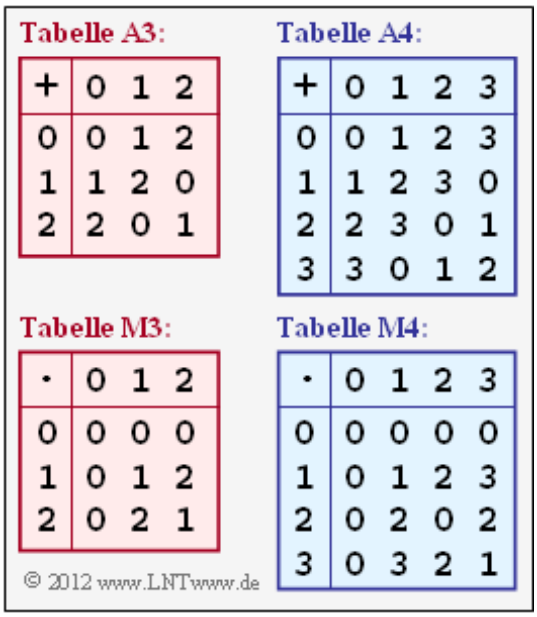
A2.1: Gruppe, Ring, Körper



Im Theorieteil zu diesem Kapitel 2.1 wurden verschiedene algebraische Begriffe definiert. Für das Folgende setzen wir voraus, dass alle Mengen aus jeweils q Elementen bestehen, wobei hier entweder $q = 3$ oder $q = 4$ gelten soll. Dann gilt:

- Eine **algebraische Gruppe** ist eine endliche Menge $G = \{0, 1, \text{...} , q–1\}$ zusammen mit einer zwischen allen Elementen definierten Verknüpfungsvorschrift. Eine additive Gruppe wird mit $(G, +)$ bezeichnet, eine multiplikative mit $(G, \cdot)$.
- Ein **algebraischer Ring** kennzeichnet eine Menge $R = \{0, 1, \text{...} , q–1\}$ zusammen mit zwei darin definierten Rechenoperationen, nämlich der Addition („+") und der Multiplikation („·").
- Ein **algebraischer Körper** ist ein Ring, bei dem zusätzlich die Division erlaubt ist und stets das Kommutativgesetz erfüllt wird.

Da wir hier ausschließlich endliche Mengen betrachten, ist ein Körper (englisch: *Field*) gleichzeitig ein Galoisfeld GF(q) der Ordnung q.

Eine wesentliche Eigenschaft des Galoisfeldes

$$\mathrm{GF}(q) = \{ z_0, z_1, \text{...}, z_{q-1} \}$$

ist, dass es mindestens ein primitives Element besitzt. Ein Element $z_i \neq 0$ bezeichnet man als primitiv, wenn die folgende Bedingung erfüllt ist (k ganzzahlig).

$$z_i^k \bmod q = \begin{cases} \neq 1 & \text{für } 1 \le k < q-1 \\ 1 & \text{für } k = q-1 \end{cases} \quad \Rightarrow \quad z_i \text{ ist ein primitives Element.}$$

Nur bei einem primitiven Element z_i ergeben sich durch die Rechenoperation z_i^k (mit $k = 1, 2, 3, \text{...}$) alle Elemente des Galoisfeldes mit Ausnahme des Nullelementes $z_0 = 0$.

Hinweis: Die Aufgabe behandelt das Themengebiet von **Kapitel 2.1.** Beachten Sie, dass bei Gruppe, Ring und Körper mit jeweils q Elementen die Rechenoperationen „+" und „·" jeweils modulo q zu verstehen sind.

Fragebogen zu "A2.1: Gruppe, Ring, Körper"

a) Welche der angegebenen Tabellen beschreiben eine Gruppe?

- ☐ Tabelle A3,
- ☐ Tabelle M3,
- ☐ Tabelle A3 und Tabelle M3 gemeinsam,
- ☐ Tabelle A4 und Tabelle M4 gemeinsam.

b) Welche der angegebenen Tabellen beschreiben einen Ring?

- ☐ Tabelle A3,
- ☐ Tabelle M3,
- ☐ Tabelle A3 und Tabelle M3 gemeinsam,
- ☐ Tabelle A4 und Tabelle M4 gemeinsam,
- ☐ Tabelle A3 und Tabelle M4 gemeinsam.

c) Welche der Tabellen beschreiben einen Körper bzw. ein Galoisfeld?

- ☐ Tabelle A3,
- ☐ Tabelle M3,
- ☐ Tabelle A3 und Tabelle M3 gemeinsam,
- ☐ Tabelle A4 und Tabelle M4 gemeinsam.

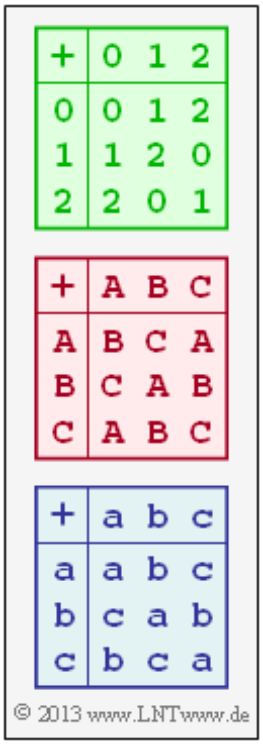
d) Welche Elemente der Menge $\{0, 1, 2\} \Rightarrow q = 3$ sind primitiv?

- ☐ $z_0 = 0$,
- ☐ $z_1 = 1$,
- ☐ $z_2 = 2$.

e) Welche Elemente der Menge $\{0, 1, 2, 3\} \Rightarrow q = 4$ sind primitiv?

- ☐ $z_0 = 0$,
- ☐ $z_1 = 1$,
- ☐ $z_2 = 2$,
- ☐ $z_3 = 3$.

Z2.1: Welche Tabellen beschreiben Gruppen?



In dieser Aufgabe betrachten wir Mengen mit jeweils drei Elementen, allgemein bezeichnet mit $\{z_0, z_1, z_2\}$. Die Elemente können dabei sein:

- Zahlen, beispielsweise $z_0 = 0$, $z_1 = 1$, $z_2 = 2$,
- algebraische Ausdrücke wie $z_0 = A$, $z_1 = B$, $z_2 = C$,
- irgendwas, beispielsweise z_0 = „Apfel”, z_1 = „Birne”, z_2 = „Citrone”.

Eine Gruppe (G, „+”) hinsichtlich der Addition ergibt sich dann, wenn durch eine Tabelle die „+”–Verknüpfung zwischen je zwei Elementen so definiert wurde, dass folgende Bedingungen erfüllt sind (die Laufvariablen i, j, k können dabei jeweils die Werte 0, 1, 2 annehmen):

- Für alle $z_i \in G$ und $z_j \in G$ gilt $(z_i + z_j) \in G$ $\Rightarrow$ **Closure–Kriterium**. Die Bedingung muss auch für $i = j$ erfüllt sein.
- Für alle z_i, z_j, z_k gilt $(z_i + z_j) + z_k = z_i + (z_j + z_k)$ $\Rightarrow$ **Assoziativgesetz**.
- Es gibt ein **hinsichtlich Addition neutrales Element** $N_{\rm A} \in G$, so dass für alle $z_i \in G$ gilt: $z_i + N_{\rm A} = z_i$.
- Für alle $z_i \in G$ gibt es ein **hinsichtlich Addition inverses Element** $\text{Inv}_{\rm A}(z_i) \in G$, so dass für die Summe $z_i + \text{Inv}_{\rm A}(z_i) = N_{\rm A}$ gilt.

Wird zudem für alle $z_i \in G$ und $z_j \in G$ zusätzlich noch das **Kommutativgesetz** $\Rightarrow$ $z_i + z_j = z_j + z_i$ erfüllt, so spricht man von einer kommutativen Gruppe oder – nach dem norwegischen Mathematiker **Niels Hendrik Abel** – von einer **abelschen Gruppe**.

Die Zahlenmenge {0, 1, 2} ist eine abelsche (kommutative) Gruppe. Entsprechend der grün umrandeten Additionstabelle in obiger Grafik ist hier die Addition modulo 3 zu verstehen. Somit ist auch die Summe stets 0, 1 oder 2. Das neutrale Element ist $N_{\rm A} = 0$ und das zu z_i inverse Element $\text{Inv}_{\rm A}(z_i) = -z_i$:

$$\text{Inv}_{\rm A}(0) = 0,\ \text{Inv}_{\rm A}(1) = (-1)\ \text{mod}\ 3 = 2,\ \text{Inv}_{\rm A}(2) = (-2)\ \text{mod}\ 3 = 1\,.$$

In dieser Aufgabe sollen Sie überprüfen, ob auch die beiden weiteren in der obigen Grafik dargestellten Additionstabellen jeweils zu einer algebraischen Gruppe gehören.

Hinweis: Die Aufgabe bezieht sich auf die Seite **Algebraische Gruppe und Beispiele** im **Kapitel 2.1.**

Fragebogen zu "Z2.1: Welche Tabellen beschreiben Gruppen?"

a) Welche Aussagen ergeben sich aus der rot umrandeten Additionstabelle?

- ☐ Das neutrale Element ist N_A = C.
- ☐ Die Inversen sind $\text{Inv}_A(A) = B$, $\text{Inv}_A(B) = A$, $\text{Inv}_A(C) = C$.
- ☐ Es handelt sich hier um eine additive Gruppe $(G, +)$.
- ☐ Auch die Bedingung einer abelschen Gruppe wird erfüllt.

b) Ändert sich etwas gegenüber Teilaufgabe a), wenn die Elemente A, B, C nun für „Apfel", „Birne" und „Citrone" stehen?

- ○ Ja.
- ○ Nein.

c) Welche Aussagen ergeben sich aus der blau umrandeten Additionstabelle?

- ☐ Das neutrale Element ist N_A = a.
- ☐ Die additiven Inversen sind $\text{Inv}_A(a) = a$, $\text{Inv}_A(b) = b$, $\text{Inv}_A(c) = c$.
- ☐ Es handelt sich um eine abelsche Gruppe.

A2.2: Eigenschaften von Galoisfeldern

Wir betrachten hier die Zahlenmengen

- $Z_5 = \{0, 1, 2, 3, 4\} \Rightarrow q = 5$,
- $Z_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow q = 6$.

In nebenstehender Grafik sind die (teilweise unvollständigen) Additions– und Multiplikationstabellen für $q = 5$ und für $q = 6$ angegeben, wobei sowohl die Addition („+") als auch die Multiplikation („·") modulo q zu verstehen sind.

Zu überprüfen ist, ob die Zahlenmengen Z_5 und Z_6 alle Bedingungen eines Galoisfeldes GF(5) bzw. GF(6) erfüllen. Im **Theorieteil** werden insgesamt acht Bedingungen genannt, die alle erfüllt sein müssen. Von ihnen überprüft werden sollen nur zwei dieser Bedingungen:

(D) Für alle Elemente gibt es eine **additive Inverse** (*Inverse for* „+"):

$$\forall\ z_i \in \mathrm{GF}(q),\ \exists\ \mathrm{Inv_A}(z_i) \in \mathrm{GF}(q):$$
$$z_i + \mathrm{Inv_A}(z_i) = 0 \quad \Rightarrow \quad \mathrm{Inv_A}(z_i) = -z_i.$$

(E) Alle Elemente haben eine **multiplikative Inverse** (*Inverse for* „·"):

$$\forall\ z_i \in \mathrm{GF}(q),\ z_i \neq 0,\ \exists\ \mathrm{Inv_M}(z_i) \in \mathrm{GF}(q):$$
$$z_i \cdot \mathrm{Inv_M}(z_i) = 1 \quad \Rightarrow \quad \mathrm{Inv_M}(z_i) = z_i^{-1}.$$

Die weiteren Bedingungen für ein Galoisfeld, nämlich

- Closure,
- Existenz von Null– und Einselement,
- Gültigkeit von Kommutativ–, Assoziativ– und Distributivgesetz

werden sowohl von Z_5 als auch von Z_6 erfüllt.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.1.**

Operationen für $q = 5$:

+	0	1	2	3	4
0	0	1	2	3	A_{04}
1	1	2	3	4	A_{14}
2	2	3	4	0	A_{24}
3	3	4	0	1	A_{34}
4	4	0	1	2	A_{44}

·	0	1	2	3	4
0	0	0	0	0	M_{04}
1	0	1	2	3	M_{14}
2	0	2	4	1	M_{24}
3	0	3	1	4	M_{34}
4	0	4	3	2	M_{44}

Operationen für $q = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	0	1
2	2	3	4	0	1	2
3	3	4	0	1	2	3
4	4	0	1	2	3	4
5	5	4	0	1	2	3

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Fragebogen zu "A2.2: Eigenschaften von Galoisfeldern"

a) Ergänzen Sie die Additionstabelle für $q = 5$. Geben Sie folgende Werte ein:

$$A_{04} =$$

$$A_{14} =$$

$$A_{44} =$$

b) Ergänzen Sie die Multiplikationstabelle für $q = 5$. Geben Sie folgende Werte ein:

$$M_{04} =$$

$$M_{14} =$$

$$M_{44} =$$

c) Erfüllt die Menge Z_5 die Bedingungen eines Galoisfeldes?

- ☐ Ja.
- ☐ Nein, es gibt nicht für alle Elemente (0 – 4) eine additive Inverse.
- ☐ Nein, die Elemente 1–4 haben nicht alle eine multiplikative Inverse.

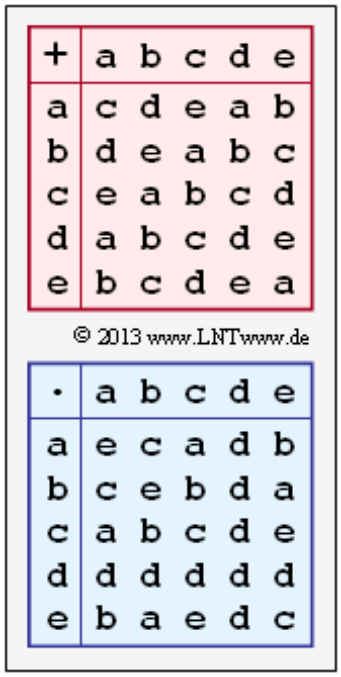
d) Erfüllt die Menge Z_6 die Bedingungen eines Galoisfeldes?

- ☐ Ja.
- ☐ Nein, es gibt nicht für alle Elemente (0 – 5) eine additive Inverse.
- ☐ Nein, die Elemente 1–5 haben nicht alle eine multiplikative Inverse.

e) Die Zahlenmengen Z_2, Z_3, Z_5 und Z_7 ergeben ein Galoisfeld, die Mengen Z_4, Z_6, Z_8, Z_9 dagegen nicht. Was folgern Sie daraus?

- ☐ $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ist ein Galoisfeld?
- ☐ $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ ist ein Galoisfeld?
- ☐ $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ ist ein Galoisfeld?

Z2.2: Galoisfeld GF(5)



+	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

·	a	b	c	d	e
a	e	c	a	d	b
b	c	e	b	d	a
c	a	b	c	d	e
d	d	d	d	d	d
e	b	a	e	d	c

Wie in **Aufgabe A2.2** betrachten wir einen endlichen Körper der Ordnung $q = 5$ und damit das Galoisfeld

$$\mathrm{GF}(5) = \{a, b, c, d, e\}.$$

Über die Elemente werden weiter keine Aussagen getroffen. Es können sowohl ganze Zahlen sein oder irgendwelche mathematische Ausdrücke. Das Galoisfeld wird ausschließlich bestimmt durch

- eine Additionstabelle modulo 5,
- eine Multiplikationstabelle modulo 5.

Die wichtigsten Eigenschaften eines Galoisfeldes sind auf **Theorieseite 1** zusammengestellt. In dieser Aufgabe wird Bezug genommen auf

- das Kommutativ– und das Distributivgesetz,
- die neutralen Elemente von Addition und Multiplikation,
- die inversen Elemente von Addition und Multiplikation, sowie
- die Bestimmung primitiver Elemente.

Im vorliegenden Beispiel wäre β ein primitives Element, wenn β^2, β^3 und β^4 (allgemein: β^{q-1}) die übrigen Elemente des Galoisfeldes GF(5) mit Ausnahme des Nullelementes ergeben.

Hinweis: Die Aufgabe bezieht sich auf das Themengebiet von **Kapitel 2.1.**

Fragebogen zu "Z2.2: Galoisfeld GF(5)"

a) Bestimmen Sie das neutrale Element der Addition.

- ☐ $N_A = a$,
- ☐ $N_A = b$,
- ☐ $N_A = c$,
- ☐ $N_A = d$,
- ☐ $N_A = e$.

b) Bestimmen Sie das neutrale Element der Multiplikation.

- ☐ $N_M = a$,
- ☐ $N_M = b$,
- ☐ $N_M = c$,
- ☐ $N_M = d$,
- ☐ $N_M = e$.

c) Ist das Kommutativgesetz erfüllt,

- ☐ hinsichtlich Addition, z.B. $a + b = b + a$, ... , $d + e = e + d$,
- ☐ hinsichtlich Multiplikation, z.B. $a \cdot b = b \cdot a$, ... , $d \cdot e = e \cdot d$.

d) Für welche Ausdrücke ist das Distributivgesetz erfüllt?

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

e) Ersetzen Sie a, b, c, d, e durch Elemente der Zahlenmenge {0, 1, 2, 3, 4}, so dass sich gleiche Operationstabellen ergeben.

$\boldsymbol{a}$ =

$\boldsymbol{b}$ =

$\boldsymbol{c}$ =

$\boldsymbol{d}$ =

$\boldsymbol{e}$ =

f) Welche Aussagen gelten hinsichtlich der inversen Elemente?

- ☐ Für alle $z_i \in \{0, 1, 2, 3, 4\}$ gibt es eine additive Inverse.
- ☐ Nur für $z_i \in \{1, 2, 3, 4\}$ gibt es eine additive Inverse.
- ☐ Für alle $z_i \in \{0, 1, 2, 3, 4\}$ gibt es eine multiplikative Inverse.
- ☐ Nur für $z_i \in \{1, 2, 3, 4\}$ gibt es eine multiplikative Inverse.

g) Welche der Elemente sind primitiv?

- ☐ $a = 3$,
- ☐ $b = 2$,
- ☐ $e = 4$.

A2.3: Reduzible und irreduzible Polynome

$m = 2$	$a_1(x) = x^2 + x$ $a_2(x) = x^2 + 1$
$m = 3$	$a_3(x) = x^3$ $a_4(x) = x^3 + 1$ $a_5(x) = x^3 + x$ $a_6(x) = x^3 + x + 1$ $a_7(x) = x^3 + x^2 + 1$
$m = 4$	$a_8(x) = x^4 + 1$ $a_9(x) = x^4 + x^3 + 1$ $a_{10}(x) = x^4 + x^2 + 1$

Wichtige Voraussetzungen für das Verständnis der Kanalcodierung sind Kenntnisse der Polynomeigenschaften. Wir betrachten in dieser Aufgabe Polynome der Form

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

wobei für die Koeffizienten $a_i \in \text{GF}(2) = \{0, 1\}$ gilt $(0 \le i < m)$ und der höchste Koeffizient stets zu $a_m = 1$ vorausgesetzt wird. Man bezeichnet m als den Grad des Polynoms. Nebenstehend sind zehn Polynome angegeben, wobei der Polynomgrad entweder $m = 2$ (rote Schrift), $m = 3$ (blaue Schrift) oder $m = 4$ (grüne Schrift) ist.

Ein Polynom $a(x)$ bezeichnet man als **reduzibel**, wenn es als Produkt zweier Polynome $p(x)$ und $q(x)$ mit jeweils niedrigerem Grad dargestellt werden kann:

$$a(x) = p(x) \cdot q(x)$$

Ist dies nicht möglich, das heißt, wenn für das Polynom

$$a(x) = p(x) \cdot q(x) + r(x)$$

mit einem Restpolynom $r(x) \neq 0$ gilt, so nennt man das Polynom als **irreduzibel**. Solche irreduziblen Polynome sind für die Beschreibung von Fehlerkorrekturverfahren von besonderer Bedeutung.

Der Nachweis, dass ein Polynom $a(x)$ vom Grad m irreduzibel ist, erfordert mehrere Polynomdivisionen $a(x)/q(x)$, wobei der Grad des jeweiligen Divisorpolynoms $q(x)$ stets kleiner ist als m. Nur wenn alle diese Modulo–2–Divisionen stets einen Rest $r(x) \neq 0$ liefern, ist nachgewiesen, dass $a(x)$ ein irreduzibles Polynom beschreibt.

Dieser exakte Nachweis ist sehr aufwändig. Notwendige Voraussetzungen dafür, dass $a(x)$ überhaupt ein irreduzibles Polynom sein könnte, sind die beiden Bedingungen (bei nichtbinärer Betrachtungsweise wäre „= 1" durch „≠ 0" zu ersetzen):

- $a(x = 0) = 1$,
- $a(x = 1) = 1$.

Ansonsten könnte man für das zu untersuchende Polynom schreiben:

$$a(x) = q(x) \cdot x \quad \text{bzw.} \quad a(x) = q(x) \cdot (x + 1) \,.$$

Die oben genannten Voraussetzungen sind zwar notwendig, jedoch nicht hinreichend, wie das folgende Beispiel zeigt:

$$a(x) = x^5 + x^4 + 1 \quad \Rightarrow \quad a(x = 0) = 1 \,, \ \ a(x = 1) = 1 \,.$$

Trotzdem ist dieses Polynom reduzibel:

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

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 2.2.**

Fragebogen zu "A2.3: Reduzible und irreduzible Polynome"

a) Wieviele Polynomdivisionen (N_D) sind erforderlich, um exakt nachzuweisen, dass ein GF(2)–Polynom $a(x)$ vom Grad m irreduzibel ist?

$$\boldsymbol{m = 2}\text{: } \boldsymbol{N_D} =$$

$$\boldsymbol{m = 3}\text{: } \boldsymbol{N_D} =$$

$$\boldsymbol{m = 4}\text{: } \boldsymbol{N_D} =$$

b) Welche der Grad–2–Polynome sind irreduzibel?

- ☐ $a_1(x) = x^2 + x$,
- ☐ $a_2(x) = x^2 + x + 1$.

c) Welche der Grad–3–Polynome sind irreduzibel?

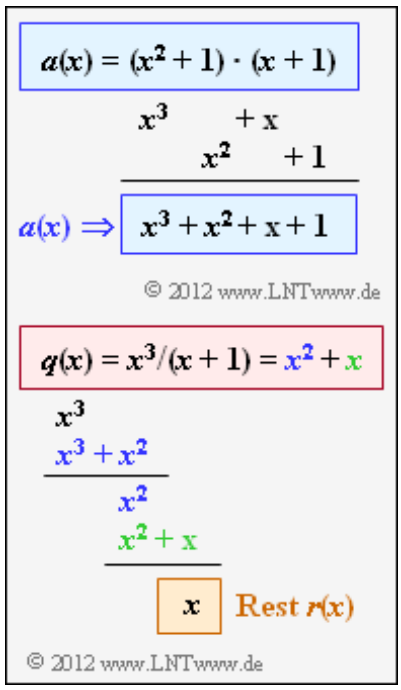
- ☐ $a_3(x) = x^3$,
- ☐ $a_4(x) = x^3 + 1$,
- ☐ $a_5(x) = x^3 + x$,
- ☐ $a_6(x) = x^3 + x + 1$,
- ☐ $a_7(x) = x^3 + x^2 + 1$.

d) Welche der Grad–4–Polynome sind irreduzibel?

- ☐ $a_8(x) = x^4 + 1$,
- ☐ $a_9(x) = x^4 + x^3 + 1$,
- ☐ $a_{10}(x) = x^4 + x^2 + 1$.

Z2.3: Polynomdivision

In dieser Aufgabe beschäftigen wir uns mit der Multiplikation und insbesondere der Division von Polynomen im Galoisfeld GF(2). In der Abbildung ist jeweils die Vorgehensweise an einem einfachen und selbsterklärenden Beispiel verdeutlicht:



- Die Multiplikation der beiden Polynome $x^2 + 1$ und $x + 1$ liefert das Ergebnis $a(x) = x^3 + x^2 + x + 1$.
- Die Division des Polynoms $a(x) = x^3$ durch $p(x) = x + 1$ liefert den Quotienten $q(x) = x^2 + x$ und den Rest $r(x) = x$.
- Man kann das letztere Ergebnis wie folgt überprüfen:

$$\begin{aligned} a(x) &= p(x) \cdot q(x) + r(x) = \\ &= [(x+1) \cdot (x^2 + x)] + x = \\ &= [x^3 + x^2 + x^2 + x] + x = x^3 . \end{aligned}$$

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 2.2.**

Fragebogen zu "Z2.3: Polynomdivision"

a) Welches Ergebnis liefert $a(x) = (x^3 + x + 1) \cdot (x^2 + 1)$?

- ☐ $a(x) = x^5 + x^3 + x^2 + 1$,
- ☐ $a(x) = x^5 + x^2 + x + 1$,
- ☐ $a(x) = x^6 + x^3 + x^2 + 1$.

b) Welche der Polynomdivisionen ergeben keinen Rest $r(x)$?

- ☐ $(x^5 + x^2 + x + 1)/(x^3 + x + 1)$,
- ☐ $(x^5 + x^2 + x + 1)/(x^2 + 1)$,
- ☐ $(x^5 + x^2 + x + 1)/(x^2)$,
- ☐ $(x^5 + x^2 + x)/(x^2 + 1)$.

c) Es sei $a(x) = x^6 + x^5 + 1$ und $p(x) = x^3 + x^2 + 1$. Bestimmen Sie $q(x)$ und $r(x)$ entsprechend der Beschreibungsgleichung $a(x) = p(x) \cdot q(x) + r(x)$.

- ☐ $q(x) = x^3 + x^2 + 1, \quad r(x) = 0$,
- ☐ $q(x) = x^3 + 1, \quad r(x) = 0$,
- ☐ $q(x) = x^3 + 1, \quad r(x) = x^2$.

A2.4: GF(2^2)–Darstellungsformen

Nebenstehend sehen Sie für den Erweiterungskörper GF(2^2) die Additions– sowie die Multiplikationstabelle in drei verschiedenen Varianten:

- die *Polynomdarstellung*,
- die *Koeffizientenvektordarstellung*,
- die *Exponentendarstelluung*.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.2.**

Alle notwendigen Informationen zu GF(2^2) finden Sie auf der **Seite 1** dieses Kapitels.

(A) Polynomdarstellung: $k_1 \cdot \alpha + k_0$

+	z_0 = 0	z_1 = 1	z_2 = α	z_3 = 1+α
0	0	1	α	1+α
1	1	0	1+α	α
α	α	1+α	0	1
1+α	1+α	α	1	0

·	z_0 = 0	z_1 = 1	z_2 = α	z_3 = 1+α
0	0	0	0	0
1	0	1	α	1+α
α	0	α	1+α	1
1+α	0	1+α	1	α

(B) Koeffizientenvektordarstellung:

+	z_0 = 00	z_1 = 01	z_2 = 10	z_3 = 11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

·	z_0 = 00	z_1 = 01	z_2 = 10	z_3 = 11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

(C) Exponentendarstellung: 0, α^i $(0 \le i \le 2)$

+	z_0 = 0	z_1 = α^0	z_2 = α^1	z_3 = α^2
0	0	α^0	α^1	α^2
α^0	α^0	0	α^2	α^1
α^1	α^1	α^2	0	α^0
α^2	α^2	α^1	α^0	0

·	z_0 = 0	z_1 = α^0	z_2 = α^1	z_3 = α^2
0	0	0	0	0
α^0	0	α^0	α^1	α^2
α^1	0	α^1	α^2	α^0
α^2	0	α^2	α^0	α^1

Fragebogen zu "A2.4: GF(2^2)–Darstellungsformen "

a) Welche Charakteristika erkennt man aus der Polynomdarstellung?

- ☐ Die Elemente α und $1+\alpha$ sind weder 0 noch 1.
- ☐ Die Rechenoperationen erfolgen modulo 2.
- ☐ Die Rechenoperationen erfolgen modulo 4.
- ☐ Man erkennt „$\alpha^2 + \alpha + 1 = 0$” aus der Additionstabelle.
- ☐ Man erkennt „$\alpha^2 + \alpha + 1 = 0$” aus der Multiplikationstabelle.

b) Welcher Zusammenhang besteht zwischen der Koeffizientenvektor– und der Polynomdarstellung? Es gelte $k_0 \in \{0, 1\}$ und $k_1 \in \{0, 1\}$.

- ☐ $(k_0\ k_1)$ bezieht sich auf das Element $k_1 \cdot \alpha + k_0$.
- ☐ $(k_1\ k_0)$ bezieht sich auf das Element $k_1 \cdot \alpha + k_0$.
- ☐ Zwischen beiden Darstellungen besteht keinerlei Zusammenhang.

c) Wie hängen Polynom– und Exponentendarstellung zusammen?

- ☐ Es sind keine Zusammenhänge erkennbar.
- ☐ Die Elemente 0, 1 und α sind in beiden Darstellungen gleich.
- ☐ Das Element $1+\alpha$ lautet in der Exponentendarstellung α^2.
- ☐ Das Element α^2 der Exponentendarstellung steht für $\alpha \cdot (1+\alpha)$.

d) Berechnen Sie die Ausdrücke A und B nach diesen drei Darstellungsformen. Welche Aussagen treffen zu?

- ☐ Es gilt $A = z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = z_0$,
- ☐ Es gilt $B = (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = z_1$,
- ☐ Es gilt $A = z_2 \cdot z_2 + z_2 \cdot z_3 + z_3 \cdot z_3 = z_2$,
- ☐ Es gilt $B = (z_0 + z_1 + z_2) \cdot (z_0 + z_1 + z_3) = z_3$.

Z2.4: Endliche und unendliche Körper

In der Mathematik unterscheidet man verschiedene Zahlenmengen:

- die Menge der natürlichen Zahlen: $N = \{0, 1, 2, ...\}$,
- die Menge der ganzen Zahlen: $Z = \{..., –1, 0, +1, ...\}$,
- die Menge der rationalen Zahlen: $Q = \{m/n\}$ mit $m \in Z$, $n \in Z \setminus \{0\}$,
- die Menge R der reellen Zahlen,
- die Menge der komplexen Zahlen: $C = \{a + \text{j} \cdot b\}$ mit $a \in R$, $b \in R$ und der imaginären Einheit j.

Eine solche Menge (englisch: *Set*) bezeichnet man dann (und nur dann) als einen **Körper** (englisch: *Field*) im algebraischen Sinne, wenn in ihr die vier Rechenoperationen Addition, Subtraktion, Multiplikation und Division erlaubt und die Ergebnisse im gleichen Körper darstellbar sind. Einige diesbezügliche Definitionen finden Sie im **Theorieteil.** Soviel vorneweg: Nicht alle der oben aufgelisteten Mengen sind Körper.

Daneben gibt es auch noch **endliche Körper** (englisch: *Finite Fields*), die in unserem Lerntutorial als **Galoisfeld** GF(P^m) bezeichnet werden, wobei

- $P \in N$ eine Primzahl angibt,
- und $m \in N$ eine natürliche Zahl bezeichnet.

Ist der Exponent $m \geq 2$, so spricht man von einem **Erweiterungskörper** (englisch: *Extension Field*). In dieser Aufgabe beschränken wir uns auf Erweiterungskörper zur Basis $P = 2$.

Die beiden ersten Teilaufgaben beziehen sich auf die Klassifizierung von Polynomen. Ein Grad–m–Polynom nennt man reduzibel im Körper K, wenn es in der Form

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

darstellbar ist und für alle Nullstellen $x_i \in K$ gilt. Ist dies nicht möglich, so spricht man von einem **irreduziblen Polynom**.

Gerolamo Cardano
(1501 – 1576)

Rafael Bambelli
(1526 – 1572)

Évariste Galois
(1811 – 1832)

Hinweis: Die Aufgabe bezieht sich auf die Thematik von **Kapitel 2.2.** Oben sehen Sie Abbildungen der italienischen Mathematiker **Gerolamo Cardano** sowie **Rafael Bombelli,** die erstmals imaginäre Zahlen zur Lösung algebraischer Gleichungen einführten, sowie von **Évariste Galois,** der schon in sehr jungen Jahren die Grundlagen der endlichen Körper geschaffen hat.

Fragebogen zu "Z2.4: Endliche und unendliche Körper"

a) Welche Polynome sind irreduzibel im reellen Körper?

- ☐ $p_1(x) = x^2 + 1$,
- ☐ $p_2(x) = x^2 - 1$,
- ☐ $p_3(x) = x^2 + x + 1$,
- ☐ $p_4(x) = x^2 + x - 2$.

b) Welche Polynome sind irreduzibel in GF(2)?

- ☐ $p_1(x) = x^2 + 1$,
- ☐ $p_2(x) = x^2 - 1$,
- ☐ $p_3(x) = x^2 + x + 1$,
- ☐ $p_4(x) = x^2 + x - 2$.

c) Bei welchen Mengen handelt es sich im algebraischen Sinne um Körper?

- ☐ die Menge N der natürlichen Zahlen,
- ☐ die Menge Z der ganzen Zahlen,
- ☐ die Menge Q der rationalen Zahlen,
- ☐ die Menge R der reellen Zahlen,
- ☐ die Menge C der komplexen Zahlen.

d) Welche Körper sind Teilmenge (Unterraum) eines anderen Körpers?

- ☐ $Q \subset C$,
- ☐ $C \subset R$,
- ☐ $\text{GF}(2) \subset \text{GF}(2^2)$,
- ☐ $\text{GF}(2^3) \subset \text{GF}(2^2)$.

e) Zwischen welchen Körpern bestehen gewisse Analogien?

- ☐ Menge Q der rationalen Zahlen und $\text{GF}(2^2)$,
- ☐ Menge C der komplexen Zahlen und $\text{GF}(2^2)$,

- Menge C der komplexen Zahlen und GF(2^3).

A2.5: Drei Varianten von GF(2^4)

Irreduzible und primitive Polynome haben große Bedeutung für die Beschreibung von Verfahren zur Fehlerkorrektur. In **[LN97]** findet man zum Beispiel die folgenden irreduziblen Polynome vom Grad $m = 4$:

- $p(x) = x^4 + x + 1$,
- $p(x) = x^4 + x^3 + 1$,
- $p(x) = x^4 + x^3 + x^2 + x + 1$.

Die beiden ersten Polynome sind auch primitiv. Dies erkennt man aus den Potenztabellen, die rechts angegeben sind – die untere Tabelle (B) allerdings nicht ganz vollständig. Aus beiden Tabellen erkennt man, dass alle Potenzen α^i für $1 \le i \le 14$ in der Polynomdarstellung ungleich 1 sind. Erst für $i = 15$ ergibt sich

$$\alpha^{15} = \alpha^0 = 1 \quad \Rightarrow \quad \text{Koeffizientenvektor } 0001\,.$$

Nicht angegeben wird, ob sich die rot hinterlegte Tabelle (A) aus dem Polynom $x^4 + x + 1$ oder aus $x^4 + x^3 + 1$ ergibt. Diese Zuordnungen sollen Sie in den Teilaufgaben (a) und (b) treffen. In der Teilaufgabe (c) sollen Sie zudem die fehlenden Potenzen α^5, α^6, α^7 und α^8 in der Tabelle (B) ergänzen.

Die Teilaufgabe (d) bezieht sich auf das ebenfalls irreduzible Polynom $p(x) = x^4 + x^3 + x^2 + x + 1$. Entsprechend den oben genannten Kriterien sollen Sie entscheiden, ob dieses Polynom primitiv ist oder nicht.

Hinweis: Die Aufgabe gehört ebenfalls zum Themengebiet von **Kapitel 2.2.**

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	????	????
α^6	????	????
α^7	????	????
α^8	????	????
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

Fragebogen zu "A2.5: Drei Varianten von GF(2^4)"

a) Welches Polynom liegt der Tabelle (A) zugrunde?

- $p(x) = x^4 + x + 1$,
- $p(x) = x^4 + x^3 + 1$.

b) Welches Polynom liegt der Tabelle (B) zugrunde?

- $p(x) = x^4 + x + 1$,
- $p(x) = x^4 + x^3 + 1$.

c) Berechnen Sie die in der Tabelle (B) fehlenden Einträge. Welche der folgenden Angaben sind richtig?

- $\alpha^5 = \alpha^3 + \alpha + 1 \Rightarrow$ Koeffizientenvektor „1011”,
- $\alpha^6 = \alpha^2 + 1 \Rightarrow$ Koeffizientenvektor „0111”,
- $\alpha^7 = \alpha^3 + \alpha^2 + \alpha + 1 \Rightarrow$ Koeffizientenvektor „1111”,
- $\alpha^8 = \alpha^3 + \alpha^2 + \alpha \Rightarrow$ Koeffizientenvektor „1110”.

d) Ist $p(x) = x^4 + x^3 + x^2 + x + 1$ ein primitives Polynom? Klären Sie diese Frage anhand der Potenzen α^i (i soweit erforderlich).

- Ja.
- Nein.

Z2.5: Einige Berechnungen über GF(2^3)

Elemente von GF(2^3) als		
Potenzen von α	Polynome in α	Vektoren der Koeffizienten
$\alpha^{-\infty}=0$	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
α^7	1	0 0 1

Wir betrachten nun den Erweiterungskörper (englisch: *Extension Field*) mit den acht Elementen ⇒ GF(2^3) entsprechend der nebenstehenden Tabelle. Da das zugrunde liegende Polynom

$$p(x) = x^3 + x + 1$$

sowohl irreduzibel als auch primitiv ist, kann das vorliegende Galoisfeld in folgender Form angegeben werden:

$$\mathrm{GF}(2^3) = \{\, 0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6 \,\}.$$

Das Element α ergibt sich dabei als Lösung der Gleichung $p(\alpha) = 0$ im Galoisfeld GF(2). Damit erhält man folgende Nebenbedingung:

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

Für die weiteren Elemente gelten folgende Berechnungen:

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

In dieser Aufgabe sollen Sie einige algebraische Umformungen in diesem Galoisfeld GF(2^3) vornehmen. Unter anderem ist gefragt nach der multiplikativen Inversen des Elementes α^4. Dann muss gelten:

$$\alpha^4 \cdot \mathrm{Inv_M}(\alpha^4) = 1\,.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.2** und ist als Ergänzung zur etwas schwierigeren **Aufgabe A2.5** gedacht.

Fragebogen zu "Z2.5: Einige Berechnungen über GF(2^3)"

a) Welche der Aussagen treffen für die höheren Potenzen von α zu ($i \geq 7$)?

- ☐ $\alpha^7 = 1$,
- ☐ $\alpha^8 = \alpha$,
- ☐ $\alpha^{13} = \alpha^2 + 1$,
- ☐ $\alpha^i = \alpha^{i \bmod 7}$.

b) Welche Umformung ist für $A = \alpha^8 + \alpha^6 - \alpha^2 + 1$ zulässig?

- ☐ $A = 1$,
- ☐ $A = \alpha$,
- ☐ $A = \alpha^2$,
- ☐ $A = \alpha^3$,
- ☐ $A = \alpha^4$.

c) Welche Umformung ist für $B = \alpha^{16} - \alpha^{12} \cdot \alpha^3$ zulässig?

- ☐ $B = 1$,
- ☐ $B = \alpha$,
- ☐ $B = \alpha^2$,
- ☐ $B = \alpha^3$,
- ☐ $B = \alpha^4$.

d) Welche Umformung ist für $C = \alpha^3 + \alpha$ zulässig?

- ☐ $C = 1$,
- ☐ $C = \alpha$,
- ☐ $C = \alpha^2$,
- ☐ $C = \alpha^3$,
- ☐ $C = \alpha^4$.

e) Welche Umformung ist für $D = \alpha^4 + \alpha$ zulässig?

- ☐ $D = 1$,

- ☐ $D = \alpha$,
- ☐ $D = \alpha^2$,
- ☐ $D = \alpha^3$,
- ☐ $D = \alpha^4$.

f) Welche Umformung ist für $E = A \cdot B \cdot C/D$ zulässig?

- ☐ $E = 1$,
- ☐ $E = \alpha$,
- ☐ $E = \alpha^2$,
- ☐ $E = \alpha^3$,
- ☐ $E = \alpha^4$.

g) Welche Aussagen gelten für die multiplikative Inverse zu $\alpha^2 + \alpha$?

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

A2.6: GF(P^m). Welches P, welches m?

+	z_0 00	z_1 01	z_2 02	z_3 10	z_4 11	z_5 12	z_6 20	z_7 21	z_8 22
00	00	01	02	10	11	12	20	21	22
01	01	02	00	11	12	10	21	22	20
02	02	00	01	12	10	11	22	20	21
10	10	11	12	20	21	22	00	01	02
11	11	12	10	21	22	20	01	02	00
12	12	10	11	22	20	21	02	00	01
20	20	21	22	00	01	02	10	11	12
21	21	22	20	01	02	00	11	12	10
22	22	20	21	02	00	01	12	10	11

·	z_0 00	z_1 01	z_2 02	z_3 10	z_4 11	z_5 12	z_6 20	z_7 21	z_8 22
00	00	00	00	00	00	00	00	00	00
01	00	01	02	10	11	12	20	21	22
02	00	02	01	20	22	21	10	12	11
10	00	10	20	11	21	01	22	02	12
11	00	11	22	21	02	10	12	20	01
12	00	12	21	01	10	22	02	11	20
20	00	20	10	22	12	02	11	01	21
21	00	21	12	02	20	11	01	22	10
22	00	22	11	12	01	20	21	10	02

Es soll ein Galoisfeld GF(q) mit $q = P^m$ Elementen analysiert werden, das durch die nebenstehenden Tabellen für Addition (gekennzeichnet mit „+”) und Multiplikation (gekennzeichnet mit „·”) vorgegeben ist. Dieses Galoisfeld

$$\mathrm{GF}(q) = \{\, z_0,\ z_1,\ \ldots,\ z_{q-1} \}$$

erfüllt alle Anforderungen an einen endlichen Körper, die im **Kapitel 2.1** aufgeführt sind. Kommutativ–, Assoziativ– und Distributivgesetz werden erfüllt. Weiterhin gibt es

- ein neutrales Element hinsichtlich Addition $\Rightarrow N_\mathrm{A}$:

$$\exists\ z_j \in \mathrm{GF}(q): \quad z_i + z_j = z_i$$
$$\Rightarrow \quad z_j = N_\mathrm{A} = \text{”0”} \quad (\text{Nullelement}),$$

- ein neutrales Element hinsichtlich Multiplikation $\Rightarrow N_\mathrm{M}$:

$$\exists\ z_j \in \mathrm{GF}(q): \quad z_i \cdot z_j = z_i$$
$$\Rightarrow \quad z_j = N_\mathrm{M} = \text{”1”} \quad (\text{Einselement}),$$

- für alle Elemente z_i eine additive Inverse $\Rightarrow$ $\mathrm{Inv_A}(z_i)$:

$$\forall\ z_i \in \mathrm{GF}(q)\ \exists\ \mathrm{Inv_A}(z_i) \in \mathrm{GF}(q):$$
$$z_i + \mathrm{Inv_A}(z_i) = N_\mathrm{A} = \text{”0”} \quad \Rightarrow \quad \text{kurz}: \mathrm{Inv_A}(z_i) = -z_i,$$

- für alle Elemente z_i mit Ausnahme des Nullelements eine multiplikative Inverse $\Rightarrow$ $\mathrm{Inv_M}(z_i)$:

$$\forall\ z_i \in \mathrm{GF}(q),\ z_i \neq N_\mathrm{A}\ \exists\ \mathrm{Inv_M}(z_i) \in \mathrm{GF}(q):$$
$$z_i \cdot \mathrm{Inv_M}(z_i) = N_\mathrm{M} = \text{”1”} \quad \Rightarrow \quad \text{kurz}: \mathrm{Inv_M}(z_i) = z_i^{-1}.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.2.** In den Tabellen sind die Elemente z_0, ... , z_8 als Koeffizientenvektoren bezeichnet. So steht zum Beispiel „21” für die ausführliche Schreibweise $2 \cdot \alpha + 1$.

Fragebogen zu "A2.6: GF(P^m). Welches P, welches m?"

a) Geben Sie die Parameter des hier betrachteten Galoisfeldes an.

$\boldsymbol{P}$ =

$\boldsymbol{m}$ =

$\boldsymbol{q}$ =

b) Wie lautet das neutrale Element für die Addition?

- ☐ Das neutrale Element der Addition ist N_A = „00”,
- ☐ Das neutrale Element der Addition ist N_A = „01”,

c) Wie lautet das neutrale Element für die Multiplikation?

- ☐ Das neutrale Element der Multiplikation ist N_M = „00”,
- ☐ Das neutrale Element der Multipliaktion ist N_M = „01”,

d) Welche Aussagen gelten hinsichtlich der additiven Inversen?

- ☐ Es gilt Inv_A („02”) = „01”,
- ☐ Es gilt Inv_A („11”) = „22”,
- ☐ Es gilt Inv_A („22”) = „00”.

e) Welche der folgenden Aussagen treffen für die Multiplikation zu?

- ☐ Die Multiplikation erfolgt modulo $p(\alpha) = \alpha^2 + 2$.
- ☐ Die Multiplikation erfolgt modulo $p(\alpha) = \alpha^2 + 2\alpha + 2$.

f) Welche Aussagen gelten hinsichtlich der multiplikativen Inversen?

- ☐ Es gibt für alle Elemente $z_i \in \text{GF}(P^m)$ eine multiplikative Inverse.
- ☐ Es gilt Inv_M(„12”) = „10”.
- ☐ Es gilt Inv_M(„21”) = „12”.

g) Gilt („20” + „12”) · („12”) = „20” · „12” + „12” · „12”?

- ○ Ja,
- ○ Nein.

A2.7: Reed–Solomon–Code $(7, 3, 5)_8$

	Potenzen von α	Polynome in α	Vektoren $k_2\, k_1\, k_0$
z_0	$\alpha^{-\infty}=0$	0	000
z_1	$\alpha^0=1$	1	001
z_2	α^1	α	010
z_3	α^2	α^2	100
z_4	α^3	$\alpha+1$	011
z_5	α^4	$\alpha^2+\alpha$	110
z_6	α^5	$\alpha^2+\alpha+1$	111
z_7	α^6	α^2+1	101

Der hier betrachtete Reed–Solomon–Code mit der Bezeichnung RSC $(7, 3, 5)_8$

- codiert einen Informationsblock $\underline{u} = (u_0, u_1, u_2)$ von $k = 3$ Symbolen, wobei $u_0, u_1, u_2 \in \text{GF}(2^3)$ gilt,
- erzeugt ein Codewort $\underline{c} = (c_0, c_1, \ ..., c_6)$ der Länge $n = 7$ mit Codesymbolen c_i ebenfalls aus $\text{GF}(2^3)$,
- besitzt die freie Distanz $d_{\rm min} = n - k + 1 = 5$, so dass bis zu $e = 4$ Symbolfehler erkannt und bis zu $t = 2$ Symbolfehler korrigiert werden können.

Die Elemente des zugrunde liegenden Galoisfeldes lauten:

$$\text{GF}(2^3) = \{\, 0,\ 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6 \,\}.$$

Diese Elemente lassen sich entsprechend der Grafik auch als Polynome oder als Koeffizientenvektoren darstellen. Man erkennt aus obiger Tabelle, dass alle $u_i \in \text{GF}(2^3)$ und alle $c_i \in \text{GF}(2^3)$ auch durch $m = 3$ Bit charakterisiert werden können, zum Beispiel α^4 durch „110”.

Sie sollen in dieser Aufgabe für die binäre Eingangsfolge

110 001 011 000 000 000 111...

den Codiervorgang nachvollziehen. Beachten Sie dabei:

- Der Reed–Solomon–Coder arbeitet blockweise. Im ersten Codierschritt werden aus den drei ersten Informationssymbolen die Codesymbole $c_0, \ ... \ , c_6$ erzeugt, im zweiten Schritt dann aus dem Informationsblock $\underline{u} = (u_3, u_4, u_5)$ die Symbole $(c_7, ..., c_{13})$ des zweiten Codewortes, usw.
- Man beschreibt den Informationsblock $\underline{u}$ durch das Polynom $u(x) = u_0 + u_1 \cdot x + u_2 \cdot x^2$ vom Grad 2. Allgemein ergibt sich für das Galoisfeld $\text{GF}(2^m)$ der Grad des Polynoms zu $m - 1$.
- Die Codesymbole $c_0, \ ..., c_6$ erhält man, indem in das Polynom $u(x)$ für x alle Elemente von $\text{GF}(2^3)$ mit Ausnahme des Nullelementes eingesetzt werden:

$$\text{GF}(2^3) \setminus \{0\} = \{\, \alpha^0,\ \alpha^1,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6 \,\}.$$

Formal lässt sich der RSC $(7, 3, 5)_8$ wie folgt beschreiben:

$$C_{\rm RS} = \left\{ \underline{c} = \big(u(\alpha^0),\ u(\alpha^1),\ u(\alpha^2)\big) \ \middle|\ u(x) = \sum_{i=0}^{2} u_i \cdot x^i,\ \ u_i \in \text{GF}(2^3) \right\}.$$

Hinweis: Die vorliegende Aufgabe behandelt die Thematik von **Kapitel 2.3.** Die **Aufgabe A2.8** ist ähnlich strukturiert wie diese. Zur Generierung eines Codewortes $\underline{c}$ soll dann aber die Generatormatrix **G** herangezogen werden.

Fragebogen zu "A2.7: Reed–Solomon–Code $(7, 3, 5)_8$"

a) Wie lautet der binäre Informationsblock im ersten Codierschritt?

- ☐ $\underline{u}_{\rm bin} = (110)$,
- ☐ $\underline{u}_{\rm bin} = (110001011)$,
- ☐ $\underline{u}_{\rm bin} = (1100010)$.

b) Wie lauten die Informationssymbole im ersten Codierschritt?

- ☐ $u_0 = \alpha^4$,
- ☐ $u_0 = 0$,
- ☐ $u_1 = \alpha^6$,
- ☐ $u_1 = \alpha^0$,
- ☐ $u_2 = \alpha^3$,
- ☐ $u_2 = \alpha^2$.

c) Wie lautet der Informationsblock als Polynom $u(x)$?

- ☐ $u(x) = \alpha^3 \cdot x + x^2 + \alpha^4 \cdot x^3$,
- ☐ $u(x) = \alpha^3 + x + \alpha^4 \cdot x^2$,
- ☐ $u(x) = \alpha^4 + x + \alpha^3 \cdot x^2$.

d) Wie lauten die Codesymbole c_0, ..., c_6 für den ersten Codierschritt.

- ☐ $c_0 = \alpha^2$,
- ☐ $c_1 = \alpha^3$,
- ☐ $c_2 = \alpha^3$,
- ☐ $c_3 = 1$,
- ☐ $c_4 = \alpha^2$,
- ☐ $c_5 = \alpha^4$,
- ☐ $c_6 = 1$.

e) Wie lautet das binäre Codewort? Genau ein Vorschlag ist richtig.

- $\underline{c}_{\rm bin} = 100|011|011|001|110|100|001$,
- $\underline{c}_{\rm bin} = 011|011|001|110|100|001|100$,
- $\underline{c}_{\rm bin} = 1001110$.

f) Welche Aussagen gelten für den zweiten Codierschritt?

- Es gilt $u_0 = u_1 = u_2 = 0$.
- Es gilt $u(x) = 1$.
- Das Codewort $\underline{c} \in {\rm GF}(2^3)$ besteht aus sieben Nullsymbolen.
- Das binäre Codewort besteht aus 21 Nullen.

Z2.7: Reed–Solomon–Code $(15, 5, 11)_{16}$

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

Die vorliegende Aufgabenstellung ist ähnlich wie diejenige bei der **Aufgabe A2.7.** Wir beziehen uns hier aber nun auf das Galoisfeld GF(2^4), dessen Elemente nebenstehend sowohl in Exponenten– und Polynomdarstellung als auch durch den Koeffizientenvektor angegeben sind. Weiter gilt in GF(2^4):

$$\alpha^{16} = \alpha^1\,,\ \ \alpha^{17} = \alpha^2\,,\ \ \alpha^{18} = \alpha^3\,, \ \text{...}$$

Zur Codierung des Informationsblockes der Länge $k = 5$,

$$\underline{u} = (u_0, u_1, u_2, u_3, u_4)\,,$$

bilden wir das Polynom

$$u(x) = u_0 + u_1 \cdot x + u_2 \cdot x^2 + u_3 \cdot x^3 + u_4 \cdot x^4$$

mit u_0, ... , $u_4 \in$ GF(2^4). Die $n = 15$ Codeworte ergeben sich dann, wenn man in $u(x)$ die Elemente von GF(2^4) \ {0} einsetzt:

$$c_0 = u(\alpha^0)\,,\ \ c_1 = u(\alpha^1)\,,\ \ c_2 = u(\alpha^2)\,,\ \ \text{...}\ ,\ \ c_{14} = u(\alpha^{14})\,.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.3.**

Fragebogen zu "Z2.7: Reed–Solomon–Code $(15, 5, 11)_{16}$"

a) Wieviele Symbolfehler können korrigiert werden?

t =

b) Wie lautet das Polynom $u(x)$ für $\underline{u} = (\alpha^3,\ 0,\ 0,\ 1,\ \alpha^{10})$?

- ☐ $u(x) = \alpha^3 + x + \alpha^{10} \cdot x^2$,
- ☐ $u(x) = \alpha^3 + x^3 + \alpha^{10} \cdot x^4$,
- ☐ $u(x) = 1 + x + x^2 + x^3 + x^4$.

c) Wie lautet das Symbol c_0 des zugehörigen Codewortes $\underline{c}$?

- ☐ $c_0 = 1$,
- ☐ $c_0 = \alpha^5$,
- ☐ $c_0 = \alpha^{11}$,
- ☐ $c_0 = \alpha^{14}$.

d) Wie lautet das Symbol c_1 des zugehörigen Codewortes $\underline{c}$?

- ☐ $c_1 = 1$,
- ☐ $c_1 = \alpha^5$,
- ☐ $c_1 = \alpha^{11}$,
- ☐ $c_1 = \alpha^{14}$.

e) Wie lautet das Symbol c_{13} des zugehörigen Codewortes $\underline{c}$?

- ☐ $c_{13} = 1$,
- ☐ $c_{13} = \alpha^5$,
- ☐ $c_{13} = \alpha^{11}$,
- ☐ $c_{13} = \alpha^{14}$.

f) Wie lautet das letzte Symbol des zugehörigen Codewortes $\underline{c}$?

- ☐ $c_{15} = 1$,

- ☐ $c_{14} = 1$,
- ☐ $c_{14} = \alpha^7$,
- ☐ $c_{14} = \alpha^{14}$.

g) Welche Aussagen treffen zu?

- ☐ Das Codesymbol „0” ist beim RSC $(15, 5, 11)_{16}$ nicht möglich.
- ☐ Ein Codesymbole „0” ergibt sich nur für $\underline{u} = (0, 0, 0, 0, 0)$.
- ☐ Auch für $\underline{u} \neq (0, 0, 0, 0, 0)$ kann es Codesymbole „0” geben.

A2.8: RS–Generatorpolynome

In der **Aufgabe A2.7** sollten Sie die Codeworte des RSC $(7, 3, 5)_8$ über ein Polynom ermitteln. Man kann aber das Codewort $\underline{c}$ auch aus dem Informationswort $\underline{u}$ und der Generatormatrix $\mathbf{G}$ gemäß der folgenden Gleichung bestimmen:

$$\underline{c} = \underline{u} \cdot \mathbf{G}.$$

Zwei der vorgegebenen Generatormatrizen beschreiben den RSC $(7, 3, 5)_8$. In der Teilaufgabe (a) ist explizit gefragt, welche. Eine weitere Generatormatrix gehört zum RSC $(7, 5, 3)_8$, der in der Teilaufgabe (c) betrachtet wird.

$$\mathbf{G}_A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\mathbf{G}_B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \end{pmatrix}$$

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

$$\mathbf{G}_D = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\ 1 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$$

Hinweis: Die Aufgabe gehört zum Themengebiet von **Kapitel 2.3.** Wichtige Informationen zu den Reed–Solomon–Codes finden Sie auch in der Angabe zur **Aufgabe A2.7.**

Fragebogen zu "A2.8: RS–Generatorpolynome"

a) Welche der Generatorpolynome beschreiben den RSC $(7, 3, 5)_8$?

- ☐ $\mathbf{G}_A$,
- ☐ $\mathbf{G}_B$,
- ☐ $\mathbf{G}_C$,
- ☐ $\mathbf{G}_D$.

b) Die Informationsfolge beginnt mit α^4, 1, α^3, 0, α^6. Bestimmen Sie das erste Codewort für den RSC $(7, 3, 5)_8$.

- ☐ Es gilt $c_0 = \alpha^2$,
- ☐ Es gilt $c_1 = \alpha^3$,
- ☐ Es gilt $c_6 = 0$.

c) Wie lautet bei gleicher Informationsfolge das Codewort für den RSC $(7, 5, 3)_8$?

- ☐ Es gilt $c_0 = 1$,
- ☐ Es gilt $c_1 = 0$,
- ☐ Es gilt $c_6 = \alpha^6$.

Z2.8: „Plus" und „Mal" in GF(2^3)

Die Grafik zeigt die Additions– und Multiplikationstabelle für den endlichen Körper GF(2^3). Die Tabellen sind nicht vollständig. Einige Felder sollen Sie ergänzen.

Die Elemente sind sowohl in der Exponentendarstellung (mit roter Beschriftung, links und oben) als auch in der Koeffizientendarstellung (graue Schrift, rechts und unten) angegeben. Aus dieser Zuordnung erkennt man bereits das zugrunde liegende irreduzible Polynom $p(\alpha)$.

Additionen (und Subtraktionen) führt man am besten in der Koeffizientendarstellung (oder mit den damit fest verknüpften Polynomen) durch. Für Multiplikationen ist dagegen die Exponentendarstellung günstiger.

Hinweis: Die Aufgabe bezieht sich auf die Thematik von **Kapitel 2.2** und **Kapitel 2.3.**

+	0	1	α^1	α^2	α^3	α^4	α^5	α^6	
0	A	1	α^1	α^2	α^3	α^4	α^5	α^6	000
1	1	A	α^3	α^6	α^1	α^5	α^4	α^2	001
α^1	α^1	α^3	A	C	1	α^2	α^6	α^5	010
α^2	α^2	α^6	C	A	α^5	α^1	α^3	1	100
α^3	α^3	α^1	1	α^5	A	α^6	D	α^4	011
α^4	α^4	α^5	α^2	α^1	α^6	A	1	α^3	110
α^5	α^5	α^4	α^6	α^3	D	1	A	B	111
α^6	α^6	α^2	α^5	1	α^4	α^3	B	A	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	F	α^2	α^3	α^4	E	G	001
α^1	0	F	α^2	α^3	α^4	E	G	1	010
α^2	0	α^2	α^3	α^4	E	G	1	F	100
α^3	0	α^3	α^4	E	G	1	F	α^2	011
α^4	0	α^4	E	G	1	F	α^2	α^3	110
α^5	0	E	G	1	F	α^2	α^3	α^4	111
α^6	0	G	1	F	α^2	α^3	α^4	E	101
	000	001	010	100	011	110	111	101	

Fragebogen zu "Z2.8: „Plus" und „Mal" in GF(2^3)"

a) Für welches Element steht „A" in der Additionstabelle?

- ☐ A = 0,
- ☐ A = 1,
- ☐ A = α^1.

b) Für welches Element steht „B" in der Additionstabelle?

- ☐ B = 0,
- ☐ B = 1,
- ☐ B = α^1.

c) Für welches Element steht „C" in der Additionstabelle?

- ☐ C = α^2,
- ☐ C = α^3,
- ☐ C = α^4.

d) Für welches Element steht „D" in der Additionstabelle?

- ☐ D = α^2,
- ☐ D = α^3,
- ☐ D = α^4.

e) Welche Zuordnungen gelten in der Multiplikationstabelle?

- ☐ E = α^5,
- ☐ F = α^1,
- ☐ G = α^6.

f) Welches irreduzible Polynom liegt diesen Tabellen zugrunde?

- ☐ $p(\alpha) = \alpha^2 + \alpha + 1$,
- ☐ $p(\alpha) = \alpha^3 + \alpha^2 + 1$,
- ☐ $p(\alpha) = \alpha^3 + \alpha + 1$,

A2.9: Reed–Solomon–Parameter

Nebenstehend finden Sie eine unvollständige Liste möglicher Reed–Solomon–Codes, die bekanntlich auf einem Galoisfeld GF(q) = GF(2^m) basieren. Der Parameter m gibt an, mit wie vielen Bit ein RS–Codesymbol dargestellt wird. Es gilt:

- m = 4 (rote Schrift),
- m = 5 (blaue Schrift),
- m = 6 (grüne Schrift).

RSC (15, 11, 5)$_4$	RSC (60, 44, 5)$_2$
RSC (15, 9, 7)$_4$	RSC (60, 36, 7)$_2$
RSC (15, 7, 9)$_4$	RSC (60, 28, 9)$_2$
RSC (15, 5, 11)$_4$	RSC (60, 20, 11)$_2$
RSC (15, 3, 13)$_4$	RSC (60, 12, 13)$_2$
RSC (31, 27, 5)$_5$	RSC (155, 135, 5)$_2$
RSC (31, 23, 9)$_5$	RSC (155, 115, 9)$_2$
RSC (31, 19, 13)$_5$	RSC (155, 95, 13)$_2$
RSC (31, 17, 15)$_5$	RSC (155, 85, 15)$_2$
RSC (31, 15, 17)$_5$	RSC (155, 75, 17)$_2$
RSC (63, 55, 9)$_6$	RSC (378, 330, 9)$_2$
RSC (63, 51, 13)$_6$	RSC (378, 306, 13)$_2$
RSC (63, 47, 17)$_6$	RSC (378, 282, 17)$_2$
RSC (63, 45, 19)$_6$	RSC (378, 270, 19)$_2$
RSC (63, 43, 21)$_6$	RSC (378, 258, 21)$_2$

Ein Reed–Solomon–Code wird wie folgt bezeichnet:

$$\textbf{RSC}(\boldsymbol{n}, \boldsymbol{k}, \boldsymbol{d}_{\rm min})_{\boldsymbol{q}}$$

Die Parameter haben folgende Bedeutung:

- n gibt die Anzahl der Symbole eines Codewortes $\underline{c}$ an ⇒ **Länge** des Codes,
- k gibt die Anzahl der Symbole eines Informationsblocks $\underline{u}$ an ⇒ **Dimension** des Codes,
- $d_{\rm min}$ kennzeichnet die **minimale Distanz** zwischen zwei Codeworten (stets gleich n–k+1),
- q gibt einen Hinweis auf die Verwendung des Galoisfeldes **GF(q)**.

Rechts daneben ist die Binärrepräsentation des gleichen Codes angegeben. Bei dieser Realisierung eines RS–Codes wird jedes Informations– und Codesymbol durch m Bit dargestellt. Beispielsweise erkennt man aus der ersten Zeile, dass die minimale Distanz hinsichtlich der Bits ebenfalls $d_{\rm min}$ = 5 ist, wenn die minimale Distanz in GF(2^m) $d_{\rm min}$ = 5 beträgt. Damit können bis zu t = 2 Bitfehler (oder Symbolfehler) korrigiert und bis zu e = 4 Bitfehler (oder Symbolfehler) erkannt werden.

Hinweis: Die Aufgabe gehört zum **Kapitel 2.3.**

Fragebogen zu "A2.9: Reed–Solomon–Parameter"

a) Es gelte $c_i \in \mathrm{GF}(2^m)$. Welche RS–Codeparameter n ergeben sich?

$m = 4$: n =

$m = 5$: n =

$m = 6$: n =

b) Im Folgenden werden zwei spezielle RS–Codes (*RSC 1*, *RSC 2*) betrachtet. Mit welchem RS–Parameter k lassen sich genau t Symbolfehler korrigieren?

RSC 1 ($m = 4$, $t = 4$): k =

RSC 1 ($m = 5$, $t = 8$): k =

c) Welche Bezeichnungen sind für RSC 1 bzw. RSC 2 richtig?

- ☐ RSC 1 nennt man auch RSC $(15, 7, 9)_{16}$.
- ☐ RSC 1 nennt man auch RSC $(15, 7, 4)_{4}$.
- ☐ RSC 2 nennt man auch RSC $(31, 17, 15)_{32}$.
- ☐ RSC 2 nennt man auch RSC $(31, 15, 17)_{32}$.

d) Wieviele Symbolfehler können höchstens erkannt werden?

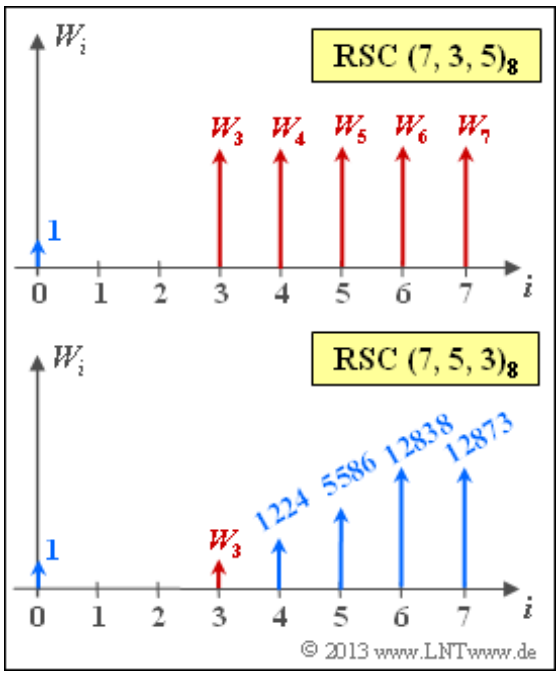
mit RSC 1: e =

mit RSC 2: e =

e) Wie lauten die betrachteten Codes in Binärschreibweise?

- ☐ RSC 1 entspricht dem Code RSC $(60, 28, 36)_2$.
- ☐ RSC 1 entspricht dem Code RSC $(60, 28, 9)_2$.
- ☐ RSC 2 entspricht dem Code RSC $(155, 75, 17)_2$.
- ☐ RSC 2 entspricht dem Code RSC $(124, 60, 17)_2$.

A2.10: Fehlererkennung bei RSC



Bei einem linearen Blockcode können bis zu $e = d_{\rm min} - 1$ Fehler erkannt werden. Bei allen Reed–Solomon–Codes beträgt dabei die minimale Distanz

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

Man muss folgende Fälle unterscheiden:

- Treten nicht mehr als $e = n - k$ Symbolfehler auf, so wird der Block als fehlerhaft erkannt.
- Die Fehlererkennung kann auch bei mehr als $n - k$ Symbolfehlern noch funktionieren, und zwar dann, wenn das Empfangswort kein gültiges Codewort des Reed–Solomon–Codes ist:

$$\underline{y} \notin C_{\rm RS} = \{\underline{c}_0, \ \cdots, \underline{c}_i, \ \cdots, \underline{c}_{n-1}\} .$$

- Ist aber das verfälschte Empfangswort ($\underline{y} \neq \underline{c}$) ein gültiges Codewort $\Rightarrow \underline{y}$, so bleibt bei der Decodierung der fehlerhafte Block unentdeckt. Wir definieren als Blockfehlerwahrscheinlichkeit:

$$\Pr(\text{Blockfehler}) = \Pr(\underline{y} \neq \underline{c}) .$$

In dieser Aufgabe soll diese Wahrscheinlichkeit für folgende Codes ermittelt werden:

- Reed–Solomon–Code $(7, 3, 5)_8$ $\Rightarrow$ $d_{\rm min} = 5$,
- Reed–Solomon–Code $(7, 5, 3)_8$ $\Rightarrow$ $d_{\rm min} = 3$.

Weiterhin soll gelten:

- Jedes Symbol wird mit der Wahrscheinlichkeit $\varepsilon_{\rm S} = 0.1$ in ein anderes Symbol verfälscht und mit der Wahrscheinlichkeit $1 - \varepsilon_{\rm S} = 0.9$ richtig übertragen.
- Für das Distanzspektrum eines Reed–Solomon–Codes der Länge n gilt mit $d = d_{\rm min}$:

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

Daneben sollen zwei Schranken für die Blockfehlerwahrscheinlichkeit betrachtet und bewertet werden:

- Ist allein die minimale Distanz bekannt, so kann man daraus eine *obere Schranke* ableiten. Die Gewichtsfaktoren W_i sind dabei so zu wählen, dass sicher ($\Rightarrow$ bei allen Konstellationen) gilt:

$$\Pr(\text{Obere Schranke}) \geq \Pr(\text{Blockfehler}) .$$

- Eine *untere Schranke* erfordert zusätzlich die Kenntnis der Gewichtsfunktion W_i für $i = d_{\rm min}$. Damit kann folgende Bedingung erfüllt werden:

$$\Pr(\text{Untere Schranke}) \leq \Pr(\text{Blockfehler}) .$$

Hinweis: Die Aufgabe gehört zu **Kapitel 2.3.** Zu berechnen sind die in der obigen Grafik rot markierten Gewichte W_i.

Fragebogen zu "A2.10: Fehlererkennung bei RSC"

a) Berechnen Sie das Distanzspektrum für den RSC $(7, 3, 5)_8$.

RSC (7, 3, 5): W_3 =

W_4 =

W_5 =

W_6 =

W_7 =

b) Wie lautet das in der Grafik fehlende Gewicht des RSC $(7, 5, 3)_8$?

RSC (7, 5, 3): W_3 =

c) Mit welcher Wahrscheinlichkeit bleibt ein fehlerhafter Block unerkannt? Die Verfälschungswahrscheinlichkeit eines Symbols sei $\varepsilon = 0.1$.

RSC (7, 3, 5): Pr(Blockfehler) =

RSC (7, 5, 3): Pr(Blockfehler) =

d) Berechnen und bewerten Sie für beide Codes die in der Angabe vorgeschlagene obere Schranke $p_{\rm oben}$ = Pr(Obere Schranke).

RSC (7, 3, 5): $p_{\rm oben}$ =

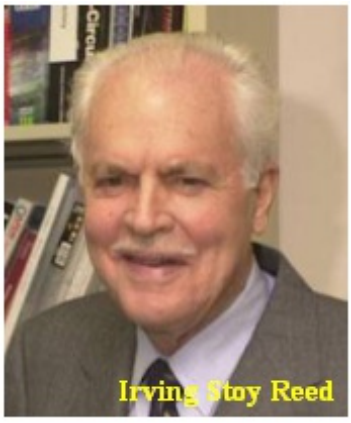
RSC (7, 5, 3): $p_{\rm oben}$ =

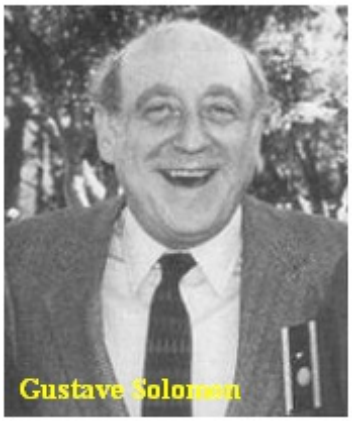
e) Berechnen und bewerten Sie für beide Codes die in der Angabe vorgeschlagene untere Schranke $p_{\rm unten}$ = Pr(Untere Schranke).

RSC (7, 3, 5): $p_{\rm unten}$ =

RSC (7, 5, 3): $p_{\rm unten}$ =

Z2.10: Coderate und minimale Distanz





Die von **Irving Stoy Reed** und **Gustave Solomon** Anfang der 1960er Jahre entwickelten Codes werden in diesem Tutorial wie folgt bezeichnet:

$$\text{RSC } (n,\ k,\ d_{\rm min})_q \ .$$

Die Codeparameter haben folgende Bedeutungen:

- $q = 2^m$ ist ein Hinweis auf die Größe des Galoisfeldes ⇒ GF(q),
- $n = q - 1$ ist die Codelänge (Symbolanzahl eines Codewortes),
- k gibt die Dimension an (Symbolanzahl eines Informationsblocks),
- $d_{\rm min}$ bezeichnet die minimale Distanz zwischen zwei Codeworten.

  Bei RS–Codes erreicht $d_{\rm min} = n - k + 1$ seinen größten Wert.

Hinweis: Die Aufgabe gehört zum **Kapitel 2.3.** Die für diese Aufgabe relevanten Informationen finden Sie am Ende des Theorieteils, nämlich auf der Seite **Codebezeichnung und Coderate.**

Fragebogen zu "Z2.10: Coderate und minimale Distanz"

a) Geben Sie die Kenngrößen des RSC (255, 223, $d_{\rm min})_q$ an.

$\boldsymbol{q}$ =

$\boldsymbol{R}$ =

$\boldsymbol{e}$ =

$\boldsymbol{t}$ =

b) Geben Sie die Kenngrößen des RSC (2040, 1784, $d_{\rm min})_2$ an.

$\boldsymbol{R}$ =

$\boldsymbol{d_{\rm min}}$ =

c) Wieviele Bitfehler darf ein Empfangswort $\underline{y}$ maximal aufweisen, damit es mit Sicherheit richtig decodiert wird?

$\underline{y}$ sicher decodierbar: $N_{\rm Bitfehler}$ =

d) Wieviele Bitfehler darf ein Empfangswort $\underline{y}$ im günstigsten Fall aufweisen, damit es noch richtig decodiert werden könnte.

$\underline{y}$ evtl. decodierbar: $N_{\rm Bitfehler}$ =

A2.11: RS–Decodierung nach „Erasures”

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

Wir betrachten hier ein Codier– und Decodiersystem entsprechend der **Grafik** im Theorieteil zu diesem Kapitel. Anzumerken ist:

- Der Reed–Solomon–Code ist durch die Generatormatrix **G** und die Prüfmatrix **H** vorgegeben, wobei alle Elemente aus dem Galoisfeld GF(2^3) \ {0} stammen:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix},$$

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix}.$$

- Alle Codesymbole $c_i \in \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ werden durch $m = 3$ Bit dargestellt und über den grün hinterlegten Auslöschungskanal (m–BEC) übertragen. Ein Codesymbol wird bereits dann als Auslöschung (*Erasure*) E markiert, wenn eines der drei zugehörigen Bit unsicher ist.
- Der *Codewortfinder* (CWF) hat die Aufgabe, aus dem teilweise ausgelöschten Empfangswort $\underline{y}$ das regenerierte Codewort $\underline{z}$ zu erzeugen. Dabei muss sicher gestellt sein, dass das Ergebnis $\underline{z}$ tatsächlich ein gültiges Reed–Solomon–Codewort ist.
- Beinhaltet das Empfangswort $\underline{y}$ zu viele Auslöschungen, so gibt der Decoder eine Meldung der Art „Symbol ist nicht decodierbar” aus. Es wird also nicht versucht, das Codewort zu schätzen. Wird $\underline{z}$ ausgegeben, so ist dieses auch richtig: $\underline{z} = \underline{c}$.
- Das gesuchte Informationswort $\underline{v} = \underline{u}$ ergibt sich durch die inverse Coderfunktion $\underline{v} = \text{enc}^{-1}(\underline{z})$. Mit der Generatormatrix **G** lässt sich diese wie folgt realisieren:

$$\underline{c} = \text{enc}(\underline{u}) = \underline{u} \cdot \mathbf{G} \quad \Rightarrow \quad \underline{z} = \text{enc}(\underline{v}) = \underline{v} \cdot \mathbf{G}$$
$$\Rightarrow \quad \underline{v} = \text{enc}^{-1}(\underline{z}) = \underline{z} \cdot \mathbf{G}^{\rm T}.$$

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.4.** Hinsichtlich des *Codewortfinders* verweisen wir insbesondere auf die Seiten **Vorgehensweise** und **Lösung der Matrixgleichungen.**

Alle Berechnungen sind in GF(2^3) durchzuführen. Die obere Grafik beschreibt deren $q = 8$ Elemente in Potenz–, Polynom– und Koeffizientenvektordarstellung.

Fragebogen zu "A2.11: RS–Decodierung nach „Erasures”"

a) Geben Sie die Codeparameter des vorliegenden Reed–Solomon–Codes an.

n =

k =

d_{min} =

b) Kann der Empfangsvektor $\underline{y}$ = (0, 0, 0, 0, 0, 0, E) decodiert werden?

- ○ JA.
- ○ NEIN.

c) Kann der Empfangsvektor $\underline{y}$ = (E, E, 1, 1, 1, 1, 1) decodiert werden?

- ○ JA.
- ○ NEIN.

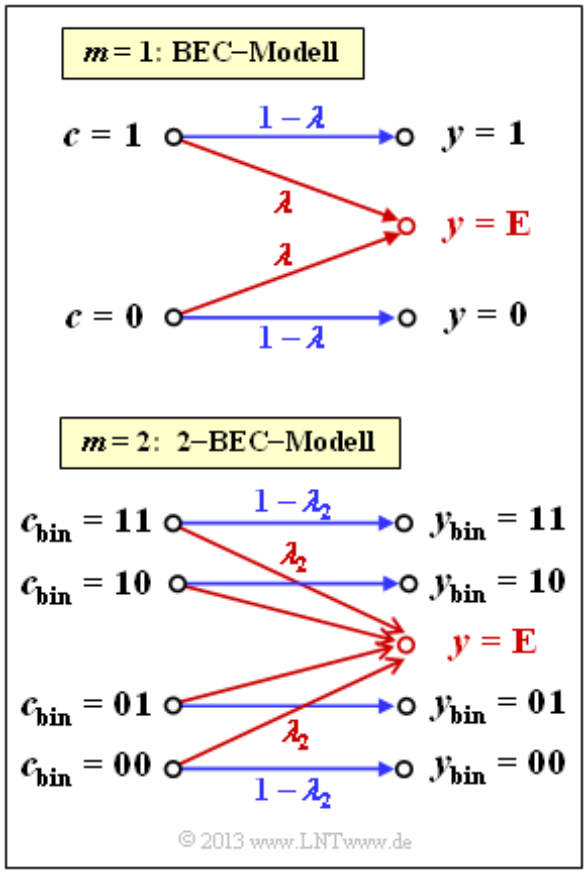
d) Welches Ergebnis liefert die Decodierung von $\underline{y}$ = (E, E, E, 0, 1, α, 0)?

- ☐ $z_0 = \alpha$, $z_1 = \alpha^3$, $z_2 = 0$.
- ☐ $z_0 = \alpha$, $z_1 = \alpha^3$, $z_2 = \alpha^3$.
- ☐ $z_0 = 1$, $z_1 = 0$, $z_2 = \alpha^3$.
- ☐ Die Decodierung führt zu keinem Ergebnis.

e) Welches Ergebnis liefert die Decodierung von $\underline{y}$ = (E, E, E, 0, 1, α, E)?

- ☐ $z_0 = \alpha$, $z_1 = \alpha^3$, $z_2 = 0$, $z_6 = 1$.
- ☐ $z_0 = \alpha$, $z_1 = \alpha^3$, $z_2 = \alpha^3$, $z_6 = 1$.
- ☐ $z_0 = 1$, $z_1 = 0$, $z_2 = \alpha^3$, $z_6 = 1$.
- ☐ Die Decodierung führt zu keinem Ergebnis.

Z2.11: Erasure–Kanal für Symbole



Das Kanalmodell **Binary Erasure Channel** (BEC) beschreibt einen Auslöschungskanal auf Bitebene. Ein Binärsymbol **0** bzw. **1** wird mit der Wahrscheinlichkeit $1 - \lambda$ richtig übertragen und mit der Wahrscheinlichkeit λ als Auslöschung E (*Erasure*) markiert. Im Gegensatz zum **BSC** kann es hier nicht zu Verfälschungen (**0** → **1**, **1** → **0**) kommen.

Ein Reed–Solomon–Code basiert auf einem Galoisfeld GF(2^m) mit ganzzahligem m. Jedes Codesymbol c lässt sich somit durch m Bit darstellen. Will man hier das BEC–Modell anwenden, so muss man dieses zum ***m*–BEC–Modell** modifizieren, wie es in der unteren Grafik für $m = 2$ gezeigt ist:

Alle Codesymbole – in binärer Darstellung **00**, **01**, **10** und **11** – werden mit der Wahrscheinlichkeit $1 - \lambda_2$ richtig übertragen. Damit beträgt die Wahrscheinlichkeit für ein ausgelöschtes Symbol λ_2. Zu beachten ist, dass bereits ein einziges ausgelöschtes Bit zum ausgelöschten Empfangssymbol y = E führt.

Hinweis: Die Aufgabe gehört zu **Kapitel 2.4.** Bei einem auf GF(2^m) basierenden Code ist das skizzierte 2–BEC–Modell zum m–BEC zu erweitern. Die Auslöschungswahrscheinlichkeit dieses Modell wird dann mit λ_m bezeichnet.

Für die Teilaufgaben (a), (b) und (c) gelte für die Auslöschungswahrscheinlichkeit des Grundmodells gemäß der oberen Grafik stets $\lambda = 0.2$.

Fragebogen zu "Z2.11: Erasure–Kanal für Symbole"

a) Es gelte $\lambda = 0.2$. Mit welchen Wahrscheinlichkeiten treten beim BEC–Modell die möglichen Empfangswerte auf?

1–BEC: $\mathbf{Pr}(y = 0) =$

$\mathbf{Pr}(y = \mathrm{E}) =$

$\mathbf{Pr}(y = 1) =$

b) Wie groß ist die Auslöschungswahrscheinlichkeit λ_2 auf Symbolebene, wenn der Reed–Solomon–Code auf GF(2^2) basiert ($\lambda = 0.2$)?

2–BEC: $\lambda_2 =$

c) Wie groß ist die Auslöschungswahrscheinlichkeit λ_m, wenn das m–BEC–Modell an den RSC $(255, 223, 33)_{256}$ angepasst wird ($\lambda = 0.2$)?

m–BEC: $\lambda_m =$

d) Wie groß darf die Auslöschungswahrscheinlichkeit λ beim Grundmodell (BEC) maximal sein, damit $\lambda_m \le 0.2$ gilt?

$\lambda_m \le$ **0.2: Max[λ]** =

e) Mit welcher Wahrscheinlichkeit wird damit das „Nullsymbol" empfangen?

$\lambda_m = 0.2$: $\mathbf{Pr}(y_{\mathrm{bin}} = 00000000) =$

A2.12: Decodierung beim RSC(7, 4, 4)$_8$

Wir analysieren den Peterson–Algorithmus, der im Theorieteil zu **Kapitel 2.5** ausführlich dargelegt ist. Vorausgesetzt wird der Reed–Solomon–Code mit den Parametern $n = 7$, $k = 4$ und $d_{\rm min} = 4$, wobei alle Codesymbole aus GF(2^3) stammen und alle Rechenoperationen in GF(2^3) durchzuführen sind.

Die Prüfmatrix dieses Codes lautet:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix}.$$

Im **Schritt (A)** des hier betrachteten Decodier–Algorithmuses muss das Syndrom $\underline{s} = \underline{y} \cdot \mathbf{H}^{\rm T}$ berechnet werden. Für das hier vorausgesetzte Empfangswort $\underline{y} = (\alpha^1, 0, \alpha^3, 0, 1, \alpha, 0)$ ergibt sich das Syndrom zu $\underline{s} = (\alpha^4, \alpha^5, \alpha^6)$, wie in **Aufgabe Z2.12** noch gezeigt wird.

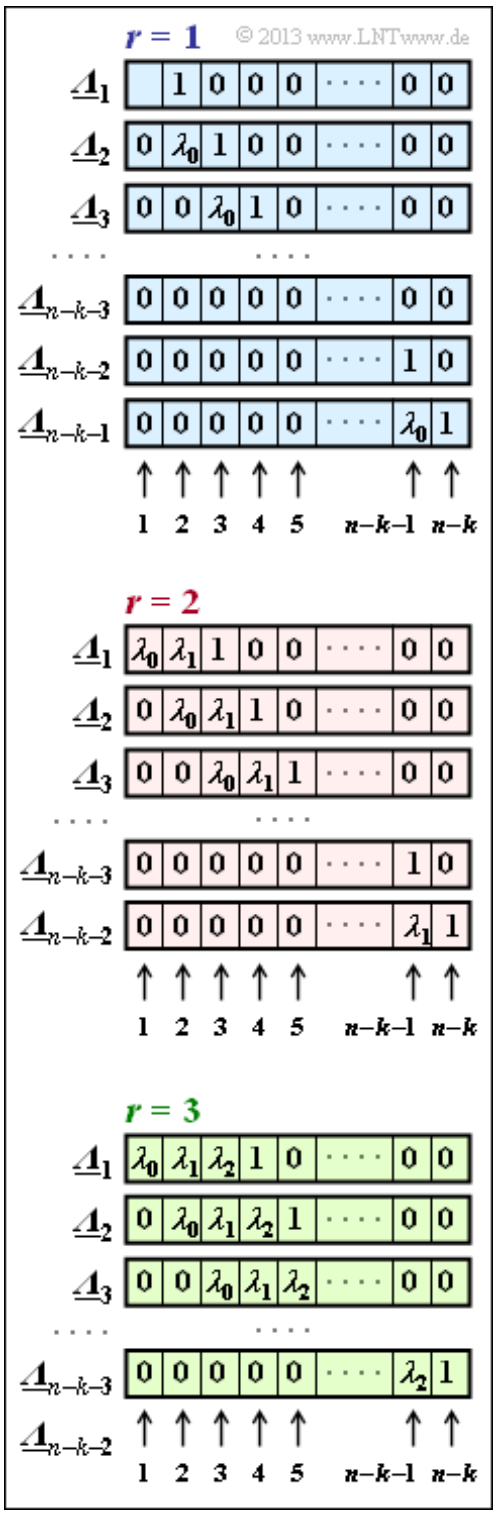
Danach müssen die **ELP–Koeffizientenvektoren** gemäß der nebenstehenden Abbildung aufgestellt und ausgewertet werden, wobei die Belegung davon abhängt, ob man von $r = 1$, $r = 2$ oder $r = 3$ Symbolfehlern im Empfangswort ausgeht.

Sind für die angenommene Symbolfehlerzahl r alle Gleichungen $\underline{\Lambda}_l \cdot \underline{s}^{\rm T} = 0$ erfüllt, so weist das Empfangswort $\underline{y}$ tatsächlich genau r Symbolfehler auf.

Die weiteren Schritte können Sie dem Theorieteil entnehmen:

- Schritt (C): **Lokalisierung der Fehlerpositionen,**
- Schritt (D): **Ermittlung der Fehlerwerte.**

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.5.**



Fragebogen zu "A2.12: Decodierung beim RSC(7, 4, 4)$_8$"

a) Welche Belegungsschemata sind für diese Aufgabe relevant?

- ☐ Das blau hinterlegte Schema ($r = 1$).
- ☐ Das rot hinterlegte Schema ($r = 2$).
- ☐ Das grün hinterlegte Schema ($r = 3$).

b) Wie lang sind die ELP–Koeffizientenvektoren $\underline{\Lambda}_l$?

$$L =$$

c) Wie viele solcher Vektoren $\underline{\Lambda}_l$ mit Index $l = 1, \ldots, l_{max}$ gibt es?

$$l_{max} =$$

d) Das Syndrom ergibt sich zu $\underline{s} = (\alpha^4, \alpha^5, \alpha^6)$. Ist die Decodierung erfolgreich?

- ○ JA.
- ○ NEIN.

e) Welche Symbole wurden verfälscht?

- ☐ Symbol 0,
- ☐ Symbol 1,
- ☐ Symbol 6.

f) Geben Sie den Wert des verfälschten Symbols $e_i \neq 0$ an.

- ☐ $e_i = \alpha^2$,
- ☐ $e_i = \alpha^3$,
- ☐ $e_i = 1$.

g) Das Syndrom sei nun $\underline{s} = (\alpha^2, \alpha^4, \alpha^5)$. Ist damit die Decodierung erfolgreich?

- ○ JA.
- ○ NEIN.

Z2.12: Reed–Solomon–Syndromberechnung

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

Wie in der **Aufgabe A2.12** betrachten wir den Reed–Solomon–Code $(7,\ 4,\ 4)_8$, der auf dem Galoisfeld GF(q) mit $q = 8 = 2^3$ basiert. Die Grafik zeigt die zugehörige Umrechnungstabelle.

Gegeben sind die möglichen Codesymbole in Exponentendarstellung (Potenzen von α) sowie in Polynom– und Koeffizientendarstellung.

Vorgegeben ist das Empfangswort $\underline{y} = (\alpha,\ 0,\ \alpha^3,\ 0,\ 1,\ \alpha,\ 0)$. Anhand des Syndroms

$$\underline{s} = (s_0, s_1, s_2) = \underline{y} \cdot \mathbf{H}^{\rm T}$$

soll überprüft werden, ob einzelne Symbole des Empfangsvektors $\underline{y}$ bei der Übertragung verfälscht wurden. Gegeben ist hierzu die Prüfmatrix **H** des betrachteten Codes und deren Transponierte:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix}, \quad \mathbf{H}^{\rm T} = \begin{pmatrix} 1 & 1 & 1 \\ \alpha^1 & \alpha^2 & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^3 & \alpha^6 & \alpha^2 \\ \alpha^4 & \alpha^1 & \alpha^5 \\ \alpha^5 & \alpha^3 & \alpha^1 \\ \alpha^6 & \alpha^5 & \alpha^4 \end{pmatrix}.$$

Hinweis: Die Aufgabe bezieht sich auf die **Seite 4** von Kapitel 2.5.

Fragebogen zu "Z2.12: Reed–Solomon–Syndromberechnung"

a) Empfangen wurde $\underline{y} = (\alpha,\ 0,\ \alpha^3,\ 0,\ 1,\ \alpha,\ 0)$. Geben Sie das erste Element des Syndroms $\underline{s} = (s_0, s_1, s_2)$ an.

- $s_0 = \alpha^4$,
- $s_0 = \alpha^5$,
- $s_0 = \alpha^6$,
- $s_0 = 0,\ 1,\ \alpha,\ \alpha^2$ oder α^3.

b) Wie lautet bei gleichem Empfangswort das zweite Syndromelement?

- $s_1 = \alpha^4$,
- $s_1 = \alpha^5$,
- $s_1 = \alpha^6$,
- $s_1 = 0,\ 1,\ \alpha,\ \alpha^2$ oder α^3.

c) Wie lautet bei gleichem Empfangswort das dritte Syndromelement?

- $s_2 = \alpha^4$,
- $s_2 = \alpha^5$,
- $s_2 = \alpha^6$,
- $s_2 = 0,\ 1,\ \alpha,\ \alpha^2$ oder α^3.

d) Bekannt ist, dass das vorliegende Empfangswort $\underline{y}$ decodiert werden kann. Wieviele Symbolfehler beinhaltet das Empfangswort?

r =

A2.13: Nun RSC $(7, 3, 5)_8$–Decodierung

In der **Aufgabe A2.12** haben wir den so genannten Petersen–Algorithmus zur Fehlerkorrektur bzw. zur Decodierung des Reed–Solomon–Codes $(7, 4, 4)_8$ angewendet, der aufgrund der Minimaldistanz $d_{\rm min} = 4$ nur einen Symbolfehler korrigieren kann ($t = 1$).

In dieser Aufgabe betrachten wir nun den RSC$(7, 3, 5)_8$ $\Rightarrow$ $d_{\rm min} = 5$ $\Rightarrow$ $t = 2$, dessen Prüfmatrix wie folgt lautet:

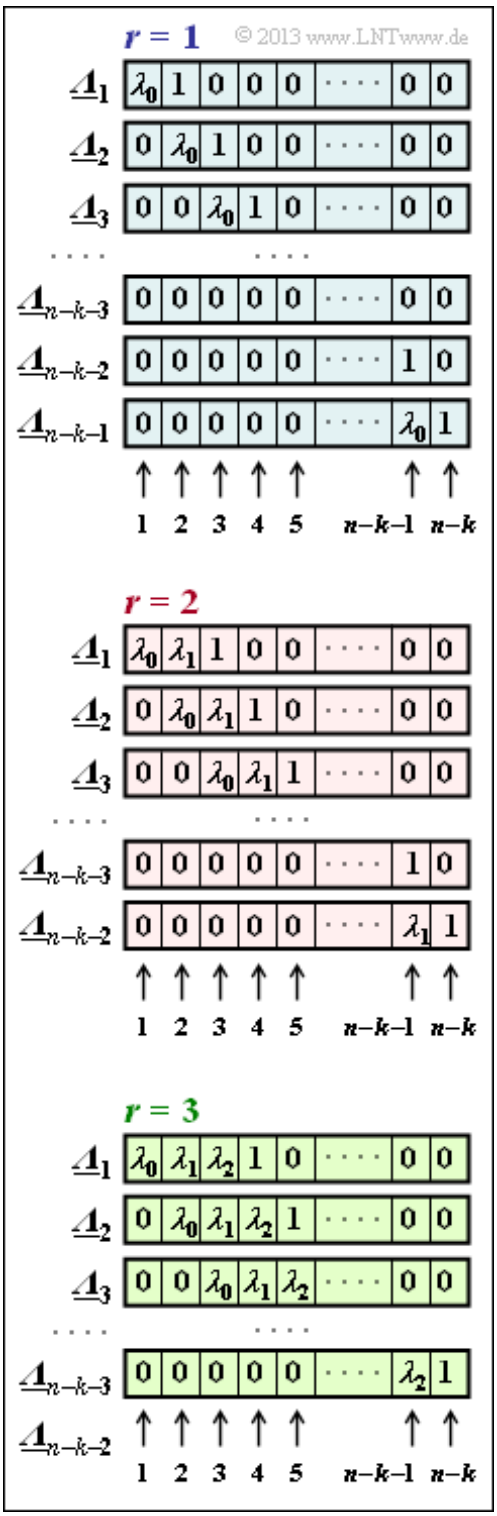
$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\ 1 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Für das betrachtete Empfangswort $\underline{y} = (\alpha^2, \alpha^3, \alpha, \alpha^5, \alpha^4, \alpha^2, 1)$ ergibt sich hier das Syndrom zu $\underline{s} = \underline{y} \cdot \mathbf{H}^{\rm T} = (0, 1, \alpha^5, \alpha^2)$.

Die weitere Vorgehensweise bei der Decodierung geschieht entsprechend den folgenden Theorieseiten:

- Schritt (B): **Bestimmung der Symbolfehleranzahl,**
- Schritt (C): **Lokalisierung der Fehlerpositionen,**
- Schritt (D): **Ermittlung der Fehlerwerte.**

Hinweis: Die Aufgabe gehört zum **Kapitel 2.5.** In obiger Grafik sehen Sie die Belegungen der **ELP–Koeffizienten** $\underline{\Lambda}_l$ unter der Annahme, dass es im Empfangswort $r = 1$, $r = 2$ bzw. $r = 3$ Symbolfehler gibt.



Fragebogen zu "A2.13: Nun RSC $(7, 3, 5)_8$–Decodierung"

a) Welche Belegungsschemata könnten für diese Aufgabe relevant sein?

- ☐ Das blau hinterlegte Schema ($r = 1$).
- ☐ Das rot hinterlegte Schema ($r = 2$).
- ☐ Das grün hinterlegte Schema ($r = 3$).

b) Kann das Syndrom $\underline{s} = (0, 1, \alpha^5, \alpha^2)$ durch einen Symbolfehler entstanden sein?

- ○ JA.
- ○ NEIN.

c) Kann das Syndrom $\underline{s} = (0, 1, \alpha^5, \alpha^2)$ durch zwei Symbolfehler entstanden sein?

- ○ JA.
- ○ NEIN.

d) Welche Symbole des Codewortes wurden also verfälscht?

- ☐ Symbol 0,
- ☐ Symbol 1,
- ☐ Symbol 2,
- ☐ Symbol 3,
- ☐ Symbol 4,
- ☐ Symbol 5,
- ☐ Symbol 6.

e) Wie lautet der Fehlervektor $\underline{e}$? Geben Sie auch das Decodierergebnis $\underline{z}$ an.

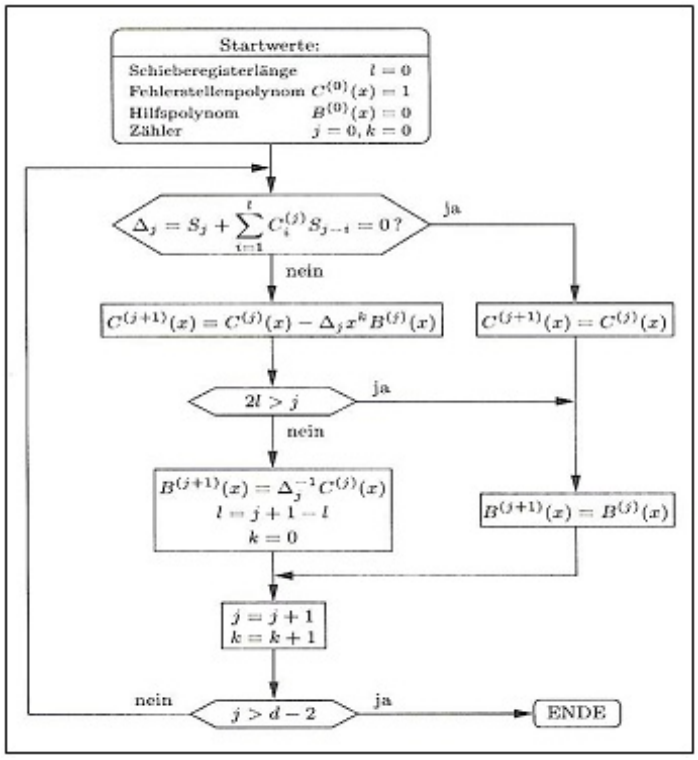
- ☐ $\underline{e} = (1, 0, 0, 0, 0, 0, \alpha^6)$,
- ☐ $\underline{e} = (\alpha^6, 0, 0, 0, 0, 0, 1)$,
- ☐ $\underline{e} = (0, 0, 1, \alpha^6, 0, 0, 0)$,
- ☐ $\underline{e} = (0, 0, \alpha^6, 1, 0, 0, 0)$.

A2.14: Petersen–Algorithmus

Im Theorieteil zu **Kapitel 2.5** haben wir die Decodierung von Reed–Solomon–Codes mit dem *Petersen–Algorithmus* behandelt.

- Dessen Vorteil ist, dass die einzelnen Schritte nachvollziehbar sind.
- Sehr von Nachteil ist aber der immens hohe Decodieraufwand.

Schon seit der Erfindung der Reed–Solomon–Codierung im Jahre 1960 beschäftigten sich viele Wissenschaftler und Ingenieure mit der Entwicklung möglichst schneller Algorithmen zur Reed–Solomon—Decodierung, und auch heute ist die *Algebraische Decodierung* noch ein hochaktuelles Forschungsgebiet.



In dieser Aufgabe sollen einige diesbezügliche Begriffe erklärt werden. Auf eine genaue Erklärung dieser Verfahren wurde in LNTwww verzichtet.

Hinweis: Die Aufgabe bezieht sich auf das **Kapitel 2.5.** Die obige Grafik aus **[Bos98]** zeigt das Flussdiagramm eines der bekanntesten Verfahren zur Decodierung von Reed–Solomon–Codes. Um welchen Algorithmus es sich dabei handelt, wird in der Musterlösung zu dieser Aufgabe genannt.

Fragebogen zu "A2.14: Petersen–Algorithmus"

a) Bei welchen Codes wird die Syndromdecodierung eingesetzt? Bei den

- ☐ binären Blockcodes,
- ☐ Reed–Solomon–Codes,
- ☐ Faltungscodes.

b) Was ist beim Petersen–Algorithmus am aufwändigsten?

- ☐ Überprüfung, ob überhaupt (ein oder mehrere) Fehler vorliegen,
- ☐ die Lokalisierung der Fehler,
- ☐ die Fehlerwertbestimmung.

c) Welche Begriffe beziehen sich auf die Reed–Solomon–Decodierung?

- ☐ Der Berlekamp–Massey–Algorithmus,
- ☐ der BCJR–Algorithmus,
- ☐ der Euklidische Algorithmus,
- ☐ Frequenzbereichsverfahren, basierend auf der DFT,
- ☐ der Viterbi–Algorithmus.

A2.15: Pr($\underline{v} \neq \underline{u}$) vs. E_B/N_0

Am Beispiel des RSC $(7, 3, 5)_8$ mit den Parametern

- $n = 7$ (Anzahl der Codesymbole),
- $k = 3$ (Anzahl der Informationssymbole),
- $t = 2$ (Korrekturfähigkeit)

soll die Berechnung der Blockfehlerwahrscheinlichkeit beim **Bounded Distance Decoding** (BDD) gezeigt werden. Die entsprechende Gleichung lautet:

$$\Pr(\text{Blockfehler}) = \sum_{f=t+1}^{n} \binom{n}{f} \cdot \varepsilon_S{}^f \cdot (1-\varepsilon_S)^{n-f} .$$

Die Berechnung erfolgt für den **AWGN–Kanal,** der durch den Parameter E_B/N_0 gekennzeichnet ist. Dieser Quotient lässt sich über die Beziehung

$$\varepsilon = Q\left(\sqrt{\frac{2 \cdot R \cdot E_B}{N_0}}\right)$$

in das **BSC–Modell** überführen, wobei R die Coderate bezeichnet (hier: $R = 3/7$) und $Q(x)$ das **komplementäre Gaußsche Fehlerintegral** angibt. Da aber beim betrachteten Code die Symbole aus GF(2^3) entstammen, muss das BSC–Modell mit Parameter ε ebenfalls noch an die Aufgabenstellung adaptiert werden. Für die Verfälschungswahrscheinlichkeit des ***m*–BSC–Modells** gilt:

$$\varepsilon_S = 1 - (1-\varepsilon)^m ,$$

wobei hier $m = 3$ zu setzen ist (3 Bit pro Codesymbol).

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	???	???
???	???	???	≈ 0.1	$2.57 \cdot 10^{-2}$
7 dB	5.012	0.0192	0.0565	$5.30 \cdot 10^{-3}$
8 dB	6.310	≈ 0.01	≈ 0.03	???
???	???	???	≈ 0.01	$3.40 \cdot 10^{-5}$
10 dB	10.000	0.0017	≈ 0.005	???
???	???	???	≈ 0.001	$3.49 \cdot 10^{-8}$
12 dB	15.849	0.00012	0.00035	$1.63 \cdot 10^{-9}$

Für einige E_B/N_0–Werte sind alle Ergebnisse bereits in obiger Tabelle eingetragen. Die gelb hinterlegten Zeilen werden hier kurz erläutert.

- Für $10 \cdot \lg E_B/N_0 = 4$ dB ergibt sich $\varepsilon \approx Q(1.47) \approx 0.071$ und $\varepsilon_S \approx 0.2$. Der einfachste Weg zur Berechnung der Blockfehlerwahrscheinlichkeit führt hier über das Komplement:

$$\Pr(\text{Blockfehler}) = 1 - \left[\binom{7}{0} \cdot 0.8^7 + \binom{7}{1} \cdot 0.2 \cdot 0.8^6 + \binom{7}{2} \cdot 0.2^2 \cdot 0.8^5\right] \approx 0.148 .$$

- Für $10 \cdot \lg E_B/N_0 = 12$ dB erhält man $\varepsilon \approx 1.2 \cdot 10^{-4}$ und $\varepsilon_S \approx 3.5 \cdot 10^{-4}$. Mit dieser sehr kleinen Verfälschungswahrscheinlichkeit dominiert der $f = 3$–Term und man erhält

$$\Pr(\text{Blockfehler}) \approx \binom{7}{3} \cdot (3.5 \cdot 10^{-4})^3 \cdot (1 - 3.5 \cdot 10^{-4})^4 \approx 1.63 \cdot 10^{-9} .$$

In dieser Aufgabe sollen Sie für die rot hinterlegten Zeilen ($10 \cdot \lg E_B/N_0 = 5$ dB, 8 dB und 10 dB) die Blockfehlerwahrscheinlichkeiten berechnen.

Die blau hinterlegten Zeilen zeigen einige Ergebnisse der **Zusatzaufgabe Z2.15.** Dort wird Pr($\underline{v} \neq \underline{u}$) für

ε_S = 10%, 1% und 0.1% berechnet. In den Teilaufgaben (d) und (e) sollen Sie den Zusammenhang zwischen dieser Größe ε_S und dem AWGN–Parameter E_B/N_0 herstellen und somit die obige Tabelle vervollständigen.

Hinweis: Die Aufgabe gehört zum **Kapitel 2.6.** Wir weisen Sie auf folgende Interaktionsmodule hin:

Komplementäre Gaußsche Fehlerfunktionen

Wahrscheinlichkeiten der Binominalverteilung

Fragebogen zu "A2.15: Pr($\underline{v} \neq \underline{u}$) vs. E_B/N_0

a) Wie groß ist die Blockfehlerwahrscheinlichkeit für $10 \cdot \lg E_B/N_0 = 5$ dB?

$E_B/N_0 = 5$ dB: Pr(Blockfehler) =

b) Wie groß ist die Blockfehlerwahrscheinlichkeit für $10 \cdot \lg E_B/N_0 = 8$ dB?

$E_B/N_0 = 8$ dB: Pr(Blockfehler) =

c) Wie groß ist die Blockfehlerwahrscheinlichkeit für $10 \cdot \lg E_B/N_0 = 10$ dB?

$E_B/N_0 = 10$ dB: Pr(Blockfehler) =

d) Wie hängt $\varepsilon_S = 0.1$ mit $10 \cdot \lg E_B/N_0$ zusammen? *Hinweis:* Verwenden Sie das angegebene Flash–Modul zur Berechnung von Q(x).

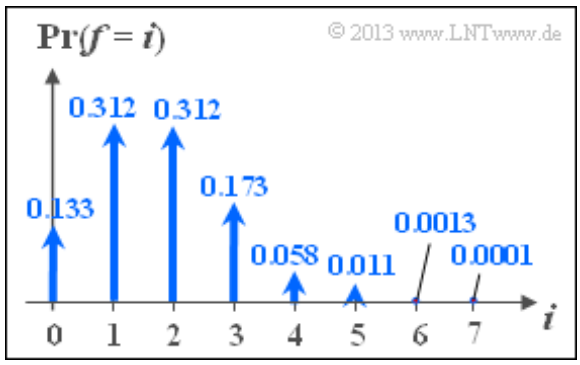
$\varepsilon_S = 0.1$: $10 \cdot \lg E_B/N_0$ = dB

e) Ermitteln Sie auch die E_B/N_0–Werte (in dB) für $\varepsilon_S = 0.01$ und $\varepsilon_S = 0.001$ und vervollständigen Sie die Tabelle.

$\varepsilon_S = 0.01$: $10 \cdot \lg E_B/N_0$ = dB

$\varepsilon_S = 0.001$: $10 \cdot \lg E_B/N_0$ = dB

Z2.15: Nochmals Pr($\underline{v} \neq \underline{u}$) für BDD



Bei Verwendung eines Reed–Solomon–Codes mit der Korrekturfähigkeit t und **Bounded Distance Decoding** (BDD) erhält man mit

- der Codewortlänge n und
- der Symbolverfälschungswahrscheinlichkeit ε_S

für die Blockfehlerwahrscheinlichkeit:

$$\Pr(\text{Blockfehler}) = \sum_{f=t+1}^{n} \binom{n}{f} \cdot {\varepsilon_S}^f \cdot (1-\varepsilon_S)^{n-f} .$$

In dieser Aufgabe soll die Blockfehlerwahrscheinlichkeit für den RSC $(7, 3, 5)_8$ und verschiedene ε_S–Werte berechnet und angenähert werden. Obige Gleichung erinnert an die **Binominalverteilung.** Die Grafik zeigt die Wahrscheinlichkeiten der Binominalverteilung für die Parameter $n = 7$ (Codewortlänge) und $\varepsilon_S = 0.25$ (Symbolverfälschungswahrscheinlichkeit).

Hinweis: Die Aufgabe gehört zum **Kapitel 2.6.** Zur Kontrolle können Sie das folgende interaktive Flash–Modul nutzen:

Wahrscheinlichkeiten der Binominalverteilung

Fragebogen zu "Z2.15: Nochmals Pr($\underline{v} \neq \underline{u}$) für BDD"

a) Welche Blockfehlerwahrscheinlichkeit ergibt sich für $\varepsilon_S = 0.1$?

$\varepsilon_S = 0.1$: Pr(Blockfehler) =

b) Welche Blockfehlerwahrscheinlichkeit ergibt sich für $\varepsilon_S = 0.01$?

$\varepsilon_S = 0.01$: Pr(Blockfehler) =

c) Welches Ergebnis erhält man, wenn man nur den Term $f = t + 1$ berücksichtigt?

Näherung: Pr(Blockfehler) =

d) Welches Ergebnis erhält man näherungsweise für $\varepsilon_S = 10^{-3}$?

$\varepsilon_S = 10^{-3}$: Pr(Blockfehler) =

e) Welches ε_S benötigt man für die Blockfehlerwahrscheinlichkeit 10^{-10}?

Pr(Blockfehler) = 10^{-10}: ε_S =

A2.16: BDD–Entscheidungskriterien

Wir gehen von einem Blockcode der Länge n mit Symbolen $c_i \in \text{GF}(2^m)$ aus, der bis zu t Symbole korrigieren kann. Jedes mögliche Empfangswort $\underline{y}_i$ kann dann als ein Punkt in einem hochdimensionalen Raum angesehen werden. Geht man von der Basis GF(2) = {0, 1} aus, so beträgt die Dimension $n \cdot m$.

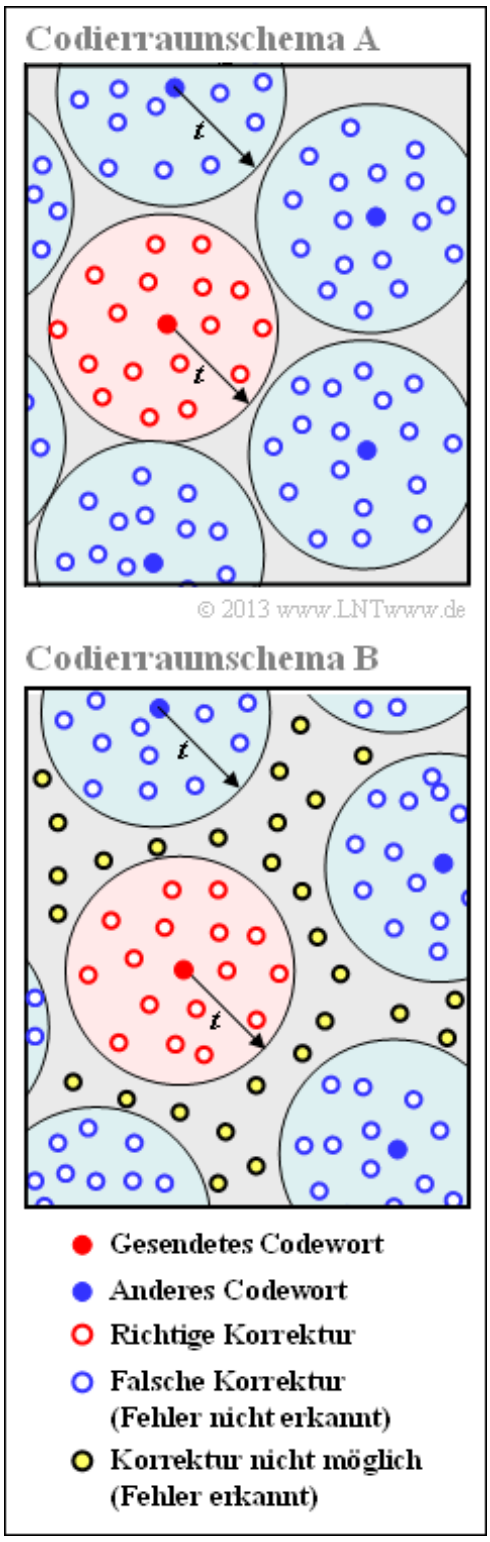
Die Grafik zeigt einen solchen Raum in stark vereinfachender 2–Darstellung. Die Abbildung ist wie folgt zu interpretieren:

- Gesendet wurde der rote Punkt $\underline{c}_j$. Alle rot umrandeten Punkte $\underline{y}_i$ in einer Hyperkugel um diesen Punkt $\underline{c}_j$ mit dem Parameter t als Radius können korrigiert werden. Mit der Nomenklatur gemäß der **Grafik** im Theorieteil gilt dann $\underline{z}_i = \underline{c}_j$ ⇒ „Die Fehlerkorrektur ist erfolgreich”.
- Bei sehr vielen Symbolfehlern kann $\underline{c}_j$ in einen blauen (oder weißblauen) Punkt $\underline{y}_j$ verfälscht werden, der zur Hyperkugel eines anderen Codewortes $\underline{c}_{k \neq j}$ gehört. In diesem Fall trifft der Decoder eine falsche Entscheidung ⇒ „Das Empfangswort $\underline{y}_j$ wird falsch decodiert” .
- Schließlich kann es wie in der unteren Skizze auch noch gelbe Punkte geben, die zu keiner Hyperkugel gehören ⇒ „Das Empfangswort $\underline{y}_j$ ist nicht decodierbar”.

In dieser Aufgabe sollen Sie entscheiden, welches der beiden Coderaumschemata geeignet ist zur Beschreibung der

- **BDD–Decodierung von Hamming–Codes** bzw.
- **BDD–Decodierung von Reed–Solomon–Codes.**

Hinweis: Die Aufgabe ergänzt die Thematik von **Kapitel 2.6** und soll signifikante Unterschiede bei der Decodierung von Reed–Solomon–Codes und Hamming–Codes verdeutlichen.



Fragebogen zu "A2.16: BDD–Entscheidungskriterien"

a) Welches Codierraumschema trifft für die Hamming–Codes zu?

- ○ Codierraumschema **A**,
- ○ Codierraumschema **B**.

b) Welche Aussage gilt für die Wahrscheinlichkeit, dass bei Hamming–Codierung ein Empfangswort $\underline{y}$ nicht decodiert werden kann?

- ☐ Die Wahrscheinlichkeit Pr($\underline{y}$ ist nicht decodierbar) ist exakt 0.
- ☐ Pr($\underline{y}$ ist nicht decodierbar) ist ungleich 0, aber vernachlässigbar.
- ☐ Es gilt Pr($\underline{y}$ ist nicht decodierbar) > Pr($\underline{y}$ wird falsch decodiert).

c) Welches Codierraumschema trifft für die Reed–Solomon–Codes zu?

- ☐ Codierraumschema **A**,
- ☐ Codierraumschema **B**.

d) Welche Aussage gilt für die Wahrscheinlichkeit, dass ein Empfangswort $\underline{y}$ nach Reed–Solomon–Codierung nicht decodiert werden kann?

- ☐ Die Wahrscheinlichkeit Pr($\underline{y}$ ist nicht decodierbar) ist exakt 0.
- ☐ Pr($\underline{y}$ ist nicht decodierbar) ist ungleich 0, aber vernachlässigbar.
- ☐ Es gilt Pr($\underline{y}$ ist nicht decodierbar) > Pr($\underline{y}$ wird falsch decodiert).