# INTRODUCTION TO FINITE FIELDS GF($2^m$)

EXAMPLE . $m=4$, $x^4+x+1=0$, $x^4=x+1$

| | BINARY VECTORS | POLYNOMIALS | EXPONENTS |
|---|---|---|---|
| 0 | 0000 | 0 | |
| 1 | 0001 | 1 | $x^0$ |
| 2 | 0010 | $x$ | $x^1$ |
| 3 | 0011 | $x+1$ | $x^4$ |
| 4 | 0100 | $x^2$ | $x^2$ |
| 5 | 0101 | $x^2+1$ | $x^8$ |
| 6 | 0110 | $x^2+x$ | $x^5$ |
| 7 | 0111 | $x^2+x+1$ | $x^{10}$ |
| 8 | 1000 | $x^3$ | $x^3$ |
| 9 | 1001 | $x^3+1$ | $x^{14}$ |
| 10 | 1010 | $x^3+x$ | $x^9$ |
| 11 | 1011 | $x^3+x+1$ | $x^7$ |
| 12 | 1100 | $x^3+x^2$ | $x^6$ |
| 13 | 1101 | $x^3+x^2+1$ | $x^{13}$ |
| 14 | 1110 | $x^3+x^2+x$ | $x^{11}$ |
| 15 | 1111 | $x^3+x^2+x+1$ | $x^{12}$ |

$x^4+x+1$ is primitive $x^i \neq x^j$ $(i \neq j = 1, \ldots, 2^4-2)$

Addition: $0111+1010=1101$,

$(x^2+x+1)+(x^3+x)=x^3+x^2+1$, $x^{10}+x^9=x^{12}$.

MULTIPLICATION: $x^{10} \cdot x^9 = x^{19} = x^4$,

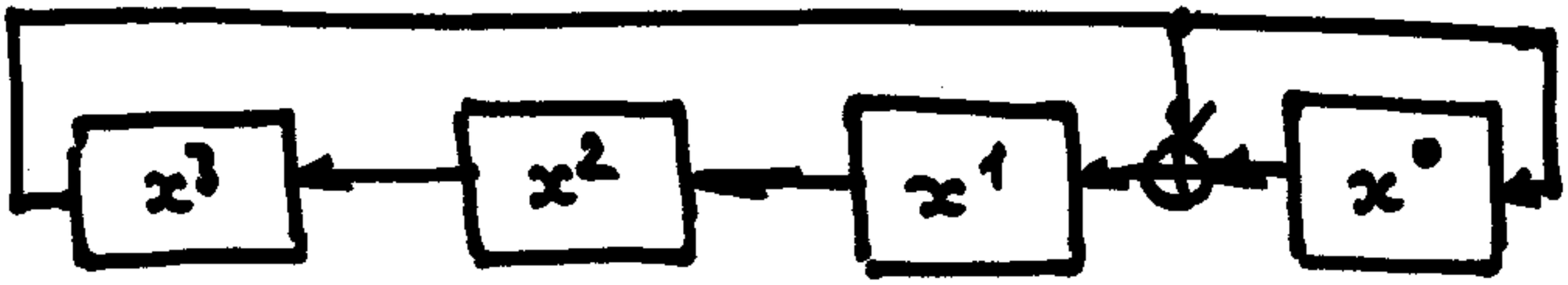
$(x^2+x+1)(x^3+x)=x^5+x^4+x^3+x^3+x^2+x=x^4$

$(0111)(1010)=0011$.

# LFSRS AND POLYNOMIALS OVER FINITE FIELDS

$p(x) = x^4 + x + 1$ PRIMITIVE $x^i \neq x^j$ $i,j = 0,1,\ldots,2^k-2$

AUTONOMOUS LFSR:




∴ IF $S(t)$ IS INT. STATE OF THE LFSR AT MOMENT $t$, THEN:

$S(t+1) = x\,S(t)$ $\quad x^4 = x+1$

EX. $S(t) = 1011 = x^3 + x + 1 \Rightarrow$

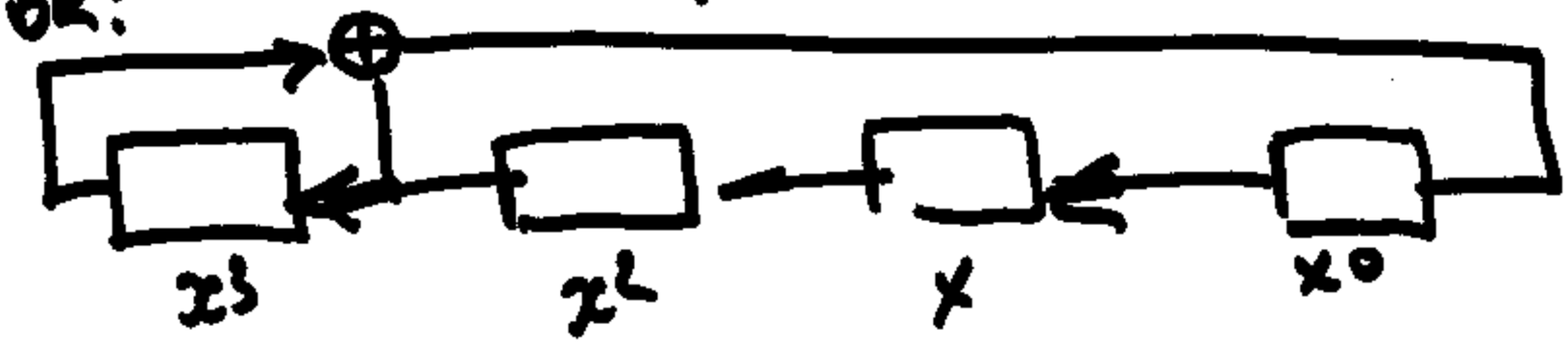
$S(t+1) = x(x^3 + x + 1) = x^4 + x^2 + x = x^2 + 1 = 0101$

or: $S(t) = x^7$ and $S(t+1) = x^8$

THIS PRIMITIVE LFSR generates the SEQUENCE OF PSEUDORANDOM VECTORS

$x^0, x^1, x^2, x^3, x^4, \ldots, x^{14} = 0001, 0010, 0100, 1000,$
$0011, 0110, 1100, \ldots, 1001$

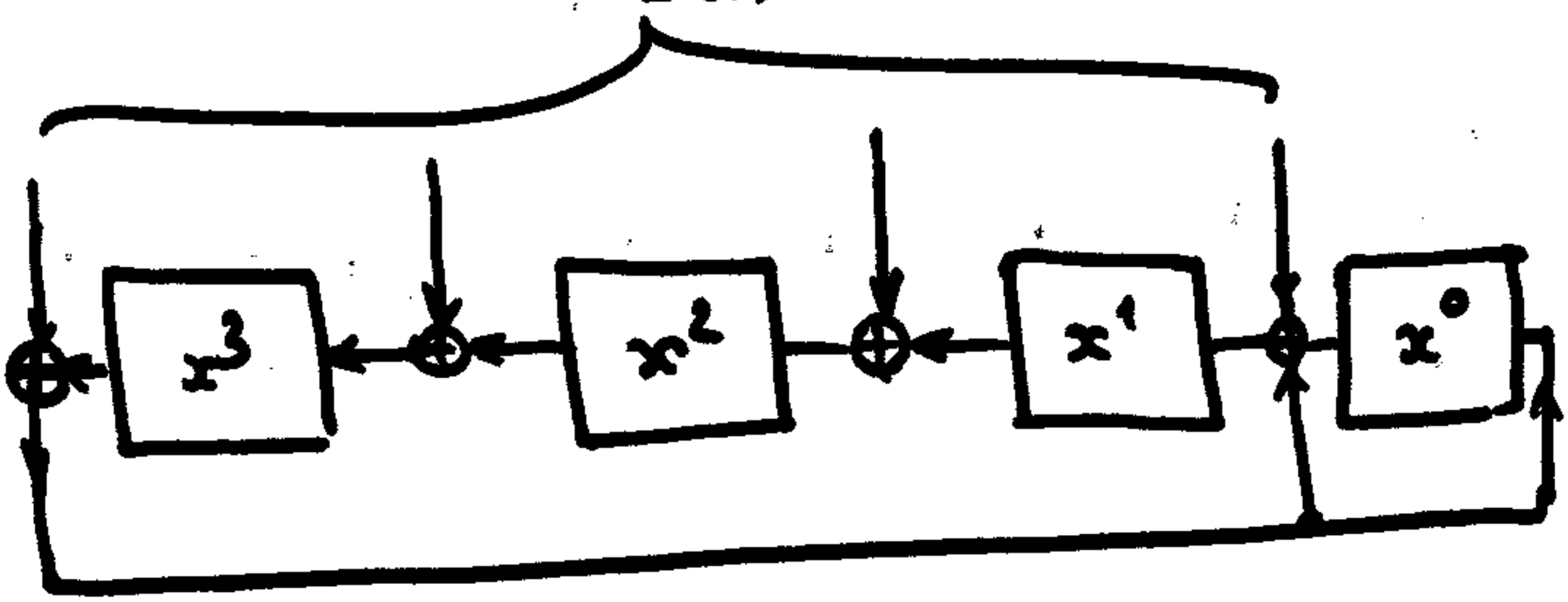
FOR:




$S(t+1) = x^{-1} S(t)$

# LFSRs WITH PARALLEL INPUTS

$P(x) = x^4 + x + 1$




$$S(t+1) = x\,S(t) \oplus y(t+1)$$

TRANSITION FUNCTION OF PARALLEL INPUT LFSRs

Autonomous LFSRs (with $y(t)=0$ for all $t$) can be used as generators of pseudorandom sequences $x^0=1, x, x^2, \ldots, x^{2^m-2}$

! INITIAL STATE OF LFSR

$x^{2^m-1} = x^0$

# Cyclic codes

## BINARY BCH codes

Let $n = 2^m - 1$ . Consider $GF(2^m)$

Let $\alpha$ primitive $\alpha^i \neq \alpha^j$

$(i \neq j \; ; \; i, j = 0, 1, \ldots, 2^m - 2)$ $\quad P(\alpha) = 0$

$l$-error correcting BCH code

$[2^m - 1, \; 2^m - l \cdot m - 1, \; 2l + 1]$ has the

following check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \ldots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \ldots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha^t & \alpha^{2t} & \alpha^{3t} & \ldots & \alpha^{t(n-1)} \end{bmatrix} \Big\} e$$

where $t = 2l - 1$ , $\alpha$ is a binary column of length $m$.

## EXAMPLE

[15,7,5] double error correcting BCH code, $m=4$, $\alpha = 0010$, $\alpha^{15}=1$

$$H=\begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}$$

$$= \left[\begin{array}{ccccc|ccccc|ccccc} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Suppose $e = (0 \ldots 0\overset{i}{1}0 \ldots 0\overset{j}{1}0 \ldots 0)$

Then $$S = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = He = \begin{pmatrix} \alpha^i + \alpha^j \\ \alpha^{3i} + \alpha^{3j} \end{pmatrix}$$

Thus $S_1 = \alpha^i + \alpha^j$

$S_2 = \alpha^{3i} + \alpha^{3j}$

FROM HERE ONE CAN FIND $i, j$ in a unique way.

$$S_2 = S_1 (\alpha^{2i} + \alpha^{i+j} \alpha^{2j}) =$$

$$= S_1 (S_1^2 + \alpha^{i+j})$$

$$\boxed{\alpha^{i+j} = \frac{S_2}{S_1} + S_1^2}$$

Thus $\alpha^i, \alpha^j$ are roots of the following quadratic equation

$$x^2 + S_1 x + \left[\frac{S_2}{S_1} + S_1^2\right] = 0.$$

Since $\alpha^i \neq \alpha^j$:

For $\ell = 1$ BCH codes become HAMMING CODES

RATE OF BCH codes:

$$R = \frac{k}{n} = 1 - \frac{r}{n} = 1 - \frac{\ell m}{2^m - 1}$$

For small $\ell$ and large $m$ $R \to 1$.

Decoding of BCH codes (constructing $e$ from $S$) is a difficult problem

Example $n=15$

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ y=(0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1) \end{matrix} \Rightarrow$$

$$y(x) = x^2+x^3+x^5+x^7+x^8+x^{12}+x^{13}+x^{14}$$

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ Shy=(1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1) \end{matrix}$$

$$Shy(x) = 1+x^3+x^4+x^6+x^8+x^9+x^{13}+x^{14} = x\,y(x)$$

$x^{15}=x^0$

$$y \in V \Leftrightarrow y(\alpha^{2i-1})=0 \qquad i=0,1,\dots,\ell$$

Let $g(x) = x\,y(x) \Rightarrow g(\alpha^{2i-1})=0$

Thus $y \in V \Rightarrow Shy \in V$

BCH codes are cyclic

HAMMING code $[2^m-1,\ 2^m-m-1,\ 3]$ with

$H=[1\ \alpha\ \alpha^2\ \alpha^3\ \dots\ \alpha^{n-2}]$ is cyclic.

Let $n=2^m-1$ $\quad y=(y_0, y_1, \ldots, y_{n-1})$ $\quad . y_i \in \{0,1\}$

We can represent $y$ as

$$y(x) = \sum_{i=0}^{n-1} y_i x^i \qquad (x^n = x^0 = 1)$$

Consider $[15, 7, 5]$ BCH code $V$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}$$

Let $y \in V$ then

$$S = Hy = 0 \Rightarrow \quad S_1 = \sum_{i=0}^{n-1} y_i \alpha^i = 0$$

$$S_2 = \sum_{i=0}^{n-1} y_i \alpha^{3i} = 0$$

thus $y \in V$ iff $\alpha^i$ and $\alpha^{3i}$ are roots of $y(x)$.

In general: $n = 2^m - 1$ $\quad \alpha \in GF(2^m)$

$\alpha^i \neq \alpha^j$ $\quad i, j = 0, 1, \ldots, n-1$ $\quad \alpha^n = \alpha^0$

For $[2^m - 1,\ 2^m - lm - 1,\ 2l+1]$ BCH code $V$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \cdots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \cdots & \alpha^{5(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{2l-1} & \alpha^{2(2l-1)} & \alpha^{3(2l-1)} & \cdots & \alpha^{(2l-1)(n-1)} \end{bmatrix}$$

and $y \in V$ iff $y(x)$ has roots $\alpha, \alpha^3, \alpha^5, \ldots, \alpha^{2l-1}$

or $\boxed{y(\alpha^{2i+1}) = 0 \qquad i = 0, 1, \ldots, l-1}$

$$y(x) = \sum_{i=0}^{n-1} y_i x^i \qquad x^n = x^0$$

$$y = (y_0, y_1, \ldots, y_{n-1})$$

Let

$$sh\,y = (y_{n-1}, y_0, y_1, \ldots, y_{n-2})$$

$$\Rightarrow sh\,y(x) = \sum_{i=0}^{n-1} y_i x^{i+1} = x\,y(x)$$

Cyclic shift of $y$ results in multiplying $y(x)$ by $x$.

Hamming $[2^m-1, 2^m-m-1, 3]$ codes are special case of BCH codes for $l=1$

HAMMING code $V$ with

$$H = [1\ \alpha\ \alpha^2 \dots \alpha^{n-1}]$$

is cyclic. $y \in V$ if $y(\alpha)=0$

For a $[2^m-1,\ 2^m-l\cdot m-1,\ 2l+1]$ $l$-error correcting BCH code with $d=2l+1$ add one bit to every codeword to make number of ones in any codeword even

Then a new extended BCH code has parameters $[2^m,\ 2^m-l\cdot m-1,\ 2l+2]$