Prüfung: Algebraische Codierung für die sichere Datenübertragung

Dr.-Ing. Klaus Huber

07.03.2012 Ruhr-Universität Bochum

Prüfungsteilnehmer/in

Vorname:

Name:

Matrikelnr.:

DPO:

Aufgabe 1: Für die Konstruktion des Körpers $GF(2^6)$ wird das primitive Polynom $p(x) = x^6+x^5+1$ 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	1	0	1	0
1	α	0	0	0	0	1	0	33	α^{33}	1	1	0	1	0	0
2	α^2	0	0	0	1	0	0	34	α^{34}	0	0	1	0	0	1
3	α^3	0	0	1	0	0	0	35	α^{35}	0	1	0	0	1	0
4	α^4	0	1	0	0	0	0	36	α^{36}	1	0	0	1	0	0
5	α^5	1	0	0	0	0	0	37	α^{37}	1	0	1	0	0	1
6	α^6	1	0	0	0	0	1	38	α^{38}	1	1	0	0	1	1
7	α^7							39	α^{39}						
8	α^8							40	α^{40}						
9	α^9	1	0	1	1	1	1	41	α^{41}						
10	α^{10}							42	α^{42}						
11	α^{11}							43	α^{43}	0	1	0	0	0	1
12	α^{12}							44	α^{44}						
13	α^{13}							45	α^{45}						
14	α^{14}	1	1	1	0	1	0	46	α^{46}	1	0	1	0	1	1
15	α^{15}							47	α^{47}	1	1	0	1	1	1
16	α^{16}							48	α^{48}	0	0	1	1	1	1
17	α^{17}							49	α^{49}	0	1	1	1	1	0
18	α^{18}	0	0	1	0	1	1	50	α^{50}	1	1	1	1	0	0
19	α^{19}							51	α^{51}	0	1	1	0	0	1
20	α^{20}							52	α^{52}	1	1	0	0	1	0
21	α^{21}							53	α^{53}	0	0	0	1	0	1
22	α^{22}							54	α^{54}	0	0	1	0	1	0
23	α^{23}	1	0	0	1	1	0	55	α^{55}	0	1	0	1	0	0
24	α^{24}	1	0	1	1	0	1	56	α^{56}	1	0	1	0	0	0
25	α^{25}	1	1	1	0	1	1	57	α^{57}	1	1	0	0	0	1
26	α^{26}	0	1	0	1	1	1	58	α^{58}	0	0	0	0	1	1
27	α^{27}	1	0	1	1	1	0	59	α^{59}						
28	α^{28}	1	1	1	1	0	1	60	α^{60}						
29	α^{29}	0	1	1	0	1	1	61	α^{61}						
30	α^{30}	1	1	0	1	1	0	62	α^{62}						
31	α^{31}	0	0	1	1	0	1	63	α^{63}						

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

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

$$\alpha^{25} + \alpha^{44} =$$

$$\alpha^{55} + \alpha^{62} =$$

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

$$\alpha^{23} \cdot \alpha^{14} =$$

$$\alpha^{13} \cdot \alpha^{52} =$$

$$\alpha^{53} \cdot \alpha^{-61} =$$

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 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:

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

c.) Wieviele Informationsbits k hat der Code?

Es gilt $k =$.

d.) Das Generatorpolynom hat die folgende Gestalt:

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

Ergänzen Sie in voriger Gleichung die fehlenden Minimalpolynome.

e.) Bestimmen Sie die Minimalpolynome von α und α^9.

$$m_1(x) =$$

$$m_9(x) =$$

Hinweis: Benutzen Sie zur Bestimmung von $m_1(x)$ und $m_9(x)$ die Darstellung des Körpers $GF(2^6)$ aus Aufgabe 1.

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 $r(x) = x^{55} + x^{54} + x^{53} + x^{50} + x^{48} + x^{46}$ 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 Einzelfehlers gilt $S_3 = S_1^3$.

richtig: ☐ falsch: ☐

c:) Prüfen Sie, ob die Bedingung für einen Einzelfehler erfüllt ist und bestimmen Sie in diesem Fall 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 $G(z) = z^2 + z + \alpha^{23}$ mit

$$L = GF(2^6) - \{\text{Nullstellen von } G(z) \text{ in } GF(2^6)\}$$

bestimmt einen binären Goppa Code.

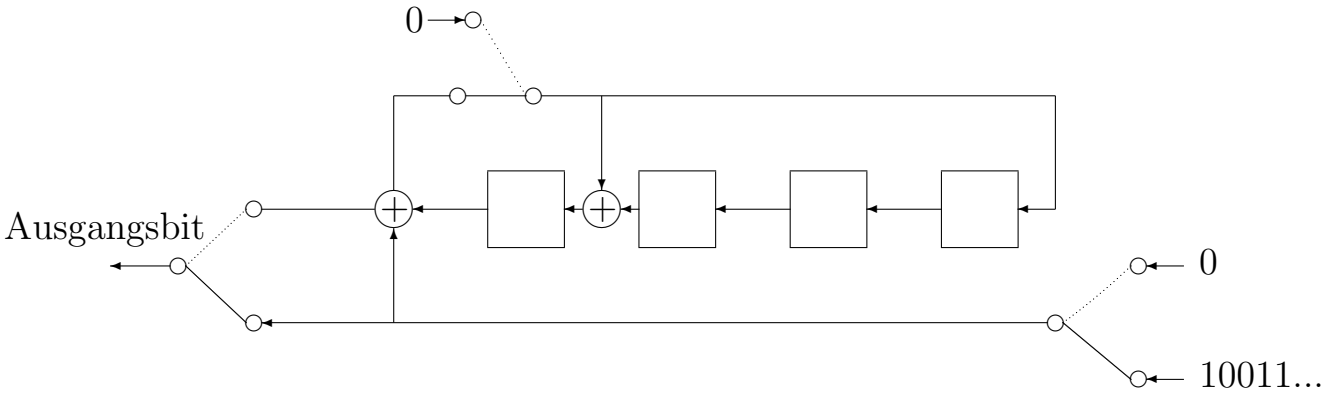
Ergänzen Sie nachfolgend die Gleichung bzw. Ungleichungen für Länge n, Mindestdistanz d sowie Anzahl der Informationsstellen k des Codes.

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

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 $g(x) = x^4+x^3+1$ erzeugt wird.

Benutzen Sie die nachfolgende Schieberegisterschaltung und codieren Sie die Datenfolge 10011101110. 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	1	0	0	1
2	0	1	0	1	1
3	0				
4	1				
5	1				
6	1				
7					
8					
9					
10					
11					
12					
13					
14					
15					

Aufgabe 8: Decodieren Sie den Binärvektor

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

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 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

$$r(x) = x^4 + 13\,x^2$$

zum nächsten Codewort des $[9, 7, 5]$ negazyklischen Codes über $GF(19)$, 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:

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

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

Lösung Aufgabe 2:

$$\alpha^{30} + \alpha^{14} = \alpha^{60}$$

$$\alpha^{25} + \alpha^{44} = \alpha^{51}$$

$$\alpha^{55} + \alpha^{62} = \alpha^{36}$$

Lösung Aufgabe 3:

$$\alpha^{23} \cdot \alpha^{14} = \alpha^{37}$$

$$\alpha^{13} \cdot \alpha^{52} = \alpha^{2}$$

$$\alpha^{53} \cdot \alpha^{-61} = \alpha^{55}$$

Lösung Aufgabe 4:

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

b.)

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

c.) Es gilt $k = 63 - 7 \cdot 6 - 3 = 18$.

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

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

$$m_1(x) = x^6 + x^5 + 1$$

$$m_9(x) = (x - \alpha^9) \cdot (x - \alpha^{18}) \cdot (x - \alpha^{36}) \ .$$

$$\begin{aligned} &\text{Koeffizient bei } x^3\text{:} \quad 1 \\ &\text{Koeffizient bei } x^2\text{:} \quad \alpha^9 + \alpha^{18} + \alpha^{36} = 0 \\ &\text{Koeffizient bei } x^0\text{:} \quad 1 \ . \end{aligned}$$

Daß der Koeffizent bei x gleich 1 ist folgt sofort, da das Polynom $x^3 + 1$ durch $(x + 1)$ teilbar ist.

$$\Rightarrow m_9(x) = x^3 + x + 1 \ .$$

Lösung Aufgabe 5:
a.)

$$\begin{aligned} S_1 &= \alpha^{55} + \alpha^{54} + \alpha^{53} + \alpha^{50} + \alpha^{48} + \alpha^{46} = \alpha^{58} \\ S_3 &= \alpha^{3\cdot 55} + \alpha^{3\cdot 54} + \alpha^{3\cdot 53} + \alpha^{3\cdot 50} + \alpha^{3\cdot 48} + \alpha^{46} \\ &= \alpha^{39} + \alpha^{36} + \alpha^{33} + \alpha^{24} + \alpha^{18} + \alpha^{12} = \alpha^{48} \end{aligned}$$

b.) richtig

c.) $S_3 = S_1^3$ (da $58 \cdot 3 \equiv 48 \bmod 63$) folgt

$$e(x) = x^{58} \quad \text{und} \quad c(x) = x^{58} + x^{55} + x^{54} + x^{53} + x^{50} + x^{48} + x^{46} \ .$$

Lösung Aufgabe 6:

$\mathrm{tr}(\alpha^{23}) = \alpha^{23} + \alpha^{46} + \alpha^{29} + \alpha^{58} + \alpha^{53} + \alpha^{43} = 1$, d.h. das Goppa Polynom hat keine Nullstellen im Körper $GF(2^6)$.

$$\begin{aligned} \Rightarrow n &= |L| = 64 \\ d &\geq 5 \\ k &\geq 64 - 2 \cdot 6 = 52. \end{aligned}$$

Lösung Aufgabe 7:

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

Lösung Aufgabe 8:
a.)

$$\begin{aligned} S(z) &= \frac{1}{z-\alpha_2} + \frac{1}{z-\alpha_7} + \frac{1}{z-\alpha_9} \\ &= \alpha^4 z + \alpha^8 + \alpha^8 z + \alpha^6 + \alpha^3 z + \alpha^5 \\ &= (\alpha^4 + \alpha^8 + \alpha^3) z + (\alpha^8 + \alpha^6 + \alpha^5) \\ \Rightarrow S(z) &= \alpha^{11} \cdot z + \alpha^{12} \ . \end{aligned}$$

b.)

$$(z^2 + z + \alpha^3) : (\alpha^{11} z + \alpha^{12}) = \alpha^4 z + \alpha^8 \ \text{ Rest } \alpha^{11}.$$

d.h.

$$\begin{aligned} \alpha^{11} &= 1 \cdot G(z) + (\alpha^4 z + \alpha^8) \cdot S(z) \\ \Rightarrow 1 &\equiv (\alpha^8 z + \alpha^{12}) \cdot S(z) \bmod G(z). \end{aligned}$$

$$\Rightarrow T(z) = \alpha^8 z + \alpha^{12} \ .$$

c.)

$$T(z) + z = \alpha^2 \cdot z + \alpha^{12} \Rightarrow R(z) = \sqrt{\alpha^{12} + z \cdot \alpha^2} \bmod G(z).$$

$$\begin{aligned} R(z) &= \alpha^6 + w(z) \cdot \alpha \\ &= \alpha^6 + (z + \alpha^9) \cdot \alpha \\ \Rightarrow R(z) &= \alpha \cdot z + \alpha^7 \ . \end{aligned}$$

d.)

$$\begin{aligned} a(z) &= \alpha \cdot z + \alpha^7 \\ b(z) &= 1 \\ \sigma(z) &= a(z)^2 + z \cdot b(z)^2 = \alpha^2 z^2 + \alpha^{14} + z \\ \Rightarrow \sigma(z) &= \alpha^2 z^2 + z + \alpha^{14} \ . \end{aligned}$$

e.) Die Nullstellen von $\sigma(z)$ sind $\alpha_6 = \alpha^5$ und $\alpha_8 = \alpha^7$.

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

Lösung Aufgabe 9:
a.)

$$\begin{aligned} S_1 &= r(\alpha) = 2^4 + 13 \cdot 2^2 = 16 + 13 \cdot 4 \equiv 11 \bmod 19 \\ S_3 &= r(\alpha^3) = 8^4 + 13 \cdot 8^2 \equiv 11 + 13 \cdot 7 \equiv 7 \bmod 19 \end{aligned}$$

$$\Rightarrow \tilde{S}(z) = 11z + 7z^3.$$

b.)

$$\begin{aligned} U_1 &= -S_1 = 8 \\ U_3 &= \frac{-S_3 + U_1^2 S_1}{3} = \frac{-7 + 7 \cdot 11}{3} \equiv 17 \bmod 19 \end{aligned}$$

$$\Rightarrow U(z) = 8z + 17z^3.$$

c.)

$$\begin{aligned} 1 + T(z^2) &= \frac{1}{1 + 8z^2 + 17z^4} = 1 + (-8z^2 - 17z^4) + (-8z^2 - 17z^4)^2 + \ldots \\ &= 1 - 8z^2 - 17z^4 + 7z^4 \ldots \\ &= 1 + 11z^2 + 9z^4 + \ldots \end{aligned}$$

$$\Rightarrow 1 + T(z) = 1 + 11z + 9z^2 + z^3(\ldots) \ .$$

d.)
Durchführen des erweiterten Euklidschen Algorithmus führt zu

$$11z + 6 = 1 \cdot z^3 + (2z + 6) \cdot (9z^2 + 11z + 1) \ .$$

Hieraus folgt

$$\begin{aligned} & 11z + 6 \equiv (2z + 6) \cdot (9z^2 + 11z + 1) \bmod z^3 \\ \Rightarrow \omega(z) = \ & 11z + 6 \qquad \phi(z) = 2z + 6 \ . \end{aligned}$$

e.)

$$\begin{aligned} \hat{\sigma} &= \omega(z^2) = 11z^2 + 6 \\ \tilde{\sigma} &= \frac{\phi(z^2) - \hat{\sigma}(z)}{z} = \frac{2z^2 + 6 - (11z^2 + 6)}{z} = 10z \end{aligned}$$

$$\Rightarrow \sigma(z) = 11z^2 + 10z + 6 \ .$$

f.) Das Polynom $\sigma(z)$ hat die Nullstellen $z_1 = 12$ und $z_2 = 13$. Da $12 \equiv \alpha^{15}$ und $13 \equiv \alpha^5$ und somit $\alpha^3 = \alpha^{-15}$ und $\alpha^{13} = \alpha^{-5}$, liegen die Fehlerstellen an den Positionen 3 und 4 mit den Fehlerwerten 1 und -1.

$$\begin{aligned} e(x) &= -x^4 + x^3 \\ c(x) &= 2x^4 - x^3 + 13x^2 \ . \end{aligned}$$