# A Note on Hamming Code

**Dr Aruna M. Kulkarni**
Department of Mathematics,
Smt. S.K.Gandhi Arts, Amolak Science and
P.H. Gandhi Commerce College, Kada
Dist. Beed (M.S.)
Email- abhiarud@gmail.com

**Abstract**

Richard W. Hamming, mathematician and computer scientist, Introduced error correcting and error detecting codes known as Hamming codes. It requires adding additional parity bits with the data. Here message encoding and decoding method that is reliable, efficient, reasonable and easy to implement. The role of the interaction between human and computer in the world of contemporary communication is considered, together with an emphasis on Hamming's fundamental contributions from information theory to computer technology. Hamming code, Hamming distance, Hamming weight are now standard terms that reflect him as a leader in the development of coding theory. His ideas in coding theory continue to have practical use in computer design.

*Key words- Hamming code, parity bits*

**Introduction**:

Richard W Hamming was born on February 11, 1915. He was one of the first users of early electronic computers. Richard Hamming published his famous work on error detecting and error correcting codes. This work started a branch of information theory. The Hamming codes are used in many modern computers. Hamming code is an error correction system that can detect and correct errors when data is stored or transmitted. It requires adding additional parity bits with the data. Whenever data is transmitted or stored, it's possible that the data may become corrupted. This can take the form of bit flips, where a binary1 becomes a 0 or vice versa. Error correcting codes seek to find when an error is introduced into some data. This is done by adding parity bits, or redundant information, to the data.

**2 Preliminaries**

In this section, we present some definitions and theorems which are useful in further development of this paper.

Definition- 2.1 Hamming Code

$(n, k)$ Hamming Code is a code in coding theory where $n$ is the code length and $k$ is the message length. (7, 4) is one of the simplest Hamming code.

Definition- 2.2 Hamming Distance

The Hamming Distance between two vectors of a vector space is the number of components in which they differ.

Definition- 2.3 Hamming Weight

The Hamming Weight of a vector is the number of nonzero components of the vector.

Example- Let $s = 0010111,\ v = 1101101$

Then $d(s, v)$= 5

$$wt(s) = 4, wt(v) = 5$$

Theorem 2.1- For any vectors $u, v\ and\ w,\ d(u, v) \leq\ d(u, w)$+ $d(w, v)$

And $d(u, v) =\ wt(u - v)$

Theorem 2.2- Correcting capability of Linear code

If the Hamming Weight of a linear code is at least $2t + 1$, then the code can correct any1 or fewer errors. Alternatively, the same code can detect any $2t$ or fewer errors.

Standard Generator Matrix – We can find a matrix G that carries a subspace $V\ of\ F^k$ to a subspace of $F^n$ in such a way that for any k- tuple $v\ in\ V$, the vector $vG$

Will agree with $v$ in the first k components and build in some redundancy in the last $n - k$ components. This matrix is $k \times n$ matrix of the form

$$\begin{bmatrix} 1 & 0 \ldots\ldots.. & 0 & a_{11} & \ldots\ldots\ldots & a_{1n-k} \\ 0 & 1 \ldots\ldots.. & 0 & . & \ldots\ldots\ldots.. & . \\ 0 & 0 \ldots\ldots.. & 0 & . & \ldots\ldots\ldots\ldots & . \\ 0 & 0 \ldots\ldots.. & 1 & a_{k1} & \ldots\ldots\ldots\ldots.. & a_{kn-k} \end{bmatrix}$$

Where the $a_{ij}$ belong to $F$ is called the standard generator matrix.

Example- Determination of the Hamming (7, 4) code with Generator matrix

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

Now our message set consist of all possible 4-tuplesof 0's and 1's that is we wish to send a sequence of 0's and 1's of length 4. Encoding will be done by viewing these messages as $1 \times 4$ matrices with entries from $Z_2$ and multiplying each of 16 messages on the right by the matrix $G$. All arithmetic is done modulo 2. The resulting 7-tuples are called code words.

| Message | Encoder $G$ | Code word | Message | Encoder $G$ | Code word |
|---|---|---|---|---|---|
| 0000 | → | 0000000 | 0110 | → | 0110010 |
| 0001 | → | 0001011 | 0101 | → | 0101110 |
| 0010 | → | 0010111 | 0011 | → | 0011100 |
| 0100 | → | 0100101 | 1110 | → | 1110100 |
| 1000 | → | 1000110 | 1101 | → | 1101000 |
| 1100 | → | 1100011 | 1011 | → | 1011010 |
| 1010 | → | 1010001 | 0111 | → | 0111001 |
| 1001 | → | 1001101 | 1111 | → | 1111111 |

Notice that the first four digits of each code word constitute just the original message corresponding to the code word. The last three digits of the code word constitute redundancy features. For this code we use nearest –neighbor decoding method decoding method. For any received word $v$ we assume that the word sent is the code word $v'$, which differs from $v$ in the fewest number of positions. If choice of $v'$ is not unique we can decide not to decode or arbitrarily choose one of the code words closest to $v$. Once we have decoded the received word, it obtain the massage by deleting the last three digits of $v'$.

For example suppose that $1000$ were the intended message. It would be encoded and transmitted as $u = 1000110$. If the received word were $v = 1100110$, error is in second position. It would still be decoded as $u$, since $v$ and $u$ differ in only one position, whereas $v$ and any other code word differ in at least two positions.

Parity check Matrix Decoding

Suppose that $V$ is a systematic linear code over the field $F$ given by the standard generator matrix $G = [I_k|A]$, where $I_k$ represents $k \times k$ identity matrix and $A$ is the $k \times (n-k)$ matrix obtained from $G$ by deleting the first $k$ columns of $G$.

Then the $n \times (n-k)$ matrix

$$H = \left[\frac{-A}{I_{n-k}}\right]$$

Where $-A$ is the negative of $A$ and $I_{n-k}$ is $(n-k) \times (n-k)$ identity matrix, is called the parity check matrix $V$.

The decoding done as

1. For any received word $w$ compute $wH$.
2. If $wH$ is the zero vector, assume that no error was made.
3. For the binary code, if $wH$ is the

Example-

Find all code words of the (7, 4) binary linear code whose generator matrix is

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

Find the parity check matrix of this code. Will this code correct any single error?

With respect to given generator matrix, all code words of the (7,4) binary linear code are given as

| Message | Encoder $G$ | Code word | Message | Encoder $G$ | Code word |
|---|---|---|---|---|---|
| 0000 | → | 0000000 | 0110 | → | 0110011 |
| 0001 | → | 0001011 | 0101 | → | 0101110 |
| 0010 | → | 0010110 | 0011 | → | 0011101 |
| 0100 | → | 0100101 | 1110 | → | 1110100 |
| 1000 | → | 1000111 | 1101 | → | 1101001 |
| 1100 | → | 1100010 | 1011 | → | 1011010 |
| 1010 | → | 1010001 | 0111 | → | 0111000 |
| 1001 | → | 1001100 | 1111 | → | 1111111 |

The parity check matrix is given by

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

**Conclusion –**

Hamming code system is very much important where we need only one error correction and two error detection system. It is very easy to implement and for large number of block of bits it is more efficient.

**References-**

1] Contemporary Abstract Algebra by Joseph Gallian.

2] “Notes on Coding Theory” by J.I. Hall

http://www.mth.msu.edu/jhall/classes/codenotes/coding-notes.html

3] The Art of Error Correcting Coding by Robert H. Morelos- Zaragoza.

4] Error Correcting Coding, mathematical methods and Algorithm by Todd K. Moon.