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

$$\begin{aligned}\boldsymbol{g}(X) =&(X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{\rho-2})\\ =&g_0+g_1X+g_2X^2+\cdots+X^{\rho-2}\end{aligned}$$

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

1089-7798/03$17.00 © 2003 IEEE

with the same code symbol, consequently their symbol location vectors have at most one 1-component in common. Let $\mathcal{Z}(\mathcal{C}_b^{(i)}) = \{z(\boldsymbol{b}) : \boldsymbol{b} \in \mathcal{C}_b^{(i)}\}$ be the set of symbol location vectors of the p^s codewords in the ith coset $\mathcal{C}_b^{(i)}$ of $\mathcal{C}_b^{(1)}$. It follows from the structural properties of the cosets of $\mathcal{C}_b^{(1)}$ developed in Section II that two symbol location vectors in $\mathcal{Z}(\mathcal{C}_b^{(i)})$ do not have any 1-component in common.

For $1 \leq i \leq p^s$, form a $p^s \times \rho p^s$ matrix $\boldsymbol{A}_i$ over GF(2) whose rows are the p^s symbol location vectors in $\mathcal{Z}(\mathcal{C}_b^{(i)})$. Since the weight of each vector in $\mathcal{Z}(\mathcal{C}_b^{(i)})$ is ρ, the total number of 1-entries in $\boldsymbol{A}_i$ is ρp^s. Since no two symbol location vectors in $\mathcal{Z}(\mathcal{C}_b^{(i)})$ have any 1-component in common, the weight of each column of $\boldsymbol{A}_i$ is one. Therefore, $\boldsymbol{A}_i$ is a (1, ρ)-regular matrix with column and row weights 1 and ρ, respectively. In fact, it follows from the definition of the symbol location vector of a codeword in $\mathcal{C}_b$ and the structural properties of the codewords in each coset $\mathcal{C}_b^{(i)}$ that $\boldsymbol{A}_i$ consists of a row of ρ $p^s \times p^s$ *permutation matrices*. Matrix $\boldsymbol{A}_i$ is called the *symbol location matrix* of the coset $\mathcal{C}_b^{(i)}$. The class of symbol location matrices, $\mathcal{A} = \{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_{p^s}\}$, has the following structural properties: (1) no two rows in the same matrix $\boldsymbol{A}_i$ have any 1-component in common; and (2) no two rows from two different member matrices, $\boldsymbol{A}_i$ and $\boldsymbol{A}_j$, have more than one 1-component in common.

Let γ be a positive integer such that $1 \leq \gamma \leq p^s$. Form the following $\gamma p^s \times \rho p^s$ matrix over GF(2):

$$\boldsymbol{H}_{GA}(\gamma) = \begin{bmatrix} \boldsymbol{A}_1 \\ \vdots \\ \boldsymbol{A}_\gamma \end{bmatrix}.$$

This matrix is a (γ, ρ)-regular matrix with column and row weights γ and ρ, respectively. It follows from the structural properties of the member matrices $\boldsymbol{A}_i$ in the class $\mathcal{A}$ that no two rows (or two columns) of $\boldsymbol{H}_{GA}(\gamma)$ have more than one 1-component in common. This implies that there are no 4 ones in $\boldsymbol{H}_{GA}(\gamma)$ at the 4 corners of a rectangle. This ensures that the associated Tanner graph of $\boldsymbol{H}_{GA}(\gamma)$ is free of cycles of length 4 and hence its girth is at least 6. We note that $\boldsymbol{H}_{GA}(\gamma)$ is exactly in Gallager's original form [1] for the parity check matrix of a (γ, ρ)-regular LDPC code. Therefore, the null space of this matrix gives a (γ, ρ)-regular *Gallager-LDPC code*, denoted $\mathcal{C}_{GA}(\gamma)$, of length $n = \rho p^s$ whose Tanner graph has girth at least 6. The rate of this code is at least $(\rho - \gamma)/\rho$. If $\rho = q - 1$, the code is quasicyclic.

Since no two rows in $\boldsymbol{H}_{GA}(\gamma)$ have more than one 1-component in common and each column of the matrix has weight γ, there are γ rows in $\boldsymbol{H}_{GA}(\gamma)$ that are orthogonal [10] on every code bit of $\mathcal{C}_{GA}(\gamma)$. It follows from *Massey's orthogonality theorem*, [10], [11] that the minimum distance of $\mathcal{C}_{GA}(\gamma)$ is at least $\gamma + 1$. This lower bound on minimum distance can be improved if the structure of parity check matrix $\boldsymbol{H}_{GA}(\gamma)$ is taken into account. Recall that each symbol location matrix $\boldsymbol{A}_i$ in $\mathcal{A}$ consists of a row of ρ $p^s \times p^s$ permutation matrices. Therefore, the parity check matrix $\boldsymbol{H}_{GA}(\gamma)$ consists of ρ columns of $p^s \times p^s$ permutation matrices. Each column of $\boldsymbol{H}_{GA}(\gamma)$ consists of γ sections, each section consists of a single 1-component. For a set of columns in the parity check matrix $\boldsymbol{H}_{GA}(\gamma)$ to sum to zero, the number of columns in the set must be even. This implies that the minimum distance of $\mathcal{C}_{GA}(\gamma)$ must be even. As a result, for even γ, the minimum distance of $\mathcal{C}_{GA}(\gamma)$ is then at least $\gamma + 2$. Summarizing the above results, we have the following lower bound on the minimum distance $d_{\min}(\gamma)$ of $\mathcal{C}_{GA}(\gamma)$:

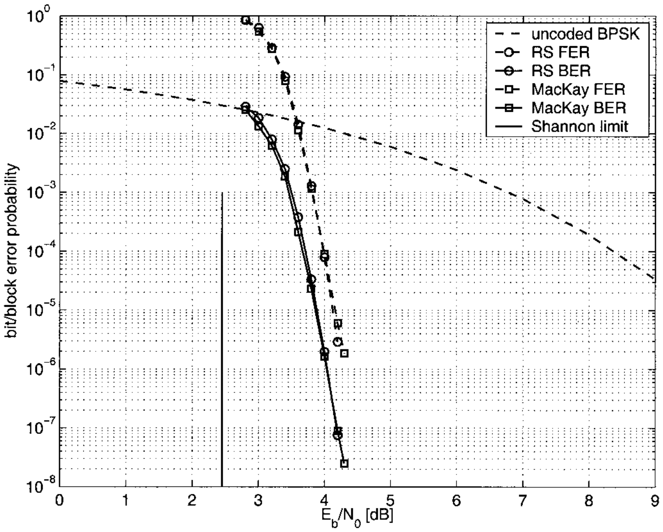

Fig. 1. Error performance of the (2048,1723) RS-based Gallager (6,32)-regular LDPC code with construction field $\mathrm{GF}(2^6)$.

$$d_{\min}(\gamma) \geq \begin{cases} \gamma + 1, & \text{for odd } \gamma \\ \gamma + 2, & \text{for even } \gamma. \end{cases}$$

For a given choice of p, s, and ρ, we can construct a sequence of Gallager-LDPC codes of length $n = \rho p^s$ for $\gamma = 1, 2, \ldots, p^s$. For a given choice of p, s, and γ, we can construct a sequence of Gallager-LDPC codes of different lengths with minimum distance at least $\gamma + 1$ or $\gamma + 2$ by varying ρ.

Since the construction is based on the $(\rho, 2, \rho - 1)$ shortened RS code $\mathcal{C}_b$ over $\mathrm{GF}(p^s)$, we call $\mathcal{C}_b$ and $\mathrm{GF}(p^s)$ the base code and construction field, respectively.

IV. Some RS-Based Gallager-LDPC Codes and Their Error Performances

In this section, we present several RS-based LDPC codes and their error performances with iterative decoding using the SPA. For performance computation, we assume BPSK transmission over an AWGN channel.

A. Example 1

Let GF(2^6) be the field for code construction. Let $\rho = 32$. Then the base code is the (32,2,31) shortened RS code over GF(2^6). The location vector of each symbol in GF(2^6) is a 64-tuple over GF(2) with a single 1-component. Suppose we set $\gamma = 6$. Then the RS-based Gallager-LDPC code $\mathcal{C}_{GA}(6)$ is a (6,32)-regular (2048,1723) code with rate 0.841 and minimum distance at least 8. The bit and block error performances with the SPA decoding are shown in Fig. 1. At the BER of 10^{-6}, the code performs only 1.55 dB from the Shannon limit and achieves a 6-dB coding gain over the uncoded BPSK. For LDPC codes, the code length of 2048 is considered to be short. For such a short LDPC code, its error performance is very good. For comparison, the performance of the MacKay's computer generated code of

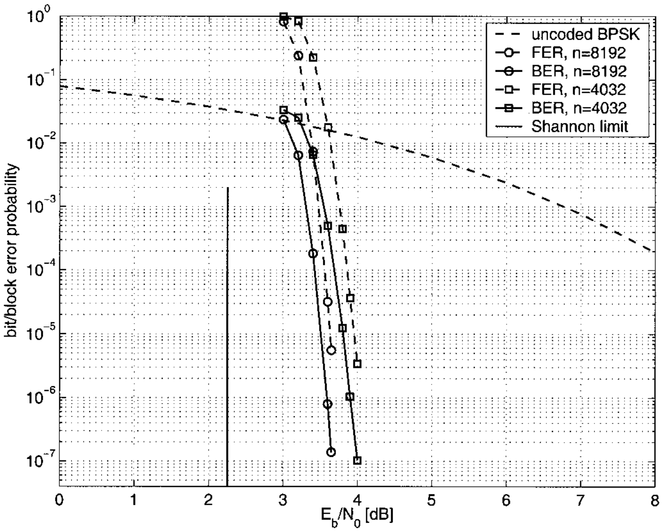

Fig. 2. Error performances of the (8192,6754) RS-based Gallager (6,32)-regular LDPC code with construction field $\mathrm{GF}(2^8)$, and the (4032,3307) RS-based Gallager (60,63)-regular quasi-cyclic LDPC code with construction field $\mathrm{GF}(2^6)$.

the same length and rate is also given in Fig. 1. We can see that the two codes have almost the same error performance. △△

B. Example 2

Again we use $\mathrm{GF}(2^6)$ as the construction field. Let $\rho = 63$. Then the base code for construction is the (63,2,62) RS code. Set $\gamma = 60$. The code constructed is a (60,63)-regular (4032,3307) LDPC quasicylic code with rate 0.82 and minimum distance at least 62. The error performance of the code is shown in Fig. 2. At the BER of 10^{-6}, the code performs 1.65 dB from the Shannon limit. Since the code has a very large minimum distance, there should not be any error floor or the error floor occurs at a very low bit error rate. △△

C. Example 3

Suppose we construct a (32,2,31) shortened RS code $\mathcal{C}_b$ over $\mathrm{GF}(2^8)$. Set $\gamma = 6$. Then the Gallager-LDPC code constructed based on $\mathcal{C}_b$ is a (6,32)-regular (8192,6754) code with rate 0.824 and minimum distance at least 8. The error performance of the LDPC code is also shown in Fig. 2. At the BER of 10^{-6}, the code performs 1.25 dB from the Shannon limit and achieves a 6.7-dB coding gain over the uncoded BPSK. △△

D. Example 4

Again we use $\mathrm{GF}(2^8)$ as the construction field. The shortened RS code $\mathcal{C}_b$ used for code construction is the (48,2,47) code over $\mathrm{GF}(2^8)$. Set $\gamma = 6$. Then the Gallager-LDPC code constructed is a (6,48)-regular (12288,10845) code with rate 0.8825 and minimum distance at least 8. The error performance is shown in Fig. 3. At the BER of 10^{-6}, the code performs 1.1 dB from the Shannon limit. For comparison, the performance of the MacKay's computer generated code of the same length and rate is also given in Fig. 3. We see that in this case MacKay's code is 0.2 dB better than RS-based Gallager-LDPC code. However, the error performance of the RS-based Gallager-LDPC code has larger dropping rate. The performance curves of the two codes may cross each other at lower BER. △△

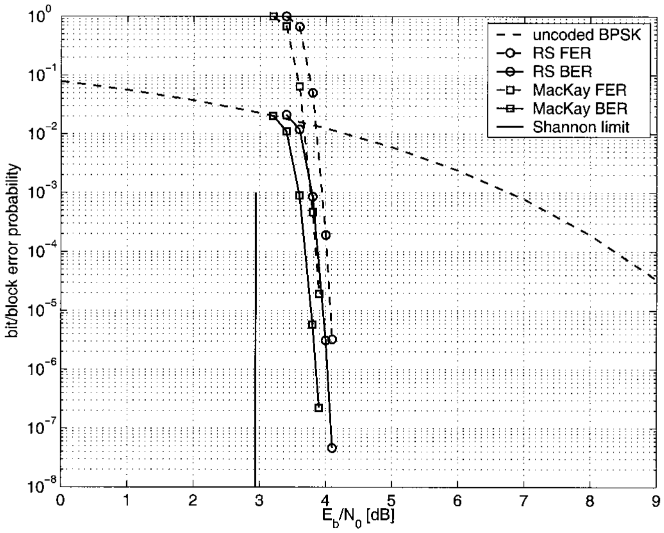

Fig. 3. Error performance of the (12288,10845) RS-based Gallager (6,48)-regular LDPC code with construction field $\mathrm{GF}(2^8)$.

V. Conclusion

In this letter, a simple RS-based algebraic method for constructing regular LDPC codes with girth at least 6 has been presented. Construction gives a large class of regular LDPC codes in Gallager's original form that perform well with the SPA.

References

[1] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, pp. 1645–1646, 1996.

[3] M. Sipser and D. Spielman, "Expander codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1710–1722, Nov. 1996.

[4] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–432, Mar. 1999.

[5] T. J. Richardson, M. A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619–637, Feb. 2001.

[6] T. J. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599–618, Feb. 2001.

[7] S.-Y. Chung, G. D. Forney Jr, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Communun. Lett.*, vol. 5, pp. 58–60, Feb. 2001.

[8] Y. Kou, S. Lin, and M. Fossorier, "Low density parity check codes: A rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2711–2736, Nov. 2001.

[9] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.

[10] S. Lin and D. J. Costello Jr, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice Hall, 1983.

[11] J. L. Massey, *Threshold Decoding*. Cambridge, MA: MIT Press, 1963.