

*Prüfung: Algebraische Codierung für die
sichere Datenübertragung*

Dr.-Ing. Klaus Huber

06.03.2009 Ruhr-Universität-Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

Aufgabe 1: Für die Konstruktion des Körpers $GF(2^5)$ wird das primitive Polynom $p(x) = x^5 + x^4 + x^2 + x + 1$ benutzt. Ergänzen Sie die fehlenden 5-Tupel in der nachfolgenden Tabelle.

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	0	1	1	1
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	0	1
15	α^{15}					
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:

$$\alpha^{14} + \alpha^4 =$$

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

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

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

$$\alpha^{15} \cdot \alpha^{18} =$$

$$\alpha^{27} \cdot \alpha^9 =$$

$$\alpha^{23} \cdot \alpha^{-27} =$$

Hinweis: Im Ergebnis sollen die Exponenten jeweils aus der Menge $\{0, 1, 2, \dots, 30\}$ 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 Minstdistanz gilt $d \geq$ entwerfende Distanz = .

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

$$\begin{aligned} C_1 &= \{1, 2, 4, 8, 16, 32, 64, 128\} \\ C_3 &= \{3, 6, 12, 24, 48, 96, 192, 129\} \\ C_5 &= \{5, 10, 20, 40, 80, 160, 65, 130\} \\ &= \{ \} \\ &= \{ \} \\ &= \{ \} \\ &= \{ \} \\ &= \{ \} \\ &= \{ \} \end{aligned}$$

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

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

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

e.) Bestimmen Sie die Minimalpolynome von α und α^{17} .

$$m_1(x) =$$

$$m_{17}(x) =$$

Hinweis: Benutzen Sie zur Bestimmung von $m_1(x)$ und $m_{17}(x)$ den Körper $GF(2^8)$ mit dem primitiven Polynom $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. Es gilt $p(\alpha) = 0$ und $\alpha^{17} + \alpha^{34} + \alpha^{68} + \alpha^{136} = 0$.

Aufgabe 5: Bestimmen Sie das Generatorpolynom eines $[31,28,4]$ -Reed-Solomon Codes über dem Körper $GF(2^5)$. Benutzen Sie hierzu die Tabelle aus Aufgabe 1.

$$g(x) =$$

Hinweis: Die Koeffizienten von $g(x)$ sollen als Potenzen von α angegeben werden.

Aufgabe 6: Gegeben sei der Körper $GF(2^5)$. Das Goppa Polynom $G(z) = z^3 + 1$ 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.

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

Aufgabe 7: Die nachfolgend angegebene Prüfmatrix $\mathbf{H}$ beschreibt einen nichtbinären $[14, 12, 3]$ Hamming Code über $GF(13)$ in systematischer Form.

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 & 1 \end{pmatrix}$$

a.) Bestimmen Sie die zugehörige Generatormatrix $\mathbf{G}$.

$$\mathbf{G} =$$

b.) Decodieren Sie die Vektoren

$$\mathbf{r}_1 = (4, 2, 3, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\mathbf{r}_2 = (4, 3, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

zu den nächsten Codewörtern $\mathbf{c}_1$ und $\mathbf{c}_2$:

$$\mathbf{c}_1 =$$

$$\mathbf{c}_2 =$$

c.) Codieren Sie die Nachrichtenvektoren

$$\mathbf{m}_a = (1, 2, 3, 4, 5, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\mathbf{m}_b = (2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

$$\mathbf{c}_a =$$

$$\mathbf{c}_b =$$

Aufgabe 8: Decodieren Sie den Binärvektor

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

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

Hinweis: Es handelt sich um den Code, der in der Vorlesung behandelt wurde (siehe z.B. Aufgabe 21, Vorlesung vom 19.12.2008, 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 das Fehlerstellenpolynom $\sigma(z)$:

$$\sigma(z) =$$

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

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Aufgabe 9: Decodieren Sie das Polynom

$$r(x) = 5x + 3$$

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.

Hinweis: Es handelt sich um den Code, der in der Vorlesung behandelt wurde (siehe z.B. Aufgabe 24, Folie 1, 23.01.2009).

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 $\omega(z)$

$$\phi(z) =$$

$$\omega(z) =$$

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:

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

Lösung Aufgabe 2:

$$\alpha^{14} + \alpha^4 = \alpha^0 = 1$$

$$\alpha^{14} + \alpha^{24} = \alpha^{10}$$

$$\alpha^{14} + \alpha^{18} = \alpha^{28}$$

Lösung Aufgabe 3:

$$\alpha^{15} \cdot \alpha^{18} = \alpha^2$$

$$\alpha^{27} \cdot \alpha^9 = \alpha^5$$

$$\alpha^{23} \cdot \alpha^{-27} = \alpha^{27}$$

Lösung Aufgabe 4:

a.) Für die Minstdistanz gilt $d \geq$ entwerfende 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 $k = 187$.

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

e.) Das Minimalpolynom $m_1(x)$ ist gleich dem primitiven Polynom mit dem der Körper konstruiert wurde.

$$m_1(x) = x^8 + x^4 + x^3 + x^2 + 1$$

$$m_{17}(x) = (x - \alpha^{17}) \cdot (x - \alpha^{34}) \cdot (x - \alpha^{68}) \cdot (x - \alpha^{36}).$$

Koeffizient bei x^4 : 1

Koeffizient bei x^3 : $\alpha^{17} + \alpha^{34} + \alpha^{68} + \alpha^{236} = 0$

Koeffizient bei x^0 : 1 .

Daß der Koeffizient bei x^2 gleich 0 und der Koeffizient bei x gleich 1 ist folgt ohne Rechnung, da nur das Polynom $x^4 + x + 1$ irreduzibel ist. In den anderen Fällen bei denen der Koeffizient von x^3 gleich Null ist erhält man reduzible binäre Polynome.

$$\Rightarrow m_{17}(x) = x^4 + x + 1 .$$

Lösung Aufgabe 5:

$$\begin{aligned}g(x) &= (x + \alpha) \cdot (x + \alpha^2) \cdot (x + \alpha^3) \\&= (x^2 + (\alpha + \alpha^2)x + \alpha^3) \cdot (x + \alpha^3) \\&= x^3 + (\alpha + \alpha^2 + \alpha^3)x^2 + ((\alpha + \alpha^2) \cdot \alpha^3 + \alpha^3) \cdot x + \alpha^6 \\&= x^3 + \alpha^{24}x^2 + (\alpha^4 + \alpha^5 + \alpha^3) \cdot x + \alpha^6 \\&= x^3 + \alpha^{24}x^2 + (1 + \alpha + \alpha^2 + \alpha^3) \cdot x + \alpha^6 \\ \Rightarrow g(x) &= x^3 + \alpha^{24}x^2 + \alpha^{26}x + \alpha^6 .\end{aligned}$$

Lösung Aufgabe 6:

$$\begin{aligned}n &= |L| = 31 \\d &\geq 7 \\k &\geq 16.\end{aligned}$$

Lösung Aufgabe 7:

a.)

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 12 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 11 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 10 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 8 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 12 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 12 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 12 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 12 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 12 & 1 \end{pmatrix}$$

b.)

$$\begin{aligned} \mathbf{H} \cdot \mathbf{r}_1^\top &= \binom{4}{4} + \binom{2}{4} + \binom{3}{9} + \binom{4}{3} = 7 \binom{0}{1} \\ \Rightarrow \mathbf{e}_1 &= (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7) \end{aligned}$$

$$\Rightarrow \mathbf{c}_1 = (4, 2, 3, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6)$$

$$\begin{aligned} \mathbf{H} \cdot \mathbf{r}_2^\top &= \binom{4}{4} + \binom{3}{6} + \binom{2}{6} + \binom{1}{4} = 10 \binom{1}{2} \\ \Rightarrow \mathbf{e}_2 &= (0, 10, 0, 0, 0, 0, 0, 6, 0, 0, 0, 0, 0, 0) \end{aligned}$$

$$\Rightarrow \mathbf{c}_2 = (4, 6, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

c.)

$$\mathbf{c}_a = (1, 2, 3, 4, 5, 0, 0, 0, 0, 0, 0, 0, 0, 11, 10)$$

$$\mathbf{c}_b = (2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 3, 9).$$

Lösung Aufgabe 8:

a.)

$$\begin{aligned}
 S(z) &= \frac{1}{z - \alpha_1} + \frac{1}{z - \alpha_7} + \frac{1}{z - \alpha_8} + \frac{1}{z - \alpha_9} + \frac{1}{z - \alpha_{13}} + \frac{1}{z - \alpha_{14}} \\
 &= \alpha^{12}z + \alpha^8z + \alpha^6 + \alpha^6z + 1 + \alpha^3z + \alpha^5 + \alpha^2z + \alpha^{13} + \alpha^8z + \alpha^{14} \\
 &= (\alpha^{12} + \alpha^8 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha^8)z + (\alpha^6 + 1 + \alpha^5 + \alpha^{13} + \alpha^{14}) \\
 \Rightarrow S(z) &= \alpha^{12} \cdot z + \alpha^{12} .
 \end{aligned}$$

b.)

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

d.h.

$$\begin{aligned}
 \alpha^3 &= 1 \cdot G(z) + (\alpha^3z) \cdot S(z) \\
 \Rightarrow 1 &\equiv z \cdot S(z) \text{ mod } G(z).
 \end{aligned}$$

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

c.)

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

d.) Die Nullstelle von $\sigma(z) = z$ ist gleich α_0 .

$$\Rightarrow \mathbf{e} = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\Rightarrow \mathbf{c} = (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$$

Lösung Aufgabe 9:

a.)

$$\begin{aligned} S_1 &= r(\alpha) = 5 \cdot 2 + 3 \equiv 2 \pmod{11} \\ S_3 &= r(\alpha^3) = 5 \cdot 8 + 3 \equiv 10 \pmod{11} \\ &\Rightarrow \tilde{S}(z) = 2z + 10z^3. \end{aligned}$$

b.)

$$\begin{aligned} U_1 &= -S_1 = 9 \\ U_3 &= \frac{-S_3 + U_1^2 S_1}{3} = \frac{1 + 4 \cdot 2}{3} \equiv \frac{9}{3} \equiv 3 \pmod{11} \\ &\Rightarrow U(z) = 9z + 3z^3. \end{aligned}$$

c.)

$$\begin{aligned} 1 + T(z^2) &= \frac{1}{1 + 9z^2 + 3z^4} = 1 + (2z^2 + 8z^4) + (2z^2 + 8z^4)^2 + \dots \\ &= 1 + 2z^2 + 8z^4 + 4z^4 + \dots \\ &= 1 + 2z^2 + z^4 + \dots \\ &\Rightarrow 1 + T(z) = 1 + 2z + z^2 + z^3(\dots). \end{aligned}$$

d.)

Durchführen des erweiterten Euklidschen Algorithmus führt zu

$$3z + 2 = 1 \cdot z^3 - (z + 9) \cdot (z^2 + 2z + 1).$$

Hieraus folgt

$$\begin{aligned} 3z + 2 &\equiv (10z + 2) \cdot (z^2 + 2z + 1) \pmod{z^3} \\ \Rightarrow \omega(z) &= 3z + 2 \quad \phi(z) = 10z + 2. \end{aligned}$$

e.)

$$\begin{aligned} \hat{\sigma} &= \omega(z^2) = 3z^2 + 2 \\ \tilde{\sigma} &= \frac{\phi(z^2) - \hat{\sigma}(z)}{z} = \frac{10z^2 + 2 - 3z^2 - 2}{z} = 7z \end{aligned}$$

$$\Rightarrow \sigma(z) = 3z^2 + 7z + 2 .$$

f.) Das Polynom $\sigma(z)$ hat die Nullstellen $z_1 = 7$ und $z_2 = 9$. Da $7 \equiv \alpha^7$ und $9 \equiv \alpha^6$ und somit $\alpha^3 = \alpha^{-7}$ und $\alpha^4 = \alpha^{-6}$, liegen die Fehlerstellen bei den Positionen 3 und 4 mit Fehlerwert 1.

$$\begin{aligned} e(x) &= x^4 + x^3 \\ c(x) &= -x^4 - x^3 + 5x + 3 . \end{aligned}$$