Efficient Network for Non-Binary QC-LDPC Decoder

Chuan Zhang and Keshab K. Parhi
Department of Electrical and Computer Engineering
University of Minnesota, Twin Cities
Minneapolis, MN 55455, USA
{zhan0884, parhi}@umn.edu

Abstract—This paper presents approaches to develop efficient network for non-binary quasi-cyclic LDPC (QC-LDPC) decoders. By exploiting the intrinsic shifting and symmetry properties of the check matrices, significant reduction of memory size and routing complexity can be achieved. Two different efficient network architectures for Class-I and Class-II non-binary QC-LDPC decoder have been proposed, respectively. Comparison results have shown that for the code of the 64-ary (1260, 630) rate-0.5 Class-I code, the proposed scheme can save more than 70.6% hardware required by shuffle network than the state-of-the-art designs. The proposed decoder example for the 32-ary (992, 496) rate-0.5 Class-II code can achieve a 93.8% shuffle network reduction compared with the conventional ones. Meanwhile, based on the similarity of Class-I and Class-II codes, similar shuffle network is further developed to incorporate both classes of codes at a very low cost.

I. INTRODUCTION

Compared with binary ones, LDPC codes defined upon Galois field \( GF(q) \) with order higher than two have even more excellent error correction capabilities with proper encoding approach and code length [1]. However, with the improvement of decoding performance, higher computation complexity will follow. To this end, [2] proposed several sub-optimal selecting algorithms based on \( n \)-norm \( \| \| \) construction. As \( n \) decreases to 1, the optimal algorithm reduces to the Min-Max algorithm, which proves very suitable for practical purposes by achieving a good compromise between hardware costs and decoding performance. Meanwhile, a special class of non-binary QC-LDPC codes named non-binary QC-LDPC codes are constructed with the architecture-aware scheme [3]. Even though, the few implementations of non-binary QC-LDPC decoders employing Min-Max algorithm still suffer from a high hardware cost [4]-[5]. Without exploiting the inherent geometry properties of QC-LDPC codes, those designs employ either a conventional bi-directional network or two shuffle networks for re-shuffling, leading to a \( q \)-time increase of the network complexity.

In this paper, to make full use of benefits introduced by architecture-aware scheme, special emphasis has been placed on investigating the geometry properties of the corresponding \( H \) matrices. Rather than reconfiguring the global shuffle networks for each layer, the proposed approach employs two kinds of local shuffle network to eliminate the unnecessary network costs for Class-I and Class-II QC-LDPC codes, respectively. The designs are reconfigurable, memory efficient, highly parallel, and of low routing complexity. In order to demonstrate the advantages, both the 64-ary (1260, 630) rate-0.5 Class-I code and 32-ary (992, 496) rate-0.5 Class-II code are employed as examples. It is shown that, if flexibility is taken into account, 70.6% shuffle network cost can be reduced compared with the state-of-the-art designs for Class-I code and 93.8% for Class-II code. On the other hand, if flexibility is not a necessity, more memory and control logic can be eliminated. Moreover, a new local shuffle network which is compatible with both classes has been further proposed along with a minimum cost.

The remainder of this paper is organized as follows. In Section II, construction methods for both Class-I and Class-II codes are briefly reviewed. In Section III, geometry properties of both codes are investigated and summarized, respectively. Different layer partition choices have been proposed in Section IV. Section V describes the shuffle networks. The hardware costs estimation and comparisons with other designs are given in Section VI. Finally, Section VII concludes the whole paper.

II. NON-BINARY QC-LDPC CODES CONSTRUCTION

Like their binary counterparts, non-binary QC-LDPC codes are initiated by the motivation of architecture-aware design [3]. Using two similar array dispersions of matrices, constructions for two classes of QC-LDPC codes, referred as Class-I and Class-II codes, are proposed as well. It is know that elements of \( GF(q) \) can be represented in the power of primitive element: \( \alpha^\infty = 0, \alpha^0 = 1, \alpha^1, \ldots, \alpha^{q-2} \). The location vector \( z(\alpha) \) is defined as \( z(\alpha) = (z_0, z_1, \ldots, z_{q-2}) \), where the \( i \)-th component \( z_i = \alpha^i \), and all others are zeros. In addition, \( z(0) \) is the all-zero \((q-1)\)-tuple. The definition of circular permutation matrix (CPM) of \( z(\delta) \) is given by \( (z(\delta), z(\alpha \delta), \ldots, z(\sigma^{q-2} \delta)) \) accordingly, where \( \delta \) can be any element in \( GF(q) \). Therefore, the construction steps for Class-I codes can be stated as follows:

**Construction for Class-I Non-Binary QC-LDPC Codes**

1. **Factorization**: \( q-1 = c \times n, \text{gcd}(c, n) = 1; \)
2. **Element definition**: \( \beta = \alpha^\gamma, \delta = \alpha^\iota; \)
3. **Subgroup expansion**: \[
\begin{align*}
\mathcal{G} &= \{\beta^0 = 1, \beta, \ldots, \beta^{q-1}\}, \\
\mathcal{G} &= \{\delta^0 = 1, \delta, \ldots, \delta^{q-1}\};
\end{align*}
\]
4. **Matrix formation**: \[
\begin{align*}
W(i,j) &= [W(i,j)]_{\delta^{i} \times \delta^{j}}; \\
W_{i,j} &= [\delta^{-i} \beta^\gamma - \beta^\iota]_{\delta^{i} \times \delta^{j}};
\end{align*}
\]
5. **Substitution**: Replace each entry of \( W(i,j) \) by its CPM to get \( A^{(1)} = [A^{(1)}]_{\delta^{i} \times \delta^{j}}; \)
6. **Truncation**: \( H^{(1)} = A^{(1)}(\gamma, \rho) = [A^{(1)}]_{\delta^{i} \times \delta^{j} \times \delta^{k}}; \)
7. **Output**: \( H^{(1)}. \)

By simply changing the multiplications with additions, we obtain the construction steps for Class-II codes as follows. The similar construction steps for both codes yields resemblances in corresponding geometry properties and network designs, which are stated in Section III and V, respectively.
Construction for Class-II Non-Binary QC-LDPC Codes

1: Factorization: $q = 2^m$, $c = 2^m$, and $n = 2^t$;

2: Elements definition:
   \[
   \left\{ \beta \in \mathbb{Z} \right\} = \left\{ \alpha, \alpha^{-1}, \ldots, \alpha^{\frac{c-1}{2}} \right\};
   \left\{ \beta \in \mathbb{Z} \right\} = \left\{ \alpha, \alpha^{-1}, \ldots, \alpha^{\frac{c-1}{2}} \right\};
   \]

3: Subgroup expansion:
   \[
   \mathcal{T}_m = \left\{ \beta \in \mathbb{Z} \right\};
   \left\{ \beta \in \mathbb{Z} \right\} = \left\{ \alpha, \alpha^{-1}, \ldots, \alpha^{\frac{c-1}{2}} \right\};
   \]

4: Matrix formation:
   \[
   \mathbf{W}^{(2)} = \begin{bmatrix} \mathbf{W}^{(2)}_{i,j} \end{bmatrix}_{\mathcal{T}_m \times \mathcal{T}_m};
   \]

5: Substitution: Replace each entry of $\mathbf{W}^{(2)}$ by its CPM
   \[
   \beta \mathbf{A}^{(2)} = \begin{bmatrix} \mathbf{A}^{(2)}_{i,j} \end{bmatrix}_{\mathcal{T}_m \times \mathcal{T}_m};
   \]

6: Truncation: $\mathbf{H}^{(2)} = \mathbf{A}^{(2)}(\gamma, \rho) = \begin{bmatrix} \mathbf{A}^{(2)}_{i,j} \end{bmatrix}_{\mathcal{T}_m \times \mathcal{T}_m};
   \]

7: Output: $\mathbf{H}^{(2)}$.

III. PROPERTIES OF NON-BINARY QC-LDPC CODES

Although some apparent properties of non-binary QC-LDPC codes have been addressed by previous literatures [4]-[5], more geometry properties hidden behind the algebra architectures need to be revealed for efficient network designs.

A. Shifting Properties of Class-I Codes

According to the construction steps, one can verify the identity of $\mathbf{W}^{(2)}_{i,j}$ and its upper-left neighbor $\mathbf{W}^{(2)}_{(i-1)\mod c,(j-1)\mod c}$:
\[
\begin{align*}
\mathbf{W}^{(2)}_{i,j} &= \left[ \delta^{i-1} \beta^{j-1} - \beta^{j-1} \right] \\
&= \left[ \delta^{(i-1)\mod c} \beta^{(j-1)\mod c} - \beta^{(j-1)\mod c} \right] \\
&= \mathbf{W}^{(2)}_{(i-1)\mod c,(j-1)\mod c}.
\end{align*}
\]

Similar permutation property holds at the lower level:
\[
\begin{align*}
\mathbf{W}^{(2)}_{(i,j)(k,l)} &= \delta^{i-1} \beta^{j-1} - \beta^{j-1} \\
&= \beta^{(k-1)\mod n} - \beta^{(l-1)\mod n} \\
&= \mathbf{W}^{(2)}_{(i,j)(k-l)\mod n,(l-j)\mod n}.
\end{align*}
\]

Moreover, with the definition of CPM, the useful properties of Class-I codes can be summarized as follows:

Proposition 1 The Class-I non-binary QC-LDPC codes satisfy shifting properties at three different levels:

1. The $i$-th row of the base matrix $\mathbf{W}^{(1)}$ is exactly the 1-step right cyclic-shift of the $[(i-1)\mod c]$-th row. Therefore,
   \[
   \mathbf{W}^{(1)}_{i,j} = \mathbf{W}^{(1)}_{(i-1)\mod c,(j-1)\mod d};
   \]

2. The $k$-th row of the sub-matrix $\mathbf{W}^{(1)}_{i,j}$ is exactly the 1-step right cyclic-shift of the $[k\mod n]$-th row multiplied by $\beta$, that is,
   \[
   \mathbf{W}^{(1)}_{(i,j)(k+1)\mod n} = \beta \mathbf{W}^{(1)}_{(i,j)(k-1)\mod n};
   \]

3. The $m$-th row of the CPM corresponding to $\mathbf{W}^{(1)}_{(i,j)(k,l)}$ is the 1-step right cyclic-shift of the $[(m-1)\mod c]$-th row multiplied by $\alpha$, which is given by the definition of CPM.

B. Symmetry Properties of Class-II Codes

Unlike Class-I codes, it is not that trivial to uncover the geometry properties of Class-II codes. Since the surjective function mapping from elements of subgroups $\mathcal{T}_m$ to power forms of $\alpha$ is not specified, candidate(s) for value assignment scheme is not unique. Given this degree of freedom, a specific surjective function which yields symmetry properties is introduced purposely. Without loss of generality, details of the surjective function are described with the subgroup $\mathcal{T}_m$:

Index Assignment of Surjective Function

1: Suppose $\beta = \sum_{n=0}^{m-1} \alpha^n$, $\beta = \sum_{n=0}^{m-1} \alpha^n$, with $0 \leq m, n < t$;

2: if $p < q$ then $i < j$;

3: else if $p > q$ then $i > j$;

4: else

5: for $l = 0, 1, \ldots, t, l < p$ do

6: if $m_i < n_i$ then $i < j$ break;

7: else $m_i > n_i$ then $i > j$ break;

8: endfor

9: end

According to the proposed function, it can be verified that for any element $\beta$ in sub-group $\mathcal{T}_m$, Eq. (3) holds,
\[
\beta + \beta^{(2-t)\mod t} = \beta_{2-t} \tag{3}
\]

For sub-group $\mathcal{T}_m^*$, similar symmetry property holds as well,
\[
\delta + \delta^{(2-t)\mod t} = \delta_{2-t} \tag{4}
\]

Substituting Eq. (3) into the construction steps, we show that matrix $\mathbf{W}^{(2)}$ has the symmetry property shown in Eq. (5). Denote the sub-matrix of $\mathbf{W}^{(2)}$ by $\mathbf{W}^{(2)}_{i,j}$, then we have,
\[
\mathbf{W}^{(2)}_{i,j} = \mathbf{W}^{(2)}_{i-j+1,c-l-i-1}, \tag{5}
\]

Combining this fact with the matrix structure, it follows that $\mathbf{W}^{(2)}$ and its mirror about the anti-diagonal are identical. Similarly, Eq. (4) corresponds to the self-symmetry of $\mathbf{W}^{(2)}$ about its own anti-diagonal,
\[
\mathbf{W}^{(2)}_{(i,j)(k,l)} = \mathbf{W}^{(2)}_{(i,j)(k-l+1, c-l-i+1)}, \tag{6}
\]

On the other hand, for Class-II codes, both the base matrix $\mathbf{W}^{(2)}$ and its sub-matrix $\mathbf{W}^{(2)}_{i,j}$ are self-symmetric about their own diagonals. This is apparent from the 4th step of the construction for Class-II codes as follows,
\[
\mathbf{W}^{(2)}_{i,j} = \left[ \delta^{i-1} \beta^{j-1} + (\beta_{i-1} - \beta_j) \right] \tag{7}
\]

The above properties help to derive the following proposition:

Proposition 2 The Class-II non-binary QC-LDPC codes satisfy the geometry properties at three different levels:

1. The base matrix $\mathbf{W}^{(2)}$ is symmetric about its diagonal and anti-diagonal, i.e., $\mathbf{W}^{(2)}_{i,j} = \mathbf{W}^{(2)}_{i,j}$ and $\mathbf{W}^{(2)}_{i,j} = \mathbf{W}^{(2)}_{i-j+1,c-l-i-1}$.

2. The sub-matrix $\mathbf{W}^{(2)}_{i,j}$ is also symmetric about its diagonal and anti-diagonal, i.e., we have $\mathbf{W}^{(2)}_{(i,j)(k,l)} = \mathbf{W}^{(2)}_{(i,j)(k-l+1, c-l-i+1)}$ and $\mathbf{W}^{(2)}_{(i,j)(k,l)} = \mathbf{W}^{(2)}_{(i,j)(k+l-c, c-l-i+1)}$.

3. Each row of one CPM $\mathbf{W}^{(2)}_{(i,j)(k,l)}$ is the right cyclic-shift of the row above it multiplied by $\alpha$ and the first row is the right cyclic-shift of the last row multiplied by $\alpha$. 
1. Choose each sub-block row of $W^{(1)}_{i,j}$ or $W^{(2)}_{i,j}$ as one layer, which consists of $(q-1)$ rows. This option is defined as the Layer-I choice;
2. Choose each row of CPM $w^{(1)}_{i,j,k}$ or $w^{(2)}_{i,j,k}$ as one layer, which consists of only one row. This option is defined as the Layer-II choice.

V. LOCAL SHUFFLE NETWORKS FOR BOTH CODES

The architecture of the $(u, v)$ non-binary QC-LDPC decoder is shown in Fig. 2. $u = q(q-1)$ is the code length, $u+v = q(q-1)$ is the number of check bits, $w$ is the layer height. It is composed of $w$ CNUs, a de-/permutation block, a global shuffle network (GSN), and $u$ VNU$s$ with a local shuffle network (II). In what follows, with proposed geometry properties, different reduced-complexity shuffle networks for both codes are presented.

Figure 2: Block diagram of the layered non-binary QC-LDPC decoder.

A. Local Shuffle Network for Class-I Codes

1) Generating Algorithm for Local Shuffle Network

Apparently, Proposition 1.2 and 1.3 only differ in the value of the multiplicand ($\beta$ or $\alpha$). Without loss of generality, the Layer-I decoding scheme is chosen as an example.

Scheduling Algorithm for Local Shuffle Network - I

1: for all $0 \leq i < \rho$ do
2:     for all $0 \leq j < q-1$ do
3:         Pass the extrinsic result of last layer from
4:         VNU$_{i(q-1)+j}$ to VNU$_{(i+1)(q-1)+j}$
5:     endfor
6: endfor

The index of each VNU can be rewritten in the form of $i(q-1)+j$ (for short $(i, j)$). For the example depicted in Fig. 3, the index of VNU$_7$ can be rewritten as $(2, 1)$. Based on the new scheduling algorithm, the destination index is $(1, 0)$. Therefore, the extrinsic message should be transferred from VNU$_7$ to VNU$_3$ $(1 \times 3 + 0 = 3)$, which matches the previous analysis.

Figure 3: Layered decoding example of the 4-ary $(9, 3)$ rate-$\frac{1}{3}$ Class-I code.

2) Architecture of Local Shuffle Network

It is observed that the inter-layer shuffle scheduling is irrelevant of the current layer index. That is, no matter what number $i$ is, the extrinsic message transferring between the $i$-th layer and the $(i+1)$-th layer is exactly the same, which can be implemented by using fixed interconnections shown in Fig. 4.

Figure 4: Local shuffle network of Class-I codes case.
derived from the B. codes can be constructed based on the symmetry properties: choosing of the first row are defined by 0, symmetry properties. For instance, to do

\end{verbatim}

Different designs | Proposed designs | References
--- | --- | ---
Global shuffle network | | |
Wires' | $b_{n_0}(q-1)1d_c$ | |
De-MUX's | $0$ | $0$ |
LUT bits | $p(q-1)y$ | $p(q-1)y$ |
Local shuffle network | | |
Wires | $b_q(1)γ$ | $b_q(1)γ$ |
De-MUX's | $0$ | $0$ |
Crossbars | $0$ | $0$ |
LUT bits | $p(q-1)y$ | $p(q-1)y$ |
Class-I code | Yes | Yes |
Class-II code | Yes | Yes |
Flexibility | Yes | No |

*Both designs are for a 32-ary (837, 726) rate-0.85 Class-I code. 'n0' is the selecting parameter for Min-Max decoding algorithm.*

**B. Local Shuffle Network for Class-II Codes**

1) Generating Algorithm for Local Shuffle Network

Similar to Class-I codes, local shuffle network for Class-II codes can be constructed based on the symmetry properties:

**Scheduling Algorithm for Local Shuffle Network - II**

1: for all $0 < v \leq l$, the beginning of decoding the $v$th layer do
2: for all $0 \leq i < \rho do$
3: for all $0 \leq j < q-1 do$
4: Pass result of VNU $(q-1)(index_{i, j} + \rho \cdot \lfloor i/y \rfloor) + j$
5: to VNU $(q-1)(index_{i, j} + \rho \cdot \lfloor i/y \rfloor) + j$
6: endfor
7: endfor
8: endfor

INDEX$^{(o)}$ is an $n \times n$ matrix of $[\text{index}_{i, j}]_{0 \leq i, j < n}$. Entries of the first row are defined by $\text{index}_{0, j} = j$. Other entries are derived from the index assignment of surjective function and symmetry properties. For instance, INDEX$^{(4)}$ is given by,

\[
\text{INDEX}^{(4)} = \begin{bmatrix}
0 & 1 & 2 & 3 \\
1 & 0 & 3 & 2 \\
2 & 3 & 0 & 1 \\
3 & 2 & 1 & 0
\end{bmatrix}.
\]

A message shuffling example of 4-ary (12, 6) rate-½ Class-II code is illustrated in Fig. 5, the parameters are obtained by choosing $t = 1$, then $c = 2^{m_1} = 2$, and $n = 2^2 = 2$ over $GF(2^5)$.

![Figure 5: Layered decoding example of the 4-ary (12, 6) rate-½ Class-II code.](image)

2) Architecture of Local Shuffle Network

![Figure 6: Local shuffle network of the Class-II code defined by Eq. (12).](image)

The complexity of the resulting network is $1/q$ of that for the conventional one. Only $2\log_2\rho$ stages and $\rho\log_2\rho/2$ 2×2 crossbar switches are required. The number of control bits, which can be pre-acquired with INDEX$^{(o)}$ is $\rho\log_2\rho/2$. The local shuffle network for Eq. (12) is given in Fig. 6. With a modified INDEX$^{(o)}$, this approach is suitable for Class-I codes.

**VI. IMPLEMENTATION COMPLEXITY COMPARISONS**

Without loss of generality, it is assumed that the proposed $(u, v)$ decoder employs Layer-I partition. A $(b_q, b_h)$ uniform quantization is adopted, in which $b_q$ out of $b_h$ bits are used for fraction parts. Table I lists the comparison of the proposed design with others. Compared with the state-of-the-art decoders, the proposed one can greatly reduce the hardware complexity. According to [4] and [5], their network could not incorporate flexibility into the design due to the use of ROM. In Table I, there are two approaches to design the local shuffle network for Class-I codes. The first one (#1) is reconfigurable for any Class-I codes with code length $\rho(q-1)$. The second one (#2) is only suitable for a specific Class-I code. The #3 and #4 approaches deal with Class-II codes and codes of both classes, respectively. Take the 64-ary (1260, 630) rate-0.5 Class-I code as an example. While having more flexibility, the proposed shuffle network #1 achieves hardware saving of 69.2% and 70.6% compared with [4] and [5], respectively. Because the #2 approach can further eliminate all memory elements required by #1, more reduction can be expected. For configurable version of the 32-ary (992, 496) rate-0.5 Class-II code decoder with #3 network, the total saving is $(k-1)/k = 15/16 \approx 93.8\%$

**VII. CONCLUSIONS**

In this paper, with the exploited geometry properties of non-binary QC-LDPC codes, novel approaches to design efficient network for decoders are proposed, which outperform the state-of-the-art designs with more than 69.2% savings.

**REFERENCES**

[1] M. Davey and D. J. C. MacKay, “Low density parity check codes over $GF(q)$,” IEEE Commun. Lett., vol. 2, no. 6, pp. 165-167, June 1998.

[2] V. Savin, ”Min-Max decoding for non-binary LDPC codes”, in Proc. Int. Symp. on Commun. and Info. Tech., pp. 960-964, July 2008.

[3] B. Zhou, L. Zhang, J. Kang, Q. Huang, S. Lin, and K. Abdel-Ghaffar, “Array dispersions of matrices and constructions of quasi-cyclic LDPC codes over non-binary fields,” in Proc. IEEE Int. Symp. on Info. Theory, pp. 1158-1162, July 2008.

[4] X. Zhang and F. Cai, “Partial-parallel decoder architecture for quasi-cyclic non-binary LDPC codes,” in Proc. Int. Conf. Acoust., Speech, and Sig. Proc. (ICASSP), pp. 1506-1509, Mar. 2010.

[5] X. Zhang and F. Cai, “Reduced-complexity decoder architecture for non-binary LDPC codes,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 7, pp. 1229-1238, July 2011.