16548Notes11

University of Idaho

EE 455

Lec 31

Basic strategy:

1) come up w/ systematic cyclic codes (modulo polynomial arithmetic)

2) Show how we can do mod. poly. arithmetic with a state machine

= to showing an algorithm in state variable format

3) write down the circuit

University of Idaho

In chap. 4, we viewed encoding as

$$\underset{1\times n}{\bar{c}} = \underset{1\times k}{\bar{m}}\ \underset{k\times n}{G}$$

let's do an example of a <u>cyclic</u> generator matrix.

let $k=3 \quad n=7 \quad \Rightarrow r=4$

for a cyclic code, a generator G can always be found in the form

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & g_4 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & g_4 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & g_4 \end{bmatrix}$$

$$\bar{c} = (m_0\, m_1\, m_2) \cdot G$$

University of Idaho

$$\bar{g} = (g_0 \; g_1 \; g_2 \; g_3 \; g_4 \; 0 \; 0)$$

let $g(x) = g_0 + g_1 x + g_2 x^2 + g_3 x^3 + g_4 x^4$

Then we can re-express G as

$$G = \begin{bmatrix} g(x) \\ \hline x\,g(x) \\ \hline x^2 g(x) \end{bmatrix}$$

Now we can write

$$\bar{c} = \begin{pmatrix} m_0 & m_1 & m_2 \end{pmatrix} \begin{bmatrix} g(x) \\ x\,g(x) \\ x^2 g(x) \end{bmatrix}$$

$$= m_0 g(x) + m_1 x g(x) + m_2 x^2 g(x)$$

$$= (m_0 + m_1 x + m_2 x^2)\, g(x)$$

$$\boxed{c(x) = m(x) \cdot g(x)}$$

one issue: This code is non-systematic

University of Idaho

In other words

$$\bar{c} = (c_0\ c_1\ c_2\ c_3\ c_4\ c_5\ c_6)$$

$$\neq (c_0\ c_1\ c_2\ c_3\ m_0\ m_1\ m_2)$$

systematic form

$c(x) = m(x)\,g(x)$ as we have done it here does not give us a $c(x)$ corresponding to a systematic $\bar{c}$

University of Idaho

Is there an easy way to find a <u>systematic</u> form for our code?

Answer: yes.

To see how to get there, let's look at the problem in "hardware form"

$$m(x) = m_0 + m_1 x + m_2 x^2$$

m_0	m_1	m_2	0	0	0	0

[illegible]

University of Idaho

for a systematic codeword $c(x)$,

we want is

$$c(x) = \underbrace{c_0 + c_1 x + c_2 x^2 + c_3 x^3}_{r \text{ check bits}} + \underbrace{m_0 x^4 + m_1 x^5 + m_2 x^6}_{k \text{ message bits}}$$

c_0	c_1	c_2	c_3	m_0	m_1	m_2
0			$r-1$	bit position r		

University of Idaho

for a systematic codeword $c(x)$,
we want is

$$c(x) = \underbrace{c_0 + c_1 x + c_2 x^2 + c_3 x^3}_{r \text{ check bits}} + \underbrace{m_0 x^4 + m_1 x^5 + m_2 x^6}_{k \text{ message bits}}$$

c_0	c_1	c_2	c_3	m_0	m_1	m_2
↑ 0			↑ $r-1$	↑ bit position r		

University of Idaho

How do we shift $m(x)$ up into the k "top" positions in the register?

answer: multiply by x^r

Then we can say

$$c(x) = x^r \cdot m(x) + d(x)$$

check bit Polynomial

with $\deg(d(x)) \leq r-1$

University of Idaho

now, $\deg(g(x)) = r$ provided that $g_r \neq 0$

But if $g_r = 0$, then we'd really have a bigger k and a smaller r

it is always true for an (n, k) cyclic that $g_r = 1$, $r = n-k$

If $\deg(g(x)) = r$ what is the degree of $f(x)/g(x)$? $\deg[f(x)/g(x)] < r$

University of Idaho

what if we make "$f(x)$" equal to

$x^r m(x)$?

Then we'd be saying that

$$c(x) = x^r m(x) + \underbrace{\left[x^r m(x) / g(x) \right]}_{d(x)}$$

This satisfies our formal requirement for a systematic code.

The only question is: does this actually give us a cyclic code?

As it happens, if we pick any old $g(x)$ at random, the resulting set of $c(x)$ "codewords" will generally **not** form a cyclic code.

But, we **will** have a cyclic code **if** $g(x)$ satisfies one little property, namely

$$(x^n - 1)/g(x) = 0$$

remember the definition of polynomial division, e.g. $f(x) \div g(x)$ is defined

$$f(x) = Q(x)\, g(x) + \rho(x)$$

if $f(x) = x^n + 1$ (in $GF(2)[x]$)

and if $(x^n+1)/g(x) = 0 = \rho(x)$

Then we can say

$$x^n + 1 = \underbrace{h(x)}_{\text{degree } k} \cdot \underbrace{g(x)}_{\text{degree } = r}$$

Summarize: systematic (n,k) cyclic code has

- $g(x)$ such that $\deg(g(x)) = r = n-k$
- $h(x)g(x) = x^n + 1$

(which by the way means $g_0 = 1, h_0 = 1$)

- $c(x) = x^r m(x) + [x^r m(x)/g(x)]$

$h(x)$ is also the generator poly for the <u>dual</u> <u>code</u>

Remember "syndromes"?

Let me propose the following method for doing syndrome calculation in a cyclic code:

$$s(x) \triangleq v(x)/g(x)$$

$$v(x) = c(x) + e(x)$$

if $e(x) = 0$ so that $v(x) = c(x)$, This gives us

$$s(x) = c(x)/g(x) = \left[x^r m(x) + d(x)\right]/g(x)$$

University of Idaho

using our ~~3rd~~ 2nd handy identity

$$[x^r m(x) + d(x)]/g(x) = [x^r m(x)]/g(x) + d(x)/g(x)$$

$$= d(x) + d(x) = 0$$

$$\therefore \quad s(x) = c(x)/g(x) = 0$$

which is what we want.

if $e(x) \neq 0$, then $s(x) = v(x)/g(x) = e(x)/g(x)$

University of Idaho EE455

Lec 32

Last time, we said we could a systematic cyclic code as follows:

$$c(x) = x^r m(x) + [x^r m(x)]/g(x)$$

with $g(x)$ such that

$$(x^n - 1)/g(x) = 0$$

$$\Rightarrow \quad x^n - 1 = x^n + 1 = h(x)\,g(x) + 0$$

$$\deg(g(x)) = r = n - k$$

University of Idaho

How do we generate this?

First we need $g(x)$.

One way to get $g(x)$ is to factor

x^n+1

Example: $n=7$

$$x^7+1 = (x+1)(x^3+x+1)(x^3+x^2+1)$$

Suppose $r=3$. Then pick either

Suppose $r=4$: then pick $(x+1)\cdot p(x)$; $p(x)$

Suppose $r=5$: Too BAD

Once we've got $g(x)$, we could generate our $d(x)$ by table lookup.

What we do is build a remainder table

Example: $n=7$, $r=3$ $\quad (n,k)=(7,4)$

$$c(x) = x^3 m(x) + [x^3 m(x)]/g(x)$$

$$\left.\begin{array}{lllll} m_0 & \Rightarrow & m_0 x^3 & \Rightarrow & x^3/g(x) \\ m_1 & \Rightarrow & m_1 x^4 & \Rightarrow & x^4/g(x) \\ m_2 & \Rightarrow & m_2 x^5 & \Rightarrow & x^5/g(x) \\ m_3 & \Rightarrow & m_3 x^6 & \Rightarrow & x^6/g(x) \end{array}\right\} \text{remainder table}$$

4

Example 5.4.1: Construct a systematic (7, 4) cyclic code.

Solution: We previously found the factorization $x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1)$. The generator polynomial must be of degree $r=n-k=7-4=3$. Let our generator polynomial be

$$g(x)=x^3+x+1.$$

The codewords are the 16 polynomials defined by

$$c(x)=x^3\left(m_0+m_1x+m_2x^2+m_3x^3\right)/g(x)+x^3m(x)=d(x)+x^3m(x).$$

In example 5.3.2, we found the remainders for this $g(x)$ for the terms x^3, x^4, x^5, and x^6. Using these results and equation (5.3.2), we get the following code table.

$m(x)$	$c(x)$	$m(x)$	$c(x)$
0	0	x^3	$1+x^2+x^6$
1	$1+x+x^3$	$1+x^3$	$x+x^2+x^3+x^6$
x	$x+x^2+x^4$	$x+x^3$	$1+x+x^4+x^6$
$1+x$	$1+x^2+x^3+x^4$	$1+x+x^3$	$x^3+x^4+x^6$
x^2	$1+x+x^2+x^5$	x^2+x^3	$x+x^5+x^6$
$1+x^2$	$x^2+x^3+x^5$	$1+x^2+x^3$	$1+x^3+x^5+x^6$
$x+x^2$	$1+x^4+x^5$	$x+x^2+x^3$	$x^2+x^4+x^5+x^6$
$1+x+x^2$	$x+x^3+x^4+x^5$	$1+x+x^2+x^3$	$1+x+x^2+x^3+x^4+x^5+x^6$

We could do it this way, but there's a better way. To find this better way, we need to look at the mechanics of long division. What we will find is that calculating the remainder $\rho(x)$ can be expressed recursively using state variables and $\therefore$ $x^r m(x)/g(x)$ can be implemented as a state machine.

Example: $n = 7$, $r = 3$

$$g(x) = x^3 + g_2 x^2 + g_1 x + 1$$

$m(x)$ has deg. $(m(x)) \leq ~~n~~-1 = 4-1 = 3$

$x^3 m(x)$ has degree $\leq n-1$

let's look at $x^{n-1}/g(x) = x^6/g(x)$

by long division

University of Idaho

7

$$
\begin{array}{r l}
 & x^3 \\
x^3 + g_2 x^2 + g_1 x + 1 & \overline{) \; x^6 \qquad\qquad\qquad\qquad} \\
 & \underline{x^6 + g_2 x^5 + g_1 x^4 + x^3} \\
 & g_2 x^5 + g_1 x^4 + x^3
\end{array}
$$

← Partial remainder

define a vector $S_1 = \begin{bmatrix} g_2 \\ g_1 \\ 1 \end{bmatrix}$

1 cycle of The long division

University of Idaho

$g_2 \cdot g_2 = g_2$ in GF(2)

8

next cycle:

$$
\begin{array}{r}
g_2 x^2 \\
x^3+g_2x^2+g_1x+1 \overline{\left)\, g_2 x^5 + g_1 x^4 + x^3 \right.} \\
g_2 x^5 + g_2 x^4 + g_1 g_2 x^3 + g_2 x^2 \\
\hline
(g_1+g_2) x^4 + (1+g_1 g_2) x^3 + g_2 x^2
\end{array}
$$

$$S_2 = \begin{bmatrix} g_1+g_2 \\ 1+g_1 g_2 \\ g_2 \end{bmatrix} \equiv \underbrace{\begin{bmatrix} g_2 & 1 & 0 \\ g_1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}}_{\Gamma} \underbrace{\begin{bmatrix} g_2 \\ g_1 \\ 1 \end{bmatrix}}_{S_1}$$

What do you suppose we'll get from the 3rd cycle of long division?

$$
\begin{array}{r|l}
 & (g_1+g_2)x \\
\hline
x^3+g_2x^2+g_1x+1 & (g_1+g_2)x^4+(1+g_1g_2)x^3+g_2x^2
\end{array}
$$

What do you think the partial remainder will be?

$$\boxed{S_3 = \Gamma S_2}$$

and in general, the t^{th} cycle will give $S_t = \Gamma S_{t-1}$

University of Idaho

To calculate $x^6 / g(x)$

Ex: let $g(x) = x^3 + x + 1$

$g_2 = 0$
$g_1 = 1$

$$\Gamma = \begin{bmatrix} g_2 & 1 & 0 \\ g_1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} g_2 \\ g_1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

University of Idaho

$$S_3 = T S_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$S_4 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{array}{c} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \end{array} \begin{array}{l} \leftarrow x^2 \\ \leftarrow x^1 \\ \leftarrow x^0 \end{array}$$

4 shifts and $k = 4$; this means that the poly. represented by S_k has deg of $r-1 = 2$

$$x^6 / (x^3 + x + 1) = x^2 + 1$$

University of Idaho

Does This trick generalize?

Does it work for

$$g(x) = x^r + g_{r-1}x^{r-1} + g_{r-2}x^{r-2} + \cdots + g_1 x + 1$$

?

Yep.

$$\Gamma = \left[\begin{array}{c|c} g_{r-1} & \\ g_{r-2} & I_{(r-1)\times(r-1)} \\ \vdots & \\ g_1 & \\ \hline 1 & 0 \; 0 \cdots 0 \end{array}\right] \leftarrow \text{State Matrix}$$

Now, what if $m(x)$ is general

$$m(x) = m_{k-1} x^{k-1} + m_{k-2} x^{k-2} + \cdots + m_1 x + m_0$$

$$x^r m(x) = m_{k-1} x^{n-1} + m_{k-2} x^{n-2} + \cdots + m_1 x^{r+1} + m_0 x^r$$

Our "State vector" containing the partial remainders (shifting in $m(x)$ one bit at a time) generalizes to

$$S_t = \Gamma S_{t-1} + \begin{bmatrix} g_{r-1} \\ g_{r-2} \\ \vdots \\ g_0 \end{bmatrix} \cdot m_{k-t} \qquad S_0 = \bar{0}$$

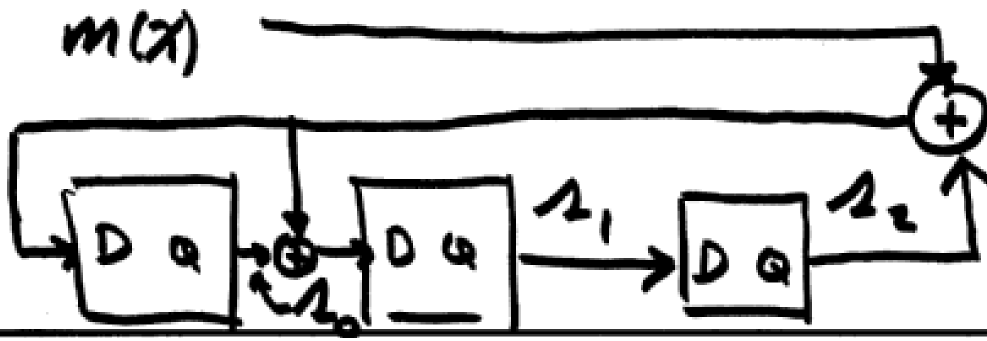
University of Idaho

14

This implies we can build our $x^r m(x)/g(x)$ calculator as follows:

EX. $g(x) = x^3 + x + 1$; $S_0 = \bar{0}$

$$S_t = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} S_{t-1} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} m_{k-t} \quad \Big\{ S_t = \begin{bmatrix} s_2 \\ s_1 \\ s_0 \end{bmatrix}_t$$



$1+1=0$

$n=7$
$r=3$
$k=4$

University of Idaho

Enduring Big Ideas :

1) $g(x) = x^r + g_{r-1}x^{r-1} + \cdots + g_1 x + 1$

$$\Gamma = \left[\begin{array}{c|ccc} g_{r-1} & & & \\ g_{r-2} & & I_{(r-1)\times(r-1)} & \\ \vdots & & & \\ g_1 & & & \\ \hline 1 & 0 \cdots & 0 & \cdots 0 \end{array}\right]$$

$$S_t = \Gamma S_{t-1} + \begin{bmatrix} g_{r-1} \\ g_{r-2} \\ \vdots \\ 1 \end{bmatrix} m_{k-t} \qquad S_0 = \bar{0}$$

Shift k times

2)

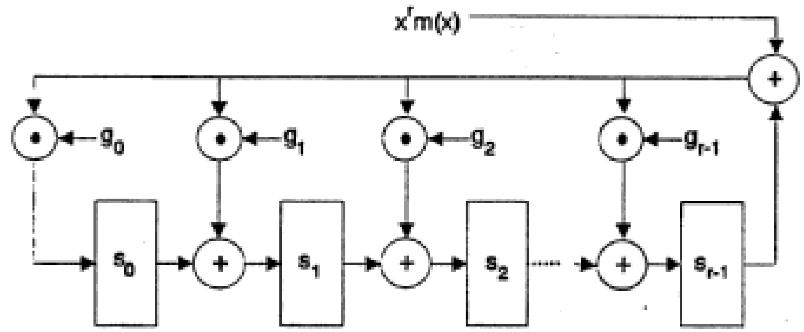


Figure 5.4.1: Divide by g(x) Circuit

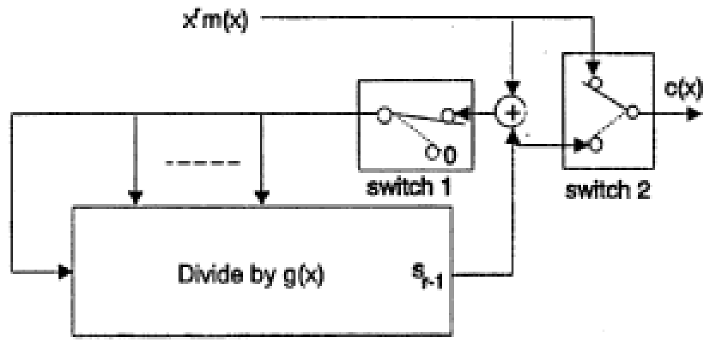


Figure 5.4.2: Systematic Encoder

after k shifts, change the switches

University of Idaho

Decoding systematic cyclic block codes

codeword:

$$c(x) = x^r m(x) + d(x)$$

where $d(x) = [x^r m(x)]/g(x)$

$$\deg(g(x)) = r \quad ; \quad (x^n+1)/g(x) = 0$$

we can write the received block as

$$v(x) = c(x) + e(x)$$

University of Idaho

where

$$e(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_{n-1} x^{n-1}$$

$e_i = 0 \Rightarrow$ no error

$e_i = 1 \Rightarrow$ error

For decoding, we will use the syndrome decoding method

gen. linear

$$\bar{s} = \bar{v} H^T$$

cyclic codes

let

$$s(x) = [x^r v(x)] / g(x)$$

$$
\begin{aligned}
s(x) &= [x^r v(x)]/g(x) \\
&= [x^r c(x) + x^r e(x)]/g(x) \\
&= [x^r c(x)]/g(x) + [x^r e(x)]/g(x) \\
&= [(x^r/g(x)) \cdot (c(x)/g(x))]/g(x) \\
&\quad + [x^r e(x)]/g(x)
\end{aligned}
$$

Now

$$c(x)/g(x) = [x^r m(x) + d(x)] / g(x)$$

$$= [x^r m(x)]/g(x) + d(x)/g(x)$$

$$= d(x) + d(x) = 0$$

$$\therefore \boxed{s(x) = [x^r e(x)]/g(x)}$$

if $e(x) \in C$ then $s(x) = 0$ undetectable errors

$$s(x) = [x^r e(x)] / g(x)$$

$$= s_0 + s_1 x + s_2 x^2 + \cdots + s_{r-1} x^{r-1}$$

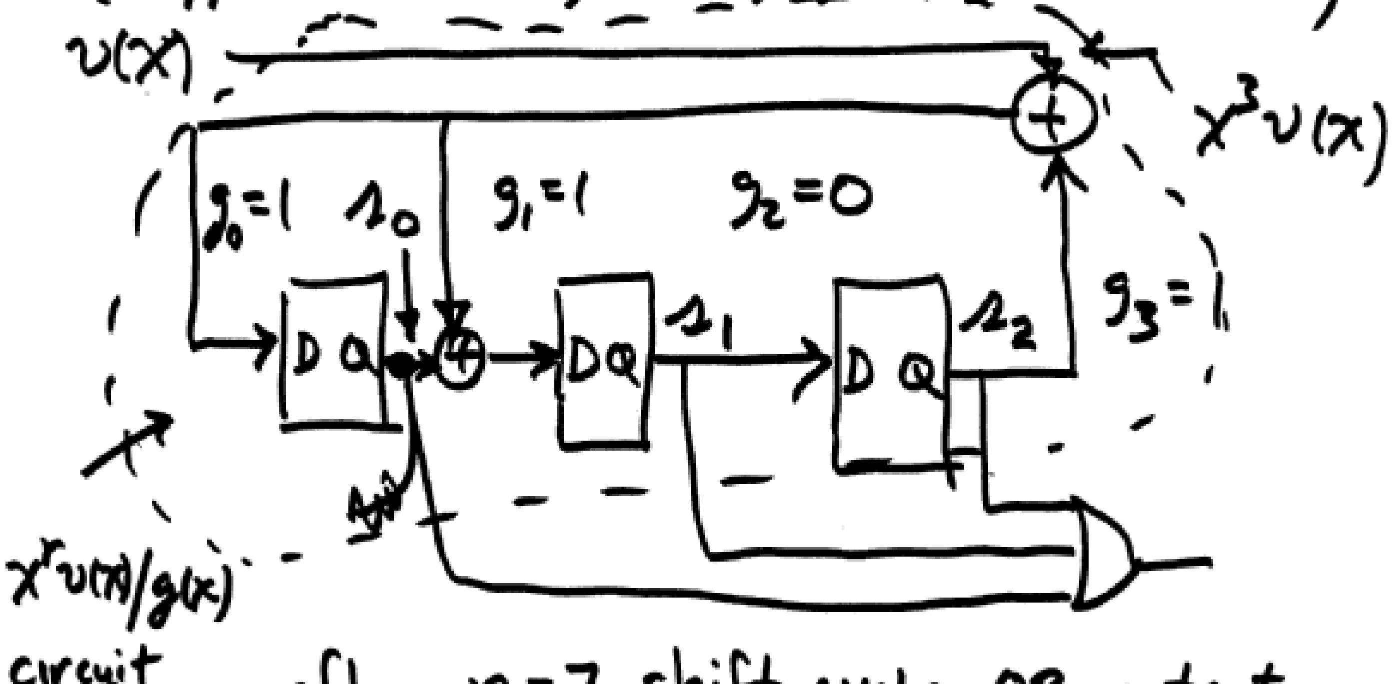
If all we want is error <u>detection</u> then

$s(x) \neq 0$ tells us we have an error

University of Idaho

Error detect circuit

(suppose $n=7$, $r=3$, $g(x) = x^3+x+1$)



after $n=7$ shift cycles, OR-output $=1$ if we detect an error

University of Idaho

State variable equation for the circuit

$$S_t = \begin{bmatrix} s_2 \\ s_1 \\ s_0 \end{bmatrix}$$

$$S_t = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} S_{t-1} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} v_{n-t}$$

for $t = 1$ to n

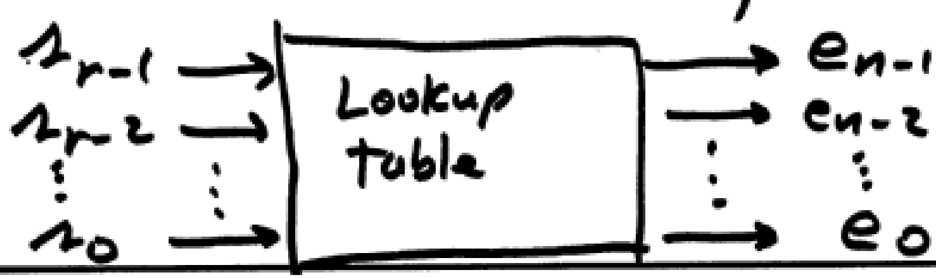
with $S_0 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ $\Bigg\}$ $S_t = T S_{t-1} + \begin{bmatrix} g_{r-1} \\ g_{r-2} \\ \vdots \\ g_0 \end{bmatrix} v_{n-t}$

How about error correction?

Codes are designed to correct up to some maximum number, t_c, of errors

One way to do it could be to build a syndrome table that maps

$$s(x) \Longrightarrow e(x)$$



How big is the lookup table in this method?

One entry per correctable error

Suppose the code corrects t_c errors

$$d_{min} \geq 2t_c + 1$$

$$w_H(\bar{e}) = 1 : \quad n_1 = n = \binom{n}{1}$$

$$w_H(\bar{e}) = 2 : \quad n_2 = n \cdot (n-1)$$

The total table size $\sim n^{t_c}$

University of Idaho

11

Pipelined correction circuit

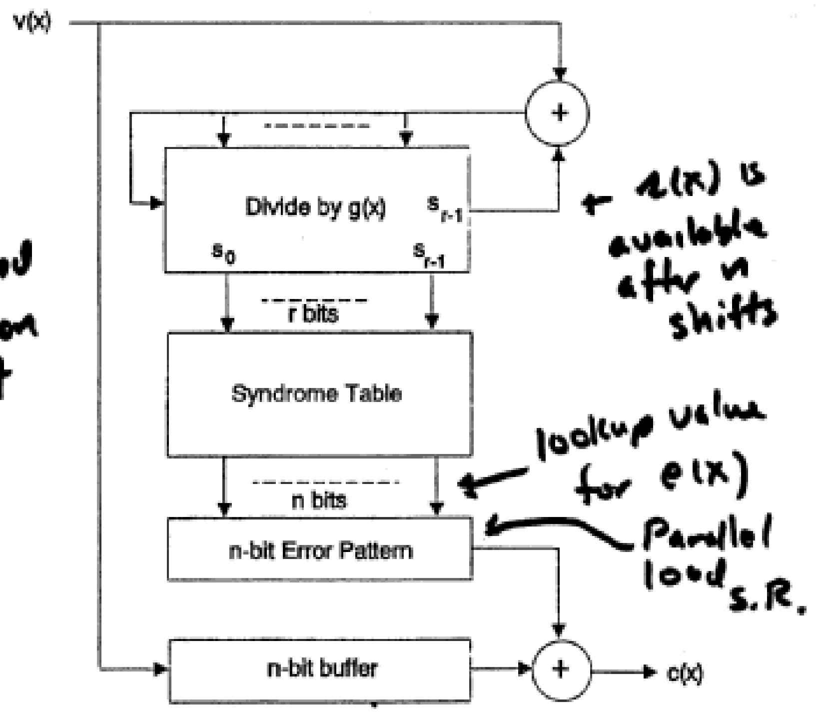


Figure 5.4.3: Error Correction

University of Idaho

Secret to simplifying even more is:

Meggitt's Theorem (Th. 5.3.1)

$$g(x)h(x) = x^n + 1 \quad = x^n - 1$$

Suppose that $f(x)/g(x) = \rho(x)$

Then

$$[x f(x) \bmod (x^n - 1)]/g(x) = [x\rho(x)]/g(x)$$

a cyclic property to syndromes

example:

Suppose we have $n=7$, $k=4$,

$g(x) = x^3+x+1$

also suppose $e(x) = x^5$

oops! where's x^r? wells!?

0	0	0	0	0	1	0

$$
\begin{array}{r|l}
 & x^2+1 \\
\hline
x^3+x+1 & x^5 \\
 & x^5+x^3+x^2 \\
\cline{2-2}
 & x^3+x^2 \\
 & x^3+x+1 \\
\cline{2-2}
\end{array}
$$

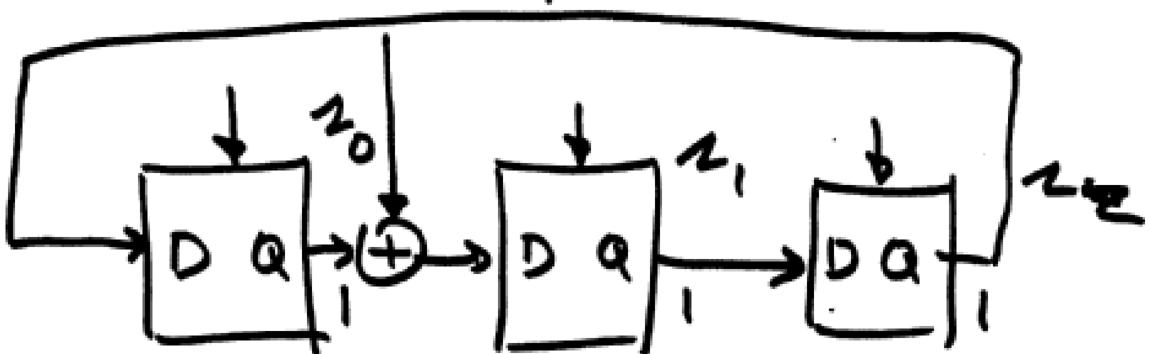
$\Big\} \Rightarrow r(x) = x^2+x+1$

University of Idaho

what if we pre-load this $r(x)$

$$r(x) = x^2 + x + 1$$

into another $\div$ by $g(x)$ circuit



$$S_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \end{bmatrix}$$

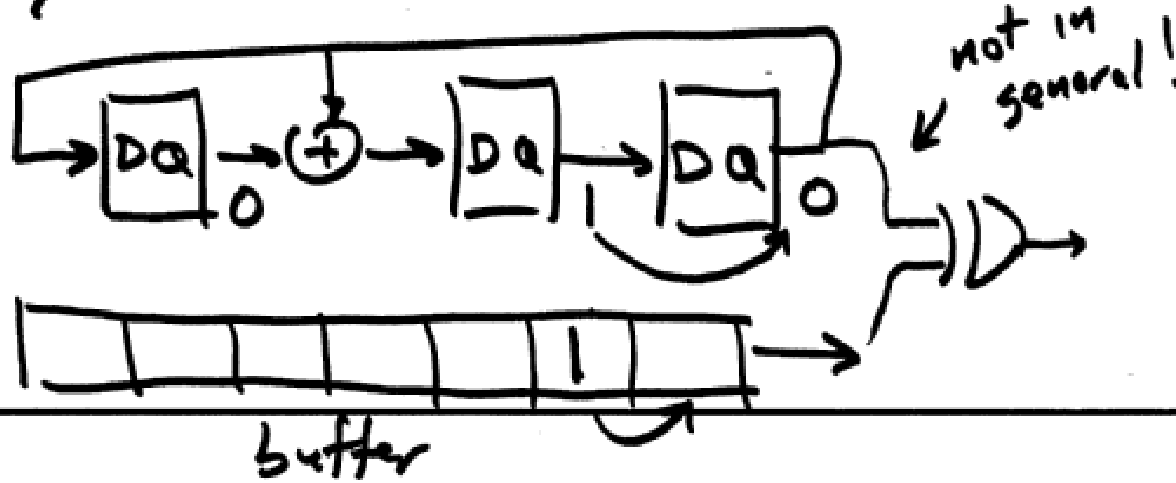
University of Idaho

Fix Rick's glitch!

$$e(x) = x^5$$

$$x^r e(x) = x^3 \cdot x^5 = x^8$$

$$x^8 / (x^3 + x + 1) = r(x) = x$$



University of Idaho

To build up a general solution, we do this trick:

let $\mathcal{E} = \{ e(x) \mid 0 < w_H(\bar{e}) \leq t_c \}$

define 2 <u>subsets</u> of $\mathcal{E}$

$$\mathcal{E}_{meg} \triangleq \{ e(x) \in \mathcal{E} \mid e_{n-1} = 1 \}$$

$$\mathcal{E}_{shift} \triangleq \{ e(x) \in \mathcal{E} \mid e_{n-1} = 0 \}$$

University of Idaho

if $e(x) = x^{n-1}$

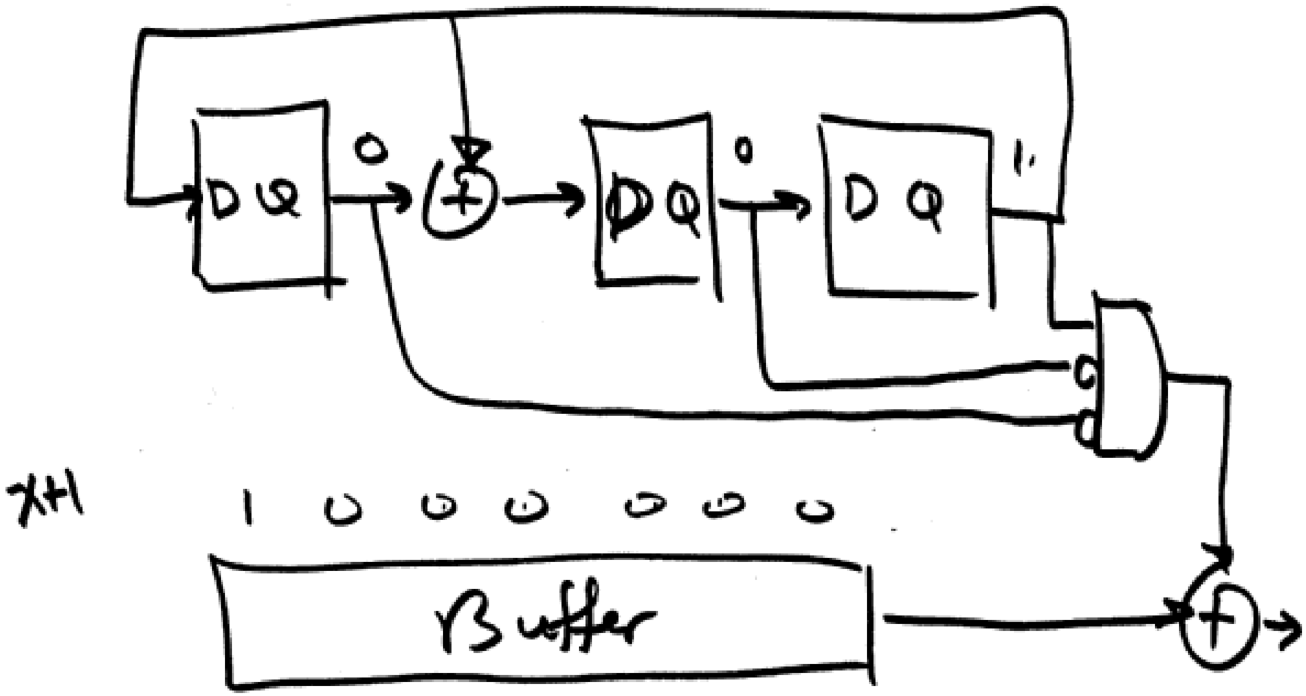
then $\left[x^r e(x)\right] / g(x) \equiv x^{r-1}$

Consider a Hamming code:

$t_c = 1$ $\quad \mathcal{E}_{meg} = \{ x^{n-1} \}$

syndrome for x^{n-1} is $s(x) = x^{r-1}$

$(7,4)$ H.C. has $r = 3 \Rightarrow s(x) = x^2$



all the $e(x) \in \mathcal{E}_{shift}$ have syndromes that "shift" to $s(x) = x^2$ when they come out