N-BYTE ERROR DETECTING AND CORRECTING CODE USING REED-SOLOMON AND CELLULAR AUTOMATA APPROACH

Parul Gaur¹, Deepak Gaur², Aruna Tomar³

Department of Electrical and Electronics Engineering, UIET, PanjabUniversity, Chandigarh, India., parul34@gmail.com
Department of Computer Science and Engineering, ASET, Amity University, Noida(U.P.), India, dgaur@amity.edu
Department of ECE, Marathwada Institute of Technology, Delhi, India, aruna_tomar07@yahoo.com

Abstract

Single and double byte errors are most common errors in memory systems. With the advancement of technologies, more information bytes can be send over a transmission channel, but this increases the probability of more errors. Here we propose a methodology for detecting and correcting N-byte errors in the information bytes based on cellular automata (CA) concept. Cellular automata already accepted as an attractive structure for error detecting and correcting codes. In this paper, highly efficient, reliable and less complex cellular automata based N-byte error correcting encoder and decoder has been proposed. The design is capable of adding 2N check bytes corresponding to N information bytes at the encoder, which are used at the decoder section to detect and correct the byte errors.

**Keywords**— Cellular Automata (CA), Reed-Solomon (RS) code, Information Bytes (IB), Check Bytes (CB)

1. INTRODUCTION

During transmission of information bytes, it may be possible that information signal is corrupted by noise, which leads to change in information signal. It is very important to detect the errors in the information bytes and correct them. Various coding techniques have been used for error detecting and correcting. Error correcting codes have been used to enhance system reliability and data integrity. The basic concept is to add check bytes or redundancy to the information bytes at the encoder so that decoder can recover the information bytes from the received block possibly corrupted by the channel noise. Reed-Solomon (RS) codes are most commonly used codes for error correction because these codes can detect both random as well as burst errors. Reed-Solomon codes were invented in 1960 by Irving S. Reed and Gustave Solomon, at the MIT Lincoln Laboratory. Reed-Solomon codes are used in many applications like wireless communication, satellite communications, high speed modems and storage devices like CD, DVD. For example RS (28, 24) and RS (32, 28) is popularly used for multistorage CD. In this four check bytes are added to the information bytes, which detects the two byte errors. Complexity of RS encoder and decoder increases with the error correcting capability of the codes. A general decoding scheme for RS decoder based upon pipelined degree computationless modified Euclidean algorithm is found in [1]. In [1], a high speed pipelined architecture was proposed with the aim of reducing hardware complexity because of absence of degree computation circuit and improving the clock frequency in RS decoders. However conventional RS decoders [2][4] induce relatively huge hardware complexity. A system designer always prefer to have simple and regular structure for reliable high speed operations of the circuit. It has been found that these parameters are supported by local neighbourhood cellular automata (CA). CA based byte error correcting code has been proposed in [5]. Till now single, double and atmost three bytes errors are corrected [5]. In our research paper, a methodology for detecting and correcting N-byte errors based upon cellular automata has been proposed. Whatever will be the value of N, system will detect and correct the errors in the information bytes. A logic has been generated, which detects and corrects the errors.

2. PRELIMINARIES

A. CA Preliminaries

CA is an array of cells, where each cell is in any one of the permissible states. At each discrete time step, the evolution of the cell depends on the combination logic which is function of the present state of the cell itself and states of the neighbouring cells. For two state three neighbourhood, the evolution of the ith cell can be represented as a function of the present states of (i-1)th , ith and (i+1)th cells as:

\[ x_i(t+1) = f\{ x_{i-1}(t), x_i(t), x_{i+1}(t) \} \]

where \( f \) represents the combinational logic. For a two state three cellular automata there are \( 2^3 \) that is, 8 distinct neighbourhood configurations and \( 2^8 \) that is, 256 distinct next state functions. The CA characterized by a rule known as rule 90, specifies an evolution from neighbourhood configuration to next state as:

\[
\begin{array}{cccccccccc}
111 & 110 & 101 & 100 & 011 & 010 & 001 & 000 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0
\end{array}
\]


he corresponding combinational logic for rule 90 is:

\[ x(t+1) = x_i(t) \overline{x_{i-1}(t)} + x_{i+1}(t) \overline{x_i(t)} \]

\[ x(t+1) = x_i(t) \oplus x_{i-1}(t) \]

that is, the next state of \( i \)th cell depends on the present states of its left and right neighbours (Figure 1). Similarly, the combinational logic for rule 150 is given by:

\[ x(t+1) = x_i(t) \oplus x_{i-1}(t) \oplus x_{i+1}(t) \]

that is, the next state of \( i \)th cell depends on the present states of its left and right neighbours as well as its own present state (Figure 1).

**Figure 1** A Hybrid Cellular Automata

A CA characterized by EXOR or EXNOR dependence is called an additive CA. If in a CA, the neighbourhood dependence is EXOR, then it is called non-complemented CA and the corresponding rule is non-complemented rule. For EXNOR dependence, CA is called complemented CA and the corresponding rule is called complemented rule. There exists 16 additive rules which are:

Rule 0, 15, 51, 60, 85, 90, 102, 105, 150, 153, 165, 170, 195, 204, 240 & 255

A uniform CA is one in which same rule applies to all cells while in hybrid CA (Figure 1) different rules are applied to different cells. In our methodology, rule 90 and rule 150 are used for cells in CA. Based upon this, an efficient error detecting and correcting code is designed.

**B. Reed-Solomon Code**

In RS code, we assume that \( n \) storage devices hold data \( D_1, D_2, D_3, \ldots, D_{n-1}, D_n \) and \( m \) storage devices hold checksums \( C_1, C_2, C_3, \ldots, C_{m-1}, C_m \). These checksums are computed from the data. In this code, if any \( m \) devices fail then they can be reconstructed from the surviving devices. The value of checksum device is computed using a function \( F \):

\[
\begin{align*}
D_1 & = F(D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8) \\
C_1 & = F(D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8)
\end{align*}
\]

If any data \( D_j \) changes that is becomes \( D'_j \) then from check bytes we can recover the data.

**3. MECHANISM FOR CA BASED N-BYTE ERROR DETECTING AND CORRECTING CODE**

**A. Encoder Section**

In encoder, check bytes are added. For N-byte error detecting and correcting code, encoder generates \( 2N \) check bytes and these check bytes are concatenated with the information bytes, which forms the codeword, given as \( C = DG \) (Figure 2) where \( D = (D_0, D_1, D_2, \ldots, D_{N-1}) \) is N-byte information data and \( G \) is generator matrix given as:

\[
I = \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & 1 & T & T^2 & T^3 \\
0 & 0 & 0 & \ldots & 0 & 1 & T^3 & T^4 & T^5 \\
0 & 0 & 0 & \ldots & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & \ldots & 0 & 0 & 1 & 0 & 1 \\
\end{pmatrix}
\]

\[
G = \begin{pmatrix}
I & T^N & T^{2N} & T^{3N} \\
\end{pmatrix}
\]

Here \( T_N \) is \( N \times N \) characteristics matrix corresponding to \( N \) information bytes and \( I \) is \( N \times N \) identity matrix.

\[
T_N \times N = \begin{pmatrix}
1 & 1 & 0 & \ldots & 0 & 0 \\
1 & 1 & 1 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 0 & 0 & \ldots & 1 & 1 \\
\end{pmatrix}
\]
One such rule vector of N cell length CA is \( <150,150,90,150,..............,150,90,150> \). Now check bytes (CB) computed from characteristics matrix can be given as:

\[
CB_\alpha = T^\alpha D_{N-1} \oplus T^{2\alpha} D_{N-2} \oplus T^{3\alpha} D_{N-3} \oplus \ldots \oplus T^{(N-1)\alpha} D_1 \oplus T^{N\alpha} D_0
\]  

(1)

Where \( 0 \leq \alpha \leq (2N-1) \), corresponding to N-byte error correcting code. Based upon this, figure 3 shows the encoder section.

**B. Decoder Section**

We consider the problem of decoding to detect and correct the erroneous byte positions from the received codeword C. The first step is to compute the syndrome. If the received codeword is \( C = D' | CB' \), where

\[
D' = D \oplus D_e \quad (D \text{ is original information and } D_e \text{ is error in information}) \quad \text{and} \quad CB' = CB \oplus CB_e \quad \text{, then the syndrome of codeword can be expressed as } S(C) = HC^T = H(D' | CB').
\]

Here \( H \) is the parity check matrix formed by concatenating the compressed matrix \( T' \) with the identity matrix \( I_{N \times N} \).

The syndrome corresponding to jth check byte \( S_j \) is given by equation (2):

\[
S_j(C) = CB_j \oplus CB'_j
\]  

(2)

where \( 0 \leq j \leq (2N-1) \).

If the syndrome \( S(C) \) of a received codeword C is 0, then the word is assumed to be error free. If \( S(C) \neq 0 \), then errors are detected (Table I).

**4. ALGORITHM FOR ERROR CORRECTION**

For N-byte error correcting code, following (N+1) cases may occur:

- **Case I.** Single information byte error
- **Case II.** Double information byte error
- **Case III.** Triple information byte error
- **Case IV.** Quadruple information byte error

- **Case N.** N information byte error
- **Case (N+1).** Information byte error and check byte error
From above equations, we get:

**Equation (5):**

$$E_k = T^i [S_0] \oplus S_1$$

**Equation (6):**

$$E_j = S_0 \oplus E_i$$

Equations (5) and (6) give the errors.

Similarly for triple, quadruple,.............N IB, error equations can be found.

**Equation (7):**

$$E_k = T^i [S_{N-2}] \oplus S_{N-1}$$

For IB and CB errors, out of 2N CB error can be in any CB, so we have found that there will be 2N cases for CB. Suppose $E_i$ is the error in $i$th information byte and $e_0$ is in first CB, then the syndrome equations are:

**Equation (8):**

$$S_0 = E_i \oplus e_0, S_1 = T^k E_i, S_2 = T^{2k} E_i, \ldots$$

$$S_{N-2} = T^{(N-1)k} E_i$$

From above equations, we can find $E_i$. If $E_i$ is error in $i$th IB and $e_1, e_2, e_3, \ldots, e_{2N-2}, e_{2N-1}$ are errors in CB, we can find syndrome equations. In general, we have:

**Equation (9):**

$$S_0 = E_i \oplus e_0, S_1 = T^k E_i, S_2 = T^{2k} E_i, \ldots$$

$$S_{N-2} = T^{(N-1)k} E_i$$
Knowing the error location and error magnitudes, errors are corrected using XOR operation. Suppose $D_i$ and $E_i$ are the received $i$th IB and the calculated $i$th error byte respectively, then the correct IB can be calculated as:

$$D_i = D'_i \oplus E_i$$  \hfill (7)$$

Where $0 \leq i \leq N$.

5. RESULTS AND COMPARISON FROM PREVIOUS EXISTING TWO BYTES CODES

Table II shows the final errors detection and from equation (7), errors can be corrected resulting in correct information bytes. In [5], byte error correcting code using CA has been given. But this code detects and corrects the almost three bytes code. In our research paper, general algorithm for detecting and correcting N-byte code has been proposed. Whatever will be value of N, depending upon information bytes proposed system will detect and correct the errors. In contrast, the proposed encoder section has less hardware complexity than the other previously reported architectures [1]-[4].

CONCLUSION AND FUTURE SCOPE

This paper presents a novel design and algorithm for N-byte error detecting and correcting code using cellular automata and Reed-Solomon code approach. The circuit design requires much less hardware. So the implementation of the proposed scheme provides a simple high speed and cost effective solution. The proposed algorithm can be implemented in VHDL by using Xilinx ISE 9.1i tool for N-byte information signal.

REFERENCES