

Übungspalte 6

Aufgabe 1

zyklischer $[6,3]_2$ -Code mit $G(x) = x^3 + x^2 + 4x + 7$.

a) ges. $H(x) \rightsquigarrow (x^6 - 1) : G(x)$ um $H(x)$ zu finden

$$\begin{array}{r}
 (x^6 - 1) : (x^3 + x^2 + 4x + 7) = x^3 + 6x^2 + 4x + 6 \quad \text{Rest: 0} \\
 - (x^6 + x^5 + 4x^4 + x^3) \\
 \hline
 6x^5 + 3x^4 + 6x^3 + 6 \\
 - (6x^5 + 6x^4 + 3x^3 + 6x^2) \\
 \hline
 4x^4 + 3x^3 + x^2 + 6 \\
 - (4x^4 + 4x^3 + 2x^2 + 4x) \\
 \hline
 6x^3 + 6x^2 + 3x + 6 \\
 - (6x^3 + 6x^2 + 3x + 6) \\
 \hline
 0
 \end{array}$$

$$\Rightarrow H(x) = \underline{x^3 + 6x^2 + 4x + 6}$$

b) $m(x) = 5 + 3x + x^2$

$$\rightsquigarrow c_m(x) = m(x) \cdot G(x)$$

$$\begin{aligned}
 &= (5 + 3x + x^2) \cdot (1 + 4x + x^2 + x^3) \\
 &= 5 + 6x + 5x^2 + 5x^3 \\
 &\quad + 3x + 5x^2 + 3x^3 + 3x^4 \\
 &\quad + 7x^2 + 4x^3 + 7x^4 + x^5 \\
 &= 5 + 2x + 4x^2 + 5x^3 + 4x^4 + x^5
 \end{aligned}$$

$$\rightsquigarrow c_m = \underline{(5, 2, 4, 5, 4, 1)}$$

$n(x) = 2 + 3x + 4x^2$

$$\rightsquigarrow c_n(x) = n(x) \cdot G(x)$$

$$\begin{aligned}
 &= (2 + 3x + 4x^2) \cdot (1 + 4x + x^2 + x^3) \\
 &= 2 + 7x + 2x^2 + 2x^3 \\
 &\quad + 3x + 5x^2 + 3x^3 + 3x^4 \\
 &\quad + 4x^2 + 2x^3 + 4x^4 + 4x^5 \\
 &= 2 + 4x + 4x^2 + 0x^3 + 0x^4 + 4x^5
 \end{aligned}$$

$$\rightsquigarrow c_n = \underline{(2, 4, 4, 0, 0, 4)}$$

c)

Ansatz: $a(x) : G(x) = m(x)$ Rest: $s(x)$

\hookrightarrow wenn $s(x) = 0$, dann ist $a(x)$ ein Codewort und $m(x)$ ist zugehörige Nachricht.

$$a(x) = s + 4x + 4x^2 + 4x^3 + 6x^4 + 3x^5$$

$$\sim (3x^5 + 6x^4 + 4x^3 + 4x^2 + 4x + 5) : (x^3 + x^2 + 4x + 7) = 3x^2 + 3x + 3$$

$$-(3x^5 + 3x^4 + 5x^3 + 3x^2)$$

$$\text{Rest: } 3x + 2$$

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

$\Rightarrow a$ ist kein Codewort vom Code C

$$b(x) = 4x^5 + 6x^3 + x^4 + 5x^5$$

$$\sim (5x^5 + x^4 + 6x^3 + 0x^2 + 5x + 4) : (x^3 + x^2 + 4x + 7) = 5x^2 + 3x + 4$$

$$-(5x^5 + 5x^4 + 6x^3 + 5x^2)$$

$$\text{Rest: } 0$$

$$\begin{array}{r} 3x^4 + 0x^3 + 2x^2 + 5x + 4 \\ -(3x^4 + 3x^3 + 5x^2 + 3x) \\ \hline 4x^3 + 4x^2 + 2x + 4 \\ -(4x^3 + 4x^2 + 2x + 4) \\ \hline 0 \end{array}$$

$\Rightarrow b$ ist Codewort vom Code C und die zugehörige Nachricht ist: (4, 3, 5)

Aufgabe 2

$$\mathbb{F}_8 \text{ mit } \alpha^3 = \alpha + 1 \quad \sim \alpha^4 = \alpha^2 + \alpha, \quad \alpha^5 = \alpha^2 + \alpha + 1, \quad \alpha^6 = \alpha^2 + 1$$

a) zyklischer $[7, 4]_p$ -Code

Ansatz: Wenn $G(x)$ Erzeugerpolynom von C ist, dann gibt es ein $H(x)$, sodass $x^2 - 1 = G(x) \cdot H(x)$

$$\sim (x^2 - 1) : (x^3 + \alpha^4 x^2 + \alpha^4 x + 7) = x^4 + \alpha^4 x^3 + \alpha^2 x^2 + \alpha^4 x + 7$$

$$-(x^2 + \alpha^4 x^6 + \alpha^4 x^5 + \alpha^4)$$

$$\text{Rest: } 0$$

$$\begin{array}{r} \alpha^4 x^6 + \alpha^4 x^5 + x^4 + 7 \\ -(\alpha^4 x^6 + \alpha x^5 + \alpha x^4 + \alpha^4 x^3) \\ \hline \alpha^2 x^5 + \alpha^3 x^4 + \alpha^4 x^3 + 7 \end{array}$$

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

$$\begin{array}{r} \alpha^4 x^4 + \alpha^3 x^3 + \alpha^2 x^2 + 7 \\ -(\alpha^4 x^4 + \alpha x^3 + \alpha x^2 + \alpha^4 x) \end{array}$$

$$\begin{array}{r} x^3 + \alpha^4 x^2 + \alpha^4 x + 7 \\ -(x^3 + \alpha^4 x^2 + \alpha^4 x + 7) \end{array}$$

$$0$$

$$\Rightarrow H(x) = x^4 + (\alpha^2 + \alpha)x^3 + \alpha^2x^2 + (\alpha^2 + \alpha)x + 1$$

\Rightarrow Da $G(x) \cdot H(x) = x^7 - 1$, ist $G(x)$ Erzeugerpolynom von C .

6)

z.z.: $d(C) \geq 3$

PPM: $\begin{pmatrix} 1 & \alpha^2 + \alpha & \alpha^2 & \alpha^2 + \alpha & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 + \alpha & \alpha^2 & \alpha^2 + \alpha & 1 & 0 \\ 0 & 0 & 1 & \alpha^2 + \alpha & \alpha^2 & \alpha^2 + \alpha & 1 \end{pmatrix}$ wobei H eine PPM für C ist.

\rightsquigarrow keine Nullspalte $\Rightarrow d(C) \geq 2$

$\rightsquigarrow d(C) \geq 3$ g.d.w. keine 2 Spaltenvektoren in H lin. abhängig sind.

Wir nennen die Spaltenvektoren $\vec{v}_1, \dots, \vec{v}_7$. Dann gilt offensichtlich

$\vec{v}_1 \neq r \cdot \vec{v}_i \quad \forall i \in \{2, \dots, 7\}$
da die 2. Komponente von \vec{v}_1 0 ist und $r \cdot 0 = 0 \quad \forall r$.
Genauso lässt sich begründen, dass

$$\vec{v}_2 \neq r \cdot \vec{v}_i \quad \forall i \in \{3, \dots, 7\},$$

$$\vec{v}_3 \neq r \cdot \vec{v}_i \quad \forall i \in \{4, \dots, 7\},$$

$$\vec{v}_4 \neq r \cdot \vec{v}_i \quad \forall i \in \{5, \dots, 7\}.$$

Die einzigen Paare an Spaltenvektoren, die dann noch lin. abhängig sein könnten, sind $\langle \vec{v}_3, \vec{v}_4 \rangle, \langle \vec{v}_3, \vec{v}_5 \rangle$ und $\langle \vec{v}_4, \vec{v}_5 \rangle$.

$$\rightsquigarrow \vec{v}_3 = r \cdot \vec{v}_4 : \begin{array}{l} I \quad \alpha^2 = r \cdot (\alpha^2 + \alpha) \rightsquigarrow r = \alpha^2 + \alpha \\ II \quad \alpha^3 + \alpha = r \cdot \alpha^2 \rightsquigarrow r = \alpha^2 \end{array} \quad \square$$

$$\rightsquigarrow \vec{v}_3 = r \cdot \vec{v}_5 : \begin{array}{l} I \quad \alpha^2 = r \cdot 1 \rightsquigarrow r = \alpha^2 \\ II \quad \alpha^3 + \alpha = r \cdot (\alpha^2 + \alpha) \rightsquigarrow r = 1 \end{array} \quad \square$$

$$\rightsquigarrow \vec{v}_4 = r \cdot \vec{v}_5 : \begin{array}{l} I \quad \alpha^3 + \alpha = r \cdot 1 \rightsquigarrow r = \alpha^3 + \alpha \\ II \quad \alpha^2 = r \cdot (\alpha^2 + \alpha) \rightsquigarrow r = \alpha^2 + \alpha \end{array} \quad \square$$

\Rightarrow keine 2 Spaltenvektoren sind lin. abhängig

$\Rightarrow d(C) \geq 3 \quad \square$

$$c) m(x) = (\alpha+1) + \alpha^2x + (\alpha^3+1)x^2 + x^3$$

$$\rightsquigarrow c_m(x) = m(x) \cdot G(x)$$

$$= (\alpha^3 + \alpha^2x + \alpha^6x^2 + x^3) \cdot (1 + \alpha^4x + \alpha^4x^2 + x^3)$$

$$\begin{aligned} &= \alpha^3 + \alpha^2x + \alpha^2x^2 + \alpha^3x^3 \\ &\quad + \alpha^2x + \alpha^6x^2 + \alpha^6x^3 + \alpha^2x^4 \\ &\quad + \alpha^6x^2 + \alpha^3x^3 + \alpha^3x^4 + \alpha^6x^5 \\ &\quad + \alpha^2x^3 + \alpha^4x^4 + \alpha^4x^5 + \alpha^2x^6 \end{aligned}$$

$$= \alpha^3 + \alpha^6x + \alpha^2x^2 + \alpha^2x^3 + \alpha^2x^4 + \alpha^3x^5 + \alpha^2x^6$$

$$\rightsquigarrow c_m = (\alpha+1, \alpha^2+1, 1, \alpha^2, 1, \alpha+1, 1)$$

$$n(x) = \alpha + \alpha x + \alpha^2x^2 + \alpha^2x^3$$

$$\rightsquigarrow c_n(x) = n(x) \cdot G(x)$$

$$= (\alpha + \alpha x + \alpha^2x^2 + \alpha^2x^3) \cdot (1 + \alpha^4x + \alpha^4x^2 + x^3)$$

$$\begin{aligned} &= \alpha + \alpha^5x + \alpha^5x^2 + \alpha x^3 \\ &\quad + \alpha x + \alpha^5x^2 + \alpha^5x^3 + \alpha x^4 \\ &\quad + \alpha^2x^2 + \alpha^6x^3 + \alpha^6x^4 + \alpha^2x^5 \\ &\quad + \alpha^2x^3 + \alpha^6x^4 + \alpha^6x^5 + \alpha^2x^6 \end{aligned}$$

$$= \alpha + \alpha^6x + \alpha^2x^2 + \alpha^2x^3 + \alpha x^4 + \alpha^2x^5 + \alpha^2x^6$$

$$\rightsquigarrow c_n = (\alpha, \alpha^2+1, \alpha^2, \alpha^2, \alpha, 1, \alpha^2)$$

Aufgabe 3 Ffg mit $\alpha^3 = \alpha + 1$ und zyklischer $[7,4]_F$ -Code C mit $G(x) = x^3 + \alpha^4x^2 + \alpha^4x + 1$

$$a) a(x) = \alpha^2x + \alpha^2x^2 + \alpha x^3 + \alpha^2x^4 + x^5 + \alpha^2x^6$$

$$\rightsquigarrow a(x) : G(x)$$

$$\begin{aligned} &\rightsquigarrow \left(\alpha^2x^6 + x^5 + \alpha^2x^4 + \alpha x^3 + \alpha^2x^2 + x + \alpha^2 \right) : (x^3 + \alpha^4x^2 + \alpha^4x + 1) = \alpha^2x^3 + \alpha^3x^2 \\ &\quad - (\alpha^2x^6 + \alpha^6x^5 + \alpha^6x^4 + \alpha^2x^3) \\ &\quad - (\alpha^2x^5 + x^4 + \alpha^2x^3 + \alpha^2x^2 + x + \alpha^2) \\ &\quad - (\alpha^2x^5 + \alpha^6x^4 + \alpha^6x^3 + \alpha^2x^2) \\ &\quad - (\alpha^2x^4 + x^3 + \alpha x^2 + x + \alpha^2) \\ &\quad - (\alpha^2x^4 + \alpha^6x^3 + \alpha^6x^2 + \alpha^2x) \\ &\quad - (\alpha^2x^3 + \alpha^6x^2 + \alpha^6x + \alpha^2) \\ &\quad - (\alpha^2x^3 + \alpha^6x^2 + \alpha^6x + \alpha^2) \\ &\quad 0 \end{aligned}$$

$$\Rightarrow m = (\alpha^2, \alpha^2, \alpha^2, \alpha^2)$$

Aufgabe 3 b)

$$b(x) = \alpha^4 + \alpha^3x + \alpha^3x^2 + x^4 + \alpha^3x^5 + \alpha x^6$$

$$\rightsquigarrow (\alpha x^6 + \alpha^3x^5 + x^4 + \alpha^3x^2 + \alpha^3x + \alpha^4) : (x^3 + \alpha^4x^2 + \alpha^4x + 1) = \alpha x^3 + \alpha^3x^2 + \alpha^3x + \alpha^4$$

$$- (\alpha x^6 + \alpha^5x^5 + \alpha^5x^4 + \alpha x^3)$$

$$\text{Rest: } \alpha^2x^2 + \alpha x$$

$$\underline{\alpha^2x^5 + \alpha^4x^4 + \alpha x^3 + \alpha^3x^2 + \alpha^3x + \alpha^4}$$

$$- (\alpha^2x^5 + \alpha^6x^4 + \alpha^6x^3 + \alpha^2x^2)$$

$$\underline{\alpha^3x^4 + \alpha^5x^3 + \alpha^5x^2 + \alpha^3x + \alpha^4}$$

$$- (\alpha^3x^4 + x^3 + x^2 + \alpha^3x)$$

$$\underline{\alpha^4x^3 + \alpha^4x^2 + \alpha x + \alpha^4}$$

$$- (\alpha^4x^3 + \alpha x^2 + \alpha x + \alpha^4)$$

$$\underline{\alpha^2x^2 + \alpha x}$$

\rightsquigarrow Nachricht fehlerhaft übertragen

\rightsquigarrow wir wissen, dass $d(C) \geq 3$ und dank Singleton-Schranke gilt außerdem $d(C) \leq 4$

\rightsquigarrow wir wissen außerdem, dass die Fehlerkorrekturschranke gleich 7 ist, egal ob $d(C) = 3$ oder $d(C) = 4$. Entsprechend ließe sich nur ein einzelner Fehler korrigieren. Da der Rest der Polynomdivision aber zwei Koeffizienten ungleich 0 hat, müssen min. 2 Fehler in der Übertragung aufgetreten sein.

\rightsquigarrow Ansatz 2: $c(x) = b(x) - (\alpha^2x^2 + \alpha x)$

\rightsquigarrow Da $d(c, b) = 2$, könnte es nach $d(c) \geq 3$ noch ein anderes Codewort c' mit $d(c', b) = 7$ geben, aber da min. 2 Fehler korrigiert werden müssen, wissen wir, dass es kein Codewort c' mit $d(c', b) < 2$ gibt.

\rightsquigarrow Überprüfung, dass c ein Codewort ist \rightarrow Polynomdivision

$$\rightsquigarrow (\alpha x^6 + \alpha^3x^5 + x^4 + \alpha^5x^2 + x + \alpha^4) : (x^3 + \alpha^4x^2 + \alpha^4x + 1) = \alpha x^3 + \alpha^2x^2$$

$$- (\alpha x^6 + \alpha^5x^5 + \alpha^5x^4 + \alpha x^3)$$

$$+ \alpha^3x + \alpha^4$$

$$\underline{\alpha^2x^5 + \alpha^4x^4 + \alpha x^3 + \alpha^5x^2 + x + \alpha^4}$$

$$\text{Rest: } 0$$

$$- (\alpha^2x^5 + \alpha^6x^4 + \alpha^6x^3 + \alpha^2x^2)$$

$$\underline{\alpha^3x^4 + \alpha^5x^3 + \alpha^3x^2 + x + \alpha^4}$$

$$- (\alpha^3x^4 + x^3 + x^2 + \alpha^3x)$$

$$\underline{\alpha^4x^3 + \alpha x^2 + \alpha x + \alpha^4}$$

$$- (\alpha^4x^3 + \alpha x^2 + \alpha x + \alpha^4)$$

$$\underline{0}$$

$\rightsquigarrow c = (\alpha^4, 1, \alpha^5, 0, 1, 1, \alpha^3, \alpha)$ ist das korrigierte Codewort mit der zugehörigen Nachricht:

$$\underline{n = (\alpha^4, \alpha^3, \alpha^2, 1, \alpha)}$$

Aufgabe 4

Bew. per Induktion.

Ind. Anf.: $n=2 \rightsquigarrow V(r_1, r_2) = \begin{pmatrix} r_1 & r_1 \\ r_1 & r_2 \end{pmatrix}$

$$\det(V(r_1, r_2)) = r_2 - r_1 = \prod_{\substack{1 \leq i < j \leq n}} (r_j - r_i)$$

Ind. Vermutung:

Für alle $x \in \mathbb{N}$ mit $2 \leq x \leq n$ für ein beliebiges $n \in \mathbb{N}$, gilt

$$\det(V(r_1, \dots, r_x)) = \prod_{\substack{1 \leq i < j \leq n}} (r_j - r_i)$$

Ind. Schritt:

Generell gilt, dass sich die Determinante einer Matrix nicht ändert, wenn man einen Zeilenvektor der Matrix mit dem Skalar-Multiplikationen eines anderen Zeilenvektors der Matrix addiert bzw. subtrahiert. Wir nutzen diese Gleichheit nur für unseren Beweis, indem wir für jede i -te Zeile (außer der ersten) die $i-1$ -te Zeile mal r_1 abziehen. Entsprechend gilt:

$$\det(V(r_1, \dots, r_{n+1})) = \left| \begin{array}{cccccc} r_1 & r_1 & r_1 & \cdots & r_1 & \\ 0 & r_2 - r_1 & r_3 - r_1 & \cdots & r_{n+1} - r_1 & \\ 0 & r_2^2 - r_2 r_1 & r_3^2 - r_3 r_1 & \cdots & r_{n+1}^2 - r_{n+1} r_1 & \\ \vdots & \vdots & \vdots & & \vdots & \\ 0 & r_2^{n-1} - r_2^{n-1} r_1 & r_3^{n-1} - r_3^{n-1} r_1 & \cdots & r_{n+1}^{n-1} - r_{n+1}^{n-1} r_1 & \end{array} \right|$$

Nach Laplace können wir die Determinante nun nach der i -ten Spalte entwickeln und erhalten:

$$\det(V(r_1, \dots, r_{n+1})) = \left| \begin{array}{ccccc} r_2 - r_1 & r_3 - r_1 & \cdots & r_{n+1} - r_1 & \\ r_2(r_2 - r_1) & r_3(r_3 - r_1) & \cdots & r_{n+1}(r_{n+1} - r_1) & \\ \vdots & \vdots & & \vdots & \\ r_2^{n-1}(r_2 - r_1) & r_3^{n-1}(r_3 - r_1) & \cdots & r_{n+1}^{n-1}(r_{n+1} - r_1) & \end{array} \right|$$

Da alle Spalten denselben Faktor $(r_{i+1} - r_1)$ für die i -te Spalte haben, können wir den Faktor r_1 herausziehen. Wir erhalten also:

$$\det(V(r_1, \dots, r_{n+1})) = (r_2 - r_1)(r_3 - r_1) \cdots (r_n - r_1) \left| \begin{array}{ccccc} 1 & 1 & \cdots & 1 & \\ r_2 & r_3 & \cdots & r_n & \\ \vdots & \vdots & & \vdots & \\ r_2^{n-1} & r_3^{n-1} & \cdots & r_n^{n-1} & \end{array} \right|$$

Das Produkt an Faktoren lässt sich mit \prod umschreiben und die verbleibende Determinante ist $\det(V(r_2, \dots, r_{n+1}))$, wobei offensichtlich gilt:

$$\begin{aligned}\det(V(r_1, \dots, r_n)) &= \prod_{1 \leq i < j \leq n} (r_j - r_i) \Rightarrow \det(V(r_{1+x}, \dots, r_{n+x})) \\ &= \prod_{1+x \leq i < j \leq n+x} (r_j - r_i)\end{aligned}$$

Per IndoVermutung erhalten wir also:

$$\begin{aligned}\det(V(r_1, \dots, r_{n+1})) &= \overline{\prod_{1 < i < j \leq n} (r_j - r_i)} \cdot \det(V(r_2, \dots, r_{n+1})) \\ &= \overline{\prod_{1 < i < j \leq n} (r_j - r_i)} \cdot \overline{\prod_{2 \leq i < j \leq n+1} (r_j - r_i)} \\ &= \overline{\prod_{1 \leq i < j \leq n+1} (r_j - r_i)} \quad \square\end{aligned}$$