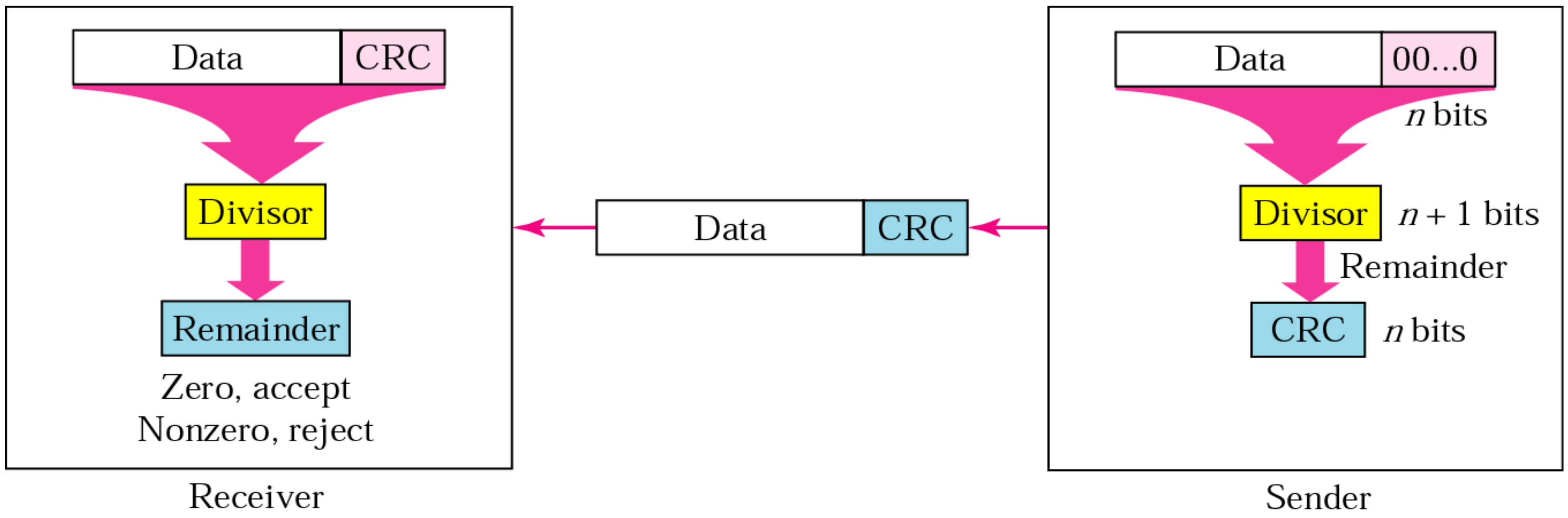
Part 2.2 Cyclic redundancy check (CRC) codes

Overview of Cyclic Redundancy Check Codes

- **Cyclic redundancy check (CRC) codes**
  - Invented by *W. Wesley Peterson*, and published in 1961
  - A type of linear block codes
    - Generally, not cyclic, but derived from cyclic codes
  - A systematic ***error detecting code***
    - *a group of error control bits (which is the remainder of a polynomial division of a message polynomial by a generator polynomial) is appended to the end of the message block*
    - with considerable *burst-error detection* capability
  - The receiver generally has the ability to send retransmission requests back to the data source through a feedback channel.

CRC Generator and Checker



Cyclic Redundancy Check Codes (1)

- **Binary (N, k) CRC codes**
  - k message or data bits are encoded into N code bits by appending to the message bits a sequence of $\boxed{n=N-k}$ bits.
  - ***Polynomial representation***
    - ✓ ***Message bits:*** $\mathbf{m}=\begin{bmatrix} m_{k-1} & m_{k-2} & \dots & m_1 & m_0 \end{bmatrix}$

$$\boxed{\mathbf{m}(X)=m_{k-1}X^{k-1}+m_{k-2}X^{k-2}+\dots+m_1X+m_0 \qquad \text{degree } (k-1)}$$

    - ✓ ***Appended bits:*** $\mathbf{R}=\begin{bmatrix} r_{n-1} & r_{n-2} & \dots & r_1 & r_0 \end{bmatrix}$

$$\boxed{\mathbf{R}(X)=r_{n-1}X^{n-1}+r_{n-2}X^{n-2}+\dots+r_1X+r_0 \qquad \text{degree } (n-1)}$$

    - ✓ ***CRC code bits:***

$$\mathbf{C}=\begin{bmatrix} c_{N-1} & c_{N-2} & \dots & c_1 & c_0 \end{bmatrix}=\begin{bmatrix} m_{k-1} & m_{k-2} & \dots & m_1 & m_0 & r_{n-1} & r_{n-2} & \dots & r_1 & r_0 \end{bmatrix}$$

$$\boxed{\begin{aligned}\mathbf{C}(X)&=c_{N-1}X^{N-1}+c_{N-2}X^{N-2}+\dots+c_1X+c_0 \qquad \text{degree } (N-1)\\ &=X^n\mathbf{m}(X)+\mathbf{R}(X)\end{aligned}}$$

Cyclic Redundancy Check Codes (2)

➢ **Example: (*k=10, N=13, n=N-k=3*) CRC code**

$$\mathbf{m} = [1010100101]$$

$$\mathbf{m}(X) = X^9 + X^7 + X^5 + X^2 + 1$$

$$\mathbf{R} = [111]$$

$$\mathbf{R}(X) = X^2 + X + 1$$

$$\mathbf{C} = [1010100101{\color{red}111}]$$

$$\mathbf{C}(X) = \mathrm{X}^n \mathbf{m}(X) + \mathbf{R}(X)$$

$$= X^3(X^9 + X^7 + X^5 + X^2 + 1) + X^2 + X + 1$$

$$= X^{12} + X^{10} + X^8 + X^5 + X^3 + X^2 + X + 1$$

$X^n m(X)$ is the polynomial corresponding to the message bit sequence to which a number n of 0's is appended. [1010100101000]

Cyclic Redundancy Check Codes (3)

➢ How to obtain the polynomial R(X) (the appended bits)

– CRC codes are designated by a *generator polynomial* g(X) with degree of *n*

$$\mathbf{g} = \begin{bmatrix} g_n & g_{n-1} & \cdots & g_1 & g_0 \end{bmatrix}$$

$$\boxed{\mathbf{g}(X) = g_n X^n + g_{n-1} X^{n-1} + \ldots + g_1 X + g_0 \qquad \text{degree (n)}}$$

– Divide $X^n m(X)$ by g(X) (modulo-2 division) and obtain the remainder, which is R(X)

$$X^n m(X) = p(X)g(X) + R(X)$$

- *The remainder R(X) is always a polynomial of maximum order (n-1).*

Cyclic Redundancy Check Codes (4)

➢ Example: the polynomial R(X) (the appended bits)

Message $[11100110]$ 8 bits

$\mathbf{m}(X) = X^7 + X^6 + X^5 + X^2 + X$

Given N-k=n=4, generator polynomial $\mathbf{g}(X) = X^4 + X^3 + 1 \rightarrow [11001]$

$$\frac{X^n \mathbf{m}(X)}{\mathbf{g}(X)} = \frac{X^{11} + X^{10} + X^9 + X^6 + X^5}{X^4 + X^3 + 1}$$

$$= X^7 + X^5 + X^4 + X^2 + X + \frac{X^2 + X}{X^4 + X^3 + 1}$$

$X^n m(X)$ is the polynomial corresponding to the message bit sequence to which a number n of 0's is appended. [111001100000]

The remainder **R**(X)=$X^2 + X$,

therefore the appended bits are $[0110]$ (since n=4).

The CRC code bits are $[111001100110]$

Error Detection (1)

- **The polynomial for the received code word T(X) is divided by the generator polynomial g(X)**
  - ✓ ***Upon the reception without error***
    - – $T(X)=C(X)=X^n m(X)+R(X)$
    - – The remainder of $T(X)/g(X)$ $=R(X)+R(X)=$ $\boxed{\textit{the all-zero row}}$ (modulo-2 addition).
    - – Example:

$$\mathbf{g}(X)=X^4+X^3+1$$

The transmitted CRC code bits are $[111001100110]$

$$\mathbf{T(X)}=\mathbf{C}(X)=X^{11}+X^{10}+X^9+X^6+X^5+X^2+X$$

$$=(X^7+X^5+X^4+X^2+X)\mathbf{g}(X)$$

The remainder of $[\mathbf{C}(X)/\mathbf{g}(X)]=\mathbf{0}\longrightarrow[0000]$

Error Detection (2)

➢ **The polynomial for the received code word T(X) is divided by the generator polynomial g(X)**

✓ ***The remainder is not zero***

– An indication that an error has occurred in transmission and the received codeword is not a valid code word.

– Example:

$$\mathbf{g}(X) = X^4 + X^3 + 1$$

The transmitted CRC code bits are $[111001100110]$

The received CRC code bits are $[11\underline{0}0\underline{1}1100110]$

$$\mathbf{T}(X) = X^{11} + X^{10} + X^7 + X^6 + X^5 + X^2 + X = \mathbf{C}(X) + X^9 + X^7$$

$$\frac{\mathbf{T}(X)}{\mathbf{g}(X)} = \frac{\mathbf{C}(X) + X^9 + X^7}{X^4 + X^3 + 1} = (X^7 + X^2) + \frac{X}{X^4 + X^3 + 1}$$

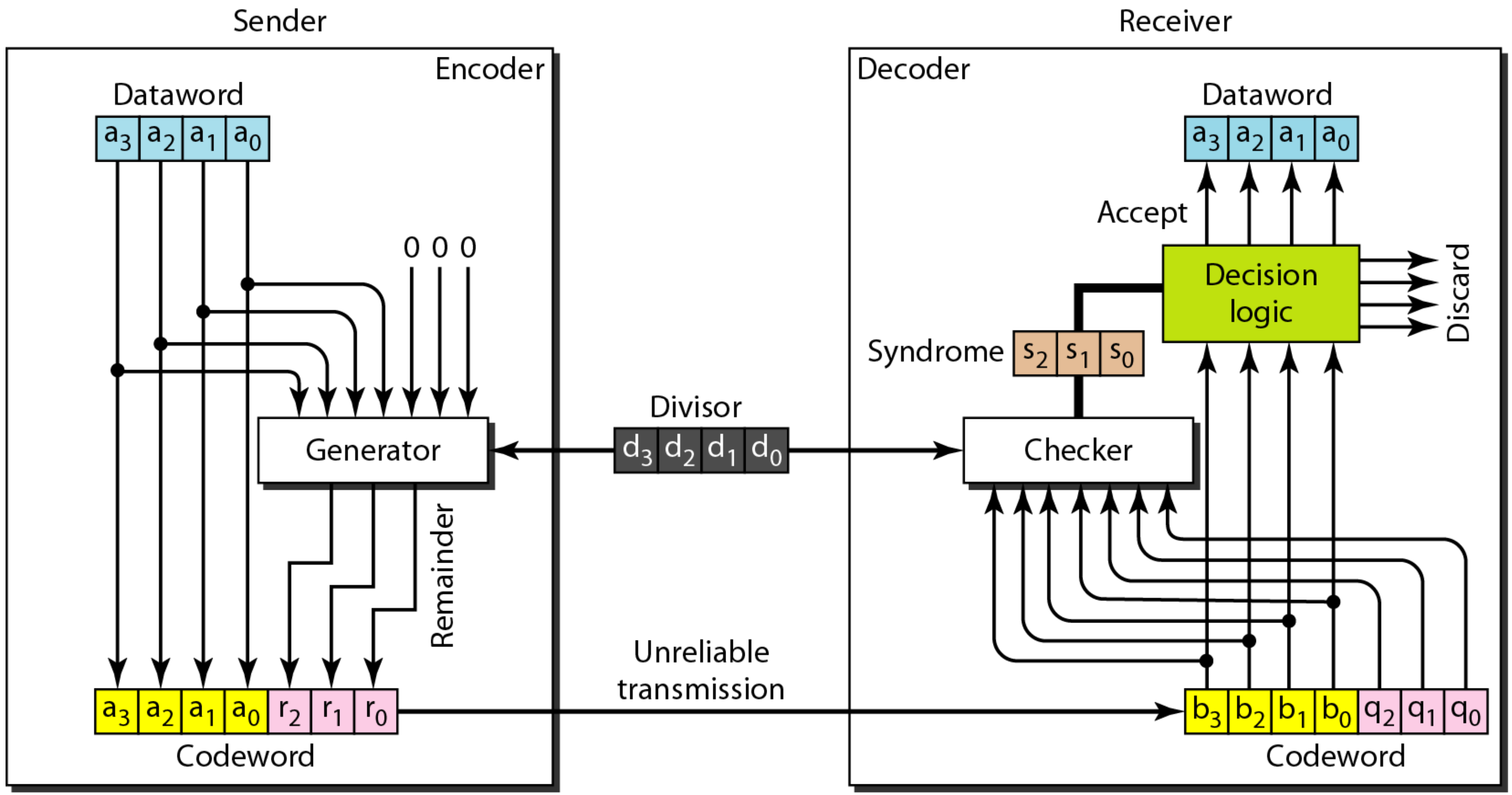
The remainder of $[\mathbf{T}(X)/\mathbf{g}(X)] = X \longrightarrow [0010]$

Example of CRC (7, 4) in Vector Form (1)

$$\text{Generator polynomial } \mathbf{g}(X) = X^3 + X + 1 \rightarrow [1011]$$

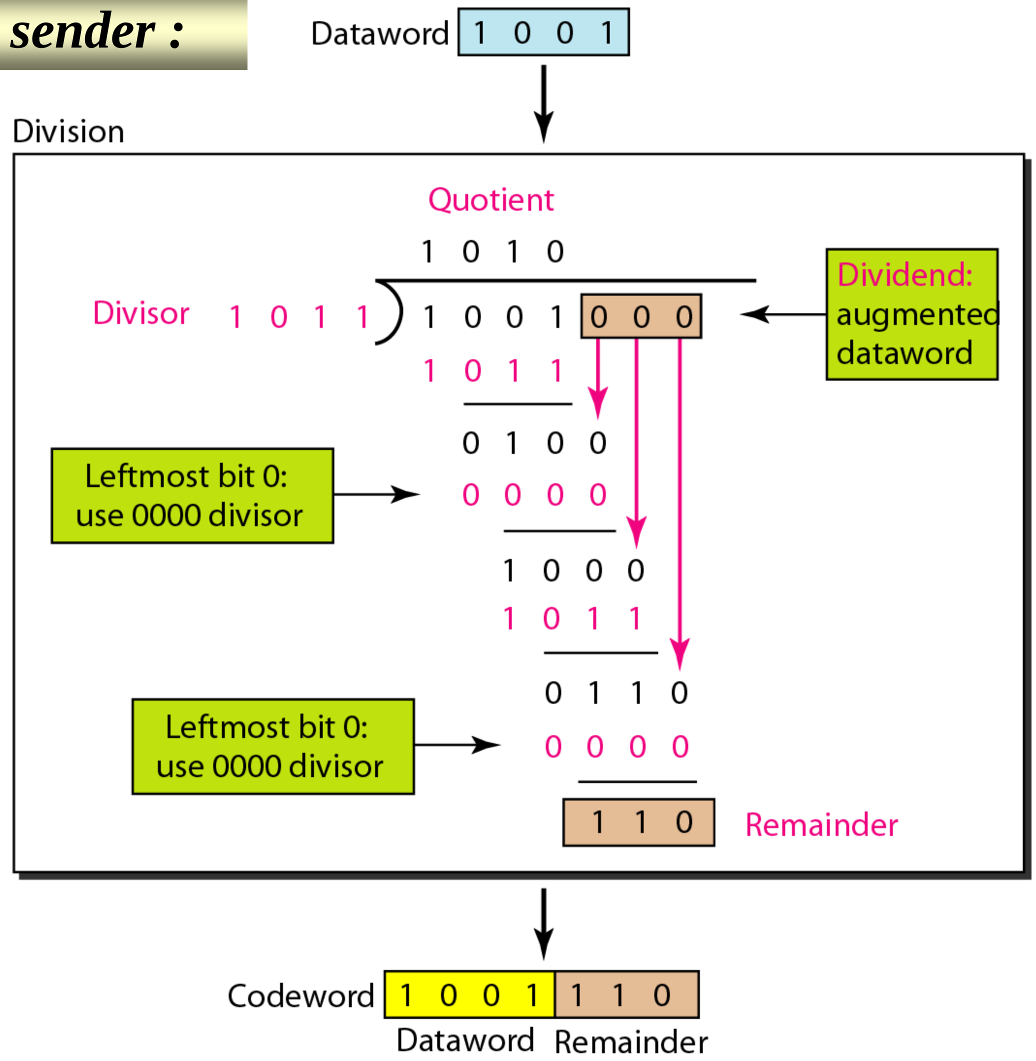
Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

Example of CRC (7, 4) in Vector Form (2)



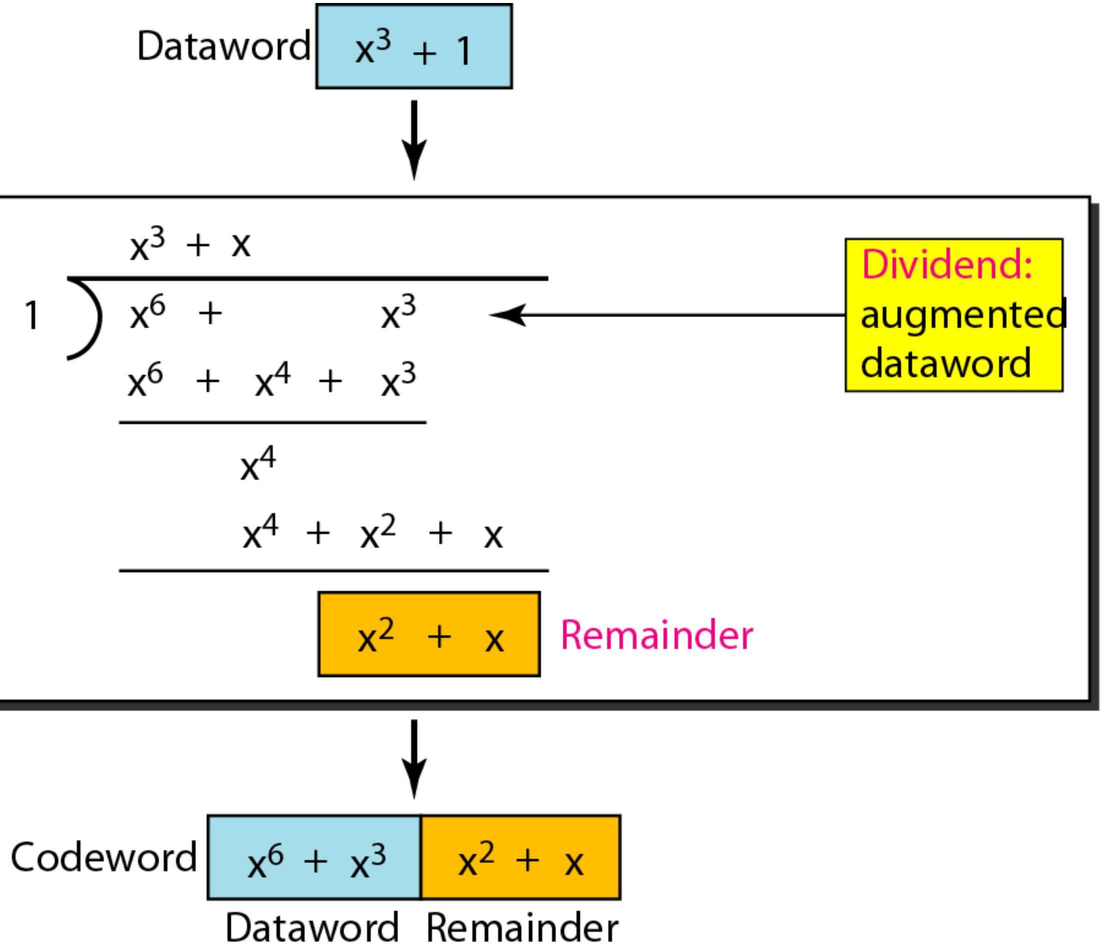
Example of CRC (7, 4) in Vector Form (3)

Division in the sender :



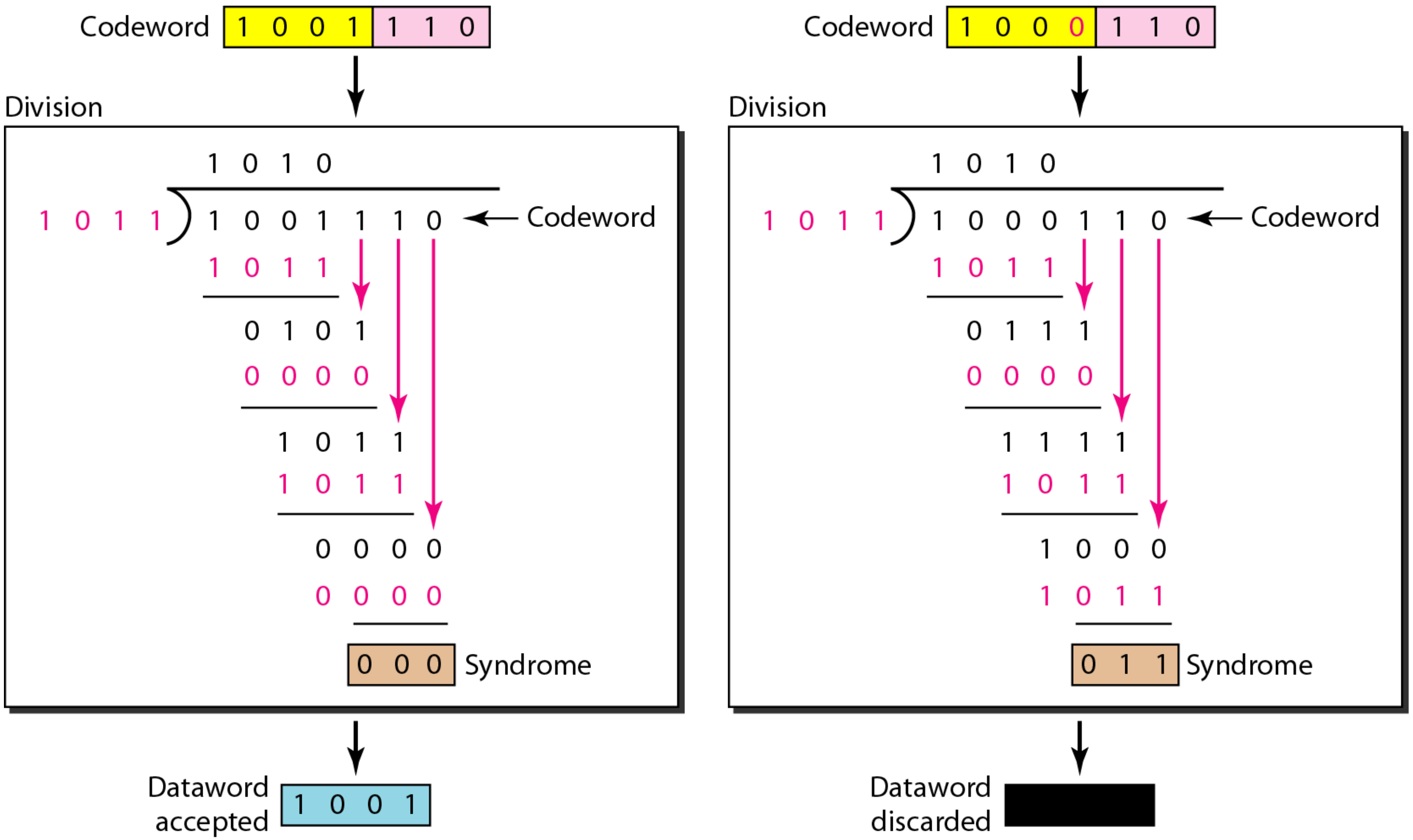
Example of CRC (7, 4) in Vector Form (4)

Division in the sender (Polynomial form):



Example of CRC (7, 4) in Vector Form (5)

Division in the receiver (two cases) :

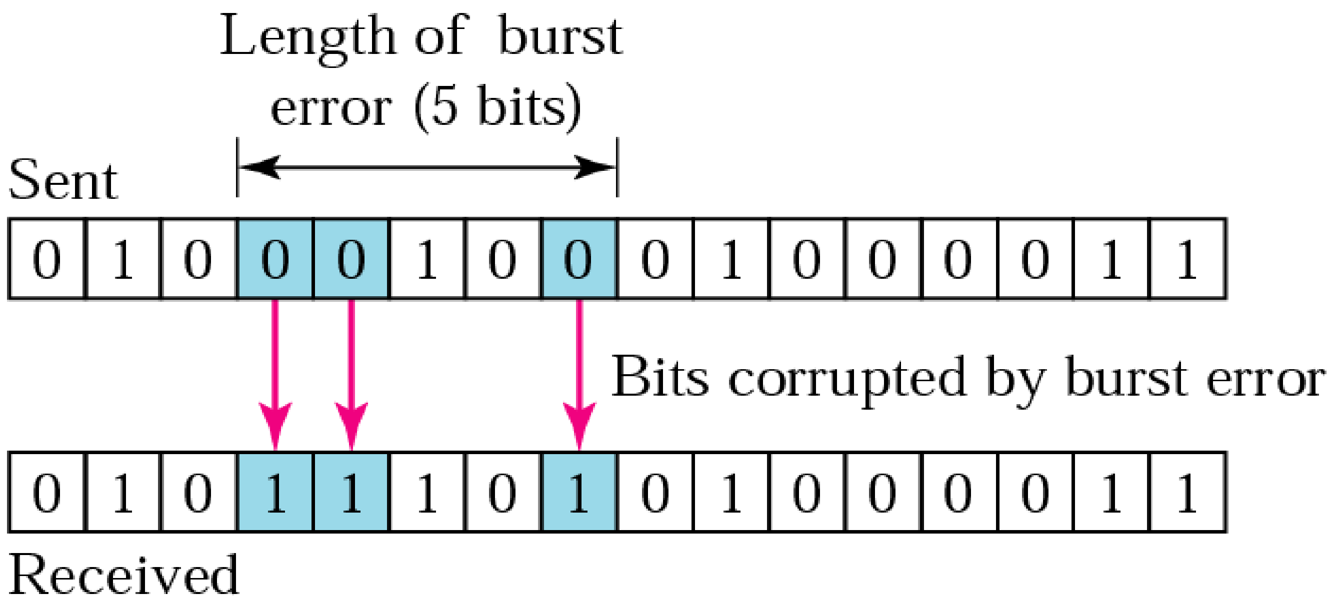


Error Detection Capability

- **Binary (N, k) CRC codes (with N-k appended bits) can detect the following error patterns:**
  1. All error bursts of length N-k or less
  2. A fraction of error bursts of length equal to N-k+1; the fraction equals $(1-2^{-(N-k-1)})$
  3. A fraction of error bursts of length greater than N-k+1; the fraction equals $(1-2^{-(N-k)})$
  4. All combinations of d_{min}- 1 or fewer errors, where d_{min} is the minimum distance
  5. All error patterns with an odd number of errors if the generator polynomial g(X) has an even number of nonzero coefficients

Example of Error Burst

An error burst of length B in an N-bit received word is defined as a contiguous sequence of B bits in which the first and last bits or any number of intermediate bits are received in error.



Example of Error Detection Capability

The CRC-12 code with generator polynomial as

$$\mathbf{X^{12} + X^{11} + X^3 + X^2 + X + 1}$$

which has 12 appended bits:

✓detects all burst errors affecting an odd number of bits

✓detects all burst errors with a length less than or equal to 12

✓detects, 99.95 percent of the time, burst errors with a length of 13

✓detects, 99.97 percent of the time, burst errors with a length more than 13.

Common CRC Codes

Code	Generator Polynomial g(X)	Appended Bits	Applications
CRC-4	$X^4 + X + 1$	4	ITU G.704
CRC-8	$X^8 + X^2 + X + 1$	8	ATM header
CRC-10	$X^{10} + X^9 + X^5 + X^4 + X + 1$	10	ATM AAL
CRC-16-CCITT	$X^{16} + X^{12} + X^5 + 1$	16	Bluetooth
CRC-32	$X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$	32	LANs