Wdh. vom 31.10.2014

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$n-k$ Zeilen

n Spalten

$[7, 4, 3]$-Code (n, k, d)

$R = \frac{k}{n} = \frac{4}{7}$

Beschreibung mit $GF(2^3)$:

$$\tilde{H} = (\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$$

$$\Rightarrow \sum_{i=0}^{n-1} c_i \alpha^i = 0 \qquad \underline{c} \leftrightarrow c(x)$$

$$\underline{r} = \underline{c} + \underline{e} \leftrightarrow r(x) = c(x) + e(x)$$

$$c(\alpha) = 0 \Rightarrow r(\alpha) = \underbrace{c(\alpha)}_{=0} + e(\alpha)$$

$$c(x) = i(x) \cdot g(x)$$

$g(x)$: bin. Polynom kleinsten Grades, das α als NS enthält

Im Beispiel: $c(x) = \underbrace{i(x)}_{\text{Grad} \le 3} \cdot \underbrace{(x^3 + x + 1)}_{\text{Grad } 3}$

$c(x)$: Grad ≤ 6

$\Rightarrow 2^4$ Codewörter

$i(x)$: Grad $\le k-1$

$g(x)$: Grad $n-k$

$c(x)$: Grad $\le n-1$

BCH - Codes

$$\underline{H} = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1} \\ \alpha^0 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & & & & \\ \alpha^0 & \alpha^{\delta-1} & \alpha^{(\delta-1)2} & \cdots & \alpha^{(\delta-1)(n-1)} \end{pmatrix}$$

$GF(q^m)$

α: primitives Element von $GF(q^m)$

BCH-Codes über $GF(q)$: $n = q^m - 1$

$k = n - \text{grad } g(x)$

$d \geq \delta$

Verallgemeinerung q statt p ↑ Primzahlpotenz

$g(x) = kgV \text{ der } m_j(x)$, $j = 1, 2, \ldots \delta-1$

BCH-Codes bei denen α ein primitives Element von $GF(q^m)$ ist nennt man primitive BCH-Codes.

(nicht primitive BCH-Codes führen zu weiteren Codes.)

Die Bedingung $g(\alpha^j) = 0$ für $j = 1, 2, \ldots, \delta-1$

kann verallgemeinert werden zu $g(\alpha^j) = 0$ für

$j = b, b+1, \ldots, \delta+b-2$

Bei der Wahl von $b=1$ spricht man auch

von BCH-Codes im engeren Sinn (narrow sense).

zyklische Codes

mit $\underline{c} = (c_0, c_1, c_2, \dots, c_{n-1})$ ist auch

$\hat{\underline{c}} = (c_{n-1}, c_0, c_1, \dots, c_{n-2})$ ein Codewort.

Polynomdarstellung:

$$\hat{\underline{c}}(x) = x \cdot c(x) - c_{n-1} \cdot (x^n - 1) \qquad (*)$$

Das Polynom $x^{p^m-1} - 1$ enthält alle Elemente (z.B. im Binärfall $2^m - 1$)

von $GF(p^m) \setminus \{0\}$ als Wurzeln. $n = p^m - 1$

Wenn $g(x)$ nur Wurzeln aus $GF(p^m)$ hat: $g(x) \mid (x^n - 1)$

Wenn $c(x) = i(x) \cdot g(x)$ folgt mit $(*)$, daß

auch $\hat{c}(x)$ vom $g(x)$ geteilt wird.

Die Codeworte $i(x) \cdot g(x)$ bilden einen

zyklischen Code.

Systematische Codierung von zyklischen Codes

$$c(x) = i(x) \cdot g(x)$$

↑ Information nicht direkt im Codewort ablesbar

$$x^{n-k} \cdot i(x) = u(x) \cdot g(x) + \xi(x) \qquad \text{Grad } \xi(x) < \text{Grad } g(x) \uparrow = n-k$$

$$\Rightarrow \quad x^{n-k} \cdot i(x) - \xi(x) = u(x) \cdot g(x)$$

$$\xi(x) = x^{n-k} \, i(x) \bmod g(x)$$

Systematische Codierung:

$$c(x) = x^{n-k} \cdot i(x) - \left(x^{n-k} \, i(x) \bmod g(x) \right)$$

↑

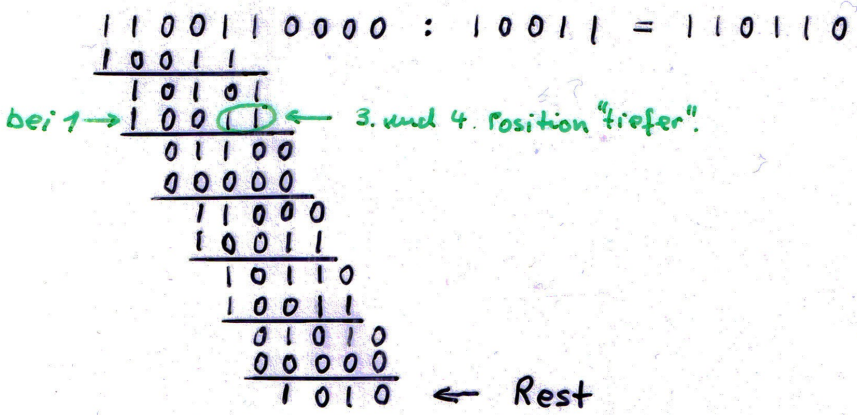
auch leicht in Software durchführbar.

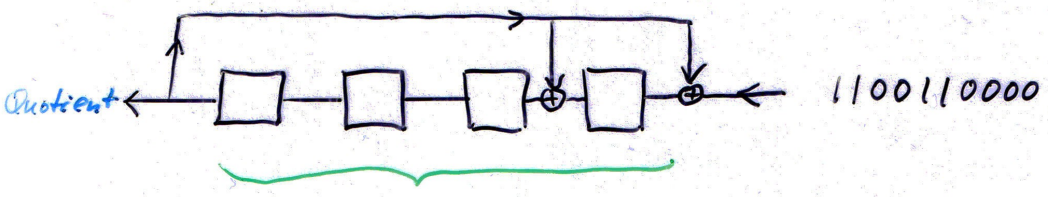
Insbesondere für binäre Codes gibt es schnelle Schieberegisterschaltungen.

Beispiel für Schieberegisterschaltung

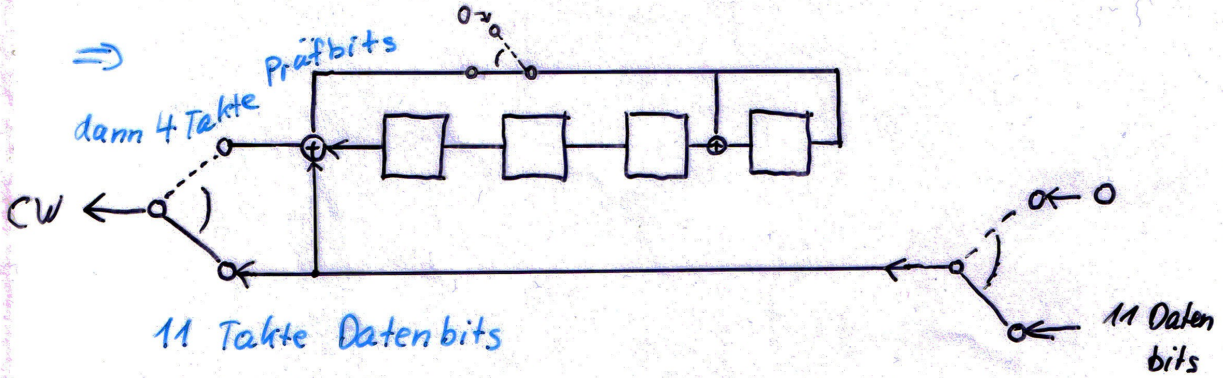
Bin. $[15, 11, 3]$ Code mit $g(x) = x^4 + x + 1$

z.B. $i(x) = x^5 + x^4 + x + 1 \rightsquigarrow i(x) \cdot x^{n-k} = x^9 + x^8 + x^5 + x^4$





Nach Einlesen der Bitfolge steht der Rest im Schieberegister.



Reed-Solomon Codes (RS-Codes)

Gleiche Prüfmatrix wie BCH-Codes

$$\underline{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \\ \vdots & & & & \\ 1 & \alpha^{\delta-1} & \alpha^{(\delta-1)2} & & \alpha^{(\delta-1)(N-1)} \\ & & \alpha & \dots & \alpha \end{pmatrix}$$

$\alpha \in GF(q)$

$q = p^m$

wesentliche Änderung: Codealphabet identisch $GF(q)$!

$$g(x) = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{\delta-1})$$

Mindestdistanz: $D = \delta$

$N = q-1$

$D = \delta$

$K = N-(D-1)$

$D = N-K+1$

↖ Singleton-Schranke!

Reed-Solomon Codes

$$\underline{H} = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{N-1} \\ \alpha^0 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)} \\ \vdots & & & & \vdots \\ \alpha^0 & \alpha^{\delta-1} & \alpha^{(\delta-1)2} & \cdots & \alpha^{(\delta-1)(N-1)} \end{pmatrix}$$

α primitiv in $GF(q)$

Code alphabet identisch $GF(q)$.

$[N = q-1,\ K,\ D = N-K+1]$ – Codes $\qquad g(x) = (x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{D-1})$

Bei RS-Codes: Großschreibung (Konvention)

Beispiel: $GF(8) = GF(2^3)$, $p(x) = x^3 + x + 1$

$[7, 5, 3]$ RS-Code über $GF(2^3)$

$$g(x) = (x-\alpha)(x-\alpha^2) = x^2 + (\alpha+\alpha^2)x + \alpha^3 = x^2 + \alpha^4 x + \alpha^3$$

$$c(x) = \underbrace{i(x)}_{\text{Grad}=4} \cdot \underbrace{g(x)}_{\text{Grad}=2}$$

$$c_0(x) = 0 \cdot g(x) = (0,0,0,0,0,0,0) = (000, 000, \ldots, 000)$$
$$c_1(x) = 1 \cdot g(x) = (0,0,0,0,1,\alpha^4,\alpha^3) = (000,000,000,000,001,110,011)$$
$$c_2(x) = \alpha \cdot g(x) = (0,0,0,0,\alpha,\alpha^5,\alpha^4) = (000,000,000,000,010,111,110)$$
$$\vdots$$
$$\tilde{c}(x) = (\alpha^4 x^4 + x) \cdot g(x) = (\alpha^4, \alpha^8, \alpha^7, 1, \alpha^4, \alpha^3, 0) = (110,010,001,001,110,011,000)$$
$$\qquad\qquad\qquad\qquad\quad \alpha^8 = \alpha \quad \alpha^7 = 1$$

Decodierung von BCH- und RS-Codes

Anfang der '60-er: Peterson, Gorenstein, Zierler
→ Matrixmethoden

1967/68 : Berlekamps Algorithmus

1969 : Schieberegisterinterpretation / Massey
Berlekamp-Massey Algorithmus

1974/75 : Decodierung mit Euklidschem Algorithmus / Sugiyama, Kasahara, Hirasawa, Namekawa

Universeller, effizienter, eleganter und einfacher Algorithmus zur Decodierung von BCH-, RS- und Goppa codes.

empfangenes Polynom

$r(x) = c(x) + e(x)$; $c(x) = i(x) \cdot g(x)$

$g(x)$: Generatorpolynom des Codes

Gesucht: Nächstes Codewort, bzw.
Fehlerpolynom mit kleinstem Gewicht.

$S_k = r(\alpha^k)$; $k = 1, 2, \ldots, 2t$

$\alpha^1, \alpha^2, \ldots \alpha^{2t}$ NS von $g(x)$

Code kann t Fehler korrigieren

$S_k = e(\alpha^k)$

$$S_k = \sum_{i=1}^{f} Y_i \, \alpha^{k j_i}$$

$$S_k = \sum_{i=1}^{f} Y_i \, X_i^k$$

Matrixgleichung

f : Anzahl der aufgetretenen Fehler
$1 \leq f \leq t$

j_i : Position des i-ten Fehlers

Y_i : Fehlerwert des i-ten Fehlers an Position j_i

$X_i = \alpha^{j_i}$

Unbekannt: f, die Anzahl der Fehler

X_i → liefern Fehlerstellen

Y_i → liefern Fehlerwerte

Fehlerstellenpolynom: $\sigma(z) = \prod_{i=1}^{f} (1 - X_i z)$

Die Nullstellen von $\sigma(z)$ liefern die Fehlerstellen.

Syndrompolynom: $S(z) = \left(\sum_{j=1}^{\infty} S_j z^j \right) / z$

S_j: $2t$ Werte sind bekannt

$/z$: um pass. Grad zu erhalten

$$S(z) = \frac{1}{z} \sum_{j=1}^{\infty} \sum_{i=1}^{f} Y_i X_i^j z^j = \frac{1}{z} \sum_{i=1}^{f} Y_i \sum_{j=1}^{\infty} (X_i z)^j$$

$$= \frac{1}{z} \sum_{i=1}^{f} Y_i \frac{X_i z}{1 - X_i z} = \sum_{i=1}^{f} \frac{Y_i X_i}{1 - X_i z}$$

$$S(z) \cdot \sigma(z) = \sum_{i=1}^{f} Y_i X_i \prod_{j \neq i} (1 - X_j z)$$

Def.: Fehlerwertpolynom: $\omega(z) = \sum_{i=1}^{f} Y_i X_i \prod_{j \neq i} (1 - X_j z)$

$$\Rightarrow \quad \omega(z) = \sigma(z) \cdot S(z) \bmod z^{2t}$$

Schlüsselgleichung

Grad $\sigma(z) = f$; Grad $\omega(z) < f$

$$\omega(z) = \sigma(z) \cdot S(z) \mod z^{2t}$$

Bekannt: $2t$ Stellen des Syndrompolynoms ($S(z) \mod z^{2t}$)

Gesucht: $\sigma(z)$ mit Grad f $(1 \le f \le t)$.

↑ NS von $\sigma(z)$ liefern Fehlerpositionen

$\omega(z)$ mit Grad $< f$ ← Im Nichtbinärfall liefert $\omega(z)$ die Fehlerwerte.

Fehlerwertbestimmung: $\omega(z) = \sum_{i=1}^{f} Y_i X_i \prod_{j \neq i} (1 - X_j z)$

$\sigma(z) = \prod_i (1 - X_i z) \quad \searrow \quad \sigma'(z) = \sum_{i=1}^{f} -X_i \prod_{j \neq i} (1 - X_j z)$

↑ Ableitung

$$\left.\begin{aligned} \omega\left(\frac{1}{X_k}\right) &= Y_k X_k \prod_{j \neq k} \left(1 - X_j \frac{1}{X_k}\right) \\ \sigma'\left(\frac{1}{X_k}\right) &= -X_k \prod_{j \neq k} \left(1 - X_j \frac{1}{X_k}\right) \end{aligned}\right\} \quad Y_k = \frac{-\omega\left(\frac{1}{X_k}\right)}{\sigma'\left(\frac{1}{X_k}\right)}$$

Gelingt es mit der Schlüsselgleichung $\sigma(z)$ und $\omega(z)$ zu bestimmen, so kann man die Fehlerstellen und Fehlerwerte bestimmen und für $1 \le f \le t \Rightarrow$ Korrektur

siehe 25. Folie vom 17.10.2014

Erweiterter Euklidscher Algorithmus für Polynome

$$r_{-2}(x) = 1 \cdot m(x) + 0 \cdot n(x)$$

$$r_{-1}(x) = 0 \cdot m(x) + 1 \cdot n(x)$$

$$\vdots$$

$$r_k(x) = q_k(x) \cdot m(x) + p_k(x) \cdot n(x)$$

$$\vdots$$

$$ggT(m(x), n(x)) = q_L(x) \cdot m(x) + p(x)_L \cdot n(x)$$

$$0 = q_{L+1}(x) \cdot m(x) + p(x)_{L+1} \cdot n(x)$$

3x die gleiche Rekursionsgleichung:

$$r_k(x) = r_{k-2}(x) - a_k(x) \cdot r_{k-1}(x)$$

$$q_k(x) = q_{k-2}(x) - a_k(x) \cdot q_{k-1}(x)$$

$$p_k(x) = p_{k-2}(x) - a_k(x) \cdot p_{k-1}(x)$$

wobei $a_k(x) = \dfrac{r_{k-2}(x)}{r_{k-1}(x)}$ ← Division ohne Rest

Es gilt: $\text{Grad}\, r_i(z) < \text{Grad}\, r_{i-1}(z)$

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

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

H. A.: Beweis (z.B. durch Induktion)

Setze $m(z) = z^{2t}$ und $n(z) = S(z)$ (d.h. $S(z) \bmod z^{2t}$)

$$\Rightarrow \quad r_i(z) = p_i(z) \cdot S(z) \bmod z^{2t}$$

Lösungen der Schlüsselgleichung.

Wenn $1 \le f \le t$ gilt, ist Schlüsselgleichung eindeutig lösbar.

(f = grad $\sigma(z)$)

$\Rightarrow$ Wähle $r_R(z)$ mit $\text{Grad}\, r_{R-1}(z) \ge t$ und $\text{Grad}\, r_R(z) < t$

$$\Rightarrow \quad \text{Grad}\, p_R(z) + \text{Grad}\, r_{R-1}(z) = 2t$$

$$1 \le \text{Grad}\, p_R(z) \le t$$

(Grad $S(z) \bmod z^{2t} = 2t-1$)

$\Rightarrow$ $p_R(z)$ und $r_R(z)$ lösen Schlüsselgleichung.

Lösung der Schlüsselgleichung mit dem erweiterten Euklidschen Algorithmus

genauer $S(z) \bmod z^{2t}$

$$r_{-2}(z) = 1 \cdot z^{2t} + 0 \cdot S(z)$$

$$r_{-1}(z) = 0 \cdot z^{2t} + 1 \cdot S(z)$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$r_k(z) = q_k(z) \cdot z^{2t} + p_k(z) \cdot S(z)$$

Starte den Algorithmus mit z^{2t} und $S(z)$.

Stoppe sobald Grad $r_{k-1}(z) \geq t$ und Grad $r_k(z) < t$.

Dann gilt: $\sigma(z) = p_k(z)$

Konstante $p_k(0)$ kann ignoriert werden

$$\omega(z) = r_k(z)$$

Beispiel: Decodierung eines RS-Codes über GF(7)

$N = q-1 = 6$

$k = 2$

$D = N - k + 1 = 5$

1. primitives Element von GF(7) suchen

Teste: $\alpha = 2$ → nicht primitiv

$\alpha = 3$ → primitiv

$$g(x) = (x-3)(x-2)(x-6)(x-4)$$

$$\downarrow \quad g(x) = x^4 + 6x^3 + 3x^2 + 2x + 4$$

Annahme: $r(x) = 3x^2 + 2x + 4$

$$S_1 = r(3) = \ldots = 2$$
$$S_2 = r(2) = \ldots = 6$$
$$S_3 = r(6) = \ldots = 5$$
$$S_4 = r(4) = \ldots = 4$$

$$\Rightarrow \quad S(z) = 4z^3 + 5z^2 + 6z + 2$$

z^{2t}, $t=2$

$$z^4 = 1 \cdot z^4 + 0 \cdot S(z)$$

$$S(z) = 0 \cdot z^4 + 1 \cdot S(z)$$

$$4z^2+4z+5 = 1 \cdot z^4 + (5z+6) \cdot S(z)$$

$$6 = (6z+5) \cdot z^4 + (2z^2+5z+3) \cdot S(z)$$

$\frac{z^4}{S(z)} = 2z+1$

$\frac{S(z)}{4z^2+4z+5} = z+2$

Grad $\geq t$ Grad $< t$

$$\Rightarrow \quad G(z) = 2z^2+5z+3$$

$$\omega(z) = 6$$

z	$2z^2+5z+3$
1	$2+5+3 \equiv 3$
2	$1+3+3 \equiv 0$ ←
3	$4+1+3 \equiv 1$
4	$4+6+3 \equiv 6$
5	$1+4+3 \equiv 1$
6	$2+2+3 \equiv 0$ ←

Nullstellen von $G(z)$:

$2 = 3^2 = 3^{-4}$ → Fehlerposition 4

$6 = 3^3 = 3^{-3}$ → " 3

Fehlerwerte: $G'(z) = 4z+5$

an Position 4: $\left.\frac{-\omega(z)}{G'(z)}\right|_{z=2} = \frac{-6}{4 \cdot 2+5} = \frac{-6}{6} = -1 = 6$

an Position 3: " $\left|_{z=6}\right. = \frac{-6}{4 \cdot 6+5} = \frac{-6}{1} = 1$

$$\Rightarrow \quad e(x) = 6 \cdot x^4 + x^3 \quad \Rightarrow \quad C(x) = r(x) - e(x) = g(x)$$

hier

Beispiel: Decodierung des binären [15, 5, 7] BCH-Codes

$C_1 = \{1, 2, 4, 8\}$
$C_3 = \{3, 6, 12, 9\}$
$C_5 = \{5, 10\}$

$GF(2^4)$ mit $p(x) = x^4 + x + 1$ konstruiert

$|C_1 \cup C_3 \cup C_5| = 10 \stackrel{!}{=} n - k$
$\delta = 7$
} [15, 5, 7] Code

Generatorpolynom: $g(x) = m_1(x) \cdot m_3(x) \cdot m_5(x)$

aus Ü.A. bereits bekannt

$g(x) = (x^8 + x^7 + x^6 + x^4 + 1) \cdot (x^2 + x + 1)$

← Minimalpolynom von α^5

```
  1 1 1 0 1 0 0 0 1
  1 1 1 0 1 0 0 0 1
1 1 1 0 1 0 0 0 1
-----------------
1 0 1 0 0 1 1 0 1 1 1
```

$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$

Annahme: $r(x) = x^5 + x^2 + x + 1$

Decodierung:
$S_1 = r(\alpha) = \ldots$
$S_2 = r(\alpha^2) = \ldots$
$\ldots$

Hausaufgabe.

Aufgabe 9: Decodieren Sie

$$r(x) = x^4 + x^2 + x$$

und $r(x) = x^5 + x$

zum nächsten Codewort. $H = (\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^6)$

$p(x) = x^3 + x + 1$; $p(\alpha) = 0$

$$r(\alpha) = \underbrace{\alpha^4 + \alpha^2}_{\alpha^2+\alpha} + \alpha = 0 \Rightarrow r(x) = x^4 + x^2 + x \text{ ist Codewort}$$

dies sieht man auch mit: $x^4 + x^2 + x = x \cdot g(x)$

$g(x) = p(x)$

Generatorpolynom des Codes.

$$r(x) = x^5 + x \Rightarrow r(\alpha) = \underbrace{\alpha^5 + \alpha}_{\alpha^2+\alpha+1} = \alpha^2 + 1$$

$$\rightsquigarrow r(\alpha) = \alpha^6$$

$\Rightarrow$ Fehler an letzter Stelle $e(x) = x^6$

$r(x) - e(x) = x^6 + x^5 + x$ ist nächstes Codewort.

Aufgabe 10: Verifikation der quadratischen Lösungsformel für $x^2 + x + y = 0$.

Beh.: Lösungen: x_1 und $x_1 + 1$ $\quad tr(u) = 1$

mit $x_1 = yu^2 + (y + y^2)u^{2^2} + \dots + (y + y^2 + \dots + y^{2^{m-2}})u^{2^{m-1}}$

Bew.:

$$x_1^2 = y^2u^{2^2} + (y^2 + y^{2^2})u^{2^3} + \dots + (y^2 + y^{2^2} + \dots + y^{2^{m-1}})u^{2^m}$$

$$+$$

$$x_1 = yu^2 + (y + y^2)u^{2^2} + (y + y^2 + y^{2^2})u^{2^3} + \dots$$

$$x_1^2 + x_1 = y \cdot u^2 + y \cdot u^{2^2} + yu^{2^3} + \dots + yu^{2^{m-1}} + \underbrace{(y^2 + y^{2^2} + \dots + y^{2^{m-1}})}_{= y} u$$

$$= y \cdot \underbrace{tr(u)}_{=1} = y \quad \checkmark$$

da $tr(y) = 0$.

Beispiel $GF(2^4)$ $\quad p(x) = x^4 + x + 1$

$tr(\alpha) =$			$tr(\alpha^3) =$	
0010	α		1000	α^3
0100	α^2		1100	α^6
0011	α^4		1111	α^{12}
0101	α^8		1010	α^9
0			1 ✓	

$u = \alpha^3$

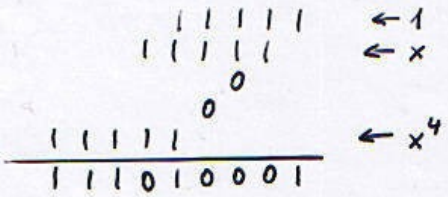
$$x_1 = y \cdot u^2 + (y + y^2)u^{2^2} + (y + y^2 + y^{2^2})u^{2^3}$$

$$x_1 = y \cdot \alpha^{14} + y^2\alpha^8 + y^4\alpha^9$$

Aufgabe 11

Generatorpolynom des binären [15, 7, 5] BCH-Codes

$$g(x) = m_1(x) \cdot m_3(x) = (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1)$$



$$g(x) = x^8 + x^7 + x^6 + x^4 + 1$$

Aufgabe 12

Lösen von $z^2 + \alpha^8 z + \alpha^3 = 0$ in $GF(2^4)$ ↑ $p(x) = x^4 + x + 1$.

mit quadratischer Lösungsformel.

Setze $z = \alpha^8 x$ ⇝ $x^2 + x + \underbrace{\alpha^2}_{\gamma} = 0$

in $GF(2^4)$: $x_1 = \gamma\alpha^{14} + \gamma^2\alpha^8 + \gamma^4\alpha^9$

(siehe vorige Folie)

⋮

⇝ $x_1 = \alpha^{14}$ $x_2 = 1 + x_1 = \alpha^3$

⇝ $z_1 = \alpha^{22} = \alpha^7$ ✓

$z_2 = \alpha^{11}$ ✓

Aufgabe 13 Bestimmen Sie die Parameter $[511, k, d]$ aller binären BCH-Codes mit $\delta \leq 11$

$C_1 = \{1, 2, 4, 8, 16, 32, 64, 128, 256\}$

$\delta = 3 \Rightarrow [511, 502, 3]$-Code

$C_3 = \{3, 6, 12, 24, 48, 96, 192, 384, 257\}$

$768 \equiv 257 \bmod 511$

$C_1 \cup C_3$ enthält $\{1, 2, 3, 4\} \Rightarrow \delta = 5 \Rightarrow [511, 493, d \geq 5]$-Code

---

$C_5 = \{5, 10, 20, 40, 80, 160, 320, 129, 258\}$

$640 \equiv 129 \bmod 511$

$C_1 \cup C_3 \cup C_5$ enthält $\{1, 2, 3, 4, 5, 6\} \Rightarrow \delta = 7 \Rightarrow [511, 484, d \geq 7]$-Code

---

$C_7 = \{7, 14, 28, 56, 112, 224, 448, 385, 259\}$

$896 \equiv 385 \bmod 511$

$770 \equiv 259 \bmod 511$

$C_1 \cup C_3 \cup C_5 \cup C_7$ enthält $\{1, 2, 3, 4, 5, 6, 7, 8\}$

$\Rightarrow \delta = 9 \Rightarrow [511, 475, d \geq 9]$-Code

---

$C_9 = \{9, 18, 36, 72, 144, 288, 65, 130, 260\}$

$C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_9$ enthält $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\Rightarrow \delta = 11 \Rightarrow [511, 466, d \geq 11]$-Code