

Definition 1. Linear Code

An (n, k) linear code over a finite field F is a k -dimensional subspace V of the vector space

$$F^n = \underbrace{F \oplus F \oplus \cdots \oplus F}_{n \text{ copies}}$$

over F . The members of V are called the *code words*. The ratio k/n is called the *information rate* of the code. When F is \mathbb{Z}_2 , the code is called binary.

Example 1. The Hamming (7,4) Code

Assuming that our message consists of all possible 4-tuples of 0's and 1's (i.e., we wish to send a sequence of 0's and 1's of length 4). Encoding will be done by viewing these messages as four-dimensional vectors over the field \mathbb{Z}_2 and multiplying each of the 16 possible messages on the right by the matrix

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

The resulting seven-dimensional vectors are called *code words*. See Table 1.

Message	Encoder G	Code Word
0000	→	0000000
0001	→	0001111
0010	→	0010110
0100	→	0100101
1000	→	1000011
1100	→	1100110
1010	→	1010101
1001	→	1001100
0110	→	0110011
0101	→	0101010
0011	→	0011001
1110	→	1110000
1101	→	1101001
1011	→	1011010
0111	→	0111100
1111	→	1111111

Table 1

Definition 2. Hamming Distance, Hamming Weight

The *Hamming distance* between two vectors of a vector space is the number of components in which they differ. The *Hamming weight* of a vector is the number of nonzero components of the vector.

We will use $d(u, v)$ to denote the Hamming distance between the vectors u and v and $\text{wt}(u)$ for the Hamming weight of the vector u .

Theorem 1. Properties of Hamming Distance and Hamming Weight

For any vectors u, v and w of a linear code, $d(u, v) \leq d(u, w) + d(w, v)$ and $d(u, v) = \text{wt}(u - v)$.

Theorem 2. Correcting Capability of a Linear Code

If the Hamming weight of every nonzero code word in a linear code is at least $2t+1$, then the code can correct for any t or fewer errors. Furthermore, the same code can detect any $2t$ or fewer errors..

Theorem 3. *Singleton Bound*

Let C be a code of length n over an alphabet of size q with minimum Hamming distance d . Then $|C| \leq q^{n-d+1}$.

Definition 3. Maximum Distance Separable code

A code of length n over an alphabet of size q with $|C| = q^k$ and minimum Hamming distance d satisfying $k = n - d + 1$ is said to be a Maximal Distance Separable (MDS) code.

Theorem 4. *Sphere Packing Bound*

Let C be a code of length n over an alphabet of size q with minimum Hamming distance $2t + 1$. Then

$$|C| \left(\sum_{s=0}^t \binom{n}{s} (q-1)^s \right) \leq q^n$$

Theorem 5. If C is a linear code over a ring R , the t th minimum Hamming distance and the minimum Hamming weight are equal.

Definition 4. Generator Matrix

A Generator Matrix is any $k \times n$ matrix G whose rows form a basis for C .

Definition 5. Parity-check Matrix

A parity-check matrix H is a $(n-k) \times n$ matrix, for a (n, k) code C , defined by

$$C = \{x \in \mathbb{F}_q^n \mid Hx^T = 0\}.$$

Note that C is the kernel of the linear transformation H , because a linear code is a subspace of a vector space.

Theorem 6. If $G = [I_k \mid A]$ is a generator matrix for the (n, k) code C in standard form, then $H = [-A^T \mid I_{n-k}]$ is a parity check matrix for C .

Definition 6. Let R be a finite ring. A linear code C over the alphabet R of length n is a submodule of R^n .

Note: If R is a field then the linear codes are vector spaces and we have the full force of linear algebra at our disposal!