Non-Binary Algebraic Spatially-Coupled Quasi-Cyclic LDPC Codes

Keke Liu, Mostafa El-Khamy, Jungwon Lee, Inyup Kang, and Arvind Yedla

Department of Electrical and Computer Engineering, University of California, Davis, CA, 95616

Email: kkeliu@ucdavis.edu, {mostafa.e, jungwon2.lee, inyup.kang, arvind.yedla}@samsung.com

Abstract—This paper considers the algebraic construction and performance of non-binary spatially-coupled low density parity check (LDPC) codes. A replicate-and-mask approach is presented to construct finite-length algebraic quasi-cyclic (QC) spatially-coupled (SC) LDPC codes. Numerical results show the superiority of non-binary algebraic SC QC LDPC codes over the corresponding random non-binary (block and SC) LDPC codes. In this paper, it is demonstrated that the threshold saturation phenomenon, previously demonstrated for binary SC LDPC codes, also holds for non-binary SC LDPC codes over the binary-input AWGN channel with BPSK modulation.

I. INTRODUCTION

Spatially-coupled low-density parity-check (SC LDPC) codes, also known as LDPC convolutional codes [1], have received much attention due to their excellent thresholds. It has been discovered and proved that for the binary erasure channel (BEC), the maximum a posteriori probability (MAP) threshold of a regular LDPC block ensemble can be approached by the belief propagation (BP) threshold of an ensemble generated by spatially coupling a collection of the original LDPC block ensembles [2]. This phenomenon is called threshold saturation. This phenomenon has been recently extended to general binary memoryless symmetric (BMS) channels [3]. Recently, non-binary SC LDPC codes also started to receive the attention of researchers. The threshold saturation phenomenon of non-binary SC LDPC codes has only been reported for the BEC [4]. A well-known construction of SC LDPC codes, categorized as a graph cover construction, is based on unwrapping the parity-check matrix of an LDPC block code to obtain the parity-check matrix of a SC LDPC code [1], [5]. Quasi-cyclic (QC) LDPC codes are typically given by the null space of an array of sparse circulants of the same size over a finite field [6]. QC LDPC codes have the advantages of good finite length performance and efficient hardware implementations [7]–[9].

The goal of this paper is to study both the finite length and the asymptotic performances of non-binary SC LDPC codes. To design SC LDPC codes with good performance at finite length, algebraic constructions of non-binary QC LDPC codes are considered. Recent constructions of binary SC QC LDPC codes [10] used a modified progressive-edge-growth (PEG) algorithm [11]. In contrast, our construction of non-binary SC QC LDPC codes is a deterministic construction based on finite fields. This avoids time-consuming computer search, while ensuring that the Tanner graph of the parity-check matrix has a girth at least 6, which often guarantees a good performance. Moreover, our construction is based on replicating and masking the parity-check matrix of a non-binary QC LDPC block code. This provides more flexibility in the design of code parameters (such as rate and degree distribution) compared to the conventional unwrapping technique, while ensuring a certain girth property of the resultant SC LDPC code. The conventional unwrapping construction can be shown to be a special instance of the proposed construction. Moreover, the proposed construction provides a much larger class of SC QC LDPC codes than the construction proposed in [12]. Asymptotically, the threshold saturation phenomenon is investigated for non-binary SC LDPC codes over binary-input AWGN channel with BPSK modulation. It is verified that the threshold saturation phenomenon holds, with reasonable accuracy, for SC LDPC codes over GF(2^2) on binary-input additive white Gaussian noise (AWGN) channels.

II. PRELIMINARIES

A. Unwrapping Construction of SC LDPC Codes

Let $G$ be a $(d_v, d_c)$ regular protograph, where $d_v$ and $d_c$ denote the variable node (VN) and check node (CN) degrees, respectively. The Tanner graph $G_{sc}$ of a $(d_v, d_c, L)$ SC LDPC code is obtained by spatially coupling a chain of $L$ copies of $G$. Fig. 1 gives an example of constructing a $(3,6,5)$ SC LDPC Tanner graph.

Let $H$ be the parity-check matrix of an LDPC block code, and suppose $H$ can be decomposed into a set of $L$ matrices \[ H \]_L \text{ such that } H = \sum_{i=0}^{L-1} H_i \text{ (in } \mathbb{Z}). \] The matrix
unwrapping process [1], [5] arranges \( \{H_i\}_{0 \leq i < \ell} \) in such a way that the following SC array is formed:

\[
H_{sc} = \begin{bmatrix}
H_0 & H_0 & \cdots & H_0 \\
H_1 & H_0 & \cdots & H_0 \\
\vdots & \ddots & \ddots & \vdots \\
H_{\ell-1} & H_{\ell-2} & \cdots & H_0
\end{bmatrix}
\]  

(1)

B. Algebraic Construction of QC LDPC Block Codes

Algebraic tools, such as finite fields, have been shown to be very effective in constructing QC LDPC block codes with excellent overall performance [9], [13], [14]. In most of the algebraic constructions of QC LDPC block codes, the parity-check matrix of a code is an array of circulant permutation matrices (CPMs) and/or zero matrices (ZMs).

Let \( \alpha \) be a primitive element of a finite field \( \text{GF}(q) \). The construction of a QC parity-check matrix \( H_{qc} \) starts with a matrix \( B \) over \( \text{GF}(q) \) (called base matrix). Given an \( m \times n \) matrix \( B = [b_{i,j}] \) over \( \text{GF}(q) \), \( H_{qc} \) can be constructed as follows: for each entry \( b_{i,j} \) in \( B \), if \( b_{i,j} \neq 0 \), let \( b_{i,j} = \alpha^l \), with \( 0 \leq l < q - 1 \), then replace \( b_{i,j} \) by \( (q - 1) \times (q - 1) \) CPM whose first row has a single 1-component at position \( l \). This direct construction of \( H_{qc} \) from the base matrix \( B \) is referred to as \((q - 1)\)-fold dispersion of \( B \).

It follows from the above construction process that \( H_{qc} \) is uniquely specified by the base matrix \( B \). It has been proved that a necessary and sufficient condition for the Tanner graph of \( H_{qc} \) to have a girth of at least 6 is that every \( 2 \times 2 \) submatrix of \( B \) contains at least one zero entry or is non-singular [14]. This constraint on the \( 2 \times 2 \) submatrices of \( B \) is referred to as the \( 2 \times 2 \) submatrix constraint (SM-constraint). We call a matrix that satisfies the \( 2 \times 2 \) SM-constraint over \( \text{GF}(q) \) an \( 2 \times 2 \) SM-constrained matrix. Therefore, the construction of \( H_{qc} \) whose Tanner graph has a girth of at least 6 is equivalent to the construction of \( 2 \times 2 \) SM-constrained base matrices \( B \) over \( \text{GF}(q) \). The masking technique [9] can be applied to construct QC-LDPC block codes with various degree distributions.

C. EXIT Analysis of SC LDPC codes

Extrinsic information transfer (EXIT) charts are popular tools for studying the asymptotic performance of an LDPC code ensemble [15] which is usually specified by decoding threshold [15], [16]. Protograph-based EXIT (PEXIT) chart analysis [17] extends the baseline EXIT to the binary protograph-based LDPC codes [18]. Recently, PEXIT charts have also been extended to the non-binary protograph [19] LDPC codes for threshold computation and analysis. Generalized EXIT (GEXIT) functions [16], [20] extend the EXIT concept to general BMS channels. GEXIT functions satisfy the area theorem [16] by definition and maintain most of the basic properties of EXIT functions.

For the GEXIT analysis, a general BMS channel is usually parameterized by channel entropy, denoted by \( h = H(X|Y) \), where \( X \) and \( Y \) are the input and the output of the BMS channel, respectively. Let \( X = (X_0, X_1, ..., X_{n-1}) \) be the input vector of a BMS channel and let \( Y = (Y_0, Y_1, ..., Y_{n-1}) \) denote the corresponding output vector. For \( 0 \leq i < n \), let \( X_{-i} = (X_0, ..., X_{i-1}, X_{i+1}, ..., X_{n-1}) \) and \( Y_{-i} = (Y_0, ..., Y_{i-1}, Y_{i+1}, ..., Y_{n-1}) \). Let \( \phi(Y_{-i}) \) be an extrinsic estimator of \( X_i \), then the GEXIT function is defined by

\[
g(h) = \frac{dH(X_i|Y_i, \phi(Y_{-i}))}{dh},
\]

and we have the following generalized area theorem:

\[
\int g(h) dh = r,
\]

where \( r \) is the rate of the code. The GEXIT function is useful in bounding the MAP decoding performance of LDPC codes using the above area theorem.

Let \( p_i(u) \) be the probability density function of the extrinsic estimator \( u = \phi(Y_{-i}) \), then it has been proved that the GEXIT function for \( \phi(Y_{-i}) \) can be expressed as:

\[
g(h) = \int p_i(u) l(h, u) du.
\]

III. REPLICATE-AND-MASK ALGEBRAIC CONSTRUCTION OF SC QC LDPC CODES

In this section, we propose a systematic construction of algebraic QC LDPC codes based on finite fields, called replicate-and-mask construction.

A. General Replicate-and-Mask Algebraic Construction

Consider a finite field \( \text{GF}(q) \), where \( q = 2^s \), and let \( B = [b_{i,j}] \) be an \( m \times n \) \( 2 \times 2 \) SM-constrained matrix over \( \text{GF}(q) \). We replicate \( B \) to form a semi-infinite array of \( B \), denoted by \( B_{rep} \), as follows:

\[
B_{rep} = [b_{rep,i,j}]_{0 \leq i,j < \infty} = \begin{bmatrix}
B & B & B & \cdots \\
B & B & B & \cdots \\
\vdots & \vdots & \vdots & \ddots \\
B & B & B & \cdots
\end{bmatrix},
\]

(5)

where \( b_{rep,i,j} = b_{i,(j \mod m),(j \mod m)} \) for all \( i, j \geq 0 \).

Suppose we have a binary matrix \( W = [w_{i,j}]_{0 \leq i,k,0 \leq j < t} \) of size \( s \times t \) with a SC pattern. Let \( B_{rep}(s,t) \) denote the \( s \times t \) submatrix of \( B_{rep} \) taken from the upper left corner of \( B_{rep} \). We can construct a \( s \times t \) SC base matrix \( B_{sc} \) by masking \( B_{rep}(s,t) \) using \( W \), i.e., \( B_{sc} = B_{rep}(s,t) \odot W \), where ‘\( \odot \)’ denotes the Hadamard product [21] (i.e., entry-wise product of two matrices). We refer to the above process as the ‘replicate-and-mask’ construction, which can be summarized as follows:

‘Replicate-and-Mask’ Algebraic Construction of SC QC LDPC codes

Step 1. Find a \( 2 \times 2 \) SM-constrained base matrix \( B \) over \( \text{GF}(q) \).
Step 2. Replicate \( B \) to form an array \( B_{rep} \) of \( B \) as in (5).
Step 3. Design a \( s \times t \) masking matrix \( W \) with a SC pattern.
Step 4. Mask $B_{rep}(s,t)$ using $W$ to obtain $B_{sc} = B_{rep}(s,t) \odot W$.

Step 5. Apply $(q - 1)$-fold dispersion on $B_{sc}$ to obtain an $s \times t$ SC QC array $H_{sc,qc}$ of $(q - 1) \times (q - 1)$ CPMs and/or ZMs, whose null space gives a binary SC QC LDPC code.

We can construct non-binary SC QC LDPC codes over GF($2^p$) by replacing each 1-entry in $H_{sc,qc}$ by a nonzero element from GF($2^p$) in a systematic way.

B. Designing the Masking Matrix

Given a QC LDPC block code specified by the base matrix $B$, the parity-check matrix of the SC QC LDPC code formed with the replicate-and-mask construction depends entirely on the masking matrix $W$. The following Theorem 1 specifies a general guideline of designing $W$ to ensure that the SC base matrix $B_{sc}$ also satisfies the SM-constraint, so that the Tanner graph of $H_{sc,qc}$ has a girth of at least 6. Due to space limitations, all the proofs for the theorems given in this paper are omitted.

**Theorem 1.** Suppose $B$ satisfies the $2 \times 2$ SM-constraint. Then $B_{sc}$ also satisfies the $2 \times 2$ SM-constraint if the following condition is satisfied: for any $i, j \leq t$, let $M(i) = \{ j : w_{i,j} = 1 \}$ and $N(j) = \{ i : w_{i,j} = 1 \}$. Now we consider a special case that $W$ is constructed by conventional unwrapping of an all-one matrix of the same size as $B$. Then it follows that for $0 \leq i < s$ and $0 \leq j < t$, $i_1, i_2 \mod m \neq i_2 \mod m$ for any $i_1, i_2 \in N(j)$, and $j_1, j_2 \mod n \neq j_2 \mod n$ for any $j_1, j_2 \in M(i)$. Hence, the condition in Theorem 1 is satisfied. On the other hand, it is clear that in this case, $B_{sc}$ can be obtained by applying the same conventional unwrapping procedure to $B$. Therefore, we see that the conventional unwrapping is a special case of the replicate-and-mask construction with the masking matrix $W$ constructed by conventional unwrapping of an all-one matrix of the same size as $B$.

Next, we consider the replicate-and-mask construction of regular SC QC LDPC codes. Given the base matrix $B$ for a QC LDPC block code, then it remains to design a regular masking matrix $W$ with the desired SC pattern.

Suppose $W$ contains $L$ SC all-one matrices of size $a \times b$ with the ‘step size’ $c$. In this case, $W$ is uniquely determined by four parameters $a, b, c$ and $L$, i.e., $W = W(a, b, c, L) = \{ w_{i,j} \}_{0 \leq i \leq L(a+c)-1, 0 \leq j \leq b-1}$, where

$$w_{i,j} = \begin{cases} 1 & \text{if } kc \leq i < kc + a \text{ and } kb \leq j < (k+1)b \text{ for } 0 \leq k < L \\ 0 & \text{otherwise}. \end{cases}$$

(6)

Fig. 2 gives an example of a regular masking matrix $W(a, b, c, L)$ where $a = 4, b = 3, c = 2$ and $L = 4$.

Based on Theorem 1, we have the following theorem.

**Theorem 2.** If $B$ satisfies the $2 \times 2$ SM-constraint, the masking matrix $W(a, b, c, L)$ results in a $2 \times 2$ SM-constrained masked matrix $B_{sc}$ if $a \leq m$ and $\lfloor (a-1)/c \rfloor \leq n$.

Fig. 2. An example of $W(a, b, c, L)$ for $a = 4, b = 3, c = 2, L = 4$

Theorem 2 gives an easily-implementable guideline for constructing regular SC QC LDPC codes with length $bL(q - 1)$, while satisfying a minimum girth of 6. The following Theorem 3 gives a more desirable girth property for the constructed SC QC LDPC codes.

**Theorem 3.** Suppose $H$ is the $(q - 1)$-fold dispersion of $B$. If $a \leq m$ and $\lfloor a/c \rfloor b \leq n$, the girth of the Tanner graph of $H_{sc,qc}$ is at least as large as that of the Tanner graph of $H$.

Note that the rate of the SC QC LDPC codes constructed based on the masking matrix $W(a, b, c, L)$ is at least $1 - (cL + a - c)/bL = (b - c)/b - (a - c)/bL$, where $(b - c)/b$ is the designed rate, and $(a - c)/bL$ is the rate loss due to the edge effect. Next, we determine how tighter bounds on rate can be found by rank analysis of the constructed code.

Suppose $q = 2^e$. Using the Fourier transform domain analysis [14], we have the following two theorems on the upper bounds of the rank of $H_{sc,qc}$.

**Theorem 4.** If $B$ does not contain any zero entry, the rank of $H_{sc,qc}$ is upper bounded by $(cL + a - c)(q - 1) - ((c - 1)L + a - c)$.

**Theorem 5.** If $a = m$, $B$ does not have any zero entry and does not have full row rank, the rank of $H_{sc,qc}$ is upper bounded by $(cL + a - c)(q - 1) - ((c - 1)L + a - c + r)$.

The bound given in Theorem 5 is tight in many cases, and is verified by numerical analysis.

IV. SIMULATED PERFORMANCE ANALYSIS

Now we use an example to illustrate the proposed algebraic constructions of the SC QC LDPC codes. Suppose the constructed code is over GF($2^p$). For simplicity, we assume BPSK transmission over the AWGN channel, where each symbol in GF($2^p$) is expanded into $p$ bits for BPSK transmission. All the simulations are performed using Fast Fourier Transform (FFT) $q$-ary sum-product decoding [9], with 1000 maximum iterations for both SC and block codes.

**Example 1.** (An SC QC LDPC code over GF($2^7$)) We choose $r = 7, m = 3$ and $n = 64$. Consider the following SM-constrained matrix $B$ over GF($2^7$), which is constructed using the method proposed in [13].

$$B = \begin{bmatrix} \alpha^{63} & \alpha^{64} & \cdots & \alpha^{125} \\ 1 + \alpha^{63} & 1 + \alpha^{64} & \cdots & 1 + \alpha^{125} \\ \alpha + \alpha^{63} & \alpha + \alpha^{64} & \cdots & \alpha + \alpha^{125} \end{bmatrix}.$$

(7)
We choose $L = 80$, $a = 3$, $b = 2$ and $c = 1$ and the construct masking matrix $W$ based on (6). Using the replicate-and-mask process, we construct a $42 \times 80$ SC matrix $B_{sc}$. Applying the 127-fold dispersion to $B_{sc}$, we obtain a $42 \times 80$ SC array $H_{sc,qc}$ of $127 \times 127$ CPMs and ZMs. Label the columns of CPMs and ZMs from 0 to 79. Then, for $0 \leq i < 80$, we replace all the non-zero entries in the $i$-th column of CPMs and ZMs in $H_{sc,qc}$ by $\beta^i$, where $\beta$ is a primitive element of $GF(2^2)$. After such replacement procedure, we obtain a $42 \times 80$ SC array $H_{sc,qc,nb}$ of $127 \times 127$ weighted CPMs and ZMs, which is a $5334 \times 10160$ matrix over $GF(2^2)$. We find that the rank of $H_{sc,qc,nb}$ is equal to 5325. Note that $H_{sc,qc,nb}$ is obtained by performing elementary column operations on $H_{sc,qc}$, we see that the upper bound on the rank of $H_{sc,qc}$ given by Theorem 5 is tight in this example. Thus, the null space of $H_{sc,qc,nb}$ gives an $(10160,4826)$ algebraic Block $C$-CPM and ZMs. Label the columns of $H_{sc,qc,nb}$ as CPMs $A_1, A_2, \ldots, A_80$ and ZMs $B_1, B_2, \ldots, B_80$. The columns of $H_{sc,qc,nb}$ are such that the first $A_1$ column consists of all zero $127 \times 127$ matrix, the second $A_2$ column consists of all zero $42 \times 80$ matrix, the third $A_3$ column of $H_{sc,qc,nb}$ is the result of applying the $80 \times 80$ elementary column operation on $B_1$, the fourth $A_4$ column of $H_{sc,qc,nb}$ is the result of applying the $80 \times 80$ elementary column operation on $B_2$, and so on. The number of CPMs and ZMs for each column is obtained by performing elementary column operations on $H_{sc,qc}$.

The parity-check matrix $H_{sc,PEG}$ of an $(762,381)$ $(3,6)$-regular PEG LDPC block code. The parity-check matrix of an $(762,381)$ $(3,6)$-regular PEG LDPC block code. The parity-check matrix $H_{sc,PEG}$ of this SC LDPC code has the same degree distributions as $H_{sc,qc,nb}$. It is shown that at the BLER of $10^{-2}$, the algebraic SC QC LDPC code, constructed by techniques in this paper, has about 0.15 dB coding gain over the corresponding SC LDPC code constructed by unwrapping a PEG block code. It is also observed that, contrary to turbo codes, the constructed codes do not suffer from error floors.

Similar results of comparison have also been observed for a set of codes over $GF(2^2)$, which are omitted here due to the space limitation.

V. THRESHOLD SATURATION OF NON-BINARY SC LDPC CODES OVER THE BINARY INPUT AWGN CHANNEL

In this section, we investigate the threshold saturation phenomenon for the non-binary SC LDPC codes over the binary input AWGN channel. Since it is not practical to evaluate the GEXIT kernel function for general non-binary memoryless channel [20], we propose to find the equivalent bit-wise BP extrinsic estimator of non-binary BP decoder to evaluate the binary GEXIT function. Here we focus on the codes over $GF(2^2)$, but the method can be extended to the codes over a higher order field.

Let $x = (x_0, x_1, \ldots, x_{n-1})$ be a transmitted codeword over $GF(2^2)$. We expand each symbol $x_i$ ($0 \leq i < n$) into 2 bits, denoted by $x_{i,0}, x_{i,1}$, and each bit is mapped into a BPSK symbol with unit energy. Let $y_{i,0}, y_{i,1}$ denote the received signal corresponding to $x_{i,0}, x_{i,1}$, respectively, and let

$$y_i = (y_{i,0}, y_{i,1}, \ldots, y_{i,10}, y_{i,11}, y_{i,11}, \ldots, y_{i,10}, y_{i,11}).$$

Let $L_{ext,i} = (L_{ext,i,1}, L_{ext,i,2}, L_{ext,i,3})$ be the symbol-wise extrinsic BP estimator of $x_i$, where for $1 \leq j \leq 3$, $L_{ext,i,j} = \log \frac{P(x_i = 0 | y_i = 0)}{P(x_i = 1 | y_i = 0)}$ is and is computed by non-binary BP decoder. Let $L_{i,0}, L_{i,1}$ denote the channel LLR-values of $x_{i,0}$ and $x_{i,1}$, respectively.

We have the following theorem on the bit-wise BP extrinsic estimator.

**Theorem 6.** The bit-wise BP extrinsic estimator of $x_{i,0}$, denoted by $L_{bin,ext,i,0}$, can be expressed as:

$$L_{bin,ext,i,0} = \log \frac{e^{L_{ext,i,1} + L_{i,1}} + 1}{e^{L_{ext,i,2}} + e^{L_{ext,i,3} + L_{i,1}}}$$

(8)

Theorem 6 indicates that the bit-wise BP extrinsic estimator is a function of both the symbol-wise BP extrinsic estimator and the LLR of the other bit within this symbol. Fig. 4 gives a probability density function (PDF) of the estimator $L_{bin,ext,i,0}$ obtained by Monte-Carlo simulation. We see that this estimator can be well-approximated by a Gaussian distribution. Then, we only need to numerically compute the mean and variance of $L_{bin,ext,i,0}$ to compute its binary BP GEXIT function.

The numerical BP threshold results computed based on non-binary PEXIT for the $(3.6, L)$ SC LDPC code ensembles over $GF(2^2)$ are reported as follows in the pairs of $(L, \sigma)$, where $\sigma$ denotes the threshold corresponding to the given $L$: $(5, 1.13), (10, 0.99), (20, 0.97), (40, 0.97), (60, 0.96)$ and $(80, 0.96)$. Moreover, the upper bound (UB) of MAP threshold of the $(3.6)$ LDPC block code ensemble over $GF(2^2)$ computed based on the proposed equivalent bit-wise GEXIT analysis is also 0.96. All the thresholds are given in terms of the standard
deviation of the noise. We see that as $L$ increases, the BP threshold approaches\(^1\) the UB of MAP threshold of the block code. Therefore, we have verified that, under the Gaussian distribution assumption for the bit-wise extrinsic estimator, the threshold saturation holds for the SC LDPC codes over $\text{GF}(2^2)$ for binary-input AWGN channel.

VI. CONCLUSION

This paper considers the application of SC LDPC codes to practical communication systems by proposing finite-length algebraic quasi-cyclic constructions of SC LDPC codes. The proposed replicate-and-mask approach can guarantee desirable rank and girth properties of the SC QC LDPC codes. Numerical simulations show that the constructed algebraic non-binary SC QC LDPC codes outperform the corresponding non-binary random counterparts. The asymptotic performance of the non-binary SC LDPC is also investigated, where it is shown numerically that the threshold saturation phenomenon also holds for SC LDPC codes over $\text{GF}(2^2)$ on binary input AWGN channels. The methods in this paper can be extended to investigate the threshold saturation for SC LDPC codes over a higher order field for binary-input AWGN channel.

REFERENCES


\(^1\) For large $L$, the BP threshold approaches (but is not higher than) the UB of the MAP threshold. The first 4 BP thresholds are higher (or better) than the UB of the MAP threshold since the first 4 SC codes have lower rates.