Hamming and Golay Codes

Satish kumar Buddha
Indiana State University
Terre Haute,IN 47809 , USA

December 14, 2011

Abstract

This project is about error detection and correction using hamming and golay codes.

An error-correcting code is a technique where the message is expressed in the form of numbers in which the errors can be detected and corrected based on the pattern of the remaining numbers. There are many methods for detecting the errors occurred after transmission, whereas only few can correct them. Hamming codes and Golay codes are the technique which helps in detecting and also correcting the errors in the code. Hamming codes are the error correcting codes that helps to correct bit errors, it helps to detect .(d-1). bit errors and correct .((d-1)/2).bit errors; where.d. is the hamming distance between the pairs of the code words. Golay codes are the perfect linear error correcting codes which also helps to detect and correct the errors in the code. There are two types of Golay codes binary golay code (G_{23}(23,12,7)) and ternary golay code(G_{11}(11,6,5) and it is the unique code with these parameters. .

1 Statement Of The Problem

An error-correcting code is a technique where the message is expressed in the form of numbers in which the errors can be detected and corrected based on the pattern of the remaining numbers. Hamming code is the linear error correcting code which helps in detecting and correcting single bit errors occurred when transmission of data. Binary golay code encodes 12 bits of data in a 24-bit word in such a way that any triple-bit error can be corrected and any quadruple-bit error can be detected.

2 History

An error-correcting code is a technique where the message is expressed in the form of numbers in which the errors can be detected and corrected based on the pattern of the remaining numbers. The study of error-correcting codes is called as coding theory.

Hamming code is named for R. W. Hamming of Bell Labs. His search for error- correcting codes led to the Hamming Codes, correcting codes led to the Hamming Codes, perfect 1-error correcting codes, and the perfect 1- error correcting codes, and the extended Hamming Codes, 1-error correcting extended Hamming Codes, 1-error correcting and 2-error detecting codes and 2-error detecting code. Hamming Codes are still widely used in computing, telecommunication, in computing, telecommunication, and other applications and other applications.

In 1949 Marcel Golay (specialist of radars) produced two remarkably efficient codes called the Golay code. There are two Golay codes the ternary cyclic code G_{11} and the binary cyclic code G_{23}.

3 Definitions

Error Detection
Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver.

Error Correction
Error correction is the detection of errors and reconstruction of the original, error-free data.

Convolutional code An encoder for a binary block code takes a block of information bits and converts it into a block of transmitted bits (a code word). A binary convolutional encoder takes a stream of information bits and converts it into a stream of transmitted bits, using a shift register bank.

Black codes
A block code is a code that uses sequences of n symbols, for some positive integer n. Each sequence of length n is a code word or code block, and contains k information digits (or bits). The remaining n- k digits in the code word are called redundant digits or parity-check bits.

Hamming distance: The minimum number of bits that must be changed in order to convert one bit string into another.

Weight: The count of bits which are ones in a binary word. For

example, the weight of the byte 01011011 is five since it contains five 1s.

4 Error detection and correction schemes

The following are the error detecting and correcting schemes.

Error detecting schemes:

1. Repetition codes.
2. Parity bits
3. Checksums
4. Cyclic redundancy checks (CRCs)
5. Cryptographic hash functions

Error correcting schemes:

1. Automatic repeat request
2. Error-correcting code
3. Hybrid schemes

5 Algorithm for Hamming codes

The following general algorithm generates a single-error correcting (SEC) code for any number of bits.

1. Number the bits starting from 1: bit 1, 2, 3, 4, 5, etc.
2. Write the bit numbers in binary. 1, 10, 11, 100, 101, etc
3. All bit positions that are powers of two (have only one 1 bit in the binary form of their position) are parity bits.
4. All other bit positions, with two or more 1 bits in the binary form of their position, are data bits.
5. Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.
    a. Parity bit 1 covers all bit positions which have the least significant bit set: bit 1 (the parity bit itself), 3, 5, 7, 9, etc.
    b. Parity bit 2 covers all bit positions which have the second least significant bit set: bit 2 (the parity bit itself), 3, 6, 7, 10, 11, etc.

c. Parity bit 4 covers all bit positions which have the third least significant bit set: bits 4.7, 12.15, 20.23, etc.
d. Parity bit 8 covers all bit positions which have the fourth least significant bit set: bits 8.15, 24.31, 40.47, etc.
e. In general each parity bit covers all bits where the binary AND of the parity position and the bit position is non-zero.

6 Golay codes

7 Algorithm for Golay codes

1. Receive a codeword.
2. Compute syndrome s=r∗transpose(H) and its weight w(s)
3. If w(s)=0, then go to End.
4. If w(s).t, then c=r−(s<<k), and go to End.
5. Searching table, if s is in table. If s is in table, then C=r−ei, and go to end
6. Compute $sd = s - si$, and compute the weight of syndrome difference w(sd).
7. if $w(sd).1$, then $c = r - (sd << k) - ei$, and go to end
8. $r.$=(left cyclic shift n-k bits) r, and compute syndrome $s. = r.HT$and its weight w(s)
9. If $w(s.) = t$, then $c = r - (s << k)$, then $c. = r. - (s. << k)$.
10. c=(right cyclic shift n-k bits) c., and go to End.
11. Compute $sd. = s. - si$, and compute $c. = r. - (s. << k) - ei.$. Go to Step 10.

8 Example Implementing Decoding algorithm of Golay code

Decoding three errors of (23, 12, 7) Cyclic code. A message m=(100000000000) is encoded into a codeword c=(10101110001100000000000) by an encoder. If the received codeword is r =(10111110001100010001000), then the decoding procedure is:

1. Receive a codeword r=(10111110001100010001000), go to Step 2.
2. Compute syndrome $s = r * H^T$ =(10000110010) and its weight w(s)=4, go to Step 3.
3. w(s).0, go to Step 4.
4. $w(s) > 3$, go to Step 5.
5. s is not in table, go to Step 6.
6. Compute $sd = s - si = s - s46 = (10000110010) - (10010110010) =$ (00010000000) and compute the weight of syndrome difference $w(sd) =$ 1, go to Step7.
7. $w(sd).1, soc = r - (sd << k) - ei = r - (sd << 12) - e46 =$ (10111110001100010001000)−((00010000000) << 12)−(00000000000000010001000) = (10101110001100000000000), go to end.

9 Flowchart

Flowchart to decode golay codes.

10 Time Complexity

The time complexity for hamming codes is 0(n2) since it is multiplication of two matrices The time complexity for golay binary code is as follows 0(n) for calculating syndrome that is calculating error.

References

[1] Vera Pless *Introduction to the theory of error-correcting codes*

[2] David J.C MacKay, , *Inference, and Learning Algorithms,year = 2003.*

[3] Homan, D. G., and Leonard, D, "Coding Theory: The Essentials, year = 1991.

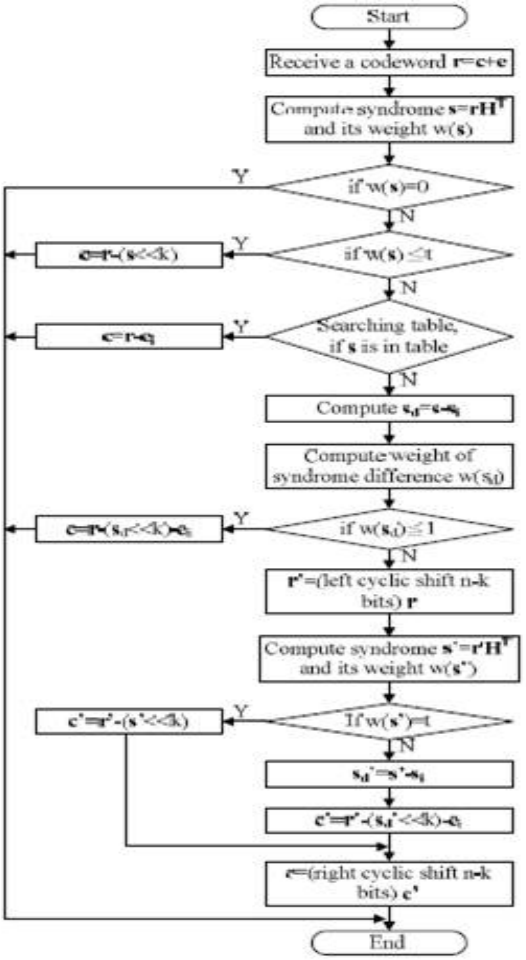

Figure 1: Decoding algorithm for golay codes