Error Control

Computer Networks(CS31204)

Prof. Sudip Misra

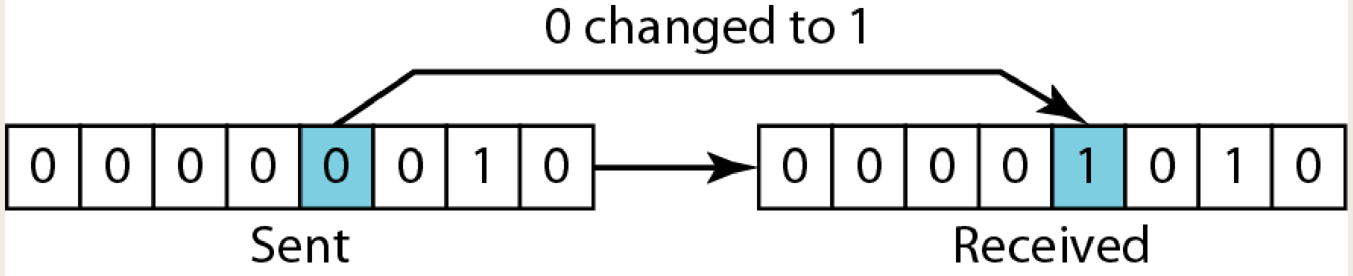
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/
Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Errors

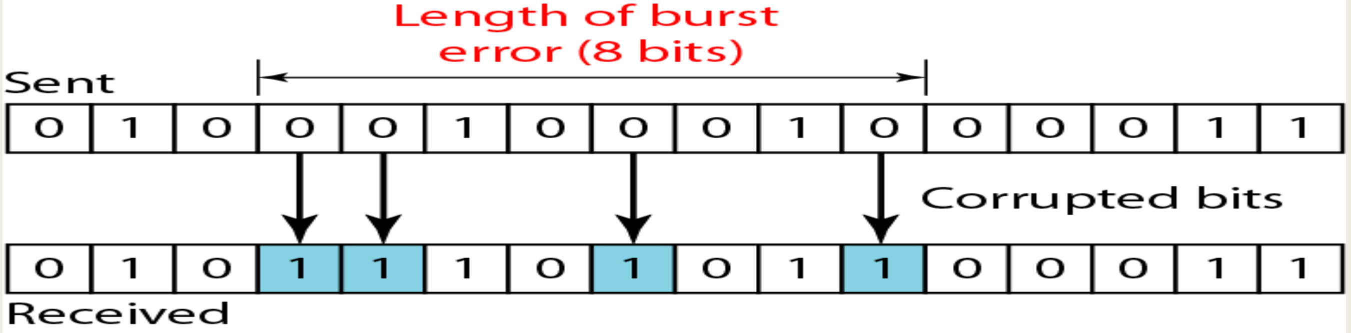
Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. These changes are errors.

Types:

- Single-Bit Error: The term *single-bit error* means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.



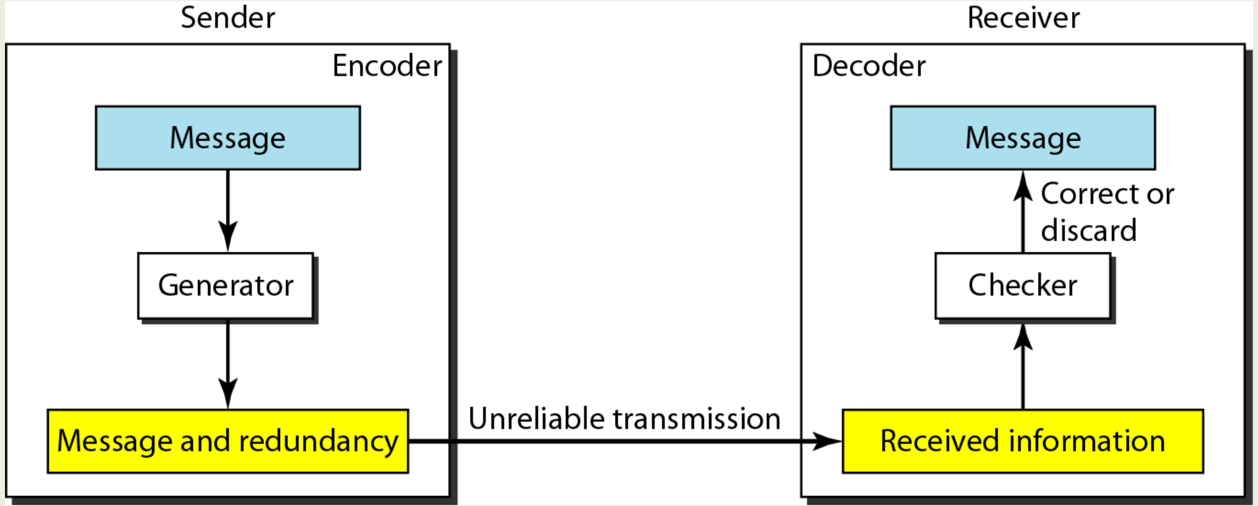
- Burst Error: The term *burst error* means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Redundancy

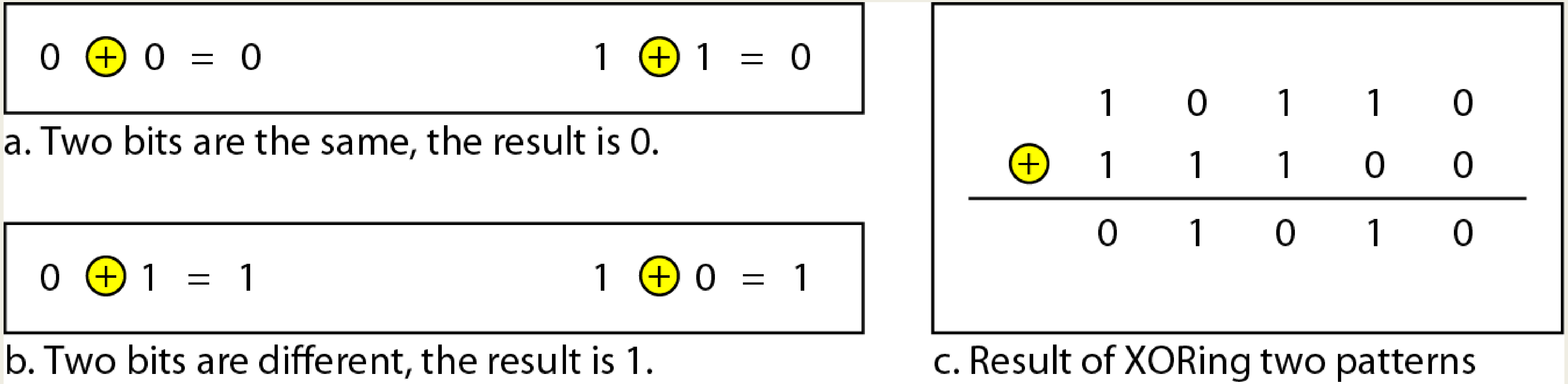
- To detect or correct errors, we need to send extra (redundant) bits with data.
- Redundancy is achieved through various coding schemes.
- The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits.
- The receiver checks the relationships between the two sets of bits to detect or correct the errors.
- The ratio of redundant bits to the data bits and the robustness of the process are important factors in any coding scheme.



Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Modulo Arithmetic

- In modulo-N arithmetic, we use only the integers in the range 0 to N −1, inclusive.
- In this arithmetic we use the XOR (exclusive OR) operation for both addition and subtraction.
- The result of an XOR operation is 0 if two bits are the same; the result is I if two bits are different.



$0 \oplus 0 = 0$ $\quad$ $1 \oplus 1 = 0$

a. Two bits are the same, the result is 0.

$0 \oplus 1 = 1$ $\quad$ $1 \oplus 0 = 1$

b. Two bits are different, the result is 1.

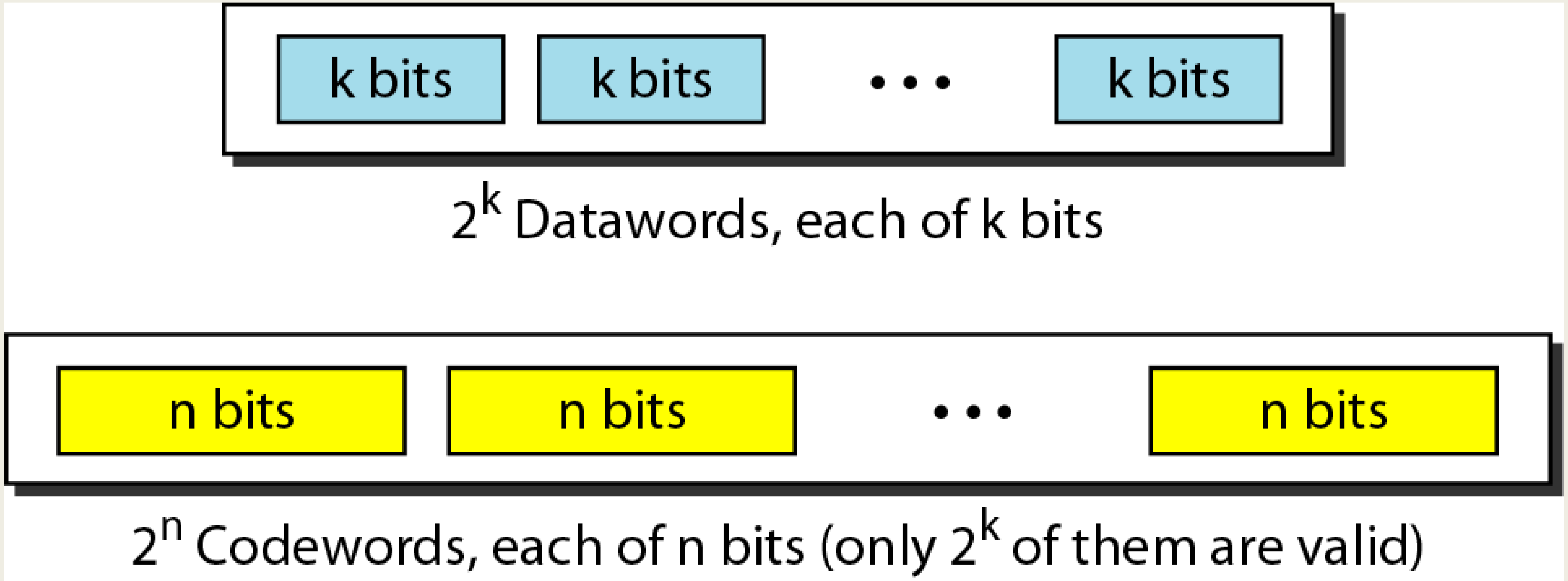
$$\begin{array}{rccccc} & 1 & 0 & 1 & 1 & 0 \\ \oplus & 1 & 1 & 1 & 0 & 0 \\ \hline & 0 & 1 & 0 & 1 & 0 \end{array}$$

c. Result of XORing two patterns

Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.

Block Coding

- In block coding, we divide our message into blocks, each of k bits, called datawords.
- We add r redundant bits to each block to make the length n = k + r.
- The resulting n-bit blocks are called codewords.



k bits k bits • • • k bits

2^k Datawords, each of k bits

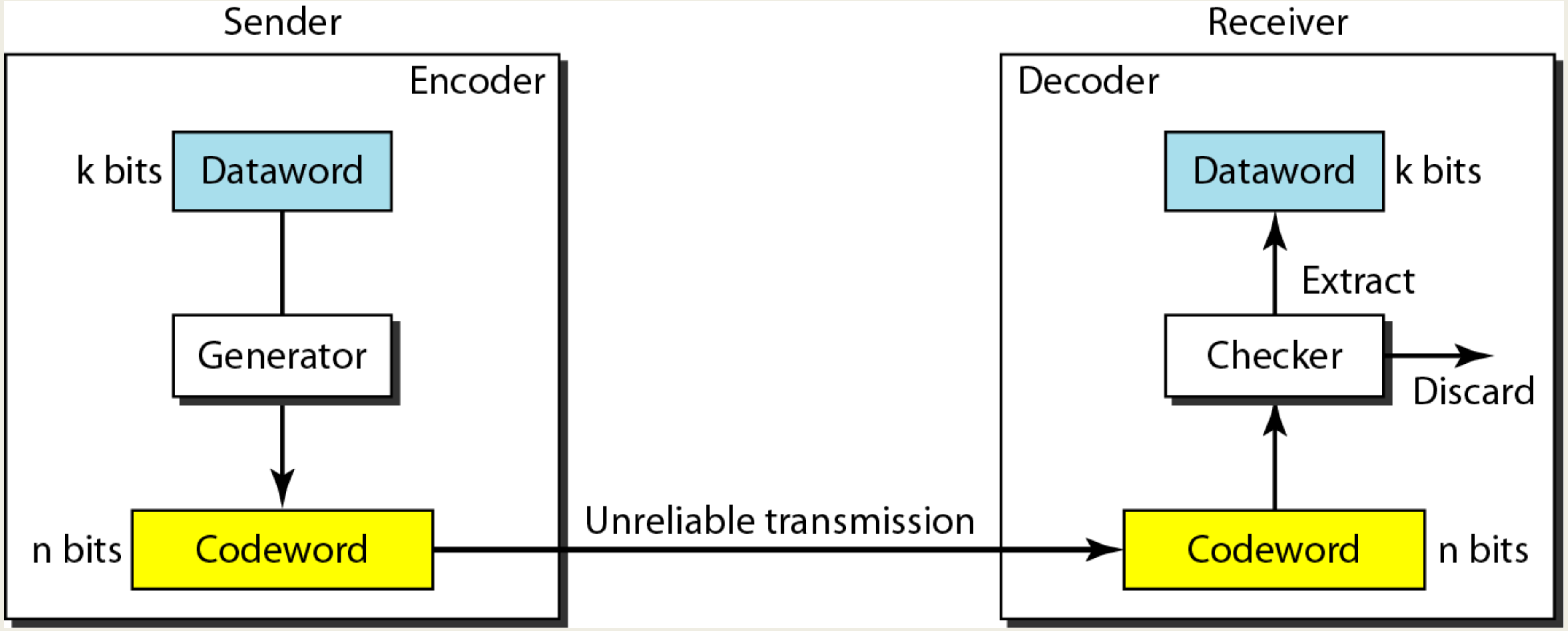
n bits n bits • • • n bits

2^n Codewords, each of n bits (only 2^k of them are valid)

Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.

Error Detection

- Enough redundancy is added to detect an error.
- The receiver knows an error occurred but does not know which bit(s) is(are) in error.
- Has less overhead than error correction.



Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.

Error Detection Methods

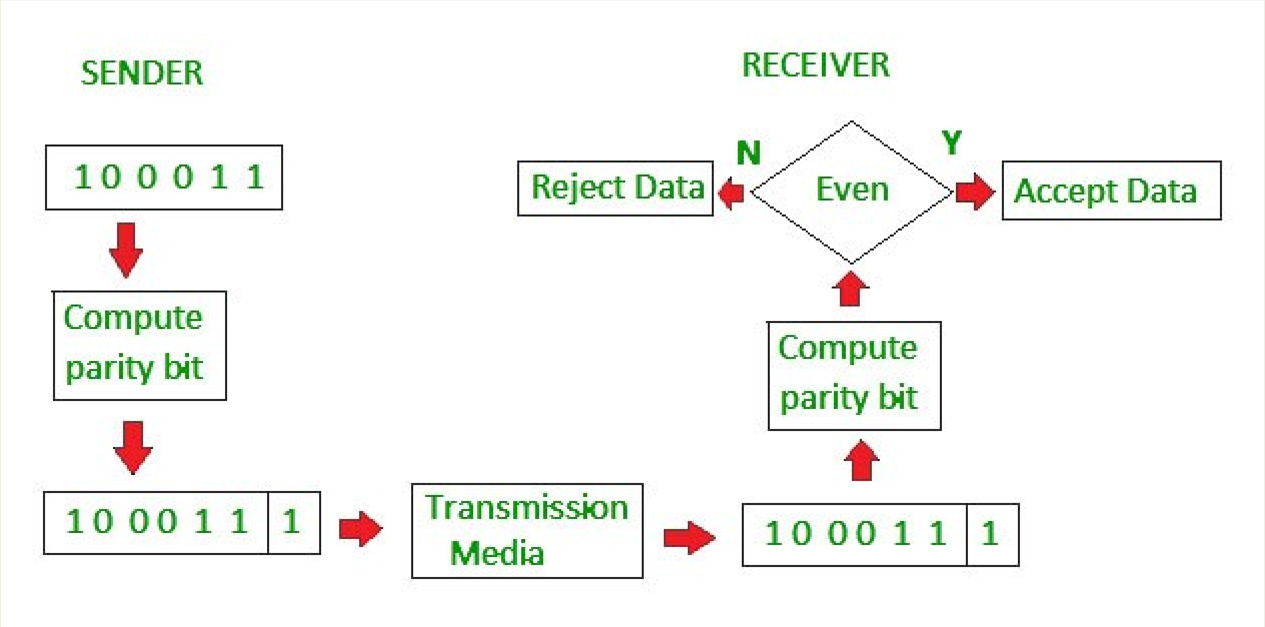
- Parity Check
- Cyclic Redundancy Check
- Checksum

Parity check

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.

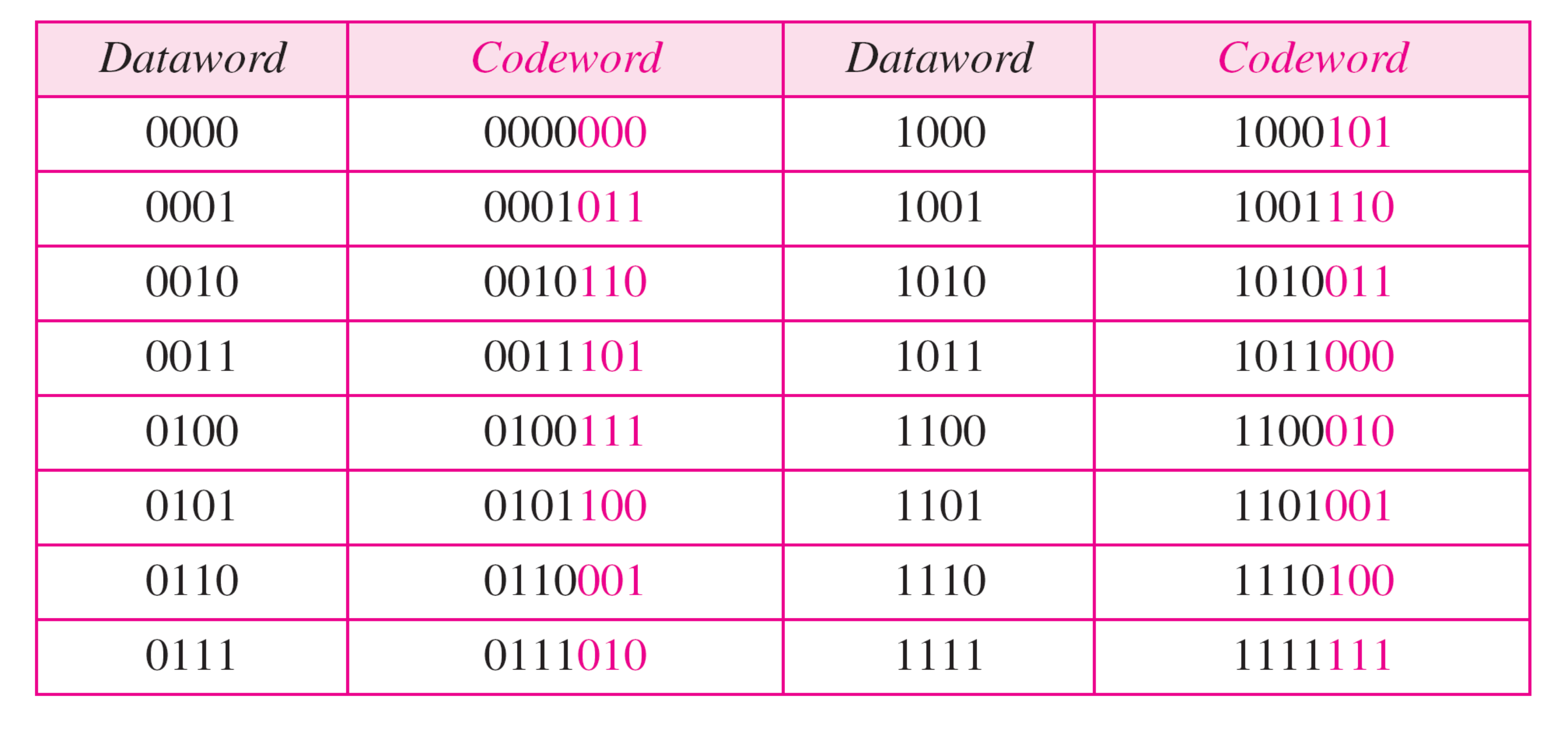


Source: [Online], Link: https://www.geeksforgeeks.org/error-detection-in-computer-networks/

Cyclic Code

Cyclic codes are special linear block codes with one extra property.
In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.

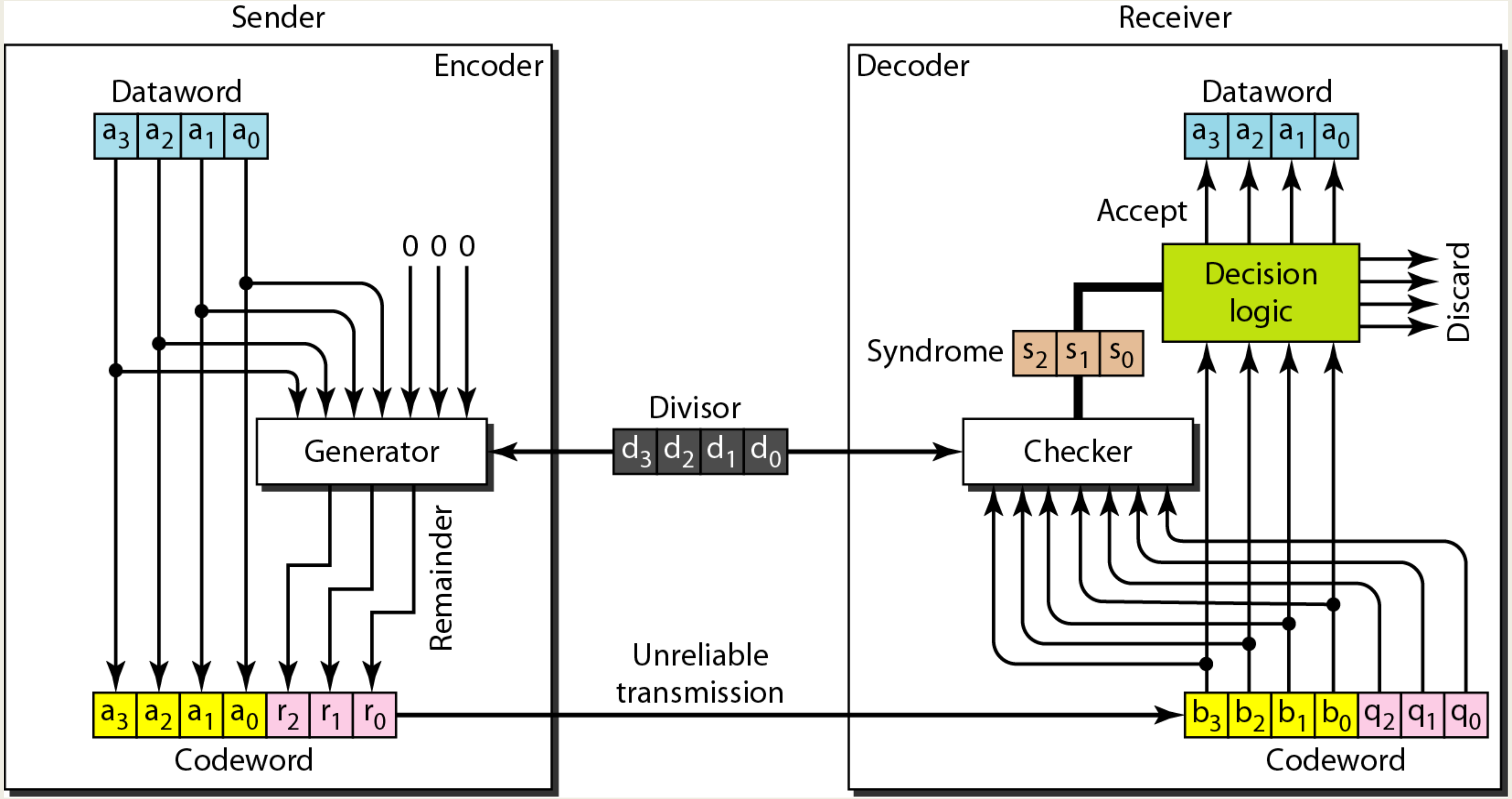
A CRC code with C(7, 4)



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

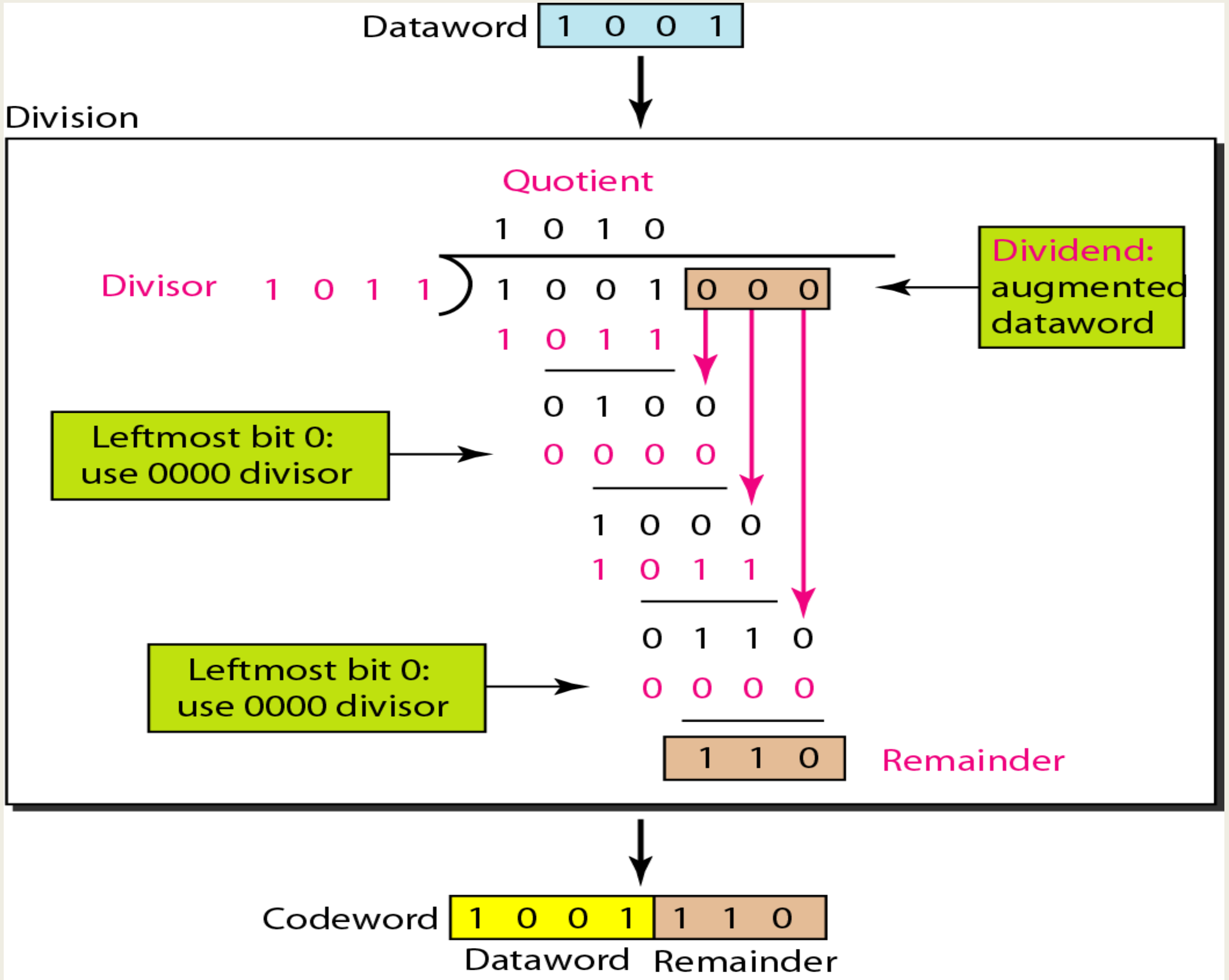
Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.

CRC Encoder and Decoder



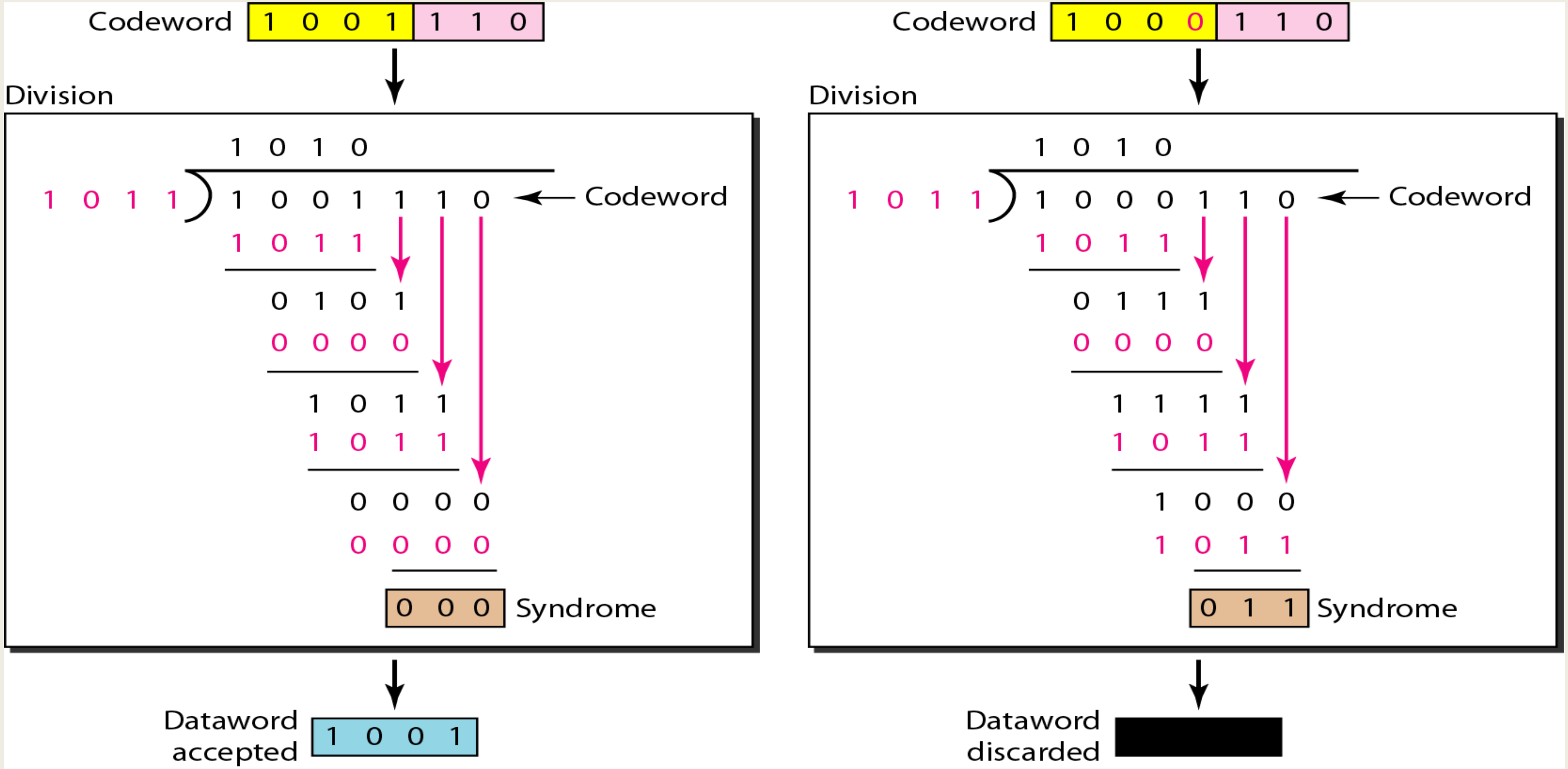
Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.

Division in CRC Encoder



Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

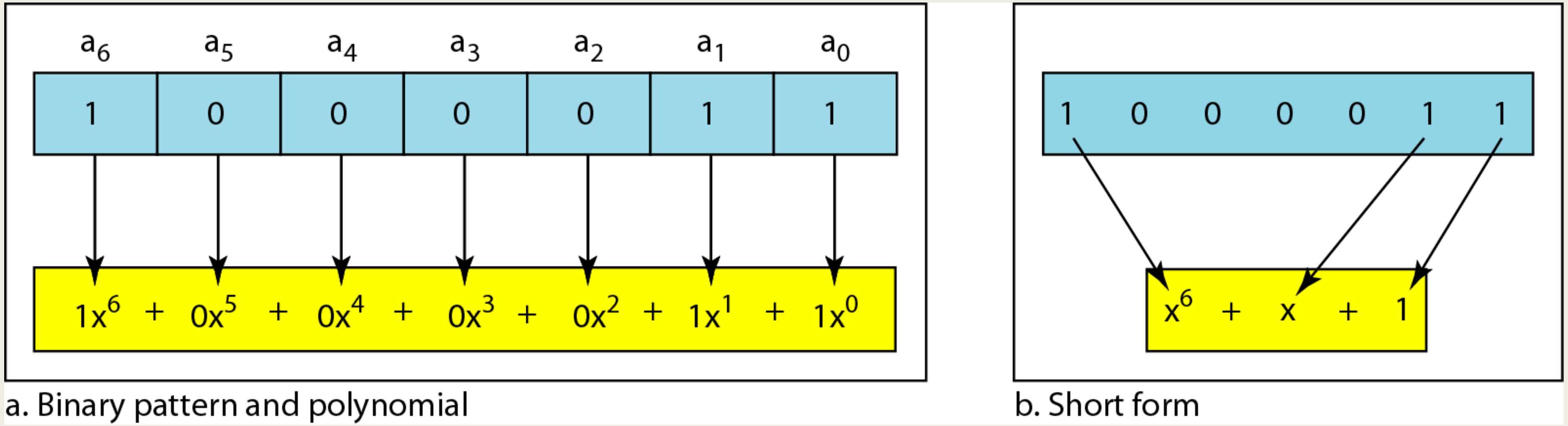
Division in CRC Decoder in Two Cases



Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Polynomials

- We can use a polynomial to represent a binary word.
- Each bit from right to left is mapped onto a power term.
- The rightmost bit represents the "0" power term. The bit next to it the "1" power term, etc.
- If the bit is of value zero, the power term is deleted from the expression.



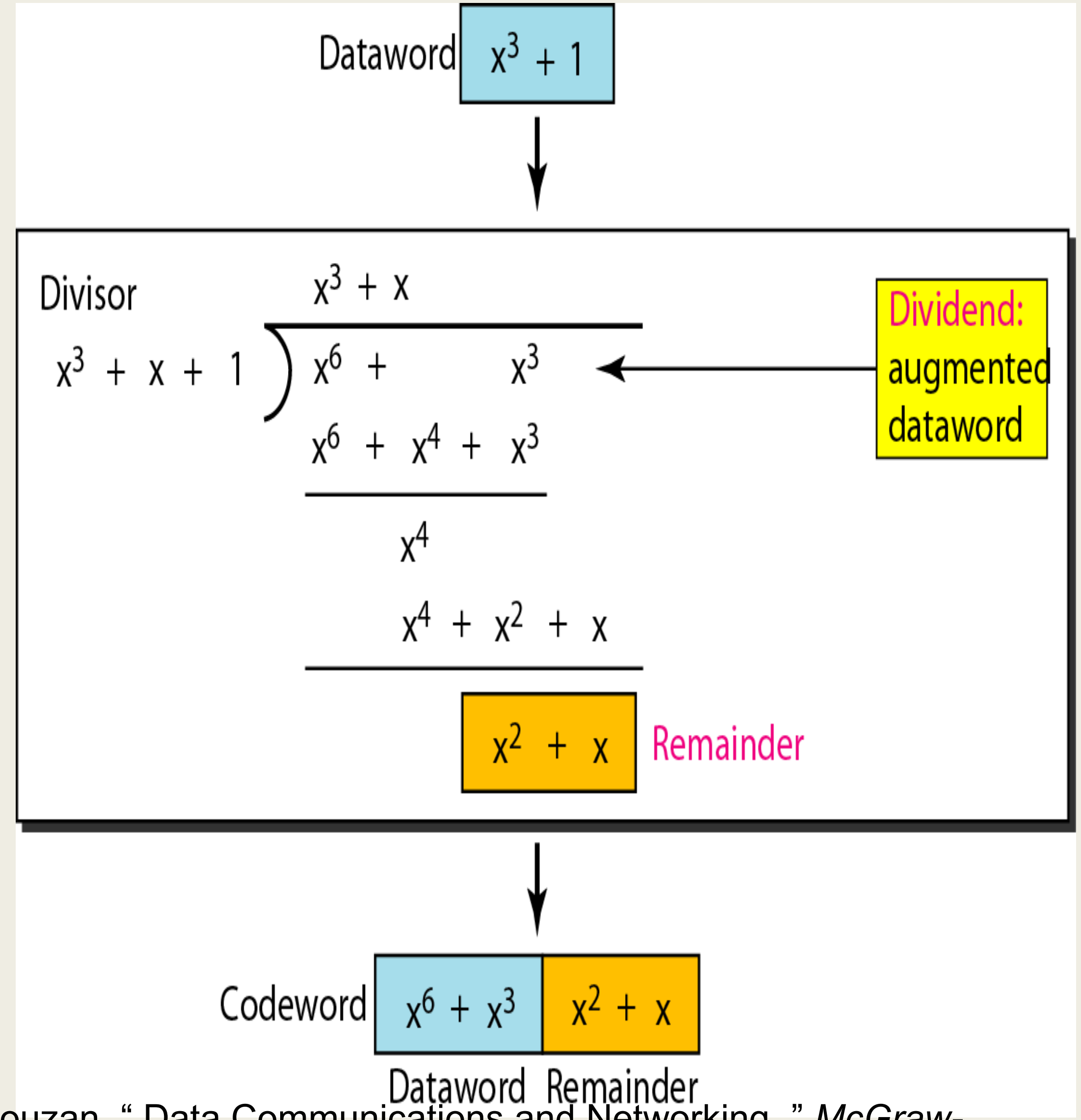
a_6 a_5 a_4 a_3 a_2 a_1 a_0
1 0 0 0 0 1 1
$1x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$
a. Binary pattern and polynomial
1 0 0 0 0 1 1
$x^6 + x + 1$
b. Short form

Fig.: A polynomial to represent a binary word

Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

CRC Division Using Polynomial

- The divisor in a cyclic code is normally called the generator polynomial or simply the generator.
- In a cyclic code, If $s(x) \neq 0$, one or more bits is corrupted.
- If $s(x) = 0$, either: No bit is corrupted. Or some bits are corrupted, but the decoder failed to detect them.
- If the generator has more than one term and the coefficient of x^0 is 1, all single errors can be caught.



Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Cont...

- If a generator cannot divide $x^t + 1$ (t between 0 and n – 1), then all isolated double errors can be detected.
- A generator that contains a factor of $x + 1$ can detect all odd-numbered errors.
- All burst errors with $L \le r$ will be detected.
- All burst errors with $L = r + 1$ will be detected with probability $1 – (1/2)^{r–1}$.
- All burst errors with $L > r + 1$ will be detected with probability $1 – (1/2)^r$.

A good polynomial generator needs to have the following characteristics:

- It should have at least two terms.
- The coefficient of the term x^0 should be 1.
- It should not divide $x^t + 1$, for t between 2 and $n - 1$.
- It should have the factor $x + 1$.

Checksum

The checksum is used in the Internet by several protocols although not at the data link layer.

Sender site:

- The message is divided into m-bit words if m bit checksum is used.
- The value of the checksum word is set to 0.
- All words including the checksum are added using one’s complement addition.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

Receiver site:

- The message (including checksum) is divided into m-bit words.
- All words are added using one’s complement addition.
- The sum is complemented and becomes the new checksum.
- If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

Checksum: Example

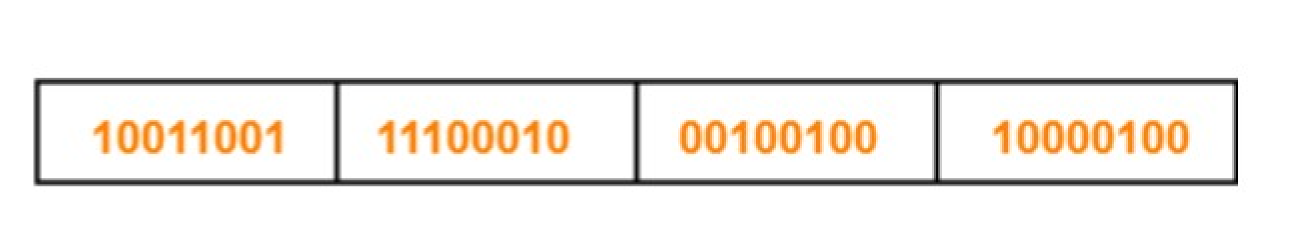
Consider the data unit to be transmitted is-

1001100111100010001001000010000100

Consider 8 bit checksum is used.

At sender's side:

The data is divided as:



10011001	11100010	00100100	10000100

Now, all the segments are added and the result is obtained as-

- 10011001 + 11100010 + 00100100 + 10000100 = 1000100011
- Since the result consists of 10 bits, so extra 2 bits are wrapped around.
- 00100011 + 10 = 00100101 (8 bits)
- Now, 1's complement is taken which is 11011010.
- Thus, checksum value = 11011010

Source: [Online], Available: https://www.gatevidyalay.com/checksum-checksum-example-error-detection

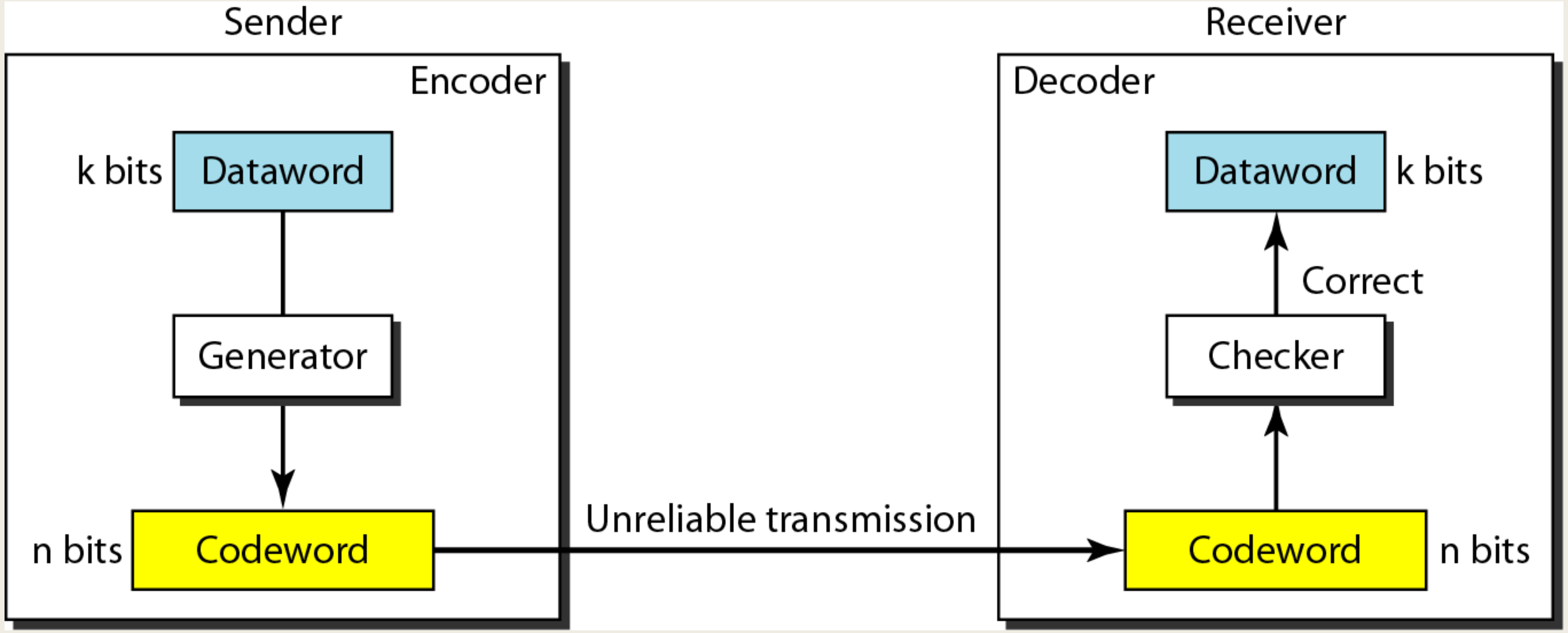
Cont…

At receiver side,

- The received data unit is divided into segments of 8 bits.
- All the segments along with the checksum value are added.
- Sum of all segments + Checksum value = 00100101 + 11011010 = 11111111
- Complemented value = 00000000
- Since the result is 0, receiver assumes no error occurred in the data and therefore accepts it.

Error Correction

- Error correction is much more difficult than error detection.
- In error correction the receiver needs to find (or guess) the original codeword sent.
- Need more redundant bits for error correction than for error detection.
- Hamming codes can be used for error correction.



Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.

Thank You!!!

Appendix

Hamming Distance

- The Hamming distance between two words is the number of differences between corresponding bits.
- The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words.
- To guarantee the detection of up to s errors in all cases, the minimum hamming distance in a block code must be $d_{min} = s + 1$.

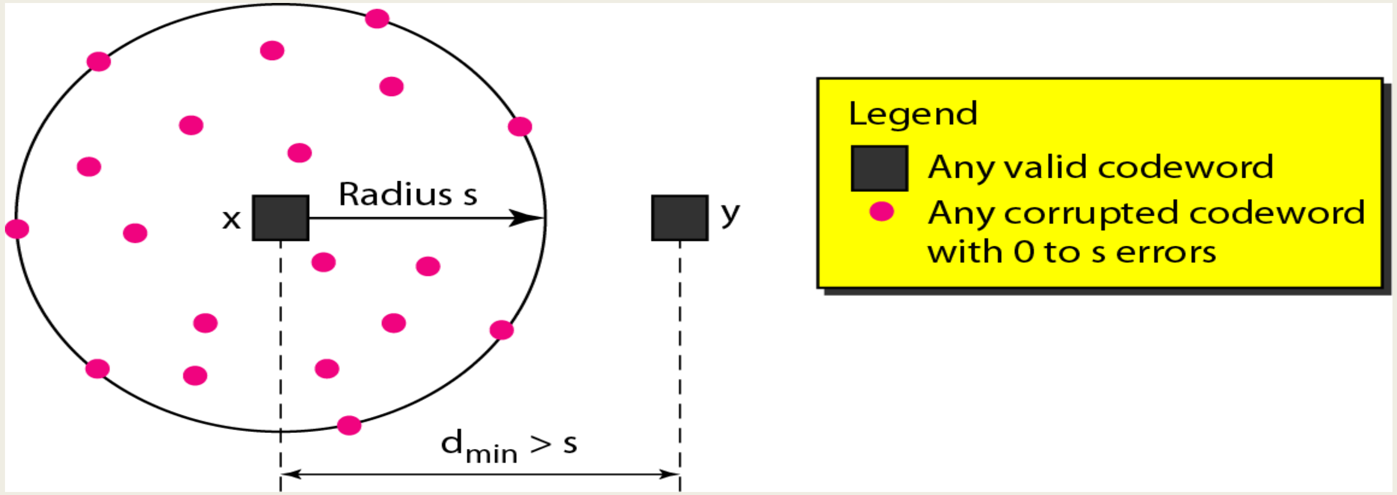


Fig. : Geometric concept for finding d_{min} in error detection

Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Cont...

To guarantee correction of up to *t* errors in all cases, the minimum hamming distance in a block code must be $d_{min} = 2t + 1$.

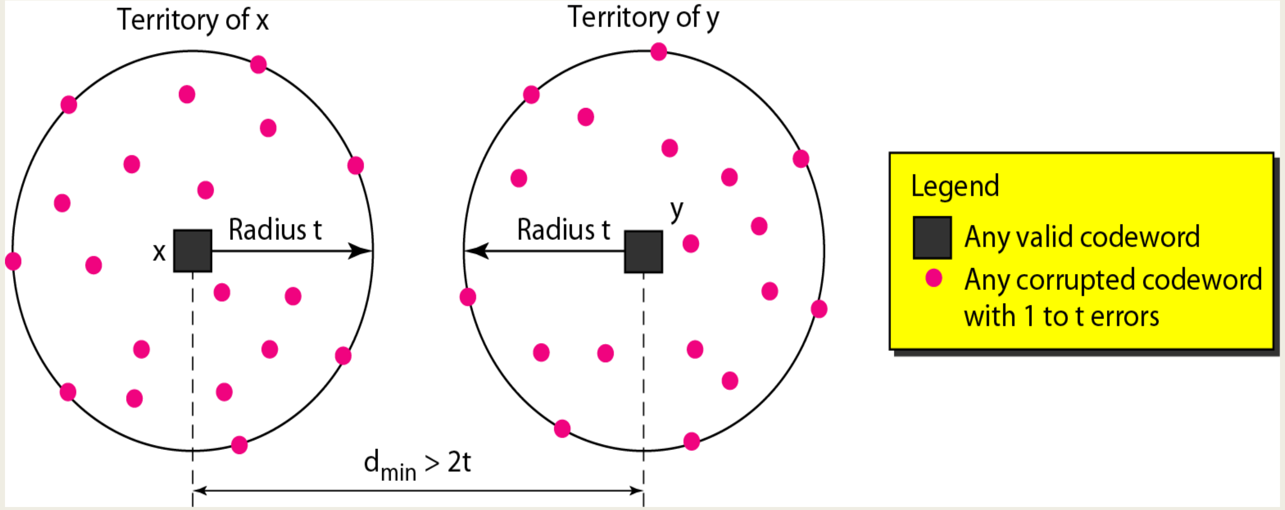


Fig. : Geometric concept for finding d_{min} in error correction

Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Linear Block Codes

- A linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.
- In a linear block code, the exclusive OR (XOR) of any two valid codewords creates another valid codeword.

Simple Parity-Check Code

- A simple parity-check code is a single-bit error-detecting code in which n = k + 1 with d_{min} = 2.
- Even parity (ensures that a codeword has an even number of 1's) and odd parity.
- A simple parity-check code can detect an odd number of errors.

Cont...

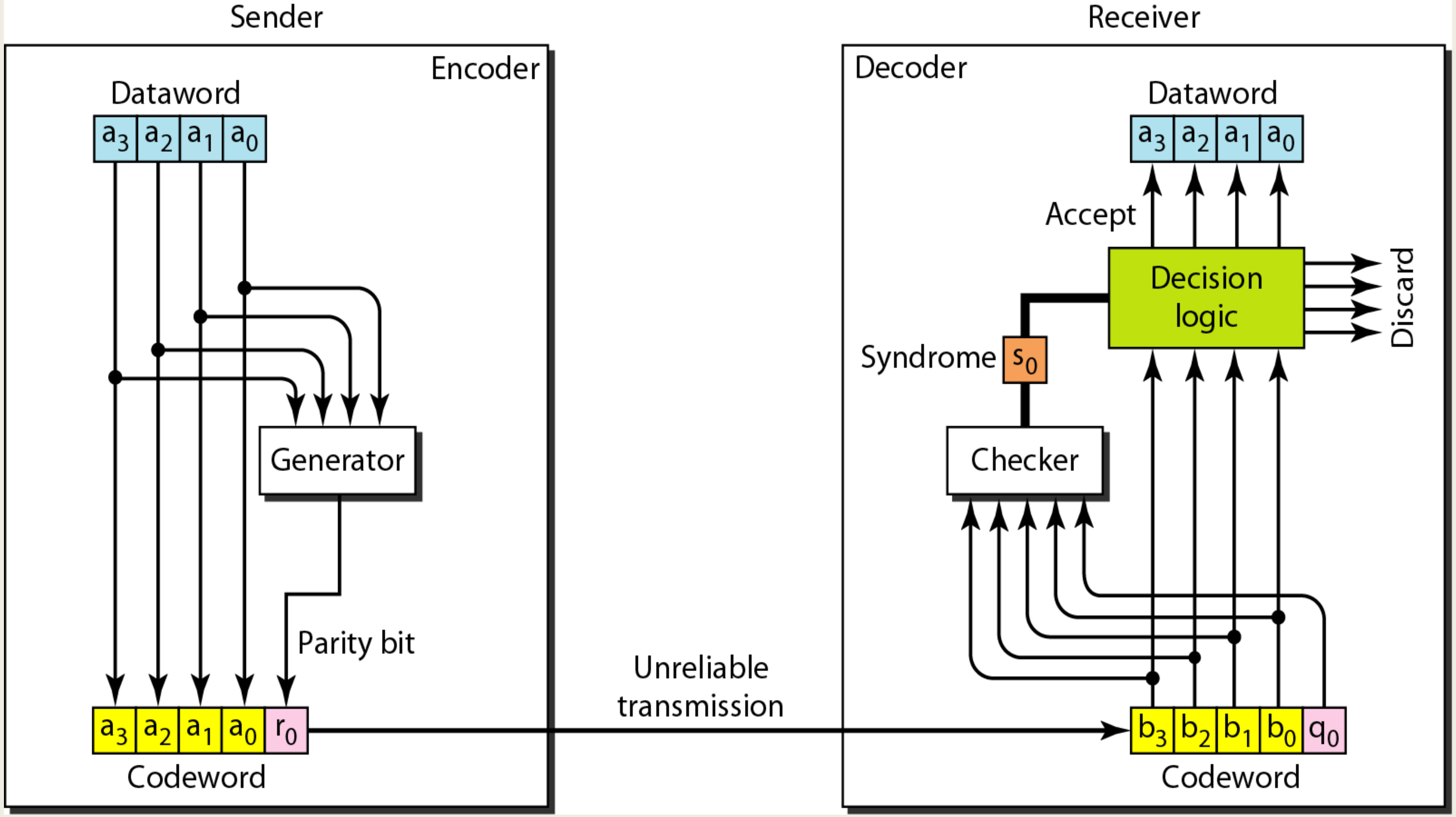


Fig.: Encoder and decoder for simple parity-check code

Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

Hamming Code

A Hamming code can only correct a single error or detect a double error. To make the Hamming code respond to a burst error of size *N*, we need to make *N* codewords out of our frame.

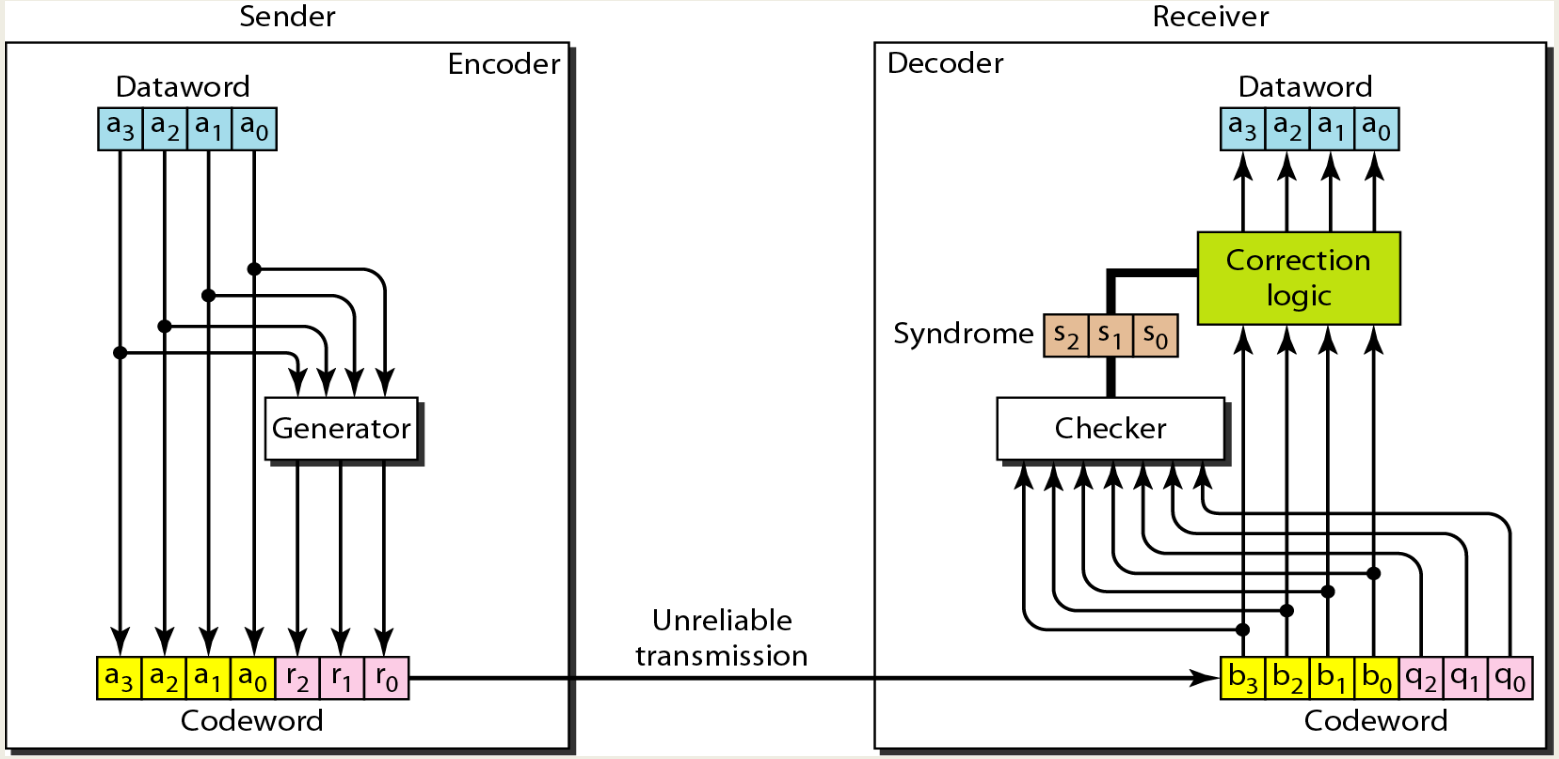


Fig.: Encoder and decoder for hamming code

Source: B. A. Forouzan, " Data Communications and Networking ," *McGraw-Hill Forouzan Networking Series*,5E.

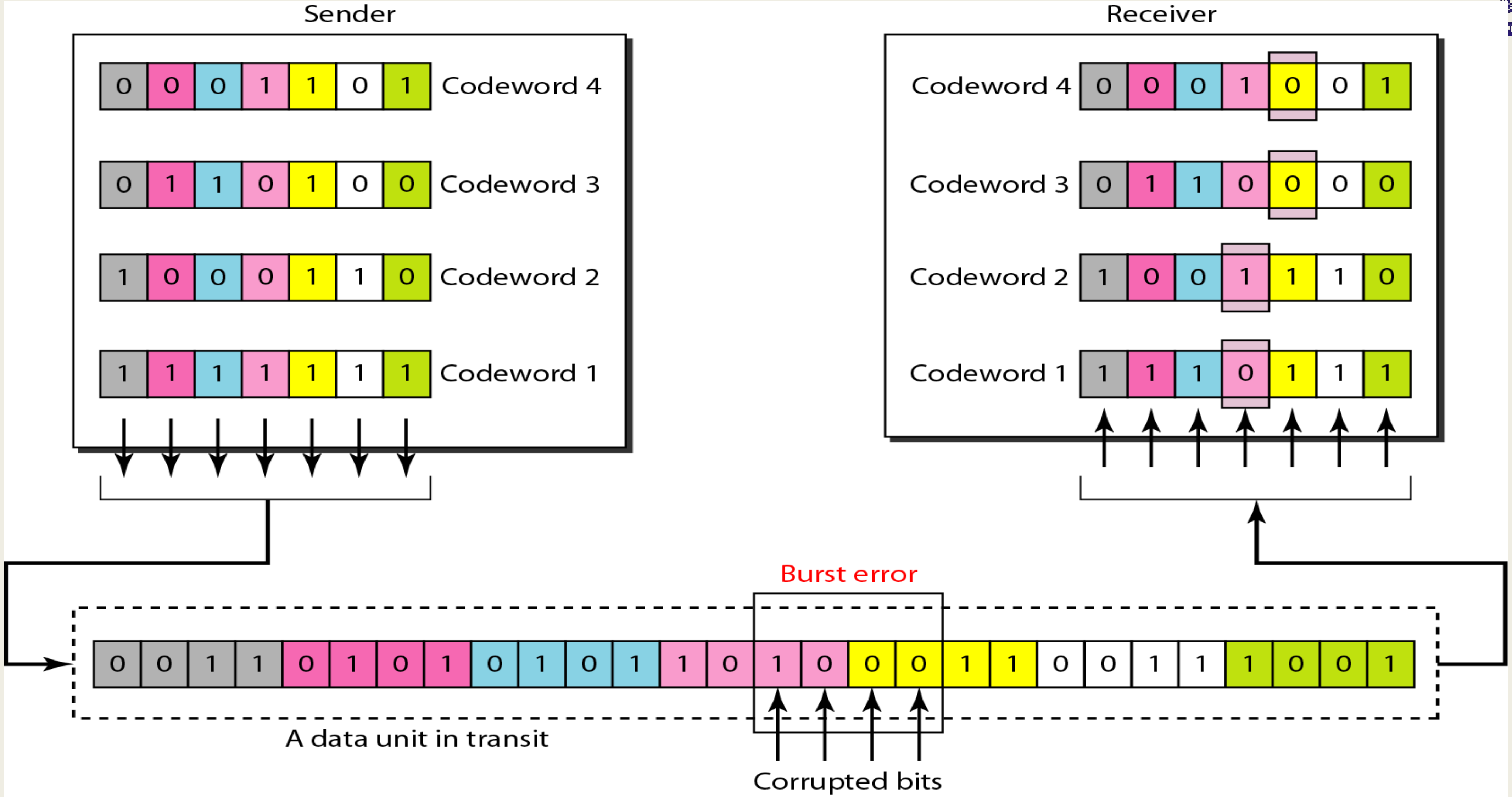
Burst Errors

- Burst errors are very common, in particular in wireless environments where a fade will affect a group of bits in transit. The length of the burst is dependent on the duration of the fade.

- One way to counter burst errors, is to break up a transmission into shorter words and create a block (one word per row), then have a parity check per word.

- The words are then sent column by column. When a burst error occurs, it will affect 1 bit in several words as the transmission is read back into the block format and each word is checked individually.

Burst Error Correction Using Hamming Code



Sender

0 0 0 1 1 0 1 Codeword 4

0 1 1 0 1 0 0 Codeword 3

1 0 0 0 1 1 0 Codeword 2

1 1 1 1 1 1 1 Codeword 1

Receiver

Codeword 4 0 0 0 1 0 0 1

Codeword 3 0 1 1 0 0 0 0

Codeword 2 1 0 0 1 1 1 0

Codeword 1 1 1 1 0 1 1 1

Burst error

0 0 1 1 0 1 0 1 0 1 0 1 1 0 1 0 0 0 1 1 0 0 1 1 1 0 0 1

A data unit in transit

Corrupted bits

Source: B. A. Forouzan, “ Data Communications and Networking ,” *McGraw-Hill Forouzan Networking Series*,5E.