Prüfung: Algebraische Codierung für die sichere Datenübertragung

Dr.-Ing. Klaus Huber

20.02.2014 Ruhr-Universität Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

Aufgabe 1: Für die Konstruktion des Körpers $GF(2^6)$ wird das primitive Polynom $p(x) = x^6+x^5+x^2+x+1$ 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}	0	1	1	1	0	0
1	α	0	0	0	0	1	0	33	α^{33}	1	1	1	0	0	0
2	α^2	0	0	0	1	0	0	34	α^{34}	0	1	0	1	1	1
3	α^3	0	0	1	0	0	0	35	α^{35}	1	0	1	1	1	0
4	α^4	0	1	0	0	0	0	36	α^{36}	1	1	1	0	1	1
5	α^5	1	0	0	0	0	0	37	α^{37}	0	1	0	0	0	1
6	α^6	1	0	0	1	1	1	38	α^{38}	1	0	0	0	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}	0	1	1	1	1	1	47	α^{47}	1	0	0	1	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	1	0	0	1	0	56	α^{56}	0	1	0	0	1	0
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	0	0	0	0	61	α^{61}	1	0	1	0	1	0
30	α^{30}	0	0	0	1	1	1	62	α^{62}	1	1	0	0	1	1
31	α^{31}	0	0	1	1	1	0	63	α^{63}	0	0	0	0	0	1

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

$$\alpha^{47} + \alpha^{49} =$$

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

$$\alpha^{4} + \alpha^{39} =$$

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

$$\alpha^{29} \cdot \alpha^{23} =$$

$$\alpha^{13} \cdot \alpha^{60} =$$

$$\alpha^{17} \cdot \alpha^{-32} =$$

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

Aufgabe 4: Sie wollen einen binären BCH-Code der Länge $n = 127$ konstruieren, der mindestens 10 Fehler korrigieren kann.

a.) Ergänzen Sie die folgende Zeile:

Für die Mindestdistanz gilt $d \geq$ entworfende Distanz = .

b.) Geben Sie die relevanten noch fehlenden Kreisteilungsklassen an:

$$
\begin{aligned}
C_1 &= \{1,\ 2,\ \ 4,\ \ 8,\ \ 16,\ 32,\ 64\} \\
C_3 &= \{3,\ 6,\ 12,\ 24,\ 48,\ 96,\ 65\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\} \\
&= \{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\}
\end{aligned}
$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

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

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 einen Fehler korrigieren und zwei 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.

$$\begin{aligned} n &= |L| = \\ d &\geq \\ k &\geq \quad . \end{aligned}$$

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

Aufgabe 7: Benutzen Sie die Kugelpackungsschranke um herauszufinden, ob die folgenden Codes perfekt sind und machen Sie in den entsprechenden Kästchen ein Kreuz.

a.) Der binäre $[23, 12, 7]$ Code ist

perfekt: ☐ nicht perfekt: ☐

b.) Der binäre $[23, 14, 5]$ Code ist

perfekt: ☐ nicht perfekt: ☐

c.) Der ternäre $[11, 6, 5]$ Code ist

perfekt: ☐ nicht perfekt: ☐

Hinweis: ternär bedeutet, es handelt sich um einen Code über $GF(3)$.

Aufgabe 8: Decodieren Sie den Binärvektor

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

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 $\alpha_0 = 0$, $\alpha_i = \alpha^{i-1}$, $i = 1, 2, \ldots, 15$.

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 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 $\mathbf{c}$:

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Aufgabe 9: Decodieren Sie das Polynom

$$r(x) = 10\,x^4 + 6\,x^2 + 10\,x$$

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

Lösung Aufgabe 2:

$$\alpha^{47} + \alpha^{49} = \alpha^{34}$$

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

$$\alpha^{4} + \alpha^{39} = \alpha^{62}$$

Lösung Aufgabe 3:

$$\alpha^{29} \cdot \alpha^{23} = \alpha^{52}$$

$$\alpha^{13} \cdot \alpha^{60} = \alpha^{10}$$

$$\alpha^{17} \cdot \alpha^{-32} = \alpha^{48}$$

Lösung Aufgabe 4:

a.) Für die Mindestdistanz gilt $d \geq$ entworfende Distanz $= 21$.

b.)

$$\begin{aligned}
C_1 &= \{1, 2, 4, 8, 16, 32, 64\} \\
C_3 &= \{3, 6, 12, 24, 48, 96, 65\} \\
C_5 &= \{5, 10, 20, 40, 80, 33, 66\} \\
C_7 &= \{7, 14, 28, 56, 112, 97, 67\} \\
C_9 &= \{9, 18, 36, 72, 17, 34, 68\} \\
C_{11} &= \{11, 22, 44, 88, 49, 98, 69\} \\
C_{13} &= \{13, 26, 52, 104, 81, 35, 70\} \\
C_{15} &= \{15, 30, 60, 120, 113, 99, 71\} \\
C_{19} &= \{19, 38, 76, 25, 50, 100, 73\}
\end{aligned}$$

c.) Es gilt $k = 127 - 9 \cdot 7 = 64$.

d.) $g(x) = m_1 \cdot m_3 \cdot m_5 \cdot m_7 \cdot m_9 \cdot m_{11} \cdot m_{13} \cdot m_{15} \cdot m_{19}$.

Lösung Aufgabe 5:
Um einen Fehler korrigieren und zwei Fehler erkennen zu können, muss die Mindestdistanz gleich $d = 4$ sein.

$$\begin{aligned} g(x) &= (x-\alpha)\cdot(x-\alpha^2)\cdot(x-\alpha^3) \\ &= x^3 + (\alpha^3+\alpha^2+\alpha)\cdot x^2 + (\alpha^{2+3}+\alpha^{1+3}+\alpha^{1+2})\cdot x + \alpha^{1+2+3} \\ &= x^3 + \alpha^{31}\cdot x^2 + \alpha^{33}\cdot x + \alpha^6 \ . \end{aligned}$$

Lösung Aufgabe 6:

Es gilt

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

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

$$\begin{aligned} \Rightarrow n &= |L| = 64 \\ d &\geq 9 \\ k &\geq 64 - 4\cdot 6 = 40. \end{aligned}$$

Lösung Aufgabe 7:

a.) Die linke Seite der Kugelpackungsungleichung lautet

$$2^{12} \cdot \left(1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}\right) = 2^{12} \cdot (1+23+253+1771) = 2^{12} \cdot 2048$$

Da $2^{11} \cdot 2048 = 2^{12+11}$ exakt 2^{23} ergibt, ist die Kugelpackungsbedingung mit Gleichheit erfüllt und der Code somit perfekt.

b.) Die linke Seite der Kugelpackungsungleichung lautet

$$2^{14} \cdot \left(1 + \binom{23}{1} + \binom{23}{2}\right) = 2^{14} \cdot (1 + 23 + 253) = 2^{14} \cdot 277$$

Da $2^{14} \cdot 277$ kleiner als $2^{23} = 2^{14} \cdot 512$ ist, ist der Code nicht perfekt.

c.) Die linke Seite der Kugelpackungsungleichung lautet

$$3^6 \cdot \left(1 + \binom{11}{1} \cdot 2^1 + \binom{11}{2} \cdot 2^2\right) = 3^6 \cdot (1 + 22 + 220) = 3^6 \cdot 243$$

Da $3^6 \cdot 243 = 3^{6+5}$ exakt 3^{11} ergibt, ist der Code perfekt.

Lösung Aufgabe 8:
a.)

$$\begin{aligned} S(z) &= \frac{1}{z-\alpha_6} + \frac{1}{z-\alpha_9} + \frac{1}{z-\alpha_{12}} \\ &= \alpha z + \alpha^{11} + \alpha^3 z + \alpha^5 + \alpha^2 z + \alpha^{14} \\ &= (\alpha + \alpha^3 + \alpha^2) \cdot z + (\alpha^{11} + \alpha^5 + \alpha^{14}) \\ \Rightarrow S(z) &= \alpha^{11} \cdot z + 1 \ . \end{aligned}$$

b.)

$$(z^2 + z + \alpha^3) : (\alpha^{11} z + 1) = \alpha^4 z + \alpha^5 \ \text{ Rest } \alpha^{11}.$$

d.h.

$$\begin{aligned} \alpha^{11} &= 1 \cdot G(z) + (\alpha^{11} z + 1) \cdot S(z) \\ \Rightarrow 1 &\equiv (\alpha^8 z + \alpha^9) \cdot S(z) \bmod G(z). \end{aligned}$$

$$\Rightarrow T(z) = \alpha^8 z + \alpha^9 \ .$$

c.)

$$T(z) + z = \alpha^2 z + \alpha^9 \Rightarrow R(z) = \sqrt{\alpha^9 + z\alpha^2} \bmod G(z).$$

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

d.)

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

e.) Die Nullstellen von $\sigma(z)$ sind $\alpha_{10} = \alpha^9$ und $\alpha_{11} = \alpha^{10}$.

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

Lösung Aufgabe 9:
a.)

$$\begin{aligned} S_1 = r(\alpha) &= 10 \cdot 2^4 + 6 \cdot 2^2 + 10 \cdot 2 \equiv 6 \bmod 11 \\ S_3 = r(\alpha^3) &= 10 \cdot 8^4 + 6 \cdot 8^2 + 10 \cdot 8 \equiv 9 \bmod 11 \end{aligned}$$

$$\Rightarrow \tilde{S}(z) = 6z + 9z^3.$$

b.) Die Berechnung von $\sigma(z)$ erfolgt in gleicher Weise wie bei Aufgabe 24 mit Berlekamps oder Roths Algorithmus (identische Rechnung, siehe Folie 4 und 5 vom 24.01.2014 oder Folie 3 mit Roths Algorithmus).

$$\Rightarrow \sigma(z) = \text{const} \cdot (6z^2 + 5z + 1) \ .$$

b.) Das Polynom $\sigma(z)$ hat die Nullstellen $z_1 = 5$ und $z_2 = 7$. Rechnung Identisch mit Aufgabe 24.

$$\begin{aligned} e(x) &= x^3 - x \\ c(x) &= 10x^4 + 10x^3 + 6x^2 \ . \end{aligned}$$