TSKS01 Digital Communication
Lecture 11

Convolutional codes, CRC codes

Emil Björnson

Department of Electrical Engineering (ISY)

Division of Communication Systems

Outline of the Lecture

- Convolutional codes
  - Trellis representation and Viterbi

- CRC codes
  - Introduction
  - Error detection

Generating a Convolutional Code

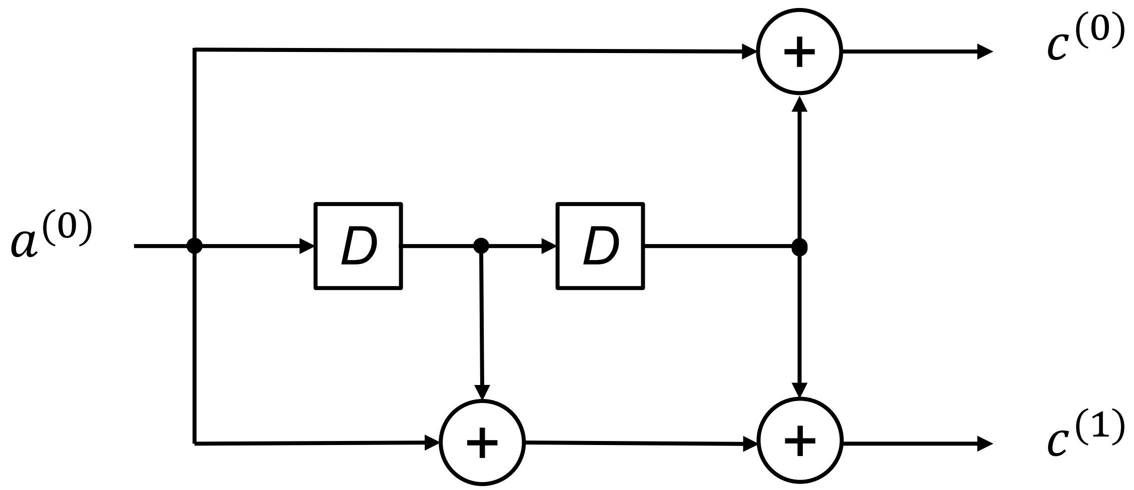
- Dimensions:
  - k inputs to encoder
  - n outputs from encoder

  Coding rate: $R = \frac{k}{n}$

- Generator matrix $G(D)$
  - Dimension $k\ x\ n$

- Generating codewords
  - Input: $A(D) = a_0 + a_1 D + a_2 D^2 + \cdots$
  - Output: $C(D) = A(D)G(D)$

Example:



- Generator matrix:

$$G(D) = (1 + D^2, 1 + D + D^2)$$

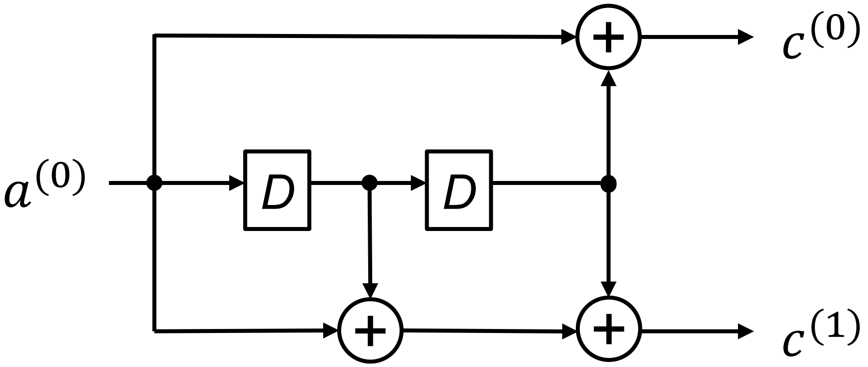
  - Obtained since impulse $A(D) = 1$ gives output

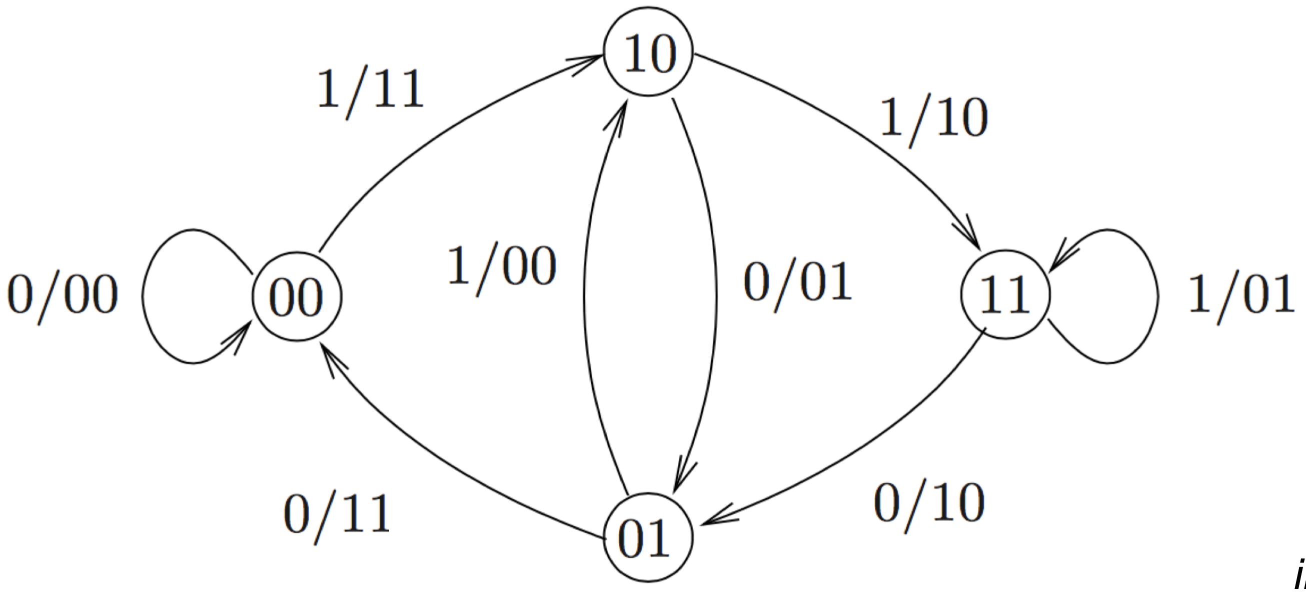
$$C^{(0)}(D) = 1 + D^2 \text{ and } C^{(1)}(D) = 1 + D + D^2$$

State Transition Diagram

Shows

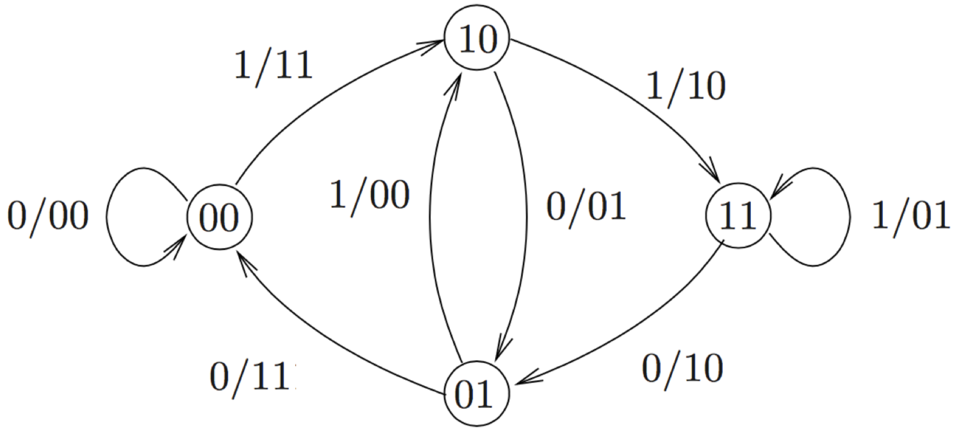
- Number of states: $2^{\text{nbr of delay elements}}$
- Possible state transitions
- Corresponding input and output



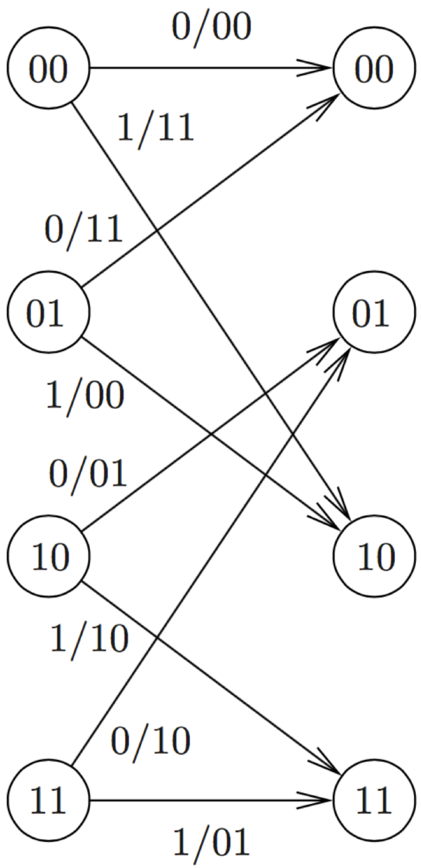


Notation: input/outputs

Trellis Representation (1/2)

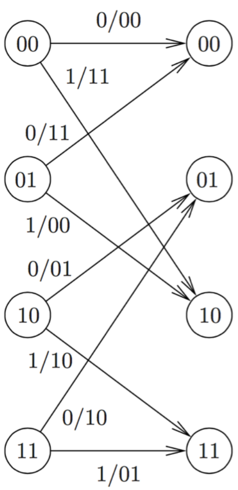


State transition diagram



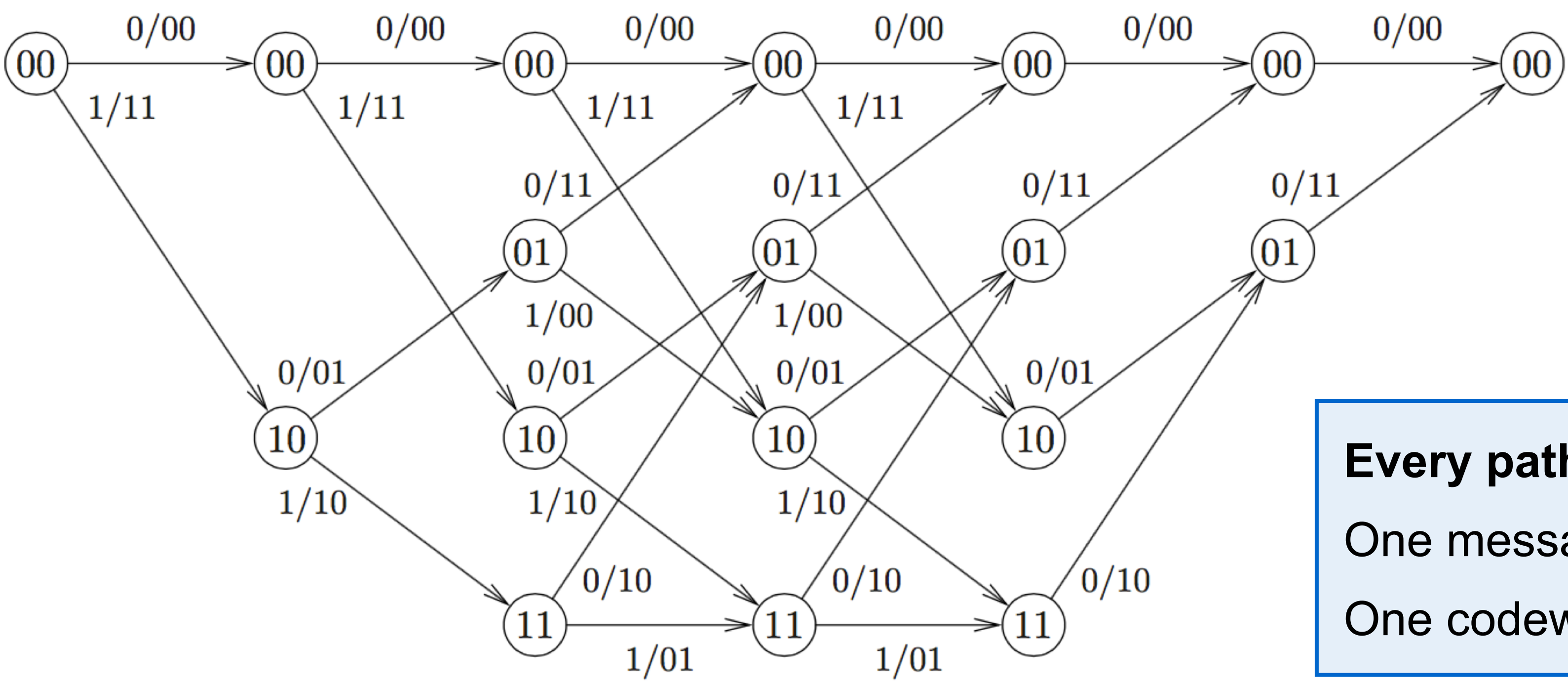
Section of a trellis

Trellis Representation (2/2)



Suppose

- We begin in 00
- We add two extra zeros at end of message to end in 00



Every path:

One message

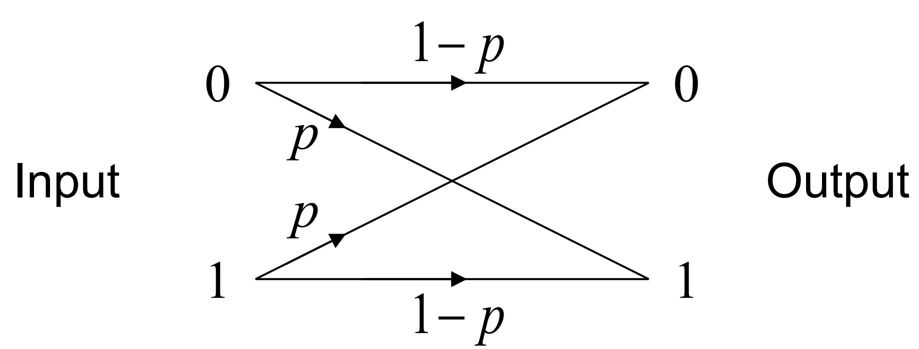
One codeword

Decoding of a Convolutional Code

Decoding: Obtain $\hat{a}$ from a received bit sequence that contains errors

Approach:

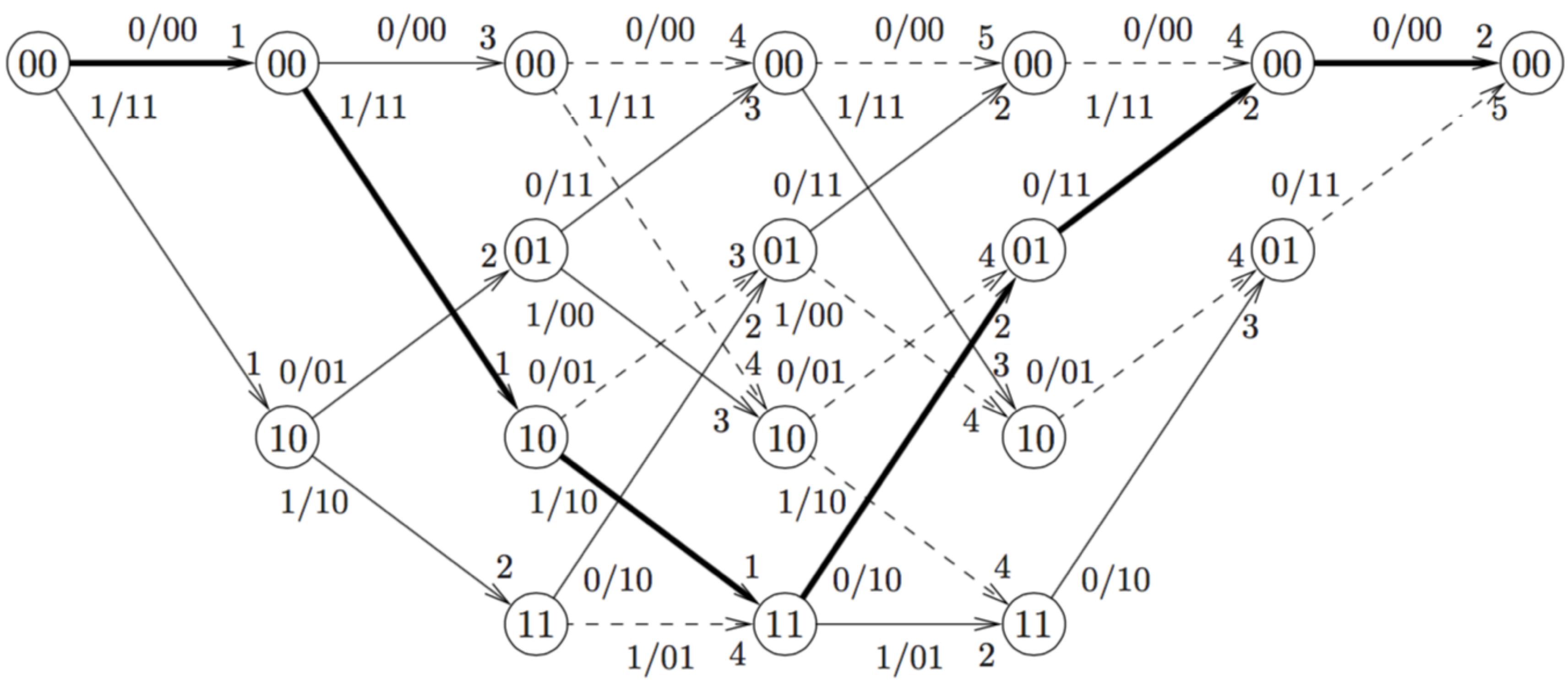
- Use trellis representation and apply Viterbi algorithm
- Begin in state 00 and end in state 00
- If binary symmetric channel with $p \leq 0.5$:
  Choose the path with fewest bit errors (smallest Hamming distance)



p = Bit error probability

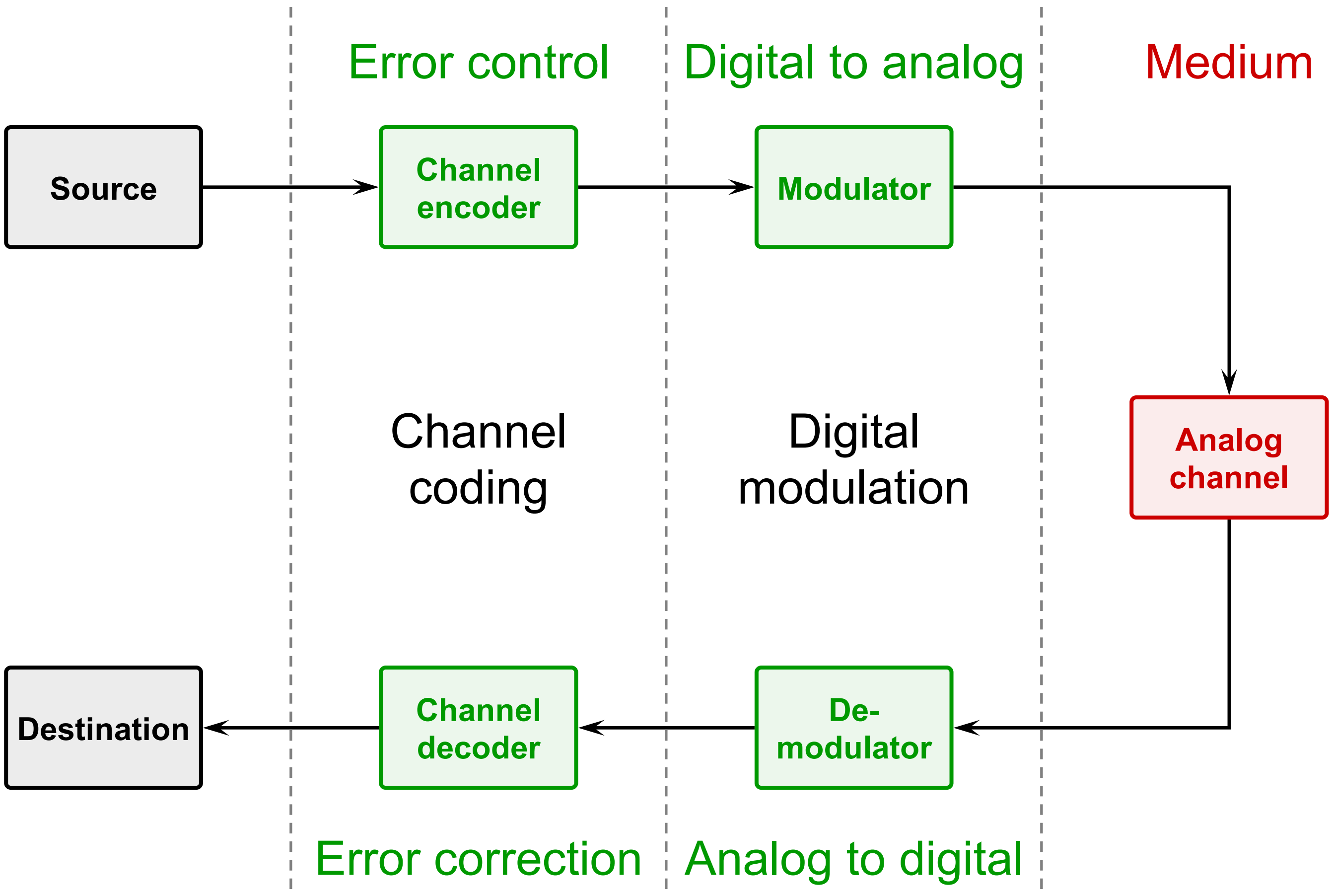
Example: Viterbi for Convolutional Code

Received signal: 01 11 10 11 11 00



ML decoding: 0 1 1 0 0 0

Detection of Errors

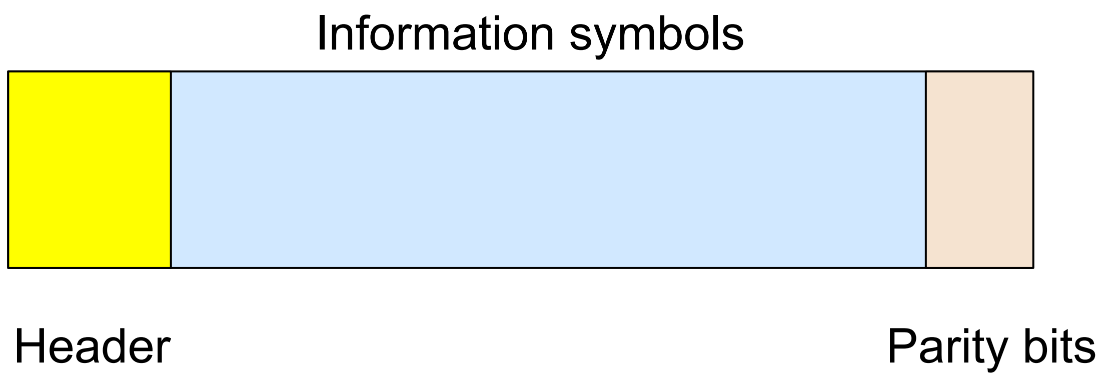


What if we detect an error, but cannot correct it?

ARQ: Automatic Repeat reQuest

Simple packet structure

- Header: Describes the content and destination
- Parity bits: Detect packet errors



If the packet has (uncorrectable) errors: **Request retransmission**

Cyclic Redundancy Check (CRC) codes

- Commonly used in digital communications to detect errors
  - Redundancy: Add parity bits
  - Check: **Detect** it there are any errors

Can in principle be used for error correction, but normally not

Based on division of binary polynomials

Integer and Polynomial Division

Integer division

Ex: $\frac{1732}{15} = 115 + \frac{7}{15}$

```
        1 1 5  ← Quotient
15 |  1 7 3 2
     -1 5
        2 3
       -1 5
          8 2
         -7 5
            7  ← Remainder
```

Polynomial division (binary polynomials)

Ex: $\frac{x^5+x^3+x+1}{x^2+x+1} = x^3+x^2+x+\frac{1}{x^2+x+1}$

$$\begin{array}{r} 1\cdot x^3+1\cdot x^2+1\cdot x+0\cdot 1 \\ x^2+x+1 \;\big)\; 1\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2+1\cdot x+1\cdot 1 \\ 1\cdot x^5+1\cdot x^4+1\cdot x^3 \\ \hline 1\cdot x^4+0\cdot x^3+0\cdot x^2 \\ 1\cdot x^4+1\cdot x^3+1\cdot x^2 \\ \hline 1\cdot x^3+1\cdot x^2+1\cdot x \\ 1\cdot x^3+1\cdot x^2+1\cdot x \\ \hline 0\cdot x^2+0\cdot x+1\cdot 1 \\ 0\cdot x^2+0\cdot x+0\cdot 1 \\ \hline 0\cdot x+1\cdot 1 \end{array}$$

With bits only:

```
          1 1 1 0
111 | 1 0 1 0 1 1
      1 1 1
        1 0 0
        1 1 1
          1 1 1
          1 1 1
            0 0 1
            0 0 0
              0 1
```

Division Algorithms

Division Algorithm for Integers (2000 years old wisdom) :

Given integers a and b, $b \neq 0$. Then there exist unique integers q and r, $0 \leq r < |b|$, such that $a = qb + r$ holds.

Division Algorithm for Binary Polynomials (slightly newer wisdom):

Given binary polynomials $a(x)$ and $b(x)$, $b(x) \neq 0$. Then there exist unique binary polynomials $q(x)$ and $r(x)$, $\deg\{r(x)\} < \deg\{b(x)\}$, such that $a(x) = q(x)b(x) + r(x)$ holds.

CRC Code Generation

- Input
  - $m(x)$: Message of length k, as polynomial with degree up to $k-1$
  - $p(x)$: CRC polynomial of degree $n-k$
- Generation
  - Compute remainder $r(x)$:

$$x^{n-k}m(x) = q(x)p(x) + r(x)$$

  - Create codeword:

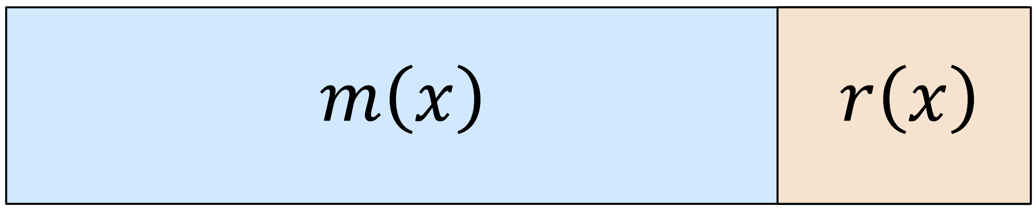
$$c(x) = x^{n-k}m(x) + r(x)$$

Result: $c(x) = q(x)p(x)$ with zero remainder

Interpreting CRC Code as Block Code

- Codeword

$$c(x) = x^{n-k}m(x) + r(x)$$



  - The factor x^{n-k} makes sure that all terms in $x^{n-k}m(x)$ have a higher degree than $r(x)$

- Example: $c(x) = x^5 + x^4 + x$
  - Write as binary sequence 110010
  - Send on bit at a time over the channel

CRC Error Detection

- Received signal:

$$y(x) = c(x) + w(x)$$

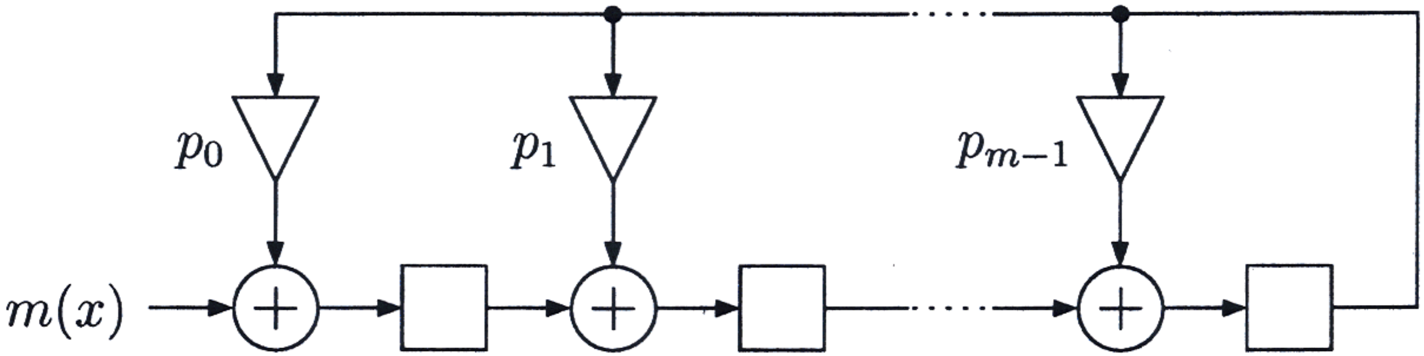
  - Polynomial with errors: $w(x)$
  - No errors: $w(x) = 0$

Detect error: $y(x)$ has a non-zero remainder when divided by $p(x)$

  - Design CRC polynomial $p(x)$ to make it unlikely that it divides $w(x)$
  - For each choice we can compute how many errors it can detect
  - Some examples are given in the book

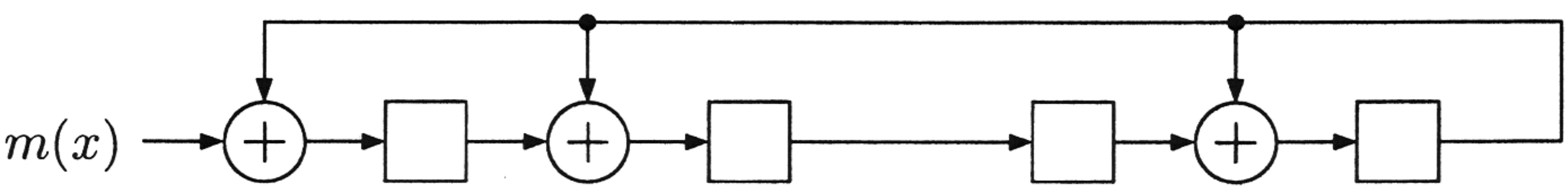
Shift Register Implementation

$$p(x) = \sum_{i=0}^{m} p_i x^i, \qquad p_m = 1, \qquad m = n - k.$$



Example:

$$p(x): \quad 1 \quad + \quad 1 \cdot x \quad + \quad 0 \cdot x^2 \quad + \quad 1 \cdot x^3 \quad + \quad 1 \cdot x^4$$



LINKÖPING UNIVERSITY

www.liu.se