EC500
Design of Secure and Reliable Hardware

Lecture 14

Mark Karpovsky

1 Detection of Unidirectional Attacks

Unidirectional attacks only include $0 \to 1$ or $1 \to 0$ errors. It may happen that for one message we have $0 \to 1$ errors and for another, $1 \to 0$ errors.

1.1 m out of n Codes

These are nonsystematic codes. The size of the set of codewords $|C| = \binom{n}{m}$, implying that $|C|$ is maximum if $m = \left\lfloor \frac{n}{2} \right\rfloor$. The special case when $m = 1$ is called 1-hot coding. 1 out of 2 for dual rail and 2 out of 5 for decimal characters.

1.2 Berger Codes

These are systematic codes. $(y\omega) \in C$ iff ω is a binary representation of a number of zeros in y. $y \in GF(2^k)$, $\omega \in GF(2^r)$, and $r = \lceil \log_2 (k+1) \rceil$.

Example
$k = 10$, $r = 4$
A valid codeword could be $(1001001001\ 0110)$ where $y = (1001001001)$ and $\omega = (0110)$

- For detection of all unidirectional errors, the best is $\left\lfloor \frac{n}{2} \right\rfloor$ out of n codes (nonsystematic) with $\binom{n}{\left\lfloor \frac{n}{2} \right\rfloor}$ codewords.
- Systematic codes for detection of all unidirectional errors can use Berger codes with $r = \lceil \log_2 (k+1) \rceil$.

1.3 Redundancy Estimations

$k -$ the number of outputs in a PLA
$N_0 -$ maximum number of 0s in a fault-free output vector
$r -$ the number of redundant outputs (the number of FFs in the counter)

$r \le \lceil \log_2 (N_0 + 1) \rceil \le \lceil \log_2 (k+1) \rceil$

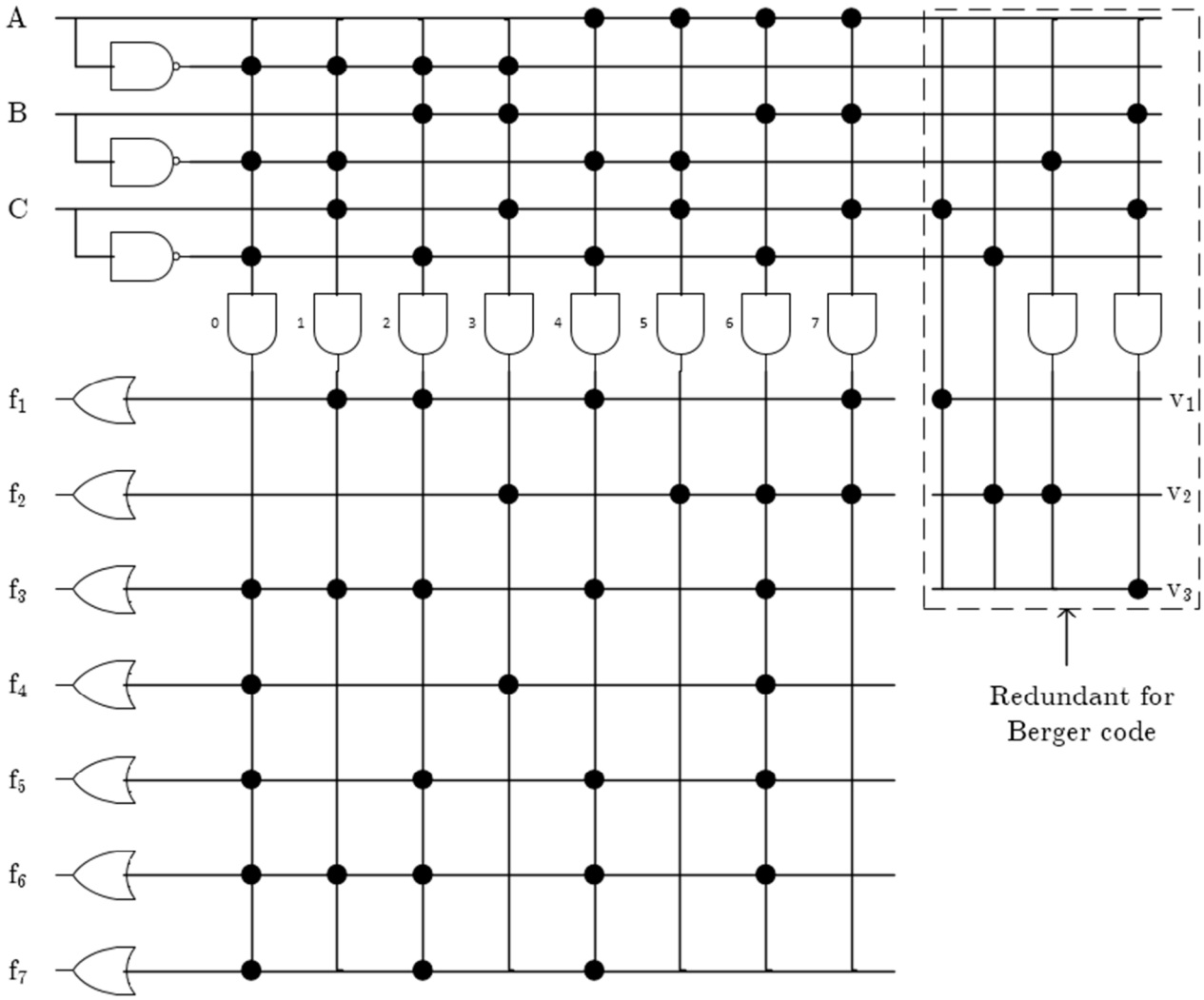
1.4 Modified Berger Codes

Let $n_1, n_2, \cdots, n_t$ be different numbers of 0s in the output vectors for the original device where $0 \le n_1 \le n_2 \le \cdots \le n_t \le N_0$. For the next example, $n_1 = 2$, $n_2 = 4$, $n_3 = 5$, $n_4 = 6$ and we encode $n_1 \leftrightarrow 0 \cdots 0$, $n_2 \leftrightarrow 0 \cdots 01$, $n_3 \leftrightarrow 0 \cdots 010$ into redundant bits with $r = \lceil \log_2 t \rceil$. See the example on the next page where $2 \leftrightarrow 00$, $4 \leftrightarrow 01$, $5 \leftrightarrow 10$, $6 \leftrightarrow 11$ for $r = 2$.

Example

$m = 3,\ k = 7 \rightarrow r = 3$

										Berger code			Modified Berger code	
										Redundant bits				
A	B	C	f_1	f_2	f_3	f_4	f_5	f_6	f_7	v_1	v_2	v_3	v_1	v_2
0	0	0	0	0	1	1	1	1	1	0	1	0	0	0
0	0	1	1	0	1	0	0	1	0	1	0	0	0	1
0	1	0	1	0	1	0	1	1	1	0	1	0	0	0
0	1	1	0	1	0	1	0	0	0	1	0	1	1	0
1	0	0	1	0	1	0	1	1	1	0	1	0	0	0
1	0	1	0	1	0	0	0	0	0	1	1	0	1	1
1	1	0	0	1	1	1	1	1	0	0	1	0	0	0
1	1	1	1	1	0	0	0	0	0	1	0	1	1	0



2 Correction of Unidirectional Error with Multiplicity l

- For $l = 1$, use Hamming codes
- For unidirectional errors when only $0 \to 1$ distortions are possible, $y \to y + e$ (this is or)
  For $1 \to 0$ distortions, use $y \to y \cdot \bar{e}$
- For $0 \to 1$ errors, the necessary and sufficient condition is that for any two codewords v_1 and v_2, $v_1 + e_1 \neq v_2 + e_2$ for $\|e_1\|, \|e_2\| \leq l$.
  For $1 \to 0$ errors, $v_1 \cdot \bar{e_1} \neq v_2 \cdot \bar{e_2}$ or $\overline{v_1} + e_1 \neq \overline{v_2} + e_2$.

Thus the problem is to construct a maximum code C for a given n and l such that $\forall v_1, v_2 \in C$, $\forall e_1, e_2$ such that $\|e_1\|, \|e_2\| \leq l$, we have the result $v_1 + e_1 \neq v_2 + e_2$ and $\overline{v_1} + e_1 \neq \overline{v_2} + e_2$. This problem is still open even for $l = 2$.

3 Codes Detecting All Symmetrical Errors with Multiplicity up to t and Unidirectional Errors with Any Multiplicity

t-ED/AUED codes V has $d(V) = t + 1$ and a $2t$-ED/AUD code is sthe same as a t-error correcting and AUED code $\to 2t$-ED/AUED. These codes are useful since faults affecting a large number of output lines often result in unidirectional errors.

3.1 Construction for t-ED/AUED Codes

1. For a given k (number of information bits), construct a best $(k + r_H, k, d = t + 1)$ code with distance $t + 1$.
2. For any codeword v add r_u bits, $r_u = \left\lceil \log_2 \left(\left\lfloor \frac{1}{d}(k + r_H) \right\rfloor + 1 \right) \right\rceil$, which are <u>negation</u> of a binary representation for $\left\lfloor \frac{\|V\|}{d} \right\rfloor$, $\|V\|$ is the Hamming weight.

- This construction results in t-ED/AUED codes which are systematic codes. These codes are nonlinear.
- For $t = 0$ $(d = 1)$, this construction produces the Berger code.
- For this construction, r_H bits provide for a given distance $d = t + 1$.
  $r_u = \left\lceil \log_2 \left(\left\lfloor \frac{1}{t+1}(k + r_H) \right\rfloor + 1 \right) \right\rceil$ bits provide for detection of all unidirectional errors.

<u>Example</u>
2-ED/AUED or a 1-EC/AUED for $k = 4$

For the (7,4) Hamming code with $r_H = 3$ and $d = 3$. We construct the generating matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

We have the following valid codewords where $r_u = \left\lceil \log_2 \left(\left\lfloor 1 + \frac{7}{3} \right\rfloor \right) \right\rceil$:

k				r_H			r_u	
0	0	0	0	0	0	0	1	1
1	0	0	0	1	1	0	1	0
0	1	0	0	1	0	1	1	0
1	1	0	0	0	1	1	1	0
0	0	1	0	0	1	1	1	0
1	0	1	0	1	0	1	1	0
0	1	1	0	1	1	0	1	0
1	1	1	0	0	0	0	1	0
0	0	0	1	1	1	1	1	0
1	0	0	1	0	0	1	1	0
0	1	0	1	0	1	0	1	0
1	1	0	1	1	0	0	1	0
0	0	1	1	1	0	0	1	0
1	0	1	1	0	1	0	1	0
0	1	1	1	0	0	1	1	0
1	1	1	1	1	1	1	0	0

This is a (9,4) 1-EC/AUED code.