7. Lecture

Mittwoch, 4. Oktober 2023 09:56

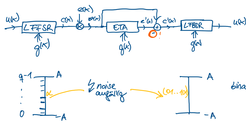
TEAMS wegen Hickhack 😡

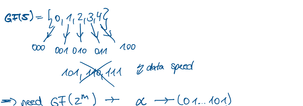
RS codes are cyclic !!! ⇒ faster implement. so fast
↓ ↓
any number of errors can be corrected in optimal way (MDS) shift registers

Code design: given "t" (number of errors to be corrected)

$n-k = 2t$, $n = q-1$, q - prime number $\longrightarrow$ $\alpha \in GF(q)$ (choose primitive element)

$\longrightarrow$ $g(x) = \prod_{i=1}^{n-k} (x-\alpha^i) = g_0 + g_1 x + \dots + x^{n-k}$





$GF(5) = \{0, 1, 2, 3, 4\}$

000 001 010 011 100

101 ~~110~~ ~~111~~ 2 data speed

⇒ need $GF(2^m)$ → $\alpha \rightarrow \underbrace{(0\,1\dots\,1\,0\,1)}_{\text{m-bit long sequence}}$ ⇒ code corrupted ⇒ not robust on data speed ⇒ eee

$GF(8) \rightarrow 2 \cdot 4 \bmod 8 = 0$ ↯ axiom verletzt

Irreducible polynoms

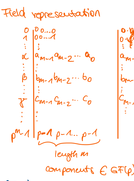
$p(y) \neq p_1(y) p_2(y)$ $\quad \deg(p_i(y)) < p(y)$ $\quad i = 1,2$

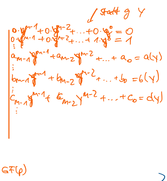
$p(y) = y^2+y+1$
y^3+y+1
y^4+y+1
y^5+y+1
y^6+y+1
⋮

Algebra over $GF(p^m)$

p is prime ($p=2$); $p(y)$; $\deg(p(y)) = m$

Field representation





components $\in GF(p)$

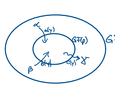
Symbolling domain

operational domain

$\alpha + \beta$
$\vec{a} + \vec{b} \rightarrow a_i + b_i \bmod p$
$\overline{a} + \overline{b} = \overline{c}$

$\alpha * \beta$
$a(y)\,b(y) = g(y)p(y) + d(y)$ $\quad \deg(c(y)) \leq m-1$
$c(y) \in GF(p^m) \rightarrow \gamma$
↓
$\alpha * \beta = \gamma \bmod p(y)$

Algebra over $GF(2^2)$



GIVEN (Lemma) $p(y) = y^2+y+1$

0	0 0	$0\cdot y^1+0\cdot y^0=0$
1	0 1	$0\cdot y^1+1\cdot y^0=1$
2	1 0	$1\cdot y^1+0\cdot y^0=y$
3	1 1	$1\cdot y^1+1\cdot y^0=y+1$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

schiefe Inverse

$1+1=0 \pmod 2$
$1+2=1+y=3$
$1+3=1+y+1=y=2$
$2+2=y+y=0 \pmod 2$
$2+3=y+y+1=1$
$3+3=y+1+y+1$

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$2 \cdot 2 = y \cdot y$ $\quad y^2 \rightarrow p(y): y^2 \rightarrow y+1$
$2 \cdot 3 = y \cdot y + y$ $\quad y \cdot y = y^2 = 1 \cdot (y^2+y+1)(y+1)$
$= y^2 + y = 1$
$3 \cdot 3 = (y+1)(y+1)$
$= y^2 + 2y + 1$
$= y^2 + 1 \quad 2 \,\hat{=}\, 2$
$= 1\,(y^2+y+1) + y$

$y \rightarrow 2 \in GF(2^2)$ → 2 immer primitive element

Powertable of $GF(8) = GF(2^3)$ ← irred. polyn of degree 3

→ $p(y) = y^3+y+1$

0	0 0 0	0
1	0 0 1	1
2	0 1 0	y
3	0 1 1	$y+1$
4	1 0 0	y^2
5	1 0 1	y^2+1
6	1 1 0	y^2+y
7	1 1 1	y^2+y+1

y^0	1
y^1	y
y^2	y^2
y^3	$y+1$
y^4	y^2+y
y^5	y^2+y+1
y^6	y^2+1
y^7	1 repeats sich
y^8	y

$y^3 = 1\,(y^3+y+1) + y + 1$

$y^4 = y \cdot (y^3+y+1) + y^2+y$
$y^4 + y^2 + y$

$y^5 = (y^2+1)(y^3+y+1) + y^2+y+1$
$y^5 + y^4 + y^2 + y^3 + y + 1$ ← wechsen durch polynomial division ⇒ get table in exam

$y^6 = (y^3+y+1)(y^3+y+1) + y^2+1$
$y^6 + y^4 + y^3 + y^4 + y^2 + y^3 + y + 1$

$y^2 \cdot 6 + 2$
$y^2 + y + 1 + y$
$y^2 \,\hat{=}\, 4$

$6 * 2$
$\hat{=} (y^2+y) \cdot y$
$= y^4 \cdot y = y^5 = y^2+y+1 = 7$

$3 * 4$
$(y+1) * (y^2)$
$= y^3 \cdot y^2$
$= y^5 = y+1 = 5$??

Polynoms over $GF(2^m)$

$\alpha(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n \rightarrow \alpha_0, \alpha_1, \dots, \alpha_n \in GF(2^m)$
$\deg(\alpha(x)) = n$

$\alpha(x) = a_0(y) + a_1(y)x + a_2(y)x^2 + \dots + a_n(y)x^n$

$\alpha(x) = y^{i_0} + y^{i_1}x + y^{i_2}x^2 + \dots + y^{i_n}x^n$ → standard form

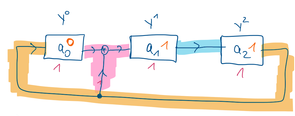
E.g. $\alpha(x) = \overline{5} + \overline{3}x + \overline{6}x^2 + \overline{7}x^3$ $\quad GF(8)$
$\alpha(x) = (y^2+1) + (y+1)x + (y^2+y)x + (y^2+y+1)x^3$
$\alpha(x) = y^0 + y^3x + y^4x^2 + y^5x^3$

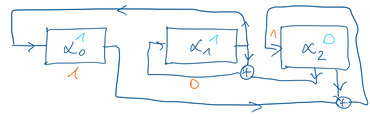
power table always given!

y^0	1
y^1	y
y^2	y^2
y^3	$y+1$
y^4	y^2+y
y^5	y^2+y+1
y^6	y^2+1
y^7	1
y^8	y

$2 * \alpha = y\,(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 \overset{\text{power table}}{=} a_0 y + a_1 y^2 + a_2 (y+1)$
$= a_2 + (a_0 + a_2) y + a_1 y^2$

$4 * \alpha = y^2 (\alpha_0 + \alpha_1 y + \alpha_2 y^2) = \alpha_0 y^2 + \alpha_1 y^3 + \alpha_2 y^4 = \alpha_0 y^2 + \alpha_1 (y+1) + \alpha_2 (y^2+y)$
$= \alpha_1 + (\alpha_1 + \alpha_2) y + (\alpha_0 + \alpha_2) y^2$





"Z" structure of SR

α downloaded

$2 * \alpha = y \cdot (y^2+y) = y+y^4 = y^5 \overset{\text{power table}}{=} y^2+y+1 = 7$

$4 * 3 = y^2 + (y+1) = y^2 \cdot y^3 = y^5 = y^2+1 = 5$

structure ↑ downloaded