LDPC Code Designs Based on $\sqrt{I}$ Matrices

Shayan G. Srinivasa
Department of Electronic Systems Engineering
Indian Institute of Science, Bangalore, 560012
Email: shayan.gs@dese.iisc.ernet.in

Abstract—LDPC codes can be constructed by tiling permutation matrices that belong to the square root of identity type and similar algebraic structures. We investigate into the properties of such codes. We also present code structures that are amenable for efficient encoding.

Index Terms—LDPC codes, permutation matrices

I. INTRODUCTION

Low density parity check codes (LDPC) [1] are deployed in practical data transmission and storage systems due to their excellent error correction capabilities. The code construction, design of efficient encoding/decoding architectures and theoretical analysis towards provably guaranteed performance have been the subject of active research over the last few years. From an information-theoretic perspective, in order to get towards capacity, we need to build LDPC codes with (a) long block lengths, and (b) random structures, along with a near optimal decoding algorithm. The original sum-product algorithm is optimal for Tanner graphs that are acyclic.

The design of practical LDPC codes is guided by girth, degree distributions and structures that avoid dominant trapping sets [2]. Though random codes are attractive from performance perspective, they are not pragmatic due to high computational complexity associated with the encoding and decoding algorithms. Also, random codes have a huge storage complexity associated with the storing of parity and generator matrices. Hence, structured codes with algebraic and combinatorial structures are more amenable for practical coding architectures. One of the most popular code designs is based on the class of quasi-cyclic (QC) matrices [3]. QC codes can be encoded using simple shift registers. The decoding of QC-LDPC codes can be done in a parallel fashion by exploiting cyclic symmetry in the code using barrel shifters and modulo operations. Properly constructed QC-LDPC codes achieve performance close to random codes in the waterfall and error floor regions. This has paved way for their deployment in most Silicon integrated circuit (IC) applications.

Permutation matrices offer flexible degrees of parallelism in the construction of LDPC codes suited for high speed applications. By grouping a subset of permutation matrices with a predefined algebraic structure, we can construct structured LDPC codes for parallel encoding and decoding of data. In this paper, we are interested in constructing structured LDPC codes by tiling permutation matrices that belong to the square-root of identity class. We show that the generator matrix comprises of a tile of submatrices, each of which can be realized a sum of $\sqrt{I}$ matrices. This is similar to QC-codes that have generator matrices expressed in systematic-circulant (SC) form. We also highlight an efficient on-the-fly encoding method that can work with these codes. We show that $\sqrt{I}$ matrices offer efficient encoding and decoding structures amenable for practical realization of coding architectures and performance gains comparable to the QC-LDPC family of codes.

The remainder of this paper is organized as follows. In section II, we describe the construction of binary $\sqrt{I}$ LDPC codes guided by girth, code rate and degree distributions. We study the properties of these matrices, in particular, the rank of these matrices, with an eye towards efficient encoding. In section III, we show an equivalence between generator matrices from $\sqrt{I}$ LDPC codes with QC family of LDPC codes. We also highlight the conditions for efficient on-the-fly encoding for these codes. Simulation results are discussed in section IV followed by conclusions in section V.

II. TILING $\sqrt{I}$ LDPC MATRICES

Let $\mathcal{P}$ denote the set of all permutation matrices of order $p$. We have $|\mathcal{P}| = p!$ such matrices. The set of all permutation matrices of order $p$ forms a special linear group $SLG(p)$. Let $\mathcal{S}_p \subset \mathcal{P}$ be a subset of permutation matrices defined for even order $p$ with the property $A^2 = I$ for $A \in \mathcal{S}$. The matrices in $\mathcal{S}_p$ are defined to belong to the $\sqrt{I}$ family of matrices over $GF(2)$, and are full rank.

Example: For $p = 2$, we have

$$S_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$ 

In the following subsection, we will explore a few properties of these matrices.

A. Structure and properties

Let bin$(a)$ be the binary representation of an integer $a$ such that $0 \leq a \leq p - 1$. Given $a$, the basic tile for a $p \times p \sqrt{I}$ matrix can be constructed as follows:

- Represent the rows $0 \leq i < p - 1$ and columns $0 \leq j < p - 1$ in the form of binary tuples corresponding to the row/column positions.
- Populate a ‘1’ in the array position $(i, j)$ if bin$(i) + \text{bin}(j) = \text{bin}(a) \mod (2)$.

Example: For $p = 4$ and $a = 1$, we can build a matrix $\phi(a) \in \mathcal{S}_p$ as,
\[
\phi^{(1)} = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

Let \( A \) and \( B \) any two matrices \( \in \mathcal{S}_p \), i.e., \( A^2 = I \) and \( B^2 = I \).

**Lemma 1:** The following properties hold true:

1) \( AB = BA \).
2) \( (AB)^2 = I \).

**Proof:**

(1) In order to prove the first property, we note that \( A = A^T \) and \( B = B^T \) since commutative addition holds true over the code coordinates.

\[
(AB)^T = B^T A^T = BA
\]

But,

\[
(AB)^T = AB.
\]

Using equations (1) and (2), the first property is proved.

(2) In order to prove the second property, we note that \( A^{-1} = A \) and \( B^{-1} = B \), where \( I \) is the identity element.

\[
(AB)^2 = (AB)(AB).
\]

Using the property \( BA = AB \) in equation (3), we have,

\[
(AB)^2 = (AB)(BA).
\]

This establishes the second property.

For \( A \) and \( B \in \mathcal{S}_p \), the following result is true regarding the rank of the matrices under modulo binary addition.

**Lemma 2:** \( \text{gfrank}(A + B) = \frac{1}{2} p \).

**Proof:**

Let \( a \) and \( b \) be integers for construction of the matrices \( A \) and \( B \) respectively. We note that \( A + B \) has repeated rows since the positions of ones occurring in the \( i \)-th row of \( A + B \) are identical to a positions of ones occurring in the \( j \)-th row of \( A + B \) when \( \text{bin}(i) + \text{bin}(j) = (\text{bin}(a) + \text{bin}(b)) \mod(2) \). Since such rows \( i \) and \( j \) form a pair,

\[
\text{gfrank}(A + B) = \frac{1}{2} p.
\]

**III. Properties towards efficient encoding**

We will address how efficient encoding can be done for parity check matrices obtained by tiling \( \sqrt{T} \) matrices. We first show that the generator matrix comprises of a tile of submatrices, each of which can be realized a sum of \( \sqrt{T} \) matrices. Let \( X \) be a \( p \times p \) matrix such that \( X = \sum_{i=1}^{n} X_i \), where \( X_i \in \mathcal{S}_p \). Let \( y \) and \( z \) be \( p \times 1 \) row vectors with 0,1 entries and weights \( s \) and \( t \) respectively. Suppose \( Z \) is expressed as a sum of matrices \( \in \sqrt{T} \), which we have the following result.

**Theorem 1:** The solution to \( (\sum_{i=1}^{n} X_i) y = z \) exists such that \( Y \) is a sum of matrices \( \in \sqrt{T} \).

**Proof:**

Suppose we have a solution to the equation

\[
\left( \sum_{i=1}^{n} X_i \right) y = z.
\]

We can express equation (6) as

\[
\sum_{i=1}^{n} X_i \sum_{i=1}^{s} y_i = \sum_{i=1}^{t} z_i.
\]

Suppose \( \phi^{(\text{dec}(y_i))} \) and \( \phi^{(\text{dec}(z_i))} \) are the equivalent matrices belonging to \( \sqrt{T} \) class, where, the function \( \text{dec}(\cdot) \) is the decimal equivalent of the integer representing the \( \sqrt{T} \) matrix tile. We can express equation (7) as

\[
\sum_{i=1}^{n} X_i \left( \sum_{i=1}^{s} \phi^{(\text{dec}(y_i))} \right) [10...0]^T = \left( \sum_{i=1}^{t} \phi^{(\text{dec}(z_i))} \right) [10...0]^T.
\]

Let \( \psi^{(k)} \) be a matrix belonging to \( \sqrt{T} \) class such that \( k \) is the integer representing decimal equivalent of the binary vector in first column of \( \psi^{(k)} \).

Pre-multiplying both sides of equation (8) by \( \psi^{(k)} \), and using the fact that \( \psi^{(k)} \) and \( \sum_{i=1}^{n} X_i \) commute as per Lemma 1, we have,

\[
\sum_{i=1}^{n} X_i \psi^{(k)} \left( \sum_{i=1}^{s} \phi^{(\text{dec}(y_i))} \right) [10...0]^T = \psi^{(k)} \left( \sum_{i=1}^{t} \phi^{(\text{dec}(z_i))} \right) [10...0]^T.
\]

Since \( \psi^{(k)} \) operating on \( \sum_{i=1}^{s} \phi^{(\text{dec}(y_i))} \) is essentially reading off the \( k \)-th column from each of \( \phi^{(\text{dec}(y_i))} \) and \( \phi^{(\text{dec}(z_i))} \), we can express (9) as follows

\[
\sum_{i=1}^{n} X_i \left( \sum_{i=1}^{s} \phi^{(\text{dec}(y_i))} \right) [0..1..0]^T = \left( \sum_{i=1}^{t} \phi^{(\text{dec}(z_i))} \right) [0..1..0]^T.
\]

The equation (10) holds for every \( \psi^{(k)}, 0 \leq k \leq p - 1 \), implying that, generator matrices for \( \sqrt{T} \) matrices can be expressed in systematic-square root of identity form.
We note that this result is similar to the quasi-cyclic codes [3]. The efficient encoding procedure from [3] can be easily applied to the above case.

A. On-the-fly encoding

Some times fast encoding circuitry is needed in applications such as dynamic network coding where throughput and storage requirements are stringent. For this purpose, we can use the on-the-fly method [4]. Let \( k \) and \( n \) denote the user and code lengths respectively. The key idea is to decompose the parity check matrix as \( H := [A|B] \) in systematic form, where \( A \) is of order \( (n-k) \times k \) and \( B \) is of order \( (n-k) \times (n-k) \) belonging to \( \sqrt{I} \) type of matrices. By choosing prototype masks [4] with the desired flexibility of degree distribution and parallelism \( p \) over the matrix \( B \), we can ensure that the parity bits can be constructed on-the-fly. The following theorem provides the conditions for the existence of such encoders.

**Theorem 2:** The condition \( \text{gfrank}(B) = n - k \) is necessary and sufficient for the construction of on-the-fly encoders [4].

IV. Code performance evaluation

To validate the efficacy of the codes, we evaluate the \( \sqrt{I} \) LDPC codes under the additive white Gaussian noise (AWGN) channel model with zero mean and variance \( \sigma^2 \). The code rate was fixed to be around \( \frac{8}{9} \) with column weight 4 and block length of 8192 bits. The signal-to-noise ratio (SNR) was evaluated as

\[
\text{SNR}(dB) = 10 \log_{10} \left( \frac{1}{R\sigma^2} \right).
\]

![SNR vs. Probability of code failure](image)

**Fig. 1.** Probability of code failure over the AWGN channel model.

For the purposes of comparison, codes from QC family were compared against \( \sqrt{I} \) class. As we can observe from Fig. 1, the performance difference between the two code families is very marginal for two particular code instances simulated.

V. Conclusions

Permutation matrices offer a wide range of flexibility in the design of structured LDPC codes. Codes constructed from \( \sqrt{I} \) family of matrices share similarities in the structure of generator and parity check matrices. As a consequence, efficient encoding methods can be realized for this class of codes similar to the QC family of codes. The generalizations into \( \sqrt{I} \) matrices, and an efficient encoding structure in the most general form is of theoretical interest.

Acknowledgement

The author would like to acknowledge his former colleague Dr. Razmik Karabed for very fruitful and insightful discussions on \( \sqrt{I} \) matrices.

References


