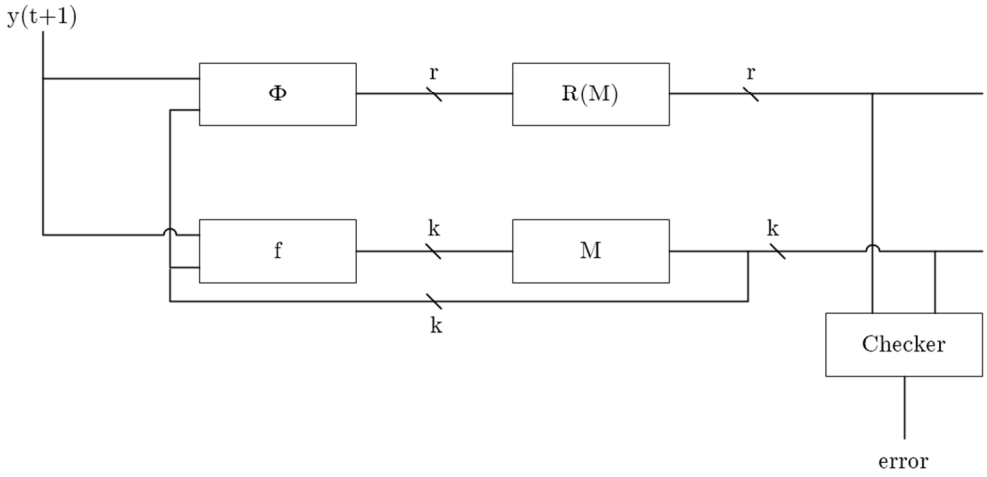
EC500
Design of Secure and Reliable Hardware

Lecture 15

Mark Karpovsky

1 Protecting Sequential Devices with Systematic Codes

For the original device, we have $D(t+1) = f\big(y(t+1), D(t)\big)$ and $Z(t+1) = D(t+1)$. We design the predictor to be $R\big(D(t+1)\big) = R\left(f\big(y(t+1), D(t)\big)\right) = f\big(y(t+1), D(t)\big) \cdot P = \varphi\big(y(t+1), D(t)\big)$, where $D(t) \in \{0,1\}^k$, $R\big(D(t)\big) \in \{0,1\}^r$.



1.1 Sequential Fault-Tolerant Networks (Abstract synthesis)

State assignment for internal states by codewords of error correcting/detecting codes.

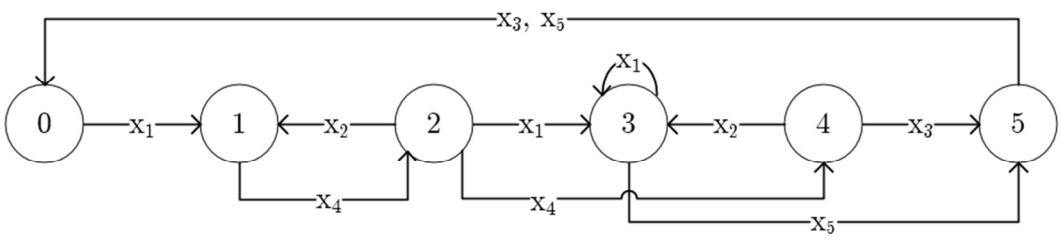
Example

Correction of single errors $l_c = 1$

We denote the number of redundant FFS as r, where $r \geq \log_2 (k + r + 1)$, and n_a as the number of internal states, where $k = \lceil \log_2 (n_a) \rceil$.

Inputs assumed to be fault-free.

1.



$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \; G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \; k = 3, \; r = 3$$

State Assignment –

0 – 000 000

1 – 100 011

2 – 010 101

3 – 110 110

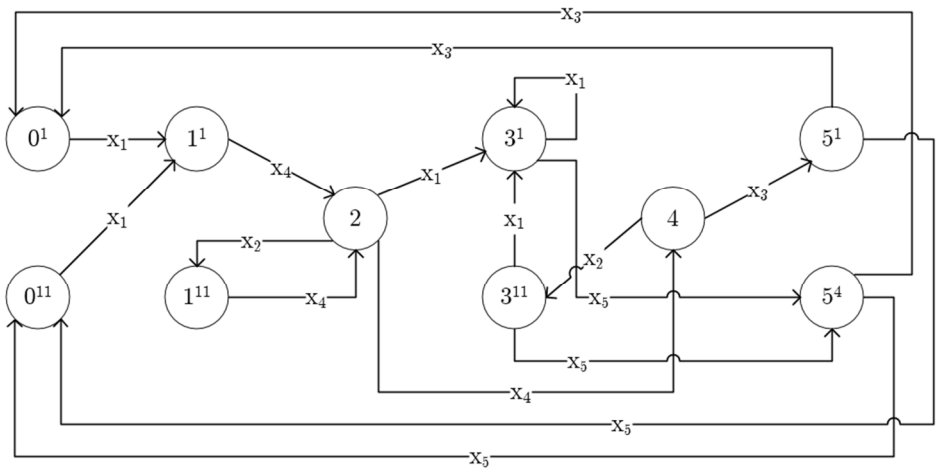
4 – 001 110

5 – 101 101

6 – 011 011

2. Splitting Internal States

Redundancy at the abstract level (the same example)



State Assignment –

$0^1 - 0000$, $5^1 - 0111$ } For x_3

$0^{11} - 0001$, $5^{11} - 0110$ } For x_5

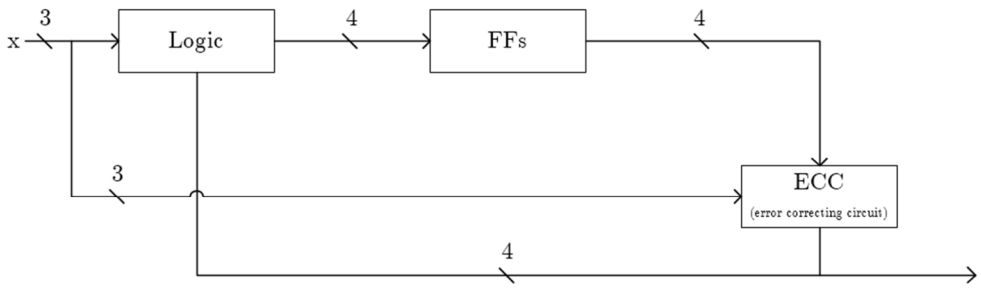
$1^1 - 0010$, $3^1 - 0101$ } For x_1

$1^{11} - 0100$, $3^{11} - 0011$ } For x_2

$2 - 1000$, $4 - 1111$ } For x_4

Total number of FFs is 4.

Block Diagram for 2):



3. Partial Splitting of Internal States

   Select the following grouping of inputs $\lambda_0 = (\{x_1, x_2\}, \{x_3, x_5\}, \{x_4\})$. Then the state assignment is as follows:

   $\left.\begin{matrix} 0-000 \\ 5-111 \end{matrix}\right\}$ For $\{x_3, x_5\}$

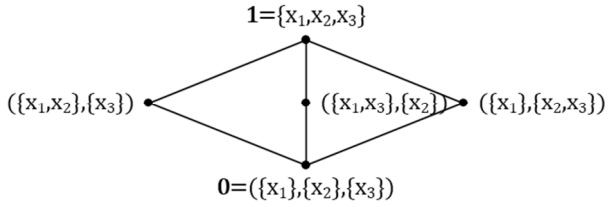
   $\left.\begin{matrix} 1-001 \\ 3-110 \end{matrix}\right\}$ For $\{x_1, x_2\}$

   $\left.\begin{matrix} 2-010 \\ 4-101 \end{matrix}\right\}$ For $\{x_4\}$

   Total number of FFS is 3. Optimal number of FFs is the same as for the case when there were no error correction. The same block-diagram as in 2). For 3) we split only those internal states which are reachable by inputs from different blocks of the grouping (no splitting for λ_0).

2 Minimization of the Number of FFS by Optimal Selection of a Grouping of Inputs

Denote $\mathbf{1} = \{x_1, x_2, x_3, x_4, x_5\}$, $\mathbf{0} = (\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\})$. For two groupings λ_1 and λ_2, we denote $\lambda_1 \geq \lambda_2$ if blocks of λ_2 are subsets of blocks of λ_1 $(\{x_1, x_2, x_3\}, \{x_4, x_5\}) \geq (\{x_1, x_2\}, \{x_3\}, \{x_4, x_5\})$. For any λ: $\mathbf{0} \leq \lambda \leq \mathbf{1}$. Set of groupings λ form a partially ordered set called a lattice. We denote this lattice as L_x. For 3 inputs, x_1, x_2, x_3:



Denote $n(\lambda)$ as the total number of FFs required for grouping λ. For the previous example,

λ	**1**	**0**	λ_0
$n(\lambda)$	6	4	3

For $l_c = 1$, $n(\mathbf{1}) = \lceil \log_2 n_a \rceil + r$ where $r \geq \log_2 (\lceil \log_2 n_a \rceil + r + 1)$.

Problem: Find $\min_{\lambda \in L_x} n(\lambda)$

Minimization of a function defined on the lattice L_x. For this example, $\min_{\lambda \in L_x} n(\lambda) = n(\lambda_0) = 3$.