EXAMPLE 5.8

The (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$ has a minimum distance of 3. It is capable of detecting any combination of two or fewer random errors or any burst of length 3 or less. It also detects many bursts of length greater than 3.

5.5 DECODING OF CYCLIC CODES

Decoding of cyclic codes consists of the same three steps as for decoding linear codes: syndrome computation, association of the syndrome with an error pattern, and error correction. It was shown in Section 5.4 that syndromes for cyclic codes can be computed with a division circuit whose complexity is linearly proportional to the number of parity-check digits (i.e., $n - k$). The error-correction step is simply adding (modulo-2) the error pattern to the received vector. This addition can be performed with a single EXCLUSIVE-OR gate if correction is carried out serially (i.e., one digit at a time); n EXCLUSIVE-OR gates are required if correction is carried out in parallel, as shown in Figure 3.8. The association of the syndrome with an error pattern can be completely specified by a decoding table. A straightforward approach to the design of a decoding circuit is via a combinational logic circuit that implements the table-lookup procedure; however, the limit to this approach is that the complexity of the decoding circuit tends to grow exponentially with the code length and with the number of errors that are going to be corrected. Cyclic codes have considerable algebraic and geometric properties. If these properties are properly used, decoding circuits can be simplified.

The cyclic structure of a cyclic code allows us to decode a received vector $\mathbb{r}(X) = r_0 + r_1X + r_2X^2 + \cdots + r_{n-1}X^{n-1}$ serially. The received digits are decoded one at a time, and each digit is decoded with the same circuitry. As soon as the syndrome has been computed the decoding circuit checks whether the syndrome $\mathbb{s}(X)$ corresponds to a correctable error pattern $\mathbb{e}(X) = e_0 + e_1X + \cdots + e_{n-1}X^{n-1}$ with an error at the highest-order position X^{n-1} (i.e., $e_{n-1} = 1$). If $\mathbb{s}(X)$ does not correspond to an error pattern with $e_{n-1} = 1$, the received polynomial (stored in a buffer register) and the syndrome register are cyclically shifted once simultaneously. Thus, we obtain $\mathbb{r}^{(1)}(X) = r_{n-1} + r_0X + \cdots + r_{n-2}X^{n-1}$, and the new contents in the syndrome register form the syndrome $\mathbb{s}^{(1)}(X)$ of $\mathbb{r}^{(1)}(X)$. Now, the second digit r_{n-2} of $\mathbb{r}(X)$ becomes the first digit of $\mathbb{r}^{(1)}(X)$. The same decoding circuit will check whether $\mathbb{s}^{(1)}(X)$ corresponds to an error pattern with an error at location X^{n-1}.

If the syndrome $\mathbb{s}(X)$ of $\mathbb{r}(X)$ does correspond to an error pattern with an error at location X^{n-1} (i.e., $e_{n-1} = 1$), the first received digit r_{n-1} is an erroneous digit, and it must be corrected. The correction is carried out by taking the sum $r_{n-1} \oplus e_{n-1}$. This correction results in a modified received polynomial, denoted by $\mathbb{r}_1(X) = r_0 + r_1X + \cdots + r_{n-2}X^{n-2} + (r_{n-1} \oplus e_{n-1})X^{n-1}$. The effect of the error digit e_{n-1} on the syndrome is then removed from the syndrome $\mathbb{s}(X)$, by adding the syndrome of $\mathbb{e}'(X) = X^{n-1}$ to $\mathbb{s}(X)$. This sum is the syndrome of the modified received polynomial $\mathbb{r}_1(X)$. Now, $\mathbb{r}_1(X)$ and the syndrome register are cyclically shifted once simultaneously. This shift results in a received polynomial $\mathbb{r}_1^{(1)}(X) = (r_{n-1} \oplus e_{n-1}) + r_0X + \cdots + r_{n-2}X^{n-1}$. The syndrome $\mathbb{s}_1^{(1)}(X)$ of $\mathbb{r}_1^{(1)}(X)$ is the remainder resulting from dividing $X[\mathbb{s}(X) + X^{n-1}]$ by the generator polynomial

$\mathbf{g}(X)$. Because the remainders resulting from dividing $X\mathbf{s}(X)$ and X^n by $\mathbf{g}(X)$ are $\mathbf{s}^{(1)}(X)$ and 1, respectively, we have

$$\mathbf{s}_1^{(1)}(X) = \mathbf{s}^{(1)}(X) + 1.$$

Therefore, if 1 is added to the left end of the syndrome register while it is shifted, we obtain $\mathbf{s}_1^{(1)}(X)$. The decoding circuitry proceeds to decode the received digit r_{n-2}. The decoding of r_{n-2} and the other received digits is identical to the decoding of r_{n-1}. Whenever an error is detected and corrected, its effect on the syndrome is removed. The decoding stops after a total of n shifts. If $\mathbf{e}(X)$ is a correctable error pattern, the contents of the syndrome register should be zero at the end of the decoding operation, and the received vector $\mathbf{r}(X)$ has been correctly decoded. If the syndrome register does not contain all 0's at the end of the decoding process, an uncorrectable error pattern has been detected.

A general decoder for an (n, k) cyclic code is shown in Figure 5.8. It consists of three major parts: (1) a syndrome register, (2) an error-pattern detector, and (3) a buffer register to hold the received vector. The received polynomial is shifted into the syndrome register from the left end. To remove the effect of an error digit on the syndrome, we simply feed the error digit into the shift register from the left end through an EXCLUSIVE-OR gate. The decoding operation is as follows:

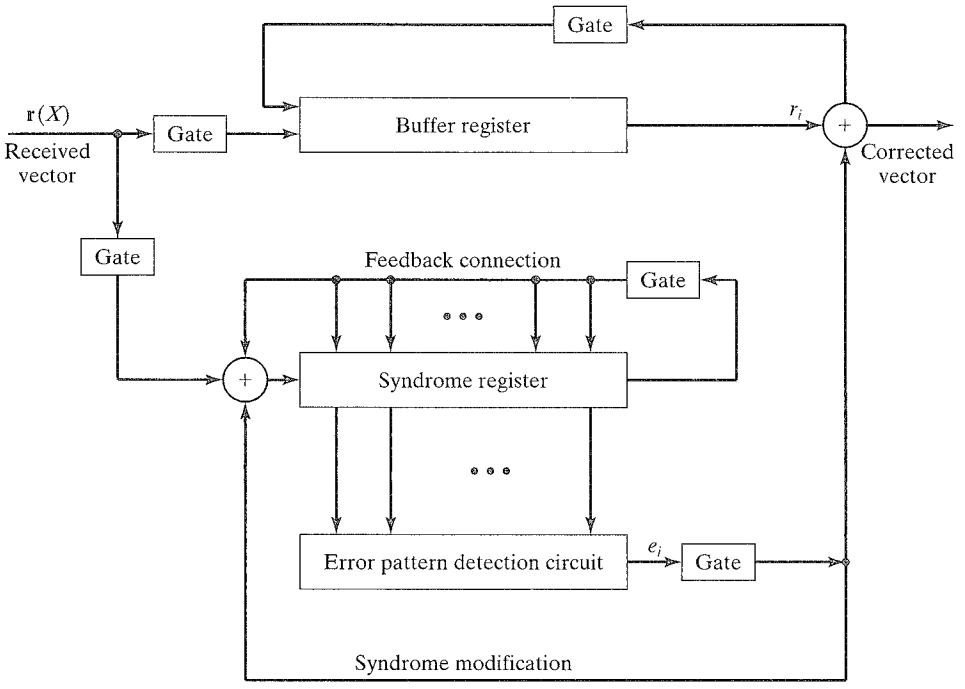

FIGURE 5.8: General cyclic code decoder with received polynomial $\mathbf{r}(X)$ shifted into the syndrome register from the left end.

Step 1. The syndrome is formed by shifting the entire received vector into the syndrome register. The received vector is simultaneously stored in the buffer register.

Step 2. The syndrome is read into the detector and is tested for the corresponding error pattern. The detector is a combinational logic circuit that is designed in such a way that its output is 1 if and only if the syndrome in the syndrome register corresponds to a correctable error pattern with an error at the highest-order position X^{n-1}. That is, if a 1 appears at the output of the detector, the received symbol in the rightmost stage of the buffer register is assumed to be erroneous and must be corrected; if a 0 appears at the output of the detector, the received symbol at the rightmost stage of the buffer register is assumed to be error-free, and no correction is necessary. Thus, the output of the detector is the estimated error value for the symbol to come out of the buffer.

Step 3. The first received symbol is read out of the buffer. At the same time, the syndrome register is shifted once. If the first received symbol is detected to be an erroneous symbol, it is then corrected by the output of the detector. The output of the detector is also fed back to the syndrome register to modify the syndrome (i.e., to remove the error effect from the syndrome). This operation results in a new syndrome, which corresponds to the altered received vector shifted one place to the right.

Step 4. The new syndrome formed in step 3 is used to detect whether the second received symbol (now at the rightmost stage of the buffer register) is an erroneous symbol. The decoder repeats steps 2 and 3. The second received symbol is corrected in exactly the same manner as the first received symbol was corrected.

Step 5. The decoder decodes the received vector symbol by symbol in the manner outlined until the entire received vector is read out of the buffer register.

The preceding decoder is known as a Meggitt decoder [11], which applies in principle to any cyclic code. But whether it is practical depends entirely on its error-pattern detection circuit. In some cases the error-pattern detection circuits are simple. Several of these cases are discussed in subsequent chapters.

EXAMPLE 5.9

Consider the decoding of the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$. This code has a minimum distance of 3 and is capable of correcting any single error over a block of seven digits. There are seven single-error patterns. These seven error patterns and the all-zero vector form all the coset leaders of the decoding table. Thus, they form all the correctable error patterns. Suppose that the received polynomial $r(X) = r_0 + r_1X + r_2X^2 + r_3X^3 + r_4X^4 + r_5X^5 + r_6X^6$ is shifted into the syndrome register from the left end. The seven single-error patterns and their corresponding syndrome are listed in Table 5.4.

TABLE 5.4: Error patterns and their syndromes with the received polynomial $\mathbf{r}(X)$ shifted into the syndrome register from the left end.

Error pattern $\mathbf{e}(X)$	Syndrome $\mathbf{s}(X)$	Syndrome vector (s_0, s_1, s_2)
$\mathbf{e}_6(X) = X^6$	$\mathbf{s}(X) = 1 + X^2$	(1 0 1)
$\mathbf{e}_5(X) = X^5$	$\mathbf{s}(X) = 1 + X + X^2$	(1 1 1)
$\mathbf{e}_4(X) = X^4$	$\mathbf{s}(X) = X + X^2$	(0 1 1)
$\mathbf{e}_3(X) = X^3$	$\mathbf{s}(X) = 1 + X$	(1 1 0)
$\mathbf{e}_2(X) = X^2$	$\mathbf{s}(X) = X^2$	(0 0 1)
$\mathbf{e}_1(X) = X^1$	$\mathbf{s}(X) = X$	(0 1 0)
$\mathbf{e}_0(X) = X^0$	$\mathbf{s}(X) = 1$	(1 0 0)

We see that $\mathbf{e}_6(X) = X^6$ is the only error pattern with an error at location X^6. When this error pattern occurs, the syndrome in the syndrome register will be (1 0 1) after the entire received polynomial $\mathbf{r}(X)$ has entered the syndrome register. The detection of this syndrome indicates that r_6 is an erroneous digit and must be corrected. Suppose that the single error occurs at location X^i [i.e., $\mathbf{e}_i(X) = X^i$] for $0 \leq i < 6$. After the entire received polynomial has been shifted into the syndrome register, the syndrome in the register will not be (1 0 1); however, after another $6 - i$ shifts, the contents in the syndrome register will be (1 0 1), and the next received digit to come out of the buffer register will be the erroneous digit. Therefore, only the syndrome (1 0 1) needs to be detected, and this can be accomplished with a single three-input AND gate. The complete decoding circuit is shown in Figure 5.9. Figure 5.10 illustrates the decoding process. Suppose that the codeword $\mathbf{v} = (1\,0\,0\,1\,0\,1\,1)$ [or $\mathbf{v}(X) = 1 + X^3 + X^5 + X^6$] is transmitted and $\mathbf{r} = (1\,0\,1\,1\,0\,1\,1)$ [or $\mathbf{r}(X) = 1 + X^2 + X^3 + X^5 + X^6$] is received. A single error occurs at location X^2. When the entire received polynomial has been shifted into the syndrome and buffer registers, the syndrome register contains (0 0 1). In Figure 5.10, the contents in the syndrome register and the contents in the buffer register are recorded after each shift. Also, there is a pointer to indicate the error location after each shift. We see that after four more shifts the contents in the syndrome register are (1 0 1), and the erroneous digit r_2 is the next digit to come out from the buffer register.

The (7, 4) cyclic code considered in Example 5.9 is the same code considered in Example 3.9. Comparing the decoding circuit shown in Figure 3.9 with the decoding circuit shown in Figure 5.9, we see that the circuit shown in Figure 5.9 is simpler than the circuit shown in Figure 3.9. Thus, the cyclic structure does simplify the decoding circuit; however, the circuit shown in Figure 5.9 takes a longer time to decode a received vector because the decoding is carried out serially. In general, there is a trade-off between speed and simplicity, as they cannot be achieved at the same time.

The Meggitt decoder described decodes a received polynomial $\mathbf{r}(X) = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1}$ from the highest-order received digit r_{n-1} to the lowest-order received digit r_0. After decoding the received digit r_i, both the buffer and syndrome

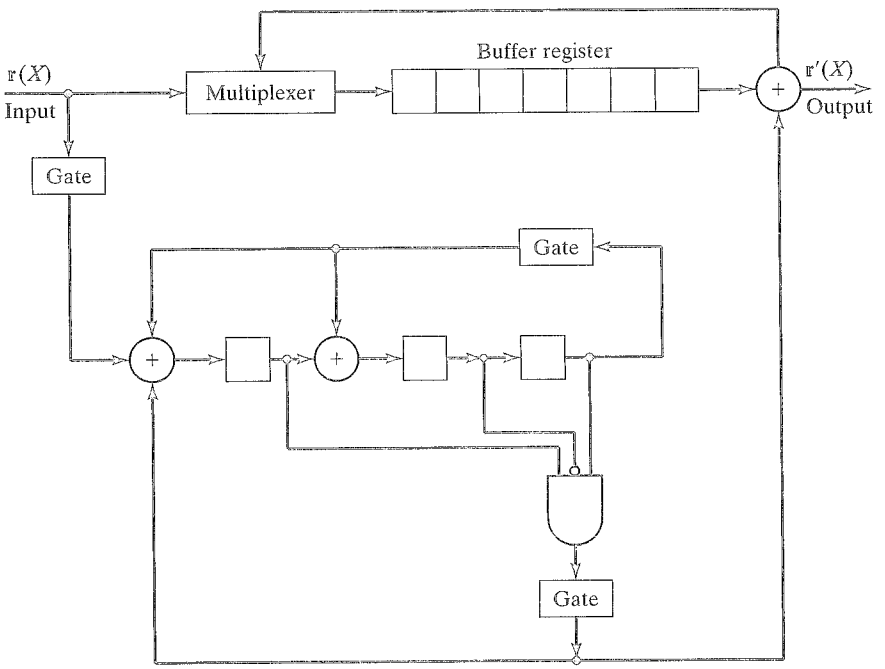

FIGURE 5.9: Decoding circuit for the $(7, 4)$ cyclic code generated by $g(X) = 1+X+X^3$.

registers are shifted once to the right. The next received digit to be decoded is r_{i-1}. It is possible to implement a Meggitt decoder to decode a received polynomial in the reverse order (i.e., to decode a received polynomial from the lowest-order received digit r_0 to the highest-order received digit r_{n-1}). After decoding the received digit r_i, both the buffer and syndrome registers are shifted once to the left. The next received digit to be decoded is r_{i+1}. The details of this decoding of a received polynomial in reverse order are left as an exercise.

To decode a cyclic code, the received polynomial $r(X)$ may be shifted into the syndrome register from the right end for computing the syndrome. When $r(X)$ has been shifted into the syndrome register, the register contains $s^{(n-k)}(X)$, which is the syndrome of $r^{(n-k)}(X)$, the $(n-k)$th cyclic shift of $r(X)$. If $s^{(n-k)}(X)$ corresponds to an error pattern $e(X)$ with $e_{n-1} = 1$, the highest-order digit r_{n-1} of $r(X)$ is erroneous and must be corrected. In $r^{(n-k)}(X)$, the digit r_{n-1} is at the location X^{n-k-1}. When r_{n-1} is corrected, the error effect must be removed from $s^{(n-k)}(X)$. The new syndrome, denoted by $s_1^{(n-k)}(X)$, is the sum of $s^{(n-k)}(X)$ and the remainder $\rho(X)$ resulting from dividing X^{n-k-1} by the generator polynomial $g(X)$. Because the degree of X^{n-k-1} is less than the degree of $g(X)$,

$$\rho(X) = X^{n-k-1}.$$

Therefore,

$$s_1^{(n-k)}(X) = s^{(n-k)}(X) + X^{n-k-1},$$

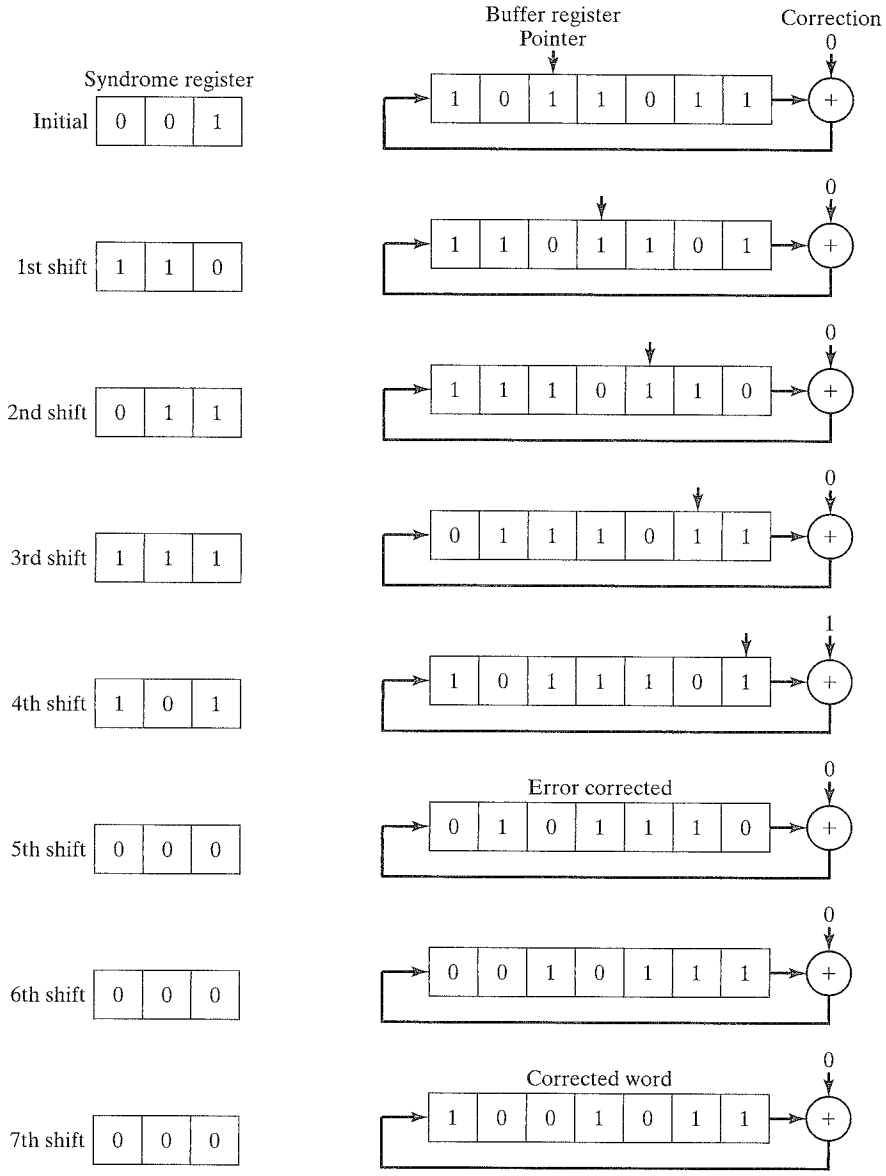

FIGURE 5.10: Error-correction process of the circuit shown in Figure 5.9.

which indicates that the effect of an error at the location X^{n-1} on the syndrome can be removed by feeding the error digit into the syndrome register from the right end through an EXCLUSIVE-OR gate, as shown in Figure 5.11. The decoding process of the decoder shown in Figure 5.11 is identical to the decoding process of the decoder shown in Figure 5.8.