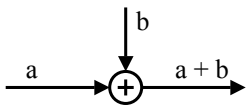
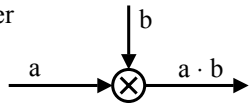
Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

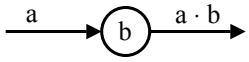
- Addierer



- Multiplizierer



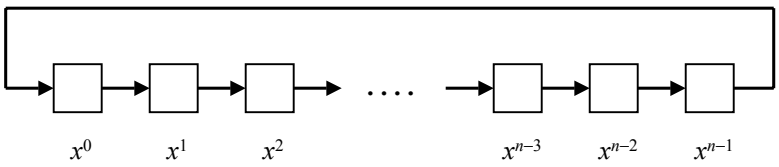
- Skalierung



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- zyklisches Verschieben eines Polynoms

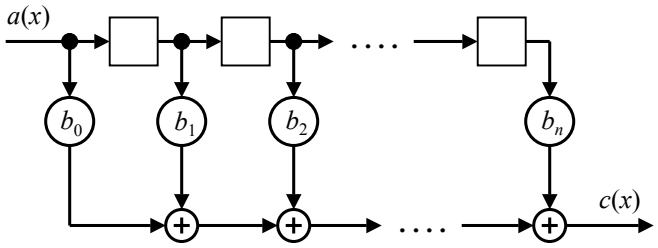


- Schaltung berechnet: $x^i \cdot a(x) \bmod (x^n + 1)$
- einfachstes Beispiel eines rückgekoppelten Schieberegisters

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Multiplikation zweier Polynome

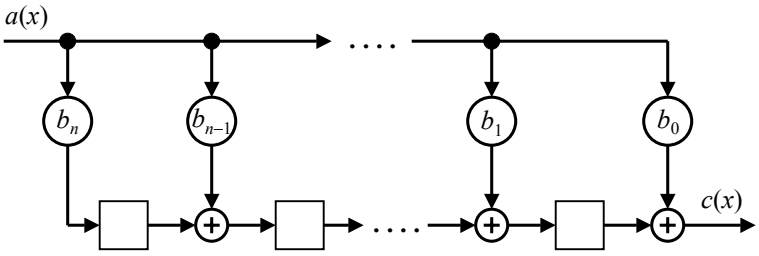


$$c(x) = a(x) \cdot [b_0 + b_1 x + b_2 x^2 + ... + b_n x^n]$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Multiplikation zweier Polynome: alternative Struktur

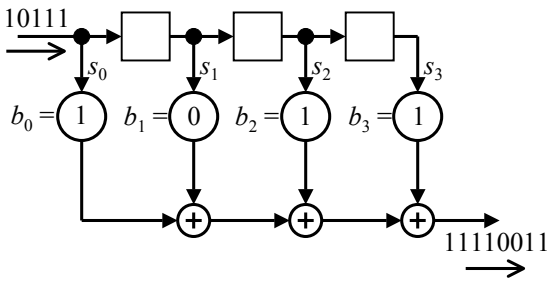


$$c(x) = a(x) \cdot [b_0 + b_1 x + b_2 x^2 + ... + b_n x^n]$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für eine Multiplikation



i	s_0	s_1	s_2	s_3	c_i
−1	0	0	0	0	0
0	1	0	0	0	1
1	1	1	0	0	1
2	1	1	1	0	0
3	0	1	1	1	0
4	1	0	1	1	1
5	0	1	0	1	1
6	0	0	1	0	1
7	0	0	0	1	1
8	0	0	0	0	0

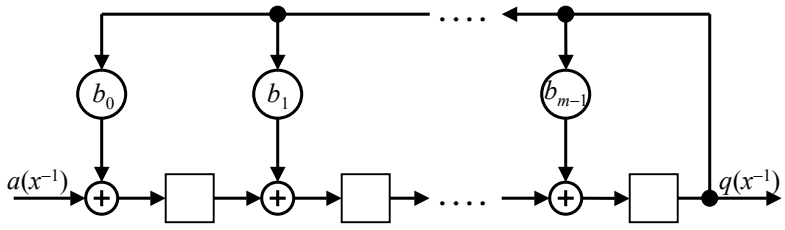
$$c(x) = a(x) \cdot b(x) = (x^4 + x^2 + x + 1) \cdot (x^3 + x^2 + 1)$$

$$= x^7 + x^6 + x^5 + x^4 + 0 + 0 + x + 1$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Division zweier Polynome



$$q(x^{-1}) = a(x^{-1})\, x^m + q(x^{-1})\, [b_0\, x^m + b_1\, x^{m-1} + \ldots + b_{m-1}\, x]$$

$$\Rightarrow \quad a(x^{-1}) = q(x^{-1})\, [b_0 + b_1\, x^{-1} + \ldots + b_{m-1}\, x^{-(m-1)} + x^{-m}] = q(x^{-1})\, b(x^{-1})$$

Substitution $x^{-1} \rightarrow x \quad \Rightarrow \quad a(x) = q(x)\, b(x) \quad \Rightarrow \quad q(x) = \dfrac{a(x)}{b(x)}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Division zweier Polynome mit Rest:

$$\frac{a(x)}{b(x)} = q(x) + \frac{s(x)}{b(x)}$$

Abbruch der Division, wenn die letzte Stelle von $a(x^{-1})$ in das Schieberegister eingeschrieben wurde.

$\Rightarrow$ Die ganzzahlige Division ist beendet.

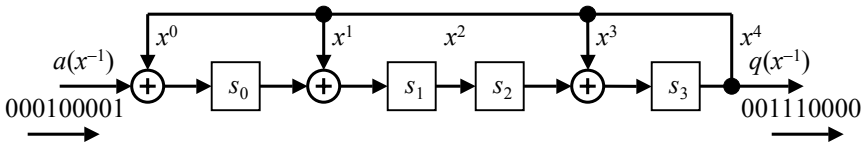
$q(x^{-1})$ = Ausgangswort

$s(x^{-1})$ = Inhalt der Speicherzellen

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für Division zweier Polynome mit Rest:



$$(x^8 + x^3) : (x^4 + x^3 + x + 1) = x^4 + x^3 + x^2 + \frac{x^3 + x^2}{x^4 + x^3 + x + 1}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

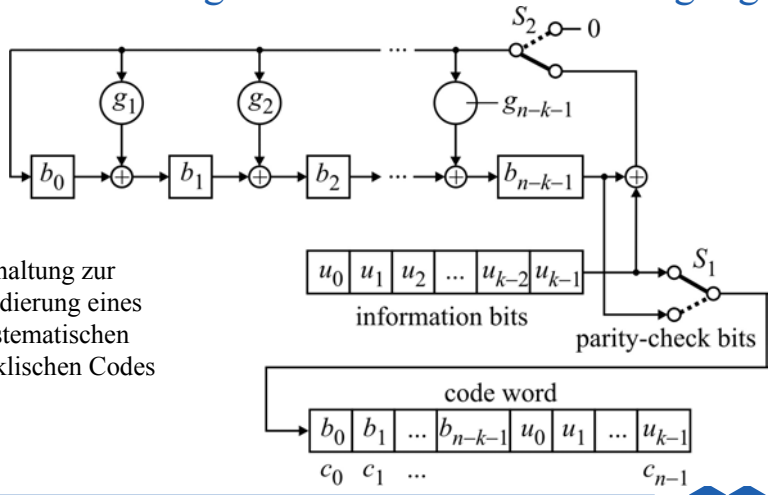
- Beispiel für Division zweier Polynome (Fortsetzung)

i	a_i	s_0	s_1	s_2	s_3	q_i
9	0	0	0	0	0	0
8	1	1+0=1	0+0=0	0	0+0=0	0
7	0	0+0=0	1+0=1	0	0+0=0	0
6	0	0+0=0	0+0=0	1	0+0=0	0
5	0	0+0=0	0+0=0	0	1+0=1	0
4	0	0+1=1	0+1=1	0	0+1=1	1
3	1	1+1=0	1+1=0	1	0+1=1	1
2	0	0+1=1	0+1=1	0	1+1=0	1
1	0	0+0=0	1+0=1	1	0+0=0	0
0	0	0+0=0	0+0=0	1	1+0=1	0

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Schaltung zur Codierung eines systematischen zyklischen Codes



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Funktionsweise
  - 1. Schritt: Einlesen der Informationsbits $u_0, u_1, u_2, \ldots, u_{k-1}$, beginnend mit u_{k-1}

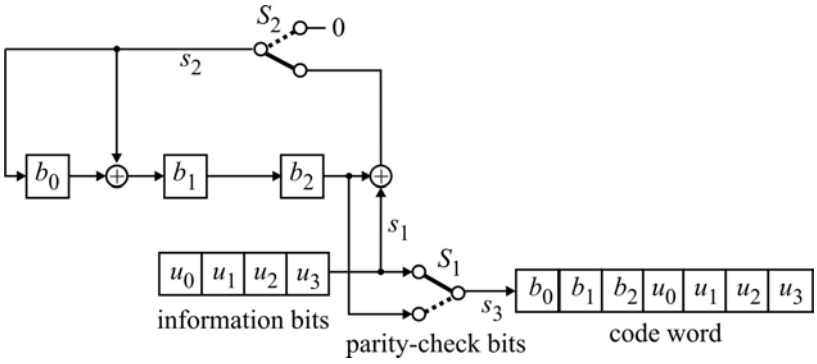
    Einlesen von „rechts“ entspricht Multiplikation mit x^{n-k}

    Nach dem Einlesen der k Informationsbits enthält das Schieberegister den Divisionsrest $r(x)$
  - 2. Schritt: Umlegen der Schalter S_1 und S_2 (Unterbrechung der Rückkopplungsschleife)
  - 3. Schritt: Ausgabe der Prüfbits

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: $u(x) = x^3 + x^2 + 1$ und $g(x) = x^3 + x + 1$



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

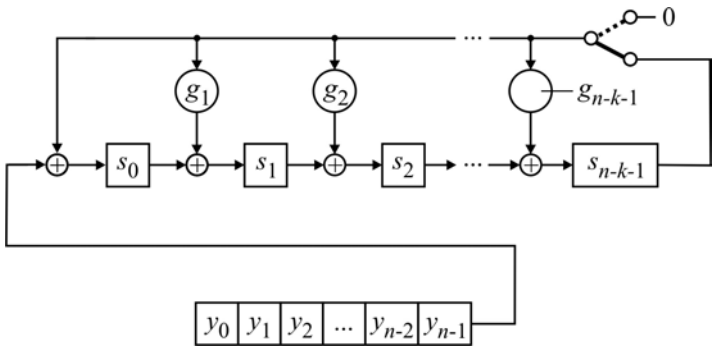
- Beispiel: $u(x) = x^3 + x^2 + 1$ und $g(x) = x^3 + x + 1$

t	s_1	b_0	b_1	b_2	s_2	s_3
0	0	0	0	0	0	0
1	1	1	1	0	1	1
2	1	1	0	1	1	1
3	0	1	0	0	1	0
4	1	1	0	0	1	1
5		0	1	0	0	0
6		0	0	1	0	0
7		0	0	0	0	1

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

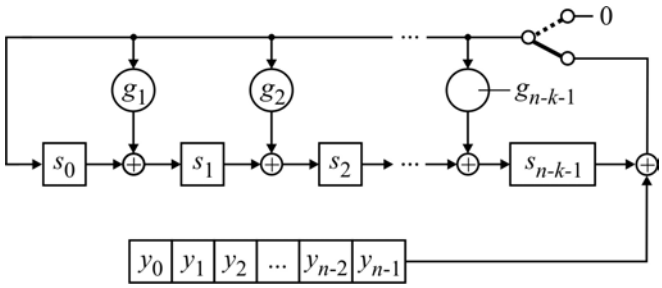
- Schaltung zur Decodierung: Division des Empfangsworts durch das Generatorpolynom und Berechnung des Syndroms



Nachrichtentechnik 4

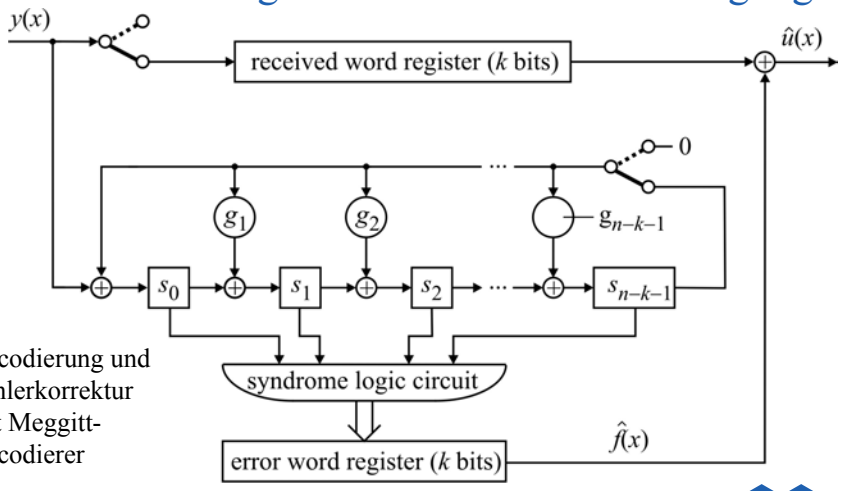
3 Kanalcodierung in der Nachrichtenübertragung

- Schaltung zur Decodierung: Einlesen des Empfangsworts von rechts



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung



- Decodierung und Fehlerkorrektur mit Meggitt-Decodierer

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Gruppen
  - Definition: Eine Menge $\boldsymbol{G}$ und eine Verknüpfung $\circ$ werden als **Gruppe** $(\boldsymbol{G},\circ)$ bezeichnet, wenn die folgenden Bedingungen erfüllt sind:
    - Die Verknüpfung ist assoziativ: $a \circ (b \circ c) = (a \circ b) \circ c$ mit $a,b,c \in \boldsymbol{G}$
    - Die Menge $\boldsymbol{G}$ ist abgeschlossen: für $a,b \in \boldsymbol{G}$ ist auch $a \circ b \in \boldsymbol{G}$
    - Die Menge $\boldsymbol{G}$ enthält ein neutrales Element e mit der Eigenschaft: $a \circ e = e \circ a = a$ mit $a, e \in \boldsymbol{G}$
    - Für jedes Element a in $\boldsymbol{G}$ existiert ein inverses Element a', so dass: $a \circ a' = a' \circ a = e$ mit $a, e \in \boldsymbol{G}$

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Eine Gruppe wird als kommutative oder abelsche Gruppe bezeichnet, wenn für beliebige $a,b \in \boldsymbol{G}$ gilt: $a \circ b = b \circ a$
- Das neutrale Element einer Gruppe ist eindeutig:

  Beweis mit Annahme: es gibt zwei neutrale Elemente e_1 und e_2:
  $e_1 = e_1 \circ e_2 = e_2 \circ e_1 = e_2$
- Beispiele:
  - Die Menge der ganzen Zahlen $\boldsymbol{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$ bildet bezüglich der Addition eine kommutative Gruppe:

    neutrales Element: 0,

    inverses Element zu a: $-a$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Die Menge der ganzen Zahlen $\boldsymbol{Z} = \{... -2, -1, 0, 1, 2, ...\}$ bildet bezüglich der Multiplikation keine Gruppe:

  inverse Elemente fehlen.

- Definition: Besitzt eine Gruppe endlich viele Elemente, so wird sie als **endliche** oder **finite** Gruppe bezeichnet.
  - Beispiel: endliche Menge ganzer Zahlen $\boldsymbol{G} = \{0, 1, 2, ... , m-1\}$ und Modulo-m-Addition „⊕“:

$$\frac{a+b}{m} = q + \frac{r}{m} \quad \Leftrightarrow \quad a + b = q \cdot m + r$$

neutrales Element: 0,

inverses Element zu a: $a' = m - a$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiel: binäre Menge $\boldsymbol{B} = \{0, 1\}$ und Modulo-2-Addition „⊕“

  neutrales Element: 0,

  inverse Elemente: $a = 1 \Rightarrow a' = 1$

  $a = 0 \Rightarrow a' = 0$

⊕	0	1
0	0	1
1	1	0

- Beispiel: $\boldsymbol{G} = \{0, 1, 2, 3, 4, 5, 6\}$ und Modulo-7-Addition „⊕“

  neutrales Element: 0,

  inverses Element zu a:

  $a' = m - a$

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

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiel: endliche Menge ganzer Zahlen $\boldsymbol{G} = \{1, 2, 3, \ldots, p-1\}$ mit p = Primzahl und Modulo-p-Multiplikation „⊗“:

$$\frac{a \cdot b}{p} = q + \frac{r}{p} \quad \Leftrightarrow \quad a \cdot b = q \cdot p + r$$

Abgeschlossenheit: $a \cdot b$ ist nicht durch p ohne Rest teilbar, da p Primzahl ist

neutrales Element: 1,

inverse Elemente existieren

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiel: $p = 7 \Rightarrow \boldsymbol{G} = \{1, 2, 3, 4, 5, 6\}$ und Modulo-7-Multiplikation „⊗“

⊗	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Zyklische Gruppen
  - Definition: Lassen sich alle Elemente einer multiplikativen Gruppe $\boldsymbol{G} = \{1, g_1, g_2, \ldots, g_{m-1}\}$ als Potenzen von mindestens einem Element g_i darstellen, so heißt die Gruppe zyklisch.
  - $\boldsymbol{G} = \{1, g_1, g_2, \ldots, g_{m-1}\}$ besteht aus m Elementen g_i^j : $\boldsymbol{G} = \{g_i^0, g_i^1, g_i^2, \ldots, g_i^{m-1}\}$
  - g_i heißt primitives Element der Gruppe der Ordnung m
  - Einselement: $1 = g_i^0$
  - Ordnung (g_k) = Anzahl von Elementen, die durch g_k^l gebildet werden können

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiele:

multiplikative modulo-5-Gruppe

$\boldsymbol{G} = \{1, 2, 3, 4\}$

z	z^1	z^2	z^3	z^4	Ordnung
1	1	1	1	1	1
2	2	4	3	1	4
3	3	4	2	1	4
4	4	1	4	1	2

primitive Elemente

multiplikative modulo-7-Gruppe

$\boldsymbol{G} = \{1, 2, 3, 4, 5, 6\}$

z	z^1	z^2	z^3	z^4	z^5	z^6	Ordnung
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Ringe
  - Definition: Für $\boldsymbol{R}$ sind $\oplus$ und $\otimes$ definiert sowie folgende Gesetze gültig:
    - $\boldsymbol{R}$ ist kommutative Gruppe bezüglich $\oplus$
    - $\boldsymbol{R}$ ist bezüglich $\otimes$ abgeschlossen: $a,b \in \boldsymbol{R} \rightarrow a \otimes b \in \boldsymbol{R}$
    - $\boldsymbol{R}$ ist bezüglich $\otimes$ ist assoziativ: $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ mit $a,b,c \in \boldsymbol{R}$
    - Distributivgesetz gilt: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ mit $a,b,c \in \boldsymbol{R}$
  - kommutativer Ring, wenn $\otimes$ kommutativ
  - Ring mit neutralem Element: $a \otimes 1 = 1 \otimes a = a$ mit $a \in \boldsymbol{R}$

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Beispiel eines kommutativen Rings mit neutralem Element: ganze Zahlen $\boldsymbol{Z}$ mit gewöhnlicher Addition und Multiplikation
- Beispiel eines kommutativen Rings mit neutralem Element: ganze Zahlen $\boldsymbol{Z}_m = \{0,1,2,\ldots,m-1\}$ mit modulo-m-Addition und modulo-m-Multiplikation
  - eindeutiges inverses Element nur, wenn m = Primzahl

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Körper (field)
  - Definition: Für $\boldsymbol{K}$ sind $\oplus$ und $\otimes$ definiert sowie folgende Gesetze gültig:
    - $\boldsymbol{K}$ ist kommutative Gruppe bezüglich $\oplus$, 0 ist neutrales Element
    - $\boldsymbol{K}$ ohne 0 ist kommutative Gruppe bezüglich $\otimes$, 1 ist neutrales Element
    - Distributivgesetz gilt: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ mit $a,b,c \in \boldsymbol{R}$
  - Körper mit endlich vielen Elementen = **Galois-Feld**
  - Ganze Zahlen $\boldsymbol{Z}_m = \{0,1, 2, \ldots , m-1\}$ bilden ein Galois-Feld $\boldsymbol{GF}(m) = \boldsymbol{Z}_m$, wenn m Primzahl ist, d. h. $m = p$, oder wenn $m = p^k$

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Einige Eigenschaften von Galois-Feldern ohne Beweis:
  - $a \otimes 0 = 0 \otimes a = 0$
  - $a \neq 0$ und $b \neq 0 \rightarrow a \otimes b \neq 0$ (keine Nullteiler – folgt aus Abgeschlossenheit der Multiplikation)
  - $a \otimes b = 0$ und $a \neq 0 \rightarrow b = 0$
  - $-(a \otimes b) = (-a) \otimes b = a \otimes (-b)$
  - $a \otimes b = a \otimes c$ und $a \neq 0 \rightarrow b = c$
  - $\underbrace{1 \oplus 1 \oplus 1 \oplus \ldots \oplus 1}_{m \text{ Summanden}} = 0$
  - Jedes Galois-Feld besitzt zumindest ein primitives Element.

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiel: ***GF***(2)

⊕	0	1
0	0	1
1	1	0

⊗	0	1
0	0	0
1	0	1

- Beispiel: ***GF***(5)

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiele in ***GF***(5)
  - Addition direkt mit Tabelle: $1 + 2 = 3$, $2 + 4 = 1$, $4 + 4 = 3$
  - inverse Elemente der Addition: $a + (-a) = 0$

a	0	1	2	3	4
$-a$	0	4	3	2	1

  - Subtraktion mit inversen Elementen der Addition:

$3 - 2 = 3 + (-2) = 3 + 3 = 1$

$1 - 4 = 1 + (-4) = 1 + 1 = 2$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiele in ***GF***(5)
  - Multiplikation direkt mit Tabelle: $1 \cdot 2 = 2, \quad 2 \cdot 4 = 3, \quad 4 \cdot 4 = 1$
  - inverse Elemente der Multiplikation: $a \cdot (a^{-1}) = 1$

a	1	2	3	4
a^{-1}	1	3	2	4

  - Division mit inversen Elementen der Multiplikation:

$3 \div 2 = 3 \cdot (2^{-1}) = 3 \cdot 3 = 4$

$1 \div 3 = 1 \cdot (3^{-1}) = 1 \cdot 2 = 2$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiel in ***GF***(5): lineares Gleichungssystem

I: $2\,x_0 + x_1 = 2$

II: $3\,x_1 + x_2 = 3$

III: $x_0 + x_1 + 2\,x_2 = 3$

I: $2\,x_0 = 2 - x_1$

II: $x_2 = 3 - 3\,x_1$

$2 \cdot$ III: $(2 - x_1) + 2\,x_1 + 4\,(3 - 3\,x_1) = 2 \cdot 3$

$\Rightarrow \quad 2 + 4 \cdot 3 - 2 \cdot 3 = x_1(1 - 2 + 4 \cdot 3) \quad \Rightarrow \quad 3 = x_1$

$\Rightarrow \quad x_2 = 3 - 3\,x_1 = 4$

$\Rightarrow \quad x_0 = 2^{-1}\,(2 - x_1) = 2$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Erweiterungskörper
  - $\boldsymbol{G} = \{0, 1, 2, 3\}$ bildet zusammen mit Modulo-4-Addition und Modulo-4-Multiplikation **kein** Galois-Feld !

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Erweiterungskörper
  - Erweiterung von Galois-Feldern entsprechend Erweiterung von reellen Zahlen zu komplexen Zahlen
  - Definition komplexer Zahlen: $\boldsymbol{R} \rightarrow \boldsymbol{C}$
    - $x^2 + 1 = 0$ besitzt keine Lösung für $x \in \boldsymbol{R}$
    - Körpererweiterung: $\alpha^2 + 1 \overset{!}{=} 0 \quad \Leftrightarrow \quad \alpha^2 = -1 \quad \Leftrightarrow \quad \alpha = \sqrt{-1}$
    - Definition komplexer Zahlen: $c = c_0 + c_1\alpha$ mit $c_0, c_1 \in \boldsymbol{R}$
  - Definition eines erweiterten Galois-Feldes: $\boldsymbol{GF}(2) \rightarrow \boldsymbol{GF}(2^2)$
    - $x^2 + x + 1 = 0$ besitzt keine Lösung für $x \in \boldsymbol{GF}(2)$
    - Körpererweiterung: $\alpha^2 + \alpha + 1 \overset{!}{=} 0 \quad \Leftrightarrow \quad \alpha^2 = \alpha + 1 \bmod 2$
    - Def. der Elemente von $\boldsymbol{GF}(2^2)$: $c = c_0 + c_1\alpha$ mit $c_0, c_1 \in \boldsymbol{GF}(2)$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Definition eines erweiterten Galois-Feldes: $\boldsymbol{GF}(p) \rightarrow \boldsymbol{GF}(p^m)$
  - $p(x) = x^m + p_{m-1}x^{m-1} + \ldots + p_1 x + p_0 = 0$ besitzt keine Lösung für $x \in \boldsymbol{GF}(p)$ und $x \in \boldsymbol{GF}(p^n)$ mit $n < m$
  - Körpererweiterung: $p(\alpha) = 0 \Leftrightarrow \alpha^n = -p_{m-1}\alpha^{n-1} - \ldots - p_1\alpha - p_0$
  - Def. der Elemente von $\boldsymbol{GF}(p^m)$: $c = c_0 + c_1\alpha + \ldots + c_{m-1}\alpha^{n-1}$ mit $c_i \in \boldsymbol{GF}(p)$
  - $\boldsymbol{GF}(p^m)$ enthält p^m Elemente
- besonders wichtig für die Codierung in der digitalen Nachrichtentechnik: $\boldsymbol{GF}(p^m)$ mit $p = 2$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Addition in $\boldsymbol{C}$:

$$\begin{aligned} c &= a + b \\ &= (a_0 + a_1\alpha) + (b_0 + b_1\alpha) \\ &= (a_0 + b_0) + (a_1 + b_1)\alpha \end{aligned} \qquad (4.1)$$

Multiplikation in $\boldsymbol{C}$:

$$\begin{aligned} c &= a \cdot b \\ &= (a_0 + a_1\alpha)\cdot(b_0 + b_1\alpha) \\ &= a_0b_0 + (a_1b_0 + a_0b_1)\alpha + a_1b_1(-1) \\ &= a_0b_0 - a_1b_1 + (a_1b_0 + a_0b_1)\alpha \end{aligned} \qquad (4.2)$$

- Addition in $\boldsymbol{GF}(2^2)$:

$$\begin{aligned} c &= a + b \\ &= (a_0 + a_1\alpha) + (b_0 + b_1\alpha) \\ &= (a_0 + b_0) + (a_1 + b_1)\alpha \end{aligned} \qquad (4.3)$$

Multiplikation in $\boldsymbol{GF}(2^2)$:

$$\begin{aligned} c &= a \cdot b \\ &= (a_0 + a_1\alpha)\cdot(b_0 + b_1\alpha) \\ &= a_0b_0 + (a_1b_0 + a_0b_1)\alpha + a_1b_1(\alpha + 1) \\ &= a_0b_0 + a_1b_1 + (a_1b_0 + a_0b_1 + a_1b_1)\alpha \end{aligned} \qquad (4.4)$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Additions- und Multiplikationstabellen für $\boldsymbol{GF}(2^2) = \{0, 1, \alpha, 1+\alpha\}$ in Komponentendarstellung:

$\oplus$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\otimes$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Interpretation als Polynomrestklasse:
  - Bedingung $x^2 + x + 1 = 0$ entspricht einer Berechnung modulo $x^2 + x + 1$
  - Beispiel in $\boldsymbol{GF}(2^2)$: $(1 + \alpha) \cdot (1 + \alpha) = 1 + \alpha^2$

$$(\alpha^2 + 1) : (\alpha^2 + \alpha + 1) = 1 + \frac{\alpha}{\alpha^2 + \alpha + 1}$$
$$\underline{+ (\alpha^2 + \alpha + 1)}$$
$$\alpha = r(\alpha)$$

  - $\boldsymbol{GF}(2^2)$ ist definiert durch alle möglichen Ergebnisse von $p(\alpha)$ modulo $\alpha^2 + \alpha + 1$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Additions- und Multiplikationstabellen für $GF(2^2)$ in Vektordarstellung:

$\oplus$	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10
11	11	01	10	00

$\otimes$	00	10	01	11
00	00	00	00	00
10	00	10	01	11
01	00	01	11	10
11	00	11	10	01

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Exponenten-Darstellung

$$\alpha^k = \alpha^{k \bmod (p^m - 1)} \qquad (4.5)$$

$$\alpha^k = \alpha^{k \bmod 3}$$

0	=	0
1	=	α^0
α	=	α^1
$1+\alpha$	=	α^2

1	=	$\alpha^3 = \alpha^0$
α	=	$\alpha^4 = \alpha^1$
$1+\alpha$	=	$\alpha^5 = \alpha^2$
...		...

- Additions- und Multiplikationstabellen für $GF(2^2)$ in Exponentendarstellung:

$\oplus$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\otimes$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Definition: **irreduzibles Polynom** $p(x)$ = Polynom mit Grad m, das nicht als Produkt zweier Polynome $p_a(x)$, $p_b(x)$ mit Grad ≥ 1 und < m dargestellt werden kann
- Beispiel: $p(x) = x^2 + x + 1$

  Testpolynome mit Grad 1: $p_a(x) = x, \quad p_b(x) = x + 1$

  $(x^2 + x + 1) \div x = x + 1 + \frac{1}{x}$

  $(x^2 + x + 1) \div (x + 1) = x + \frac{1}{x+1}$
- irreduzible Polynome haben vergleichbare Eigenschaften wie Primzahlen
- Satz: Irreduzible Polynome haben keine Nullstelle in ***GF*** (p).

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Definition: **primitives Polynom** = irreduzibles Polynom $p(x)$ vom Grad m, das eine Nullstelle α (d.h. $p(\alpha) = 0$) mit der folgenden Eigenschaft besitzt:

  Die Terme $\alpha^i \bmod p(\alpha)$ erzeugen alle möglichen $p^m - 1$ von 0 verschiedenen Elemente des Galoisfelds ***GF***(p^m).

  $\alpha \in$ ***GF***(p^m) heißt **primitives Element**

  mit $\alpha^0 = \alpha^n = 1 \quad$ für $\quad n = p^m - 1$
- Für jeden Primkörper ***GF***(p^m) und jedes m existiert mindestens ein primitives Polynom $p(x)$.
- Primitive Polynome sind irreduzibel, Umkehrung gilt im Allgemeinen nicht.

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Darstellung des primitiven Polynoms durch seine Nullstellen:

$$p(x) = \prod_{i=0}^{m-1} (x - \alpha^{p^i}) \qquad (4.6)$$

- Faktorisierung durch alle $n = p^m - 1$ von 0 verschiedenen Elemente $a_i \in \boldsymbol{GF}(p^m)$:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - a_i) \qquad (4.7)$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Tabelle der primitiven Polynome

m	primitives Polynom
1	$x + 1$
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x + 1$
8	$x^8 + x^6 + x^5 + x^4 + 1$

m	primitives Polynom
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^7 + x^4 + x^3 + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^8 + x^6 + x + 1$
15	$x^{15} + x + 1$
16	$x^{16} + x^{12} + x^3 + x + 1$

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Diskrete Fourier-Transformation (DFT)
  - Transformation von Polynomen:
    $A(x) = \mathrm{DFT}(a(x)) \quad \Leftrightarrow \quad a(x) = \mathrm{IDFT}(A(x))$
  - gegeben: Polynome vom Grad $\leq n-1 = p^m - 2$ mit Koeffizienten aus $\boldsymbol{GF}(p^m)$, z = primitives Element von $\boldsymbol{GF}(p^m)$:

$$\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \quad \Leftrightarrow \quad a(x) = \sum_{i=0}^{n-1} a_i x^i \tag{4.8}$$

$$\mathbf{A} = (A_0, A_1, \ldots, A_{n-1}) \quad \Leftrightarrow \quad A(x) = \sum_{j=0}^{n-1} A_j x^j \tag{4.9}$$

Nachrichtentechnik 4
4 Algebraische Grundbegriffe für Codes

- Schreibweisen für die DFT:

$$a(x) \circ\!\!-\!\!\bullet\, A(x)$$

$$\mathbf{a} \circ\!\!-\!\!\bullet\, \mathbf{A}$$

Zeitbereich $\circ\!\!-\!\!\bullet$ Frequenzbereich

Transformationsvorschrift:

$$A_j = -a(z^{-j}) = -\sum_{i=0}^{n-1} a_i z^{-i \cdot j} \tag{4.10}$$

$$a_i = A(z^i) = \sum_{j=0}^{n-1} A_j z^{i \cdot j} \tag{4.11}$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Eigenschaften
  - eineindeutige Transformation
  - IDFT(DFT($a(x)$)) = $a(x)$
  - DFT(DFT($a(x)$)) = $-a(x)$
  - DFT(DFT(DFT(DFT($a(x)$)))) = $a(x)$
  - z^{-j} ist Nullstelle von $a(x)$ $\Leftrightarrow$ $A_j = 0$

    $a(z^{-j}) = 0 \quad \Leftrightarrow \quad \mathbf{A} = (A_0, A_1, \ldots, A_{j-1}, 0, A_{j+1}, \ldots, A_{n-1})$ (4.12)
  - z^{i} ist Nullstelle von $A(x)$ $\Leftrightarrow$ $a_i = 0$

    $A(z^{i}) = 0 \quad \Leftrightarrow \quad \mathbf{a} = (a_0, a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_{n-1})$ (4.13)

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Darstellung in Matrix-Schreibweise:

$$\begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{n-1} \end{pmatrix} = - \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & z^{-1} & z^{-2} & \cdots & z^{-(n-1)} \\ 1 & z^{-2} & z^{-4} & \cdots & z^{-2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & z^{-(n-1)} & z^{-2(n-1)} & \cdots & z^{-(n-1)^2} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} \tag{4.14}$$

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & z^{1} & z^{2} & \cdots & z^{n-1} \\ 1 & z^{2} & z^{4} & \cdots & z^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & z^{n-1} & z^{2(n-1)} & \cdots & z^{(n-1)^2} \end{pmatrix} \cdot \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ \vdots \\ A_{n-1} \end{pmatrix} \tag{4.15}$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Beispiel: $\boldsymbol{GF}(7),\ z = 5,\ A(x) = 4 + 5x$

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & z^1 & z^2 & z^3 & z^4 & z^5 \\ 1 & z^2 & z^4 & z^0 & z^2 & z^4 \\ 1 & z^3 & z^0 & z^3 & z^0 & z^3 \\ 1 & z^4 & z^2 & z^0 & z^4 & z^2 \\ 1 & z^5 & z^4 & z^3 & z^2 & z^1 \end{pmatrix} \cdot \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \end{pmatrix}$$

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 5 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 4 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + 5 \cdot \begin{pmatrix} 1 \\ 5 \\ 4 \\ 6 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 3 \\ 6 \\ 0 \\ 5 \end{pmatrix}$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Rücktransformation: $\boldsymbol{GF}(7),\ z = 5,\ a(x) = 2 + x + 3x^2 + 6x^3 + 5x^5$

$$\begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \end{pmatrix} = -\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & z^{-1} & z^{-2} & z^{-3} & z^{-4} & z^{-5} \\ 1 & z^{-2} & z^{-4} & z^{-0} & z^{-2} & z^{-4} \\ 1 & z^{-3} & z^{-0} & z^{-3} & z^{-0} & z^{-3} \\ 1 & z^{-4} & z^{-2} & z^{-0} & z^{-4} & z^{-2} \\ 1 & z^{-5} & z^{-4} & z^{-3} & z^{-2} & z^{-1} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix}$$

$$\begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \end{pmatrix} = -\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & z^5 & z^4 & z^3 & z^2 & z^1 \\ 1 & z^4 & z^2 & z^0 & z^4 & z^2 \\ 1 & z^3 & z^0 & z^3 & z^0 & z^3 \\ 1 & z^2 & z^4 & z^0 & z^2 & z^4 \\ 1 & z^1 & z^2 & z^3 & z^4 & z^5 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix}$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Rücktransformation: $\boldsymbol{GF}(7)$, $z = 5$, $a(x) = 2 + x + 3x^2 + 6x^3 + 5x^5$

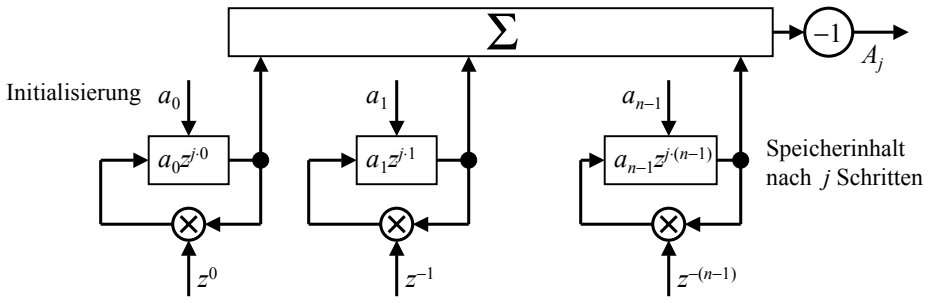
$$\begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \end{pmatrix} = -\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \\ 3 \\ 6 \\ 0 \\ 5 \end{pmatrix} = -\begin{pmatrix} 3 \\ 2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$\mathbf{A} = (4,5,0,0,0,0) \quad \bullet\!\!-\!\!\circ \quad \mathbf{a} = (2,1,3,6,0,5)$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

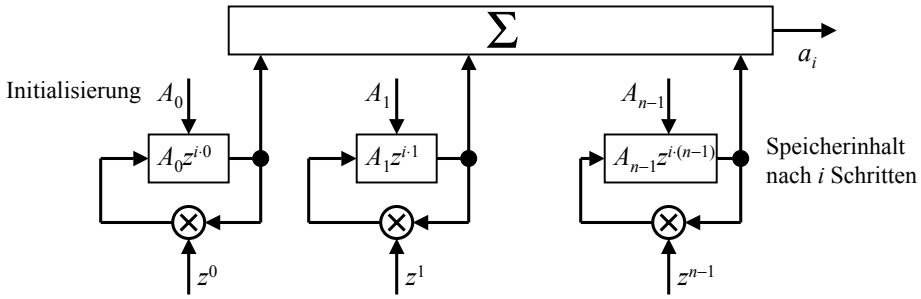
- Schieberegisterschaltung für die DFT: $A_j = -\sum_{i=0}^{n-1} a_i \, z^{-i \cdot j}$



Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Schieberegisterschaltung für die IDFT: $a_i = \sum_{j=0}^{n-1} A_j \, z^{i \cdot j}$



Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- **Faltungssatz** der DFT

  gegeben: Polynome $a(x)$, $b(x)$, $c(x)$ vom Grad $\leq n-1 = p^m - 2$ mit Koeffizienten aus $\boldsymbol{GF}(p^m)$, z = primitives Element von $\boldsymbol{GF}(p^m)$:

  x ist Element aus $\boldsymbol{GF}(p^m) \Rightarrow x^n = x^0 = 1 \Rightarrow$ Rechnung modulo $x^n - 1$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Produkt zweier Polynome: $a(x) \cdot b(x) = c(x)$

$$(a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) \cdot (b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}) = (c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) \quad (4.16)$$

$$c_0 = b_0 \cdot a_0 + b_1 a_{n-1} + b_2 a_{n-2} + \ldots + b_{n-1} a_1$$
$$c_1 = b_0 \cdot a_1 + b_1 a_0 + b_2 a_{n-1} + \ldots + b_{n-1} a_2$$
$$\vdots$$
$$c_i = \sum_{j=0}^{n-1} b_j \cdot a_{j-i \bmod n} \quad (4.17)$$

Produkt zweier Polynome entspricht **zyklischer Faltung** der Koeffizienten:

$$\mathbf{a} * \mathbf{b} \quad \Leftrightarrow \quad a(x) \cdot b(x) \bmod (x^n - 1) \quad (4.18)$$

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- Faltungssatz:

$$a(x) \cdot b(x) \bmod (x^n - 1) \quad \circ\!\!-\!\!\bullet \quad -A_j \cdot B_j \quad (4.19)$$
$$a_i \cdot b_i \quad \circ\!\!-\!\!\bullet \quad A(x) \cdot B(x) \bmod (x^n - 1) \quad (4.20)$$

mit $a(x) \circ\!\!-\!\!\bullet A(x)$, $b(x) \circ\!\!-\!\!\bullet B(x)$

Beweis von (4.19):

$$c(x) = a(x) \cdot b(x) + \gamma(x) \cdot (x^n - 1)$$
$$C_j = -c(z^{-j}) = -\underbrace{a(z^{-j})}_{-A_j} \cdot \underbrace{b(z^{-j})}_{-B_j} - \gamma(z^{-j}) \cdot \underbrace{(z^{-jn} - 1)}_{=1}$$

■

Nachrichtentechnik 4

4 Algebraische Grundbegriffe für Codes

- **Verschiebungssatz** der DFT:

$$x \cdot a(x) \bmod (x^n - 1) \quad \circ\!\!-\!\!\bullet \quad z^{-j} \cdot A_j \qquad (4.21)$$

$$z^i \cdot a_i \quad \circ\!\!-\!\!\bullet \quad x \cdot A(x) \bmod (x^n - 1) \qquad (4.22)$$

mit $a(x) \quad \circ\!\!-\!\!\bullet \quad A(x)$

Beweis durch Einsetzen von $b(x) = x$ bzw. $B(x) = x$ in den Faltungssatz

Nachrichtentechnik 4

5 Blockcodes

- Reed-Solomon- und Bose-Chaudhuri-Hocquenghem-Codes
  - RS- und BCH-Codes ca. 1960 entwickelt
  - geschlossene analytische Konstruktion
  - Mindestdistanz kann vorgegeben werden (Gewichtsverteilung ist bekannt)
  - Singleton-Schranke für RS-Codes mit Gleichheitszeichen erfüllt
  - sehr leistungsfähig und von großer praktischer Bedeutung
    - Kommunikation mit Raumfahrzeugen
    - CD (Compact Disk), Mobilfunk

Nachrichtentechnik 4
5 Blockcodes

- Reed-Solomon-Codes
  - Fundamentalsatz der linearen Algebra:

    Ein Polynom $A(x) = A_0 + A_1\,x + A_2\,x^2 + \ldots + A_{k-1}\,x^{k-1}$ vom Grad $k-1$ mit Koeffizienten $A_i \in \boldsymbol{GF}(p^m)$ und $A_{k-1} \neq 0$ hat höchstens $k-1$ verschiedene Nullstellen.
  - Beweis: Darstellung des Polynoms durch Linearfaktoren:

$$A(x) = A_{k-1} \cdot \prod_{i=1}^{k-1} (x - x_i) \qquad (4.23)$$

Nachrichtentechnik 4
5 Blockcodes

- Satz zum Mindestgewicht von Vektoren:

Gegeben: $A(x) = A_0 + A_1\,x + A_2\,x^2 + \ldots + A_{k-1}\,x^{k-1}$ mit Koeffizienten $A_i \in \boldsymbol{GF}(p^m)$

$$\text{grad}\,A(x) = k - 1 \leq n - d \qquad (4.24)$$

$$A(x) \bullet\!\!-\!\!\circ\; a(x) \quad \Leftrightarrow \quad \mathbf{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$$

$$\Rightarrow \; w_H(\mathbf{a}) \geq d \qquad (4.25)$$

Beweis:

(4.13): Nullstellen von $A(z^i)$ korrespondieren zu Elementen $a_i = 0$

$\Rightarrow$ Anzahl der Stellen $\neq 0$: $n - (k-1) \geq d$ (s.o.)

Nachrichtentechnik 4
5 Blockcodes

- Definition der Reed-Solomon-Codes:

Gegeben: z ist primitives Element aus $\boldsymbol{GF}(p^m)$.

Ein RS-Code $\mathcal{C}$ mit der Dimension $k = p^m - d$ und Mindestdistanz $d = n - k + 1$ ist durch alle Codewörter $\mathbf{a} = (a_0, a_1, a_2, \ldots, a_{n-1})$ der Länge $n = p^m - 1$ bestimmt, für die gilt:

$$a_i = A(z^i) \quad \text{mit} \quad \text{grad}\, A(x) \le k - 1 = n - d \tag{4.26}$$

$$\mathbf{a} = (a_0, a_1, a_2, \ldots, a_{n-1}) \quad \multimap \quad \mathbf{A} = (A_0, A_1, A_2, \ldots, A_{k-1}, \underbrace{0,0, \ldots, 0}_{d-1 \text{ Prüffrequenzen}})$$

Nachrichtentechnik 4
5 Blockcodes

- RS-Codes erfüllen die Singleton-Schranke $d_{\min} \le 1 + (n - k)$

  mit Gleichheit: $\boxed{n - k = d_{\min} - 1}$ (4.27)

  günstigster Fall: $d_{\min}$ ist ungerade $\Rightarrow$ $t = (d_{\min} - 1)/2$

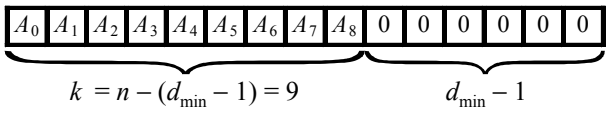
  $$\boxed{n - k = 2t} \tag{4.28}$$

  $\Rightarrow$ Anzahl erkennbarer und korrigierbarer Fehler einstellbar

- Beispiel:
  - Auswahl des Galois-Feldes $\boldsymbol{GF}(p^m)$: $p = 2$, $m = 4$ $\Rightarrow$ $\boldsymbol{GF}(2^4)$
  - Codewortlänge: $n = p^m - 1 = 16 - 1 = 15$
  - Zahl korrigierbarer Symbole: $t = 3$ $\Rightarrow$ $n - k = d_{\min} - 1 = 6$

Nachrichtentechnik 4
5 Blockcodes

- Codewort im Frequenzbereich:



- $A_j \in \{0, 1, z, z+1, z^2, z^2+1, z^2+z, z^2+z+1,$
  $z^3, z^3+1, z^3+z, z^3+z+1, z^3+z^2, z^3+z^2+1, z^3+z^2+z, z^3+z^2+z+1\}$
- Anzahl von Informationsstellen: $k = 9$
- Anzahl von Informationsbits: $k \cdot m = 9 \cdot 4 = 36$
- Anzahl von Codewortstellen: $n = 15$
- Anzahl von Codewortbits: $n \cdot m = 15 \cdot 4 = 60$

Nachrichtentechnik 4
5 Blockcodes

- $\Rightarrow$ hexadezimaler (15,9)-RS-Code = binärer (60,36)-RS-Code
- Korrekturfähigkeit: $t = 3$ hexadezimale Symbole

  $\Rightarrow$ maximal $t_{b,max} = 3 \cdot 4 = 12$ korrigierbare Bits

  $\Rightarrow$ minimal $t_{b,min} = 3 \cdot 1 = 3$ korrigierbare Bits
- Beispiele für Fehlervektoren in binärer Schreibweise

  $\mathbf{f}$ = (0000 0000 0000 1111 1111 1111 0000 0000 0000 0000
  0000 0000 0000 0000 0000) $\Rightarrow$ korrigierbar

  $\mathbf{f}$ = (0000 0000 0001 1111 1111 1110 0000 0000 0000 0000
  0000 0000 0000 0000 0000) $\Rightarrow$ nicht korrigierbar

  $\mathbf{f}$ = (0100 0000 0000 0000 0001 0000 0000 0100 0000 0000
  0000 0000 0000 0010 0000) $\Rightarrow$ nicht korrigierbar

- 3 Einzelfehler und 9 direkt aufeinanderfolgende Fehler korrigierbar

- Büschelfehler korrigierbar bis zu einer Länge von

$$t_{b,\text{Büschel}} = m\,(t-1)+1 = m\;(d-3)/2+1 \quad \text{(bit)} \qquad (4.29)$$

- Coderate:

$$R_C = \frac{k}{n} = \frac{n-(d-1)}{n} = 1-\frac{d-1}{n} \qquad (4.30)$$

  - Beispiel: $k / n = 9 / 15 = 60\ \%$

- Generatorpolynom
  - Codewort im Frequenzbereich: $A_j = 0$ für $j = k \ldots n-1$
  - DFT: $A_j = -a(z^{-j})$
  - jedes Codewortpolynom besitzt Nullstellen:

    $a(z^{-j}) = 0$ für $j = k \ldots n-1$
  - Produkt aller Linearfaktoren, die sich aus den Nullstellen ergeben:

$$g(x) = \prod_{j=k}^{n-1}(x - z^{-j}) = \prod_{j=1}^{n-k}(x - z^{j}) \qquad (4.31)$$

  - jedes Codewortpolynom lässt sich darstellen als: $a(x) = u(x) \cdot g(x)$
    $\Rightarrow$ $g(x)$ ist das Generatorpolynom

Nachrichtentechnik 4
5 Blockcodes

- Prüfpolynom
  - Das Prüfpolynom enthält alle anderen von 0 verschiedenen Nullstellen:

$$h(x) = \prod_{j=0}^{k-1}(x - z^{-j}) = \prod_{j=n-k+1}^{n}(x - z^{j}) \qquad (4.32)$$

  - Beweis:

$$a(x)\cdot h(x) = u(x)\cdot g(x)\cdot h(x)$$
$$= u(x)\cdot\prod_{i=0}^{n-1}(x - z^{i}) = u(x)\cdot(x^{n}-1) = 0 \qquad \bmod (x^{n}-1)$$

  - $\text{grad}(g(x)) = n - k$, $\text{grad}(u(x)) = k - 1$, $\text{grad}(g(x)\cdot u(x)) = n - 1$

    $\text{grad}(h(x)) = k$

Nachrichtentechnik 4
5 Blockcodes

- Beispiel: (6,2)-RS-Code über $\boldsymbol{GF}(7)$ mit $z = 5$

$$g(x) = \prod_{i=2}^{5}(x - 5^{-i}) = \prod_{i=1}^{4}(x - 5^{i})$$
$$= (x-5)(x-4)\cdot(x-6)(x-2)$$
$$= (6+5x+x^{2})\cdot(5+6x+x^{2}) = 2+5x+6x^{2}+4x^{3}+x^{4}$$

$$h(x) = \frac{x^{n}-1}{g(x)} \qquad (4.33)$$

$$h(x) = \frac{x^{6}-1}{2+5x+6x^{2}+4x^{3}+x^{4}} = x^{2}+3x+3 = (x-1)(x-3)$$

Nachrichtentechnik 4
5 Blockcodes

- Generatormatrix (Codierung zyklischer Codes): $\mathbf{a} = \mathbf{u} \cdot \mathbf{G}$

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 \\ 0 & 0 & \cdots & 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix}$$

  - Beispiel:

$$\mathbf{G} = \begin{pmatrix} 2 & 5 & 6 & 4 & 1 & 0 \\ 0 & 2 & 5 & 6 & 4 & 1 \end{pmatrix}$$

Nachrichtentechnik 4
5 Blockcodes

- Systematisierung

  erste Zeile durch Summe der Zeilen ersetzen:

$$\mathbf{G}_1 = \begin{pmatrix} 2 & 0 & 4 & 3 & 5 & 1 \\ 0 & 2 & 5 & 6 & 4 & 1 \end{pmatrix}$$

  alle Elemente mit 4 multiplizieren:

$$\mathbf{G}_{\text{syst}} = \begin{pmatrix} 1 & 0 & 2 & 5 & 6 & 4 \\ 0 & 1 & 6 & 3 & 2 & 4 \end{pmatrix}$$

Nachrichtentechnik 4
5 Blockcodes

- Prüfmatrix, 1. Version

$$\mathbf{H}_1 = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 \\ 0 & 0 & \dots & 0 & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 \end{pmatrix}$$

$$\mathbf{H}_1 = \begin{pmatrix} 1 & 3 & 3 & 0 & 0 & 0 \\ 0 & 1 & 3 & 3 & 0 & 0 \\ 0 & 0 & 1 & 3 & 3 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 \end{pmatrix}$$

Nachrichtentechnik 4
5 Blockcodes

- Prüfmatrix, 2. Version: $\mathbf{G} = [\mathbf{I}_k \; \mathbf{P}] \;\Rightarrow \mathbf{H}_2 = [-\mathbf{P}^T \; \mathbf{I}_{n-k}]$

$$\mathbf{H}_2 = \begin{pmatrix} -2 & -6 & 1 & 0 & 0 & 0 \\ -5 & -3 & 0 & 1 & 0 & 0 \\ -6 & -2 & 0 & 0 & 1 & 0 \\ -4 & -4 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 1 & 0 & 0 & 0 \\ 2 & 4 & 0 & 1 & 0 & 0 \\ 1 & 5 & 0 & 0 & 1 & 0 \\ 3 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- Prüfmatrix, 3. Version: direkte Auswertung der Prüfgleichungen

$$A_j = -a(z^{-j}) = 0 \qquad \text{für} \qquad j = k \dots n-1$$
$$= -\sum_{i=0}^{n-1} a_i \cdot z^{-ij} \qquad \text{für} \qquad j = k \dots n-1$$

$$A_k = -a_0 \cdot z^0 - a_1 z^{-k} - a_2 z^{-2k} - \dots - a_{n-1} z^{-(n-1)k}$$
$$A_{k+1} = -a_0 \cdot z^0 - a_1 z^{-(k+1)} - a_2 z^{-2(k+1)} - \dots - a_{n-1} z^{-(n-1)(k+1)}$$
$$\dots$$

Nachrichtentechnik 4
5 Blockcodes

- Darstellung in Matrixform:

$$\underbrace{-\begin{pmatrix} 1 & z^{-k} & z^{-2k} & \dots & z^{-(n-1)k} \\ 1 & z^{-(k+1)} & z^{-2(k+1)} & \dots & z^{-(n-1)(k+1)} \\ 1 & z^{-(k+2)} & z^{-2(k+2)} & \dots & z^{-(n-1)(k+2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & z^{-(n-1)} & z^{-2(n-1)} & \dots & z^{-(n-1)^2} \end{pmatrix}}_{\mathbf{H}_3} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (4.34)$$

- Beispiel:

$$-\mathbf{H}_3 = \begin{pmatrix} 1 & z^{-2} & z^{-4} & z^{0} & z^{-2} & z^{-4} \\ 1 & z^{-3} & z^{0} & z^{-3} & z^{0} & z^{-3} \\ 1 & z^{-4} & z^{-2} & z^{0} & z^{-4} & z^{-2} \\ 1 & z^{-5} & z^{-4} & z^{-3} & z^{-2} & z^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix}$$

Nachrichtentechnik 4
5 Blockcodes

- Syndromberechnung
  - Empfangssignal: $\mathbf{r} = \mathbf{a} + \mathbf{f} \quad \circ\!\!-\!\!\bullet \quad \mathbf{R} = \mathbf{A} + \mathbf{F}$ (4.35)

    bzw. $r(x) = a(x) + f(x) \quad \circ\!\!-\!\!\bullet \quad R(x) = A(x) + F(x)$ (4.36)
  - Syndrom: Empfangsvektor im Frequenzbereich an den Prüffrequenzen

$$A(x) = A_0x^0 + A_1x^1 + \dots + A_{k-1}x^{k-1} \qquad (4.37)$$

$$F(x) = F_0x^0 + F_1x^1 + \dots + F_{k-1}x^{k-1} + F_kx^k + \dots + F_{n-1}x^{n-1} \qquad (4.38)$$

$$R(x) = R_0x^0 + R_1x^1 + \dots + R_{k-1}x^{k-1} + \underbrace{F_kx^k + \dots + F_{n-1}x^{n-1}}_{\text{Syndromkoeffizienten}} \qquad (4.39)$$

mit $R_j = A_j + F_j$ (4.40)

$$\boxed{S(x) = S_0x^0 + \dots + S_{n-k-1}x^{n-k-1} = F_kx^0 + \dots + F_{n-1}x^{n-k-1}} \qquad (4.41)$$

Nachrichtentechnik 4
5 Blockcodes

- Syndrom als Vektor: $\mathbf{S} = (S_0, S_1, \ldots, S_{n-k-1})$
- Syndrom als Multiplikation mit der Prüfmatrix:

$$\mathbf{S} = \mathbf{r} \cdot \mathbf{H}_3^{\mathrm{T}} \quad \Leftrightarrow \quad \mathbf{S}^{\mathrm{T}} = \mathbf{H}_3 \cdot \mathbf{r}^{\mathrm{T}} \tag{4.42}$$

$$\begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ \vdots \\ S_{n-k-1} \end{pmatrix} = - \begin{pmatrix} 1 & z^{-k} & z^{-2k} & \cdots & z^{-(n-1)k} \\ 1 & z^{-(k+1)} & z^{-2(k+1)} & \cdots & z^{-(n-1)(k+1)} \\ 1 & z^{-(k+2)} & z^{-2(k+2)} & \cdots & z^{-(n-1)(k+2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & z^{-(n-1)} & z^{-2(n-1)} & \cdots & z^{-(n-1)^2} \end{pmatrix} \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ \vdots \\ r_{n-1} \end{pmatrix} \tag{4.43}$$

Nachrichtentechnik 4
5 Blockcodes

- Codierung von RS-Codes
  - Erweiterung der Definition (4.26):

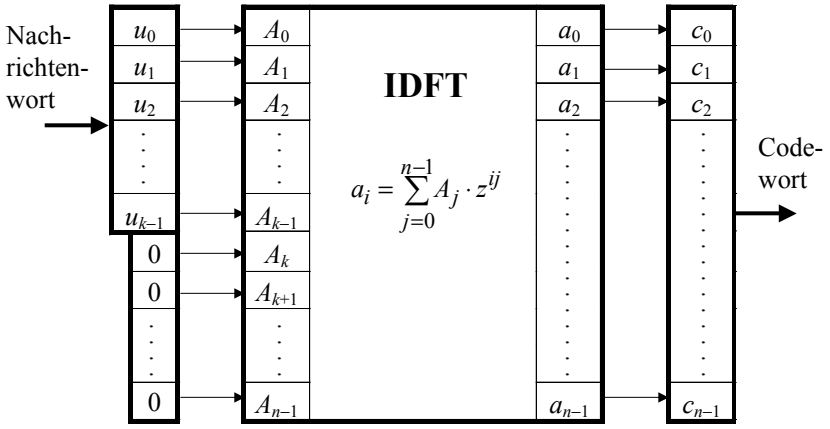
$$\mathcal{C} = \{\mathbf{a} \mid a_i = A(z^i) \text{ mit } A_j = 0 \text{ für } n-k \text{ zyklisch aufeinander folgene Stellen } j\} \tag{4.44}$$

  - **Methode 1**: Codierung im Frequenzbereich

    Transformation der Nachrichtenstellen mit der IDFT

$$\mathbf{A} = (u_0, u_1, u_2, \ldots, u_{k-1}, 0, 0, \ldots, 0) \circ\!\!-\!\!\bullet\; \mathbf{a} = (a_0, a_1, a_2, \ldots, a_{n-1}) \tag{4.45}$$

Nachrichtentechnik 4
5 Blockcodes



Nachrichtentechnik 4
5 Blockcodes

- Beispiel: (6,2)-RS-Code über $GF(7)$ mit $z = 5$

$n = p - 1 = 7 - 1 = 6, \quad k = 2 \Rightarrow \text{grad}\,(A(x)) \le k - 1 = 1$

$A(x) = 3 + 3x \qquad a_i = A(x = z^i)$

$a_0 = A(x = z^0 = 5^0 = 1) = A_0 + A_1 z^0 = 3 + 3 \cdot 1 = 6$

$a_1 = A(x = z^1 = 5^1 = 5) = A_0 + A_1 z^1 = 3 + 3 \cdot 5 = 4$

$a_2 = A(x = z^2 = 5^2 = 4) = A_0 + A_1 z^2 = 3 + 3 \cdot 4 = 1$

$a_3 = A(x = z^3 = 5^3 = 6) = A_0 + A_1 z^3 = 3 + 3 \cdot 6 = 0$

$a_4 = A(x = z^4 = 5^4 = 2) = A_0 + A_1 z^4 = 3 + 3 \cdot 2 = 2$

$a_5 = A(x = z^5 = 5^5 = 3) = A_0 + A_1 z^5 = 3 + 3 \cdot 3 = 5$

$\mathbf{A} = (3,3,0,0,0,0) \quad \circ\!\!-\!\!\bullet \quad \mathbf{a} = (6,4,1,0,2,5)$

Nachrichtentechnik 4
5 Blockcodes

$B(x) = 1 + 1x$

$\mathbf{B} = (1,1,0,0,0,0) \quad \bullet\!\!-\!\!\circ \quad \mathbf{b} = (2,6,5,0,3,4)$

$d_H(\mathbf{a},\mathbf{b}) = d_H((6,4,1,0,2,5),(2,6,5,0,3,4)) = 5$

zum Vergleich: $d_{min} = n - k + 1 = 6 - 2 + 1 = 5$

- **Methode 2**: Unsystematische Codierung im Zeitbereich
  - Multiplikation von Informations- und Generatorpolynom

$$a(x) = u(x) \cdot g(x) \tag{4.46}$$

Nachrichtentechnik 4
5 Blockcodes

- **Methode 3**: Systematische Codierung im Zeitbereich
  - Multiplikation des Informationspolynoms mit x^{n-k} :

$$u(x) \cdot x^{n-k} = u_0 x^{n-k} + u_1 x^{n-k+1} + \ldots + u_{k-1} x^{n-1} \tag{4.47}$$

  - Division von $u(x) \cdot x^{n-k}$ durch $g(x)$:

$$u(x) \cdot x^{n-k} = q(x) \cdot g(x) + r(x) \tag{4.48}$$

Ergebnis: $r(x) = r_0 + r_1 x + \ldots + r_{n-k-1} x^{n-k-1}$ (4.49)

  - Auflösen nach dem Codewort:

$$-r(x) + u(x) \cdot x^{n-k} = q(x) \cdot g(x) = a(x) \tag{4.50}$$

$$\mathbf{a} = (-r_0, -r_1, -r_2, \ldots, -r_{n-k-1}, u_0, u_1, u_2, \ldots, u_{k-1}) \tag{4.51}$$

Nachrichtentechnik 4
5 Blockcodes

- Beispiel: (6,2)-RS-Code über $GF(7)$ mit $z = 5$

$\mathbf{u} = (3,4) \Rightarrow u(x) = 3 + 4x \Rightarrow u(x) \cdot x^{n-k} = 3x^4 + 4x^5$

Division durch $g(x) = 2 + 5x + 6x^2 + 4x^3 + x^4$:

$$(4x^5 + 3x^4) \div (1x^4 + 4x^3 + 6x^2 + 5x + 2) = 4x + 1 + \frac{r(x)}{g(x)}$$

$$\begin{array}{r} -(4x^5 + 2x^4 + 3x^3 + 6x^2 + 1x) \\ \hline 1x^4 + 4x^3 + 1x^2 + 6x \\ -(1x^4 + 4x^3 + 6x^2 + 5x + 2) \\ \hline 2x^2 + 1x + 5 = r(x) \end{array}$$

$$-r(x) + u(x)\,x^{n-k} = 2 + 6x + 5x^2 + 3x^4 + 4x^5 \Rightarrow \mathbf{a} = (\underbrace{2, 6, 5, 0}_{-\mathbf{r}}, \underbrace{3, 4}_{\mathbf{u}})$$

Nachrichtentechnik 4
5 Blockcodes

- Alternative: Codierung mit systematischer Generatormatrix:

$\mathbf{u} = (3,4)$

$$\mathbf{b} = \mathbf{u} \cdot \mathbf{G}_{\text{syst}} = (3, 4) \cdot \begin{pmatrix} 1 & 0 & 2 & 5 & 6 & 4 \\ 0 & 1 & 6 & 3 & 2 & 4 \end{pmatrix} = (3, 4, 2, 6, 5, 0)$$

- Beispiel: (7,3)-RS-Code über $GF(2^3)$
  - » Codewortlänge: $n = p^m - 1 = 8 - 1 = 7$
  - » Zahl korrigierbarer Symbole: $t = 2 \Rightarrow n - k = 4,\ k = 3$
  - » primitives Polynom: $p(x) = 1 + x + x^3$
  - » primitives Element: $1 + z + z^3 = 0$

Nachrichtentechnik 4
5 Blockcodes

» Erweiterungskörper:

$0 = 0$	$z^1 = z$	$z^3 = 1+z$	$z^5 = 1+z+z^2$
$z^0 = 1$	$z^2 = z^2$	$z^4 = z+z^2$	$z^6 = 1+z^2$

» Generatorpolynom:

$$g(x) = (x - z)\,(x - z^2)\,(x - z^3)\,(x - z^4)$$
$$= (x^2 + xz^4 + z^3)\,(x^2 + xz^6 + 1)$$
$$= x^4 + x^3z^3 + x^2 + xz + z^3$$

» Prüfpolynom:

$$h(x) = (x - z^5)\,(x - z^6)\,(x - z^7)$$
$$= x^3z^3 + x^2z^3 + xz^2 + z^4$$

Nachrichtentechnik 4
5 Blockcodes

» Codierung von: $\mathbf{u} = (1, 1, 1) \Rightarrow u(x) = 1 + x + x^2$

$$\Rightarrow u(x) \cdot x^{n-k} = x^4 + x^5 + x^6$$

Division durch $g(x) = x^4 + x^3z^3 + x^2 + xz + z^3$:

$$(x^6 + x^5 + x^4) \div (x^4 + x^3z^3 + x^2 + xz + z^3) = x^2 + xz + z^4 + \frac{r(x)}{g(x)}$$

$$+ (x^6 + x^5z^3 + x^4 + x^3z + x^2z^3)$$
$$x^5z + x^3z + x^2z^3$$
$$+ (x^5z + x^4z^4 + x^3z + x^2z^2 + xz^4)$$
$$x^4z^4 + x^2z^5 + xz^4$$
$$+ (x^4z^4 + x^3 + x^2z^4 + xz^5 + 1)$$
$$x^3 + x^2 + x + 1 = r(x)$$

$$-r(x) + u(x)\,x^{n-k} = 1+x+x^2+x^3+x^4+x^5+x^6 \Rightarrow \mathbf{a} = (1,1,1,1,1,1,1)$$

Nachrichtentechnik 4
5 Blockcodes

» Generatormatrix:

$$\mathbf{G} = \begin{pmatrix} z^3 & z & 1 & z^3 & 1 & 0 & 0 \\ 0 & z^3 & z & 1 & z^3 & 1 & 0 \\ 0 & 0 & z^3 & z & 1 & z^3 & 1 \end{pmatrix}$$

- Gewichtsfunktion von RS-Codes (allgemein für MDS-Codes, $q = p^m$):

$$A(z) = \sum_{i=0}^{n} A_i \, z^i \tag{4.52}$$

$$A_i = \begin{cases} 1 & \text{für } i = 0 \\ 0 & \text{für } 1 \le i < d \end{cases} \tag{4.53}$$

$$A_i = \binom{n}{i}(q-1)\sum_{j=0}^{i-d}(-1)^j \binom{i-1}{j} q^{i-d-j} \quad \text{für } i \ge d \tag{4.54}$$

Nachrichtentechnik 4
5 Blockcodes

- Beispiel für eine Gewichtsverteilung: (7,3)-RS-Code über $\boldsymbol{GF}(2^3)$
  - Mindestdistanz: $d = (n - k) + 1 = 5$

$$A_0 = 1$$

$$A_1 = A_2 = A_3 = A_4 = 0$$

$$A_5 = \binom{7}{5} \cdot 7 \cdot 1 = \frac{7!}{5! \cdot (7-5)!} \cdot 7 = 21 \cdot 7 = 147$$

$$A_6 = \binom{7}{6} \cdot 7 \cdot \left(8 - \binom{5}{1} \cdot 1\right) = \frac{7!}{6! \cdot (7-6)!} \cdot (8-5) = 147$$

$$A_7 = \binom{7}{7} \cdot 7 \cdot \left(8^2 - \binom{6}{1} \cdot 8 + \binom{6}{2} \cdot 1\right) = 7 \cdot (64 - 48 + 15) = 217$$

Nachrichtentechnik 4
5 Blockcodes

- Gewichtsfunktion:
  $A(z) = 1 + 147z^5 + 147z^6 + 217z^7$
- Kontrolle:
  $\sum_{i=0}^{n} A_i = 1 + 147 + 147 + 217 = 512 = q^3 = 8^3$

- RS-Codes sind besonders geeignet zur Korrektur von Bündelfehlern
- RS-Codes können für Einzelfehler ineffizient sein, da immer ganze Symbole korrigiert werden müssen, wobei eine entsprechende Redundanz notwendig ist

Nachrichtentechnik 4
5 Blockcodes

- Decodierung von RS-Codes
  - algebraische Decodierung
  - Tabellen-Decodierung: benötigter Speicherplatz
- Algebraische Decodierung
  - Vorgehensweise
    - Berechnung des Syndroms
    - Berechnung der Lage der Fehlerstellen (Schlüsselgleichung)
    - Berechnung (des Inhalts) des Fehlervektors, da RS-Codes keine binären Codes sind
    - Korrektur der Fehler

Nachrichtentechnik 4
5 Blockcodes

- Berechnung der Fehlerstellen
  - Fehlerstellenpolynom: Nullstellen markieren Fehlerstellen

$c(x) \circ\!\!-\!\!\bullet\; C(x)$ (4.55)

Definition: $c_i = 0$ für $f_i \neq 0$

$\Rightarrow \boxed{c_i \cdot f_i = 0 \quad \text{für} \quad i = 0, 1, \ldots, n-1}$ (4.56)

jede Fehlerstelle $c_i = 0$ erzeugt eine Nullstelle / einen Linearfaktor in $C(x)$:

$$C(x) = \prod_{i, f_i \neq 0} (x - z^i) \quad (4.57)$$

grad $(C(x))$ = Anzahl der Fehlerstellen e

Nachrichtentechnik 4
5 Blockcodes

- DFT des Produkts $c_i \cdot f_i$:

$\boxed{c_i \cdot f_i = 0 \;\circ\!\!-\!\!\bullet\; C(x) \cdot F(x) = 0 \mod (x^n - 1)}$ (4.58)

$C(x) \cdot F(x)$ besitzt alle möglichen Nullstellen

Annahme: $e \leq t = \dfrac{n-k}{2}$

Fehlerstellenpolynom:

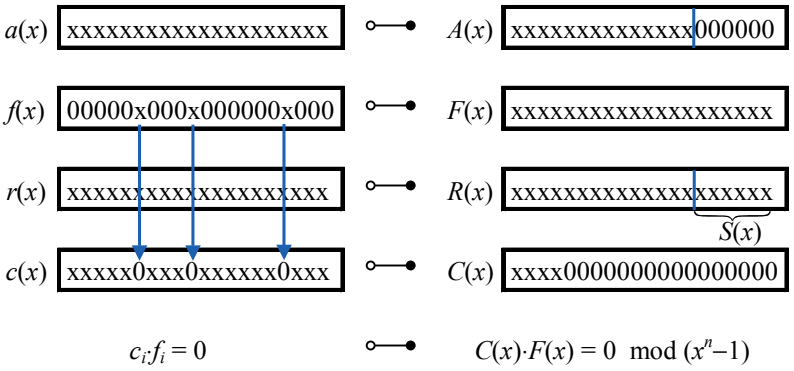
$$C(x) = C_0 + C_1 x + \ldots + C_e x^e \quad (4.59)$$

Wahl von C_0 : $C_0 = 1$

$$C(x) = \prod_{i, f_i \neq 0} (1 - z^{-i} \cdot x) = 1 + C_1 x + \ldots + C_e x^e \quad (4.60)$$

Nachrichtentechnik 4
5 Blockcodes

- Fehlerstellenpolynom



$c_i f_i = 0$ ⟷ $C(x)\cdot F(x) = 0 \mod (x^n - 1)$

Nachrichtentechnik 4
5 Blockcodes

- Bestimmung der Koeffizienten C_i : Annahme: $e = t$
- Darstellung von $C(x) \cdot F(x) = 0 \mod (x^n - 1)$ als Gleichungssystem:

$$
\begin{array}{llllll}
C_0F_0 & + C_1F_{n-1} & + C_2F_{n-2} & +\ldots+ & C_tF_{n-t} & = 0 \\
C_0F_1 & + C_1F_0 & + C_2F_{n-1} & +\ldots+ & C_tF_{n-t+1} & = 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
C_0F_{n-t-1} & + C_1F_{n-t-2} & + C_2F_{n-t-3} & +\ldots+ & C_tF_{n-2t-1} & = 0 \\
C_0F_{n-t} & + C_1F_{n-t-1} & + C_2F_{n-t-2} & +\ldots+ & C_tF_{n-2t} & = 0 \\
C_0F_{n-t+1} & + C_1F_{n-t} & + C_2F_{n-t-1} & +\ldots+ & C_tF_{n-2t+1} & = 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
C_0F_{n-2} & + C_1F_{n-3} & + C_2F_{n-4} & +\ldots+ & C_tF_{n-t-2} & = 0 \\
C_0F_{n-1} & + C_1F_{n-2} & C_2F_{n-3} & +\ldots+ & C_tF_{n-t-1} & = 0
\end{array}
\qquad (4.61)
$$

Nachrichtentechnik 4
5 Blockcodes

- Rahmen in (4.61):
  - t Gleichungen und t Unbekannte
  - Koeffizienten des Fehlerstellenpolynoms sind bekannt:

$$S_0 = F_{n-2t}\,, \quad S_1 = F_{n-2t+1}\,, \ \ldots\ , \quad S_{2t-1} = F_{n-1}$$

$$\Rightarrow \quad \begin{array}{lllllll} C_0S_t & + & C_1S_{t-1} & + & C_2S_{t-2} & +\ldots+ & C_tS_0 = 0 \\ C_0S_{t+1} & + & C_1S_t & + & C_2S_{t-1} & +\ldots+ & C_tS_1 = 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ C_0S_{2t-1} & + & C_1S_{2t-2} & + & C_2S_{2t-3} & +\ldots+ & C_tS_{t-1} = 0 \end{array} \qquad (4.62)$$

= zyklische Faltung: $\sum_{i=0}^{t} C_i \cdot S_{j-i} = 0$ für $j = t,\ldots,2t-1$ (4.63)

Nachrichtentechnik 4
5 Blockcodes

- Alternative Darstellung durch einfache Polynommultiplikation:

$$\begin{array}{ll} x^0 & C_0S_0 \\ x^1 & C_0S_1 + C_1S_0 \\ \vdots & \vdots \quad \ddots \\ x^{t-1} & C_0S_{t-1} + C_1S_{t-2} + \ldots + C_{t-1}S_0 \\ x^t & C_0S_1 + C_1S_{t-1} + C_2S_{t-2} + \ldots + C_tS_0 = 0 \\ x^{t+1} & C_0S_1 + C_1S_t + C_2S_{t-1} + \ldots + C_tS_1 = 0 \\ \vdots & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ x^{2t-1} & C_0S_1 + C_1S_{1t-2} + C_2S_{2t-3} + \ldots + C_tS_{t-1} = 0 \\ x^{2t} & C_1S_{2t-1} + C_2S_{2t-2} + \ldots + C_tS_t = T_0 \\ \vdots & \qquad\qquad\qquad\qquad\quad \ddots \qquad \vdots \qquad \vdots \\ x^{3t-1} & C_tS_{2t-1} = T_{t-1} \end{array} \qquad (4.64)$$

Nachrichtentechnik 4
5 Blockcodes

- Definition des Polynoms $T(x)$, das zur Bestimmung der Fehlerwerte verwendet wird:

$$T(x) = T_0 + T_1 x + \ldots + T_{t-1} x^{t-1} \tag{4.65}$$

- Koeffizientenvergleich $\Rightarrow$ Schlüsselgleichung:

$$C(x) \cdot F(x) = 0 \mod (x^n - 1) = T(x) \cdot (x^n - 1) = T(x) \cdot x^n - T(x) \tag{4.66}$$

- im Allgemeinen ist Anzahl der Fehler unbekannt: $e \neq t$
- Fehler mit kleinem Gewicht sind wahrscheinlicher als Fehler mit großem Gewicht $\Rightarrow$ Annahme: $e \leq t$

Nachrichtentechnik 4
5 Blockcodes

- gesuchte Koeffizienten: $C_1, C_2, \ldots, C_e$
- Zahl der Variablen: e, Zahl der Gleichungen: t
- überbestimmtes Gleichungssystem $\Rightarrow$ unterschiedliche Ansätze für $C(x)$ notwendig

$$\sum_{i=0}^{e} C_i \cdot S_{j-i} = 0 \quad \text{für} \quad j = e, \ldots, 2t-1 \quad \text{für} \quad e = 1,2,\ldots,t \tag{4.67}$$

- Matrixschreibweise:

$$\begin{pmatrix} S_e & S_{e-1} & \cdots & S_1 & S_0 \\ S_{e+1} & S_e & \cdots & S_2 & S_1 \\ \vdots & \vdots & & \vdots & \vdots \\ S_{2t-2} & S_{2t-3} & \cdots & S_{2t-e-1} & S_{2t-e-2} \\ S_{2t-1} & S_{2t-2} & \cdots & S_{2t-e} & S_{2t-e-1} \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \\ \vdots \\ C_{e-1} \\ C_e \end{pmatrix} = \mathbf{0} \quad \text{für} \quad e = 1,2,\ldots,t \tag{4.68}$$

Nachrichtentechnik 4
5 Blockcodes

- Beginn der Suche nach den Koeffizienten des Fehlerstellenpolynoms mit dem wahrscheinlichsten Fehlerereignis $e = 1$, $e = 2$, ...
- Decodierversagen auch möglich, wenn kein Fehlerstellenpolynom mit e Nullstellen gefunden wird
- Lösung der Schlüsselgleichung mit geringem Rechenaufwand:
  - Berlekamp-Massey-Algorithmus
  - Euklid'scher Divisionsalgorithmus

Nachrichtentechnik 4
5 Blockcodes

- Beispiel: (6,2)-RS-Code über $\boldsymbol{GF}(7)$ mit $z = 5$
  - Parameter: $n = 6$, $k = 2$, $d = d_{\mathrm{H,min}} = 5$, $t = 2$
  - Empfangsvektor und Syndrom:

$$\mathbf{r} = (r_0,r_1,r_2,r_3,r_4,r_5) = (1,2,3,1,1,1)$$

$$\mathbf{R} = (R_0,R_1,R_2,R_3,R_4,R_5) = (R_0,R_1,F_2,F_3,F_4,F_5) = (5,0,\underbrace{4,6,6,1}_{\mathbf{S}})$$

$$\mathbf{S} = (F_2,F_3,F_4,F_5) = (S_0,S_1,S_2,S_3) = (4,6,6,1)$$

  - Annahme $e = 1$: $C(x) = C_0 + C_1 x$ Normierung: $C_1 = 1$

$$\begin{pmatrix} S_1 & S_0 \\ S_2 & S_1 \\ S_3 & S_2 \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 6 & 6 \\ 1 & 6 \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Nachrichtentechnik 4
5 Blockcodes

$6\,C_0 + 4 = 0 \quad \Rightarrow \; C_0 = 4$
$6\,C_0 + 6 = 0 \quad \Rightarrow \; C_0 = 6$
$1\,C_0 + 6 = 0 \quad \Rightarrow \; C_0 = 1$

- Widerspruch $\Rightarrow e = 2$:

$C(x) = C_0 + C_1 x + C_2 x^2$ Normierung: $C_2 = 1$

$$\begin{pmatrix} S_2 & S_1 & S_0 \\ S_3 & S_2 & S_1 \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 6 & 6 & 4 \\ 1 & 6 & 6 \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

I: $6\,C_0 + 6\,C_1 + 4 = 0$
II: $1\,C_0 + 6\,C_1 + 6 = 0$
I–II: $5\,C_0 - 2 = 0 \quad \Rightarrow \; C_0 = 2 \cdot 5^{-1} = 6$
II: $6\,C_1 + 5 = 0 \quad \Rightarrow \; C_1 = -5 \cdot 6^{-1} = 5$

Nachrichtentechnik 4
5 Blockcodes

- Fehlerstellenpolynom: $C(x) = 6 + 5\,x + x^2$
- Suche der Nullstellen (Chien search):

$C(x = z^0 = 1) = 6 + 5 + 1 = 5$
$C(x = z^1 = 5) = 6 + 4 + 4 = 0 \Rightarrow$ Nullstelle bei z^1
$C(x = z^2 = 4) = 6 + 6 + 2 = 0 \Rightarrow$ Nullstelle bei z^2
$C(x = z^3 = 6) = 6 + 2 + 1 = 2$
$C(x = z^4 = 2) = 6 + 3 + 4 = 6$
$C(x = z^5 = 3) = 6 + 1 + 2 = 2$

- Fehler in der 1. und 2. Stelle
- Probe: $C(x) = (x - z^1) \cdot (x - z^2) = 6 + 5\,x + x^2$