A Class of Low-Density Parity-Check Codes Constructed Based on Reed-Solomon Codes With Two Information Symbols

Ivana Djurdjevic, Jun Xu, Khaled Abdel-Ghaffar, *Member, IEEE*, and Shu Lin, *Fellow , IEEE*

***Abstract*—This letter presents an algebraic method for constructing regular low-density parity-check (LDPC) codes based on Reed–Solomon codes with two information symbols. The construction method results in a class of LDPC codes in Gallager's original form. Codes in this class are free of cycles of length 4 in their Tanner graphs and have good minimum distances. They perform well with iterative decoding.**

***Index Terms*—Low-density parity-check codes (LDPCs), Reed–Solomon codes, sum product algorithm.**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes were discovered by *Gallager* in early 1960s [1]. After being overlooked for almost 35 years, this class of codes has been recently rediscovered and shown to form a class of *Shannon limit* approaching codes [2]–[8]. This class of codes decoded with iterative decoding, such as the *sum-product algorithm* (SPA) [1], [4]–[6], performs amazingly well. Since their rediscovery, LDPC codes have become a focal point of research.

In this letter, an algebraic method for constructing regular LDPC codes is presented. This construction method is based on the simple structure of *Reed–Solomon* (RS) codes with two information symbols. It guarantees that the Tanner graphs [9] of constructed LDPC codes are free of cycles of length 4 and hence have girth at least 6. The construction results in a class of LDPC codes in Gallager's original form [1]. These codes are simple in structure and have good minimum distances. They perform well with iterative decoding.

II. RS Codes With Two Information Symbols

Consider the Galois field $\mathrm{GF}(p^s)$ where p is a prime and s is a positive integer. Let α be a primitive element of $\mathrm{GF}(p^s)$. Let $q = p^s$. Then $0 = \alpha^\infty, 1 = \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}$ form all the elements of $\mathrm{GF}(p^s)$. Let ρ be a positive integer such that $2 \le \rho < q$. Then the generator polynomial [10] of the cyclic $(q-1, q-\rho+1, \rho-1)$ RS code $\mathcal{C}$ of length $q-1$, dimension $q-\rho+1$, and minimum distance $\rho-1$ is

$$\boldsymbol{g}(X) = (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{\rho-2}) = g_0 + g_1 X + g_2 X^2 + \cdots + X^{\rho-2}$$

where $g_i \in \mathrm{GF}(p^s)$.

Suppose we shorten $\mathcal{C}$ by deleting the first $q-\rho-1$ information symbols from each codeword of $\mathcal{C}$[10]. We obtain a (ρ, 2, $\rho-1$) shortened RS code $\mathcal{C}_b$ with only two information symbols whose generator matrix is

$$\boldsymbol{G}_b = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & 1 \end{bmatrix}.$$

The nonzero codewords of $\mathcal{C}_b$ have two different weights, $\rho-1$ and ρ.

In the following, we develop a number of structural properties of $\mathcal{C}_b$ which are keys to the construction of a class of regular LDPC codes whose Tanner graphs are free of cycles of length 4. Since the minimum distance of $\mathcal{C}_b$ is $\rho-1$, two codewords in $\mathcal{C}_b$ have at most one location with the same code symbol. Let $\boldsymbol{c}$ be a codeword in $\mathcal{C}_b$ with weight ρ. Then the set $\mathcal{C}_b^{(1)} = \{\beta\boldsymbol{c} : \beta \in GF(p^s)\}$ of p^s codewords in $\mathcal{C}_b$ forms a one-dimensional subcode of $\mathcal{C}_b$. Each nonzero codeword in $\mathcal{C}_b^{(1)}$ has weight ρ. Two codewords in $\mathcal{C}_b^{(1)}$ differ at every location. Partition $\mathcal{C}_b$ into p^s cosets, $\mathcal{C}_b^{(1)}, \mathcal{C}_b^{(2)}, \ldots, \mathcal{C}_b^{(p^s)}$, based on the subcode $\mathcal{C}_b^{(1)}$. Then two codewords in any coset $\mathcal{C}_b^{(i)}$ must differ in all the locations. If we arrange the p^s codewords of a coset $\mathcal{C}_b^{(i)}$ as a $p^s \times \rho$ array, then all the p^s elements of any column of the array are different.

III. RS-Based Gallager-LDPC Codes

Consider the p^s elements, $\alpha^\infty, \alpha^0, \alpha^1, \ldots, \alpha^{p^s-2}$, of $\mathrm{GF}(p^s)$. Let $\boldsymbol{z} = (z_\infty, z_0, z_1, \ldots, z_{p^s-2})$ be a p^s-tuple over GF(2) whose components correspond to the p^s elements of $\mathrm{GF}(p^s)$, i.e, z_i corresponds to the field element α^i. We call α^i the *location number* of z_i. For $i = \infty, 0, 1, \ldots, p^s-2$, we define the *location vector* of α^i as a p^s-tuple over GF(2) for which the ith component z_i is equal to 1 and all the other components are equal to zero.

Let $\boldsymbol{b} = (b_1, b_2, \ldots, b_\rho)$ be a codeword in $\mathcal{C}_b$. For $1 \le j \le \rho$, replacing each component b_j of $\boldsymbol{b}$ by its location vector $\boldsymbol{z}(b_j)$, we obtain a ρp^s-tuple over GF(2)

$$\boldsymbol{z}(\boldsymbol{b}) = (\boldsymbol{z}(b_1), \boldsymbol{z}(b_2), \ldots, \boldsymbol{z}(b_\rho))$$

with weight ρ, which is called the *symbol location vector* of $\boldsymbol{b}$. Since any two codewords in $\mathcal{C}_b$ have at most one location

Manuscript received January 10, 2003. The associate editor coordinating the review of this letter and approving it for publication was Prof. M. Fossorier. This work was supported by the National Science Foundation under Grant CCR-0096191, Grant CCR-0117891, and Grant ECS-0121469, by the National Aeronautics and Space Administration under Grant NAG 5-10480, and by Accel Partners. This letter appeared in part in the Proceedings of the 15th Applied Algebra, Algebraic Algorithms, and Error Correcting Codes Symposium, Toulouse, France, May 2003.

The authors are with the Department of Electrical and Computer Engineering, University of California, Davis, CA 95616 USA (e-mail: idjurdje@ece.ucdavis.edu; junxu@ece.ucdavis.edu; shulin@ece.ucdavis.edu; ghaffar@ece.ucdavis.edu).

Digital Object Identifier 10.1109/LCOMM.2003.814716