Since $xf(x)$ and $h(x)$ each have degree $n - \deg(g(x))$, the coefficient of $x^{n-\deg(g(x))}$ in their sum is 0. So either $xf(x) + h(x) = 0$ or $\deg(xf(x) + h(x)) < n - \deg(g(x))$. In either case, the cyclic shift $xf(x)g(x) + (x^n + 1)$ is a code word in C. Therefore, C is a cyclic code. ◆

29.12 Definition The code C in Theorem 29.11 is called the **polynomial code of length n generated by** $g(x)$. ■

29.13 Example Find the code words for C, the polynomial code of length 7 generated by the polynomial $g(x) = x^3 + x^2 + 1$. What is the information rate for C? Determine if C detects a one-bit error and if so, can C correct a one-bit error? What about detecting and correcting two-bit errors?

Solution As in Example 29.10, one method of finding all the code words is to multiply every polynomial of degree 3 or less by $g(x)$, but there is a much simpler method if the code is cyclic. The polynomial $x^7 + 1$ can be seen to factor in $\mathbb{Z}_2[x]$ as

$$x^7 + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + 1)$$

simply by using long division of polynomials. Therefore C is a cyclic code by Theorem 29.11. Since $1 \cdot g(x) = g(x) \in C$ and C contains all cyclic shifts of $g(x)$, we have all the polynomials in the first column of Figure 29.14 as code words in C. Since C is a group, $(x^3 + x^2 + 1) + (x^4 + x^3 + x) = x^4 + x^2 + x + 1 \in C$. The fact that C is cyclic implies the second column of Figure 29.14 is contained in C. There are $2^4 = 16$ polynomials of degree less than 4 (including the zero polynomial) with coefficients in $\mathbb{Z}_2$. Thus C contains 16 elements. Since C is a subgroup, the zero polynomial is in C, leaving only one more polynomial to complete the list. This polynomial must remain the same when a cyclic shift is applied. Other than the polynomial 0, the only polynomial that remains the same when a cyclic shift is applied is

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Thus Figure 29.14 gives the code C as polynomials. Figure 29.15 gives the code as elements in $\mathbb{Z}_2^7$.

Since $|C| = 2^4$ and the code word length is 7, the information rate is $\frac{4}{7}$.

It is easy to see that the minimum weight among all the nonzero code words is 3. By Theorem 29.8, the minimum distance between code words is 3. So not only can a single-bit error be detected, it can be corrected. Since the distance between any two code words is at least 3, the code detects two-bit errors. However, the code does not correct two-bit errors since a two-bit error could produce a word with Hamming distance of one from another code word. For example, $(0, 0, 0, 0, 0, 0, 1)$ differs from the code word $(0, 0, 0, 1, 1, 0, 1)$ in two bits, but it differs from the code word $(0, 0, 0, 0, 0, 0, 0)$ in only one bit. ▲

$x^3 + x^2 + 1$	$x^4 + x^2 + x + 1$	0	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$x^4 + x^3 + x$	$x^5 + x^3 + x^2 + x$		
$x^5 + x^4 + x^2$	$x^6 + x^4 + x^3 + x^2$		
$x^6 + x^5 + x^3$	$x^5 + x^4 + x^3 + 1$		
$x^6 + x^4 + 1$	$x^6 + x^5 + x^4 + x$		
$x^5 + x + 1$	$x^6 + x^5 + x^2 + 1$		
$x^6 + x^2 + x$	$x^6 + x^3 + x + 1$		

29.14 Figure

(0,0,0,1,1,0,1)	(0,0,1,0,1,1,1)	(0,0,0,0,0,0,0)	(1,1,1,1,1,1,1)
(0,0,1,1,0,1,0)	(0,1,0,1,1,1,0)		
(0,1,1,0,1,0,0)	(1,0,1,1,1,0,0)		
(1,1,0,1,0,0,0)	(0,1,1,1,0,0,1)		
(1,0,1,0,0,0,1)	(1,1,1,0,0,1,0)		
(0,1,0,0,0,1,1)	(1,1,0,0,1,0,1)		
(1,0,0,0,1,1,0)	(1,0,0,1,0,1,1)		

29.15 Figure

Examples 29.2 and 29.13 each provide a code that can correct a one-bit error. Example 29.2 requires sending 24 bits to transmit a message of length 8. That is, the information rate is $\frac{1}{3}$. In Example 29.13, in order to transmit a message of length 8, 14 bits are required and the information rate is $\frac{4}{7}$. Clearly the code in Example 29.13 is a much more efficient way of coding data for transmission.

EXERCISES 29

1. If a code has word length 10 and transmission rate of $\frac{1}{2}$, how many code words are in the code?

2. If a linear code contains exactly 16 code words and the transmission rate is $\frac{2}{3}$, find the length of code words.

3. Find the smallest cyclic linear code C that contains $(1, 0, 0, 0, 0)$.

4. Find all cyclic linear codes C in $\mathbb{Z}_2^5$ that have a transmission rate of $\frac{2}{5}$.

5. Find all cyclic linear codes of length n for

a. $n = 2$ **b.** $n = 3$ **c.** $n = 4$

6. Determine whether each of the following is true or false.

a. A code is a subset of $\mathbb{Z}_2^n$ for some positive integer n.
b. The length of a code word in $\mathbb{Z}_2^n$ is n.
c. Every code is a linear code.
d. If the Hamming distance between any two different code words is at least 4, then the code corrects two-bit errors.
e. If C is a linear code in $\mathbb{Z}_2^n$, then the information rate is the number of elements in C divided by the number of elements in $\mathbb{Z}_2^n$.
f. Every linear code contains the code word consisting of all zeros.
g. If the Hamming distance between two code words in a linear code is d, then there is a code word with Hamming weight d.
h. The set $\{f(x)g(x) \mid f(x) \in \mathbb{Z}_2[x]\}$ is the polynomial code of length n generated by $g(x)$ if $g(x) \in \mathbb{Z}_2[x]$ and $g(x)$ has degree n.
i. Not every polynomial code is cyclic.
j. Every cyclic linear code contains at most two code words that remain the same when a cyclic shift is applied.

7. Let $g(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

a. Verify that $g(x)$ is a factor of $x^7 + 1$ in $\mathbb{Z}_2[x]$.
b. Find all the code words in the polynomial code C of length 7 generated by $g(x)$.
c. Determine if C detects single-bit errors and if so, determine if it corrects single-bit errors.
d. Determine if C detects two-bit errors and if so, determine if it corrects two-bit errors.

8. The transmission of a code word from the previous exercise produced the polynomial $p(x) = x^6 + x^5 + x^4 + x^3$. Was there a transmission error? If so, find the closest code word from C as measured by the Hamming distance.

9. Let $g(x) = x^6 + x^3 + 1 \in \mathbb{Z}_2[x]$.

a. Verify that $g(x)$ is a factor of $x^9 + 1$ in $\mathbb{Z}_2[x]$.

b. Find all the code words in the polynomial code C of length 9 generated by $g(x)$.

c. Determine if C detects single-bit errors and if so, determine if it corrects single-bit errors.

d. Determine if C detects two-bit errors and if so, determine if it corrects two-bit errors.

10. Let $g(x) = x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ and let C be the code generated by $g(x)$ with code word length 7.

a. Is C cyclic?

b. Find all the code words in the polynomial code C of length 7 generated by $g(x)$.

c. Can C detect one-bit errors and if so, can C correct one-bit errors?

d. Can C detect two-bit errors and if so, can C correct two-bit errors?

11. Find six polynomials $g(x) \in \mathbb{Z}_2[x]$ so that the code generated by $g(x)$ with code words of length 9 is a cyclic code.

12. If the minimal weight among all nonzero code words in a cyclic linear code $C \subseteq \mathbb{Z}_2^n$ is 1, prove that $C = \mathbb{Z}_2^n$.

13. Let $g(x)$ be a polynomial in $\mathbb{Z}_2[x]$. Prove that if the polynomial code C generated by $g(x)$ with length n is cyclic, then $g(x)$ is a factor of $x^n + 1$ in $\mathbb{Z}_2[x]$.

14. Let $C \subseteq \mathbb{Z}_2^n$ be a linear code with d the minimal weight among the nonzero code words. Determine necessary and sufficient conditions on d for C to correct k-bit errors.

15. Let $C \subseteq \mathbb{Z}_2^n$ be a linear code. Show that as a group, C is isomorphic with $\mathbb{Z}_2^k$ for some k.

16. Is there a polynomial $g(x) \in \mathbb{Z}_2[x]$ such that the code generated by $g(x)$ of length 9 is the same code as in Example 29.5? Prove your answer.

SECTION 30 HOMOMORPHISMS AND FACTOR RINGS

Factor Rings

In Section 12 we investigated which subgroups of a given groups could be used to form a factor group. In this section we wish to do an analogous construction on a ring to form a factor ring. We start with an example.

30.1 Example For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Thinking of $\mathbb{Z}$ as an abelian group, we know that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. As we have seen, $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ forms a group using addition defined by adding coset representatives. Furthermore, $\mathbb{Z}/n\mathbb{Z}$ is a ring where multiplication is defined by

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}.$$

We check that this multiplication is well defined. Let $a' \in a + n\mathbb{Z}$ and $b' \in b + n\mathbb{Z}$. Then $a' = a + nk$ and $b' = b + nr$ for some integers k and r. Thus

$$\begin{aligned} a'b' &= (a + nk)(b + nr) \\ &= ab + n(kb + knr) + anr \\ &= ab + n(kb + knr + ar) \\ &\in ab + n\mathbb{Z}. \end{aligned}$$

From this calculation we see that regardless of which representatives from $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ we pick, our product is in the coset $ab + n\mathbb{Z}$. So we have a well-defined multiplication on the cosets of $n\mathbb{Z}$. ▲