A Novel Method of Constructing Quasi-Cyclic RS-LDPC Codes for 10GBASE-T Ethernet

Seong-In Hwang and Hanho Lee
Dept. of Information and Communication Engineering
Inha University, Incheon, 402-751, Korea
hhlee@inha.ac.kr

Shin-Ill Lim
Dept. of Electronics Engineering
Seokyeong University, Seoul, 136-704, Korea

Abstract—This paper presents a novel method of constructing of Quasi-Cyclic Reed-Solomon-based LDPC (QC-RS-LDPC) codes for the application of 10GBASE-T Ethernet. The proposed code construction method makes RS-LDPC codes to be quasi-cyclic codes without bit error rate performance degradation. Therefore, QC-RS-LDPC decoder using the proposed method can use Banyan network or QSN that are efficient switch networks for QC codes. For performance comparison, the switch networks have been implemented. The results show that the switch network using the proposed method requires less memory size than existing switch network like Benes network. Since the switch network optimized for QC codes reduces critical path delay, the clock speed of QC-RS-LDPC decoder can be improved. The proposed method is able to construct QC-RS-LDPC codes, which reduces hardware size and improves clock speed.

keywords—low-density parity-check (LDPC) codes, Reed-Solomon (RS)-LDPC codes, QC-RS-LDPC codes, 10GBASE-T Ethernet, switch network.

I. INTRODUCTION

LDPC codes have been demonstrated to perform very close to the Shannon limit with iterative decoding, such as belief-propagation algorithm [1]-[4]. Many applications, such as digital video broadcasting (DVB-S2) [5], 10 Gigabit Ethernet (10GBASE-T) [6], broadband wireless access (WiMax) [7] and Wireless Gigabit Alliance (WiGig) [8], have included LDPC codes.

Specifically, 10GBASE-T Ethernet adopts (2048, 1723) Reed-Solomon-based LDPC (RS-LDPC) code. RS-LDPC code was introduced first in [9]. This code has large girth and good performance. But in process of forming coset there are combinations of irrelative codewords. This process makes a random parity check matrix structure, which leads to large hardware complexity in switch network. To handle random structure of RS-LDPC code, RS-LDPC decoder uses Benes network architecture [10], which has high hardware complexity. Furthermore, to reduce complexity, other method like grouping method [11] is proposed for switch network.

The parity-check matrices of the quasi-cyclic (QC) LDPC codes have submatrices, which are circulant permutation matrices (CPMs) or zero matrices. Submatrix size and the circular-shift value of submatrix determine interconnection network between the check-node processing units and the variable-node processing units. Since the structure of QC-LDPC codes is more efficient for hardware implementation, highly paralleled decoder architecture can be implemented using QC-LDPC codes. Thus, QC-LDPC codes are highly recommended for LDPC decoder.

In this paper, we propose a novel method to construct parity-check matrix of QC-RS-LDPC codes without performance degradation. The proposed method retains internal structural property of RS-LDPC codes but changes external structural property. Therefore, QC-RS-LDPC decoders using the proposed method are able to adopt QC-LDPC shift network (QSN) [12] or Banyan network [13] for efficient switch network design. Moreover, the parity-check matrix of QC-RS-LDPC codes reduces hardware complexity and improves performance with parallel processing.

The rest of this paper is organized as follows. Section II introduces proposed construction method of QC-RS-LDPC codes. In Section III, simulation result is presented to compare bit error rate (BER) performance. Section IV describes synthesis result for several switch networks and compares the hardware complexity. Finally, the conclusion is drawn in section V.

II. PROPOSED CONSTRUCTION METHOD OF QC-RS-LDPC CODES

A. Review of RS-LDPC Codes

Fig. 1 presents flowchart of constructing RS-LDPC codes, in which the construction method has six steps [9].

First, consider the Galois-filed $GF(p^\rho)$ where $p$ is a prime and $s$ is a positive integer. If $a$ is a primitive element of $GF(p^\rho)$, with a positive integer $\rho$, where $2 \leq \rho < p^s$, we can construct RS code over $GF(p^\rho)$, whose generator polynomial over $GF(p^\rho)$ is given by

$$g(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{p^\rho-2}) = g_0 + g_1X + g_2X^2 + \cdots + X^{p^\rho-2} \quad (1)$$

where $g_\rho \in GF(p^\rho)$. $g(X)$ is a minimum weight code polynomial hence all its $p-1$ coefficients are nonzero. If we shorten the RS code by eliminating the first $p-1$ information symbols, then we can obtain a shortened RS code $C_s$ with two information symbols. With coefficient of $g(X)$, we obtain generator matrix of a shortened RS code.

$$G_s = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & 1 \end{bmatrix} \quad (2)$$
All the linear combinations of the two rows of \( G_b \) make \( p^2 \) the codewords of \( C_b \). The nonzero codewords of \( C_b \) have weight, \( p \) or \( p-1 \). Let first row and second row of \( G_b \) be \( r_1 \) and \( r_2 \), \( r_1 \) and \( r_2 \) have weight \( p \). Then the set

\[
C_b^{(1)} = \{ \beta(r_1 + r_2) : \beta \in GF(p^q) \}
\]

for \( 2 \leq i \leq p^2 \).

Consider the \( p^2 \) elements \( \alpha^i, \alpha^{i+1}, \alpha^{i+2} \), of \( GF(p^q) \). Let \( z = (z_0, z_1, \ldots, z_{p^2}) \) be a \( p^2 \)-tuple over \( GF(2) \) whose components correspond to the \( p^2 \) elements of \( GF(p^q) \). For \( i=\infty, 0, 1, \ldots, p^2-2 \), \( i \) th component of location vector \( z(\alpha^i) \) is equal to 1 and all the other components are equal to zero.

Let \( b=(b_1, b_2, \ldots, b_p) \) is a codeword in \( C_b \). Replacing each component \( b_i \) of \( b \) by its location vector \( z(b_i) \), where \( 1 \leq i \leq p \), we can obtain a binary weight-\( p \) \( p^2 \)-tuple \( z(b) = (z(b_1), z(b_2), \ldots, z(b_p)) \), which is called the symbol location vector of \( b \). For \( 1 \leq i \leq p^2 \), we expand \( C_b^{(i)} \) to symbol location vector, we obtain

\[
Z(C_b^{(i)}) = \{ z(b) : b \in C_b^{(i)} \}.
\]

This matrix has \( p^2 \times p \) size over \( GF(p^q) \) whose \( p^2 \) rows are the \( p^2 \) codewords in \( C_b^{(i)} \).

The null space of \( \gamma p^i \times p p^i \) matrix \( H_\gamma \) is an RS-LDPC code. Since two rows have at most one 1-component in common, there are no \( 4 \) ones in \( H_\gamma \), that make \( 4 \) corner of a rectangle. Therefore the Tanner graphs of \( H_\gamma \) is free of cycles of length \( 4 \) and its girth is at least \( 6 \). \( H_\gamma \) can be divided into \( \gamma \times p \) submatrices. Each submatrix is a permutation but not always a circulant matrix.

In the process of forming cosets \( C_b^{(2)}, C_b^{(3)}, \ldots, C_b^{(p^2)} \), there are combinations of irreleal codewords \( r_1 \) and \( r_2 \). These combinations make a random parity check matrix. The random structure increases hardware complexity particularly in switch networks. Therefore, the elimination of randomness of parity check matrix is important.

Two major properties of RS-LDPC codes are following: (1) Two rows in the same matrix \( Z(C_b^{(i)}) \) do not have any 1-component in common. (2) Two rows forming two different member matrices, \( Z(C_b^{(i)}) \) and \( Z(C_b^{(j)}) \), do not have more than one 1-component in common. This implies that there are no four 1-components, which form four corners of rectangle. This ensures that the Tanner graph of parity check matrix \( H \) is free of cycles of length \( 4 \) and hence its girth is at least \( 6 \). These properties prevent the performance degradation. However the distribution of nonzero elements in parity check matrix \( H \) is too complex, as shown in Fig. 3(a), and it results in high hardware complexity, in which nonzero elements denote interconnection of variable nodes and check nodes. Therefore, it is necessary to maintain above properties of RS-LDPC codes, while eliminating their random structure.

B. Proposed QC-RS-LDPC Codes

The proposed construction method of QC-RS-LDPC codes maintains the properties of RS-LDPC codes and has quasi-cyclic parity check matrix.
The steps of the proposed construction method of QC-RS-LDPC codes are herein: (1) Select one codeword \( c \) in set of codewords \( C_b \). (2) Expand codeword \( c \) into symbol location vector \( z(c) \). This is the first row of a coset. (3) Generate next row by performing cyclic shift on a symbol location vector. (4) Repeat \( p - 2 \) times and obtain \( Z(C_b^{(i)}) \). Similarly, using these steps on other codewords in \( C_b \), we can obtain \( Z(C_b^{(2)}), Z(C_b^{(3)}), \ldots, Z(C_b^{(p)}) \). (5) For \( 1 \leq i \leq \gamma \), by concatenating \( Z(C_b^{(i)}) \) we can obtain parity check matrix \( H \).

In the step 3, cyclic shift operation is used because multiplication cannot generate \( \alpha_\infty \). For example, the next element of \( \alpha_0^{p-2} \) in multiplication is \( \alpha_0 \), not \( \alpha_\infty \). However, the cyclic shift operation is able to include \( \alpha_\infty \). The next element of \( \alpha_0^{p-2} \) is \( \alpha_\infty \) and the next element of \( \alpha_\infty \) is \( \alpha_0 \). Therefore, the cyclic shift operation must be used for the construction of quasi-cyclic parity check matrix, as shown in Fig. 3(b).

The step 4 has different flow with the conventional method shown in Fig. 1. The proposed method makes different cosets with the conventional method and constructs a quasi-cyclic parity check matrix \( H_{QC} \), which satisfies two major properties of RS-LDPC codes.

C. Examples

(6, 32)-regular (2048, 1723) code was generated by using proposed construction method. \( GF(2^6) \) is the field for code construction. First, we randomly select one codeword \( c = \{ \alpha_24, \alpha_34, \alpha_53, \ldots, \alpha_{41}, \alpha_0, \alpha_\infty \} \) in codeword \( C_b \). The codeword \( c \) consists of 32-element in \( GF(2^6) \). Then codeword \( c \) can be expanded into symbol location vector \( z(c) \), which has 32×64 bits, since each element in \( c \) is expanded into 64 bits location vector. Next, by shifting cyclically \( z(c) \) 63 times, \( Z(C_b^{(1)}) \) can be generated. Performing these steps to other 5 codewords in \( C_b \), \( Z(C_b^{(2)}), \ldots, Z(C_b^{(5)}) \) can be generated. By concatenating these sets, the parity check matrix \( H \) can be constructed. The \( H \) matrix contains \( M = 384 \) rows and \( N = 2048 \) columns. This matrix can be partitioned into \( \gamma = 6 \) row groups and \( \rho = 32 \) column groups of \( 64\times64 \) submatrices. The minimum distance is at least 8. It was verified that the generated parity check matrix maintains two major properties of RS-LDPC codes.

The error correction performance of conventional RS-LDPC code and proposed QC-RS-LDPC code was compared with same length and same rate. For decoding process, belief-propagation algorithm (BPA) [1] and offset Min-Sum algorithm [14] was used. For performance computation, we assume BPSK transmission over AWGN channel.

Fig. 4 shows a BER performance of a (6, 32)-regular (2048, 1723) code using BPA decoding. If the decoding iteration is limited to 10, for a BER of 10^{-6}, the code performs 1.85 dB

\[
\begin{array}{c|c|c}
\text{Bit Error Rate} & \text{(2048,1723) RS-LDPC} & \text{(2048,1723) QC-RS-LDPC} \\
\hline
10^{-3} & 3.5913 & 3.5609 \\
10^{-4} & 3.8324 & 3.8501 \\
10^{-5} & 4.0816 & 4.0965 \\
10^{-6} & 4.2827 & 4.3079 \\
\end{array}
\]

As a result, every row in parity check matrix has weight 6 and every column has weight 32.

Fig. 3 illustrates submatrices of (2048, 1723) RS-LDPC code using conventional method and QC-RS-LDPC code using the proposed method. The submatrix using conventional method has 1-components that disperse randomly. However submatrices of the parity check matrix using the proposed method has only cyclic permutation form and the parity check matrix becomes quasi-cyclic. The proposed method can be applied to construct any size of parity check matrices as in the case of conventional method.

III. PERFORMANCE COMPARISON

The error correction performance of conventional RS-LDPC code and proposed QC-RS-LDPC code was compared with same length and same rate. For decoding process, belief-propagation algorithm (BPA) [1] and offset Min-Sum algorithm [14] was used. For performance computation, we assume BPSK transmission over AWGN channel.
from Shannon limit and achieves a 5.7 dB coding gain over the uncoded BPSK. Table I shows required $E_b/N_0$ to achieve some BER performance. The result shows that the proposed QC-RS-LDPC code achieves almost same BER performance with RS-LDPC code.

IV. IMPLEMENTATION RESULT

The QC-LDPC codes are highly recommended since they reduce interconnection wires and improve decoding throughput by reducing critical path delay especially in switch network. So we specifically implemented switch networks of (2048, 1723) RS-LDPC decoder for one subblock (64×64 subamtrix) using a SYNOPSIS design tool and 90-nm CMOS technology optimized for a 1.1 V supply voltage.

Table II shows the implementation results of the Benes, Banyan and QSN switch networks specifically for one submatrix of parity check matrix. It compares the total number of gates, memory size to store control signals, critical path delay and clock speed. The gate count of Benes network and Banyan network is 12673 and 9087, respectively. The results shows that Banyan network using proposed QC-LS-LDPC code has lowest hardware complexity and fast clock speed. Also, by using Banyan network, the memory size has been reduced significantly. Switch networks for (2048, 1723) QC-RS-LDPC decoder can operate at clock frequency of around 300MHz. Thus, QC-RS-LDPC decoder has much higher decoding throughput. The conventional (2048, 1723) RS-LDPC decoder results in vast variety of permutations. Therefore, the number of switch network stages and the control signals increase, and it requires higher memory size. On the other hand, the switch networks for QC-RS-LDPC decoder require only 2% of memory size of switch network using conventional method.

V. CONCLUSION

This paper presents the method of constructing QC-RS-LDPC code for high-performance 10GBASE-T Ethernet LDPC decoder. The performance comparison result shows that QC-RS-LDPC code using the proposed method does not have BER performance degradation. The proposed method enables QC-RS-LDPC decoder to use QSN or Banyan network, which are efficient switch networks for QC codes. Using 90-nm CMOS technology, switch networks of QC-RS-LDPC decoder can provide a maximum clock frequency 300 MHz and very small memory size. Thus, QC-RS-LDPC decoder has not only a much higher decoding throughput but also lower hardware complexity. The proposed method of constructing QC-RS-LDPC code can be adopted for the (2048, 1723) regular RS-LDPC code for the application of IEEE 802.3 10GBASE-T Ethernet.

ACKNOWLEDGMENT

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency)" (NIPA-2011-C1090-1111-0007)

REFERENCES