Low Complexity Encoding Algorithm of RS-based QC-LDPC Codes

Mu Zhang, Li Tang, Qin Huang*, Zulin Wang
School of Electronic and Information Engineering, Beihang University, Beijing, China, 100191
email:zhangmu@ee.buaa.edu.cn; neathe@163.com;
qhuang.smash@gmail.com (*corresponding author); wzulin_201@163.com;

***Abstract*—This paper presents a novel encoding algorithm for QC-LDPC codes constructed from Reed-Solomon codes. The encoding is performed in the transform domain via Galois Fourier transformation. Message bits are encoded in sections corresponding to sub-matrices of the parity-check matrix in the transform domain. Because of the structure of the parity-check matrices of these LDPC codes, the encoding can be easily implemented with some linear-feedback shift registers, thus efficiently reduces the hardware cost.**

***Index Terms*—LDPC codes, RS codes, encoding complexity, matrix transformation, Galois Fourier transform.**

I. Introduction

In recent years, low-density parity-check (LDPC) codes in quasi-cyclic (QC) form have been deeply investigated [1]-[9]. A number of QC-LDPC codes have been constructed and shown good error performance. Based on their QC structure, the computational complexity and memory cost of LDPC encoders can be efficiently reduced [10],[11]. RS-based LDPC codes are a sub-class of QC-LDPC codes [12]. They are constructed algebraically based on the parity-check matrices of RS codes. It has been shown that this class of QC-LDPC codes have good error-performance and structural property, e.g., minimum distance and girth [12] [13]. Moreover, their algebraic nature is even stronger in the matrix transformation domain via Galois Fourier transform (GFT).

In this paper, we propose an novel algorithm to encode RS-based LDPC codes by adopting their transform domain algebraic property. The transform domain generator matrices of RS-based LDPC codes can be constructed as a group of generator matrices of RS codes. Hence, we encode the message bits to a transformed codeword with RS encoders. Then, we devise a simple and fast post-processing to transfer the codeword binary. The computational complexity of the encoding can be reduced to about 20% or even below 10% compared to traditional time domain encoding. Moreover, due to the structure of RS codes and conjugacy constraint in the transform domain, the encoding processing can be simply implemented with some linear-feedback shift registers (LFSRs).

II. Matrix Transformation and q-Fold Dispersion

Consider the QC matrix $\mathbf{H}$ consists of $m \times n$ circulants,

$$\mathbf{H} \triangleq [\mathbf{A}_{i,j}] = \begin{bmatrix} \mathbf{A}_{0,0} & \mathbf{A}_{0,1} & \cdots & \mathbf{A}_{0,n-1} \\ \mathbf{A}_{1,0} & \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{m-1,0} & \mathbf{A}_{m-1,1} & \cdots & \mathbf{A}_{m-1,n-1} \end{bmatrix}, \quad (1)$$

where $\mathbf{A}_{i,j}$ is $q \times q$ circulant. For simplicity, we assume that $q = 2^s - 1$, which is reasonable for practical QC-LDPC codes, where s is a positive integer. It can be easily generalized when q is an odd factor of $2^s - 1$. Let α be a primary element in GF(q). Define the $q \times q$ Vandermonde matrix $\mathbf{V} = [\alpha^{-ij}]$ and the following row and column permutations $\pi_{m,n,q}$ for the $mq \times nq$ QC matrix,

$$\begin{cases} \pi_m^i &= m\,(i)_q + \lfloor i/q \rfloor\,, \quad 0 \le i < mq, \\ \pi_n^j &= n\,(j)_q + \lfloor j/q \rfloor\,, \quad 0 \le j < nq, \end{cases}$$

where $(i)_q$ denotes the smallest positive integer conjugate to $i \mod q$. Then, the GFT of $\mathbf{H}$ (1) is

$$\mathbf{H}^{\mathcal{F}} = \mathrm{diag}(\underbrace{\mathbf{V}, \mathbf{V}, \ldots, \mathbf{V}}_{m})\mathbf{H}\mathrm{diag}(\underbrace{\mathbf{V}^{-1}, \mathbf{V}^{-1}, \ldots, \mathbf{V}^{-1}}_{n}).$$

Moreover, we define the matrix transformation of $\mathbf{H}$ as

$$\hat{\mathbf{H}} \triangleq \mathbf{H}^{\mathcal{F},\pi_{m,n,q}} = \mathrm{diag}\left(\mathbf{B}_0, \mathbf{B}_1, \cdots, \mathbf{B}_{q-1}\right), \quad (2)$$

where $\mathbf{B}_t$'s, $0 \le t < q$, are matrices in GF(q). Let m' be the integer such that $n - m'$ equals to the minimum rank of $\mathbf{B}_t$'s for $0 \le t < q$. Suppose $\mathbf{D}_t$'s are $m' \times n$ matrices which define the null spaces of $\mathbf{B}_t$'s, i.e., $\mathbf{D}_t\mathbf{B}_t^{\mathsf{T}} = \mathbf{0}$ and $\mathrm{rank}(\mathbf{D}_t) + \mathrm{rank}(\mathbf{B}_t) = n$. We can construct the diagonal array

$$\hat{\mathbf{G}} = \mathrm{diag}\left(\mathbf{D}_0, \mathbf{D}_1, \cdots, \mathbf{D}_{q-1}\right).$$

Then, the $m'q \times nq$ matrix

$$\mathbf{G} = \hat{\mathbf{G}}^{\pi_{m',n,q},\mathcal{F}} \quad (3)$$

defines the null space of $\mathbf{H}$.

If $\mathbf{H}$ in (1) is binary, the diagonal submatrices in the transform domain will satisfy the following conjugacy constraint [12],

$$\mathbf{B}_{(2t)_q} = \mathbf{B}_t^{\circ 2}, \quad (4)$$

where $\circ$ denotes the Hadamard power, i.e., the entry at location (i,j) of $\mathbf{B}_{(2t)_q}$ is the square of the entry at location (i,j) of $\mathbf{B}_t$. Therefore, we can partition $\mathbf{B}_t$'s into conjugacy classes based on the constraint. In each conjugacy class, the matrices are the Hadamard powers of each other. We call the matrix with the smallest index conjugacy representative in each conjugacy class.

In addition, if $\mathbf{H}$ in (1) consists of circulant permutation circulants (CPMs) and zero matrices (ZMs), the conjugacy constraint becomes

$$\mathbf{B}_t = \mathbf{B}_1^{\circ t}. \tag{5}$$

In this case, $\mathbf{B}_1$ is called the base matrix in the transform domain. Moreover, $\mathbf{H}$ can be directly derived from its base matrix and vise versa. Actually, for each location (i,j) ($0 \leq i < m$, $0 \leq j < n$) where $\mathbf{A}_{i,j}$ has an 1 in the e-th ($0 \leq e < q$) position of the first row, the component of $\mathbf{B}_1$ at the same location is α^e; if $\mathbf{A}_{i,j}$ is a ZM, $\mathbf{B}_1$ at the location (i,j) is 0. Therefore, we can simply obtain a large class of algebra QC-LDPC codes based on the construction of their base matrices by replacing the components in the base matrices with corresponding CPMs/ZMs. This construction is referred to as q-fold dispersion [12].

III. RS-BASED LDPC CODES

Let n be a prime factor of $q = 2^s - 1$ and $2^s - 1 = cn$. Let α be a primitive element of GF(q). Suppose $\beta = \alpha^c$, then the following matrix

$$\mathbf{B} = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & \dots & (\beta^2)^{n-1} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \beta^m & (\beta^m)^2 & \dots & (\beta^m)^{n-1} \end{bmatrix}, \tag{6}$$

where $1 < m < n$, can be dispersed to the $mq \times nq$ parity-check matrix of an LDPC code with girth at least 6 [12]. Since $\mathbf{B}$ defines the null space of a cyclic RS code whose generator polynomial has $\beta, \beta^2, \dots, \beta^m$ as roots, this type of LDPC codes are called RS-based LDPC codes. The matrix transformation of $\mathbf{H}$ can be derived as

$$\mathbf{H}^{\mathcal{F},\pi} = diag(\mathbf{B}_0, \mathbf{B}_1, \dots, \mathbf{B}_{q-1}),$$

where $\mathbf{B}_1$ is the base matrix, also denoted as $\mathbf{B}$, and $\mathbf{B}_t = \mathbf{B}^{\circ t}$, $t = 0, 1, \dots, q-1$. It is straightforward that if $t = 0$ or t is divisible by n, $\mathbf{B}_t$ is an all "1" matrix so that its null space is given by

$$\mathbf{D}_t = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{bmatrix}. \tag{7}$$

Otherwise, $\mathbf{B}_t$ defines a cyclic (n, $n-m$) RS code whose generator polynomial has $\beta^t, \beta^{2t}, \dots, \beta^{mt}$ as roots. Thus, its null space is given by

$$\mathbf{D}_t = \begin{bmatrix} g_{0,t} & g_{1,t} & \cdots & g_{m-1,t} & 1 & 0 & \dots & 0 \\ 0 & g_{0,t} & \cdots & g_{m-2,t} & g_{m-1,t} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & g_{0,t} & g_{1,t} & \dots & 1 \end{bmatrix}, \tag{8}$$

where $g_{i,t}$ is the coefficient of the generator polynomial $\boldsymbol{g}_t(x) = \prod_{l=1}^{m}(x + \beta^{tl})$. Then, we obtain the cyclic form generator matrix of the RS-based LDPC codes in the transform domain,

$$\hat{\mathbf{G}} = \begin{bmatrix} \mathbf{D}_0 & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{D}_1 & \cdots & \mathbf{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{D}_{q-1} \end{bmatrix}. \tag{9}$$

IV. ENCODING IN TRANSFORM DOMAIN

Motivated by the simple implementation of encoding for RS codes, we propose to encode the RS-based LDPC codes with the transformed generator matrix. Hence, the codeword in the transform domain can be easily obtained with RS encoders.

Consider the RS-based LDPC code constructed from (6). Supposed that $\mathbf{m}$ is a binary message of length-k. Since $\mathbf{m}\hat{\mathbf{G}} \cdot \hat{\mathbf{H}}^{\mathsf{T}} = \mathbf{0}$, $\mathbf{m}\hat{\mathbf{G}}$ produces a transform domain codeword. According to the structure of $\hat{\mathbf{G}}$ (9), we can split $\mathbf{m}$ into q sections $\mathbf{m}_0, \mathbf{m}_1, \cdots, \mathbf{m}_{q-1}$. The length of each section $\mathbf{m}_t$ is equal to $r_t = \text{rank}(\mathbf{D}_t)$, $0 \leq t < q$. Thus, the encoding of $\mathbf{m}$ with $\hat{\mathbf{G}}$ can be considered as encoding of $\mathbf{m}_t$'s with $\mathbf{D}_t$'s. However, the $\mathbf{D}_t$'s in (7) and (8) produce non-systematic codewords. Hence, we apply the systematic form of $\mathbf{D}_t$'s in the encoding processing.

Moreover, thanks to the conjugacy constraint (4), we just take into account the conjugacy representatives of $\mathbf{D}_t$'s. Let l be any nonnegative integer. Suppose $t_0, t_1, ..., t_{\lambda-1}$ are the λ non-negative integers less than q that satisfy $t_i = \min_l\{(2^l t_i)_q\}$, $0 \leq i < \lambda$. Then, $\mathbf{D}_{t_0}, \mathbf{D}_{t_1}, ..., \mathbf{D}_{t_{\lambda-1}}$ are the λ conjugacy representatives in the transform domain of $\mathbf{G}$. Assume $\tilde{t}$ is the integer equal to $\min_l\{(2^l t)_q\}$, i.e., $\tilde{t} \in \{t_0, t_1, ..., t_{\lambda-1}\}$. Let $\tilde{\mathbf{D}}_t$ denote the conjugacy representative of $\mathbf{D}_t$ and $\tilde{g}_t(x)$ be the generator polynomial of $\tilde{\mathbf{D}}_t$. Then, we have $\tilde{\mathbf{D}}_t = \mathbf{D}_{\tilde{t}}$. Hence, the encoding is based on $\tilde{\mathbf{D}}_t$'s. For instance, suppose $\mathbf{m}_t = [m_{t,i}]$, $0 \leq i < r_t$. If $t = 0$ or t is divisible by n, the codeword section is

$$\tilde{\mathbf{c}}_t = [\sum_i m_{t,i} \vdots \mathbf{m}_t]. \tag{10}$$

Otherwise, $\tilde{\mathbf{c}}_t$ is generated based on polynomial calculations [14]. Let $\boldsymbol{m}_t(x)$ and $\boldsymbol{c}_t(x)$, respectively, be the polynomial representation of $\mathbf{m}_t$ and $\mathbf{c}_t$. We have

$$\tilde{\boldsymbol{c}}_t(x) = x^{n-r_t}\boldsymbol{m}_t(x) + \left(x^{n-r_t}\boldsymbol{m}_t(x)\right) \bmod \tilde{\boldsymbol{g}}_t(x). \tag{11}$$

However, the codeword $\tilde{\mathbf{c}}$ in the transform domain calculated by (10) and (11) may not satisfy the conjugacy constraint and thus produce non-binary codeword in the time domain. Thus, we perform post-processing on $\tilde{\mathbf{c}}$ by bases of sub-fields.

TABLE I

COMPLEXITY OF ETD AND TRADITIONAL ENCODING

		Bit Operations
ETD	Step 1)	$q\bar{k}(n-\bar{k})\log_2 q$
	Step 2)	$n(2q-\lambda)\log_2^2 q + nq\log_2 q$
	Step 3)	$nq^2(\log_2 q)^{\log_2 \frac{3}{4}}$
	Overall	$q\bar{k}(n-\bar{k})\log_2 q + n(2q-\lambda)\log_2^2 q + nq\log_2 q + nq^2(\log_2 q)^{\log_2 \frac{3}{4}}$
Traditional Encoding	Overall	$2q^2\bar{k}(n-\bar{k})$

Let η_i be the number of components in the conjugacy class with representative $\mathbf{D}_{t_i}$. Then, η_i divides q and GF(η_i) is a subfield of GF(q). Suppose $\beta_{i,0}, \beta_{i,1}, \ldots, \beta_{i,\eta_i-1}$ is a bases spanning GF(η_i). Then, we map $\tilde{\mathbf{c}}$ to $\hat{\mathbf{c}}$ with the following equation [15],

$$\hat{c}_{(2^\mu t_i)_q \cdot n+j} = \left(\sum_{l=0}^{\eta_i-1} \beta_{i,l} \tilde{c}_{(2^l t_i)_q \cdot n+j} \right)^{2^\mu}. \qquad (12)$$

It is obviously that $\hat{\mathbf{c}}$ satisfies the conjugacy constraint. This is because, given i and j, for all μ's that $0 \le \mu < \eta_i$, $\hat{c}_{(2^\mu t_i)_q \cdot n+j}$'s make up a conjugacy class, i.e., $\hat{c}_{(2t_i)_q \cdot n+j} = \hat{c}^2_{t_i \cdot n+j}$. Moreover, suppose $\hat{\mathbf{m}}$ is mapped from $\mathbf{m}$ by bases of sub-fields. The mapping from $\mathbf{m}$ to $\hat{\mathbf{m}}$, as well as $\tilde{\mathbf{c}}$ to $\hat{\mathbf{c}}$, is one to one, and we have $\hat{\mathbf{c}} = \hat{\mathbf{m}}\hat{\mathbf{G}}$ [15]. Then, $\hat{\mathbf{c}}\hat{\mathbf{H}}^{\mathsf{T}} = \mathbf{0}$ and thus, $\hat{\mathbf{c}}$ is also a transformed codeword of $\mathbf{m}$.

To sum up, we derive Algorithm 1 to encode RS-based LDPC codes.

Algorithm 1 Encoding in Transform Domain (ETD)

Input:

Message $\mathbf{m}$;

Transformed generator matrix $\hat{\mathbf{G}}$;

Output:

Binary codeword $\mathbf{c}$;

Steps:

1) Calculate $\tilde{\mathbf{c}}$ with (10) and (11).

2) Calculate $\hat{\mathbf{c}}$ with (12).

3) Inverse Galois Fourier transform from $\hat{\mathbf{c}}$ to binary codeword $\mathbf{c}$,

$$c_{jq+i} = \sum_{l=0}^{q-1} \hat{c}_{ln+j} \alpha^{il}.$$

Table I lists the computational complexity of Algorithm 1. Since the length of $\mathbf{m}_t$ is depend on r_t, we use $\bar{k} = k/q$ as the overall information section length for the estimation. For comparison, we also list the traditional encoding algorithm $\mathbf{c} = \mathbf{mG}$. Approximately, the proposed algorithm is cube complexity, while the traditional algorithm is biquadrate complexity. Moreover, ETD for RS-baed LDPC codes can be simply implemented based on LFSRs, as shown in Figure 1. For the first type of $\mathbf{D}_t$ (7), just one register and one binary adder are required. For the second type of $\mathbf{D}_t$ (8), we need $n-r_t$ registers, Galois field multipliers and Galois field adders.

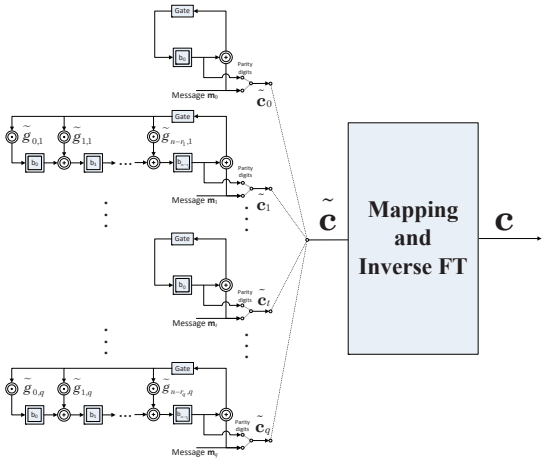

Fig. 1. The block diagram of the ETD for RS-based LDPC codes.

Thanks to the conjugacy constraint, we only need one LFSR for each conjugacy class, which contains q/λ components on average. Because there are q/n integers less than q and divisible by n, we need about $(q/n)/(q/\lambda) = \lambda/n$ LFSR's for the first type and about $(q-q/n)/(q/\lambda) = \lambda(n-1)/n$ LFSR's for the second type. Therefore, the hardware implementation of the first step of ETD only costs less than λn registers, Galois field multipliers and Galois field adders.

Example 1. *Consider the LDPC code $\mathcal{C}$ constructed by an (63,30)-RS code in GF(63). Then, $n = 63$, $q = 63$, $k = 2078$, $\bar{k} \approx 33$ and $\lambda = 13$. Thus, ETD requires 772178 bit operations while the traditional encoding requires 7858620 bit operations. In other words, the computational complexity of ETD is only 0.098 of the traditional one.*

V. CONCLUSION

In this paper we proposed a novel encoding algorithm following GFT approach for RS-based LDPC codes. The encoding takes advantages of the encoding of RS codes. Its computational complexity is much lower than the traditional time domain encoders. Apparently, this approach is also available to other cyclic-code-based QC-LDPC codes [8], [9] with a slight modification. The implementation of general encoding of these types of LDPC codes can be significant reduced.

ACKNOWLEDGMENT

This work was supported by National Natural Science Foundation of China under Grant 61201156.

REFERENCES

[1] N. Bonello, C. S. Chen, and L. Hanzo, "Construction of regular quasi-cyclic protograph LDPC codes based on Vandermonde matrices," *IEEE Trans. Vehicular Technology*, vol. 57, no. 4, pp. 2583–2588, Jul. 2008.

[2] Y. Y. Tai, L. Lan, L. Zheng, S. Lin and K. Abdel-Ghaffar, " Algebraic construction of quasi-cyclic LDPC codes for the AWGN and erasure channels," *IEEE Trans. Commun.*, vol 54, no. 7, pp. 1765–1774, Oct. 2006.

[3] J. L. Fan, "Array codes as low-density parity-check codes," in *proc. Int. Symp. Turbo Codes*, Brest, France, Sep. 2-7, 2000, pp.543-546.

[4] S. Myung and K. Yang, " A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem," *IEEE Commun. Lett.*, vol. 9, no. 9, pp. 823–825, Sep. 2005.

[5] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Disc. Appl. Math.*, vol. 111, pp. 157–175, 2001.

[6] S. J. Johnson and S. R. Weller, "A family of irregular LDPC codes with low encoding complexity," *IEEE Commun. Lett.*, vol. 7, no. 2, pp. 79–81, Feb. 2003.

[7] M. Yang and W. E. Ryan, "Performance of efficiently encodable low-density parity-check codes in noise bursts on the EPR4 channel," *IEEE Trans. Magn.*, vol. 40, no. 2, part 1, pp. 507–512. Mar. 2004.

[8] L. Lan, L. Zeng, Y. Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2429–2458, Jul. 2007.

[9] N. Kamiya, "High-rate quasi-cyclic low-density parity-check codes derived from finite affine planes," *IEEE Trans. Inform. Theory*, vol. 53, no. 4, pp. 1444–1459, Apr. 2007.

[10] Z. Li, L. Chen, L. Zeng, S. Lin and W. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *IEEE Trans. Commun.*, vol. 54, no. 1, pp. 71–81, 2006.

[11] N. Kamiya and E. Sasaki, "Efficient encoding of QC-LDPC codes related to cyclic MDS codes," *IEEE Journal on Selected Areas in Communications*,vol. 27, no. 6, pp. 846–854, 2009. 2009, 27(6): 846-854.

[12] Q. Diao, Q. Huang, S. Lin, and K. Abdel-Ghaffar, "A matrix theoretic approach for analyzing quasi-cyclic low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 58, no. 6, pp. 4030–4048, June. 2012.

[13] I. Djurdjevic, J. Xu, K. Abdel-Ghaffar, S. Lin, "A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer Berlin Heidelberg, 2003. 98-107.

[14] S. Lin,DJ. Costello, "Error control coding," Englewood Cliffs: Prentice-hall, 2004.

[15] Q. Huang, L. Tang, S. He, Z. Xiong, and Z. Wang, "Low-Complexity Encoding of Quasi-Cyclic Codes Based on Galois Fourier Transform," submitted to *IEEE Trans. Commun.*.