Lösung zu Aufgabe 9

Betrachtet wird: RS $(4,2)$ über **GF**(5)
Allgemein: RS (n,k) über **GF**(p^m)

9.1 $\mathbf{r} = \mathbf{a} + \mathbf{f}$ (modulo $p \overset{\text{hier}}{=}$ modulo 5)
r ist der Empfangsvektor im Zeitbereich

$$\begin{aligned} \Longrightarrow \mathbf{r} &= (\,0\,3\,4\,1\,) + (\,0\,0\,3\,0\,) \\ &= (\,0\,3\,7\,1\,) \quad \text{(ohne modulo 5)} \\ &= (\,0\,3\,2\,1\,) \end{aligned}$$

Transformation **r** in den Frequenzbereich (DFT)

$$\mathbf{r} \circ\!\!-\!\!\bullet\ \mathbf{R}$$

$$\begin{aligned} \mathbf{R}^{\mathrm{T}} &= \mathbf{M}_{\mathrm{DFT}} \cdot \mathbf{r}^{\mathrm{T}} \\ &= \underbrace{\begin{pmatrix} 4 & 4 & 4 & 4 \\ 4 & 2 & 1 & 3 \\ 4 & 1 & 4 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix}}_{\mathbf{M}_{\mathrm{DFT}}\text{, berechnet in Aufgabe 8}} \cdot \begin{pmatrix} 0 \\ 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0+2+3+4 \\ 0+1+2+3 \\ 0+3+3+1 \\ 0+4+2+2 \end{pmatrix} \\ &= \begin{pmatrix} 4 \\ 1 \\ 2 \\ 3 \end{pmatrix} \\ \Longrightarrow \mathbf{R} &= (\,4\ \ 1\ \vdots\ 2\ \ 3\,) \end{aligned}$$

Ohne Fehler:

$$\mathbf{R} = (\,\underbrace{\mathrm{A}_0\ \ \mathrm{A}_1}_{\substack{\text{Informations-}\\ \text{wortlänge } k}}\ \vdots\ \underbrace{0\ \ 0}_{\substack{\text{“Prüffrequenzen”}\\ \text{Länge } n-k}}\,)$$

Hier (ohne Fehler):

$$\mathbf{R} = (\,4\ \ 1\ \vdots\ \underbrace{2\ \ 3}_{\mathbf{S}}\,) \qquad \mathbf{S} = \underbrace{(\,S_0\ \ S_1\,)}_{n-k=2} = (\,2\ \ 3\,)$$

Allgemein: $\mathbf{R} = \mathbf{A} + \mathbf{F}$
$\mathbf{A} \mathrel{\hat{=}}$ Codewort im Frequenzbereich
A besteht aus 0 in den letzten $(n-k)$ Stellen
$\Longrightarrow$ **S** besteht aus den letzten $(n-k)$ Stellen von **R**
$\mathrel{\hat{=}}$ die letzten $(n-k)$ Stellen von **F**

$\Longrightarrow \mathbf{S} = \mathbf{0} \implies$ fehlerfreies Codewort
$\mathbf{S} \neq \mathbf{0} \implies$ fehlerbehaftetes Empfangswort

9.2 Fehlerstellenpolynom $c(x) \circ\!\!-\!\!\bullet\, C(x)$

Zeitbereich: $c_i \cdot f_i = 0 \Longrightarrow c_i = 0$ falls $f_i \neq 0$

$\Longrightarrow c_i = 0$ falls Fehler an Position i

Frequenzbereich: $C(x) \cdot F(x) = 0 \bmod (x^n - 1)$
$\Rightarrow x = z^i$ (z ist primitives Element) ist Nullstelle, falls Fehler an Position i auftritt
$\Rightarrow C(x) = \prod_{i, f_i \neq 0} (x - z^i)$

Bestimmung der Koeffizienten von $C(x) = C_0 + \cdots + C_e \cdot x^e$ (Grad e)
e ist Anzahl von Fehlern
$t = 1$ Fehler können korrigiert werden
Annahme: $e \leq t$

Matrix-Darstellung:

$$\underbrace{\left\{ \begin{pmatrix} S_e & \cdots & S_0 \\ \vdots & \ddots & \vdots \\ S_{2t-1} & \cdots & S_{2t-e-1} \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ \vdots \\ C_e \end{pmatrix} \right\}_{e+1}^{2t-e} \overset{!}{=} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{e+1} \qquad (*)$$

Gleichung ist erfüllt für korrektes e (unbekannt)

Da e unbekannt ist
$\Longrightarrow$ Mit dem wahrscheinlichsten Fall anfangen: $e = 1$

$t = 1 \Longrightarrow$ Index des linken Elements in der letzten Matrixzeile: $2t - 1 = 1$
Index des rechten Elements in der letzten Matrixzeile: $2t - e - 1 = 0$

$$\Longrightarrow \quad \left(S_1 S_0\right) \cdot \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} = 0$$

$$\Longrightarrow \quad S_1 \cdot C_0 + S_0 \cdot C_1 = 0$$

$$\Longrightarrow \quad 3 \cdot C_0 + 2 \cdot C_1 = 0 \quad \text{(unterbestimmt, 1 Gleichung und 2 Variablen)}$$

$\Longrightarrow$ Normiere $C(x)$: z.B. $C_1 = 1$
$C(x)$ ist immer normierbar, nur Nullstellen sind wichtig.

$$\begin{aligned} \Longrightarrow \quad 3 \cdot C_0 + 2 &= 0 && \mid -2 \quad \hat{=}\ +3 \text{ (Inverses Element)} \\ \Longrightarrow \quad 3 \cdot C_0 &= 3 && \mid \cdot 3^{-1} \quad \hat{=}\ \cdot 2 \text{ (Inverses Element)} \\ \Longrightarrow \quad C_0 &= 6 \bmod 5 \\ &= 1 \end{aligned}$$

$\Longrightarrow C(x) = 1 + 1 \cdot x$

falls die Matrixgl. $(*)$ nicht lösbar ist für $e = 1 \Longrightarrow$ versuche $e = 2, 3, 4, \ldots, t$
falls die Matrixgl. $(*)$ nicht lösbar ist $\Longrightarrow$ keine Korrektur möglich

Fehlerstellen:

$$C(x = z^i) = 0 \Longleftrightarrow \text{ Fehlerstelle } i$$

$$(\, i = 0 \cdots n-1, \quad \underbrace{z = 2}_{\text{Primitives Element}} \,)$$

$\Longrightarrow$ $C(z^0 = 1) = 2 \neq 0$
$C(z^1 = 2) = 3 \neq 0$
$C(z^2 = 4)[= 5] = 0 \pmod 5 \Longrightarrow$ Fehler an Position $i = 2$
$C(z^3 = 3) = 4 \neq 0$ (zwangsläufig, da Einzelfehler angenommen wurde, $e = 1$)
Position ist nun bekannt, der Wert allerdings noch nicht!

9.3 Fehlervektor im Frequenzbereich:

$$\begin{array}{rcl} \mathbf{r} & = & \mathbf{a} + \mathbf{f} \\ \circ\!\!\downarrow & & \\ \mathbf{R} & = & \mathbf{A} + \mathbf{F} \end{array}$$

A ist 0 in den letzten $(n-k)$ Stellen
$\Longrightarrow$ **R** und **F** sind identisch in den letzten $(n-k)$ Stellen
(ist gleich **S**, s.o.)

$$\Longrightarrow \mathbf{F} = (F_0 \quad F_1 \quad \vdots \quad \underbrace{F_2 \quad F_3}_{n-k=2})$$

$$= (F_0 \quad F_1 \quad \vdots \quad S_0 \quad S_1) = (\underbrace{F_0 \quad F_1}_{k=2} \quad \vdots \quad 2 \quad 3)$$

Rekursive Bestimmung der „linken“ Elemente F_j

$$F_j = -(C_0^{-1}) \cdot \sum_{i=1}^{e} C_{i \bmod n} \cdot F_{(j-i) \bmod n} \qquad j = 0 \cdots k-1$$

$$\begin{aligned}
\Longrightarrow F_0 &= -(C_0^{-1}) \cdot C_{1 \bmod 4} \cdot F_{(0-1) \bmod 4} \\
&= -(1^{-1}) \cdot C_1 \cdot F_{(-1) \bmod 4} \\
&= -(1) \cdot C_1 \cdot F_{3 \bmod 4} \\
&= -(1) \cdot C_1 \cdot F_3 \\
&= 4 \cdot 1 \cdot 3 \\
&[= 12] \\
&= 2
\end{aligned} \quad \Big\} x \bmod y = (x+y) \bmod y$$

$$\begin{aligned}
F_1 &= -(C_0^{-1}) \cdot C_{1 \bmod 4} \cdot F_{(1-1) \bmod 4} \\
&= 4 \cdot 1 \cdot 3 \\
&= 3 \\
\Longrightarrow \mathbf{F} &= (2 \quad 3 \quad 2 \quad 3)
\end{aligned}$$

9.4

$$\begin{aligned}
\hat{\mathbf{A}} = \mathbf{R} \text{“}-\text{”} \mathbf{F} &= (4 \quad 1 \quad 2 \quad 3) - (2 \quad 3 \quad 2 \quad 3) \\
\text{(modulo 5)} & \\
&= (4 \quad 1 \quad 2 \quad 3) + (3 \quad 2 \quad 3 \quad 2) \\
&[= (7 \quad 3 \quad 5 \quad 5)] \\
&= (2 \quad 3 \quad 0 \quad 0)
\end{aligned}$$