

Aufgabe 1: Für die Konstruktion des Körpers $GF(2^5)$ wird das primitive Polynom $p(x) = x^5 + x^3 + x^2 + x + 1$ benutzt. Ergänzen Sie die fehlenden 5-Tupel in der nachfolgenden Tabelle.

i	α^i	α^4	α^3	α^2	α^1	α^0
0	1	0	0	0	0	1
1	α	0	0	0	1	0
2	α^2	0	0	1	0	0
3	α^3	0	1	0	0	0
4	α^4	1	0	0	0	0
5	α^5	0	1	1	1	1
6	α^6					
7	α^7					
8	α^8					
9	α^9					
10	α^{10}					
11	α^{11}					
12	α^{12}					
13	α^{13}					
14	α^{14}	0	1	1	0	0
15	α^{15}					
16	α^{16}					
17	α^{17}					
18	α^{18}					
19	α^{19}					
20	α^{20}					
21	α^{21}					
22	α^{22}					
23	α^{23}					
24	α^{24}					
25	α^{25}					
26	α^{26}					
27	α^{27}					
28	α^{28}					
29	α^{29}					
30	α^{30}					

Aufgabe 2: Addieren Sie mit der Tabelle aus Aufgabe 1 die folgenden Elemente:

$$\alpha^{14} + \alpha^3 =$$

$$\alpha^{14} + \alpha^{18} =$$

$$\alpha^{14} + \alpha^{28} =$$

Aufgabe 3: Multiplizieren Sie in dem Körper von Aufgabe 1 die folgenden Elemente:

$$\alpha^{19} \cdot \alpha^3 =$$

$$\alpha^{13} \cdot \alpha^{18} =$$

$$\alpha^{21} \cdot \alpha^{25} =$$

Hinweis: Im Ergebnis sollen die Exponenten jeweils aus der Menge $\{0, 1, 2, \dots, 30\}$ sein.

Aufgabe 4: Sie wollen einen binären BCH-Code der Länge $n = 31$ konstruieren, der mindestens 5 Fehler korrigieren kann.

a.) Ergänzen Sie die folgende Zeile:

Für die Minstdistanz gilt $d \geq$ entwerfende Distanz = .

b.) Geben Sie die relevanten Kreisteilungsklassen an:

$$C_1 = \{1, 2, 4, 8, 16\}$$

$$C_3 = \{3, 6, 12, 24, 17\}$$

$$= \{ \quad \quad \quad \}$$

$$= \{ \quad \quad \quad \}$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

$$g(x) = m_1(x) \cdot m_3(x) \cdot \quad .$$

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

e.) Bestimmen Sie die Minimalpolynome von α und α^3 .

$$m_1(x) =$$

$$m_3(x) =$$

Hinweis: Benutzen Sie zur Bestimmung von $m_1(x)$ und $m_3(x)$ die Darstellung des Körpers $GF(2^5)$ aus Aufgabe 1.

Aufgabe 5: Lösen Sie mit der quadratischen Lösungsformel die Gleichung

$$\alpha^{13} \cdot z^2 + z + \alpha^{10} = 0$$

im Körper $GF(2^4)$ mit $p(x) = x^4 + x + 1$ wobei $p(\alpha) = 0$.

$$z_1 =$$

$$z_2 =$$

Aufgabe 6: Gegeben sei der Körper $GF(2^4)$, konstruiert mit dem primitiven Polynom $p(x) = x^4 + x + 1$, $p(\alpha) = 0$. Das Goppa Polynom $G(z) = z^2 + z + 1$ mit

$$L = GF(2^4) - \{\text{Nullstellen von } G(z) \text{ in } GF(2^4)\}$$

bestimmt einen binären Goppa Code.

Ergänzen Sie nachfolgend die Gleichung bzw. Ungleichungen für Länge n , Mindestdistanz d sowie Anzahl der Informationsstellen k des Codes.

$$n = |L| =$$

$$d \geq$$

$$k \geq$$

Aufgabe 7: Die nachfolgend angegebene Prüfmatrix $\mathbf{H}$ beschreibt einen nichtbinären $[8, 6, 3]$ Hamming Code über $GF(7)$ in systematischer Form.

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

a.) Bestimmen Sie die zugehörige Generatormatrix $\mathbf{G}$.

$$\mathbf{G} =$$

b.) Decodieren Sie die Vektoren

$$\mathbf{r}_1 = (1, 2, 3, 4, 5, 6, 1, 2)$$

$$\mathbf{r}_2 = (6, 5, 4, 3, 2, 1, 6, 5)$$

zu den nächsten Codewörtern $\mathbf{c}_1$ und $\mathbf{c}_2$:

$$\mathbf{c}_1 =$$

$$\mathbf{c}_2 =$$

c.) Codieren Sie die Nachrichtenvektoren

$$\mathbf{m}_a = (1, 2, 3, 4, 5, 6)$$

$$\mathbf{m}_a = (2, 2, 2, 2, 2, 2).$$

$$\mathbf{c}_a =$$

$$\mathbf{c}_b =$$

Aufgabe 8: Decodieren Sie den Binärvektor

$$\mathbf{r} = (r_0, r_1, \dots, r_{15}) = (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$$

zum nächsten Codewort des binären $[16, 8, 5]$ Goppa Codes, der mit dem Goppa Polynom $G(z) = z^2 + z + \alpha^3$ gebildet wird, wobei α Wurzel des primitiven Polynoms $x^4 + x + 1$ ist. Für die α_i gilt $\alpha_0 = 0$, $\alpha_i = \alpha^{i-1}$, $i = 1, 2, \dots, 15$.

Hinweis: Es handelt sich um den Code, der in der Vorlesung behandelt wurde (siehe z.B. Aufgabe 21, Vorlesung vom 19.01.2007, Folie 15).

a.) Bestimmen Sie zunächst das Syndrom $S(z)$:

$$S(z) =$$

b.) Bestimmen Sie mit dem Syndrom $S(z)$ das Polynom $T(z)$:

$$T(z) =$$

c.) Bestimmen Sie sodann $R(z) = \sqrt{T(z) + z} \bmod G(z)$:

$$R(z) =$$

d.) Bestimmen Sie schließlich das Fehlerstellenpolynom $\sigma(z)$:

$$\sigma(z) =$$

e.) Finden Sie mittels der Nullstellen von $\sigma(z)$ den Fehlervektor $\mathbf{e}$ und das Codewort $\mathbf{c}$:

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Hinweis: Zur Nullstellensuche siehe auch Aufgabe 5.

Aufgabe 9: Bei perfekten, linearen, binären $[n, k, d = 2t + 1]$ Codes gilt die Kugelpackungsgleichung

$$2^k \cdot \sum_{j=0}^t \binom{n}{j} = 2^n.$$

Es gilt

$$2^{78} \cdot \left(\binom{90}{0} + \binom{90}{1} + \binom{90}{2} \right) = 2^{90}. \quad (1)$$

Welche der beiden Aussagen ist richtig?

a.) Aus Gleichung (1) folgt, daß ein perfekter, linearer, binärer $[90, 78, 5]$ Code existiert.

b.) Aus Gleichung (1) folgt nicht, daß ein perfekter, linearer, binärer $[90, 78, 5]$ Code existiert.

Aufgabe 10: Gegeben seien die Vektoren $\mathbf{x}$ und $\mathbf{y}$ über dem Körper $GF(11) = \{0, 1, 2, \dots, 10\}$, wobei

$$\mathbf{x} = (1, 1, 2, 3, 1, 9, 10)$$

$$\mathbf{y} = (1, 1, 3, 2, 0, 2, 5).$$

- a.) Wie groß ist die Hamming Distanz d_H von $\mathbf{x}$ und $\mathbf{y}$?
- b.) Wie groß ist die Lee Distanz d_{Lee} von $\mathbf{x}$ und $\mathbf{y}$?

Aufgabe 11: Markieren Sie die folgenden Aussagen zu den t -fehlerkorrigierenden negazyklischen Codes für die Lee Metrik als *falsch* oder *richtig*:

- a.) Beim Polynom $S(z)$ sind nur die ersten ungeraden S_j , für $j = 1, 3, \dots, 2t - 1$ bekannt.
- b.) Man benötigt nur das Fehlerstellenpolynom und kein Fehlerwertpolynom.
- c.) Fehlerwerte ungleich 1 oder -1 dürfen bei einer Datenübertragung nicht auftreten.
- d.) Fehlerwerte ungleich 1 oder -1 führen, sofern die Fehler mit dem Code korrigierbar sind, zu mehrfachen Nullstellen von $\sigma(z)$.