Lösung zu Aufgabe 7

7.1 $n = 7 \Longrightarrow 7$ Codewortstellen

Allgemein gilt: $g(x) = g_0 + g_1 \cdot x + g_2 \cdot x^2 + g_3 \cdot x^3 + \cdots + g_{n-k} \cdot x^{n-k}$

Hier: $g(x) = 1 + x + x^3 = 1 + 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3$

$$\Longrightarrow g_0 = 1, \quad g_1 = 1, \quad g_2 = 0, \quad g_3 = 1$$

7 Codewortstellen $\Longrightarrow g_4 = 0,\ g_5 = 0,\ g_6 = 0$

$$\Longrightarrow \quad \begin{array}{ccccccc} g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \end{array}$$
$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \mathbf{G}$$

7.2

$$\begin{aligned}
\mathbf{u}_\mathrm{a} &= (\,0\,1\,1\,0\,) \\
\Longrightarrow \mathbf{c}_\mathrm{a} &= \mathbf{u}_\mathrm{a} \cdot \mathbf{G} \\
&= (\,0\,1\,1\,0\,) \cdot \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \\
&= (\,0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\,) \\
\mathbf{u}_\mathrm{b} &= (\,1\,0\,1\,0\,) \\
\Longrightarrow \mathbf{c}_\mathrm{b} &= \mathbf{u}_\mathrm{b} \cdot \mathbf{G} \\
&= (\,1\,0\,1\,0\,) \cdot \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \\
&= (\,1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\,)
\end{aligned}$$

7.3 Konversion zur Polynomdarstellung:

$$\text{Vektor} \quad \mathbf{u}_\mathrm{a} = (\ \underset{x^0}{0}\ \ \underset{x^1}{1}\ \ \underset{x^2}{1}\ \ \underset{x^3}{0}\ ) = \underbrace{(\ u_0\ \ u_1\ \ u_2\ \ u_3\ )}_{\text{Länge } \mathrm{k=4}}$$

$$\text{In Polynomdarstellung} \Longrightarrow u_a(x) = \overbrace{u_0 \cdot x^0 + u_1 \cdot x^1 + u_2 \cdot x^2 + u_3 \cdot x^3}^{\text{Grad des Polynoms } k-1}$$
$$= 0 \cdot x^0 + 1 \cdot x^1 + 1 \cdot x^2 + 0 \cdot x^3$$
$$= x + x^2$$

$$\text{Vektor} \quad \mathbf{u}_b = (\ 1 \quad 0 \quad 1 \quad 0\ ) = (\ u_0 \quad u_1 \quad u_2 \quad u_3\ )$$

$$\text{In Polynomdarstellung} \Longrightarrow u_b(x) = u_0 \cdot x^0 + u_1 \cdot x^1 + u_2 \cdot x^2 + u_3 \cdot x^3$$
$$= 1 + 0 \cdot x^1 + 1 \cdot x^2 + 0 \cdot x^3$$
$$= 1 + x^2$$

Codieren bedeutet Multiplizieren des Informationspolynoms mit dem Generatorpolynom

$$\begin{aligned} \Longrightarrow c(x) &= u(x) \cdot g(x) \\ \Longrightarrow c_a(x) &= u_a(x) \cdot g(x) \\ &= (x + x^2) \cdot (1 + x + x^3) \\ &= x \cdot (1 + x + x^3) + x^2 \cdot (1 + x + x^3) \end{aligned}$$

Die Summation $x \cdot (1 + x + x^3) + x^2 \cdot (1 + x + x^3)$ wird binär durchgeführt:

$$\begin{array}{cccccccccccc} & x & + & x^2 & + & & & x^4 & & & \\ & & & x^2 & + & x^3 & + & & & x^5 \\ \hline = & x & + & & & x^3 & + & x^4 & + & x^5 \end{array}$$

Modulo 2 Summation
$(1 + 1 = 0)$

$$\begin{aligned} \Longrightarrow \quad c_a &= x + x^3 + x^4 + x^5 \\ &= 0 + 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3 + 1 \cdot x^4 + 1 \cdot x^5 + 0 \cdot x^6 \\ &= c_{a,0} + c_{a,1} \cdot x^1 + c_{a,2} \cdot x^2 + c_{a,3} \cdot x^3 + c_{a,4} \cdot x^4 + c_{a,5} \cdot x^5 + c_{a,6} \cdot x^6 \end{aligned}$$

! (Grad des Polynoms: $n - 1 = 6$) !

$$\begin{aligned} \Rightarrow c_a &= (\ c_{a,0}\ c_{a,1}\ c_{a,2}\ c_{a,3}\ c_{a,4}\ c_{a,5}\ c_{a,6}\ ) \\ &= (\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ ) \end{aligned}$$

$$\begin{aligned} c_b(x) &= u_b(x) \cdot g(x) \\ &= (1 + x^2) \cdot (1 + x + x^3) \\ &= 1 \cdot (1 + x + x^3) + x^2 \cdot (1 + x + x^3) \end{aligned}$$

$$\begin{array}{cccccccccccc} & 1 & + & x & + & & & x^3 & & & \\ & & & & & x^2 & + & x^3 & + & x^5 \\ \hline = & 1 & + & x & + & x^2 & + & & & x^5 \end{array}$$

$= 1+1\cdot x+1\cdot x^2+0\cdot x^3+0\cdot x^4+1\cdot x^5+0\cdot x^6$

$\Rightarrow c_\mathrm{b} = (\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ )$
Nicht-systematische Codierung: $c(x) = u(x)\cdot g(x)$

7.4 Systematische Codierung
1.) Multipliere $u(x)$ mit x^{n-k} ($n-k$ Grad des Generatorpolynoms)
2.) Führe eine Polynomdivision durch mit $g(x)$
$(u(x)\cdot x^{n-k}) : g(x) = q(x) + \frac{r(x)}{g(x)}$
3.) Addiere Rest $r(x)$
$\Rightarrow$ Codewort: $c_\mathrm{b}(x) = u(x)\cdot x^{n-k} + r(x)$
$\Rightarrow g(x)$ ist ganzzahlig teilbar durch $c(x)$

$$c_\mathrm{b}(x) \hat{=} \mathbf{c}_\mathrm{b} = (\ \mathbf{r} \vdots \mathbf{u}_\mathrm{a}\ )$$

$\underline{u_\mathrm{a} = (\ 0\ 1\ 1\ 0\ )}$

1.) $x^{n-k} = x^{7-4} = x^3$
$u_\mathrm{a}(x)\cdot x^{n-k} = u_\mathrm{a}(x)\cdot x^3 = (x+x^2)\cdot x^3$
$= x^4+x^5$

2.) $u_\mathrm{a}(x)\cdot x^{n-k} : g(x)$

$$\begin{array}{lllllllllll}
 & (x^5 & + & x^4) & : & (x^3 & + & & x & + & 1) = x^2+x+1+\frac{1}{x^3+x+1} \\
+ & (x^5 & + & & & x^3 & + & x^2) & \ldots\ldots\ldots\ldots\ldots & & x^2\cdot(x^3+x+1) \\ \hline
 & 0 & + & x^4 & + & x^3 & + & x^2 & & & \\
 & & & x^4 & + & & & x^2 & + & x & \ldots\ldots\ x\cdot(x^3+x+1) \\ \hline
 & & & 0 & + & x^3 & + & 0 & + & x & \\
 & & & & & x^3 & + & & x & + & 1\cdots\ 1\cdot(x^3+x+1) \\ \hline
 & & & & & 0 & + & & 0 & + & 1\cdots\ r(x)
\end{array}$$

3.) $c_{\mathrm{a,s}}(x) = u_\mathrm{a}(x)\cdot x^{n-k} + r(x)$
$= 1+x^4+x^5$
$= 1+0\cdot x+0\cdot x^2+0\cdot x^3+1\cdot x^4+1\cdot x^5+0\cdot x^6$

$$\Rightarrow \mathbf{c}_{\mathrm{a,s}} = (\underbrace{1\ 0\ 0}_{\hat{=} r(x)} \vdots \underbrace{0\ 1\ 1\ 0}_{\hat{=} u_\mathrm{a}(x)})$$

$\underline{u_\mathrm{b} = (\ 1\ 0\ 1\ 0\ )}$

1.) $u_\mathrm{b}(x)\cdot x^{n-k} = (1+x^2)\cdot x^3$
$= x^3+x^5$

2.) $u_\mathrm{b}(x)\cdot x^{n-k} : g(x)$

$$\begin{array}{lllllll}
 & (x^5 & + & x^3) & : & (x^3 + x + 1) & = x^2+\frac{x^2}{x^3+x+1} \\
+ & (x^5 & + & x^3 & + & x^2) & \\ \hline
 & & & & & x^2 & = r(x)
\end{array}$$

3.) $c_{\mathrm{b,s}}(x) = u_{\mathrm{b}}(x) \cdot x^{n-k} + r(x)$
$\quad = x^2 + x^3 + x^5$
$\quad = 0 + 0 \cdot x + 1 \cdot x^2 + 1 \cdot x^3 + 0 \cdot x^4 + 1 \cdot x^5 + 0 \cdot x^6$

$\Rightarrow \mathbf{c}_{\mathrm{b,s}} = (\underbrace{0\,0\,1}_{\hat{=}r(x)} \,\vdots\, \underbrace{1\,0\,1\,0}_{\hat{=}u_{\mathrm{b}}(x)})$

7.5 Zyklische Codes: Die Codewortlänge n ist gleich der Periode r des Generatorpolynoms, wobei r die kleinste ganze Zahl ist mit

$$\begin{aligned} x^r + 1 &= 0 \bmod g(x) \\ \Longrightarrow x^r + 1 : g(x) &= h(x) \text{ ohne Rest} \end{aligned}$$

Bestimmung von r durch Umkehrung der Polynomdivision:

$$\begin{array}{ccccccccccccccc|l} & & & & & & & & x^3 & + & 0 & + & x & + & 1 & = g(x) \cdot 1 \\ & & & & & & x^4 & + & 0 & + & x^2 & + & x^1 & & & = g(x) \cdot x \\ & & & & x^5 & + & 0 & + & x^3 & + & x^2 & & & & & = g(x) \cdot x^2 \\ x^7 & + & 0 & + & x^5 & + & x^4 & & & & & & & & & = g(x) \cdot x^4 \\ \hline x^7 & + & 0 & + & 0 & + & 0 & + & 0 & + & 0 & + & 0 & + & 1 & = x^7 + 1 \\ & & & & & & & & & & & & & & & \Rightarrow r = 7 \end{array}$$

Beweis: $(x^7 + 1) : (x^3 + x + 1) = \underbrace{x^4 + x^2 + x + 1}_{h(x)}$

$$\begin{array}{ccccccccccccccc} x^7 & + & & & x^5 & + & x^4 & & & & & & & & \\ \hline & & & & x^5 & + & x^4 & + & & & & & & & 1 \\ & & & & x^5 & + & & & x^3 & + & x^2 & & & & \\ \hline & & & & & & x^4 & + & x^3 & + & x^2 & + & & & 1 \\ & & & & & & x^4 & + & & & x^2 & + & x & & \\ \hline & & & & & & & & x^3 & + & & & x & + & 1 \\ & & & & & & & & x^3 & + & & & x & + & 1 \\ \hline & & & & & & & & & & & & & & 0 \end{array}$$

Einfacher: Betrachtung ausschließlich der Koeffizienten:
(Ziel: 1 0 0 0 0 0 0 1)

$$\begin{array}{cccccccc} x^7 & x^6 & x^5 & x^4 & x^3 & x^2 & x^1 & x^0 \\ & & & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 1 & 1 & \\ & & 1 & 0 & 1 & 1 & & \\ 1 & 0 & 1 & 1 & & & & \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \; \hat{=} x^7 + 1$$

Anzahl der Informationsstellen k :

$$\begin{aligned} \text{Grad von } g(x) &= n - k = 3 \\ \Longrightarrow k &= n - \text{ Grad von } g(x) \\ &= 7 - 3 = 4 \end{aligned}$$