$$\begin{aligned}\partial(\mathbf{x}, \mathbf{y}) &= \partial(\mathbf{x}-\mathbf{y}, \mathbf{y}-\mathbf{y}) = \partial(\mathbf{x}-\mathbf{y}, \mathbf{0}) \\ &= w(\mathbf{x}-\mathbf{y}).\end{aligned}$$

Note that, since addition is modulo 2, $\mathbf{x}-\mathbf{y}$ is the same as $\mathbf{x}+\mathbf{y}$.

Theorem 24.2 Let C be a linear code, and let $w_{\min}$ denote the minimum weight of any codeword, except $\mathbf{0}$, in C. Then the minimum distance of C is given by

$$\delta = w_{\min}.$$

Proof Let $\mathbf{c}^*$ be a codeword for which $w(\mathbf{c}^*) = w_{\min}$. Since $\mathbf{c}^*$ and $\mathbf{0}$ are both codewords, we have

$$\delta \leq \partial(\mathbf{c}^*, \mathbf{0}) = w(\mathbf{c}^*) = w_{\min}.$$

On the other hand, if $\mathbf{c}^1$ and $\mathbf{c}^2$ are two codewords at minimum distance, $\mathbf{c}^1 - \mathbf{c}^2$ is also a codeword (because C is linear), and

$$\delta = \partial(\mathbf{c}^1, \mathbf{c}^2) = w(\mathbf{c}^1 - \mathbf{c}^2) \geq w_{\min}. \qquad \square$$

The calculation of δ directly from the definition would involve finding the distance between each pair of codewords, whereas Theorem 24.2 tells us that it is sufficient to calculate the weight of each individual codeword—a considerable improvement (Ex. 24.2.5).

Exercises 24.2

1 For any $n \geq 1$ the code containing just the two words $000\ldots0$ and $111\ldots1$ of length n is a linear code. What are the values of k and δ?

2 Given any word $\mathbf{x}$ in V^n let $S_2(\mathbf{x})$ denote the set of words which can be obtained by making not more than two errors in $\mathbf{x}$. Show that

$$|S_2(\mathbf{x})| = \tfrac{1}{2}(n^2 + n + 2).$$

Deduce that if E is any code (not necessarily linear) of length 8 which will correct two errors, then $|E| \leq 6$.

3 What is the maximum dimension of a *linear* code of length 8 which will correct two errors? Construct such a code.

4 Let C be a linear code. Show that the subset of C containing those codewords which have even weight is also a linear code. Deduce that either all codewords in C have even weight, or exactly half of them have even weight.

5 Let C be a code with m codewords, and define an 'operation' to be the calculation of the weight of a word. Show that the number of operations required to find the distance between each pair of codewords is $O(m^2)$. If C is linear, explain how the minimum distance of C can be found by a method requiring only $O(m)$ operations.

24.3 Construction of linear codes

Let H be a binary matrix with n columns, and let $\mathbf{x}'$ denote the word $\mathbf{x}$ in V^n considered as a *column vector*. In particular, $\mathbf{0}'$ denotes the all-zero column vector. If $\mathbf{a}$ and $\mathbf{b}$ are words satisfying

$$H\mathbf{a}' = H\mathbf{b}' = \mathbf{0}',$$

then $\mathbf{a}+\mathbf{b}$ has the same property since and these equations determine $x_1, x_2, \ldots, x_r$ when the values of $x_{r+1}, x_{r+2}, \ldots, x_n$ are given. There are 2^{n-r} ways of choosing the latter values, and so we obtain a linear code with dimension $k = n - r$.

Theoretically speaking, the order of the columns of H is not important, since a rearrangement of columns corresponds to a rearrangement of the order of the bits in each codeword. Consequently, H may be taken to be any matrix which can be put in the form given above by rearranging the columns. We shall refer to this as the *standard form* for H.

Exercises 24.3

1 Write down all the codewords belonging to the linear code associated with the check matrix

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

2 What are the parameters n, k, δ for the code constructed in Ex. 1?

3 Suppose we wish to be able to send 128 different messages, and each message is to be represented by a binary codeword of length 11. Explain how to construct a linear code for this purpose.

4 Professor McBrain has decided that each mathematics student at the University of Folornia will be allocated an 'identity number' in the form of a binary word.

(i) If there are 53 students, find the least possible dimension of a *linear* code for this purpose. (It is assumed that some codewords will not be allocated.)

(ii) If the code must allow for the detection and correction of one error, find the least possible length of the codewords.

(iii) Write down a check matrix for a code which achieves the values found in (i) and (ii).

24.4 Correcting errors in linear codes

There is a very simple way of ensuring that a linear code defined by a check matrix H will correct at least one error.

Theorem 24.4 If no column of H consists entirely of zeros, and no two columns are the same, then the code C defined by H will correct one error.

Proof By Theorem 24.1 we have to show that $\delta \geq 3$, and by Theorem 24.2 this is equivalent to $w_{\min} \geq 3$.

Suppose C contains a codeword $\mathbf{a}$ with $w(\mathbf{a}) = 1$. Then $\mathbf{a}$ has just one bit equal to 1: suppose it is the bit in position i. Since all the other bits are 0, $H\mathbf{a}'$ is equal to the ith column $\mathbf{h}^{(i)}$ of H, and the condition $H\mathbf{a}' = \mathbf{0}'$ means that $\mathbf{h}^{(i)}$ consists entirely of zeros, contrary to hypothesis. Hence C contains no words of weight 1.

Suppose C contains a codeword $\mathbf{b}$ with $w(\mathbf{b}) = 2$, so that $\mathbf{b}$ has 1's in bits i and j only. Then

$$H\mathbf{b}' = \mathbf{h}^{(i)} + \mathbf{h}^{(j)},$$

and so $H\mathbf{b}' = \mathbf{0}'$ implies that $\mathbf{h}^{(i)} = \mathbf{h}^{(j)}$, contrary to the hypothesis. Hence C contains no words of weight 2 and $w_{\min} \geq 3$, as required. □

(i) Compute $H\mathbf{z}'$, where $\mathbf{z}$ is the received word.
(ii) If $H\mathbf{z}' = \mathbf{0}'$, $\mathbf{z}$ is a codeword.
(iii) If $H\mathbf{z}' \neq \mathbf{0}'$, locate the column $\mathbf{h}^{(i)}$ of H such that $H\mathbf{z}' = \mathbf{h}^{(i)}$, and change the ith bit of $\mathbf{z}$.

For example, suppose we are using the code with check matrix given in Ex. 24.3.1, and the word $\mathbf{z} = 1110111$ is received. We calculate that

$$H\mathbf{z}' = [1010]',$$

which is the first column of H. Hence there is an error in the first bit and the intended codeword is 0110111.

The Hamming codes provide a particularly neat application of the error-correcting procedure described above. When the check matrix for a Hamming code is written down in the natural way, the column $\mathbf{h}^{(i)}$ is just the binary representation of i. So if $\mathbf{z}$ is a received word containing one error, $H\mathbf{z}'$ is the binary representation of the integer i in which bit the error occurs. For instance, in the Hamming code of length 7 described in the *Example*, suppose the received word is $\mathbf{z} = 0\,1\,1\,1\,0\,1\,0$. We have

$$H\mathbf{z}' = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix},$$

and since 0 1 1 is the binary representation of 3, we conclude that the third bit must be corrected. Thus the correct codeword is 0 1 0 1 0 1 0.

Exercises 24.4

1 Let C be the linear code defined by the check matrix

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

If the word 110110 is received, and only one error has been made, what is the intended codeword?

2 Write down a check matrix for the Hamming code of length 15. How many codewords are there? Assuming that the columns of your matrix have been written down in the natural order, as in part (ii) of the *Example*, which of the following are codewords?

011010110111000
100000000000011
110110110111111

Correct those words which are not codewords, assuming that only one error has been made.

3 Suppose we wish to be able to send 256 different messages by means of a linear code which will correct one error.

(i) What is the least possible length of such a code?
(ii) Write down a suitable check matrix.
(iii) Find a lower bound for the length of the code if two errors are to be corrected.

4 Show by arithmetical arguments that there cannot be a perfect code of length n which corrects e errors in the cases

(i) $n = 5$, $e = 1$;
(ii) $n = 10$, $e = 2$.