ELG 5372 Error Control Coding

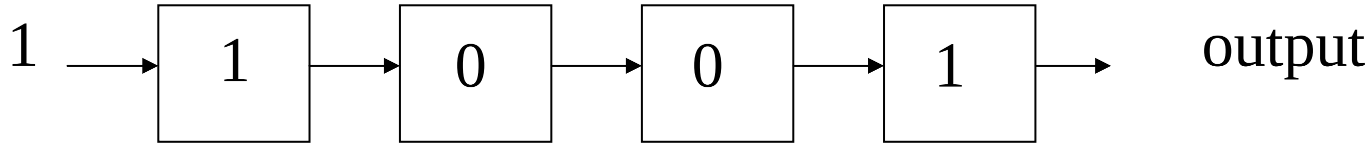
Lecture 14: Shift Registers for Encoding and Decoding of Cyclic Codes

Université d'Ottawa | University of Ottawa

uOttawa
L'Université canadienne
Canada's university

Register State and Polynomial Representation

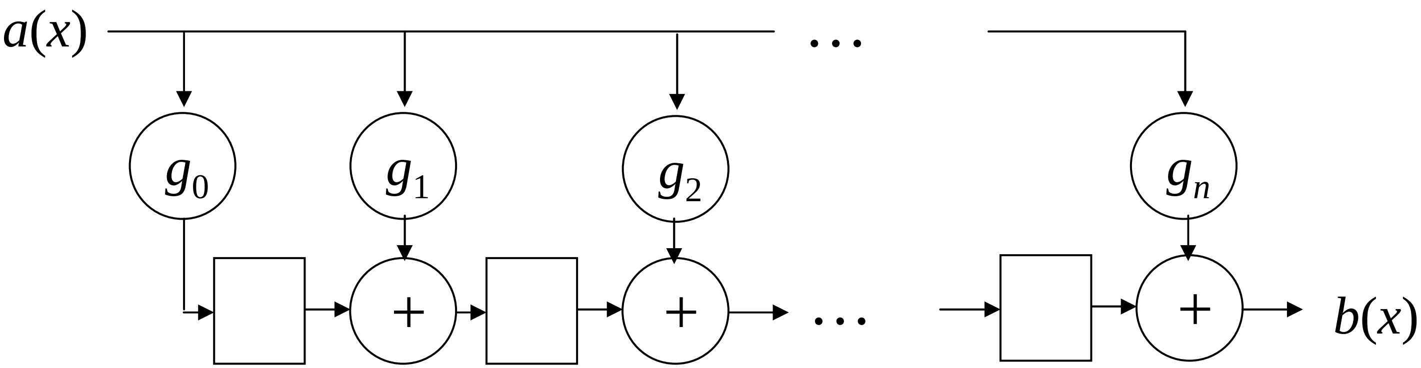
- State of register is the contents of the storage devices



- State = 1001
- A delay of n time units is represented as x^n.
- The polynomial output by the above circuit is $1+x^3+x^4$. (First element first representation). Or $1+x+x^4$ (last element first representation).

Polynomial Multiplication

- Let $a(x) = a_0+a_1x+\ldots+a_mx^m$ and $g(x) = g_0+g_1x+\ldots+g_nx^n$
- Let $b(x) = a(x)g(x) = g_0a(x)+xg_1a(x)+x^2g_2a(x)+\ldots+x^ng_na(x)$.

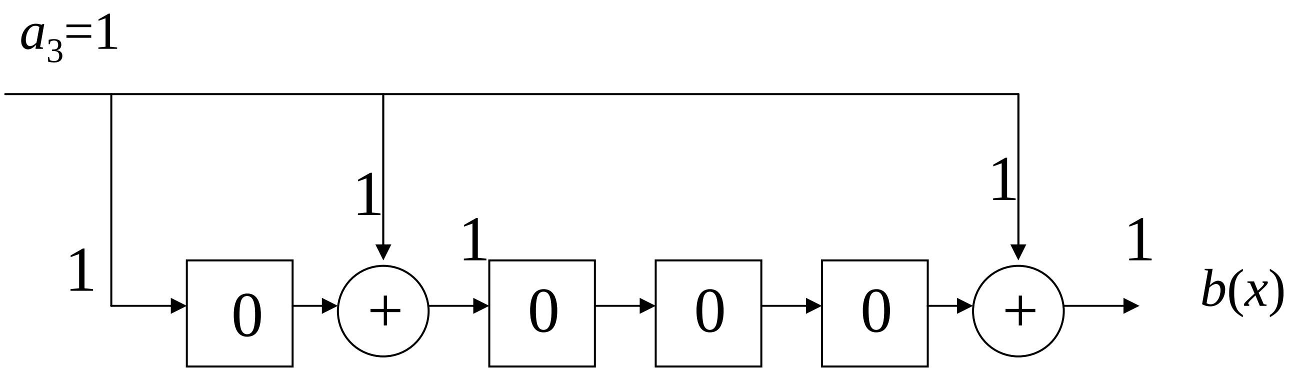


Last element first implementation

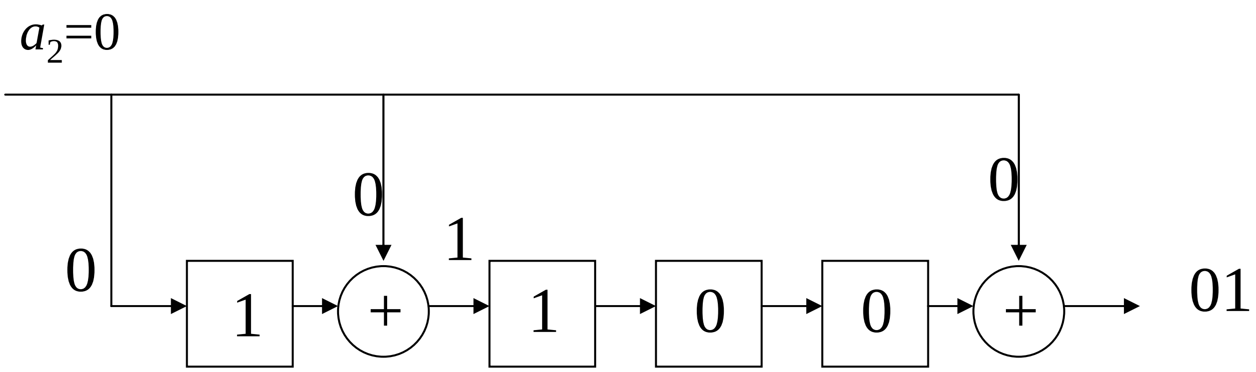
Example

- Let $g(x) = 1+x+x^4$ in GF(2)[x].
- Let $a(x) = 1+x+x^3$.
- Then $b(x) = 1+x^2+x^3+x^5+x^7$.

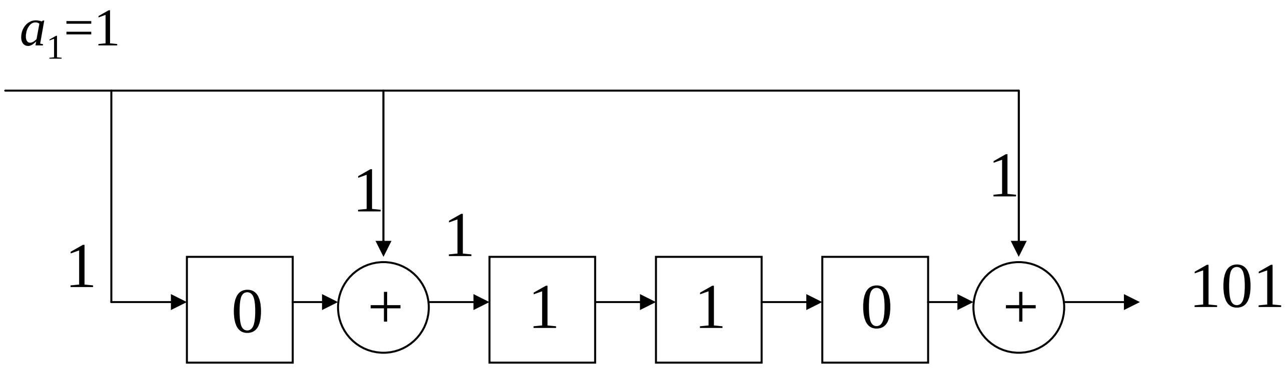
Example cont'd



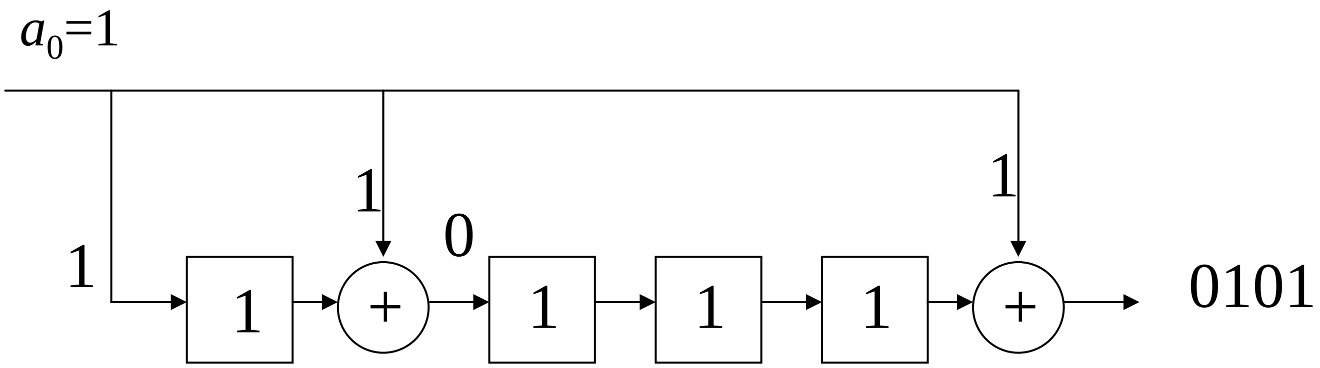
Example cont'd



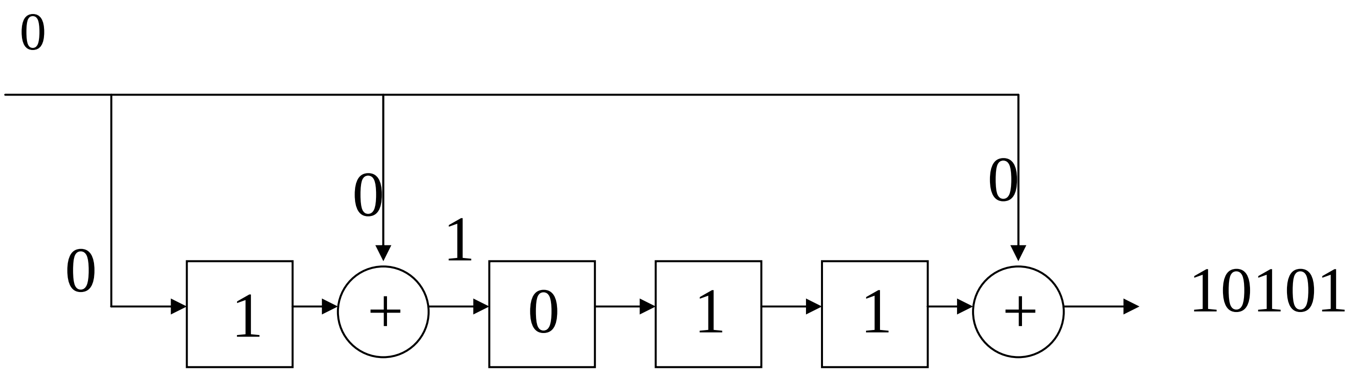
Example cont'd



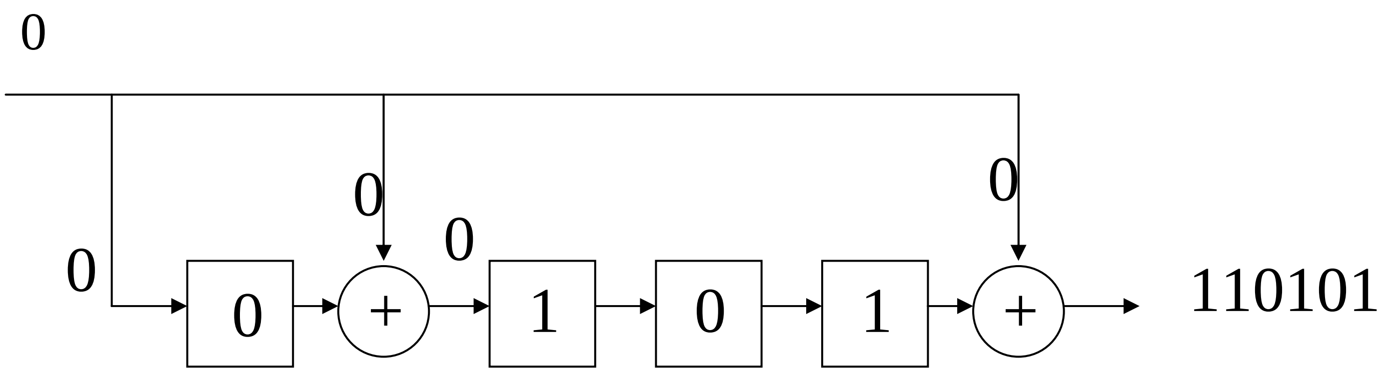
Example cont'd



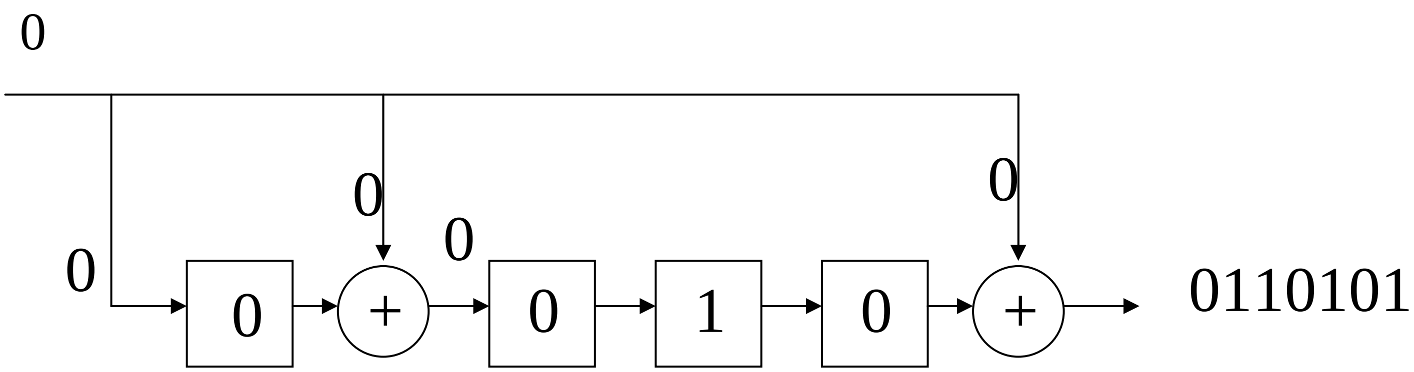
Example cont'd



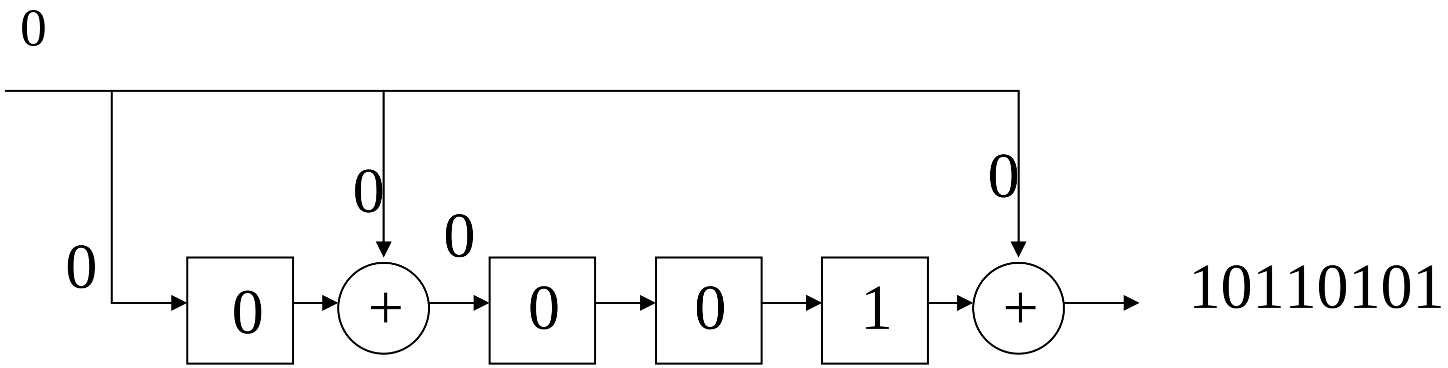
Example cont'd



Example cont'd



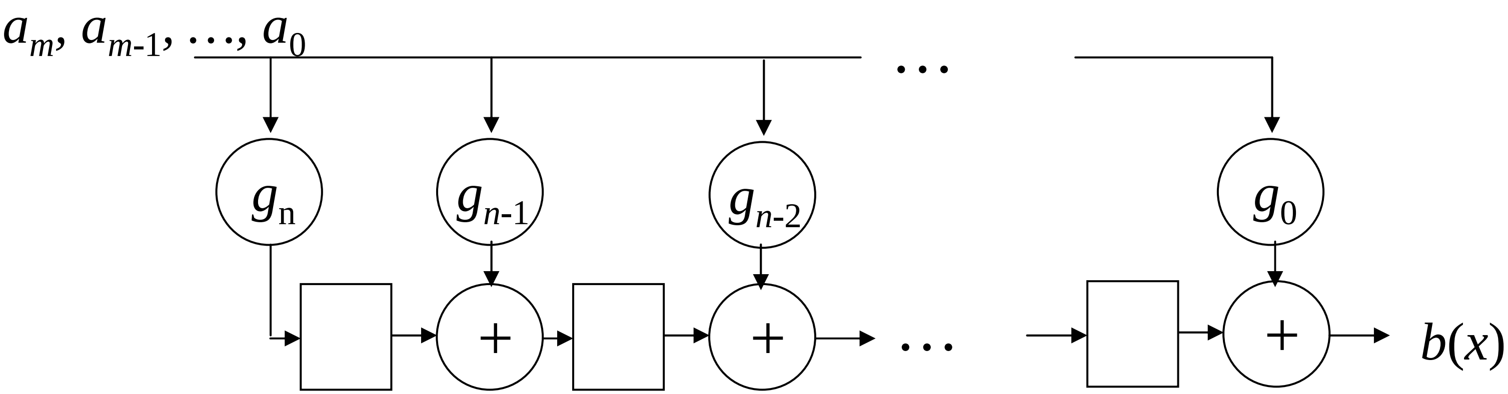
Example cont'd



$1+x^2+x^3+x^5+x^7$

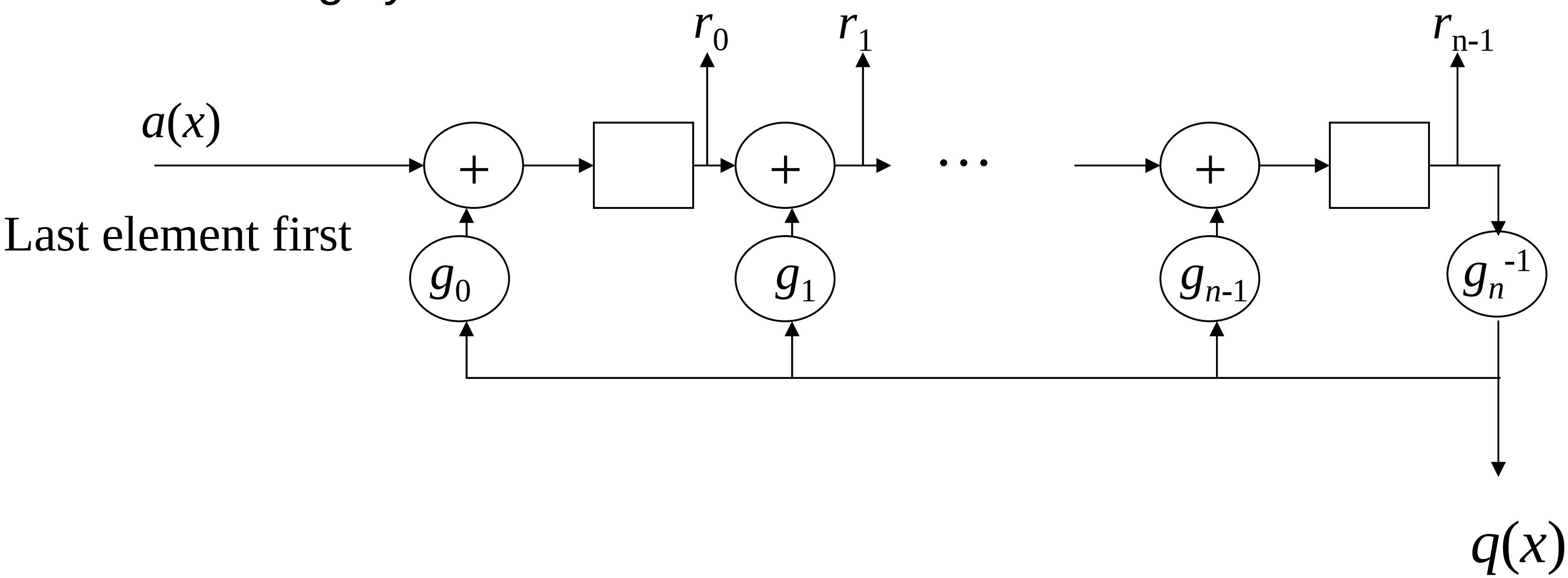
Polynomial Multiplication First Element First

- To implement the multiplier for First element first processing, reverse the order of the coefficients of $g(x)$ in the register.



Polynomial Division

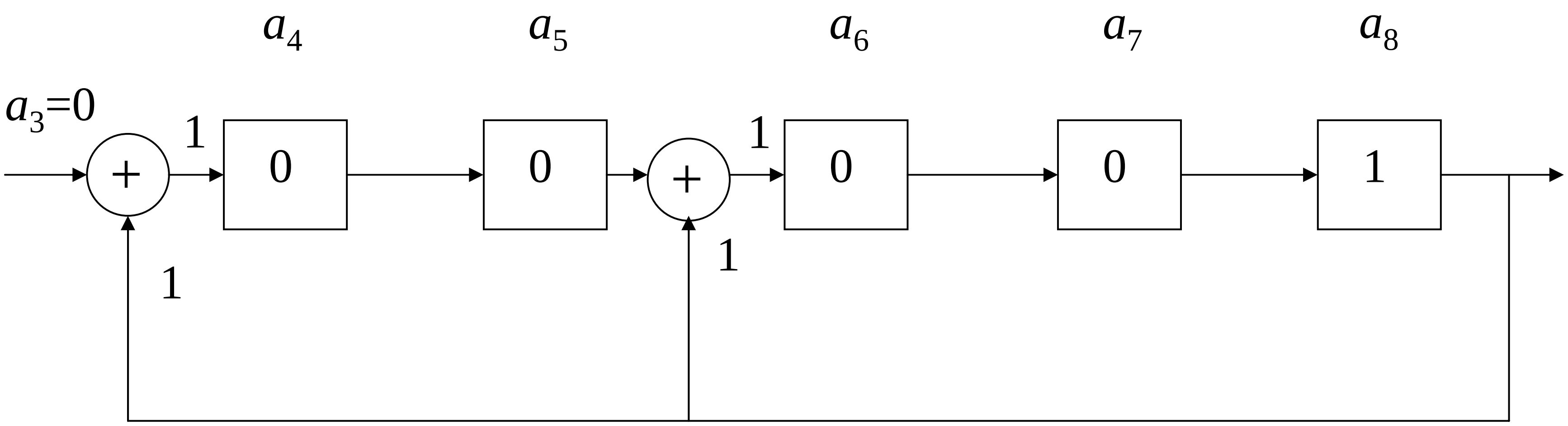
- Computing polynomial division, and more importantly, computing the remainder after division are important tasks in encoding cyclic codes.



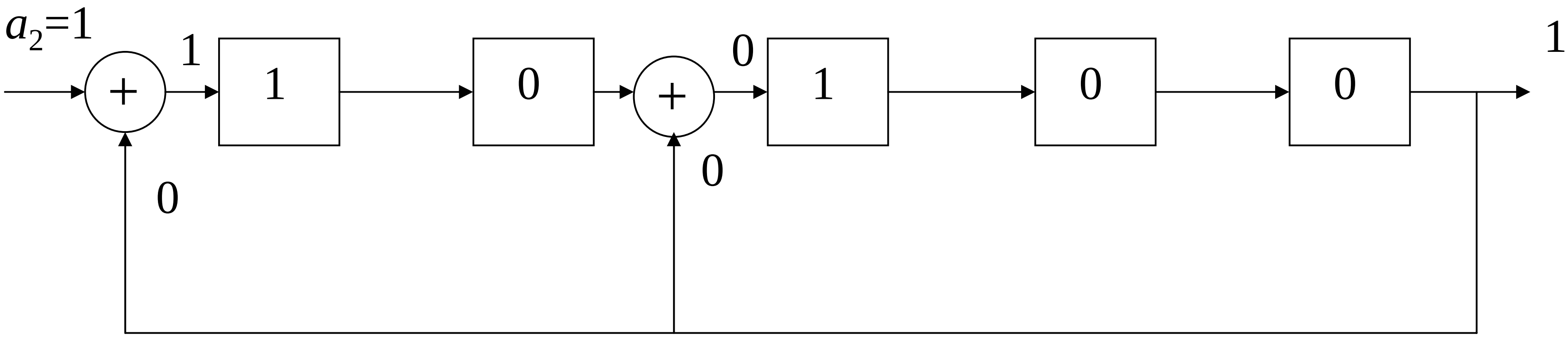
Example

- Let $g(x) = x^5+x^2+1$ in GF(2)[x].
- We wish to find $a(x) = q(x)g(x)+d(x)$. Let $a(x) = x^8+x^2+1$.
- We can see that $a(x) = (x^3+1)g(x)+x^3$.

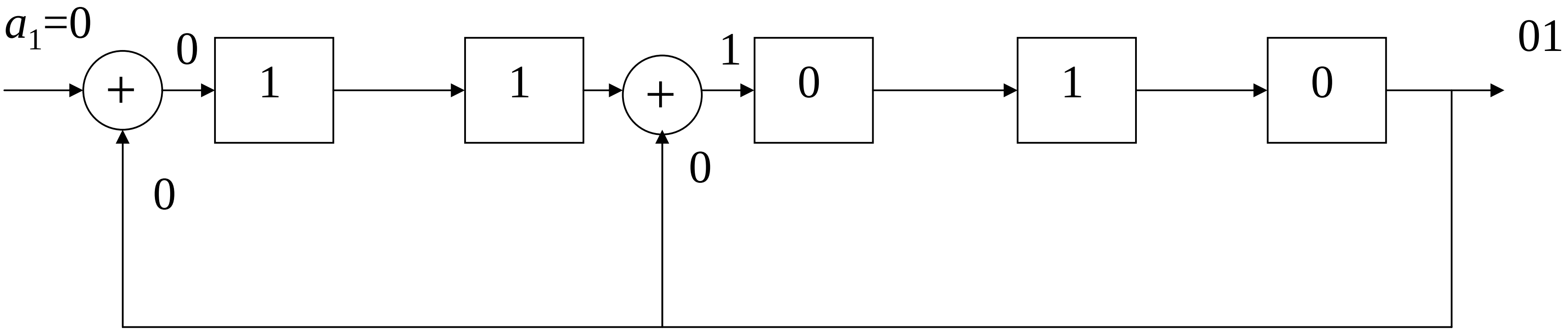
Example cont'd



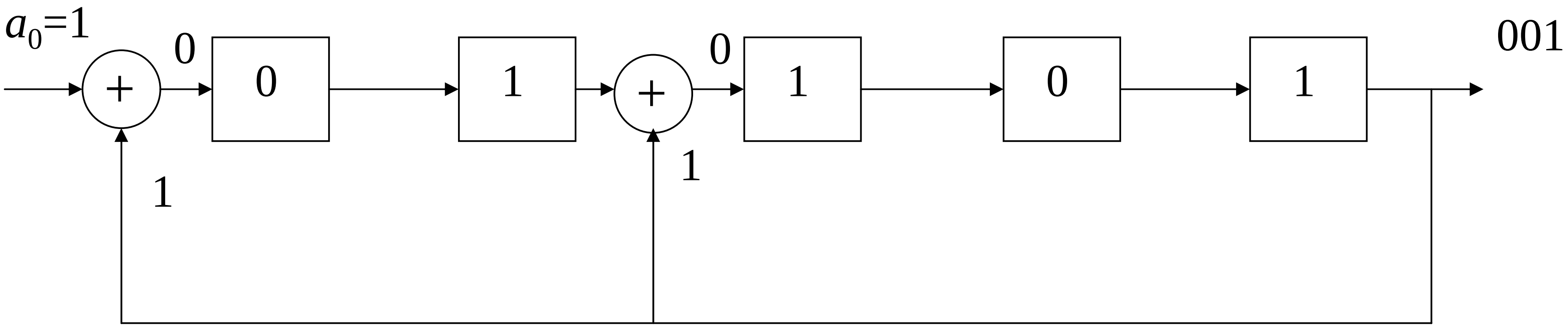
Example cont'd



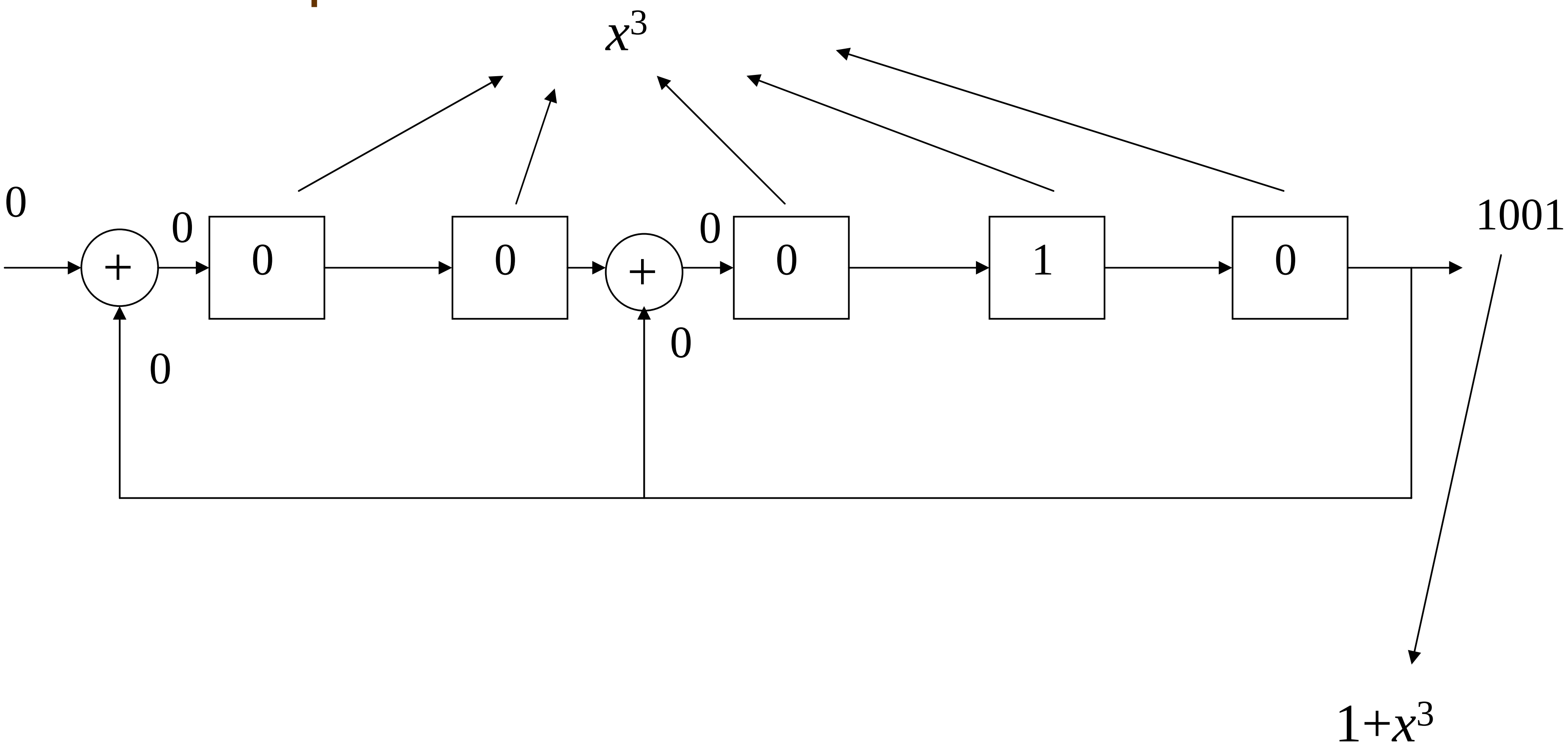
Example cont'd



Example cont'd

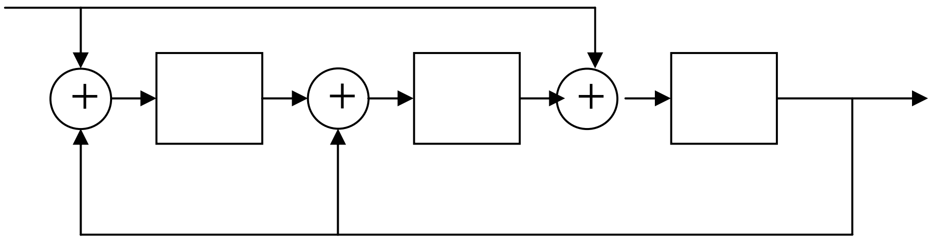


Example cont'd



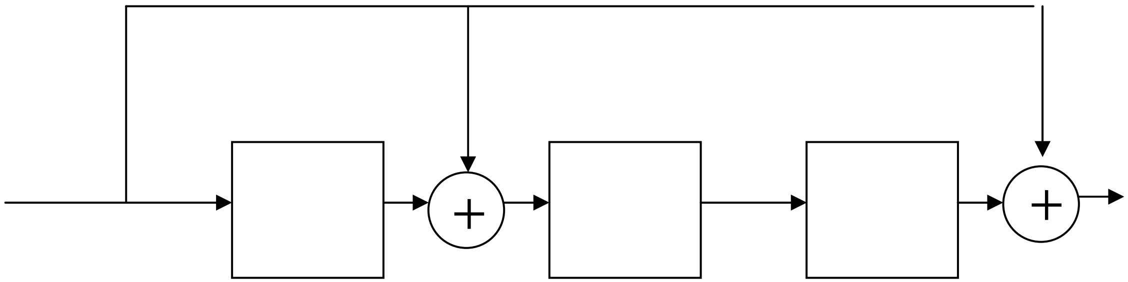
Joint multiplication-division

- Note that a multiplier circuit is essentially an FIR filter and a division circuit is essentially an IIR filter.
- If we wanted a circuit to compute $a(x) \times (p_1(x)/p_2(x))$, we could cascade a multiplier circuit followed by a division circuit.
- For example, the circuit with response x^2+1/x^3+x+1 is



Non-Systematic Encoding of Cyclic Codes

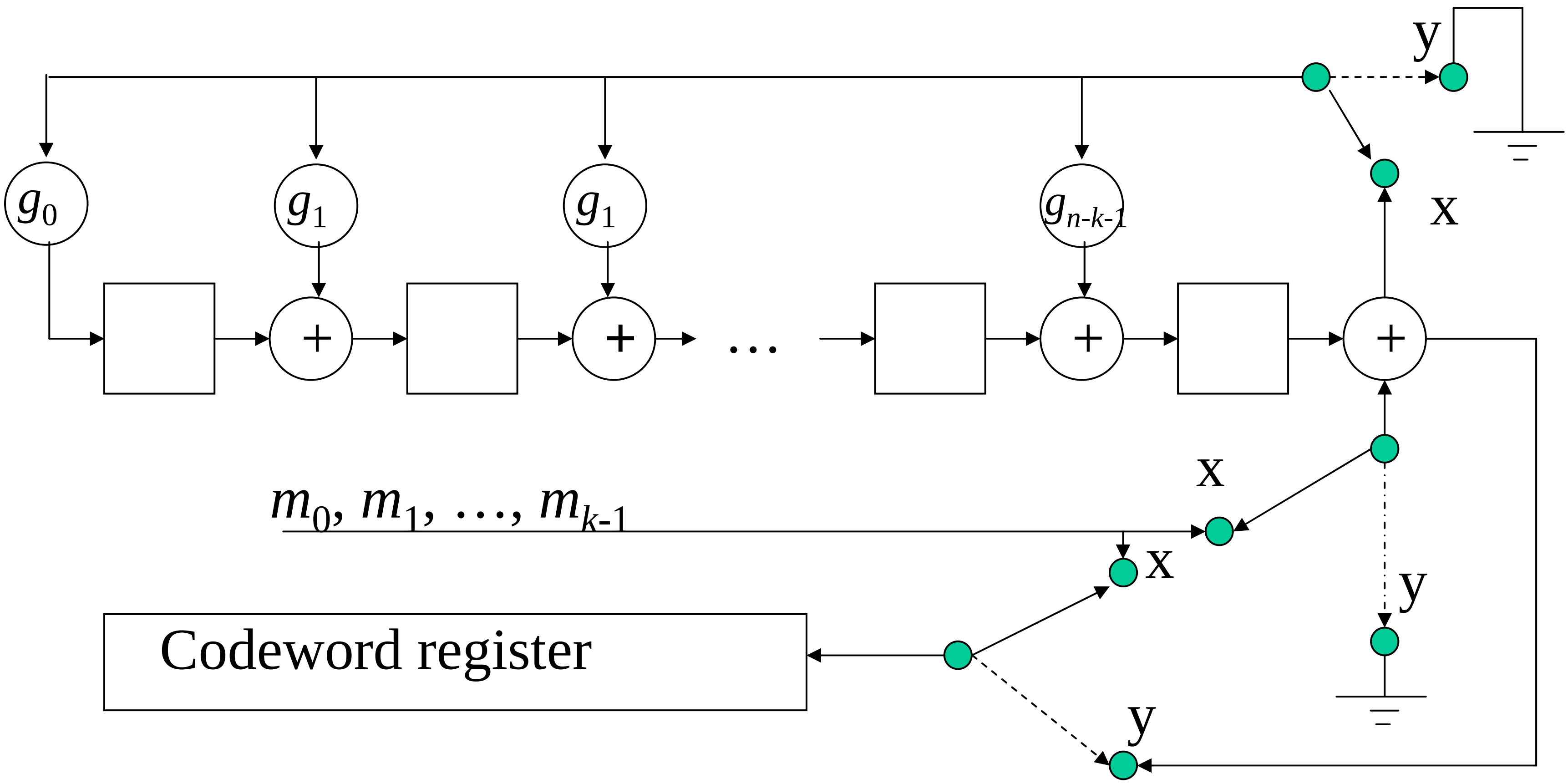
- Non-Systematic encoding of cyclic codes is simply polynomial multiplication.
- The encoder for a (7,4) cyclic code generated by $g(x) = x^3+x+1$ is:



Systematic Encoding of Cyclic Codes

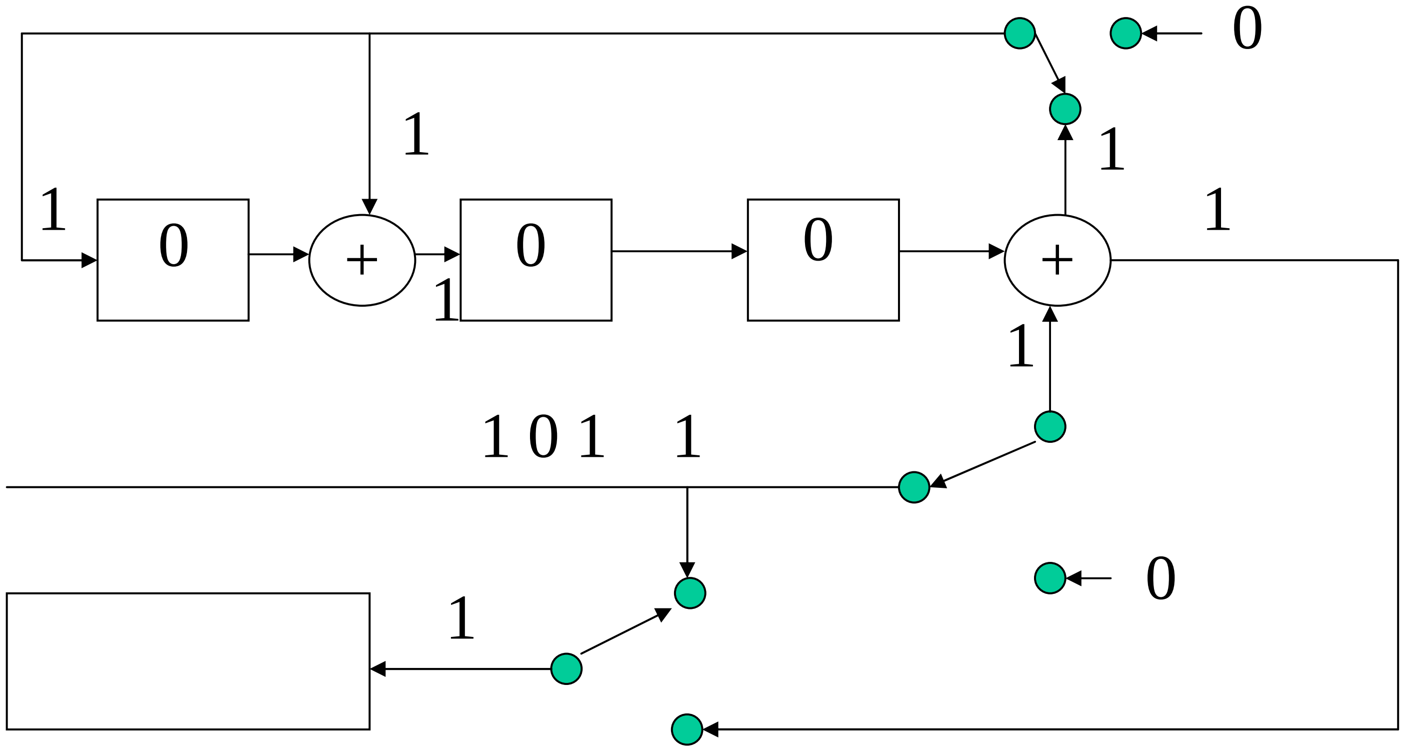
- Here we will use a switched circuit.
- We need a divider circuit to compute the remainder of $x^{n-k}m(x)/g(x)$.
- There are two parts: 1) message part of codeword, 2) calculation of parity symbols of codeword.

Systematic Encoding of Cyclic Codes



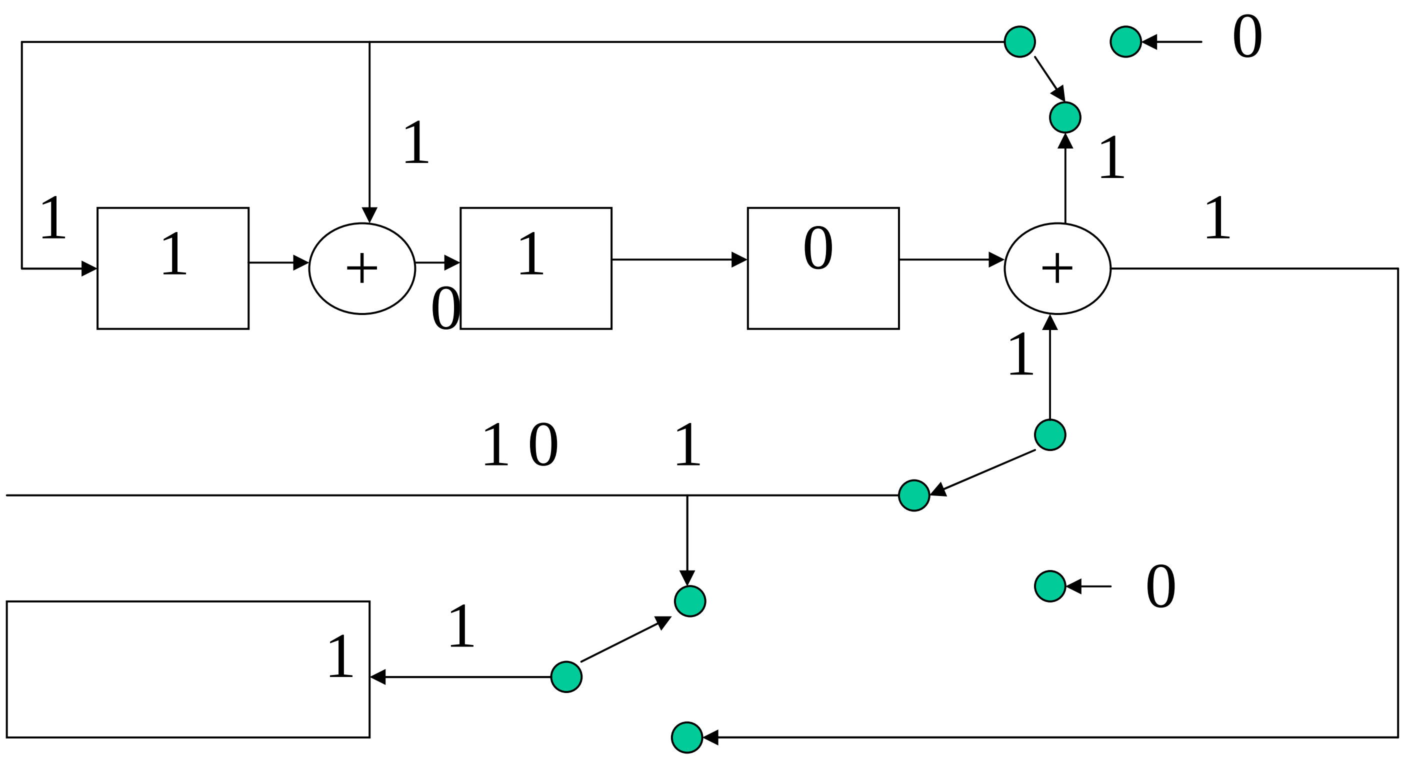
Initially all switches to x until message word is completely entered, then all switches to y.

Example (7,4) code, $g(x) = x^3+x+1$

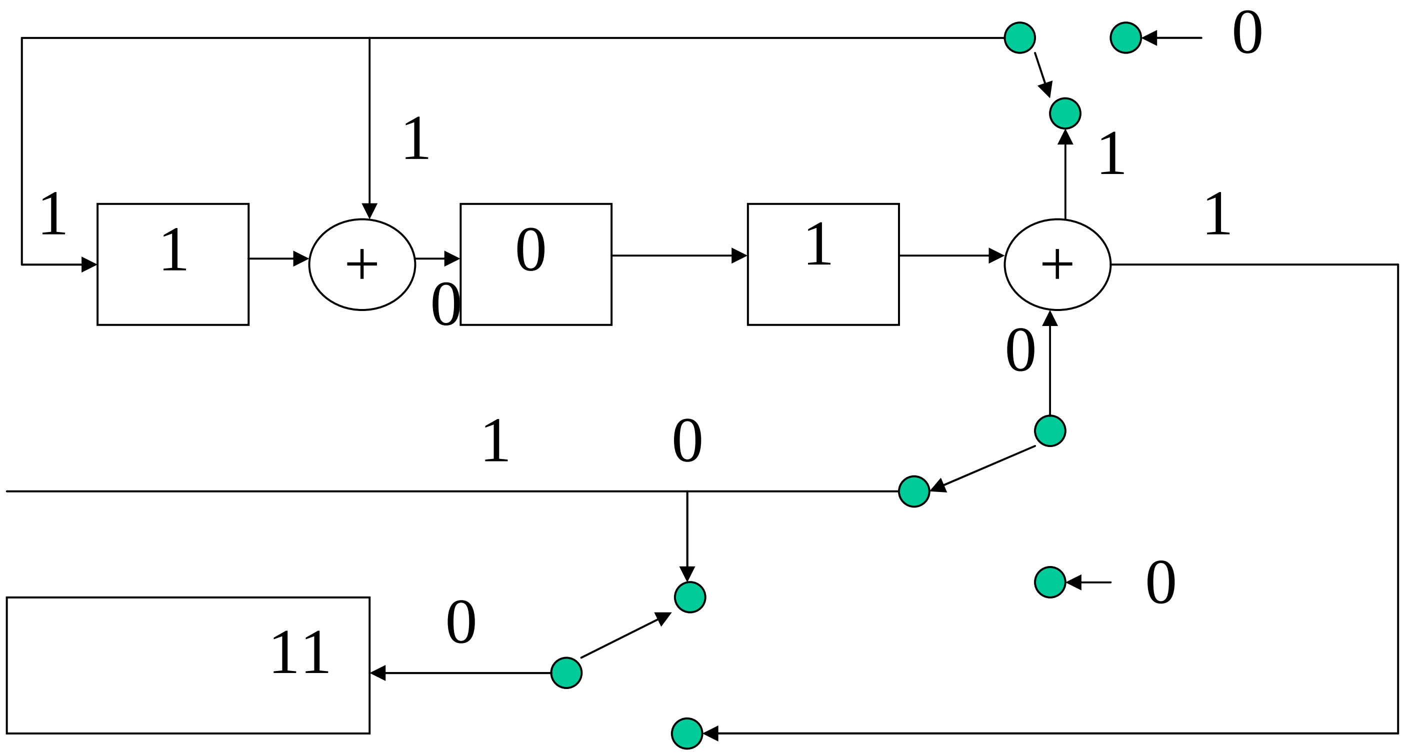


Message $m(x) = x^3+x^2+1$

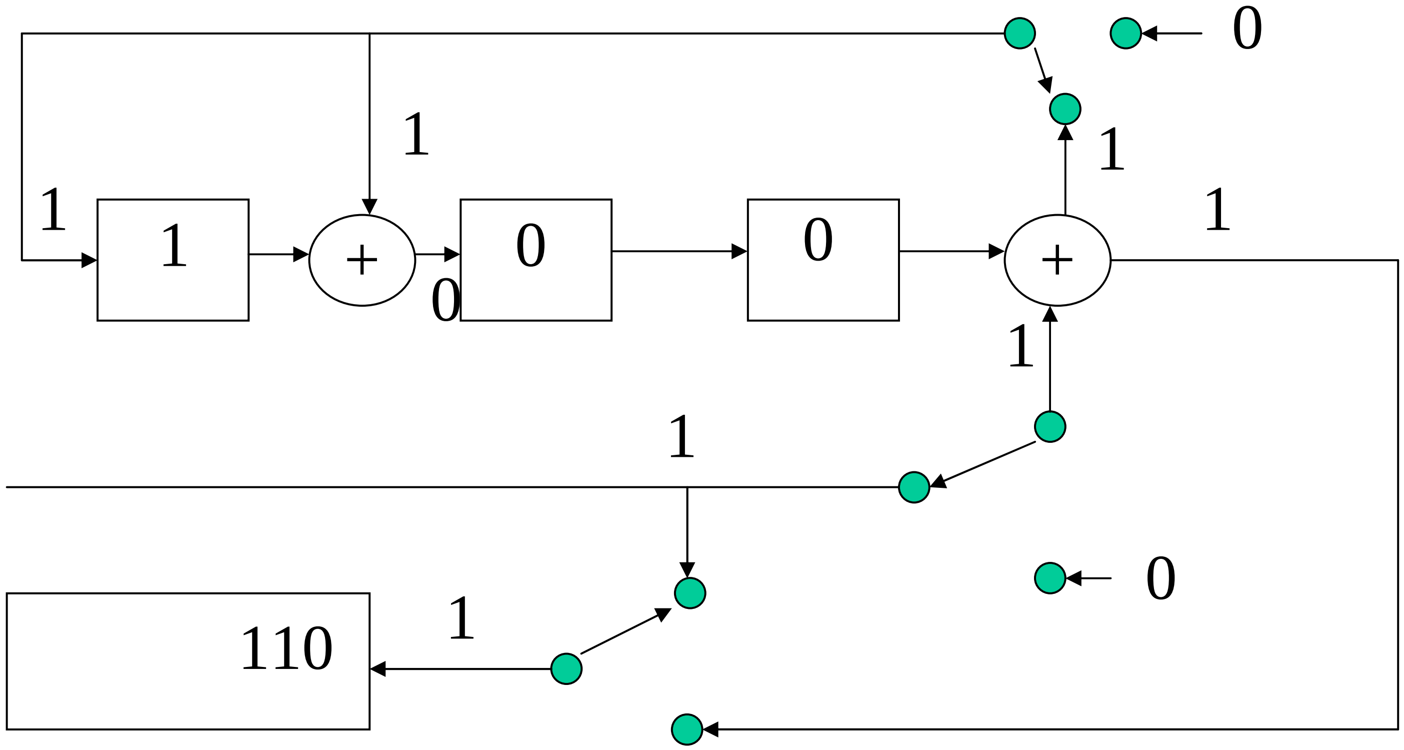
Example (7,4) code, $g(x) = x^3+x+1$



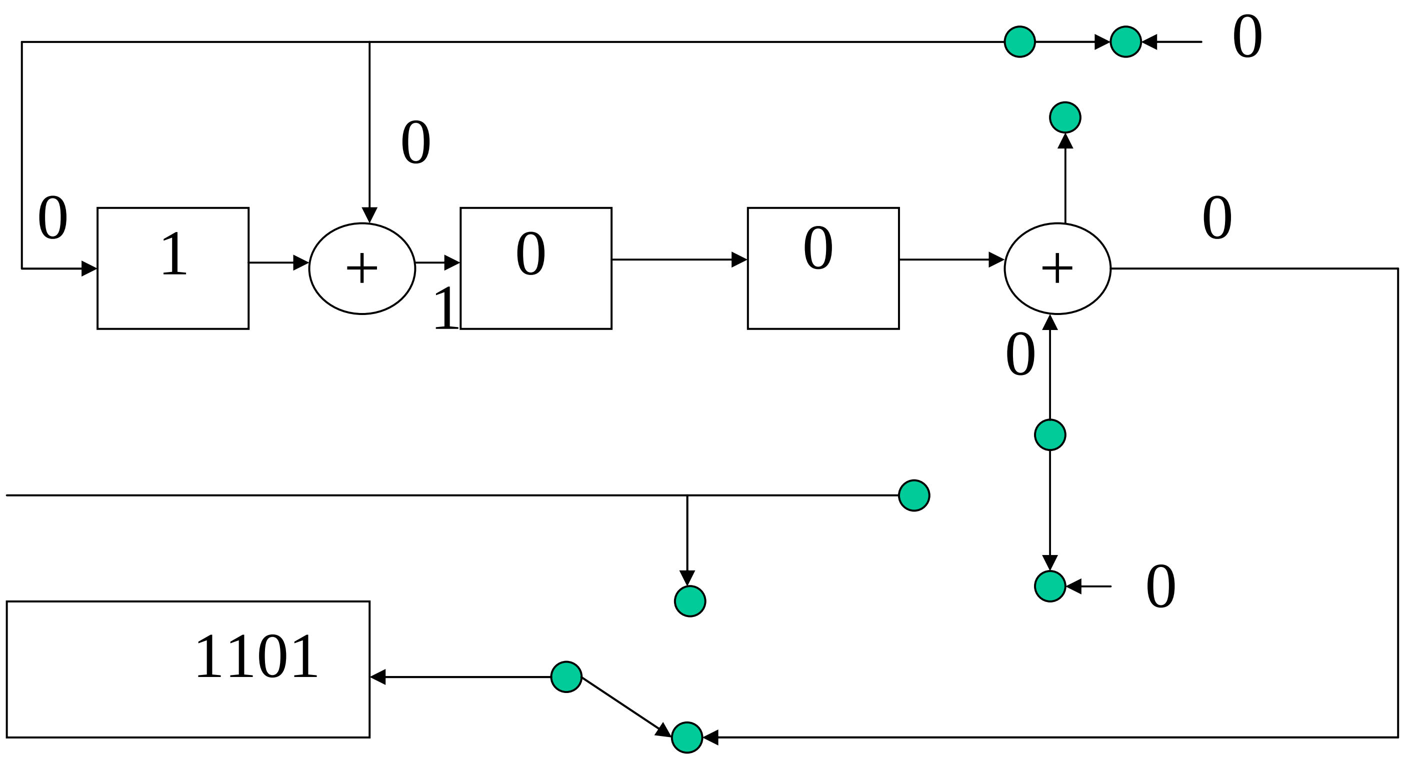
Example (7,4) code, $g(x) = x^3+x+1$



Example (7,4) code, $g(x) = x^3+x+1$

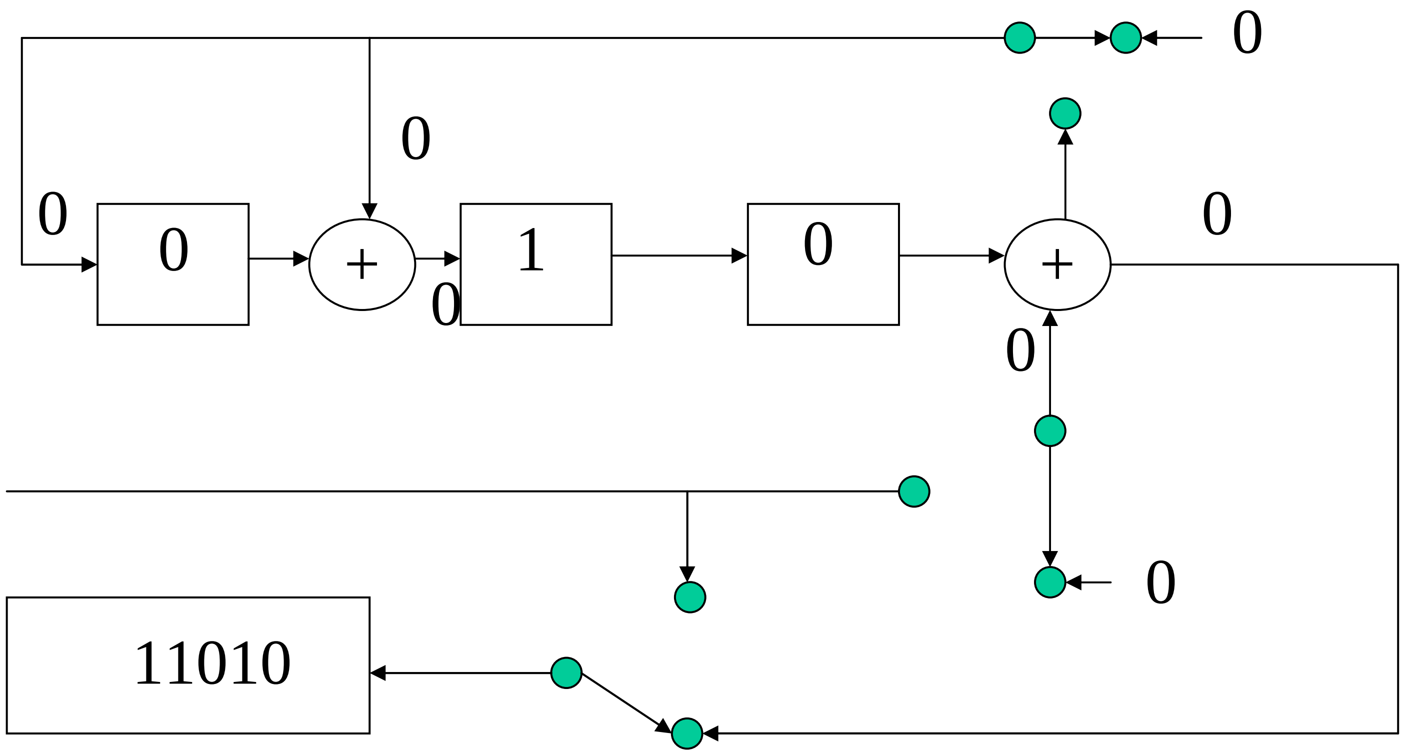


Example (7,4) code, $g(x) = x^3+x+1$

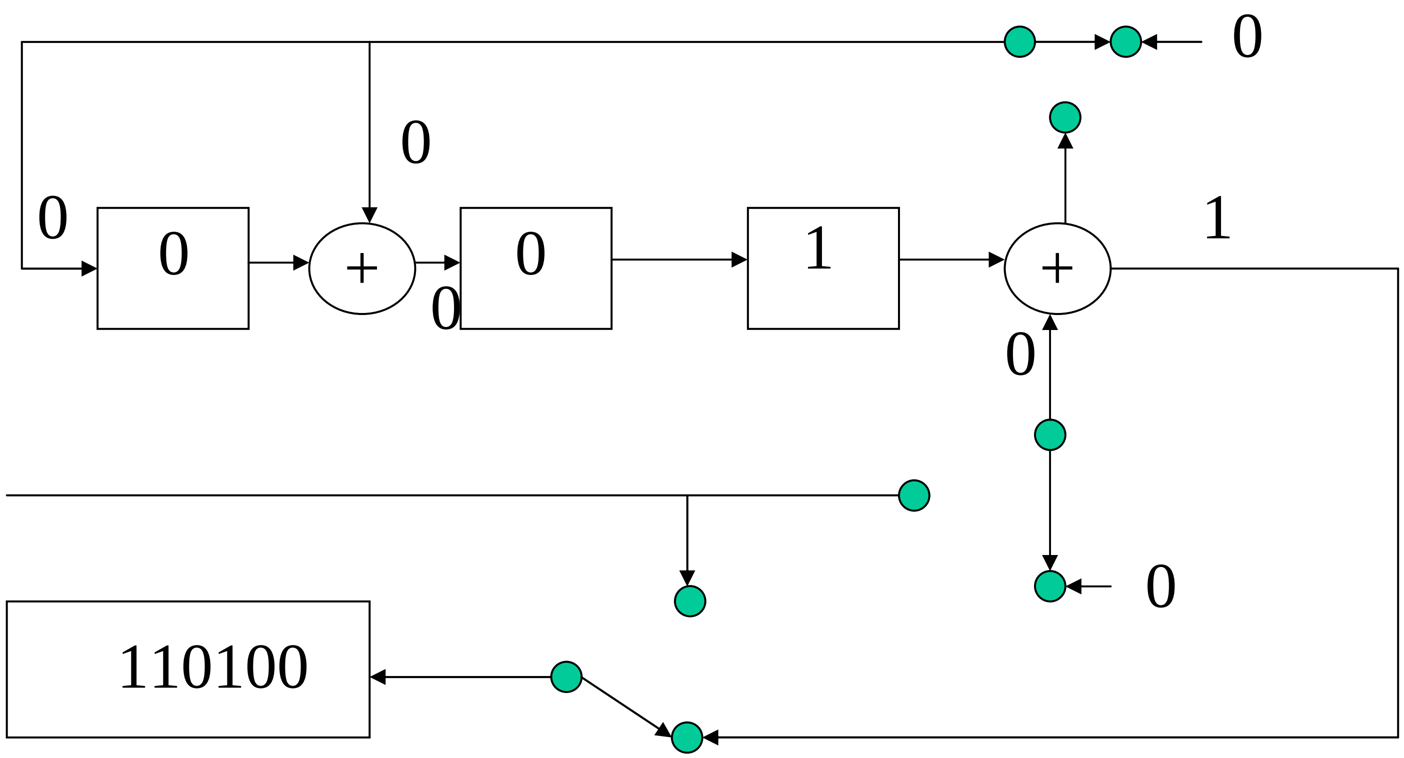


Over next three cycles,
the remainder will shift out of the register

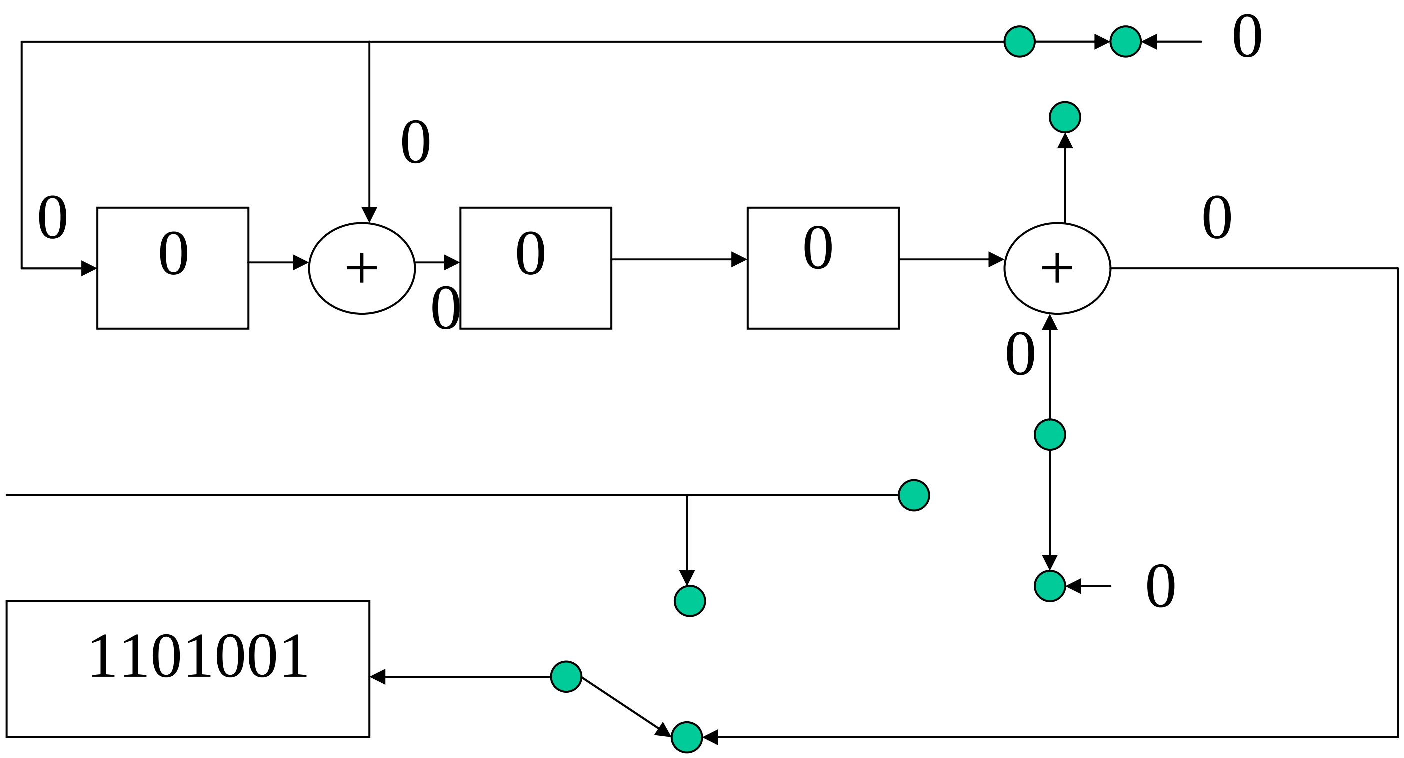
Example (7,4) code, $g(x) = x^3+x+1$



Example (7,4) code, $g(x) = x^3+x+1$



Example (7,4) code, $g(x) = x^3+x+1$



Syndrome decoding

- Let us define the syndrome as the remainder in the following equation:
  - $r(\mathrm{x}) = q(x)g(x)+\mathrm{s}(x)$, where $r(x) = c(x)+e(x)$.
  - $s(x) = s_0+s_1x+\ldots+s_{n-k-1}x^{n-k-1}$.
- Let $r^R(x)$ be the right cyclic shift of $r(x)$.
  - $r^R(x) = xr(x) \bmod(x^n-1)$.

Cyclic Coding Theorem 2

- For $r(x)$ having syndrome $s(x)$, $r^R(x)$ has syndrome $s'(x) = xs(x) \bmod g(x)$.
- Proof
  - $r(x) = q(x)g(x)+s(x)$
  - $r^R(x) = xr(x)-(x^n-1)r_{n-1}$.
  - $r^R(x) = q'(x)g(x)+s'(x) = x(q(x)g(x)+s(x))-(x^n-1)r_{n-1}$
  - $x^n-1 = g(x)h(x)$.
  - Therefore $q'(x)g(x)+s'(x) = x(q(x)g(x)+s(x))-g(x)h(x)r_{n-1}$
  - $xs(x) = (q'(x)-xq(x)+h(x)r_{n-1})g(x)+s'(x)$.
  - Therefore, $s'(x)$ is the remainder when we divide $xs(x)$ by $g(x)$.

Syndrome calculation

- Assume that we transmit 0000000 for the cyclic code with generator $g(x) = x^3+x+1$.
- If we receive 1000000 ($r(x) = 1$), $s(x) = 1$
- For $r(x) = x$, $s(x) = x$
- For $r(x) = x^2$, $s(x) = x^2$
- For $r(x) = x^3$, $s(x) = x+1$
- For $r(x) = x^4$, $s(x) = x^2+x$
- For $r(x) = x^5$, $s(x) = x^2+x+1$
- For $r(x) = x^6$, $s(x) = x^2+1$
- For systematic codes, when the error is in the parity bits, the syndrome is equal to the error polynomial $e(x)$.