NON BINARY ERROR DETECTING / CORRECTING codes

Let $q = 2^b$ $F_q = \{0,1\}^b$ set of all b-bit vectors

and $F_q^n = \{(y_1, \dots, y_n) \mid y_i \in F_q\}$.

V is a q-ary code of length n if $V \subseteq F_q^n$

FOR $x, y \in F_q^n$ $d(x,y)$ is a number of noncoinsiding components in x and y.
HAMMING DISTANCE

$0 \le d(x,y) \le n$ $d(x,y) = 0 \Rightarrow x = y$

For any x, y, z

$$d(x,y) + d(y,z) \ge d(x,z)$$

$d(x, \mathbf{0}) = \|x\|$ - norm (weight) of x

$$d(V) = \min_{x,y \in V} d(x,y)$$

V <u>detects</u> set $E \subseteq F_q^n$ of errors iff.

for any $v \in V$ and $e \in E$

$$v \oplus e \notin V$$

V <u>corrects</u> set $E \subseteq F_q^n$ of errors iff

for any $v, w \in V$, $e^{(1)}, e^{(2)} \in E$

$$v \oplus e^{(1)} \neq w \oplus e^{(2)}$$

Th. Let $E_\ell = \{ e \mid \|e\| \le \ell \}$ - all errors with multiplicity at most ℓ.

V detects E_ℓ iff $d(V) \ge \ell + 1$

V corrects E_ℓ iff $d(V) \ge 2\ell + 1$.

<u>HAMMING BOUND</u>: For any $(n, K, 2\ell+1)$ q ary code

$$q^n \ge q^K \left(\sum_{i=0}^{\ell} (q-1)^i \binom{n}{i} \right)$$

<u>EXAMPLE</u> $q=4$ $(b=2)$ $F_q = F_4$:

00	0
01	1
10	α
11	$\alpha^2 = \alpha + 1$

$P(x) = x^2 \oplus x \oplus 1$

α - primitive

$P(\alpha) = 0$

$\alpha^2 \oplus \alpha \oplus 1 = 0$

Take $n=3$ let $V = \begin{matrix} 0\,0\,0 \\ 1\,\alpha\,\alpha^2 \\ \alpha\,\alpha^2\,1 \\ \alpha^2\,1\,\alpha \end{matrix}$

then $d(V) = 3$

V is <u>linear</u> if $v, w \in V \Rightarrow v \oplus w \in V$

For the previous example: $1\alpha\alpha^2 \oplus \alpha\alpha^2 1 =$
$((1 \oplus \alpha), (\alpha \oplus \alpha^2), (\alpha^2 \oplus 1)) =$
$= (\alpha^2 \ 1 \ \alpha) \in V$

For a <u>linear</u> code V $|V| = q^k$ - number of codewords k - number of information symbols

Generating matrix

$$G = \underbrace{\begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix}}_{n} \Big\} k$$

elements of G are from F_q

<u>EXAMPLE</u>

$$G = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & \alpha^2 \end{bmatrix} \quad (3,2) \text{ code over } F_4$$

Let $v_1, v_2, \ldots, v_k$ are rows of G

then $v_1, v_2, \ldots, v_k$ are linearly independent,

$$c_1 v_1 \oplus c_2 v_2 \oplus \ldots \oplus c_k v_k \neq 0$$

for any $c_1, \ldots, c_k \in F_q$

G can always be represented as

$$G = [\underbrace{I_k}_{k} \mid \underbrace{P}_{n-k}]^{k}$$ where I_k is the $(k \times k)$ identity matrix

Denote H a check matrix for V

Then H is the $(n-k) \times n$ q-ary matrix

such that

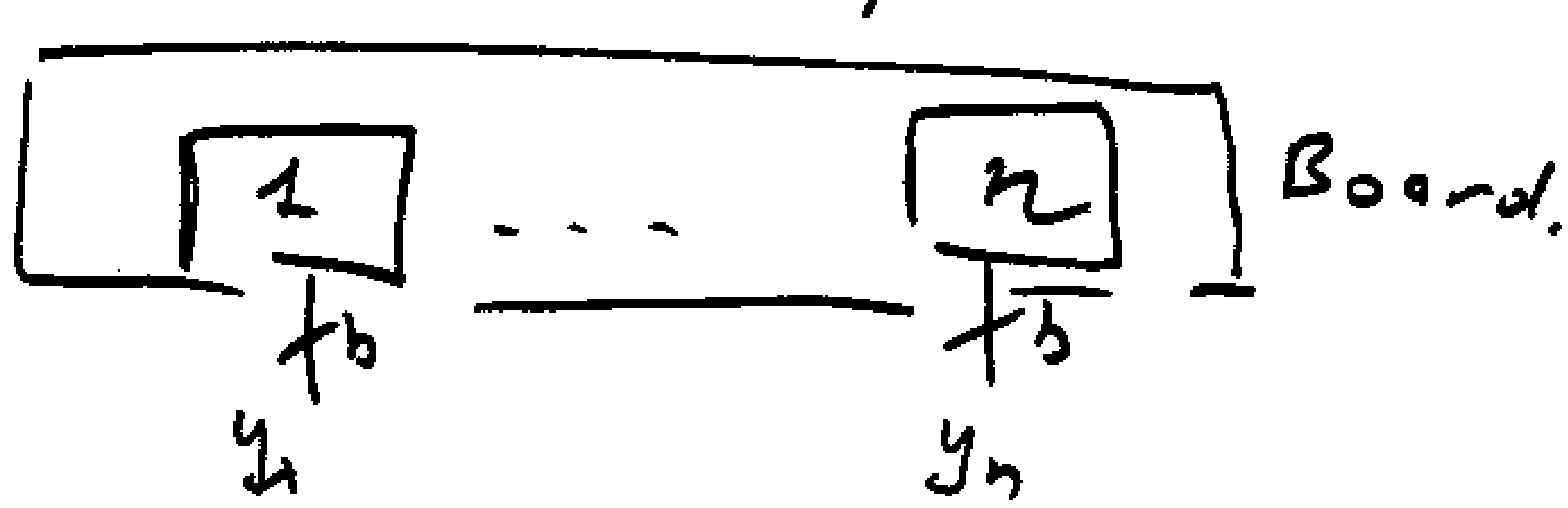
$$Hv = 0 \quad \text{for any } v \in V$$

If $G = [I_k \mid P]$ then

$$H = [P^{TR} \mid I_{n-k}]$$

TRANSPOSED P.

For many applications y_i is the b-bit response of a component i



we assume $q >> n$ For example for $b=32$ $q=2^{32}$ and $n \simeq 100$

Ⓣ. For any q-ary (n,k) code $\mathcal{V}$

$\underline{d(\mathcal{V}) \le n-k+1 = r+1}$ - Singleton Bound

Detection of single errors

$H = [1\ 1 \dots 1]$ $r=1.$ $(k+1, k, 2)$ code.

$v = (v_1, \dots, v_n) \in \mathcal{V} \iff v_1 \oplus v_2 \oplus \dots \oplus v_n = 0$

$v_i \in F_q$

Since $e = (0 \dots 0\ e_i\ 0 \dots)$ $\hat{y} = y \oplus e$

$y \in \mathcal{V}$

$H\hat{y} = H(y \oplus e) = He = e_i \neq 0.$

Correction of Single errors $\quad d=3$

$$H(y \oplus e^{(1)}) \neq H(v \oplus e^{(2)}) \qquad y, v \in V$$

$$He^{(1)} \neq He^{(2)}$$

$$e^{(1)} = (0 \ldots 0\ e_i^{(1)}, 0 \ldots, 0)$$

$$e^{(2)} = (0 \ldots 0\ e_j^{(2)}\ 0, \ldots, 0)$$

Let

$$H = [\,h_1\ h_2 \ldots\ h_n\,] \qquad h_i \text{ column in } H$$

then

$$He^{(1)} = h_i e_i^{(1)}$$

$$He^{(2)} = h_j e_j^{(2)} \qquad e_i^{(1)}, e_j^{(2)} \in F_q$$

Thus, if h_i is a column in H then all multiples ch_i are not columns of H.

~~Example~~ since $n \le q-1$ we can take

$$H = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \end{bmatrix} \qquad \begin{matrix} \alpha^i \neq \alpha^j \\ \alpha^i, \alpha^j \in F_q \end{matrix}$$

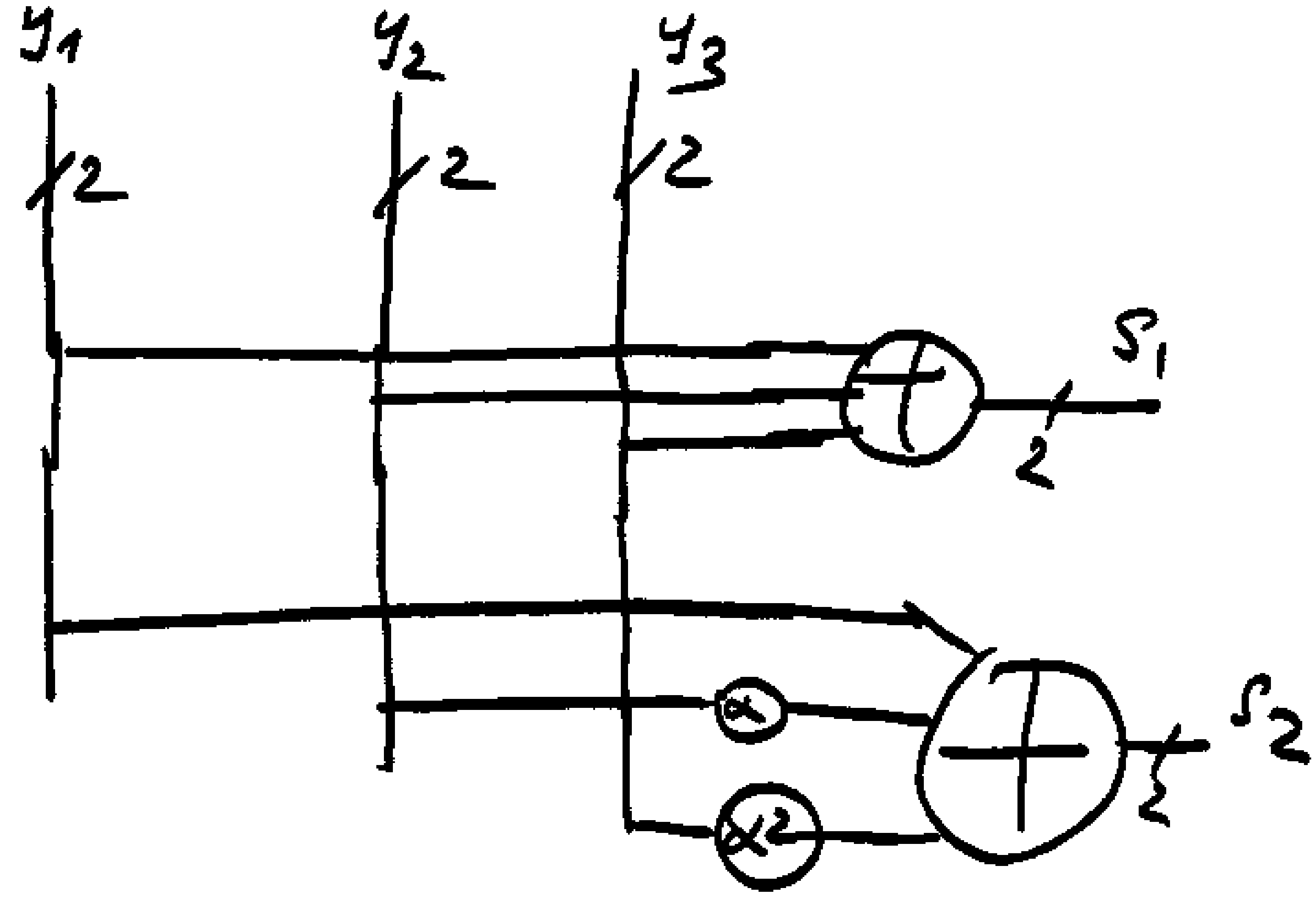
Thus we have $(k+2, k, 3)$ single error correcting codes. These codes are the best since $r = 2 = d-1$

(For binary case $r = \lceil \log_2(n+1) \rceil$ for Hamming in our case $(q > n)$ $r = 2$)

<u>Example</u> $n = 3$ then

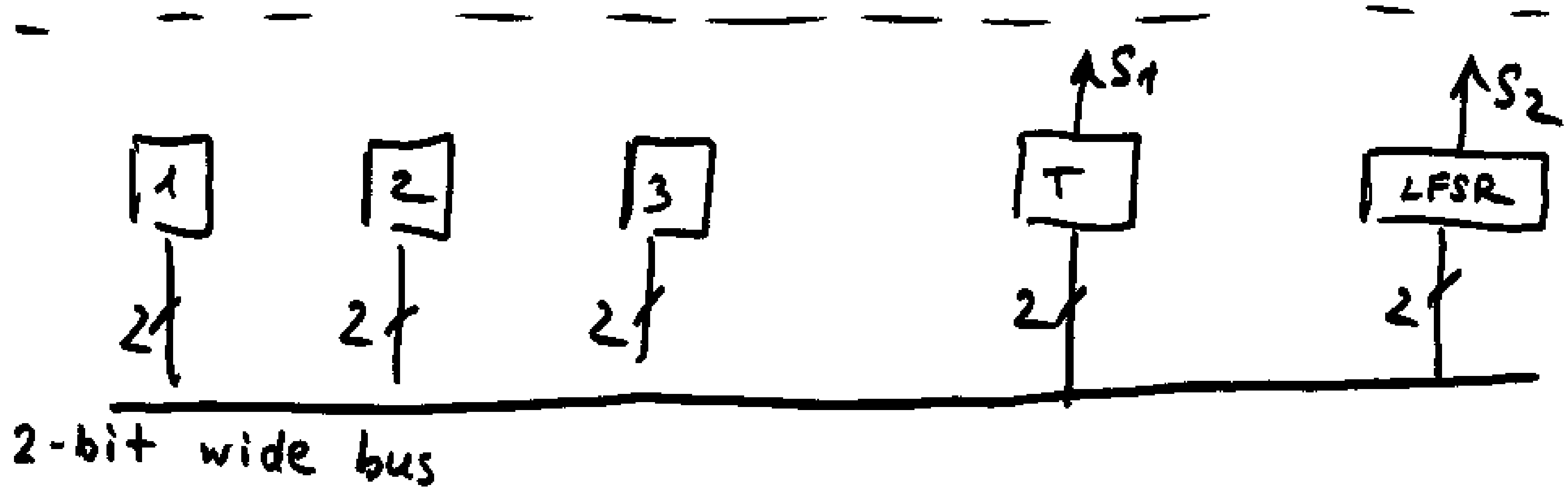
$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{bmatrix} \cancel{\begin{matrix} 1 \\ \alpha^3 \end{matrix}} \qquad \begin{matrix} \alpha = 10 \\ \alpha^2 = 11 \end{matrix} \qquad q = 4$$

For this code



Combinational network computing

syndrome $S = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_1 \oplus \alpha y_2 \oplus \alpha^2 y_3 \end{pmatrix}.$



sequential network computing $\begin{pmatrix} s_1 \\ s_2 \end{pmatrix}$

T - is the 2-bit T flip-flop register

LFSR is the 2-bit LFSR with $P(x) = x^2 \oplus x \oplus 1$
$P(\alpha) = 0$