Musterlösung zur Aufgabe A2.1

a) Mit der Zahlenmenge $Z_3 = \{0, 1, 2\}$ beschreibt

- die Tabelle A3 die additive Gruppe $(Z_3, +)$,
- die Tabelle M3 die multiplikative Gruppe $(Z_3, \cdot)$.

⇒ Lösungsvorschlag 1 und 2. Die Lösungsvorschläge 3 und 4 treffen dagegen hier nicht zu, da bei einer Gruppe jeweils nur eine Rechenoperation (Addition oder Multiplikation) definiert ist.

b) Auf einem algebraischen Ring sind im Gegensatz dazu zwei Rechenoperationen definiert. Richtig sind somit die Lösungsvorschläge 3 und 4:

- Die Tabellen A3 und M3 beschreiben den Ring $(Z_3, +, \cdot)$.
- Die Tabellen A4 und M4 beschreiben den Ring $(Z_4, +, \cdot)$.

Dagegen beschreiben A3 und M4 keinen Ring, da sie sich auf unterschiedliche Mengen beziehen.

c) Jeder Körper ist gleichzeitig auch ein Ring, aber nicht jeder Ring ist auch ein Körper. Bei letzterem ist auch die Division definiert und es gibt für jedes Element auch die **multiplikative Inverse**. Ein endlicher Zahlenring der Ordnung q – also mit q Elementen – ist nur dann ein Körper, wenn q eine Primzahl ist. Man spricht dann auch von einem Galoisfeld GF(q).

Richtig ist also Antwort 3. Die Rechenoperationen gemäß den Tabellen A3 und M3 ergeben zusammen das Galoisfeld GF(3).

Dagegen führen die Operationstabellen A4 (Addition) und M4 (Multiplikation) zusammen mit der Menge $\{0, 1, 2, 3\}$ nicht zum Galoisfeld GF(4). Eine Bedingung für ein Galoisfeld ist, dass es für jedes Element z_i eine multiplikative Inverse $\text{Inv}_\text{M}(z_i)$ gibt, so dass die Gleichung $z_i \cdot \text{Inv}_\text{M}(z_i) = 1$ erfüllt ist. Nach Tabelle M4 existiert $\text{Inv}_\text{M}(2)$ aber nicht. In der dritten Zeile gibt es keine „1”.

Ein Galoisfeld GF(4) ergibt sich zum Beispiel durch Erweiterung der binären Menge $\{0, 1\}$ zur Menge $\{0, 1, \alpha, 1+\alpha\}$. Genaueres hierzu finden Sie auf der Seite **Beispiel eines Erweiterungskörpers (1).**

d) Das Nullelement ist nie ein primitives Element. Auch $z_1 = 1$ ist kein primitives Element, denn dann müsste mit $q = 3$ gelten:

$$z_1^1 \bmod 3 \neq 1, \quad z_1^2 \bmod 3 = 1.$$

Dagegen ist $z_2 = 2$ ein primitives Element wegen

$$2^1 \bmod 3 = 2, \quad 2^2 \bmod 3 = 1.$$

Richtig ist also der Lösungsvorschlag 3.

e) Die Menge $\{0, 1, 2, 3\}$ besitzt kein primitives Element und erfüllt dementsprechend auch nicht die Erfordernisse eines Galoisfeldes:

$$\begin{aligned}
z_1 &= 1: \quad 1^1 = 1,\ 1^2 = 1,\ 1^3 = 1,\\
z_2 &= 2: \quad 2^1 = 2,\ 2^2 \bmod 4 = 0,\ 2^3 \bmod 4 = 0,\\
z_3 &= 3: \quad 3^1 = 3,\ 3^2 \bmod 4 = 1,\ 3^3 \bmod 4 = 3.
\end{aligned}$$

Musterlösung zur Zusatzaufgabe Z2.1

a) Es treffen alle Aussagen zu. Das neutrale Element N_A = C erkennt man aus der letzten Zeile der Additionstabelle. Aus der Bedingung $z_i + \text{Inv}_A(z_i) = N_A$ = C erhält man:

- Inv_A(A) = B, da an der zweiten Stelle der ersten Zeile das einzige C steht,
- Inv_A(B) = A, da an der ersten Stelle der zweiten Zeile das einzige C steht,
- Inv_A(C) = C, da an der letzten Stelle der dritten Zeile das einzige C steht.

Das Assoziativgesetz überprüfen wir (unzulässigerweise) nur an einem einigen Beispiel. Durch zweimalige Anwendung der Additionstabelle erhält man beispielsweise (A + B) + C = C + C = C. Das gleiche Ergebnis ergibt sich für A + (B + C) = A + B = C.

Damit sind alle Bedingungen für eine additive Gruppe erfüllt. Die Gültigkeit des Kommutativgesetzes erkennt man aus der Symmetrie der Additionstabelle zur Diagonalen. Damit ist die Gruppe auch abelsch.

Übrigens: Die (rote) Additionstabelle ergibt sich aus der grünen Tabelle durch die Umbenennungen 0 → C, 1 → A und 2 → B und anschließender ABC–Sortierung.

b) Richtig ist Nein. Alle Aussagen sind allein durch die Additionstabelle bestimmt und nicht durch die Bedeutung der Elemente. Auch der Autor dieser Aufgabe kann allerdings nicht tiefergehend begründen, warum die Modulo–3–Addition von „Apfel" und „Birne" das neutrale Element „Citrone" ergibt.

c) Die beiden ersten Aussagen treffen zu im Gegensatz zur letzten. Das Kommutativgesetz wird verletzt (keine Symmetrie bezüglich der Tabellendiagonalen). Beispielsweise gilt:

$$\begin{aligned} \mathrm{a}+\mathrm{b} &= \mathrm{b} \quad \neq \quad \mathrm{b}+\mathrm{a}=\mathrm{c}\,,\\ \mathrm{a}+\mathrm{c} &= \mathrm{c} \quad \neq \quad \mathrm{c}+\mathrm{a}=\mathrm{b}\,,\\ \mathrm{b}+\mathrm{c} &= \mathrm{b} \quad \neq \quad \mathrm{c}+\mathrm{b}=\mathrm{c}\,. \end{aligned}$$

Damit ist die hier betrachtete Verknüpfung keine abelsche (kommutative) Gruppe. Mehr noch, wegen der Verletzung des Assoziativgesetzes liegen hier auch die Grundvoraussetzungen einer Gruppe nicht vor. Beispielsweise gilt:

$$\begin{aligned} \mathrm{c}+(\mathrm{c}+\mathrm{c}) &= \mathrm{c}+\mathrm{a}=\mathrm{b}\,,\\ (\mathrm{c}+\mathrm{c})+\mathrm{c} &= \mathrm{a}+\mathrm{c}=\mathrm{c}\,. \end{aligned}$$

Musterlösung zur Aufgabe A2.2

a) Allgemein gilt für $0 \le \mu \le 4$: $A_{\mu 4} = (\mu + 4) \bmod 5$. Daraus folgt:

$$A_{04} = (0+4) \bmod 5 \underline{= 4}, \quad A_{14} = (1+4) \bmod 5 \underline{= 0}, \quad A_{24} = (2+4) \bmod 5 \underline{= 1},$$
$$A_{34} = (3+4) \bmod 5 \underline{= 2}, \quad A_{44} = (4+4) \bmod 5 \underline{= 3}.$$

Aufgrund des Kommutativgesetzes der Addition,

$$z_i + z_j = z_j + z_i \quad \text{für alle } z_i, z_j \in Z_5,$$

ist natürlich die letzte Spalte der Additionstabelle identisch mit der letzten Zeile der gleichen Tabelle.

b) Nun gilt $M_{\mu 4} = (\mu \cdot 4) \bmod 5$ und man erhält:

$$M_{04} = (0 \cdot 4) \bmod 5 \underline{= 0}, \quad M_{14} = (1 \cdot 4) \bmod 5 \underline{= 4}, \quad M_{24} = (2 \cdot 4) \bmod 5 \underline{= 3},$$
$$M_{34} = (3 \cdot 4) \bmod 5 \underline{= 2}, \quad M_{44} = (4 \cdot 4) \bmod 5 \underline{= 1}.$$

Da die Multiplikation ebenfalls kommutativ ist, stimmt auch in der Multiplikationstabelle die letzte Spalte wieder mit der letzten Zeile überein.

c) Die Grafik zeigt die vollständigen Additions– und Multiplikationstabellen für $q = 5$. Man erkennt:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- In der Additionstabelle gibt es in jeder Zeile (und auch in jeder Spalte) genau eine Null. Zu jedem $z_i \in Z_5$ gibt es also ein $\text{Inv}_\text{A}(z_i)$, das die Bedingung $[z_i + \text{Inv}_\text{A}(z_i)] \bmod 5 = 0$ erfüllt:

$$z_i = 0: \ \text{Inv}_\text{A}(z_i) = 0,$$
$$z_i = 1: \ \text{Inv}_\text{A}(z_i) = (-1) \bmod 5 = 4,$$
$$z_i = 2: \ \text{Inv}_\text{A}(z_i) = (-2) \bmod 5 = 3,$$
$$z_i = 3: \ \text{Inv}_\text{A}(z_i) = (-3) \bmod 5 = 2,$$
$$z_i = 4: \ \text{Inv}_\text{A}(z_i) = (-4) \bmod 5 = 1.$$

- In der Multiplikationstabelle lassen wir das Nullelement (erste Zeile und erste Spalte) außer Betracht. In allen anderen Zeilen und Spalten der unteren Tabelle gibt es tatsächlich jeweils genau eine Eins. Aus der Bedingung $[z_i \cdot \text{Inv}_\text{M}(z_i)] \bmod 5 = 1$ erhält man:

$$z_i = 1 \ \Rightarrow \ \text{Inv}_\text{M}(z_i) = 1 \ \Rightarrow \ z_i \cdot \text{Inv}_\text{M}(z_i) = 1,$$
$$z_i = 2 \ \Rightarrow \ \text{Inv}_\text{M}(z_i) = 3 \ \Rightarrow \ z_i \cdot \text{Inv}_\text{M}(z_i) = 6 \bmod 5 = 1,$$
$$z_i = 3 \ \Rightarrow \ \text{Inv}_\text{M}(z_i) = 2 \ \Rightarrow \ z_i \cdot \text{Inv}_\text{M}(z_i) = 6 \bmod 5 = 1,$$
$$z_i = 4 \ \Rightarrow \ \text{Inv}_\text{M}(z_i) = 4 \ \Rightarrow \ z_i \cdot \text{Inv}_\text{M}(z_i) = 16 \bmod 5 = 1.$$

Da sowohl die erforderlichen additiven als auch die multiplikativen Inversen existieren, beschreibt Z_5 ein Galoisfeld GF(5) $\Rightarrow$ Richtig ist der Lösungsvorschlag 1.

d) Aus der blauen Additionstabelle auf der Angabenseite erkennt man, dass alle Zahlen 0, 1, 2, 3, 4, 5 der Menge Z_6 eine additive Inverse besitzen $\Rightarrow$ in jeder Zeile (und Spalte) gibt es genau eine Null.

Eine multiplikative Inverse $\text{Inv}_\text{M}(z_i)$ gibt es dagegen nur für $z_i = 1$ und $z_i = 5$, nämlich

$$z_i = 1 \;\Rightarrow\; \mathrm{Inv_M}(z_i) = 1 \;\Rightarrow\; z_i \cdot \mathrm{Inv_M}(z_i) = 1\,,$$
$$z_i = 5 \;\Rightarrow\; \mathrm{Inv_M}(z_i) = 5 \;\Rightarrow\; z_i \cdot \mathrm{Inv_M}(z_i) = 25 \bmod 6 = 1\,.$$

Für $z_i = 2$, $z_i = 3$ und $z_i = 4$ findet man dagegen kein Element z_j, so dass $(z_i \cdot z_j) \bmod 6 = 1$ ergibt. Richtig ist somit der Lösungsvorschlag 3. Die blauen Tabellen für $q = 6$ ergeben kein Galoisfeld GF(6).

e) Eine endliche Zahlenmenge $Z_q = \{0, 1, \ldots, q–1\}$ natürlicher Zahlen führt nur dann zu einem endlichen Zahlenkörper (dies ist die deutsche Bezeichung für ein Galoisfeld), wenn q eine Primzahl ist. Von den oben genannten Zahlenmengen trifft dies nur auf Z_{11} zu $\Rightarrow$ Lösungsvorschlag 2.

Musterlösung zur Zusatzaufgabe Z2.2

a) Das neutrale Element hinsichtlich Addition (genannt $N_{\rm A}$) muss für alle Elemente z_i ($i = 0, \ ... \ , q–1$) die folgende Gleichung erfüllen:

$$z_i + N_{\rm A} = N_{\rm A} + z_i = z_i.$$

Aus der Additionstabelle folgt $N_{\rm A} = d$.

b) Dagegen erfüllt das neutrale Element der Multiplikation ($N_{\rm M}$) für alle Elemente z_i ($i = 1, \ ... \ , q–1$) die folgende Bedingung:

$$z_i \cdot N_{\rm M} = N_{\rm M} \cdot z_i = z_i.$$

Aus der Multiplikationstabelle erkennt man $N_{\rm M} = c$.

c) Das Kommutativgesetz ist bei diesem Galoisfeld in beiden Fällen (Addition und Multiplikation) erfüllt, da Additionstabelle und Multiplikationstabelle jeweils symmetrisch zur Tabellendiagonalen sind.

d) Betrachten wir zunächst den ersten Ausdruck. Bei Gültigkeit des Distributivgesetzes muss gelten:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Für die linke Seite erhält man:

$$a \cdot (b + c) = a \cdot a = e,$$

und für die rechte Seite:

$$a \cdot b + a \cdot c = c + a = e.$$

Das Distributivgesetz ist hier ebenso erfüllt wie auch bei den beiden anderen vorgegebenen Ausdrücken:

$$d \cdot (b + c) \ = \ d \cdot a = d, \quad d \cdot b + d \cdot c = d + d = d,$$
$$e \cdot (a + c) \ = \ e \cdot e = c, \quad e \cdot a + e \cdot c = b + e = c.$$

Alle Lösungsvorschläge treffen zu.

e) Das Nullelement $N_{\rm A} = d$ wird zu $N_{\rm A} = 0 \ \Rightarrow \ d = 0$, das Einselement $N_{\rm M} = c$ zu $N_{\rm M} = 1 \ \Rightarrow \ c = 1$. Die weiteren Elemente a, b und e können modulo 5 aus der Additionstabelle oder der Multiplikationstabelle bestimmt werden. Zum Beispiel folgt aus der ersten Zeile der Additionstabelle:

$$(a + b) \bmod 5 = d = 0.$$

Da sowohl a als auch b nicht 0 oder 1 sein können (da diese bereits für c und d vergeben sind), ergibt sich als Folgerung:

$$a = 2, \ b = 3 \quad \text{oder} \quad a = 3, \ b = 2.$$

Aus der zweiten Zeile der Additionstabelle folgt beispielsweise

$$(b + b) \bmod 5 = e.$$

Aus $b = 3$ ergäbe sich $e = 1$. Dies ist aber wiederum nicht möglich, da bereits $c = 1$ festgelegt wurde. Also erhält man als Endergebnis:

$$a = 3, \ b = 2, \ c = 1, \ d = 0, \ e = 4.$$

+	3	2	1	0	4
3	1	0	4	3	2
2	0	4	3	2	1
1	4	3	2	1	0
0	3	2	1	0	4
4	2	1	0	4	3

·	3	2	1	0	4
3	4	1	3	0	2
2	1	4	2	0	3
1	3	2	1	0	4
0	0	0	0	0	0
4	2	3	4	0	1

Die Grafik zeigt die Additions– und die Multiplikationstabelle für diese Zahlenmenge.

f) Zutreffend sind die Aussagen 1 und 4. Man erkennt in der Additionstabelle in jeder Zeile und Spalte genau ein $d = 0$. Das heißt: Für alle $z_i \in \{0, 1, 2, 3, 4\}$ existiert eine eindeutige additive Inverse.

Die multiplikative Inverse erkennt man in der Multiplikationstabelle durch den Eintrag $c = 1$. Die multiplikativen Inversen lauten wie folgt:

$$\begin{aligned}
&\text{Zeile 1}: \ \text{Inv}_{\text{M}}(a = 3) = b = 2\,,\\
&\text{Zeile 2}: \ \text{Inv}_{\text{M}}(b = 2) = a = 3\,,\\
&\text{Zeile 3}: \ \text{Inv}_{\text{M}}(c = 1) = c = 1\,,\\
&\text{Zeile 5}: \ \text{Inv}_{\text{M}}(e = 4) = e = 4\,.
\end{aligned}$$

Für das Nullelement $d = 0$ existiert dagegen keine multiplikative Inverse.

g) Bezüglich der primitiven Elemente erhält man

$$\begin{aligned}
&a = 3,\ a^2 = 9 \bmod 5 = 4,\ a^3 = 27 \bmod 5 = 2,\ a^4 = 81 \bmod 5 = 1 \ \Rightarrow\ \text{primitiv}\,,\\
&b = 2,\ b^2 = 4,\ b^3 = 8 \bmod 5 = 3,\ b^4 = 16 \bmod 5 = 1 \ \Rightarrow\ \text{primitiv}\,,\\
&e = 4,\ e^2 = 16 \bmod 5 = 1\,,\ e^3 = \ldots = 4,\ e^4 = \ldots = 1 \ \Rightarrow\ \text{nicht primitiv}\,.
\end{aligned}$$

Von der Menge $Z_5 = \{0, 1, 2, 3, 4\}$ sind „2" und „3" primitive Elemente $\Rightarrow$ Lösungsvorschlag 1 und 2.

Musterlösung zur Aufgabe A2.3

a) Das Polynom

$$a(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ \ldots \ + a_m \cdot x^m$$

mit $a_m = 1$ und gegebenen Koeffizienten a_0, a_1, ... , a_{m-1} (jeweils 0 oder 1) ist dann irreduzibel, wenn es kein einziges Polynom $q(x)$ gibt, so dass die Modulo–2–Division $a(x)/q(x)$ keinen Rest ergibt. Der Grad aller zu betrachteten Teilerpolynome $q(x)$ ist mindestens 1 und höchstens $m - 1$.

- Für $m = 2$ sind zwei Polynomdivisionen $a(x)/q_i(x)$ erforderlich, nämlich mit

$$q_1(x) = x \quad \text{und} \quad q_2(x) = x + 1 \quad \Rightarrow \quad \underline{N_{\rm D} = 2}.$$

- Für $m = 3$ gibt es schon $\underline{N_{\rm D} = 6}$ Teilerpolynome, nämlich neben $q_1(x) = x$ und $q_2(x) = x + 1$ noch

$$q_3(x) = x^2, \ \ q_4(x) = x^2 + 1, \ \ q_5(x) = x^2 + x, \ \ q_6(x) = x^2 + x + 1.$$

- Schließlich müssen für $m = 4$ außer $q_1(x)$, ... , $q_6(x)$ auch noch alle möglichen Teilerpolynome mit Grad $m = 3$ berücksichtigt werden, also:

$$q_i(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + x^3, \quad a_0, a_1, a_2 \in \{0, 1\}.$$

Für den Index gilt dabei $7 \le i \le 14 \ \Rightarrow \ \underline{N_{\rm D} = 14}$.

b) Für das erste Polynom gilt: $a_1(x = 0) = 0$. Deshalb ist dieses Polynom reduzibel: $a_1(x) = x \cdot (x + 1)$.

Dagegen gilt für das zweite Polynom:

$$a_2(x = 0) = 1, \ \ a_2(x = 1) = 1.$$

Diese notwendige, aber nicht hinreichende Eigenschaft zeigt, dass $a_2(x)$ irreduzibel sein könnte. Der endgültige Beweis ergibt sich erst durch zwei Modulo–2–Divisionen:

- $a_2(x)$ geteilt durch x liefert $x + 1$, Rest $r(x) = 1$,
- $a_2(x)$ geteilt durch $x + 1$ liefert x, Rest $r(x) = 1$.

Richtig ist demnach der <u>Lösungsvorschlag 2</u>.

c) Die drei ersten Polynome sind reduzibel, wie die folgenden Rechenergebnisse zeigen:

$$a_3(x = 0) = 0, \ \ a_4(x = 1) = 0, \ \ a_5(x = 0) = 0, \ \ a_5(x = 1) = 0.$$

Das hätte man auch durch Nachdenken herausfinden können:

$$\begin{aligned} a_3(x) &= x \cdot x \cdot x, \\ a_4(x) &= (x^2 + x + 1) \cdot (x + 1), \\ a_5(x) &= x \cdot (x + 1) \cdot (x + 1). \end{aligned}$$

Das Polynom $a_6(x)$ ist sowohl für $x = 0$ als auch für $x = 1$ ungleich 0. Das heißt, dass

- „nichts dagegen spricht", dass $a_6(x)$ irreduzibel ist,
- die Division durch die irreduziblen Grad–1–Polynome x bzw. $x + 1$ nicht ohne Rest möglich ist.

Da aber auch die Division durch das einzige irreduzible Grad–2–Polynom einen Rest liefert,

$$(x^3 + x + 1)/(x^2 + x + 1) = x + 1\,, \quad \text{Rest } r(x) = x\,,$$

ist nachgewiesen, dass $a_6(x)$ ein irreduzibles Polynom ist. Mit gleichem Rechengang kann auch gezeigt werden, dass $a_7(x)$ ebenfalls irreduzibel ist ⇒ Lösungsvorschläge 4 und 5.

d) Aus $a_8(x + 1) = 0$ folgt die Reduzibilität von $a_8(x)$. Für die beiden anderen Polynome gilt dagegen:

$$\begin{aligned} a_9(x = 0) &= 1\,, \quad a_9(x = 1) = 1\,,\\ a_{10}(x = 0) &= 1\,, \quad a_{10}(x = 1) = 1\,. \end{aligned}$$

Beide könnten also irreduzibel sein. Der exakte Nachweis der Irreduzibilität ist aufwändiger. Man muss zur Überprüfung zwar nicht alle vier Divisorpolynome mit Grad $m = 2$ heranziehen, nämlich x^2, $x^2 + 1$, $x^2 + x$ sowie $x^2 + x + 1$, sondern es genügt die Division durch das einzige irreduzible Grad–2–Polynom. Man erhält hinsichtlich des Polynoms $a_9(x)$:

$$(x^4 + x^3 + 1)/(x^2 + x + 1) = x^2 + 1\,, \quad \text{Rest } r(x) = x\,.$$

Auch die Division durch die beiden irreduziblen Grad–3–Polynome liefern jeweils einen Rest:

$$\begin{aligned} (x^4 + x^3 + 1)/(x^3 + x + 1) &= x + 1\,, \quad \text{Rest } r(x) = x^2\,,\\ (x^4 + x^3 + 1)/(x^3 + x^2 + 1) &= x\,, \qquad \text{Rest } r(x) = x + 1\,. \end{aligned}$$

Betrachten wir schließlich noch das Polynom $a_{10}(x) = x^4 + x^2 + 1$. Hier gilt

$$(x^4 + x^2 + 1)/(x^2 + x + 1) = x^2 + x + 1\,, \quad \text{Rest } r(x) = 0\,.$$

Daraus folgt: Nur das Polynom $a_9(x)$ ist irreduzibel ⇒ Lösungsvorschlag 2.

Musterlösung zur Zusatzaufgabe Z2.3

a) Die Modulo–2–Multiplikation der beiden Polynome führt zum Ergebnis

$$a(x) = (x^3 + x + 1) \cdot (x^2 + 1) = \\ = x^5 + x^3 + x^2 + x^3 + x + 1 = x^5 + x^2 + x + 1\,.$$

Richtig ist somit der Lösungsvorschlag 2. Der letzte Lösungsvorschlag kann schon alleine deshalb nicht stimmen, da der Grad des Produktpolynoms ≠ 5 wäre.

b) Mit den Abkürzungen

$$a(x) = x^5 + x^2 + x + 1\,, \quad p(x) = x^3 + x + 1\,, \quad q(x) = x^2 + 1$$

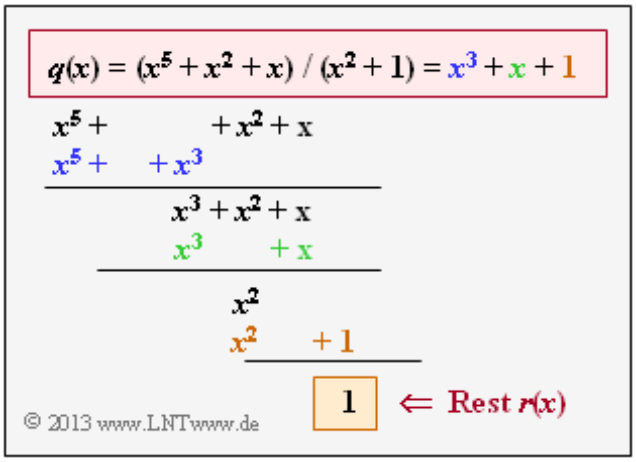
und dem Ergebnis aus der Teilaufgabe (a) erhält man $a(x) = p(x) \cdot q(x)$. Das heißt: Die Divisionen $a(x)/p(x)$ und $a(x)/q(x)$ sind restfrei möglich ⇒ Richtig sind die Lösungsvorschläge 1 und 2. Auch ohne Rechnung erkennt man, dass $a(x)/x^2$ einen Rest ergeben muss. Nach Rechnung ergibt sich explizit:

$$(x^5 + x^2 + x + 1)/(x^2) = x^3 + 1\,, \quad \text{Rest } r(x) = x + 1\,.$$

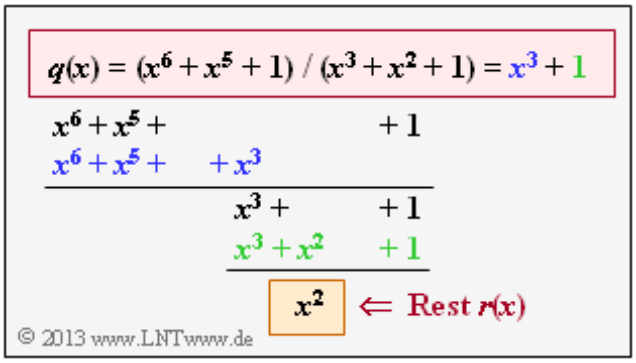
Zum letzten Lösungsvorschlag. Wir verwenden zur Abkürzung $b(x) = x^5 + x^2 + x = a(x) + 1$. Damit ist der vorgegebene Quotient:

$$b(x)/q(x) = a(x)/q(x) + 1/q(x)\,.$$

Der erste Quotient $a(x)/q(x)$ ergibt entsprechend der Teilaufgabe (b) genau $p(x)$ ohne Rest, der zweite Quotient 0 mit Rest 1. Somit ist hier der Rest des Quotienten $b(x)/q(x)$ gleich $r(x) = 1$, wie auch die nebenstehende Rechnung zeigt.



c) Die Polynomdivision ist nachfolgend ausführlich erläutert. Richtig ist der Lösungsvorschlag 3.



Musterlösung zur Aufgabe A2.4

a) Zutreffend sind die Lösungsvorschläge 1, 2 und 5. Begründung:

- Wäre $\alpha = 0$ oder $\alpha = 1$, so wäre das Pseudoelement α nicht mehr unterscheidbar von den beiden anderen GF(2)–Elementen 0 und 1.
- Die Modulo–2–Rechnung erkennt man aus der Additionstabelle. Beispielsweise gilt $1 + 1 = 0$, $\alpha + \alpha = 0$, $(1 + \alpha) + (1 + \alpha) = 0$, usw.
- Aus der Multiplikationstabelle geht hervor, dass $\alpha^2 = \alpha \cdot \alpha = 1+\alpha$ gilt (3. Zeile, 3. Spalte). Daraus lässt sich die Bedingung $\alpha^2 + \alpha + 1 = 0$ ablesen.

b) Richtig ist Lösungsvorschlag 2. So steht „01" für das Element „1" und „10" für das Element „α".

c) Richtig sind die Lösungsvorschläge 2 und 3. Es gilt $\alpha^0 = 1$ und $\alpha^1 = \alpha$. Bei dem zugrundeliegenden Polynom $p(x) = x^2 + x + 1$ folgt aus $p(\alpha) = 0$ weiterhin:

$$\alpha^2 + \alpha + 1 = 0 \quad \Rightarrow \quad \alpha^2 = \alpha + 1\,.$$

d) Entsprechend den Tabellen der Polynomdarstellung gilt:

$$\begin{aligned} A &= z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = \\ &= \alpha \cdot \alpha + \alpha \cdot (1+\alpha) + (1+\alpha) \cdot (1+\alpha) = (1+\alpha) + (1) + (\alpha) = 0 = z_0\,, \\ B &= (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = \\ &= (0+1+\alpha) \cdot (0+1+1+\alpha) = (1+\alpha) \cdot \alpha = 1 = z_1\,. \end{aligned}$$

Richtig sind demnach die Lösungsvorschläge 1 und 2. Zu den gleichen Ergebnissen kommt man mit der Koeffizientenvektordarstellung:

$$\begin{aligned} A &= z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = \\ &= (10) \cdot (10) + (10) \cdot (11) + (11) \cdot (11) = (11) + (01) + (10) = (00) = 0 = z_0\,, \\ B &= (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = \\ &= [(00) + (01) + (10)] \cdot [(00) + (01) + (11)] = (11) \cdot (10) = (01) = z_1\,. \end{aligned}$$

Und schließlich mit der Exponentendarstellung:

$$\begin{aligned} A &= z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = \\ &= \alpha^1 \cdot \alpha^1 + \alpha^1 \cdot \alpha^2 + \alpha^2 \cdot \alpha^2 = \alpha^2 + \alpha^3 + \alpha^4 = \alpha^2 + \alpha^0 + \alpha^1 = 0 = z_0\,, \\ B &= (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = \\ &= [0 + \alpha^0 + \alpha^1] \cdot [0 + \alpha^0 + \alpha^2] = \alpha^2 \cdot \alpha^1 = \alpha^3 = \alpha^0 = z_1\,. \end{aligned}$$

Musterlösung zur Zusatzaufgabe Z2.4

a) Im Angabenteil steht sinngemäß: Ein Polynom vom Grad m nennt man reduzibel im Körper K, wenn es in der Form

$$p(x) = \prod_{i=1}^{m}(x - x_i) = (x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_m)$$

dargestellt werden kann und für alle Nullstellen $x_i \in K$ gilt. Ist dies nicht möglich, so spricht man von einem irreduziblen Polynom.

Im reellen Zahlenraum gilt für die jeweils $m = 2$ Nullstellen x_1 und x_2:

$$\begin{aligned}
&p_1(x): \quad x_1 = +\mathrm{j}, \; x_2 = -\mathrm{j},\\
&p_2(x): \quad x_1 = +1, \; x_2 = -1,\\
&p_3(x): \quad x_1 = -0.5 + \mathrm{j} \cdot \sqrt{3}/2, \; x_2 = -0.5 - \mathrm{j} \cdot \sqrt{3}/2,\\
&p_4(x): \quad x_1 = +1, \; x_2 = -2.
\end{aligned}$$

Die beiden Nullstellen von $p_2(x)$ und $p_4(x)$ sind jeweils reell. Somit handelt es sich hierbei mit Sicherheit um reduzible Polynome. Die beiden anderen Polynome weisen dagegen keine reellen Nullstellen auf (vielmehr imaginäre bzw. komplexe) und sind nach obiger Definition irreduzibel im reellen Körper ⇒ Lösungsvorschlag 1 und 3.

b) Richtig ist der Lösungsvorschlag 3: $p_3(x) = x^2 + x + 1$ ist das einzige irreduzible Polynom im Galoisfeld GF(2^2). Im **Theorieteil** wurden hierfür die Additions– und die Multiplikationstabelle angegeben. Für die anderen Polynome gilt:

- Das Polynom $p_1(x)$ ist in GF(2) = {0, 1} reduzibel, da dieses Polynom faktorisiert werden kann:

$$p_1(x) = x^2 + 1 = (x + 1)^2.$$

- Da in GF(2) kein Unterschied zwischen Summe und Differenz besteht, ist auch das Polynom $p_2(x) = x^2 – 1$ reduzibel.
- Das Polynom $p_4(x) = x^2 + x – 2$ ist schon allein deshalb für GF(2) ungeeignet, da nicht alle Polynomkoeffizienten 0 oder 1 sind. Die „2” wäre nur im Galoisfeld GF(3) möglich.

c) Richtig sind die letzten drei Lösungsvorschläge:

- Die Menge N ist kein Körper, da schon die Subtraktion nicht für alle Elemente zulässig ist, z.B. ist $2 – 3 = –1 \notin N$.
- Auch die Menge Z der ganzen Zahlen ist kein Körper, da beispielsweise die Gleichung $2 \cdot z = 1$ für kein $z \in Z$ zu erfüllen ist.

d) Richtig sind die Antworten 1 und 3. Es gilt $Q \subset R$ (rationale Zahlen sind eine Untermenge der reellen Zahlen) und $R \subset C$ (reelle Zahlen sind eine Untermenge der komplexen Zahlen) und damit auch $Q \subset C$. Bei den endlichen Körpern bedeutet GF(2^m) ⊂ GF(2^M), dass $m < M$ gelten muss.

e) Richtig ist der Lösungsvorschlag 2:

- Die Menge der komplexen Zahlen ist eine Erweiterung der reellen Zahlen (R) in eine zweite

Dimension. Hierfür kann geschrieben werden:

$$C = \{k_0 + \mathrm{j} \cdot k_1 \,|\, k_0 \in R, k_1 \in R\}\,.$$

- GF(2^2) ist eine Erweiterung des endlichen Körpers GF(2) = {0, 1} in eine zweite Dimension:

$$\mathrm{GF}(2^2) = \{k_0 + \alpha \cdot k_1 \,|\, k_0 \in \mathrm{GF}(2), k_1 \in \mathrm{GF}(2)\}\,.$$

Die imaginäre Einheit j $\notin R$ ergibt sich als Lösung der Gleichung $\mathrm{j}^2 + 1 = 0$, während das neue Element von GF(2^2) mit $\alpha \notin$ GF(2) bezeichnet wird und aus der Gleichung $\alpha^2 + \alpha + 1 = 0$ folgt.

Musterlösung zur Aufgabe A2.5

a) Aus der oberen Potenztabelle (A) auf der Angabenseite erkennt man unter anderem

$$\alpha^4 = \alpha + 1 \quad \Rightarrow \quad \alpha^4 + \alpha + 1 = 0 \quad \Rightarrow \quad p(x) = x^4 + x + 1.$$

Richtig ist somit Lösungsvorschlag 1.

b) Entsprechend der Vorgehensweise in Teilaufgabe (a) kann gezeigt werden, dass Potenztabelle (B) auf dem Polynom $p(x) = x^4 + x^3 + 1$ basiert ⇒ Lösungsvorschlag 2.

c) Ausgehend von Polynom $p(x) = x^4 + x^3 + 1$ erhält man aus der Bestimmungsgleichung $p(\alpha) = 0$ das Ergebnis $\alpha^4 = \alpha^3 + 1$. Damit ergibt sich weiter:

$$\begin{aligned}
\alpha^5 &= \alpha \cdot \alpha^4 = \alpha \cdot (\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + \alpha + 1 \Rightarrow \text{Vektor } 1011,\\
\alpha^6 &= \alpha \cdot \alpha^5 = \alpha \cdot (\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 \Rightarrow \text{Vektor } 1111,\\
\alpha^7 &= \alpha \cdot \alpha^6 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1 \Rightarrow \text{Vektor } 0111,\\
\alpha^8 &= \alpha \cdot \alpha^7 = \alpha \cdot (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha \Rightarrow \text{Vektor } 1110.
\end{aligned}$$

Richtig sind somit nur die Lösungsvorschläge 1 und 4. Die beiden anderen Angaben sind vertauscht. Nachfolgend finden Sie die vollständigen Potenztabellen für $p(x) = x^4 + x + 1$ (links, rot hinterlegt) und für $p(x) = x^4 + x^3 + 1$ (rechts, blau hinterlegt).

Tabelle (A)

Potenz von α	Polynom in α	Vektor der Koeffizienten
$\alpha^{-\infty}=0$	0	0000
$\alpha^0=1$	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001
α^{15}	1	0001

Tabelle (B)

Potenz von α	Polynom in α	Vektor der Koeffizienten
$\alpha^{-\infty}=0$	0	0000
$\alpha^0=1$	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	α^3+1	1001
α^5	$\alpha^3+\alpha+1$	1011
α^6	$\alpha^3+\alpha^2+\alpha+1$	1111
α^7	$\alpha^2+\alpha+1$	0111
α^8	$\alpha^3+\alpha^2+\alpha$	1110
α^9	α^2+1	0101
α^{10}	$\alpha^3+\alpha$	1010
α^{11}	$\alpha^3+\alpha^2+1$	1101
α^{12}	$\alpha+1$	0011
α^{13}	$\alpha^2+\alpha$	0110
α^{14}	$\alpha^3+\alpha^2$	1100
α^{15}	1	0001

d) Die beiden Polynome $p(x) = x^4 + x + 1$ und $p(x) = x^4 + x^3 + 1$ sind primitiv. Dies erkennt man daran, dass α^i für $0 < i < 14$ jeweils ungleich 1 ist. Dagegen gilt $\alpha^{15} = \alpha^0 = 1$. In beiden Fällen kann das Galoisfeld wie folgt ausgedrückt werden:

$$\text{GF}(2^4) = \{\, 0,\ \alpha^0 = 1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{14} \,\}.$$

Dagegen erhält man für das Polynom $p(x) = x^4 + x^3 + x^2 + x + 1$:

$$\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1 \quad \Rightarrow \quad \text{Vektor } 1111\,,$$
$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha =$$
$$= (\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha = 1 \quad \Rightarrow \quad \text{Vektor } 0001\,.$$

Hier ist also bereits $\alpha^5 = \alpha^0 = 1$ ⇒ $p(x)$ ist kein primitives Polynom ⇒ Lösungsvorschlag 2. Für die weiteren Potenzen gilt für dieses Polynom:

$$\alpha^6 = \alpha^{11} = \alpha\,,\ \alpha^7 = \alpha^{12} = \alpha^2\,,\ \alpha^8 = \alpha^{13} = \alpha^3\,,$$
$$\alpha^9 = \alpha^{14} = \alpha^4\,,\ \alpha^{10} = \alpha^{15} = \alpha^0 = 1\,.$$

Musterlösung zur Zusatzaufgabe Z2.5

a) Beispielsweise findet man mit Hilfe der vorne angegebenen Tabelle:

$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha \cdot (\alpha^2 + 1) = \alpha^3 + \alpha = (\alpha + 1) + \alpha = 1,$$
$$\alpha^8 = \alpha \cdot \alpha^7 = \alpha \cdot 1 = \alpha,$$
$$\alpha^{13} = \alpha^7 \cdot \alpha^6 = 1 \cdot \alpha^6 = \alpha^2 + 1.$$

Die Tabelle lässt sich also modulo 7 fortsetzen. Das bedeutet: Alle Lösungsvorschläge sind richtig.

b) Mit $\alpha^8 = \alpha$ (nach Teilaufgabe a), $\alpha^6 = \alpha^2 + 1$ (gemäß Tabelle) und $-\alpha^2 = \alpha^2$ (Operationen im binären Galoisfeld) erhält man Lösungsvorschlag 2:

$$A = \alpha^8 + \alpha^6 - \alpha^2 + 1 = \alpha + (\alpha^2 + 1) + \alpha^2 + 1 = \alpha.$$

c) Mit $\alpha^{16} = \alpha^{16-14} = \alpha^2$ sowie $\alpha^{12} \cdot \alpha^3 = \alpha^{15} = \alpha^{15-14} = \alpha$ erhält man den Lösungsvorschlag 5:

$$B = \alpha^2 + \alpha = \alpha^4.$$

d) Es gilt $\alpha^3 = \alpha + 1$ und damit $C = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$ $\Rightarrow$ Lösungsvorschlag 1.

e) Mit $\alpha^4 = \alpha^2 + \alpha$ erhält man $D = \alpha^4 + \alpha = \alpha^2$ $\Rightarrow$ Lösungsvorschlag 3.

f) Richtig ist Lösungsvorschlag 4:

$$E = A \cdot B \cdot C/D = \alpha \cdot \alpha^4 \cdot 1/\alpha^2 = \alpha^3.$$

g) Laut Tabelle gilt $\alpha^2 + \alpha = \alpha^4$. Deshalb muss gelten:

$$\alpha^4 \cdot \text{Inv}_\text{M}(\alpha^4) = 1 \quad \Rightarrow \quad \text{Inv}_\text{M}(\alpha^2 + \alpha) = \text{Inv}_\text{M}(\alpha^4) = \alpha^{-4} = \alpha^3.$$

Wegen $\alpha^3 = \alpha + 1$ sind somit die Lösungsvorschläge 2 und 3 richtig.

Musterlösung zur Aufgabe A2.6

a) Jedes Element besteht aus zwei Ternärzahlen ⇒ $P = 3$, $m = 2$. Es gibt $q = P^m = 3^3 = 9$ Elemente.

b) Das neutrale Element der Addition (N_A) erfüllt für alle $z_i \in \text{GF}(P^m)$ die Bedingung $z_i + N_\text{A} = z_i$. Aus der Additionstabelle kann abgelesen werden, dass „00” diese Bedingung erfüllt ⇒ Lösungsvorschlag 1.

c) Das neutrale Element der Multiplikation (N_M) muss stets die Bedingung $z_i \cdot N_\text{M} = z_i$ erfüllen. Aus der Multiplikationstabelle ergibt sich N_M = „01” ⇒ Lösungsvorschlag 2. In der Polynomscheibweise entspricht dies mit $k_1 = 0$ und $k_0 = 1$:

$$k_1 \cdot \alpha + k_0 = 1\,.$$

d) Mit der Polynomdarstellung ergeben sich folgende Berechnungen:

$$\begin{aligned}
\text{Inv}_\text{A}(\text{”02”}) &= \text{Inv}_\text{A}(2) = (-2) \bmod 3 = 1 \;\Rightarrow\; \text{Vektor ”01”}\,,\\
\text{Inv}_\text{A}(\text{”11”}) &= \text{Inv}_\text{A}(\alpha + 1) = [(-\alpha) \bmod 3] + [(-1) \bmod 3] =\\
&= 2\alpha + 2 \;\Rightarrow\; \text{Vektor ”22”}\,,\\
\text{Inv}_\text{A}(\text{”22”}) &= \text{Inv}_\text{A}(2\alpha + 2) = [(-2\alpha) \bmod 3] + [(-2) \bmod 3] =\\
&= \alpha + 1 \;\Rightarrow\; \text{Vektor ”11”}\,.
\end{aligned}$$

Demzufolge sind nur die beiden ersten Lösungsvorschläge richtig. Die Aufgabe kann aber auch ohne Rechnung allein anhand der Additionstabelle gelöst werden. Beispielsweise findet man die Inverse zu „22”, indem man in der letzten Zeile die Spalte mit dem Eintrag „00” sucht. Man findet die mit „11” bezeichnete Spalte und damit Inv_A(„22”) = „11”.

e) Die Multiplikation von α (Vektor „10”) mit sich selbst ergibt α^2.

- Würde der erste Lösungsvorschlag gültig sein, so müsste sich aus der Bedingung $\alpha^2 + 2 = 0$ und damit $\alpha^2 = (-2) \bmod 3 = 1$ ergeben, also der Vektor „01”.
- Geht man vom zweiten Lösungsvorschlag aus, so folgt aus der Bedingung $\alpha^2 + 2\alpha + 2 = 0$ in der Polynomschreibweise

  $$\alpha^2 = [(-2\alpha) \bmod 3] + [(-2) \bmod 3] = \alpha + 1$$

  und damit der Koeffizientenvektor „11”.

In der Multiplikationstabelle findet man in Zeile 4, Spalte 4 genau den Eintrag „11” → Richtig ist also der Lösungsvorschlag 2.

f) Die multiplikative Inverse zu „12” findet man in der Zeile 6 der Multiplikationstabelle als diejenige Spalte mit dem Eintrag „01” ⇒ Der Lösungsvorschlag 2 ist also richtig im Gegensatz zu Vorschlag 3. Es gilt nämlich Inv_M(„21”) = „20”.

Wir überprüfen diese Ergebnisse unter Berücksichtigung von $\alpha^2 + 2\alpha + 2 = 0$ durch Multiplikationen:

$$
\begin{aligned}
\text{”12”} \cdot \text{”10”} \quad &\Rightarrow \quad (\alpha+2)\cdot\alpha = \alpha^2 + 2\alpha = (-2\alpha - 2) + 2\alpha = -2 \bmod 3 = 1 \\
&\Rightarrow \quad \text{Vektor ”01”} \;\Rightarrow\; \text{multiplikative Inverse}. \\
\text{”21”} \cdot \text{”12”} \quad &\Rightarrow \quad (2\alpha+1)\cdot(\alpha+2) = 2\alpha^2 + \alpha + 4\alpha + 2 = 2\alpha^2 + 5\alpha + 2 = \\
&\Rightarrow \quad 2\cdot(-2\alpha - 2) + 5\alpha + 2 = (\alpha - 2) \bmod 3 = \alpha + 1 \\
&\Rightarrow \quad \text{Vektor ”11”} \;\Rightarrow\; \text{keine multiplikative Inverse}.
\end{aligned}
$$

Der Lösungsvorschlag 1 ist deshalb nicht richtig, weil es für „00” keine multiplikative Inverse gibt.

g) Die beiden Ausdrücke stimmen überein ⇒ Ja, wie die folgenden Berechnungen zeigen:

$$
\begin{aligned}
(\text{”20”} + \text{”12”}) \cdot \text{”12”} \;&=\; \text{”02”} \cdot \text{”12”} = \text{”21”}\,, \\
\text{”20”} \cdot \text{”12”} + \text{”12”} \cdot \text{”12”} \;&=\; \text{”02”} + \text{”22”} = \text{”21”}\,.
\end{aligned}
$$

Das bedeutet: Das Distributivgesetz wurde zumindest an einem einzigen Beispiel nachgewiesen.

Musterlösung zur Aufgabe A2.7

a) Alle Informationssymbole entstammen hier dem Galoisfeld GF(2^3). In Binärschreibweise wird jedes Symbol durch drei Binärzeichen dargestellt. Aufgrund des RS–Codeparameters $k = 3$ besteht ein Informationsblock aus drei Informationssymbolen: $\underline{u} = (u_0, u_1, u_2)$. Dementsprechend beinhaltet der binäre Informationsblock $\underline{u}_{\rm bin}$ genau $3 \cdot 3 = 9$ Bit $\Rightarrow$ Lösungsvorschlag 2.

b) Entsprechend der Tabelle auf der Angabenseite besteht folgender Zusammenhang zwischen dem Koeffizientenvektor und der Exponentialdarstellung:

$$(110) \Rightarrow u_0 = \alpha^4, \quad (001) \Rightarrow u_1 = \alpha^0 = 1, \quad (011) \Rightarrow u_2 = \alpha^3.$$

Richtig sind also die Lösungsvorschläge 1, 4 und 5, und der Informationsblock im ersten Codierschritt lautet $\underline{u} = (\alpha^4, 1, \alpha^3)$.

c) In Polynomdarstellung ergibt sich für den Informationsblock $\underline{u} = (\alpha^4, 1, \alpha^3)$:

$$u(x) = u_0 + u_1 \cdot x + u_2 \cdot x^2 = \alpha^4 + x + \alpha^3 \cdot x^2.$$

Richtig ist demnach der Lösungsvorschlag 3. Der erste Lösungsvorschlag kann schon allein deshalb nicht stimmen, da der Polynomgrad höchstens 2 sein kann, wenn alle Informations– und Codesymbole aus GF(2^3) entstammen.

d) Für die Codesymbole erhält man mit der Polynomdarstellung entsprechend der Angabenseite:

$$\begin{aligned}
c_0 &= u(x = \alpha^0 = 1) = \alpha^4 + 1 + \alpha^3 \cdot 1^2 = (110) + (001) + (011) = (100) = \alpha^2,\\
c_1 &= u(x = \alpha^1) = \alpha^4 + \alpha + \alpha^5 = (110) + (010) + (111) = (011) = \alpha^3,\\
c_2 &= u(x = \alpha^2) = \alpha^4 + \alpha^2 + \alpha^7 = (110) + (100) + (001) = (011) = \alpha^3,\\
c_3 &= u(x = \alpha^3) = \alpha^4 + \alpha^3 + \alpha^9 = (110) + (011) + (100) = (001) = 1,\\
c_4 &= u(x = \alpha^4) = \alpha^4 + \alpha^4 + \alpha^{11} = \alpha^4,\\
c_5 &= u(x = \alpha^5) = \alpha^4 + \alpha^5 + \alpha^{13} = (110) + (111) + (101) = (100) = \alpha^2,\\
c_6 &= u(x = \alpha^6) = \alpha^4 + \alpha^6 + \alpha^{15} = (\alpha^2 + \alpha) + (\alpha^2 + 1) + \alpha = 1.
\end{aligned}$$

Richtig sind also die Lösungsvorschläge 1, 2, 3, 4, 7. Die Lösungen zu 5 und 6 sind genau vertauscht.

e) Richtig ist der erste Lösungsvorschlag. Dieser ergibt sich aus dem Ergebnis der Teilaufgabe (d) und der Zuordnung

$$\alpha^2 \leftrightarrow 100,\ \alpha^3 \leftrightarrow 011,\ \alpha^3 \leftrightarrow 011,\ 1 \leftrightarrow 001,\ \alpha^4 \leftrightarrow 110,\ \alpha^2 \leftrightarrow 100,\ 1 \leftrightarrow 001.$$

Der letzte Lösungsvorschlag kann schon allein deshalb nicht stimmen, da das binäre Codewort aus $n \cdot m = 7 \cdot 3 = 21$ Bit bestehen muss. Selbst wenn Sie in der Teilaufgabe d) nur das Ergebnis $c_0 = \alpha^2$ ermittelt haben, so wissen Sie schon, dass auch der Lösungsvorschlag 2 nicht der richtige sein kann.

f) Die Aussagen 1, 2, 4 sind richtig. Die Bit 10, ... , 18 der Eingangssequenz sind alle 0 und damit auch die Informationssymbole $u_0, u_1, u_2 \in$ GF(2^3). Dementsprechend ist auch $u(x) = 0$, so dass alle Codesymbole $c_i = u(x = \alpha^i)$ dem Nullsymbol entsprechen (Index: $0 \le i \le 6$). Die binäre Codefolge besteht somit aus $n \cdot m = 21$ Nullen.

Musterlösung zur Zusatzaufgabe Z2.7

a) Aus $n = 15$ und $k = 5$ folgt:

$$d_{\rm min} = n - k + 1 = 15 - 5 + 1 = 11 \quad \Rightarrow \quad t = \frac{d_{\rm min} - 1}{2} \underline{= 5}.$$

b) Allgemein gilt für das gesuchte Polynom $u(x)$ mit $k = 5$:

$$u(x) = \sum_{i=0}^{k-1} u_i \cdot x^i = u_0 + u_1 \cdot x + u_2 \cdot x^2 + u_3 \cdot x^3 + u_4 \cdot x^4 .$$

Für $u_0 = \alpha^3$, $u_1 = u_2 = 0$, $u_3 = 1$ und $u_4 = \alpha^{10}$ erweist sich der Lösungsvorschlag 2 als richtig.

c) Es gilt $c_0 = u(\alpha^0) = u(1)$:

$$c_0 = \alpha^3 + 1 \cdot 1^3 + \alpha^{10} \cdot 1^4 = (1000) + (0001) + (0111) = (1110) = \alpha^{11} .$$

Richtig ist somit der Lösungsvorschlag 3.

d) Aus $c_1 = u(\alpha)$ erhält man den Lösungsvorschlag 4:

$$c_1 = u(\alpha^1) = \alpha^3 + 1 \cdot \alpha^3 + \alpha^{10} \cdot \alpha^4 = \alpha^{14}.$$

e) Für das vorletzte Symbol gilt $c_{13} = u(\alpha^{13})$:

$$\begin{aligned} c_{13} &= u(\alpha^{13}) = \alpha^3 + 1 \cdot \alpha^{13 \cdot 3} + \alpha^{10} \cdot \alpha^{13 \cdot 4} = \alpha^3 + \alpha^{39} + \alpha^{62} = \\ &= \alpha^3 + \alpha^{15 \cdot 2} \cdot \alpha^9 + \alpha^{15 \cdot 4} \cdot \alpha^2 = \alpha^3 + \alpha^9 + \alpha^2 = \\ &= (1000) + (1010) + (0100) = (0110) = \alpha^5 . \end{aligned}$$

Richtig ist Lösungsvorschlag 2.

f) Das letzte Codesymbol ist $c_{14} = u(\alpha^{14})$:

$$\begin{aligned} c_{14} &= u(\alpha^{14}) = \alpha^3 + 1 \cdot \alpha^{14 \cdot 3} + \alpha^{10} \cdot \alpha^{14 \cdot 4} = \alpha^3 + \alpha^{42} + \alpha^{66} = \\ &= \alpha^3 + \alpha^{15 \cdot 2} \cdot \alpha^{12} + \alpha^{15 \cdot 4} \cdot \alpha^6 = \alpha^3 + \alpha^{12} + \alpha^6 = \\ &= (1000) + (1111) + (1100) = (1011) = \alpha^7 . \end{aligned}$$

⇒ Lösungsvorschlag 3.

g) Das Codesymbol „0” tritt genau so oft auf wie alle anderen Symbole „α^i” ⇒ Lösungsvorschlag 3.

Musterlösung zur Aufgabe A2.8

a) Richtig sind die Lösungsvorschläge 2 und 3 ⇒ Matrizen $\mathbf{G}_B$ und $\mathbf{G}_C$, wobei in der Matrix $\mathbf{G}_C$ bereits die erlaubten Umformungen $\alpha^8 = \alpha$, $\alpha^{10} = \alpha^3$ und $\alpha^{12} = \alpha^5$ berücksichtigt wurden. Die Matrix $\mathbf{G}_A$ gilt für den (7, 5, 3)–Hamming–Code und $\mathbf{G}_D$ gehört zum RSC $(7, 5, 3)_8$. Siehe hierzu Teilaufgabe (c).

b) Beim RSC $(7, 3, 5)_8$ werden in jedem Codierschritt $k = 3$ Informationssymbole verarbeitet, im Codierschritt 1 die Symbole α^4, 1 und α^3. Mit der Generatormatrix $\mathbf{G}_C$ gilt somit:

$$\underline{c} = \underline{u} \cdot \mathbf{G}_C = \begin{pmatrix} \alpha^4 & 1 & \alpha^3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \end{pmatrix}.$$

Damit ergibt sich entsprechend der nebenstehenden Tabelle:

$$\begin{aligned}
c_0 &= \alpha^4 \cdot 1 + 1 \cdot 1 + \alpha^3 \cdot 1 = \\
&= (110) + (001) + (011) = (100) = \alpha^2, \\
c_1 &= \alpha^4 \cdot 1 + 1 \cdot \alpha + \alpha^3 \cdot \alpha^2 = \\
&= (110) + (010) + (110) = (011) = \alpha^3, \\
c_2 &= \alpha^4 \cdot 1 + 1 \cdot \alpha^2 + \alpha^3 \cdot \alpha^4 = \\
&= (110) + (100) + (001) = (011) = \alpha^3, \\
c_3 &= \alpha^4 \cdot 1 + 1 \cdot \alpha^3 + \alpha^3 \cdot \alpha^6 = \\
&= (110) + (011) + (100) = (001) = 1, \\
c_4 &= \alpha^4 \cdot 1 + 1 \cdot \alpha^4 + \alpha^3 \cdot \alpha^1 = \alpha^4, \\
c_5 &= \alpha^4 \cdot 1 + 1 \cdot \alpha^5 + \alpha^3 \cdot \alpha^3 = \\
&= (110) + (111) + (101) = (100) = \alpha^2, \\
c_6 &= \alpha^4 \cdot 1 + 1 \cdot \alpha^6 + \alpha^3 \cdot \alpha^5 = \\
&= (\alpha^2 + \alpha) + (\alpha^2 + 1) + \alpha = 1.
\end{aligned}$$

Potenzen von α	Polynome in α	Vektoren $k_2\, k_1\, k_0$
$\alpha^{-\infty} = 0$	0	0 0 0
$\alpha^0 = 1$	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha + 1$	0 1 1
α^4	$\alpha^2 + \alpha$	1 1 0
α^5	$\alpha^2 + \alpha + 1$	1 1 1
α^6	$\alpha^2 + 1$	1 0 1

Man erhält das genau gleiche Ergebnis wie in der Teilaufgabe (d) von **Aufgabe A2.7.** Richtig sind die Lösungsvorschläge 1 und 2. Es gilt nicht $c_6 = 0$, sondern $c_6 = 1$.

c) Beim RSC $(7, 5, 3)_8$ ist nun das Informationswort $\underline{u} = (u_0, u_1, u_2, u_3, u_4)$ zu berücksichtigen. Mit der Generatormatrix $\mathbf{G}_D$ erhält man somit:

$$\underline{c} = \underline{u} \cdot \mathbf{G}_D = \begin{pmatrix} \alpha^4 & 1 & \alpha^3 & 0 & \alpha^6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\ 1 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Daraus folgt:

$$\begin{aligned}
c_0 &= \alpha^4 \cdot 1 + 1 \cdot 1 + \alpha^3 \cdot 1 + 0 \cdot 1 + \alpha^6 \cdot 1 = \\
&= (110) + (001) + (011) + (000) + (101) = (001) = 1, \\
c_1 &= \left[\alpha^4 \cdot 1 + 1 \cdot \alpha + \alpha^3 \cdot \alpha^2\right] + 0 \cdot \alpha^3 + \alpha^6 \cdot \alpha^4 = \left[\alpha^3\right] + \alpha^3 = 0.
\end{aligned}$$

Hierbei ist berücksichtigt, dass der Klammerausdruck [...] genau dem Ergebnis c_1 der Teilaufgabe (b) entspricht. Entsprechendes wird bei den folgenden Berechnungen ebenfalls berücksichtigt:

$$\begin{aligned}
c_2 &= \left[\alpha^3\right] + \alpha^6 \cdot \alpha^1 = \left[\alpha^3\right] + \alpha^7 = (011) + (001) = (010) = \alpha^1\,,\\
c_3 &= [1] + \alpha^6 \cdot \alpha^5 = [1] + \alpha^4 = (001) + (110) = (111) = \alpha^5\,,\\
c_4 &= \left[\alpha^4\right] + \alpha^6 \cdot \alpha^2 = \left[\alpha^4\right] + \alpha^1 = (110) + (010) = (100) = \alpha^2\,,\\
c_5 &= \left[\alpha^2\right] + \alpha^6 \cdot \alpha^6 = \left[\alpha^2\right] + \alpha^5 = (100) + (111) = (011) = \alpha^3\,,\\
c_6 &= [1] + \alpha^6 \cdot \alpha^3 = [1] + \alpha^2 = (001) + (100) = (101) = \alpha^6\,.
\end{aligned}$$

Das heißt: Alle Lösungsvorschläge sind richtig.

Musterlösung zur Zusatzaufgabe Z2.8

a) Die Addition eines jeden Elements eines Erweiterungskörpers, der auf GF(2) basiert, mit sich selbst ergibt stets 0, wie man anhand der Koeffizientendarstellung leicht erkennt, zum Beispiel:

$$\alpha^3 + \alpha^3 = (011) + (011) = (000) = 0\,.$$

Das heißt: „A" steht für das Nullelement ⇒ Lösungsvorschlag 1.

b) B ist das Ergebnis der Addition von α^5 und α^6 ⇒ Lösungsvorschlag 3:

$$\alpha^5 + \alpha^6 = (111) + (101) = (010) = \alpha^1\,.$$

Man hätte dieses Ergebnis auch einfacher finden könen, da in jeder Zeile und Spalte jedes Element genau einmal vorkommt. Nachdem A = 0 festliegt, fehlt in der letzten Zeile und der letzten Spalte genau nur noch das Element α^1.

c) C ist das Ergebnis der Summe von α^1 und α^2 ⇒ Lösungsvorschlag 3:

$$\alpha^1 + \alpha^2 = (010) + (100) = (110) = \alpha^4\,.$$

d) *D* ist das Ergebnis von α^3 und α^5 ⇒ Lösungsvorschlag 1:

$$\alpha^3 + \alpha^5 = (011) + (111) = (100) = \alpha^2\,.$$

e) Alle Lösungsvorschläge sind richtig, wie man aus der Zeile 2 (Multiplikation mit dem Einselement) erkennt. Aufgrund der Gültigkeit von

$$\alpha^i \cdot \alpha^j = \alpha^{(i+j)\ \mathrm{mod}\ 7}$$

ergibt sich bei der Multiplikation eine gewisse Symmetrie, die man ebenfalls zur Lösung nutzen könnte.

Nachfolgend sehen Sie die vollständigen Tabellen für die Addition und die Multiplikation.

+	0	1	α^1	α^2	α^3	α^4	α^5	α^6	
0	0	1	α^1	α^2	α^3	α^4	α^5	α^6	000
1	1	0	α^3	α^6	α^1	α^5	α^4	α^2	001
α^1	α^1	α^3	0	α^4	1	α^2	α^6	α^5	010
α^2	α^2	α^6	α^4	0	α^5	α^1	α^3	1	100
α^3	α^3	α^1	1	α^5	0	α^6	α^2	α^4	011
α^4	α^4	α^5	α^2	α^1	α^6	0	1	α^3	110
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α^1	111
α^6	α^6	α^2	α^5	1	α^4	α^3	α^1	0	101
	000	001	010	100	011	110	111	101	

·	0	1	α^1	α^2	α^3	α^4	α^5	α^6	
0	0	0	0	0	0	0	0	0	000
1	0	1	α^1	α^2	α^3	α^4	α^5	α^6	001
α^1	0	α^1	α^2	α^3	α^4	α^5	α^6	1	010
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α^1	100
α^3	0	α^3	α^4	α^5	α^6	1	α^1	α^2	011
α^4	0	α^4	α^5	α^6	1	α^1	α^2	α^3	110
α^5	0	α^5	α^6	1	α^1	α^2	α^3	α^4	111
α^6	0	α^6	1	α^1	α^2	α^3	α^4	α^5	101
	000	001	010	100	011	110	111	101	

f) Richtig ist hier der Lösungsvorschlag 3. Alle Polynome sind zwar irreduzibel. Man benötigt aber für GF(2^3) ein Grad–3–Polynom. Der dritte Lösungsvorschlag ergibt sich aus der Beziehung

$$\alpha^3 = \alpha + 1 \quad \Rightarrow \quad p(\alpha) = \alpha^3 + \alpha + 1 = 0\,.$$

Musterlösung zur Aufgabe A2.9

a) Für die RS–Codelänge gilt allgemein:

$$n = q - 1 = 2^m - 1$$
$$\Rightarrow \quad m = 4\text{: } \underline{n = 15}, \quad m = 5\text{: } \underline{n = 31}, \quad m = 6\text{: } \underline{n = 63}.$$

b) Um t Symbolfehler korrigieren zu können, muss die minimale Distanz $d_{\rm min} = 2t + 1$ betragen. Der Reed–Solomon–Code ist ein sogenannter MDS–Code (*Maximum Distance Seperable*). Für diese gilt:

$$d_{\rm min} = n - k + 1 = 2t + 1 \quad \Rightarrow \quad k = n - 2t = 2^m - (2t + 1).$$

Damit erhält man für den

- RSC 1 (mit $m = 4$, $t = 4$): $k = 2^4 - (2 \cdot 4 + 1) = \underline{7}$,
- RSC 2 (mit $m = 5$, $t = 8$): $k = 2^5 - (2 \cdot 8 + 1) = \underline{15}$.

c) Die Bezeichnung eines Reed–Solomon–Codes lautet RSC $(n, k, d_{\rm min})_q$ mit $q = 2^m = n + 1$. Richtig sind demnach die <u>Lösungsvorschläge 1 und 4</u>:

- RSC 1 ⇒ RSC $(15, 7, 9)_{16}$,
- RSC 2 ⇒ RSC $(31, 15, 17)_{32}$.

d) Bezeichnet $d_{\rm min}$ die minimale Distanz eines Blockcodes, so können damit $e = d_{\rm min} - 1$ Symbolfehler erkannt und $t = e/2$ Symbolfehler korrigiert werden:

- RSC 1: $d_{\rm min} = 9$, $t = 4$, $\underline{e = 8}$,
- RSC 2: $d_{\rm min} = 17$, $t = 8$, $\underline{e = 16}$.

e) Richtig sind die beiden mittleren <u>Lösungsvorschläge 2 und 3</u>. Bei RSC 1 ($m = 4$) entsprechen $n = 15$ Codesymbole aus GF(2^5) gleich 60 Bit und $k = 7$ Informationssymbole genau 28 Bit:

- RSC 1 ⇒ RSC $(15, 7, 9)_{16}$ ⇒ RSC $(60, 28, 9)_2$,
- RSC 2 ⇒ RSC $(31, 15, 17)_{32}$ ⇒ RSC $(155, 75, 17)_2$.

Für die minimale Distanz auf Bitebene ergeben sich mit $d_{\rm min} = 9$ bzw. $d_{\rm min} = 17$ die gleichen Werte wie auf Symbolebene (siehe **Theorieteil).**

Musterlösung zur Aufgabe A2.10

a) Die Gleichung zur Beschreibung der Gewichte W_i lautet ($d_{\rm min}$ ist hier mit d abgekürzt):

$$W_i = \binom{n}{i} \cdot \sum_{j=0}^{i-d} (-1)^j \cdot \binom{i}{j} \cdot \left[q^{i-j-d+1} - 1\right].$$

Wegen der minimalen Distanz $d_{\rm min} = 5$ sind $W_3 \underline{= 0}$ und $W_4 \underline{= 0}$. Die weiteren Gewichte ergeben sich zu

$$W_5 = \binom{7}{5} \cdot (8^1 - 1) = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} \cdot 7 = 21 \cdot 7 \underline{= 147},$$

$$W_6 = \binom{7}{6} \cdot \sum_{j=0}^{1} (-1)^j \cdot \binom{6}{j} \cdot (8^{2-j} - 1) =$$

$$= 7 \cdot \left[(8^2 - 1) - 6 \cdot (8^1 - 1)\right] = 7 \cdot (63 - 42) \underline{= 147},$$

$$W_7 = \binom{7}{7} \cdot \sum_{j=0}^{2} (-1)^j \cdot \binom{7}{j} \cdot (8^{3-j} - 1) =$$

$$= (8^3 - 1) - 7 \cdot (8^2 - 1) + 21 \cdot (8^1 - 1) = 511 - 7 \cdot 63 + 21 \cdot 7 \underline{= 217},$$

$$\Rightarrow \quad W_0 + W_5 + W_6 + W_7 = 1 + 147 + 147 + 217 = 512 = 8^3 = q^k.$$

b) Analog zur Teilaufgabe (a) erhält man:

$$W_3 = \binom{7}{3} \cdot (8^1 - 1) = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} \cdot 7 = 35 \cdot 7 \underline{= 245}.$$

c) Die Verfälschungswahrscheinlichkeit eines einzelnen Symbols ist mit $\varepsilon_{\rm S} = 0.1$ gegeben. Dann gilt für die Wahrscheinlichkeit, dass in einem Codewort mit $n = 7$ Codesymbolen

- genau 3 Symbole verfälscht werden:

  $$p_3 = 0.1^3 \cdot 0.9^4 = 0.6561 \cdot 10^{-3},$$

- genau 4 Symbole verfälscht werden:

  $$p_4 = 0.1^4 \cdot 0.9^3 = 0.729 \cdot 10^{-4},$$

- genau 5 Symbole verfälscht werden:

  $$p_5 = 0.1^5 \cdot 0.9^2 = 0.81 \cdot 10^{-5},$$

- genau 6 Symbole verfälscht werden:

  $$p_6 = 0.1^6 \cdot 0.9 = 0.9 \cdot 10^{-6},$$

- alle $n = 7$ Symbole verfälscht werden:

  $$p_7 = 0.1^7 = 10^{-7}.$$

Beim **RSC (7, 3, 5)$_8$** kann das Nullwort durch Symbolfehler in eines von $q^k - 1 = 8^3 - 1 = 511$ anderen Codeworten verfälscht werden. Damit erhält man mit den Gewichtsfunktionen von Teilaufgabe (a):

$$\Pr(\text{Blockfehler}) = \frac{W_5 \cdot p_5 + W_6 \cdot p_6 + W_7 \cdot p_7}{511} =$$

$$= \frac{147 \cdot 0.81 \cdot 10^{-5} + 147 \cdot 0.9 \cdot 10^{-6} + 217 \cdot 10^{-7}}{511} \underline{\approx 0.263 \cdot 10^{-5}}.$$

Beim **RSC (7, 5, 3)$_8$** muss wegen $k = 5$ über $8^5 - 1 = 32767$ Verfälschungswahrscheinlichkeiten gemittelt werden. Mit $W_3 = 245$ aus Teilaufgabe (b) und den Gewichten $W_4 = 1224$, $W_5 = 5586$, $W_6 = 12838$, $W_7 = 12873$ entsprechend dem Angabenblatt erhält man hierfür:

$$\Pr(\text{Blockfehler}) = \frac{W_3 \cdot p_3 + W_4 \cdot p_4 + W_5 \cdot p_5 + W_6 \cdot p_6 + W_7 \cdot p_7}{32767} =$$

$$= \frac{245 \cdot 0.656 \cdot 10^{-3} + \ \ldots \ + 12873 \cdot 10^{-7}}{32767} \underline{\approx 0.942 \cdot 10^{-5}}.$$

d) Bekannt sei nur $d_{\min}$ (im Folgenden mit d abgekürzt) und damit auch $p_d = \varepsilon_S{}^d \cdot (1 - \varepsilon_S)^{n-d}$. Dies ist gleichzeitig die gesuchte obere Schranke:

- RSC $(7, 3, 5)_8$: Pr(Obere Schranke) = $p_5 = \underline{0.81 \cdot 10^{-5}}$,
- RSC $(7, 5, 3)_8$: Pr(Obere Schranke) = $p_3 = \underline{0.656 \cdot 10^{-3}}$.

Da das Gewicht W_d als nicht bekannt vorausgesetzt wurde, setzt man dieses auf den maximal möglichen Wert ($W_5 = 511$ bzw. $W_3 = 32767$), so dass die Vorfaktoren in den Gleichungen zur Teilaufgabe (c) verschwinden. Nur so ist eine obere Schranke sichergestellt.

Die obere Schranke liegt in beiden Fällen deutlich über den Ergebnissen der Teilaufgabe (c):

- RSC $(7, 3, 5)_8$: $0.810 \cdot 10^{-5}$ statt $0.263 \cdot 10^{-5}$ (Faktor ca. 3),
- RSC $(7, 5, 3)_8$: $0.656 \cdot 10^{-3}$ statt $0.942 \cdot 10^{-5}$ (Faktor 117ca. 70).

e) Mit der Abkürzung $d = d_{\min}$ erhält man für die untere Schranke:

$$\Pr(\text{Untere Schranke}) = \frac{W_d \cdot p_d}{q^k - 1}.$$

- Für den RSC $(7, 3, 5)_8$ liegt wegen $W_d = W_5$ und $p_d = p_5$ die untere Schranke

$$\Pr(\text{Untere Schranke}) = \frac{147 \cdot 0.81 \cdot 10^{-5}}{511} \underline{\approx 0.233 \cdot 10^{-5}}$$

um etwa 11% unterhalb des tatsächlichen Wertes ($0.263 \cdot 10^{-5}$).

- Für den RSC $(7, 5, 3)_8$ gilt mit $W_d = W_3$ und $p_d = p_3$:

$$\Pr(\text{Untere Schranke}) = \frac{245 \cdot 0.656 \cdot 10^{-3}}{32767} \underline{\approx 0.494 \cdot 10^{-5}}.$$

Die untere Schranke weicht hier vom tatsächlichen Wert stärker ab, weil bei diesem Code die Beiträge der höheren Gewichte (W_4, W_5, W_6, W_7) in Relation zu W_3 relevanter sind.

Musterlösung zur Zusatzaufgabe Z2.10

a) Aus der Codelänge $n = 255$ folgt $q = 256$. Die Coderate ergibt sich zu

$$R = \frac{223}{255} = 0.8745$$

Die minimale Distanz beträgt

$$d_{\rm min} = n - k + 1 = 255 - 223 + 1 = 33.$$

Damit können

- $e = d_{\rm min} - 1 = 32$ Symbolfehler erkannt werden,
- $t = e/2$ (abgerundet), also $t = 16$ Symbolfehler korrigiert werden.

b) Dieser Code ist die Binärrepräsentation des unter (a) behandelten RSC $(255, 223, 33)_{256}$ mit genau der gleichen Coderate $R = 0.8745$ und ebenfalls gleicher Minimaldistanz $d_{\rm min} = 33$ wie dieser. Hier werden pro Codesymbol 8 Bit (1 Byte) verwendet.

c) Aus $d_{\rm min} = 33$ folgt wieder $t = 16 \Rightarrow N_{\rm Bitfehler} = 16$. Ist in jedem Codesymbol genau ein Bit verfälscht, so bedeutet dies gleichzeitig auch 16 Symbolfehler. Dies ist der maximale Wert, den der Reed–Solomon–Decoder noch verkraften kann.

d) Der RS–Decoder kann 16 verfälschte Codesymbole korrigieren, wobei es egal ist, ob in einem Codesymbol nur ein Bit oder alle $m = 8$ Bit verfälscht wurden. Deshalb können bei der günstigsten Fehlerverteilung bis zu $8 \cdot 16 = 128$ Bit verfälscht sein, ohne dass das Codewort falsch decodiert wird.

Musterlösung zur Aufgabe A2.11

a) Die Spaltenanzahl der Prüfmatrix **H** gibt die Codelänge an: $n = 7$. Zum gleichen Ergebnis kommt man, wenn man von der Ordnung $q = 8$ des Galoisfeldes ausgeht. Bei den Reed–Solomon–Codes gilt nämlich $n = q - 1$. Die Zeilenanzahl der Prüfmatrix ist gleich $n - k = 3 \Rightarrow k = 4$. Von allen Reed–Solomon–Codes wird die **Singleton–Schranke** erfüllt $\Rightarrow d_{\rm min} = n - k + 1 = 4$. Es handelt sich also um den Reed–Solomon–Code $(7, 4, 4)_8$.

b) Eine Decodierung ist sicher möglich, so lange die Anzahl e der Auslöschungen kleiner ist als die Minimaldistanz $d_{\rm min}$. Diese Bedingung ist hier erfüllt ⇒ JA. Nachdem bei allen RS–Codes das Nullwort zulässig ist und jedes andere Codewort mindestens vier Symbole ungleich „0" beinhaltet, ist bereits ohne Rechnung sicher, dass das Nullwort gesendet wurde. Die formale Rechnung bestätigt dieses Ergebnis:

$$\mathbf{H}_{\rm K} \cdot \underline{z}_{\rm K}^{\rm T} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} \alpha^6 \\ \alpha^5 \\ \alpha^4 \end{pmatrix} \cdot z_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \Rightarrow \quad z_6 = 0\,.$$

c) Auch hier ist $e = 2$ kleiner als $d_{\rm min} = 4 \Rightarrow$ JA. Da auch (1, 1, 1, 1, 1, 1, 1) ein gültiges Codewort ist, erwarten wir bei der formalen Überprüfung $z_0 = 1$ und $z_1 = 1$.

$$\mathbf{H}_{\rm K} \cdot \underline{z}_{\rm K}^{\rm T} = \begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 \\ \alpha^4 + \alpha^6 + \alpha^1 + \alpha^3 + \alpha^5 \\ \alpha^6 + \alpha^2 + \alpha^5 + \alpha^1 + \alpha^4 \end{pmatrix} =$$

$$= \begin{pmatrix} (100) + (011) + (110) + (111) + (101) \\ (110) + (101) + (010) + (011) + (111) \\ (101) + (100) + (111) + (010) + (110) \end{pmatrix} = \begin{pmatrix} (011) \\ (101) \\ (010) \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^6 \\ \alpha^1 \end{pmatrix}.$$

Bei dieser Berechnung wurde zwischen der Polynomdarstellung und der Koeffizientendarstellung auf der Angabenseite variiert. Damit lautet das Gleichungssystem:

$$\begin{pmatrix} (001) + (010) \\ (001) + (100) \\ (001) + (011) \end{pmatrix} \cdot \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} (011) \\ (101) \\ (010) \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} (001) + (010) \\ (001) + (100) \\ (000) + (111) \end{pmatrix} \cdot \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} (011) \\ (101) \\ (111) \end{pmatrix}.$$

Die zweite Form ergibt sich, wenn man die dritten Zeile aus der Modulo–2–Summe der Zeilen 2 und 3 ersetzt. Aus der letzten Zeile folgt nun $z_1 = 1$ und die Zeilen 1 und 2 lauten dann:

$$(1) \quad z_0 + (010) \cdot 1 = (011) \quad \Rightarrow \quad z_0 = (001) = 1\,,$$
$$(2) \quad z_0 + (100) \cdot 1 = (101) \quad \Rightarrow \quad z_0 = (001) = 1\,.$$

Beide Gleichungen führen zum gleichen Ergebnis $z_0 = 1$, $z_1 = 1$. Die Decodierung ist erfolgreich.

d) Die Decodierung passiert auf folgenden Schritten:

$$\mathbf{H}_{\rm K} \cdot \underline{z}_{\rm K}^{\rm T} = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ \alpha \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha^4 + \alpha^6 \\ \alpha^1 + \alpha^4 \\ \alpha^5 + \alpha^2 \end{pmatrix} =$$

$$= \begin{pmatrix} (110) + (101) \\ (010) + (110) \\ (111) + (100) \end{pmatrix} = \begin{pmatrix} (011) \\ (100) \\ (011) \end{pmatrix},$$

$$\mathbf{H}_{\rm E} \cdot \underline{z}_{\rm E}^{\rm T} = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \\ 1 & \alpha^3 & \alpha^6 \end{pmatrix} \cdot \begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix}$$

$$\Rightarrow \quad \begin{pmatrix} (001) & (010) & (100) \\ (001) & (100) & (110) \\ (001) & (011) & (101) \end{pmatrix} \cdot \begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} (011) \\ (100) \\ (011) \end{pmatrix}.$$

Wir ersetzen nun die Zeile 2 durch die Modulo–2–Summe der Zeilen 1 und 2 sowie die Zeile 3 durch die Modulo–2–Summe der Zeilen 1 und 3:

$$\begin{pmatrix} (001) & (010) & (100) \\ (000) & (110) & (010) \\ (000) & (001) & (001) \end{pmatrix} \cdot \begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} (011) \\ (111) \\ (000) \end{pmatrix}.$$

Aus der letzten Zeile folgt $z_1 + z_2 = 0 \;\Rightarrow\; z_2 = z_1$. Eingesetzt in die zweite Zeile dieser Matrixgleichung erhält man:

$$[(110) + (010)] \cdot z_1 = (100) \cdot z_1 = (111) \;\Rightarrow\; \alpha^2 \cdot z_1 = \alpha^5 \;\Rightarrow\; z_1 \underline{= \alpha^3},\; z_2 \underline{= \alpha^3}.$$

Mit diesem Ergebnis folgt aus der ersten Matrixzeile:

$$z_0 + [(010) + (100)] \cdot z_1 = z_0 + (110) \cdot z_1 = (011)$$

$$\Rightarrow \;\; z_0 + \alpha^4 \cdot \alpha^3 = z_0 + 1 = \alpha^3 \;\Rightarrow\; z_0 = \alpha^3 + 1 = (\alpha + 1) + 1 \underline{= \alpha}.$$

Richtig ist demnach der Lösungsvorschlag 2.

e) Richtig ist der Lösungsvorschlag 4. Begründung:

- Aus den drei bekannten Symbolen 0, 1, α kann man nicht vier Informationssymbole gewinnen.
- Die **H**–Matrix dieses $(7, 4, 4)_8$–Codes hat genau $n - k = 3$ Zeilen. Man hat damit auch nur drei Gleichungen. Benötigen würde man aber vier Gleichungen für die Unbekannten z_0, z_1, z_2 und z_6.

Musterlösung zur Zusatzaufgabe Z2.11

a) Aufgrund der Symmetrie des vorgegebenen BEC–Modells (Auslöschungskanal auf Bitebene) gilt für die *Erasure*–Wahrscheinlichkeit: $\Pr(y = \text{E}) = \lambda = \underline{0.2}$. Da die Codesymbole 0 und 1 gleichwahrscheinlich sind, erhält man für deren Wahrscheinlichkeiten $\Pr(y = 0) = \underline{0.4}$ und $\Pr(y = 1) = \underline{0.4}$.

b) Ohne Einschränkung der Allgemeingültigkeit gehen wir zur Lösung dieser Aufgabe vom Codesymbol $c_{\text{binär}}$ = „00” aus. Entsprechend dem 2–BEC–Modell kann dann das Empfangssymbol $y_{\text{binär}}$ entweder „00” oder ausgelöscht (E) sein und es gilt:

$$\Pr(y_{\text{bin}} = \text{"00"} \,|\, c_{\text{bin}} = \text{"00"}) = (1-\lambda)^2 = 0.8^2 = 0.64 = 1 - \lambda_2$$
$$\Rightarrow \quad \lambda_2 = 1 - (1-\lambda)^2 \underline{= 0.36}.$$

Es ist vorausgesetzt, dass ein *Erasure* nur vermieden wird, wenn keines der zwei Bit ausgelöscht wurde.

c) Der RSC $(255, 223, 33)_{256}$ basiert auf dem Galoisfeld GF(256) = GF(2^8) $\Rightarrow$ $m = 8$. Das Ergebnis der Teilaufgabe (b) muss nun an diesen Fall angepasst werden. Für den 8–BEC gilt:

$$1 - \lambda_8 = (1-\lambda)^8 = 0.8^8 \approx 0.168 \quad \Rightarrow \quad \lambda_m = \lambda_8 \underline{\approx 0.832}.$$

d) Aus der Bedingung $\lambda_m \le 0.2$ folgt direkt $1 - \lambda_m \ge 0.8$. Daraus folgt weiter:

$$(1-\lambda)^8 \ge 0.8 \quad \Rightarrow \quad 1 - \lambda \ge 0.8^{0.125} \approx 0.9725 \quad \Rightarrow \quad \lambda \underline{\le 0.0275}.$$

e) Mit $\lambda = 0.0275$ $\Rightarrow$ $\lambda_m = 0.2$ sind 20% der Empfangssymbole *Erasures*. Die anderen $2^8 = 256$ Empfangssymbole „000000000” .... „11111111” sind alle gleichwahrscheinlich. Daraus folgt:

$$\Pr(y_{\text{bin}} = \text{"00000000"}) = \ldots = \Pr(y_{\text{bin}} = \text{"11111111"}) = \frac{0.8}{256} \underline{= 0.003125}.$$

Musterlösung zur Aufgabe A2.12

a) Der betrachtete Reed–Solomon–Code $(7, 4, 4)_8$ kann wegen $d_{\rm min} = 4$ nur $t = \lfloor (d_{\rm min} - 1)/2 \rfloor = 1$ Symbolfehler korrigieren. Relevant ist also nur das blau hinterlegte Schema, das für den Fall gilt, dass es genau einen Symbolfehler im Empfangswort gibt ($r = 1$) ⇒ Lösungsvorschlag 1.

b) Entsprechend der Grafik auf der Angabenseite besitzt der Vektor $\underline{\Lambda}_l$ hier $L = n - k = 3$ Elemente.

c) Es gibt nur die beiden ELP–Koeffizientenvektoren $\underline{\Lambda}_1 = (\lambda_0, 1, 0)$ und $\underline{\Lambda}_2 = (0, \lambda_0, 1)$ ⇒ $l_{\rm max} = 2$.

d) Aus $\underline{\Lambda}_1$ und $\underline{\Lambda}_2$ ergeben sich zwei skalare Bestimmungsgleichungen $\underline{\Lambda}_l \cdot \underline{s}^{\rm T} = 0$ für den Parameter λ_0:

$$\lambda_0 \cdot \alpha^4 + \alpha^5 = 0 \quad \Rightarrow \quad \lambda_0 \cdot \alpha^4 = -\alpha^5 = \alpha^5 \quad \Rightarrow \quad \lambda_0 = \alpha,$$
$$\lambda_0 \cdot \alpha^5 + \alpha^6 = 0 \quad \Rightarrow \quad \lambda_0 = \alpha.$$

Das Gleichungssystem ist eindeutig lösbar ⇒ Antwort JA.

e) Mit dem Ergebnis der Teilaufgabe (d) ⇒ $\lambda_0 = \alpha$ erhält man für das *Error Locator Polynom*

$$\Lambda(x) = x \cdot (\lambda_0 + x) = x \cdot (\alpha + x)$$
$$\Rightarrow \quad \Lambda(\alpha^0) = 1 \cdot (\alpha + 1) = \alpha + 1 \neq 0 \quad \Rightarrow \quad \text{Keine Nullstelle},$$
$$\Lambda(\alpha^1) = \alpha \cdot (\alpha + \alpha) = 0 \quad \Rightarrow \quad \textbf{Nullstelle}.$$

Verfälscht wurde also das Symbol an der Position 1 ⇒ Lösungsvorschlag 2. Da die Berechnung in der Teilaufgabe (d) unter der Bedingung $r = 1$ erfolgte, wurden alle anderen Symbole richtig übertragen:

$$\underline{e} = (0, e_1, 0, 0, 0, 0, 0).$$

f) Aus der Bedingung $\underline{e} \cdot \mathbf{H}^{\rm T} = \underline{s}^{\rm T}$ folgt

$$(0, e_1, 0, 0, 0, 0, 0) \cdot \begin{pmatrix} 1 & 1 & 1 \\ \alpha^1 & \alpha^2 & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^3 & \alpha^6 & \alpha^9 \\ \alpha^4 & \alpha^8 & \alpha^{12} \\ \alpha^5 & \alpha^{10} & \alpha^{15} \\ \alpha^6 & \alpha^{12} & \alpha^{18} \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} \alpha^4 \\ \alpha^5 \\ \alpha^6 \end{pmatrix}$$

$$\Rightarrow \quad e_1 \cdot \alpha = \alpha^4, \quad e_1 \cdot \alpha^2 = \alpha^5, \quad e_1 \cdot \alpha^3 = \alpha^6.$$

Potenzen von α	Polynome in α	Vektoren $k_2\, k_1\, k_0$
$\alpha^{-\infty} = 0$	0	0 0 0
$\alpha^0 = 1$	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha + 1$	0 1 1
α^4	$\alpha^2 + \alpha$	1 1 0
α^5	$\alpha^2 + \alpha + 1$	1 1 1
α^6	$\alpha^2 + 1$	1 0 1

Die Lösung führt stets zum Ergebnis $e_1 = \alpha^3$ ⇒ Antwort 2. Mit dem Empfangswort $\underline{y} = (\alpha^1, 0, \alpha^3, 0, 1, \alpha^1, 0)$ erhält man das Decodierergebnis $\underline{z} = (\alpha^1, \alpha^3, \alpha^3, 0, 1, \alpha^1, 0)$.

g) Analog zur Teilaufgabe (d) lautet nun das Gleichungssystem:

$$\lambda_0 \cdot \alpha^2 + \alpha^4 = 0 \quad \Rightarrow \quad \lambda_0 = \alpha^2,$$
$$\lambda_0 \cdot \alpha^4 + \alpha^5 = 0 \quad \Rightarrow \quad \lambda_0 = \alpha.$$

Die beiden Lösungen widersprechen sich. Bei der Übertragung müssen also mindestens zwei Symbole verfälscht worden sein und die Decodierung versagt ⇒ Antwort NEIN. Man müsste nun einen neuen Versuch gemäß dem roten Schema ($r = 2$) starten.

Musterlösung zur Zusatzaufgabe Z2.12

a) Die entsprechende Gleichung zur Syndromberechnung lautet:

$$\underline{s} = (s_0, s_1, s_2) =$$

$$= (\alpha, 0, \alpha^3, 0, 1, \alpha, 0) \cdot \begin{pmatrix} 1 & 1 & 1 \\ \alpha^1 & \alpha^2 & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^3 & \alpha^6 & \alpha^2 \\ \alpha^4 & \alpha^1 & \alpha^5 \\ \alpha^5 & \alpha^3 & \alpha^1 \\ \alpha^6 & \alpha^5 & \alpha^4 \end{pmatrix} .$$

Potenzen von α	Polynome in α	Vektoren $k_2\, k_1\, k_0$
$\alpha^{-\infty}=0$	0	0 0 0
$\alpha^0=1$	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+1$	0 1 1
α^4	$\alpha^2+\alpha$	1 1 0
α^5	$\alpha^2+\alpha+1$	1 1 1
α^6	α^2+1	1 0 1

Das erste Element ergibt sich zu

$$s_0 = \alpha \cdot 1 + \alpha^3 \cdot \alpha^2 + 1 \cdot \alpha^4 + \alpha \cdot \alpha^5 = \alpha + \alpha^5 + \alpha^4 + \alpha^6 =$$
$$= (\alpha) + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) + +(\alpha^2 + 1) = \alpha^2 + \alpha = \alpha^4 .$$

Richtig ist der Lösungsvorschlag 1.

b) Entsprechend gilt für das zweite Syndromelement

$$s_1 = \alpha \cdot 1 + \alpha^3 \cdot \alpha^4 + 1 \cdot \alpha^1 + \alpha \cdot \alpha^3 = \alpha + \alpha^7 + \alpha + \alpha^4 =$$
$$= 1 + \alpha^4 = \alpha^2 + \alpha + 1 = \alpha^5 .$$

Richtig ist der Lösungsvorschlag 2.

c) Zur Berechnung von s_2 muss mit der letzten Matrixspalte multipliziert werden:

$$s_2 = \alpha \cdot 1 + \alpha^3 \cdot \alpha^6 + 1 \cdot \alpha^5 + \alpha \cdot \alpha^1 = \alpha + \alpha^2 + \alpha^5 + \alpha^2 =$$
$$= \alpha^5 + \alpha = (\alpha^2 + \alpha + 1) + \alpha = \alpha^2 + 1 = \alpha^5 .$$

⇒ Lösungsvorschlag 3.

d) Aufgrund des errechneten Syndroms $\underline{s} = (\alpha^4, \alpha^5, \alpha^6) \neq 0$ beinhaltet das Empfangswort mindestens einen Symbolfehler ⇒ $r > 0$. Da der vorliegende Reed–Solomon–Code $(7, 4, 4)_8$ ⇒ $d_{\rm min} = 4$ auch nicht mehr als $t = \lfloor d_{\rm min}/2 \rfloor = 1$ Fehler korrigieren kann und das Empfangswort vereinbarungsgemäß ebenfalls decodiert werden kann, gilt $r = 1$.

Musterlösung zur Aufgabe A2.13

a) Der RSC $(7, 3, 5)_8$ kann bis zu $t = 2$ Symbolfehler korrigieren. Die tatsächliche Symbolfehleranzahl r darf nicht größer sein ⇒ Lösungsvorschläge 1 und 2.

b) Unter der Annahme $r = 1$ lauten die n–k–1 Bestimmungsgleichungen für λ_0 gemäß $\underline{\Lambda}_l \cdot \underline{s}^{\rm T} = 0$:

$$\begin{aligned}\lambda_0 \cdot 0 \;+\; 1 = 0 \quad &\Rightarrow \quad \lambda_0 \text{ unbestimmt},\\ \lambda_0 \cdot 1 \;+\; \alpha^5 = 0 \quad &\Rightarrow \quad \lambda_0 = \alpha^5,\\ \lambda_0 \cdot \alpha^5 \;+\; \alpha^2 = 0 \quad &\Rightarrow \quad \lambda_0 = \alpha^{-3} = \alpha^4.\end{aligned}$$

Potenzen von α	Polynome in α	Vektoren $k_2\, k_1\, k_0$
$\alpha^{-\infty}=0$	0	0 0 0
$\alpha^0=1$	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+1$	0 1 1
α^4	$\alpha^2+\alpha$	1 1 0
α^5	$\alpha^2+\alpha+1$	1 1 1
α^6	α^2+1	1 0 1

Die Annahme $r = 1$ wäre nur dann gerechtfertigt, wenn sich aus allen diesen drei Gleichungen der gleiche λ_0–Wert ergäbe. Dies ist hier nicht der Fall ⇒ Antwort NEIN.

c) Geht man von der Belegung für $r = 2$ aus, so erhält man zwei Bestimmungsgleichungen für λ_0 und λ_1:

$$\begin{aligned}\lambda_0 \cdot 0 \;+\; \lambda_1 \cdot 1 + \alpha^5 = 0 \quad &\Rightarrow \quad \lambda_1 = \alpha^5,\\ \lambda_0 \cdot 1 \;+\; \lambda_1 \cdot \alpha^5 + \alpha^2 = 0 \quad &\Rightarrow \quad \lambda_0 = \alpha^{5+5} + \alpha^2 = \alpha^3 + \alpha^2 = \alpha^5.\end{aligned}$$

Das Gleichungssystem lässt sich unter der Annahme $r = 2$ lösen ⇒ Antwort JA. Die hier gewonnenen Ergebnisse $\lambda_0 = \lambda_1 = \alpha^5$ werden in der nächsten Teilaufgabe verarbeitet.

d) Mit dem Ergebnis $\lambda_0 = \lambda_1 = \alpha^5$ lautet das *Error Locator Polynom* (oder die Schlüsselgleichung):

$$\Lambda(x) = x \cdot \left(\lambda_0 + \lambda_1 \cdot x + x^2\right) = x \cdot \left(\alpha^5 + \alpha^5 \cdot x + x^2\right).$$

Diese Funktion weist Nullstellen für $x = \alpha^2$ und $x = \alpha^3$ auf:

$$\begin{aligned}\Lambda(x = \alpha^2) \;&=\; \alpha^2 \cdot \left(\alpha^5 + \alpha^7 + \alpha^4\right) = \alpha^2 \cdot \left(\alpha^5 + 1 + \alpha^4\right) = 0,\\ \Lambda(x = \alpha^3) \;&=\; \alpha^3 \cdot \left(\alpha^5 + \alpha^8 + \alpha^6\right) = \alpha^3 \cdot \left(\alpha^5 + \alpha + \alpha^6\right) = 0.\end{aligned}$$

Verfälscht sind folglich die Symbole an den Positionen 2 und 3 ⇒ Lösungsvorschläge 3 und 4.

e) Nach dem Ergebnis der Teilaufgabe (d) kommen nur noch die beiden letzten Lösungsvorschläge in Frage ⇒ $\underline{e} = (0, 0, e_2, e_3, 0, 0, 0)$. Der Ansatz lautet deshalb entsprechend $\underline{e} \cdot \mathbf{H}^{\rm T} = \underline{s}$:

$$(0, 0, e_2, e_3, 0, 0, 0) \cdot \begin{pmatrix} 1 & 1 & 1 & 1\\ \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4\\ \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1\\ \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5\\ \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2\\ \alpha^5 & \alpha^3 & \alpha^1 & \alpha^6\\ \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 \end{pmatrix} \;\stackrel{!}{=}\; (0, 1, \alpha^5, \alpha^2).$$

$$\begin{aligned}\Rightarrow \quad e_2 \cdot \alpha^2 \;+\; e_3 \cdot \alpha^3 = 0, \quad &e_2 \cdot \alpha^4 + e_6 \cdot \alpha^3 = 1,\\ e_2 \cdot \alpha^6 \;+\; e_3 \cdot \alpha^2 = \alpha^5, \quad &e_2 \cdot \alpha^1 + e_6 \cdot \alpha^5 = \alpha^2.\end{aligned}$$

Alle vier Gleichungen werden mit $e_2 = 1$ sowie $e_3 = \alpha^6$ erfüllt ⇒ Lösungsvorschlag 3:

$$\underline{e} = (0,\ 0,\ 1,\ \alpha^6,\ 0,\ 0,\ 0)$$

Mit $\alpha + 1 = \alpha^3$ und $\alpha^5 + \alpha^6 = \alpha$ kommt man vom gegebenen Empfangswort $\underline{y} = (\alpha^2, \alpha^3, \alpha, \alpha^5, \alpha^4, \alpha^2, 1)$ zum Decodierergebnis

$$\underline{z} = (\alpha^2,\ \alpha^3,\ \alpha^3,\ \alpha,\ \alpha^4,\ \alpha^2,\ 1)\,.$$

In der **Aufgabe A2.7** wurde gezeigt, dass dies ein zulässiges Codewort des RSC $(7, 3, 5)_8$ ist. Das zugehörige Informationswort lautet $\underline{u} = (\alpha^4, 1, \alpha^3)$.

Musterlösung zur Aufgabe A2.14

a) Richtig ist die Antwort 1. Prinzipiell wäre ein Syndromdecoder auch bei Reed–Solomon–Codes möglich, aber bei den hier üblichen großen Codewortlängen n ergäben sich extrem lange Decodierzeiten. Bei Faltungscodes (diese arbeiten seriell) macht Syndromdecodierung gar keinen Sinn.

b) Wie aus den Ausführungen im Theorieteil hervorgeht, ist die Fehlerlokalisierung mit dem weitaus größten Aufwand verbunden $\Rightarrow$ Antwort 2.

c) Richtig sind die Antworten 1, 3 und 4, die auf der Seite **Schnelle Reed–Solomon–Decodierung** kurz zusammengefasst sind. Der BCJR– und der Viterbi–Algorithmus beziehen sich dagegen auf die Decodierung von Faltungscodes – siehe **Kapitel 3.4.**

Die Grafik auf der Angabenseite zeigt den Berlekamp–Massey–Algorithmus (BMA). Die Erklärung zu dieser Abbildung finden Sie in **[Bos98]** ab Seite 73.

Musterlösung zur Aufgabe A2.15

a) Aus der Tabelle auf der Angabenseite kann der BSC–Parameter $\varepsilon = 0.0505$ abgelesen werden. Damit erhält man für die Symbolverfälschungswahrscheinlichkeit ε_S mit $m = 3$:

$$1 - \varepsilon_S = (1 - 0.0505)^3 \approx 0.856 \quad \Rightarrow \quad \varepsilon_S \approx 0.144\,.$$

Der schnellste Weg zur Berechnung der Blockfehlerwahrscheinlichkeit führt hier über die Formel

$$\begin{aligned}\Pr(\text{Blockfehler}) &= 1 - \Pr(f = 0) - \Pr(f = 1) - \Pr(f = 2) = \\ &= 1 - 1 \cdot 0.856^7 - 7 \cdot 0.144^1 \cdot 0.856^6 - 21 \cdot 0.144^2 \cdot 0.856^5 = \\ &= 1 - 0.3368 - 0.3965 - 0.2001 \underline{= 0.0666}\,.\end{aligned}$$

b) Nach gleichem Rechengang wie in Teilaufgabe (a) ergibt sich mit $\varepsilon_S \approx 0.03 \Rightarrow 1 - \varepsilon_S = 0.97$:

$$\begin{aligned}\Pr(\text{Blockfehler}) &= 1 - 1 \cdot 0.97^7 - 7 \cdot 0.03^1 \cdot 0.97^6 - 21 \cdot 0.03^2 \cdot 0.97^5 = \\ &= 1 - 0.8080 - 0.1749 - 0.0162 = 1 - 0.9991 = 9 \cdot 10^{-4}\,.\end{aligned}$$

Man sieht, dass hier die Differenz zwischen zwei fast gleich großen Zahlen gebildet werden muss, so dass das Ergebnis mit einem Fehler behaftet sein könnte. Deshalb berechnen wir noch folgende Größen:

$$\Pr(f = 3) = \binom{7}{3} \cdot \varepsilon_S^3 \cdot (1 - \varepsilon_S)^4 = 35 \cdot 0.03^3 \cdot 0.97^4 = 8.366 \cdot 10^{-4}\,,$$

$$\Pr(f = 4) = \binom{7}{4} \cdot \varepsilon_S^4 \cdot (1 - \varepsilon_S)^3 = 35 \cdot 0.03^4 \cdot 0.97^3 = 0.259 \cdot 10^{-4}\,,$$

$$\Pr(f = 5) = \binom{7}{5} \cdot \varepsilon_S^5 \cdot (1 - \varepsilon_S)^2 = 21 \cdot 0.03^5 \cdot 0.97^2 = 0.005 \cdot 10^{-4}$$

$$\Rightarrow \quad \Pr(\text{Blockfehler}) \approx \Pr(f = 3) + \Pr(f = 4) + \Pr(f = 5) \underline{= 8.63 \cdot 10^{-4}}\,.$$

Auf die Terme für $f = 6$ und $f = 7$ kann hier verzichtet werden. Sie liefern keinen relevanten Beitrag.

c) Hier ist bereits $\varepsilon_S = 0.005 \Rightarrow 1 - \varepsilon_S = 0.995$ in der Tabelle vorgegeben. Der (weitaus) dominierende Term bei der Berechnung der Blockfehlerwahrscheinlichkeit ist Pr ($f = 3$):

$$\Pr(\text{Blockfehler}) \approx \Pr(f = 3) = \binom{7}{3} \cdot 0.005^3 \cdot 0.995^4 \underline{\approx 4.3 \cdot 10^{-6}}\,.$$

d) Für den BSC–Parameter ε gilt mit $\varepsilon_S = 0.1$:

$$\varepsilon = 1 - (1 - \varepsilon_S)^{1/3} = 1 - 0.9^{1/3} \approx 0.0345\,.$$

Der Zusammenhang zwischen ε und E_B/N_0 lautet:

$$\varepsilon = \text{Q}(x)\,, \quad x = \sqrt{2 \cdot R \cdot E_B/N_0}\,.$$

Die Inverse $x = \text{Q}^{-1}(0.0345)$ ergibt sich mit dem Programm **Gaußsche Fehlerfunktionen** zu $x = 1.82$. Damit erhält man weiter:

$$E_B/N_0 = \frac{x^2}{2R} = \frac{1.82^2}{2R \cdot 3/7} \approx 3.864 \quad \Rightarrow \quad 10 \cdot \lg\,(E_B/N_0) \underline{\approx 5.87\ \text{dB}}\,.$$

e) Nach gleicher Rechnung erhält man

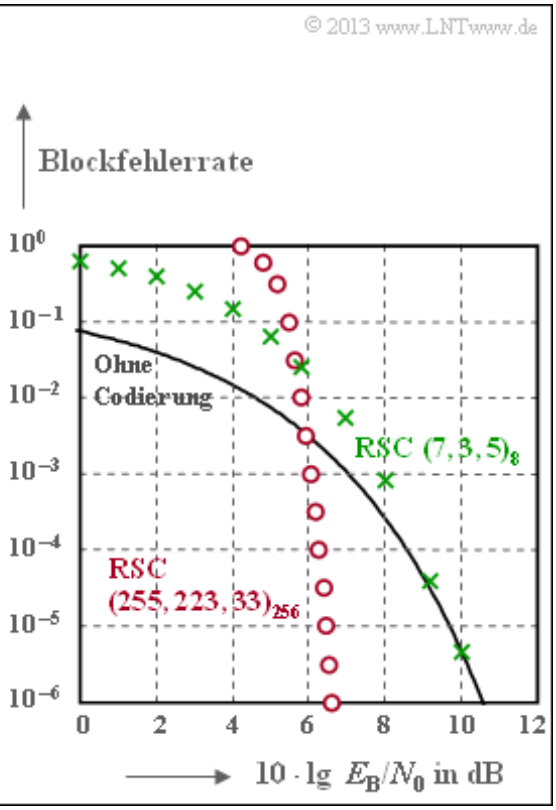
- für $\varepsilon_S = 10^{-2} \;\Rightarrow\; \varepsilon \approx 0.33 \cdot 10^{-2} \;\Rightarrow\; x = Q^{-1}(\varepsilon) = 2.71$:

$$E_B/N_0 = \frac{x^2}{2R} = \frac{2.71^2}{2R \cdot 3/7} \approx 8.568 \quad \Rightarrow \quad 10 \cdot \lg\,(E_B/N_0) \approx \underline{9.32\ \text{dB}},$$

- für $\varepsilon_S = 10^{-3} \;\Rightarrow\; \varepsilon \approx 0.33 \cdot 10^{-3} \;\Rightarrow\; x = Q^{-1}(\varepsilon) = 3.4$:

$$E_B/N_0 = \frac{x^2}{2R} = \frac{3.4^2}{2R \cdot 3/7} \approx 13.487 \quad \Rightarrow \quad 10 \cdot \lg\,(E_B/N_0) \approx \underline{11.3\ \text{dB}}.$$

E_B/N_0 log.	E_B/N_0 lin.	BSC ε	3–BSC ε_S	$Pr(\underline{v} \neq \underline{u})$
0 dB	1.000	0.176	0.441	0.666
1 dB	1.259	0.149	0.384	0.545
2 dB	1.585	0.123	0.325	0.470
3 dB	1.995	0.095	0.259	0.263
4 dB	2.512	0.071	≈ 0.2	0.148
5 dB	3.162	0.0505	0.144	$6.66 \cdot 10^{-2}$
5.87 dB	3.864	0.0345	≈ 0.1	$2.57 \cdot 10^{-2}$
7 dB	5.012	0.0192	0.0565	$5.30 \cdot 10^{-3}$
8 dB	6.310	≈ 0.01	≈ 0.03	$8.63 \cdot 10^{-4}$
9.32 dB	8.568	0.0033	≈ 0.01	$3.40 \cdot 10^{-5}$
10 dB	10.000	0.0017	≈ 0.005	$4.29 \cdot 10^{-6}$
11.3 dB	13.487	0.0003	≈ 0.001	$3.49 \cdot 10^{-8}$
12 dB	15.849	0.00012	0.00035	$1.63 \cdot 10^{-9}$



Die Grafik zeigt den Verlauf der Blockfehlerwahrscheinlichkeit in Abhängigkeit von $10 \cdot \lg\, E_B/N_0$ sowie die vollständig ausgefüllte Ergebnistabelle. Man erkennt das deutlich ungünstigere (asymptotische) Verhalten dieses kurzen (grünen) Codes RSC $(7, 5, 3)_8$ gegenüber dem (roten) Vergleichscode RSC $(255, 223, 33)_8$.

Für Abszissenwerte kleiner als 10 dB ergibt sich sogar ein schlechteres Ergebnis als ohne Codierung. Deshalb soll hier nochmals darauf hingewiesen werden, dass dieser RSC $(7, 3, 5)_8$ wenig praktische Bedeutung hat. Er wurde für diese Aufgabe nur deshalb ausgewählt, um mit vertretbarem Aufwand die Berechnung der BDD–Blockfehlerwahrscheinlichkeit demonstrieren zu können.

Musterlösung zur Zusatzaufgabe Z2.15

a) Für den RSC $(7, 3, 5)_8$ ergibt sich wegen $d_{\rm min} = 5 \Rightarrow t = 2$ für die Blockfehlerwahrscheinlichkeit:

$$\begin{aligned}{\rm Pr(Blockfehler)} &= \sum_{f=3}^{7} \binom{7}{f} \cdot \varepsilon_{\rm S}{}^f \cdot (1-\varepsilon_{\rm S})^{7-f} = \\ &= \binom{7}{3} \cdot 0.1^3 \cdot 0.9^4 + \binom{7}{4} \cdot 0.1^4 \cdot 0.9^3 + \binom{7}{5} \cdot 0.1^5 \cdot 0.9^2 + \\ &+ \binom{7}{6} \cdot 0.1^6 \cdot 0.9 + \binom{7}{7} \cdot 0.1^7 .\end{aligned}$$

Nach dieser Berechnung müssten fünf Terme berücksichtigt werden. Da aber auch

$${\rm Pr(Blockfehler)} = \sum_{f=0}^{n} \binom{n}{f} \cdot \varepsilon_{\rm S}{}^f \cdot (1-\varepsilon_{\rm S})^{n-f} = 1$$

gilt, kommt man über den nachfolgenden Rechenweg schneller zum Erfolg:

$$\begin{aligned}{\rm Pr(Blockfehler)} &= 1 - \left[\binom{7}{0} \cdot 0.9^7 + \binom{7}{1} \cdot 0.1 \cdot 0.9^6 + \binom{7}{2} \cdot 0.1^2 \cdot 0.9^5\right] = \\ &= 1 - \left[0.4783 + 0.3720 + 0.1240\right] \underline{= 0.0257}.\end{aligned}$$

b) Analog zur Teilaufgabe erhält man hier:

$$\begin{aligned}{\rm Pr(Blockfehler)} &= 1 - \left[0.99^7 + 7 \cdot 0.01 \cdot 0.99^6 + 21 \cdot 0.01^2 \cdot 0.99^5\right] = \\ &= 1 - \left[0.9321 + 0.0659 + 0.0020\right] \approx 0.\end{aligned}$$

Das bedeutet: Für die Wahrscheinlichkeit $\varepsilon_{\rm S} = 0.01$ ist die vereinfachte Rechnung sehr fehleranfällig, weil sich für den Klammerausdruck ein Wert nahezu 1 ergibt. Die vollständige Rechnung ergibt hier:

$$\begin{aligned}{\rm Pr(Blockfehler)} &= \binom{7}{3} \cdot 0.01^3 \cdot 0.99^4 + \binom{7}{4} \cdot 0.01^4 \cdot 0.99^3 + \binom{7}{5} \cdot 0.01^5 \cdot 0.99^2 + \\ &= \binom{7}{6} \cdot 0.01^6 \cdot 0.99 + \binom{7}{7} \cdot 0.01^7 = \\ &= 10^{-6} \cdot \left[33.6209 + 0.3396 + 0.0021 + \ldots\right] \underline{\approx 3.396 \cdot 10^{-5}}.\end{aligned}$$

c) Aus der Musterlösung zur Teilaufgabe (b) kann das Ergebnis direkt abgelesen werden:

$${\rm Pr(Blockfehler)} \underline{\approx 3.362 \cdot 10^{-5}}.$$

Der relative Fehler beträgt ca. –1%. Das Minuszeichen zeigt an, dass es sich hier nur um eine Näherung handelt und nicht um eine Schranke: Der Näherungswert ist etwas kleiner als der tatsächliche Wert.

d) Beschränkt man sich auf den relevanten Term ($f = 3$), so ergibt sich für $\varepsilon_{\rm S} = 0.001$:

$${\rm Pr(Blockfehler)} \approx \binom{7}{3} \cdot \left[10^{-3}\right]^3 \cdot 0.999^4 \underline{\approx 3.49 \cdot 10^{-8}}.$$

Der relative Fehler beträgt hier nur noch etwa –0.1%.

e) Entsprechend der hergeleiteten Näherung gilt für den betrachteten Code:

$$\Pr(\text{Blockfehler}) \approx \binom{7}{3} \cdot {\varepsilon_\text{S}}^3 = 35 \cdot {\varepsilon_\text{S}}^3$$

$$\Rightarrow \quad \Pr(\text{Blockfehler}) = 10^{-10}: \quad \varepsilon_\text{S} = \left(\frac{10^{-10}}{35}\right)^{1/3} = 2.857^{1/3} \cdot 10^{-4} \ \underline{\approx 1.42 \cdot 10^{-4}}.$$

Musterlösung zur Aufgabe A2.16

a) Das Codierraumschema **A** beschreibt einen perfekten Code. Da jeder Hamming–Code $(n, k, 3)$ ein perfekter Code ist, gilt Antwort 1. Bei diesen gibt es insgesamt 2^n mögliche Empfangsworte $\underline{y}_i$, die bei der Syndromdecodierung einem von 2^k möglichen Codeworten $\underline{c}_j$ zugeordnet werden.

Aufgrund der HC–Eigenschaft $d_{\rm min} = 3$ haben alle Kugeln im n–dimensionalen Raum den Radius $t = 1$.

In allen Kugeln gibt es somit 2^{n-k} Punkte, zum Beispiel

- **HC (7, 4, 3)**: Einen Punkt für die fehlerfreie Übertragung und sieben Punkte für einen Bitfehler ⇒ $1 + 7 = 8 = 2^3 = 2^{7-4}$.
- **HC (15, 11, 3)**: Auch hier wieder einen Punkt für die fehlerfreie Übertragung und nun 15 Punkte für einen Bitfehler ⇒ $1 + 15 = 16 = 2^4 = 2^{15-11}$.

Hinweis: Da der Hamming–Code ein Binärcode ist, hat hier der Coderaum die Dimension n.

b) Richtig ist Antwort 1. Im grauen Bereich außerhalb von „Kugeln" gibt es bei einem perfekten Code keinen einzigen Punkt, wie die Rechnung zur Teilaufgabe (a) gezeigt hat.

c) Die Reed–Solomon–Codes werden durch das Codierraumschema **B** beschrieben ⇒ Antwort 2. Hier gibt es zahlreiche gelbe Punkte im grauen Bereich, also Punkte, die bei *Bounded Distance Decoding* (BDD) keiner Kugel zugeordnet werden können.

Betrachten wir beispielsweise den RSC $(7, 3, 5)_8$ mit den Codeparametern $n = 7$, $k = 3$ und $t = 2$, so gibt es hier insgesamt $8^7 = 2097152$ Punkte und $8^3 = 512$ Hyperkugeln. Wäre dieser Code perfekt, so müsste es also innerhalb jeder Kugel $8^4 = 4096$ Punkte geben. Es gilt aber:

$$\Pr(\underline{y}_i \text{ liegt innerhalb der roten Kugel}) = \Pr(f \le t) =$$
$$= \Pr(f = 0) + \Pr(f = 1) + \Pr(f = 2) = 1 + \binom{7}{1} \cdot 7 + \binom{7}{2} \cdot 7^2 = 1079\,.$$

Für $\Pr(f = 1)$ ist berücksichtigt, dass es „7 über 1" = 7 Fehlerpositionen geben kann, und für jede Fehlerposition auch 7 unterschiedliche Fehlerwerte. Entsprechendes ist auch für $\Pr(f = 2)$ berücksichtigt.

d) Richtig ist hier die Antwort 3. Ein Punkt im grauen Niemandsland wird mit weniger Symbolfehlern erreicht als ein Punkt in einer anderen Hyperkugel. Für lange Codes wird in der Literatur eine obere Schranke für die Verfälschungswahrscheinlichkeit angegeben:

$$\Pr(\underline{y}_i \text{ wird falsch decodiert}) = \Pr(\underline{z} \ne \underline{c}) \le \frac{1}{t!}\,.$$

Für den RSC $(225, 223, 33)_{256}$ ⇒ $t = 16$ liefert diese obere Schranke den Wert $1/(16\,!) < 10^{-14}$.