

## Linearkode

### Kanalkodierung mit Matrizen

Wir betrachten das Kanalkodealphabet A (Seite 71).

Sei  $a_1 = a_1^*$  und  $a_1^* = (1101)$ . Damit ergibt sich:

$$(1 \ 1 \ 0 \ 1) \cdot \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}}^{G_{4 \times 7}} = (1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1) = a$$

Die Generatormatrix für einen linearen Kanalkode ergibt sich immer aus:

$$G_{l \times n} = \begin{pmatrix} 1 & 0 & \dots & 0 & c_{11} & c_{12} & \dots & c_{1k} \\ 0 & 1 & \dots & 0 & c_{21} & c_{22} & \dots & c_{2k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & c_{l1} & c_{l2} & \dots & c_{lk} \end{pmatrix} = I_l C$$

$$\longrightarrow H_{k \times n} = C^T I_k \cdot \begin{pmatrix} c_{11} & c_{12} & \dots & c_{l1} & 1 & 0 & \dots & 0 \\ c_{21} & c_{22} & \dots & c_{l2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{1k} & c_{2k} & \dots & c_{lk} & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$G_{l \times n} = I_l C \longrightarrow H_{k \times n} = C^T I_k$$

Sei nun wie oben angenommen  $a_1^* = (1101)$  und  $a_1 = (1101001) = (l_1 l_2 l_3 l_4 k_1 k_2 k_3)$ . Dann ergeben sich  $k_1, k_2$  und  $k_3$  wie folgt aus den letzten drei Spalten der Generatormatrix  $G_{4 \times 7}$ :

$$k_1 = l_1 \oplus l_2 \oplus l_3$$

$$k_2 = l_2 \oplus l_3 \oplus l_4$$

$$k_3 = l_1 \oplus l_2 \oplus l_4$$

### Einfachster Linearkode - Fehlerkorrektur

Es sei  $(n, n-1, d_{min} = 2)$  ein Paritätskode. Die Generatormatrix ist:

$$G_{(n-1) \times n} = \begin{pmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 \end{pmatrix}$$

Daraus ergibt sich wie folgt die Kontrollmatrix:

$$\longrightarrow H_{1 \times n} = (l_1 \ l_2 \ \dots \ l_l \ k) = (1 \ 1 \ \dots \ 1 \ 1)$$

Beispiel:

Sei die Kontrollmatrix wie im Skript (Seite 82) vorgegeben:

$$H_{k \times n} = H_{3 \times 7} =$$

$$\begin{matrix} n_7 & n_6 & n_5 & n_4 & n_3 & n_2 & n_1 \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ l_4 & l_3 & l_2 & k_3 & l_1 & k_2 & k_1 \end{matrix}$$

Es ergeben sich die folgenden Bestimmungsgleichungen aus den Zeilen der Kontrollmatrix (in dem nur die nicht redundanten Stellen - mit  $l_i$  gekennzeichnet - betrachtet werden):

$$k_3 = l_4 \oplus l_3 \oplus l_2$$

$$k_2 = l_4 \oplus l_3 \oplus l_1$$

$$k_1 = l_4 \oplus l_2 \oplus l_1$$

Die Kontrollgleichungen ergeben sich ebenfalls aus den Zeilen der Kontrollmatrix, indem zusätzlich zu den nicht redundanten Stellen auch die redundanten Stellen - mit  $k_i$  gekennzeichnet - betrachtet werden. Alle Stellen gemeinsam sind mit  $n_i$  bezeichnet:

$$s_3 = n_7 \oplus n_6 \oplus n_5 \oplus n_4$$

$$s_2 = n_7 \oplus n_6 \oplus n_3 \oplus n_2$$

$$s_1 = n_7 \oplus n_5 \oplus n_3 \oplus n_1$$

Für das Beispiel mit  $a^* = \overset{l_4 \ l_3 \ l_2 \ l_1}{(1 \ 0 \ 0 \ 1)}$  ist  $a = \overset{l_4 l_3 l_2 k_3 l_1 k_2 k_1}{(1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0)}$ . Bei einer Störung des Kanals mit  $l = (0010000)$  erhält man  $b = (1011100) \notin A$ . Durch Einsetzen in die Kontrollgleichungen

$$s = \begin{pmatrix} s_3 \\ s_2 \\ s_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

zeigt sich dass die Stelle  $n_5$  fehlerhaft ist, da diese in der Kontrollmatrix die Spalte  $(1 \ 0 \ 1)^T$  enthält. Der Fehler kann leicht korrigiert werden und man erhält  $b^* = (1001)$

In den *Notizen zur Vorlesung Mathematik für Informatiker II* von Professor Ganter findet man zum Sinn der Kontrollmatrix noch folgenden Absatz:

Der Empfänger kann prüfen, ob das empfangene 7-Tupel  $x$  ein Codewort ist, indem er  $x$  mit der Matrix  $H_{3 \times 7}$  multipliziert. Kommt der Nullvektor heraus, so wird man annehmen, dass  $x$  fehlerfrei übertragen wurde. Ist das der Fall, so erhält man durch Streichen der ersten, zweiten und vierten Komponente von  $x$  das ursprüngliche Nachrichten4Tupel zurück. [Text leicht abgeändert]

## Verkürzter und dichtgepackter Kode

	Bedingung	Beispiel
dichtgepackter Kode	$l = 2^k - 1 - k$	$(7, 4, d_{min} = 3)$ -Hammingkode
verkürzter Kode	$l < 2^k - 1 - k$	$(5, 2, d_{min} = 3)$ -Hammingkode

Dabei steht das Tripel  $(n,l,k)$  für die Kodewortlänge, wobei

$n$ ... Anzahl der Kodestellen (insgesamt)

$l$ ... Anzahl der Informationsstellen (nicht-redundante Kodestellen)

$k$ ... minimaler Hamming-Abstand

# Zyklischer Kode

## Generatorpolynom

Gegeben sei das Modularpolynom  $M(x)$  eines primitiven BCH<sup>1</sup>-Kodes (Skript ab Seite 94):

$$M(x) = x^4 + x + 1$$

Weil es sich um einen primitiven Kode handelt gilt außerdem:

$$n = 2^{k_1} - 1 \text{ und } k_1 = \text{grad } M(x)$$

Der Grad des Modularpolynoms  $\text{grad } M(x)$  ist 4. Es ergibt sich die Zahl der Kodewortstellen  $n = 2^4 - 1 = 15$ . Die Elemente des  $GF(2^4)^2$  erhält man nach dem Prinzip  $a^i, a^{2i}, a^{4i}, \dots$ , wobei der Exponent jedesmal *modulon* gerechnet wird.

Beispiel für  $\alpha^1$ :

Wegen  $2 \cdot 1 \pmod{15} = 2$ ,  $4 \cdot 1 \pmod{15} = 4$  und  $8 \cdot 1 \pmod{15} = 8$  sind  $\alpha^2, \alpha^4, \alpha^8$  Erweiterungselemente von  $\alpha^1$ .  $\alpha^{16}$  ist kein Erweiterungselement von  $\alpha^1$ , weil  $16 \pmod{15} = 1$  ist und  $\alpha^1$  natürlich schon enthalten ist.

$$\begin{aligned} &\alpha^0 \\ &\alpha^1, \alpha^2, \alpha^4, \alpha^8 \\ &\alpha^3, \alpha^6, \alpha^{12}, \alpha^9 \\ &\alpha^5, \alpha^{10} \\ &\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11} \end{aligned}$$

Aus diesen Elementen hat man nun die folgenden Minimalpolynome:

$$\begin{aligned} m_0(x) &= (x + \alpha^0) \\ m_1(x) = m_2(x) = m_4(x) = m_8(x) &= (x + \alpha^1)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8) \\ m_3(x) = m_6(x) = m_{12}(x) = m_9(x) &= (x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^9) \\ m_5(x) = m_{10}(x) &= (x + \alpha^5)(x + \alpha^{10}) \\ m_7(x) = m_{14}(x) = m_{13}(x) = m_{11}(x) &= (x + \alpha^7)(x + \alpha^{14})(x + \alpha^{13})(x + \alpha^{11}) \end{aligned}$$

Es gibt 3 Minimalpolynome vom Grad 4 und je ein Minimalpolynom vom Grad 2 und vom Grad 1. Um die Kodeeigenschaften  $l$  und  $d_{min}$  zu den Generatorpolynomen zu berechnen, nutzt man folgende Formeln:

$$\mu + d_{min} - 2 = x$$

Dabei ist  $\mu$  der kleinste Exponent der Aufeinanderfolge und  $x$  der größte Exponent der Aufeinanderfolge. Eine Aufeinanderfolge (von Exponenten) ist dabei immer die größte Folge der Art  $\alpha^1, \alpha^2, \alpha^3$ . Die Anzahl der Informationsstellen  $l$  erhält man aus  $l = n - k$  und  $k$  ist die Summe der Polynomgrade.

Die Generatorpolynome und ihre Codes sind also:

Generatorpolynome (Auswahl)	Polynomgrade	$\mu$	$x$	$(n, l, d_{min})$
$g(x) = m_1(x)$	4	1	2	(15,11,3)
$g(x) = m_1(x) \cdot m_3(x)$	4 + 4	1	4	(15,7,5)
$g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x)$	4 + 4 + 2	1	6	(15,5,7)
$g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x) \cdot m_7(x)$	4 + 4 + 2 + 4	1	14	(15,1,15)
$g(x) = m_0(x)$	1	0	0	(15,15,2)
$g(x) = m_0(x) \cdot m_1(x)$	1 + 4	0	2	(15,11,4)
$g(x) = m_0(x) \cdot m_1(x) \cdot m_3(x)$	1 + 4 + 4	0	4	(15,7,6)
$g(x) = m_0(x) \cdot m_1(x) \cdot m_3(x) \cdot m_5(x)$	1 + 4 + 4 + 2	0	6	(15,5,8)
$g(x) = m_1(x) \cdot m_7(x)$	4 + 4	1	2	(15,7,3)
$g(x) = m_3(x) \cdot m_7(x)$	4 + 4	11	14	(15,7,5)

<sup>1</sup>Bose-Chaudhuri-Hochquenghem-Kode

<sup>2</sup>Galois field / Erweiterungskörper: Elemente in einem Ring, in diesem Fall 4-Tupel aus  $\mathbb{Z}_2$

## Multiplikationsverfahren

Die Kanalkodewörter  $a(x)$  eines Codes werden durch ein Generatorpolynom  $g(x)$  erzeugt.

$$a(x) = a^*(x) \cdot g(x) \text{ mit } a^* = (1100)$$

Es handelt sich dabei um einen (7,4,3)-Kode mit dem Modularpolynom

$$M(x) = x^3 + x^2 + 1 \text{ und } g(x) = M(x).$$

Daraus folgt:

$$\begin{aligned} a(x) &= (x^3 + x^2 + 1) \cdot a^*(x) = (x^3 + x^2 + 1) \cdot (1100) = (x^3 + x^2 + 1) \cdot (x^3 + x^2) \\ &= x^6 + x^5 + x^3 + x^5 + x^4 + x^2 = x^6 + x^4 + x^3 + x^2 \end{aligned}$$

Die zwei  $x^5$  gehen verloren weil die Rechnung mit  $\oplus$  (XOR), also (*mod* 2) erfolgt. Zur Probe kann man  $a(x)$  noch einmal binär ausrechnen.

$$a = a^* \cdot g :$$

$$\begin{array}{r} 1100 * 1101 \\ \phantom{1100} 1100 \\ \phantom{1100} 0000 \\ \phantom{1100} 1100 \\ \phantom{1100} 1100 \\ \hline 1011100 \end{array}$$

$$a = (1011100) = x^6 + x^4 + x^3 + x^2$$

## Divisionsverfahren

Ziel ist es ein durch ein anderes Polynom teilbares Polynom zu erhalten. Dazu führt man mit einem beliebigen Polynom eine Division aus und addiert dann den Rest hinzu. Es gilt:

$$a(x) = a^*(x) \cdot x^k + r(x)$$

Sei wie zuvor  $a^*(x) = (1100)$ .

$$a^*(x) = x^3 + x^2 \text{ und } a^*(x) \cdot x^k = (x^3 + x^2) \cdot x^3 = x^6 + x^5$$

$$\begin{array}{r} x^6 + x^5 \div x^3 + x^2 + 1 = x^3 + 1 \\ x^6 + x^5 + x^3 \\ \phantom{x^6 + x^5} x^3 + x^2 + 1 \\ \phantom{x^6 + x^5} x^2 + 1 \end{array}$$

$$a(x) = x^6 + x^5 + x^2 + 1$$

Wie beim Multiplikationsverfahren führen wir eine binäre Probe durch:

$$\begin{array}{r} 1100000 : 1101 \\ 1101 \\ \phantom{1101} 1000 \\ \phantom{1101} 1101 \\ \phantom{1101} 101 \end{array}$$

$$a = (1100101) = x^6 + x^5 + x^2 + 1$$

Die Generatormatrix aus dem Generatorpolynom erhält man wie im Skript definiert (Seite 99). Sie lautet für  $g(x) = x^3 + x^2 + 1$  wie im folgenden angegeben und konstruiert aus  $a^* = (1100)$  das Wort  $a = (0010111)$ .

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

## Fehlererkennung

Sei  $a = (1011100)$  das zu übertragende Kodewort. Bei der Übertragung tritt der Fehler  $l = (0011010)$  auf. Daraus ergibt sich das folgende Empfangswort:  $b = (1000110)$ . Wie kann dieser Fehler behoben werden?

Um den Fehler festzustellen wird  $b$  durch das Generatorpolynom (Skript, Seite 99) geteilt. Bleibt dabei ein Rest, so enthält das Wort einen Fehler, da es ja mit dem Generatorpolynom erzeugt wurde. Wir führen zuerst die Division in Polynomdarstellung durch:

$$\begin{array}{r} x^6 + x^2 + x \div x^3 + x^2 + 1 = x^3 + x^2 + x \\ x^6 + x^5 + x^3 \\ \quad x^5 + x^3 + x^2 + x \\ \quad \quad x^5 + x^4 + x^2 \\ \quad \quad \quad x^4 + x^3 + x \\ \quad \quad \quad \quad x^4 + x^3 + x \\ \quad \quad \quad \quad \quad 0 \end{array}$$

Zur Probe noch einmal die Division (XOR) in Binärform:

$$\begin{array}{r} 1000110 : 1101 \\ 1101 \\ \quad 1011 \\ \quad \quad 1101 \\ \quad \quad \quad 1101 \\ \quad \quad \quad \quad 1101 \\ \quad \quad \quad \quad \quad 1101 \\ \quad \quad \quad \quad \quad \quad 0 \end{array}$$

Die Empfangsfolge  $b$  ist also ohne Rest durch das Generatorpolynom teilbar. Das heißt es wird kein Fehler erkannt! Das liegt daran, dass in diesem Fall  $l \in A$  gilt. Und damit ist auch  $b \in A$  (zyklischer Kode). Der Fehler kann also unter keinen Umständen erkannt werden.

Was für Fehler kann dieser Kode eigentlich erkennen?

Wie man an den Kodewörtern erkennt ist die Zahl der Kodestellen  $n = 7$ . Die Anzahl der Informationsstellen ergibt sich wie auf den vorigen Seiten erklärt aus der Anzahl der Kodestellen abzüglich des Grades des Generatorpolynoms. Daraus folgt:  $k = 7 - 3 = 4$ .

Den minimale Hamming-Abstand  $d_{min}$  kann man auch aus der Länge des Zyklus der zugehörigen Erweiterungselemente ablesen. Der Zyklus ist  $\alpha^1, \alpha^2, \alpha^4$ .  $\alpha^8$  gehört nicht zum Zyklus da ja  $mod n$ , also in diesem Fall  $mod 7$  gerechnet wird. Und damit ist  $\alpha^{18} = \alpha^1$  und das ist ja bereits im Zyklus enthalten. Der Zyklus hat also eine Länge von 3.

$$(n, l, d_{min}) = (7, 4, 3)$$

Wegen  $f_e = d_{min} - 1 = 2$  können also maximal 2-Bit-Fehler erkannt werden. Dafür lässt der Kode Bündelfehler (Skript, Seite 100) bis zur Länge  $k$  erkennen. Den Prozentsatz der erkennbaren Fehler berechnet man wie folgt:

$$p_{FE} = 100 \cdot (1 - 2^{-k})$$

$2^{-k}$  erhält man auch aus:

$$\frac{\text{nicht erkennbare Fehler}}{\text{mögliche Fehler}} = \frac{2^l}{2^n} = \frac{2^l}{2^{l+k}} = 2^{-k}$$

Für unser Beispiel (7, 4, 3) gilt also:

$$2^{-k} = \frac{1}{8} \quad \text{und} \quad p_{FE} = \frac{7}{8} = 87,5\%$$