High-Rate Nonbinary Regular Quasi-Cyclic LDPC Codes for Optical Communications

Murat Arabaci, *Student Member, IEEE*, Ivan B. Djordjevic, *Member, IEEE*, Ross Saunders, and Roberto M. Marcoccia

***Abstract*—The parity-check matrix of a nonbinary (NB) low-density parity-check (LDPC) code over Galois field $\mathrm{GF}(q)$ is constructed by assigning nonzero elements from $\mathrm{GF}(q)$ to the 1s in corresponding binary LDPC code. In this paper, we state and prove a theorem that establishes a necessary and sufficient condition that an NB matrix over $\mathrm{GF}(q)$, constructed by assigning nonzero elements from $\mathrm{GF}(q)$ to the 1s in the parity-check matrix of a binary quasi-cyclic (QC) LDPC code, must satisfy in order for its null-space to define a nonbinary QC-LDPC (NB-QC-LDPC) code. We also provide a general scheme for constructing NB-QC-LDPC codes along with some other code construction schemes targeting different goals, e.g., a scheme that can be used to construct codes for which the fast-Fourier-transform-based decoding algorithm does not contain any intermediary permutation blocks between bit node processing and check node processing steps. Via Monte Carlo simulations, we demonstrate that NB-QC-LDPC codes can achieve a net effective coding gain of 10.8 dB at an output bit error rate of 10^{-12}. Due to their structural properties that can be exploited during encoding/decoding and impressive error rate performance, NB-QC-LDPC codes are strong candidates for application in optical communications.**

***Index Terms*—Low-density parity-check (LDPC) codes, optical communications, quasi-cyclic (QC) codes.**

I. Introduction

In 1962, Gallager introduced low-density parity-check (LDPC) codes in his seminal work [1]. Having been almost completely forgotten for over 30 years, LDPC codes were rediscovered by MacKay and Neal. They showed that if decoded by using the sum–product algorithm (SPA), the performance of LDPC codes can approach the Shannon limit [2], [3]. After their rediscovery, there has been a lot of research on LDPC codes and their applications in communication, broadcasting, and storage systems [4], [5].

Recently, there has been a growing interest in nonbinary LDPC (NB-LDPC) codes, which were initially proposed by Davey and MacKay [6]. Davey and MacKay showed that NB-LDPC codes can outperform their binary counterparts when decoded using a modified SPA, which we refer to as q-ary SPA (QSPA). They also provided an efficient way of conducting QSPA using the fast Fourier transform (FFT), in short FFT-QSPA. FFT-QSPA is further analyzed and improved in [7]. A mixed-domain version of the FFT-QSPA (MD-FFT-QSPA), which reduces the computational complexity by transforming the multiplications into additions with the help of logarithm and exponentiation operations, is proposed in [8].

Quasi-cyclic LDPC (QC-LDPC) codes comprise a subclass of LDPC codes. They are particularly advantageous due to their simple encoders [9], [10], and modular structure that reduces the hardware implementation complexity of their decoders [11], [12]. Combining the benefits of NB-LDPC codes and QC-LDPC codes, NB-QC-LDPC codes are a particularly important subclass of LDPC codes. NB-QC-LDPC codes are studied from the algebraic code design perspective in [13]. The authors use finite fields to generate a parity-check matrix $\mathbf{H}$ for a binary QC-LDPC (B-QC-LDPC) code with a girth of at least 6, and then, following certain design criteria, they assign nonzero elements from the Galois field $\mathrm{GF}(q)$ to the 1s in $\mathbf{H}$ to construct $\mathbf{H}^{(q)}$. The null-space of the resulting parity-check matrix $\mathbf{H}^{(q)}$ defines a q-ary NB-QC-LDPC code having a girth of at least 6. In this paper, we generalize their work with a theorem that establishes a necessary and sufficient condition in order for the null-space of a matrix $\mathbf{H}^{(q)}$, constructed from the parity-check matrix $\mathbf{H}$ of a B-QC-LDPC code by assigning nonzero elements from $\mathrm{GF}(q)$ to the 1s in $\mathbf{H}$, to define an NB-QC-LDPC code. This theorem is our main contribution. We also demonstrate that high-rate, regular NB-QC-LDPC codes are very suitable for use in optical communications. In addition to the NB-QC-LDPC code construction, we discuss several NB-LDPC code constructions that might better suit certain design goals.

In Section II, we introduce QC-LDPC codes, and state and prove our theorem. Section III presents different assignment schemes that yield different NB-LDPC codes using the same B-QC-LDPC code. We provide our simulation results and discussions in Section IV. Finally, we conclude the paper with directions for future work in Section V.

II. QC-LDPC Codes

The parity-check matrix $\mathbf{H}$ of a (γ, ρ)-regular B-QC-LDPC code is given by

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{0,0} & \mathbf{H}_{0,1} & \cdots & \mathbf{H}_{0,\rho-1} \\ \mathbf{H}_{1,0} & \mathbf{H}_{1,1} & \cdots & \mathbf{H}_{1,\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{\gamma-1,0} & \mathbf{H}_{\gamma-1,1} & \cdots & \mathbf{H}_{\gamma-1,\rho-1} \end{bmatrix} \quad (1)$$

Manuscript received January 15, 2009; revised May 26, 2009 and July 23, 2009. First published August 04, 2009; current version published October 09, 2009. This work was supported in part in part by Opnext, Inc., and by the National Science Foundation under Grant IHCS-0725405.

M. Arabaci and I. B. Djordjevic are with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA (e-mail: arabaci@ece.arizona.edu; ivan@ece.arizona.edu).

R. Saunders and R. M. Marcoccia are with Opnext, Inc., Los Gatos, CA 95032 USA (e-mail: rsaunders@opnext.com; rmarcoccia@opnext.com).

Digital Object Identifier 10.1109/JLT.2009.2029062

where each $\mathbf{H}_{i,j}$ is a $B \times B$ circulant matrix over $\mathrm{GF}(2)$, for $0 \leq i < \gamma$ and $0 \leq j < \rho$ [9], [13]. According to Tanner [14], a code $\mathfrak{C}$ is a B-QC-LDPC code if whenever $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{\rho-1})$, where each section $\mathbf{v}_j$ has B components, is a codeword in $\mathfrak{C}$, so is its sectional cyclic shift by l places to the right $\mathbf{v}^{(l)} = (\mathbf{v}_0^{(l)}, \mathbf{v}_1^{(l)}, \ldots, \mathbf{v}_{\rho-1}^{(l)})$ for all $l, 0 \leq l \leq B$. (Note that $\mathbf{v} = \mathbf{v}^{(0)} = \mathbf{v}^{(B)}$.) We refer to this property as the *fundamental property* of QC-LDPC codes.

Every LDPC code can be represented by a bipartite graph known as its Tanner graph. The girth of an LDPC code is the length of the shortest cycle in its Tanner graph [10]. Girth is an important parameter in LDPC code design since it affects the code performance under SPA decoding. Especially, cycles of length 4 must be avoided in the code. In this paper, we only consider LDPC codes of girth greater than 4, i.e., no two rows of the parity-check matrix have more than one position where they both have nonzero components.

In this paper, we focus our attention on regular NB-QC-LDPC codes over the extension field $\mathrm{GF}(q)$, where $q = 2^m$ for some positive integer m. By extending Tanner's definition, we define a q-ary QC-LDPC code as a linear block code over $\mathrm{GF}(q)$ for which the fundamental property of QC-LDPC codes hold. It is natural to attempt to construct parity-check matrices of (γ, ρ) -regular NB-QC-LDPC codes by assigning nonzero elements from $\mathrm{GF}(q)$ to the nonzero components in the parity-check matrices of corresponding (γ, ρ) -regular B-QC-LDPC codes. The following example shows that this method does not always result in an NB-QC-LDPC code.

Example: Let $\mathbf{H}$ be obtained by randomly assigning nonzero elements from $\mathrm{GF}(4)$ to the nonzero components of the binary parity-check matrix of a B-QC-LDPC code

$$\mathbf{H} = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \quad (2)$$

Observe that

$$\mathbf{v} = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 2 \quad 2 \quad 3 \quad 0 \quad 0 \quad 3] \quad (3)$$

is a codeword in the corresponding code, i.e., $\mathbf{v}\mathbf{H}^{\mathrm{T}} = \mathbf{0}$, whereas

$$\mathbf{v}^{(1)} = [0 \quad 1 \quad 0 \quad 0 \quad 2 \quad 0 \quad 0 \quad 2 \quad 3 \quad 3 \quad 0 \quad 0] \quad (4)$$

is not, i.e., $\mathbf{v}^{(1)}\mathbf{H}^{\mathrm{T}} \neq \mathbf{0}$. That is, the null-space of $\mathbf{H}$ does not define a 4-ary QC-LDPC code. $\diamondsuit$

The following theorem provides a necessary and sufficient condition that $\mathbf{H}$ must satisfy in order for the code defined by its null-space to preserve the fundamental property. The definitions of rotation and scaling matrices, and the proof of Theorem 1 can be found in the Appendix.

Theorem 1: The fundamental property of QC-LDPC codes is preserved by a code with the parity-check matrix of $\mathbf{H}$ if and only if

$$\mathbf{R}_{M,B}\mathbf{H}\mathbf{R}_{N,B}^{-1} = \mathbf{C}\mathbf{H} \quad (5)$$

for some rotation matrices $\mathbf{R}_{M,B}$ and $\mathbf{R}_{N,B}$, and a scaling matrix $\mathbf{C}$.

III. Assignment Schemes

Suppose that we are given the parity-check matrix $\mathbf{H}^{(b)}$ of a (γ, ρ) -regular B-QC-LDPC code and that $\mathbf{H}$ is obtained by assigning nonzero elements from $\mathrm{GF}(q)$ to the nonzero components of $\mathbf{H}^{(b)}$. If $\mathbf{H}$ satisfies the condition given in Theorem 1, then its null-space defines an NB-QC-LDPC code; otherwise, it defines an NB-LDPC code, which does not possess the fundamental property. In this section, in addition to NB-QC-LDPC code construction, we discuss several NB-LDPC code constructions that might better suit certain design goals.

A. Scheme 1 (Random Assignment Scheme)

In this scheme, nonzero elements from $\mathrm{GF}(q)$ are randomly assigned to the 1s in $\mathbf{H}^{(b)}$ to generate $\mathbf{H}$. The null-space of $\mathbf{H}$ defines a (γ, ρ) -regular NB-LDPC code. Intuitively, random assignment scheme should yield the best performance among the (γ, ρ)-regular NB-LDPC codes since there is no interdependence between the selection of nonzero elements from $\mathrm{GF}(q)$.

B. Schemes 2 and 3

Our goal in these schemes is to design NB-LDPC codes such that when decoded using the FFT-based decoding algorithm [6], [7], the intermediary permutation operations before processing the data at the nodes are eliminated. In schemes 2 and 3, we achieve this by assigning the same elements from $\mathrm{GF}(q)$ to the 1s in the same column and row of $\mathbf{H}^{(b)}$, using

$$\mathbf{H} = \mathbf{H}^{(b)}\mathbf{C}_r \quad (6)$$

$$\mathbf{H} = \mathbf{C}_l\mathbf{H}^{(b)} \quad (7)$$

respectively, for some scaling matrices $\mathbf{C}_r$ and $\mathbf{C}_l$ whose nonzero components are selected randomly from $\mathrm{GF}(q)$.

By eliminating all the permutation blocks in the decoding algorithm, these assignment schemes result in codes whose decoders require smaller silicon area when implemented in the hardware.

C. Scheme 4

Here, our goal is to construct an NB-QC-LDPC code whose parity-check matrix $\mathbf{H}$ satisfies Theorem 1. One way of constructing such an $\mathbf{H}$ matrix is as follows. Extract the 0th row of submatrices of $\mathbf{H}^{(b)}$. Randomly select ρ nonzero elements from $\mathrm{GF}(q)$ and assign these ρ random elements to ρ 1s in each row of the 0th row of submatrices of $\mathbf{H}^{(b)}$, preserving the order. Now, randomly generate a scaling matrix over $\mathrm{GF}(q)$. Left multiply the 0th row of submatrices of $\mathbf{H}^{(b)}$ by this scaling matrix, and assign the resulting matrix to the 0th row of submatrices of $\mathbf{H}$. Repeat this process for the rest of the $\gamma - 1$ row of submatrices of $\mathbf{H}^{(b)}$.

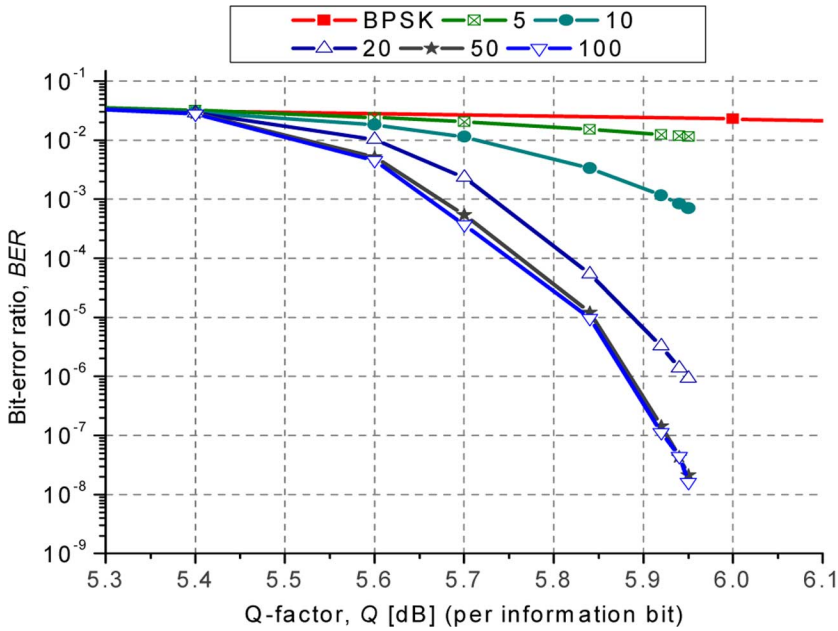

Fig. 1. Effect of the number of iterations on the BER performance of a (3,15)-regular, girth-8 LDPC code over GF(4) when decoded using FFT-QSPA.

It is worth noting that scheme 3 given by (7) does indeed generate an NB-QC-LDPC code while simultaneously eliminating the need for permutation blocks in the FFT-based decoding. Hence, it achieves the design goals of two different schemes together.

IV. Results and Discussion

In this section, we provide simulation results for a set of codes constructed using the aforementioned schemes and compare their performances based on their bit error rate (BER) versus Q-factor curves.

Optical communication channels require high-rate codes, i.e., code rates equal to or above 0.8. As we discussed before, the girth of an LDPC code affects the code's performance under SPA, and must be kept as large as possible. Hence, while designing our codes, we followed a two-stage code design technique, addressing both of these issues [15]. In the two-stage design, using the algebraic code construction techniques discussed in [13], we first obtain a matrix of the form given in (1) and of girth 6. In the second stage, we extract a portion of the matrix created in the first stage to obtain a parity-check matrix of a B-QC-LDPC code with the desired girth and rate. Lastly, we assign nonzero elements from $\mathrm{GF}(q)$ to the 1s in this binary parity-check matrix following the guidelines provided in one of the schemes discussed in Section III. For a fair comparison, all the codes that we constructed using the two-stage design technique are (3,15)—regular (i.e., rate of 0.8 or slightly above) LDPC codes that are of girth 8.

In our simulations, we used binary additive-white Gaussian (BI-AWGN) channel model [6] and employed FFT-QSPA to decode the NB-LDPC codes. In the first two experiments, we used scheme 1 of Section III to construct NB-LDPC codes to minimize the effects of the element selection scheme on the results. In the last experiment, we compared the effects of different element selection schemes described in Section III based on the BER performance.

Our first set of simulations was targeted to determine the effect of the number of iterations in FFT-based decoding. In Fig. 1, we present the simulation results for a (3,15)-regular, girth-8 LDPC code over $\mathrm{GF}(4)$ that is constructed using the two-stage design technique and the guidelines in scheme 1. As we can see, the additional coding gain obtained by increasing the number of iterations is miniscule after 50 iterations. Even though in the case of 20 iterations, the BER curve gets quite close (approximately 0.05 dB at 10^{-6}) to the BER curves obtained by using 50 and 100 iterations, we can claim that using 50 iterations is favorable since it provides almost optimum performance. As opposed to 500 iterations used in decoding of NB-LDPC codes in [6] and [16], we show in Fig. 1 that 50 iterations are satisfactory in FFT-based decoding of NB-QC-LDPC codes.

We conducted another experiment to figure out the effect of the finite field size on the BER performance. Toward this goal, we constructed several bit-length-matched NB-LDPC codes over different finite fields using the two-stage design technique and the guidelines in scheme 1. All the NB-LDPC codes had a rate of approximately 0.8 and a girth of 8. In addition, we constructed a girth-10 B-QC-LDPC of rate approximately 0.8 to compare against the NB codes. Note that even though the bit lengths of the NB codes and the binary code are matched, the binary code has a larger girth than the NB codes, which gives an advantage to the binary code in the performance comparison. We ran simulations on the BI-AWGN channel and set the maximum number of iterations to 50 in the FFT-QSPA. Fig. 2 depicts the BER versus Q-factor curves for our simulations. Clearly, girth-8 NB-LDPC codes over $\mathrm{GF}(4), \mathrm{GF}(8)$, and $\mathrm{GF}(16)$ outperform the bit-length-matched B-QC-LDPC code of a larger girth. We also observe that increasing the field order above 8 deteriorates the performance of an NB-LDPC code. We should note that a similar trend for column weight 3 rate-1/2 codes was reported by Davey [6, Fig 3.5, p. 24].

The complexity of the FFT-QSPA is proportional to the field order. Hence, it is preferable to keep the order of the field that an

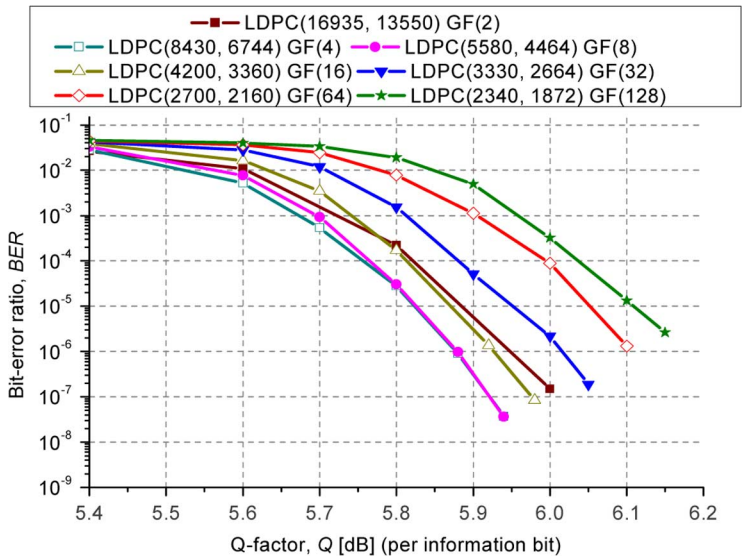

Fig. 2. BER performance comparison between a set of bit-length-matched (3,15)-regular, girth-8 LDPC codes over various extension fields of the binary field and a bit-length-matched (3,15)-regular, girth-10 LDPC code. Decoding is performed using FFT QSPA, where the maximum number of iterations is set to 50.

NB-LDPC code is designed over as small as possible. In other words, among the NB-LDPC codes over $\mathrm{GF}(2^m)$, codes over $\mathrm{GF}(4)$ must be preferred from the complexity standpoint. We also compared in [15] the complexity of decoding algorithms for regular NB-LDPC codes and regular B-LDPC codes. We showed that MD-FFT-QSPA when used for decoding a 4-ary (3,15)-regular NB-LDPC code requires 91.28% of the computational resources required by a commonly used, more stable version of SPA known as min-sum-with-correction-term algorithm (or J-LLR-SPA) used for decoding a bit-length-matched, (3,15)-regular B-LDPC code. Therefore, from the simulation results and the complexity analysis, we can conclude that it is most advantageous to use NB-LDPC codes over $\mathrm{GF}(4)$ when the code rate is approximately 0.8 and the girth of the code is fixed at 8.

In our third experiment, we compared the BER performances of NB-LDPC codes constructed by using different schemes described in Section III. First, we constructed a (3,15)-regular, girth-8 binary parity-check matrix. Then, we assigned nonzero elements from $\mathrm{GF}(4)$ to the 1s in this binary parity-check matrix using different schemes to construct different NB-LDPC codes. Due to the reasons stated in the previous paragraph, we focused our attention only on NB-LDPC codes over $\mathrm{GF}(4)$. We used BI-AWGN channel model in our simulations and set the maximum number of iterations in the FFT-QSPA decoding to 50. We depicted our results in Fig. 3. As we can observe, there is no loss in performance by switching from scheme 1, which proposes random element selection, to scheme 2, which aims to reduce hardware implementation complexity of the decoder, or to scheme 4, which generates an NB-QC-LDPC code. However, there is a notable, although not significant, performance loss when scheme 3 is employed instead of any one of the other three. On the contrary to one's intuition, our results suggest that there is no particular reason to prefer random element selection over other element selection schemes targeting different design goals. Since all of the codes are based on the same binary parity-check matrix of a B-QC-LDPC code, they all have similar modular structure. However, the encoders of the codes constructed using scheme 4, which yields NB-QC-LDPC codes, are much simpler than the others.

In addition to depicting that NB-QC-LDPC codes perform as good as randomly constructed regular codes of the same rate, Fig. 3 also shows that a rate-0.8, girth-8 NB-QC-LDPC code over $\mathrm{GF}(4)$ significantly outperforms a competitive BCH(128,113) $\times$ BCH(256,239) turbo product code (TPC). Its coding gain improvement over the TPC code is 0.885 dB at BER of 4×10^{-8}. Also, via extrapolation, we computed the expected net effective coding gain (NECG) of this 4-ary, rate-0.8, girth-8 code as 10.8 dB at the BER of 10^{-12}, which indicates that this code is very suitable for application in optical communications.

V. Conclusion

We have shown that it is not always possible to construct the parity-check matrix of an NB-QC-LDPC code by randomly assigning nonzero elements from the desired field to the 1s in the parity-check matrix of a corresponding B-QC-LDPC code. Using a theorem, we proved that in order for this to happen, the constructed NB matrix has to satisfy a necessary and sufficient condition.

We then proposed a general scheme for constructing NB-QC-LDPC codes. We also discussed some other schemes that might be employed under different design goals. Then, with the help of simulations, we concluded that the FFT-QSPA-based decoding yields almost optimum results when 50 iterations are used. In addition, we showed that there is no performance difference between an NB-QC-LDPC code and an NB-LDPC code obtained by using a random element assignment scheme when both codes are based on the same B-QC-LDPC code. Our simulations also demonstrated that high-rate, regular NB-QC-LDPC codes are excellent candidates for use in optical communications due to their good NECG figure, simple encoders, and comparably lower complexity decoders than non-QC NB-LDPC codes.

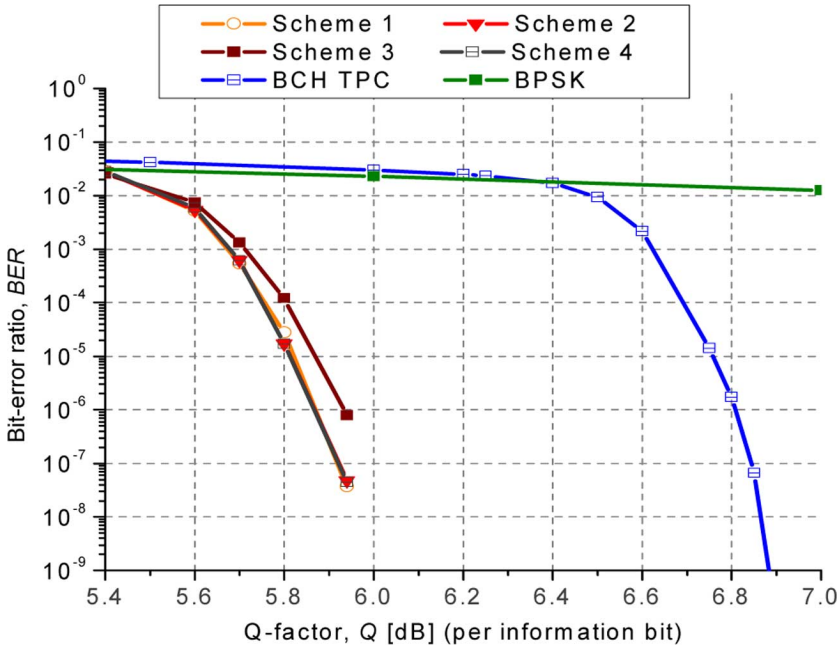

Fig. 3. BER performance comparison between rate-0.8, girth-8 NB-LDPC codes over GF(4), constructed using different element selection schemes, BCH(128,113) × BCH(256,239) TPC. Decoding is performed using FFT-QSPA, where the maximum number of iterations is set to 50.

Our future work includes a comprehensive study of the systematic encoders for NB-QC-LDPC codes, hardware implementations of encoders and decoders for NB-QC-LDPC codes, and the integration of these hardware elements into a real-world optical communication system.

APPENDIX

We begin with the definitions of rotation and scaling matrices. A *rotation matrix* $\mathbf{R}_{T,T}$ is obtained by cyclically rotating the columns of a $T \times T$ identity matrix $\mathbf{I}$ toward left by one place. Let $S = QT + T'$ for some integers Q and T' such that $0 \leq T' < T$. Then, an $S \times S$ rotation matrix $\mathbf{R}_{S,T}$ has the form

$$\mathbf{R}_{S,T} = \left[\begin{array}{c|c} \mathbf{R}_{QT,T} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{R}_{T',T'} \end{array}\right] \tag{8}$$

where $\mathbf{0}$ denotes a zero matrix of appropriate size and $\mathbf{R}_{QT,T}$ is a $QT \times QT$ square matrix given by

$$\mathbf{R}_{QT,T}(i,j) = \begin{cases} \mathbf{R}_{T,T}(\bar{i},\bar{j}), & \lfloor i/T \rfloor T \leq j < \lfloor i/T \rfloor T + T \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

for $0 \leq i,j < QT$, where $\bar{i} = i \bmod T$ and $\bar{j} = j \bmod T$. Clearly, if S is divisible by T, then $\mathbf{R}_{S,T}$ is just a $QT \times QT$ square matrix since T' is zero. Scaling matrices have a comparably simpler structure. We define a *scaling matrix* $\mathbf{C}$ as a diagonal matrix whose components along the main diagonal are all nonzero.

Proof of Theorem 1: We assume $\mathbf{H}$ to be an $M \times N$ matrix, where $M < N$, which is obtained by replacing the nonzero components of the parity-check matrix of a (γ,ρ)-regular B-QC-LDPC code, whose Tanner graph is assumed to be free of four cycles, by nonzero elements from $\mathrm{GF}(q)$. We also assume $\mathbf{G}$ to be a $K \times N$ matrix, where $K < N$, whose rows span the null-space of $\mathbf{H}$, i.e., $\mathbf{G}\mathbf{H}^{\mathrm{T}} = \mathbf{0}$.

First, we establish the necessary condition. Suppose that whenever $\mathbf{v}$ is a vector such that $\mathbf{v}\mathbf{H}^{\mathrm{T}} = \mathbf{0}$, we also have $\mathbf{v}^{(l)}\mathbf{H}^{\mathrm{T}} = \mathbf{0}$ for all $l, 0 \leq l \leq B$. Since rows of $\mathbf{G}$ span the null-space of $\mathbf{H}$, we can write $\mathbf{v} = \mathbf{u}\mathbf{G}$ for some $\mathbf{u}$ in the K-dimensional vector space $(\mathrm{GF}(q))^K$. Using a rotation matrix, we can express $\mathbf{v}^{(l)}$ as $\mathbf{v}^{(l)} = \mathbf{v}\mathbf{R}_{N,B}^{-l}$. Thus, we have

$$\mathbf{v}^{(l)}\mathbf{H}^{\mathrm{T}} = \mathbf{u}\mathbf{G}\mathbf{R}_{N,B}^{-l}\mathbf{H}^{\mathrm{T}} = \mathbf{0} \tag{10}$$

for all $l, 0 \leq l \leq B$. Equation (10) must hold for all $\mathbf{u}$ in $(\mathrm{GF}(q))^K$; hence, we must have $\mathbf{G}\mathbf{R}_{N,B}^{-l}\mathbf{H}^{\mathrm{T}} = \mathbf{0}$, or equivalently,

$$\mathbf{G}\left[\mathbf{H}\left(\mathbf{R}_{N,B}^{-l}\right)^{\mathrm{T}}\right]^{\mathrm{T}} = \mathbf{G}[\mathbf{H}\mathbf{R}_{N,B}^{l}]^{\mathrm{T}} = \mathbf{0} \tag{11}$$

for all $l, 0 \leq l \leq B$, where we used the fact that $(\mathbf{R}_{N,B}^{-l})^{\mathrm{T}} = \mathbf{R}_{N,B}^{l}$. Since $\mathbf{G}$ is unaltered, the null-space of $\mathbf{G}$ remains unaltered, i.e., the subspace generated by the rows of $\mathbf{H}$ must also be generated by the rows of $\mathbf{H}\mathbf{R}_{N,B}^{l}$. Therefore, the conditions under which $\mathbf{H}\mathbf{R}_{N,B}^{l}$ can be obtained from $\mathbf{H}$ by elementary row operations are also the necessary conditions for a code generated by the null-space of $\mathbf{H}$ to preserve the fundamental property.

When $l = 0$ or $l = B$, we have $\mathbf{H}\mathbf{R}_{N,B}^{0} = \mathbf{H}\mathbf{R}_{N,B}^{B} = \mathbf{H}$, so we have nothing to do in these cases. For $0 < l < B$, we use our assumption that the Tanner graph of $\mathbf{H}$ is free of four cycles. Now suppose that $l = 1$, and consider the kth row of $\mathbf{X} = \mathbf{H}\mathbf{R}_{N,B}$ denoted by $\mathbf{X}(k,\cdot), 0 \leq k < \gamma B$. Since $\mathbf{H}$ is of girth greater than 4, among the rows of $\mathbf{H}$, $\mathbf{H}(k-1 \bmod B, \cdot)$ is the only row whose nonzero components are at the same positions as the nonzero components of $\mathbf{X}(k,\cdot)$. Clearly, applying a sequence of elementary row-switching operations, which can be

effectively accomplished by multiplying $\mathbf{H}$ by a rotation matrix $\mathbf{R}_{M,B}$ from the left, we can align the positions of the nonzero elements of $\mathbf{H}$ with those of $\mathbf{X}$. Let the resulting intermediary matrix be $\mathbf{Y} = \mathbf{R}_{M,B}\mathbf{H}$. Now, the kth row of $\mathbf{Y}$ must be a scalar multiple of the kth row of $\mathbf{X}$, and thus, we can write

$$\mathbf{X} = \mathbf{K}_1\mathbf{Y} = \mathbf{K}_1\mathbf{R}_{M,B}\mathbf{H} = \mathbf{R}_{M,B}(\mathbf{C}_1\mathbf{H}) \tag{12}$$

where $\mathbf{K}_1$ and $\mathbf{C}_1$ are scaling matrices satisfying $\mathbf{C}_1 = \mathbf{R}_{M,B}\mathbf{K}_1\mathbf{R}_{M,B}^{-1}$. Using the definition of $\mathbf{X}$ in combination with (12), we obtain the necessary condition for (11) to hold when $l = 1$ as follows:

$$\mathbf{R}_{M,B}^{-1}\mathbf{H}\mathbf{R}_{N,B} = \mathbf{C}_1\mathbf{H}. \tag{13}$$

Now, we show that (13) implies

$$\mathbf{R}_{M,B}^{-l}\mathbf{H}\mathbf{R}_{N,B}^{l} = \mathbf{C}_l\mathbf{H} \tag{14}$$

which, in turn, implies

$$\mathbf{H}\mathbf{R}_{N,B}^{l} = \mathbf{R}_{M,B}^{l}(\mathbf{C}_l\mathbf{H}) \tag{15}$$

for all $l, 0 \le l \le B$. When $l = 0$ or $l = B$, (14) holds with $\mathbf{C}_0 = \mathbf{C}_B = \mathbf{I}$, where $\mathbf{I}$ is the $M \times M$ identity matrix. When $l = 2$, we proceed as follows:

$$\begin{aligned}
\mathbf{R}_{M,B}^{-2}\mathbf{H}\mathbf{R}_{N,B}^{2} &= \mathbf{R}_{M,B}^{-1}\mathbf{C}_1\mathbf{H}\mathbf{R}_{N,B} \\
&= \mathbf{R}_{M,B}^{-1}\mathbf{C}_1\left(\mathbf{R}_{M,B}\mathbf{R}_{M,B}^{-1}\right)\mathbf{H}\mathbf{R}_{N,B} \\
&= \mathbf{R}_{M,B}^{-1}\mathbf{C}_1\mathbf{R}_{M,B}\left(\mathbf{R}_{M,B}^{-1}\mathbf{H}\mathbf{R}_{N,B}\right) \\
&= \mathbf{R}_{M,B}^{-1}\mathbf{C}_1\mathbf{R}_{M,B}(\mathbf{C}_1\mathbf{H}) \\
&= \left(\mathbf{R}_{M,B}^{-1}\mathbf{C}_1\mathbf{R}_{M,B}\mathbf{C}_1\right)\mathbf{H} \\
&= \mathbf{C}_2\mathbf{H}
\end{aligned} \tag{16}$$

where $\mathbf{C}_2 = \mathbf{R}_{M,B}^{-1}\mathbf{C}_1\mathbf{R}_{M,B}\mathbf{C}_1$. In general, (14) holds for all $l, 0 \le l \le B$, with $\mathbf{C}_l = \mathbf{R}_{M,B}^{-l+1}(\mathbf{C}_1\mathbf{R}_{M,B})^{l-1}\mathbf{C}_1$. That is, (13) gives the necessary condition for $\mathbf{H}$ to hold in order for the code defined by its null-space to preserve the fundamental property.

Conversely, suppose that $\mathbf{H}$ is a parity-check matrix over $\mathrm{GF}(q)$, constructed using a corresponding binary parity-check matrix as explained before, such that (13) holds for some rotation matrices $\mathbf{R}_{M,B}$ and $\mathbf{R}_{N,B}$, and a scaling matrix $\mathbf{C}_1$. We can show that (11) holds for $\mathbf{H}$ as follows:

$$\begin{aligned}
\mathbf{G}\mathbf{R}_{N,B}^{-l}\mathbf{H}^{\mathrm{T}} &= \mathbf{G}\mathbf{R}_{N,B}^{-l}\mathbf{H}^{\mathrm{T}}\left(\mathbf{R}_{M,B}^{l}\mathbf{R}_{M,B}^{-l}\right) \\
&= \mathbf{G}\left[\mathbf{R}_{M,B}^{-l}\mathbf{H}\mathbf{R}_{N,B}^{l}\right]^{\mathrm{T}}\mathbf{R}_{M,B}^{-l} \\
&= \mathbf{G}[\mathbf{C}_l\mathbf{H}]^{\mathrm{T}}\mathbf{R}_{M,B}^{-l} \\
&= (\mathbf{G}\mathbf{H}^{\mathrm{T}})\mathbf{C}_l^{\mathrm{T}}\mathbf{R}_{M,B}^{-l} \\
&= \mathbf{0}
\end{aligned} \tag{17}$$

where the third equation follows from (14).

ACKNOWLEDGMENT

The authors also would like to thank the anonymous reviewers whose comments helped improve the quality of their paper. M. Arabaci would like to thank Dr. Lux of the Department of Mathematics, University of Arizona, Tuscon, for fruitful discussions in the preparation of this manuscript.

REFERENCES

[1] R. G. Gallager, "Low density parity check codes," *IRE Trans. Inf. Theory*, vol. IT-8, pp. 21–28, Jan. 1962.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 33, no. 6, pp. 457–458, Mar. 1997.

[3] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[4] T. Ohtsuki, "LDPC codes in communications and broadcasting," *IEICE Trans. Commun.*, vol. E90-B, no. 3, pp. 440–453, Mar. 2007.

[5] A. Dholakia, E. Eleftheriou, T. Mittelholzer, and M. P. C. Fossorier, "Capacity-approaching codes: Can they be applied to the magnetic recording channel?," *IEEE Commun. Mag.*, vol. 42, no. 2, pp. 122–130, Feb. 2004.

[6] M. C. Davey, "Error-correction using low-density parity-check codes," Ph.D. dissertation, Univ. Cambridge, Cambridge, U.K., 1999.

[7] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over $\mathrm{GF}(q)$," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, Apr. 2007.

[8] C. Spagnol, W. Marnane, and E. Popovici, "FPGA implementations of LDPC over $\mathrm{GF}(2^m)$ decoders," in *Proc. IEEE Workshop Signal Process. Syst.*, Shanghai, China, 2007, pp. 273–278.

[9] Z.-W. Li, L. Chen, L.-Q. 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, Jan. 2006.

[10] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2004.

[11] Z. Wang and Z. Cui, "Low-complexity high-speed decoder design for quasi-cyclic LDPC codes," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 15, no. 1, pp. 104–114, Jan. 2007.

[12] Y. Chen and K. K. Parhi, "Overlapped message passing for quasi-cyclic low-density parity check codes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 6, pp. 1106–1113, Jun. 2004, .

[13] 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. Inf. Theory*, vol. 53, no. 7, pp. 2429–2458, Jul. 2007.

[14] R. Tanner, D. Sridhara, A. Sridharan, T. Fuja, and D. Costello, Jr., "LDPC block and convolutional codes based on circulant matricies," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

[15] M. Arabaci, I. B. Djordjevic, R. Saunders, and R. Marcoccia, "A class of non-binary regular girth-8 LDPC codes for optical communication channels," in *Proc. OFC/NFOEC 2009*, San Diego, CA, , Paper No. JThA.

[16] B. Rong, T. Jiang, X. Li, and M. R. Soleymani, "Combine LDPC codes over $\mathrm{GF}(q)$ with q-ary modulations for bandwidth-efficient transmission," *IEEE Trans. Broadcast.*, vol. 54, no. 1, pp. 78–84, Mar. 2008.

Murat Arabaci (S'01) received the B.Sc. degree in electrical and electronics engineering from Osmangazi University, Eskisehir, Turkey, in 2003, and the M.Sc. degree in electrical engineering in 2006 from the University of Arizona, Tucson, where he is currently working toward the Ph.D. degree in electrical engineering.

His current research interests include coding theory, communication theory, and information theory.

Ivan B. Djordjevic (M'04) received the B.Sc., M.Sc., and Ph.D. degrees from the University of Nis, Yugoslavia, in 1994, 1997 and 1999, respectively, all in electrical engineering.

He was with the University of Arizona, Tucson (as a Research Assistant Professor); University of the West of England, Bristol, U.K.; University of Bristol, Bristol; Tyco Telecommunications, Eatontown, NJ; and National Technical University of Athens, Athens, Greece. He is currently an Assistant Professor of electrical and computer engineering at the University of Arizona, Tucson, where he is the Director of the Optical Communications Systems Laboratory, Department of Electrical and Computer Engineering. He is a co-author of the book OFDM for Optical Communications, Elsevier, 2009. He is the author or coauthor of more than 100 journal publications and more than 100 conference papers. His current research interests include optical networks, error control coding, constrained coding, coded modulation, turbo equalization, orthogonal frequency-division multiplexing applications, and quantum error correction.

Dr. Djordjevic was an Associate Editor for the *Research Letters in Optics* and the *International Journal of Optics.*

Ross Saunders, photograph and biography not available at the time of publication.

Roberto M. Marcoccia, photograph and biography not available at the time of publication.