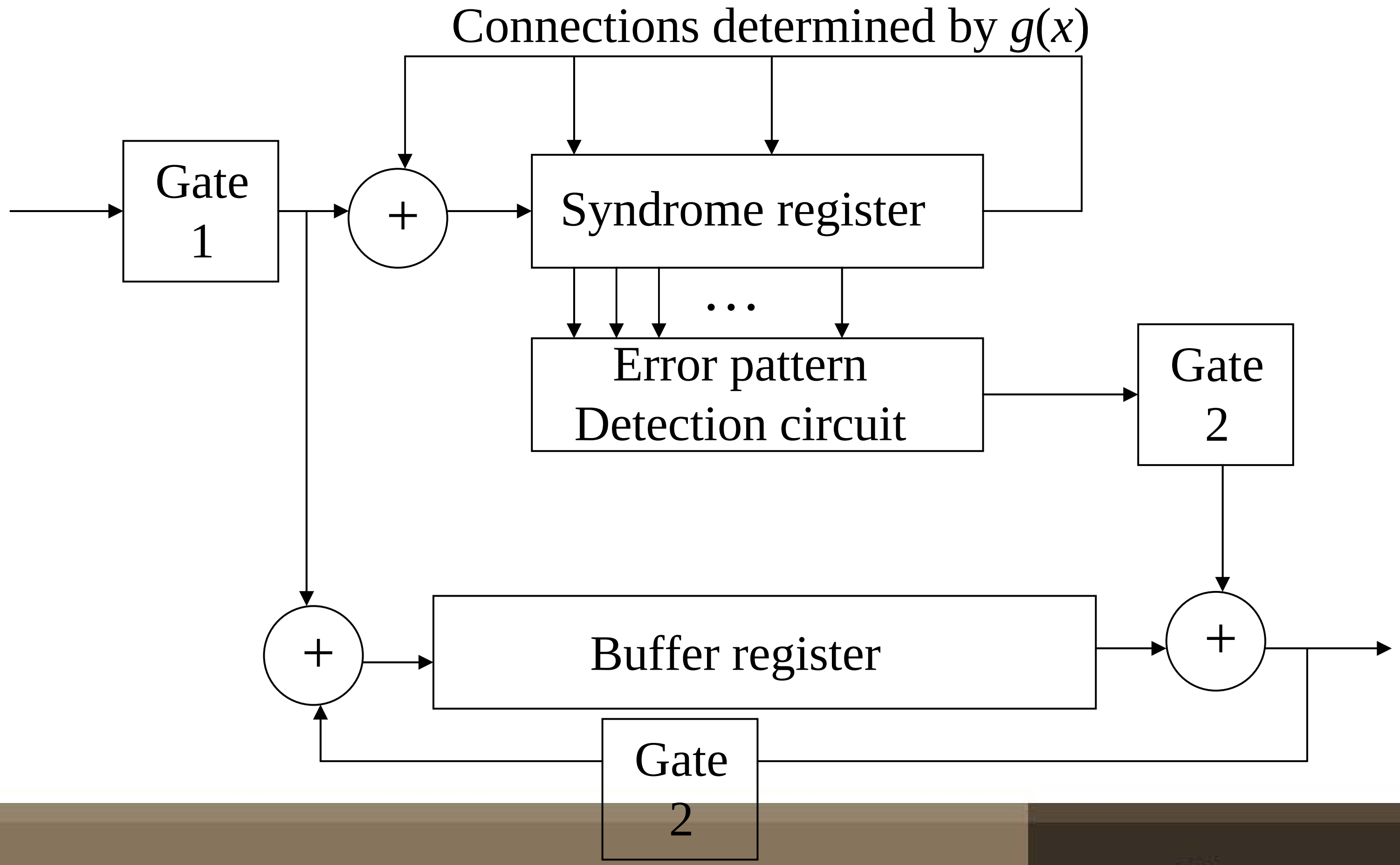
ELG 5372 Error Control Coding

Lecture 15: Decoding of Cyclic Codes and Intro to BCH codes

Meggitt Decoder

- Consider the decoder shown below



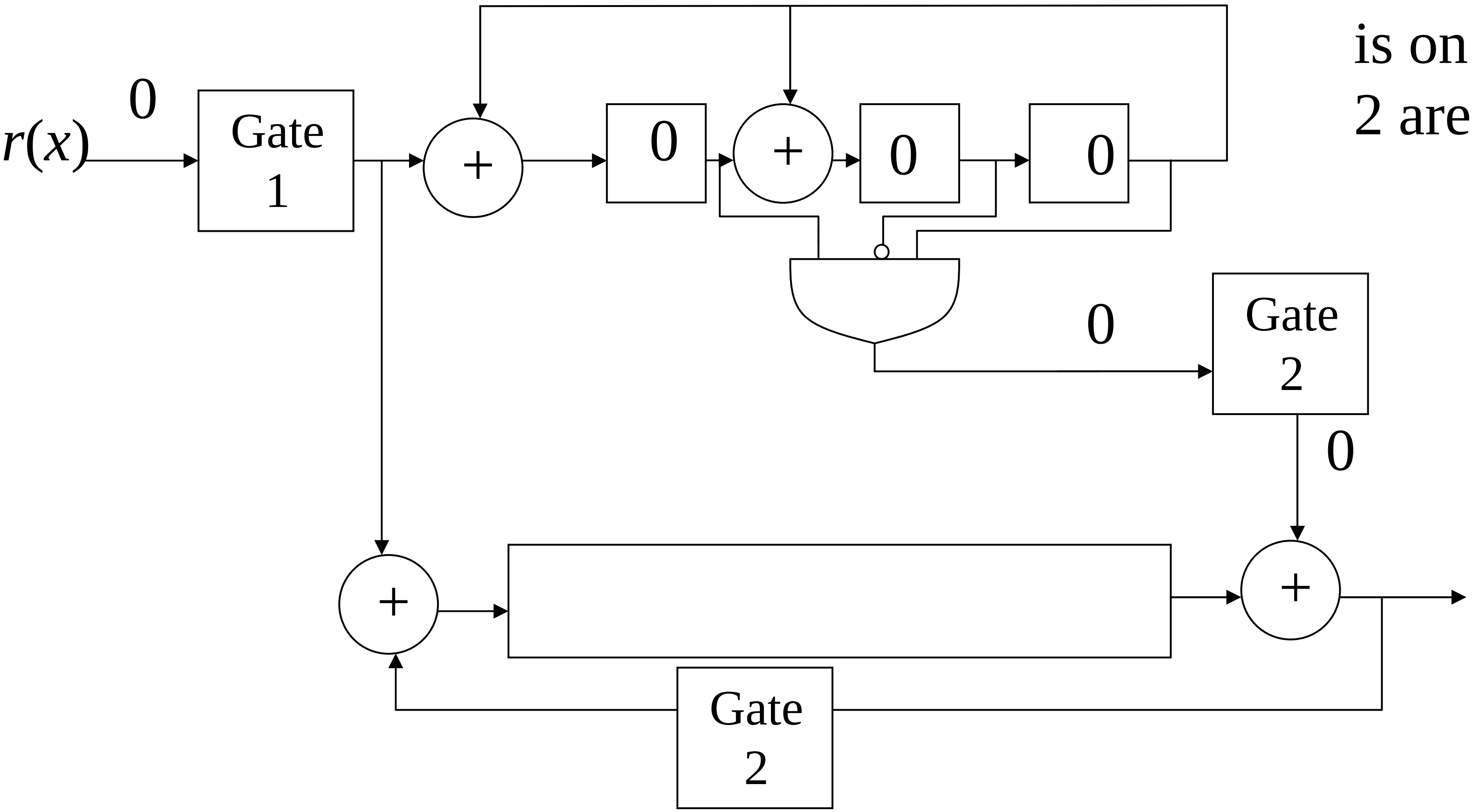
Meggitt Decoder 2

- The Meggitt decoder shifts the received word (and its corresponding syndrome) until a syndrome corresponding to a error in the first bit (ie $e_{n-1}(x) \neq 0$).
- Then it corrects that error and adjusts the syndrome and continues shifting until all errors are corrected.

Example

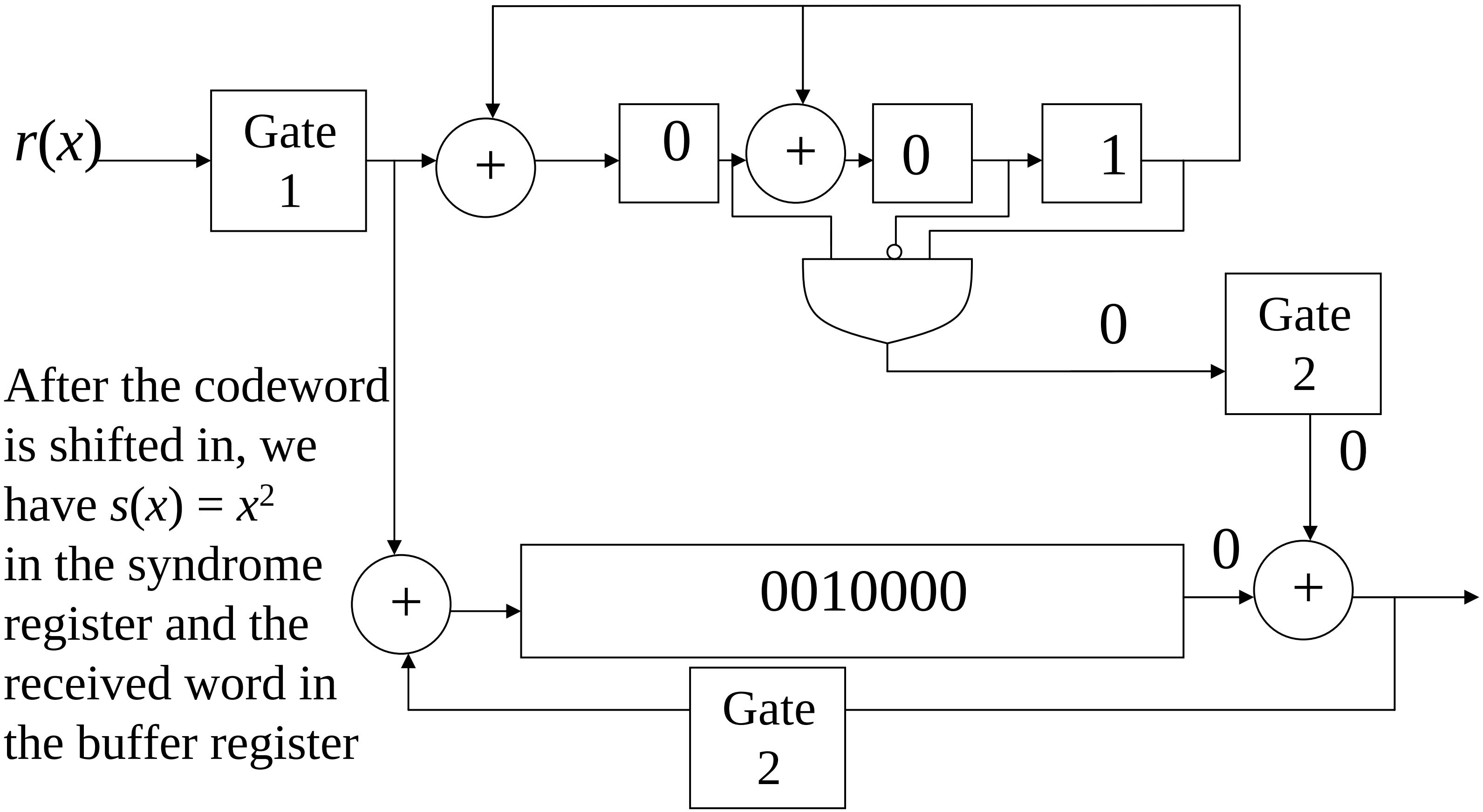
- Consider the (7,4) single error correcting code for which $g(x) = x^3+x+1$.
- As we saw, for $e(x) = x^6$, $s(x) = x^2+1$. $s_0=1$, $s_1=0$ and $s_2=1$.
- Therefore the decoder shifts the received word until the syndrome x^2+1 is detected ($s_0 s_1' s_2$).
- Let us assume that the received word is $r(x) = x^2$.

Example



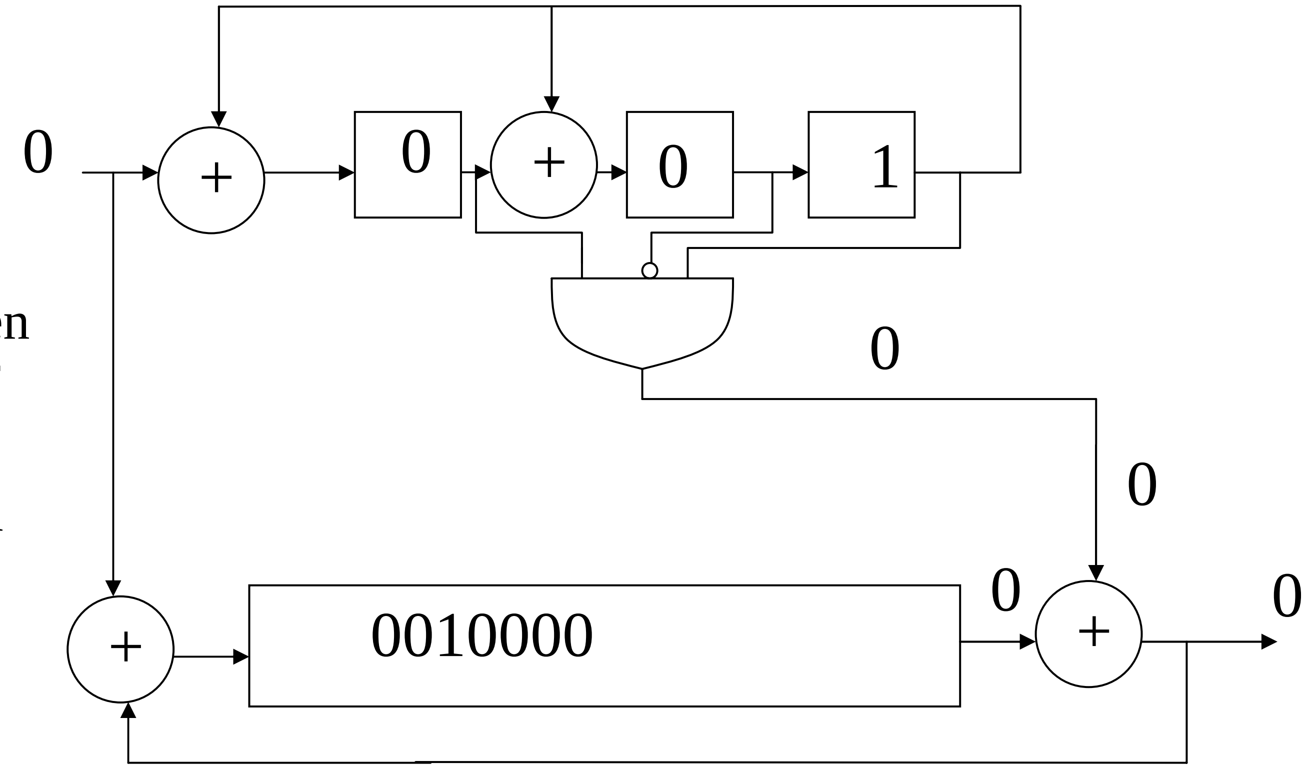
Initially gate 1 is on and gates 2 are off.

Example



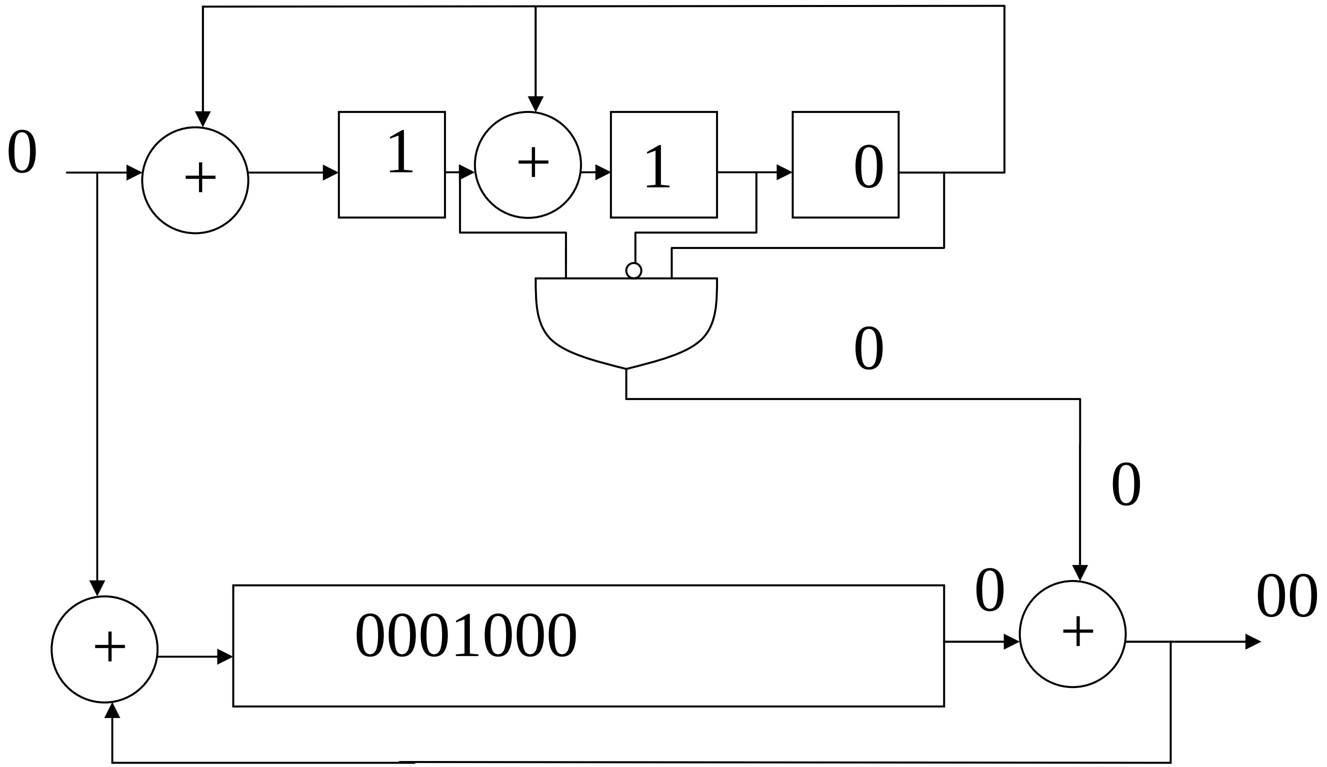
After the codeword is shifted in, we have $s(x) = x^2$ in the syndrome register and the received word in the buffer register

Example

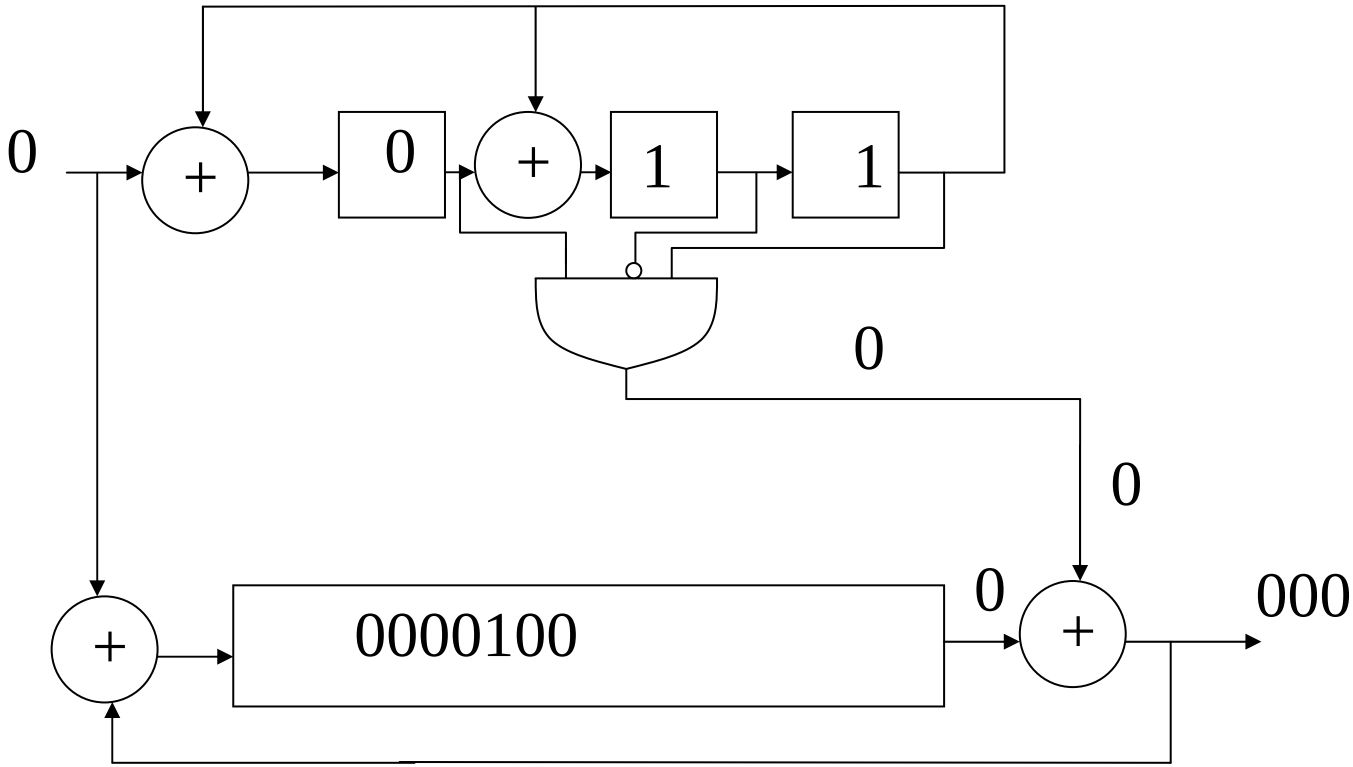


Gate 1 is then switched off and Gates 2 are switched on.

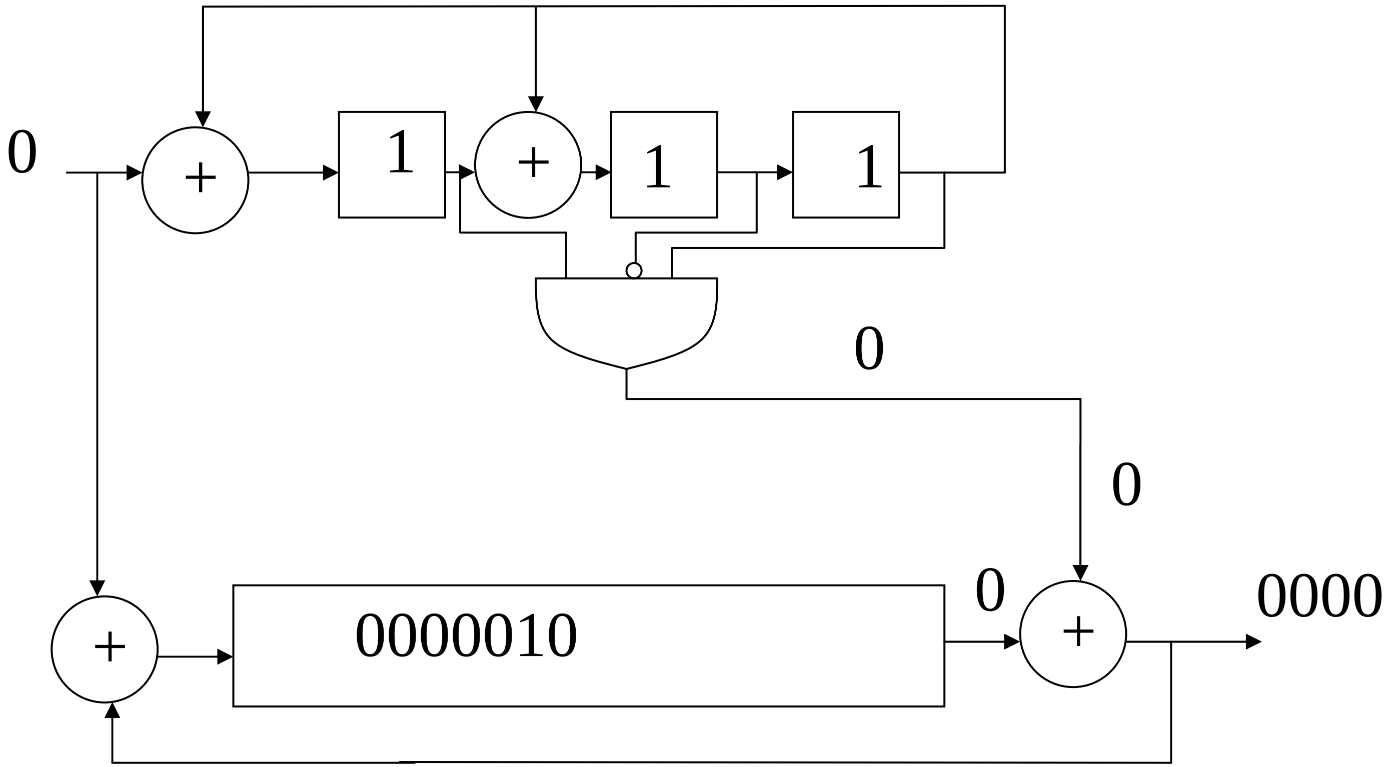
Example



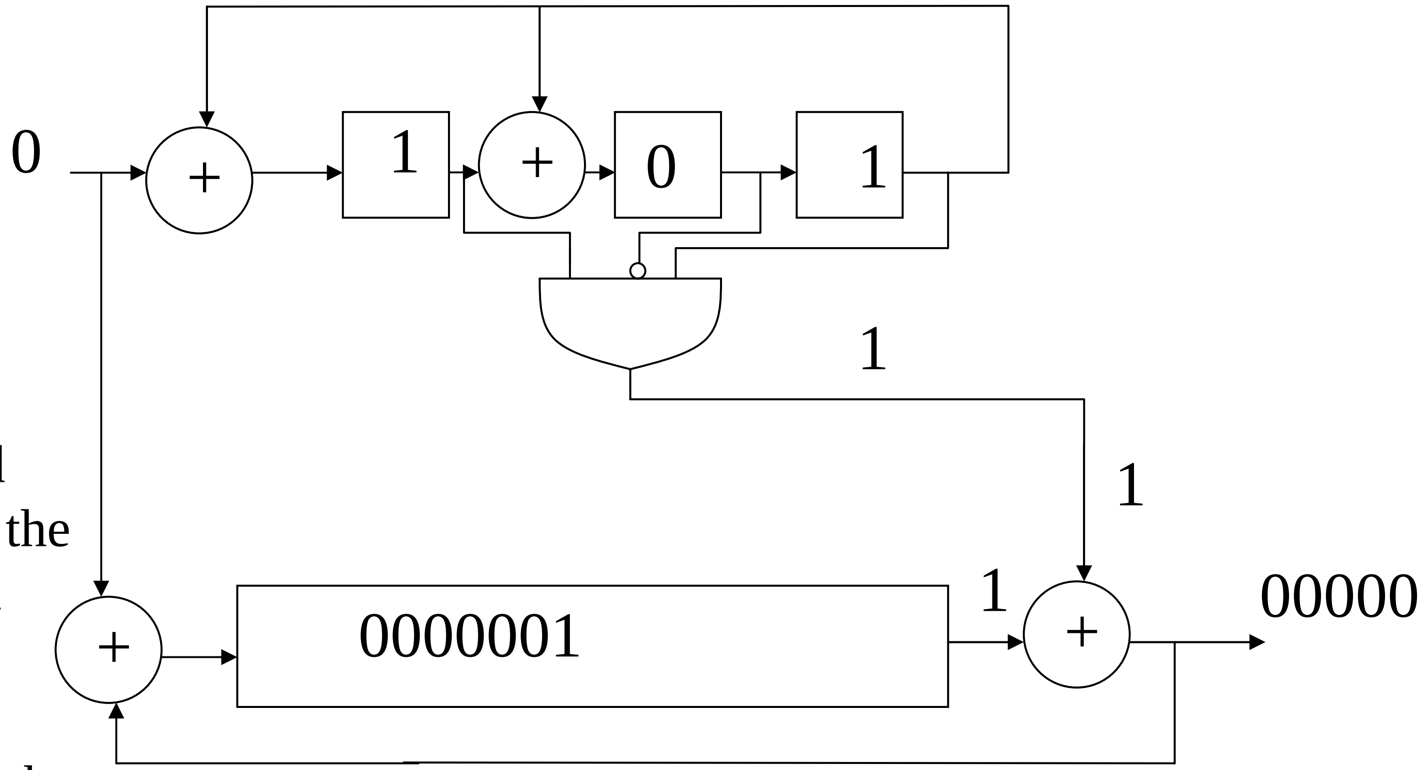
Example



Example



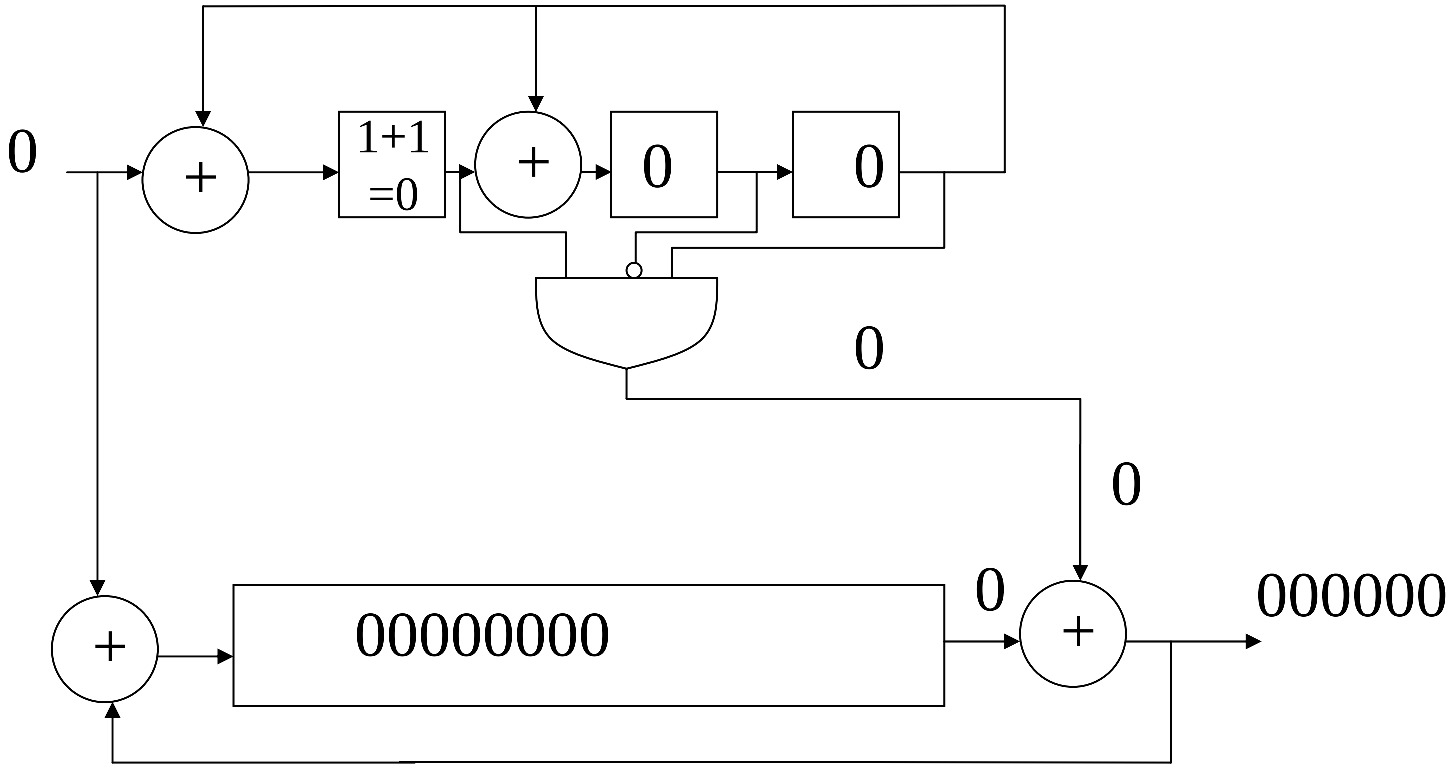
Example



Here we add x^6 to the shifted received word to correct the error. We must adjust the syndrome to account for the change

Example

$R_{new}(x) =$
$r(x)+x^6.$
$s'_{new}(x) =$
$(xr(x)+xx^6)$
$\text{mod}(x^7+1) =$
$s'(x)+1$



Since syndrome = 0, just shift out remaining bits.

Meggitt Decoder

- The syndrome correction after an error is corrected allows the decoder to search for more errors in the event of a multiple error correcting code.
- The error pattern detection circuit has to be hardwired to search for all error patterns in which the MSB is in error.

BCH and RS codes

- BCH codes are named for Bose, Ray-Chaudhuri and Hocquenghem who developed a means of designing cyclic codes with a specified design distance.
- RS code are named for their inventors as well.
- It was later determined that these codes are related and their decoding algorithms are quite similar.

Designing BCH codes

- BCH codes can be specified by a generator polynomial.
- A BCH code over GF(q) of length n with $d_{min} \geq \delta+1$:
  - Determine the smallest m such that GF(q^m) has an nth root of unity β.
  - Select a nonnegative integer b (usually b = 1).
  - Write down a list of δ consecutive powers of β: β^b, β^{b+1}, $\beta^{b+2}, \ldots, \beta^{b+\delta-1}$.
  - Find the associated minimal polynomials for each of these elements wrt GF(q). These minimal polynomials may not be distinct.
  - The generator polynomial $g(x)$ = LCM of the minimal polynomials found above.

Example

- We wish to design a binary BCH code of length 9 capable of correcting 2 errors (we want $d_{min} \geq 5$).
- In GF(64), $\beta = \alpha^7$ has order 9.
- Let us choose $b = 1$, $\delta = 4$.
- Therefore we need to find the minimal polynomials of α^7, α^{14}, α^{21}, α^{28}.
- The elements α^7, α^{14}, and α^{28} are all in the same conjugacy class, therefore they share the same minimal polynomial -> x^6+x^3+1.
- The remaining element has minimal polynomial x^2+x+1.
- Therefore $g(x) = \mathrm{LCM}(x^6+x^3+1, x^6+x^3+1, x^2+x+1, x^6+x^3+1) = (x^6+x^3+1)(x^2+x+1) = x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$. ($d_{min} = 8$)

Example cont'd

- Suppose we had chosen $b = 2$.
- Our list of elements becomes
  - $(\alpha^7)^2 = \alpha^{14}$, $(\alpha^7)^3 = \alpha^{21}$, $(\alpha^7)^4 = \alpha^{28}$, $(\alpha^7)^5 = \alpha^{35}$.
  - The generator polynomial is still $g(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
  - Still a (9,1) repetition code.

Example 2

- We want to design a binary BCH code of length 15 with $d_{min} \geq 5$.
- In GF(16), α has order 15.
  - The list of 4 elements is: α, α^2, α^3, α^4.
  - x^4+x+1
  - $x^4+x^3+x^2+x+1$
  - $g(x) = x^8+x^7+x^6+x^4+1$
  - Since $g(x)$ is a codeword of weight 5, we know that $d_{min} \leq 5$ and from the BCH bound, $d_{min} \geq 5$, therefore $d_{min} = 5$ for this (15,7) code.

Definitions

- A BCH code is said to be narrow sense if $b = 1$.
- A BCH code is said to be primitive if the root of its generator polynomial (β) is a primitive element in GF(q^m). This is only the case when $n = q^m$-1.
- BCH Bound: For generator polynomial $g(x)$, δ is the number of consecutive powers of the nth root of unity β that are roots of $g(x)$. Then $d_{min} \geq \delta+1$. See proof of this bound on pages 237-239 of text.

Example 3

- Design a binary BCH code of length 7 that corrects one error ($d_{min} \geq 3$)
  - Choose α which has order 7 in GF(8): α, α^2 from GF(8).
  - $g(x) = x^3+x+1$
  - $g(x)$ is the primitive polynomial used to generate GF(8).
  - This is the Hamming (7,4) code.
  - All Hamming codes use the primitive polynomial as their generator matrix. They all have two consecutive powers of α as roots, therefore $d_{min} \geq 3$ (actually $d_{min} = 3$ for all Hamming codes).

Non Binary BCH Codes

- Codes are constructed on GF(q) where $q \neq 2$.
- For example, suppose we wanted to design a 4-ary code of length 15.
  - Need to find minimal polynomials of GF(16) wrt GF(4).

Example

- $\{1\} \rightarrow (x+1)$
- $\{\alpha, \alpha^4\} \rightarrow (x^2+x+\alpha^5)$
- $\{\alpha^2, \alpha^8\} \rightarrow (x^2+x+\alpha^{10})$
- $\{\alpha^3, \alpha^{12}\} \rightarrow (x^2+\alpha^{10}x+1)$
- $\{\alpha^5\} \rightarrow (x+\alpha^5)$
- $\{\alpha^6, \alpha^9\} \rightarrow (x^2+\alpha^5x+1)$
- $\{\alpha^7, \alpha^{13}\} \rightarrow (x^2+\alpha^5x+\alpha^5)$
- $\{\alpha^{10}\} \rightarrow (x+\alpha^{10})$
- $\{\alpha^{11}, \alpha^{14}\} \rightarrow (x^2+\alpha^{10}x+\alpha^{10})$

□ α^5 and α^{10} are elements in GF(16) with order 3, they are α and α^2 of GF(4).

Example

- Design a 4-ary BCH code of length 15 with $d_{min} \geq 5$.
- Choose α, α^2, α^3, α^4.
- $g(x) = (x^2+x+\alpha)(x^2+x+\alpha^2)(x^2+\alpha^2x+1) = (x^6+x^5+\alpha^2x^4+x^3+\alpha x+\alpha^2)$.
- The code is a (15,9) code.
- Rate = 9/15
- For the Binary BCH code with $d_{min} \geq 5$, rate = 7/15.

Reed Solomon Codes

- An RS code is a q-ary BCH code of length q-1.
- We need minimal polynomials of GF(q) wrt GF(q).
- Conjugacy class is β, β^q, β^{q^2} …

□ $\beta^q = \beta$.

- Conjugacy classes contain 1 element and minimal polynomial is in the form (x-β).

Example

- Design a 16-ary length 15 RS code with $d_{min} \geq 5$.
- $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4) = x^4+a^{13}x^3+\alpha^6x^2+\alpha^3x+a^{10}$.
- Since there are no extraneous roots, $k = n-\delta$., therefore $\delta = n-k$ and $d_{min} \geq n-k+1$.
- But Singleton bound states that $d_{min} \leq n-k+1$.
- Therefore $d_{min} = n-k+1$.