# A2.7: Reed–Solomon–Code $(7, 3, 5)_8$

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

© 2013 www.LNTwww.de

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

Die Elemente des zugrunde liegenden Galoisfeldes lauten:

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

Diese Elemente lassen sich entsprechend der Grafik auch als Polynome oder als Koeffizientenvektoren darstellen. Man erkennt aus obiger Tabelle, dass alle $u_i \in \mathrm{GF}(2^3)$ und alle $c_i \in \mathrm{GF}(2^3)$ auch durch $m = 3$ Bit charakterisiert werden können, zum Beispiel $\alpha^4$ 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 $\mathrm{GF}(2^m)$ 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 $\mathrm{GF}(2^3)$ mit Ausnahme des Nullelementes eingesetzt werden:

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

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

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

**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.

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

f) Welche Aussagen gelten für den zweiten Codierschritt?

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

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

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

© 2013 www.LNTwww.de

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.

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

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

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

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

© 2013 www.LNTwww.de

**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 $\alpha^4$, $1$, $\alpha^3$, $0$, $\alpha^6$. 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 $c_6 = \alpha^6$.

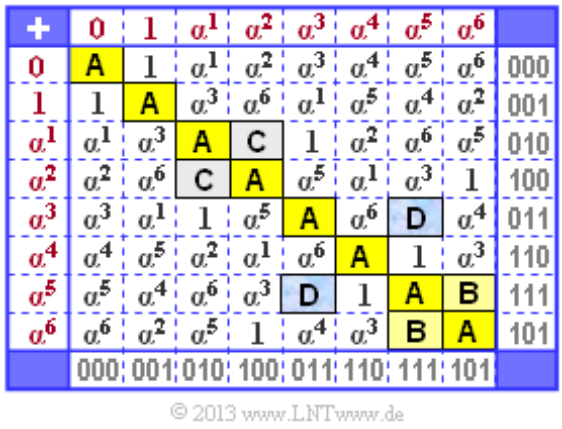
# Z2.8: „Plus" und „Mal" in GF($2^3$)

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

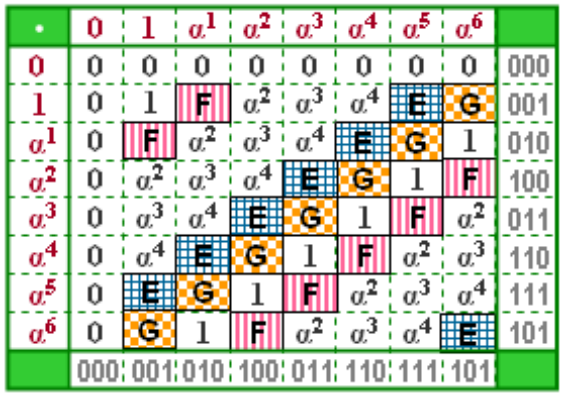
Die Elemente sind sowohl in der Exponentendarstellung (mit roter Beschriftung, links und oben) als auch in der Koeffizientendarstellung (graue Schrift, rechts und unten) angegeben. Aus dieser Zuordnung erkennt man bereits das zugrunde liegende irreduzible Polynom $p(\alpha)$.

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.**




© 2013 www.LNTwww.de



## 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 = $\alpha^1$.

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

- ☐ B = 0,
- ☐ B = 1,
- ☐ B = $\alpha^1$.

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

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

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

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

e) Welche Zuordnungen gelten in der Multiplikationstabelle?

- ☐ E = $\alpha^5$,
- ☐ F = $\alpha^1$,
- ☐ G = $\alpha^6$.

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)$_2$ |

© 2013 www.LNTwww.de

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?

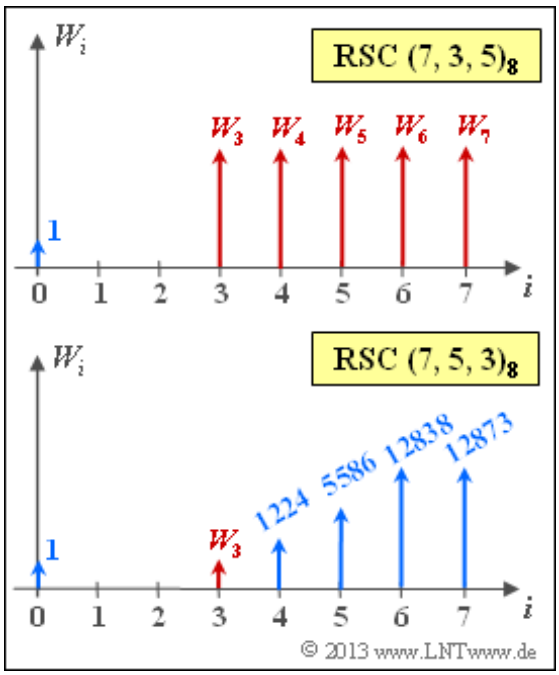
**mit RSC 1: $e$ =**

**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):** $p_{\rm oben}$ =

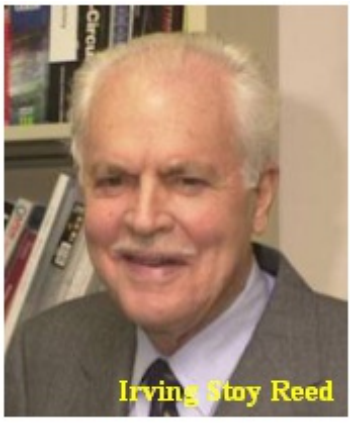
**RSC (7, 5, 3):** $p_{\rm oben}$ =

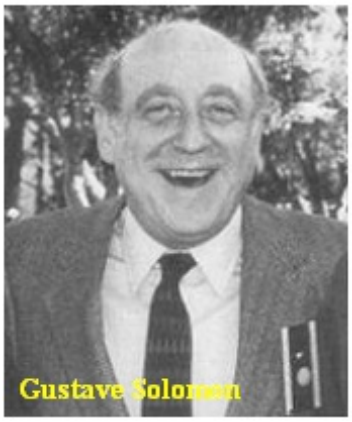
e) Berechnen und bewerten Sie für beide Codes die in der Angabe vorgeschlagene untere Schranke $p_{\rm unten}$ = Pr(Untere Schranke).

**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: $N_{\rm Bitfehler}$** =