_{I \subset M,\ |I| \leq r} m_I \cdot \prec P_{I,(1,\ldots,1)}, P_{J^c,t} \succ \overset{(viii)}{=} m_J.$$

So kann man den Koeffizienten m_J von f berechnen.

(x) **Behauptung:** Sei $f \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ und sei $J \subset M$. Dann ist

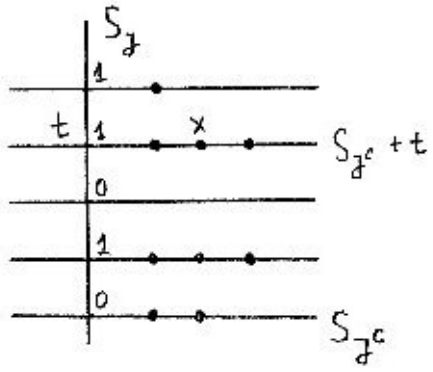
$$w(f) \overset{(i)}{=} |\operatorname{supp}(f)| \overset{!}{\geq} |\{t \in S_J \mid \prec f, P_{J^c,t} \succ = 1\}|.$$

Beweis:

$$\begin{aligned} |\operatorname{supp}(f) \cap (S_{J^c} + t)| \mod 2 \quad &\overset{(viii)}{=} \quad \prec f, P_{J^c,t} \succ = 1 \\ &\Longrightarrow \quad \exists\, x \in \operatorname{supp}(f) \cap (S_{J^c} + t). \end{aligned}$$

Es folgt sogar: $|...|$ ungerade $\Longleftrightarrow \prec f, P_{J^c,t} \succ = 1$.
Man erhält eine injektive Abbildung

$$\begin{aligned} \{t \in S_J \mid \prec f, P_{J^c,t} \succ = 1\} \quad &\longrightarrow \quad \dot{\bigcup}_{t \in S_J} (\operatorname{supp}(f) \cap (S_{J^c} + t)) = \operatorname{supp}(f) \\ t \quad &\longmapsto \quad \text{solch ein } x \end{aligned}$$



□

Satz 5.7 *(Dekodierung von Reed-Muller-Codes)*
Sei $m \in \mathbb{N}$ *und* $r \in \{0, 1, \ldots, m\}$,

$$\begin{aligned} f &= \sum_{I\subset M,\ |I|\le r} m_I P_{I,(1,\ldots,1)} \in \mathcal{R}(r,m) \quad \text{ein gesendetes Wort,} \\ g &= f + e \in Abb\ (\mathbb{F}_2^m, \mathbb{F}_2) \quad \text{das empfangene Wort } (e \text{ für "error"}) \\ \text{mit} \quad & w(e) < 2^{m-r-1}. \end{aligned}$$

Dann bestimmt man, ausgehend von g*, einen Koeffizienten* m_I *von* f *für ein* I *mit* $|I| = r$ *folgendermaßen:*
Man berechnet alle $\prec g, P_{I^c,t} \succ \in \mathbb{F}_2$ *für* $t \in S_I = \mathrm{supp}(P_{I,0})$ *[Untervektorraum,* $|S_I| = 2^{m-r}$*]. Mehr als die Hälfte hat den Wert* m_I*. "Mehrheitsentscheid" liefert* m_I*.*
Wenn alle m_I *für* I *mit* $|I| = r$ *berechnet sind, macht man folgendermaßen weiter: Man arbeitet mit*

$$\widetilde{f} := f - \sum_{I\subset M,\ |I|=r} m_I P_{I,(1,\ldots,1)} = \sum_{I\subset M, |I|<r} m_I P_{I,(1,\ldots,1)}$$

(ohne es zu kennen) statt f*, als neuem gesendeten Wort, und mit*

$$\widetilde{g} := g - \sum_{I\subset M} m_I P_{I,0}$$

statt g *als neuem empfangenen Wort (das man kennt) und mit* $r-1$ *statt* r*.*

Beweis:
Nach Bemerkung 5.6 (ix) ist $\prec f, P_{I^c,t} \succ = m_I \ \forall\ t \in S_I$ (sogar $\forall\ t \in \mathbb{F}_2^m$).
Nach Bemerkung 5.6 (x) ist $\prec e, P_{I^c,t} \succ = 1$ für höchstens $w(e)$ Werte von $t \in S_I$.
Daher sind mindestens $|S_I| - w(e) > 2^{m-r} - 2^{m-r-1} = 2^{m-r-1}$ der 2^{m-r} Werte $\prec g, P_{I^c,t} \succ = \prec f + e, P_{I^c,t} \succ$ gleich zu m_I. □

Bemerkung 5.8 Vergleich mit der Dekodierung von $\mathcal{C}(H_{2^m}^{(st)})$ Lemma 4.14: Bei $\mathcal{R}(r,m)$ muss man in Satz 5.7 2^{m-r} Produkte von Zeilenvektoren der Länge 2^m berechnen, bei $\mathcal{C}(H_{2^m}^{(st)})$ 2^m Produkte.
Aber in Lemma 4.14 sind die Koeffizienten in $\{-1,1\}$ und die Werte in $\mathbb{Z}$, und am Ende ist das gesendete Wort bekannt. In Satz 5.7 sind die Koeffizienten und Werte in $\mathbb{F}_2$, und am Ende ist nur ein Koeffizient m_I bestimmt.
In Satz 5.7 braucht man für das ganze gesendeten Wort

$$\binom{m}{r}\cdot 2^{m-r}\cdot(2^m-1)+\binom{m}{r-1}2^{m\cdot(r-1)}\cdot(2^m-1)+\cdots+\binom{m}{0}2^{m-0}\cdot(2^m-1)$$

Additionen (hier ist $\binom{m}{r}=$ Anzahl der $I\subset M$ mit$|I|=r$,
$2^{m-r}=|S_I|$,
$2^m-1=$ Anzahl der Additionen bei einem Skalarprodukt $\prec g, P_{I^c,t}\succ$).
[Wahrscheinlich kann man das verbessern, aber so etwas elegantes wie Satz 4.16 sehe ich nicht.]

Jetzt als Nachtrag ein anderer Zugang zu den Reed-Muller-Codes:

Definition 5.9 Es seien $C_1, C_2 \subset \mathbb{F}_q^n$ zwei Codes (nicht notwendig linear). Ein Code $(C_1 \mid C_2) \subset \mathbb{F}_q^{2n}$ ist definiert durch

$$(C_1 \mid C_2) := \{(u, u+v) \mid u \in C_1, v \in C_2\} \subset \mathbb{F}_q^{2n}.$$

Diese Konstruktion heißt $(u, u+v)$-Konstruktion.
[Vorsicht: i.a. $(C_2 \mid C_1) \neq (C_1 \mid C_2)$]

Satz 5.10 *Es seien* $C_1, C_2 \subset \mathbb{F}_q^n$

(a)

$$(C_1 \mid C_2) \subset \mathbb{F}_q^{2n}, \qquad |(C_1 \mid C_2)| = |C_1|\cdot|C_2|)$$
$$d((C_1 \mid C_2)) = \min(2d(C_1), d(C_2))$$

also ist $(C_1 \mid C_2)$ *ein* $(2n, |C_1|\cdot|C_2|, \min(2d(C_1), d(C_2))$ *- Code.*

(b) C_1 *und* C_2 *seien lineare Codes.*

(i) Dann ist (C_1, C_2) *ein linearer* $[2n,$ *dim* C_1 $+$ *dim* C_2, *min* $(2d(C_1), d(C_2))]$ *- Code.*

(ii) Sind G_1 *und* G_2 *Erzeugermatrizen von* C_1 *und* C_2, *so ist*

$$\begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$$

eine Erzeugermatrix von $(C_1 \mid C_2)$.

Beweis:
(a) Nur $d((C_1 \mid C_2)) = \min(2d(C_1), d(C_2))$ ist nicht trivial.

" $\leq$ " : Seien $u_1, u_2 \in C_1,\ v_1, v_2 \in C_2$.

$$\begin{aligned} d_H((u_1, u_1+v_1), (u_2, u_2+v_1)) &= 2d_H(u_1, u_2) \\ d_H(u_1, u_1+v_1), (u_1, u_1+v_2)) &= d_H(v_1, v_2) \end{aligned}$$

" $\geq$ " : Seien $u_1, u_2 \in C_1,\ v_1, v_2 \in C_2$

$$\begin{aligned} & d_H((u_1, u_1+v_1), (u_2, u_2+v_2)) \\ = & \begin{cases} 2d_H(u_1, u_2) & \text{falls } v_1 = v_2 \\ d_H(u_1, u_2) + d_H(u_1+v_1, u_2+v_2) & \text{falls } v_1 \neq v_2 \end{cases} \end{aligned}$$

Im zweiten Fall schätzt man mit der Dreiecksungleichung ab

$$d_H(u_1+v_1, u_1+v_2) \leq d_H(u_1+v_1, u_2+v_2) + d_H(u_1+v_2, u_2+v_2)$$

und erhält

$$\begin{aligned} & d_H((u_1, u_1+v_1), (u_2, u_2+v_2)) \\ = \ & d_H(u_1, u_2) + d_H(u_1+v_1, u_2+v_2) \\ \geq \ & d_H(u_1, u_2) + d_H(u_1+v_1, u_1+v_2) - d_H(u_1+v_2, u_2+v_2) \\ = \ & d_H(u_1, u_2) + d_H(v_1, v_2) - d_H(u_1, u_2) \\ = \ & d_H(v_1, v_2). \end{aligned}$$

(b)

(i) Linear ist klar, der Rest folgt aus a).

(ii) aus der Definition von $(C_1 \mid C_2)$; weil beide Codes linear sind, ist $u = 0 \in C_1$ und $v = 0 \in C_2$.

□

Satz 5.11 *Die Reed-Muller-Codes $\mathcal{R}(r, m)$ für $m \in \mathbb{N}, r \in \{-1, 0, \ldots, m\}$ erfüllen:*

(α) $\mathcal{R}(-1, m) = \{0\} \subset \mathbb{F}_2^{2^m}$

(β) $\mathcal{R}(m, m) = \mathbb{F}_2^{2^m}$

(γ) $\mathcal{R}(r, m) = (\mathcal{R}(r, m-1) \mid \mathcal{R}(r-1, m-1))$ *für* $0 \leq r \leq m-1$.

Dadurch sind sie eindeutig bestimmt. Also kann man sie durch diese Eigenschaften definieren. Das ist der zweite elegantere Zugang zu den Reed-Muller-Codes.

Beweis:
(α) und (β) folgen aus Satz 5.5a)

(γ) Wegen der $(u, u+v)$-Konstruktion ist es interessant, wie sich die Einbettungen

$$\begin{aligned} \chi_1 : \mathbb{F}_2^{2^{m-1}} &\hookrightarrow \mathbb{F}_2^{2^m} \quad \text{und} \\ u &\mapsto (u, u) \\ \chi_2 : \mathbb{F}_2^{2^{m-1}} &\hookrightarrow \mathbb{F}_2^{2^m} \\ v &\mapsto (0, v) \end{aligned}$$

übersetzen, wenn man mit den Bijektionen von Lemma 5.2 (a) von den Räumen $\mathbb{F}_2^{2^{m-1}}$ und $\mathbb{F}_2^{2^m}$ zu den Räumen $\mathrm{Abb}(\mathbb{F}_2^{m-1}, \mathbb{F}_2)$ und $\mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ übergeht.

Behauptung: χ_1 geht über in φ_1, und χ_2 geht über in φ_2, mit

$$\begin{aligned} \varphi_1 : \mathrm{Abb}(\mathbb{F}_2^{m-1}, \mathbb{F}_2) &\to \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \\ f(z_1, ..., z_{m-1}) &\mapsto f(z_2, ..., z_m), \\ \varphi_2 : \mathrm{Abb}(\mathbb{F}_2^{m-1}, \mathbb{F}_2) &\to \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \\ f(z_1, ..., z_{m-1}) &\mapsto z_1 \cdot f(z_2, ..., z_m) = z_1 \cdot \varphi_1(f). \end{aligned}$$

Beweis: Die Funktion $z_{k+1} \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ bildet $(j_m, j_{m-1}, ..., j_1)$ auf j_{m-2+k} ab, und die Funktion $z_k \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ bildet $(j_{m-1}, ..., j_1)$ auf j_{m-2+k} ab. Daraus folgt die Behauptung für φ_1 und χ_1.
Die Funktion $z_1 \in \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2)$ bildet $(j_m, j_{m-1}, ..., j_1)$ auf j_m ab. Daher entspricht sie unter der Bijektion von Lemma 5.2 (a) dem Tupel $(0, ..., 0, 1, ..., 1)$ (mit 2^{m-1} mal 0 und 2^{m-1} mal 1). Und eine Abbildung $z_1 \cdot \widetilde{f}(z_1, ..., z_m)$ entspricht dem Tupel $(0, ..., 0, f(2^{m-1}), ..., f(2^m - 1))$. Daraus folgt die Behauptung für φ_2 und χ_2. ($\square$)

Ein Polynom in $\mathcal{R}(r, m)$ lässt sich nun auf eindeutige Weise schreiben als $\varphi_1(f) + z_1 \cdot \varphi_1(g)$ mit $f \in \mathcal{R}(r, m-1), g \in \mathcal{R}(r-1, m-1)$.

$$\begin{aligned} \mathrm{Abb}(\mathbb{F}_2^{m-1}, \mathbb{F}_2) &\to \mathbb{F}_2^{2^{m-1}} \\ f &\to u \\ g &\to v \end{aligned}$$

$$\begin{aligned} \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) &\to \mathbb{F}_2^{2^m} \\ \varphi_1(f) &\to (u, u) \\ z_1 \cdot \varphi_1(g) &\to (0, v) \\ \varphi_1(f) + z_1 \cdot \varphi_1(g) &\to (u, u+v) \end{aligned}$$

$\square$

Bemerkung 5.12 Aus Satz 5.10 und Satz 5.11 folgt $d(\mathcal{R}(r,m)) = 2^{m-r}$ für $r \in \{0,1,\ldots,m\}$.

Beweis: Für $\mathcal{R}(m,m)$ ist $d(\mathcal{R}(m,m)) = 1 = 2^{m-m}$ klar.
Für $\mathcal{R}(0,m)$ ist $\mathcal{R}(0,m) = \{\{(0,...,0),(1,...,1)\}$ und $d(\mathcal{R}(0,m)) = 2^{m-0}$.
Induktion nach m für $1 \leq r \leq m-1$: Im Induktionsschritt gehen die oben behandelten Werte $d(\mathcal{R}(m-1,m-1))$ und $d(\mathcal{R}(0,m-1)$ ein.
Induktionsschritt $m-1 \to m$:

$$\begin{aligned} d(\mathcal{R}(r,m)) &= \min(2d(\mathcal{R}(r,m-1)), d(\mathcal{R}(r-1,m-1)) \\ &= \min\,(2 \cdot 2^{(m-1)-r}, 2^{(m-1)-(r-1)}) \\ &= \min\,(2^{m-r}, 2^{m-r}) = 2^{m-r}. \end{aligned}$$

□

6 Endliche Körper, Polynome

Dieses Kapitel ist ein Schnellkurs über endliche Körper und Polynome. Es ist Algebra, nicht Kodierungstheorie. Ich werde es in der Vorlesung sehr schnell abhandeln.
Der Inhalt dieses Kapitels wird nicht für sich abgefragt im Rahmen von Prüfungen zur Kodierungstheorie. Insbesondere muss man die Beweise nicht lesen. Wer die Aussagen schon aus einer Algebra-Vorlesung kennt, muss das ganze Kapitel nicht lesen.
Aber viele der Aussagen werden implizit ab Kapitel 7 gebraucht. Und in dieser impliziten Form, nämlich bei Anwendungen, können sie auch geprüft werden.

Satz 6.1 *Zu jeder Primzahlpotenz $q = p^n$ (mit p Primzahl und $n \in \mathbb{N}$) gibt es genau einen Körper mit q Elementen.*
(Definition:) Er heißt $\mathbb{F}_q$.
Es gibt keine anderen endlichen Körper.

Hauptziel von Kapitel 6: diesen Satz beweisen und die $\mathbb{F}_q$ konstruieren.

Definition 6.2 (=Erinnerung)
Eine *Gruppe* ist eine Menge G zusammen mit einer Verknüpfung

$$\circ : G \times G \to G, \quad (a, b) \mapsto a \circ b$$

mit den Eigenschaften:

(a) Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c)$.

(b) Einselement: es gibt ein Element $e \in G$ mit $a \circ e = e \circ a = a$.

(c) Inverses: Für alle $a \in G$ gibt es ein "Inverses" $b \in G$ mit $a \circ b = b \circ a = e$.

Eine Gruppe heißt *abelsch* (oder *kommutativ*), falls gilt:

(d) Kommutativität: $a \circ b = b \circ a$.

Bemerkungen 6.3 (i) Das Einselement e ist eindeutig, $e = e \circ e' = e'$.

Das Inverse von $a \in G$ auch; es heißt a^{-1}, falls $\circ = \cdot$ = Multiplikation, und $-a$, falls $\circ = +$ = Addition.

(ii) Bei $\circ = \cdot$ = Multiplikation läßt man das Produktzeichen oft ganz weg.

Bei $\circ = +$ = Addition ist die Gruppe abelsch (nach Konvention). Dann wird e mit 0 bezeichnet und *Nullelement* genannt.

(iii) Beispiele abelsche Gruppen sind $(\mathbb{Z}^n, +)$, $(\mathbb{Q}^n, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{C}^n, +)$ (für $n \in \mathbb{N}$) und $(\mathbb{Q}^+, \cdot)$, $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{C} - \{0\}, \cdot)$.

Nicht abelsche Gruppen sind die symmetrischen Gruppen $(S_n, \circ)$ (für $n \geq 3$) und die Gruppen $(GL(n, \mathbb{R}), \cdot)$ (für $n \geq 2$).

(iv) Fast immer spricht man von der Gruppe G und meint die Gruppe $(G, \circ)$.

Definition 6.4 (=Erinnerung)

(a) Ein *Ring* ist eine abelsche Gruppe $(R, +)$ zusammen mit einer Multiplikation $\cdot : R \times R \to R$ mit den Eigenschaften:

(A) Assoziativität: $(ab)c = a(bc)$.

(B) Distributivgesetze: $(a + b)c = ac + bc$ und $a(b + c) = ab + ac$.

(b) Ein *kommutativer Ring* ist ein Ring $(R, +, \cdot)$ mit

(C) Kommutativität: $ab = ba$.

(c) Ein *Ring mit Eins* ist ein Ring $(R, +, \cdot)$ mit einem *Einselement* 1_R mit

(D) $1_R \cdot a = a \cdot 1_R = a$.

(d) Ein *Körper* ist ein kommutativer Ring mit Eins, so daß $(R - \{0\}, \cdot)$ eine (natürlich abelsche) Gruppe ist.

Bemerkungen 6.5 (i) Man spricht vom Ring R und meint $(R, +, \cdot)$.

(ii) Beispiele für nicht kommutative Ringe mit Eins sind die Mengen $M(n \times n, \mathbb{R})$ (für $n \geq 2$) von $n \times n$-Matrizen mit reellen Einträgen.

Beispiele für kommutative Ringe ohne Eins sind die Mengen

$$m\mathbb{Z} := \{m \cdot k \mid k \in \mathbb{Z}\}$$

für $m \in \mathbb{N}$, $m \geq 2$.

Ein Beispiel eines kommutativen Ringes mit Eins ist $\mathbb{Z}$.

Beispiele für Körper sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(iii) Ist R ein (kommutativer) Ring [mit Eins], so ist auch der Polynomring

$$R[t] := \{a_0 + a_1 t + ... + a_n t^n \mid n \in \mathbb{N}, a_0, ..., a_n \in R\}$$

ein (kommutativer) Ring [mit Eins], mit der "offensichtlichen" Addition und Multiplikation.

(iv) In einem Ring ist $0 \cdot a = 0 = a \cdot 0$, denn

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a, \text{ etc..}$$

(v) In einem Ring mit Eins ist $1_R \neq 0$, falls $R \neq \{0\}$, denn für $a \neq 0$ ist

$$1_R \cdot a = a \neq 0 = 0 \cdot a.$$

(vi) In einem Körper ist $a \cdot b \neq 0$, falls $a \neq 0$ und $b \neq 0$, denn

$$a^{-1}(ab) = (a^{-1}a)b = 1_R \cdot b = b \neq 0 = a^{-1} \cdot 0.$$

Definition 6.6 (=Erinnerung)
Sei R ein kommutativer Ring mit Eins.

(a) Ein *Ideal* in R ist eine Teilmenge $I \subset R$ mit $I \neq R$ mit den Eigenschaften:

(α) I ist abgeschlossen unter der Addition, d.h. I ist eine Untergruppe von $(R, +)$.

(β) I ist abgeschlossen unter der Multiplikation mit Elementen von R, d.h.

$$a \in R,\ b \in I \Longrightarrow a \cdot b \in I.$$

(b) Ein Ideal I heißt *Hauptideal*, falls es ein $b \in I$ gibt mit $I = \{a \cdot b \mid a \in R\}$. Notation: $I = (b)$.

(c) Die *Summe zweier Ideale* I_1 und I_2 ist die Menge

$$I_1 + I_2 := \{a + b \mid a \in I_1, b \in I_2\}.$$

Lemma: sie ist auch ein Ideal oder sie ist R.

(d) Ein Ideal I heißt *maximal*, falls gilt:

$$\forall\ a \in R - I \quad \text{ist} \quad (a) + I = R.$$

Satz 6.7 *(=Erinnerung, ohne Beweis)*

(a) Alle Ideale im Ring $\mathbb{Z}$ sind Hauptideale, d.h. sie sind von der Gestalt $m\mathbb{Z} = (m) = \{k \cdot m \mid k \in \mathbb{Z}\}$, $m \in \mathbb{N}$, $m \geq 2$.

(b) *Ein Ideal $m\mathbb{Z} = (m)$ ist genau dann ein maximales Ideal, wenn m eine Primzahl ist.*

Definition/Satz 6.8 *(=Erinnerung, Beweis leicht, hier nur Beweis von e))*

(a) *(Definition) Sei R ein kommutativer Ring mit Eins und I ein Ideal. Die Nebenklassen von I sind die Mengen*

$$[a] := a + I := \{a + b \mid b \in I\}.$$

(b) *(Satz) Entweder ist $[a] = [b]$ oder $[a] \cap [b] = \emptyset$;*
und es ist

$$[a] = [b] \iff a - b \in I.$$

(c) *(Satz/Definition) Die Relation $\sim$ mit*

$$a \sim b \overset{\text{Def.}}{\iff} [a] = [b]$$

ist eine Äquivalenzrelation.
Die Äquivalenzklassen sind die Nebenklassen.
Die Menge der Nebenklassen heißt R/I = Quotient von R nach I.

(d) *(Satz) R/I ist ein kommutativer Ring mit Eins*

$$\text{mit der Addition} \qquad [a] + [b] := [a + b]$$

$$\text{und mit der Multiplikation} \qquad [a] \cdot [b] := [a \cdot b].$$

[Zu zeigen ist hier, daß diese Verknüpfungen nicht von der Wahl der Repräsentanten abhängen, d.h.

$[a_1] = [a_2]$ und $[b_1] = [b_2] \Longrightarrow [a_1 + b_1] = [a_2 + b_2]$ und $[a_1 \cdot b_1] = [a_2 \cdot b_2]$.*]*

(e) *(Satz) R/I ist ein Körper $\iff$ I ist ein maximales Ideal.*

Beweis von (e):
"⇒": Sei $a \in R - I$. Insbesondere ist $a \neq 0$.
Also existiert a^{-1}. Also ist $1_R = a^{-1} \cdot a \in (a) + I$.
Also ist $(a) + I = R$. Also ist I maximal.

"⇐": Sei $a \in R - I$. Also ist $(a) + I = R$. Also existieren ein $b \in R$ und ein $c \in I$ mit $1_R = b \cdot a + c$.
Also ist $[b] \cdot [a] = [1_R]$ in R/I. Also hat $[a] \in R/I$ ein Inverses bezüglich der Multiplikation.
Also ist R/I ein Körper.

□

Beispiele 6.9 (i) $R = \mathbb{Z}$, $I = 5\mathbb{Z}$, $R/I = \mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$,

+	[0]	[1]	[2]	[3]	[4]
[0]	0	1	2	3	4
[1]	1	2	3	4	0
[2]	2	3	4	0	1
[3]	3	4	0	1	2
[4]	4	0	1	2	3

·	[0]	[1]	[2]	[3]	[4]
[0]	0	0	0	0	0
[1]	0	1	2	3	4
[2]	0	2	4	1	3
[3]	0	3	1	4	2
[4]	0	4	3	2	1

(Die Klammern im Inneren der Tabellen sind nur weggelassen, um die Tabellen übersichtlicher zu machen).

(ii) Aus Satz 6.7 (b) und Satz 6.8 (e) folgt:

$\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\iff$ m ist eine Primzahl.

(Definition) Sei p eine Primzahl. Der Körper $\mathbb{Z}/p\mathbb{Z}$ wird auch $\mathbb{F}_p$ genannt.

Definition/Satz 6.10 *(=Erinnerung)*
Sei K ein Körper.

(a) (Definition) Der Grad eines Polynoms $f(t) \in K[t]$ ist

$$\deg f(t) := \begin{cases} -\infty & \text{falls } f(t) = 0 \\ n \in \mathbb{N} \cup \{0\} & \text{falls } f(t) = a_0 + a_1 t + ... + a_n t^n \text{ mit } a_n \neq 0. \end{cases}$$

(b) Er erfüllt

$$\deg(f(t) \cdot g(t)) = \deg f(t) + \deg g(t).$$

Insbesondere folgt:

$$f(t) \neq 0 \text{ und } g(t) \neq 0 \Rightarrow f(t)g(t) \neq 0.$$

(c) (Polynomdivision mit Rest)

$$\forall\ f(t), g(t) \in K[t] \text{ mit } \deg g(t) \geq 1 \quad \exists!\ q(t), r(t) \in K[t] \text{ mit } \deg r(t) < \deg g(t) \text{ und } f(t) = q(t)g(t) + r(t).$$

(d) Ist $f(t) \in K[t]$ mit $\deg f(t) \geq 1$ und ist $c \in K$ mit $f(c) = 0$, so existiert ein eindeutiges $g(t) \in K[t]$ mit $f(t) = (t - c) \cdot g(t)$.

(e) Ein Polynom $f(t) \in K[t]$ mit $\deg f(t) = n \geq 0$ hat höchstens n verschiedene Nullstellen.

(f) Alle Ideale in $K[t]$ sind Hauptideale, d.h. sie sind von der Gestalt

$$(f(t)) = \{g(t)f(t) \mid g(t) \in K[t]\}$$

mit $f(t) \in K[t]$, $\deg f(t) \geq 1$ oder $f(t) = 0$.
[Bei $\deg f(t) = 0$ ist $f(t) \in K - \{0\}$ und $(f(t)) = K[t]$.]

(g) (Definition) Ein Polynom $f(t)$ mit $\deg f(t) \geq 1$ heißt irreduzibel *(in $K[t]$), wenn gilt:*

$$g(t) \text{ teilt } f(t) \iff g(t) \in K - \{0\} \text{ oder } g(t) = c \cdot f(t) \text{ mit } c \in K - \{0\}.$$

(h) Ein Ideal $I = (f(t))$ ist genau dann ein maximales Ideal, wenn $f(t)$ irreduzibel ist.

(i) Sei $f(t) \in K[t]$ irreduzibel. Es gilt

$$f(t) \mid a(t)b(t) \Rightarrow f(t) \mid a(t) \text{ oder } f(t) \mid b(t)$$

(d.h. $f(t)$ ist ein Primelement*).*

(j) Jedes Polynom $f(t) \in K[t] - \{0\}$ besitzt eine eindeutige Zerlegung

$$f(t) = c \cdot \prod_{j=1}^{m} f_j(t)$$

mit $c \in K - \{0\}$, $f_j(t)$ unitär *(d.h. der Leitkoeffizient ist 1) und irreduzibel in $K[t]$.*

Beweis(skizze) nach den Bemerkungen 6.11.

Bemerkungen 6.11 (i) Das Polynom $t^2 - 2 \in \mathbb{Q}[t] \subset \mathbb{R}[t]$ ist irreduzibel in $\mathbb{Q}[t]$, aber reduzibel in $\mathbb{R}[t]$, denn $t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$ und $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$.

Das Polynom $t^2 + 2$ ist irreduzibel in $\mathbb{R}[t]$, aber reduzibel in $\mathbb{C}[t]$.

Die Polynome $t^2 + t + 1$ und $t^3 + t + 1$ sind irreduzibel in $\mathbb{F}_2[t]$ (Beweis in Beispiel 6.15).

(ii) Ist $f(t) \in K[t]$ mit $\deg f(t) = n \geq 1$, so ist $K[t]/(f(t))$ wegen Satz 6.8 (d) ein kommutativer Ring mit Eins.

$K[t]/(f(t))$ ist auch ein K-Vektorraum der Dimension n. Eine Basis des K-Vektorraums besteht aus den Klassen $[1], [t], ..., [t^{n-1}] = [t]^{n-1}$.

Die Multiplikation ergibt sich aus den Distributivgesetzen und aus

$$a_n[t]^n = -a_{n-1}[t]^{n-1} - ... - a_1[t] - a_0$$

bei

$$f(t) = a_n t^n + ... + a_1 t + a_0,$$

d.h. aus $[f(t)] = 0$.

(iii) Aus Satz 6.8 (e) und Satz 6.10 (h) folgt:

$K[t]/(f(t))$ ist ein Körper, falls $f(t)$ irreduzibel in $K[t]$ ist.

(iv) Ist $K = \mathbb{F}_p$, p eine Primzahl, und ist $f(t) \in \mathbb{F}_p[t]$ irreduzibel mit $\deg f(t) = n \geq 1$, so ist der Körper $\mathbb{F}_p[t]/(f(t))$ ein $\mathbb{F}_p$-Vektorraum der Dimension n und hat p^n Elemente.

(v) Zum Beweis von Satz 6.1 bleibt zu zeigen:

- (α) Zu einem endlichen Körper K gibt es eine Primzahl p und ein $n \in \mathbb{N}$ mit $|K| = p^n$.
- (β) Für alle $n \in \mathbb{N}$ gibt es ein irreduzibles Polynom $f(t) \in \mathbb{F}_p[t]$ mit $\deg f(t) = n$. (Dann gibt es wegen (iv) einen Körper mit p^n Elementen.)
- (γ) Es gibt nur einen Körper mit p^n Elementen.

(vi) Sobald (v) (γ) und die letzte Aussage in (i) gezeigt sind, sieht man zum Beispiel

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[t]}{(t^2+t+1)} \qquad \text{und} \qquad \mathbb{F}_8 = \frac{\mathbb{F}_2[t]}{(t^3+t+1)}.$$

(vii) Es ist zum Beispiel

$$\begin{array}{rcl} \dfrac{\mathbb{Q}[t]}{(t^2-2)} & \xrightarrow{\cong} & \mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\cdot\sqrt{2} \subset \mathbb{R} \\ [t] & \mapsto & \sqrt{2}. \end{array}$$

Hier ist $\xrightarrow{\cong}$ ein Körperisomorphismus.

Beweisskizze von Satz 6.10:

(a) Definition.

(b) Leicht: Leitterme der Polynome ....

(c) Schulstoff (?), induktiv ....

(d) Anwendung von (c) mit $g(t) = t - c$.

(e) Man iteriert (d) solange wie möglich und erhält

$$f(t) = (t-c_1)\cdot ... \cdot (t-c_l)\cdot g_l(t)$$

mit $g_l(c) \neq 0$ für alle $c \in K$.

Dann ist $l \leq n$ und $f(c) \neq 0$ für alle $c \in K - \{c_1, ..., c_l\}$, wegen Bemerkung 6.5 (vi): $a \neq 0, b \neq 0 \Rightarrow a \cdot b \neq 0$ für $a, b \in K$.

(f) Sei $I \subset K[t]$ ein Ideal und $I \neq \{0\}$; sei
$f(t) \in I - \{0\}$ mit minimalem Grad $\deg f(t)$
(so eines existiert).

Behauptung: $I = (f(t))$.

Beweis: Sei $g(t) \in I$. Nach (c) existieren $q(t)$ und $r(t)$ mit $\deg r(t) < \deg f(t)$ und $g(t) = q(t)f(t) + r(t)$. Daher ist $r(t) \in I$.

Wäre $r(t) \neq 0$, so wäre $\deg f(t)$ nicht minimal, ein Widerspruch.

Also ist $r(t) = 0$ und $g(t) = q(t)f(t) \in (f(t))$.

(g) Definition.

(h) "⇒": Sei $(f(t)) \subset K[t]$ ein maximales Ideal und $g(t) \in K[t]$ ein Teiler von $f(t)$.

1. Fall, $\deg g(t) \geq \deg f(t)$: dann ist $g(t) = c \cdot f(t)$, $c \in K - \{0\}$.

2. Fall, $\deg g(t) < \deg f(t)$: dann ist $g(t) \notin I$, also (wegen I maximal)

$$(g(t)) + I = K[t],$$

also

$$\begin{aligned} 1 &= \alpha(t) \cdot g(t) + \beta(t) \cdot f(t) \quad \text{für geeignete } \alpha(t), \beta(t) \in K[t] \\ &= g(t)(\alpha(t) + \beta(t) \cdot \frac{f(t)}{g(t)}), \end{aligned}$$

also

$g(t) \in K - \{0\}$.

"⇐": Sei $f(t)$ irreduzibel. Sei $g(t) \in K[t] - (f(t))$.

Nach (f) gibt es ein $h(t) \in K[t]$ mit

$$(h(t)) = (g(t)) + (f(t)).$$

Aus $f(t) \in (h(t))$ folgt, daß $h(t)$ $f(t)$ teilt. Aus $g(t) \in (h(t))$ folgt $h(t) \notin (f(t))$.

Mit $f(t)$ irreduzibel folgt $h(t) = c$ für ein $c \in K - \{0\}$, also $(g(t)) + (f(t)) = K[t]$. Also ist $(f(t))$ ein maximales Ideal.

(i) Annahme: $f(t)$ teilt nicht $a(t)$.

Dann gilt $a(t) \notin (f(t))$. Also ist $K[t] = (a(t)) + (f(t))$; also existieren $\alpha(t)$ und $\beta(t)$ mit

$$1 = \alpha(t)a(t) + \beta(t)f(t).$$

Also ist

$$b(t) = \alpha(t)a(t)b(t) + \beta(t)f(t)b(t).$$

Daher ist $b(t)$ durch $f(t)$ teilbar.

(j) Annahme:

$$\prod_{j=1}^{m} f_j(t) = \prod_{k=1}^{\widetilde{m}} \widetilde{f}_k(t)$$

mit $f_j(t), \widetilde{f}_k(t)$ *irreduzibel und unitär.*

Wegen (i) gilt: f_1 teilt $\prod_{k=2}^{\widetilde{m}} \widetilde{f}_k$ oder $\widetilde{f}_1$.

Induktiv folgt: f_1 teilt (mindestens) eines der Polynome $\widetilde{f}_1$, $\widetilde{f}_2$, ..., $\widetilde{f}_{\widetilde{m}}$.

OBdA teile f_1 $\widetilde{f}_1$. Weil $\widetilde{f}_1$ irreduzibel (und unitär) ist, ist $f_1 = \widetilde{f}_1$. Daher ist

$$\left(\prod_{j=2}^{m} f_j(t) - \prod_{k=2}^{\widetilde{m}} \widetilde{f}_k(t) \right) \cdot f_1(t) = 0.$$

Mit (b) folgt

$\prod_{j=2}^{m} f_j(t) - \prod_{k=2}^{\widetilde{m}} \widetilde{f}_k(t) = 0.$

Induktiv folgt die Behauptung. □

Definition/Lemma 6.12 *(=Erinnerung)*

(a) (Definition) Die Charakteristik $\mathrm{char}(K) \in \mathbb{N} \cup \{0\}$ *eines Körpers* K *ist*

$$\mathrm{char}(K) := \begin{cases} 0 & \text{falls } n \cdot 1_K (= 1_K + ... + 1_K) \neq 0 \ \forall \ n \in \mathbb{N} \\ \min(n \in \mathbb{N} \mid n \cdot 1_K = 0) & \text{sonst} \end{cases}$$

(b) (Lemma) $\mathrm{char}(K) = 0$ *oder* $\mathrm{char}(K)$ *ist eine Primzahl.*

Beweis von (b):
Sei $\mathrm{char}(K) = a \cdot b$ mit $a, b \in \mathbb{N}$. Dann ist

$$0 = (a \cdot b) \cdot 1_K = (a \cdot 1_K) \cdot (b \cdot 1_K).$$

Mit Bemerkung 6.5 (vi) folgt: $a \cdot 1_K = 0$ oder $b \cdot 1_K = 0$.
Daher ist $\mathrm{char}(K) \leq a$ oder $\mathrm{char}(K) \leq b$. Also ist $b = 1$ oder $a = 1$. □.

Lemma 6.13 *Sei* K *ein endlicher Körper.*
Dann ist $\mathrm{char}(K)$ *eine Primzahl,* $\mathrm{char}(K) = p$. *Es ist* $\mathbb{F}_p \subset K$, *und* K *ist ein* $\mathbb{F}_p$*-Vektorraum von endlicher Dimension* n. *Der Körper* K *hat* p^n *Elemente.*

Beweis:
K endlich $\Rightarrow \mathbb{Z} \not\subset K \Rightarrow \mathrm{char}(K)$ ist endlich, also eine Primzahl.
Es ist

$$\mathbb{F}_p \cong \{l \cdot 1_K \mid l \in \{0, 1, ..., p-1\}\} \subset K.$$

Also ist K ein $\mathbb{F}_p$-Vektorraum.
Wäre $\dim_{\mathbb{F}_p} K = \infty$, so wäre K nicht endlich.
Also ist $\dim_{\mathbb{F}_p} K = n \in \mathbb{N}$. Als $\mathbb{F}_p$-Vektorraum ist K dann isomorph zu $\mathbb{F}_p^n$.
Daher hat K p^n Elemente.

□

Satz 6.14 *Sei p eine Primzahl, $n \in \mathbb{N}$.*

(a) Für jedes $r \in \mathbb{N}$ ist die Menge

$$J_{r,p} := \{f(t) \in \mathbb{F}_p[t] \quad | \quad \deg f(t) = r, f(t) \text{ unitär und irreduzibel}\}$$

nicht leer.

(b)

$$p^n = \sum_{r \text{ teilt } n} r \cdot |J_{r,p}|.$$

(c) (Verfeinerung von (b))

$$t^{p^n} - t = \prod_{r \text{ teilt } n} \prod_{f(t) \in J_{r,p}} f(t) \quad \text{in } \mathbb{F}_p[t].$$

(d) Es gibt genau einen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen. Er ist isomorph zu $\mathbb{F}_p[t]/(f(t))$ mit $f(t) \in J_{n,p}$ beliebig.

In ihm zerfällt $t^{p^n} - t$ so:

$$t^{p^n} - t = \prod_{a \in \mathbb{F}_{p^n}} (t - a).$$

Beweis nach den Beispielen 6.15.

Beispiele 6.15 p=2 (also $-1 = 1$, also z.B. $t - 1 = t + 1$).

$$\begin{aligned}
J_{1,2} &= \{t, t-1\}, \quad 2^1 = 1 \cdot |J_{1,2}| = 1 \cdot 2, \\
&\qquad t^{2^1} - t = t(t-1); \\
J_{2,2} &= \{t^2+t+1\}, \quad 2^2 = 1 \cdot |J_{1,2}| + 2 \cdot |J_{2,2}| = 1 \cdot 2 + 2 \cdot 1, \\
&\qquad t^{2^2} - t = t^4 - t \stackrel{?}{=} t(t-1)(t^2+t+1) = t(t^3-1) = t^4 - t; \\
J_{3,2} &= \{t^3+t+1, t^3+t^2+1\}, \quad 2^3 = 1 \cdot |J_{1,2}| + 3 \cdot |J_{3,2}| = 1 \cdot 2 + 3 \cdot 2, \\
&\qquad t^{2^3} - t = t^8 - t \stackrel{\text{nachrechnen}}{=} t(t-1)(t^3+t+1)(t^3+t^2+1).
\end{aligned}$$

Alle Polynome $f \in J_{2,2} \cup J_{3,2}$ sind tatsächlich irreduzibel: denn sie erfüllen alle $f(0) = 1 = f(1)$ und haben daher keinen linearen Faktor; wegen $\deg f(t) \leq 3$ haben sie gar keinen nichttrivialen Faktor. (Das gibt die letzte Aussage in Bemerkung 6.11 (i).)
Es ist auch leicht zu sehen: alle anderen unitären Polynome vom Grad 2 oder 3 haben Linearfaktoren und sind daher nicht irreduzibel.

Beweis von Satz 6.14:
Zuerst (b): Mit erzeugenden Funktionen (eine Methode der analytischen Zahlentheorie).
Die Menge

$$\{\text{unitäre Polynome in } \mathbb{F}_p[t] \text{ vom Grad } m\}$$

ist via

$$t^m + a_{m-1}t^{m-1} + ... + a_1 t + a_0 \mapsto (a_0, a_1, ..., a_{m-1})$$

kanonisch bijektiv zu $\mathbb{F}_p^m$ und hat daher p^m Elemente. Die erzeugende Funktion der Ordnungen dieser Mengen für alle $m \in \mathbb{N} \cup \{0\}$ ist definiert als

$$\sum_{m=0}^{\infty} p^m z^m = \frac{1}{1-pz}.$$

Nach Satz 6.10 (j) ist jedes unitäre Polynom auf eindeutige Weise als Produkt irreduzibler unitärer Polynome schreibbar. Daher erhält man für die erzeugende Funktion oben folgende Produktformel.

$$\begin{aligned}
\sum_{m=0}^{\infty} p^m z^m &= \prod_{r=1}^{\infty} \prod_{f(t) \in J_{r,p}} (1 + z^r + z^{2r} + z^{3r} + ...) \\
&= \prod_{r=1}^{\infty} \left(\frac{1}{1-z^r} \right)^{|J_{r,p}|}.
\end{aligned}$$

Also ist

$$(1-pz)^{-1} = \prod_{r=1}^{\infty}(1-z^r)^{-|J_{r,p}|},$$

also

$$(-1)\log(1-pz) = \sum_{r=1}^{\infty}(-|J_{r,p}|)\cdot\log(1-z^r).$$

Ableiten und mit z multiplizieren gibt

$$\frac{pz}{1-pz} = \sum_{r=1}^{\infty} r\cdot|J_{r,p}|\cdot\frac{z^r}{1-z^r}.$$

Der Koeffizient von z^n $(n\geq 1)$ ist links p^n und rechts $\sum_{r \text{ teilt } n} r\cdot|J_{r,p}|$, also ist

$$p^n = \sum_{r \text{ teilt } n} r\cdot|J_{r,p}| \qquad \text{für } n\geq 1.$$

Als zweites (a): Mit einer Funktion und einer Formel der Zahlentheorie und mit b).
(Definition:) Die *Möbiusfunktion* $\mu : \mathbb{N}\to\{1,-1,0\}$ ist definiert durch

$$\mu(n) := \begin{cases} 1 & \text{falls } n=1, \\ (-1)^k & \text{falls } n=p_1p_2...p_k, \text{ wobei die } p_i \\ & \text{verschiedene Primzahlen sind,} \\ 0 & \text{sonst.} \end{cases}$$

Ein Satz der Zahlentheorie ("Möbius-Inversion", hier ohne Beweis): *Sind* $F,G:\mathbb{N}\to\mathbb{C}$ *Funktionen mit*

$$F(m) = \sum_{r \text{ teilt } m} G(r),$$

so ist

$$G(m) = \sum_{s \text{ teilt } m} \mu(s)F(\frac{m}{s}).$$

Anwendung hier mit $F(m)=p^m$, $G(m)=m\cdot|J_{m,p}|$ und Teil (b). Es folgt

$$
\begin{aligned}
|J_{m,p}| &= \frac{1}{m} \sum_{s \text{ teilt } m} \mu(s) \cdot p^{\frac{m}{s}} \\
&\geq \frac{1}{m} \left(p^m - \sum_{s \text{ teilt } m, s>1} p^{\frac{m}{s}} \right) \\
&> \frac{1}{m} \left(p^m - \sum_{i=0}^{[m/2]} p^i \right) \\
&= \frac{1}{m} \left(p^m - \frac{p^{[m/2]+1} - 1}{p-1} \right) \\
&> \begin{cases} 0 & \text{für } m = 1, 2 \\ \frac{1}{m}(p^m - p^{[m/2]+1}) > 0 & \text{für } m \geq 3. \end{cases}
\end{aligned}
$$

Wegen $|J_{m,p}| > 0$ ist $J_{m,p} \neq \emptyset$.

Teil (c) wird nach Satz 6.16 bewiesen mit Hilfe von Satz 6.16 (a).

Nun (d): Mit Hilfe von (a) und (c).
Sei $f_0(t) \in J_{n,p}$ ($\neq \emptyset$ nach a)). Nach Bemerkung 6.11 (iv) ist $\mathbb{F}_p[t]/(f_0(t))$ ein Körper mit p^n Elementen.
Es soll gezeigt werden, daß jeder Körper mit p^n Elementen zu diesem Körper isomorph ist.
Sei nun K ein beliebiger Körper mit p^n Elementen.
Nach Lemma 6.13 ist $\text{char}(K) = p$, und K ist ein $\mathbb{F}_p$-Vektorraum der Dimension n.
Die Ordnung der multiplikativen Gruppe $(K - \{0\}, \cdot)$ ist $p^n - 1$.

Ein Satz der Gruppentheorie (hier ohne Beweis): *Die Ordnung eines Elementes einer endlichen Gruppe teilt die Gruppenordnung.*

Also ist

$$a^{p^n-1} = 1 \text{ für alle } a \in K - \{0\};$$

also ist

$$a^{p^n} = a \text{ für alle } a \in K.$$

Also sind alle $a \in K$ Nullstellen von $t^{p^n} - t \in \mathbb{F}_p[t]$. Wegen Satz 6.10 (e) ist

$$t^{p^n} - t = \prod_{a \in K} (t - a).$$

Wegen (c) ist $f_0 \in J_{n,p}$ ein Teiler von $t^{p^n} - t$.
Also existiert ein $a_0 \in K$ mit $f_0(a_0) = 0$.

Behauptung: *Die Elemente* $1, a_0, ..., a_0^{n-1}$ *sind linear unabhängig in* K *als* $\mathbb{F}_p$*-Vektorraum.*

Das folgt daraus, daß f_0 irreduzibel in $\mathbb{F}_p[t]$ ist, und aus folgendem Argument: Gäbe es ein $g(t) \in \mathbb{F}_p[t]$ mit $\deg g(t) < n$ und $g(a_0) = 0$, so wäre a_0 Nullstelle von jedem Polynom in $(g(t)) + (f(t))$; aber weil $f(t)$ irreduzibel ist, ist diese Summe gleich $\mathbb{F}_p[t]$, ein Widerspruch.
Also ist $1, a_0, ..., a_0^{n-1}$ eine Basis von K als $\mathbb{F}_p$-Vektorraum.
Aus $f_0(a_0) = 0$ folgt dann, daß die Abbildung

$$\begin{array}{rcl} K & \xrightarrow{\cong} & \mathbb{F}_p[t]/(f_0(t)) \\ \kappa_0 + \kappa_1 \cdot a_0 + ... + \kappa_{n-1} \cdot a_0^{n-1} & \mapsto & \kappa_0 + \kappa_1 \cdot [t] + ... + \kappa_{n-1} \cdot [t]^{n-1} \end{array}$$

(mit $\kappa_0, ..., \kappa_{n-1} \in \mathbb{F}_p$) ein Isomorphismus von $\mathbb{F}_p$-Vektorräumen und von Körpern ist.
Also gibt es (bis auf Isomorphie) nur einen Körper mit p^n Elementen. □

Satz 6.16 *(a) Sind* $L \subset K$ *endliche Körper mit* $|L| = p^r$ *und* $|K| = p^s$*, so ist* r *ein Teiler von* s *(Verfeinerung in Satz 6.17 (a)).*

(b) Die multiplikative Gruppe $(K - \{0\}, \cdot)$ *eines endlichen Körpers* K *ist zyklisch.*

Beweis:

(a) $(L - \{0\}, \cdot)$ ist eine Untergruppe von $(K - \{0\}, \cdot)$.
Daher gilt: $p^r - 1 = |L - \{0\}|$ teilt $p^s - 1 = |K - \{0\}|$.
Sei

$$s = \varphi \cdot r + \psi \quad \text{mit } \varphi, \psi \in \mathbb{Z}, \quad 0 \leq \psi < r.$$

Es ist

$$p^s - 1 = (p^r)^\varphi \cdot p^\psi - 1 \equiv p^\psi - 1 \mod (p^r - 1).$$

Daher ist $p^s - 1 \equiv 0 \mod (p^r - 1)$ genau dann, wenn $\psi = 0$ ist, d.h. wenn r ein Teiler von s ist.

(b) Gruppentheorie $\Rightarrow (K - \{0\}, \cdot)$ ist isomorph zu einer additiven Gruppe der Gestalt

$$\begin{array}{rl} & \left(\mathbb{Z}/(p_1^{l_{11}}\mathbb{Z})\right) \times \left(\mathbb{Z}/(p_1^{l_{12}}\mathbb{Z})\right) \times ... \times \left(\mathbb{Z}/(p_1^{l_{1\lambda_1}}\mathbb{Z})\right) \\ \times & ... \\ \times & \left(\mathbb{Z}/(p_k^{l_{k1}}\mathbb{Z})\right) \times \left(\mathbb{Z}/(p_k^{l_{k2}}\mathbb{Z})\right) \times ... \times \left(\mathbb{Z}/(p_k^{l_{k\lambda_k}}\mathbb{Z})\right), \end{array}$$

wobei

$p_1, ..., p_k$ lauter verschiedene Primzahlen sind und

$$\begin{aligned} l_{11} &\geq l_{12} \geq ... \geq l_{1\lambda_1}, \\ &\vdots \\ l_{k1} &\geq l_{k2} \geq ... \geq l_{k\lambda_k} \end{aligned}$$

ist. Sei

$$r := p_1^{l_{11}} \cdot ... \cdot p_k^{l_{k1}}.$$

Dann ist

$$a^r = 1 \quad \text{für alle } a \in K - \{0\}.$$

Das Polynom $t^r - 1$ hat also alle $a \in K - \{0\}$ als Nullstellen.

Andererseits hat es höchstens r Nullstellen (Satz 6.10 (e)).

Also ist $\lambda_1 = ... = \lambda_k = 1$, und $(K - \{0\}, \cdot)$ ist isomorph zur zyklischen Gruppe

$$\left(\mathbb{Z}/(p_1^{l_{11}}\mathbb{Z})\right) \times \left(\mathbb{Z}/(p_2^{l_{21}}\mathbb{Z})\right) \times ... \times \left(\mathbb{Z}/(p_k^{l_{k1}}\mathbb{Z})\right).$$

□

Beweis von Satz 6.14 (c):

Aus Satz 6.10 (j) folgt: das Polynom $t^{p^n} - t$ hat eine eindeutige Zerlegung

$$t^{p^n} - t = \prod_{j=1}^{l} f_j(t) \in \mathbb{F}_p[t]$$

in unitäre Polynome $f_j(t)$ in $\mathbb{F}_p[t]$, die in $\mathbb{F}_p[t]$ irreduzibel sind.

Sei K irgendein Körper mit p^n Elementen

$$\left(\text{zum Beispiel} \quad K = \frac{\mathbb{F}_p[t]}{(f_0(t))} \quad \text{mit } f_0(t) \in J_{n,p}\right).$$

Nach dem Beweis von (d) ist (ohne Anwendung von c)!)

$$t^{p^n} - t = \prod_{a \in K} (t - a).$$

Weil hier alle Nullstellen einfach sind, sind die Polynome $f_j(t)$ alle verschieden.

Sei $a_j \in K$ mit $f_j(a_j) = 0$.

Wie im Beweis von d) folgt (ohne Anwendung von (c)!):

- $1, a, a^2, ..., a^{\deg f_j(t)-1}$ sind linear unabhängig in K.
- $L := \mathrm{span}_{\mathbb{F}_p}(1, a_j, a_j^2, ..., a_j^{\deg f_j(t)-1})$ ist ein Unterkörper von K mit $p^{\deg(f_j(t))}$ Elementen.

Mit Satz 6.16 (a) folgt: $\deg f_j(t)$ teilt n.
Also gibt es für r mit $r \mid n$ Teilmengen $\widetilde{J}_{r,p} \subset J_{r,p}$ mit der Eigenschaft

$$t^{p^n} - t = \prod_{r \mid n} \prod_{f \in \widetilde{J}_{r,p}} f(t).$$

Wegen Satz 6.14 (b) ist $\widetilde{J}_{r,p} = J_{r,p}$. □

Satz 6.17 *Sei $q = p^n$ (p eine Primzahl, $n \in \mathbb{N}$).*

(a) Die Unterkörper von $\mathbb{F}_q$ sind genau die $\mathbb{F}_{p^r}$ mit $r \mid n$.

(b) (Frobenius-Automorphismus) Sei $l \in \mathbb{N}$. Die Abbildung

$$\mathrm{Frob}_q : \mathbb{F}_{q^l} \to \mathbb{F}_{q^l}, \quad a \mapsto a^q$$

erfüllt

$$a^q + b^q = (a+b)^q, \quad \text{d.h. } \mathrm{Frob}_q(a) + \mathrm{Frob}_q(b) = \mathrm{Frob}_q(a+b).$$

Sie ist ein Körperautomorphismus. Ihre Fixpunktmenge
$\{a \in \mathbb{F}_{q^l} \mid a^q = a\}$ ist der Unterkörper $\mathbb{F}_q$ von $\mathbb{F}_{q^l}$.

Beweis: Erst (b), dann (a).

(b) Es ist

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot a^i b^{p-i} = a^p + b^p;$$

denn p teilt $\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!}$

für

$1 \leq i \leq p-1$,

weil p eine Primzahl ist; daher ist $\binom{p}{i} = 0$ in $\mathbb{F}_{q^l}$.

Induktiv folgt

$$(a+b)^q = [(a+b)^p]^{p^{n-1}} = [a^p + b^p]^{p^{n-1}} = ... = a^q + b^q.$$

Trivialerweise ist

$$\mathrm{Frob}_q(a \cdot b) = a^q \cdot b^q = (a \cdot b)^q = \mathrm{Frob}_q(a \cdot b).$$

Daher ist Frob_q ein Körper*homomorphismus*. Sein Kern muß ein Ideal in $\mathbb{F}_{q^l}$ sein; weil das aber ein Körper ist, ist der Kern Null. Daher ist Frob_q injektiv. Weil $\mathbb{F}_{q^l}$ endlich ist, ist Frob_q auch surjektiv, also ein Körperisomorphismus.

Die Fixpunktmenge $\{a \in \mathbb{F}_{q^l} \mid a^q = a\}$ ist abgeschlossen bezüglich der Addition und Multiplikation. Daher ist sie ein Unterkörper.

Weil $(\mathbb{F}_{q^l} - \{0\}, \cdot)$ eine *zyklische* Gruppe ist (Satz 6.16 (b)) und weil $q-1$ ihre Ordnung $q^l - 1$ teilt, hat das Polynom $t^{q-1} - 1$ in $\mathbb{F}_{q^l}$ $q-1$ Nullstellen.

Die Fixpunktmenge besteht aus diesen Nullstellen und der Null. Also hat sie q Elemente. Also ist sie als Körper isomorph zu $\mathbb{F}_q$ (Satz 6.14 (d)).

(a) Aus Satz 6.16 (a) folgt, daß $r \mid n$ eine notwendige Bedingung ist.

Aus Satz 6.17 (b) folgt, daß $\mathbb{F}_q$ ein Unterkörper von $\mathbb{F}_{q^l}$ ist. Daher ist sie auch hinreichend. □

Satz 6.18 *Sei $q = p^n$ (p eine Primzahl, $n \in \mathbb{N}$), $l \in \mathbb{N}$.*

(a) *Sei* $f(t) \in \mathbb{F}_q[t]$ *und sei* $\alpha \in \mathbb{F}_{q^l}$ *eine Nullstelle von* f, *d.h.* $f(\alpha) = 0$. *Dann ist auch* $f(\alpha^q) = 0$.

(b) *Sei* $\{\alpha_1, ..., \alpha_d\} \subset \mathbb{F}_{q^l}$ *mit* $\alpha_i \neq \alpha_j$ *für* $i \neq j$.
Sei

$$\mathrm{Frob}_q(\{\alpha_1, ..., \alpha_d\}) = \{\alpha_1, ..., \alpha_d\}.$$

Dann ist das Polynom

$$f(t) := \prod_{i=1}^{d}(t - \alpha_i) \quad (\in \mathbb{F}_{q^l}[t] \text{ a priori})$$

in $\mathbb{F}_q[t]$.

(c) *Sei* $\alpha \in \mathbb{F}_{q^l} - \{0\}$ *und sei* $o(\alpha)$ *die Ordnung von* α *in der Gruppe* $(\mathbb{F}_{q^l} - \{0\}, \cdot)$, *d.h.* $o(\alpha) = \min(k \in \mathbb{N} \mid \alpha^k = 1)$.
Sei

$$r(\alpha, q) := \min(r \in \mathbb{N} \mid q^r \equiv 1 \mod o(\alpha)).$$

Das Polynom

$$m_{\alpha,q}(t) := \prod_{i=0}^{r(\alpha,q)-1} (t - \alpha^{q^i})$$

ist in $\mathbb{F}_q[t]$, *es ist irreduzibel in* $\mathbb{F}_q[t]$ *und unitär. Seine Nullstellenmenge* $\alpha, \alpha^q, ..., \alpha^{q^{r(\alpha,q)-1}}$ *ist "zyklisch unter* Frob_q*", d.h.*

$$\alpha \xrightarrow{\mathrm{Frob}_q} \alpha^q \xrightarrow{\mathrm{Frob}_q} ... \xrightarrow{\mathrm{Frob}_q} \alpha^{q^{r(\alpha,q)-1}} \xrightarrow{\mathrm{Frob}_q} \alpha.$$

Es heißt Minimalpolynom von α in $\mathbb{F}_q[t]$.

(d) *Sei* $f(t) \in \mathbb{F}_q[t]$ *unitär. Es gibt ein* $m \in \mathbb{N}$, *so daß* $f(t)$ *in* $\mathbb{F}_{q^m}[t]$ *in Linearfaktoren zerfällt.*

(e) *Jedes in* $\mathbb{F}_q[t]$ *irreduzible und unitäre Polynomf*$(t) \in \mathbb{F}_q[t]$ *ist von der Gestalt wie in (c). Genauer:*
Ist $\alpha \in \mathbb{F}_{q^m}[t]$ *(m geeignet) irgendeine Nullstelle von* $f(t)$, *so ist* $f(t) = m_{\alpha,q}(t)$.

Beweis nach Bemerkung 6.19.

Bemerkung 6.19 Vorsicht, van Lint hat aus (b) und (d) eine Schlußfolgerung gezogen, die so nicht stimmt: (van Lint (1999) (1.1.20) Theorem (ii); van Lint & van der Geer (1.9)):

"Sei $K \supset \mathbb{F}_q$ ein Erweiterungskörper. Sei $g(t) \in K[t]$ mit der Eigenschaft

$$g(\alpha) = 0 \Rightarrow g(\alpha^q) = 0$$

(α in irgendeinem Erweiterungskörper von K). Dann ist $g(t) \in \mathbb{F}_q[t]$."

Der Fehler ist aber leicht zu korrigieren. Man muß die Eigenschaft verschärfen: α^q muß als Nullstelle von $g(t)$ die gleiche Vielfachheit haben wie α.

Beweis von Satz 6.18:

(a) Sei $f(t) = \sum_{i=0}^{\deg f(t)} a_i \cdot t^i$. Es ist $a_i \in \mathbb{F}_q$, also $a_i^q = a_i$.

Aus $(a+b)^q = a^q + b^q$ für $a, b \in \mathbb{F}_{q^l}$ (Satz 6.17 (b)) folgt $\overset{(*)}{=}$ in

$$0 = 0^q = (f(\alpha))^q \overset{(*)}{=} \sum_{i=0}^{\deg f(t)} a_i^q \cdot (\alpha^i)^q = \sum_{i=0}^{\deg f(t)} a_i \cdot (\alpha^q)^i = f(\alpha^q).$$

(b) Die Koeffizienten von f sind (bis aufs Vorzeichen) die elementarsymmetrischen Polynome in den $\alpha_1, ..., \alpha_d$. Da Frob_q die $\alpha_1, ..., \alpha_d$ bloß permutiert, läßt Frob_q die Koeffizienten von f invariant. Daher sind sie in $\mathbb{F}_q$, wegen Satz 6.17 (b).

(c) Die Aussage, daß die Menge $\alpha, \alpha^q, ..., \alpha^{q^{r(\alpha,q)-1}}$ "zyklisch unter Frob_q" ist, ist klar nach Konstruktion.

Daher und wegen (b) ist $m_{\alpha,q}(t)$ in $\mathbb{F}_q[t]$.

Wegen (a) hat *jedes* Polynom in $\mathbb{F}_q[t]$, das α als Nullstelle hat, $\alpha, \alpha^q, ..., \alpha^{q^{r(\alpha,q)-1}}$ als Nullstellen. Daher ist $m_{\alpha,q}(t)$ irreduzibel in $\mathbb{F}_q[t]$.

(d) **1. Fall,** $f(t)$ ist irreduzibel in $\mathbb{F}_q[t]$:

Dann ist $\mathbb{F}_q[t]/(f(t))$ ein Körper mit $q^{\deg(f)}$ Elementen. Das Element $\alpha := [t] \in \mathbb{F}_q[t]/(f(t))$ ist eine Nullstelle von $f(t)$ in diesem Körper.

Nach (c) ist in diesem Körper

$$f(t) = m_{\alpha,q}(t).$$

Also zerfällt $f(t)$ in diesem Körper in Linearfaktoren.

2. Fall, $f(t)$ ist nicht irreduzibel in $\mathbb{F}_q[t]$:

Sei $f(t) = \prod_{i=1}^{m} f_j(t)$ mit $f_j(t)$ irreduzibel in $\mathbb{F}_q[t]$ und unitär.

Nach Satz 6.17 (a) sind all die Körper $\mathbb{F}_q[t]/(f_j(t))$ Unterkörper des Körpers $\mathbb{F}_{q^k}$ mit $k := kgV(\deg f_1(t), ..., \deg f_m(t))$.

In ihm zerfällt $f(t)$ in Linearfaktoren.

(e) Das folgt nun aus (c). □

Definition 6.20 Sei $q = p^n$ (p eine Primzahl, $n \in \mathbb{N}$), $l \in \mathbb{N}$.

(a) Man nennt alle $\alpha \in \mathbb{F}_{q^l} - \{0\}$ *Einheitswurzeln*, denn $\alpha^{q^l-1} = 1$. Genauer: α ist eine *primitive Einheitswurzel der Ordnung* $o(\alpha) = \min(k \mid \alpha^k = 1)$.

(b) Ist $\alpha \in \mathbb{F}_{q^l} - \{0\}$ mit $o(\alpha) = q^l - 1$, so heißt das Minimalpolynom $m_{\alpha,q}(t) \in \mathbb{F}_q[t]$ auch *primitives Polynom*. (Nicht alle Minimalpolynome sind primitiv, siehe Beispiel 6.21.)

(Anscheinend ist es eine gute Wahl, endliche Körper mit q^l Elementen in der Form $\mathbb{F}_q[t]/(f(t))$ zu schreiben, wo $f(t)$ ein primitives Polynom vom Grad l in $\mathbb{F}_q[t]$ ist.)

Beispiel 6.21 $q = p = 2$, $q^l = 2^4$, vgl. Beispiel 6.15.

$$J_{4,2} = \{t^4 + t + 1,\ t^4 + t^3 + 1,\ t^4 + t^3 + t^2 + t + 1\}.$$

Wegen $(t^4+t^3+t^2+t+1)(t-1) = t^5-1$ sind die Nullstellen von $t^4+t^3+t^2+t+1$ primitive Einheitswurzeln der Ordnung 5. Also ist $t^4 + t^3 + t^2 + t + 1$ kein primitives Polynom.
Die zyklische Gruppe

$$(\mathbb{Z}/15\mathbb{Z}, +) \cong (\mathbb{F}_{2^4} - \{0\}, \cdot)$$

hat 8 Elemente der Ordnung 15, die Klassen (von Zahlen modulo 15) $[1], [2], [4], [7], [8], [11], [13], [14]$.
Die zugehörigen Elemente von $\mathbb{F}_{2^4} - \{0\}$ sind genau die Nullstellen von $t^4 + t + 1$ und $t^4 + t^3 + 1$. Diese Polynome sind daher primitive Polynome. Sei $\alpha \in \mathbb{F}_{2^4} - \{0\}$ eine beliebige der Nullstellen von $t^4 + t + 1$.

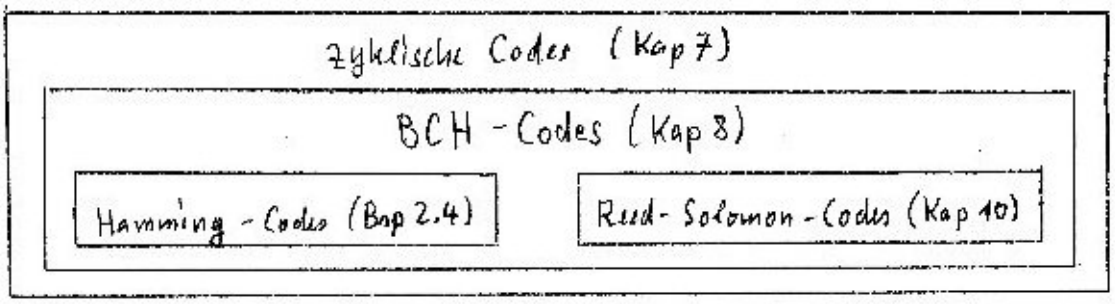
Nullstellen von $t^4 + t + 1$: $\alpha, \alpha^2, \alpha^4, \alpha^8$.

Nullstellen von $t^4 + t^3 + 1$: $\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{26} = \alpha^{11}$.

Nullstellen von $t^4 + t^3 + t^2 + t + 1$: $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$.

7 Zyklische Codes

Die zyklischen Codes sind die wichtigsten und die am besten untersuchten linearen Codes.



Definition 7.1 Ein linearer Code $C \subset \mathbb{F}_q^n$ ist zyklisch, falls gilt:

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$$

Wir machen die Zusatzvoraussetzung (wie alle Quellen, die ich angesehen habe):

$$\mathrm{ggT}(n, q) = 1.$$

Satz 7.2 *(a) Bei $f(t) \in \mathbb{F}_q[t]$ bezeichnet $[f(t)]$ die Klasse von $f(t)$ in $\frac{\mathbb{F}_q[t]}{(t^n-1)}$. Die Abbildung*

$$\begin{aligned} \mathbb{F}_q^n &\to \frac{\mathbb{F}_q[t]}{(t^n-1)} \\ (c_0, c_1, \ldots, c_{n-1}) &\to [c_0 t^0 + c_1 t^1 + \cdots + c_{n-1} t^{n-1}] \end{aligned}$$

ist ein Isomorphismus von $\mathbb{F}_q$-Vektorräumen. Mit ihr werden die beiden $\mathbb{F}_q$-Vektorräume identifiziert.

(b) Ein linearer Code $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ ist genau dann zyklisch, wenn er ein Ideal im Ring $\frac{\mathbb{F}_q[t]}{(t^n-1)}$ ist oder wenn er der ganze Ring ist.

(c) Zu einem Ideal $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ (inklusive $C = \{0\}$, was wegen $|C| < 2$ und Definition 1.3 (a) kein Code ist) und auch im Fall $C = \frac{\mathbb{F}_q[t]}{(t^n-1)}$ gibt es genau ein unitäres Polynom $g(t) \in \mathbb{F}_q[t]$ mit den zwei Eigenschaften:

- *$g(t)$ teilt $t^n - 1$ und*
- *$C = ([g(t)]) := \frac{\mathbb{F}_q[t]}{(t^n-1)} \cdot [g(t)] \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$*

Das Polynom heißt Erzeugerpolynom von C.

(d) Es sei $t^n - 1 = f_1(t) \cdot \cdots \cdot f_r(t)$ *mit* $f_1(t), \ldots, f_r(t) \in \mathbb{F}_q[t]$ *irreduzibel. Aus* $\mathrm{ggT}(n, q) = 1$ *(das ist die Zusatzvoraussetzung in Definition 7.1) folgt* $f_i(t) \neq f_j(t)$ *für* $i \neq j$.

(e) Inklusive $\{0\}$ *und* $\frac{\mathbb{F}_q[t]}{(t^n-1)}$ *gibt es* 2^r *zyklische Codes in* $\frac{\mathbb{F}_q[t]}{(t^n-1)}$. *Ihre Erzeugerpolynome sind alle möglichen Produkte von* $f_1(t), \ldots, f_r(t)$.

Das Produkt $f_1(t) \ldots f_r(t) = t^n - 1$ *gibt die Menge* $\{0\}$, *und das "leere Produkt"* 1 *gibt die Menge* $\frac{\mathbb{F}_q[t]}{(t^n-1)}$.

Beweis: (a) ok.
(b) Sei $\mathrm{pr} : \mathbb{F}_q[t] \to \frac{\mathbb{F}_q[t]}{(t^n-1)}$ die Projektion auf den Quotienten. Sei $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ ein linearer Code. Damit ist $\mathrm{pr}^{-1}(C) \subset \mathbb{F}_q[t]$ ein Untervektorraum.
Sei $f(t) = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1} \in \mathrm{pr}^{-1}(C)$. Dann ist

$$c_{n-1} + c_0 t + c_1 t^2 + \cdots + c_{n-2} t^{n-1} = t \cdot f(t) - c_{n-1} \cdot (t^n - 1),$$

also

$$c_{n-1} + c_0 t + c_1 t^2 + \cdots + c_{n-2} t^{n-1} \in \mathrm{pr}^{-1}(C) \iff t \cdot f(t) \in \mathrm{pr}^{-1}(C).$$

Nun argumentiert man so:

$$\begin{aligned}
& C \text{ ist ein Ideal in } \frac{\mathbb{F}_q[t]}{(t^n - 1)} \\
\iff\ & \mathrm{pr}^{-1}(C) \text{ ist ein Ideal in } \mathbb{F}_q[t] \\
\iff\ & \Big(f(t) \in \mathrm{pr}^{-1}(C) \Rightarrow t \cdot f(t) \in \mathrm{pr}^{-1}(C) \Big) \\
\iff\ & \Big((c_0, ..., c_{n-1}) = [c_0 + \cdots + c_{n-1} t^{n-1}] \in C \\
& \Rightarrow (c_{n-1}, c_0, ..., c_{n-2}) = [c_{n-1} + c_0 t + c_t^2 + \cdots + c_{n-2} t^{n-1}] \in C \Big) \\
\iff\ & C \text{ ist ein zyklischer Code.}
\end{aligned}$$

(c) Die Menge $\mathrm{pr}^{-1}(C) \subset \mathbb{F}_q[t]$ ist ein Ideal nach (b), also ein Hauptideal (siehe 6.10 f)), oder sie ist gleich $\mathbb{F}_q[t]$. In jedem Fall gibt es ein eindeutiges unitäres Polynom $g(t)$ mit $\mathrm{pr}^{-1}(C) = (g(t))$.
Wegen $t^n - 1 \in \mathrm{pr}^{-1}(C)$ (denn $t^n - 1$ ist ein Urbild von 0 unter pr) gilt $g(t) \mid t^n - 1$. Offenbar ist $C = ([g(t)])$.
(d)

$$\begin{aligned}
\mathrm{ggT}(n, q) = 1 \ &\Rightarrow\ n \neq 0 \text{ in } \mathbb{F}_q \\
&\Rightarrow\ f'(t) = n \cdot t^{n-1} \neq 0 \text{ in } \mathbb{F}_q[t] \\
&\Rightarrow\ \text{Die einzige Nullstelle von } f'(t) \text{ ist } 0 \\
&\Rightarrow\ t^n - 1 \text{ hat keine doppelte Nullstelle} \\
&\quad\ \text{(in irgendeinem Erweiterungskörper von } \mathbb{F}_q) \\
&\Rightarrow\ \text{alle } f_r \text{ sind verschieden.}
\end{aligned}$$

(e) Klar. □

Beispiel 7.3 $q = p = 2,\ n = 3,$

$$t^3 - 1 = (t-1)(t^2+t+1) =: f_1(t) \cdot f_2(t)$$

mit $f_1(t), f_2(t)$ irreduzibel in $\mathbb{F}_2[t]$ (siehe Beispiel 6.15). Daher gibt es 4 zyklische Codes in $\mathbb{F}_2^3 \approx \frac{\mathbb{F}_2[t]}{(t^3-1)}$, inklusive $\{0\}$, nämlich:

$$\begin{array}{lcll}
\{0\} & \leftrightarrow & 0 \equiv t^3 - 1 = f_1 \cdot f_2 & : \text{ 1 El., dim 0,} \\
\frac{\mathbb{F}_2[t]}{(t^3-1)} & \leftrightarrow & 1 \equiv \text{ leeres Produkt} & : \text{ 8 El., dim 3,} \\
\text{das Ideal } ([t-1]) & \leftrightarrow & f_1 = t - 1 & : \text{ 4 El., dim 2,} \\
\text{das Ideal } ([t^2+t+1]) & \leftrightarrow & f_2 = t^2 + t + 1 & : \text{ 2 El., dim 1.}
\end{array}$$

Die letzten beiden konkreter:

$$\begin{aligned}
([t-1]) &= \{[t-1], [t^2-t], [t^3-t^2] = [1-t^2], 0\} \subset \frac{\mathbb{F}_2[t]}{(t^3-1)} \\
&\cong \{(1,1,0), (0,1,1), (1,0,1), (0,0,0)\} \subset \mathbb{F}_2^3, \\
([t^2+t+1]) &= \{[t^2+t+1], 0\} \subset \frac{\mathbb{F}_2[t]}{(t^3-1)} \\
&\cong \{(1,1,1), (0,0,0)\} \subset \mathbb{F}_2^3.
\end{aligned}$$

Bemerkung: Jedes der 7 Elemente v von $\mathbb{F}_2^3 - \{0\}$ erzeugt einen linearen Code $\{v, 0\} = \mathbb{F}_2 \cdot v$ der Dimension 1 in $\mathbb{F}_2^3$, aber nur der zu $v = (1,1,1)$ ist zyklisch.

Satz 7.4 *Sei $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ ein zyklischer Code mit Erzeugerpolynom $g(t) = g_0 + g_1 t + \cdots + g_{n-k}t^{n-k}$ (natürlich $0 \le k \le n$) mit $g_{n-k} = 1$.*

(a) Dann ist dim $(C) = k$. (Im Fall $k = 0$ ist $C = \{0\}$ wegen $|C| = 1 < 2$ eigentlich kein Code, siehe die (korrigierte) Definition 1.3 (a)).

(b) Die $k \times n$-Matrix

$$G := \begin{pmatrix}
g_0 & & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\
0 & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & 0 \\
0 & \dots & 0 & g_0 & g_1 & \dots & & g_{n-k}
\end{pmatrix} = (g_{j-i})_{ij}$$

(mit $g_a := 0$ für $a \in \mathbb{Z} - \{0, ..., n-k\}$) ist eine Erzeugermatrix von C.

(c) Sei $t^n - 1 = g(t) \cdot h(t)$ *mit* $h(t) = h_0 + h_1 t + \cdots + h_k t^k$

Es ist $h_k = 1$ *(denn* $h_k \cdot g_{n-k} = 1$ *und* $g_{n-k} = 1$*).*

Die $(n-k) \times n$*-Matrix*

$$H := \begin{pmatrix} 0 & \dots & & 0 & h_k & h_{k-1} & \dots & h_0 \\ \vdots & & \ddots & \ddots & \ddots & & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & & \ddots & \ddots & & \vdots \\ h_k & h_{k-1} & \dots & h_0 & 0 & & & 0 \end{pmatrix} = (h_{n+1-i-j})_{ij}$$

(mit $h_a := 0$ *für* $a \in \mathbb{Z} - \{0, ..., k\}$*) ist eine Kontrollmatrix von C.*

(d) Erinnerung an Definition/Lemma 2.7: Der duale Code $C^\perp$ *hat Erzeugermatrix H und Kontrollmatrix G.*

Er ist via $\sigma \in S_n,\ \sigma : i \to n+1-i$*, äquivalent (im Sinne von Definition 2.1 (f)) zum zyklischen Code mit Erzeugerpolynom* $h(t)$*.*

Beweis:
(a) und (b) Die Zeilen von G "sind" die Elemente

$$[g(t)], [t \cdot g(t)], \dots, [t^{k-1} \cdot g(t)] \in \frac{\mathbb{F}_q[t]}{(t^n - 1)}.$$

Diese sind offensichtlich linear unabhängig. Sie bilden eine $\mathbb{F}_q$- Basis von C, denn

$$\begin{aligned} C &= \{[f(t)] \mid f(t) \in \mathrm{pr}^{-1}(C)\} \\ &= \{[f(t)] \mid f(t) \in \mathrm{pr}^{-1}(C),\ \deg f(t) \le n-1\} \\ &= \{[f(t)] \mid g(t) \text{ teilt } f(t),\ \deg f(t) \le n-1\} \\ &= \{[a(t) \cdot g(t)] \mid a(t) \in \mathbb{F}_q[t],\ \deg a(t) \le k-1\} \\ &= \bigoplus_{i=0}^{k-1} \mathbb{F}_q \cdot [t^i \cdot g(t)]. \end{aligned}$$

(c) Zuerst ist zu zeigen: $H \cdot G^{tr} = 0$
Für $a \in \mathbb{Z} - \{0, 1, \dots, n-k\}$ sei $g_a := 0$, für $a \in \mathbb{Z} - \{0, 1, \dots, k\}$ sei $h_a := 0$.
Dann ist

$$\begin{aligned} & \text{(j-te Zeile von H)} \cdot \text{(i-te Zeile von G)} \\ = & \sum_{a \in \mathbb{Z}} h_{n+1-j-a} \cdot g_{a-i} \\ = & \text{ Koeffizient von } t^{n+1-i-j} \quad \text{ in } t^n - 1 (= g(t) \cdot h(t)) \\ = & \ 0, \quad \text{denn } 1 \le n+1-i-j \le n-1. \end{aligned}$$

Also ist $H \cdot G^{tr} = 0$ Wegen $h_k = 1$ ist rang $H = n - k$. Mit Lemma 2.3 folgt: H ist Kontrollmatrix von C.

(d) klar. □

Satz 7.5 *[Nötig für die BCH-Codes in Kapitel 8]*
Sei $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ ein zyklischer Code mit Erzeugerpolynom $g(t)$.
Sei $g(t) = g_1(t) \dots g_s(t)$ die eindeutige Zerlegung von $g(t)$ in unitäre irreduzible Polynome in $\mathbb{F}_q[t]$, und seien für ein geeignetes $l \in \mathbb{N}$ (so eines existiert nach Satz 6.18 d)) $\beta_1, \dots, \beta_s \in \mathbb{F}_{q^l}$ Nullstellen von $g_1(t), \dots, g_s(t)$, d.h. $g_i(\beta_i) = 0$.

(a) Dann ist

$$[c_0 + c_1 t + \dots, c_{n-1} t^{n-1}] \in C \iff \forall\ i\ c_0 + c_1 \beta_i + \dots + c_{n-1} \beta_i^{n-1} = 0.$$

(b) [Von (a) zu einer Kontrollmatrix]

Sei $v_1, \dots, v_l \in \mathbb{F}_q^l$ eine beliebige Basis von $\mathbb{F}_{q^l}$ als $\mathbb{F}_q$-Vektorraum, und sei $\Psi : \mathbb{F}_{q^l} \to M(l \times 1, \mathbb{F}_q)$ der Isomorphismus von $\mathbb{F}_q$- Vektorrumen

$$\sum_{i=1}^{l} \gamma_i v_i \ \to \ \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_l \end{pmatrix}.$$

Die Matrix

$$\widetilde{H} := \begin{pmatrix} \Psi(1) & \Psi(\beta_1) & \Psi(\beta_1^2) & \dots & \Psi(\beta_1^{n-1}) \\ \vdots & \vdots & \vdots & & \vdots \\ \Psi(1) & \Psi(\beta_s) & \Psi(\beta_s^2) & \dots & \Psi(\beta_s^{n-1}) \end{pmatrix}$$

ist eine $(s \cdot l) \times n$-Matrix mit Einträgen in $\mathbb{F}_q$. Läßt man linear abhängige Zeilen weg, so erhält man eine Kontrollmatrix.

Beweis: (a) Sei $c(t) := c_0 + c_1 t + \dots + c_{n-1} t^{n-1} \in \mathbb{F}_q[t]$. Die Behauptung folgt aus

$$[c(t)] \in C \iff c(t) \in (g(t)) \overset{(*)}{\iff} \forall\ i \in \{1, ..., s\} \text{ ist } c(\beta_i) = 0.$$

$\overset{(*)}{\Rightarrow}$: Klar.
$\overset{(*)}{\Leftarrow}$: $g_i(t)$ ist das Minimalpolynom von β_i in $\mathbb{F}_q[t]$ (Satz 6.18 (e)). Es gilt:

$$\begin{aligned} \forall\ i\ c(\beta_i) = 0 \ &\Rightarrow \ \text{(mit Satz 6.18)} \quad \forall\ i\ g_i(t) \text{ teilt } C(t) \\ &\Rightarrow \ g(t) \text{ teilt } c(t) \\ &\Rightarrow \ [c(t)] \in C. \end{aligned}$$

(b)

$$
\begin{aligned}
& [c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}] \in C \\
\overset{(a)}{\iff} \quad & \begin{pmatrix} 1 & \beta_1 & \dots & \beta_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_s & \dots & \beta_s^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0 \\
\iff \quad & \widetilde{H} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0
\end{aligned}
$$

Also erhält man aus $\widetilde{H}$ eine Kontrollmatrix, wenn man linear abhängige Zeilen wegläßt. □

Beispiel 7.6 (a) Erinnerung an binäre Hamming-Codes (Beispiel 2.4):

$r \in \mathbb{N},\ n := 2^r - 1 = \ | \mathbb{F}_2^r - \{0\}|,$
$H :=$ die $r \times n$- Matrix, deren Spalten die Elemente von
$M(r \times 1, \mathbb{F}_2) - \{0\}$ sind,
Hamming-Code $C := \{x \in \mathbb{F}_2^n \mid H \cdot x^{tr} = 0\},$

also ist C der Code in $\mathbb{F}_2^n$ mit Kontrollmatrix H. Lemma 2.5: Es ist ein $[n, n-r, 3]$- Code. Verschiedene Anordnungen der Spalten von H geben äquivalente Codes (im Sinne von Definition 2.1 (f)).

(b) Sei $\beta \in \mathbb{F}_{2^r} - \{0\}$ ein erzeugendes Element der zyklischen Gruppe $(\mathbb{F}_2 r - \{0\}, \cdot)$ (Satz 6.16 (b)).
Sei $\Psi : \mathbb{F}_{2^r} \to M(r \times 1, \mathbb{F}_2)$ ein Isomorphismus von $\mathbb{F}_2$-Vektorräumen wie im Satz 7.5 (b). Die Matrix

$$\widetilde{H} = \begin{pmatrix} \psi(1) & \psi(\beta) & \psi(\beta^2) & \dots & \psi(\beta^{n-1}) \end{pmatrix} \quad [\text{bei } n = 2^r - 1]$$

ist eine $r \times n$-Matrix mit rang $\widetilde{H} = r$ (da sie alle Elemente von $M(r \times 1, \mathbb{F}_2) - \{0\}$ enthält, enthält sie eine Basis von $M(r \times 1, \mathbb{F}_2)$).
Nach Satz 7.5 (b) ist sie eine Kontrollmatrix des zyklischen Codes, dessen Erzeugerpolynom das Minimalpolynom von β in $\mathbb{F}_2[t]$ ist.
Wegen (a) ist dieser zyklische Code einer der Hamming-Codes in (a).

(c) Ein Rezept, einen zyklischen Code herzustellen, ist, Forderungen an die irreduziblen Faktoren seines Erzeugerpolynoms zu stellen.
In (b) war es: β ist ein erzeugendes Element der zyklischen Gruppe $(\mathbb{F}_{2^r} - \{0\}, \cdot)$, und $g(t)$ ist sein Minimalpolynom über $\mathbb{F}_2$, d.h. $g(t)$ ist ein primitives Polynom zur Körpererweiterung $\mathbb{F}_{2^r} \supset \mathbb{F}_2$ (Definition 6.21).
In Kapitel 8 wird das verallgemeinert.

8 BCH-Codes

Von großer praktischer und theoretischer Bedeutung sind die BCH-Codes von R.C. Bose & D.K. Ray-Chaudhury (1960) und A. Hocquenghem (1959) (unabhängig).
Sie sind zyklische Codes. Sie verallgemeinern die Hamming-Codes.

Definition 8.1 Ein zyklischer Code $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ mit Erzeugerpolynom $g(t)$ ist ein BCH-Code mit designiertem Abstand $\delta \leq n$, falls gilt:
Es gibt ein $b \in \mathbb{N}$ und es gibt ein $\alpha \in \mathbb{F}_{q^m} - \{0\}$ (m geeignet) mit $o(\alpha) = n$ [dann gilt: n teilt $q^m - 1$], so dass gilt:

$$g(t) = \text{kgV(Minimalpolynome in } \mathbb{F}_q[t] \text{ von } \alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}).$$

Im Fall $b = 1$ heißt C BCH-Code im engeren Sinn.
Im Fall $n = q^m - 1$ heißt C primitiver BCH-Code.
[Die Reed-Solomon-Codes in Kapitel 10 sind Spezialfälle von primitiven BCH-Codes.]

Satz 8.2 *Ist $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ ein BCH-Code mit designiertem Abstand δ, so ist $d(C) \geq \delta$.*

Beweis:

$$\widetilde{\widetilde{H}} := \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix} \in M((\delta-1) \times n, \mathbb{F}_{q^m}),$$

$$[c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}] \in C \Leftrightarrow \widetilde{\widetilde{H}} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0. \qquad (*)$$

Sei $[c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}] \in C$ mit $w([c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}]) \leq \delta - 1$.
Zu zeigen ist: $c_0 = \cdots = c_{n-1} = 0$.
Seien $0 \leq i_1 < \cdots < i_{\delta-1} \leq n-1$ mit $c_j = 0$ für $j \in \{0, 1, \ldots, n-1\}$-$\{i_1, \ldots, i_{\delta-1}\}$.
$(*)$ gibt

$$\begin{pmatrix} \alpha^{i_1 \cdot b} & \alpha^{i_2 \cdot b} & \ldots & \alpha^{i_{\delta-1} \cdot b} \\ \vdots & \vdots & & \vdots \\ \alpha^{i_1 \cdot (b+\delta-2)} & \alpha^{i_2 \cdot (b+\delta-2)} & \ldots & \alpha^{i_{\delta-1} \cdot (b+\delta-2)} \end{pmatrix} \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_{\delta-1}} \end{pmatrix} = 0.$$

Es ist

$$\det(\text{diese Matrix}) = \alpha^{i_1 \cdot b} \cdot \ldots \cdot \alpha^{i_{\delta-1} \cdot b} \cdot \det \begin{pmatrix} 1 & \ldots & 1 \\ \alpha^{i_1} & \ldots & \alpha^{i_{\delta-1}} \\ \vdots & & \vdots \\ \alpha^{i_1 \cdot (\delta-1)} & \ldots & \alpha^{i_{\delta-1} \cdot (\delta-1)} \end{pmatrix} \neq 0,$$

denn die Matrix rechts ist eine (transponierte) Vandermonde-Matrix. Also ist

$$\begin{pmatrix} c_{i_1} \\ \vdots \\ c_{i_{\delta-1}} \end{pmatrix} = 0,$$

also sind alle $c_j = 0$. □

Beispiel 8.3 Binäre Hamming-Codes, Beispiel 7.6: Dort wurde ein zyklischer Code $C \subset \frac{\mathbb{F}_2[t]}{(t^n-1)}$ mit $n = 2^r - 1$ und Erzeugerpolynom

$$g(t) = \text{Minimalpolynom von } \beta$$

betrachtet, wobei $\beta \in \mathbb{F}_{2^r} - \{0\}$ die Ordnung $o(\beta) = 2^r - 1$ hat. Es war gezeigt worden, daß C ein binärer Hamming-Code ist.
Satz 6.18 (c) $\Rightarrow g(\beta^2) = 0 = g(\beta)$. Also ist C ein BCH-Code im engeren Sinne (b=1 in Definition 8.1) zu β und β^2, d.h. mit designiertem Abstand $\delta = 3$.
Satz 8.2 gibt $d(c) \geq 3$. Allerdings wissen wir schon $d(c) = 3$.

Beispiel 8.4 $q = p = 2, n = 2^6 - 1 = 63, \alpha \in \mathbb{F}_{2^6} - \{0\}$ mit $o(\alpha) = 63$, d.h. α ist Erzeuger der endlichen Gruppe $(\mathbb{F}_{2^6} - \{0\}, \cdot)$.
Sei $C \subset \frac{\mathbb{F}_2[t]}{(t^n-1)}$ der zyklische Code mit Erzeugerpolynom

$$\begin{aligned} g(t) &= (\text{Minimalpolynom von } \alpha) \cdot (\text{Minimalpolynom von } \alpha^3) \\ &= m_1(t) \cdot m_3(t). \end{aligned}$$

Satz 6.18 $\Rightarrow$

$$\begin{aligned} m_1(t) &\quad \text{hat die Nullstellen } \alpha^i \text{ mit } i = 1, 2, 4, 8, 16, 32, \\ m_3(t) &\quad \text{hat die Nullstellen } \alpha^i \text{ mit } i = 3, 6, 12, 24, 48, 33, \\ m_1(t) &= \prod_{i=1,2,4,8,16,32} (t - \alpha^i) \in \mathbb{F}_2[t], \\ m_3(t) &= \prod_{i=3,6,12,24,48,33} (t - \alpha^i) \in \mathbb{F}_2[t], \end{aligned}$$

also $\deg m_1(t) = 6 = m_3(t)$, $\deg g(t) = 12$.

$g(t)$ hat die Nullstellen $\alpha, \alpha^2, \alpha^3, \alpha^4,\ (\alpha^6, \alpha^8, \alpha^{12}, \alpha^{16}, \alpha^{24}, \alpha^{32}, \alpha^{33}, \alpha^{48})$,
also ist $g(t) = \text{kgV}$ (Minimalpolynome zu $\alpha, \alpha^2, \alpha^3, \alpha^4$).
Der zyklische Code C ist ein primitiver BCH-Code im engeren Sinne (nämlich $b = 1$) mit designiertem Abstand $\delta = 5$. Also ist $d(C) \geq 5$.
Ohne Beweis: $d(C) = 5$. Also ist C ein $[63, 51, 5]$-Code.

Bemerkungen 8.5 (a) Die BCH-Codes sind viel studiert worden. Es gibt viele Abschätzungen und präzise Aussagen in Spezialfällen zu

$$\dim C = n - \deg\ g(t) \quad \text{und zu} \quad d(c)\ (\geq \delta).$$

(b) Sehr lange BCH-Codes sind schlecht.

Mac-Williams-Sloane (1977) Seite 269:

Es gibt keine Folge von (C_{n_i}) von BCH-Codes, $C_{n_i} \in \frac{\mathbb{F}_q[t]}{(t^{n_i}-1)}$ mit $n_i \to \infty$, so dass die Informationsrate $\frac{\dim C_{n_i}}{n_i}$ und der relative Hamming-Abstand $\frac{d(C_{n_i})}{n_i}$ für $i \to \infty$ von Null weg beschränkt sind.

[Dagegen tun es die Goppa-Codes: Kapitel 12.]

(c) Aber für klein n (bis zu mehrere hundert) sind die BCH-Codes gut zu benutzen.

(d) Sie sind einfach zu kodieren und dekodieren.

Dekodieren von BCH-Codes

Bemerkung 8.6 (a) Situation: Gegeben ist ein BCH-Code $C \subset \frac{\mathbb{F}_q[t]}{(t^n-1)}$ im engeren Sinne ($b = 1$) mit designiertem Abstand $\delta = 2t + 1$ und mit Erzeugerpolynom

$$g(t) = \text{kgV}(\text{Minimalpolynome in } \mathbb{F}_q[t] \text{ von } \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}),$$

bei $\alpha \in \mathbb{F}_{q^m} - \{0\}$ mit Ordnung $o(\alpha) = n$ (natürlich teilt n dann $q^m - 1$).

(b) Wegen $d(C) \geq \delta = 2t+1$ ist C t-fehlerkorrigierend (Definition 1.3 (c)). Das heißt: Sind $c \in C$ und $R \in \frac{\mathbb{F}_q[t]}{(t^n-1)}$ mit $d_H(c, R) \leq t$, so ist c dadurch eindeutig bestimmt, d. h. $\nexists\ \widetilde{c} \in C$ mit $\widetilde{c} \neq C$ und $d_H(\widetilde{c}, R) \leq t$.

(c) Ziel ist es, Objekte und einen Algorithmus anzugeben, mit denen man in dieser Situation c finden kann.

Definition 8.7 Gegeben sind: die Situation in Bemerkung 8.6 (a) und Wörter c und R wie in Bemerkung 8.6 (b),

$$\begin{aligned} c = [c(t)] &\in C \text{ ist das gesuchte Wort,} \\ c(t) &= c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}, \\ R = [R(t)] &\in \frac{\mathbb{F}_q[t]}{(t^n - 1)} \text{ ist das empfangene Wort,} \\ R(t) &= R_0 + R_1 t + \ldots, R_{n-1} t^{n-1}. \end{aligned}$$

Annahme: Die Anzahl der Fehler in R ist $\leq t$. Dann ist

$$\begin{aligned} E := R - c &= [R(t) - c(t)] = [E(t)] \text{ der Fehlervektor,} \\ E(t) = R(t) - c(t) &= (R_0 - C_0) + (R_1 - c_1)t + \cdots + (R_{n-1} - c_{n-1})t^{n-1} \\ &= E_0 + E_1 t + \cdots + E_{n-1} t^{n-1}. \end{aligned}$$

Man definiert

$$\begin{aligned} M &:= \{i \in \{0, 1, \ldots, n-1\} \mid E_i \neq 0\}, \\ e &:= |M| \quad (\leq t \text{ nach Annahme}), \\ \sigma(z) &:= \prod_{k \in M} (1 - \alpha^k \cdot z) \in \mathbb{F}_{q^m}[z], \\ \omega(z) &:= \sum_{k \in M} E_k \cdot \alpha^k \cdot \prod_{j \in M - \{k\}} (1 - \alpha^j \cdot z) \in \mathbb{F}_{q^m}[z]. \end{aligned}$$

Bemerkungen 8.8 Bemerkung 8.6 gab die Situation, in der man dekodieren will. Definition 8.7 gab die nötigen Objekte, vor allem $\sigma(z)$ und $w(z)$. Lemma 8.9 sagt, warum und wie sie ausreichen, um c zu finden.
Satz 8.10 gibt 3 Eigenschaften und eine darauf fußende Charakterisierung von $\sigma(z)$ und $\omega(z)$.
Satz 8.11 ist der Euklidische Algorithmus mit Zusatzinformation. Bemerkung 8.12 sagt, wie man mit 8.10 und 8.11 und R (und natürlich dem Code C) $\sigma(z)$ und $\omega(z)$ berechnet.

Lemma 8.9 *In der Situation von 8.6 und 8.7 gilt:*

(a) Fehler in Position $i \in \{0, \ldots, n-1\} \iff i \in M \iff \sigma(\alpha^{-i}) = 0$.
[Deshalb nennt man $\sigma(z)$ "error locater".]

(b) Bei $i \in M$ ist

$$E_i = \frac{-\omega(\alpha^{-i})}{\sigma'(\alpha^{-i})}.$$

[Deshalb nennt man $\omega(z)$ "error evaluator".]

(c) Wenn man $\sigma(z)$ und $\omega(z)$ kennt, kann man die Fehler im empfangenen Wort R korrigieren und das gesendete Wort c bestimmen.

Beweis: (a) ok.
(b)

$$\begin{aligned}
\sigma(z) &= \prod_{k\in M}(1-\alpha^k z),\\
\sigma'(z) &= \sum_{k\in M}(-\alpha^k)\cdot\prod_{j\in M-\{k\}}(1-\alpha^j z),\\
\sigma'(\alpha^{-i}) &= (-\alpha^i)\cdot\prod_{j\in M-\{i\}}(1-\alpha^{j-i})\neq 0,\\
\omega(z) &= \sum_{k\in M}E_k\alpha^k\prod_{j\in M-\{k\}}(1-\alpha^j z),\\
\omega(\alpha^{-i}) &= E_i\alpha^i\prod_{j\in M-\{i\}}(1-\alpha^{j-i}).
\end{aligned}$$

(c) Das folgt aus (a) und (b): $\sigma(z)$ gibt die Fehlerpositionen, $\sigma(z)$ und $\omega(z)$ geben die Fehlerwerte. □

Satz 8.10 *Situation wie in 8.6 + 8.7 + 8.9. Sei*

$$\begin{aligned}
\rho(z) &= \sum_{k=0}^{2t-1}R(\alpha^{k+1})\cdot z^k\in\mathbb{F}_{q^m}[z]\\
&= \sum_{k=0}^{2t-1}E(\alpha^{k+1})\cdot z^k,
\end{aligned}$$

die zweite Gleichung gilt, denn $E(t)=R(t)-c(t)$ und $c(\alpha^{k+1})=0$ für $1\le k+1\le 2t$, wegen $c\in C$ und der Definition von C.

(a) $\deg\sigma(z)=e\le t,\quad deg\ \omega(z)<e\le t,\quad \sigma(0)=1.$

(b) $\mathrm{ggT}(\sigma(z),\omega(z))=1.$

(c) $\omega(z)\equiv\sigma(z)\cdot\rho(z)\mod z^{2t}.$

(d) Erfüllen $\widetilde{\sigma}(z),\ \widetilde{\omega}(z)\in\mathbb{F}_{q^m}[z]$ die Eigenschaften

(i) $\deg\widetilde{\sigma}(z)\le t,\ \deg\widetilde{\omega}(z)<t,$

(ii) $\widetilde{\omega}(z)\equiv\widetilde{\sigma}(z)\cdot\rho(z)\mod z^{2t},$

so ist

$$\sigma(z) = \frac{\widetilde{\sigma}(z)}{\mathrm{ggT}(\widetilde{\sigma}(z), \widetilde{\omega}(z))} \quad \text{und} \quad \omega(z) = \frac{\widetilde{\omega}(z)}{\mathrm{ggT}(\widetilde{\sigma}(z), \widetilde{\omega}(z))}.$$

Hier ist ggT(..) *a priori nur eindeutig bis auf ein skalares Vielfaches, und dieses kann und muß geeignet gewählt werden.*

Beweis:

(a) ok.

(b) Die Nullstellen von $\sigma(z)$ sind genau die Elemente der Menge $\{\alpha^{-i} \mid i \in M\} \subset \mathbb{F}_{q^m}$. Für $i \in M$ ist

$$\omega(\alpha^{-i}) = E_i \alpha^i \prod_{j \in M - \{i\}} (1 - \alpha^{j-i}) \neq 0.$$

Also haben $\sigma(z)$ und $\omega(z)$ keine Nullstelle gemeinsam. Also ist $\mathrm{ggT}(\sigma(z), \omega(z)) = 1$.

(c) Man kann in dem formalen Potenzreihenring $\mathbb{F}_{q^m}[[z]]$ rechnen. Wegen $\sigma(0) = 1$ ist $\sigma(z)$ darin eine Einheit, also invertierbar. Daher ist die Behauptung in (c) äquivalent zur Behauptung

$$\frac{\omega(z)}{\sigma(z)} \equiv \rho(z) \mod z^{2t}.$$

Die wird durch folgende Rechnung bewiesen.

$$\begin{aligned}
\frac{\omega(z)}{\sigma(z)} &= \sum_{i \in M} \frac{E_i \alpha^i}{1 - \alpha^i z} = \sum_{i \in M} E_i \cdot z^{-1} \cdot \sum_{k=1}^{\infty} (\alpha^i z)^k \\
&= \sum_{k=1}^{\infty} z^{k-1} \cdot \sum_{i \in M} E_i (\alpha^k)^i \\
&= \sum_{k=1}^{\infty} z^{k-1} \cdot E(\alpha^k) \\
&\equiv \sum_{k=1}^{2t} z^{k-1} \cdot E(\alpha^k) \mod z^{2t} \\
&= \sum_{k=1}^{2t} z^{k-1} \cdot R(\alpha^k) = \rho(z).
\end{aligned}$$

Die vorletzte Gleichung benutzt $c(\alpha^k) = 0$, also $E(\alpha^k) = R(\alpha^k)$, für $1 \leq k \leq 2t$.

(d) Das wird in zwei Schritten gezeigt. Im 1. Schritt wird gezeigt, daß $\sigma(z)$ ein Teiler von $\widetilde{\sigma}(z)$ ist. Dann gibt es ein $\gamma(z) \in \mathbb{F}_{q^m}[z]$ mit

$$\widetilde{\sigma}(z) = \gamma(z) \cdot \sigma(z).$$

Im 2. Schritt wird $\widetilde{\omega}(z) = \gamma(z) \cdot \omega(z)$ gezeigt. Daher und wegen (b) ist $\mathrm{ggT}(\widetilde{\sigma}(z), \widetilde{\omega}(z)) = \gamma(z)$ (bis auf ein beliebiges skalares Vielfaches) und

$$\sigma(z) = \frac{\widetilde{\sigma}(z)}{\mathrm{ggT}(\widetilde{\sigma}(z), \widetilde{\omega}(z))} \quad \text{und} \quad \omega(z) = \frac{\widetilde{\omega}(z)}{\mathrm{ggT}(\widetilde{\sigma}(z), \widetilde{\omega}(z))}.$$

1. Schritt: Es reicht zu zeigen: $\widetilde{\sigma}(\alpha^{-i}) = 0$ für $i \in M$.

Dazu wird benutzt, dass wegen (ii) $(\widetilde{\omega}(z) \equiv \widetilde{\sigma}(z) \cdot \rho(z)) \mod z^{2t})$ und wegen $\deg \widetilde{\omega}(z) \leq t-1$ (Teil von (i)) die Koeffizienten von $z^t, z^{t+1}, \ldots, z^{2t-1}$ in $\widetilde{\sigma}(z) \cdot \rho(z)$ verschwinden.

Für $t \leq k \leq 2t-1$ ist der Koeffizient von z^k in $\widetilde{\sigma}(z) \cdot \rho(z)$

$$\begin{aligned}
0 \overset{!}{=} & \sum_{i+j=k} \widetilde{\sigma}_i \cdot R(\alpha^{j+1}) \quad (\text{mit } 0 \leq i \leq t,\ 0 \leq j \leq k \leq 2t-1) \\
& \qquad \text{bei } \widetilde{\sigma}(z) = \sigma_0 + \sigma_1 \cdot z + \cdots + \sigma_t \cdot z^t \\
= & \sum_{i+j=k} \widetilde{\sigma}_i \cdot E(\alpha^{j+1}) \quad (\text{wegen } 1 \leq j+1 \leq 2t) \\
= & \sum_{i+j=k} \widetilde{\sigma}_i \cdot \sum_{l \in M} E_l \cdot (\alpha^{j+1})^l \\
= & \sum_{l \in M} E_l \cdot \alpha^{(k+1)l} \cdot \sum_{i+j=k} \widetilde{\sigma}_i \cdot (\alpha^{-l})^i \\
= & \sum_{l \in M} (\alpha^{k+1})^l \cdot E_l \cdot \widetilde{\sigma}(\alpha^{-l}).
\end{aligned}$$

Das kann man als Matrixgleichung schreiben,

$$\left(\alpha^{(k+1)\cdot l}\right)_{\substack{k=t,t+1,\ldots,t+l-1 \\ l \in M}} \cdot \left(E_l \cdot \widetilde{\sigma}(\alpha^{-l})\right)_{l \in M} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

der mittlere Spaltenvektor hat Länge $e = |M|$, der rechte hat Länge t.

Ein Teil der linken Matrix ist eine Vandermonde-Matrix und hat daher Determinante $\neq 0$,

$$\det\left(\alpha^{(k+1)l}\right)_{\substack{k=t,t+1,\ldots,t+e-1 \\ l \in M}} \neq 0.$$

$\Rightarrow$ der Spaltenvektor $\left(E_l \cdot \widetilde{\sigma}(\alpha^{-l})\right)_{l \in M} = 0$,
$\Rightarrow \forall\, l \in M \quad E_l \cdot \widetilde{\sigma}(\alpha^{-l}) = 0$,
$\Rightarrow \forall\, l \in M \quad \widetilde{\sigma}(\alpha^{-l}) = 0$.

2. Schritt: Nach dem 1. Schritt existiert ein $\gamma(z) \in \mathbb{F}_{q^m}[z]$ mit $\widetilde{\sigma}(z) = \gamma(z) \cdot \sigma(z)$. Es soll gezeigt werden, dass $\widetilde{w}(z) = \gamma(z) \cdot w(z)$ gilt.

Aus (ii) und (c) und dem 1. Schritt folgt

$$\begin{aligned} \widetilde{\omega}(z) - \gamma(z) \cdot \omega(z) &\equiv \widetilde{\sigma}(z) \cdot \rho(z) - \gamma(z) \cdot \sigma(z) \cdot \rho(z) \mod z^{2t} \\ &= (\widetilde{\sigma}(z) - \gamma(z) \cdot \sigma(z)) \cdot \rho(z) \\ &= 0 \cdot \rho(z) = 0. \end{aligned}$$

Die folgenden Gradabschätzungen zeigen aber auch

$$\deg(\widetilde{\omega}(z) - \gamma(z) \cdot \omega(z)) \leq 2t - 1.$$

Zusammen mit der Kongruenz zu 0 modulo z^{2t} gibt das wie gewünscht

$$\widetilde{\omega}(z) - \gamma(z) \cdot \omega(z) = 0.$$

Gradabschätzungen: $\deg \widetilde{\omega}(z) \leq t - 1$ nach Eigenschaft (i),

$$\begin{aligned} \deg(\gamma(z) \cdot \omega(z)) &= \deg \gamma(z) + \deg \omega(z) \\ &\leq \deg \widetilde{\sigma}(z) + \deg \omega(z) \\ &\leq t + (t-1) = 2t - 1. \end{aligned}$$

□

Wegen Satz 8.10 (c) ist $\omega(z)$ ein Vielfaches des $\mathrm{ggT}(\rho(z), z^{2t})$. Tatsächlich stößt man bei der Berechnung dieses ggT mit dem euklidischen Algorithmus auf solche $\widetilde{\sigma}(z)$ und $\widetilde{\omega}(z)$. Das wird in Bemerkung 8.12 ausgeführt.

Satz 8.11 *(Euklidischer Algorithmus mit Zusatzinformation)*
Sei K ein Körper, $a_0(t), a_1(t) \in K[t] - \{0\}$ mit $\deg a_0(t) \geq \deg a_1(t)$.

(a) Dann $\exists!\ m \in \mathbb{N}$ und $\exists!\ a_i, (t), q_i(t), \in K[t] \backslash \{0\}$ für $i = 1, \ldots, m+1$ mit

$$\begin{aligned} a_{i-1} &= q_i \cdot a_i + a_{i+1} \quad \text{für } i = 1, \ldots, m, \\ \textit{und} \quad a_m &= q_{m+1} \cdot a_{m+1} \\ \textit{und} \quad \deg a_{i+1} &< \deg a_i \quad \text{für } i = 1, \ldots, m. \end{aligned}$$

Dann ist

$$a_{m+1} = \mathrm{ggT}(a_0, a_1).$$

(b) *(Zusatzinformation) Man definiert rekursiv*

$$\begin{array}{llllll} f_0 := 1, & f_1 := 0, & f_{i+1} & := & f_{i-1} - q_i f_i & \text{für } i = 1, \ldots, m, \\ g_0 := 0, & g_1 := 1, & g_{i+1} & := & g_{i-1} - q_i g_i & \text{für } i = 1, \ldots, m. \end{array}$$

Dann gilt:

$$\begin{array}{ll} (I) & a_i = f_i \cdot a_0 + g_i \cdot a_1 \quad \text{für } i = 0, 1, \ldots, m+1, \\ (II) & \deg g_{i+1} \leq \deg a_0 - \deg a_i \quad \text{für } i = 0, 1, \ldots, m. \end{array}$$

Beweis: (a) wohlbekannt, Polynomdivision iterieren.

(b)Beweis mit Induktion.

(I) ist klar für $i = 0, 1$.

(II) ist klar für $i = 0$.

Induktionsschritt:

(I) Für $i \geq 1$ ist

$$\begin{array}{rcl} a_{i+1} & = & a_{i-1} - q_i a_i \\ & = & (f_{i-1} \cdot a_0 + g_{i-1} \cdot a_1) - q_i (f_i \cdot a_0 + g_i \cdot a_1) \\ & = & f_{i+1} \cdot a_0 + g_{i+1} \cdot a_1. \end{array}$$

(II) Für $i \geq 1$ ist

$$\begin{array}{rcl} \deg g_{i+1} & \leq & \max(\deg g_{i-1}, \deg(q_i g_i)), \\ \deg g_{i-1} & & \begin{cases} \leq \deg a_0 - \deg a_{i-2} < \deg a_0 - \deg a_i & \text{für } i \geq 2, \\ = -\infty < \deg a_0 - \deg a_1 & \text{für } i = 1, \end{cases} \\ \deg(q_i g_i) & = & \deg q_i + \deg g_i = (\deg a_{i-1} - \deg a_i) + \deg g_i \\ & \leq & (\deg a_{i-1} - \deg a_i) + \deg a_0 - \deg a_{i-1} \\ & = & \deg a_0 - \deg a_i. \end{array}$$

□

Bemerkung 8.12 Anwendung von 8.11 in der Situation von 8.6–8.10:

$$a_0(z) := z^{2t}, \quad a_1(z) := \rho(z),$$

$$\exists!\ i \text{ mit } \deg a_{i-1}(z) \geq t > \deg a_i(z).$$

Es ist

$$a_i(z) = f_i(z) \cdot z^{2t} + g_i(z) \cdot \rho(z)$$

und

$$\deg g_i(z) \leq \deg a_0(z) - \deg a_{i-1}(z) \leq 2t - t = t.$$

$g_i(z)$ und $a_i(z)$ erfüllen die Eigenschaften (i) und (ii) von $\widetilde{\sigma}(z)$ und $\widetilde{\omega}(z)$ in Satz 8.10 (d). Man erhält

$$\sigma(z) = \frac{g_i(z)}{\mathrm{ggT}(g_i(z), a_i(z))} \quad \text{und} \quad \omega(z) = \frac{a_i(z)}{\mathrm{ggT}(g_i(z), a_i(z)}.$$

9 MDS-Codes

Satz 9.1 *(Singleton-Schranke)*

(a) Ein (nicht notwendig linearer) $(n, |C|, d)$-Code $C \subset \mathbb{F}_q$ erfüllt

$$|C| \leq q^{n-d+1}.$$

(b) Ein linearer $[n, k, d]$-Code $C \subset \mathbb{F}_q^n$ erfüllt

$$k \leq n - d + 1,$$

$$\text{äquivalent:} \quad k + d \leq n + 1 \quad \text{bzw.} \quad d \leq n - k + 1.$$

Beweis:
(b) folgt aus (a).
(a) Für $1 \leq i_1 < i_2 < \cdots < i_{d-1} \leq n$ und $i = (i_1, \ldots, i_{d-1})$ sei $\mathrm{pr}_{(i)} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-(d-1)}$ die Projektion, die man durch Streichen der Einträge an den Positionen $i_1, i_2, \ldots, i_{d-1}$ erhält. Wegen $d(C) = d$ ist $(\mathrm{pr}_{(i)})_{|C} : C \to \mathbb{F}_q^{n-(d-1)}$ injektiv. Also ist $|C| \leq |\mathbb{F}^{n-(d-1)}| = q^{n-d+1}$. □

Definition 9.2 Ein (nicht notwendig linearer) $(n, |C|, d)$-Code $C \subset \mathbb{F}_q^n$ heißt MDS-Code ("maximum distance separable"), falls $|C| = q^{n-d+1}$ ist.

Bemerkungen 9.3 (a) Das ist äquivalent zu $\log_q |C| = n - d + 1$ bzw. $d + \log_q |C| = n + 1$ bzw. $d = n - \log_q |C| + 1$.

(b) Ein (linearer) $[n, k, d]$-Code ist ein MDS-Code $\iff k + d = n + 1$.

Satz 9.4 *(Existenz von linearen MDS-Codes)*
Sei $q = p^l$ mit p Primzahl, $l \in \mathbb{N}$. Sei $n \leq q - 1, 1 \leq k \leq n$. Dann gibt es einen linearen MDS-Code $C \subset \mathbb{F}_q^n$ mit $\dim C = k$. Das ist also ein $[n, k, n - k + 1]$-Code.

Beweis: Im Fall $n = q - 1$ hat man die Reed-Solomon-Codes von Lemma 10.2 (d). Im Fall $n < q - 1$ wendet man Lemma 9.8 (c) auf diese Reed-Solomon-Codes an. □

Lemma 9.5 *Sei $C \subset \mathbb{F}_q^n$ ein linearer $[n, k, d]$-Code und H eine Kontrollmatrix (H ist eine $(n - k) \times n$-Matrix). Dann ist*

$$d = \min(\widetilde{d} \mid \exists\ \widetilde{d} \text{ linear abhängige Spalten in } H).$$

Beweis: Erinnerung 1: $C = \{x \in \mathbb{F}_q^n \mid H \cdot x^{tr} = 0\}$.
Erinnerung 2: Bei einem linearen Code ist $d = \min(w(x) \mid x \in C - \{0\})$.
Damit ist das Lemma klar. □

Satz 9.6 *Sei $C \subset \mathbb{F}_q^n$ ein (linearer) $[n,k,d]$-Code.*
Äquivalent sind:

(α) C ist ein MDS-Code, d.h. $k+d=n+1$.

(β) Für jedes $i=(i_1,\ldots,i_{n-k})$ mit $1 \le i_1 < i_2 < \ldots, < i_{n-k} \le n$ ist die Einschränkung der Projektion

$$\mathrm{pr}_{(i)} : \mathbb{F}_q^n \to \mathbb{F}_q^k, \quad (x_1,\ldots,x_n) \to (x_j)_{j\in\{1,\ldots,n\}-\{i_1,\ldots,i_{n-k}\}}$$

auf C eine Bijektion $(\mathrm{pr}_{(i)})_{|C} : C \to \mathbb{F}_q^k$.

(γ) Je k Spalten einer Erzeugermatrix von C sind linear unabhängig.

(δ) Je $n-k$ Spalten einer Kontrollmatrix von C sind linear unabhängig.

(ϵ) Der duale Code $C^\perp \subset \mathbb{F}_q^n$ (Definition 2.7 (a)) ist ein MDS-Code.

(ζ) Zu je d Indices $\{i_1,\ldots,i_d\} \subset \{1,\ldots,n\}$ gibt es ein $x \in C$ mit

$$x_i \neq 0 \iff i \in \{i_1,\ldots,i_d\}.$$

Beweis:

$(\alpha) \Rightarrow (\beta)$: $d = n-k+1$. Daher ist $(\mathrm{pr}_{(i)})_{|C} : C \to \mathbb{F}_q^k$ injektiv.
Wegen $|C| = q^n = |\mathbb{F}_q^k|$ ist es auch surjektiv, also bijektiv.

$(\beta) \Rightarrow (\alpha)$: Für jedes i ist $(\mathrm{pr}_{(i)})_{|C}$ injektiv $\Rightarrow d \ge n-k+1$. Wegen Satz 9.1 ist $d = n-k+1$.

$(\beta) \Leftrightarrow (\gamma)$: Sei $i=(i_1,\ldots,i_{n-k})$ mit $1 \le i_1 < i_2 < \cdots < i_{n-k} \le n$.

(β) für dieses i
$\iff$ $(\mathrm{pr}_{(i)})_{|C}$ ist eine Bijektion
$\iff$ $(\mathrm{pr}_{(i)})_{|C}$ ist ein VR-Isomorphismus
$\iff$ $(\mathrm{pr}_{(i)})_{|C} : C \to \mathbb{F}_q^k$ bildet eine Basis von C auf eine Basis von $\mathbb{F}_q^k$ ab
$\iff$ Streicht man in einer Erzeugermatrix von C (eine $(k \times n)$-Matrix, deren Zeilen eine Basis von C bilden) die $n-k$ Spalten mit den Indices $i_1,\ldots,i_{n-k}$, so sind die k Zeilen der neuen Matrix eine Basis von $\mathbb{F}_q^k$
$\iff$ die neue $(k \times k)$-Matrix hat $\det \neq 0$
$\iff$ die k Spalten der neuen Matrix sind linear unabhängig.

$(\alpha) \Rightarrow (\delta)$: Mit $d = n - k + 1$ und Lemma 9.5.

$(\delta) \Rightarrow (\alpha)$: (δ) & Lemma 9.5 $\Rightarrow d \geq n - k + 1 \overset{\text{Satz 9.1}}{\Rightarrow} d = n - k + 1$.

$(\delta) \Leftrightarrow (\epsilon)$: Das folgt aus $(\delta) \Leftrightarrow (\alpha) \Leftrightarrow (\gamma)$ und Lemma 2.7 (c),

$$(\text{Kontrollmatrix von } C) = (\text{Erzeugermatrix von } C^{\perp}).$$

$(\alpha)\&(\beta) \Rightarrow (\zeta)$: Seien d verschiedene Indices $i_1, ..., i_d \in \{1, ..., n\}$ gegeben.
Sei $i' := (i_1, \ldots, i_{d-1})$, es ist $d - 1 = n - k$ nach (α),
und $\text{pr}_{(i')} : C \to \mathbb{F}_q^k$ ist eine Bijektion nach (β).
Das Urbild x unter $\text{pr}_{(i')}$ von

$$(y_j)_{j \in \{1,\ldots,n\} - \{i_1,\ldots,i_{d-1}\}} \quad \text{mit} \quad y_j = \begin{cases} 0, & \text{falls } \ j \neq i_d \\ 1, & \text{falls } \ j = i_d \end{cases}$$

erfüllt die Behauptung in (ζ), denn

$$x_{i_d} = 1 \Rightarrow x \neq 0 \Rightarrow w(x) \geq d \Rightarrow x_{i_l} \neq 0 \text{ für } 1 \leq l \leq d - 1.$$

$(\zeta) \Rightarrow (\alpha)$: Zu $(i_1, \ldots, i_{d-1}) := (1, \ldots, d-1)$ und $i_d =: l \in \{d, d+1, \ldots, n\}$ gibt es nach (ζ) ein Wort $x^{(l)} \in C$ mit $x_j^{(l)} \neq 0 \Leftrightarrow j \in \{1, \ldots, d-1\} \cup \{l\}$.
Die Worte $x^{(d)}, x^{(d+1)}, \ldots, x^{(n)}$ sind offenbar linear unabhängig:

$$(* \mid \ddots).$$

Also ist $\dim C \geq n - d + 1$ und $|C| \geq q^{n-d+1}$. Nach Satz 9.1 und Definition 9.2 ist C ein MDS - Code. □

Bemerkung 9.7 (β) sagt, dass man k beliebige Einträge als Informationssymbole und die anderen $n - k$ Einträge als Kontrollsymbole benutzen kann (Definition in Lemma 2.3 (c)).

Definition/Lemma 9.8 *Sei $C \subset \mathbb{F}_q^n$ ein $[n, k, d]$-Code. Sei $1 \leq l \leq k - 1$ und $1 \leq i_1 < i_2 < \cdots < i_l \leq n,\ i = (i_1, \ldots, i_l)$.*

(a) (Definition) Dann ist

$$\begin{aligned} C^{(i)} &:= \{(x_j)_{j \in \{1\ldots,n\} - \{i_1,\ldots,i_l\}} \mid x \in C, x_j = 0 \text{ für } j \in \{i_1, \ldots, i_l\}\} \subset \mathbb{F}_q^{n-l} \\ &= \text{Bild}\left(\text{pr}_{(i)} : C \cap \{x \in \mathbb{F}_q^n \mid x_j = 0 \text{ für } j \in \{i_1, ..., i_l\}\} \to \mathbb{F}_q^{n-l}\right). \end{aligned}$$

Man sagt, dass man den Code $C^{(i)}$ aus C durch <u>Verkürzen</u> erhält.

(b) (Lemma) $C^{(i)}$ ist ein $[n - l, k', d']$-Code mit $k - l \leq k' \leq k$ und $d' \geq d$.

(c) (Lemma) Ist C ein MDS-Code, so auch $C^{(i)}$. Dann ist $C^{(i)}$ ein $[n-l, k-l, d]$-Code.

Beweis: (a) Definition.
(b) Durch Ergänzen von Nullen werden aus Wörtern in $C^{(i)}$ Wörter in C. Daraus folgt $k' \leq k$ und $d' \geq d$.

Jede der Bedingungen $x_j = 0$ erniedrigt die Dimension höchstens um 1. Daraus folgt $k - l \leq k'$.

(c) $k' + d' \geq (k-l) + d = k + d - l = n + 1 - l = (n-l) + 1$. Mit Satz 9.1 folgt Gleichheit, $k' + d' = (n-l) + 1$. Daher ist $C^{(i)}$ ein MDS-Code, und es ist $k' = k - l, d' = d$ □

Beispiele 9.9 Kapitel 10 wird zeigen: Es gibt einen $[255, 251, 5]$-MDS-Code, ein Reed-Solomon-Code.
Durch Verkürzen erhält man einen $[32, 28, 5]$-MDS-Code und einen $[28, 24, 5]$-MDS-Code. Diese beiden werden im CD-Spieler benutzt.

10 Reed-Solomon-Codes

Bemerkung 10.1 a) Reed-Solomon-Codes (RS-Codes) sind Spezialfälle von BCH-Codes. Aber man kann die Reed-Solomon-Codes im engeren Sinn auch anders beschreiben (Satz 10.4), in einer Weise, die zu Goppa-Codes (Kapitel 12) und zu algebraisch-geometrischen Codes (nicht in dieser Vorlesung) führt.

b) Reed-Solomon-Codes sind MDS-Codes, siehe unten.

Definition/Lemma 10.2 *(a) (Definition) Ein BCH-Code* $C \subset \frac{\mathbb{F}_q\{t\}}{(t^n-1)}$ *mit designiertem Abstand* δ *und mit Erzeugerpolynom*

$$g(t) = \text{kgV}\,(\text{Minimalpolynome in } \mathbb{F}_q[t] \text{ von } \alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2})$$

mit $b \in \mathbb{N}$, $\alpha \in \mathbb{F}_{q^m} - \{0\}$, $o(\alpha) = n$ *(also* $n|(q^m-1)$*) ist ein Reed-Solomon-Code, falls er primitiv ist, d.h.* $n = q^m - 1$, *und falls* $m = 1$ *gilt.*

Er heißt Reed-Solomon-Code im engeren Sinn, falls zusätzlich $b = 1$ *ist.*

(b) (Lemma) Dann ist offenbar $n = q - 1$,

$$(\text{Minimalpolynom von } \alpha^j) = (t - \alpha^j),$$

$$g(t) = \prod_{j=b}^{b+\delta-2} (t - \alpha^j).$$

(c) (Lemma) Es ist $t^n - 1 = g(t) \cdot h(t)$ *mit*

$$h(t) = \prod_{j=b+\delta-1}^{n+b-1} (t - \alpha^j),$$

$$\dim C = \deg h(t) = n - \delta + 1.$$

(d) (Lemma) C *ist ein* $[n, n-\delta+1, \delta]$ *- MDS-Code.*

(e) (Lemma) Satz 7.5 gibt die Kontrollmatrix

$$H = \left(\alpha^{(b+i)j}\right)_{\substack{i=0,1,\ldots,\delta-2 \\ j=0,1,\ldots,n-1}}.$$

Eine andere Kontrollmatrix erhält man mit Satz 7.4 (c).

Beweis:

(a) Definition.

(b) Klar.

(c) Wegen $o(\alpha) = n = q^m - 1$ ist $\mathbb{F}_{q^m} - \{0\} = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, daher ist $t^n - 1 = \prod_{j=1}^{n-1}(t - \alpha^j)$, und $h(t)$ ist wie beschrieben.

$\dim C = \deg h(t)$ folgt aus 7.4 (a) + (c).

(d) Nach Satz 8.2 ist $d(C) \geq \delta$. Es ist

$$d(C) + (n - \delta + 1) \geq \delta + (n - \delta + 1) = n + 1.$$

Wegen Satz 9.1 ist daher $d(C) = \delta$, und C ist ein MDS-Code.

(e) Die Abbildung $\Psi : \mathbb{F}_q \to M(1 \times 1, \mathbb{F}_q)$ und die Matrix $\widetilde{H}$ sind $\Psi = \mathrm{id}$ und $\widetilde{H} = \left(\alpha^{(b+i)j}\right)_{\substack{i=0,1,...,\delta-2 \\ j=0,1,...,n-1}}$. Die Teilmatrix $\left(\alpha^{(b+i)j}\right)_{\substack{i=0,1,...,\delta-2 \\ j=0,1,...,\delta-2}}$ ist eine Vandermonde-Matrix und hat det $\neq 0$. Daher hat $\widetilde{H}$ linear unabhängige Zeilen, und $\widetilde{H}$ ist selber eine Kontrollmatrix. □

Definition/Satz 10.3 *(a) (Erinnerung an Definition/Lemma 2.11) Ein erweiterter RS-Code $\overline{C}$ entsteht aus einem RS-Code $C \subset \mathbb{F}_q^n \cong \frac{\mathbb{F}_q[t]}{(t^n-1)}$ folgendermaßen:*

$$\overline{C} = \{(x_1, \ldots, x_n, x_{n+1}) \mid (x_1, \ldots, x_n) \in C, \sum_{i=1}^{n+1} x_i = 0 \text{ in } \mathbb{F}_q\} \subset \mathbb{F}_q^{n+1}.$$

$\overline{C}$ ist ein $[n+1, n-\delta+1, d(\overline{C})]$- Code mit

$$\delta + 1 \geq d(\overline{C}) \geq \delta = d(C).$$

(b) (Satz) Sei C ein RS-Code im engeren Sinn, dann ist $d(\overline{C}) = \delta + 1$ und $\overline{C}$ ist ein $[n+1, n-\delta+1, \delta+1]$-MDS - Code.

Beweis: (a) Siehe Definition/Lemma 2.11.

(b) Es reicht $d(\overline{C}) = \delta + 1$ zu zeigen, d.h. $w(x) \geq \delta + 1 \; \forall \; x \in \overline{C} - \{0\}$.

1. Fall, $x \in \overline{C}$ mit $x_{n+1} \neq 0 : (x_1, \ldots, x_n) \in C - \{0\}$ hat Gewicht $\geq \delta$ also ist $w(x_1, \ldots x_{n+1}) \geq \delta + 1$.

2. Fall, $x \in \overline{C} - \{0\}$ mit $x_{n+1} = 0$: Dann ist $x_1 + \cdots + x_n = 0$. Also ist 1 eine Nullstelle von $x_1 + x_2 t + x_3 t^2 + \cdots + x_n t^{n-1} =: \xi(t) \in \mathbb{F}_q[t]$.

Nach Definition von C sind auch $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ Nullstellen von $\xi(t)$ (denn betrachtet wird ein RS-Code im engeren Sinn, also $b = 1$). Nun verläuft das Argument wie im Beweis von Satz 8.2. Es ist

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{(\delta-1)2} & \ldots & \alpha^{(\delta-1)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Je δ Spalten geben eine Vandermonde-Matrix, sind also linear unabhängig. Daher ist $w(x_1, \ldots, x_n) \geq \delta + 1$. □

Satz 10.4 *Sei $\alpha \in \mathbb{F}_q - \{0\}$ mit $o(\alpha) = q - 1$, also $\mathbb{F}_q - \{0\} = \{1, \alpha, \alpha^2, ..., \alpha^{q-2}\}$. Sei $n := q - 1$ und $1 \leq l < n$. Sei*

$$\mathbb{F}_q[t]_{\leq l} := \{f(t) \in \mathbb{F}_q[t] \mid \deg f(t) \leq l\}.$$

Es ist dim $\mathbb{F}_q[t]_{\leq l} = l + 1$. Seien

$$\begin{aligned} C &:= \{(f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1})) \mid f \in \mathbb{F}_q[t]_{\leq l}\}, \\ \text{und } \widetilde{C} &:= \{(f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1}), f(0)) \mid f \in \mathbb{F}_q[t]_{\leq l}\}. \end{aligned}$$

(a) Dann ist C der RS-Code im engeren Sinn zu $n = q - 1$, zu α und zu $\delta = n - l$.

(b) Es ist $\widetilde{C} = \overline{C}$ der erweiterte RS-Code aus Satz 10.3.

Beweis: (a)

$$f \neq 0 \;\Rightarrow\; w((f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1}))) \geq n - l,$$

denn ein Polynom vom Grad $\leq l$ kann höchstens l Nullstellen haben.
Daher ist auch die natürliche Abbildung $\mathbb{F}_q[t]_{\leq l} \to C$ injektiv, und $\dim C \stackrel{!}{=} \dim \mathbb{F}_q[t]_{\leq l} = l + 1$.
Nun hat man $d(C) \geq n - l$. Mit Satz 9.1 folgt $d(C) = n - l$. Also ist C ein $[n, l + 1, n - l]$-MDS-Code.
Es reicht nun zu zeigen

$$\sum_{i=0}^{n-1} f(\alpha^i) \cdot (\alpha^j)^i = 0 \text{ für } j = 1, \ldots, (n - l) - 1.$$

Dann ist C im Reed-Solomon-Code im engeren Sinn (zu $n = q - 1,\ \alpha,\ \delta = n - l$) enthalten, und wegen gleicher Dimension sind sie gleich.

Sei $f(t) = \sum_{k=0}^{l} f_k \cdot t^k$.

$$\begin{aligned} \sum_{i=0}^{n-1} f(\alpha^i) \cdot (\alpha^j)^i &= \sum_{k=0}^{l} f_k \cdot \sum_{i=0}^{n-1} (\alpha^{k+j})^i = 0, \\ \text{denn } \sum_{i=0}^{n-1} (\alpha^{k+j})^i &= 0, \end{aligned}$$

$$\text{denn } 1 \le k+j \le l + (n-l-1) = n-1, \qquad \text{also } 1 - \alpha^{k+j} \neq 0$$

$$\text{und } (1-\alpha^{k+j}) \Big(\sum_{i=0}^{n-1} (\alpha^{k+j})^i \Big) = 1 - (\alpha^{k+j})^n = 0$$

[analog zu $\sum_{j=0}^{m-1} e^{2\pi i \frac{k}{m} \cdot j} = 0$ bei $\frac{k}{m} \notin \mathbb{Z}$].

(b) Es reicht zu zeigen

$$\sum_{i=0}^{n-1} f(\alpha^i) + f(0) = 0.$$

Es ist

$$\begin{aligned} \sum_{i=0}^{n-1} f(\alpha^i) + f(0) &= \sum_{k=0}^{l} f_k \cdot \Big(\sum_{i=0}^{n-1} \alpha^{k \cdot i} + 0^k \Big) \\ &\quad (\text{mit } 0^0 = 1,\ 0^k = 0 \text{ für } k > 0) \\ &= \sum_{k=1}^{l} f_k \cdot \sum_{i=0}^{n-1} (\alpha^k)^i + f_0 \cdot (n+1) \\ &= \sum_{k=1}^{l} f_k \cdot 0 + f_0 \cdot 0 = 0 \in \mathbb{F}_q. \end{aligned}$$

□

Beispiel 10.5 $q = 2^8 = 256$, $n = q - 1$ und $\delta = 5$ geben für jedes $b \in \{1, ..., 256\}$ einen Reed-Solomon-Code, der ein $[255, 251, 5]$-MDS-Code ist. Vergleiche Beispiel 9.9: Durch Verkürzen gewinnt man aus einem dieser Codes (ich weiß leider nicht, aus welchem) zwei MDS-Codes, einen $[32, 28, 5]$-Code und einen $[28, 24, 5]$-Code, die im CD-Spieler benutzt werden.

$M(n_1 \times n_2, \mathbb{F}_q) \to \mathbb{F}_q^{n_1 - n_2}$ gibt dann einen Code $M(n_1 \times n_2, \mathbb{F}_q)$

11 Schranken für Codes

Definition 11.1 Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

(a) Die Sphäre vom Radius d um 0 in $\mathbb{F}_q^n$ bezüglich Hamming-Metrik ist die Menge $\{x \in \mathbb{F}_q^n : w(x) = d\}$. Die Anzahl ihrer Elemente ist

$$S_q(n,d) := |\{x \in \mathbb{F}_q^n \mid w(x) = d\}| = \binom{n}{d} (q-1)^d.$$

Der Ball vom Radius d um 0 in $\mathbb{F}_q^n$ bezüglich der Hamming-Metrik ist die Menge $\{x \in \mathbb{F}_q^n \mid w(x) \leq d\}$. Die Anzahl seiner Elemente ist

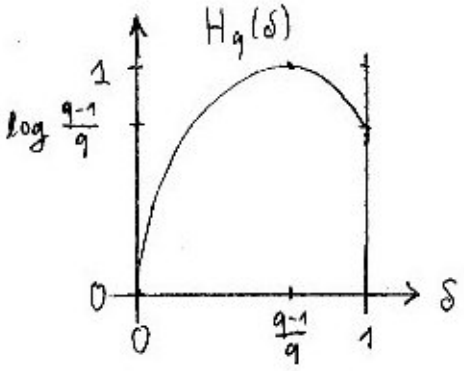
$$V_q(n,d) := |\{x \in \mathbb{F}_q^n \mid w(x) \leq d\}| = \sum_{i=0}^{d} \binom{n}{i} (q-1)^i.$$

(b) Die Entropiefunktion $H_q : [0,1] \to \mathbb{R}$ ist definiert durch

$$\begin{aligned} H_q(0) &:= 0, \quad H_q(1) := \log_q(q-1) \in]0,1[, \\ H_q(x) &:= x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x) \quad \text{für } x \in]0,1[. \end{aligned}$$

Satz 11.2 *(a) H_q ist stetig auf $[0,1]$ und differenzierbar auf $]0,1[$ mit*

$$\begin{aligned} H_q(0) &= 0, \quad H_q\left(\frac{q-1}{q}\right) = 1, \quad H_q(1) = \log_q(q-1) \in]0,1[, \\ H_q'(x) &= \log_q\left((q-1)\frac{1-x}{x}\right) \begin{cases} > 0 & \text{für } 0 < x < \frac{q-1}{q}, \\ = 0 & \text{für } x = \frac{q-1}{q}, \\ < 0 & \text{für } \frac{q-1}{q} < x < 1, \end{cases} \\ & \lim_{x \to 0} H_q'(x) = +\infty, \quad \lim_{x \to 1} H_q'(x) = -\infty, \\ H_q''(x) &= \frac{1}{\log_e q} \cdot \left(-\frac{1}{x} - \frac{1}{1-x}\right) < 0 \quad \text{für } 0 < x < 1. \end{aligned}$$



(b) Sei $\delta \in [0, \frac{q-1}{q}]$ fest. Dann ist

$$\lim_{n\to\infty}\left(\frac{1}{n}\log_q V_q(n,[\delta n])\right) = \lim_{n\to\infty}\left(\frac{1}{n}\log_q S_q(n,[\delta n])\right) = H_q(\delta).$$

Also wachsen für große n $V_q(n,[\delta n])$ und $S_q(n,[\delta n])$ ungefähr so wie $q^{n\cdot H_q(\delta)}$.

Beweis: (a) Man rechnet aus

$$\begin{aligned}
\lim_{\substack{x\to 0\\ x>0}} H_q(x) &= 0 - \lim_{\substack{x\to 0\\ x>0}}(x\log_q x) - 0 = 0 = H_q(0),\\
H_q(\frac{q-1}{q}) &= \frac{q-1}{q}\log_q(q-1) - \frac{q-1}{q}(\log_q(q-1) - \log_q q)\\
&\quad -(1-\frac{q-1}{q})\log_q(1-\frac{q-1}{q})\\
&= \frac{q-1}{q} + \frac{1}{q} = 1,\\
\lim_{\substack{x\to 1\\ x<1}} H_q(x) &= \log_q(q-1) - 0 - \lim_{\substack{x\to 1\\ x<1}}(1-x)\log_q(1-x) = \log_q(q-1) = H_q(1).
\end{aligned}$$

Bemerkung: für $a > 0$ und $b > 0$ ist

$$\log_a b = \frac{\log_e b}{\log_e a},$$

denn

$$e^{\log_e b} = b = a^{\log_a b} = (e^{\log_e a})^{\log_a b} = e^{\log_e a\cdot\log_a b}.$$

Mit dieser Bemerkung kann man $\log_q x = \frac{\log_e x}{\log_e q}$ und $\log_q(1-x) = \frac{\log_e(1-x)}{\log_e q}$ schreiben. Damit rechnet man für $0 < x < 1$ aus

$$\begin{aligned}
H_q'(x) &= \log_q(q-1) - \log_q x - x\cdot\frac{1}{x}\cdot\frac{1}{\log_e q}\\
&\quad + \log_q(1-x) - (1-x)\cdot\frac{-1}{1-x}\cdot\frac{1}{\log_e q}\\
&= \log_q(q-1) - \log_q x + \log_q(1-x)\\
&= \log_q\left((q-1)\cdot\frac{1-x}{x}\right)\\
&> 0\\
&\iff (q-1)\cdot\frac{1-x}{x} > 1\\
&\iff (q-1)\cdot\frac{1}{x} > 1 + (q-1)\\
&\iff x < \frac{q-1}{q}.
\end{aligned}$$

Genauso rechnet man für $0 < x < 1$ aus

$$H_q''(x) = \frac{1}{\log_e q} \cdot (-\frac{1}{x} - \frac{1}{1-x}) < 0.$$

(b) Zuerst eine
Behauptung: (Vergleich der Summanden in $V_q(n, [\delta n])$)

$$\text{Jeder Summand } \leq \text{ letzter Summand } = S_q(n, [\delta n]) = \binom{n}{[\delta n]} \cdot (q-1)^{[\delta n]}.$$

[Anschaulich: Mit wachsendem Radius sollten Sphären mehr Punkte erhalten. Aber Vorsicht: man könnte sich vorstellen, daß manche Sphären so unglücklich liegen, daß sie wenige Punkte enthalten.]

Beweis: Für $1 \leq i \leq \frac{n}{2}$ ist $\binom{n}{i-1} \leq \binom{n}{i}$ (das Pascalsche Dreieck ist spiegelsymmetrisch entlang der senkrechten Achse), und daher ist dann

$$\binom{n}{i-1} \cdot (q-1)^{i-1} < \binom{n}{i} \cdot (q-1)^i.$$

Aber für $\frac{n+1}{2} \leq i \leq [\delta n]$ ist $\binom{n}{i-1} \geq \binom{n}{i}$. Man muß dann vorsichtiger abschätzen. Folgende vorsichtigere Abschätzung funktioniert für alle i mit $1 \leq i \leq [\delta n]$:

$$\begin{aligned} \frac{\binom{n}{i}}{\binom{n}{i-1}} &= \frac{\frac{n!}{i!(n-i)!}}{\frac{n!}{(i-1)!(n-i+1)!}} = \frac{n-i+1}{i} = \frac{n+1}{i} - 1 \\ &\geq \frac{n+1}{[\delta n]} - 1 \geq \frac{n+1}{\delta(n+1)} - 1 = \frac{1}{\delta} - 1 \geq \frac{q}{q-1} - 1 = \frac{1}{q-1}. \end{aligned}$$

Daraus folgt die Behauptung. (□)

Damit ist

$$\binom{n}{[\delta n]}(q-1)^{[\delta n]} = S_q(n, [\delta n]) \leq V_q(n, [\delta n]) \leq (1 + [\delta n]) \cdot S_q(n, [\delta n]).$$

Es ist

$$\lim_{n\to\infty} \frac{\log_q(1 + [\delta n])}{n} = 0$$

wegen $\lim_{x\to\infty} \frac{\log_q x}{x} = 0$. Daher und wegen $\lim_{n\to\infty} \frac{[\delta n]}{n} = \delta$ ist

$$\begin{aligned} &\lim_{n\to\infty} \left(\frac{1}{n} \log_q S_q(n, [\delta n]) \right) = \lim_{n\to\infty} \left(\frac{1}{n} \log V_q(n, [\delta n]) \right), \\ = \ &\delta \cdot \log_q(q-1) + \lim_{n\to\infty} \left(\frac{1}{n} \log_q \binom{n}{[\delta n]} \right), \end{aligned}$$

falls dieser letzte Limes existiert!
Wegen der Bemerkung im Beweis von (a) ist

$$\frac{1}{n}\log_q \binom{n}{[\delta n]} = \frac{1}{n}\cdot \log_e \binom{n}{[\delta n]} \cdot (\log_e q)^{-1},$$

und man muß nur $\frac{1}{n}\log\binom{n}{[\delta n]}$ diskutieren.

Zitat: (Eine grobe Version der Stirlingschen Formel)

$$\log n! = n\cdot\log n - n + O(\log n) \quad \text{für } n\to\infty.$$

Anwendung der Stirlingschen Formel gibt das zweite Gleichheitszeichen in den folgenden Umformungen,

$$\begin{aligned}
\frac{1}{n}\log\binom{n}{[\delta n]} &= \frac{1}{n}(\log n! - \log[\delta n]! - \log(n-[\delta n])!) \\
&\overset{n \text{ groß}}{=} \frac{1}{n}(n\cdot\log n - n + O(\log n) - [\delta n]\log[\delta n] + [\delta n] + O(\log[\delta n]) \\
&\quad -(n-[\delta n])\log(n-[\delta n]) + (n-[\delta n]) + O(\log(n-[\delta n])) \\
&\qquad \text{(für großes } n \text{ ist } [\delta n]\approx \delta n, \text{ also)} \\
&\overset{n \text{ groß}}{\approx} \log n - \delta\log(\delta n) - (1-\delta)\log((1-\delta)n) + \frac{1}{n}O(\log n) \\
&= \log n - \delta\log\delta - \delta\log n - (1-\delta)\log(1-\delta) \\
&\quad -(1-\delta)\log n + \frac{1}{n}O(\log n) \\
&= -\delta\log\delta - (1-\delta)\log(1-\delta) + \frac{1}{n}O(\log n).
\end{aligned}$$

Also ist

$$\begin{aligned}
\lim_{n\to\infty}\left(\frac{1}{n}\log_q\binom{n}{[\delta n]}\right) &= (-\delta\log\delta - (1-\delta)\log(1-\delta))\cdot(\log_e q)^{-1} \\
&= -\delta\log_q\delta - (1-\delta)\log_q(1-\delta).
\end{aligned}$$

Bei beiden Gleichheitszeichen wird die Bemerkung im Beweis von (a) benutzt. Nun erhält man

$$\lim_{n\to\infty}\left(\frac{1}{n}\log_q V_q(n,[\delta n])\right) = \lim_{n\to\infty}\left(\frac{1}{n}\log_q S_q(n,[\delta n])\right) = H_q(\delta).$$

□

Definition 11.3 Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

(a) $A_q(n,d) := \max(M \in \mathbb{N} \mid \text{es existiert ein } (n,M,d)\text{-Code in } \mathbb{F}_q^n)$.

(b) Sei $0 < \delta \leq 1$.

$$\alpha_q(\delta) := \limsup_{\tilde{n}\to\infty} \left(\frac{1}{\tilde{n}} \log_q A_q(\tilde{n}, [\delta\tilde{n}]) \right).$$

Bemerkungen 11.4 (i) $\frac{[\delta\tilde{n}]}{\tilde{n}} \approx \delta$ in (b) ist ein "relativer Hammingabstand".

(ii) Die Größe $\alpha_q(\delta)$ steht in Beziehung zum Channel coding theorem von Shannon (Satz 1.7). Sie sagt, eine wie gute Informationsrate ($\approx \alpha_q(\delta)$) man mit sehr langen Codes ($\tilde{n} \to \infty$) erreichen kann, wenn man relativen Hamming-Abstand δ fordert.

(iii) Die genauen Werte von $A_q(n,d)$ und $\alpha_q(\delta)$ sind unbekannt. Satz 11.5 (b) gibt eine berühmte alte (1952/1957) untere Schranke für $\alpha_q(\delta)$, die erst 1982 mit Ideen der algebraischen Geometrie (Satz 11.6, ohne Beweis) verbessert wurde.

(iv) Die Sätze 11.7, 11.8 und 11.9 geben obere Schranken. Die Skizze in Bemerkung 11.10 zeigt alle Schranken zugleich.

Satz 11.5 *(Gilbert-Varshamov-Schranke, 1952/57)*
Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

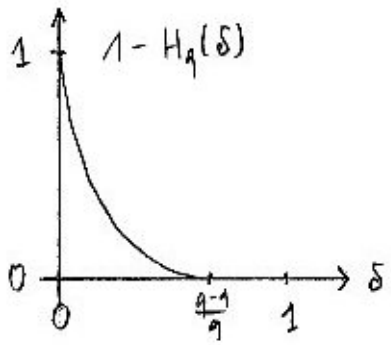
(a)

$$A_q(n,d) \geq \frac{q^n}{V_q(n, d-1)}.$$

(b)

$$\alpha_q(\delta) \geq 1 - H_q(\delta) \quad \text{für } 0 < \delta \leq \frac{q-1}{q}.$$

(Für $\delta = \frac{q-1}{q}$ ist $1 - H_q(\delta) = 1 - 1 = 0$.)



(c) (Verfeinerung von (a) mit linearen Codes) Sei

$$k = min(\tilde{k} \in \mathbb{N} \mid q^{\tilde{k}} \geq \frac{q^n}{V_q(n, d-1)}).$$

Dann gibt es einen linearen $[n, k, d]$-Code.

[Aus (c) folgt (a). Der unabhängige Beweis von (a) ist eigentlich überflüssig, aber er ist instruktiv.]

Beweis: (a) Sei $C \subset \mathbb{F}_q^n$ ein Code mit $d(C) = d$, zu dem man kein Wort hinzufügen kann, ohne daß der minimale Hamming-Abstand fällt. Dann ist

$$\mathbb{F}_q^n = \bigcup_{x \in C} (\text{Ball um } x \text{ mit Radius } d-1).$$

(nicht notwendig disjunkte Vereinigung) und

$$q^n = |\mathbb{F}_q^n| \leq |C| \cdot V_q(n, d-1),$$

also

$$\frac{q^n}{V_q(n, d-1)} \leq |C| \leq A_q(n, d).$$

(b)

$$\begin{aligned} \alpha_q(\delta) &:= \limsup_{\tilde{n} \to \infty} \frac{\log_q A_q(\tilde{n}, [\delta\tilde{n}])}{\tilde{n}} \geq \limsup_{\tilde{n} \to \infty} \left(1 - \frac{\log_q V_q(\tilde{n}, [\delta\tilde{n}] - 1)}{\tilde{n}}\right) \\ &= 1 - \lim_{\tilde{n} \to \infty} \frac{\log_q V_q(\tilde{n}, [\delta\tilde{n}] - 1)}{\tilde{n}} \overset{11.2}{=} 1 - H_q(\delta). \end{aligned}$$

(c) Behauptung: Sei $k_0 \in \mathbb{N}$ mit $q^{k_0} < \frac{q^n}{V_q(n,d-1)}$, und es gebe einen (linearen) $[n, k_0, d]$-Code. Dann gibt es einen (linearen) $[n, k_0 + 1, d]$- Code.

Wiederholte Anwendung der Behauptung liefert (c).

Beweis der Behauptung: Sei C ein $[n, k_0, d]$-Code. Aus

$$|C| \cdot V_q(n, d-1) = q^{k_0} \cdot V_q(n, d-1) < q^n = |\mathbb{F}_q^n|$$

folgt, dass es ein Wort $x \in \mathbb{F}_q^n - C$ mit $d_H(x, y) \geq d \; \forall \; y \in C$ gibt.
Behauptung: Der Code $\tilde{C} := C + \mathbb{F}_q \cdot x$ erfüllt $d(\tilde{C}) = d(C) = d$.
Beweis: Denn für $a \in \mathbb{F}_q \backslash \{0\}, y \in C$ ist $w(y) \geq d$ (schon bekannt) und

$$w(ax + y) = w(x + a^{-1}y) = d_H(x, -a^{-1}y) \geq d,$$

also ist $\forall \; \tilde{y} \in \tilde{C} \; w(\tilde{y}) \geq d$. □

Satz 11.6 *(Tsfasman/Vladut/Zink, 1982)*
Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

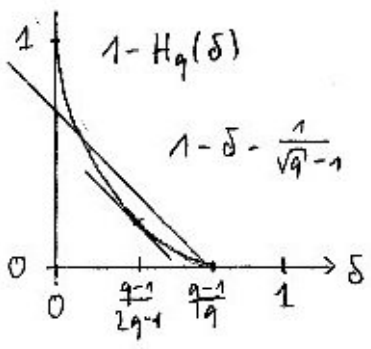
(a) (Hauptresultat) Für $q = p^2$ mit p Primzahl und $0 < \delta < 1$ ist

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q} - 1} \cdot .$$

(b) (Zusatz) Für gewisse q und δ ist diese Schranke besser als die Gilbert-Varshamov-Schranke. Die Kurve $\delta \to 1 - H_q(\delta)$ hat Steigung -1 genau bei $\delta_0 = \frac{q-1}{2q-1}$. Die Gerade $\delta \to 1 - \delta - \frac{1}{\sqrt{q}-1}$ (= neue Schranke) liegt bei δ_0 oberhalb der Kurve $\delta \to 1 - H_q(\delta)$, falls

$$1 - H_q(\delta_0) < 1 - \delta_0 - \frac{1}{\sqrt{q} - 1}$$

gilt.



Das ist erfüllt für $q \geq 43$, insbesondere für $p \geq 7, q = p^2$. Für $p \geq 7, q = p^2$ und δ nahe δ_0 ist die Tsfasman - Vladut - Zink Schranke daher besser als die Gilbert-Varshamov-Schranke.

Beweis: (a) Schwer, hier nicht. Mit Methoden der algebraischen Geometrie. Siehe

M.A. Tsfasman, S.G. Vladut, Th. Zink: On Goppa Codes wich are better than the Gilbert-Varshamov bound. Math. Nachrichten **109** (1982), 21-28.

Sie konstruieren "gute" Folgen (von Verallgemeinerungen?) von Goppa-Codes. Ihr Ergebnis wurde als spektakulär gewertet. Stichtenoth hat später vergleichbar starke elementarere Konstruktionen gefunden.

(b)

$$\begin{aligned} & 1 \stackrel{?}{=} H_q'(\delta_0) \stackrel{11.2(a)}{=} \log_q \left((q-1)(\frac{1}{\delta_0} - 1) \right) \\ \iff & q = (q-1)(\frac{1}{\delta_0} - 1) \\ \iff & 2q - 1 = (q-1)\frac{1}{\delta_0} \\ \iff & \delta_0 = \frac{q-1}{2q-1}. \end{aligned}$$

Die genannte Ungleichung ist äquivalent zu

$$1 + \frac{1}{\sqrt{q} - 1} < 1 - \delta_0 + H_q(\delta_0)$$

und die rechte Seite ist

$$\begin{aligned} = & \ 1 - \delta_0 + \delta_0 \log_q(q-1) - \delta_0 \log_q \delta_0 - (1-\delta_0) \log_q(1-\delta_0) \\ = & \ 1 - \delta_0 + \delta_0 \log_q(q-1) - \delta_0(\log_q(q-1) - \log_q(2q-1)) \\ & -(1-\delta_0)(\log_q q - \log_q(2q-1)) \\ = & \ \log_q(2q-1) \end{aligned}$$

Übung: Die Ungleichung ist für $q \geq 43$ erfüllt. □

In den Sätzen 11.7, 11.8 und 11.9 kommen nun drei obere Schranken.

Satz 11.7 *(= Satz 9.1, Singleton-Schranke)*
Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

(a) Es ist

$$A_q(n,d) \leq q^{n-d+1}.$$

(b) Für $0 < \delta \leq 1$ ist

$$\alpha_q(\delta) \leq 1 - \delta.$$

Beweis:

(a) Satz 9.1.

(b)

$$\alpha_q(\delta) =_{\text{Def}} \limsup_{\tilde{n} \to \infty} \frac{\log_q A_q(\tilde{n}, [\delta\tilde{n}])}{\tilde{n}} \leq \lim_{\tilde{n} \to \infty} \frac{\tilde{n} - [\delta\tilde{n}] + 1}{\tilde{n}} = 1 - \delta.$$

□

Satz 11.8 *(Hamming-Schranke (Lütkebohmert), Kugelpackungsschranke (van Lint))*
Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

(a) Bei $d = 2e + 1$ ist

$$A_q(n, d) \leq \frac{q^n}{V_q(n, e)}.$$

(b) Für $0 < \delta \leq 1$ ist

$$\alpha_q(\delta) \leq 1 - H_q(\frac{\delta}{2}).$$

Beweis:

(a) Sei $C \subset \mathbb{F}_q^n$ ein (n, M, d)-Code mit $d = 2e + 1$. Es ist

$$\mathbb{F}_q^n \supset \dot{\bigcup}_{x \in C} (\text{Ball um } x \text{ vom Radius } e),$$

das ist eine disjunkte Vereinigung wegen $d(C) = 2e + 1$. Daher ist

$$q^n \geq |C| \cdot V_q(n, e).$$

(b) Nach Definition ist

$$\alpha_q(\delta) = \limsup_{\tilde{n} \to \infty} \frac{\log_q A_q(\tilde{n}, [\delta\tilde{n}])}{\tilde{n}}.$$

1. Fall, $[\delta\tilde{n}]$ ungerade: $2e + 1 = [\delta\tilde{n}]$, dann ist

$$e = \frac{[\delta\tilde{n}] - 1}{2} \stackrel{!}{=} \left[\frac{\delta}{2}\tilde{n}\right], \quad A_q(\tilde{n}, [\delta\tilde{n}]) \leq \frac{q^{\tilde{n}}}{V_q(\tilde{n}, e)}.$$

2. Fall, $[\delta\tilde{n}]$ gerade: Definiere e durch $2e + 1 = [\delta\tilde{n}] - 1$, dann ist

$$e = \frac{[\delta\tilde{n}]}{\tilde{n}} - 1 \stackrel{!}{=} \left[\frac{\delta}{2}\tilde{n}\right] - 1, \quad A_q(\tilde{n}, [\delta\tilde{n}]) \leq A_q(\tilde{n}, [\delta\tilde{n}] - 1) \leq \frac{q^{\tilde{n}}}{V_q(\tilde{n}, e)}.$$

In beiden Fällen ist daher

$$\alpha_q(\delta) \leq \lim_{\tilde{n} \to \infty} \left(\frac{1}{\tilde{n}} \log_q \frac{q^{\tilde{n}}}{V_q(\tilde{n}, e)}\right) \stackrel{11.2\,(b)}{=} 1 - H_q(\frac{\delta}{2}).$$

□

Schwerer ist der Beweis des folgenden Satzes.

Satz 11.9 *(Plotkin-Schranke)*
Sei q eine Primzahlpotenz, seien $n, d \in \mathbb{N}$ mit $n \geq d$.

(a) Sei $n\frac{q-1}{q} < d \leq n$. *Dann ist*

$$A_q(n,d) \leq \frac{d}{d - n\frac{q-1}{q}}.$$

(b) Für $\frac{q-1}{q} < \delta \leq 1$ *ist*

$$\alpha_q(\delta) = 0.$$

(c) Sei $d \leq n\frac{q-1}{q}$, *definiere (hier ist* [.] *die Gaußklammer)*

$$n' := \left[\frac{q}{q-1}(d-1)\right] \leq \frac{q}{q-1}(d-1) < \frac{q}{q-1} \cdot d \leq n.$$

Dann ist $d - n' \cdot \frac{q-1}{q} > 0$ *und*

$$A_q(n,d) \leq q^{n-n'} \cdot \frac{d}{d - n' \cdot \frac{q-1}{q}}.$$

(d) Für $0 < \delta \leq \frac{q-1}{q}$ *ist*

$$\alpha_q(\delta) \leq 1 - \frac{q}{q-1} \cdot \delta.$$

Beweis: (a) Sei $C \subset \mathbb{F}_q^n$ ein (n, M, d)-Code und $n\frac{q-1}{q} < d \leq n$. Für $a \in \mathbb{F}_q$ und $i = 1, 2, ..., n$ sei

$$m_{i,a} := |\{x \in C \mid x_i = a\}|.$$

Es ist

$$\sum_{a \in \mathbb{F}_q} m_{i,a} = M.$$

Nun schätzt man ab:

$$\begin{aligned}
M(M-1)d &\leq \sum_{x,y \in C,\ x \neq y} d_H(x,y) = \sum_{x,y \in C} d_H(x,y) \\
&= \sum_{i=1}^{n} \sum_{x,y \in C} (1 - \delta_{x_i,y_i}) \qquad (\delta_{.,.} \text{ ist das Kroneckersymbol}) \\
&= \sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q} \sum_{x \in C:\, x_i = a} \sum_{y \in C:\, y_i \neq a} 1 = \sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q} m_{i,a} \cdot (M - m_{i,a}) \\
&= \sum_{i=1}^{n} \left(M \cdot M - \sum_{a \in \mathbb{F}_q} m_{i,a}^2 \right) \\
&\overset{\text{s.u.}}{\leq} \sum_{i=1}^{n} \left(M^2 - \frac{1}{q} \left(\sum_{a \in \mathbb{F}_q} m_{i,a} \right)^2 \right) = n \cdot \frac{q-1}{q} \cdot M^2,
\end{aligned}$$

hier folgt die Abschätzung $\overset{\text{s.u.}}{\leq}$ mit der folgenden Anwendung der Cauchy-Schwarzschen Ungleichung:

$$\left(\sum_{a\in\mathbb{F}_q} m_{i,a}\cdot 1\right)^2 \leq \left(\sum_{a\in\mathbb{F}_q} m_{i,a}^2\right)\cdot\left(\sum_{a\in\mathbb{F}_q} 1^2\right) = q\cdot\sum_{a\in\mathbb{F}_q} m_{i,a}^2.$$

Also ist

$$(M-1)\cdot d \leq n\cdot\frac{q-1}{q}\cdot M,$$

und das ist äquivalent zu

$$-d \leq (-d + n\cdot\frac{q-1}{q})\cdot M.$$

Im Fall $d - n\frac{q-1}{q} > 0$ ist das äquivalent zu

$$M \leq \frac{d}{d-n\frac{q-1}{q}}.$$

(b) Für $\frac{q-1}{q} < \delta \leq 1$ ist

$$\begin{aligned}
\alpha_q(\delta) &= \limsup_{n\to\infty}\left(\frac{1}{n}\log_q A_q(n,[\delta n])\right)\\
&\overset{(a)}{\leq} \lim_{n\to\infty}\left(\frac{1}{n}\log_q\frac{[\delta n]}{[\delta n]-n\frac{q-1}{q}}\right)\\
&= \lim_{n\to\infty}\left(\frac{1}{n}\log_q\frac{\delta}{\delta-\frac{q-1}{q}}\right) = 0.
\end{aligned}$$

(c) Sei C ein (n,M,d)-Code mit $M = A_q(n,d)$. Sei $y\in\mathbb{F}_q^{n-n'}$. Definiere

$$C_y := \{x\in C \mid (x_1,...,x_{n-n'}) = y\}.$$

Dann ist

$$C = \dot{\bigcup}_{y\in\mathbb{F}^{n-n'}} C_y \qquad \text{(disjunkte Vereinigung)}.$$

Sei $y_0\in\mathbb{F}^{n-n'}$ mit $|C_{y_0}|$ maximal unter allen $|C_y|$. Man schätzt ab

$$M = |C| = \sum_{y\in\mathbb{F}^{n-n'}} |C_y| \leq q^{n-n'}\cdot|C_{y_0}|.$$

Nach Weglassen der Einträge $(x_1,...,x_{n-n') } = y$ in allen Wörtern in C_{y_0} wird aus C_{y_0} eine Menge $\tilde{C}_{y_0}\subset\mathbb{F}_q^{n'}$. Diese Menge ist offensichtlich ein $(n',|C_{y_0}|,d(C_{y_0}))$-Code mit $d(C_{y_0})\geq d = d(C)$.

Die Voraussetzung von (a) ist erfüllt:

$$d(\tilde{C}_{y_0}) \geq d > n' \cdot \frac{q-1}{q} \qquad \text{nach Definition von } n'.$$

(a) gibt

$$|C_{y_0}| = |\tilde{C}_{y_0}| \leq \frac{d}{d - n' \cdot \frac{q-1}{q}}.$$

Daraus folgt

$$M \leq q^{n-n'} \cdot \frac{d}{d - n' \cdot \frac{q-1}{q}}.$$

(d)

$$\begin{aligned}
\alpha_q(\delta) &= \limsup_{n\to\infty} \left(\frac{1}{n} \log_q A_q(n, [\delta n]) \right) \\
&\leq \lim_{n\to\infty} \left(\frac{1}{n} \log_q \left(q^{n-n'} \cdot \frac{[\delta n]}{[\delta n] - n' \cdot \frac{q-1}{q}} \right) \right) \\
&= \lim_{n\to\infty} \left(1 - \frac{n'}{n} + \frac{1}{n} \log_q \frac{\delta}{\delta - \frac{n'}{n} \cdot \frac{q-1}{q}} \right) \\
&\overset{(*)}{=} \lim_{n\to\infty} \left(1 - \frac{n'}{n} \right) \overset{(**)}{=} 1 - \frac{q}{q-1} \cdot \delta.
\end{aligned}$$

Die Gleichung $(**)$ folgt aus

$$\frac{n'}{n} = \frac{1}{n} \left[\frac{q}{q-1} \left([\delta n] - 1 \right) \right] \longrightarrow_{n\to\infty} \frac{q}{q-1} \cdot \delta.$$

Die Gleichung $(*)$ folgt aus

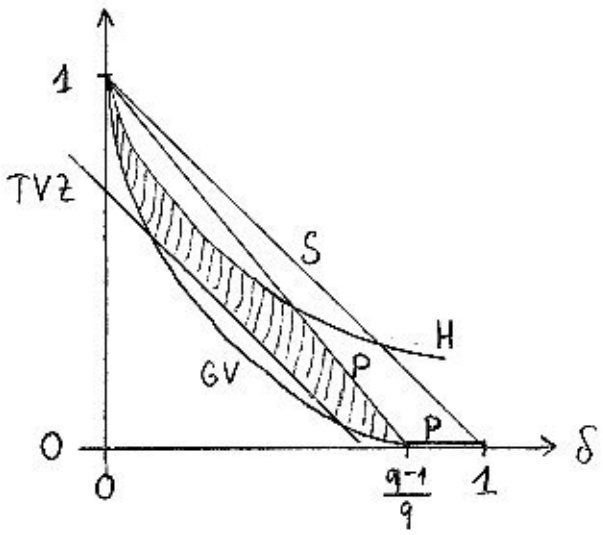
$$\begin{aligned}
\delta - \frac{n'}{n} \cdot \frac{q-1}{q} &= \frac{1}{n}\delta n - \frac{1}{n} \left[\frac{q}{q-1} \left([\delta n] - 1 \right) \right] \cdot \frac{q-1}{q} \\
&\geq \frac{1}{n}[\delta n] - \frac{1}{n} \cdot \frac{q}{q-1}([\delta n] - 1) \cdot \frac{q-1}{q} \\
&= \frac{1}{n}[\delta n] - \frac{1}{n}[\delta n] + \frac{1}{n} = \frac{1}{n}
\end{aligned}$$

und

$$\frac{1}{n} \log_q \frac{\delta}{\delta - \frac{n'}{n} \cdot \frac{q-1}{q}} \leq \frac{1}{n} \log_q \frac{\delta}{1/n} \longrightarrow_{n\to\infty} 0.$$

□

Bemerkung 11.10 Die folgende Skizze zeigt alle Schranken zusammen.
GV = Gilbert-Varshamov-Schranke (untere),
TVZ = Tsfasman-Vladut-Zink-Schranke (untere),
S = Singleton-Schranke (obere),
H = Hamming-Schranke (obere),
P = Plotkin-Schranke (obere).
$\alpha_q(\delta)$ liegt im schraffierten Bereich.



12 Goppa-Codes

Bemerkungen 12.1 (i) Man kann relativ leicht zeigen, dass es Folgen von Goppa-Codes gibt, die sich von unten der Gilbert-Varshamov-Schranke annähern (Satz 12.5).

(ii) Tsfasman/Vladut/Zink (1982) und Stichtenoth (später) haben mit Hilfe von Techniken der algebraischen Geometrie Folgen (von Verallgemeinerungen?) von Goppa-Codes konstruiert, die oberhalb der Gilbert-Varshamov-Schranke liegen.

(iii) Goppa-Codes (Definition 12.2) sind Verallgemeinerungen von BCH-Codes im engeren Sinn (Definition 8.1). Man betrachtet die BCH-Codes im engeren Sinn von einem neuen Blickwinkel.

Zuerst ihre alte Definition:

$$\begin{aligned} C &\subset \frac{\mathbb{F}_q[t]}{(t^n-1)}, \qquad \text{mit designiertem Abstand } \delta \text{ und mit} \\ \alpha &\in \mathbb{F}_{q^m} \text{ mit } o(\alpha) = n \quad (\text{natürlich gilt } n|(q^m-1)), \\ C &= ([g(t)]) \text{ mit Erzeugerpolynom} \\ g(t) &= \text{kgV}\left(\text{Minimalpolynome in } \mathbb{F}_q[t] \text{ von } \alpha, \alpha^2, \ldots, \alpha^{\delta-1}\right). \end{aligned}$$

Es ist

$$\begin{aligned} & [c_0 + c_1 t + \cdots + c_{n-1}t^{n-1}] = [c(t)] \in C \\ \iff \quad & c(\alpha^j) = 0 \quad \text{für } j = 1, 2, \ldots, \delta - 1 \quad (*). \end{aligned}$$

Nun eine Zwischenrechnung: Beachte

$$\begin{aligned} (z^n - 1) &= (z - (\alpha^{-i}))(z^{n-1} + z^{n-2}(\alpha^{-i}) + \cdots + (\alpha^{-i})^{n-1}) \\ &= (z - (\alpha^{-i})) \sum_{k=0}^{n-1} z^k (\alpha^{-i})^{n-1-k}. \end{aligned}$$

Daher ist für ein beliebiges Polynom $c(t) = c_0 + c_1 t + c_{n-1}t^{n-1} \in \mathbb{F}_q[t]$

$$\begin{aligned} (z^n - 1) \sum_{i=0}^{n-1} \frac{c_i}{z - \alpha^{-i}} &= \sum_{i=0}^{n-1} c_i \cdot \frac{z^n - 1}{z - \alpha^{-i}} \\ &= \sum_{i=0}^{n-1} c_i \cdot \sum_{k=0}^{n-1} z^k \cdot (\alpha^{-i})^{n-1-k} \\ &= \sum_{k=0}^{n-1} z^k \cdot \sum_{i=0}^{n-1} c_i \cdot (\alpha^{k+1})^i \\ &= \sum_{k=0}^{n-1} z^k \cdot c(\alpha^{k+1}). \end{aligned}$$

Nun der neue Blickwinkel = eine neue Charakterisierung:

Aus der Zwischenrechnung und der Charakterisierung $(*)$ der Elemente $[c(t)]$ von C folgt

$$[c(t)] \in C \quad \overset{!}{\Longleftrightarrow} \quad (z^n-1)\cdot \sum_{i=0}^{n-1} \frac{c_i}{z-\alpha^{-i}} \equiv 0 \mod z^{\delta-1}$$

$$\overset{\text{klar}}{\Longleftrightarrow} \quad \sum_{i=0}^{n-1} \frac{c_i}{z-\alpha^{-i}} \equiv 0 \mod z^{\delta-1}.$$

Definition 12.2 (Goppa-Codes)
Gegeben seien: q eine Primzahlpotenz, $m, t, n \in \mathbb{N}$,

$$\begin{aligned} f(z) &\in \mathbb{F}_{q^m}[z] \quad \text{ein Polynom vom Grad } t, \\ L &= (\gamma_0, \gamma_1, \ldots, \gamma_{n-1}) \in \mathbb{F}_{q^m}^n \quad \text{ein Vektor mit} \\ &\quad \gamma_i \neq \gamma_j \text{ für } i \neq j \quad \text{und} \\ &\quad f(\gamma_i) \neq 0 \ \forall\ i = 0, 1, \ldots n-1. \end{aligned}$$

Der Goppa-Code $\Gamma(L, f) \subset \mathbb{F}_q^n$ ist

$$\Gamma(L,f) := \{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} \equiv 0 \mod f(z)\}.$$

Bemerkungen 12.3 (i) Er ist ein linearer Code.

(ii) Ein BCH-Code im engeren Sinn ist ein Goppa-Code $\Gamma(L, f)$ mit

$$L = (\alpha^0, \alpha^{-1}, \ldots, \alpha^{-(n-1)}) \text{ und } f(z) = z^t,\ t = \delta - 1.$$

(iii) Eine Bedingung

$$\sum_{j=1}^{l} \frac{a_j(z)}{b_j(z)} \equiv 0 \mod f(z) \qquad (**)$$

ist nur sinnvoll, wenn gilt

$$\forall\ j\ \ \text{ggT}(f(z), b_j(z)) = 1,$$

denn nur dann ist die Klasse $[b_j(z)]$ im Quotientenring $\mathbb{F}_{q^m}[z]/(f(z))$ invertierbar und $1/[b_j(z)]$ darin wohldefiniert. In dem Fall sagt die Bedingung $(**)$ gerade, daß die Summe links in diesem Quotientenring das Nullelement ist,

$$\sum_{j=1}^{l} \frac{[a_j(z)]}{[b_j(z)]} = 0 \quad \text{in} \quad \frac{\mathbb{F}_{q^m}[z]}{(f(z))}.$$

Die Bedingung $(**)$ läßt sich aber auch ohne den Quotientenring schreiben, sie ist äquivalent zur Bedingung

$$f(z) \mid \sum_{j=1}^{l} \left(a_j(z) \cdot \prod_{i \neq j} b_j(z) \right) \quad \text{in} \quad \mathbb{F}_{q^m}[z].$$

In Definition 12.2 ist $\mathrm{ggT}(f(z), z - \gamma_i) = 1$ wegen $f(\gamma_i) \neq 0$.

(iv) Der Spezialfall in Definition 12.2 der Bedingung $(**)$ lässt sich mit den Formeln (I) und (II) anders schreiben:

$$\frac{1}{z-\gamma} \equiv \frac{-1}{f(\gamma)} \cdot \frac{f(z)-f(\gamma)}{z-\gamma} \mod f(z) \qquad (I),$$

und bei $f(z) = \sum_{i=0}^{t} f_i \cdot z^i$ ist

$$\begin{aligned} \frac{f(z)-f(\gamma)}{z-\gamma} &= \sum_{i=1}^{t} f_i \, \frac{z^i - \gamma^i}{z-\gamma} = \sum_{i=1}^{t} f_i (z^{i-1} + z^{i-2}\gamma + \cdots + \gamma^{i-1}) \\ &= \sum_{k,l \text{ mit } k+l \leq t-1} f_{k+l+1} \cdot z^k \cdot \gamma^l \qquad (II) \end{aligned}$$

ein Polynom vom Grad $t-1$ in z.

Satz 12.4 *Seien L und $f(z)$ wie in Definition 12.2 und sei $C = \Gamma(L, f)$ der zugehörige Goppa-Code.*

(a) Sei $h_i := \frac{1}{f(\gamma_i)}$, und sei

$$H := \begin{pmatrix} h_0 & h_1 & \dots & h_{n-1} \\ h_0\gamma_0 & h_1\gamma_1 & \dots & h_{n-1}\gamma_{n-1} \\ \vdots & \vdots & & \vdots \\ h_0\gamma_0^{t-1} & h_1\gamma_1^{t-1} & \dots & h_{n-1}\gamma_{n-1}^{t-1} \end{pmatrix} \in M(t \times n, \mathbb{F}_{q^m}).$$

Mit einem $\mathbb{F}_q$-Vektorraum-Isomorphismus

$$\Psi : \mathbb{F}_{q^m} \to M(m \times 1, \mathbb{F}_q)$$

erhält man aus H eine Matrix

$$\widetilde{H} \in M((mt) \times n, \mathbb{F}_q).$$

Nach Weglassen linear abhängiger Zeilen wird daraus eine Kontrollmatrix des Goppa-Codes $C = \Gamma(L, f)$.

(b) $\dim C \geq n - m \cdot t$.

(c) $d(C) \geq t + 1$.

Beweis: (a) Es gelten folgende Äquivalenzen

$$
\begin{aligned}
& (c_0, c_1, \ldots, c_{n-1}) \in \Gamma(L, f) \\
\iff \quad & \sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i} \equiv 0 \mod f(z) \quad \text{(Definition des Goppa-Codes)} \\
\iff \quad & \sum_{i=0}^{n-1} \frac{c_i}{f(\gamma_i)} \cdot \frac{f(z) - f(\gamma_i)}{z - \gamma_i} \equiv 0 \mod f(z) \quad \text{(Bem. 12.3}(iv)(I)\text{)} \\
\iff \quad & \sum_{i=0}^{n-1} c_i \cdot h_i \cdot \sum_{k,l \text{ mit } k+l \leq t-1} f_{k+l+1}\, z^k \cdot \gamma_i^l \equiv 0 \mod f(z) \quad \text{(Bem. 12.3}(iv)(II)\text{)} \\
\iff \quad & \sum_{i=0}^{n-1} c_i \cdot h_i \cdot \sum_{k,l \text{ mit } k+l \leq t-1} f_{k+l+1}\, z^k \cdot \gamma_i^l = 0 \\
& \qquad (\text{da } \deg(\text{linke Seite}) \leq t - 1 < t = \deg f(z)) \\
\iff \quad & \forall\, k \in \{0, \ldots, t-1\} \sum_{i=0}^{n-1} h_i \cdot \left(\sum_{l \text{ mit } k+l \leq t-1} f_{k+l+1} \gamma_i^l \right) \cdot c_i = 0
\end{aligned}
$$

Das sind t lineare Bedingungen. Sie lassen sich in folgender Matrizengleichung zusammenstellen (oberste Zeile $\leftrightarrow k = t-1$, unterste Zeile $\leftrightarrow k = 0$),

$$
0 = \begin{pmatrix}
h_0 f_t & \cdots & h_{n-1} f_t \\
h_0(f_{t-1} + f_t \gamma_0) & \cdots & h_{n-1}(f_{t-1} + f_t \gamma_{n-1}) \\
\vdots & & \vdots \\
h_0(f_1 + f_2 \gamma_0 + \cdots + f_t \gamma_0^{t-1}) & \cdots & h_{n-1}(f_1 + f_2 \gamma_{n-1} + \cdots + f_t \gamma_{n-1}^{t-1})
\end{pmatrix}
\begin{pmatrix} c_0 \\ c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}.
$$

Wegen $\deg f(z) = t$ ist $f_t \neq 0$.
Zeilenumformungen geben die äquivalente Bedingung

$$
0 = H \cdot \begin{pmatrix} c_0 \\ c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}.
$$

Der Rest von (a) ist klar.

(b) $\dim C = n - \operatorname{rang} \widetilde{H}$, und natürlich $\operatorname{rang} \widetilde{H} \leq m \cdot t$.

(c) Sei $(c_0, c_1, \ldots, c_{n-1}) \in C - \{0\}$ und $w := w((c_0, c_1, \ldots, c_{n-1}))$.

Es reicht zu zeigen, daß $w \geq t+1$ ist. Schreibe

$$\sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} = \sum_{i \text{ mit } c_i \neq 0} \frac{c_i}{z-\gamma_i} = \frac{\sum\limits_{i \text{ mit } c_i \neq 0} c_i \prod\limits_{j \text{ mit } c_j \neq 0, i \neq j} (z-\gamma_j)}{\prod\limits_{i \text{ mit } c_i \neq 0} (z-\gamma_i)} =: \frac{a(z)}{b(z)}.$$

Wegen $f(\gamma_i) \neq 0 \ \forall \ i$ ist $\mathrm{ggT}(f(z), b(z)) = 1$.
Nach Definition des Goppa-Codes gilt

$$(c_0, c_1, \ldots, c_{n-1}) \in C \iff f(z) \mid a(z).$$

Daher ist $f(z) \mid a(z)$ und (wegen $(c_0, c_1, \ldots, c_{n-1}) \neq 0$ ist $a(z) \neq 0$)

$$\deg a(z) \geq \deg f(z) = t.$$

Anderseits ist

$$\deg a(z) \leq w - 1.$$

Also ist $w \geq t+1$. □

Satz 12.5 *(Goppa-Codes und die Gilbert-Varshamov-Schranke)*
Sei q eine Primzahlpotenz, $0 < \delta \leq 1, \varepsilon > 0, N \in \mathbb{N}$.
Es existieren Goppa-Codes $C = \Gamma(L, f) \subset \mathbb{F}_q^n$ mit $n > N$, relativem Hamming-Abstand $\frac{d(C)}{n} \geq \delta$ und Informationsrate

$$R(C) = \frac{dim(C)}{n} \geq 1 - H_q(\delta) - \epsilon.$$

Deutung dieses Resultats: Die asymptotische Gilbert-Varshamov-Schranke $\alpha_q(\delta) \geq 1 - H_q(\delta)$ zeigte die Existenz von Codes C mit $\frac{d(C)}{n} \geq \delta$ und $R(C) = \frac{dim(C)}{n} \geq 1 - H_q(\delta) - \epsilon$. Das Resultat hier gibt einen zweiten viel komplizierteren, aber konstruktiven Beweis dieser Existenzaussage.

Beweis: Man wählt erstmal die Zahlen m und t groß, später werden beide nach ∞ laufen. Dann setzt man

$$\begin{aligned} n &:= q^m, \\ L &:= (\gamma_0, \gamma_1, \ldots, \gamma_{n-1}) \quad \text{mit} \quad \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} = \mathbb{F}_{q^m} \\ &\qquad \text{(die Reihenfolge der Körperelemente } \gamma_i \text{ von } \mathbb{F}_{q^m} \text{ ist egal)}, \\ J_{t,q^m} &:= \{\text{irreduzible Polynome vom Grad } t \text{ in } \mathbb{F}_{q^m}[z]\} \\ &\qquad \text{(vgl. Satz 6.14 (a) für den Spezialfall } q^m = \text{Primzahl)}. \end{aligned}$$

Später wird dann mit großer Sorgfalt ein gutes $f(z) \in J_{t,q^m}[z]$ ausgewählt. Aus $f(z)$ irreduzibel folgt natürlich $\forall \ i \ f(\gamma_i) \neq 0$. Der Goppa-Code $\Gamma(L, f)$ wird am Ende den Satz 12.5 erfüllen.

Ansatz: *Man sucht ein möglichst großes $d \in \mathbb{N}$, so daß die Teilmenge*

$$\{f(z) \in J_{t,q^m} \mid d(\Gamma(L,f)) < d\}$$

eine echte *Teilmenge von J_{t,q^m} ist. Dazu muß man diese Teilmenge abschätzen. Danach wird $f(z)$ in der Komplementärmenge gewählt werden.*

Gegeben seien (irgendein) $d \in \mathbb{N}$ und irgendein Wort $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n - \{0\}$ mit $w((c_0, c_1, \ldots, c_{n-1})) = w < d$.
Wie im Beweis von Satz 12.4 (c) ist der Zähler $a(z)$ in

$$\sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} = \sum_{i \text{ mit } c_i \neq 0} \frac{c_i}{z-\gamma_i} = \frac{\displaystyle\sum_{i \text{ mit } c_i \neq 0} c_i \prod_{j \text{ mit } c_j \neq 0, i \neq j} (z-\gamma_j)}{\displaystyle\prod_{i \text{ mit } c_i \neq 0} (z-\gamma_i)} =: \frac{a(z)}{b(z)}.$$

ein Polynom in $\mathbb{F}_{q^m}[z]$ mit Grad $\leq w-1$. Und wie dort folgt für jedes $f(z) \in J_{t,q^m}$ aus der Definition des Goppa-Codes $\Gamma(L,f)$

$$(c_0, c_1, ..., c_{n-1}) \in \Gamma(L,f) \iff f(z) \mid a(z).$$

Wegen $\deg a(z) \leq w-1$ wird der Zähler $a(z)$ von höchstens $\left[\frac{w-1}{t}\right]$ Polynomen in J_{t,q^m} geteilt. Für jeden dieser Teiler $f_{Teiler} \in J_{t,q^m}$ ist $\Gamma(L, f_{Teiler})$ ein Goppa-Code mit $(c_0, ..., c_{n-1}) \in \Gamma(L, f_{Teiler})$ und daher mit $d(\Gamma(L, f_{Teiler})) \leq w < d$.
Diese f_{Teiler} müssen alle vermieden werden, wenn man ein $f \in J_{t,q^m}$ mit $d(\Gamma(L,f)) \geq d$ wählen möchte.
Man durchläuft alle Worte $(c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$ mit Gewicht $\leq d$ und schätzt ab. Man erhält

$$\begin{aligned}
& |\{f(z) \in J_{t,q^m} \mid d(\Gamma(L,f)) < d\}| \\
\leq\ & \sum_{w=1}^{d-1} \left[\frac{w-1}{t}\right] \cdot |\{(c_0, ..., c_{n-1}) \in \mathbb{F}_q^n \mid w((c_0, ..., c_{n-1})) = w\}| \\
=\ & \sum_{w=1}^{d-1} \left[\frac{w-1}{t}\right] \cdot S_q(n,w) \leq \frac{d-2}{t} \cdot \sum_{w=1}^{d-1} S_q(n,w) \\
\leq\ & \frac{d-2}{t} \cdot V_q(n, d-1).
\end{aligned}$$

Fazit: *Für d mit*

$$\frac{d-2}{t} \cdot V_q(n, d-1) < |J_{t,q^m}| \qquad (***)$$

gibt es Polynome $f(z) \in J_{t,q^m}$ mit $d(\Gamma(L,f)) \geq d$.

Es wird gleich gezeigt werden, daß diese Ungleichung für folgende Tupel (q, m, t, n, d) erfüllt ist: q eine feste Primzahlpotenz, m genügend groß und dann beliebig, t sorgfältig gewählt und automatisch auch groß,

$$n = q^m, \quad d = [\delta n] + 1.$$

Beim Beweis sind folgende Resultate nützlich:

(I) Satz 11.2 (b):

$$\lim_{\tilde{n}\to\infty} \frac{\log_q V_q(\tilde{n}, [\delta\tilde{n}])}{\tilde{n}} = H_q(\delta).$$

(II) Zitat: Für großes q^m ist

$$|J_{t,q^m}| = \frac{1}{t}(q^m)^t(1 + o(1))$$

Hier ohne Beweis. Bloß der Spezialfall q^m =Primzahl wird im Beweis von Satz 6.14 (a) behandelt. Ein vollständiger Beweis steht in Lütkebohmert, Korollar A.2.6 (allerdings muß die dort stehende Ungleichung $2 \cdot \mathrm{card} I_t \geq \frac{q^t}{t}(1 - q^{-t/2})$ durch die Ungleichung $2 \cdot \mathrm{card} I_t \geq \frac{q^t}{t}(1 - t \cdot q^{-t/2})$ ersetzt werden).

Mit ihnen erhält man

$$\begin{aligned}
(***) \quad &\iff \quad \frac{d-2}{t} \cdot V_q(n, d-1) < |J_{t,q^m}| = \frac{1}{t}(q^m)^t(1 + o(1)) \\
&\iff \quad ([\delta n] - 1) \cdot V_q(n, [\delta n]) < q^{mt}(1 + o(1)) \\
&\iff \quad H_q(\delta) + \frac{\log([\delta n] - 1)}{n} < \frac{mt}{n} + o(1) \\
&\iff \quad H_q(\delta) < \frac{mt}{n} + o(1)
\end{aligned}$$

Ansatz: Nun seien wie im Satz 12.5 $0 < \delta \leq 1$ und $\varepsilon > 0$ (klein) und $N \in \mathbb{N}$ (groß) gegeben. Man kann wählen und wählt m so groß, dass

$$n = q^m > N \quad \text{und} \quad \frac{m}{q^m} = \frac{m}{n} < \varepsilon$$

ist. Dann kann man wählen und wählt $t \in \mathbb{N}$ so, daß

$$0 < \frac{mt}{n} - H_q(\delta) < \varepsilon$$

ist. Dann ist t automatisch auch groß, falls ε deutlich kleiner als $H_q(\delta)$ ist. Dann ist $(***)$ erfüllt, und man kann ein $f(z) \in J_{t,q^m}$ wählen mit

$$d(\Gamma(L, f)) \geq d = [\delta n] + 1.$$

Es erfüllt auch

$$1 - \frac{mt}{n} > 1 - H_q(\delta) - \varepsilon$$

Wegen Satz 12.4 (b) ist daher

$$R(\Gamma(L, f)) = \frac{\dim \Gamma(L, f)}{n} \geq 1 - \frac{mt}{n} > 1 - H_q(\delta) - \varepsilon.$$

Bemerkung: Das $\frac{mt}{n}$ in den Umformungen von $(***)$ kam von $|J_{t,q^m}|$, aber es tritt auch in der Abschätzung in Satz 11.4 (b) von $R(\Gamma(L, f))$ auf. Diese Übereinstimmung ist a priori Zufall. Wenn man Satz 11.4 (b) verbessern könnte zu einer Ungleichung

$$R(\Gamma(L, f)) \geq 1 - \frac{mt}{n} + \varepsilon_1$$

mit einem $\varepsilon_1 > 0$, würde der Ansatz oben Goppa-Codes liefern, die die Gilbert-Varshamov-Schranke brechen. □