

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.1 Words, codes, and errors

24.1.1

Find the minimum distance δ for each of the following codes.

- (i) $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$ in V^4 ;
- (ii) $\{10000, 01010, 00001\}$ in V^5 ;
- (iii) $\{000000, 101010, 010101\}$ in V^6 .

In each case, state the number of errors which can be detected and corrected.

Solution (i) Here $\delta = 2$. Changing one bit in any codeword results in a word that is not a codeword, so one error can be detected. However, such an error cannot be corrected: for example the word 1110 could be result of making an error in the the third bit of codeword 1100 or the result of making an error in the last bit of codeword 1111.

(ii) Here $\delta = 2$ also, and similar arguments apply.

(iii) Here $\delta = 3$. Any word obtained by making 1 or 2 errors in a codeword is not a codeword, so two errors can be detected. One error can be corrected, since making one error in any codeword produces a word that is at distance 2 or more from every other other codeword.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.1.2

Which of the codes in Ex. 24.1.1 can be extended by the inclusion of an extra codeword without altering δ ?

Solution

- (i) This code contains all words of length 4 that have none, two, or four 1s. Any extra word must therefore have one or three 1s, and in either case it will be a distance 1 from a word in the list.
- (ii) For example, 00100 can be added without changing the value $\delta = 2$.
- (iii) For example, 111100 can be added without changing the value $\delta = 3$.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.1.4

Prove the ‘triangle inequality’

$$\partial(\mathbf{x}, \mathbf{y}) \leq \partial(\mathbf{x}, \mathbf{z}) + \partial(\mathbf{z}, \mathbf{y})$$

where \mathbf{x} , \mathbf{y} , \mathbf{z} are any words in V^n .

Solution Let

$$\partial(\mathbf{x}, \mathbf{z}) = A, \quad \partial(\mathbf{z}, \mathbf{y}) = B.$$

The first equation means that changing A bits in \mathbf{x} gives \mathbf{z} and the second means that changing B bits in \mathbf{z} gives \mathbf{y} . Thus, changing *at most* $A + B$ bits in \mathbf{x} gives \mathbf{y} , and $\partial(\mathbf{x}, \mathbf{y}) \leq A + B$.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.2 Linear codes

24.2.1

For any $n \geq 1$ the code containing just the two words $000\dots 0$ and $111\dots 1$ of length n is a linear code. What are the values of k and δ ?

Solution Since there are two words and $2^1 = 2$, the dimension k is 1. Also

$$\delta = \vartheta(000\dots 0, 111\dots 1) = n.$$

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.2.2

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

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

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

Solution Counting the words at distance 0, 1, 2 from \mathbf{x} we get

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

In order to correct 2 errors, all the sets $S_2(\mathbf{x})$ for $\mathbf{x} \in E$ must be disjoint, so

$$|E| \times \frac{1}{2}(n^2 + n + 2) \leq 2^n.$$

In particular, when $n = 8$ we require

$$|E| \times 37 \leq 256, \quad \text{that is } |E| \leq 6.$$

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.3 Construction of linear codes

24.3.1

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

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

Solution The codewords \mathbf{x} are the solutions of $H\mathbf{x}' = \mathbf{0}'$, where H is the given matrix. This system of equations can be written in a form that expresses x_2, x_3, x_5, x_6 in terms of x_1, x_4, x_7 (this follows from the fact that columns 2, 3, 5, 6 are the columns of an identity matrix). In fact the rows of the matrix determine the following equations:

$$x_2 = x_1 + x_4 + x_7$$

$$x_5 = x_4 + x_7$$

$$x_3 = x_1 + x_4 + x_7$$

$$x_6 = x_7.$$

There are eight possible values for x_1, x_4, x_7 , and each determines a codeword.

0000 000	1110 000
0110 111	1000 111
0111 100	1001 100
0001 011	1111 011

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.3.2

What are the parameters n, k, δ for the code constructed in Ex. 24.3.1?

Solution The length of the words is $n = 7$. There are $8 = 2^3$ codewords, so $k = 3$. By inspection of the list, it is clear that $\delta = 3$; the general reason for this is discussed in Section 24.4.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.4 Correcting errors in linear codes

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?

Solution If $\mathbf{z} = 110110$, then

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

This is the second column of H . Therefore we conclude that there is an error in second bit, and the intended codeword was 100110.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.4.2

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.

Solution The check matrix for the Hamming code of length 15, using the order in which the columns represent the binary representations of the numbers 1, 2, 3, ..., 15, is

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

The dimension is $n = 15$ and the number of rows is $r = 4$, so the number of codewords is $2^{n-r} = 2^{11} = 2048$.

Let

$$z_1 = 011010110111000, \quad z_2 = 100000000000011, \quad z_3 = 110110110111111.$$

$H z_1' = [0110]'$, which represents 6, so the sixth bit is in error, and the intended word was 011011110111000.

$H z_2' = [0000]'$, so z_2 is a codeword.

$H z_3' = [1100]'$, which represents 12, so the 12th bit is in error, and the intended word was 110110110110111.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.5 Cyclic codes

24.5.1

Which of the following codes are cyclic?

- (i) {000, 100, 010};
- (ii) {000, 100, 010, 001};
- (iii) {000, 111};
- (iv) {0000, 1010, 0101, 1111}.

Solution

- (i) No. This code is not cyclic because the cyclic shift of 010, that is 001, is not included.
- (ii) No. In this case the shift property is satisfied, but the code is not linear: $100 + 010 = 110$, which is not included. The definition of a cyclic code requires linearity, so the code is not cyclic.
- (iii) Yes.
- (iv) Yes.

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.5.2

Write down the codewords of the cyclic code corresponding to the ideal $\langle 1 + x + x^2 \rangle$ in $V^3[x]$, and find a check matrix for this code.

Solution The codewords correspond to the polynomials

$$f(x) \times (1 + x + x^2),$$

where $f(x)$ is any one of the eight polynomials in $V^3[x]$, and multiplication is modulo $x^3 - 1$. You should check that there are only two distinct answers: 0 and $1 + x + x^2$. Hence the codewords are 000 and 111.

Clearly these words satisfy the equations $x_1 = x_2 = x_3$ and so a suitable check matrix is

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

Solutions to Chapter 24 Exercises

in *Discrete Mathematics* by Norman L. Biggs;
2nd Edition 2002

24.6 Classification and properties of cyclic codes

24.6.1

Write down the irreducible factors of $x^5 - 1$ in $\mathbb{Z}_2[x]$, and hence determine all cyclic codes of length 5. (There are four of them, all rather dull.)

Solution We have

$$x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Hence the divisors of $x^5 - 1$ are:

$$1, \quad x + 1, \quad x^4 + x^3 + x^2 + x + 1, \quad x^5 - 1.$$

The corresponding ideals are

$$\langle 1 \rangle = V^5;$$

$$\langle x + 1 \rangle, \text{ the words with even weight (Ex. 24.5.3);}$$

$$\langle x^4 + x^3 + x^2 + x + 1 \rangle = \{00000, 11111\};$$

$$\langle x^5 - 1 \rangle = \{00000\}.$$