Nichtbinäre Hamming Codes

$GF(q)$

Alle $q^m - 1$ von Null verschiedene Spalten?

$\Rightarrow$ klappt nicht!

Abhilfe: In H-Matrix nur solche Spalten zulassen, bei denen der erste von Null verschiedene Eintrag $= 1$ ist

Beisp.:

$GF(3)$ $\quad H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$

m Zeilen in H

Es gibt $q^{m-1} + q^{m-2} + \ldots + 1 = \frac{q^m - 1}{q-1}$

derartige Spalten.

$\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3\right]$-Code

über $GF(q)$

Hausaufgabe: Geben Sie H und G Matrix eines $[6,4,3]$ Codes über $GF(5)$ an.

Gilbert-Varshamov Schranke

Linearer $[n, k, d]$ Code

Für ✓ Binärcodes

existiert, wenn gilt:

$$\sum_{j=0}^{d-2} \binom{n-1}{j} < 2^{n-k}$$

Mindestdistanz = kleinste Anzahl von linear ~~un~~abhängigen Spalten von $\underline{H}$

$d-1$ Spalten müssen linear unabhängig sein.

Solange $\binom{i}{1} + \binom{i}{2} + \cdots \binom{i}{d-2} < 2^{n-k} - 1$

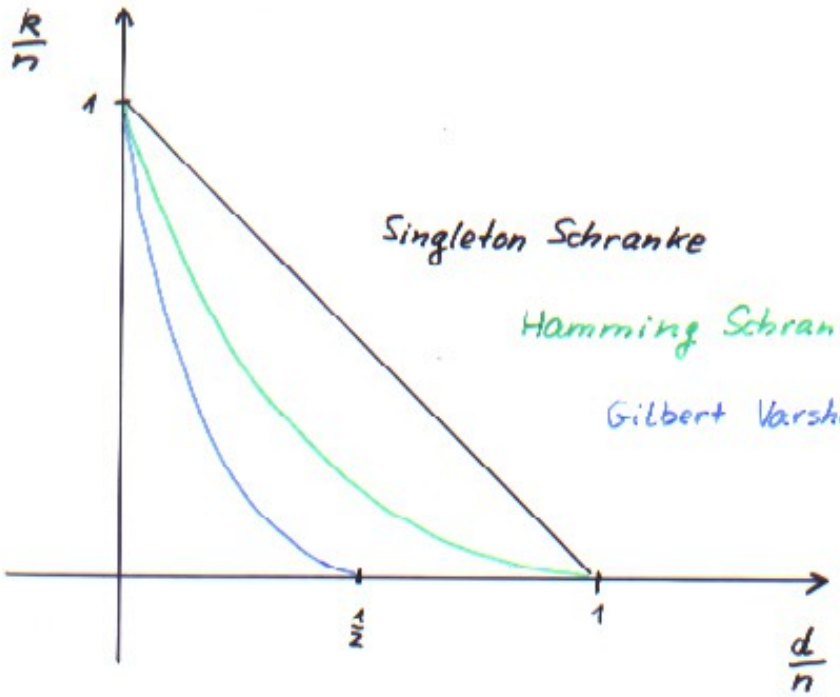
ist, findet man eine weitere linear unabh. Spalte.

Hausaufgabe: Wie lauten Hamming Schranke und Gilbert Varsh. Schranke für nicht-binäre Codes?

Asymptotisch gute Codes

$$\lim_{n\to\infty} \frac{k}{n} > 0 \quad \text{und} \quad \lim \frac{d}{n} > 0 \,,$$

bei festem Codealphabet (z.B. Binärcodes).



Asymptotische Schranken für Binärcodes.

Gilbert Schranke: Es existieren Binärcodes, die die Schranke erreichen!

Die Singleton Schranke wird bei Binärcodes nie erreicht.
nichttrivialen

Goppa Codes

- Enthalten viele Codes, die besser als entsprechende BCH-Codes sind
  z.B. $[15, 7, 5]$ BCH-Code
  $[16, 8, 5]$ Goppa-Code
- Es existieren effiziente Decodierverfahren
- Goppa Codes enthalten sehr viele asymptotisch gute Codes

1970 / 1971 von Goppa eingeführt
(Goppa Codes enthalten BCH-, und RS-Codes)

1975 Decodieralgorithmus mit Euklidschem Algorithmus
(Sugiyama et al)

1975 Decodieralgorithmus mit Berlekamp-Massey Algorithmus
sowie Dec. Alg. für binäre Goppa-Codes
→ Patterson

BCH- und RS-Codes sind Spezialfälle von Goppa Codes. Zunächst andere Darstellung dieser Codes: $C(x)$ mit $c(\alpha^j) = 0$, $j = 1, 2 \dots, 2t$

$$S_j = \sum_{i=0}^{n-1} r_i \alpha^{ij} \qquad r(x) = c(x) + e(x)$$

$$S(z) = \frac{1}{z} \sum_{j=1}^{2t} S_j z^j = \frac{1}{z} \sum_{i=0}^{n-1} \sum_{j=1}^{2t} r_i \alpha^{ij} z^j$$

$$= \frac{1}{z} \sum_{i=0}^{n-1} r_i \sum_{j=1}^{2t} (\alpha^i z)^j = \frac{1}{z} \sum_{i=0}^{n-1} r_i \alpha^i z \cdot \frac{1 - (\alpha^i z)^{2t}}{1 - \alpha^i z}$$

$$S(z) = \sum_{i=0}^{n-1} \frac{-r_i \left(1 - (\alpha^i z)^{2t}\right)}{z - \alpha^{-i}}$$

$$\rightsquigarrow \quad S(z) = \sum_{i=0}^{n-1} \frac{-r_i}{z - \alpha^{-i}} \mod z^{2t}$$

Wenn $r(x)$ = Codewort, d.h. $r_i = c_i$ $\quad i = 0, \dots n-1$

$\Rightarrow$ alternative Definition von BCH- und RS-Codes

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \alpha^{-i}} \equiv 0 \mod z^{2t}$$

Modifikation dieser Def. von BCH- und RS-Codes führt zu Goppa Codes. $\alpha^{-i} \rightarrow \alpha_i$, $z^{2t} \rightarrow G(z)$

Def.: **Goppa Code $\Gamma(L, G)$**

Für die Codewörter $\underline{c} = (c_0, c_1, c_2, \ldots, c_{n-1})$

eines Goppacodes über $GF(q)$ gilt:

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \alpha_i} \equiv 0 \mod G(z)$$

wobei α_i Elemente aus der Menge $L \subseteq GF(q^m)$

und $G(z)$ das Goppa Polynom vom Grad s

über $GF(q^m)$ ist. Es gilt $G(\alpha_i) \neq 0$.

Für Goppa Codes gilt:

$$n = |L|$$

$$k \geq n - m \cdot \underbrace{\text{Grad}\{G(z)\}}_{= s}$$

$$d \geq s + 1$$

Für binäre Goppa Codes gilt: Wenn $G(z)$ nur einfache Nullstellen hat: $d \geq 2 \cdot s + 1$

$\frac{1}{z-\alpha_i} \bmod G(z)$ ist ein Polynom vom Grad $\leq s-1$

$\Rightarrow 0 \equiv \sum \frac{c_i}{z-\alpha_i} \bmod G(z)$ entspricht $s \cdot m$ (Prüf) Gleichungen über $GF(q)$.

$\Rightarrow \quad k \geq n - m \cdot s$ ✓

Ebenso folgt: Goppa Codes sind lineare Codes.

Beweis der Mindest distanz: $d \geq s+1$

Annahme $d \leq s \quad \Rightarrow \quad \sum_{i=1}^{r} \frac{K_i}{z-\beta_i} \equiv 0 \bmod G(z)$

mit $r \leq s$ und $\beta_i \in L$, $K_i \in GF(q) \setminus \{0\}$

$$\Rightarrow \sum_{i=1}^{r} \frac{K_i \prod_{j \neq i} (z-\beta_j)}{\prod_{j=1}^{r} (z-\beta_j)} = \frac{p(z)}{q(z)} \equiv 0 \bmod G(z)$$

$q(z)$

$p(z)$ ist ein Polynom mit Grad $\leq s-1$. Widerspruch!

Da $ggT(q(z), G(z)) = 1 \quad \Rightarrow \quad p(z) \equiv 0 \bmod G(z)$

$\Rightarrow$ Dies kann nicht sein $\Rightarrow$ $d \geq s+1$. ✓

Für binäre Goppa Codes:

Annahme: $d \leq 2s$, $r \leq 2s$

$$K_i = 1 \;\searrow\; \sum_{i=1}^{n} \frac{\prod_{j \neq i} (z - \beta_j)}{\prod_{j=1}^{r} (z - \beta_j)} = \frac{g'(z)}{g(z)} \equiv 0 \bmod G(z)$$

$$g(z) = \prod_{j=1}^{r} (z - \beta_j)$$

$$g'(z) = \sum_{i=1}^{r} \prod_{j \neq i} (z - \beta_j)$$

Setze $g(z) = a^2(z) + z \cdot b(z)^2 \;\searrow\; g'(z) = b(z)^2$

$\Rightarrow$ Die Nullstellen von $g'(z)$ sind doppelte NS.

$G(z)$ hat einfache Nullstellen. $ggT(g(z), G(z)) = 1$

$\Rightarrow g'(z) \equiv 0 \bmod G(z) \Rightarrow b(z) \equiv 0 \bmod G(z)$

Grad $g(z) \leq 2s \;\searrow$ Grad $g'(z) \leq 2s-2 \Rightarrow$ Grad $b(z) \leq s-1$

Widerspruch! Grad $b(z)$ kann nicht $< s$ sein

$\Rightarrow d \geq 2s+1$. ✓

Bestimmung von $(z-\alpha_i)^{-1} \bmod G(z)$

EEA: $1 = u(z) \cdot G(z) + \underbrace{(z-\alpha_i)^{-1}}_{\text{Polynom vom Grad } s-1 \; \xi(z)} \cdot (z-\alpha_i)$

$\text{Grad}\, u(z) = 0 \Leftarrow$

$\Rightarrow \quad 1 = c \cdot G(z) + \xi(z) \cdot (z-\alpha_i)$

$z = \alpha_i \Rightarrow \quad 1 = c \cdot G(\alpha_i) \Rightarrow c = \frac{1}{G(\alpha_i)}$

$\Rightarrow \quad \xi(z) = \frac{1 - G(z)/G(\alpha_i)}{z-\alpha_i}$

$$\boxed{\frac{1}{z-\alpha_i} \bmod G(z) = -\frac{G(z)-G(\alpha_i)}{G(\alpha_i)\cdot(z-\alpha_i)}}$$

↑

|L| Polynome vom Grad $s-1$.

($\hat{=}$ $s \cdot m$ Prüfgleichungen)

$$\sum_{i=0}^{n-1} c_i \cdot \frac{G(z)-G(\alpha_i)}{G(\alpha_i)(z-\alpha_i)} = 0$$

Decodierung von Goppa Codes

$\underline{c} \rightarrow \underline{r} = \underline{c} + \underline{e}$; $r_i = c_i + e_i$

Syndrompolynom: $S(z) = \sum_{i=0}^{n-1} \frac{r_i}{z - \alpha_i} \mod G(z)$ (ohne Minuszeichen)

$= \sum_{i=0}^{n-1} \frac{e_i}{z - \alpha_i} \mod G$

Fehlerstellenpolynom: $\sigma(z) = \prod_{i \in \mathcal{F}} (z - \alpha_i)$ $|\mathcal{F}| = f$

$\Rightarrow \sigma(z) \cdot S(z) = \sum_{i=0}^{n-1} e_i \prod_{j \neq i} (z - \alpha_j) \mod G(z)$

$\omega(z)$ ← Fehlerwertpolynom

$$\boxed{\omega(z) \equiv \sigma(z) \cdot S(z) \mod G(z)}$$

Lösung mit Euklidschem Algorithmus mit $G(z)$ und $S(z)$ als Startpolynomen.

$$\Rightarrow \quad e_i = \begin{cases} 0 & \text{für } \sigma(\alpha_i) \neq 0 \\ \frac{\omega(\alpha_i)}{\sigma'(\alpha_i)} & \text{für } \sigma(\alpha_i) = 0 \end{cases}$$

Decodierung von binären Goppa Codes

$$\omega(z) \equiv \sigma(z) \cdot S(z) \bmod G(z)$$

$$\sigma(z) = \prod_{i \in F} (z - \alpha_i) \qquad \omega(z) = \sum_{i=0}^{n-1} e_i \prod_{j \neq i} (z - \alpha_j)$$

($\prod_{j \neq i}$: $=1$)

$$\omega(z) = \sigma'(z)$$

$$\left.\begin{aligned} \sigma(z) &= a(z)^2 + z \cdot b(z)^2 \\ \sigma'(z) &= b(z)^2 \end{aligned}\right\} \quad \sigma'(z) \equiv \sigma(z) S(z) \bmod G(z)$$

$$b(z)^2 \equiv (a'(z) + z b'(z)) S(z)$$

Bestimme $T(z)$ mit $S(z) \cdot T(z) \equiv 1 \bmod G(z)$

$$\Rightarrow \quad (T(z) + z) \cdot b(z)^2 \equiv a(z)^2 \bmod G(z)$$

1.) Für $T(z) = z \Rightarrow a(z) = 0 \Rightarrow b^2 \equiv z b^2 S \bmod G$

$$\Rightarrow 1 \equiv z \cdot S \bmod G$$

$$\Rightarrow \sigma(z) = z$$

2.) Für $T(z) \neq z$

Bestimme Polynom $R(z)$ für das gilt:

$$R(z)^2 \equiv T(z) + z \mod G(z)$$

→ Algorithmus hierfür folgt später

$$\Rightarrow \quad R^2(z) \cdot b(z)^2 \equiv a(z)^2 \mod G(z)$$

$$\Rightarrow \quad a(z) \equiv b(z) \cdot R(z) \mod G(z)$$

"Neue Schlüsselgleichung", die mit EEA gelöst werden kann. $\Rightarrow a(z), b(z)$

$$\Rightarrow G(z) = a^2(z) + z \cdot b^2(z)$$

H. A.: Verifizieren Sie, daß Grad{a(z)} und Grad{b(z)} derart sind, daß die neue Schlüsselgleichung mit dem EEA gelöst werden kann.

Wurzelziehen von Polynomen mod $f(x)$ in Körpern der Char. zwei

$$y(z)^2 \equiv t(z) \bmod f(z)$$

$t(z)$: gegeben — Bestimme $y(z)$

"Klassische" Methode: Wurzelziehen bei Char. 2 ist lineare Operation
→ Mit Matrix

Besser:

Mit Polynom $w(z)$ für das gilt: $w(z)^2 \equiv z \bmod f(z)$

Setze: $t(z) = t_0^2(z) + z \cdot t_1^2(z)$

(t_0, t_1: leicht von $t(z)$ zu erhalten)

$$\Rightarrow \quad y(z) = t_0(z) + w(z) \cdot t_1(z) \bmod f(z)$$

Bestimmung von $w(z)$:

$$f(z) = f_0(z)^2 + z\, f_1(z)^2$$

$$f_0^2(z) \equiv z f_1^2(z) \bmod f$$

Mit EEA:

$$1 = v_1(z) f_0(z) + v_0(z) f_1(z)$$

$$\Rightarrow \quad w(z) = v_0(z) f_0(z) + z \cdot v_1(z) f_1(z)$$

Beweis:

$$w(z)^2 = v_0^2 f_0^2 + z^2 v_1^2 f_1^2 \equiv z v_0^2 f_1^2 + z v_1^2 f_0^2 \bmod f$$

$$\equiv z (v_0^2 f_1^2 + v_1^2 f_0^2) \equiv z \underbrace{(v_0 f_1 + v_1 f_0)^2}_{1} \bmod f$$

$$\Rightarrow \quad w(z)^2 \equiv z \bmod f \quad \checkmark$$

Beispiel

Bestimmen von $w(z)$ mit $w(z)^2 \equiv z \bmod f(z)$

für $f(z) = z^5 + z^2 + 1$.

$$f(z) = \underbrace{z^2+1}_{f_0^2} + z \cdot \underbrace{z^4}_{f_1^2}$$

$f_0(z) = z+1$

$f_1(z) = z^2$

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

$$1 = \underbrace{1}_{v_0} \cdot \underbrace{z^2}_{f_1} + \underbrace{(z+1)}_{v_1} \cdot \underbrace{(z+1)}_{f_0}$$

$$\Rightarrow w(z) = \underbrace{z+1}_{v_0 \cdot f_0} + z \cdot \underbrace{z(z+1)}_{f_1 v_1}$$

$$w(z) = z^4 + z^3 + z + 1$$

$z^2 : (z+1) = z+1$

$z^2 + z$

z

$z+1$

1

Beispiel $G(z) = z^2 + z + \alpha^3$

Gesucht: $w(z)$ mit $w(z)^2 \equiv z \bmod G(z)$

$$G(z) = (z^2 + \alpha^3) + z \cdot 1$$

$$f_0^2 \mathrel{\hat{=}} z^2 + \alpha^3 = (z + \alpha^9)^2 \quad \leftarrow \quad \sqrt{\alpha^3} = \sqrt{\alpha^{3+15}} = \alpha^9$$

$$f_1^2 \mathrel{\hat{=}} 1 = 1^2$$

EEA:

$$z + \alpha^9 = 1 \cdot (z + \alpha^9) + 0 \cdot 1$$

$$1 = 0 \cdot (z + \alpha^9) + 1 \cdot 1$$

v_1 f_0 v_0 f_1

$$\Rightarrow \quad w(z) = 1 \cdot (z + \alpha^9) + z \cdot 0 \cdot 1$$

$$\underline{w(z) = z + \alpha^9}$$

Test: $w(z)^2 = z^2 + \alpha^{18} \equiv z \bmod G(z)$

Beispiel: Goppa Polynom $G(z) = z^2 + z + \alpha^3$ über $GF(2^4)$ mit $p(x) = x^4 + x + 1$

Siehe Folie 10 vom 31.10.14 sowie Folie 19 vom 14.11.'14 →

$h(\alpha^3) = 1 \Rightarrow G(z)$ hat keine Wurzeln in $GF(2^4)$

$L = GF(2^4) \Rightarrow$ Binärer $[16, 8, 5]$ Code.

z.B. $\alpha_0 = 0$, $\alpha_i = \alpha^{i-1}$, $i = 1 \ldots 15$; $n = |L|$; $k \geq n - 4 \cdot 2 = 8$; $d \geq 2 \cdot 2 + 1$

(α: prim. Element)

Für Codewörter gilt: $\sum_{i=0}^{15} \frac{c_i}{z - \alpha_i} \equiv 0 \mod G(z)$

bzw. $\sum_{i=0}^{15} c_i \cdot \frac{G(z) - G(\alpha_i)}{G(\alpha_i)(z - \alpha_i)} = 0$

Terme können vorberechnet werden

Annahme: $\underline{c} = 0$, $\underline{r} = (0, 1, 0, 1, 0, \ldots, 0, 0)$ ($r_0, r_1, r_2, r_3, r_{15}$)

$$S(z) = \sum_{i=0}^{15} r_i \frac{G(z) - G(\alpha_i)}{G(\alpha_i)(z - \alpha_i)} = \frac{G(z) - G(\alpha_1)}{G(\alpha_1)(z - \alpha_1)} + \frac{G(z) - G(\alpha_3)}{G(\alpha_3)(z - \alpha_3)}$$

$$\alpha_0 = 0 \rightsquigarrow \frac{1}{z - 0} \mod G(z) = \frac{z^2 + z + \alpha^3 - \alpha^3}{\alpha^3 (z - 0)} = \frac{z + 1}{\alpha^3} = \alpha^{12} z + \alpha^{12}$$

$$\alpha_1 = 1 \rightsquigarrow \frac{1}{z - 1} \text{ " } = \frac{z^2 + z + \alpha^3 - \alpha^3}{\alpha^3 (z - 1)} = \frac{z}{\alpha^3} = \alpha^{12} z$$

$\alpha_2 = \alpha \rightsquigarrow$ H.A. für α_2 sowie $\alpha_4 \ldots \alpha_{15}$ die Polynome bestimmen.

$$\alpha_3 = \alpha^2 \rightsquigarrow \frac{1}{z - \alpha^2} \mod G(z) = \frac{z^2 + z + \alpha^3 - \alpha^{12}}{\alpha^{12}(z - \alpha^2)} = \frac{z + \alpha^8}{\alpha^{12}} = \alpha^3 z + \alpha^{11}$$

($\alpha^{12} = \alpha^4 + \alpha^2 + \alpha^3$)

$$S(z) = \alpha^{12} z + \alpha^3 z + \alpha^{11} \Rightarrow S(z) = \alpha^{10} z + \alpha^{11}$$

Bestimme $T(z)$ mit : $T(z) \cdot S(z) \equiv 1 \bmod G(z)$

EEA :

$$G(z) = 1 \cdot G(z) + 0 \cdot S(z)$$
$$S(z) = 0 \cdot G(z) + 1 \cdot S(z)$$
$$\alpha^{11} = 1 \cdot G(z) + (\alpha^5 z + \alpha^9) \cdot S(z) \quad | \cdot \alpha^4$$

$$\Rightarrow \underline{1 \equiv (\alpha^9 z + \alpha^{13}) S(z) \bmod G}$$

Nebenrechnung:

$$(z^2 + z + \alpha^3) : (\alpha^{10} z + \alpha^{11}) = \alpha^5 z + \alpha^9 \quad \Rightarrow T(z) \neq z$$
$$z^2 + \alpha z$$
$$\alpha^4 z + \alpha^3$$
$$\alpha^4 z + \alpha^5$$
$$\alpha^{11}$$

$$\Rightarrow T(z) + z = \alpha^7 z + \alpha^{13} = R^2(z)$$

$$R^2(z) = \alpha^{13} + z \cdot \alpha^7$$

$$\Rightarrow R(z) = \alpha^{13/2} + w(z) \cdot \alpha^{7/2}$$

$$\underline{R(z) = \alpha^{14} + (z + \alpha^9) \cdot \alpha^{11} = \alpha^{11} z + \alpha^{12}}$$

EEA:

$$z^2 + z + \alpha^3 = 1 \cdot (z^2 + z + \alpha^3) + 0 \cdot (\alpha^{11} z + \alpha^{12})$$
$$\alpha^{11} z + \alpha^{12} = 0 \cdot (z^2 + z + \alpha^3) + 1 \cdot (\alpha^{11} z + \alpha^{12})$$
$$\Rightarrow \underbrace{\alpha^{11} z + \alpha^{12}}_{a(z)} \equiv \underbrace{1}_{b(z)} \cdot (\alpha^{11} z + \alpha^{12}) \bmod G(z)$$

$$\Rightarrow G(z) = a^2(z) + z\, b^2(z) \quad \Rightarrow \underline{G(z) = \alpha^7 z^2 + z + \alpha^9}$$

H.A.: Decodieren Sie den [16, 8, 5] Goppa Code

mit $\underline{r} = (0, 0, 0, 1, 0, 1, 0, \dots)$

r_0, r_3, r_5

und $\underline{r} = (0, 0, 0, 0, 1, 0, 0, 1, 0, \dots)$

r_4, r_7

H.A. Bestimmen Sie mit den $\frac{G(z) - G(\alpha_i)}{G(\alpha_i)(z - \alpha_i)}$

eine Prüfmatrix für den binären [16, 8, 5] Goppa Code

Aufgabe 14 Bei der Rekursion für den erweiterten Euklidschen Algorithmus

$$r_i(z) = q_i(z) \cdot m(z) + p_i(z) \cdot n(z)$$

gilt $\text{Grad}\, p_i(z) + \text{Grad}\, r_{i-1}(z) = \text{Grad}\, m(z)$

Beweis: Mit Induktion

$m(z) = 1 \cdot m(z) + 0 \cdot n(z)$

$n(z) = 0 \cdot m(z) + 1 \cdot n(z)$

$r_0(z) = q_0(z)\, m(z) + p_0(z) \cdot n(z)$

Die Behauptung gilt für $i=0$:

$\text{Grad}\, p_0(z) + \text{Grad}\, n(z) =$

$a_0(z) = \frac{m(z)}{n(z)}$ ← Div. ohne Rest

$p_0(z) = 0 - a_0(z) \cdot 1$

$\text{Grad}\, m(z) - \text{Grad}\, n(z) + \text{Grad}\, n(z)$

$= \text{Grad}\, m(z)$ ✓

Annahme: Aussage gilt für i

$\text{Grad}\, p_i(z) + \text{Grad}\, r_{i-1}(z) = \text{Grad}\, m(z)$

$p_{i+1}(z) = p_{i-1}(z) - \frac{r_{i-1}(z)}{r_i(z)} \cdot p_i(z)$

$\text{Grad}\, p_i(z) > \text{Grad}\, p_{i-1}(z)$

$\text{Grad}\, p_{i+1}(z) = \text{Grad}\, r_{i-1}(z) - \text{Grad}\, r_i(z) + \text{Grad}\, p_i(z)$

$\text{Grad}\, p_{i+1}(z) + \text{Grad}\, r_i(z) = \text{Grad}\, p_i(z) + \text{Grad}\, r_{i-1}(z)$ ✓

$= \text{Grad}\, m(z)$

Aufgabe 15: bin. $[15, 5, 7]$-BCH Code

$g(x)$ → Folie 17, 14.11.14

$GF(2^4)$ → Folie 21, 31.10.14

Decodierung von $r(x) = x^5 + x^2 + x + 1$.

$$
\begin{aligned}
S_1 &= r(\alpha) = \alpha^5 + \alpha^2 + \alpha + 1 = 1 \\
S_2 &= r(\alpha^2) = S_1^2 = 1 \\
S_3 &= r(\alpha^3) = \alpha^{15} + \alpha^6 + \alpha^3 + 1 = \alpha^2 \\
S_4 &= r(\alpha^4) = S_2^2 = 1 \\
S_5 &= r(\alpha^5) = \alpha^{25} + \alpha^{10} + \alpha^5 + 1 = \alpha^{10} \\
S_6 &= r(\alpha^6) = S_3^2 = \alpha^4
\end{aligned}
$$

$$\Rightarrow \quad S(z) = 1 + z + \alpha^2 z^2 + z^3 + \alpha^{10} z^4 + \alpha^4 \cdot z^5$$

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

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

$$z^4 + \alpha^{14} z^3 + \alpha^{13} z^2 + \alpha^9 z + \alpha^2 = 1 \cdot z^6 + (\alpha^{11} z + \alpha^2) \cdot S(z)$$

$$\alpha^7 z^3 + \alpha^{11} z^2 + z + \alpha^3 = (\alpha^4 z + \alpha^{12}) \cdot z^6 + (z^2 + \alpha^{14} z + \alpha^3) \cdot S(z)$$

$$\underbrace{\alpha^8 z^2 + \alpha}_{\omega(z)\ (= \sigma'(z))} = (\dots) \cdot z^6 + \underbrace{(\alpha^8 z^3 + \alpha^{12} z^2 + \alpha z + \alpha)}_{\sigma(z)} \cdot S(z)$$

$$z^6 : (\alpha^4 z^5 + \alpha^{10} z^4 + z^3 + \alpha^2 z^2 + z + 1) = \alpha^{11} z + \alpha^2$$

$$\underline{z^6 + \alpha^6 z^5 + \alpha^{11} z^4 + \alpha^{13} z^3 + \alpha^{11} z^2 + \alpha^{11} z}$$

$$\alpha^6 z^5 + \alpha^{11} z^4 + \alpha^{13} z^3 + \alpha^{11} z^2 + \alpha^{11} z$$

$$\underline{\alpha^6 z^5 + \alpha^{12} z^4 + \alpha^2 z^3 + \alpha^4 z^2 + \alpha^2 z + \alpha^2}$$

$$z^4 + \alpha^{14} z^3 + \alpha^{13} z^2 + \alpha^9 z + \alpha^2$$

$$\left(\alpha^4 z^5 + \alpha^{10} z^4 + z^3 + \alpha^2 z^2 + z + 1\right) : \left(z^4 + \alpha^{14} z^3 + \alpha^{13} z^2 + \alpha^9 z + \alpha^2\right) = \alpha^4 z + \alpha^{12}$$

$$\underline{\alpha^4 z^5 + \alpha^3 z^4 + \alpha^2 z^3 + \alpha^{13} z^2 + \alpha^6 z}$$

$$\alpha^{12} z^4 + \alpha^8 z^3 + \alpha^{14} z^2 + \alpha^{13} z + 1$$

$$\underline{\alpha^{12} z^4 + \alpha^{11} z^3 + \alpha^{10} z^2 + \alpha^6 z + \alpha^{14}}$$

$$\alpha^7 z^3 + \alpha^{11} z^2 + z + \alpha^3$$

$$\left(z^4 + \alpha^{14} z^3 + \alpha^{13} z^2 + \alpha^9 z + \alpha^2\right) : \left(\alpha^7 z^3 + \alpha^{11} z^2 + z + \alpha^3\right) = \alpha^8 z + \alpha^2$$

$$\underline{z^4 + \alpha^4 z^3 + \alpha^8 z^2 + \alpha^{11} z}$$

$$\alpha^3 z^3 + \alpha^3 z^2 + \alpha^2 z + \alpha^2$$

$$\underline{\alpha^3 z^3 + \alpha^{13} z^2 + \alpha^2 z + \alpha^5}$$

$$\alpha^8 z^2 + \alpha$$

$$0 - (\alpha^{11} z + \alpha^2) \cdot 1 = \alpha^{11} z + \alpha^2$$

$$1 - (\alpha^4 z + \alpha^{12}) \cdot (\alpha^{11} z + \alpha^2) = \alpha^{15} z^2 + (\alpha^6 + \alpha^{23}) z + \alpha^{14} + 1$$

$$= z^2 + \alpha^{14} z + \alpha^3$$

$$(\alpha^{11} z + \alpha^2) - (\alpha^8 z + \alpha^2) \cdot (z^2 + \alpha^{14} z + \alpha^3) = \alpha^8 z^3 + \alpha^{12} z^2 + \alpha \cdot z + \alpha$$

Die Nullstellen von $G(z) = \alpha^8 z^3 + \alpha^{12} z^2 + \alpha z + \alpha$

sind: α^5, α^7 und α^{11}

$\Rightarrow$ Fehlerpositionen: $15-5 = 10$

$15-7 = 8$

$15-11 = 4$

$\Rightarrow e(x) = x^{10} + x^8 + x^4$ ← bei Binärcodes → Fehlerwert = 1.

$\Rightarrow r(x) - e(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$

$(= g(x))$