*Prüfung: Algebraische Codierung für die
sichere Datenübertragung*

Dr.-Ing. Klaus Huber

07.08.2015 Ruhr-Universität Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

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

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

$$\alpha^{30} + \alpha^{62} =$$

$$\alpha^{39} + \alpha^{48} =$$

$$\alpha^{22} + \alpha^{45} =$$

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

$$\alpha^{23} \cdot \alpha^{31} =$$

$$\alpha^{17} \cdot \alpha^{58} =$$

$$\alpha^{13} \cdot \alpha^{-51} =$$

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

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 $G(z) = (z^2 + z + \alpha^5) \cdot (z^2 + z + \alpha^{11})$ 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: Bestimmen Sie für binäre Codes der Länge $n = 16$ die sich durch die Hamming Schranke ergebenden Werte für die obere Schranke der Anzahl der Fehler t , die korrigiert werden können und tragen Sie diese in die Tabelle ein.

k	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
t															

Hinweis: Die Hamming Schranke für binäre Codes der Länge n , die t Fehler korrigieren können lautet

$$\sum_{j=0}^t \binom{n}{j} \leq 2^{n-k}$$

(siehe Vorlesung vom 17.10.2014, Folie 20 und 31.10.2014, Folie 19).

Aufgabe 8: Decodieren Sie den Binärvektor

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

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.

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 den Fehlervektor $\mathbf{e}$ und das Codewort $\mathbf{c}$:

$$\mathbf{e} =$$

$$\mathbf{c} =$$

Aufgabe 9: Decodieren Sie das Polynom

$$r(x) = 11x^2 + 10x$$

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

Lösung Aufgabe 2:

$$\alpha^{29} + \alpha^{61} = \alpha^{33}$$

$$\alpha^{47} + \alpha^{50} = \alpha^{21}$$

$$\alpha^{15} + \alpha^{24} = \alpha^{37}$$

Lösung Aufgabe 3:

$$\alpha^{29} \cdot \alpha^{32} = \alpha^{54}$$

$$\alpha^{12} \cdot \alpha^{59} = \alpha^{12}$$

$$\alpha^{17} \cdot \alpha^{-49} = \alpha^{25}$$

Lösung Aufgabe 4:

a.) Für die Mindestdistanz gilt $d \geq$ entwerfende Distanz = 11.

b.)

$$C_1 = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048\}$$

$$C_3 = \{3, 6, 12, 24, 48, 96, 192, 384, 768, 1536, 3072, 2049\}$$

$$C_5 = \{5, 10, 20, 40, 80, 160, 320, 640, 1280, 2560, 1025, 2050\}$$

$$C_7 = \{7, 14, 28, 56, 112, 224, 448, 896, 1792, 3584, 3073, 2051\}$$

$$C_9 = \{9, 18, 36, 72, 144, 288, 576, 1152, 2304, 513, 1026, 2052\}$$

c.) Es gilt $k = 4095 - 5 \cdot 12 = 4035$.

d.) $g(x) = m_1 \cdot m_3 \cdot m_5 \cdot m_7 \cdot m_9$.

Lösung Aufgabe 5:

Um drei Fehler erkennen zu können, muss die Mindestdistanz d gleich 4 sein.

$$\begin{aligned}g(x) &= (x - \alpha) \cdot (x - \alpha^2) \cdot (x - \alpha^3) \\ &= x^3 + (\alpha^3 + \alpha^2 + \alpha) \cdot x^2 + (\alpha^{2+3} + \alpha^{1+3} + \alpha^{1+2}) \cdot x + \alpha^{1+2+3} \\ &= x^3 + \alpha^{27} \cdot x^2 + \alpha^{29} \cdot x + \alpha^6 .\end{aligned}$$

Lösung Aufgabe 6:

Es gilt

$$\begin{aligned}\text{tr}(\alpha^5) &= \alpha^5 + \alpha^{10} + \alpha^{20} + \alpha^{40} + \alpha^{17} + \alpha^{34} = 1 \\ \text{und} \quad \text{tr}(\alpha^{11}) &= \alpha^{11} + \alpha^{22} + \alpha^{44} + \alpha^{25} + \alpha^{50} + \alpha^{37} = 1 ,\end{aligned}$$

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

$$\Rightarrow n = |L| = 64$$

$$d \geq 9$$

$$k \geq 64 - 4 \cdot 6 = 40.$$

Lösung Aufgabe 7:

$$\binom{16}{0} = 1 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 16$$

$$\binom{16}{0} + \binom{16}{1} = 17 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 11$$

$$\binom{16}{0} + \binom{16}{1} + \binom{16}{2} = 137 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 8$$

$$\sum_{j=0}^3 \binom{16}{j} = 697 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 6$$

$$\sum_{j=0}^4 \binom{16}{j} = 2517 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 4$$

$$\sum_{j=0}^5 \binom{16}{j} = 6885 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 3$$

$$\sum_{j=0}^6 \binom{16}{j} = 14893 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 2$$

$$\sum_{j=0}^7 \binom{16}{j} = 30909 \leq 2^{16-k} \quad \Rightarrow \quad k \leq 1$$

Somit erhält man die Tabelle:

k	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
t	0	0	0	0	1	1	1	2	2	3	3	4	5	6	7

Lösung Aufgabe 8:

a.)

$$\begin{aligned} S(z) &= \frac{1}{z - \alpha_1} + \frac{1}{z - \alpha_4} + \frac{1}{z - \alpha_7} + \frac{1}{z - \alpha_{14}} + \frac{1}{z - \alpha_{15}} \\ &= \alpha^{12}z + \alpha^9z + \alpha^8 + \alpha^8z + \alpha^6 + \alpha^8z + \alpha^{14} + \alpha^9z + \alpha^{12} \\ &= (\alpha^{12} + \alpha^9 + \alpha^8 + \alpha^8 + \alpha^9)z + (\alpha^8 + \alpha^6 + \alpha^{14} + \alpha^{12}) \\ \Rightarrow S(z) &= \alpha^{12} \cdot z + \alpha^{12} . \end{aligned}$$

b.)

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

d.h.

$$\alpha^3 \equiv (\alpha^3z) \cdot S(z) \text{ mod } G(z)$$

$$\Rightarrow 1 \equiv z \cdot S(z) \text{ mod } G(z).$$

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

c.)

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

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

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

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

Lösung Aufgabe 9:

a.)

$$S_1 = r(\alpha) = 11 \cdot 2^2 + 10 \cdot 2 \equiv -1 \pmod{13}$$

$$S_3 = r(\alpha^3) = 11 \cdot 8^2 + 10 \cdot 8 \equiv 4 \pmod{13}$$

$$\Rightarrow \tilde{S}(z) = -z + 4z^3 .$$

b.) Die Berechnung von $\sigma(z)$ erfolgt in gleicher Weise wie bei der Prüfung 2010, Aufgabe 9 mit Berlekamps Algorithmus oder nachfolgend mit Roths Algorithmus.

Roths Algorithmus liefert zunächst das Polynom $V(z) = 1 + 2z + 2z^2 + 3z^3 + 4z^4$. Durchführen des Euklidischen Algorithmus liefert:

$$\begin{aligned} z^5 &= (10z - 1) \cdot (4z^4 + 3z^3 + 2z^2 + 2z + 1) + 9z^3 + 8z^2 + 5z + 1 \\ 4z^4 + 3z^3 + 2z^2 + 2z + 1 &= (-z + 7) \cdot (9z^3 + 8z^2 + 5z + 1) + 3z^2 + 7z + 7 \end{aligned}$$

$$\Rightarrow \sigma(z) = \text{const} \cdot (3z^2 + 7z + 7) .$$

c.) Das Polynom $\sigma(z)$ hat die Nullstellen 5 und 10. Da $5 \equiv 2^9$ und $10 \equiv 2^{10}$ und somit $2^9 \equiv 2^{-3}$ und $2^{10} = 2^{-2}$, erhält man das Fehlerpolynom und schließlich das Codewortpolynom.

$$e(x) = x^3 + x^2$$

$$c(x) = -x^3 + 10x^2 + 10x .$$