Communication and Networking
Forward Error Correction Basics

D. Richard Brown III

(selected figures from Stallings Data and Computer Communications 10th edition)

Error Detection vs. Forward Error Correction

Three common methods for **error detection**:

- Parity
- Checksum
- Cyclic redundancy check (CRC)

Generally, these methods do not provide any way to locate/correct the errors. If an error is detected in a block of data, the block of data must be retransmitted.

Problems:

1. What if link is not bi-directional, e.g., HDTV?
2. What if BER on link is very high, e.g., 10%?
3. What if the link has high latency, e.g., satellite communications?

Forward error correction (FEC) is a way of adding redundancy to messages so that the receiver can both detect and correct common errors.

(n, k) Block Encoder/Decoder

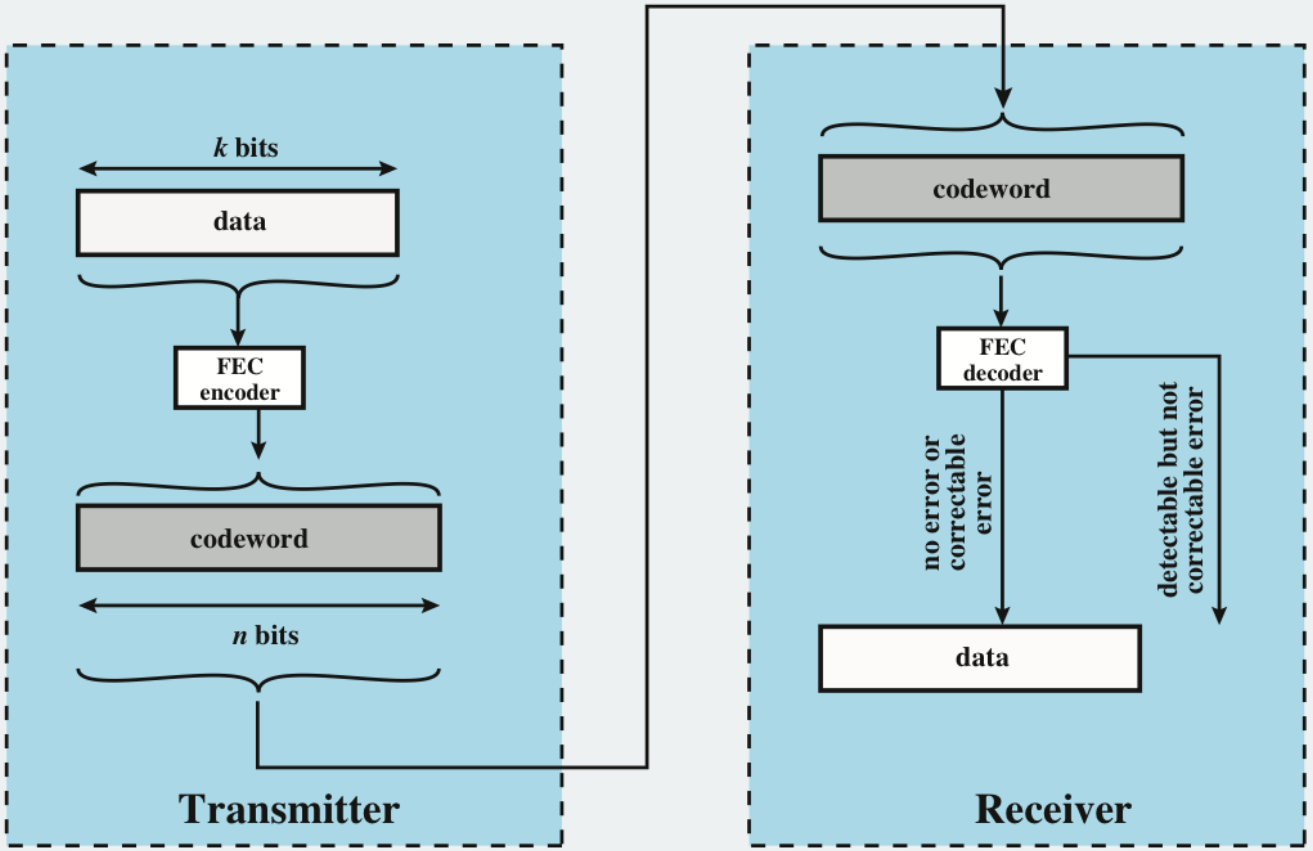


Figure 6.8 Error Correction Process

Codebook

A codebook is a mapping from k-bit data sequences to n-bit codewords with $n > k$. The code rate $r = \frac{k}{n} < 1$. Example (5,2) code ($r = \frac{2}{5}$):

Data Block	Codeword
00	00000
01	00111
10	11001
11	11110

Remarks:

- The transmitter and receiver both know the codebook.
- The transmitter takes data blocks, maps them to codewords and transmits the codeword (not the data block).
- The receiver receives the codewords (potentially with one or more errors) and maps them back to data blocks.

Hamming Distance

The error correction capability of a block code is directly related to the "Hamming distance" between each of the codewords. The Hamming distance between n-bit codewords v_1 and v_2 is defined as

$$d(v_1, v_2) = \sum_{\ell=0}^{n-1} \text{XOR}(v_1(\ell), v_2(\ell))$$

This is simply the number of bits in which v_1 and v_2 are different.

Example: $v_1 = 011011$ and $v_2 = 110001$. An XOR of these codewords gives $\text{XOR}(v_1, v_2) = 101010$. Hence the Hamming distance $d(v_1, v_2) = 3$.

The **minimum distance** is defined as

$$d_{\min} = \min_{i \neq j} d(v_i, v_j).$$

Hamming Distance vs. Redundancy

The redundancy of an (n, k) code is

$$\text{redundancy} = \frac{n-k}{k}.$$

Our (5,2) example code again:

Data Block	Codeword
00	v_1=00000
01	v_2=00111
10	v_3=11001
11	v_4=11110

The redundancy is $\frac{5-2}{2} = \frac{3}{2}$.

The Hamming distances are

$$\begin{aligned} d(v_1, v_2) &= 3 \\ d(v_1, v_3) &= 3 \\ d(v_1, v_4) &= 4 \\ d(v_2, v_3) &= 4 \\ d(v_2, v_4) &= 3 \\ d(v_3, v_4) &= 3 \end{aligned}$$

hence $d_{\min} = 3$.

In general, we want $d_{\min}$ to be large and the redundancy to be small.

Which Code is Better?

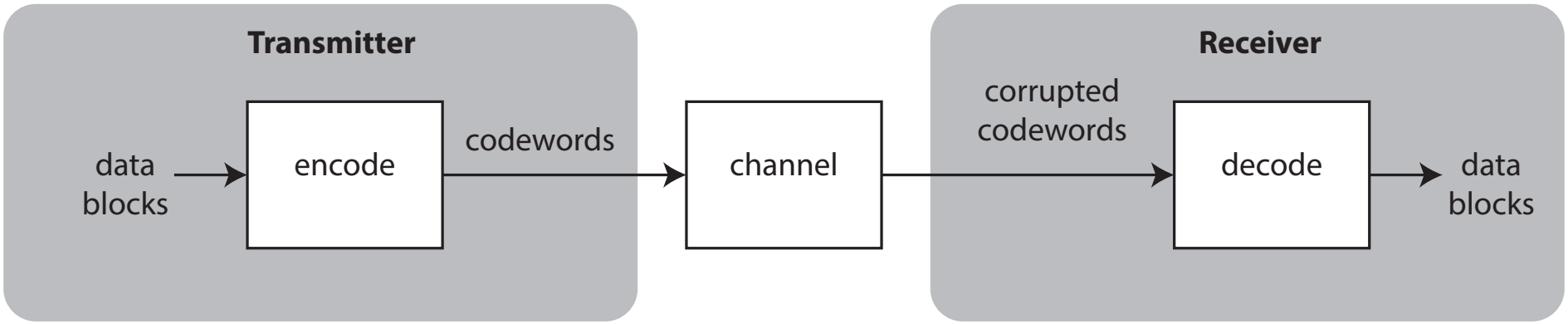
Code 1:

Data Block	Codeword
00	v_1=00000
01	v_2=00111
10	v_3=11001
11	v_4=11110

Code 2:

Data Block	Codeword
0	v_1=000
1	v_2=111

Decoding Invalid Codewords



Suppose the transmitter wants to send data block 00 using our (5,2) block code.

This gets encoded as 00000 and sent through the channel.

Suppose the output of the channel is 00100 (one bit received in error). This is not a valid codeword. What should the receiver do?

Minimum Distance Decoding

When an invalid codeword is received, the receiver should choose the valid codeword with the minimum Hamming distance to the invalid codeword.

Our (5,2) example code again:

Data Block	Codeword
00	v_1=00000
01	v_2=00111
10	v_3=11001
11	v_4=11110

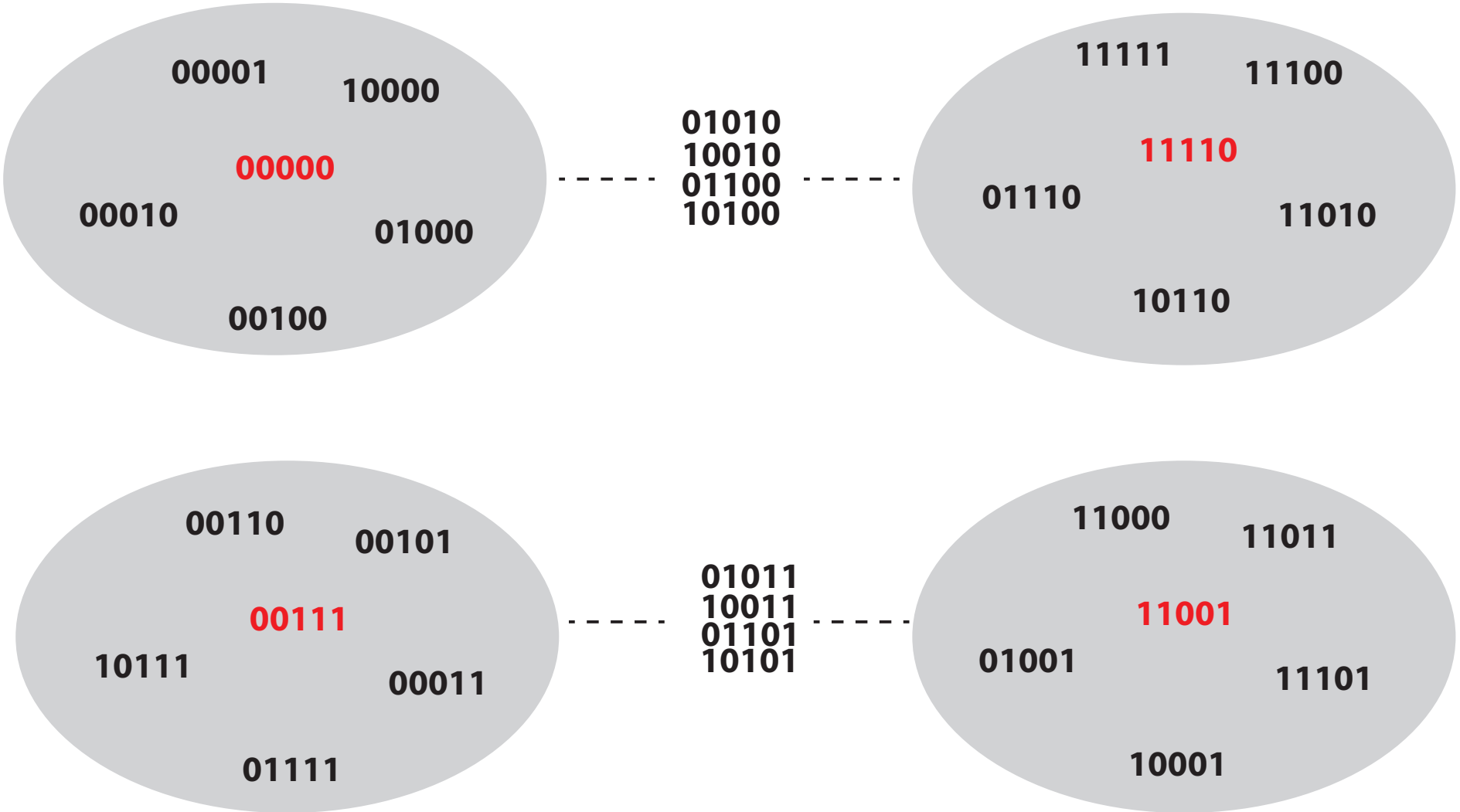
If we receive 00100, the Hamming distances are

$$d(00100, v_1) = 1$$
$$d(00100, v_2) = 2$$
$$d(00100, v_3) = 4$$
$$d(00100, v_4) = 3$$

hence we should pick codeword v_1. The receiver then decodes this codeword as the data block 00 and the data is correctly received.

This (5,2) code can always correct codewords received with one error.

Minimum Distance Decoding: (5,2) Example



Correctable Errors

For some positive integer t_c, if a code satisfies

$$d_{\min} \geq 2t_c + 1$$

then the code can correct up to t_c bit errors in a received codeword.

Equivalently, we can say the number of guaranteed correctable errors per codeword is

$$t_c = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

where $\lfloor x \rfloor$ is the "floor" operator which always rounds down.

Detectable Errors

The number of guaranteed detectable errors per codeword is

$$t_d = d_{\min} - 1.$$

Intuition:

- a codeword received with $d_{\min}$ different bits could be another valid codeword (undetected error)
- a codeword received with $d_{\min} - 1$ different must be invalid (detected error, although not necessarily correctable)

The (7,4) Hamming Code

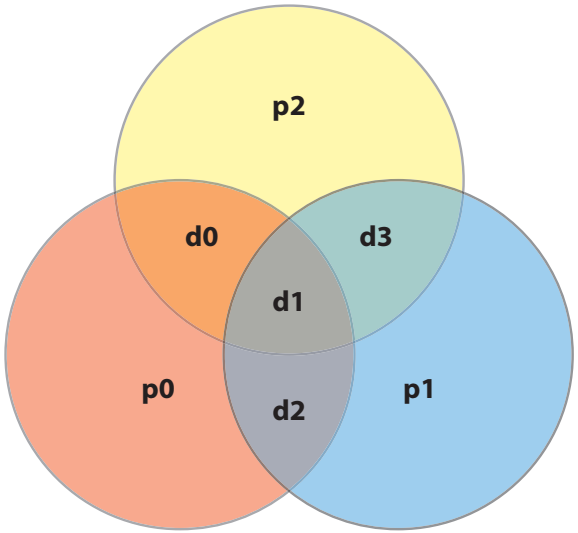
An example of a low-redundancy code that can always correct one error is the (7,4) Hamming code.

TABLE 10.1 *Code words of a (7, 4) Hamming code*

Message Word	Code Word	Weight of Code Word	Message Word	Code Word	Weight of Code Word
0 0 0 0	0 0 0 0 0 0 0	0	1 0 0 0	1 1 0 1 0 0 0	3
0 0 0 1	1 0 1 0 0 0 1	3	1 0 0 1	0 1 1 1 0 0 1	4
0 0 1 0	1 1 1 0 0 1 0	4	1 0 1 0	0 0 1 1 0 1 0	3
0 0 1 1	0 1 0 0 0 1 1	3	1 0 1 1	1 0 0 1 0 1 1	4
0 1 0 0	0 1 1 0 1 0 0	3	1 1 0 0	1 0 1 1 1 0 0	4
0 1 0 1	1 1 0 0 1 0 1	4	1 1 0 1	0 0 0 1 1 0 1	3
0 1 1 0	1 0 0 0 1 1 0	3	1 1 1 0	0 1 0 1 1 1 0	4
0 1 1 1	0 0 1 0 1 1 1	4	1 1 1 1	1 1 1 1 1 1 1	7

Unlike the (5,2) code we saw earlier with 8 uncorrectable sequences, the (7,4) Hamming code is a "perfect" code in that every possible received sequence is Hamming distance 1 from a valid codeword.

How to Calculate the (7,4) Hamming Code w/o a Table



Data block format:

d3	d2	d1	d0

Usual codeword format:

p2	p1	p0	d3	d2	d1	d0

Steps:

1. Get 4-bit block of data d_1, d_2, d_3, d_4 and place bits in figure.
2. Choose p_1, p_2, p_3 so that parity of red, blue, yellow circles are all even.
3. Put parity bits into codeword as shown and transmit.

Note that there are different formats for the Hamming code but the principle is the same. See Wikipedia and `http://goo.gl/vDoiy0`.

Computing the Bit Error Rate of a Block Code

Procedure, given $\mathcal{E}_b/N_0$ for uncoded transmission:

1. Compute $\mathcal{E}'_b/N_0$ for the coded transmission

$$\mathcal{E}'_b/N_0 = \frac{k}{n}\mathcal{E}_b/N_0$$

since the energy for the n-bit codeword must be the same as for the original k-data bits.

2. Compute the BER at $\mathcal{E}'_b/N_0$ with a particular modulation format, e.g. BPSK, and set this to p.

3. The probability of an uncorrectable error ($t+1$ or more bit errors in the codeword) can then be upper bounded as

$$P_B \leq \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

$$\approx \binom{n}{t+1} p^{t+1} \text{ when } p \text{ is close to zero}$$

where the bound is met with equality for perfect codes like Hamming (7,4).

Example: Hamming (7,4)

Suppose we have $\mathcal{E}_b/N_0 = 10$dB. For uncoded QPSK, the bit error rate from from Fig. 5.13(b) is $q \approx 10^{-5}$. The probability of one or more errors in a 4-bit block is then

$$P_B = 1 - (1 - 10^{-5})^4 \approx 4 \times 10^{-5}.$$

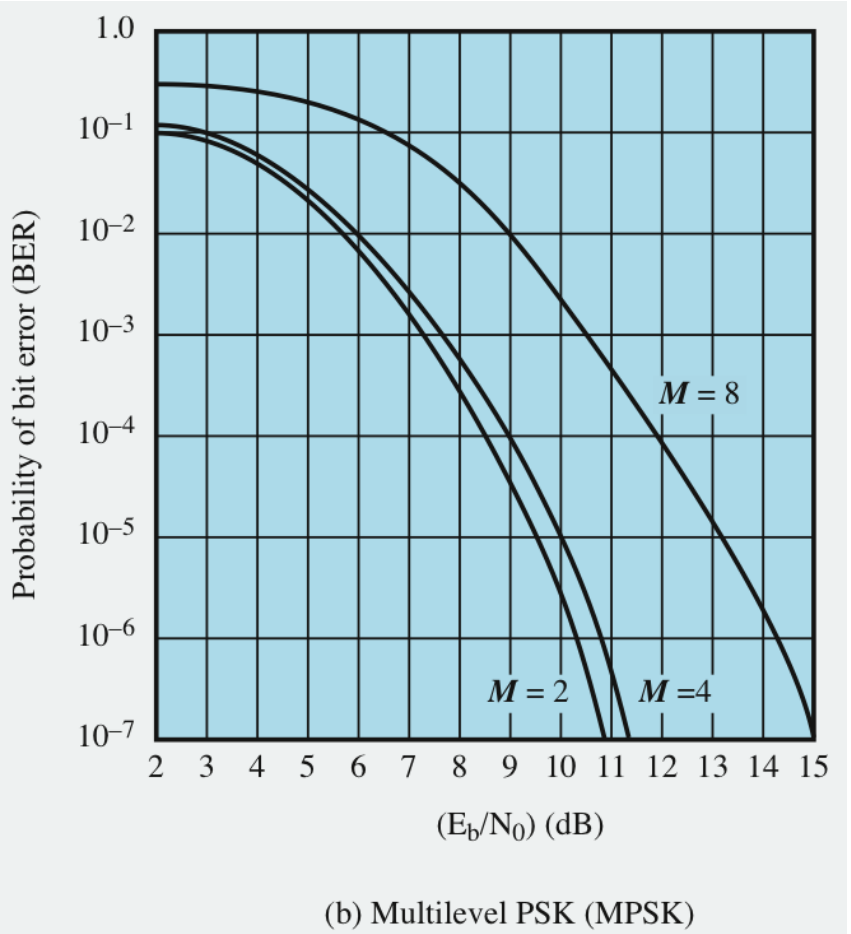
We can compute $\mathcal{E}_b'/N_0$ for the coded transmission as

$$\mathcal{E}_b'/N_0(\text{dB}) = 10 \log_{10} \left(\frac{4}{7} \cdot 10^{10/10} \right) \approx 7.5 \text{ dB}$$

Assuming QPSK transmission, we can get the BER from Fig. 5.13(b) $\Rightarrow p \approx 1 \times 10^{-3}$.

From the previously developed formula, the probability of an uncorrectable error is then

$$P_B \approx 21 \cdot (1 \times 10^{-3})^2 \approx 2.1 \times 10^{-5}.$$



(b) Multilevel PSK (MPSK)

Some Other Common Codes

1. More Hamming codes. All have $n = 2^r - 1$ and $k = 2^r - r - 1$ for positive integer $r \geq 3$. All have $d_{\min} = 3$.
2. Golay codes including a perfect Golay code (23,12) with $d_{\min} = 7$.
3. Reed-Muller codes with variable $d_{\min}$.
4. Reed-Solomon codes with variable $d_{\min}$. Used in lots of things:
   - digital video broadcasting
   - compact discs
   - QR codes

Modern codes that approach the Shannon limit:

- Turbo codes (mid 1990s)
- Low density parity check (LDPC) codes (Robert Gallagher, 1960s)

Coding Gain Example $r = \frac{1}{2}$

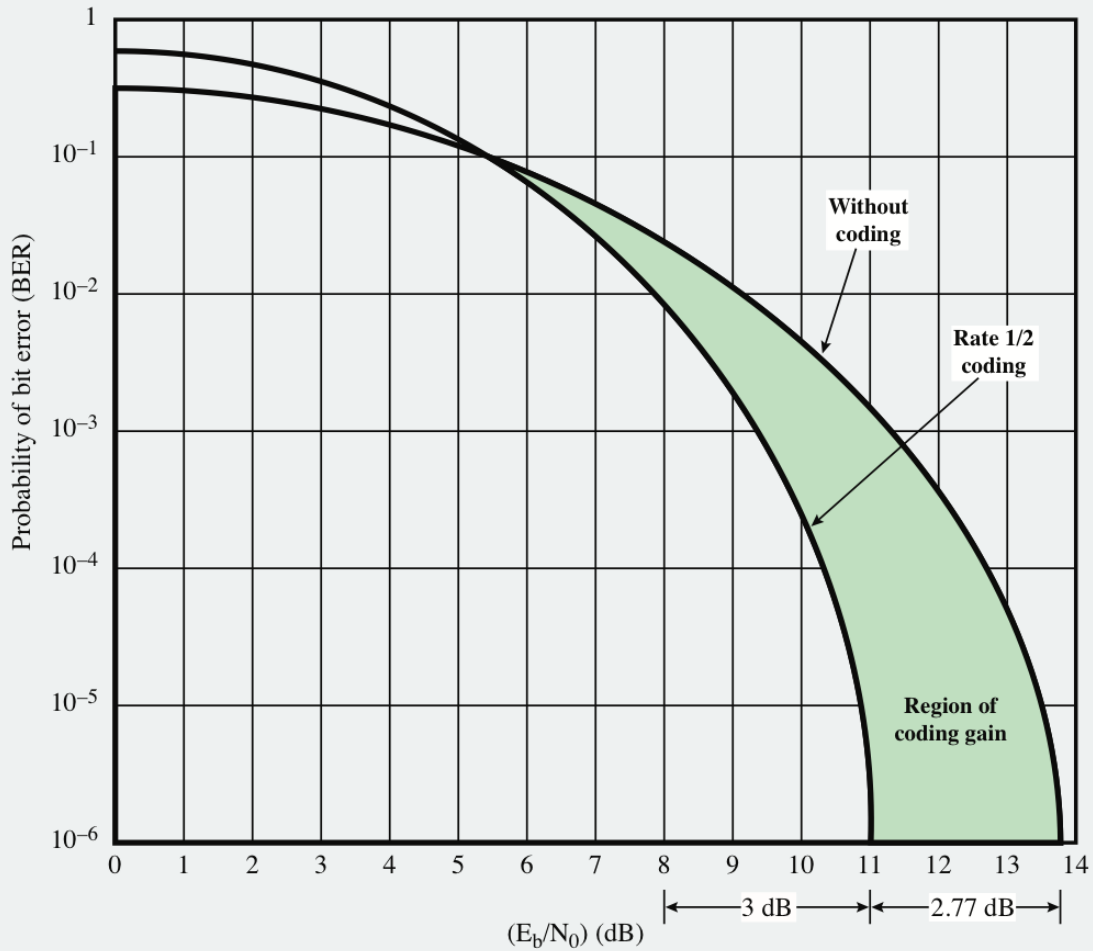


Figure 6.9 How Coding Improves System Performance

Final Remarks

- Forward error correction is used extensively in wireless and wired communication systems.
- Rather than rejecting and re-requesting erroneous messages, the receiver can automatically correct the most common types of errors.
- Block coding (as covered here) is just one type of coding.
- Performance of block codes (with hard-decision decoding) characterized by $d_{\min}$ and redundancy.
- Inherent tradeoff: increasing $d_{\min}$ requires increasing redundancy (lowering r).
- Modern codes can get very close to the Shannon limit such that $P_B \to 0$ if $r \leq C$.