formed by changing each of the first t digits of c. Then $d(c, c') = t \leq r$, and so c could be sent and c' received with no more than r errors. We will show that $d(c^*, c') \leq d(c, c')$.

Case 1: $s \leq r$ By the definition of t, we have $t = s$. Hence $c' = c^*$ in this case, and it follows that

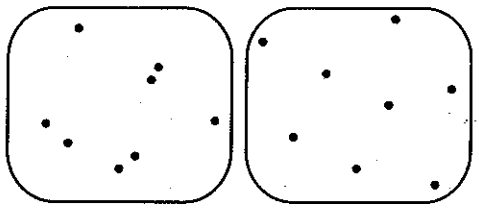
$$d(c^*, c') = 0 \leq d(c, c').$$

Case 2: $s > r$ By the definition of t, we have $t = r$. Because c' agrees with c^* in precisely the first r and the last $n - s$ digits, we obtain

$$d(c^*, c') = n - (r + n - s) = s - r \leq 2r - r = r = t = d(c, c').$$

Thus, in either case, $d(c^*, c') \leq d(c, c') = t \leq r$. It follows that if either c or c^* were the intended codeword and no more than r errors occurred in transmission, then the received word could be c'. Hence c' cannot be corrected by this coding scheme, and so this scheme cannot correct r errors. ■

Theorem 3.7 shows that in order to have a good code—that is, one that corrects as many errors in a block as possible—the minimum distance between codewords must be as large as possible. (See Figure 3.2, where the large colored dots represent codewords.) In subsequent sections, we describe how to create such good codes.



a bad code a good code

FIGURE 3.2

EXERCISES 3.4

In Exercises 1–8, determine the parity check digit that should be appended to each block so that the total number of 1*s is even.*

1. 01001010 **2.** 01101011 **3.** 00110011 **4.** 00110100
5. 01101010 **6.** 01010000 **7.** 00101010 **8.** 01110111

In Exercises 9–16, use formula (3.1) to determine the probability of exactly k errors in the transmission of n digits if the probability of an error in the transmission of a single digit is .01.

9. $k = 1, n = 5$ **10.** $k = 0, n = 6$ **11.** $k = 2, n = 7$ **12.** $k = 1, n = 8$
13. $k = 0, n = 8$ **14.** $k = 2, n = 10$ **15.** $k = 1, n = 10$ **16.** $k = 0, n = 10$

In Exercises 17–24, determine the Hamming distance between the given codewords.

17. $c_1 = 0110, c_2 = 1010$
18. $c_1 = 1001, c_2 = 1101$
19. $c_1 = 11001, c_2 = 01110$
20. $c_1 = 01010, c_2 = 10101$
21. $c_1 = 001100, c_2 = 111100$
22. $c_1 = 101010, c_2 = 001110$
23. $c_1 = 10011100, c_2 = 00111010$
24. $c_1 = 01101100, c_2 = 11000011$

In Exercises 25–32, add the given codewords using addition over Z_2 in each place. For example, $0110 + 0101 = 0011$.

25. $c_1 = 1110, c_2 = 0010$
26. $c_1 = 0101, c_2 = 1001$
27. $c_1 = 10111, c_2 = 10010$
28. $c_1 = 01011, c_2 = 11100$
29. $c_1 = 101011, c_2 = 001110$
30. $c_1 = 010111, c_2 = 110001$
31. $c_1 = 01100011, c_2 = 10110101$
32. $c_1 = 11010100, c_2 = 01001101$

In Exercises 33–36, suppose that the minimal Hamming distance between codewords in a certain block code is the given value m.

(a) *Determine the maximum number of errors that can be detected.*

(b) *Determine the maximum number of errors that can be corrected.*

33. $m = 8$ **34.** $m = 13$ **35.** $m = 15$ **36.** $m = 20$

37. Show that, for two codewords c_1 and c_2 of the same length, the Hamming distance between c_1 and c_2 equals the number of 1s in $c_1 + c_2$, where the addition is performed as described in Exercises 25–32.

38. Suppose that the minimal Hamming distance between codewords in a certain block code is m. Prove Theorem 3.7(a) by establishing each of the following results:

(a) If $m \geq r + 1$, then all errors in r or fewer digits can be detected.

(b) If all errors in r or fewer digits can be detected, then $m \geq r + 1$.

39. Consider the following table:

c_1	c_2	c_5
c_3	c_4	c_6
c_7	c_8	

Define a (4, 8)-block code as follows: Encode the message word $c_1c_2c_3c_4$ as the codeword $c_1c_2c_3c_4c_5c_6c_7c_8$, where c_5 is chosen so that the number of 1s in the first row is even, c_6 is chosen so that the number of 1s in the

even number of 1s, and $w_7 = 1$ if $[w_1 \quad w_2 \quad w_3]$ contains an odd number of 1s. Thus $[w_1 \quad w_2 \quad w_3 \quad w_4 \quad w_5 \quad w_6 \quad w_7]A^* = [0 \quad 0 \quad 0 \quad 0]$ when $[w_4 \quad w_5 \quad w_6]$ is identical to $[w_1 \quad w_2 \quad w_3]$ and w_7 is a check digit of 0 or 1, according to whether the number of 1s in $[w_1 \quad w_2 \quad w_3]$ is even or odd. But these are exactly the requirements that make xA^* a codeword for this code. ■

In Section 3.6, we will learn how to use the check matrix A^* to efficiently decode words that are encoded with the generator matrix A.

EXERCISES 3.5

In Exercises 1–4, determine the number of words in the given set.

1. $\mathcal{W}_5$ **2.** $\mathcal{W}_6$ **3.** $\mathcal{W}_8$ **4.** $\mathcal{W}_{10}$

In Exercises 5–8, suppose that the generator matrix for a (4, 8)*-code is*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Determine the codeword corresponding to each of the given message words.

5. 1001 **6.** 0011 **7.** 1101 **8.** 0111

In Exercises 9–12, determine the size of the check matrix for the given code.

9. a (3, 9)-block code
10. a (4, 11)-block code
11. a (5, 10)-block code
12. a (7, 13)-block code

13. If the check matrix of a matrix code is a 9×3 matrix, what is the efficiency of the code?

14. If the check matrix of a matrix code is an 11×4 matrix, what is the efficiency of the code?

In Exercises 15–20, determine all the codewords for the code having the given generator matrix.

15. $\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$

16. $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$

17. $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$

18. $\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$

19. $\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$

20. $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$

In Exercises 21–28, determine the check matrix associated with the given generator matrix.

Suppose that we have a Hamming code, and a word c' is received. The syndrome of c' is $s = c'A^*$. If $s = O$, then c' is a codeword, and we assume that there has been no error in transmission. But if $s \neq O$, then s appears as a row of A^* because every nonzero word of length r appears as a row of A^*. Let row i of A^* equal s. Then c' will be decoded as the first k digits of c, where c is the word obtained by changing the ith digit of c'. Thus, when check matrix row decoding is used with a Hamming code, *step 4 never happens, and every received word can be decoded.* The efficiency of the Hamming code for a particular value of r is

$$\frac{k}{n} = \frac{2^r - r - 1}{2^r - 1} = 1 - \frac{r}{2^r - 1}.$$

It can be shown that this quantity can be made arbitrarily close to 1 by choosing r to be sufficiently large. Thus there are Hamming codes with efficiencies that are arbitrarily close to 1.

EXERCISES 3.6

In Exercises 1–8, determine the syndrome of each word using the check matrix

$$A^* = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then decode the word if it is a codeword or if it differs from a codeword in a single digit.

1. 101111 **2.** 001001 **3.** 010110 **4.** 011010
5. 101010 **6.** 101001 **7.** 110110 **8.** 010000

In Exercises 9–28, the given word was received after being encoded using the generator matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

and transmitted. Determine the syndrome of each word, and decode it if it is a codeword or if it differs from a codeword in a single digit.

9. 1010101 **10.** 1110001 **11.** 1011001 **12.** 1001101
13. 0111011 **14.** 0110011 **15.** 1100110 **16.** 1100001
17. 0011101 **18.** 1010111 **19.** 1011100 **20.** 0011111
21. 1001100 **22.** 1011000 **23.** 1101100 **24.** 0010111
25. 1001011 **26.** 0100110 **27.** 0101011 **28.** 0000110