36. Examples and Modifications of Linear Block Codes

Examples of Binary Linear Block Codes

The problem of finding a code with a given degree of error protection reduces to that of finding a code with a given minimum distance. Unfortunately, there is no general rule for finding codes with a given $d_{\min}$. The construction of some simple and well-known binary linear block codes is presented here [1].

36.1 Repetition Codes

Repetition is the simplest form of error protection. Each information digit may be transmitted n times. The generator and parity-check matrices of an (n, 1) binary repetition block code are

$$\mathbf{G} = [1\ 1\ ...\ 1] \tag{36.1}$$

and

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{bmatrix} \tag{36.2}$$

respectively. It can be seen that the minimum Hamming distance of an (n, 1) repetition block code is n. In general, n transmissions of the same digit enable n-1 errors to be detected, or $\leq (n-1)/2$ errors to be corrected.

36.2 Single-Parity-Check Codes

A single-parity-check code of block length n may be formed by taking a parity-check over $k = n$-1 information digits. The parity-check digit v_{n-1} may be written as

$$v_{n-1} = u_0 + u_1 + ... + u_{k-1} \tag{36.3}$$

where + implies modulo-2 addition. We choose an even-parity rule so that each codeword has an even number of ones. The generator and parity-check matrices of an (n, n - 1) binary single-parity-check block code are

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 \end{bmatrix} \tag{36.4}$$

and

$$\mathbf{H} = [1\ 1\ \ldots\ 1] \tag{36.5}$$

respectively. Single, triple, and all odd number of errors in the block n may be detected. The coding rate is

$$R_C = (n\text{-}1) / n \tag{36.6}$$

As n goes to infinity, the code rate goes to 1. The code was very widely used for computer punched tape.

Example 36.1

The generator and parity-check matrices of an (3, 2) binary single-parity-check code are $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ and $\mathbf{H} = [1\ \ 1\ \ 1]$, respectively. If the input information sequence is $\mathbf{U} = [1\ 1]$, the encoded code sequence is $\mathbf{V} = \mathbf{U}\ \mathbf{G} = [1\ 1\ 0]$.

36.3 Single-Error-Correcting Hamming Codes

R. W. Hamming found an optimum class of single-error correcting codes in 1950 [2]. The code was used for long-distance telephony. For some integers $c \geq 2$, the family of binary Hamming codes has the following parameters:

Block length :	$n = 2^c - 1$
Information digits :	$k = 2^c - c - 1$
Number of check digits :	$c = n - k$
Minimum distance :	$d_{\min} = 3$
Error correcting capability :	$t' = 1$.

To construct the parity-check matrix of an (n, k) binary Hamming code, we simply place all non-zero binary c-tuples in the columns of the c-by-n parity-check matrix in any order.

For example, the parity-check and the corresponding generator matrices of an (7, 4) single-error-correcting binary Hamming code are

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{36.7}$$

and

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{36.8}$$

If the input information sequence is **U** = [0 1 1 1] , the encoded code sequence is **V** = **U G** = [0 1 1 1 0 1 0].

Modifications of Linear Block Codes

To suit a particular application, the parameters n and k may need modifications. An (n, k) block code can be augmented, expurgated, extended, punctured, lengthened, or shortened. In all cases, the minimum Hamming distance property of the code may change after the modifications. These six basic modifications are briefly explained as follows:

Augmenting a code. An (n, k) code may be augmented by adding new codewords. The process increases the number of information symbols without changing the codeword length. This corresponds to increasing the number of rows of the generator matrix. Augmentation has very little to offer in most practical applications.

Expurgating a code. An (n, k) code may be expurgated by discarding some of the codewords from the code. This process is the inverse of augmenting a code. It decreases the number of information symbols without changing the codeword length. This corresponds to decreasing the number of rows of the generator matrix.

Extending a code. An (n, k) code can be extended by annexing parity-check symbols to every codeword of the code. The additional parity-check symbols are carefully chosen to improve the minimum distance of the code. The process increases the codeword length without changing the number of information symbols. This corresponds to increasing the number of columns of the generator matrix. The most common modification is the addition of a 0 parity-check symbol to every codeword of an (n, k) block code with even weight, and a 1 parity-check symbol to every codeword with odd weight. In terms of the parity-check matrix, a column of zeros followed by a row of ones are adding to the parity-check matrix of the (n, k) code. If the minimum distance, $d_{\min}$, of the (n, k) code was odd, the new minimum distance is $d_{\min} + 1$.

Example 36.2

Annexing a parity-check symbol to the (7, 4) binary Hamming code of $\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$, we get an (8, 4) extended binary Hamming code of $\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$. The extended binary Hamming code is formed by adding a column of zeros followed by a row of ones to the parity-check matrix of the binary Hamming code. The binary Hamming code has a minimum Hamming distance of 3 and the extended binary Hamming code has a minimum Hamming distance of 4.

Puncturing a code. An (n, k) code can be punctured by deleting one or more code symbols of the (n, k) code. This process is the inverse of extending a code. It decreases the codeword length without changing the number of information symbols. This corresponds to decreasing the number of columns of the generator matrix. The minimum distance may decrease as a result of the puncturing operation.

Example 36.3

Deleting the last column from the generator matrix $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$ of an (8, 4) binary code, we get an (7, 4) punctured binary code of $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. Both codes have the same minimum Hamming distance of 3.

Lengthening a code. Given an (n, k) block code, it is possible to form an $(n + i, k + i)$ block code by adding i extra information symbols. The lengths of the information vector and the codeword are increased by the same amount. This corresponds to increasing the number of rows and columns of the generator matrix by i. In practice, lengthening a code is rarely used.

Shortening a code. Given an (n, k) block code, it is always possible to form an (n- i, k - i) block code by making the i leading information symbols identically 0 and omitting them from all code vectors. This is equivalent to omitting the first i rows and columns of the generator matrix **G**. This process is the inverse of lengthening a code. The lengths of the information vector and the codeword are decreased by the same amount.

Example 36.4

Deleting the first row and the first column in the generator matrix $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ of the (7, 4) binary Hamming code, we get an (6, 3) shortened binary code of $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. Both codes have the same minimum Hamming distance of 3.

The encoder circuit for an (n, k) block code can be used to encode an (n- i, k - i) shortened block code by making the i leading information symbols identically 0 and omitting them from all code vectors before the transmission.

References

[1] Lee, L. H. C., Error-Control Block Codes for Communications Engineers, Artech House, 2000.

[2] Hamming, R. W., "Error Detecting and Error Correcting Codes," *Bell System Technical Journal*, Vol. 29, April 1950, pp. 147-160.