DESIGN OF HAMMING CODE FOR 64 BIT SINGLE ERROR DETECTION AND CORRECTION USING VHDL

Adham Hadi Saleh
Assistant Lecturer, Department of Electronic engineering, College of Engineering, University of Diyala
adham.hadi@yahoo.com
(Received: 16/2/2014; Accepted: 21/9/2014)

ABSTRACT: - Hamming code is an efficient error detection and correction technique which can be used to detect single and burst errors, and correct errors. In communication system information data transferred from source to destination by channel, which may be corrupted due to a noise. So to find original information we use Hamming code.

In this paper, we have described how we can generate 7 redundancy bit for 64 bit information data. These redundancy bits are to be interspersed at the bit positions (n = 1, 2, 4, 8, 16, 32 and 64) of the original data bits, so to transmit 64 bit information data we need 7 redundancy bit generated by even parity check method to make 71 bit data string. At the destination receiver point, we receive 71 bit data, this receives data may be corrupted due to noise. In Hamming technique the receiver will decided if data have an error or not, so if it detected the error it will find the position of the error bit and corrects it. This paper presents the design of the transmitter and the receiver with Hamming code redundancy technique using VHDL. The Xilinx ISE 10.1 Simulator was used for simulating VHDL code for both the transmitter and receiver sides.

Keywords: Hamming code, error correction, error detection, even parity check method, Redundancy bits, VHDL language, Xilinx ISE 10.1 Simulator

INTRODUCTION

The theory of linear block codes is well established since many years ago. In 1948 Shannon's work showed that any communication channel could be characterized by a capacity at which information could be reliably transmitted. In 1950, Hamming introduced a single error correcting and double error detecting codes with its geometrical model (1).

In telecommunication, Hamming code as a class of linear block codes is widely used, Hamming codes are a family of linear error-correcting codes that generalize the
Hamming(7,4)-code. Hamming codes can detect up to two-bit errors or correct one-bit errors. By contrast, the simple parity code cannot correct errors, and can detect only an odd number of bits in error. Hamming codes are perfect codes, that is, they achieve the highest possible rate for codes with their block length and minimum distance $3$ ($2.3$).

Due to the limited redundancy that Hamming codes add to the data, they can only detect and correct errors when the error rate is low. This is the case in computer memory (Error Checking & Correction, ECC memory), where bit errors are extremely rare and Hamming codes are widely used. In this context, an extended Hamming code having one extra parity bit is often used. Extended Hamming codes achieve a Hamming distance of 4, which allows the decoder to distinguish between when at most one bit error occurred and when two bit errors occurred. In this sense, extended Hamming codes are single-error-correcting (SED) and double-error-detecting (DED). The ECC functions described in this application note are made possible by Hamming code, a relatively simple yet powerful ECC code. It involves transmitting data with multiple check bits (parity) and decoding the associated check bits when receiving data to detect errors. The check bits are parallel parity bits generated from XORing certain bits in the original data word. If bit error(s) are introduced in the codeword, several check bits show parity errors after decoding the retrieved codeword. The combination of these check bit errors display the nature of the error. In addition, the position of any single bit error is identified from the check bits ($2.4$).

Error detection and correction codes are used in many common systems including: storage devices (CD, DVD, DRAM), mobile communication (cellular telephones, wireless, microwave links), digital television, and high-speed modems. Hamming codes is a Forward Error Correction (FEC), as a fundamental principle of channel coding techniques, provides the ability to correct transmission errors without requiring a feedback channel for a correct retransmission. The exact correction capability of an FEC code varies depending on the coding schemes used ($5.6$).

The basic idea for achieving error detection is to add some redundancy bits to the original message to be used by the receivers to check consistency of the delivered message and to recover the correct data. Error-detection schemes can be either systematic or non-systematic: In a systematic scheme the transmitter sends the original data and attaches a fixed number of check bits. That is derived from the data bits by some deterministic algorithm. If only error detection is required a receiver can simply apply the same algorithm to the received data bits and compare its output with the received check bits if the values do not match an error has occurred at some point during the transmission. In a system that uses a
non-systematic code the original message is transformed into an encoded message that has at least as many bits as the original message. Error correction & detection Hamming code may perform using Even parity or Odd parity $^{7,8}$.

Suppose, we want to transmit 64 information data bit is “0101010101010101010101010101010101010101010101010101010101010101” which equal in hexadecimal”555555555555555555”. For this 64 bit information data we need 7 redundancy bits using even parity method. After generating redundancy bits, add these bits to 64 bit information data for making 71 bit data string for transmission at source end. How we can generate 7 redundancy bits for 64 bit information data for making 71 bit data string for transmission at source end by using even parity method will be discussed in details at communication with even parity method. At destination receiver receives 71 bit data string from channel and check it, is it corrupted or not? If it is corrupted then the receiver find the error location according to parity check method correct it.

2. Error Detection and Correction

For a given practical requirement, detection of errors is simpler than the correction of errors. The decision for applying detection or correction in a given code design depends on the characteristics of the application. When the communication system is able to provide a full duplex transmission (that is, a transmission for which the source and the destination can communicate at the same time, and in a two way mode, as it is in the case of telephone connection, for instance), codes can be designed for detecting errors, because the correction is performed by requiring a repetition of the transmission $^{3,8}$.

These schemes are known as automatic repeat request (ARQ) schemes. In any ARQ system there is the possibility of requiring a retransmission of a given message. There are on the other hand communication systems for which the full-duplex mode is not allowed. An example of one of them is the communication system called paging, a sending of alphanumerical characters as text messages for a mobile user. In this type of communication system, there is no possibility of requiring retransmission in the case of a detected error, and so the receiver has to implement some error-correction algorithm to properly decode the message. This transmission mode is known as forward error correction (FEC) $^{3,8}$.

3. HAMMING CODE

Hamming code is a linear error-correcting code named after its inventor, Richard Hamming. Hamming codes can detect up to two simultaneous bit errors, and correct single-bit error. By contrast, the simple parity code cannot correct errors, and can only detect an odd
number of errors. In 1950 Hamming introduced the (7, 4) code. It encodes 4 data bits into 7 bits by adding three parity bits. Hamming (7, 4) can detect and correct single – bit errors. With the addition of overall parity bit, it can also detect (but not correct) double bit errors. Hamming code is an improvement on parity check method. It can correct 1 error bit only.\(^9\)

Hamming code used two methods (even parity and odd parity) for generating redundancy bit. The number of redundancy bits depends on the size of information data bits as shown below:\(^8,9,10,11\):

\[
2^r \geq m + r + 1 \tag{1}
\]

Where \( r \) = number of redundancy bit.

\( m \) = number of information data bits.

According to (1), 7 redundancy bits required for a 64 input data bits. Hamming-based codes are widely used in memory systems for reliability improvements. The algorithm consists of two phases: encoding and decoding. Hamming encoding involves deriving a set of parity check bits over data bits. These parity check bits are concatenated or merged with the data bits. These extra bits are called redundancy bits. We add these redundancy bits to the information data at the source end and remove at destination end. Presence of redundancy bit allows the receiver to detect or correct corrupted bits. The concept of including extra information in the transmission for error detection is a good one. But in place of repeating the entire data stream, a shorter group of bits may be added to the end of each unit. This technique is called redundancy because the extra bits are redundant to the information.\(^8,12,13,14\).

### 3.1 Hamming Encoder

In communication system need two main part one of them is the source for sending data and another is the destination to receive the transmitted data. Even parity check method count the number of one’s if number of one’s are even it adds zero (0) otherwise it adds one (1).\(^8\).

At the transmitter the 64 bit information data needs 7 redundancy bit according to equation (1). Suppose, these redundancy bits are \( R(1), R(2), R(4), r(8), R(16), R(32), R(64) \), and to calculate these redundancy bits easily done by XORing operation of the original data bit positions as shown below:

\[
R(1) = D1 \oplus D2 \oplus D4 \oplus D5 \oplus D7 \oplus D9 \oplus D11 \oplus D12 \oplus D14 \oplus D16 \oplus D18 \oplus D20 \oplus D22 \oplus D24 \oplus D26 \oplus D27 \oplus D29 \oplus D31 \oplus D33 \oplus D35 \oplus D37 \oplus D39 \oplus D41 \oplus D43 \oplus D45 \oplus D47 \oplus D49 \oplus D51 \oplus D53 \oplus D55 \oplus D57 \oplus D58 \oplus D60 \oplus D62 \oplus D64 \tag{2}
\]
DESIGN OF HAMMING CODE FOR 64 BIT SINGLE ERROR DETECTION AND CORRECTION USING VHDL

\[ \begin{align*}
R(2) &= D_1 \oplus D_3 \oplus D_4 \oplus D_6 \oplus D_7 \oplus D_{10} \oplus D_{11} \oplus D_{13} \oplus D_{14} \oplus D_{17} \oplus D_{18} \oplus D_{21} \oplus D_{22} \oplus D_{25} \oplus D_{26} \oplus D_{28} \oplus D_{29} \oplus D_{32} \oplus D_{33} \oplus D_{36} \oplus D_{37} \oplus D_{40} \oplus D_{41} \oplus D_{44} \oplus D_{45} \oplus D_{48} \oplus D_{49} \oplus D_{52} \oplus D_{53} \oplus D_{56} \oplus D_{57} \oplus D_{59} \oplus D_{60} \oplus D_{63} \oplus D_{64}. \tag{3} \\
R(4) &= D_2 \oplus D_3 \oplus D_4 \oplus D_8 \oplus D_9 \oplus D_{10} \oplus D_{11} \oplus D_{15} \oplus D_{16} \oplus D_{17} \oplus D_{18} \oplus D_{23} \oplus D_{24} \oplus D_{25} \oplus D_{26} \oplus D_{30} \oplus D_{31} \oplus D_{32} \oplus D_{33} \oplus D_{38} \oplus D_{39} \oplus D_{40} \oplus D_{41} \oplus D_{46} \oplus D_{47} \oplus D_{48} \oplus D_{49} \oplus D_{54} \oplus D_{55} \oplus D_{56} \oplus D_{57} \oplus D_{61} \oplus D_{62} \oplus D_{63} \oplus D_{64}. \tag{4} \\
R(8) &= D_5 \oplus D_6 \oplus D_7 \oplus D_8 \oplus D_9 \oplus D_{10} \oplus D_{11} \oplus D_{19} \oplus D_{20} \oplus D_{21} \oplus D_{22} \oplus D_{23} \oplus D_{24} \oplus D_{25} \oplus D_{26} \oplus D_{34} \oplus D_{35} \oplus D_{36} \oplus D_{37} \oplus D_{38} \oplus D_{39} \oplus D_{40} \oplus D_{41} \oplus D_{50} \oplus D_{51} \oplus D_{52} \oplus D_{53} \oplus D_{54} \oplus D_{55} \oplus D_{56} \oplus D_{57}. \tag{5} \\
R(16) &= D_{12} \oplus D_{13} \oplus D_{14} \oplus D_{15} \oplus D_{16} \oplus D_{17} \oplus D_{18} \oplus D_{19} \oplus D_{20} \oplus D_{21} \oplus D_{22} \oplus D_{23} \oplus D_{24} \oplus D_{25} \oplus D_{26} \oplus D_{42} \oplus D_{43} \oplus D_{44} \oplus D_{45} \oplus D_{46} \oplus D_{47} \oplus D_{48} \oplus D_{49} \oplus D_{50} \oplus D_{51} \oplus D_{52} \oplus D_{53} \oplus D_{54} \oplus D_{55} \oplus D_{56} \oplus D_{57}. \tag{6} \\
R(32) &= D_{27} \oplus D_{28} \oplus D_{29} \oplus D_{30} \oplus D_{31} \oplus D_{32} \oplus D_{33} \oplus D_{34} \oplus D_{35} \oplus D_{36} \oplus D_{37} \oplus D_{38} \oplus D_{39} \oplus D_{40} \oplus D_{41} \oplus D_{42} \oplus D_{43} \oplus D_{44} \oplus D_{45} \oplus D_{46} \oplus D_{47} \oplus D_{48} \oplus D_{49} \oplus D_{50} \oplus D_{51} \oplus D_{52} \oplus D_{53} \oplus D_{54} \oplus D_{55} \oplus D_{56} \oplus D_{57}. \tag{7} \\
R(64) &= D_{58} \oplus D_{59} \oplus D_{60} \oplus D_{61} \oplus D_{62} \oplus D_{63} \oplus D_{64}. \tag{8}
\end{align*} \]

The value of redundancy bits can be calculated using an even parity check method. The value of redundancy bit can be calculated by XORing of different locations of information data bits, as shown in Figure (1). The calculation of redundancy bit of Hamming encoder is done by VHDL code written in Xilinx ISE 10.1 project navigator window as shown in Figure (2).

Suppose, we want to transmit 64 information data bit is “0101010101010101010101010101010101010101010101010101010101010101” which equal in Hexadecimal "5555555555555555". Calculation for redundancy bits, by XORing input bit, according to hamming code with even parity redundancy the transmitted data will be 71 bits “0100 1011 0101 0100 1010 1010 1010 1011 0101 0101 0101 0101 0101 0101 0101 1010 101” which equal in Hexadecimal "25AA555555555555" as explained in Figure (1).

The simulation of Hamming code generation code for VHDL code for source end as shown in Figure (3) and Figure(4). The schematic circuit diagram is shown in Figure (5), and Hamming encoder design status is shown in Table (1).
3.2 Hamming Decoder

At the receiver side 71 bit information data is received, 64 bit encrypted information data and redundancy 7 bits. At the destination, the receiver receives 71 bit encrypted data and check for any error that may occurred. If any error is occurred, receiver find the error location and corrects it. Hamming decoder detect the error by EXORing data and corrected it by a NOT gate (8). Then the receiver removes the redundancy bit and get the original data information, if there are no error the result of even parity check was (0000000) else it detect the location of error bit as shown in Figure (6).

The detection and correction of a single error bit by Hamming decoder is done by VHDL code written in Xilinx ISE 10.1 project navigator window as shown in Figure (7).

So according the supposed example the received data with no error (noiseless channel) will be “0100 1011 0101 0100 1010 1010 1011 0101 0101 0101 0101 0101 0101 0101 0101 0101 1010 101” which equal in Hexadecimal "25AA5555AAAAAA55". As shown in Figure (8) and Figure (9), where ’ded means detection error’ and ’ne means no error.

Suppose, transmitter of source end transmit data is “0100 1011 0101 0100 1010 1010 1011 0101 0101 0101 0101 0101 0101 0101 0101 0101 0101 0101 1010 101" which equal in Hexadecimal "25AA5555AAAAAA55" and at destination receiver received error data is “0110 1011 0101 0100 1010 1010 1011 0101 0101 0101 0101 0101 0101 0101 0101 0101 0101 0101 0101 1010 101” which equal in Hexadecimal "35AA5555AAAAAA55", Hamming decoder at first detect the error location by even parity checking method and corrected it as shown in Figure (10).

According to Hamming detection method take even parity check to get the address of error location is = 0000011 (the third bit at the input data). After getting the location of error bit, the receiver correct, that error bit by replacing zero by one and one by zero. To produce the actual transmitted data.

We write VHDL code to find the error bit location, correction it and decrypt this encrypted data. Simulated results for destination end shown in Xilinx ISE 10.1 Simulation window which shows 71 bit receives encrypted data string and 64 bit actual error free information data string after correction the errors, as shown in Figure (11) and Figure (12). Where Figure (13) show schematic circuit diagram of Hamming decoder. The design status of Hamming decoder is shown in Table (2).

4. CONCLUSION

As a conclusion, Hamming code error detection and correction with even parity check method can be design using 64 bits data string in VHDL and can be implemented in FPGA. it
speed up the communication as we can encode the total data bits as a whole and send as soon, so there are no need for data splitting, therefore more combination (more information in a single frame) of data can be transmitted easily. The complexity of circuit also reduced for regenerating actual information data from encrypted corrupt received data at destination end by using of the same method at the source end, so the original data can be correctly recovered.

5. REFERENCES


2) en.wikipedia.org/wiki/Hamming code.


4) Simon Tam "Single Error Correction and Double Error Detection" XILINIX, XAPP645 (v2.2) August 9, 2006.


10) Mr. Brajesh Kumar Gupta and Prof. Rajeshwar Lal Dua “COMMUNICATION BY 31 BIT HAMMING CODE TRANSCEIVER WITH EVEN PARITY AND ODD PARITY CHECK METHOD BY USING VHDL” International Journal Of Computational Engineering Research / Vol. 2 | Issue No.2 |278-288, Mar-Apr 2012
DESIGN OF HAMMING CODE FOR 64 BIT SINGLE ERROR DETECTION AND CORRECTION USING VHDL


**Table (1):** Hamming encoder design status.

<table>
<thead>
<tr>
<th>Logic Utilization</th>
<th>Used</th>
<th>Available</th>
<th>Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Slices</td>
<td>28</td>
<td>1920</td>
<td>1%</td>
</tr>
<tr>
<td>Number of 4 input LUTs</td>
<td>50</td>
<td>3840</td>
<td>1%</td>
</tr>
<tr>
<td>Number of bonded IOBs</td>
<td>135</td>
<td>173</td>
<td>78%</td>
</tr>
</tbody>
</table>

**Table (2):** Hamming decoder design status.

<table>
<thead>
<tr>
<th>Logic Utilization</th>
<th>Used</th>
<th>Available</th>
<th>Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Slices</td>
<td>135</td>
<td>1920</td>
<td>7%</td>
</tr>
<tr>
<td>Number of 4 input LUTs</td>
<td>245</td>
<td>3840</td>
<td>6%</td>
</tr>
<tr>
<td>Number of bonded IOBs</td>
<td>137</td>
<td>173</td>
<td>79%</td>
</tr>
<tr>
<td>Number of GCLKs</td>
<td>1</td>
<td>8</td>
<td>12%</td>
</tr>
</tbody>
</table>
Figure (1): Hamming Code Generation for 64 Bits.
DESIGN OF HAMMING CODE FOR 64 BIT SINGLE ERROR DETECTION AND CORRECTION USING VHDL

Figure (2): Hamming Encoder in VHDL Using ISE 10.1.

Figure (3) Hamming Code Generation for 64 Bits in Hexadecimal Form
Figure (4): Hamming Code Generation for 64 Bits in Binary Form.

Figure (5): Schematic Circuit Diagram of Hamming Encode.
Figure (6): Hamming Code Detection Method for 64 Bits with no Error State
Figure (7): Hamming Decoder in VHDL Using ISE 10.1.

Figure (8): Hamming Code Error Detection and Correction for a Single Error in Hexadecimal Form (With no error state).

Figure (9): Hamming Code Error Detection and Correction for a Single Error in Binary Form (With no Error state).
Figure (10): Hamming Code Detection Method for 64 Bits with Error State.
**Figure (11):** Hamming Decoder for a Single Error with Error Received Data (Error at Third Bit) in Hexadecimal Form.

**Figure (12):** Hamming Decoder for a Single Error with Error Received Data (Error at Third Bit) in Binary Form.

**Figure (13):** Schematic Circuit Diagram of Hamming Decoder.
تصميم شفرة (Hamming) لـ 64 بت لاكتشاف ومعالجة الخطأ المفرد باستخدام لغة VHDL

أدهم هادي صالح  
مدرس مساعد، قسم الهندسة الإلكترونية، كلية الهندسة، جامعة ديالى

الخلاصة:

شفرة (Hamming) هي تقنية لإكتشاف الخطأ وتصحيحه والتي يمكن أن تستخدم للكشف عن خطأ واحد أو عدة أخطاء، أن قابلية هذه التقنية في الكشف عن الخطأ الذي يحدث لبت واحد ومعالجته تم بكفاءة عالية و التي يمكن أن تحدث عند نقل البيانات من جهاز إلى آخر. في أنظمة الاتصالات يتم نقل البيانات من المرسل إلى المستلم خلال الوسط الناقل، والتي قد ت تعرض للتلف بسبب الضوضاء. تعمل شفرة (Hamming) على العثور على المعلومات الأصلية من خلال الكشف الخطأ ومعالجته. هذا البحث، يصف كيف يمكننا توليد 7 بت إضافية أثناء نقل البيانات الأصلية ذات الـ 64 بت. هذه البتات الإضافية ستتولَّد تفاعلات (n = 1, 2, 4, 8, 16, 32, 64) مع بات البيانات الأصلية. يتم نقل البيانات والعلومات (64 بت مع 7) لجعل سلسلة البيانات 71 بت. يتم بث شفرات الخطأ المزدوجات الثنائية عند المرسل. عند نقطة الاستلام، قد تصل البيانات ذات 71 بت وزوج من البيانات تلف بسبب الضوضاء. يتم عند المستقبل باستخدام تقنية (Hamming) تحديد إذا كان هناك خطأ في البيانات أم لا. وفي حال الكشف عن الخطأ سيتم العثور على موقع الخطأ وتصحيحه. هذا يمكن استخدام لمحاكاة XILINX ISE 10.1 لغة VHDL في هذا البحث تم تصميم المرسل والمستقبل لشفرة بيتيشية (Hamming) باستخدام لغة VHDL وهي لغة وصفية تستخدم لتصميم الدوائر الإلكترونية.

الكلمات الرئيسية: شفرة (Hamming)، تصحيح الخطأ، اكتشاف الخطأ، طريقة اكتشاف الخطأ بالزوجات الثنائية، بت التكرار، لغة XILINX ISE 10.1، VHDL.