Aufgabe 24: Decodieren des negazyklischen $[5, 3, 5]$ Codes über $GF(11)$.

$g(x) = (x-2)(x-2^3)$ ← Generatorpolynom

$\alpha = 2$ (prim. Element von $GF(11)$)

1.) Decodieren von $r(x) = -x + x^3$ (← d.h. $c(x)=0$)

$S_1 = r(\alpha) = -2 + 2^3 = 6$

$S_3 = r(\alpha^3) = -8 + 8^3 \equiv 9 \bmod 11$

$\Rightarrow \tilde{S}(z) = 6z + 9z^3$

$u_1 = -S_1 = 5$

$u_3 = \frac{-S_3 + u_1^2 S_1}{3}$

$\curvearrowright u_3 = 3$

$U(z) = 5z + 3z^3$

$$1 + T(z^2) = \frac{1}{1 + z\,U(z)} = \frac{1}{1 + 5z^2 + 3z^4} = \frac{1}{1 - (-5z^2 - 3z^4)}$$

$$1 + T(z^2) = 1 + (-5z^2 - 3z^4) + (-5z^2 - 3z^4)^2 + \dots$$

$$1 + T(z^2) = 1 + 6z^2 + \underbrace{8z^4 + 3z^4}_{=0 \bmod 11} + z^6(\dots)$$

$$1 + T(z) = 1 + 6z + z^3(\dots)$$

$$\omega(z) = \phi(z) \cdot (1 + 6z) \bmod z^3$$

Grad $\omega \le \frac{t}{2} = 1$

Grad $\phi \le \frac{t+1}{2}$

$\Rightarrow$ Grad $\phi \le 1$

$$z^3 = 1 \cdot z^3 + 0 \cdot (6z+1)$$

$$6z+1 = 0 \cdot z^3 + 1 \cdot (6z+1)$$

$$\Rightarrow \underbrace{6z+1}_{\omega} \equiv \underbrace{1}_{\phi} \cdot (6z+1) \bmod z^3$$

$$\left.\begin{aligned}\phi(z) &= 1\\ \omega(z) &= 6z+1\end{aligned}\right\} \Rightarrow \begin{aligned}\hat{\sigma}(z) &= \omega(z^2)\\ \overset{S}{\sigma}(z) &= (\phi(z^2) - \overset{1}{\sigma}(z))/z\end{aligned}$$

$$\overset{1}{\sigma}(z) = 6z^2+1$$

$$\overset{S}{\sigma}(z) = (1-(6z^2+1))/z = 5z$$

$$\Rightarrow \quad \sigma(z) = 6z^2+5z+1$$

z	$\sigma(z) = 6z^2+5z+1$
0	1
1	1
2	$24+10+1 \equiv 3 \mod 11$
3	$54+15+1 \equiv 4 \mod 11$
4	$30+20+1 \equiv 7 \mod 11$
5	$18+3+1 \equiv 0 \mod 11$ ←
6	$18+30+1 \equiv 5 \mod 11$
7	$30+2+1 \equiv 0 \mod 11$ ←

i	α^i
0	1
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6

NS: $5 = \alpha^4 \Rightarrow -4 \equiv 6 \Rightarrow$ Position 1 Wert -1

$7 = \alpha^7 \Rightarrow -7 \equiv 3$ " 3 " $+1$

$$\Rightarrow \quad \underline{e(x) = -x + x^3} \quad \Rightarrow c(x) = 0$$

2. Decodieren von $r(x) = 2x^2$

$S_1 = 2\alpha^2 = 8$

$S_3 = 2(\alpha^3)^2 = 2 \cdot 64 \equiv 7 \bmod 11$

$\Rightarrow \overset{n}{S}(z) = 8z + 7z^3$

$\begin{cases} u_1 = -S_1 = 3 \\ u_3 = \frac{-S_3 + u_1^2 S_1}{3} = 7 \end{cases}$

$u(z) = 3z + 7z^3$

$$1 + T(z^2) = \frac{1}{1 + 3z^2 + 7z^4} = \frac{1}{1 - (-3z^2 - 7z^4)} = 1 + (-3z^2 - 7z^4) + ()^2 \ldots$$

$$1 + T(z^2) = 1 + 8z^2 + 2z^4 + z^6(\ldots)$$

$$1 + T(z) = 1 + 8z + 2z^2 + z^3(\ldots)$$

$$\omega(z) \equiv \phi(z) \cdot (2z^2 + 8z + 1) \bmod z^3$$

$$z^3 = 1 \cdot z^3 + 0 \cdot (2z^2 + 8z + 1)$$

$$2z^2 + 8z + 1 = 0 \cdot z^3 + 1 \cdot (2z^2 + 8z + 1)$$

$$10z + 2 = 1 \cdot z^3 + (5z + 2)(2z^2 + 8z + 1)$$

$$\Rightarrow \underbrace{10z + 2}_{\omega(z)} \equiv \underbrace{(5z + 2)}_{\phi(z)} \cdot (2z^2 + 8z + 1) \bmod z^3$$

$\overset{3}{G}(z) = \omega(z^2) = 10z^2 + 2$

$\overset{5}{G}(z) = \frac{\phi(z^2) - \hat{G}(z)}{z} = \frac{5z^2 + 2 - 10z^2 - 2}{z} = 6z$

$\Rightarrow \underline{G(z)} = \overset{n}{G}(z) + \hat{G}(z) = \underline{10z^2 + 6z + 2}$

Position

$G(z)$: Doppelte NS bei 3: $3 = \alpha^8 \quad -8 \equiv 2 \bmod 10$

$0 \le 2 \le 4$ ⇓ wert 1

$\Rightarrow e(x) = 2x^2$

$\Rightarrow C(x) = 0$

3.) Decodieren von $r(x) = -2x$

$$S_1 = -2 \cdot 2 = -4 \equiv 7 \bmod 11$$

$$S_3 = -2 \cdot 2^3 = -16 \equiv 6 \bmod 11$$

$$\tilde{S}(z) = 7z + 6z^3$$

$$U(z) = 4z + 6z^3$$

$$\Leftarrow \begin{cases} u_1 = -S_1 \equiv 4 \\ u_3 = -\frac{S_3 + u_1^2 S_1}{3} = 6 \end{cases}$$

$$1 + T(z^2) = \frac{1}{1 + zU(z)} = \frac{1}{1 - (-4z^2 - 6z^4)} = 1 + (7z^2 + 5z^4) + (\ldots)^2 + \ldots$$

$$1 + T(z^2) = 1 + 7z^2 + 5z^4 + 5z^4 + z^6(\ldots)$$

$$1 + T(z) = 1 + 7z + 10z^2 + z^3(\ldots)$$

$$\omega(z) \equiv \phi(z)\,(10z^2 + 7z + 1) \bmod z^3$$

$$z^3 = 1 \cdot z^3 + 0 \cdot (10z^2 + 7z + 1)$$

$$10z^2 + 7z + 1 = 0 \cdot z^3 + 1 \cdot (10z^2 + 7z + 1)$$

$$6z + 7 = 1 \cdot z^3 + (z + 7) \cdot (10z^2 + 7z + 1)$$

$$\Rightarrow \underbrace{6z + 7}_{\omega(z)} \equiv \underbrace{(z + 7)}_{\phi(z)} (10z^2 + 7z + 1) \bmod z^3$$

$$\hat{G}(z) = \omega(z^2) = 6z^2 + 7$$

$$\tilde{G}(z) = \frac{\phi(z^2) - \hat{G}(z)}{z} = \frac{z^2 + 7 - 6z^2 - 7}{z} = 6z$$

$$\Rightarrow G(z) = 6z^2 + 6z + 7$$

$\mod p-1$ (10 → 6)

$G(z)$: Doppelte NS bei 5 : $5 = \alpha^4$ $\quad -4 \equiv 6 \rightarrow$ Pos. 1

Wert -1

$$\Rightarrow e(x) = -2 \cdot X$$

$$\Rightarrow C(x) = 0$$

Hinweis: Quadratische Gleichungen mod p können mit der "gängigen" quadratischen Lösungsformel gelöst werden.

Das Wurzelziehen mod p ist besonders einfach für $p \equiv 3 \bmod 4$.

Die Gleichung $x^2 \equiv a \bmod p$

hat dann (falls sie in GF(p) liegen) die Lösungen

$$x = \pm\sqrt{a} \equiv \pm a^{\frac{p+1}{4}} \bmod p.$$

Beweis: Wenn $\pm x$ in GF(p) liegt gilt

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv \underbrace{x^{p-1}}_{=1 \text{ für } x \neq 0} \bmod p$$

$$\Rightarrow \left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}+1} = a \bmod p. \checkmark$$

Aufgabe 25: Zeigen Sie $\underline{c}_a \cdot \underline{c}_b^T = 0$

mit $\underline{c}_a \in \mathcal{C}$ und $\underline{c}_b \in \mathcal{C}^\perp$

$\underline{G}$: Generatormatrix von $\mathcal{C}$ ($k \times n$ Matrix)

$\underline{H}$: Prüfmatrix von $\mathcal{C}$ ($(n-k) \times n$ Matrix)

$\underline{c}_a = \underline{m}_a \cdot \underline{G}$ $\quad \underline{m}_a : 1 \times k$

$$\underline{H} \cdot \underline{c}_a^T = \underline{0}$$

$\underline{H}$ ist Generatormatrix des dualen Codes $\mathcal{C}^\perp$.

$\underline{c}_b = \underline{m}_b \cdot \underline{H}$ $\quad \underline{m}_b : 1 \times (n-k)$

$$\Rightarrow \underline{m}_b \cdot \underline{H} \cdot \underline{c}_a^T = 0$$

$$\underline{c}_b \cdot \underline{c}_a^T = 0$$

$$\curvearrowright \underline{c}_a \cdot \underline{c}_b^T = 0 .$$

Aufgabe 26: Darstellen von $c(x) \cdot h(x) = 0 \bmod x^n - 1$ in Matrixform ($c(x) = \sum_{i=0}^{n-1} c_i x^i$, $h(x) = \sum_{i=0}^{k} h_i x^i$).

$$\searrow \quad \sum_{j=0}^{n-1} c_j \, h_{i-j} = 0 \qquad \leftarrow \text{Indizes mod } n$$

$$\Rightarrow \begin{pmatrix} h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & & & \ddots & \ddots & & & 0 \\ 0 & 0 & h_k & & & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & h_k & h_{k-1} & \cdots & \cdots & h_0 & \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ \\ c_{n-1} \end{pmatrix} = \underline{0}$$

Aufgabe 27: Generatorpolynom des zu dem $[7, 4, 3]$ Hamming-Codes dualen Codes. ($g(x) = x^3 + x + 1$).

$$x^7 + 1 = g(x) \cdot h(x) \quad \Rightarrow (x^7 + 1) : g(x) = \underbrace{x^4 + x^2 + x + 1}_{h(x)}$$

$\Rightarrow$ Generatorpolynom des dualen Codes:

$$x^4 \cdot h(1/x) = x^4 + x^3 + x^2 + 1$$

Aufgabe 28: Gewichtsverteilung des $[7,4,3]$ Codes mit der " des $[7,3,4]$ Codes bestimmen.

$x^4 + x^3 + x^2 + 1$ erzeugt den

Code:

0	0	0	0	0	0	0
0	0	1	1	1	0	1
0	1	1	1	0	1	0
0	1	0	0	1	1	1
1	1	1	0	1	0	0
1	1	0	1	0	0	1
1	0	1	0	0	1	1
1	1	0	1	0	0	1

$\Rightarrow A(z) = 1 + 7z^4$

Gewichtsverteilung des $[7,4,3]$ Codes:

$$B(z) = \frac{(1+z)^7}{z^3} \cdot A\left(\frac{1-z}{1+z}\right)$$

$$= \frac{(1+z)^7}{z^3} \cdot \left(1 + 7\left(\frac{1-z}{1+z}\right)^4\right)$$

$$= \frac{1}{8} \cdot \left((1+z)^7 + 7(1+z)^3 \cdot (1-z)^4\right)$$

$$\Rightarrow \quad B(z) = 1 + 7z^3 + 7z^4 + z^7$$