Prüfung: Algebraische Codierung für die sichere Datenübertragung

Dr.-Ing. Klaus Huber

31.07.2014 Ruhr-Universität Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

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

$$\alpha^{22} \cdot \alpha^{24} =$$

$$\alpha^{14} \cdot \alpha^{61} =$$

$$\alpha^{13} \cdot \alpha^{-31} =$$

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 $n = 255$ konstruieren, der mindestens 9 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:

$$
\begin{aligned}
C_1 &= \{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128\} \\
C_3 &= \{3,\ 6,\ 12,\ 24,\ 48,\ 96,\ 192,\ 129\} \\
&= \{\ \} \\
&= \{\ \} \\
&= \{\ \} \\
&= \{\ \} \\
&= \{\ \} \\
&= \{\ \} \\
&= \{\ \}
\end{aligned}
$$

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 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.

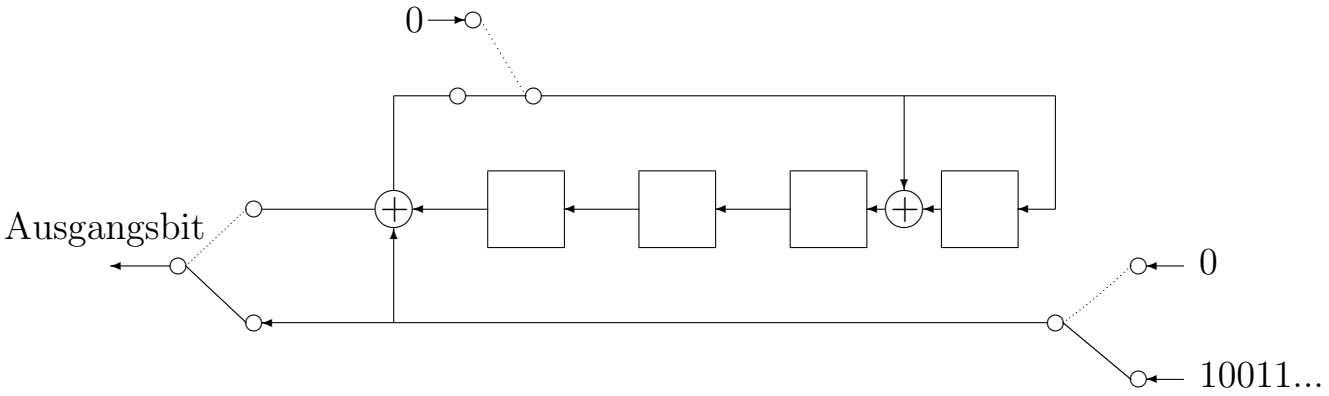
Ergänzen Sie nachfolgend die Gleichung bzw. Ungleichungen für Länge n, Mindestdistanz d sowie Anzahl der Informationsstellen k des Codes.

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

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

Aufgabe 7: Führen Sie eine systematische Codierung mit dem binären [15,11,3]-Code durch, der mit dem Generatorpolynom $g(x) = x^4 + x + 1$ erzeugt wird.

Benutzen Sie die nachfolgende Schieberegisterschaltung und codieren Sie die Datenfolge 10011101010. Vervollständigen Sie hierzu die untenstehende Tabelle, in der die Ausgangsbits und die Inhalte des Schieberegisters nach dem i-ten Takt eingetragen sind.



Takt	Ausgangsbit	Zelle 3	Zelle 2	Zelle 1	Zelle 0
1	1	0	0	1	1
2	0	0	1	1	0
3	0				
4	1				
5	1				
6	1				
7					
8					
9					
10					
11					
12					
13					
14					
15					

Aufgabe 8: Decodieren Sie den Binärvektor

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

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

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 das Fehlerstellenpolynom $\sigma(z)$:

$$\sigma(z) =$$

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

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Aufgabe 9: Decodieren Sie das Polynom

$$r(x) = 9\,x^3 + x$$

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:

$p(x) = x^6 + x^5 + x^4 + x + 1$

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

Lösung Aufgabe 2:

$$\alpha^{47} + \alpha^{49} = \alpha^{62}$$

$$\alpha^{15} + \alpha^{24} = \alpha^{60}$$

$$\alpha^{4} + \alpha^{39} = \alpha^{44}$$

Lösung Aufgabe 3:

$$\alpha^{22} \cdot \alpha^{24} = \alpha^{46}$$

$$\alpha^{14} \cdot \alpha^{61} = \alpha^{12}$$

$$\alpha^{13} \cdot \alpha^{-31} = \alpha^{45}$$

Lösung Aufgabe 4:

a.) Für die Mindestdistanz gilt $d \geq$ entworfende Distanz $= 19$.

b.)

$$\begin{aligned}
C_1 &= \{1, 2, 4, 8, 16, 32, 64, 128\} \\
C_3 &= \{3, 6, 12, 24, 48, 96, 192, 129\} \\
C_5 &= \{5, 10, 20, 40, 80, 160, 65, 130\} \\
C_7 &= \{7, 14, 28, 56, 112, 224, 193, 131\} \\
C_9 &= \{9, 18, 36, 72, 144, 33, 66, 132\} \\
C_{11} &= \{11, 22, 44, 88, 176, 97, 194, 133\} \\
C_{13} &= \{13, 26, 52, 104, 208, 161, 67, 134\} \\
C_{15} &= \{15, 30, 60, 120, 240, 225, 195, 135\} \\
C_{17} &= \{17, 34, 68, 136\}
\end{aligned}$$

c.) Es gilt $k = 255 - 8 \cdot 8 - 4 = 187$.

d.) $g(x) = m_1 \cdot m_3 \cdot m_5 \cdot m_7 \cdot m_9 \cdot m_{11} \cdot m_{13} \cdot m_{15} \cdot m_{17}$.

Lösung Aufgabe 5:
Um drei Fehler erkennen zu können, muss die Mindestdistanz d gleich 4 sein.

$$\begin{aligned} g(x) &= (x-\alpha)\cdot(x-\alpha^2)\cdot(x-\alpha^3) \\ &= x^3+(\alpha^3+\alpha^2+\alpha)\cdot x^2+(\alpha^{2+3}+\alpha^{1+3}+\alpha^{1+2})\cdot x+\alpha^{1+2+3} \\ &= x^3+\alpha^{36}\cdot x^2+\alpha^{38}\cdot x+\alpha^6\ . \end{aligned}$$

Lösung Aufgabe 6:

Es gilt

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

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

$$\begin{aligned} \Rightarrow n &= |L|=62 \\ d &\geq 9 \\ k &\geq 62-4\cdot 6=38. \end{aligned}$$

Lösung Aufgabe 7:

Takt	Ausgangsbit	Zelle 3	Zelle 2	Zelle 1	Zelle 0
1	1	0	0	1	1
2	0	0	1	1	0
3	0	1	1	0	0
4	1	1	0	0	0
5	1	0	0	0	0
6	1	0	0	1	1
7	0	0	1	1	0
8	1	1	1	1	1
9	0	1	1	0	1
10	1	1	0	1	0
11	0	0	1	1	1
12	0	1	1	1	0
13	1	1	1	0	0
14	1	1	0	0	0
15	1	0	0	0	0

Lösung Aufgabe 8:
a.)

$$\begin{aligned} S(z) &= \frac{1}{z-\alpha_0}+\frac{1}{z-\alpha_1}+\frac{1}{z-\alpha_2}+\frac{1}{z-\alpha_3}+\frac{1}{z-\alpha_9}+\frac{1}{z-\alpha_{10}} \\ &= \alpha^{12}z+\alpha^{12}+\alpha^{12}z+\alpha^4 z+\alpha^8+\alpha^3 z+\alpha^{11}+\alpha^3 z+\alpha^5+\alpha^6 z+\alpha^{13} \\ &= (\alpha^{12}+\alpha^{12}+\alpha^4+\alpha^3+\alpha^3+\alpha^3)z+(\alpha^{12}+\alpha^8+\alpha^{11}+\alpha^5+\alpha^{13}) \\ \Rightarrow S(z) &= \alpha^{12}\cdot z+\alpha^{12}\ . \end{aligned}$$

b.)

$$(z^2+z+\alpha^3):(\alpha^{12}z+\alpha^{12})=\alpha^3 z \ \text{ Rest } \alpha^3.$$

d.h.

$$\alpha^3 = 1\cdot G(z)+(\alpha^3 z)\cdot S(z)$$
$$\Rightarrow 1 \equiv z\cdot S(z) \bmod G(z).$$

$$\Rightarrow T(z)=z\ .$$

c.)

$$\Rightarrow \sigma(z)=z.$$

d.)

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

Lösung Aufgabe 9:
a.)

$$\begin{aligned} S_1 = r(\alpha) &= 9 \cdot 2^3 + 2 \equiv 8 \bmod 11 \\ S_3 = r(\alpha^3) &= 9 \cdot 8^3 + 8 \equiv 7 \bmod 11 \end{aligned}$$

$$\Rightarrow \tilde{S}(z) = 8z + 7z^3.$$

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 6 vom 24.01.2014).
Roths Algorithmus liefert zunächst das Polynom $V(z) = 1 + 6z + 7z^2 + 2z^3 + 4z^4$. Durchführen des Euklidschen Algorithmus liefert:

$$z^5 = (3z + 4) \cdot (4z^4 + 2z^3 + 7z^2 + 6z + 1) + 4z^3 + 9z^2 + 6z + 7$$
$$4z^4 + 2z^3 + 7z^2 + 6z + 1 = (z + 1) \cdot (4z^3 + 9z^2 + 6z + 7) + 3z^2 + 4z + 5$$

$$\Rightarrow \sigma(z) = \text{const} \cdot (3z^2 + 4z + 5) \ .$$

c.) Das Polynom $\sigma(z)$ hat die doppelte Nullstelle 3. Rechnung identisch mit Aufgabe 24 führt auf das Fehlerpolynom und schließlich auf das Codewortpolynom.

$$\begin{aligned} e(x) &= 2x^2 \\ c(x) &= 9x^3 + 9x^2 + x \ . \end{aligned}$$