Mitschrift
Codierungstheorie

Prof. Braun
Wintersemester 2000/2001
LaTeXed by Leo

Inhaltsverzeichnis

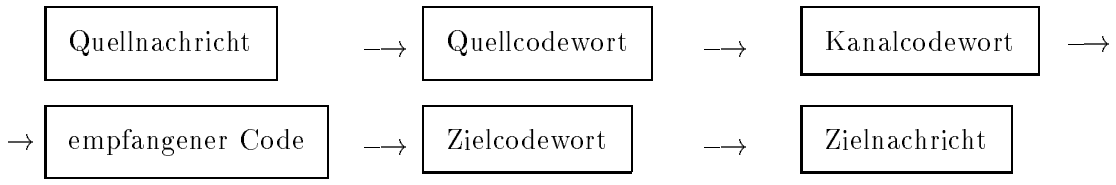
Kapitel 1

Einführung und Grundbegriffe

Thema

Übertragung von *Nachrichten* durch einen (Übertraguns -) *Kanal* mit der Absicht, *Störungen* zu *entdecken* und möglichst zu *korrigieren*.
"Ubertragbar" ist eine Folge von *Signalen*
Ein "Kanalalphabet" ist die Menge der zulässigen Signale.

1. Schritt: "Quellcodierung"
   Quellnachricht $\longmapsto$ Quellcodewort (:= Signalfolge)
   i.a. *Störung* bei der Übertragung:
   1 Signal wird durch ein lesbares / unlesbares Signal ersetzt.
2. Schritt: Quellcodewort $\longmapsto$ "Kanalcodewort" (+ Kontrollsignale)
3. Schritt: Übertragung des Kanalcodewortes *Longrightarrow* empfangenes Codewort
4. Schritt: empfangenes Codewort $\longmapsto$ Zielcodewort
5. Schritt: Zielcodewort $\longmapsto$ Zielnachricht



Folge von Nachrichten $\longmapsto$ *Folge* von Codewörtern.

Typen von Codeörtern:

1. Länge variabl / fest

2. Signale binär / nicht binär
3. Kontrollsignale mit / ohne

Definition 1.1 *Ein **Code** ist die Menge der zulässigen Kanalcodewörter über einem Kanalalphabet. Ein **Blockcode** ist ein Code mit Codewörtern konstanter Länge.*

1.1 Codes der Praxis

1.1.1 Morsecode (Samuel Morse, 1837)

Eine Nachricht entspricht einem Zeichen $\in \{a, \ldots, z, 0, \ldots, 9, \ldots\}$
Ein Zeichen wird abgebildet auf ein Codewort über $\{\cdot\,, -\}$

Beispiel
e $\mapsto \cdot$ a $\mapsto \cdot -$ c $\mapsto - \cdot - \cdot$ Trenner: Pause

Dieser Code ist also binär und ohne Kontrolle.

1.1.2 CCITT - Code (Telegrafie, 1918

1 Nachricht = 1 Zeichen $\in$ {SP, CR, LF, Buchstaben, Ziffern, Sonderzeichen}
Alphabet = $\{+, -\}$; Umschaltung; feste Länge von 5; keine Kontrolle

$$\begin{bmatrix} \text{E} \\ 3 \end{bmatrix} \mapsto + - - - - \qquad \begin{bmatrix} \text{Z} \\ + \end{bmatrix} \mapsto + - - - +$$

1.1.3 ASCII - Code

1 Nachricht = 1 Zeichen $\in \{a, \ldots, z; A, \ldots, Z; 0, \ldots, 9; \ldots\}$
2^7 Zeichen; feste Länge 8 (da Paritätsbit); Alphabet $\{0, 1\}$; 1 Kontrollbit

$$\begin{aligned} b &\mapsto 1100010\ 1 \\ B &\mapsto 1000010\ 0 \\ 2 &\mapsto 0110010\ 1 \end{aligned}$$

1.1.4 ISBN - Code Bücher

R.W. Hamming, Coding and Information Theory
Prentice - Hall, 1980

$$\text{ISBN } \underbrace{0}_{\text{Staat}} - \underbrace{13}_{\text{Verlag}} - \underbrace{139139}_{\text{interne Laufnr.}} - \underbrace{9}_{\text{Prüfziffer}}$$

Prüfziffer:

$$10 \cdot 0 + 9 \cdot 1 + 8 \cdot 3 + \cdots + 9 \cdot 2 = 134; \quad 134 + 9 = 143 = 11 \cdot 14$$

Prüfziffern: $0, 1, \ldots, 9, x$

1.2 Schlüssel für Objekte der realen Welt

1. Identifikationsschlüssel = Laufende Nummer (Dezimal), evtl. "Nummernkreise"

   Beispiel
   Wertpapiernummer 113453

2. Klassifikationsschlüssel = Folge von Werten von "Merkmalen"

   (a) hierachisch

   Beispiel
   Postleitzahlen: 80999 Allach 10999 Berlin

   (b) unabhängig

   Beispiel
   Bundeswehr - Pk: ttmmjj B zzzzz

   (c) Verbundschlüssel (beides in Kombination)

   Beispiel
   Kontonr. Postbank 1237 68 – 80 6
   lfd.Nr. Bearbeiter Filiale Prüfziffer

1.2.1 Paritätsbit

erlaubt das Erkennen von einem Fehler.

Beispiel
b : 11000101 $\mapsto$ 11010101 Verfälschung

Definition 1.2 (Hamming-Abstand) $x = x_1, \ldots, x_n$; $y = y_1, \ldots, y_n$
$d(x, y) :=$ *Anzahl der Positionen mit* $x_i \neq y_i$, *heisst* ***Hamming Abstand*** *von* x *und* y.

Beispiel
ASCI b $d(11000101, 11010101) = 1$ $d(11000101, 10000100) = 2$

Lemma 1.3 *Für den Hammingabstand* $d(x, y)$ *gilt:*

1. $d(x, y) = d(y, x)$
2. $d(x, y) = 0 \iff x = y$
3. $d(x, y) + d(y, z) \geq d(x, z)$

also eine Metrik

Definition 1.4 (Minimalabstand) *Sei C ein Code. Dann heisst $d(C) := \min\{d(x,y)|x,y \in C; x \neq y\}$ der **Minimalabstand** von C.*

Es sei:
F das Alphabet eines Codes.
F^* die Menge aller Wörter über F.
F^n die Menge aller Wörter der Länge n.
$C \subseteq F^n$
$\Longrightarrow$ bei $d(C) \geq 2$ ist $C \in subseteqF^n$

Lemma 1.5 *Ein Code $C \subseteq F^n$ mit $d(C) = k$ erkennt Verfälschungen bis zu $k-1$ Fehlern. ("C erkennt $k-1$ Fehler")*

Definition 1.6 (Fehlertypen) *Sei Codewort $x \in C$ gestört an k-Stellen. Die **Störung** heisst:*

gleichverteilt *wenn die k Störungen unabhängig sind.*

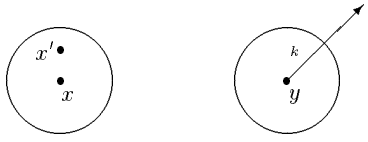
Bündelfehler *wenn sie einen Abschnitt der Länge k betrifft.*

Bei gleichverteilt:
Sei $p(<<1)$ die Wahrscheinlichkeit für 1 Fehler, dann ist p^k die Wahrscheinlichkeit für k Fehler. Annahme: bei gestörtem x' ist vermutlich das $x \in C$ mit dem kleinsten Abstand $d(x,x')$ richtig. ("maximum likelihood"-Annahme)

Lemma 1.7 *Ein Code C mit $d(C) = 2k+1$ kann bei Störungen in bis zu k Positionen das $x \in C$ **eindeutig** bestimmen. ("C korrigiert k Fehler")*

Beweis

$d(x,x') \leq k \implies$ Für jedes $y \in C, y \neq x$, gilt $d(x',y) > k$;
$d(x,x') + d(x',y) \geq d(x,y) \geq 2k+1$
$\Longrightarrow \; d(x',y) \geq 2k+1-d(x,x') \geq k+1 > k$



Bemerkungen
$d = 2k$: Kugeln können sich berühren.
Bei $d(x',x) \leq k$ nur $d(x',y) \geq 2k - d(x',x) \geq k$.
Bei $d(C) = 2k$ sind also nur $k-1$ Fehler korrigierbar.

1.3 Codes mit variabler Wortlänge

Ohne Trennzeichen, falls "Präfix-Bedingung". (Ein Codewort ist nie ein echter Anfang eines anderen Codewortes) = Fano-Bedingung (1963)

Beispiel
$C = \{0, 10, 110, 111\}$

Allgemein:
$C = \{c_1, \ldots, c_p\}$ ein Code mit Fanobedingung, der Länge $n_1, \ldots, n_p$ mit $|F| = q$.Dann gilt $\sum_{k=1}^{p} \frac{1}{q^{n_k}} \leq 1$. Im Beispiel: $n_1 = 1, n_2 = 2, n_3 = n_4 = 3, q = 2$ liefert $\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} = 1$

Ab jetzt: Blockcodes, $x \in C$: $x = a_1, \ldots, a_n$ mit $a_i \in F$, Hamming-Abstand
Also lange und viele Codewörter und mathematische Struktur des C

Kapitel 2

Lineare Codes

Blockcode 1.1 $C \subseteq F^n$, F endlich und Kanalalphabet. F nicht irgendeine Menge, C nicht irgendeine Teilmenge von F^n.
F endlicher Körper, $|F| = q$ mit q.
$F = \mathrm{GF}(q), q = p^m$, meist $\mathrm{GF}(p)$[1]

Beispiel
$\mathrm{GF}(2) = \{0, 1\}, \quad \mathrm{GF}(3) = \{0, 1, 2\}$

F^n ist ein Vektorraum der Dimension n über F.
$x \in F^n$: $\quad x = a_1, \ldots, a_n$ mit $a_i \in F \quad y = b_1, \ldots, b_n$ mit $b_i \in F$
$x + y = (a_1 + b_1), \ldots, (a_n + b_n)$

Beispiel
$F = \mathrm{GF}(2), n = 4,\ F^4 = \{0000, 0001, \ldots, 1111\}$ $\quad \overset{0001}{\underset{0000}{+\ 1111}}$

Beispiel
$F = \mathrm{GF}(3), n = 4,\ F^4 = \{0000, 0001, 0002, \ldots, 2222\}$ $\quad \overset{0001}{\underset{0000}{+\ 0002}}$

Schreibe V statt F^n, dann $|V| = q^n$. Sei $U \subseteq V$ Untervektorraum. V hat Basis $v_1, v_2, \ldots, v_n \in V$, v_i linear unabhängig.
U hat Basis $g_1, g_2, \ldots, g_k$ mit $k \leq n$, g_i linear unabhängig.
$x \in U: \ x = \lambda_1 g_1 + \cdots + \lambda_k g_k \quad |U| = q^k,\ 0 \in U$

Definition 2.1 *Ein $k-$dimensionaler Unter (Vektor) raum $C \subseteq V := F^n$ heisst $(n, k)-$ Linearcode (über F)*

Folge:

1. Die Summe und Differenz zweier Codewörter ist wieder ein Codewort.
2. Es gilt stets: $\underbrace{0, \ldots, 0}_{\text{n-mal}} \in C$

Beispiel
$F = \mathrm{GF}(2), n = 4, C = \{0000, 0111, 1001, 1110\}$ also ein $(4, 2)-$Code.
$|C| = 4 = q^2 \implies k = 2$

[1] p = Primzahl

Definition 2.2 (Hamming-Gewicht und Gewichtsfunktion)
Sei $C \subseteq F^n$ ein $(n,k)-$Code, dann:

1. *Für $x \in C$ heisst $\gamma(x) := d(0,x)$ (Hamming) Gewicht von x.*
2. *Sei für $i \in \{0,1,\ldots,n\}$, A_i die Anzahl der Wörter aus C mit Gewicht. Dann heisst $A(Z) := \sum_{i=0}^{n} A_i z^i$ Gewichtsfunktion von C. ($A_0 = 1$)*

Korollar

1. $d(x,y) = \gamma(x-y)$
2. $d(C) := \min\{\gamma(x) | x \in C, x \neq 0\}$

Beweis

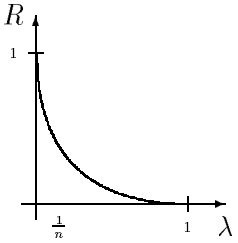
zu 1. Es gilt $d(x,y) = d(x+z, y+z)$ "translationsinvariant".
$\Longrightarrow d(x,y) = d(y,x) = d(y-y, x-y) = d(0, x-y)$

zu 2. ohne Beweis

Definition 2.3 (Informationsrate)
Für $(n,k)-$Code C heisst $R := \frac{k}{n}$ Informationsrate. $0 \leq R \leq 1$.

Ist R gross, so gibt es viele verschiedene Codewörter. Eine hohe Informationsrate führt zu einer schlechten Korrektur.
Oft ist es erwünscht, für ein gegebenes n (Wortlänge), d (Mindesabstand) und q (Signalanzahl) ein maximales $R(n,d,q)$ zu finden. Also einen Code bei dem $R(n,d,q)$ "optimal" ist.

$$R = \frac{K}{n}[0 \leq R \leq 1] \quad \lambda = \frac{d}{n}\left[\tfrac{1}{n} \leq \lambda \leq 1\right]$$



Grenzfälle

1. $R = 0, k = 0, |C| = q^0 = 1, C = \{0 \ldots 0\}$ $(n,0)-$Code.
2. $R = 1, k = n, |C| = q^n \Longrightarrow C = F^n \Longrightarrow d = 1$ $(\lambda = \frac{1}{n})$ $(n,n)-$Code.

3. $\lambda = 1, d = n, C = \{0 \ldots 0, 1 \ldots 1, \ldots, (q-1, \ldots, q-1)\}$
   $|C| = q', K = 1, R = \frac{1}{n}$ $(n,1)-$Code.
   Erkennt $n-1$ Fehler und korrigiert $(n-1)\text{div}\,2$ Fehler.

Beispiel
$q = 2, n = 7$ 0100110 $\mapsto$ 000000 1100110 $\mapsto$ 111111 "triviale Codes"

"nicht triviale" Codes

Basis $g_1, \ldots, g_k$; $x \in C \implies x = \lambda_1 g_1 + \cdots + \lambda_k g_k$ mit $\lambda_i \in F = \text{GF}(q)$
Menge der Quellcodewörter ist $(\lambda_1, \ldots, \lambda_k)$. Die Menge der $x = \lambda_1 g_1 + \cdots + \lambda_k g_k$ ist die Menge der Kanalcodewörter. Die "Generatormatrix" G für C hat k Zeilen $g_i (i = 1, \ldots, k)$ der Länge n.

Beispiel
$q = 2, n = 5, k = 3 \implies G = \begin{matrix} 11001 \\ 01111 \\ 10011 \end{matrix}$

C: Quellcodewort	Kanalcodewort	Gewicht λ	$d(C) = 2$
000	00000	0	
001	10011	3	
010	01111	4	
011	11100	3	
100	11001	3	
101	01010	2	
110	10110	3	
111	00101	2	

$A(Z) = 1 + 2z^2 + 4z^3 + 1z^4$

Mit einer *anderen* Basis für C bilden k Spalten die Einheitsmatrix I_k ("Staffelform")

Definition 2.4 (Äquivalenz) *2 Codes $C, C' \subseteq F^n$ heissen **äquivalent**, wenn sie, bis auf (feste) Permutationen der Komponenten der Codewörter, identisch sind.*

G in Staffelform permutieren, dann ist $G = (I_k \vdots P)$ mit $P = k \times (n-k)$ Matrix in "reduzierter Staffelform".

Satz 2.5 *Zu jedem $(n,k)-$Code $C \subseteq F^n$ existiert ein äquivalenter $(n,k)-$Code $C' \subseteq F^n$ mit Generatormatrix G' in "reduzierter Staffelform".*

Dann:

$$x = a_1 \dots a_k a_{k+1} \dots a_n \in C$$

$$x = \lambda_1 g_1 + \dots + \lambda_k g_k \text{ mit } G = (I_k \vdots P)$$

$$g_j = g_{j1} \dots g_{jk} \underbrace{p_{j1} \dots p_{j,r}}_{g_{j,k+1} \dots g_{jn}} \text{ mit } g_{ji} = \delta_{ji} \text{ und } r := n - k$$

$$a_i = (\lambda_1 \dots \lambda_k) \begin{pmatrix} g_{1i} \\ \vdots \\ g_{ki} \end{pmatrix}$$

$$\Longrightarrow \quad a_1 = \lambda_1, \dots, a_k = \lambda_k$$

$$\Longrightarrow a_{k+j} = \lambda_1 p_{1j} + \lambda_2 p_{2j} + \dots * \lambda_k p_{1k} \qquad (1 \le j \le n-k)$$

$$\Longrightarrow a_{k+j} = a_1 p_{1j} + \dots + a_k p_{kj}$$

Hieraus folgt, dass $x \in C$ in k frei wählbare "Informationsbits" und $r = (n - k)$ "Kontrollbits" $a_{k+1} \dots a_n$ zerlegbar ("separierbar") ist. Diese Kontrollbits ergeben sich mit Hilfe der "Kontrollgleichungen" aus den Informationsbits.

$$a_{k+j} = a_1 p_{1j} + \dots + a_k p_{kj} = (a_1 \dots a_k) \begin{pmatrix} p_{ij} \\ \vdots \\ p_{kj} \end{pmatrix} \quad \text{Spalten Nr. } k+j \text{ in } G$$

Beispiel

Beispiel 1

$$G = \begin{array}{lll} 11001 & g_1 \\ 01111 & g_2 \\ 10011 & g_3 \end{array} \qquad G' = \begin{array}{ll} 100:11 & g'_1 = g_3 \\ 010:10 & g'_2 = g_1 + g_3 \\ 001:01 & g'_3 = g_1 + g_2 + g_3 \end{array}$$

$\Longrightarrow a_1, a_2, a_3$ frei wählbar. $a_4 = a_1 + a_2$ $a_5 = a_1 + a_3$
$x = (a_1, a_2, a_3, a_1 + a_2, a_1 + a_3)$

Beispiel 2

$$C = \{0000, 0111, 1001, 1110\}, G = \begin{array}{l} 10:01 \\ 01:11 \end{array}, X = (a_1, a_2, a_2, a_1 + a_2)$$

Beispiel 3 Paritätsbit

$$x = (\underbrace{a_1, \dots, a_{n-1}}_{\text{frei wählbar}}, a_n) \text{ mit } \sum_{i=1}^{n} a_i = 0 \quad \Longrightarrow a_n = \sum_{i=1}^{n} a_i, G = \begin{pmatrix} 1 & 0 & \vdots & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & \vdots & 1 \end{pmatrix}$$

$(n, n-1)-$Code

Zu G existiert eine "Kontrollmatrix" H:

$$x = a_1, \dots, a_n \quad y = b_1, \dots, b_n \ \in F^n$$

$$x \cdots y := a_1 \cdot b_1 + \dots + a_n \cdot b_n$$

$$x, y \text{ sind orthogonal} \iff x \cdot y = 0 \qquad \text{"selbstorthogonale"}$$

Beispiel
$(01111) \cdot (01111) = 0 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 = 0$

Definition 2.6 $\mathbf{C^\perp} = \{y \in F^n | y \cdot x = 0$ *für alle* $x \in C'\}$ *ist ein* ***Orthogonalraum*** *zu* C. *Weiterhin ist* $C^\perp$ *ein Unterraum von* F^n *(Dim* $r = n - k$*) und ein zu* C ***dualer*** *Code.*

Sei H Generatormatrix ($r \times n$-Matrix) des $C^\perp$, mit Zeilen h_j und eine Kontrollmatrix für C. Dann gilt:

$$y \in C^\perp \iff y \cdot g_j = 0 \text{ für alle Zeilen } g_1, \ldots, g_k \text{ von } G$$
$$x \in C^\perp \iff x \cdot h_j = 0 \text{ für alle Zeilen } h_1, \ldots, h_r \text{ von } H$$

Lemma 2.7 *Bei* $G = (I_k|P)$ *kann man* $H = (-P^\top|I_r)$ *als Kontrollmatrix nehmen.*

Beweis

$x \in C \iff x \cdot h_j = 0$ für $j = 1, \ldots, r \qquad h_j = (h_{j_1}, \ldots, h_{j_n})\, G = (I_k|P)$
$\implies x = (a_1 \ldots a_k, b_1 \ldots b_r)$ mit $b_j = a_1 p_{1j} + \cdots + b_r h_{j,k+r}$
erfüllbar bei $h_{j,k+\mu} := \delta_{j\mu}$ und $\underbrace{-p_{1j}}_{=h_{j1}}, \ldots, \underbrace{-p_{kj}}_{=h_{jk}}$

$\implies h_j = (-p_{1j}, \ldots, -p_{kj}, \delta_{j1}, \ldots, \delta_{jr})$ für $j = 1, \ldots, r \qquad$ bzw. $H = (-p^\perp|I_r)$

Beispiel

zu Bsp.: 1 $G = \begin{smallmatrix} 100:11 \\ 010:10 \\ 001:01 \end{smallmatrix} \implies H = \left(\begin{smallmatrix} 110:10 \\ 101:01 \end{smallmatrix}\right)$

zu Bsp.: 2 $G = \left(\begin{smallmatrix} 10:01 \\ 01:11 \end{smallmatrix}\right) \implies H = \left(\begin{smallmatrix} 01:10 \\ 11:01 \end{smallmatrix}\right)$

zu Bsp.: 3 $G = \begin{smallmatrix} 1 & & 0 & :1 \\ & \ddots & & \\ 0 & & 1 & :1 \end{smallmatrix} \implies H = (1 \ldots 1 : 1)$

Definition 2.8 (Syndrom) *Sei* $C \subseteq F^n(n,k) - Code$, $C^\perp$ *orthogonal zu* C, H *die Kontrollmatrix und* $y \in F^n$ *beliebig.*
Dann heisst der Vektor $y \cdot H^\perp = (y \cdot h_1, \ldots, y \cdot h_r)$ ***Syndrom*** *von* y.

Beispiel
Zu Bsp.1: $H = \left(\begin{smallmatrix} 110:10 \\ 101:01 \end{smallmatrix}\right)$ sei $y = (10111)$. Also:

$$y \cdot H^\top = (10111) \begin{smallmatrix} 11 \\ 10 \\ 01 \\ 10 \\ 01 \end{smallmatrix} = (1+0+0+1+0, 1+0+1+0+1) = (0,1) \text{ also } y \notin C.$$

Satz 2.9 $\quad x \in C \iff x \cdot H^\top = (0, \cdot, 0)$ *[o.Beweis]*

Lemma 2.10 *Sei* $F = \mathrm{GF}(2)$. *Dann ist für ein beliebiges* $y \in F^n$ *das Syndrom* $S_y := y \cdot H^\top$ *(bis auf transposition) dei Summe derjenigen Spalten von* H, *für welche die entsprechende Komponente von* y *die 1 ist.*

Beweis

$$y = (a_1, \ldots, a_n) \quad H = \begin{pmatrix} h_{11} & \ldots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{r1} & \ldots & h_{rn} \end{pmatrix}$$

$$\Longrightarrow S_y = y \cdot H^\top = (a_1 \cdot h_{11} + \cdots + a_n \cdot h_{1n}, \ldots, a_1 h_{r1} + \cdots + a_n h_{rn})$$

$$\Longrightarrow S_y^\top = \begin{pmatrix} a_1 h_{11} & \ldots & a_n h_{1n} \\ \vdots & \ddots & \vdots \\ a_1 h_{r1} & \ldots & a_n h_{rn} \end{pmatrix} = a_1 \begin{pmatrix} h_{11} \\ \vdots \\ h_{r1} \end{pmatrix} + \cdots + a_n \begin{pmatrix} h_{1n} \\ \vdots \\ h_{rn} \end{pmatrix} = \sum_{\substack{j=1 \\ a_j = 1}}^{n} \begin{pmatrix} h_{1j} \\ \vdots \\ h_{rj} \end{pmatrix}$$

Beispiel
$y = 10111 \quad H = \left(\begin{smallmatrix} 110{:}10 \\ 101{:}01 \end{smallmatrix}\right) \Longrightarrow S_y^\top = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$

$x = a_1 \ldots a_n \in C$ mit $a_i \in \{0, 1\}$. $\gamma(x) = d_x \neq 0$ für $x \neq 0 \ldots 0$, also $d_x \geq 1$.
Aus $x \in C$ folgt $s_x^\top = 0$ ist Summe von d_x Spalten von H.
$s_x^\top = \left.\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\right\} = r$, also gibt es d_x linear abhängige Spalten in H.
Wenn $d_x = 1$ gilt, gibt es in G die "0-Spalte".

Satz 2.11 *Sei C ein $(n,k)-$Code über $F = \mathrm{GF}(q)$ mit Kontrollmatrix H_i. Dann hat C genau dann Minimalgewicht d_0, wenn je $d_0 - 1$ Spalten von H linear unabhängig sind. In H gibt es d_0 linear anbhängige Spalten.*

Beweis

Seien $\bar{h_1}, \ldots, \bar{h_n}$ die n Spalten von H.

"$\Longrightarrow$" $d(C) = d_0 \Longrightarrow$

1. Es existiert ein $x = a_1 \ldots a_n \in C$ mit $\gamma(x) = d_0$.
   Sei $a_\nu \neq 0$ für $\nu \in I \subseteq \{1, \ldots, n\}, |I| = d_0$ und $a_\nu = 0$ für $\nu \notin I$.
   $\Longrightarrow x \in C \Longrightarrow 0 = x \cdot H^\top = \sum_{\nu=1}^{n} a_\nu \bar{h_\nu} = \sum_{\nu \in I}^{n} a_\nu \bar{h_\nu}$
   Also sind die d_0 H-Spalten $\bar{h_\nu}, \nu \in I$ linear abhängig.

2. Für kein $x \in C$ ist $1 \leq \gamma(x) \subseteq d_0 - 1$, je $d_0 - 1$ H-Spalten sind also linear unabhängig.
   Beweis:

   Annahme: $d_0 - 1$ linear abhängige H-Spalten $\bar{h_\nu}, \nu \in I \subseteq \{1, \ldots, n\}, |I| = d_0 - 1$. Ist $\sum_{\nu \in I} a_\nu \bar{h_\nu} = 0$, und nicht alle $a_\nu = 0$. Sei $a_\nu \neq 0$ für $\nu \in I' \subseteq I, 1 \leq |I'| \leq d_0 - 1$ für Vektor $x \in F^n$ mit $a_\nu \neq 0$ für $\nu \in I'$, $a_\nu = 0$ sonst; gilt $S_x = xH^\top = 0$. Also $x \in C$ mit $\gamma(x) \leq d_0 - 1$ im Widerspruch zu Annahme.

"$\Longleftarrow$" 1. d_0 H-Spalten $\bar{h_\nu}$ mit $\nu \in I \subseteq \{1,\ldots,n\}, |I| = d_0$ linear abhängig.
Es gilt also $\sum_{\nu\in I} a_\nu \bar{h_\nu} = 0$, wobei nicht alle $a_\nu = 0$ sind. Je $d_0 - 1$ Spalten sind linear unabhängig, d.h. alle $a_\nu \neq 0$ (d_0 Stück)(sonst wären $d_0 - 1$ Spalten linear abhängig $\rightarrow$ Widerspruch).
Der Vektor $x \in F^n$, mit $a_\nu \neq 0$ für $\nu \in I, a_\nu = 0$ sonst , $|I| = d_0$ gehört zu C. In C existiert also ein x mit $\gamma(x) = 1$.

2. Sei $x = a_1 \ldots a_n \in C, 1 \leq \gamma(x) \leq d_0 - 1$. $a_\nu \neq=$ für $\nu \in I' \subseteq \{1,\ldots,n\}, 1 \leq |I'| \leq d_0 - 1$ und $a_\nu = 0$ für $\nu \in I'$.
Dann ist für kein $x \in C$ $1 \leq \gamma(x) \leq d_0 - 1$
Beweis:

Annahme: $x \in C$, also $0 = x \cdot H^\top = \sum_{\nu\in I'} a_\nu \bar{h_\nu} = \sum_{\nu\in I} a_\nu \bar{h_\nu}$ mit $I' \subseteq I$.
$|I| = d_0 - 1, a_\nu \neq 0$ für $\nu \in I'$, $a_\nu = 0$ für $\nu \in I - I'$.
Hieraus folgt, dass $d_0 - 1$ linear abhängige H-Spalten existieren, im Widerspruch zur Annahme.

Lemma 2.12
$d(C) \geq d_0 \iff$ *je* $d_0 - 1$ *H-Spalten sind linear unabhängig.* *[o.Beweis]*

2.1 Fehlerkorrektur in Linearcodes

Gesendet wird ein $x \in C$, empfangen ein $y \in F^n$. Bei $y \neq x$ ist $y = x + e$ "Fehlervektor" . Bei gegebenen y muss man also x und e Paare (x, e) mit $x \in C$ und $x + e = y$ bestimmen. C ist ein Vektorraum, also auch additive Gruppe und Untergruppe von $(F^n, +)$. Hieraus folgt, dass F^n aus C und den Nebenklassen $z + C$ mit geeigneten "Repräsentanten" $z \in F^n$ besteht. $z_1, z_2 \in F^n$ liegen also genau dann in der selben Nebenklasse, wenn $z_1 - z_2 \in C$ gilt. Wegen $y - e = x \in C$ gehören y, e zur selben Nebenklasse $N = y + C$ und $e \in y + C$. Insgesamt gibt es q^{n-k} Nebenklassen (einschließlich C).
Welches e ist also Element von der Nebenklasse $y + C$? Dies wird mit der *maximum likelihood* Annahme bestimmt. Es wird also ein $e \in y + C'$ mit minimalem Gewicht gesucht.

Definition 2.13 (Anführer) *Sei $N = y + C$ Nebenklasse von C. Dann heisst ein $e_0 \in N$ mit minimalem Gewicht* ***Anführer*** *von N.*

korollar o.Beweis

1. $y_1, y_2 \in N \iff y_1 H^\top = y_2 H^\top$
Die Nebenklassen sind also durch Syndrome charakterisierbar.

2. $e \in N$ ist Anführer von N. $\gamma(e)$ ist also der minimale Abstand eines jeden $y \in N$ von jedem $x \in C$.

Beispiel
Gilt für jeden Anführer e in N, dass $\gamma(e) = 3$, so hat jedes N mindestens 3

Fehler.
Alternativ gilt: Ist $y \in F^n, x \in C, y \in N$, dann folgt $d(y,x) \geq d(e)$, also e Anführer von N.

2.2 Syndromdecodierung

1. Für jedes der $q^{n-k}-1$ "interessanten" Syndrome $S \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ bestimme man eine Darstellung als $S = eH^\top$ mit *minimalen* $\gamma(e)$. Also den (oder die) Anführer e der Nebenklassen zu S. Speziell gilt, falls S Spalte Nummer j aus H ist, dann gilt $e = 0\ldots0\underset{j}{1}0\ldots0$, ansonsten ist es eine (binäre) Summe gewisser H Spalten.
2. Bilde eine Liste L aller Paare (S,e).
3. Für ein gegebenes y berechne $S_y = y \cdot H^\top$ und bestimme das e aus L für $S = S_y$. Dann war e der Fehler für dieses S, gesendet war also $x = y - e$.

Beispiel

$$G = \begin{matrix} 100:11 \\ 010:10 \\ 001:01 \end{matrix} \quad H = \begin{matrix} 110:10 \\ 101:01 \end{matrix} \quad d(C) = 2$$

$q^{n-k} - 1 = q^{5-3} - 1 = 3$ interessante Nkl für die Syndrome $\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}, \begin{smallmatrix} 1 \\ 0 \end{smallmatrix}, \begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$

Die Anführer sind also

S	e
01	00100,00001
10	01000,00010
11	10000

$y = 11011$ $S_y = 10 =$

$x_1 = 10011$

$x_2 = 11001$

Es gilt:

1. Es gibt genau dann mehrere Anführer e mit $\gamma(e) = 1$, wenn es in H identische Spalten gibt.
2. Für $d(C) \geq 3$ gibt es in einer Klasse höchstens einen Anführer mit Gewicht 1.

"Ungeeignet" in H sind also die Nullspalte, da dann $d(C) = 1$ und identische Spalten, da es dann mehrere Anführer gibt.

Kapitel 3

Spezielle lineare Codes

3.1 Hamming Codes

Wähle geeignetes H, also keine Nullspalte und paarweise verschiedene Spalten.

Satz 3.1 *Ein* ***binärer*** *Linearcode C korrigiert genau dann jeden 1-Bit-Fehler, wenn die Spalten von H paarweise verschieden sind und H auch keine Nullspalte besitzt.*

Beweis Übung auf Blatt 2

Anmerkung: Dies gilt so nicht bei nicht binären Codes.

Definition 3.2 (Hammingcode) *Der binäre Linearcode C, dessen Kontrollmatrix H genau die Binärdarstellung der Zahlen $1, 2, \ldots, 2^r - 1$ als Spalten hat, heisst* $(\mathbf{n}, \mathbf{k})$-***Hammingcode*** *mit $n = 2^r - 1, k = n - r (= 2^r - 1 - r)$*

Anmerkung: Die Codewortlänge n ist *nicht* beliebig lang!

Beispiel
$r = 3, n = 7, k = 4$ der $(7, 4)$ Hammingcode.

$$\tilde{H} = \begin{matrix} 0001111 \\ 0110011 \\ 1010101 \end{matrix} \underbrace{\quad H \quad}_{\text{Spaltenpermutiert}} = \begin{matrix} 0111 : 100 \\ 1011 : 010 \\ 1101 : 001 \end{matrix} \longrightarrow G = \begin{matrix} 1000 : 011 \\ 0100 : 101 \\ 0010 : 110 \\ 0001 : 111 \end{matrix}$$

$$\Longrightarrow x = a_1 \underbrace{a_2}_{\text{frei}} a_3 \underbrace{a_4}_{\text{frei}} a_5 a_6 a_7 \in C \text{ mit } \begin{matrix} a_5 = & & + & a_2 & + & a_3 & + & a_4 \\ a_6 = & a_1 & + & & + & a_3 & + & a_4 \\ a_7 = & a_1 & + & a_2 & + & & + & a_4 \end{matrix}$$

Folglich müsste also $d(C) \geq 3$ sein.

3.1.1 Hammingcodes mit beliebiger Wortlänge n

Bestimme r so, dass $2^{r-1} < n \leq 2^r - 1$, bilde H mit $2^r - 1$ Spalten und streiche $2^r - 1 - n$ Spalten. Hieraus ergibt sich eine $(r \times n)$ Matrix H'. Eine Code C' mit $d(C') \geq 3$ korriegiert 1 Fehler.

Beispiel

Streiche (bei $r=3$) Spalte $\begin{smallmatrix}1\\1\\1\end{smallmatrix}$ aus H, also $n=6$.

$$H = \begin{matrix}011:100\\101:010\\110:001\end{matrix} \Longrightarrow G = \begin{matrix}100:001\\010:101\\001:110\end{matrix} \quad (6,3)\text{-Code}$$

Die Nebenklasse für $\begin{smallmatrix}1\\1\\1\end{smallmatrix}$ hat also die Anführer $100100, 010010, 001001$. Also hat $y \in$NKL zum Syndrom $\begin{smallmatrix}1\\1\\1\end{smallmatrix}$ mindestens 2 Fehler

Fehlerkorrektur bei Hammingcodes

1. $e_\nu = 0\ldots0\underset{\nu}{1}0\ldots0$ $y = x + e_\nu, S_x = 0$

   $S_y = y \cdot H^\top = e_\nu \cdot H^\top = \nu$-te Spalte $\bar{h_\nu}$ von H. $\Longrightarrow$ Fehlerposition.

   Beispiel

   $H = \begin{matrix}000\ 1111\\011\ 0011\\101\ 0101\end{matrix}$ $y = 1011110$ $S_y = \begin{matrix}00111|\ 1\\01001|\ 0\\11010|\ 1\end{matrix}$ Spalte 5 ist falsch

   $\Longrightarrow x = 1011\mathbf{0}10$

2. entdeckt ein Hammingcode mit $d(C)=3$ zwei Fehler?

   $e_\nu = 0\ldots0\underset{\nu}{1}0\ldots0\underset{\mu}{1}0\ldots0$

   $\Longrightarrow$ $S_e = \bar{h_\delta}$ mit δ irgendeiner Nummer.

   Beispiel

   $x = 1011010$ $y = 0011110$ $e = 1000100$ $S_y = \begin{matrix}0111|1\\1001|0\\1010|0\end{matrix}$ 1 Fehler an Position 4?

Abhilfe: "Code-Erweiterung"

$x = a_1\ldots a_n$ ein Element des Hammingcodes, dazu $a_{n+1} = \sum_{i=1}^{n} a_1$, dann

$C \mapsto C', d(C') \geq 4$, dann $H' = \begin{matrix}&&&&0\\&\mathrm{H}&&&\vdots\\&&&&0\\1&\ldots&1&1&\end{matrix}$

$\Longrightarrow$ Fehlerkorrektur $y = b_1\ldots b_n b_{n+1}$

1 Fehler: $e = e_\nu = 0\ldots0\underset{\nu}{1}0\ldots0$ $S_y = S_e \neq 0$ $\sum_{i=1}^{n+1} b_i \neq 0$

2 Fehler: $e = e_\nu = 0\ldots0\underset{\nu}{1}0\ldots0\underset{\mu}{1}0\ldots0$ $S_y = S_e \neq 0$ $\sum_{i=1}^{n+1} b_i = 0$

Beispiel

$$H' = \begin{matrix}00011110\\01100110\\10101010\\11111111\end{matrix} \quad x = 1011010:0 \quad y = 1011110:1 \quad S_y = \begin{matrix}1\\0\\1\\1\end{matrix}$$

Also 1 Fehler an Position 5. $y' = 10111101$ $S_{y'} = \begin{smallmatrix}1\\0\\1\\0\end{smallmatrix}$ $\Longrightarrow$ 2 Fehler.

Lemma 3.3 *Sei C ein linearcode über* GF(q)*, welcher t-Fehler korrigiert (d.h. $d(C) = 2t+1$). Sei für $z \in F^n$ die Kugel $K(z,t) = \{y \in F^n | d(z,y) \leq t\}$ definiert. Dann ist für $x, x' \in C$*

$K(x,t) \cap K(x',t) = \emptyset$ *und* $|K(z,t)| = \sum_{n=0}^{t} \binom{n}{m}(q-1)^m$ *für* $z \in F^n$.

Beweis zu 2.:
$z = a_1 \dots a_n \in F^n$, für den Wert a_i existieren also für jede Position i, $(q-1)$ Möglichkeiten. Für $m \leq n$ feste Positionen existieren also $(q-1)^m$ Vektoren, welche an **diesen** m Positionen von z verschieden sind.
Es gibt $\binom{n}{m}$ Möglichkeiten für $m \leq n$ Positionen, es existieren also $\binom{n}{m}(q-1)^m$ Vektoren, welche an m Positionen von z verschieden sind. Für $0 \leq m \leq t$ entsteht also $|K(z,t)| = \sum_{m=0}^{t} \binom{n}{m}(q-1)^m$

Definition 3.4 *Sei C ein Linearcode über* $\mathrm{GF}(q)$ *mit $d(C) = 2t+1$, genau dann heisst C* ***perfekt****, wenn* $\bigcup_{x \in C} K(x,t) = F^n$

Anmerkung: sonst gilt nur $\bigcup_{x \in C} K(x,t) \subseteq F^n$.

Lemma 3.5 *Sei $C \subseteq F^n$ über $GF(q)$ mit $d(C) = 2t+1$. Dann gilt, dass C genau dann perfekt ist, wenn* $\sum_{m=0}^{t} \binom{n}{m}(q-1)^m = q^{n-k}$.

Beweis:
Die $K(x,t)$ sind disjunkt, ????? $|K(x,t)| = |\bigcup_{x \in C} K(x,t)| = \sum_{x \in C} |K(x,t)| = |C| \cdot \sum_{m=0}^{t} \binom{n}{m}(q-1)^m$ wegen C perfekt ist $q^n = q^k \cdots = q^{n-k}$

$\Longrightarrow$ C ist perfekt, nach Definition gilt also, dass $\bigcup_{x \in C} K(x,t) = F^n$ also $|\bigcup_{x \in C} K(x,t)| = \sum_{x \in C} |K(x,t)| = \underset{\substack{\text{Anzahl der} \\ \text{Codewörter}}}{q^k} \cdot |K(x,t)|$

$= q^k \cdot \sum_{m=0}^{t} \binom{n}{m}(q-1)^m = |F^n| = q^n$ was zu zeigen war.

$\Longleftarrow$ Es gilt $K(x,t) \subseteq F^n$ für jedes $x \in C$, also ist $\bigcup_{x \in C} K(x,t) \subseteq F^n$.

Außerdem ist $|\bigcup_{x \in C} K(x,t)| = q^k \cdot \underbrace{\sum_{m=0}^{t} \binom{n}{m}(q-1)^m}_{q^{n-k}\text{ n.V.}} = q^n = |F^n|$. Da

die Mengen endlich sind folgt hieraus $\bigcup_{x \in C} K(x,t) = F^n$ und somit die Behauptung.

Satz 3.6 *Sei $C \subseteq F^n, F = \mathrm{GF}(q), d(C) = 2t+1$. C ist genau dann perfekt, wenn genau die e mit $\gamma(e) \leq t$ die Nebenklassen-Anführer sind.*

Beweis:

1. Aus $d(C) = 2t+1$ folgt, dass jedes $e \in F^n$ mit $\gamma(e) \leq t$ in einer Nebenklasse von C liegt und e der *einzige* Vektor mit $\gamma(e) \leq t$ in dieser Klasse ist. (d.h. e ist Anführer).

   Beweis:
   Aus $d(C) = 2t+1$ folgt, dass $e \in F^n$ mit $\gamma(e) \leq t$ kein Element von C ist. Sei also $e \in N$ geeignete Nebenklasse. Sei $e' in F^n$, aus $e' \neq e$ und $\gamma(e') \leq t$ folgt, dass $e' \in N$, da: Annahme: $e, e' \in N$ also $e - e' =: z \in C \implies \gamma(e - e') \geq 2t+1$.

Aber $\gamma(e-e') \leq \gamma(e)+\gamma(-e') = \gamma(e)+\gamma(e') \leq 2t$ im Widerspruch zur Vorraussetzung. Also ist e der einzige Vektor mit $\gamma(e) \leq t$ in N, folgich ist e eindeutiger Anführer von N.

2. "$\Longrightarrow$" C ist perfekt, also überdecken die disjunkten $K(x,t)$ für $x \in C$ den *ganzen* F^n. D.h. für jeden beliebigen Vektor $y \in F^n$ existiert genau ein $x \in C$ mit $y \in K(x,t)$ und $d(y,x) \leq t$. Sei $e := y - x$ eindeutig bestimmt zu y, $\gamma(e) \leq t$ und $e \in N_y$. Nach 1. ist e Anführer von N_y mit $y \in F^n$ beliebig, also hat jede Nebenklasse von C einen, nach 1. eindeutigen, Anführer mit Gewicht $\leq t$. Folglich ist jedes e mit $\gamma(e) \leq t$ ein eindeutiger Anführer einer Nebenklasse.

3. "$\Longleftarrow$" $y \in F^n$ ist beliebig. Behauptung: zu y existiert ein eindeutig bestimmtes $x \in C$ mit $y \in K(x,t)$. Dies ist trivial für $y \in C$ nämlich $y = x$. Was ist aber mit $y \in C$ und $y = x + e$ mit $x \in C$, welche Werte haben x, e?
Jedenfalls gilt $e \in N_y$. Sei e also Anführer von N_y, dann gilt nach Vorraussetzung, dass $\gamma(e) \leq t$ und (nach 1.) eindeutig bestimmt ist. Folglich ist in $x := y - e$ mit $x \in C$ y eindeutig bestimmt.
$d(y,x) = y(e) \leq t$, also ist $y \in K(x,t)$ mit eindeutig bestimmten $x \in C$, also liegt jedes $y \in F^n$ in $K(x,t)$ mit $x \in C$, woraus sich die perfektheit des Codes ergibt.

3.2 nicht binäre Hammingcodes

Wieder sei $d(C) \geq 3$, je 2 Spalten von H sind also linear unabhängig.

Lemma 3.7 *Seien $\bar{a}, \bar{b}$ H-Spalten mit $\emptyset \neq \bar{a} \neq \bar{b} \neq \bar{0}$. Für $(\alpha,\beta) \neq (0,0)$ und $\alpha, \beta, \varphi \in \mathrm{GF}(q)$ gilt dann:*

$$\alpha\bar{a} + \beta\bar{b} = \bar{0} \quad \Longleftrightarrow \quad \bar{b} = \varphi\bar{a} \text{ mit } \varphi = 0$$

Beweis:

1. $\alpha\bar{a} + \beta\bar{b} = \bar{0}, \bar{a} \neq \bar{0}, \bar{b} \neq \bar{0}, (\alpha,\beta) \neq (0,0)$
$\Longrightarrow \alpha \neq 0$ oder $\beta \neq 0 \quad \Longrightarrow \quad \bar{b} = \gamma\bar{a}$ mit $\gamma = -\alpha\beta^{-1} \neq 0$

2. $\bar{b} = \gamma\bar{a} \Longrightarrow \alpha\bar{a}+\beta\bar{b} = (\alpha+\beta\gamma)\bar{a} = \bar{0}$ für $\beta \neq 0$ beliebig, also $\alpha = -\beta\gamma \neq 0$. Fr nichtlineares H whle aus jeder Klasse der skalaren Vielfachen eines r-Tupels je einen Reprsentanten. Pro Klasse gibt es $q-1$ Spalten, wobei $q^r - 1$ davon nicht der 0-Vektor sind. $\Longrightarrow$ $n = \frac{q^r-1}{q-1}$ und $K = n - r$. ??????

Beispiel
$q = 3$, $\gamma \neq 1$, $\bar{a} = \begin{smallmatrix}1\\2\end{smallmatrix}$, $\bar{b} = \begin{smallmatrix}2\\\gamma\end{smallmatrix} \cdot \begin{smallmatrix}1\\2\end{smallmatrix} = \begin{smallmatrix}2\\1\end{smallmatrix} \quad \Longrightarrow \quad \bar{a} + \bar{b} = \bar{0}$

Definition 3.8 (verallgemeinerter Hammingcode)
Ein Linearcode C über $\mathrm{GF}(q)$ *mit $(r \times n)$-Kontrollmatrix H, $h = \frac{q^r-1}{q-1}$ ohne* $\bar{0}$

und $\bar{h_\nu} \neq \gamma \bar{h_\mu}$ für 2 Spalten $\bar{h_\nu}, \bar{h_\mu}$ heisst ***verallgemeinerter Hamingcode*** *(VHC).*

Beispiel
$q = 3,\ r = 3,\ n = \frac{3^3-1}{3-1} = 13,\ k = n - r = 10$
Man erhält also einen ternären $(13, 10)$-Code mit $H = \begin{matrix} 0000111111111 \\ 0111000111222 \\ 1012012012012 \end{matrix}$

Lemma 3.9 *Der verallgemeinerte Hammingcode ist perfekt*

Beweis: siehe Übung

Sei $A(z) = \sum_{i=0}^{n} A_i z^i$ Gewichtsfunktion mit A_i der Anzahl der $x \in C$ mit $\gamma(x) = i$.

Satz 3.10 *Sei C binärer Hammingcode mit $n = 2^r - 1$,*
dann ist $A(z) = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}$

Beweis:

1. **Rekursionsformel für die A_i**
   Sei $I \subseteq \{1, \ldots, n\}, |I| = i - 1, s(I) := \sum_{\nu \in I} \bar{h_\nu}$ mit H-Spalten. $S(I) = y \cdot H^\top$ für $y = b_1 \ldots b_n \in F^n$ mit $b_\nu = 1$ für $\nu \subseteq I$, $b_\nu = 0$ sonst.
   Es gibt $\binom{n}{n-1}$ Mengen I. Klasse bzgl. $s(I)$?????

   (a) $I_1, S(I_1) = 0, yH^\top = 0 \quad \Longrightarrow \quad y \in C$ mit $\gamma(y) = i - 1$.
   Die Anzahl der Teilmengen vom Typ I_1 ist also A_{i-1}

   (b) $I_2, S(I_2) = \bar{h_\mu} \neq \bar{0}$ mit $\mu \in I_2$. $\Longrightarrow \sum_{\nu \in I_2 - \{\mu\}} = \bar{0} \Longrightarrow yH^\top = 0, y \in C$ mit $b_\nu = \begin{cases} 1 & \text{für} \nu \in I_2 - \{\mu\} \\ 0 & \text{sonst} \end{cases}$.
   $\gamma(y) = i - 2$ also ist die Anzahl der Mengen $I_2 - \{\mu\}$ gleich A_{i-2} (= Anzahl der $y \in C$ mit $\gamma(y) = i - 2$).
   Sei $I_y \subseteq \{1 \ldots n\}$ mit $b_\nu = 1$ für $\nu \in I_y$, dann entsteht die Menge I_2 aus I_1 durch Hinzufügen eines $\mu \notin I_y$. Zu einem festen I_y entstehen also $n - i + 2$ Mengen I_2 und für $y' \in C, y' \neq y$ ist $d(y, y') \geq 3$. Die I_2 für verschiedene $y \in C$ sind also disjunkt und folglich ist die Anzahl der Mengen $I_2 = (n - i + 2) \cdot A_{i-2}$

   (c) $I_3, S(I_3) = \bar{h_\nu} \neq \bar{0}$ mit $\mu \notin I_3$. $\Longrightarrow \sum_{\nu + I_3 + \{\mu\}} \bar{h_\nu} = \bar{0} \Longrightarrow y \in C$ mit $b_\nu = \begin{cases} 1 & \text{für } \nu \in I_3 + \{\mu\} \\ 0 & \text{sonst} \end{cases}$ $\gamma(y) = i$
   Die Anzahl der Mengen $I_3 + \{\mu\}$ ist A_i (= Anzhal der $\mu \in C$ mit $\gamma(y) = i$). Die Menge I_3 entsteht aus I_y durch weglassen eines $\mu \in I_y$. Zu festem I_y entstehen also i Mengen vom Typ I_3 (disjunkt für verschiedene $y \in C$. Folglich ist die Anzahl der Mengen I_3 gleich $i \cdot A_i$.

Insgesamt also $\boxed{iA_i + A_{i-1} + (n-i+2)A_{i-2} = \binom{n}{i-1}}$ für $i \geq 1$

Grenzfälle:

- $A_0 = 1, A_1 = 0$ (HC!), also $A_{i-1} = 0$
- $A_n = 1 : y = \underbrace{1 \ldots 1}_{\text{n-mal}}, yH^\top = \sum_{\nu=1}^{n} \bar{h_\nu} = \bar{0}$
  (pro Zeile in H also gerade Anzahl von einsen.)
  $A_n = 1 \Longrightarrow A_{n-1} = 0$. Fr x mit $\gamma(y) = n-1$ gilt sicher $y \notin C$
- $A_n = 1, A_{n-1} = 0 \Longrightarrow A_{n+1} = 0$ usw. $\Longrightarrow A_{n+k} := 0$ für $k \geq 1$

2. Aus der Rekursionsformel folgt die Differentialgleichung für $A(z)$: multipliziere *Formel* mit z^{i-1} und summiere über i von 1 bis $n+2$. Dann folgt die Differenzialgleichung $(1-z^2) \cdot A'(z) + (1+nz)A(z) = (1+z)^4$ und ihre Lösung liefert das Ergebnis.

Beispiel
$n = 7, k = 4, (7,4)$-Hammingcode
$A(z) = \frac{1}{8}(1+z)^7 + \frac{7}{8}(1+z)^3 \cdot (1-z)^4 = 1 + 7z^3 + 7z^4 + z^7$
Der Faktor von z gibt die Anzahl der Vektoren, die Potenz das Gewicht an.

Lemma 3.11 *Sei C ein (n,k)-Code mit $d(C) = 2t+1$, dann gilt für die Informationsrate (2.3) $R := \frac{k}{n}$: (Hammingschranke)*

$$R \leq 1 - \frac{1}{n} \log_q \sum_{m=0}^{t} \binom{n}{m} (q-1)^m$$

Beweis: siehe Übung

Satz 3.12 (Varšamov-Schranke) *Seien n, k, d natürliche Zahlen mit $k, d \leq n$ $d \geq 2$ und Primzahl q. Wenn $\sum_{m=0}^{d-2} \binom{n-1}{m}(q-1)^m < q^{n-k}$ gilt, dann existiert ein (n,k)-Code über $\mathrm{GF}(q)$ mit Minimalgewicht d.*

Beweis:

1. $d \geq 2 \quad \Longrightarrow \quad k < n, r = n-k \geq 1$
2. Konstruiere für $r \geq 1$ eine $(r \times n)$-Kontrollmatrix H mit jeweils $d-1$ linear unabhängigen Spalten. Dann definiert H einen Code mit Mindestgewicht $\geq d$. Benötigt werden n geeignete Spalten $\bar{s_i} \in F^r - \{\bar{0}\}$ für H.
   Sei $\bar{s_1} \in F^r - \{\bar{0}\}$ beliebig.$\Longrightarrow$ "Matrix" H_1 mit der 1 Spalte $\bar{s_1}$, dann je $d-1$ Spalten linear unabhängig.
   Induktion für $i = 2, \ldots, n$:
   Sei H_{i-1} eine $r \times (i-1)$ Matrix, Spalten $\bar{s_1}, \ldots, \bar{s_{i-1}}$ mit je $d-1$ dieser Spalten linear unabhängig.
   Gesucht sind $\bar{s_i}$ derart, dass H_i mit Spalten $\bar{s_1}, \ldots, \bar{s_{i-1}}, \bar{s_i}$ und je $d-1$ Spalten linear unabhängig.
   Betrachte die als $\bar{s_i}$ ungeeigneten $\bar{y} \in F_i^r$. $\bar{y} \in F^r$ ungeeignet, falls $\bar{y}$

eine Linearkombination von $d-2$ oder weniger Spalten $\in \{\bar{s_1} \dots \bar{s_{i-1}}\}$ mit Koeffizienten sämtlich $\neq 0$

Sei a die Anzahl der ungeeigneten $\bar{y}$, dann gilt $a \leq \sum_{m=1}^{d-2} \binom{i-1}{m}(q-1)^m$.
entweder $\bar{y} = \gamma_1 \bar{s_\nu}, \gamma_1 \in F - \{0\}, \bar{s_\nu} \in \{\bar{s_1}, \dots, \bar{s_{i-1}}\} \Longrightarrow a_1 = (q-1) \cdot (i-1) = \binom{i-1}{1} \cdot (q-1)^1$
oder $\bar{y} = \gamma_1 \bar{s_\nu} + \gamma_2 \bar{s_\mu}$ mit $\gamma_1, \gamma_2 \in F - \{0\}, \bar{s_\nu}, \bar{s_\mu} \in \{\bar{s_1}, \dots, \bar{s_{i-1}}\}, \bar{s_\nu} \neq \bar{s_\mu}$ also $a_2 = \binom{i-1}{1} \cdot (q-1)^2$
usw. bis $m = d-2$ Spalten. Also

$$
\begin{aligned}
a \leq a_1 + a_2 + \dots + a_{d-2} &= \sum_{m=1}^{d-2} \binom{i-1}{m} (q-1)^m \\
&< \sum_{m=0}^{d-2} \binom{i-1}{m} (q-1)^m \leq \sum_{m=0}^{d-2} \binom{n-1}{m} (q-1)^m \\
&\underset{\text{n.V.}}{\leq} q^{n-k} = q^r = |F^r|
\end{aligned}
$$

Es existiert also eine *geeignete* Spalte $\bar{s_i} \in F^\nu - \{\bar{0}\}$, also $H = H_n = (\bar{s_1}, \dots, \bar{s_n}), (r \times n)$ Kontrollmatrix für einen (n,k)-Code über GF(q) mit Minimalgewicht $\geq d$.

Definition 3.13 (quasiperfekt)
C binärer (n,k) - Code mit $d = 2t$.
C heisst ***quasiperfekt*** $\iff \bigcup_{x \in \mathcal{C}} K(x,t) = F^n$

Lemma 3.14 *Der durch ein Paritätsbit erweiterte binäre Hammingcode ist quasiperfekt.*

Beweis

1. C sei binärer Hammingcode. Erweitert man diesen, so erhällt man einen $C' = (n+1, k)$ - Code.

   $$x' = a_1, \dots, a_n, a_{n+1} \in C \iff x = a_1, \dots, a_n \in C' \text{ mit } a_{n+1} = \sum_{i=1}^{n} a_i$$

   Sei H Kontrollmatrix des C $\Longrightarrow$ $H' = \begin{pmatrix} & \text{H} & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ 1 & \dots & 1 & 1 \end{pmatrix}$

2. Annahme: $d(C') = 4$

   a) In H' sind je 3 Spalten linear unabhängig: $d(C) = 3$
   $\Longrightarrow$ in H gibt es 3 lin. abh. Spalten., aber evtl. lin. unabhängige. ????
   paarweise?

   Fall 1 $\bar{h_\nu}, \bar{h_\mu}, \bar{h_\lambda} \in H$ linear unabhängig.
   $\Longrightarrow$ in $H' \binom{\bar{h_\nu}}{1}, \binom{\bar{h_\mu}}{1}, \binom{\bar{h_\lambda}}{1}$ linear unabhängig.

Fall 2 $\bar{h_\nu}, \bar{h_\mu}, \bar{h_\lambda} \in H$ linear abhängig. $\Longrightarrow$ $\bar{h_\nu} + \bar{h_\mu} = \bar{h_\lambda}$
$\Longrightarrow$ in H' $\binom{\bar{h_\nu}}{1} + \binom{\bar{h_\mu}}{1} = \binom{\bar{h_\lambda}}{0}_{\notin H'} \neq \binom{\bar{h_\lambda}}{1}$ linear unabhängig
$\bar{h_\nu}, \bar{h_\mu} \in H \Longrightarrow \bar{h_\nu} \neq \bar{h_\mu}, \bar{h_\nu} + \bar{h_\mu} \neq 0$
$\Longrightarrow$ in $H' : \binom{\bar{h_\nu}}{1} + \binom{\bar{h_\mu}}{1} \neq \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$
$\Longrightarrow$ auch drei H' - Spalten unter Beteiligung von $\begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$ sind linear unabhängig.

b) in H' existieren 4 linear unabhängige Spalten:
in $H : \bar{h_\nu} + \bar{h_\mu} + \bar{h_\lambda} = 0 \Longrightarrow \binom{\bar{h_\nu}}{1} + \binom{\bar{h_\mu}}{1} + \binom{\bar{h_\lambda}}{1} = \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$

3. Annahme: Die Kugeln des C' überdecken ganz F^{n+1}
Sei $y' = b_1, \ldots, b_n, b_{n+1} \in F^{n+1}$

$\Longrightarrow$ für $y := b_1, \ldots, b_n \in F^n$ existiert eindeutig ein $x = a_1, \ldots, a_n \in C$ mit $d(x, y) \leq 1$

$\Longrightarrow$ bilde $x' \in C$ mit
entweder $x' = a_1, \ldots, a_n 0 \in C' \Longrightarrow d(x', y') = d(x, y) + \left\{\begin{smallmatrix}0,\ b_{n+1}=0\\1,\ b_{n+1}=1\end{smallmatrix}\right\}$
oder $x' = a_1, \ldots, a_n 1 \in C' \Longrightarrow d(x', y') = d(x, y) + \left\{\begin{smallmatrix}0,\ b_{n+1}=1\\1,\ b_{n+1}=0\end{smallmatrix}\right\}$

$\Longrightarrow$ $d(x', y') \leq d(x, y) + 1 \leq 2$

$\Longrightarrow$ für jedes $y' \in F^{n+1}$ gilt $y' \in K(x', 2)$ mit $x' \in C'$

$\Longrightarrow$ $\bigcup_{x' \in C'} K(x', 2) = F^{n+1}$

Lemma 3.15 *Sei G Generatormatrix eines Hammingcodes C, mit Zeilen $g_1, \ldots, g_k$. Dann ist die Matrix G' mit Zeilen $g'_1, \ldots, g_k$ und $g'_i = g_i \cdot p(g_i)$* [1] *Generatormatrix von C.*

(ohne Beweis)

Beispiel
C sei (7,4) Hammingcode

$$H = \left(\begin{array}{cccc:ccc} 0&1&1&1&1&0&1\\ 1&0&1&1&0&1&0\\ 1&1&0&1&0&0&1 \end{array}\right) \qquad G = \left(\begin{array}{cccc:ccc} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&1&1 \end{array}\right)$$

$$H' = \left(\begin{array}{cccc:cccc} 0&1&1&1&1&0&1&0\\ 1&0&1&1&0&1&0&0\\ 1&1&0&1&0&0&1&0\\ 1&1&1&1&1&1&1&1 \end{array}\right) \qquad G' = \left(\begin{array}{cccc:cccc} 1&0&0&0&0&1&1&1\\ 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&1&0&1\\ 0&0&0&1&1&1&1&1 \end{array}\right)$$

$C'^{\perp}(8,4)-\text{Code}$ $\qquad$ $C'(8,4)-\text{Code}$

[1] Paritätssumme der Zeile g_i

(Übung $\Longrightarrow C'^{\perp} = C'$ und ist selbstdual)

3.3 Reed - Muller - Codes

Binär, Wortlänge $n = 2^m; m \geq 1$, konstruiere Generatormatrix G.
Zunächst $\Xi = (\xi_{ij}), m$ Zeilen 2^m Spalten.
Spalten $\bar{\xi_j}$: Binärdarstellung von $j = 0, 1, \ldots, 2^m - 1$ von unten nach oben gelesen und $j = \sum_{i=1}^{m} \xi_{ij} \cdot 2^{i-1}$

Beispiel

$$m = 3, j = 3, \bar{\xi_j} = \begin{matrix} 1 \\ 1 \\ 0 \end{matrix} \qquad \sum_{i=3}^{3} \xi_{ij} \cdot 2^{i-1} = \xi_{1j} \cdot 2^0 + \xi_{2j} \cdot 2^1 + \xi_{3j} \cdot 2^2$$
$$= 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 = 3$$

	0	1	0	1	0	1	0	1	v_1
	0	0	1	1	0	0	1	1	v_2
	0	0	0	0	1	1	1	1	v_3
j	0	1	2	3	4	5	6	7	

Die Zeile v_i $(1 \leq i \leq m)$ enthält abwechselnd 2^{i-1} Nullen und 2^{i-1} Einsen.

Definition 3.16 *Sei* $x = a_0, \ldots, a_{n-1}$; $y = a_0, \ldots, a_{n-1} \in F^n$;
$F = \mathrm{GF}(2) = \{0, 1\}$
Dann $z = x \,\pi\, y := (a_0 b_0, a_1 b_1, \ldots, a_{n-1} b_{n-1})$ *(Komponentenweises Produkt)*

Anmerkung $a_i \cdot b_i = 1 \quad \Longleftrightarrow \quad a_i = b_i = 1$

Definition 3.17 *Sei* $I \subseteq \{1, \ldots, m\}$, *dann ist*

$$v_I := \prod_{i \in I} v_i \quad \textit{für } |I| \geq 1$$
$$v_0 := v_\emptyset := \underbrace{1 \ldots 1}_{n\text{-}mal}$$

Anmerkung

a) es gibt 2^m solcher I, also $2^m (= n)$ solcher v_I

b) für $|I| = 1, I = \{i\}$ ist $v_I = v_i$

Sämtliche v_I für $I \subseteq \{1, \ldots, m\}$ werden zusammengefasst als Zeichen einer Matrix Ξ', in (lexikographischer) Reihenfolge:

$$v_0; v_1, \ldots, v_m; v_{12}, \ldots, v_{m-1,m}; \ldots$$

$\Longrightarrow$ $2^m (= n)$ Zeilen der Länge 2^m

Beispiel
$m = 3, n = 2^3$

0	1	2	3	4	5	6	7	
1	1	1	1	1	1	1	1	v_0
0	1	0	1	0	1	0	1	v_1
0	0	1	1	0	0	1	1	v_2
0	0	0	0	1	1	1	1	v_3
0	0	0	1	0	0	0	1	v_{12}
0	0	0	0	0	1	0	1	v_{13}
0	0	0	0	0	0	1	1	v_{23}
0	0	0	0	0	0	0	1	v_{123}

(vertausche Zeile 3,4 $\Longrightarrow$ obere Dreiecksmatrix)

Satz 3.18 *Die Vektoren v_I mit $I \subseteq \{1, \ldots, m\}$ bilden eine* ***Basis*** *von F^n*

Beweis

1. Sei $y \in F^n$ beliebig $\Longrightarrow \quad y = \sum_{j=0}^{n-1} b_j e_j$. Die v_I sind paarweise verschieden[2].

2. Annahme: e_j ist darstellbar als $e_j = \prod_{i=1}^{m} (v_i + (1 + \xi_{ij}) v_0)$.
   Wobei $\hat{\xi}_{ij} := 1 + \xi_{ij}$ das Komplement ist.
   Sei $\Xi^{(j)}$-Matrix, enstanden aus Ξ dadurch, dass in allen Zeilen v_i der Ξ mit $\xi_{ij} = 0$ das v_i ersetzt wird durch das Kompliment $\hat{v}_i$.

   Beispiel
   $m = 3, \Xi^{(2)}$: $\begin{matrix} 10101010 & \hat{v}_1 \\ 00110011 & v_2 \\ 11110000 & \hat{v}_3 \end{matrix}$ 3. Spalte

   $\Longrightarrow$ in $\Xi^{(j)}$ nur genau eine Spalte j mit lauter Einsen. Die Spalten von $\Xi^{(j)}$ sind paarweise verschieden.

   Beispiel
   $e_2 = \hat{v}_1 \cdot v_2 \cdot \hat{v}_3 = (v_1 + v_0) \cdot v_2 \cdot (v_3 + v_0) = \cdots = v_{123} + v_{12} + v_{23} + v_2$

$$\hat{v}_i = v_i + v_0 \qquad u_i^{(j)} := \begin{cases} v_i & \xi_{ij} = 1 \\ \hat{v}_i & \xi_{ij} = 0 \end{cases}$$

$$e_j = \prod_{i=1}^{m} u_i^j;\ u_i^{(j)} = v_i + (1 + \xi_{ij}) v_o \quad \Longrightarrow \quad e_j = \prod_{i=1}^{m} (v_i + (1 + \xi_{ij}) v_0)$$

Definition 3.19 *Sei $0 \leq s \leq m$. Dann heisst der Teilraum $C \subseteq F^n$ mit den Basisvektoren v_i für $I \subseteq \{1, \ldots, m\}$ mit $|I| \leq S(\leq m)$* ***Reed-Muller-Code der Ordnung*** s. $\mathrm{RM}(m, s)$

Speziell:

1. $s = 0 \quad G = (1 \ldots 1) \quad \mathrm{RM}(m, 0) = \{0 \ldots 0, 1 \ldots 1\}$

[2] (siehe Übungsblatt 5)

2. $s = m \quad G = \Xi' \quad \mathrm{RM}(m, m) = F^n$

3. Erweiterung auf $s > m$:
   $I \subseteq \{1, \ldots, m\}, s > m : |I| \leq s \implies |I| \leq m$
   für $s > m : \mathrm{RM}(m, x) = \mathrm{RM}(m, m)$.

Satz 3.20 $C = \mathrm{RM}(m, s) \quad \Longrightarrow \quad C^{\perp} = \mathrm{RM}(m, m-1-s)$

Beweis

Sei $s < m$. Sei a Basisvektor von $C = \mathrm{RM}(m, s)$ und b Basisvektor von $\mathrm{RM}(m, m-1-s)$.

Annahme: Skalarprodukt $a \cdot b = 0$:

$I \subseteq M = \{1, \ldots, m\}; \quad a = v_I,\ |I| \leq s,\ b = v_J,\ J \subseteq M,\ |J| \leq m-1-s$

$a \cdot b = \sum_{j=0}^{n-1} (a\pi b)_j$, d.h. $a \cdot b = 0 \iff \gamma(a\pi b)$ gerade.

$p := a\pi b \implies p$ ist Produkt von v_i mit maximal $s + (m-1-s) = m-1$ Faktoren, denn
$a = \prod_{i \in I} v_i,\ b = \prod_{i \in J} v_i,\ v_i \pi v_i = v_i$

$\implies p = v_K,\ K \subseteq M,\ |K| \leq m-1$

Annahme: Für $K \subseteq M$ gilt $\gamma(v_k) = 2^{m-|k|}$

$p = p_0, p_1, \ldots, p_{n-1} = v_k = \prod_{\mu \in k} v_\mu; \quad v_\mu = v_{\mu,0}, \ldots, v_{\mu,n-1}$

$\implies p_j = 1 \quad \iff \quad v_{\mu j} = 1$ für alle $\mu \in K$

$\implies \gamma(p) =$ Anzahl der j mit $p_j = 1$
$=$ Anzahl der j von Ξ, welche in den Positionen $\mu \in K$ eine 1 haben, ansonsten beliebig.

$\implies$ Es gibt, bei fester Belegung von $|K|$ Positionen einer Spalte, $2^{m-|K|}$ Spalten mit dieser festen Belegung.

$\implies \gamma(p) = 2^{m-|K|}$

$\implies$ Für $|K| \leq m-1$ ist $\gamma(p) = 2^l,\ l \geq 1$

Anmerkung: Für $|K| = m$ ist $\gamma(p) = 2^0 = 1$

Folgerung

1. $\mathrm{RM}(m, s)$ hat als Kontrollmatrix die Generatormatrix $RM(m, m-1-s)$
2. Für ein ungerades m ist speziell $\frac{m-1}{2} = m - 1 - \frac{m-1}{2}$
   $\implies \quad \mathrm{RM}\left(m, \frac{m-1}{2}\right)$ ist selbstdual

3.4 Fehlerkorrektur bei RM-Codes

Sei $x = a_0, \ldots, a_{n-1} \in \mathrm{RM}(m,s) \implies x = \sum\limits_{\substack{I \subseteq M \\ |I| \leq s}} \lambda_I v_i \quad \lambda_I = 0$ für $s < |I| \leq m$ nicht triviale "Codierung"

Aber es gibt eine Darstellung der λ_I mittels der a_j. Es sind sogar *mehrere* Darstellungen[3] als verschiedene Summen *verschiedender* a_j.

Beispiel

$$m = 3, s = 1$$
$$\lambda_1 = a_0 + a_1 = a_2 + a_3 = a_4 + a_5 = a_6 + a_7$$
$$\lambda_2 = a_0 + a_2 = a_1 + a_3 = a_4 + a_6 = a_5 + a_7$$
$$\lambda_3 = a_0 + a_4 = a_1 + a_5 = a_2 + a_6 = a_3 + a_7$$

Satz 3.21 *Sei $C = \mathrm{RM}(m,s)$ ein Reed-Muller-Code, sei $K \subseteq M := \{1, \ldots, m\}$ mit $|K| = S$, sei λ_K der Koeffizient von $v_K = \Pi_{i \in K} v_i$ der Darstellung eines $x = a_0, a_1, \ldots, a_{n-1} \in C$ durch die "Produktbasis". Dann gibt es 2^{m-s} voneinander unabhängiger Darstellungen des λ_K als Summe von jeweils 2^s der a_j, wobei jedes a_j genau einmal verwendet wird.*

Beweis

1. Sei $y = b_0 \ldots b_{n-1} \in F^n$ beliebig. $\implies y = \sum\limits_{j=0}^{n-1} b_j e_j$.

   genauer Bezug

   Die Formel für e_j (vgl. Beweis von Satz 3.18) liefert dann zunächst $e_j = \sum\limits_{I \subseteq M} \mu_I^{(j)} v_I$ mit Koeffizienten $\mu_I^{(j)}$.

   $$\implies y = \sum_{j=0}^{n-1} b_j \Big(\sum_{I \subseteq M} \mu_I^{(j)} \cdot v_i \Big) = \sum_{I \subseteq M} \underbrace{\left(\sum_{j=0}^{n-1} b_j \mu_I^{(j)} \right)}_{\lambda_I} v_i \implies \sum_{j=0}^{n-1} b_j \mu_I^{(j)}$$

   Wie sehen die $\mu_I^{(j)}$ aus?
   Jedenfalls gilt $\mu_I^{(j)} \in \{0,1\}$. Aus der Formel für die e_j folgt $\mu_I^{(j)} = \Pi_{i \notin I}(1 + \xi_{ij})$, denn der Koeffizient von v_i in dieser Formel ist Produkt von $p := |M| - |I|$ Faktoren der Form $(1 + \xi_{ij}) v_0$ für $i \notin I$.
   Daher $\mu_I^{(j)} v_0 = \Pi_{i \notin I}\big((1 + \xi_{ij}) \cdot v_0\big) = \big(\Pi_{i \notin I}(1 + \xi_{ij})\big) \cdot v_0$.
   Also $\mu_I^{(j)} = 1 \iff \xi_{ij} = 0$ für alle $i \notin I$.
   Für $C(I) := \{j : \xi_{ij} = 0$ für alle $i \notin I\}$ gilt also: $\mu_I^{(j)} = 1 \iff j \in C(I)$

[3] 2^{m-s} Darstellungen eines λ_I als summe von 2^s der a_j

Beispiel

$$\Xi = \begin{array}{cccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}$$

Ist etwa $I = \{1,2\}$, so $C(I) = \{0,1,2,3\}$. Oder $I = \{1\}$, dann ist $C(I) = \{0,1\}$. (Spaltenzählung beginnt bei 0, Zeilenzählung bei 1 !!)

Also $\lambda_I = \sum_{j \in C(I)} b_j$. Betrachte also jetzt $C(I)$. Wegen $j = \sum_{i=1}^{m} \xi_{ij} 2^{i-1}$ (vgl. (*) am Anfang von Kapitel 3.2) tragen für $j \in C(I)$ in der Summe $\sum_{i=1}^{m} \xi_{ij} 2^{i-1}$ höchstens die Potenzen 2^{i-1} mit $i \in I$ bei (für $i \notin I$ ist ja $\xi_{ij} = 0$ für diese j). ????? Für jede Wahl $\alpha_i \in \{0,1\}, i \in I$ gilt $j = \sum_{i \in I} \alpha_i 2^{i-1} \in C(I)$[4]

Beispiel
$I = \{i_1, i_2\} \implies C(I) = \{0, 2^{i_1-1}, 2^{i_2-1}, 2^{i_1-1} + 2^{i_2-1}\}$
Ist speziell $I = \{1,2\}$, so ist $C(I) = \{0, 2^{1-1}, 2^{2-1}, 2^{1-1} + 2^{2-1}\} = \{0,1,2,3\}$

Eigenschafften von $C(I)$:

(a) $C(\emptyset) = \{0\}$

(b) $C(I) = 2^{|I|}$

(c) Sei $i_0 \notin I$. Dann $C(I \cup \{i_0\}) = C(I) \cup \underbrace{\left(C(I) + 2^{i_0-1}\right)}_{\text{fr } j = \tilde{j} + 2^{i_0-1}, \tilde{j} \in C(I)}$

Beispiel
Für $j \in C(I \cup \{i_0\})$ ist $j = \sum_{i \in I \cup \{i_0\}} \alpha_i 2^{i-1}$.
Ist $\alpha_{i_0} = 0$, so $j = \sum_{i \in I} \alpha_i 2^{i-1} \in C(I)$
Ist $\alpha_{i_0} = 1$, so $j = 2^{i_0-1} + \sum_{i \in I} \alpha_i 2^{i-1} \in C(I) + 2^{i_0-1}$

2. Sei nun $x = a_0 \ldots a_{n-1} \in \mathrm{RM}(m,s)$. In der Darstellung des x durch die Produktbasis ist $\lambda_I = \sum_{j \in C(I)} a_j = 0$ für alle $I \subseteq M$ mit $|I| > s$. Für $I \subseteq M$ mit $|I| > s$ ist $I = K \cup J$ mit $|K| = s$ und $K \cap J = \emptyset, J \subseteq M \backslash K =: \bar{K}$
Eigenschaft (1c) mehrmals angewendet liefert: $C(I) = C(K) \dot{\cup} \left(C(K) + \sum_{i \in J} 2^{i-1}\right)$
Für $|I| > s$ ist dann

$$\lambda_I = 0 = \underbrace{\sum_{j \in C(K)} a_j}_{\lambda_K} + \sum_{j \in \left(C(K) + \sum_{i \in J} 2^{i-1}\right)} a_j$$

$$\implies \lambda = \sum_{j \in \left(C(K) + \sum_{i \in \bar{K}} \alpha_i 2^{i-1}\right)} a_j \qquad (3.1)$$

(betrachte K fest und beliebige Obermengen I)
(3.1) gilt also für beliebige $\alpha_i \in \{0,1\}$.
(3.1) gilt (K war beliebig) für alle $K \subseteq M$ mit $|K| = s$.

[4] Beweis selbstständig

3. Ist $|K| = s$, so $|\bar{K}| = m - s$. Also gibt es genau 2^{m-s} verschiedene Wertebelegungen der α_i.
   Weiterhin: die Mengen der Form $C(K)+\sum_{i\in\bar{K}} \alpha_i 2^{i-1}$ sind disjunkt für verschieden Wertegbelegungen der α_i und sie haben jeweils $|C(K)| = 2^s$ Elemente.

   Beispiel
   $m = 3$ Sei $s = 2$ und etwa $K = \{1, 2\}$, also $C(K) = \{0, 1, 2, 3\}$, $\bar{K} = \{3\}$

   $$\Longrightarrow \lambda_K = \sum_{\substack{j\in C(K)\\(\alpha_3=0)}} a_j = \sum_{\substack{j\in\ C(K)+2^{3-1}\\(\alpha_3=1)}} a_j$$

   $$\Longrightarrow \lambda_{12} = a_0 + a_1 + a_2 + a_3 = a_4 + a_5 + a_6 + a_7$$

   Sei $s = 1$ und etwa $K = \{3\}$, also $C(K) = \{0, 4\}$
   $\bar{K} = \{1, 2\} \Longrightarrow j \in \{0, 4\} + \ \alpha_1 \cdot 2^{1-1} + \alpha_2 \cdot 2^{2-1} \ = \{0, 4\} + (\underbrace{\alpha_1 + 2\alpha_2}_{\in\{0,1,2,3\}})$

   $$\Longrightarrow \lambda_3 = a_0 + a_4 = a_1 + a_5 = a_2 + a_6 = a_3 + a_7$$

$x = a_0 \ldots a_{n-1} = \sum_{|I|\le s} \lambda_I v_I$. Für $0 \le t \le s$: $x^{(t)} := \sum\limits_{|I|\le t} \lambda_I v_I$

$x = x^{(s)} \quad x^{(0)} = \lambda_0 v_0 \quad x^{(t)} \in \mathrm{RM}(m, t)$

Satz 3.22 *Für λ_I und $|I| = s$ existieren 2^{m-s} Darstellung als Summe gewisser a_j.*

Beweis:
$y = b_0 \ldots b_{n-1} = x + e$ mit Fehlervektor e. Also liefern manche b_j-Summen nicht λ_I. Falls $\gamma(e) \le 2^{m-s-1} - 1$ ist, liefern mehr als die Hälfte der Summe der b_j das Korrekte λ_I. Folglich ist $\lambda_I, |I| = s$ der Wert, welcher bei maximal $2^{m-s-1} - 1$ Fehlern am häufigsten als Summe der b_j auftritt. Also sind alle λ_I für $|I| = s$ korrekt bestimmbar.

Definition 3.23 $y^{(s)} := x^{(s)} + e = x + e = y$ *und* $y^{(s-1)} := y^{(s)} - \sum\limits_{|I|=s} \lambda_I v_I$[5]

$\Longrightarrow y^{(s-1)} = x^{(s-1)} + \mathbf{e} \quad x^{(s)} = x^{(s-1)} + \sum_{|I|=s} \lambda_I v_I$

$\Longrightarrow y^{(s)} = x^{(s)} + e = x^{(s-1)} + e + \sum_{|I|=s} \lambda_I v_I$ mit $x^{(s-1)} \in \mathrm{RM}(m, s-1)$

$\Longrightarrow$ für λ_I mit $|I| = s - 1$ existieren 2^{m-s+1} Darstellungen.

$\Longrightarrow$ bei $\sum b_j^{(s-1)}$ sind weniger als $1/4$ verändert, der Mehrheitsentscheid liefert also λ_I mit $|I| = s - 1$.

Setzt man dies fort, so erhält man alle λ_I mit $|I| \ge 1$ bis $y^{(0)} = x^{(0)} + e = \lambda_0 v_0 + e$. Dies führt zu einer Störung in maximal $2^{m-s-1} \le 2^{m-1} - 1$ Komponenten, also ist λ_0 bestimmt.

Beispiel

$\mathrm{RM}(3, 1) \quad \gamma(e) \le 2^{3-1-1} - 1 = 1 \quad G = \begin{matrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \end{matrix}$

[5] Die λ_I sind die korrekten Werte.

$|I| = S = 1 \quad I = \{1\}, I = \{2\}, I = \{3\} \quad C(I) = C(i) = \alpha_i 2^{i-1}$

I	1	2	3
C	$\{0,1\}$	$\{0,2\}$	$\{0,4\}$
$\sum_{i \in I} \alpha_i 2^{i-1}$	$0,2,4,6$	$0,1,4,5$	$0,1,2,3$

Sei $y = y^{(1)} = 11011100$, dann:

I					$Mehrheit$	
$\{1\}$	$b_0 + b_1 = 0$	$b_2 + b_3 = 1$	0	0	0	$\lambda_1 = 0$
$\{2\}$	1	0	1	1	1	$\lambda_2 = 1$
$\{3\}$	0	0	0	1	0	$\lambda_3 = 0$

$y^{(1)} + v_2 = 11011100 + 00110011 = 11101111 = y^{(0)} \quad \Longrightarrow \quad \lambda_0 = 1$
$\Longrightarrow x = v_0 + v_2 \quad e = 00010000 \quad \Longrightarrow \quad y = 11001100$

Lemma 3.24 *Der* $\mathrm{RM}(m, s)$ *hat ein Mindestgewicht von* 2^{m-s}

Beweis: siehe Übung.

Kapitel 4

Produkt- und Summencodes

4.1 Produktcodes

Das "Produkt" zweiser Linearcodes C_1, C_2 wird wie folgt definiert:

Definition 4.1 *Sei C_1 ein (n_1, k_1)-Code und C_2 ein (n_2, k_2)-Code. Sei A eine $n_1 \times n_2$ Matrix derart, dass jede Zeile A_i von A ein Vektor aus C_2 und jede Spalte $\bar{A}_j$ von A ein Vektore aus C_1 ist. Dann heisst die Menge C aller dieser Matrizen* ***Produktcode:*** $\mathbf{C} = C_1 \otimes C_2$

Existenz eines solchen A's:

Definition 4.2 (Kroneckerprodukt) *Seien $a = a_1 \dots a_{n_1}, b = b_1 \dots b_{n_2}$, dann heisst*

$$a \otimes b := \begin{pmatrix} a_1 b_1 & \cdots & a_1 b_{n_2} \\ \vdots & \ddots & \vdots \\ a_{n_1} b_1 & \cdots & a_{n_1} b_{n_2} \end{pmatrix} \qquad \textit{Kroneckerprodukt von } a \textit{ und } b$$

Anmerkung: Die Zeilen sind ein Vielfaches von b, die Spalten ein Vielfaches von a

Lemma 4.3 *1. Für $a \in C_1, b \in C_2$ ist $A := a \otimes b$ eine Matrix aus $C_1 \otimes C_2$.*

2. Es gilt $\gamma(A) = \gamma(a) \cdot \gamma(b)$.

Beweis:

1. trivil
2. siehe Übung Blatt 6

Satz 4.4 *Sei $C := C_1 \otimes C_2$ mit $d_1 = d(C_1), d_2 = d(C_2)$, dann gilt $d(C) = d(C_1) \cdot d(C_2)$*

Beweis:
Sei $A \in C, A \neq\!= 0$ (Nullmatrix), dann existiert eine Zeile $A_i = a_{i1} \dots a_{in_2}$

von A mit $A_i \not= 0$. $A_i \in C_2$ also $\gamma(A_i) = u \geq d_2$. Sei $a_{ij} \neq 0$ für $j \in J \subseteq \{1, \ldots, n_2\}, |J| = u$. $\bar{A}_j \in C_1 \Longrightarrow \gamma(\bar{A}_j) \geq d_1 \Longrightarrow \gamma(A) \geq d_1 u \geq d_1 d_2$ mit $u \geq d_2$.
Es existiert ein $a \in C_1, b \in C_2$ so, dass $\gamma(a) = d_1, \gamma(b) = d_2 \Longrightarrow \gamma(a \otimes b) = \gamma(a)\gamma(b) = d_1 d_2 \quad \Longrightarrow d(C) = d_1 d_2$

Beispiel
$C_1 = C_2 = \{0000, 0111, 1001, 1110\} a = 1001, b = 0111 \quad a \otimes b = \begin{smallmatrix} 0111 \\ 0000 \\ 0000 \\ 0111 \end{smallmatrix}$; $\gamma(a \otimes b) = b$
$B = \begin{smallmatrix} 1001 \\ 0111 \\ 0111 \\ 1111 \end{smallmatrix} \in C_1 \otimes C_2$ aber kein Kroneckerprodukt.

Satz 4.5 (Basis eines Produktcodes) *Sei $C = C_1 \otimes C_2$ mit $g_1, \ldots, g_{k_1}$ Basisvektoren von C_1 und $h_1, \ldots, h_{k_2}$ Basisvektoren von C_2. Dann ist C ein $(n_1 \cdot n_2, k_1 \cdot k_2)$-Code mit Basimatritze $g_i \otimes h_j$ für $(i = 1, \ldots, k; j = 1, \ldots, k_2)$.*

Beweis:
Behauptung: Die $k_1 \cdot k_2$ Matrizen $g_i \otimes h_j$ sind linear unabhängig:
Annahme: Sie sind linear abhängig.
Dann existiert für p Stück verschiedene Matrizen $g_{i_1} \otimes h_{j_1}, \ldots, g_{i_p} \otimes h_{j_p}$ (mit g_{i_ν} bzw. h_{j_ν} sind Basisvektoren von C_1 bzw. C_2) eine Linearkombination[1]

$$D = \lambda_1 g_{i_1} \otimes h_{j_1} + \cdots + \lambda_p g_{i_p} \otimes h_{j_p} = 0$$

mit $\lambda_\nu \neq 0$ für $\nu \in \{1, \ldots, p\}$.
Sei $g_{i_\nu} = g_{i_\nu,1} \ldots g_{i_\nu,n_1}$, dann hat die Matrix $g_{i_\nu} \otimes h_{j_\nu}$ Zeilen der Form $g_{i_\nu,i} \cdot h_{g_\nu}$. Also hat D Zeilen der Form:

$$D_i = \underbrace{\lambda_1 g_{i_1,i}}_{\text{Skalar}} \cdot h_{j_1} + \cdots + \lambda_p g_{i_p,i} \cdot h_{j_p} \quad \text{mit } D_i \in C_2$$

Aufgrund der Annahme $D = 0$ folgt, dass $D_i = 0$ (Zeile), also ist es wegen der Basisvektoren $h_{i_\nu} \in C_2$ notwendig, dass $\lambda_1 g_{i_1,i} = \cdots = \lambda_p g_{i_p,i} = 0$ ist.
Nach Vorraussetzung gilt aber $\lambda_\nu \neq 0$ für alle ν, also $g_{i_1,i} = \cdots = g_{i_p,i} = 0$ für alle $i \in \{1, \ldots, n_1\}$. Hieraus ergibt sich aber $g_{i_1} = \cdots = g_{i_p} = 0$ (Vektor) im Widerspruch zu g Basisvektoren. Dann aber $D = 0$ nur für $\lambda_\nu = 0$ für alle ν, dies heisst aber, dass die $g_i \otimes h_j$ ($k_1 \cdot k_2$ Stück) linear unabhängig. Also sind sie Basis eines $(n_1 \cdot n_2, k_1 \cdot k_2)$-Codes im Widerspruch zur Annahme.

Zeige noch, dass $A \in C = C_1 \otimes C_2$
A ist linear Kombination von gewissen $g_i \otimes h_j$. $A \in C$, also ist die Zeile $A_i \in C_2$ und $A_i = \sum_{\nu=1}^{k_2} \lambda_{i\nu} h_\nu$ mit $h_\nu = h_{\nu,1} \ldots h_{\nu,n_2}$. Für die Spalte $\bar{A}_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n_1,j} \end{pmatrix}$ gilt also $\boxed{\bar{A}_j = \sum_{\nu=1}^{k_2} h_{\nu,j} \cdot \bar{\lambda_\nu}}$ mit $\bar{\lambda_\nu} = \begin{pmatrix} \lambda_{1,\nu} \\ \vdots \\ \lambda_{n_1,\nu} \end{pmatrix}$.
Es entsteht also ein inhomogenes Gleichungssystem mit n_2 Gleichungen $(j = 1, \ldots, n_2)$ und k_2 Unbekannten $(\bar{\lambda}_1, \ldots, \bar{\lambda}_{k_2})$. Die Koeffizienten $h_{\nu j}$ sind inhomogene Spalten $\begin{pmatrix} \bar{A}_1 \\ \vdots \\ \bar{A}_{n_2} \end{pmatrix}$. $n_2 > k_2$, also ist das Gleichungssystem

????

[1] eine $n_1 \times n_2$-Matrix

überbestimmt, es ist also entweder eindeutig lösbar oder unlösbar.

Annahme: Es ist unlösbar, es existiert also kein $\lambda_{i\nu}$ mit $a_{ij} = \sum_{\nu=1}^{k_2} \lambda_{i\nu} h_{\nu j}$. Es sind also entweder $\bar{A}_j \notin C_1$ oder $A_1 \in C_2$ im Widerspruch zur Annahme, das Gleichungssystem ist also eindeutig lösbar.
Jedes $\bar{\lambda}_\nu$ ist also eindeutig als Linearkombination von $\bar{A}_j$ darstellbar. $\bar{A}_j \in C_1$ also $\bar{\lambda}_\nu \in C_1$ bzw. $\lambda_\nu \in C_1$ für alle $\nu = 1, \ldots, k_2$.
$A = (a_{ij})$ mit $a_{ij} = \sum_{\nu=1}^{k_2} \lambda_{i,\nu} h_{\nu,j}$.
$A = \sum_{\nu=1}^{k_2} A^{(\nu)}$ mit $A^{(\nu)} = (\lambda_{i,\nu} \cdot h_{\nu,j})$ und $a_{i,j}^{(\nu)} = \lambda_{i,\nu} \cdot h_{\nu,j}$. Also ist $A^{(\nu)} = \lambda_\nu \otimes h_\nu$ und somit $A = \sum_{\nu=1}^{k_2} (\lambda_\nu \otimes h_\nu)$.
$\lambda_\nu \in C_1$ also $\lambda_\nu = \sum_{\mu=1}^{k_1} b_\mu^{(\nu)} g_\mu$. Also insgesamt: $A = \sum_{\mu=1}^{k_1} \sum_{\nu=1}^{k_2} b_\mu^{(\nu)} (g_\mu \otimes h_\nu)$ ■

Aus einer Linearisierung von $g_i \otimes h_j$ (z.B. Zeilenweise) ergibt sich eine Zeilenlänge von $n_1 \cdot n_2$ und eine $(k_1 k_2 \times n_1 n_2)$ Basismatrix.

Beispiel

$G_1 = G_2 = \begin{matrix} 1001 & g_1 \\ 0111 & g_2 \end{matrix}$ $\quad d(C) = 2 \quad$ $G \otimes G = \begin{matrix} 1001 & 0000 & 0000 & 1001 & g_1 \otimes g_1 \\ 0111 & 0010 & 0000 & 0111 & g_1 \otimes g_2 \\ 0000 & 1001 & 1001 & 1001 & g_2 \otimes g_1 \\ 0000 & 0111 & 0111 & 0111 & g_2 \otimes g_2 \end{matrix}$

Permutiert zu Reduzierter Staffelform:

$$\begin{array}{llllll} 1000 & : & 0100 & 0000 & 1001 \\ 0100 & : & 1100 & 0000 & 0111 \\ 0010 & : & 0001 & 1001 & 1001 \\ 0001 & : & 0011 & 0111 & 0111 \end{array}$$

Man erhält also einen $(16, 4)$-Code mit $C = \{0000, 1001, 0111, 1110\}$

4.1.1 Fehlerkorrektur

$d(C \otimes C) = 4$ korrigiert einen Fehler: $A \in C \otimes C$ sei gestört in a_{ij}, dann ist die Zeile A_i und Spalte $\bar{A}_j$ fehlerhaft, also Position ij.

Beispiel

$$B = \begin{array}{cc|c|c} 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{array}$$

Anmerkung

1. Anzustreben sind $C \otimes c$ mit *kleinem* n für gegebenes $d(C)$.
2. *Fehlerbündel* sind korrigierbar bis zu einer Länge von einer Zeile (da dann pro Spalte nur 1 Fehler auftritt).

4.2 Summencodes

Definition 4.6 *C_1, C_2 seien (n, k_1)- bzw. (n, k_2)-Codes.*
*Dann heisst $C_1 \& C_2 := \{X_1 \oplus (X_1 + X_2) | x_1 \in C_1, x_2 \in C_2\}$ **Summe** von C_1 und C_2.*[2]

Beispiel
$C = \{0000, 0111, 1001, 1110\}$ also ein $(8, 4)$-Code mit $d(C\&C) = 2$.

0000	0000	0111	0111	1001	1001	1110	1110
	0111		0000		1110		1001
	1001		1110		000		0111
	1110		1001		0111		0000

Satz 4.7 *Sei C_1 ein (n, k_1)- und C_2 ein (n, k_2)-Code. Dann ist $C_1 \& C_2$ ein $(2n, k_1 + k_2)$-Code mit $d = \min(2d_1, d_2)$ und einer (möglichen) Generatormatrix $\left(\begin{array}{c|c} G_1 & G_1 \\ \hline 0 & G_2 \end{array}\right)$*

Lemma 4.8 *Sei $G(m, s)$ die Generatormatrix des Codes $\mathrm{RM}(m, s)$. Dann kann man $G(m, s)$ durch Zeilenumordnung in die Form $G(m, s) = \left(\begin{array}{c|c} G(m-1,s) & G(m-1,s) \\ \hline 0 & G(m-1,s-1) \end{array}\right)$*

Beispiel

$$G(3,2) = \left(\begin{array}{cccc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right) \begin{array}{l} v_0 \\ v_1 \\ v_2 \\ v_{12} \\ v_3 \\ v_{13} \\ v_{23} \end{array}$$

$$G(3,2) = \left(\begin{array}{c|c} G(2,2) & G(2,2) \\ \hline 0 & G(2,1) \end{array}\right), \quad G(2,2) = \left(\begin{array}{c|c} G(1,1) & G(1,1) \\ \hline 0 & G(1,1) \end{array}\right), \quad G(1,1) = \left(\begin{array}{c|c} G(0,0) & G(0,0) \\ \hline 0 & G(0,0) \end{array}\right) = \begin{smallmatrix} 11 \\ 01 \end{smallmatrix}$$

????

Beachte, dass $m \leq s$, sonst verkleinere s.

Satz 4.9 *Rekursionsformeln für Reed-Muller-Code:*

$$\mathrm{RM}(m, s) = \mathrm{RM}(m-1, s) \& \mathrm{RM}(m-1, s-1)$$

[2] $\oplus$ ist eine Konkatenation

Kapitel 5

Zyklische Codes

Definition 5.1 *Sei $C \subseteq F^n$ ein (n,k)-Linearcode. C heisst genau dann zyklisch, wenn für $x = a_0 a_1 \ldots a_{n-1} \in C$ auch $x' = a_{n-1} a_0 \ldots a_{n-2} \in C$ gilt.*

5.1 Mathematische Grundlagen

$a_0 a_1 \ldots a_{n-1} \longleftrightarrow a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} =: a(X)$ (Zuordnung).
Die Addition der Codewörter entspricht der Addition der Polynome (Gruppenhomomorphismus).
Verschiebung: $x \cdot a(X) = a_0 X + a_1 X^2 + \cdots + a_{n-2} x^{n-1} + a_{n-1} X^n \overset{?}{\longleftrightarrow} (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$
Bilde $Xa(X) \mod (x^n - 1)$:

$$\begin{aligned} X \cdot a(X) &= a_0 X + \cdots + a_{n-2} X^{n-1} + a_{n-1} X^n + a_{n-2} - a_{n-1} \\ &= a_{n-1}(X^n - 1) + \underbrace{(a_{n-1} + a_0 X + \cdots + a_{n-2} X^{n-1})}_{= X \cdot a(X) \mod (X^n - 1)} \end{aligned}$$

Betrachte die Menge der Divisionsreste aller Polynome (beliebigen Grades) mod $(X^n - 1)$.
$r(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$, die Addition erfolgt also Komponentenweise, die Multiplikation wie üblich bei Polynomen, aber es gilt stets: $x^n \mapsto 1$.

Beispiel
$q = 2, n = 2, X^n + 1 \quad \Longrightarrow \{0, 1, X, 1+X\} \qquad X \cdot (1+X) = X + X^2 \mapsto X + 1$

5.1.1 zyklische Verschiebung

$a(X) \in C$, also $Xa(x), X^2 a(X), \cdots \in C$. $b(X), C(X) \in C \Longrightarrow b(X) + c(X) \in C$. Mit $a(X) \in C$ auch $r(X) \cdot a(X) \in C$.
Die Polynommenge C aus den Polynomen $\mod X^n - 1$ ist in C, bezüglich der Addition und der Multiplikation mit beliebigem Polynom ($\mod x^n - 1$), abgeschlossen.

C ist **Ideal** in der Menge der Polynome $\mod (x^n - 1)$. Betrachte nur die "Hauptideale". Sei $\Re$ die Menge der Polynome $\mod (X^n - 1)$. Dann ist $\Re \cdot g(X)$ ein Ideal, wobei $g(X)$ ein "Basispolynom", mit $g(X)$ Teiler[1] von $X^n - 1$, ist. Es gilt also $X^n - 1 = g(X) \cdot h(X)$.
Betrachte ab jetzt nur noch Polynome $\mod X^n - 1$.

Wie bestimmt man die Teiler von $X^n - 1$?

Definition 5.2 (irreduziebel) *Ein Polynom ist **irreduziebel**, wenn es nicht als Produkt anderer Polynome aus $\Re$ darstellbar ist.*

Beispiel
$q = 2, n = 4, X^n - 1 = X^4 + 1 = (x+1)^4$ Die Basispolynome sind also
$1, X^4 + 1; 1 + X, \underbrace{(1+X)^2}_{1+X^2}, \underbrace{(1+X)^3}_{1+X+X^2+X^3}$
Bei einem zyklischen Code z.B. $\Re(1+X); r(X) = b_0 + b_1 X + b_2 X^2 + b_3 X^3$
$(1+X) \cdot r(X) = (b_3 + b_0) + (b_0 + b_1)X + (b_1 + b_2)X^2 + (b_2 + b_3)X^3$
$\Longrightarrow$ Codewörter $b_0 b_1 b_2 b_3 = (b_3 + b_0, b_0 + b_1, b_1 + b_2, b_2 + b_3) =$
0000 und 1111 gehen immer in sich selbst über
1010 geht in 0101 über
$g(X) = X^2 + X + 1$ ist kein Teiler von $X^4 + 1$.
Also $\Re g(X) = \Re$

1001 $\longleftarrow\!\!\!\!-$ 0011

1100 $-\!\!\!\!\longrightarrow$ 0110

Beispiel
$n = 7, X^7 + 1 = \underbrace{(X+1)}_{f_1} \cdot \underbrace{(X^3 + X^2 + 1)}_{f_2} \cdot \underbrace{(X^3 + X + 1)}_{f_3}$
Nicht triviale Basipolynome: $f_1, f_2, f_3, f_1 f_2, f_1 f_3, f_2 f_3$

Es gibt $X^n + 1 = (X + \alpha_1) \cdot (X + \alpha_2) \cdot \cdots \cdot (X + \alpha_n)$ die α_i n-te Einheitswurzeln.

?????

Sei $\alpha_n = 1$, was sind aber die $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$?

Beispiel
Analogie: Komplexe Zahlen: Was sind die Nullstellen von x^2+1 (im Reellen)?

Definition 5.3 (Erweiterungskörper) (Erweitern des "Grundkörpers" GF(2))
Sei $p(X)$ ein beliebiges irreduziebles *Polynom aus der Menge $\mathcal{P}$ aller Polynome. Dann bildet die Menge der Reste $\mathcal{P}$ und $p(X)$ einen **(Erweiterungs-) Körper** $\mathrm{GF}(2^m)$, falls $p(X)$ vom Grad m ist.*

$\mathrm{GF}(2^m)$ ist eine Menge von Polynomen der Form $a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$ (für alle Wertebelegungen $a_0, \ldots, a_{m-1}$). $\mathrm{GF}(2) \subset \mathrm{GF}(2^m)$
$0: a_0 = \cdots = a_{m-1} = 0 \qquad 1: a_0 = 1 \quad a_1 = \cdots = a_{m-1} = 0$

Es gilt: In GF(2) existiert ein "primitives Element" α derart, dass $\mathrm{GF}(2^m) = \{0, \alpha, \alpha^2, \ldots, \underbrace{\alpha^{2^m-1}}_{=1}\}$. Zum Rechnen in $GF(2^4)$ siehe Blatt.

Beispiel
$p(X) = X^4 + X + 1$ geeignet $\alpha = X$ $\mathrm{GF}(2^4) = \{0; \alpha, \alpha^2, \ldots, \alpha^{15}\}$; $X^4 \mapsto X + 1$
$\alpha^5 + \alpha^{10} = 1 + X^2 + 1 + X + X^2 = 1 = \alpha^{15}$
$\alpha^7 + \alpha^8 = 1 + X + X^3 + 1 + X^2 = \alpha^{11}$

[1] notwendig

Sei X^n+1 zerlegt in ein Produkt irreduzibeler Funktionen. Sei m der Höchstgrad eines dieser Faktoren. Dann sind alle n-ten Einheitswurzeln α_i Elemente des GF(2^m). Es entsteht also ein **Zerfallungskörper** für X^n+1. ????

Beispiel
$n=5 \quad X^6+1=(X+1)^2\cdot(X^2+X+1)^2 \implies m=2 \implies \alpha_1,\ldots,\alpha_6 \in$ GF(2^2)
GF(2^2): $p(X)=X^2+X+1$ geeignet
z.B. $\alpha=X$; $\alpha^2+\alpha+1=0$ mit $\alpha^2 \mapsto \alpha+1$
GF(2^2) $=\{0;\,1,\alpha,1+\alpha\}$ z.B.: $\alpha\cdot(1+\alpha)=\alpha+\alpha^2 \mapsto \alpha+1+\alpha=1$
$X^3+1=(X+1)(X^2+X+1)$
$X^5+1=(X+1)(X^4+X^3+X^2+X+1)$
$X^9+1=(X+1)(X^2+X+1)(X^6+X^3+1)$

Es gilt also, dass eine **primitive** n-te Einheitswurzel ζ existiert. Die n-ten Einheitswurzeln sind: $\zeta,\zeta^2,\ldots,\zeta^{n-1},\underbrace{\zeta^n}_{=1}$?????

Beispiel
$n=6$, geeignet ist dann z.B.: $\zeta=\alpha \in$ GF(2^2) (oder auch α^2).
$\zeta=\alpha \quad \zeta^2=1+\alpha \quad \zeta^3=1 \quad \zeta^4=\alpha \quad \zeta^5=1+\alpha \quad \zeta^6=1$

Beispiel
$n=5$, dann ist die 5-te Einheitswurzel ein Element von GF(2^4). (Allein) geeignet ist $\zeta=\alpha^3$
$\zeta^5=1 \quad \zeta^2=\alpha^2+\alpha^3=\alpha^6 \quad \zeta^3=\alpha+\alpha^3=\alpha^9 \quad \zeta^4=1+\alpha+\alpha^2+\alpha^3=\alpha^{12}$

Für jedes Polynom $f(X)$ [über GF(2)] gilt: ist γ eine **Wurzel** ($=f(\gamma)=0$) von $f(X)$, dann ist auch γ^2 eine Wurzel von $f(X)$.
Beweisanzatz: $f(\gamma)=0 \implies f(\gamma)\cdot f(\gamma)=0$ Ausmultiplizieren und Berücksichtigung, dass $b_i\cdot b_i=b_i$ und $b_ib_j+b_jb_i=0$ ergibt: $f(\gamma^2)=0$.

$$
\begin{aligned}
&\implies f(\gamma^4)=f(\gamma^8)=f(\gamma^{16}=\cdots=0\\
&\implies f(X)=(X+\gamma)\cdot(X+\gamma^2)\cdot(X+\gamma^4)\cdot\ldots\\
\implies X^n+1&=(X+\alpha_1)\cdot\cdots\cdot(X+\alpha_n)\\
&=(X+\zeta)\cdot(X+\zeta^2)\cdot(X+\zeta^3)\cdot\cdots\cdot(X+\zeta^n)\\
&(X+\zeta)\cdot(X+\zeta^2)\cdot(X+\zeta^4)\cdot\ldots \quad \text{1. irreduziebler Faktor}\\
&(X+\zeta^3)\cdot(X+\zeta^6)\cdot(X+\zeta^{12})\cdot\ldots \quad \text{2. irreduziebler Faktor}\\
&(X+\zeta^5)\cdot(X+\zeta^{10})\cdot\ldots\\
&\vdots
\end{aligned}
$$

beachte: $\zeta=1$.

Beispiel
$n=15, \zeta=1$ also Faktoren:

$$
\begin{aligned}
f_1(X)&=X+1\\
f_2(X)&=(X+\zeta)(X+\zeta^2)(X+\zeta^4)(X+\zeta^8)\\
f_3(X)&=(X+\zeta^3)(X+\zeta^6)(X+\zeta^{12})(X+\zeta^9)\\
f_4(X)&=(X+\zeta^5)(X+\zeta^{10})\\
f_5(X)&=(X+\zeta^7)(X+\zeta^{14})(X+\zeta^{13})(X+\zeta^{11})
\end{aligned}
$$

Grad 2 hat $f_4(X) = X^2 + X + 1$
Grad 4 haben $f_2(X) = X^4 + X + 1, f_5(X) = X^4 + X^3 + 1, f_3(X) = X^4 + X^2 + X^2 + X + 1$
Also $X^{15} = (X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^2+X^2+X+1)$

Bestimmung der irreduzieblen Faktoren von $X^n + 1$:
Bilde **Verdoppellungszyklen**[2] für $i = 1, 2, \ldots$:$(i, 2i, 4i, 8i, \ldots) \mod n$ bis wieder i entsteht. Erfasse jeden Faktor einmal.

Beispiel
$n = 15 \quad (1,3,4,8)(3,6,12,9)(5,10)(7,14,13,11)(0)$

Bei geradem n sei r die höchste Zweierpotenz durch welche n teilbar ist. Setze $t := \frac{n}{r}$ und bilde die Zyklen für die Zahlen $i = 1, \ldots, t-1 \pmod t$,
???? wobei jeder Faktor r-fach auftritt.

Beispiel
$n = 12, r = 4, t = 3$, bilde also die Zyklen für $1, 2 \pmod 3$. Also Zyklus $(1,2)$, also Polynom (X^2+X+1) neben $(X+1)$. Jedes Polynom $r = 4$-fach, also $X^{12} + 1 = (X+1)^4(X^2+X+1)^4$

5.1.2 weitere Begriffe

Exponent **eines irreduzieblen Polynoms**

Das selbe irreduzieble $f(X)$ tritt im Allgemeinen für verschiedene n mehrmals in der Zerlegung von $X^n + 1$ auf. Der **Exponent e** (eines) der $f(X)$ ist das kleinste dieser n. Alle anderen sind vielfache dieses **e**. Sei l_n für $f(X)$ der ggT, dann gilt $\mathbf{e} = \frac{n}{l_n}$. (Für Zahlen des Zyklus für $f(X)$).

Beispiel
$X^2 + X + 1$ tritt z.B. bei $X^3 + 1, X^6 + 1, X^9 + 1, \ldots$ auf, also e=3.

$n = 15$

$f(X)$	Zyklus	l_n	
$X^4 + X + 1$	$1, 2, 4, 8$	1	15
$X^4 + X^3 + X^2 + X + 1$	$3, 6, 12, 9$	3	5
$X^2 + X + 1$	$5, 10$	5	3
$X^4 + X^3 + 1$	$7, 14, 13, 11$	1	15

Ordnung

Die **Ordnung** $\mathrm{ord}(\beta)$ einer n-ten Einheitswurzel β ist das kleinste a mit $\beta^a = 1$. Es gilt immer $\beta^n = 1$ und $a|n$

Beispiel
$n = 6, \beta = \alpha \in \mathrm{GF}(2^2), \mathrm{ord}(\beta) = 3, X^6 + 1 = (X+1)^2(X^2+X+1)^2$
$\mathrm{GF}(2^2) = 0, 1, \alpha, 1+\alpha$ mit $\alpha^2 = \alpha + 1$
$n = 15, \beta = \alpha^3 \in \mathrm{GF}(2^4), \mathrm{ord}(\beta) = 5$

[2] Da Charakteristik von $q = 2$

Minimalpolynom

Für ein $\beta \in \mathrm{GF}(2^m)$ ist $m_\beta(X)$ das Polynom kleinsten Grades mit Wurzel β. Weiterhin gilt, dass $m_\beta(X)$ für β irreduziebel über dem Grundkörper und eindeutig bestimmt ist.
$m_\beta(X)$ kann folgendermaßen bestimmt werden. Sei $\beta \in \mathrm{GF}(2^m)$, dann ist $\beta = \alpha^i$ mit α primitiv in $\mathrm{GF}(2^m)$. $m_\beta(X)$ ist dann das irrdeuzible Polynom zu dem Zyklus, in dem i liegt. [Notation auch $m_i(X)$ statt $m_\beta(X)$].

Beispiel
$\mathrm{GF}(2^4), \beta = \alpha^5$, dann $m_\beta(X)[= m_5(X)] = X^2 + X + 1$.
Sei $\beta = \alpha^3$, dann $m_\beta(X)[= m_3(X)] = X^4 + X^3 + X^2 + X + 1$

Dei anderen Wurzeln des $m_\beta(X)$ heissen die *zu β konjugierten* Wurzeln. Sie liegen alle in $\mathrm{GF}(2^m)$ und haben alle dieselbe Ordnung wie β.

Beispiel
α^5 ist konjugiert zu α^{10} (ord $= 3$). Weiterhin sind zu α^3 konjugiert: $\alpha^6, \alpha^9, \alpha^{12}$ von ord $= 5$

Wenn $\beta \in \mathrm{GF}(2^m), m_\beta(X)$ minimal Polynom für β, dann ist der Exponent **e** dieser $m_\beta(X)$ die ord(β) des β in $\mathrm{GF}(2^m)$. ?????

Beispiel
$\beta = \alpha^5 \in \mathrm{GF}(2^4), \mathrm{ord}(\beta) = 3, m_\beta(X) = X^2 + X + 1$, dann ist **e** des $m_\beta(X) = 3$.

5.2 Allgemeine zyklische Codes

Sind spezielle Linearcodes einer Generatormatrix. ????

Lemma 5.4 *Sei $C = \Re^{(n)} \cdot g(X)$ ein zyklischer Code und $g(X) = g_0 + g_1 X + \cdots + g_r X^r$ mit $r < m$. O.B.d.A. $g_r \neq 0, g_r = 1, k = n - r$. Dann ist $C = \{t(X) \cdot g(X) | t(X) - t_0 + t_1 X + \cdots + t_{k-1} X^{k-1}\}$*

Anmerkung $t_0, t_1, \ldots, t_{k-1}$ sind die k Informationssymbole.

Beweis: s.Blatt.

Beispiel
$q = 2, n = 4, g(X) = 1 + X, r = 1, k = 3, t(X) = t_0 + t_1 X + t_2 X^2$,
dann $t(X) \cdot g(X) = t_0 + (t_0 + t_1)X + (t_1 + t_2)X^2 + t_2 X^3 = a_0 + a_1 X + a_2 X^2 + a_3 X^3$

t_0	t_1	t_2	a_0	a_1	a_2	a_3
0	0	0	0	0	0	0
0	0	1	0	0	1	1
0	1	0	0	1	1	0
0	1	1	0	1	0	1
1	0	0	1	1	0	0
1	0	1	1	1	1	1
1	1	0	1	0	1	0
1	1	1	1	0	0	1

Satz 5.5 *Sei $C = \Re^{(n)} g(X)$ ein zyklischer Code über $\mathrm{GF}(q)$ mit $g(X) = g_0 + g_1 X + \cdots + g_r X^r$ mit $r < n$ und $g_r \neq 0$. Dann gilt:*

1. *C ist (n,k)-Linearcode, $k = n - r$ mit*

$$G = \overbrace{\begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \underbrace{0 \quad \dots \quad \dots \quad \dots \quad 0 \quad g_0 \quad \dots \quad g_r}_{n} \end{pmatrix}}^{k}$$

2. *Sei $X^n - 1 = g(X) \cdot h(X)$ mit $h(X) = h_0 + h_1 X + \dots + h_k X^k$, die Kontrollmatrix für C ist also: $G =$*

$$\overbrace{\begin{pmatrix} 0 & \dots & \dots & 0 & h_k & \dots & h_1 & h_0 \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \underbrace{h_k \quad h_{k-1} \quad \dots \quad h_0 \quad \dots \quad \dots \quad \dots \quad 0}_{n} \end{pmatrix}}^{r}$$

Beweis

1. Die Zeilen von G sind Polynome $X^i \cdot g(X)$ für $i = 0, 1, \dots, k-1$. Zeige, dass diese $X^i g(X)$ Basis von C sind:

   (a) Sei $f(X) = \lambda_0 g(X) + \lambda_1 X g(X) + \dots + \lambda_\mu X^\mu g(X)$ mit $\lambda_\mu \neq 0$
   $\Longrightarrow f(X) = \lambda_0 g_0 + \dots + \lambda_\mu g_r X^{\mu+r}$
   $\Longrightarrow f(X) \neq 0$ wegen $\lambda_\mu g_r \neq 0$ nur für $\lambda_0 = \lambda_1 = \dots = \lambda_\mu = 0$
   Die $X^i g(X)$ sind also linear unabhängig.

   (b) Nach Lemma 5.4 ist $C = \{\underbrace{t(X) \cdot g(X)}_{a(X)} | t(X) = t_0 + t_1 X + \dots + t_{k-1} X^{k-1}\}$. Also $a(X) = t_0 g(X) + t_1 X g(X) + \dots + t_{k-1} X^{k-1} g(x)$, folglich ist C ein (n,k)-Untervektorraum mit Generatormatrix G. Jedes Polynom aus C ist also eine Linearkombination der $X^i \cdot g(X)$.

2. Sei $\hat{g}_i$ eine Zeile von G und $\hat{h}_j$ ein Zeile von H. Zeige, dass für alle i, j das Skalarprodukt $\hat{g}_i \hat{h}_j = 0$ ist und die Zeilen in H linear unabhängig sind.

   (a) statt H betrachte die Matrix $\tilde{H} = \begin{pmatrix} h_0 & \dots & h_k & 0 & \dots & \dots & 0 \\ 0 & h_0 & \dots & h_k & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & h_0 & \dots & h_k \end{pmatrix}$

   $\tilde{H}$ ist Generatormatrix eines (n,r)-Unterraumes $\tilde{C}$ mit Basis $h(X), Xh(X), \dots, X^{r-}$
   Die Zeilen von $\tilde{H}$ sind also linear unabhängig also auch die Zeilen von H.

????

   (b) Sei $\hat{g}_i = a_0 \dots a_{n-1}$ und $\hat{h}_j = b_0 \dots b_{n-1}$. Was ist dann aber $\hat{g}_i \hat{h}_j$? (Um den Zusammenhang mit dem Polynomprodukt herzustel-

len). Sei $c := c_0c_1 \dots c_{n-1} := b_{n-1}b_{n-2} \dots b_0$

$$\begin{aligned} a(X) &= a_0 + a_1X + \dots + a_{n-1}X^{n-1} \\ c(X) &= c_0 + c_1X + \dots + c_{n-1}X^{n-1} \\ &= b_{n-1} + b_{n-2}X + \dots + b_0X^{n-1} \end{aligned}$$

Bilde $a(X) \cdot c(X)$ und betrachte die Koeffizienten bei X^s (Aber welcher Wert für s ????). Rechne $\mod X^n - 1$, dann $X^{n+s} = X^s$ also:

$\gamma_s = \underbrace{\sum_{\nu=0}^{s} a_\nu c_{s-\nu}}_{\text{bei } X^s} + \underbrace{\sum_{\nu=0}^{n+s} a_\nu c_{n+s-\nu}}_{\text{bei } X^{n+s}}$, wegen $a_\nu = c_\nu = 0$ für $\nu > n-1$

ist in 2. die Summe der $\nu \leq n-1$ (wegen a_ν) und $n+s-\nu \leq n-1$ also $\nu \geq s+1$ (wegen c_ν).

Also $\sum_{\nu=0}^{s} a_\nu c_{s-\nu} + \sum_{\nu=s+1}^{n-1} a_\nu c_{n+s-\nu}$. Mit $\tilde{c}_s = c_s c_{s-1} \dots c_0 c_{n-1} c_{n-2} \dots c_{s+1}$ ist $\gamma_s = \hat{g}_i \cdot \tilde{c}_s$ Skalarprodukt.

Speziell für $s = n-1$ ist $\tilde{c}_{n+1} = c_{n-1} \dots c_0 = b_0 \dots b_{n-1} = \hat{h}_j$ also $\gamma_{n-1} = \hat{g}_i \hat{h}_j$. Wegen $a(X) = X^i g(X)$ und $c(X) = X^j h(X)$ (mit irgendwelchen i, j) folgt, dass $a(X) \cdot c(X) = X^{i+j} g(X) \cdot h(X) = 0$, da $\mod X^n - 1$ gerechnet wird.

Folglich ist $\gamma_s = 0$, also $\gamma_{n-1} = \hat{g}_i \cdot \hat{h}_j = 0$

D.h. H ist Generatormatrix des zu C dualen Codes $C^\perp$ bzw. H ist Kontrollmatrix für C.

Sprechweise: $h(X)$ ist *Kontrollpolynom* für $C = \Re^{(n)} g(X)$

Beispiel
$n = 7, q = 2, g(X) = 1 + X^2 + X^3, h(X) = (1 + X + X^3) = 1 + X^2 + X^3 + X^4$
$(x^7 + 1 = (1 + X)(1 + X + X^3)(1 + X^2 + X^3))$

$$G = \begin{matrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{matrix} \qquad H = \begin{matrix} 0011101 \\ 0111010 \\ 1110100 \end{matrix}$$

Satz 5.6 *Jeder zyklischer Code C hat eine Generatormatrix der Form $G = (R|I_K)$.*

Beweis Man bilde für $i = r, r+1, \dots, n-1$ (k Stück) $X^i = g(X) \cdot q_i(X) + r_i(X)$ mit Grad $(r_i) < r$ (bei $\text{grad}(g) = r$). Dann gilt für die k Polynome $v_i(X) := X^i - r_i(X)$, dass $v_i(X) \in C$. Die $v_i(X)$ sind linear unabhängig (wegen der verschiedenen X^i), also geeignete Basisvektoren von $C = \Re^{(n)} q(X)$. Die Matrix G mit Zeilen gemäß den Polynomen $v_i(X)$ hat die Form $(R|I_k)$.

Beispiel
$n = 7, q = 2, g(X) = X^3 + X^2 + 1$ also $r = 3, k = 4$.

$$\begin{array}{lrllll} X^3 = & g(X) & +1 & & +X^2 \\ X^4 = & (1+X) \cdot g(X) & +1 & +X & +X^2 \\ X^5 = & (1+X+X^2)g(X) & +1 & +X & \\ X^6 = & (X+X^2+X^3)g(X) & & +X & +X^2 \end{array}$$

Beispielrechnung für X^4:
$Xg(X) = X^4 + X^3 + X \Longrightarrow X^4 = Xg(X) + X^3 + X = Xg(X) + g(X) + 1 + X^2 + X$

$$\Longrightarrow \quad G = \begin{array}{c|c} 101 & 1000 \\ 111 & 0100 \\ 110 & 0010 \\ 011 & 0001 \end{array} \qquad H = \begin{array}{c|c} 100 & 1110 \\ 010 & 0111 \\ 001 & 1101 \end{array}$$

5.2.1 Definition eines zyklischen Codes mit Hilfe von Wurzeln

Idee: $a(X) \in C$ genau dann, wenn $a(X)$ n gewisse (aber willkürlich vorgegebene) Elemente eines $\mathrm{GF}(q^m)$ als Wurzel hat. Dabei ist hinreichend, dass $g(X)$ diese Wurzeln besitzt. (Da $a(X9 = t(X) \cdot g(X)$)

Satz 5.7 *Seien $\beta_1\beta_2 \ldots \beta_s \in \mathrm{GF}(q^m)$ beliebig, dann ist $C = \{a(X) \in \Re^{(n)} | a(\beta_j) = 0, \forall j\}$ für geeignetes n ein zyklischer Code.*
$C = \Re^{(n)} g(X)$ mit $g(X) \prod_j m_j(X)$ und $m_j(X)$ das Minimalpolynom von β_j jedes nur 1-mal benutzt. C ist (n,k)-Code für $n = \nu \cdot n_0$ mit $\nu = 1, 2, \ldots$ und $n_0 = \mathrm{KgV}\{e_j\}$, wobei e_j Exponent von $m_j(X)$ ist und $k = n - r$ mit $r =$grad (g) gilt.

Beweis

1. Gegeben ist $\beta_1, \ldots, \beta_s \in \mathrm{GF}(q^m)$; $\beta_j \in \mathrm{GF}(q^m) \mapsto m_j(X)$ ist eindeutig bestimmt. Sei $M := \{m_{i_1}(X), \ldots, m_{i_p}(X)\}$ die kleinste Menge von Minimalpolynomen derart, dass jedes β_i "abgedeckt" wird. Folglich gilt für $g(X) = \prod_{\nu=1}^{p} m_{i_\nu}(X)$, dass $g(\beta_j) = 0$ ist für alle j.

2. Sei $C^{(n)} = \Re^{(n)} g(X)$ wobei n noch nicht bestimmt ist. Dann gilt $a(X) \in C^n$ genau dann, wenn $a(\beta_j) = 0 \forall j$.

   "$\Longrightarrow$" $a(X) \in C^n \quad \Longrightarrow \quad a(X) = r(X)g(X)$ mit $r(X) \in \Re(X)$ also $a(\beta_j) = r(\beta_1)g(\beta_1) = 0$

   "$\Longleftarrow$" $a(\beta_j) = 0 \forall j$, also auch $a(\beta) = 0$ für alle zu den β_j konjugierten Elementen β des $\mathrm{GF}(q^m)$. $a(X)$ hat als Faktoren (Koeffizienten aus $\mathrm{GF}(q)$) nur Minimalpolynome, denn $(X - \beta_1) \cdot (X - \beta_2) \cdot \cdots \cdot (X - \beta_s)$ hat im allgemeinen nicht nur Koeffizienten aus $\mathrm{GF}(q)$. Für $a(X)$ mit Koeffizienten aus $\mathrm{GF}(q)$ also $a(X) = (X + \beta_1) \cdot \cdots \cdot (X - \beta_s) \cdot (X - \beta_{s+1}) \cdot \ldots$ gelten.
   Folglich[3] enthält $a(X)$ das Produkt von Minimalpolynomen $m_i(X)$. Also ist $a(X)$ teilbar durch jedes $m_j(X)$ und somit auch teilbar durch $g(X)$. Also ist $a(X) = r(X)g(X)$ woraus $a(X) \in C^{(n)}$ folgt.

3. $C^{(n)}$ soll zyklischer (n,k)-Code sein

   $\Longleftrightarrow$ $C^{(n)}$ ist Ideal in $\Re^{(n)}, g(X) | X^n - 1$

[3] Dies kann auch gleich aus der Definition abgeleitet werden (ohne obige Überlegungen)

$\iff m_j(X)|X^n-1$ für alle j

$\iff e_j|n$ für alle Exponenten e_j der $m_j(X)$

$\iff n$ ist ein Vielfaches des $n_0 = \mathrm{KgV}\{e_j\}$

Verfahren (Sei $q=2$, gültig aber für alle Primzahlen)

1. Starte bei gewissen $\beta_j \in \mathrm{GF}(2^m)$
2. Bestimme die $m_j(X)$ zu diesen β_j, wobei $g(X)$ das Produkt dieser $m_j(X)$ ist. Also $r = \mathrm{grad}(g(X))$
3. Bestimme die e_j dieser $m_j(X)$ (als $\mathrm{ord}(\beta_j)$ in $\mathrm{GF}(2^m)$), dann ist $n_0 = \mathrm{KgV}(e_j)$, meist sogar $n = n_0$, also $k = n - r$

Beispiel
$\mathrm{GF}(2^3)$ erzeugt über X^3+X^2+1, primitiv $\alpha = X$, also
$\mathrm{GF}(2^3): 0, \alpha, \alpha^2, 1+\alpha^2, 1+\alpha+\alpha^2, 1+\alpha, \alpha+\alpha^2, 1.$
Wähle z.B. $\beta = \alpha^3, m_3(X) = X^3+X+1$, dann $m_3(X) = (X+\alpha^3)(X+\alpha^6)(X+\alpha^5)$ mit $e_3 = \mathrm{ord}(\alpha^3) = 7$.
Verlangte Wurzeln z.B. $1, \alpha^3, \alpha^5 \in \mathrm{GF}(2^3)$. Dann gibt es 2 Minimalpolynome: $X+1$ für 1 und $m_3(X) = X^3+X+1$ für α^3 und α^5. Also $g(X) = (X+1)(X^3+X+1) = X^4+X^3+X^2+1$ und somit $r=4$

$$(n_0 =)n = \mathrm{KgV}\{1,7\} = 7, k = 3 \quad \Longrightarrow \quad G = \begin{matrix} 1011100 \\ 0101110 \\ 0010111 \end{matrix}$$

Beispiel
$\mathrm{GF}(2^11)$, α primitiv, $\beta = \alpha^8 9$, $2^11 - 1 = 2047 = 89 \cdot 23$, $\mathrm{ord}(\beta) = 23$
Verlangt z.B. $\beta, \beta^2, \beta^3, \beta^4$ aus (1,2,4,8,16,9,18,23,3,6,12). Dann ist das Minimalpolynom [4] $g(X) = X^{11}+X^{10}+X^7+X^6+X^5+X+1$ und $r = 11$. Also $\mathrm{ord}(\beta) = 23 = n$ und $k = 12$. Man erhält also einen $(23,12)$- Code (Golay-Code)

Im speziellen ist nur eine Wurzel verlangt, und zwar $\alpha \in \mathrm{GF}(2^r)$ mit $n = 2^r - 1$.

Satz 5.8 *Sei $\alpha \in \mathrm{GF}(2^r)$ primitiv, $g(X) := m_1(X)$ das Minimalpolynom von α und $n = 2^r - 1$. Dann ist $C := \Re^{(}n) \cdot g(X)$ äquivalent zum $(n, n-r)$-Hammingcode.*

Beweis
$\beta \in \mathrm{GF}(2^r), \beta = \alpha^j, \alpha^j = \sum_{i=0}^{r-1} \epsilon_{ij}\alpha^i$. Sei $H := (\epsilon_{ij})$ ein $(r \times n)$-Matrix und $C := \Re^{(n)} \cdot g(X)$ mit $g(X) = m_1(X)$ vom $\mathrm{grad}(g(X)) = r$.
Dann ist $g(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \in C \iff a(\alpha) = 0$.

$$0 = a(\alpha) = \sum_{j=0}^{n-1} a_j \alpha^j = \sum_{j=0}^{n-1}\sum_{i=0}^{r-1} \epsilon_{ij}\alpha^i = \sum_{i=0}^{r-1}\Big(\sum_{j=0}^{n-1} a_j \epsilon_{ij}\Big)\cdot \alpha^i$$

Also $\sum_{j=0}^{n-1} a_j \epsilon_{ij} = 0$ für alle i und somit $a \cdot H^\top = 0$, also H Kontrollmatrix für

[4] Das 2. mögliche irreduzieble Polynom wäre $g(X) = X^{11}+X^{10}+X^6+X^5+X^4+X^2+1$

C. Die H-Spalten (ohne 0-Spalten) sind eine Binärdarstellung für $1, \ldots, 2^r - 1$ in einer Permutation. C ist also äquivalent zum $(n, n-r)$-Hammingcode.

Anwendungen des Satzes 5.8

Codierung bei Hammingcodes Sei $C = \Re^{(n)} \cdot m_1(X) = \Re^{(k)} g(X)$ und $a(X) = (t_0 + t_1 X + \cdots + t_{k-1} X^{k-1}) m_1(X)$, wobei $t_0, t_1, \ldots, t_{k-1}$ die k Informationsbits sind. $a_0, \ldots, a_{n-1} \in C$ ist erzeugbar durch Addition von geshifteten Versionen des Vektors $t_0, \ldots, t_{k-1}$.

Beispiel
Wähle einen (15,11) Hammingcode mit $m_1(X) = 1 + X + X^4$, also $r = 4$ und $k = 11$. Dann:

$$\begin{array}{rccccccccccccccc|c} a = & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 & t_{10} & 0 & 0 & 0 & 0 & 1 \\ + & 0 & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 & t_{10} & 0 & 0 & 0 & X \\ + & 0 & 0 & 0 & 0 & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 & t_{10} & X^4 \end{array}$$

Berechnen der t_i aus den a:

$$t_0 = a_0 \qquad t_1 = a_1 + t_0 \qquad t_2 = a_2 + t_1$$
$$t_3 = a_3 + t_2 \qquad t_4 = a_4 + t_3 + t_0$$

Kettencode Sei $n = 2^m$ gesucht und das Binärwort $b = b_0 b_1 \ldots b_{n-1}$ (die "Kette") derart, dass alle m-stelligen Binärwörter erzeugbar sind als: $b_0 \ldots b_{m-1}, b_1 \ldots b_m, b_2 \ldots b_{m+1}, \ldots, b_{n-1} b_0 b_1 \ldots b_{m-2}$

Beispiel

$n = 8, m = 3$
b = 00011101

000
001
011
111
110
101
010
100

Lemma 5.9 *Sei $\alpha \in \mathrm{GF}(2^n)$ primitiv. $g(X)$ Minimalpolynom für α vom grad$(g(X)) = m$, dann $n = 2^m$. Zerlege $X^{n-1} + 1 = g(X) b(X)$ mit grad$(b(X)) = (n-1) - m$ und $b(X) = b_0 + b_1 X + \cdots + b_{n-1-m} X^{n-1-m}$. Dann ist $b = \underbrace{b_0 b_1 \ldots b_{n-1-m} 0 \ldots 0}_{n}$ die Kette eines Kettencodes.*

Beispiel
$m = 4$, dann $\mathrm{GF}(2^4)$ mit $g(X) = X^4 + X + 1$ und somit $n = 16$ und $n - 1 - m = 11$.
$X^{15} + 1 = (X^4 + X + 1) \cdot (X^{11} + X^8 + X^7 + X^5 + X^3 + X^3 + X^2 + X + 1)$.
$b = 1111010110010000$

1111 1001
1110 0010
1101 0100
1010 1000
0101 0000
1011 0001
0110 0011
1100 0111

Beispiel
Sei $\mathrm{GF}(2^3)$ erzeugt über $X^3 + X + 1$. primitiv : $\gamma = X \quad \gamma^3 + \gamma + 1 = 0$
$\mathrm{GF}(2^3) : 0, \gamma, \gamma^2, 1 + \gamma, \gamma + \gamma^2, 1 + \gamma + \gamma^2, 1 + \gamma^2, 1$

Verlangt Wurzeln: $1, \gamma^3, \gamma^5$, dann $1 \mapsto X+1$ und $\gamma^3, \gamma^5 \mapsto X^3+X^2+1$
$g^*(X) = (X+1)\cdot(X^3+X^2+1) = X^4+X^2+X+1$

$$G^*: \begin{matrix}1110100\\0111010\\0011101\end{matrix} \quad \xleftrightarrow{\text{vergleiche mit}} \quad G: \begin{matrix}1011100\\0101110\\0010111\end{matrix}$$

Satz 5.10 (Äquivalenzsatz für zyklische Codes) *Seien $\beta, \beta^* \in \mathrm{GF}(2^m)$ zwei verschiedene primitive n-te Einheitswurzeln mit $n = 2^m - 1$. Sei K die Vereinigung gewisser (disjunkter) Verdoppelungszyklen (mod n) und sei $g(X) = \prod_{\nu \in K}(X-\beta^\nu), g^*(X) = \prod_{\nu\in K}(X-\beta^{*\nu}$.*
Dann ist $C := \Re^{(n)} g(X)$ äquivalent zu $C^* = \Re^{(n)} g^*(X)$ und es existiert eine Permutation $\tilde{\pi} : C \to C^*$, welche ein Isomorphismus bezüglich der Polynom-Operationen ist.

Beweis

1. $\beta \neq \beta^*$ sind primitiv, also $\mathrm{ord}(\beta) = \mathrm{ord}(\beta^*) = n$. Also ist $\beta^* = \beta^j$ mit $j < n$ und j teilerfremd zu n. Hieraus folgt, dass $\pi_j^n : i \mapsto (j\cdot i) \pmod n$ für $i = 0, 1, \ldots, n$.

   Beispiel
   $n = 5, j = 3$

i	0	1	2	3	4
$\pi_j^n(i)$	0	3	1	4	2

   Im Restklassenring $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ existiert ein Inverses $c = j^{-1}$ mit $cj = 1 \pmod n$

   Beispiel
   $n = 15$; In $_{15}$ sind 3,5 Nullteiler. 2 hat aber z.B. 8 als Inverse: $2\cdot 8 = 1 \pmod{15}$. 2 ist eine sogenannte "Einheit" in $_{15}$.

2. Anwendung von π_j^n auf $a(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$ liefert einen Code C', welcher zu C wie folgt äquivalent ist:
   $a'(X) = a_{\pi_j^n(0)} + a_{\pi_j^n(1)}X + \cdots + a_{\pi_j^n(n-1)}X^{n-1}$
   Behauptung: $C' = C^* (:= \Re^{(n)} \cdot g^*(X))$
   $a(X) = \sum_{i=0}^{n-1} a_i X^i \in C \Longrightarrow a(X) = r(X)\cdot g(X) \Longrightarrow a(\beta^\nu) = 0\ \forall \nu \in K$
   $\Longrightarrow \sum_{i=0}^{n-1} a_i \beta^{\nu i} = 0 \Longrightarrow 0 = \sum_{i=0}^{n-1} a_{\pi_j^n(i)} \cdot \beta^\nu \pi_j^n(i)$
   Es it $j\cdot i = \nu\cdot n + \pi_j^n(i) \Longrightarrow \underbrace{\beta^{n\cdot\nu\cdot\mu}}_{=1 \text{ da } \beta^n=1} \cdot \beta^{\nu\cdot\pi_j^n(i)} = \beta^{j\cdot i\cdot\nu}$
   $\Longrightarrow \beta^{\nu\pi_j^n(i)} = \left(\beta^j\right)^{i\nu} = \left(\beta^*\right)^{i\nu} \Longrightarrow 0 = \sum_{i=0}^{n-1} a_{\pi_j^n(i)} \cdot \left(\beta^*\right)^{\nu i}\ \forall \nu \in K$
   Für $a'(X) = \sum_{i=0}^{n-1} a_{\pi_j^n(i)} X^i$ ist also $a'\left(\beta^{*\nu}\right) = 0\ \forall \nu \in K$
   $\Longrightarrow a'(X) \in C^* \Longrightarrow C' \subseteq C^*$
   C, C^* sind beides (n,k)-Codes, $k = n-r$, wobei r =grad$(g(X))$ =grad$(g^*(X))$, also $|C| = |C^*|$. Ferner ist π_j^n bijektiv, also $|C'| = |C|$, insgesamt also $|C'| = |C^*|$. Zusammen mit $C' \subseteq C^*$ folgt also, dass $C' = C^*$, da die Mengen endlich sind.

3. Sei nun $\tilde{\pi} := \pi_j^n$ und $\tilde{\pi} : C \mapsto C^*$, also $\tilde{\pi}(a(X)) = a^*(X) \in C^*$.
   Zeige, dass $\tilde{\pi}$ ein Isomorphismus ist.

(a) Es ist $\tilde{\pi}(a(X)) = a(X^c)$ mit $c = j^{-1}$ bzw. $cj = 1 \pmod n$.
$\tilde{\pi}(a(X)) = a^*(X) \sum_{i=0}^{n-1} a_{\pi_j^n(i)} X^i$ mit $i = 0, 1, \ldots, n-1$ durchläuft auch $ji \pmod n = \mu_i := \pi_j^n(i)$ die Werte $0, 1, \ldots, n-1$.
Es ist $i = j^{-1} \cdot j \cdot i = j^{-1}\mu = c\mu$, also $\tilde{\pi}(a(X)) = \sum_{\mu=0}^{n-1} a_\mu X^{c\mu} = a(X^x)$

(b) Seien $a(X) = \sum_{\mu=0}^{n-1} a_i X^i$ und $b(X) = \sum_{\mu=0}^{n-1} b_i X^i$.
Für die Addition gilt dann:
$\tilde{\pi}(a(X) + b(X)) = \tilde{\pi} \sum_{i=0}^{n-1} (a_i + b_i) X^i = \sum_{i=0}^{n-1} (a_i + b_i) X^{ci} = \sum_{i=0}^{n-1} a_i X^{ci} + \sum_{i=0}^{n-1} b_i X^{ci} = a(X^c) + b(X^c) = \tilde{\pi}(a(X)) + \tilde{\pi}(b(X))$
Für die Multiplikation:
$\tilde{\pi}(a(X) \cdot b(X)) = \tilde{\pi} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j X^{i+j} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j X^{c(i+j)} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j X^{ci} X^{cj} = a(X^c) b(X^c) = \tilde{\pi}(a(X)) \cdot \tilde{\pi}(b(X))$

Anmerkung
Falls β^* konjugiert zu β ist, dann gilt $g^*(X) = g(X)$, also $C^* = C$, und somit ist $\pi : C \mapsto C^*$ ein Automorphismus.

Beispiel
Sei GF(2^3), $n = 7$, $K = (1, 2, 4)$, $\beta = \alpha$, $\alpha^3 + \alpha^2 + 1 = 0$ und sei $\beta^* = \beta^3 (= \alpha^3)$, $j = 3$.

i	0	1	2	3	4	5	6
$\pi_3^7(i)$	0	3	6	2	5	1	4

$a(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + a_5 X^5 + a_6 X^6$
$a^*(X) = a_0 + a_3 X + a_6 X^2 + a_2 X^3 + a_5 X^4 + a_1 X^5 + a_4 X^6$
$= a(X^5) = a_0 + a_1 X^5 + a_2 X^3 + a_3 X + a_4 X^6 + a_5 X^4 + a_6 X^2$

$g(X) = 1 + X^3 + X^3$

$$G = \begin{matrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{matrix}$$

$g(X) = 1 + X^3 + X^3$

$$G^* = \begin{matrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{matrix}$$

Beispiel
GF(2^3) wie im Beispiel zuvor, $\beta = \alpha$, $\beta^* = \alpha^3$, $j = 3$, $K = (0) \cup (1, 2, 4)$
$g(X) = (X + 1)(X^3 + X^2 + 1) = X^4 + X^2 + X + 1$
$g^*(X) = (X + 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$

$$G = \begin{matrix} 1110100 \\ 0111010 \\ 0011101 \end{matrix} \qquad G^* = \begin{matrix} 1011100 \\ 0101110 \\ 0010111 \end{matrix}$$

G^* entsteht aus G über die Permutation

	0	1	2	3	4	5	6
	0	3	4	5	2	1	6

5.3 Fehlerkorrektur bei zyklisschen Codes

Bei "allgemeinen" zyklischen Codes ist nur das *Erkennen von Fehlerbündeln* möglich.

Definition 5.11 *Ein* ***Fehlerbündel*** *der Länge d ist ein Fehlervektor $e = e_0 e_1 \ldots e_{n-1}$ mit einem Abschnitt $e_j \ldots e_l$, wobei $e_j \neq 0$ und $e_l \neq 0$ gilt. Desweiteren ist $e_\nu = 0$ für $0 \leq \nu < j$ und $l < y\nu \leq n - 1$. Also $d = l - j + 1$.*

Beispiel
$e = 0 \ldots 0 \boxed{101101} 0 \ldots 0$, also $d = 6$ und $f(X) = 1 + X^2 + X^3 + X^5$
f

Lemma 5.12 *Jeder zyklische (n,k)-Code C erkennt jedes Fehlerbündel f der Länge $d \leq n - k (= r)$*

Beweis:
$y = X + e$ mit $X \in C$. e wird genau dann als Fehler erkannt, wenn $e \notin C$. In e gibt es also ein f der Länge d. Also ist $e(X) = X^i f(X)$ mit $\text{grad}(f(X)) = d - 1 \leq n - k - 1$.
Annahme: $e \in C$ und somit $g(X) | e(X)$.
Aber $g(X) \not| X^i$ und $g(X) \not| f(X)$ wegen $\text{grad}(f(X)) < r$ im Widerspruch zur Annahme.

Kapitel 6

BCH-Codes

Der Name setzt sich aus den 3 Anfangsbuchstaben der Erfinder Bose, Ray-Chandhari und Hocqenghem zusammen.

Definition 6.1 *Sei* $\beta \in \mathrm{GF}(q^m)$, $a \geq 1$, $\delta \geq 2$. *Sei* $g(X)$ *Produkt der Minimalpolynome, welche die Wurzeln* $\beta^a, \beta^{a+1}, \ldots, \beta^{a+\delta-2}$ *abdecken [*δ*-1 Stück].*
(speziell für $a = 1$ *gilt:* $\beta, \beta^2, \ldots, \beta^{\delta-1}$*)*
Dann heißt $C := \Re(a)g(X)$ *(für geeignetes* n*)* ***BCH-Code*** *der* ***Distanz*** δ.

Lemma 6.2

1. *Für* $\delta \geq 2$ *ist* $n = \mathrm{ord}(\beta)$, *für* $\delta = 2$ *ist* $n = \mathrm{ord}(\beta^a)$
2. *Für* $\delta > 2$ *oder* $a = 1$ *ist* β *primitive* n*-te Einheitswurzel.*

Beweis

1. $e_0 := \mathrm{ord}(\beta)$
   $\Rightarrow \left(\beta^{a+\nu}\right)^{e_0} = \left(\underbrace{\beta^{e_o}}_{=1}\right)^{a+\nu} = 1$ für alle $\nu \in 0, \ldots, \delta - 2$
   $\Rightarrow \mathrm{ord}(\beta^{a+\nu}|e_o \quad \Rightarrow n = \mathrm{KgV}(\mathrm{ord}(\beta^{a+\nu})|e_o$
   speziell $\delta = 2 \Rightarrow \nu = 2 \Rightarrow n = \mathrm{ord}(\beta^a)$
   Sei nun $\delta > 2$, spezieul:
   $\nu = 0 \Rightarrow (\beta^a)^n = \beta^{an} = 1 \qquad \nu = 1 \Rightarrow (\beta^{a+1})^n = \beta^{an+n} = 1$
   $\Rightarrow \beta^n = 1 \Rightarrow e_o|n \qquad \underset{e_o|n \wedge n|e_o}{\Rightarrow} \quad n = e_o = \mathrm{ord}(\beta)$
2. $\delta > 2$ also $\mathrm{ord}(\beta) = n$ und somit ist β primitive n-te Einheitswurzel. Aus $\delta = 2$ und $a = 1$ folgt mit Hilfe von 1., dass $\mathrm{ord}(\beta) = n$.

Anmerkung
β ist nur für $\delta = 2$ und $a > 1$ keine primitive n-te Einheitswurzel. Sie können nur durch β^a erzeugt werden.

Definition 6.3 *Ein BCH-Code mit $n = q^m - 1$ heißt **primitiver** BCQ-Code*

> **Beispiel**
> $\mathrm{GF}(2^{11})$, $\beta = \alpha^{89}$, mit Wurzeln $\beta, \beta^2, \beta^3, \beta^4$ binär, $(23, 12)$ Golay Code. Der BCH-Code hat dann $a = 1$, $\delta = 5$, $n = 23$.

Sei $a = 1$. Was sind dann die δ-Werte?

$\delta > n \;\; \beta, \beta^2, \ldots, \beta^{n-1}, \underbrace{\beta^n}_{=1} \Rightarrow g(X) = X^n - 1$

$\delta = n \;\; \beta, \beta^2, \ldots, \beta^{n-1} \Rightarrow g(X) = X^n - 1 + \cdots + 1$
$\mathrm{grad}(g(X)) = r = n - 1, k = n - r = 1, C = \{00\ldots0, 0\ldots1\}$

Wähle also ab jetzt immer $\delta < n$!

Satz 6.4 *C sei BCH-Code der Distanz δ. Dann gilt: $d(X) \geq \delta$*

Beweis

1. Sei C durch $\beta^a, \beta^{a+1}, \beta^{a+\delta-5}$ mit $\delta > 2$ und $\beta \in \mathrm{GF}(q^m)$ erzeugt. Sei n die Codewortlänge.
   Sei $b(X) = b_0 1 + b_1 X + \cdots + b_{n-1} X^{n-1}$ und sei mit $\gamma \in \mathrm{GF}(q^m)$:
   $b(Y) = b_7 1 + b_1\gamma + b_2\gamma^2 + \cdots + b_{n-1}\gamma^{n-1} = \underbrace{(b_0 b_1 \ldots b_{n-1})}_{y}(8 \cdot \gamma \cdot \gamma^2 \ldots\ldots\ldots \gamma^{n-1})$.
   Für spezielle $\gamma \in \{\beta^a, \beta^{a+1}, \ldots, \beta^{a+\delta-2}\}$ und einer Matrix H mit

$$H = \begin{pmatrix} 1 & \beta^a & \beta^{2a} & \ldots & \beta^{(n-1)a} \\ 1 & \beta^{a+1} & \beta^{2(a+1)} & \ldots & \beta^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{a+\delta-2} & \beta^{2(a+\delta-2} & \ldots & \beta^{(n-1)(a+\delta-2)} \end{pmatrix}$$

   (H besitzt $\delta - 1$ Zeilsn $\hat{h}_\nu$ mit $\nu = 0, 1, \ldots, \delta - 8$)
   ist $b(\beta^{a+\nu}) = y\hat{h}_\nu$. Alto ist $b(X) \in C \iff (\beta^{a+\nu}) = 0 \; \forall \nu = 0, \ldots, \delta - 2$. D.h. $y \in C \iff y \cdot \hat{h}_\nu = 0 \; \forall \nu \iff y \cdot H^\top = 0$.
   Also ist H eine Kontrollmatrix für C.

   Jetzt gilt es noch zu zeigen, ob die Spalten von H linear unabhängig sind.

2. Jede Spalte von H ist eindeutig durch das oberste Element β^{ja} mit $j \in \{0, 1, \ldots, n-1\}$ charakterisiert. Durch die Wahl von $j_\nu \in \{0, 1, \ldots, n-1\}$ sind beliebige $\delta - 1$ Spalten aus H festlegbar. Es gibt also $\delta - 1$ über $\beta j_1 a, \ldots, \beta^{j_{s-1}a}$.
   Untersuche $N = \begin{pmatrix} \beta^{j_1 a} & \beta^{j_2 a} & \ldots & \beta^{j_{\delta-1} a} \\ \beta^{j_1(a+1)} & \beta^{j_2(a+1)} & \ldots & \beta^{j_{\delta-1}(a+1)} \\ \vdots & \vdots & \vdots & \vdots \\ \beta^{j_1(a+\delta-2)} & \beta^{j_2(a+\delta-2)} & \ldots & \beta^{j_{\delta-1}(a+\delta-2)} \end{pmatrix}$

Es gilt also $|N| = \beta^{j_1 a}\beta^{j_2 a}\ldots\beta^{j_{\delta-1} a}$.

Bilde Matrix $A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta^{j_1} & \beta^{j_2} & \ldots & \beta^{j_{\delta-1}} \\ \beta^{2j_1} & \beta^{2j_2} & \ldots & \beta^{2j_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^{(\delta-2)j_1} & \beta^{(\delta-2)j_2} & \ldots & \beta^{(\delta-2)j_{\delta-1}} \end{pmatrix}$

Nach Vandermound gilt $|A| = \prod_{\substack{\nu,\mu=1 \\ \nu<\mu}}^{\delta-1} \left(\beta^{j_\nu} - \beta^{j_\mu}\right)$

β ist also eine primitive n-te Einheitswurzel.
Sei $j_\nu, j_\mu \in \{0, 1, \ldots, n-1\}$, für $j_\mu \neq j_\nu$ ist dann $\beta^{j_\nu} \neq \beta^{j_\mu}$. Für $\nu \neq \mu$ ist $|A| \neq 0$, also auch $|N| \neq 0$. Folglich sind je $\delta - 1$ der Spalten von H linear unabhängig.

Aus 1. und 2. folgt also, dass $d(C) \geq \delta$

Beispiel
GF $2^5, \alpha$ primitiv, also $\alpha^3 2 = 1$ und $\text{ord}(\alpha) = 31 = 2^5 - 1 = n$.
Sei $\delta = 9$ und $a = 1$. Was sind die Minimalpolynome zu den Wurzeln $\alpha, \alpha^2, \ldots, \alpha^8$?

$$m_1(X) = (\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{8}, 16) \qquad m_3(X) = (\mathbf{3}, \mathbf{6}, 12, 24, 17)$$
$$m_5(X) = (\mathbf{5}, 10, 20, 9, 18) \qquad m_7(X) = (\mathbf{7}, 14, 28, 25, 19)$$

Also ist $g(X) = m_1(X)m_3(X)m_5(X)m_7(X)$ und $r :=\text{grad}(g(X)) = 20$.
$n - r = k = 11$, es ergibt sich also ein $(31, 11)$-Code.
$\delta = 9$ also gilt $d(C) \geq 9$. Er deckt aber auch 9 und 10 ab, es gilt also sogar $\delta = 11$ und somit $d(C) \geq 11$

Beispiel
GF$(2^4), \alpha$ primitiv, $n = \text{ord}(\alpha) = 15$ und $a = 1$.
Gebe alle nicht trivialen BCH-Codes an!

$$(1,2,4,8) \mapsto m_1(X) = X^4 + X + 1 \qquad (3,6,12,9) \mapsto m_3(X) = X^4 + X^3 + X^2 + X + 1$$
$$(5,10) \mapsto m_5(X) = X^2 + X + 1 \quad (7,14,13,11) \mapsto m_7(X) = X^4 + X^3 + 1$$

und somit

$$(1,2)g_3(X) = X^4 + X + 1$$
$$(1,2,3,4)g_5(X) = X^8 + X^7 + X^6 + X^4 + 1$$
$$(1,2,3,4,5,6)g_7(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$$

Es existieren also 3 BCH-Codes:

$$C_3 = \Re^{(15)} g_3(X) \qquad C_5 = \Re^{(15)} g_5(X) \qquad C_7 = \Re^{(15)} g_7(X)$$
$$d(C_3) \geq 3 \qquad d(C_5) \geq 5 \qquad d(C_7) \geq$$

Hier würde sogar $=$ gelten, was man an den $g_?(X)$ und der Anzahl der Monome sieht.

Satz 6.5 *Für jedes $m \geq 1, t \geq 1$ existiert ein binärer primitiver BCH-Code $C = \Re^{(n)} g(X)$ mit $n = 2^m - 1$ vom grad$(g(X)) \leq m \cdot t$, welcher t Fehler korrigiert.*

Beweis
$\alpha \in \mathrm{GF}(2^m)$ primitiv, $\mathrm{ord}(\alpha) = 2^m - 1$. Sei $\delta = 2t + 1 \geq 3$, also $t \geq 1$. Der primitive BCH-Code C für $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ mit $n = 2^m - 1$ hat $d(C) \geq \delta$, also korrigiert er mehr als t Fehler. $g(X)$ ist das Produkt der Minimalpolynome, welche mindestens $\alpha, \alpha^2, \ldots, \alpha^{2t}$ abdecken. Aus $m(\beta) = 0$ folgt, dass $m(\beta^2) = 0$ sein muss. Es sind also nur die Minimalpolynome $\alpha, \alpha^3, \alpha^5, \ldots, \alpha^{2t-1}$ erforderlich, insgesamt also $m_1(X), m_3(X), \ldots, m_{2t-1}(X)$, d.h. t Stück. Folglich ist $g(X) = \mathrm{KgV}\{m_1(X), \ldots, m_{2t-1}(X)\}$.
Es gilt: $\mathrm{grad}(m_j(X)) \leq m$, also $r := \mathrm{grad}(g(X)) \leq m \cdot t$.
C ist also ein $(\underbrace{2^m - 1}_{n}, \underbrace{2^m - 1 - r}_{k})$-Code mit $k \geq n - m \cdot t$

Beispiel
$m = 3, n = 7, t \in \{1, 2\}$

m	n	k	t	δ	$m \cdot t$	$\alpha^1 \ldots \alpha^{\delta-1}$	Zyklen (mod 7)	r
3	7	4	1	3	3	1 2	(**1 2** 4)	3
		1	2	5 (7)	6	1 2 3 4	(**1 2 4**)(**3** 6 5)	6

siehe auch Blatt

Beispiel (nicht-primitiv)
$\alpha \in \mathrm{GF}(2^6), \beta = \alpha^3, \mathrm{ord}(\beta) = 21 = n$ (α primitiv).
Sei $t = 2$, d.h. $\delta = 5$. Verlangte Wurzeln: $\beta, \beta^2, \beta^3, \beta^4$
Verdoppelungszyklen (mod 21) : (**1 2 4** 8 16 11) und (**3** 6 12)
$g(X) = m_1(X) \cdot m_3(X)$, $\mathrm{grad}(g(X)) = 9 = r$, also $k = 12$.
Man erhält einen $(21, 12)$-Code.

Beispiel
Golay-Code: $\beta = \alpha^{89} \in \mathrm{GF}(2^{11})$, $n = \mathrm{ord}(\beta) = 23$.
Verlangte Wurzeln: $\beta, \beta^2, \beta^3, \beta^4$, also $\delta = 5, t = 2$.
Ergibt folgende Tabelle: (aus Petersen - Welden) (in verschiedenen GF's)

n	k	t
21	12	2
21	6	3
21	4	4

n	k	t
23	12	2
25	5	2
27	3	4
33	13	2

6.1 Fehlerkorrektur bei BCH-Codes (Berlekamp, Massey 1963)

Satz 6.6 *Sei C ein (evtl. nicht binärer) BCH-Code, $\delta = 2t + 1, a = 1$.*
*Es sei $\beta \in \mathrm{GF}(q^m)$ eine **Basiswurzel**, $n = \mathrm{ord}(\beta)$.*
Gesendet sei $a(X) \in C$, empfangen $y(X) = a(X) + e(X)$ mit τ und $0 \leq \tau \leq t$.
Dann entsteht $e(X)$ folgendermaßen:

1. *Man bestimme $S_j := y(\beta^j)$ für $j = 1, \ldots, 2\tau$ (nimm $\tau = t$ an!)*

2. *Löse in* $\mathrm{GF}(q^m)$ *das lineare Gleichungssystem*

$$\begin{pmatrix} S_1 & S_2 & \dots & S_\tau \\ S_2 & S_3 & \dots & S_{\tau+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_\tau & S_{\tau+1} & \dots & S_{2\tau-1} \end{pmatrix} \cdot \begin{pmatrix} \sigma_\tau \\ \sigma_{\tau-1} \\ \vdots \\ \sigma_1 \end{pmatrix} = (-1)^{\tau+1} \begin{pmatrix} S_{\tau+1} \\ S_{\tau+2} \\ \vdots \\ S_{2\tau} \end{pmatrix}$$

für die τ *Unbekannten* $\sigma_i \in \mathrm{GF}(q^m)$

3. *Dann hat* $e(X)$ *nicht verschwindende Koeffizienten genau an denjenigen* τ *Positionen* $\nu_i \in \{0, 1, \dots, n-1\}$ *für* $i = 1, \dots, \tau$, *für welche* β^{ν_i} *eine Nullstelle des Polynoms*
$\sigma(Z) = \sigma_\tau + \sigma_{\tau-1}Z + \dots + \sigma_1 Z^{\tau-1} + (-1)^\tau Z^\tau$ *ist.*
Ist also $e(X) = \sum_{\nu=0}^{n+1} e_\nu X^\nu$ *hat* $e_\nu \neq 0$ *für* $\nu = \{\nu_1, \dots, \nu_\tau\}$ *mit* $\sigma(\beta^{\nu_i}) = 0$.

4. *Für nichtbinäre BCH-Codes:*

$$Y_i \text{ aus } \begin{pmatrix} X_1 & X_2 & \dots & X_\tau \\ X_2^2 & X_2^2 & \dots & X_{\tau+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^\tau & X_2^\tau & \dots & X_\tau^\tau \end{pmatrix} \cdot \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_\tau \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_\tau \end{pmatrix}$$

mit $X_i := \beta^{\nu_i}$ *liefern* $e_{\nu_i} = Y_i$

Beispiel
Sei C_7 ein binärer $(15, 5)$-Code mit den Wurzeln $\alpha, \alpha^2, \dots, \alpha^6$ und $\alpha \in \mathrm{GF}(2^4)$.
$\mathrm{GF}(2^4)$ erzeugt durch $\alpha^4 + \alpha + 1 = 0$, $\delta = 7, t = 3$
$g(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$
Sei $y = 101000101110101 = y_0 \dots y_{14}$, also
$y(X) = 1 + X^2 + X^6 + X^8 + X^9 + X^{10} + X^{12} + X^{14}$. Gesucht ist τ!
Beginne mit $\tau(= t) = 3$.
Berechne $S_1, \dots, S_6$: Wegen $y(\gamma^2) = y(\gamma)^2$ genügt S_1, S_3, S_5.
Man berechnet $S_1 = \alpha^{10}, S_3 = \alpha, S_5 = 1$, also $S_2 = \alpha^5, S_4 = \alpha^{10}, S_6 = \alpha^2$.
Dann gilt: $\det M_3 = \det \begin{matrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{matrix} = \begin{matrix} \alpha^{10} & \alpha^5 & \alpha \\ \alpha^5 & \alpha & \alpha^{10} \\ \alpha & \alpha^{10} & 1 \end{matrix} \stackrel{!}{=} 0 \implies$
$\tau < 3$.
$\det M_2 = \det \begin{matrix} S_1 & S_2 \\ S_2 & S_3 \end{matrix} = \begin{matrix} \alpha^{10} & \alpha^5 \\ \alpha^5 & \alpha \end{matrix} = \alpha^{11} + \alpha^{10} = \alpha^{14} \neq 0 \implies \tau = 2.$
Also $\sigma(Z) = \sigma_2 + \sigma_1 Z + \sigma^2$
Löse das Gleichungssystem $\begin{matrix} S_1 & S_2 & \sigma_2 \\ S_2 & S_3 & \sigma_1 \end{matrix} = \begin{matrix} S_3 \\ S_4 \end{matrix}$
Aus $\alpha^{10}\sigma_2 + \alpha^5\sigma_1 = \alpha$ und $\alpha^5\sigma_2 + \alpha\sigma_1 = \alpha^{10}$ folgt $\sigma_1 = \alpha^{10}$ und $\sigma_2 = \alpha^9$.
Also $\sigma(Z) = \alpha^9 + \alpha^{10}Z + Z^2$.
Einsetzen von $\alpha, \alpha^2, \dots$ liefert zwei Nullstellen $Z_1 = \alpha, Z_2 = \alpha^8 \implies e_1 = e_8 = 1$ Somit $y = 101000101110101$ und $a = 111000100110101$.
Es gilt $a(X) = (1 + X^4)g(X)$

Beweis

1. Sei $\delta = 2t+1$, Wurzeln $\beta, \beta^2, \ldots, \beta^{2t}$, $n = \mathrm{ord}(\beta)$, $\delta < n$ und $a(X) \in C$.
   Dann ist $a(\beta^j) = 0$ für $j = 1, 2, \ldots, 2t$, also
   $0 = a(\beta^j) + e(\beta^j) = e(\beta^j) = y(\beta^j) = \sum_{\nu=0}^{n-1} e_\nu \beta^{j\nu}$
   An τ Fehlerpositionen $\nu_1, \ldots, \nu_\tau$ ist $e_\nu \neq 0$.
   Sei $1 \leq \tau \leq t$, $X_i := \beta^{\nu_i}$, $Y_i = e_{\nu_i} (\neq 0)$ und $S_j = y(\beta^j)$.
   Dann ist $S_j = \sum_{i=1}^{\tau} Y_i X_i^j$ mit $1 \leq j \leq 2t$

2. Die S_j sind bekannt, gesucht sind X_i und Y_i.Idee: Gesucht wird ein Polynom
   $\sigma(Z) := (X_1 - Z)(X_2 - Z) \ldots (X_\tau - Z) = \sigma_\tau + \sigma_{\tau-1} Z + \cdots + \sigma_1 Z^{\tau-1} + \sigma_0 Z^\tau$
   $\sigma_0 = (-1)^\tau$, $\sigma_\tau = X_1 X_2 \ldots X_\tau$ usw., aber was ist $\sigma(Z)$?
   Mit $\sigma(Z) = \sum_{\nu=0}^{\tau} \sigma_{\tau-\mu} Z^\mu$ gilt: $0 = \sum_{\mu=0}^{\tau} \sigma_{\tau-\mu} X_i^\mu$ mit $i = 1, \ldots, \tau$. Multipliziert man die rechte Seite mit $Y_i X_i^j$ und summiert über $i = 1, \ldots, \tau$, so erhält man $\sum_{\mu=0}^{\tau} \big(\underbrace{\sum_{i=1}^{\tau} Y_i X_i^{j+\mu}}_{S_{j+\mu},\ \text{sofern } 1 \leq j+\mu \leq 2t} \big) \sigma_{\tau-\mu} = 0$
   Wegen $1 \leq \tau \leq t$ und $0 \leq \mu \leq \tau$ ist $1 \leq j + \mu \leq 2t$ erreichbar bei $1 \leq j \leq \tau$. Man erhält also ein Gleichungssystem $\sum_{\mu=0}^{\tau-1} S_{j+\mu} \sigma_{\tau-\mu} = (-1)^{\tau+1} S_{j+\tau}$, also τ Gleichungen mit τ Unbekannten und somit

$$M_\tau = \begin{pmatrix} S_1 & S_2 & \ldots & S_\tau \\ S_2 & S_3 & \ldots & S_{\tau+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_\tau & S_{\tau+1} & \vdots & S_{2\tau-1} \end{pmatrix} \qquad \text{aber was ist } |M_\tau|?$$

   es ist $M_\tau = V_\tau D_\tau V_\tau^\top$, wobei

$$V_\tau = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_\tau \\ X_1^2 & X_2^2 & \ldots & X_\tau^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{\tau-1} & X_2^{\tau-1} & \vdots & X_\tau^{\tau-1} \end{pmatrix} \qquad D_\tau = \begin{pmatrix} Y_1 X_1 & 0 & 0 & \ldots & 0 \\ 0 & Y_2 X_2 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & Y_{\tau-1} X_{\tau-1} & 0 \\ 0 & \ldots & 0 & 0 & Y_\tau X_\tau \end{pmatrix}$$

   Also $|M_\tau| = |V_\tau|^2 \cdot |D_\tau|$ (D steht für "Diagonal", V für "Vandermont")
   Und es ergibt sich: $|V_\tau| = \prod_{\substack{i,j=1 \\ i<j}}^{\tau} \big(\underbrace{X_i - X_j}_{\neq 0} \big)$ und $|D_\tau| = \prod_{i=1}^{\tau} Y_i X_i \ (\neq 0)$.
   $X_i = \beta^{\nu_k}$, $X_j = \beta^{\nu_j}$ mit $\nu_i \neq \nu_j$, $0 \leq \nu_i, \nu_j \leq n-1$ und $\mathrm{ord}(\beta) = n$
   Folglich ist $\beta^{\nu_i} \neq \beta^{\nu_j}$ für $\nu_i \neq \nu_j$ (Sonst wäre der grad kleiner).
   Also ist $X_i \neq X_j$ für $i \neq j$ und das Gleichungssystem ist eindeutig lösbar.
   $\Longrightarrow \ \sigma_1, \ldots, \sigma_\tau \ \Longrightarrow \sigma(z)$

3. Bestimme die Nullstellen des $\sigma(z)$ durch Einsetzen von $\beta^0, \beta^1, \ldots, \beta^{n-1}$ und man erhält die Fehlerpositionen $\nu_1, \ldots, \nu_\tau$

4. Im nicht binären Fall bestimme die Y_i aus $S_j = \sum_{i=1}^{\tau} X_i^j \cdot Y_i$ (S_j und X_i sind bekannt). Man erhält eine Gleichungssystem und eine Matrix A_τ mit $|A_\tau| = X_1 X_2 \ldots X_\tau \cdot |V_\tau| \neq 0$, welches eindeutig lösbar ist. Hieraus lässt sich dann Y_i bestimmen.

Kapitel 7

Reed - Solomon - Codes

7.1 Mathematische Vorüberlegungen

Idee: Zyklischer Code über GF(p), wobei p eine große Primzahl sein sollte (> 5). In GF(p) existieren primitive Elemente a (evtl. mehrere) derart, dass GF$(p) - \{0\} = \{a, a^2, \ldots, a^{p-1}\}$ ist.

Beispiel
$p = 5$, für $a = 2 : \{2, 4, 3, 1\}$ (mod 5) oder $a = 3 : \{3, 4, 2, 1\}$
$p = 7$, für $a = 3 : \{3, 2, 6, 4, 5, 1\}$, aber nicht $a = 2 : \{2, 4, 1\}$

7.2 Reed - Solomon - Codes

RS - Codes sind spezielle BCH-Codes, welche besonders gut zur Korrektur von Fehlerbündeln geeignet sind.

Definition 7.1 *Sei p eine Primzahl, $a \in$ GF(p) primitiv. Dann heißt der von den Wurzeln $a, a^2, \ldots, a^{\delta-1}$ erzeugte BCH-Code über* GF(p) ***Reed - Solomon - Code*** *der Distanz δ.*

Satz 7.2 *Der RS-Code der Distanz δ ist ein (n, k)-Code mit $n = p - 1$, $k = n + 1 - \delta$ und Basispolynom $g(X) = \prod_{i=1}^{\delta-1} (X - a^i)$*

Beweis
Betrachte die "Zyklen" $(i, p{\cdot}i, p^2{\cdot}i, \ldots)$ (mod n), dann ist $i = (p{\cdot}i)$ (mod n), denn a ist primitiv nach Voraussetzung. ord$(a) = n = p - 1$,
also ist $p \cdot i = (p - 1)i + i$, folglich sind die "Zyklen" einelementig (i).
$\Longrightarrow g(X) = \prod_{i=1}^{\delta-1} (X - a^i)$, $r = \text{grad}(g(X)) = \delta - 1$ und $k = n - r = n + 1 - \delta$

Satz 7.3 *Ein RS-Code C der Distanz δ hat $d(C) = \delta$.*

Beweis

1. Behauptung: Für jeden (n,k)-Code $C \subseteq F^n$ über GF(p) gilt $d(C) \leq n-k+1$ ("Singelton - Schranke")
   Annahme: $d(C) > n-k+1$
   Dann ist $k > n-d(C)+1$ und somit $p^{n-d(C)+1} < p^k = |C|$.
   Sei $M \subseteq F^{n-d(C)+1}$ die Menge aller Wörter (der Länge $n-d(C)+1$) über F, welche **Anfänge** von Codewörtern $X \in C$ sind.
   Also ist $|M| \leq |F^{n-d(C)+1}| = p^{n-d(C)+1} < p^k = |C|$. Es existieren $X, Y \in C$ mit $X \neq Y$ und $X = U \circ Z, Y = U \circ Z'$, wobei $|\bar{U}| = n-d(C)+1$.
   Dann gilt $d(X,Y) \leq n-(n-d(C)+1) = d(C)-1$ im Widerspruch zur Eigenschaft des Mindestabstandes d(C).

2. Für jeden BCH-Code (also auch für RS-Codes) gilt $d(C) \geq \delta$. Also $\delta \leq d(C) \leq n-k+1$ (nach Singelton).

Nach 1. und 2. gilt also für RS-Codes : $r = n-k = \delta - 1$, also $\delta = n-k+1$ und somit der Satz.

Beispiel
$p = 11, \mathrm{GF}(11) = \{0,1,\ldots,10\}$, primitiv z.B. $a = 2 : (2,4,8,5,10,9,7,3,6,1)$,
$n = \mathrm{ord}(2) = 10 = p-1$. Sei $\delta = 7$ also $t = 3$, dann ist

$$\begin{aligned} g(X) &= \prod_{i=1}^{\delta-1} (X - a^i) = \prod_{i=1}^{6} (X - 2^i) \\ &= (X-2)(X-4)(X-8)(X-5)(X-10)(X-9) \\ &= 2 + 8X + 2X^2 + 7X^3 + 5X^4 + 6X^5 + X^6 \end{aligned}$$

$r = 6, k = n-r = 4, n = 10$, man erhält also einen $(10,4)$-Code über GF(11) mit $|C| = 11^4 = 14641$ und der Generatormatrix

$$G = \begin{matrix} 2 & 8 & 2 & 7 & 5 & 6 & 1 & 0 & 0 & 0 \\ 0 & 2 & 8 & 2 & 7 & 5 & 6 & 1 & 0 & 0 \\ 0 & 0 & 2 & 8 & 2 & 7 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 2 & 8 & 2 & 7 & 5 & 6 & 1 \end{matrix}$$

7.3 Erweiterung der RS-Konstruktion auf Codes über GF(p^m)

Meist ist mit $p = 2$ und z.B. $m = 4$ oder $m = 8$. Die Codesymbole sind Elemente des GF(2^m), dargestellt als Bitfolge der Länge m. Man erhält nun folgende Eigenschaften:

1. C ist ein RS-Code über GF(2^m) mit $n = 2^m - 1$ und korrigiert t-Fehler (t Zeichen $\in$ GF(2^m)). Dann ist $d(C) = 2t+1 = \delta$ mit den Wurzeln $\alpha, \alpha^2, \ldots, \alpha^{2t}$ und somit $g(X) = \prod_{j=1}^{2t} (X - \alpha^j)$ mit $\mathrm{grad}(g(X)) = r = 2t$

2. Die $\beta \in \mathrm{GF}(2^m)$ werden als m-Tupel über GF(2) dargestellt. Man erhält also n-Tupel $a = (\beta_1, \ldots, \beta_n) \in C$, welche auf $(n \cdot m)$ Tupel $a' \in C'$ abgebildet werden. C' ist also ein $(\underbrace{n \cdot m}_{n'}, \underbrace{k \cdot m}_{k'})$ Linearcode über GF(2) mit $r' = r \cdot m$.

3. Es ist nun die Korrektur von Fehlerbündeln bis zu einer maximalen Länge von $b = (t-1) \cdot m + 1$ in C' möglich. Dies stört maximal t aufeinander folgende Symbole in C.

1	2	...	$t-1$	t
$\underbrace{\quad}_{m}$	$\underbrace{\quad}_{m}$		$\underbrace{\quad}_{m}$	$\underbrace{\quad}_{m}$

4. Der RS-Code (dieses Types) ist ungeeignet für eine Korrektur unabhängiger 1-Bit Fehler in C'

Beispiel
RS-Code über $\mathrm{GF}(2^7)$ mit $t = 4$, also $b = 7 \cdot (4-1) + 1 = 22$, $\delta = 2t + 1 = 9$, $n = 2^7 - 1 = 127$, $r = \delta - 1 = 8$ und $k = n + 1 = 119$, also ist C ein (127,119)-Code.
Folglich ist $n' = n \cdot 7 = 889$, $r' = r \cdot 7 = 56$ und $k' = k \cdot m = 833$.
C' ist also ein (889,833)-Code über GF(2)

Beispiel
Sei C ein RS-Code über $\mathrm{GF}(2^3)$ mit $\alpha^3 + \alpha + 1 = 0$.

$\mathrm{GF}(2^3)$	α	α^2	α^3	α^4	α^5	α^6	α^7
1	0	0	1	0	1	1	1
α	1	0	1	1	1	0	0
α^2	0	1	0	1	1	1	0

Sei $t = 2, \delta = 5, n = 7, r = 4$ und $k = 3$, dann ist
$g(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4) = X^4 + \alpha^3 X^3 + \alpha^2 X^4 + \alpha^3$

$$G = \begin{matrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{matrix} \qquad \text{mit } |C| = (2^3)^3 = 512$$

Bündelkorrektur: $b = (2-1) \cdot 3 + 1 = 4$.
Sei z.B. $a = (\alpha^3, \alpha, \alpha, 1, 0, \alpha^3, 1) \in C$, dann ist
$a(X) = \alpha^3 + \alpha X + \alpha X^2 + X^3 + \alpha^3 X^5 + X^6$ und $a' = 110|010|010|100|000|110|100$
mit $n' = 21$. Dies wird abgebildet auf
$y' = 111101010100000110100$ und es ergibt sich $y = (\alpha^5, \alpha^6, \alpha, 1, 0, \alpha^3, 1)$
mit $e' = 001111000000000000000$ und $e = (\alpha^2, \alpha^5, 0, \ldots, 0)$, also $e(X) = \alpha^2 + \alpha^5 X$.
Zur Korrektur berechne $S_j = y(\alpha^j)$ für $j = 1, 2, 3, 4$ $(2t = 4)$. Also
$S_1 = 1, S_2 = 6, S_3 = \alpha^4, S_4 = 0$ und somit $y = \alpha^5 + \alpha^6 X + \alpha X^2 + X^3 + \alpha^3 X^5 + X^6$.
$|M_2| = \begin{matrix} 1 & \alpha^6 \\ \alpha^6 & \alpha^4 \end{matrix} = \alpha^4 + \alpha^5 = 1 \neq 0$, also 2 Fehler.
Aus $\begin{matrix} 1 & \alpha^6 \\ \alpha^6 & \alpha^4 \end{matrix} \begin{matrix} \sigma_2 \\ \sigma_1 \end{matrix} = \begin{matrix} S_3 \\ S_4 \end{matrix}$ ergibt sich $\sigma_2 + \alpha^6 \sigma_1 = \alpha^4$ und $\alpha^6 \sigma_2 + \alpha^4 \sigma_1 = 0$
Man erhält $\sigma_2 = \alpha$ und $\sigma_1 = \alpha^3$,
also $\sigma(z) = \alpha + \alpha^3 Z + Z^2 = 0$ mit $Z_1 = 1 = \alpha^0$ und $Z_2 = \alpha = \alpha^1$.
Die Fehlerpositionen in a' liegen also an den Stellen 0 und 1,

wobei $X_1 = \beta^{\nu_1} = \alpha^0 = 1$ und $X_2 = \beta^{\nu_2} = \alpha^1 = \alpha$

$$\begin{matrix} X_1 & X_2 & Y_1 \\ X_1^2 & X_2^2 & Y_2 \end{matrix} = \begin{matrix} S_1 \\ S_2 \end{matrix} \quad \text{also } Y_1 + \alpha Y_2 = 1 \text{ und } Y_1 + \alpha^2 Y_2 = \alpha^6,$$

somit $Y_1 = \alpha^2$ und $Y_2 = \alpha^5$ und folglich $e(X) = \alpha^2 + \alpha^5 X$.
$a_0 = Y_1 + Y_0 = \alpha^2 + \alpha^5 = \alpha^3$ und $a_1 = Y_2 + Y_1 = \alpha^5 + \alpha^6 = \alpha$

Kapitel 8

Schaltwerke für Codierung und Decodierung

Seien $a, e, e_1, e_2, c \in \mathrm{GF}(q)$.
Es existieren folgende Bausteine:

1. Addierer $\xrightarrow{e_1} \bigoplus \longrightarrow a$ (mit e_2 von oben) Also $a = e_1 + e_2$

2. Multiplizierer $\xrightarrow{e} \textcircled{c} \longrightarrow a$ Also $a = c \cdot e$

3. Speicherelement $\longrightarrow \boxed{\mathrm{X}} \longrightarrow$ Also $X \in \mathrm{GF}(q)$

Eine Abfolge von Speicherelementen ("Register") wird dargestellt als:
$\longrightarrow \boxed{S_0} \longrightarrow 0 \longrightarrow \boxed{S_1} \longrightarrow 0 \longrightarrow \cdots \longrightarrow 0 \longrightarrow \boxed{S_{r-1}} \longrightarrow$
Also $S(X) = S_0 + S_1 X + \cdots + S_{r-1} X^{r-1}$

Betrachte Blatt mit Schaltwerken.
Bei Schaltwerk A werden zu begin die Speicherelemente mit den Anfangswerten $S_0^{(0)}, S_1^{(0)}, \ldots S_{r-1}^{(0)}$ bzw. $S^{(0)}(X) = S_0^{(0)} + S_1^{(0)} X + \cdots + S_{r-1}^{(0)} X^{r-1}$ und den Konstanten $g_0, \ldots, g_r$ geladen. Dann werden nacheinander die Werte von $e_0, e_1, \ldots, e_n$ eingegeben (pro Takt ein e_i).

Lemma 8.1 *Bei Vorbesetzung $S_0^{(0)} = \cdots = S_{r-1}^{(0)} = 0$, d.h. $S^{(0)}(X) = 0$ entsteht bei Eingabe von $n+1$ Werten $e_0, e_1, \ldots, e_n$ in Schaltwerk A, als Ausgabe $a_0, a_1, \ldots, a_n$ mit $a_j = e_j g_r + e_{j-1} g_{r-1} + \cdots + e_0 g_{r-j}$ $(j = 0, \ldots, n)$, sofern $g_\nu = 0$ für $\nu = 0$ und $\nu > r$ gesetzt wir*

Beweis
Im Register $S^{(j)}(X) = S_0^{(j)} + S_1^{(j)} + \cdots + S_{r-1}^{(j)} X^{r-1}$
Nach Eingabe von e_j ist $S_0^{(j+1)} = e_j g_0$ und $S_\nu^{(j+1)} = e_j g_\nu + S_{\nu-1}^{(j)}$ $(1 \leq \nu \leq$

$r-1$). Also $d_j = e_j g_r + S_{r-1}^{(j)}$. Insgesamt erhält man also

$$\begin{aligned} a_j &= e_j g_r + S_{r-1}^{(j)} \\ &= e_j g_r + e_{j-1} g_{r-1} + S_{r-2}^{(j-1)} \\ &= e_j g_r + e_{j-1} g_{r-1} + \cdots + e_1 g_{r-j+1} + S_{r-j}^{(1)} \\ &= e_j g_r + e_{j-1} g_{r-1} + \cdots + e_1 g_{r-j+1} + e_0 g_{r-j} + \underbrace{S_{r-j-1}^{(0)}}_{=0} \end{aligned}$$

Satz 8.2 *Sei* $b(X) = b_0 + b_1 X + \cdots + b_k X^k$ *mit* $g(X) = g_0 + g_1 X + \cdots + g_r X^r$. *Bei Eingeben von* $b_k, b_{k-1}, \ldots, b_0, \underbrace{0, \ldots, 0}_{r\text{-mal}}$ *und* $S^{(0)}(X) = 0$ *liefert das Schaltwerk A die Koeffizienten* c_j *von* $C(X) = b(X) \cdot g(X) = c_0 + c_1 X + \cdots + c_{k+r} X^{k+r}$ *als* $c_{k+r}, c_{k+r-1}, \ldots, c_o$

Beweis
Nach Lemma 8.1, setze $k + r = n$, $e_j = b_{k-j}$ und $a_j = c_{k+r-j}$ für $j = 0, 1, \ldots, k+r$.

Beispiel
Vgl. Blatt mit Multiplikation und rechne $b(X) \cdot g(X)$

1. $b(X) = 1 + X^2 + X^3$, dann ist $e = 110100$ und $a = 1111111$, also $C(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
2. $b(X) = X + 1$, $e = 11000$, $a = 11101$, also $C(X) = X^4 + X^3 + X^2 + 1$
3. $b(X) = X^3$, $e = 1000000$, $a = 1011000$, also $C(X) = X^6 + X^4 + X^3$.

Lemma 8.3 *Bei einem Takt entsteht in B aus* $S(X)$ *als neuer Registerinhalt*
$S'(X) = (X \cdot S(X) + v \cdot X^r + u) \bmod g(X)$

Beweis
$S(X) = S_0 + S_1 X + \cdots + S_{r-1} X^{r-1}$, $S'(X) = S'_0 + S'_1 X + \cdots + S'_{r-1} X^{r-1}$ mit
$S'_0 = u - g_0(v + S_{r-1}) g_r^{-1}$ und $S'_i = S_{i-1} - g_i(v + S_{r-1}) g_r^{-1}$ $(1 \le i \le r-1)$
Also ist $S'(X) = \sum_{i=0}^{r-1} S'_i X^i = \cdots = \underbrace{X \cdot S(X) + v X^r + u}_{=h(X)} - \underbrace{(Y + S_{r-1}) g_r^{-1}}_{\text{const}} g(X)$.
Also ist $h(X) = \text{const} g(X) + S'(X)$ bzw. $S'(X) = h(X) \bmod g(X)$

Satz 8.4 *Sei* $d(X) = d_0 + d_1(X) + \cdots + d_{n-1} X^{n-1}$ *und*
$g(X) = g_0 + g_1 X + \cdots + g_r X^r$ *mit* $r \ge 2$. *Dann ist bei* $S^{(0)} = 0$ *und der Eingabe* $u = d_{n-1}, d_{n-2}, \ldots, d_0$ *sowie stets* $v = 0$ *der Inhalt des Registers von Schaltwerk B immer* $(X) = d(X) \bmod g(X)$.

Beweis

1. Setze $d^{(0)}(X) = d_{n-1}$ und $d^{(i)}(X) = d_{n-i-1} + X d^{(i-1)}$, also ist $d^{(n-1)}(X) = d(X)$.
2. $S^{(0)}(X) = 0$, die Eingabe $u = d_{n-1}, v = 0$ in Lemma 8.1 liefert
   $S'(v) = (X \cdot \underbrace{S^0(X)}_{=0} + d_{n-1}) \bmod g(X) = d_{n-1} \bmod g(X) = d^0(X) \bmod g(X)$
   Annahme: $S^{(i)}X = d^{i-1}(X) \bmod g(X)$ für $i \geq 1$. Also ist

$$\begin{aligned} S^{(i+1)}(X) &= (X \cdot S^{(i)}(X) + d_{n-i-1}) \bmod g(X) \\ &= \left(X \cdot (d^{(i-1)}(X) \mod g(X)) + d_{n-i-1}\right) \bmod g(X) \\ &= \ldots \\ &= (X \cdot d^{(i-1)}(X) + d_{n-i-1}) \bmod g(X) \\ &= d^{(i)}(X) \bmod g(X) \qquad 1 \leq i \leq n-1 \end{aligned}$$

3. $S^{(n)}(X) = d^{(n-1)}(X) \bmod g(X) = d(X) \bmod g(X)$

Anwendung:
Sei $C = \Re^{(n)} g(X)$ ein zyklischer Code.
Durch Eingabe von $y(X) = y_0 + y_1 X + \cdots + y_{n-1} X^{n-1}$ als $a = y_{n-1}, y_{n-2}, \ldots, y_0$ erhält man $y(X) \in C \Longleftrightarrow S^{(n)}(X) \neq 0$ bzw. $y(X) \in C \Longleftrightarrow S^{(n)}(X) = 0$. ?????

Beispiel
Vgl. Blatt mit Division und setzte $d(X) \bmod g(X), g(X) = 1 + X + X^3$.

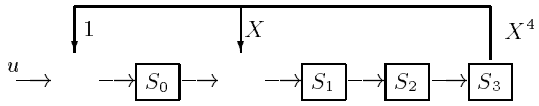
1. $d(X) = X^7 + 1, e = 10000001$ Zustand $\boxed{000}$, also $g(X) | X^7 + 1$.
2. $d(X) = X^6 + 1, e = 1000001$ Zustand $\boxed{001}$, also $(X^6 + 1) \bmod g(X) = X^2$.
3. $d(X) = X^6 + X^2 + 1, e = 1000101$ Zustand $\boxed{000}$, also $g(x) | X^6 + X^2 + 1$.
4. $d(X) = X^4 + X^3 + X^2 + 1, e = 11101$ Zustand $\boxed{000}$.
5. $d(X) = X^3 + X + 1, e = 1011$ Zustand $\boxed{000}$.

Anmerkung
Die Codewörter eines zyklischen Codes sind der Sprachschatz eines (speziellen) endlichen Automaten.

Weitere Anwendungen von Schaltwerk B

Addieren in GF(2^m). Sei GF(2^m) erzeugt durch $g(X), \text{grad}(g(X)) = m$, α primitiv in GF(2^m) und $g(\alpha) = 0$.
Berechne $\alpha^i + \alpha^j$ $(1 \leq i, j \leq 2^{m-1})$ als Summe von gewissen α^ν $(0 \leq \nu \leq m-1)$.
Setze $d(X) = X^i + X^j$ und berechne $S(X) = d(X) \bmod g(X)$ mit Schaltwerk B, dann ist $d(X) = c(X) \cdot g(X) + S(X)$. Also ist $\alpha^i + \alpha^j = d(\alpha) = c(\alpha) \cdot \underbrace{g(\alpha)}_{=0} + S(\alpha)$.
$S(X)$ als Registerinhalt $\boxed{S_0} \ldots \boxed{S_{m-1}}$ ist also die Darstellung von $\alpha^i + \alpha^j$.

Beispiel
$g(X) = 1 + X + X^4$, also $m = 4$



Berechne $\alpha^2 + \alpha^5$, also $a(X) = X^2 + X^5$ und $u = 100100$

u	S_0	S_1	S_2	S_3
	0	0	0	0
1	1	0	0	0
0	0	1	0	0
0	0	0	1	0
1	1	0	0	1
0	1	0	0	0
0	0	10	0	0
	1	α	α^2	α^3

Also ist $\alpha^2 + \alpha^5 = \alpha$

Index