EC500
Design of Secure and Reliable Hardware

Lecture 5

Mark Karpovsky

Linear Codes

Let Z_q^n be an n-dim space over $GF(q)$. q is a power of prime. Code $C \subseteq Z_q^n$ is linear iff C is a subspace. $(x, y \in C \to x + y \in C,\ a \in GF(q), x \in C \to ax \in C)$

If C is a k-dim subspace of Z_q^n, then we will write that C is a (n, q^k) code. ($|C| = q^k$) Then, C has k information digits and $r = n - k$ check digits.

Examples:
1. Repetition codes are linear
2. Parity codes are linear
3. ISBN code is linear

For linear codes, $d(x, y) = \|x + y\| \to$ Code distance = smallest of weights of the non-zero codewords.

Consider (n, q^k) code $C \subseteq Z_q^n$, C is a k-dim subspace in Z_q^n. Let $v_1, v_2, \cdots, v_k \in C$ for a basis for C. Consider the matrix $G = \left.\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}\right\} k$. G is known as a generating matrix for C. The same code C can have many generating matrices.

$\underbrace{\quad}_{n}$

Example: $q = 2$, $n = 5$
$C = \{00000, 01011, 10110, 11101\}$, C is linear, $k = 2$, $|C| = 2^k = 4$
$G_1 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}, G_2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}$

Linear Vector Spaces over Finite Fields

Let q be a prime, consider $GF(q)$ and Z_q^n. $x = (x_1, \cdots, x_n) \in GF(q)$ iff $x_i \in GF(q)$.

$x, y \in Z_q^n$:
1. $x + y = (x_1 + y_1, \cdots, x_n + y_n)\ (mod(q))$
2. $ax = (ax_1, ax_2, \cdots, ax_n)$, $a \in GF(q) \to$ a scalar
3. $a(x + y) = ax + ay$, $a \in GF(q)$
4. $a(bx) = (ab)x$, $a, b \in GF(q)$

Z_q^n is a n-dimensional linear vector space over $GF(q)$. Let $V \subseteq Z_q^n$ and if
1. $x, y \in V$, $x + y \in V$
2. $a \in GF(q)$, $x \in V$, $ax \in V$

Then V is a subspace of Z_q^n.

Let $v_1, v_2, \cdots, v_r \in Z_q^n$. Consider a linear combination $a_1v_1 + a_2v_2 + \cdots + a_rv_r$, $a_i \in GF(q)$. $v_1, v_2, \cdots, v_r$ are linear dependent iff $\exists\ a_1, a_2, \cdots, a_r$ not all equal 0 such that $a_1v_1 + a_2v_2 + \cdots + a_rv_r = 0$. Otherwise $v_1, v_2, \cdots, v_r$ are linearly independent.

A linear independent set of vectors are called basis iff all linear combinations of these vectors form the subspace and all these linar combinations are different.

Examples: $q = 2$, $n = 4$
1. {0001,0010,0100,1000} is a basis for Z_2^4
2. {0011,0010,1100,1000} is a basis for Z_2^4
3. {0011,0110,1100,1001} is not a basis for Z_2^4

Let $v_1, v_2, \cdots, v_r$ be a basis for Z_q^n, then: $v_i \in Z_q^n$
1. $r = n$
2. Any vector $x \in Z_q^n$ can be represented in a unique way as $a_1v_1 + a_2v_2 + \cdots + a_nv_n = x$.

Remark:
Z_q^n is a n-dimentional space over $GF(q)$ iff q is a prime or power of prime.

Equivalent Transformations of Linear Codes
Two codes are equivalent iff: they can be obtained by
1. Permutation of digits
2. Multiplication of all digits in the same position by a scalar

Example: $q = 3$, $n = 3$, $k = 2$

$$C_1 = \begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{matrix}, \quad C_2 = \begin{matrix} 0 & 0 & 0 \\ 2 & 2 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 2 & 2 \\ 2 & 1 & 2 \end{matrix}$$

C_1 and C_2 are equivalent (columns 1 and 3 are transposed and column 2 multiplied by $2\ mod(3)$)

T. Two $(k \times x)$ matrices generate equivalent (n, q^k) codes over $GF(q)$ if one matrix can be obtained from another by the sequence of operations of the following types:
(R1) Permutation of rows
(R2) Multiplication of a row by a non-zero scalar
(R3) Addition of a scalar multiple of one row to another
(C1) Permutations of columns
(C2) Multiplication of a column by a non-zero scalar

T. Get G to be a generating matrix of (n, q^k) code (G is a $(k \times x)$ q-ary matrix). Then using *(R1)÷(R3)* and *(C1)*, *(C2)*, G can be transformed into a standard form.

$$G = [I : P]$$

Where: I $(k \times k)$ identity matrix
P $\big(k \times (n-k)\big)$ matrix

Parity Check Matrices
Syndrome Decoding

Let $u = (u_1, \cdots, u_n) \in Z_q^n$
$v = (v_1, \cdots, v_n) \in Z_q^n$
$\langle u, v \rangle = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n$
$\langle u, v \rangle \in Z_q^n -$ scalar product of u and v

If $\langle u, v \rangle = 0$ then $u \perp v$, u is orthogonal to v

Example:
$\langle 2011{,}1210 \rangle = 0$
$\langle 1212{,}2121 \rangle = 2$

T. $\langle u, v \rangle = \langle v, u \rangle$
T. $w, u, v \in Z_q^n$, $\lambda, \mu \in Z_q$
$\langle \lambda u + \mu v, w \rangle = \lambda \langle u, w \rangle + \mu \langle v, w \rangle$

Let C be a (n, q^k) code, $C \subseteq Z_q^n$. Then $C^\perp$ (orthogonal to C or dual to C),
$C^\perp = \{v \in Z_q^n | \langle v, u \rangle = 0\ for\ all\ u \in C\}$

Examples:

1. $q = 2,\ n = 4$

$$C = \begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix} \Rightarrow C^{\perp} = C,\ C \text{ is self-dual}$$

2. $q = 2,\ n = 3$

$$C = \begin{matrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{matrix} \rightarrow G_C = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \Rightarrow k_c = 2,\ C^{\perp} = \begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix} \Rightarrow k_c = 1$$

T. $(C^{\perp})^{\perp} = C$

T. Let G_c be a generating matrix, then $v \in C^{\perp} \Leftrightarrow G_C v = 0$

T. If $\dim C = k_c \Rightarrow \dim C^{\perp} = k_{C^{\perp}} = n - k_C$ and $C^{\perp}$ is a (n, q^{n-k_c}) code

Consider a generating matrix for $C^{\perp}$, $H = G_{C^{\perp}}$. We will call H a parity check matrix for C.

$$H = \underbrace{\left[\qquad\qquad\right]}_{n}\Big\}n - k \qquad k = k_c$$

T. $HG^{TR} = 0 -$ matrix of all zeros

For any $v \in C$, $Hv = 0 -$ vector of all zeros

Any code C can be defined by its generating matrix G or check matrix H.

$C = \{v \in Z_q^n | HV = 0\}$

For $C = \begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}$, $C^{\perp} = C \rightarrow G = H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

$$v \in C \rightarrow H \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = 0 \rightarrow \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = \begin{bmatrix} v_1 + v_2 \\ v_3 + v_4 \end{bmatrix} = 0 \rightarrow \begin{cases} v_1 + v_2 = 0 \\ v_3 + v_4 = 0 \end{cases} \Rightarrow \text{parity checking equations}$$

Example:

Consider $(n, 2^{n-1})$ binary parity code. For this code C,

$v \in C \Leftrightarrow v_1 + v_2 + \cdots + v_n = 0 \Leftrightarrow H = [1 \quad 1 \quad 1 \quad \cdots \quad 1],\ r = n - k = 1$

T. Let C be a (n, q^k) code and $G = \overbrace{\left[I_k \vdots P\right]}^{n}\Big\}k$ is the generating matrix for C. Then

$H = \overbrace{\left[-P^{TR} \vdots I_{n-k}\right]}^{n}\Big\}n - k$. $-P^{TR}$ is P transposed multiplied by (-1). $H = [-P^{TR} \vdots I_{n-k}]$ is a standard form for the check matrix.

Example: $q = 2,\ n = 7,\ k = 4$

$$G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right], \text{ then } H = \left[\begin{array}{ccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \text{ (For the binary case } \ominus = \oplus)$$

Example:

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

↑ codeword of C

Detection of Single Errors (Parity Checking)

$d(U) = 2$

One equation $(r = 1)$: $(v_1, \cdots, v_n) \in U$ if $v_1 \oplus v_2 \oplus \cdots \oplus v_n = 0$

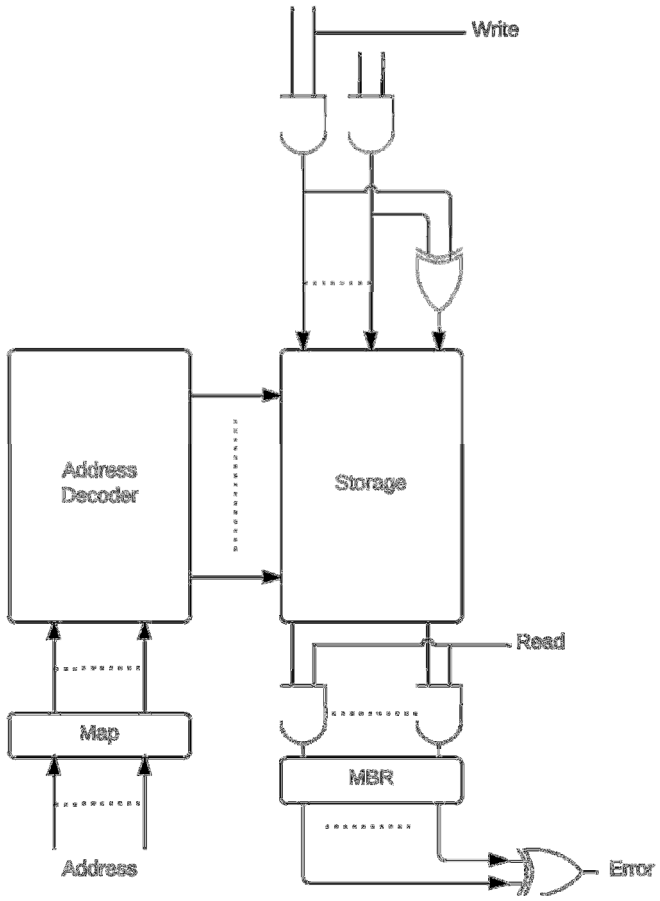
$k = n - 1$

Detects all errors of *odd* multiplicities used for memories and buses

Examples: $n = 4$, $k = 3$

v_1	v_2	v_3	v_4	
0	0	0	0	
0	0	1	1	
0	1	0	1	
0	1	1	0	, v_4 is the parity (check) bit
1	0	0	1	
1	0	1	0	
1	1	0	0	
1	1	1	1	

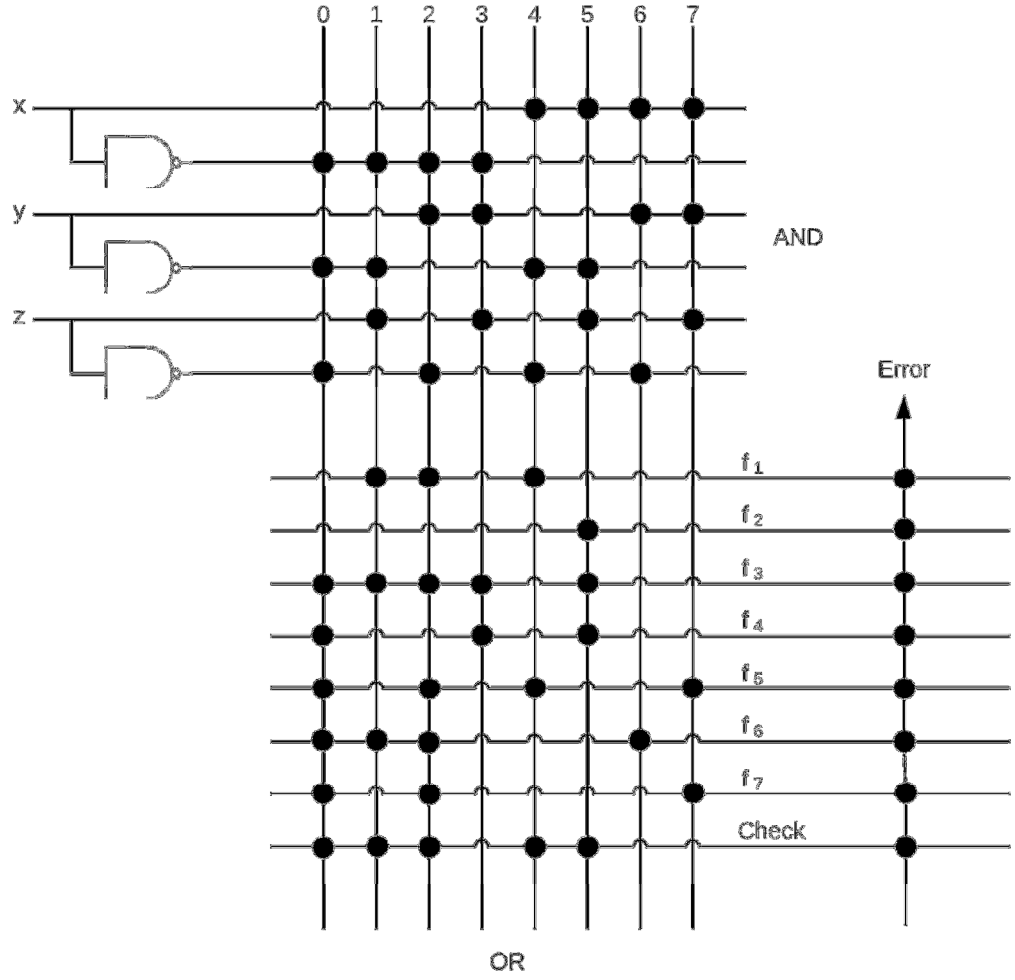
Memory with Parity Checking



Parity Prediction for PLAs

Example: $m = 3,\ k = 7,\ r = 1$

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Check
0	0	0	1	1	1	1	1	1
1	1	0	1	0	0	1	0	1
2	1	0	1	0	1	1	1	1
3	0	0	1	1	0	0	0	0
4	1	0	0	0	1	0	0	0
5	0	1	1	1	0	0	0	1
6	0	0	0	0	0	1	0	1
7	0	0	0	0	1	0	1	0



Detection of Single Errors

1. Duplication
2. 1-d parity
3. Dual rail design → Also Detects: Power analysis attacks
   Electromagnetic emission attacks

Power consumption is independent of data

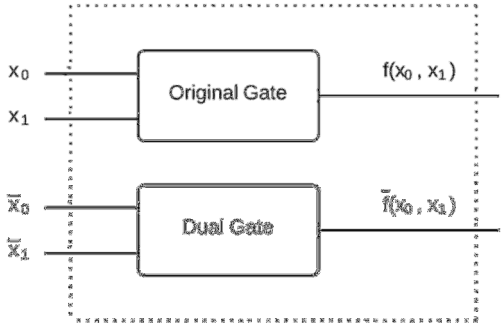
Represent $0 - 01$
$1 - 10$

Every wire is replaced by two wires. Let $f(x_0, \cdots, x_{n-1})$ be a Boolean function. Then $\varphi(x_0, \cdots, x_{n-1})$ is dual to $f(x_0, \cdots, x_{n-1})$ if $\varphi = f^D \rightarrow \varphi(x_0, \cdots, x_{n-1}) = \bar{f}(\bar{x}_0, \cdots, \bar{x}_{n-1})$. If $\varphi = f$ then f is self dual.

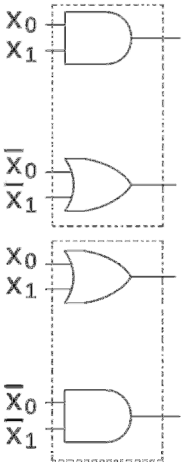
Example: $f(x_0, x_1, x_2) = x_0 \oplus x_1 \oplus x_2$

Original	Dual
AND	OR
OR	AND
NAND	NOR
NOR	NAND
XOR	XNOR
NOT	NOT

Every gate is replaced by two gates

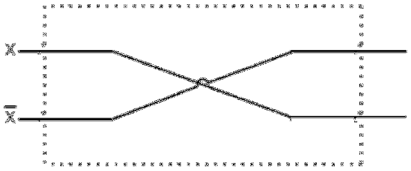


Dual Rail Gates



AND

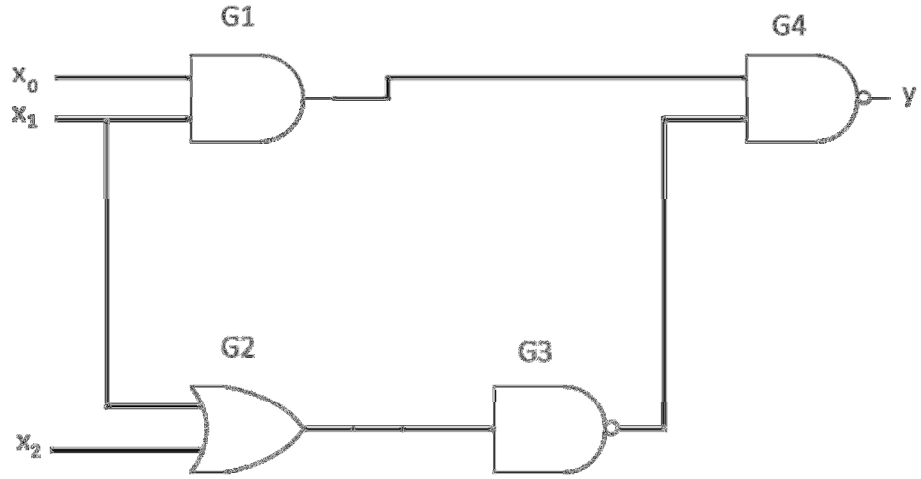
OR

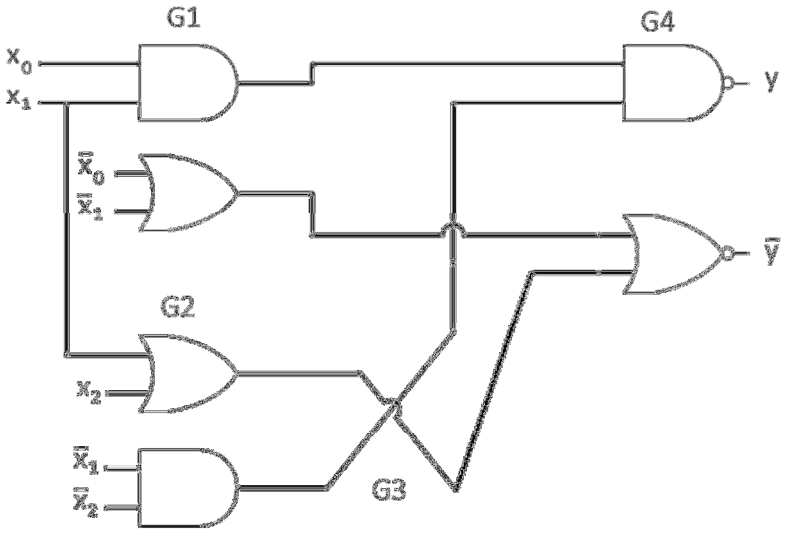


NOT

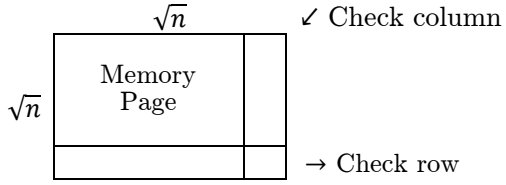
Example of Dual Rail Design

Original Network:





Two-dimensional Parity Checking



Correct: all single errors
Detect all single, double, and triple errors

Example:

↙ Check column

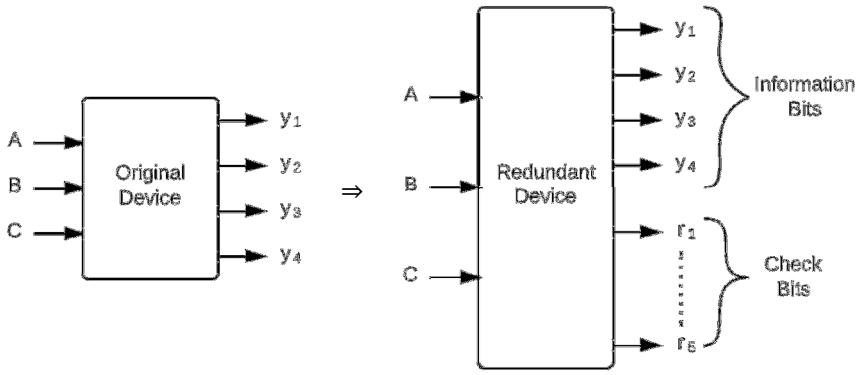
0	1	1	0	0
1	0	1	0	0
0	1	1	1	1
0	1	0	1	0
1	1	1	0	1

→ Check row

$d(V) = 4$, $n = k + 2\sqrt{k} + 1$
e.g. $k = 64 \rightarrow n = 81$

Detection of Single, Double, and Triple Errors by Two-Dimensional Parity Check Codes

Example: $k = 4$, $r = 2\sqrt{k} + 1 = 5$



$$\begin{matrix} y_1 & y_2 \\ y_3 & y_4 \end{matrix} \Rightarrow \begin{array}{cc|c} r_1 & r_2 & r_3 \\ y_1 & y_2 & r_4 \\ y_3 & y_4 & r_5 \end{array}$$

$$r_1 \oplus r_2 \oplus r_3 = 0,\ r_3 = r_1 \oplus r_2$$
$$y_1 \oplus y_2 \oplus r_4 = 0,\ r_4 = y_1 \oplus y_2$$
$$y_3 \oplus y_4 \oplus r_5 = 0,\ r_5 = y_3 \oplus y_4$$

Row checks

$$r_1 \oplus y_1 \oplus y_3 = 0,\ \ r_1 = y_1 \oplus y_3$$
$$r_2 \oplus y_2 \oplus y_4 = 0,\ \ r_2 = y_2 \oplus y_4$$
$$r_3 \oplus r_4 \oplus r_5 = 0,\ \ r_3 = r_4 \oplus r_5$$

Column checks

Example: (Ctd) Implementation