ELG 5372 Error Control Coding

Lecture 13: Nonsystematic and Systematic Encoding of Cyclic Codes

Université d'Ottawa | University of Ottawa

Nonsystematic Encoding of Cyclic Codes

- The message vector **m** = [m_0, m_1, …, m_{k-1}].
- Let this correspond to a message polynomial $m(x) = m_0+m_1x+\ldots m_{k-1}x^{k-1}$.
- The code polynomial is obtained by polynomial multiplication, $c(x) = m(x)g(x) = m_0g(x)+m_1xg(x)+\ldots+m_{k-1}x^{k-1}g(x)$.
- In matrix form:

$$c(x) = \begin{bmatrix} m_0 & m_1 & \cdots & m_{k-1} \end{bmatrix} \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

Nonsystematic Encoding of Cyclic Codes (2)

- Therefore we can write:

$$\mathbf{c} = \begin{bmatrix} m_0 & m_1 & \cdots & m_{k-1} \end{bmatrix} \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

$$\mathbf{c} = \mathbf{mG}$$

Example

- For a length 7 code, $x^7+1 = (x+1)(x^3+x+1)(x^3+x^2+1)$.
- For a (7,3) code, $g(x) = (x+1)(x^3+x^2+1) = (x^4+x^2+x+1)$.

$m(x)$	**m**	$c(x)$	**c**	$m(x)$	**m**	$c(x)$	**c**
0	000	0	0000000	x^2	001	$x^6+x^4+x^3+x^2$	0011101
1	100	x^4+x^2+x+1	11100100	x^2+1	101	x^6+x^3+x+1	1101001
x	010	$x^5+x^3+x^2+x$	01110010	x^2+x	011	$x^6+x^5+x^4+1$	1000111
$x+1$	110	$x^5+x^4+x^3+1$	10010110	x^2+x+1	111	$x^6+x^5+x^2+1$	1010011

Example cont'd

- The generator matrix for this code is:

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

- Note that the diagonals are constant. Such a matrix is called a Toeplitz matrix.

Parity Check Polynomial

- Previously, we saw that for a generator matrix **G**, there exists a matrix **H** for which $\mathbf{GH}^T = \mathbf{0}$.
- This is equivalent to having a generator polynomial $g(x)$ for which there is a polynomial $h(x)$ so that $g(x)h(x) = x^n-1$.
- $h(x)$ has degree k.

Example

- For our (7,3) code of the previous example, $h(x) = x^3+x+1$.
- Any $c(x)h(x)$ = a multiple of x^7+1. Therefore when multiplication is done modulo (x^7+1), the result is 0.
- For example for $c(x) = x^5+x^{4+}x^3+1$, $c(x)h(x) = x^8+x^7+x+1 = (x+1)(x^7+1)\text{mod}(x^7+1) = 0$.
- $c(x)h(x) = m(x)g(x)h(x) = x^n m(x)-m(x) = 0$. Since $x^n m(x)$ is n right cyclic shifts of $m(x)$ which equals $m(x)$.

Nonsystematic Parity Check Matrix

- $S(x) = c(x)h(x) \bmod (x^n-1) = 0$. $S(x) = s_0+s_1x+\ldots s_{n-1}x^{n-1}$.

$$s_0 + s_1 x + \ldots + s_{n-1}x^{n-1} = \sum_{i=0}^{n-1} c_i x^i \sum_{j=0}^{k} h_j x^j \bmod (x^n - 1)$$

$$\begin{aligned} s_0 + s_1 x + \ldots + s_{n-1}x^{n-1} &= c_0h_0 + (c_0h_1 + c_1h_0)x + (c_0h_2 + c_1h_1 + c_2h_0)x^2 + \\ &+ (c_{n-1}h_1 + c_{n-2}h_2 + \ldots + c_{n-k}h_k)x^n + \ldots \\ &+ (c_{n-1}h_k)x^{n+k-1} \bmod (x^n - 1) \end{aligned}$$

$$\begin{aligned} s_0 + s_1 x + \ldots + s_{n-1}x^{n-1} &= (c_0h_0 + c_{n-1}h_1 + c_{n-2}h_2 + \ldots + c_{n-k}h_k) \\ &+ (c_0h_1 + c_1h_0 + c_{n-1}h_2 + \ldots)x + \ldots \end{aligned}$$

$$s_t = \sum_{i=0}^{n-1} c_i h_j, \text{ where } j \text{ satisfies } (i+1) \bmod n = t.$$

Nonsystematic Parity Check Matrix 2

- The last *n-k* of these syndrome equations can be written in matrix form:

$$\mathbf{S} = \begin{bmatrix} s_k & s_{k+1} & \cdots & s_{n-1} \end{bmatrix} = \begin{bmatrix} c_0 h_k + c_1 h_{k-1} + \ldots + c_{n-1} h_1 & c_1 h_k + \ldots + c_{n-1} h_2 & \cdots & c_2 h_{k-1} + \ldots + c_{n-1} h_3 \end{bmatrix}$$

$$\mathbf{S} = \begin{bmatrix} s_k & s_{k+1} & \cdots & s_{n-1} \end{bmatrix} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{bmatrix} \begin{bmatrix} h_k & h_{k-1} & \cdots & h_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & h_k & h_{k-1} & \cdots & h_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 \end{bmatrix}^T$$

Example

- In our example, **H** is:

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

Example cont'd

$$\mathbf{GH}^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Generator Polynomial of Dual Code

- Recall that **H** is the generator matrix of the dual of the code generated by **G**.
- Therefore $g_d(x) = g_{d0}+g_{d1}x+\ldots+g_{dk}x^k = h_k+h_{k-1}x+\ldots+h_1x^k$.
- We say that $g_d(x)$ is the reciprocal of $h(x)$ ($h^*(x)$) where $h^*(x) = x^{deg(h)}h(x^{-1})$.
- $h(x) = x^3+x+1$, then $h^*(x) = x^3(x^{-3}+x^{-1}+1) = x^3+x^2+1$.

Systematic Encoding

- Recall that $c(x) = q(x)g(x)$
- For a codeword to be systematic, the first symbols must be equal to the message symbols.
- Let $x^{n-k}m(x) = m_0x^{n-k}+m_1x^{n-k+1}+\ldots+m_{k-1}x^{n-1}$.
- Dividing this by $g(x)$ we get
  - $x^{n-k}m(x) = q(x)g(x)+d(x)$, where $\deg(d(x))\leq n-k-1$.
  - $d(x) = d_0+d_1x+..+d_{n-k-1}x^{n-k-1}$.
- $q(x)g(x) = c(x) = x^{n-k}m(x) - d(x)$

Example

- For the binary cyclic (7,3) code, $g(x) = x^4+x^2+x+1$.
- Let $m(x) = x^2 = (001)$
- $x^4 m(x) = x^6$.
- $x^6 \div x^4+x^2+x+1 = x^2+1$ with remainder x^3+x+1.
- Therefore $c(x) = x^6+x^3+x^2+1 = (1011\underline{001})$

Example cont'd

$m(x)$	**m**	$x^4m(x)$	$r(x)$	$c(x)$	**c**
0	000	0	0	0	0000000
1	100	x^4	x^2+x+1	x^4+x^2+x+1	1110100
x	010	x^5	x^3+x^2+x	$x^5+x^3+x^2+x$	0111010
$x+1$	110	x^5+x^4	x^3+1	$x^5+x^4+x^3+1$	1001110
x^2	001	x^6	x^3+x^2+1	$x^6+x^3+x^2+1$	1011001
x^2+1	101	x^6+x^4	x^3+x^2	$x^6+x^4+x^3+x^2$	0011101
x^2+x	011	x^6+x^5	x^2+1	$x^6+x^5+x^2+1$	1010011
x^2+x+1	111	$x^6+x^5+x^4$	x	$x^6+x^5+x^4+x$	0100111

Generator Matrix

- To get the systematic generator, we need the codewords corresponding to all weight 1 messages.
- In our example:

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

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

Systematic Error Detection

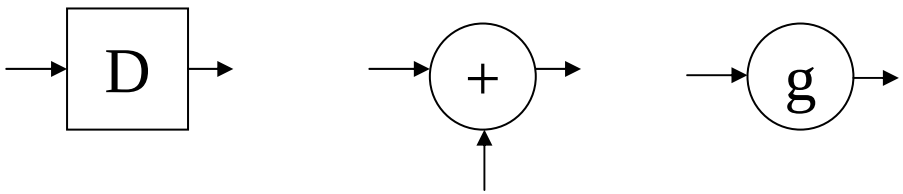
- $r(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} = c(x) + e(x) = (c_0 + e_0) + (c_1 + e_1)x + \ldots + (c_{n-1} + e_{n-1}) x^{n-1}$
- Assuming that no error have occurred, $e_i = 0$ for all i and $r(x) = c(x)$.
- For a systematic code, we would throw away the parity bits and $x^{n-k} m(x)$ would remain. This is the message part of the codeword.
- Dividing by $g(x)$ we should get the same remainder as is in the parity part of the codeword.
- If they are different, an error is detected.

Example

- $r(x) = x^6+x^3+x^2+1$.
- If $y(x)$ contains no errors, $x^4m(x) = x^6$ and $d(x) = x^3+x^2+1$.
- Dividing x^6 by x^4+x^2+x+1 yields a remainder of x^3+x^2+1. Therefore, we can conclude that $y(x)$ is a valid codeword and no error is detected.
- $y(x) = x^4+x+1$.
- Dividing x^4 by x^4+x^2+x+1 yields d(x) = x^2+x+1 which is not equal to x+1. Therefore an error is detected.

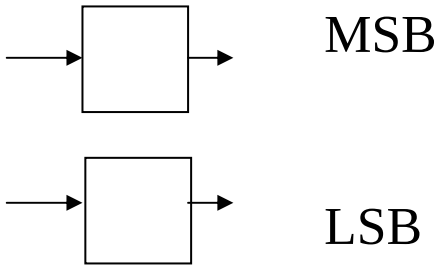
Introduction to Shift Registers

- Shift registers are made up of storage devices, adders and multipliers
- Storage devices are (generally D) flip flops.
- For binary addition, adders are XOR gates
- In GF(2), multiplication is done by 1 (closed circuit) or 0 (open circuit).
- For GF(2^m) we use combinational circuits for addition and multiplication.



Non binary storage devices

- For GF(2^m), we can place *m* FFs in parallel.



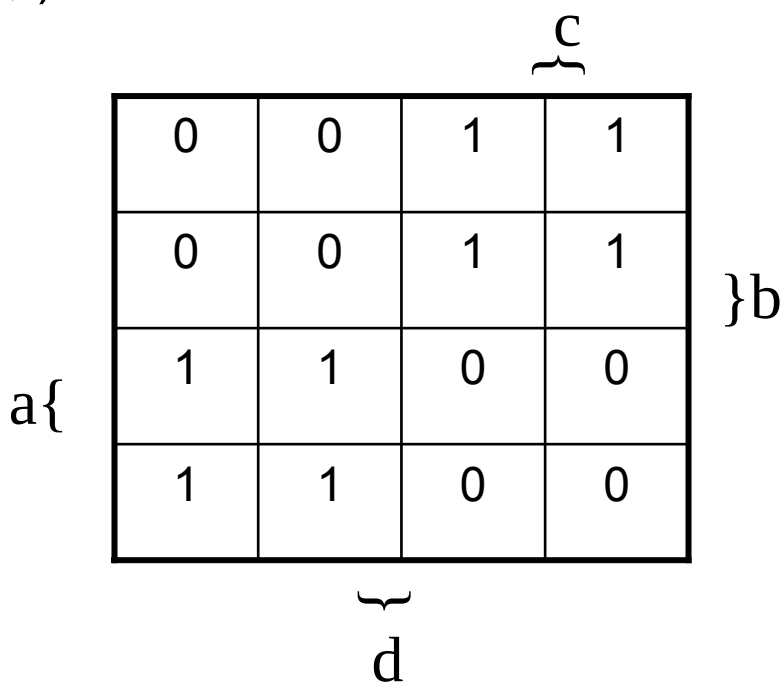
Non binary addition

- Consider GF(4)

+	0 00	1 01	α 10	α^2 11
0 00	0 00	1 01	α 10	α^2 11
1 01	1 01	0 00	α^2 11	α 10
α 10	α 10	α^2 11	0 00	1 01
α^2 11	α^2 11	α 10	1 01	0 00

Non binary addition

- $(a,b) + (c,d) = (e,f)$



$e = a$ XOR c and it is easy to show that $f = b$ XOR d

Non binary multiplication

- In GF(4), let $a = (a_1, a_0)$
- Suppose we wish to compute $b = \alpha a$.
- a=0, b=0 (0,0) → (0,0)
- a=1, b=α. (0,1) → (1,0)
- a=α, b=α^2 (1,0) → (1,1)
- a=α^2, b=1 (1,1) → (0,1)

- $b_1 = a_1$ XOR a_0, $b_0 = a_1$.