Prüfung: Algebraische Codierung für die sichere Datenübertragung

Dr.-Ing. Klaus Huber

02.03.2010 Ruhr-Universität-Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

Aufgabe 1: Ergänzen Sie die nachfolgende Galoisfeldtabelle des Körpers $GF(2^5)$. Bestimmen Sie zunächst das verwendete primitive Polynom.

$p(x) =$

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					
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}	1	0	0	1	1
15	α^{15}	1	1	0	1	1
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:

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

$$\alpha^{14} + \alpha^{24} =$$

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

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

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

$$\alpha^{20} \cdot \alpha^{18} =$$

$$\alpha^{26} \cdot \alpha^{-29} =$$

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

Aufgabe 4: Sie wollen einen binären BCH-Code der Länge $n = 1023$ konstruieren, der mindestens 6 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:

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\} \\ C_3 &= \{3, 6, 12, 24, 48, 96, 192, 384, 768, 513\} \\ C_5 &= \{5, 10, 20, 40, 80, 160, 320, 640, 257, 514\} \\ &= \{ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \} \\ &= \{ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \} \\ &= \{ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \} \end{aligned}$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

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

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

Aufgabe 5: Gegeben sei der binäre [31,21,5]-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 $GF(2^5)$ aus Aufgabe 1 gebildet werden.
Das empfangene Polynom $r(x) = x^{10} + x^9 + x^4 + x^3$ 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?
Beim Auftreten eines einzelnen Bitfehlers gilt $S_3 = S_1^3$.

richtig: ☐ falsch: ☐

c:) Bestimmen Sie das Fehlerpolynom $e(x)$ und das Codewort $c(x)$:

$e(x) =$

$c(x) =$

Aufgabe 6: Gegeben sei der Körper $GF(2^5)$ gemäß Aufgabe 1. Das Goppa Polynom $G(z) = z^2 + z + \alpha^{11}$ mit

$$L = GF(2^5) - \{\text{Nullstellen von } G(z) \text{ in } GF(2^5)\}$$

bestimmt einen binären Goppa Code.

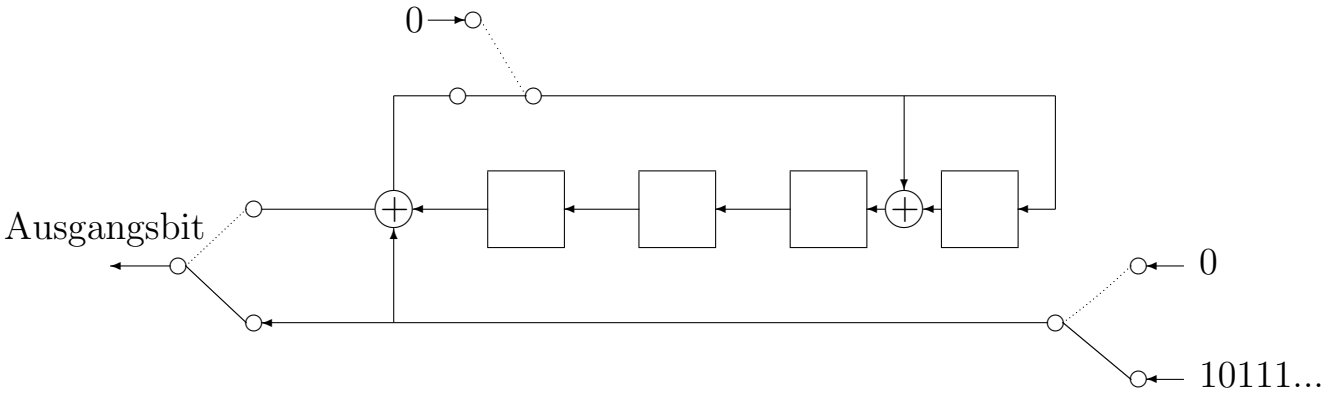
Ergänzen Sie nachfolgend die Gleichung bzw. Ungleichungen für Länge n, Mindestdistanz d sowie Anzahl der Informationsstellen k des Codes.

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

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 (siehe Vorlesung vom 20.11.2009, Folie 5).

Benutzen Sie die nachfolgende Schieberegisterschaltung und codieren Sie die Datenfolge 10111011101. 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	1				1
4	1				0
5	1				
6	0				
7					
8					
9					
10					
11					
12					
13					
14					
15					

Aufgabe 8: Decodieren Sie den Binärvektor

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

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 (siehe z.B. Aufgabe 21, Vorlesung vom 18.12.2009, Folie 29).

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

$$r(x) = 4\,x^4$$

zum nächsten Codewort des $[6, 4, 5]$ negazyklischen Codes über $GF(13)$, der mit dem Generatorpolynom $g(x) = (x-2)\cdot(x-2^3)$ 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 $c(x)$:

$$e(x) =$$

$$c(x) =$$

Lösung Aufgabe 1:

$p(x) = x^5 + x^4 + x^3 + x^2 + 1$

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

Lösung Aufgabe 2:

$$\alpha^{14} + \alpha^{3} = \alpha^{15}$$

$$\alpha^{14} + \alpha^{24} = \alpha^{30}$$

$$\alpha^{14} + \alpha^{18} = \alpha^{1}$$

Lösung Aufgabe 3:

$$\alpha^{19} \cdot \alpha^{17} = \alpha^{5}$$

$$\alpha^{20} \cdot \alpha^{18} = \alpha^{7}$$

$$\alpha^{26} \cdot \alpha^{-29} = \alpha^{28}$$

Lösung Aufgabe 4:

a.) Für die Mindestdistanz gilt $d \geq$ entworfende Distanz $= 13$.

b.)

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\} \\ C_3 &= \{3, 6, 12, 24, 48, 96, 192, 384, 768, 513\} \\ C_5 &= \{5, 10, 20, 40, 80, 160, 320, 640, 257, 514\} \\ C_7 &= \{7, 14, 28, 56, 112, 224, 448, 896, 769, 515\} \\ C_9 &= \{9, 18, 36, 72, 144, 288, 576, 129, 258, 516\} \\ C_{11} &= \{11, 22, 44, 88, 176, 352, 704, 385, 770, 517\} \end{aligned}$$

c.) Es gilt $k = 963$.

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

Lösung Aufgabe 5:

a.)

$$\begin{aligned} S_1 &= \alpha^{10} + \alpha^9 + \alpha^4 + \alpha^3 = \alpha^{13} \\ S_3 &= \alpha^{30} + \alpha^{27} + \alpha^{12} + \alpha^9 = \alpha^8 \end{aligned}$$

b.) richtig

c.) Da $S_3 = S_1^3$ folgt

$$e(x) = x^{13} \quad \text{und} \quad c(x) = x^{13} + x^{10} + x^9 + x^4 + x^3 \ .$$

Lösung Aufgabe 6:

$\mathrm{tr}(\alpha^{11}) = \alpha^{11} + \alpha^{22} + \alpha^{13} + \alpha^{26} + \alpha^{21} = 0$, d.h. das Goppa Polynom hat zwei Nullstellen im Körper $GF(2^5)$.

$$\begin{aligned} \Rightarrow n &= |L| = 30 \\ d &\geq 5 \\ k &\geq 30 - 2 \cdot 5 = 20. \end{aligned}$$

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	1	1	1	1	1
4	1	1	1	1	0
5	1	1	1	0	0
6	0	1	0	1	1
7	1	0	1	1	0
8	1	1	1	1	1
9	1	1	1	1	0
10	0	1	1	1	1
11	1	1	1	1	0
12	1	1	1	0	0
13	1	1	0	0	0
14	1	0	0	0	0
15	0	0	0	0	0

Lösung Aufgabe 8:
a.)

$$\begin{aligned} S(z) &= \frac{1}{z-\alpha_2} + \frac{1}{z-\alpha_6} + \frac{1}{z-\alpha_{11}} + \frac{1}{z-\alpha_{12}} \\ &= \alpha^4 z + \alpha^8 + \alpha z + \alpha^{11} + \alpha z + \alpha^6 + \alpha^2 z + \alpha^{14} \\ &= (\alpha^4 + \alpha + \alpha + \alpha^2) z + (\alpha^8 + \alpha^{11} + \alpha^6 + \alpha^{14}) \\ \Rightarrow S(z) &= \alpha^{10} \cdot z + \alpha^{11} \ . \end{aligned}$$

b.)

$$(z^2 + z + \alpha^3) : (\alpha^{10} z + \alpha^{11}) = \alpha^5 z + \alpha^9 \ \text{ Rest } \alpha^{11}.$$

d.h.

$$\begin{aligned} \alpha^{11} &= 1 \cdot G(z) + (\alpha^5 z + \alpha^9) \cdot S(z) \\ \Rightarrow 1 &\equiv (\alpha^9 z + \alpha^{13}) \cdot S(z) \bmod G(z). \end{aligned}$$

$$\Rightarrow T(z) = \alpha^9 z + \alpha^{13} \ .$$

c.)

$$T(z) + z = \alpha^7 \cdot z + \alpha^{13} \Rightarrow R(z) = \sqrt{\alpha^{13} + z \cdot \alpha^7} \bmod G(z).$$

$$\begin{aligned} R(z) &= \alpha^{14} + w(z) \cdot \alpha^{11} \\ &= \alpha^{14} + (z + \alpha^9) \cdot \alpha^{11} \\ \Rightarrow R(z) &= \alpha^{11} \cdot z + \alpha^{12} \ . \end{aligned}$$

d.)

$$\begin{aligned} a(z) &= \alpha^{11} \cdot z + \alpha^{12} \\ b(z) &= 1 \\ \sigma(z) &= a(z)^2 + z \cdot b(z)^2 = \alpha^7 z^2 + \alpha^9 + z \\ \Rightarrow \sigma(z) &= \alpha^7 z^2 + z + \alpha^9 \ . \end{aligned}$$

e.) Die Nullstellen von $\sigma(z)$ sind $\alpha_1 = 1$ und $\alpha_3 = \alpha^2$.

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

Lösung Aufgabe 9:
a.)

$$\begin{aligned} S_1 &= r(\alpha) = 4 \cdot 2^4 \equiv -1 \bmod 13 \\ S_3 &= r(\alpha^3) = 4 \cdot 8^4 \equiv 4 \bmod 13 \\ &\Rightarrow \tilde{S}(z) = -z + 4z^3. \end{aligned}$$

b.)

$$\begin{aligned} U_1 &= -S_1 = 1 \\ U_3 &= \frac{-S_3 + U_1^2 S_1}{3} = \frac{9 + 1 \cdot -1}{3} \equiv \frac{8}{3} \equiv 7 \bmod 13 \\ &\Rightarrow U(z) = z + 7z^3. \end{aligned}$$

c.)

$$\begin{aligned} 1 + T(z^2) &= \frac{1}{1 + z^2 + 7z^4} = 1 + (-z^2 + 6z^4) + (-z^2 + 6z^4)^2 + \ldots \\ &= 1 - z^2 + 6z^4 + z^4 + \ldots \\ &= 1 - z^2 + 7z^4 + \ldots \\ &\Rightarrow 1 + T(z) = 1 - z + 7z^2 + z^3(\ldots) \ . \end{aligned}$$

d.)
Durchführen des erweiterten Euklidschen Algorithmus führt zu

$$2z - 4 = 1 \cdot z^3 - (2z + 4) \cdot (7z^2 - z + 1) \ .$$

Hieraus folgt

$$\begin{aligned} 2z - 4 &\equiv (11z + 9) \cdot (z^2 + 2z + 1) \bmod z^3 \\ \Rightarrow \omega(z) = \ 2z - 4 \qquad & \phi(z) = 11z + 9 \ . \end{aligned}$$

e.)

$$\begin{aligned} \hat{\sigma} &= \omega(z^2) = 2z^2 - 4 \\ \tilde{\sigma} &= \frac{\phi(z^2) - \hat{\sigma}(z)}{z} = \frac{11z^2 + 9 - (2z^2 - 4}{z} = 9z \end{aligned}$$

$$\Rightarrow \sigma(z) = 2z^2 + 9z - 4 \ .$$

f.) Das Polynom $\sigma(z)$ hat die Nullstellen $z_1 = 5$ und $z_2 = 10$. Da $5 \equiv \alpha^9$ und $10 \equiv \alpha^{10}$ und somit $\alpha^9 = \alpha^{-3}$ und $\alpha^{10} = \alpha^{-2}$, liegen die Fehlerstellen bei den Positionen 2 und 3 mit Fehlerwert 1.

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