Girth-Eight Reed-Solomon Based QC-LDPC Codes

Xin Xiao, Bane Vasić
School of Electrical and Computer Engineering
University of Arizona
Tucson, Arizona
Email: {7xinxiao7,vasic}@email.arizona.edu

Shu Lin, Khaled Abdel-Ghaffar
School of Electrical and Computer Engineering
University of California, Davis
Email: {shulin,ghaffar}@ucdavis.edu

William E. Ryan
Zeta Associates Inc. USA
Email: bill.ryan.work@gmail.com

***Abstract*—This paper presents a class of regular quasi-cyclic (QC) LDPC codes whose Tanner graphs have girth at least eight. These codes are constructed based on the conventional parity-check matrices of Reed-Solomon (RS) codes with minimum distance 5. Masking their parity-check matrices significantly reduces the numbers of short cycles in their Tanner graphs and results in codes which perform well over the AWGN channel in both waterfall and low error-rate regions.**

I. Introduction

Some recent research [1]–[5] combines two powerful categories of codes, namely RS, and LDPC codes, to form powerful classes of hybrid codes which, not only perform well, but are also practically implementable. These research works take two different approaches. The first approach is to encode and decode an RS code as a powerful LDPC code through a specific mapping [1], [2]. The second approach is to construct a structured QC-LDPC code based on the conventional parity-check matrix of an RS code under certain constraints [3]–[5]. Such a code is referred to as an RS-QC-LDPC code.

In this paper, we present a specific method for constructing a class of regular RS-QC-LDPC codes whose Tanner graphs have girth at least 8. The codes in this class are constructed based on the conventional parity-check matrices of RS codes with minimum distance 5. Masking is used to reduce the numbers of short cycles of lengths 8, 10, 12 and 14 in their Tanner graphs. We show that girth-8 structure in conjunction with making results in RS-QC-LDPC codes that perform well over the AWGN channel in both waterfall and low-error rate regions.

II. Construction of QC-LDPC Codes Based on Finite Fields

In this section, we give a general description of construction of QC-LDPC codes based on finite fields of characteristic 2.

Let β be an element of order n in GF(2^s) where n is a factor of 2^s-1. The set $\mathbf{S}_n$=$\{1, \beta, ..., \beta^{n-1}\}$ forms a cyclic subgroup of GF(2^s). For $0 \leq i < n$, we represent the element β^i by a *circulant permutation matrix* (CPM) over GF(2) of size $n \times n$ (with rows and columns labeled from 0 to $n-1$, respectively) whose *generator* (the top row) has the unit-element "1" of GF(2^s) as its *single nonzero component* at the position i. We denote this CPM by $CPM_n(\beta^i)$. The representation of the element β^i by $CPM_n(\beta^i)$ is *unique* and the mapping between β^i and $CPM_n(\beta^i)$ is *one-to-one*. This matrix representation of β^i is referred to as the $n \times n$ *CPM-dispersion* of β^i with respect to the cyclic subgroup $\mathbf{S}_n$ of GF(2^s). We represent the 0-element of GF(2^s) by a *zero matrix* (ZM) of size $n \times n$.

Since n is a factor of 2^s-1, there is some l for which ln divides 2^s-1. Let δ be an element in GF(2^s) of order ln, i.e., $\delta^{ln}=1$. Then, β can be expressed as the l-th power of δ, i.e., $\beta=\delta^l$. Let $\mathbf{W}_{ln}$ be the cyclic subgroup of GF(2^s) with order ln generated by the powers of δ. Then, $\mathbf{W}_{ln}$ contains $\mathbf{S}_n$ as a subgroup. If we disperse each element in $\mathbf{W}_{ln}$ by a CPM of size $ln \times ln$ as described above, then the element $\beta^i=\delta^{il}$, $0 \leq i < n$, as an element in $\mathbf{W}_{ln}$, is dispersed into a CPM of size $ln \times ln$, denoted by $CPM_{ln}(\beta^i)$, whose generator has its single 1-component at position il. In this case, every element β^i in $\mathbf{S}_n$ is uniquely dispersed into a CPM of size $ln \times ln$ which is referred to as the $ln \times ln$ CPM-dispersion of β^i with respect to the super group $\mathbf{W}_{ln}$ of $\mathbf{S}_n$. The number ln is called the *dispersion-factor* with respect to $\mathbf{W}_{ln}$. Therefore, each element in $\mathbf{S}_n$ can be one-to-one dispersed into a CPM of a size equal to the order of a cyclic subgroup of GF(2^s) which contains $\mathbf{S}_n$ as a subgroup (including $\mathbf{S}_n$ itself).

For $0 < d < b \leq n$, let $\mathbf{B}(d,b)$ be a $d \times b$ matrix over GF(2^s) with all the nonzero entries from the cyclic subgroups $\mathbf{S}_n$ of GF(2^s). Suppose we disperse each nonzero entry in $\mathbf{B}(d,b)$ into a CPM of size of $ln \times ln$ with respect to a cyclic subgroup $\mathbf{W}_{ln}$ of GF(2^s) with order ln that contains $\mathbf{S}_n$ as a subgroup and each zero entry into a ZM of size $ln \times ln$. This results in a $d \times b$ array $\mathbf{H}_{ln}(d,b)$ of CPMs and ZMs of size $ln \times ln$. The array $\mathbf{H}_{ln}(d,b)$ is called the $ln \times ln$ *CPM-dispersion* of $\mathbf{B}(d,b)$. The array $\mathbf{H}_{ln}(d,b)$ is a $dln \times bln$ matrix over GF(2). Typically, $ln >> 1$, and $\mathbf{H}_{ln}(d,b)$ is a sparse matrix. The null space over GF(2) of $\mathbf{H}_{ln}(d,b)$ gives a QC-LDPC code, denoted by $\mathcal{C}_{ln,ldpc}(d,b)$. Since the code $\mathcal{C}_{ln,ldpc}(d,b)$ is constructed based on the matrix $\mathbf{B}(d,b)$, the matrix $\mathbf{B}(d,b)$ is referred to as the *base matrix*.

The performance of the QC-LDPC code $\mathcal{C}_{ln,ldpc}(d,b)$ very much depends on the girth, distribution of short cycles, and degree distributions of check nodes (CNs) and variable nodes (VNs) of its Tanner graph $\mathcal{G}_{ln}(d,b)$.

It is proved in [6] that the Tanner graph of $\mathcal{C}_{ln,ldpc}(d,b)$ has girth at least 6 if the base matrix $\mathbf{B}(d,b)$ satisfies the following constraint: any 2×2 submatrix of $\mathbf{B}(d,b)$ is *nonsingular* (NS). We referred this constraint as the 2×2 *submatrix NS-*

978-1-5386-7048-4/18/$31.00 ©2018 IEEE

constraint, denoted by 2×2 *SNS-constraint*. Also proved in [6] is a necessary and sufficient condition on $\mathbf{B}(d, b)$ for the Tanner graph of $\mathcal{C}_{ln,ldpc}(d, b)$ to have girth at least 8. We rephrase the condition in the following theorem.

Theorem 1: Let $\mathbf{B}$ be a matrix over GF(2^s) and $\mathcal{C}$ be the QC-LDPC code given by the null space over GF(2) of the binary CPM-dispersion of $\mathbf{B}$. A necessary and sufficient condition for the Tanner graph of $\mathcal{C}$ to have girth of at least 8 is that no 2×2 or 3×3 submatrix of $\mathbf{B}$ has two identical non-zero terms in its determinant expansion.

For simplicity, we refer the necessary and sufficient condition given in Theorem 1 as the $2 \times 2/3 \times 3$ submatrix (SM) constraint. It is clear the $2 \times 2/3 \times 3$ SM-constraint implies the 2×2 SNS-constraint. Various algebraic methods for constructing 2×2 SNS-constrained base matrices can be found in [5]–[8]. So far, no efficient method for constructing $2 \times 2/3 \times 3$ SM-constrained base matrices has been proposed. In the next section, we present a class of parity-check matrices of RS codes that satisfy $2 \times 2/3 \times 3$ SM-constraint. Hence, they can be used as base matrices to construct QC-LDPC codes whose Tanner graphs have girth at least 8.

III. Construction of a Class of Regular RS-QC-LDPC Codes with Girth Six and Eight

A. A Class of $(4, b)$-Regular RS-QC-LDPC with Girth at Least Six

Let β be an element of order n in GF(2^s) where n is factor of $2^s - 1$ and is divisible by 3. The set $\mathbf{S}_n$=$\{1, \beta, ..., \beta^{n-1}\}$ forms a cyclic subgroup of GF(2^s). Form the following $4 \times n$ RS parity-check matrix over GF(2^s):

$$\mathbf{B}_{RS}(4, n) = \left[(\beta^i)^j\right]_{1 \le i \le 4, 0 \le j < n}. \quad (1)$$

The null space over GF(2^s) of $\mathbf{B}_{RS}(4, n)$ gives a 2^s-ary $(n, n-4, 5)$ cyclic RS code, denoted by $\mathcal{C}_{RS}(4, n)$, of length n, dimension $n-4$ and minimum distance 5 whose generator polynomial has β, β^2, β^3 and β^4 as roots [7].

In general, the RS matrix $\mathbf{B}_{RS}(4, n)$ given by (1) does not satisfy the 2×2 SNS-constraint. However, if we choose a group of columns from $\mathbf{B}_{RS}(4, n)$ properly, a 2×2 constrained RS matrix can be formed. The null space over GF(2^s) of the 2×2 constrained RS matrix gives a shortened RS code of $\mathcal{C}_{RS}(4, n)$ with the same minimum distance 5. In the following, we present a method to construct 2×2 SNS-constrained submatrices of $\mathbf{B}_{RS}(4, n)$.

Label the columns of the RS matrix $\mathbf{B}_{RS}(4, n)$ from 0 to $n-1$. Since n is divisible 3, $n = 3m$. Partition the column labels of $\mathbf{B}_{RS}(4, n)$ into $m = n/3$ disjoint label-triplets, $(0, m, 2m), (1, 1+m, 1+2m), ..., (l, l+m, l+2m), ..., (m-1, 2m-1, 3m-1)$. From each label-triplet $(l, l+m, l+2m), 0 \le l < m$, we take one (any one) label. This gives us m column labels. We denote these m column labels with $j_0, j_1, ..., j_{m-1}$ and arrange them in the order $0 \le j_0 < j_1 < ... < j_{m-1} < n$. (Note that the column label j_l may not be taken from the label-triplet $(l, l+m, l+2m)$.) These m chosen column labels form a column label-set $\Lambda_m = \{j_0, j_1, ..., j_{m-1}\}$. Next, we take m columns, labeled by $j_0, j_1, ..., j_{m-1}$, from $\mathbf{B}_{RS}(4, n)$ and form the following $4 \times m$ submatrix of $\mathbf{B}_{RS}(4, n)$:

$$\mathbf{B}_{RS,\Lambda_m}(4, m) = \left[(\beta^i)^{j_l}\right]_{1 \le i \le 4, 0 \le l < m}. \quad (2)$$

This RS matrix satisfies the 2×2 SNS-constraint as proved in the following theorem.

Theorem 2: The RS matrix $\mathbf{B}_{RS,\Lambda_m}(4, m)$ given by (2) satisfies the 2×2 SNS-constraint.

Proof: Label the columns of $\mathbf{B}_{RS,\Lambda_m}(4, m)$ from 0 to $m-1$. For $1 \le i < k \le 4$ and $0 \le s < t < m$, consider a 2×2 submatrix of $\mathbf{B}_{RS,\Lambda_m}(4, m)$ with four entries $(\beta^i)^{j_s}, (\beta^i)^{j_t}, (\beta^k)^{j_s}, (\beta^k)^{j_t}$ at the locations $(i, s), (i, t), (k, s)$ and (k, t). Suppose this matrix is singular. Then, we must have $\beta^{(k-i)(j_t-j_s)} = 1$. Note that $0 < k - i \le 3$. From the composition of each label-triplet, we find that $j_t - j_s$ is not divisible by m and nonzero. Then, the product $(k-i)(j_t-j_s)$ is not divisible by $n = 3m$ and $\beta^{(k-i)(j_t-j_s)} \ne 1$. Hence, the above 2×2 submatrix of $\mathbf{B}_{RS,\Lambda_m}(4, m)$ must be nonsingular and $\mathbf{B}_{RS,\Lambda_m}(4, m)$ satisfies the 2×2 SNS-constraint.

From the above construction of a 2×2 SNS-constrained RS matrix, we readily see that for $4 < b \le m$, any b consecutive columns of $\mathbf{B}_{RS}(4, n)$, including end-around case, form a 2×2 SNS-constrained RS matrix $\mathbf{B}_{RS,\Lambda_b}(4, b)$. Or any $4 \times b$ submatrix obtained by deleting $m-b$ columns from $\mathbf{B}_{RS,\Lambda_m}(4, m)$ satisfies the 2×2 SNS-constraint. Note that all the entries in $\mathbf{B}_{RS,\Lambda_b}(4, b)$ are elements in the cyclic group $\mathbf{S}_n$ of GF(2^s) and non-zero.

The $ln \times ln$ CPM-dispersion of $\mathbf{B}_{RS,\Lambda_b}(4, b)$ gives a $4 \times b$ array $\mathbf{H}_{RS,ln}(4, b)$ of CPMs of size $ln \times ln$ which consists of 4 (b) *row (column)-blocks* of CPMs. Each CPM row (column)-block of $\mathbf{H}_{RS,ln}(4, b)$ consists of ln rows (columns). Each row (column) in a CPM row (column)-block contains b (4) 1-entries which reside in b (4) *separate* CPMs in the CPM row (column)-block, one in each. The b CPMs in each CPM row-block of $\mathbf{H}_{RS,ln}(4, b)$ are distinct, and the 4 CPMs in each CPM column-block of $\mathbf{H}_{RS,ln}(4, b)$ are distinct, except for the case that $\mathbf{B}_{RS,\Lambda_b}(4, b)$ consisting of a column of four 1-entries.

The null space over GF(2) of $\mathbf{H}_{RS,ln}(4, b)$ gives a (4, b)-regular RS-QC-LDPC code, denoted by $\mathcal{C}_{RS,ln,ldpc}(4, b)$, of length lnb. The rate of $\mathcal{C}_{RS,ln,ldpc}(4, b)$ is *at least* $(b-4)/b$ which is the rate of the RS code $\mathcal{C}_{RS}(4, b)$. Since CPM-dispersion of $\mathbf{B}_{RS}(4, b)$ may induce *redundant (linearly dependent)* rows in $\mathbf{H}_{RS,ln}(4, b)$, the rank of $\mathbf{H}_{RS,ln}(4, b)$ may be *smaller* than the number of rows dln in $\mathbf{H}_{RS,ln}(4, m)$. The 2×2 SNS-constraint structure of $\mathbf{B}_{RS}(4, b)$ ensures that $\mathbf{H}_{RS,ln}(4, b)$, as a matrix, has the following structure [6]: *any two rows (or two columns) do not have more than one position in which both have 1-entries*. Such a structure is referred to as *row-column (RC) constraint* [5]–[7]. The RC-constraint structure of $\mathbf{H}_{RS,ln}(4, b)$ ensures that the Tanner graph of the RS-QC-LDPC code $\mathcal{C}_{RS,ln,ldpc}(4, b)$ has a girth at least 6.

B. Construction of Regular RS-QC-LDPC Codes with Girth at least Eight

As pointed out earlier, Theorem 1 gives only a necessary and sufficient condition on a base matrix whose CPM-dispersion gives a QC-LDPC code with girth at least 8 but it does not provide a *specific method* for constructing such a code. In the following, we present a set of conditions on selection of columns from the RS matrix $\mathbf{B}_{RS}(4,n)$ given by (1) to form an RS submatrix to meet the $2\times 2/3\times 3$ SM-constraint. Hence, the null space of its CPM-dispersion gives an RS-QC-LDPC code whose Tanner graph has girth at least 8.

Consider the m label-triplets $(l, l+m, l+2m), 0 \le l < m$, for the columns of the $4 \times n$ RS matrix $\mathbf{B}_{RS}(4,n)$ formed in Section II.A with $m = n/3$. For $4 < b \le m$, we choose b column-labels $j_0, j_1, ..., j_{b-1}$ from b label-triplets such that $0 \le j_0 < j_1 < ... < j_{b-1} < n$. These b chosen column labels form a column label-set $\Lambda_b = \{j_0, j_1, ..., j_{b-1}\}$. Next, we take b columns, labeled with $j_0, j_1, ..., j_{b-1}$, from $\mathbf{B}_{RS}(4,n)$ and form a $4 \times b$ submatrix $\mathbf{B}_{RS,\Lambda_b}(4,b)$ of $\mathbf{B}_{RS}(4,n)$. The RS matrix $\mathbf{B}_{RS,\Lambda_b}(4,b)$ satisfies the $2 \times 2/3 \times 3$ SM-constraint if and only if the column labels in the set $\Lambda_b = \{j_0, j_1, ..., j_{b-1}\}$ satisfy the conditions given in the following theorem.

Theorem 3: The $4 \times b$ RS matrix $\mathbf{B}_{RS,\Lambda_b}(4,b)$ satisfies the $2 \times 2/3 \times 3$ SM-constraint if and only if for any three labels $j_{i_1}, j_{i_2}, j_{i_3}$ in the set $\Lambda_b = \{j_0, j_1, ..., j_{b-1}\}$ such that $j_{i_1} < j_{i_2} < j_{i_3}$, the following nine conditions satisfy:

$$\begin{array}{ll} \text{(p1)}\ \ l_{i_3} \neq 2l_{i_2} - l_{i_1}, & \text{(p2)}\ n \nmid l_{i_3} + 2l_{i_1} - 3l_{i_2}, \\ \text{(p3)}\ \ l_{i_3} \neq \frac{3l_{i_2} - l_{i_1}}{2}, & \text{(p4)}\ n \nmid l_{i_2} + l_{i_3} - 2l_{i_1}, \\ \text{(p5)}\ n \nmid l_{i_2} + 2l_{i_3} - 3l_{i_1}, & \text{(p6)}\ n \nmid 2l_{i_2} + l_{i_3} - 3l_{i_1}, \\ \text{(p7)}\ n \nmid 2l_{i_3} - l_{i_1} - l_{i_2}, & \text{(p8)}\ n \nmid 3l_{i_3} - 2l_{i_1} - l_{i_2}, \\ \text{(p9)}\ n \nmid 3l_{i_3} - l_{i_1} - 2l_{i_2}. & \end{array} \quad (3)$$

Then, the null space of the $n \times n$ CPM-dispersion $\mathbf{H}_{RS,n,\Lambda_b}(4,b)$ of $\mathbf{B}_{RS,\Lambda_b}(4,b)$ gives a (4, b)-regular RS-QC-LDPC code $\mathcal{C}_{RS,n,ldpc}(4,n)$ whose Tanner graph $\mathcal{G}_{RS,n,ldpc}(4,n)$ has girth of at least 8.

We do not provide a proof of the above theorem here due to its length and page limitation but we outline the approach to the proof. The derivations of the nine necessary and sufficient conditions given in the theorem are based the structure of the RS matrix $\mathbf{B}_{RS}(4,n)$ and the partition of column labels of $\mathbf{B}_{RS}(4,n)$. For each chosen column label j_{i_l} from a label-triplet, the locations of 1-entries in each CPM of the CPM column-block obtained by the CPM-dispersion of the 4 entries in the j_{i_l}th-column of $\mathbf{B}_{RS}(4,n)$ are uniquely specified by the label j_{i_l} and the 4 entries in the j_{i_l}-th column of $\mathbf{B}_{RS}(4,n)$. If the b labels $j_0, j_1, ..., j_{b-1}$ chosen from label-triplets for which the parity-check matrix $\mathbf{H}_{RS,n,\Lambda_b}(4,b)$ formed does not contains a sequence of six 1-entry locations in $\mathbf{H}_{RS,n,\Lambda_b}(4,b)$ that corresponds to a configuration of a cycle of length 6 in a bipartite graph, then the Tanner graph $\mathcal{G}_{RS,\Lambda_b,ldpc}(4,b)$ associated with $\mathbf{H}_{RS,n,\Lambda_b}(4,b)$ does not contain cycles of length 6. In this case, $\mathcal{G}_{RS,\Lambda_b,ldpc}(4,b)$ has girth at least 8. It follows from Theorem 1 that the RS matrix $\mathbf{B}_{RS,\Lambda_b}(4,b)$ must satisfy the necessary and sufficient conditions given by Theorem 1, i.e., the $2 \times 2/3 \times 3$ SM-constraints. Based on the above facts, we derive the nine necessary and sufficient conditions given in Theorem 3.

Since the nine necessary and sufficient conditions given in Theorem 3 are expressed only in terms of the labels (integers) for the columns of $\mathbf{B}_{RS}(4,n)$. The computation complexity required for finding a column-label set Λ_b whose labels satisfy the nine conditions given by (2) is quite simple.

C. Masking

Masking [5], [7], [8] is a technique for removing short cycles and/or enlarging the girth of the Tanner graph of a QC-LDPC code constructed by CPM-dispersion of a base matrix. Masking a $d \times b$ base matrix $\mathbf{B}(d,b) = [a_{i,j}]_{1\le i\le d, 0\le j<b}$ over GF(2^s) can be modeled mathematically as follows. Let $\mathbf{Z}(d,b) = [z_{i,j}]_{1\le i\le d, 0\le j<b}$ be a $d \times b$ matrix over GF(2), a sub-field of GF(2^s). Define the following product of $\mathbf{Z}(d,m)$ and $\mathbf{B}(d,b)$: $\mathbf{B}_{mask}(d,b) = \mathbf{Z}(d,b) \otimes \mathbf{B}(d,b) = [z_{i,j}a_{i,j}]_{1\le i\le d, 0\le j<b}$ where $z_{i,j}a_{i,j} = a_{i,j}$ if $z_{i,j} = 1$ and $z_{i,j}a_{i,j} = 0$ if $z_{i,j} = 0$. In this matrix product, the nonzero entries in $\mathbf{B}(d,b)$ at the locations corresponding to zero entries in $\mathbf{Z}(d,b)$ are replaced (or *masked*) by zeros. The binary CPM-dispersion of $\mathbf{B}_{mask}(d,b)$ gives a $d \times b$ masked array, denoted by $\mathbf{H}_{mask}(d,b)$, of CPMs and ZMs. We call $\mathbf{Z}(d,b)$ and $\mathbf{B}_{mask}(d,b)$ the *masking matrix* and the *masked base matrix*, respectively. The null space of $\mathbf{H}_{mask}(d,b)$ gives a (masked) RS-QC-LDPC code, denoted by $\mathcal{C}_{mask,ldpc}(d,b)$.

The $2 \times 2/3 \times 3$ SM-constraint structure of an RS base matrix in conjunction with proper masking will significantly reduce the number of short cycles and changing the degree distributions of CNs and VNs in the Tanner graph of the masked RS-QC-LDPC code. As a result, the masked code achieve very good error performances in both waterfall and low error rate regions. This will be demonstrated by Examples given in the next section.

In the design of a high-rate (or a medium high-rate) regular LDPC code to achieve a relative low error rate without an error-floor, the parity-check matrix of the code must have a column weight at least 4. For a regular (or irregular) LDPC code with rate below 3/4 to achieve a good waterfall error-performance, the column weight (or the average column weight) of its parity-check matrix should be small, typically 3 or between 3 and 4. If the column weight of a base matrix $\mathbf{B}(d,b)$ for constructing a low to medium high rate QC-LDPC code is large, *masking* is needed to reduce its column weight and eliminate short cycles in its Tanner graph, especially short cycles of lengths g (girth of the Tanner graph), g + 2, g + 4 and g + 6.

IV. Examples

In the following, we construct three codes to demonstrate that girth-8 structure in conjunction with masking indeed results in RS-QC-LDPC codes that perform well. In decoding of these codes, we use the *min-sum algorithm* (MSA) [9].

Example 1: Let GF(2^8) be the field for code construction. Let β be a primitive element of GF(2^8). The order of β is

255. Set $n = 255$ which is divisible by 3. Hence, $n = 3 \times 85$. We first construct a 4×255 RS matrix $\mathbf{B}_{RS}(4, 255) = [(\beta^i)^j]_{1 \le i \le 4, 0 \le j < 255}$ in the form of (1). This RS matrix does not satisfies the 2×2 SNS-constraint. Label the columns of $\mathbf{B}_{RS}(4, 255)$ from 0 to 254. Partition the column labels of $\mathbf{B}_{RS}(4, 255)$ into 85 disjoint triplets, $(l, l + 85, l + 170), 0 \le l < 85$. Set $b = 8$. From these 85 triplets, we find the following set $\Lambda_8 = \{2, 5, 7, 13, 20, 32, 54, 60\}$ of column labels which satisfy the 9 conditions given by (3). The labels in Λ_8 are the first numbers of the triplets (2, 87, 172), (5, 90, 175), (7, 92, 177), (13, 98, 183), (20, 105, 190), (32, 117, 202), (54,139, 224), (60, 145, 230), respectively.

Take 8 columns, labeled by 2, 5, 7, 13, 20, 32, 54 and 60, from $\mathbf{B}_{RS}(4, 255)$ and form a 4×8 RS matrix $\mathbf{B}_{RS,\Lambda_8}(4, 8)$. Then, $\mathbf{B}_{RS,\Lambda_8}(4, 8)$ satisfies the $2 \times 2/3 \times 3$ SM-constraint. The 255×255 CPM-dispersion of $\mathbf{B}_{RS,\Lambda_8}(4, 8)$ gives a 4×8 array $\mathbf{H}_{RS,255,\Lambda_8}(4, 8)$ of CPMs and ZMs of size 255×255. It is a 1020×2040 matrix with column and row weights 4 and 8, respectively. The rank of $\mathbf{H}_{RS,255,\Lambda_8}(4, 8)$ is 1015, not a full-rank matrix. The null space over GF(2) of $\mathbf{H}_{RS,255,\Lambda_8}(4, 8)$ gives a (4, 8)-regular (2040, 1025) RS-QC-LDPC code $\mathcal{C}_{RS,\Lambda_8,ldpc}(4, 8)$ with rate 0.5025 which is slightly higher than 0.5. Since $\mathbf{B}_{RS,\Lambda_8}(4, 8)$ satisfies the $2 \times 2/3 \times 3$ SM-constraint, the Tanner graph $\mathcal{G}_{RS,\Lambda_8,ldpc}(4, 8)$ of $\mathcal{C}_{RS,\Lambda_8,ldpc}(4, 8)$ has girth at least 8. The distribution of cycles of lengths 8, 10, 12 and 14 in $\mathcal{G}_{RS,\Lambda_8,ldpc}(4, 8)$ is $\{53805, 407490, 8168670, 133452720\}$. The girth of $\mathcal{G}_{RS,\Lambda_8,ldpc}(4, 8)$ is 8. The total number of cycles of lengths 8, 10, 12 and 14 is 142,082,685, a very large number of short cycles.

Suppose we mask the RS matrix $\mathbf{B}_{RS,\Lambda_8}(4, 8)$ with the following masking matrix:

$$\mathbf{Z}(4, 8) = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad (4)$$

We obtain a 4×8 masked RS matrix $\mathbf{B}_{RS,\Lambda_8,mask}(4, 8)$. The 255×255 CPM-dispersion of $\mathbf{B}_{RS,\Lambda_8,mask}(4, 8)$ gives a 4×8 array of $\mathbf{H}_{RS,255,\Lambda_8,mask}(4, 8)$ of CPMs and ZMs of size 255×255. It is a 1020×2040 matrix with column and row weights 3 and 6, respectively. The rank of $\mathbf{H}_{RS,255,\Lambda_8,mask}(4, 8)$ is 1020, a full-rank matrix. The null space over GF(2) of $\mathbf{H}_{RS,255,\Lambda_8,mask}(4, 8)$ gives a (3, 6)-regular (2040, 1020) QC-LDPC code $\mathcal{C}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ with rate 1/2.

The distribution of cycles of lengths 8, 10, 12, and 14 in the Tanner graph $\mathcal{G}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ of the masked code $\mathcal{C}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ is $\{765, 10200, 84405, 743580\}$. The masked Tanner graph $\mathcal{G}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ also has girth 8 but the number of cycles of length 8 is only 765 which is much smaller than the 53805 cycles of length 8 in the unmasked Tanner graph $\mathcal{G}_{RS,\Lambda_8,ldpc}(4, 8)$. The total number of cycles of lengths 8, 10, 12 and 14 in $\mathcal{G}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ is 838,950. Comparing the cycle distributions of the unmasked and masked Tanner graphs, we find that masking results in a large reduction in short cycles from 142,082,685 to 838,950, *a reduction by a factor of almost* 169.

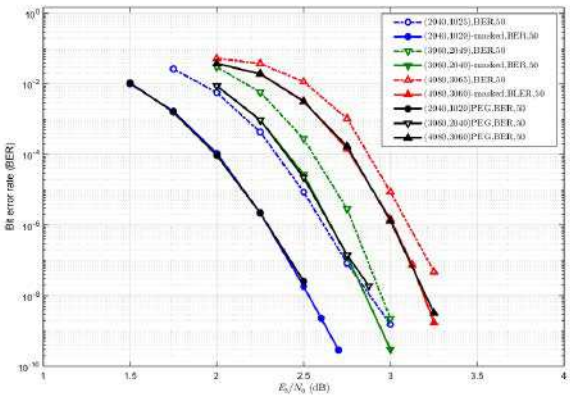

Fig. 1. The BER performances of the RS-QC-LDPC codes given in Examples 1 and 2.

The BER performances of the unmasked (4, 8)-regular (2040, 1025) RS-QC-LDPC code $\mathcal{C}_{RS,\Lambda_8,ldpc}(4, 8)$ and the masked (3, 6)-regular (2040, 1020) RS-QC-LDPC code $\mathcal{C}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ over the AWGN channel using BPSK signaling decoded with 50 iterations of the MSA scaled by factors of 0.70 and 0.75, respectively, are shown in Fig. 1. We see that the masking improves the error performances of the unmasked code. This performance improvement is due to the large reduction of short cycles and the change of degree distributions of the Tanner graph after masking, from (4, 8)-regular distribution to (3, 6)-regular distribution. The masked (3, 6)-regular (2040, 1020) RS-QC-LDPC code $\mathcal{C}_{RS,\Lambda_8,mask,ldpc}(4, 8)$ achieves a BER of 10^{-9} without a visible error-floor and at the BER of 10^{-9}, it performs 1.5 dB from its threshold (1.1 dB). It has a 0.3 dB coding gain over the unmasked (4, 8)-regular (2040, 1025) RS-QC-LDPC code.

For comparison, the performance of a (2040, 1020) LDPC code $\mathcal{C}_{PEG}$ constructed by using the *PEG-algorithm* [10] is also included in Fig.1. We see that the performances of the (2040, 1020) RS-QC-LDPC code and the PEG code $\mathcal{C}_{PEG}$ overlap with each other in the range of simulation. The parity-check matrix of the PEG code $\mathcal{C}_{PEG}$ has constant column weight 3 and row weight 6. Furthermore, it is not quasi-cyclic.

Examples 1 shows that the 4×8 masking matrix Z(4, 8) given by (4) is very effective in reducing short cycles of the Tanner graph of an unmasked RS-QC-LDPC code. This masking matrix can be used as a building block to construct larger masking matrices for larger RS base matrices. This masking matrix has a simple structure. The second pair of columns is a repetition of the first pair of columns and the fourth pair of columns is a repetition of third pair of columns. A simple expansion of this masking matrix is to repeat the first pair and the third pair of columns t times. This expansion results in a $4 \times 4t$ masking matrix $\mathbf{Z}(4, 4t)$ [8].

Example 2: This example is a continuation of Example 1.

In this example, we construct two RS-QC-LDPC codes, one with rate 2/3 and the other with rate 3/4. From the 85 column label-triplets formed in Example 1, we choose two sets, $\Lambda_{12} = \{0, 1, 4, 9, 11, 20, 24, 35, 41, 49, 90, 225\}$ and $\Lambda_{16} = \{1, 3, 6, 13, 21, 32, 44, 59, 64, 73, 77, 83, 111, 212, 226, 239\}$, of column labels from the 85 label-triplets $(l, l + 85, l + 170), 0 \leq l < 85$, formed in Example 1 for the RS matrix $\mathbf{B}_{RS}(4, 255)$. The column labels of each set satisfy the 9 conditions given by (3). Using these two sets of column labels, we form a 4×12 RS matrix $\mathbf{B}_{RS,\Lambda_{12}}(4, 12)$ and a 4×16 $\mathbf{B}_{RS,\Lambda_{16}}(4, 16)$, respectively. Both RS matrices satisfy the $2 \times 2/3 \times 3$ SM-constraint.

The null spaces over GF(2) of the 255×255 CPM-dispersions of $\mathbf{B}_{RS,\Lambda_{12}}(4, 12)$ and $\mathbf{B}_{RS,\Lambda_{16}}(4, 16)$ give a (4, 12)-regular (3060, 2049) RS-QC-LDPC code and a (4, 16)-regular (4080, 3065) RS-QC-LDPC code, respectively. The Tanner graphs of both codes have girth 8, one with 259845 cycles of length 8 and the other with 688500 cycles of length 8. The distributions of short cycles of lengths 8, 10 and 12 in the Tanner graphs are $\{259845, 3886710, 116167800\}$ and $\{688500, 17485860, 703291020\}$, respectively.

To mask the RS matrix $\mathbf{B}_{RS,\Lambda_{12}}(4, 12)$, we form a 4×12 masking matrix $\mathbf{Z}(4, 12)$ which is constructed by repeating the first pair and the third pair of columns of the masking matrix $\mathbf{Z}(4, 12)$ given by (4) three times (i.e., $t = 3$). The masking matrix $\mathbf{Z}(4, 16)$ for the 4×16 RS matrix $\mathbf{B}_{RS,\Lambda_{16}}(4, 16)$ consists of four 4×4 circulants whose generators are: (1 1 1 0), (1 1 1 0), (1 1 1 0) and (1 1 0 1). The first 3 circulants of $\mathbf{Z}(4, 16)$ are identical. Masking $\mathbf{B}_{RS,\Lambda_{12}}(4, 12)$ and $\mathbf{B}_{RS,\Lambda_{16}}(4, 16)$ with $\mathbf{Z}(4, 12)$ and $\mathbf{Z}(4, 16)$, respectively, we obtain two masked RS matrices $\mathbf{B}_{RS,\Lambda_{12},mask}(4, 12)$ and $\mathbf{B}_{RS,\Lambda_{16},mask}(4, 16)$. The null spaces over GF(2) of the 255×255 CPM-dispersions of the two masked RS matrices give a (3, 9)-regular (3060, 2040) RS-QC-LDPC code and a (3, 12)-regular (4080, 3060) RS-QC-LDPC code with rates 2/3 and 3/4, respectively. The Tanner graphs of both masked codes have girth 8. The distributions of short cycles of lengths 8, 10 and 12 in the Tanner graphs of the two masked RS-QC-LDPC codes are $\{7905, 105825, 1444320\}$ and $\{32640, 495210, 9570915\}$, respectively. We see that masking reduces the short cycles of the Tanner graphs of the two unmasked RS-QC-LDPC codes drastically.

The BER performances of the above four codes over the AWGN channel using BPSK signaling decoded with 50 iterations of the MSA are shown in Fig. 1. The scaling factors for both unmasked codes are 0.70 and the scaling factors for both masked codes are 0.75. We see that masking improves the error performances of both codes. Both performance improvements are due to the large reduction of short cycles and the change of degree distributions of the Tanner graph after masking. The masked (3, 9)-regular (3060, 2040) RS-QC-LDPC code $\mathcal{C}_{RS,\Lambda_{12},mask,ldpc}(4, 12)$ achieves a BER of 10^{-9} without a visible error-floor and at the BER of 10^{-9}, it performs 1.11 dB from its threshold (1.79 dB). The masked (3, 12)-regular (4080, 3060) RS-QC-LDPC code $\mathcal{C}_{RS,\Lambda_{16},mask,ldpc}(4, 16)$ achieves a BER of 10^{-9} without a visible error-floor and at the BER of 10^{-9}, it performs 0.98 dB from its threshold (2.27 dB). For comparison, the performances of a (3060, 2040) LDPC code and a (4080,3060) LDPC code constructed by PEG-algorithm are also included in Fig.1. We see that the performances of the RS-QC-LDPC code and the PEG code of the same length overlap with each other in the range of simulation. The (3060, 2040) PEG code even suffers from error floor at the BER of 10^{-8}. The RS-QC-LDPC code and the PEG code of the same length have the same degree distribution. However, the PEG codes are not quasi-cyclic.

V. Conclusion

In this paper, we presented designs and constructions of (4, b)- and (3, b)-regular QC-LDPC codes based on the conventional parity-check matrices of a class of RS codes of minimum distance 5. The Tanner graphs of these codes have girth at least 8. We also showed that if we mask the base matrix of a girth-8 (4, b)-regular RS-QC-LDPC code, we can reduce the number of short cycles in its Tanner graph and obtain a (3, b)-regular RS-QC-LDPC code which performs well. The methods presented in this paper for constructing binary RS-QC-LDPC codes can be generalized for constructing non-binary RS-QC-LDPC codes.

Acknowledgment

This work was partially supported by the NSF grants ECCS-1500170 and SaTC-1813401, the AppoTech and NuFront gift grants.

References

[1] S. Lin, K. Abdel-Ghaffar, J. Li and K. Liu, "Iterative soft-decision decoding of Reed-Solomon codes of prime lengths," *Proc. IEEE Int. Symp. Inform. Theory* (ISIT), Aachen, Germany, Jun. 25-30, 2017, pp. 341–345.

[2] S. Lin, K. Abdel-Ghaffar, J. Li, and K. Liu, "A scheme for encoding and iterative soft decision decoding of cyclic codes of prime lengths: Applications to Reed-Solomon, BCH, and quadratic residue codes" submitted to *the IEEE Trans. Inf. Theory*, 2016 (revised 2018).

[3] Q. Diao, J. Li, S. Lin and I. F. Blake, "New classes of partial geometries and their associated LDPC codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 2947-2965, Jun. 2016.

[4] J. Li, K. Liu, S. Lin and K. Abdel-Ghaffar, "Reed-Solomon based nonbinary globally coupled LDPC codes: Correction of random errors and bursts of erasures," *Proc. IEEE Int. Symp. Inform. Theory* (ISIT), Aachen, Germany, Jun. 25-30, 2017, pp. 381–385.

[5] J. Li, S. Lin, K. Abdel-Ghaffar, W.E. Ryan, and D.J. Costello, Jr., *LDPC Code Designs, Constructions, and Unification*, Cambridge, UK: Cambridge University Press, 2017.

[6] 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. Inf. Theory*, vol. 58, no. 6, pp. 4030 - 4048, Jun. 2012.

[7] W. E. Ryan and S. Lin, *Channel Codes: Classical and Modern*, New York, NY: Cambridge Univ. Press, 2009.

[8] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Algebraic LDPC codes: Construction, low error-floor, large girth and a reduced-complexity decoding scheme," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 2626-2637, Aug. 2015.

[9] J. Chen and M. P. C. Fossorier, "Near optimum universal belief propagation based decoding of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 50, no.3, p. 406 - 414, Mar. 2002.

[10] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graph," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386-398, Jan. 2005.