

*Prüfung: Algebraische Codierung für die
sichere Datenübertragung*

Dr.-Ing. Klaus Huber

19.02.2015 Ruhr-Universität Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

Aufgabe 1: Für die Konstruktion des Körpers $GF(2^6)$ wird das primitive Polynom $p(x) = x^6 + x^4 + x^3 + x + 1$ benutzt. Ergänzen Sie die fehlenden 6-Tupel in der nachfolgenden Tabelle.

i	α^i	α^5	α^4	α^3	α^2	α^1	α^0	i	α^i	α^5	α^4	α^3	α^2	α^1	α^0
0	1	0	0	0	0	0	1	32	α^{32}	1	1	0	0	1	0
1	α	0	0	0	0	1	0	33	α^{33}	1	1	1	1	1	1
2	α^2	0	0	0	1	0	0	34	α^{34}	1	0	0	1	0	1
3	α^3	0	0	1	0	0	0	35	α^{35}	0	1	0	0	0	1
4	α^4	0	1	0	0	0	0	36	α^{36}	1	0	0	0	1	0
5	α^5	1	0	0	0	0	0	37	α^{37}	0	1	1	1	1	1
6	α^6	0	1	1	0	1	1	38	α^{38}	1	1	1	1	1	0
7	α^7							39	α^{39}						
8	α^8							40	α^{40}						
9	α^9							41	α^{41}						
10	α^{10}							42	α^{42}						
11	α^{11}							43	α^{43}						
12	α^{12}							44	α^{44}						
13	α^{13}							45	α^{45}						
14	α^{14}							46	α^{46}						
15	α^{15}	1	0	0	1	0	0	47	α^{47}	1	1	1	0	1	0
16	α^{16}							48	α^{48}						
17	α^{17}							49	α^{49}						
18	α^{18}							50	α^{50}						
19	α^{19}							51	α^{51}						
20	α^{20}							52	α^{52}						
21	α^{21}							53	α^{53}						
22	α^{22}							54	α^{54}						
23	α^{23}							55	α^{55}						
24	α^{24}	1	0	1	0	1	1	56	α^{56}	0	0	0	0	1	1
25	α^{25}							57	α^{57}						
26	α^{26}							58	α^{58}						
27	α^{27}							59	α^{59}						
28	α^{28}							60	α^{60}						
29	α^{29}	1	1	1	1	0	1	61	α^{61}	1	1	1	0	1	1
30	α^{30}	1	0	0	0	0	1	62	α^{62}	1	0	1	1	0	1
31	α^{31}	0	1	1	0	0	1	63	α^{63}	0	0	0	0	0	1

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

$$\alpha^{29} + \alpha^{61} =$$

$$\alpha^{47} + \alpha^{50} =$$

$$\alpha^{15} + \alpha^{24} =$$

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

$$\alpha^{29} \cdot \alpha^{32} =$$

$$\alpha^{12} \cdot \alpha^{59} =$$

$$\alpha^{17} \cdot \alpha^{-49} =$$

Hinweis: Im Ergebnis sollen die Exponenten jeweils aus der Menge $\{0, 1, 2, \dots, 62\}$ sein.

Aufgabe 4: Sie wollen einen binären BCH-Code der Länge $n = 2047$ 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 noch fehlenden Kreisteilungsklassen an:

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024\} \\ C_3 &= \{3, 6, 12, 24, 48, 96, 192, 384, 768, 1536, 1025\} \\ &= \{ \hspace{15em} \} \\ &= \{ \hspace{15em} \} \\ &= \{ \hspace{15em} \} \end{aligned}$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

$$g(x) = m_1 \cdot m_3 \cdot \hspace{10em} .$$

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

Aufgabe 5: Bestimmen Sie mit Hilfe der Tabelle aus Aufgabe 1 das Generatorpolynom eines Reed-Solomon Codes über $GF(2^6)$, der drei Fehler erkennen kann.

$$g(x) =$$

Aufgabe 6: Gegeben sei der Körper $GF(2^6)$ gemäß Aufgabe 1. Das Goppa Polynom $G(z) = (z^2 + z + \alpha^{32}) \cdot (z^2 + z + \alpha^{33})$ mit

$$L = GF(2^6) - \{\text{Nullstellen von } G(z) \text{ in } GF(2^6)\}$$

bestimmt einen binären Goppa Code.

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

$$n = |L| =$$

$$d \geq$$

$$k \geq \quad .$$

Hinweis: Erläutern Sie wie Sie auf die Länge n kommen.

Aufgabe 7: Bestimmen Sie für binäre Codes der Länge $n = 16$ die durch die Gilbert-Varshamov Schranke gegebenen Werte der Minstdistanz d und tragen Sie diese in die Tabelle ein.

k	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
d															

Hinweis: Die Gilbert-Varshamov Schranke garantiert die Existenz eines $[n, k, d]$ -Codes. Für Binärcodes lautet sie

$$\sum_{j=0}^{d-1} \binom{n-1}{j} < 2^{n-k}$$

(siehe Vorlesung vom 28.11.2014, Folie 2).

Aufgabe 8: Decodieren Sie den Binärvektor

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

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.

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 das Fehlerstellenpolynom $\sigma(z)$:

$$\sigma(z) =$$

d.) Finden Sie den Fehlervektor $\mathbf{e}$ und das Codewort $\mathbf{c}$:

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Aufgabe 9: Decodieren Sie das Polynom

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

zum nächsten Codewort des $[5, 3, 5]$ negazyklischen Codes über $GF(11)$, der mit dem Generatorpolynom $g(x) = (x - 2) \cdot (x - 2^3)$ erzeugt wird.

a.) Bestimmen Sie den bekannten Teil des Syndroms $\tilde{S}(z)$:

$$\tilde{S}(z) =$$

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

$$\sigma(z) =$$

c.) Bestimmen Sie Fehlerpolynom $e(x)$ und Codewortpolynom $c(x)$:

$$e(x) =$$

$$c(x) =$$

Lösung Aufgabe 1:

i	α^i	α^5	α^4	α^3	α^2	α^1	α^0	i	α^i	α^5	α^4	α^3	α^2	α^1	α^0
0	1	0	0	0	0	0	1	32	α^{32}	1	1	0	0	1	0
1	α	0	0	0	0	1	0	33	α^{33}	1	1	1	1	1	1
2	α^2	0	0	0	1	0	0	34	α^{34}	1	0	0	1	0	1
3	α^3	0	0	1	0	0	0	35	α^{35}	0	1	0	0	0	1
4	α^4	0	1	0	0	0	0	36	α^{36}	1	0	0	0	1	0
5	α^5	1	0	0	0	0	0	37	α^{37}	0	1	1	1	1	1
6	α^6	0	1	1	0	1	1	38	α^{38}	1	1	1	1	1	0
7	α^7	1	1	0	1	1	0	39	α^{39}	1	0	0	1	1	1
8	α^8	1	1	0	1	1	1	40	α^{40}	0	1	0	1	0	1
9	α^9	1	1	0	1	0	1	41	α^{41}	1	0	1	0	1	0
10	α^{10}	1	1	0	0	0	1	42	α^{42}	0	0	1	1	1	1
11	α^{11}	1	1	1	0	0	1	43	α^{43}	0	1	1	1	1	0
12	α^{12}	1	0	1	0	0	1	44	α^{44}	1	1	1	1	0	0
13	α^{13}	0	0	1	0	0	1	45	α^{45}	1	0	0	0	1	1
14	α^{14}	0	1	0	0	1	0	46	α^{46}	0	1	1	1	0	1
15	α^{15}	1	0	0	1	0	0	47	α^{47}	1	1	1	0	1	0
16	α^{16}	0	1	0	0	1	1	48	α^{48}	1	0	1	1	1	1
17	α^{17}	1	0	0	1	1	0	49	α^{49}	0	0	0	1	0	1
18	α^{18}	0	1	0	1	1	1	50	α^{50}	0	0	1	0	1	0
19	α^{19}	1	0	1	1	1	0	51	α^{51}	0	1	0	1	0	0
20	α^{20}	0	0	0	1	1	1	52	α^{52}	1	0	1	0	0	0
21	α^{21}	0	0	1	1	1	0	53	α^{53}	0	0	1	0	1	1
22	α^{22}	0	1	1	1	0	0	54	α^{54}	0	1	0	1	1	0
23	α^{23}	1	1	1	0	0	0	55	α^{55}	1	0	1	1	0	0
24	α^{24}	1	0	1	0	1	1	56	α^{56}	0	0	0	0	1	1
25	α^{25}	0	0	1	1	0	1	57	α^{57}	0	0	0	1	1	0
26	α^{26}	0	1	1	0	1	0	58	α^{58}	0	0	1	1	0	0
27	α^{27}	1	1	0	1	0	0	59	α^{59}	0	1	1	0	0	0
28	α^{28}	1	1	0	0	1	1	60	α^{60}	1	1	0	0	0	0
29	α^{29}	1	1	1	1	0	1	61	α^{61}	1	1	1	0	1	1
30	α^{30}	1	0	0	0	0	1	62	α^{62}	1	0	1	1	0	1
31	α^{31}	0	1	1	0	0	1	63	α^{63}	0	0	0	0	0	1

Lösung Aufgabe 2:

$$\alpha^{29} + \alpha^{61} = \alpha^{57}$$

$$\alpha^{47} + \alpha^{50} = \alpha^{60}$$

$$\alpha^{15} + \alpha^{24} = \alpha^{42}$$

Lösung Aufgabe 3:

$$\alpha^{29} \cdot \alpha^{32} = \alpha^{61}$$

$$\alpha^{12} \cdot \alpha^{59} = \alpha^8$$

$$\alpha^{17} \cdot \alpha^{-49} = \alpha^{31}$$

Lösung Aufgabe 4:

a.) Für die Mindestdistanz gilt $d \geq$ entwerfende Distanz = 11.

b.)

$$C_1 = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024\}$$

$$C_3 = \{3, 6, 12, 24, 48, 96, 192, 384, 768, 1536, 1025\}$$

$$C_5 = \{5, 10, 20, 40, 80, 160, 320, 640, 1280, 513, 1026\}$$

$$C_7 = \{7, 14, 28, 56, 112, 224, 448, 896, 1792, 1537, 1027\}$$

$$C_9 = \{9, 18, 36, 72, 144, 288, 576, 1152, 257, 514, 1028\}$$

c.) Es gilt $k = 2047 - 5 \cdot 11 = 1992$.

d.) $g(x) = m_1 \cdot m_3 \cdot m_5 \cdot m_7 \cdot m_9$.

Lösung Aufgabe 5:

Um drei Fehler erkennen zu können, muss die Minstdistanz d gleich 4 sein.

$$\begin{aligned} g(x) &= (x - \alpha) \cdot (x - \alpha^2) \cdot (x - \alpha^3) \\ &= x^3 + (\alpha^3 + \alpha^2 + \alpha) \cdot x^2 + (\alpha^{2+3} + \alpha^{1+3} + \alpha^{1+2}) \cdot x + \alpha^{1+2+3} \\ &= x^3 + \alpha^{21} \cdot x^2 + \alpha^{23} \cdot x + \alpha^6 . \end{aligned}$$

Lösung Aufgabe 6:

Es gilt

$$\begin{aligned} \text{tr}(\alpha^{32}) &= \alpha^{32} + \alpha^1 + \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} = 0 \\ \text{und} \quad \text{tr}(\alpha^{33}) &= \alpha^{33} + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{24} + \alpha^{48} = 1 , \end{aligned}$$

d.h. das Goppa Polynom hat vier Nullstellen im Körper $GF(2^6)$.

$$\Rightarrow n = |L| = 62$$

$$d \geq 9$$

$$k \geq 62 - 4 \cdot 6 = 38.$$

Lösung Aufgabe 7:

$$\binom{15}{0} = 1 < 2^{16-k} \Rightarrow d = 2, \quad k \leq 15$$

$$\binom{15}{0} + \binom{15}{1} = 16 < 2^{16-k} \Rightarrow d = 3, \quad k \leq 11$$

$$\binom{15}{0} + \binom{15}{1} + \binom{15}{2} = 121 < 2^{16-k} \Rightarrow d = 4, \quad k \leq 9$$

$$\sum_{j=0}^3 \binom{15}{j} = 576 < 2^{16-k} \Rightarrow d = 5, \quad k \leq 6$$

$$\sum_{j=0}^4 \binom{15}{j} = 1941 < 2^{16-k} \Rightarrow d = 6, \quad k \leq 5$$

$$\sum_{j=0}^5 \binom{15}{j} = 4944 < 2^{16-k} \Rightarrow d = 7, \quad k \leq 3$$

$$\sum_{j=0}^6 \binom{15}{j} = 9949 < 2^{16-k} \Rightarrow d = 8, \quad k \leq 2$$

Da $\sum_{j=0}^{14} \binom{15}{j} = 2^{15} - 1 < 2^{16-k}$, folgt $d = 16$ bei $k = 1$.

Somit erhält man die Tabelle:

k	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
d	2	2	2	2	3	3	4	4	4	5	6	6	7	8	16

Lösung Aufgabe 8:

a.)

$$\begin{aligned}
 S(z) &= \frac{1}{z - \alpha_1} + \frac{1}{z - \alpha_8} + \frac{1}{z - \alpha_{13}} \\
 &= \alpha^{12}z + \alpha^6z + 1 + \alpha^2z + \alpha^{13} \\
 &= (\alpha^{12} + \alpha^6 + \alpha^2)z + 1 + \alpha^{13} \\
 \Rightarrow S(z) &= \alpha^{10} \cdot z + \alpha^6 .
 \end{aligned}$$

b.)

$$(z^2 + z + \alpha^3) : (\alpha^{10}z + \alpha^6) = \alpha^5z + \alpha^2 \text{ Rest } \alpha^{13}.$$

d.h.

$$\begin{aligned}
 \alpha^{13} &= 1 \cdot G(z) + (\alpha^5z + \alpha^2) \cdot S(z) \\
 \Rightarrow 1 &\equiv (\alpha^7z + \alpha^4) \cdot S(z) \text{ mod } G(z).
 \end{aligned}$$

$$\Rightarrow T(z) = \alpha^7z + \alpha^4 .$$

c.)

$$T(z) + z = \alpha^9z + \alpha^4 \Rightarrow R(z) = \sqrt{\alpha^4 + z\alpha^9} \text{ mod } G(z).$$

$$\begin{aligned}
 R(z) &= \alpha^2 + w(z) \cdot \alpha^{12} \\
 &= \alpha^2 + (z + \alpha^9) \cdot \alpha^{12} \\
 \Rightarrow R(z) &= \alpha^{12} \cdot z + \alpha^3 .
 \end{aligned}$$

$$\begin{aligned}
 a(z) &= \alpha^{12} \cdot z + \alpha^3 \\
 b(z) &= 1 \\
 \sigma(z) &= a(z)^2 + z \cdot b(z)^2 \\
 \Rightarrow \sigma(z) &= \alpha^9 z^2 + z + \alpha^6 .
 \end{aligned}$$

d.) Die Nullstellen von $\sigma(z)$ sind $\alpha_2 = \alpha$ und $\alpha_{12} = \alpha^{11}$.

$$\begin{aligned}
 \Rightarrow \mathbf{e} &= (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \\
 \Rightarrow \mathbf{c} &= (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)
 \end{aligned}$$

Lösung Aufgabe 9:

a.)

$$S_1 = r(\alpha) = 5 \cdot 2^3 + 4 \cdot 2^2 + 6 \equiv 7 \pmod{11}$$

$$S_3 = r(\alpha^3) = 5 \cdot 8^3 + 4 \cdot 8^2 + 6 \equiv 6 \pmod{11}$$

$$\Rightarrow \tilde{S}(z) = 7z + 6z^3.$$

b.) Die Berechnung von $\sigma(z)$ erfolgt in gleicher Weise wie bei Aufgabe 24 mit Berlekamps oder Roths Algorithmus (identische Rechnung mit Berlekamps Algorithmus: siehe Folie 4 vom 23.01.2015).

Roths Algorithmus liefert zunächst das Polynom $V(z) = 1 + 8z + 10z^2 + 8z^3 + 3z^4$. Durchführen des Euklidischen Algorithmus liefert:

$$\begin{aligned} z^5 &= (4z + 4) \cdot (3z^4 + 8z^3 + 10z^2 + 8z + 1) + 5z^3 + 5z^2 + 8z + 7 \\ 3z^4 + 8z^3 + 10z^2 + 8z + 1 &= (5z + 1) \cdot (5z^3 + 5z^2 + 8z + 7) + 9z^2 + 9z + 5 \end{aligned}$$

$$\Rightarrow \sigma(z) = \text{const} \cdot (9z^2 + 9z + 5) .$$

c.) Das Polynom $\sigma(z)$ hat die doppelte Nullstelle 5. Rechnung identisch mit Aufgabe 24 führt auf das Fehlerpolynom und schließlich auf das Codewortpolynom.

$$e(x) = -2x$$

$$c(x) = 5x^3 + 4x^2 + 2x + 6 .$$