Besides the code rate, other important parameters are the code distance and the weight of particular codewords. These are defined below.

Distance of a Code — The distance between two codewords is the number of elements in which two codewords C_i and C_j differ

$$d(C_i, C_j) = \sum_{l=1}^{N} C_{i,l} \oplus C_{j,l} \, (modulo \; q) \tag{7.84}$$

where d is the distance between the codewords and q is the total number of possible values of C_i and C_j. The length of each codeword is N elements or characters. If the code used is binary, the distance is known as the *Hamming distance*. The minimum distance d_{min} is the smallest distance for the given codeword set and is given as

$$d_{min} = Min\{d(C_i, C_j)\} \tag{7.85}$$

Weight of a Code — The weight of a codeword of length N is given by the number of nonzero elements in the codeword. For a binary code, the weight is basically the number of 1s in the codeword and is given as

$$w(C_i) = \sum_{l=1}^{N} C_{i,l} \tag{7.86}$$

Properties of Block Codes

Linearity — Suppose C_i and C_j are two codewords in an (n, k) block code. Let α_1 and α_2 be any two elements selected from the alphabet. Then the code is said to be linear if and only if $\alpha_1 C_1 + \alpha_2 C_2$ is also a code word. A linear code must contain the all-zero code word. Consequently, a constant-weight code is nonlinear.

Systematic — A systematic code is one in which the parity bits are appended to the end of the information bits. For an (n, k) code, the first k bits are identical to the information bits, and the remaining $n - k$ bits of each code word are linear combinations of the k information bits.

Cyclic — Cyclic codes are a subset of the class of linear codes, which satisfy the following cyclic shift property: If $C = [c_{n-1}, c_{n-2}, ..., c_0]$ is a codeword of a cyclic code, then $[c_{n-2}, c_{n-3}, ..., c_0, c_{n-1}]$, obtained by a cyclic shift of the elements of C, is also a code word [Pro89]. In other words, all cyclic shifts of C are code words. From the cyclic property, the codes possess a great deal of structure which is exploited to greatly simplify the encoding and decoding operations.

Encoding and decoding techniques make use of the mathematical constructs know as *finite fields*. Finite fields are algebraic systems that contain a finite set of elements. Addition, subtraction, multiplication, and division of finite field elements are accomplished without leaving the