For example, suppose

$$f(x) = 1 + x^2 \quad \text{in } V^3[x].$$

Multiplying $f(x)$ in turn by each element $p(x)$ of $V^3[x]$ (and remembering to reduce modulo $x^3 - 1$), we obtain Table 24.5.1.

Table 24.5.1

$p(x)$	$p(x)f(x) \bmod (x^3 - 1)$	Word
0	0	0 0 0
1	$1 + x^2$	1 0 1
x	$1 + x$	1 1 0
$1 + x$	$x + x^2$	0 1 1
x^2	$x + x^2$	0 1 1
$1 + x^2$	$1 + x$	1 1 0
$x + x^2$	$1 + x^2$	1 0 1
$1 + x + x^2$	0	0 0 0

So the ideal $\langle 1 + x^2 \rangle$ has just four elements

$$0, 1 + x, x + x^2, 1 + x^2$$

and the corresponding code in V^3 is the code denoted by C_2 in Section 24.1:

$$C_2 = \{000, 110, 011, 101\}.$$

Exercises 24.5

1 Which of the following codes are cyclic?

(i) $\{000, 100, 010\}$;

(ii) $\{000, 100, 010, 001\}$;

(iii) $\{000, 111\}$;

(iv) $\{0000, 1010, 0101, 1111\}$.

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.

3 Show that the ideal $\langle 1 + x \rangle$ in $V^5[x]$ corresponds to the code in V^5 containing all the words of even weight. Does this result hold when 5 is replaced by an arbitrary integer $n \geq 2$?

24.6 Classification and properties of cyclic codes

The next theorem justifies the claim that every cyclic code can be constructed by the procedure outlined at the end of the previous section.

Theorem 24.6.1 Let C be a cyclic code (ideal) in $V^n[x]$. Then there is a polynomial $g(x)$ in C such that

$$C = \langle g(x) \rangle.$$

is $\mathbf{0}$. The other codes are more interesting. In particular, let C be the code with canonical generator $g(x) = 1 + x + x^3$, so that in the notation introduced above

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

It follows from Theorem 24.6.3 that C has dimension 4, and a check matrix for C is

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

An inspection of this matrix reveals that its columns are the same as the columns of the check matrix for the Hamming code of length 7 (Section 24.4, *Example*), but in a different order. Hence the code C is essentially the same as the Hamming code.

The astute reader will have noticed that we have not said anything about the minimum distance δ of a cyclic code in general. For some classes of cyclic codes it is possible to obtain extremely useful results about δ; and these results, together with the theorems obtained in this section, mean that such codes are important both in theory and in practice. But these matters must be postponed to the course in coding theory which, it is hoped, the reader will be inspired to study after reading this book.

Exercises 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.)

2 Describe all the cyclic codes of length 7.

3 The factorization of $x^{15} - 1$ into irreducible polynomials in $\mathbb{Z}_2[x]$ is

$$x^{15} - 1 = (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4) \times (1 + x + x^2 + x^3 + x^4).$$

(i) Explain as to how this is related to the results obtained in Section 23.9.

(ii) What is the number of cyclic codes of length 15?

(iii) Find a canonical generator for a cyclic code equivalent to the Hamming code of length 15.

4 Use the results of Section 23.9 to find the number of irreducible factors of $x^{32} - x$ in $\mathbb{Z}_2[x]$, and hence determine the number of cyclic codes of length 31. Find a canonical generator for a cyclic code equivalent to the Hamming code of length 31.

24.7 Miscellaneous Exercises

1 Calculate the parameters (n, k, δ) for the linear code whose check matrix is

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

2 Decide whether or not the following words are codewords in the code defined in Ex 1, and correct those that have been corrupted, assuming that only one error has occurred in each word.

(i) 11111, (ii) [illegible] (iii) [illegible]

How many words in all cases can be corrected by changing one bit?

3 Let C be a code with minimum weight $\delta = 3$. Show that there is a word $\mathbf{x}$ such that

$$\partial(\mathbf{x}, \mathbf{c}_1) = 1, \qquad \partial(\mathbf{x}, \mathbf{c}_2) = 2,$$

for some codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ in C. What action should be taken if $\mathbf{x}$ is received?

4 Write down a check matrix for the linear code consisting of all the words of length 7 which have even weight.

5 Use the method of Section 24.2 to show that there is no code C in V^5 such that C has minimum distance $\delta = 3$ and $|C| = 6$.

6 By direct analysis of the possibilities show that the result given in the previous exercise remains true if the condition $|C| = 6$ if replaced by $|C| = 5$.

7 For which of the following values of the parameters (n, k, δ) is it possible that a linear code with those parameters exists?

(i) $(12, 7, 5)$; (ii) $(11, 4, 5)$.

8 Let C be a linear code of length n and dimension k, and suppose i is any integer in the range $1 \leq i \leq n$. Show that

$$C_0 = \{\mathbf{c} \in C \mid c_i = 0\}$$

is a linear code of length n and dimension $k - 1$.

9 Show by arithmetical means that a code C with length $n = 6$ and minimum distance $\delta = 3$ must satisfy $|C| \leq 9$. Verify by direct means that there is no code with $|C| = 9$ and construct a code with $|C| = 8$.

10 Let C be a binary code of length n which will correct two errors and is perfect. Show that

(i) $n^2 + n + 2$ is a power of 2;

(ii) there is only one value of $n \leq 10$ which satisfies condition (i);

(iii) there is a code C with the required properties for the value of n obtained in (ii), but it is trivial.

Compute the next smallest value of n for which (i) is satisfied. (Unfortunately, it can be shown that there is no code in this case, or for any other value of n.)

11 Derive a condition analogous to (i) in the previous exercise for a perfect code which will correct three errors, and show that your condition is satisfied when $n = 7$ and $n = 23$. (In the next exercise we will show that there is a non-trivial code when $n = 23$.)

12 Show that in $\mathbb{Z}_2[x]$ the polynomial $x^{23} - 1$ can be written as $(x - 1)f(x)g(x)$, where $f(x)$ and $g(x)$ are polynomials of degree 11. Show that the cyclic code generated by $f(x)$ (or $g(x)$) is a perfect code which will correct three errors.

13 Let C_1 and C_2 be cyclic codes of length n, with generators $g_1(x)$ and $g_2(x)$, respectively. Show that

$$C_1 + C_2 = \{\mathbf{x} \in V^n \mid \mathbf{x} = \mathbf{c}_1 + \mathbf{c}_2 \text{ for some } \mathbf{c}_1 \in C_1, \mathbf{c}_2 \in C_2\}$$

is a cyclic code with generator gcd $(g_1(x), g_2(x))$.

14 Show that every Hamming code is a cyclic code.

15 Show that if a cyclic code contains a codeword whose weight is odd, then it contains the word $111\cdots1$.

16 Let $B_1, B_2, \ldots, B_7$ be the blocks of the Steiner triple system with seven varieties $1, 2, \ldots, 7$. Define a set C of seven words $\mathbf{w}^{(1)}, \mathbf{w}^{(2)}, \ldots, \mathbf{w}^{(7)}$ in V^7 by the rules

$$w_j^{(i)} = \begin{cases} 1 & \text{if } j \in B_i, \\ 0 & \text{otherwise.} \end{cases}$$

Show that C is a code with minimum distance 3.

17 Let C be the code constructed by the method given in the previous example, but using a projective plane over $\mathbb{F}_q$ in place of the Steiner triple system. What is the minimum distance of C?

18 Let S denote the set of codewords of weight 3 in a Hamming code of length $2^r - 1$. For each $\mathbf{w}$ in S define a subset B of $\{1, 2, \ldots, 2^r - 1\}$ by the rule that

$$i \in B \quad \Leftrightarrow \quad w_i = 1.$$

Show that the sets B are the blocks of a Steiner triple system.