Zürcher Hochschule Winterthur

Error-Correcting Codes

Applied Coding Theory in Engineering

Andreas Steffen

Error-Correcting Codes
Overview

- Part I - Applications of Cyclic Block Codes
  - Short Theory of Cyclic Codes
  - Multiplication / Division using Shift Registers
  - Syndrome Generators
  - Systematic Encoders
  - Synchronisation Method for Cyclic Codes
  - Application Examples
- Part II - Applications of Convolutional Codes
  - Short Theory of Convolutional Codes
  - Tree and Trellis Representations
  - Viterbi Decoding
  - Application Examples

Error-Correcting Codes
Literature

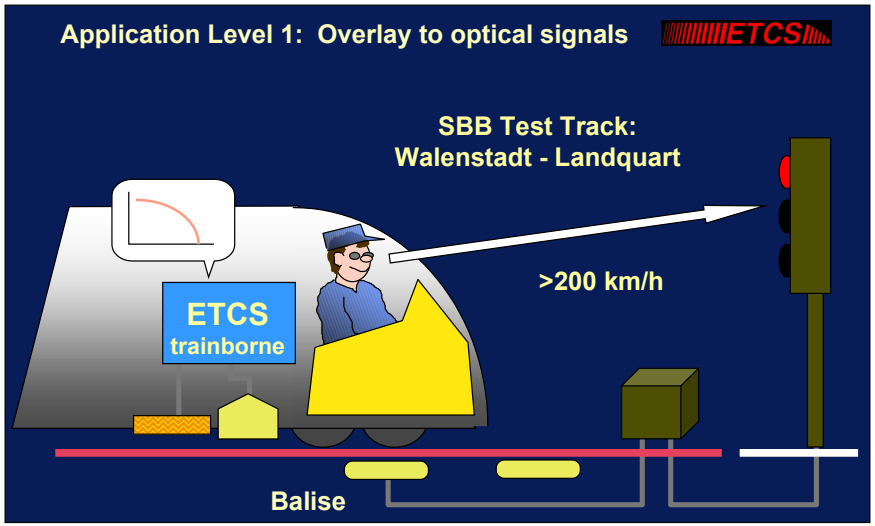
- Error-Correcting Codes, Second Edition
  - W. Wesley Peterson & E. J. Weldon
  - MIT Press, 1972, 560 pages
  - ISBN 0-262-16-039-0
- Applied Digital Information Theory
  - James L. Massey
  - ETHZ Script, 1981
  - Chapter 7 „Error-Correcting Codes“
  - Chapter 6 „Tree and Trellis Coding Principles“

Error-Correcting Codes - Part I

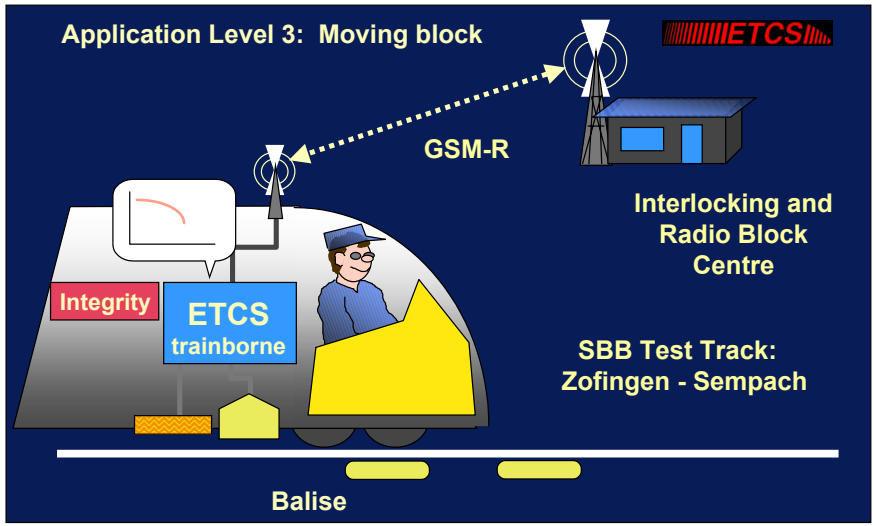
Applications of

Cyclic Block Codes

European Train Control System (ETCS)
Signalling for High-Speed Trains



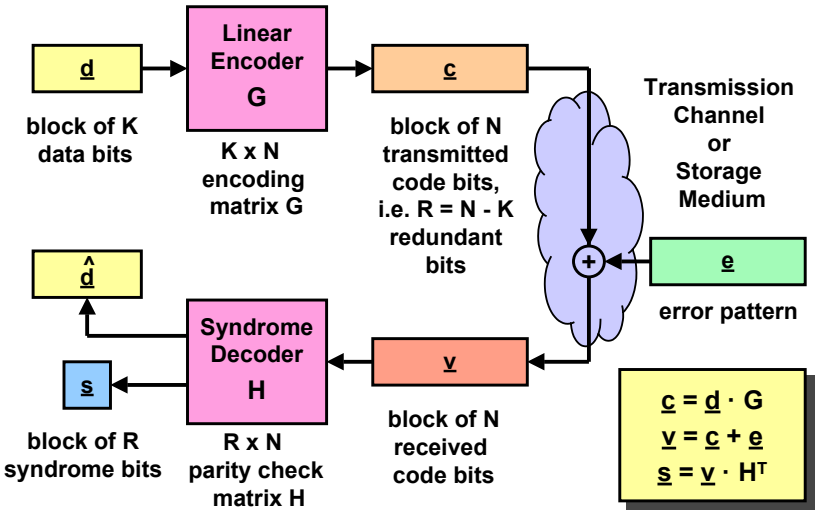
European Train Control System (ETCS)
Train Control without Trackside Signals



European Train Control System (ETCS)
Technical Data of ETCS Balise

- Magnetic loop antenna
- Telepowering of balise
- BCH coded telegrams
- 5 x 1023 bits in 10 ms

Error-Correcting Codes
Linear (N,K) Block Codes



Linear (N,K) Block Codes
Cyclic Codes - Encoding Matrix

- Encoding matrix of a general linear (N,K) block code

$$\mathbf{G} = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & \cdots & g_{0,n} & \cdots & g_{0,N-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & \cdots & g_{1,n} & \cdots & g_{1,N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{K-1,0} & g_{K-1,1} & g_{K-1,2} & \cdots & g_{K-1,n} & \cdots & g_{K-1,N-1} \end{bmatrix}$$

- Encoding matrix of a cyclic linear (N,K) block code

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{N-K} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{N-K} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{N-K} & 0 \\ 0 & \cdots & 0 & 0 & g_0 & g_1 & \cdots & g_{N-K} \end{bmatrix}$$

Linear (N,K) Block Codes
Cyclic Codes - Parity-Check Matrix

- Orthogonal subspaces: valid codeword has zero syndrome

$$\underline{\mathbf{s}} = \underline{\mathbf{c}} \cdot \mathbf{H}^{\mathrm{T}} = \underline{\mathbf{d}} \cdot \mathbf{G} \cdot \mathbf{H}^{\mathrm{T}} = \underline{\mathbf{0}} \quad \Rightarrow \quad \mathbf{G} \cdot \mathbf{H}^{\mathrm{T}} = \mathbf{0}$$

- Parity-check matrix of a cyclic linear (N,K) block code

$$\mathbf{H} = \begin{bmatrix} h_K & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_K & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \cdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_K & \cdots & h_1 & h_0 & 0 \\ 0 & \cdots & 0 & 0 & h_K & \cdots & h_1 & h_0 \end{bmatrix}$$

Cyclic Codes
Example: The (7,4) Cyclic Code

- Matrix Multiplication

$$\underline{\mathbf{c}} = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \end{bmatrix} = \underline{\mathbf{d}}\,\mathbf{G} = \begin{bmatrix} d_0 & d_1 & d_2 & d_3 \end{bmatrix} \cdot \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{bmatrix}$$

$$\underline{\mathbf{c}}^{\mathrm{T}} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{bmatrix} = \begin{bmatrix} d_0 g_0 & & & \\ d_1 g_0 + d_0 g_1 & & & \\ d_2 g_0 + d_1 g_1 + d_0 g_2 & & & \\ d_3 g_0 + d_2 g_1 + d_1 g_2 + d_0 g_3 & & & \\ d_3 g_1 + d_2 g_2 + d_1 g_3 & & & \\ d_3 g_2 + d_2 g_3 & & & \\ d_3 g_3 & & & \end{bmatrix}$$

- Polynomial Multiplication

$$c(x) = d(x) \cdot g(x) \quad \text{with}$$

$$c(x) = c_0 x^6 + c_1 x^5 + c_2 x^4 + c_3 x^3 + c_4 x^2 + c_5 x + c_6$$
$$d(x) = d_0 x^3 + d_1 x^2 + d_2 x + d_3$$
$$g(x) = g_0 x^3 + g_1 x^2 + g_2 x + g_3$$

Cyclic Codes
Generating and Parity-Check Polynomials

- Generating polynomial g(x) is monic and unique

$$g(x) = g_0 x^3 + g_1 x^2 + g_2 x + g_3 \quad \text{with} \quad g_0 = 1$$

There is a unique monic generating polynomial g(x) of degree R = N - K in every q-ary cyclic linear (N,K) block code

- Generating polynomial g(x) is a factor of $x^N - 1$

$$x^N - 1 = g(x) \cdot h(x)$$

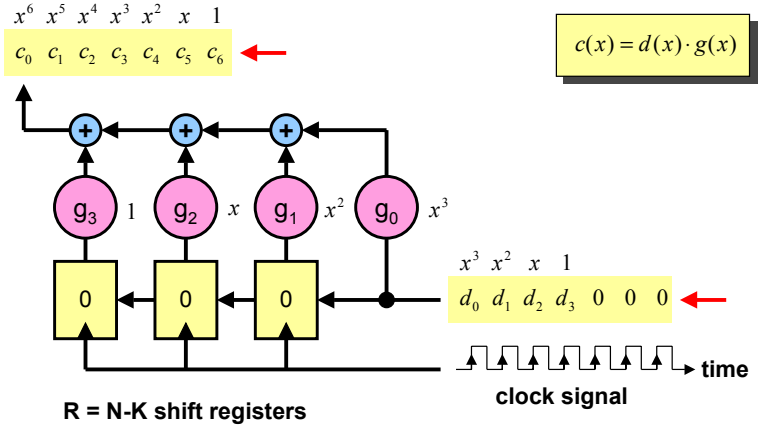
- Parity-check polynomial h(x) is the second factor of $x^N - 1$

$$h(x) = h_0 x^4 + h_1 x^3 + h_2 x^2 + h_3 x + h_4 \quad \text{with} \quad h_0 = 1$$

The monic parity-check polynomial h(x) has degree K

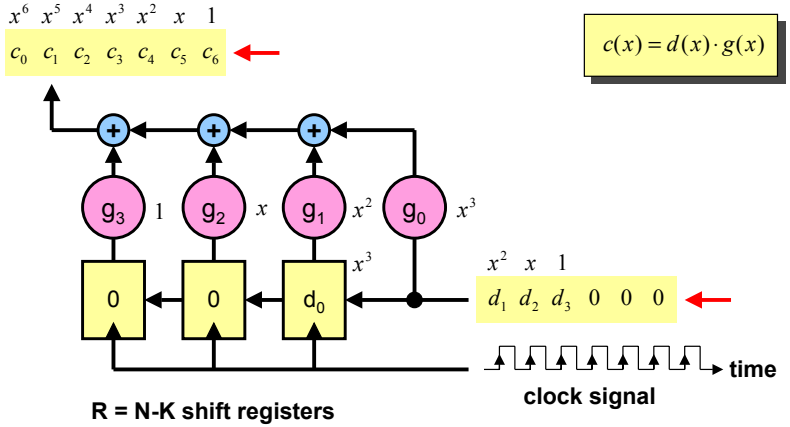
Multiplying Polynomials
Using Shift Registers I

- Time t = 0 units



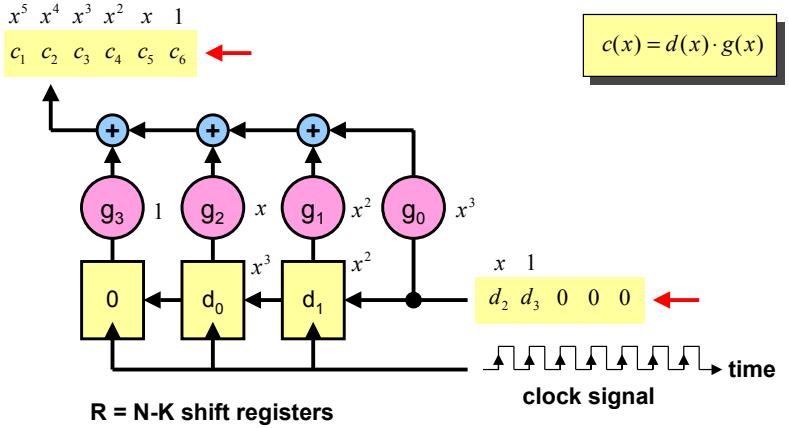
Multiplying Polynomials
Using Shift Registers II

- Time t = 1 units



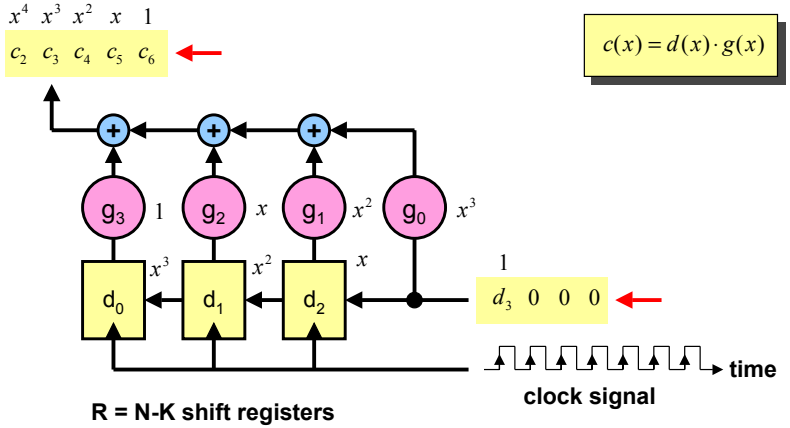
Multiplying Polynomials
Using Shift Registers III

- Time t = 2 units



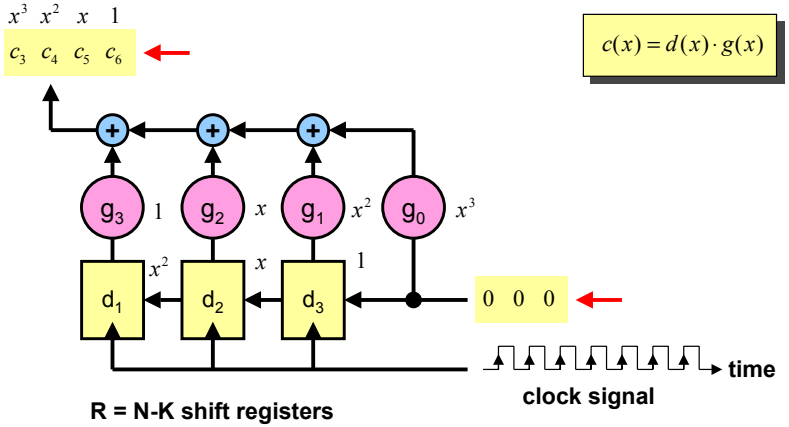
Multiplying Polynomials
Using Shift Registers IV

- Time t = 3 units



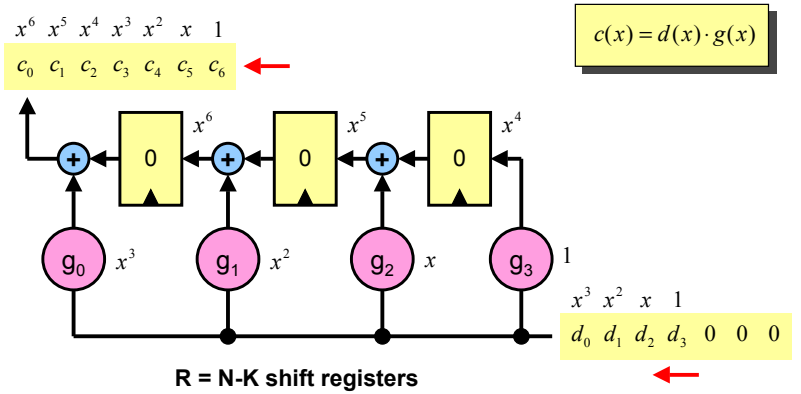
Multiplying Polynomials
Using Shift Registers V

- Time t = 4 units



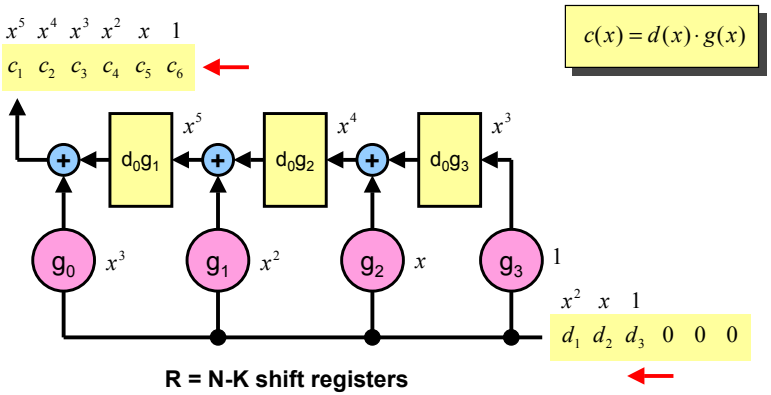
Multiplying Polynomials
Alternative Shift Register Circuit I

- Time t = 0 units



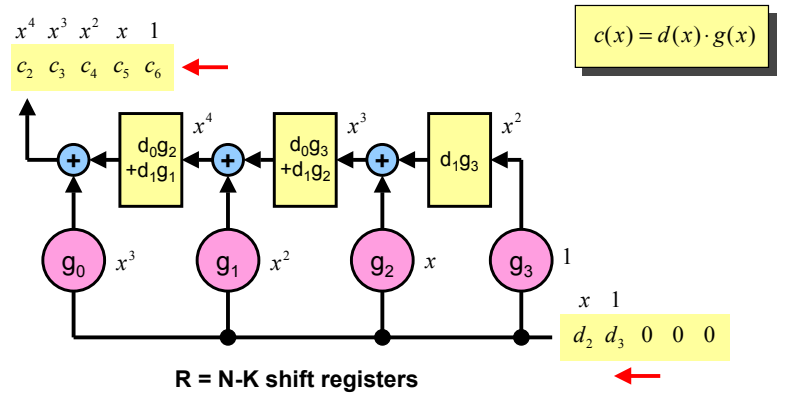
Multiplying Polynomials
Alternative Shift Register Circuit II

- Time t = 1 units



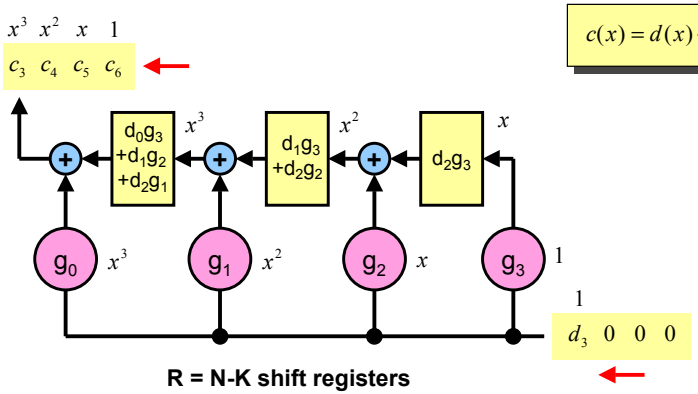
Multiplying Polynomials
Alternative Shift Register Circuit III

- Time t = 2 units



Multiplying Polynomials
Alternative Shift Register Circuit IV

- Time t = 3 units



Cyclic Codes
The (7,4) Binary Hamming Code

- Generating polynomial g(x) $g(x) = x^3 + x + 1$
- Parity-check polynomial h(x) $h(x) = x^4 + x^2 + x + 1$
- Factoring $g(x) \cdot h(x) = (x^3 + x + 1)(x^4 + x^2 + x + 1) = x^7 - 1$
- Generator Matrix G and Parity-Check Matrix H

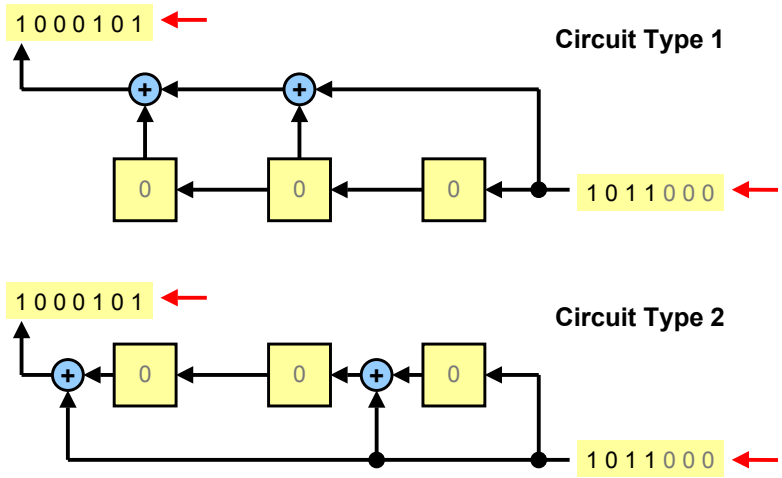
$$\mathbf{G} = \begin{bmatrix} 1&0&1&1&0&0&0 \\ 0&1&0&1&1&0&0 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{bmatrix} \quad \mathbf{H} = \begin{bmatrix} 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ 0&0&1&1&1&0&1 \end{bmatrix} \quad \mathbf{G} \cdot \mathbf{H}^T = \begin{bmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{bmatrix}$$

The (7,4) Binary Hamming Code
Table of Codewords

Data d	Codeword c = d G	Groups / Cyclic Shifts
0 0 0 0	0 0 0 0 0 0 0	1
0 0 0 1	0 0 0 1 0 1 1	2 +3
0 0 1 0	0 0 1 0 1 1 0	2 +2
0 0 1 1	0 0 1 1 1 0 1	3 +5
0 1 0 0	0 1 0 1 1 0 0	2 +1
0 1 0 1	0 1 0 0 1 1 1	3
0 1 1 0	0 1 1 1 0 1 0	3 +4
0 1 1 1	0 1 1 0 0 0 1	2 +6
1 0 0 0	1 0 1 1 0 0 0	2
1 0 0 1	1 0 1 0 0 1 1	3 +1
1 0 1 0	1 0 0 1 1 1 0	3 +6
1 0 1 1	1 0 0 0 1 0 1	2 +4
1 1 0 0	1 1 1 0 1 0 0	3 +3
1 1 0 1	1 1 1 1 1 1 1	4
1 1 1 0	1 1 0 0 0 1 0	2 +5
1 1 1 1	1 1 0 1 0 0 1	3 +2

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

The (7,4) Binary Hamming Code
Code Generators



Cyclic Codes
Syndrome Generators

- Generating polynomial g(x) divides valid codeword c(x)

$$c(x) / g(x) = d(x) \qquad s(x) = R_{g(x)}[c(x)] = R_{g(x)}[d(x)g(x)] = 0$$

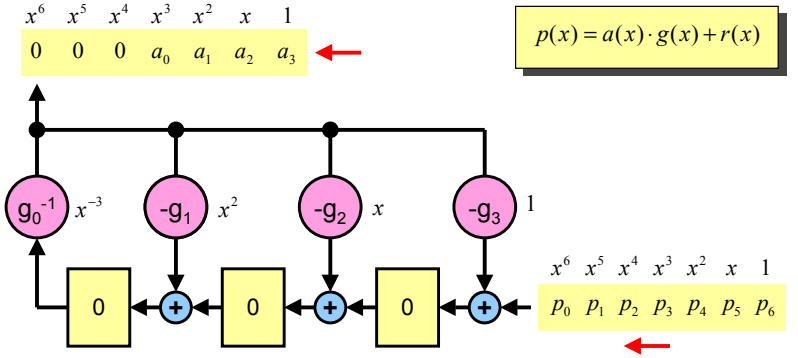
- Syndrome s(x) depends on error pattern e(x) only

$$s(x) = R_{g(x)}[c(x) + e(x)] = R_{g(x)}[e(x)]$$

- Circuits for dividing polynomials are needed !

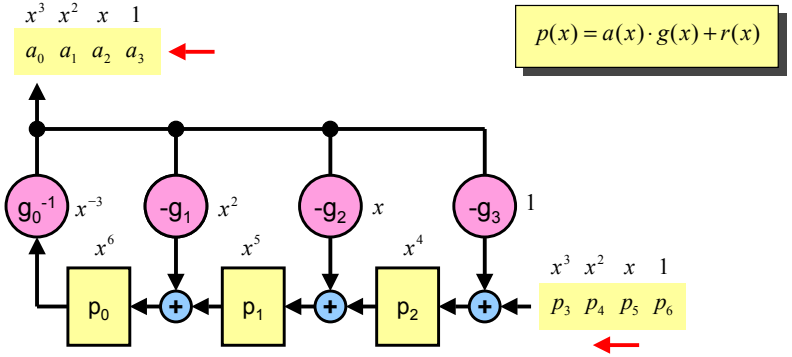
Dividing Polynomials
Using Shift Registers I

- Time t = 0 units



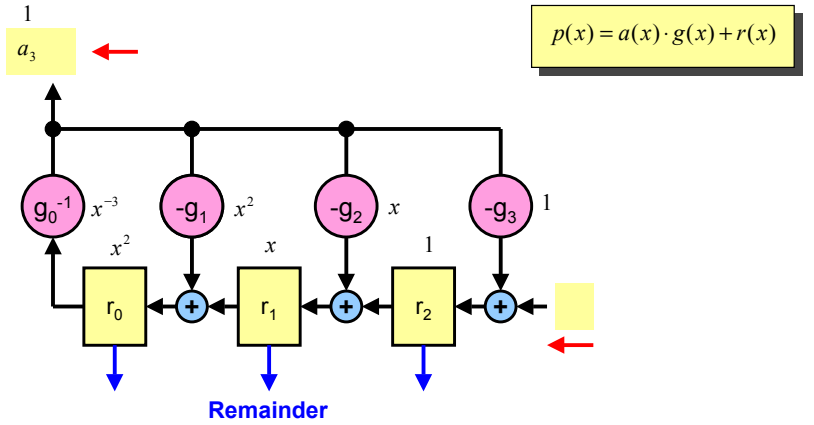
Dividing Polynomials
Using Shift Registers II

- Time t = 3 units



Dividing Polynomials
Using Shift Registers III

- Time t = 7 units



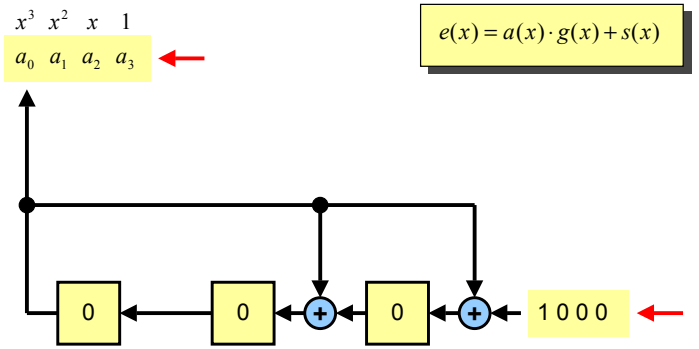
The (7,4) Binary Hamming Code
Syndrome of Single Bit Errors

Error Pattern **e**	Syndrome $\mathbf{s} = \mathbf{e}\,\mathbf{H}^T$
0 0 0 0 0 0 0	0 0 0
0 0 0 0 0 0 1	0 0 1
0 0 0 0 0 1 0	0 1 0
0 0 0 0 1 0 0	1 0 1
0 0 0 1 0 0 0	0 1 1
0 0 1 0 0 0 0	1 1 1
0 1 0 0 0 0 0	1 1 0
1 0 0 0 0 0 0	1 0 0

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

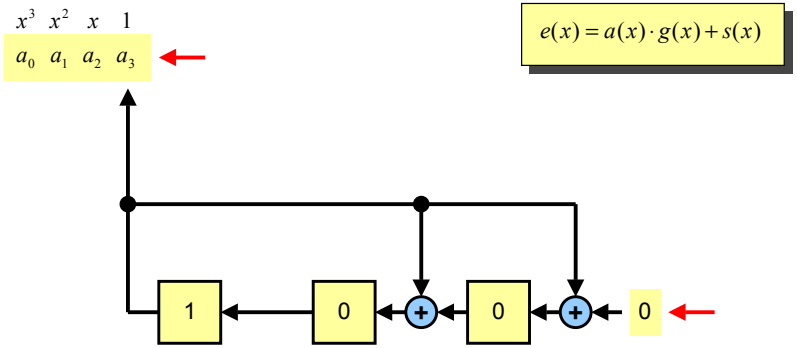
The (7,4) Binary Hamming Code
Syndrome Generator

- Time t = 3 units



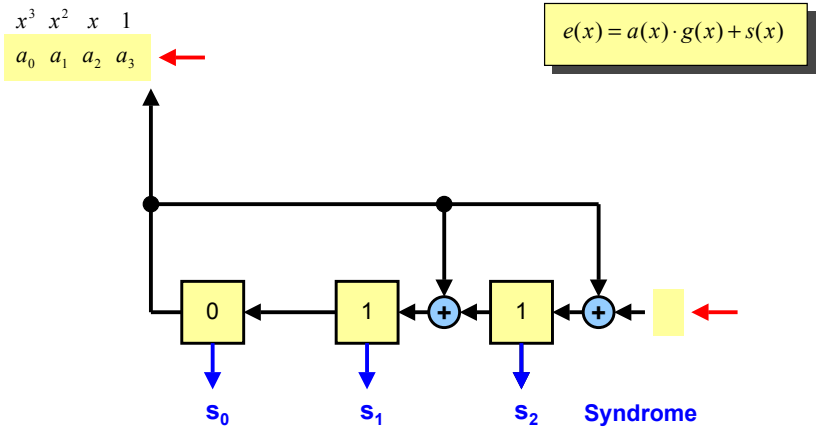
The (7,4) Binary Hamming Code
Syndrome Generator

- Time t = 6 units



The (7,4) Binary Hamming Code
Syndrome Generator

- Time t = 7 units



The (7,4) Binary Hamming Code
Systematic Encoding Matrix

$$G = \left[\begin{array}{cccc|ccc} 1&0&1&1&0&0&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{array}\right] \Rightarrow \left[\begin{array}{cccc|ccc} 1&0&0&1&1&1&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{array}\right] \Rightarrow G' = \left[\begin{array}{cccc|ccc} 1&0&0&0&1&0&1\\ 0&1&0&0&1&1&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{array}\right]$$

I_K P

N: K | R — data | redundancy → codeword

Systematic Encoder

c' = d·G'

$$H' = \left[\begin{array}{ccc|ccc} 1&1&1&0&1&0&0\\ 0&1&1&1&0&1&0\\ 1&1&0&1&0&0&1 \end{array}\right]$$

$-P^T$ I_R

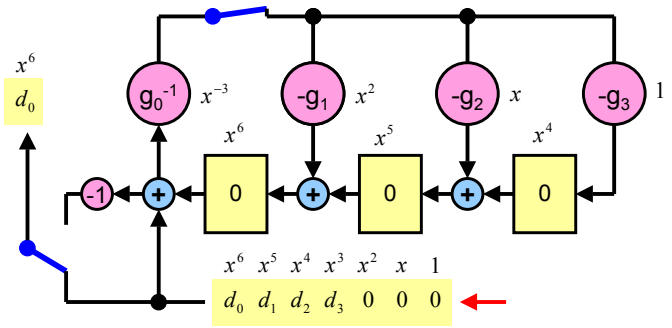
$$c'(x) = x^R d(x) - r(x) = a(x)g(x)$$
$$\Rightarrow \quad r(x) = x^R d(x) - a(x)g(x)$$
$$r(x) = R_{g(x)}\left[x^R d(x)\right]$$

degree of r(x) must be < R

Cyclic Codes
Systematic Encoder

- **Time t = 0 units**

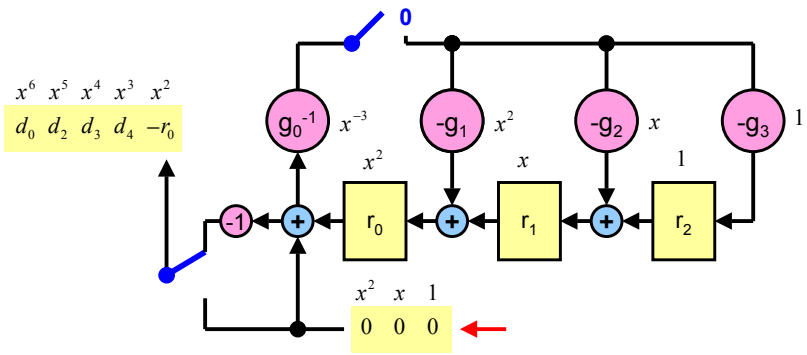
$$c'(x) = x^R d(x) - R_{g(x)}\left[x^R d(x)\right]$$



Cyclic Codes
Systematic Encoder

- **Time t = 4 units**

$$c'(x) = x^R d(x) - R_{g(x)}\left[x^R d(x)\right]$$

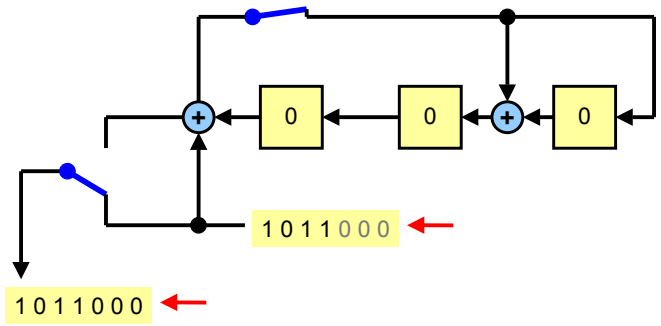


The (7,4) Binary Hamming Code
Table of Systematic Codewords

Data d	Codeword c' = d G'	Groups / Cyclic Shifts
0 0 0 0	0 0 0 0 0 0 0	1
0 0 0 1	0 0 0 1 0 1 1	2 +3
0 0 1 0	0 0 1 0 1 1 0	2 +2
0 0 1 1	0 0 1 1 1 0 1	3 +5
0 1 0 0	0 1 0 0 1 1 1	3
0 1 0 1	0 1 0 1 1 0 0	2 +1
0 1 1 0	0 1 1 0 0 0 1	2 +6
0 1 1 1	0 1 1 1 0 1 0	3 +4
1 0 0 0	1 0 0 0 1 0 1	2 +4
1 0 0 1	1 0 0 1 1 1 0	3 +6
1 0 1 0	1 0 1 0 0 1 1	3 +1
1 0 1 1	1 0 1 1 0 0 0	2
1 1 0 0	1 1 0 0 0 1 0	2 +5
1 1 0 1	1 1 0 1 0 0 1	3 +2
1 1 1 0	1 1 1 0 1 0 0	3 +3
1 1 1 1	1 1 1 1 1 1 1	4

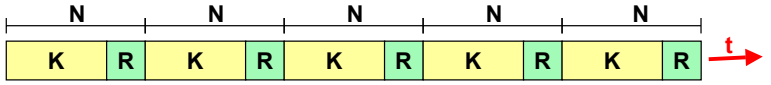
$$G' = \left[\begin{array}{cccc|ccc} 1&0&0&0&1&0&1\\ 0&1&0&0&1&1&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{array}\right]$$

The (7,4) Binary Hamming Code
Systematic Code Generator



Application Example
The Cyclic BCH Code of the ETCS Balise

- **Code Parameters:** N = 1023, K = 938, R = N - K = 85
- **Balise Transmitter:** Telepowering from the train antenna triggers the balise to transmit its telegram c(x) continuously.



- **Train Receiver:** Part of the transmitted telegram chain is received with an unknown bit offset B.

- **Synchronisation Problem:** Every cyclicly shifted codeword $v_B(x)$ is also a valid codeword. Thus telegram boundaries cannot be determined without auxiliary information.

Synchronisaton with Extended Cyclic Codes
Bose & Cauldwell (1967)

- **Code Generation:** R = 85 $$c(x) = x^R d(x) - R_{g(x)f(x)}\left[x^R d(x)\right] + g(x)$$
- **Generator polynomial:** $$g(x) = g_0 x^{75} + g_1 x^{74} + \cdots + g_{74} x + g_{75}$$
- **Synchronisation polynomial:** $$f(x) = f_0 x^{10} + f_1 x^9 + \cdots + f_9 x + f_{10}$$
- **Factors of x^N-1:** $$x^N - 1 = g(x) \cdot h(x) \qquad R_{f(x)}\left[h(x)\right] = 0$$
- **Cyclic shift of B = 0...1022 bits:** $$v_B(x) = R_{x^N-1}\left[x^B c(x)\right]$$
- **Parity check:** $$R_{g(x)}\left[v_B(x)\right] = R_{g(x)}\left[R_{x^N-1}\left[x^B c(x)\right]\right] = R_{g(x)}\left[x^B c(x)\right] = 0$$
- **Synchronisation Syndrome:** 2^{10}-1 = 1023 distinct values

$$s_B(x) = R_{f(x)}\left[v_B(x)\right] = R_{f(x)}\left[R_{x^N-1}\left[x^B c(x)\right]\right] = R_{f(x)}\left[x^B g(x)\right]$$

Cyclic Block Codes
Other Applications

- **Audio Compact Disc**
  - (32, 28) Reed-Solomon C1 code in GF(2^8), R = 4 byte symbols
  - (28, 24) Reed-Solomon C2 code in GF(2^8), R = 4 byte symbols
- **MPEG-2 Video Transmission**
  - (204, 188) Reed-Solomon code in GF(2^8), R = 16 byte symbols
- **Voyager II and Galileo Deep Space Probes**
  - (255,239) Reed-Solomon code in GF(2^8), R = 16 byte symbols
- **Combination with Convolutional Codes**
  - Especially in wireless applications cyclic block codes are often combined with an outer convolutional code