Prüfung: Algebraische Codierung für die sichere Datenübertragung

Dr.-Ing. Klaus Huber

07.03.2013 Ruhr-Universität Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

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

$$\alpha^{19} \cdot \alpha^{17} =$$

$$\alpha^{11} \cdot \alpha^{58} =$$

$$\alpha^{39} \cdot \alpha^{-47} =$$

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 $n = 63$ konstruieren, der mindestens 11 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:

$$
\begin{aligned}
C_1 &= \{1, 2, 4, 8, 16, 32\} \\
C_3 &= \{3, 6, 12, 24, 48, 33\} \\
C_5 &= \{5, 10, 20, 40, 17, 34\} \\
C_7 &= \{7, 14, 28, 56, 49, 35\} \\
&= \{ \quad \} \\
&= \{ \quad \} \\
&= \{ \quad \} \\
&= \{ \quad \} \\
&= \{ \quad \}
\end{aligned}
$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

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

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

e.) Bestimmen Sie das Minimalpolynom von α^{21}.

$$m_{21}(x) =$$

Aufgabe 5: Gegeben sei der binäre [63,51,5]-BCH-Code mit dem Generatorpolynom $g(x) = m_1(x) \cdot m_3(x)$, wobei $m_1(x)$ und $m_3(x)$ die Minimalpolynome von α und α^3 sind, die mit dem Körper $GF(2^6)$ aus Aufgabe 1 gebildet werden.
Das empfangene Polynom $r(x) = x^{14} + x^{12} + x^9 + x^6 + x^3 + x^2$ soll zum nächsten Codewort decodiert werden.

a.) Bestimmen Sie S_1 und S_3:

$S_1 =$

$S_3 =$

b.) Ist die nachfolgende Aussage richtig oder falsch?
Die Bedingung für einen Einzelfehler ist erfüllt.

richtig: ☐ falsch: ☐

c:) Falls die Bedingung für einen Einzelfehler erfüllt ist bestimmen Sie Fehlerpolynom $e(x)$ und Codewort $c(x)$:

$e(x) =$

$c(x) =$

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.

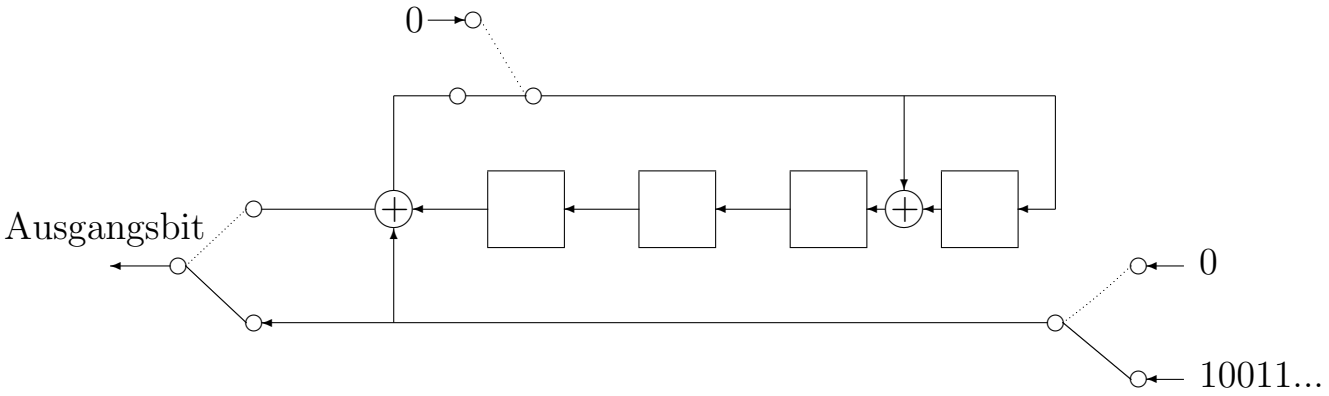
Ergänzen Sie nachfolgend die Gleichung bzw. Ungleichungen für Länge n, Mindestdistanz d sowie Anzahl der Informationsstellen k des Codes.

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

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 10011110010. 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

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

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

$$r(x) = 6\,x^7 + x^6$$

zum nächsten Codewort des $[11, 9, 5]$ negazyklischen Codes über $GF(23)$, der mit dem Generatorpolynom $g(x) = (x - 5) \cdot (x - 5^3)$ erzeugt wird.

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

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

b.) Bestimmen Sie sodann das Polynom $U(z)$:

$$U(z) =$$

c.) Bestimmen Sie die relevanten Terme des Polynoms $1 + T(z)$:

$$1 + T(z) =$$

d.) Bestimmen Sie dann die Polynome $\phi(z)$ und $\omega(z)$

$$\phi(z) = \qquad\qquad \omega(z) =$$

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

$$\sigma(z) =$$

f.) Finden Sie mittels der Nullstellen von $\sigma(z)$ das Fehlerpolynom $e(x)$ und das Codewortpolynom $c(x)$:

$$e(x) =$$

$$c(x) =$$

Hinweis: Die Nullstellen von $z^2 - 5z - 1 = 0$ in $GF(23)$ sind 8 und 20.

Lösung Aufgabe 1:

$p(x) = x^6 + x^5 + x^3 + x^2 + 1$

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

Lösung Aufgabe 2:

$$\alpha^{47} + \alpha^{49} = \alpha^0 = 1$$

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

$$\alpha^4 + \alpha^{39} = \alpha^{35}$$

Lösung Aufgabe 3:

$$\alpha^{19} \cdot \alpha^{17} = \alpha^{36}$$

$$\alpha^{11} \cdot \alpha^{58} = \alpha^6$$

$$\alpha^{39} \cdot \alpha^{-47} = \alpha^{55}$$

Lösung Aufgabe 4:

a.) Für die Mindestdistanz gilt $d \geq$ entworfende Distanz $= 23$.

b.)

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16, 32\} \\ C_3 &= \{3, 6, 12, 24, 48, 33\} \\ C_5 &= \{5, 10, 20, 40, 17, 34\} \\ C_7 &= \{7, 14, 28, 56, 49, 35\} \\ C_9 &= \{9, 18, 36\} \\ C_{11} &= \{11, 22, 44, 25, 50, 37\} \\ C_{13} &= \{13, 26, 52, 41, 19, 38\} \\ C_{15} &= \{15, 30, 60, 57, 51, 39\} \\ C_{21} &= \{21, 42\} \end{aligned}$$

c.) Es gilt $k = 63 - 7 \cdot 6 - 3 - 2 = 16$.

d.) $g(x) = m_1 \cdot m_3 \cdot m_5 \cdot m_7 \cdot m_9 \cdot m_{11} \cdot m_{13} \cdot m_{15} \cdot m_{21}$.

e.) Das Minimalpolynom $m_{21}(x)$ ist gleich

$$m_{21}(x) = (x - \alpha^{21}) \cdot (x - \alpha^{42}) = x^2 + x + 1 \ .$$

Lösung Aufgabe 5:
a.)

$$\begin{aligned} S_1 &= \alpha^{14} + \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + \alpha^2 = \alpha^{13} \\ S_3 &= \alpha^{3\cdot 14} + \alpha^{3\cdot 12} + \alpha^{3\cdot 9} + \alpha^{3\cdot 6} + \alpha^{3\cdot 3} + \alpha^{3\cdot 2} \\ &= \alpha^{42} + \alpha^{36} + \alpha^{27} + \alpha^{18} + \alpha^9 + \alpha^6 = \alpha^{39} \end{aligned}$$

b.) richtig $\quad S_3 = S_1^3$

c.) Mit $S_3 = S_1^3$ (da $13 \cdot 3 \equiv 39 \bmod 63$) folgt

$$e(x) = x^{13} \quad \text{und} \quad c(x) = x^{14} + x^{13} + x^{12} + x^9 + x^6 + x^3 + x^2 \ .$$

Lösung Aufgabe 6:

Es gilt

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

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	1	0	1	0	1
8	0	1	0	1	0
9	0	0	1	1	1
10	1	1	1	0	1
11	0	1	0	0	1
12	1	0	0	1	0
13	0	0	1	0	0
14	0	1	0	0	0
15	1	0	0	0	0

Lösung Aufgabe 8:
a.)

$$\begin{aligned} S(z) &= \frac{1}{z-\alpha_1} + \frac{1}{z-\alpha_2} + \frac{1}{z-\alpha_{13}} + \frac{1}{z-\alpha_{14}} \\ &= \alpha^{12}z + \alpha^4 z + \alpha^8 + \alpha^2 z + \alpha^{13} + \alpha^8 z + \alpha^{14} \\ &= (\alpha^{12}+\alpha^4+\alpha^2+\alpha^8)z + (\alpha^8+\alpha^{13}+\alpha^{14}) \\ \Rightarrow S(z) &= \alpha^{13} \cdot z + 1 \ . \end{aligned}$$

b.)

$$(z^2 + z + \alpha^3) : (\alpha^{13}z + 1) = \alpha^2 z + \alpha^{10} \ \text{ Rest } \alpha^{12}.$$

d.h.

$$\begin{aligned} \alpha^{12} &= 1 \cdot G(z) + (\alpha^2 z + \alpha^{10}) \cdot S(z) \\ \Rightarrow 1 &\equiv (\alpha^5 z + \alpha^{13}) \cdot S(z) \bmod G(z). \end{aligned}$$

$$\Rightarrow T(z) = \alpha^5 z + \alpha^{13} \ .$$

c.)

$$T(z) + z = \alpha^{10} \cdot z + \alpha^{13} \Rightarrow R(z) = \sqrt{\alpha^{13} + z \cdot \alpha^{10}} \bmod G(z).$$

$$\begin{aligned} R(z) &= \alpha^{14} + w(z) \cdot \alpha^5 \\ &= \alpha^{14} + (z + \alpha^9) \cdot \alpha^5 \\ \Rightarrow R(z) &= \alpha^5 \cdot z \ . \end{aligned}$$

d.)

$$\begin{aligned} a(z) &= \alpha^5 \cdot z \\ b(z) &= 1 \\ \sigma(z) &= a(z)^2 + z \cdot b(z)^2 \\ \Rightarrow \sigma(z) &= \alpha^{10} z^2 + z \ . \end{aligned}$$

e.) Die Nullstellen von $\sigma(z)$ sind $\alpha_0 = 0$ und $\alpha^{-10} = \alpha^5 = \alpha_6$.

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

Lösung Aufgabe 9:
a.)

$$\begin{aligned} S_1 = r(\alpha) &= 6 \cdot 5^7 + 5^6 = 6 \cdot 17 + 8 \equiv 18 \bmod 23 \\ S_3 = r(\alpha^3) &= 6 \cdot 10^7 + 10^6 \equiv 6 \cdot 14 + 6 \equiv 21 \bmod 23 \end{aligned}$$

$$\Rightarrow \tilde{S}(z) = 18z + 21z^3.$$

b.)

$$\begin{aligned} U_1 &= -S_1 = 5 \\ U_3 &= \frac{-S_3 + U_1^2 S_1}{3} = \frac{2 + 25 \cdot (-5)}{3} \equiv -41 \equiv 5 \bmod 23 \end{aligned}$$

$$\Rightarrow U(z) = 5z + 5z^3.$$

c.)

$$\begin{aligned} 1 + T(z^2) &= \frac{1}{1 + 5z^2 + 5z^4} = 1 + (-5z^2 - 5z^4) + (-5z^2 - 5z^4)^2 + \ldots \\ &= 1 - 5z^2 - 5z^4 + 25z^4 \ldots \\ &= 1 - 5z^2 + 20z^4 + \ldots \end{aligned}$$

$$\Rightarrow 1 + T(z) = 1 - 5z + 20z^2 + z^3(\ldots) \ .$$

d.)
Durchführen des erweiterten Euklidschen Algorithmus führt zu

$$2z - 2 = -1 \cdot z^3 + (15z - 2) \cdot (20z^2 - 5z + 1) \ .$$

Hieraus folgt

$$\begin{aligned} 2z - 2 &\equiv (15z - 2) \cdot (20z^2 - 5z + 1) \bmod z^3 \\ \Rightarrow \omega(z) = \ 2z - 2 \qquad & \phi(z) = 15z - 2 \ . \end{aligned}$$

e.)

$$\begin{aligned}\hat{\sigma} &= \omega(z^2) = 2z^2 - 2 \\ \tilde{\sigma} &= \frac{\phi(z^2) - \hat{\sigma}(z)}{z} = \frac{15z^2 - 2 - (2z^2 - 2)}{z} = 13z\end{aligned}$$

$$\Rightarrow \sigma(z) = 2z^2 + 13z - 2 = 2(z^2 - 5z - 1) \ .$$

f.) Das Polynom $\sigma(z)$ hat die Nullstellen $z_1 = 8$ und $z_2 = 20$. Da $8 \equiv \alpha^6$ und $20 \equiv \alpha^5$ und somit $\alpha^{16} = \alpha^{-6}$ und $\alpha^{17} = \alpha^{-5}$, liegen die Fehlerstellen an den Positionen 5 und 6 mit dem Fehlerwert -1.

$$\begin{aligned}e(x) &= -x^6 - x^5 \\ c(x) &= 6x^7 + 2x^6 + x^5 \ .\end{aligned}$$