Construction of Irregular Quasi-Cyclic Codes by Circulant Decomposition Based on Difference Family

XiaXu, LiYing, Moon ho Lee
Department of Information & Communication Engineering
Chonbuk National University, Chonju 561-756, Korea
Email: xiatony@mail.chonbuk.ac.kr
Tel: 82-63-279-2463

Abstract-We consider in this paper decomposing quasi-cyclic low-density parity check codes (LDPC) based on difference family. The resulting codes can be encoded with low complexity and perform well when iteratively decoded with the sum-product algorithm.

Keywords- quasi-cyclic codes, difference families and low-density parity-check codes.

I. Introduction

Low density parity-check (LDPC) codes were first presented by Gallager [4] in 1962 and have created much interest recently when rediscovered and shown to perform remarkably close to the Shannon limit. Decoding with the sum-product algorithm requires only that the parity-check matrix, \( H \), be sparse. However, decoding performance can often be improved if the code is also free of 4-cycles, which occur if two code bits are both checked by the same pair of parity-check equations. Gallager described regular codes, defined by parity-check matrices with constant column and row weights, which were constructed pseudo-randomly to avoid 4-cycles [4]. Randomly realized finite length irregular LDPC codes with block size on the order of \( 10^4 \) approach their density evolution threshold closely at rate 1/2. While optimized irregular codes are capable of excellent performance with reasonable decoding complexity, one of the main hurdles in the implementation of LDPC codes is the computational complexity of the encoding algorithm. Encoding is, in general, performed by matrix multiplication and so complexity is quadratic in the code length. One option for efficient encoding is to use algebraic code constructions and exploit the subsequent code structure. In the case of regular codes a number of algebraic constructions have been presented, such as in [7], [5], [12]. Less consideration however has been given to structured irregular codes. The aim of this paper is to give a new construction of irregular quasi-cyclic codes free of 4 cycles by circulant decomposition using difference families to improve their performance with sum-product decoding.

This paper is organized as follows: In section II and section III quasi-cyclic codes and different family are shown respectively, then we give the method of decomposing quasi-cyclic codes in section IV. Finally we present simulation results and conclusion in section V.

II. Quasi-Cyclic Codes

A code is quasi-cyclic if, for any cyclic shift of a codeword by \( p \neq 1 \) places, the resulting word is also a codeword [10]. A cyclic code is a quasi-cyclic code with \( p = 1 \). We consider binary quasi-cyclic codes described by a parity-check matrix

\[
H = \begin{bmatrix} B_1, B_2, \ldots, B_p \end{bmatrix}
\]  

(1)

where \( B_1, B_2, \ldots, B_p \) are binary \( v \times v \)
circulant matrices. Provided that one of the Circulant matrices is invertible (say $B_p$) the generator matrix for the code can be constructed in systematic form

$$
G = \begin{bmatrix}
I_{v(p-1)} & (B_p^{-1}B_1)^T \\
B_p^{-1}B_2^T & (B_p^{-1}B_{p-1})^T
\end{bmatrix}
$$

resulting in a quasi-cyclic code of length $vp$ and dimension $v(p-1)$. Encoding can be achieved with linear complexity using $v(p-1)$-stage shift register in much the same way as for cyclic codes [10]. The algebra of $v \times v$ binary Circulant matrices is isomorphic to the algebra of polynomials modulo $x^v - 1$ over GF (2) [10]. A Circulant matrix $B$ is completely characterized by the polynomial

$$
a(x) = a_0 + a_1x + \cdots + a_{v-1}x^{v-1}
$$

with coefficients from its first row, and a code $C$ with parity-check matrix of the form (1) is completely characterized by the polynomials $a_1(x), \ldots, a_p(x)$. Polynomial transpose is defined as

$$
a(x)^T = \sum_{i=0}^{n-1} a_i x^{n-i}, x^n = 1.
$$

For a binary $[n, k]$ code, length $n = vp$ and dimension $k = v(p-1)$, the $k-bit$ message $[i_0, i_1, \ldots, i_{k-1}]$ is described by the polynomial

$$
i(x) = i_0 + i_1x + \cdots + i_{k-1}x^{k-1}
$$

and the codeword for this message is

$$
c(x) = i(x) \cdot x^k p(x)
$$

where $p(x)$ is given by

$$
p(x) = \sum_{j=1}^{p-1} i_j(x) \cdot (a_p^{-1}(x) \cdot a_j(x))^T
$$

$i_j(x)$ is the polynomial representation of the information bits $i_{v(j-1)}$ to $i_{vj-1}$

$$
i_j(x) = i_{v(j-1)} + i_{v(j-1)+1}x + \cdots + i_{vj-1}x^{v-1}
$$

and polynomial multiplication ($*$) is mod $x^v - 1$.

As an example, consider a rate-1/2 quasi-cyclic code with $v = 5, p = 2$, first circulant described by $a_1(x) = 1 + x$ and second Circulant described by $a_2(x) = 1 + x^2 + x^4$

which is invertible $a_2^{-1}(x) = x^2 + x^3 + x^4$.

The generator matrix contains a $5 \times 5$ matrix described by the polynomial

$$
(a_2^{-1}(x) \cdot a_1(x))^T = (1 + x^2)^T = 1 + x^3
$$

$$
H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1
\end{bmatrix}
$$

a) Parity-check matrix with two circulants

$$
G = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1
\end{bmatrix}
$$

b) Generator matrix in systematic form

Parity checks

Bits in the first circulant

Bits in the second circulant
III. Difference Family

A difference family is an arrangement of a group of \( v \) elements such as \( \mathbb{Z}_v \) into not necessarily disjoint subsets of equal size, which meet certain difference requirements.

**Definition:** The \( t \gamma \) element subsets of the group \( \mathbb{Z}_v \), \( D_1,D_2,...,D_t \) with \( D_i = \{d_{i,1},d_{i,2},...,d_{i,\gamma}\} \) form a \( (v,\gamma,\lambda) \) difference family if the differences \( d_{i,1}-d_{i,y} \),

\[
( i=1,...,t; x,y=1,...,\gamma, x \neq y )
\]
given each nonzero element of \( \mathbb{Z}_v \) exactly \( \lambda \) times.

For a quasi-cyclic code we define the column weight distribution of a length \( vp \) rate \( p^{-1} \) code as the vector \( W = [w_1,w_2,...,w_p] \), where \( w_j \) is the column weight of the columns in the \( j \)th circulant.

**Construction 1:** To construction a length \( vp \) rate \( (p-1)/p \) quasi-cyclic code, \( H = \{a_1(x),a_2(x),...,a_p(x)\} \), with weight distribution \( W = [w_1,w_2,...,w_p] \), take \( p \) sets \( D_1,...,D_p \) of a \( (v,\gamma,\lambda) \) difference family with \( \gamma \geq w_{\text{max}} \), such that \( a_j(x) \) is defined using \( w_j \) of the elements of \( D_j \) as

\[
a_j(x) = x^{d_{j,1}} + x^{d_{j,2}} + ... + x^{d_{j,w_j}}
\]

To ensure invertibility at least one \( a_j(x) \) must divide \( x^v - 1 \).

**Lemma 1:** A pair of elements from \( \mathbb{Z}_v \) occur together exactly \( \lambda \) times in the set of translates of every set in a \( (v,\gamma,\lambda) \) difference family.

**Lemma 2:** The codes of the Construction 1 have Tanner graphs free of 4-cycles.

Proof: [14].

IV. Circulant Decomposing

Consider a \( v \times v \) circulant \( B_1 \) over GF (2) with column and row weight \( w \). Because column and row weights of a circulant are the same, for simplicity, we say that \( B_1 \) has weight \( w \). For \( 1 \leq t \leq w \), let \( w_1,w_2,...,w_t \) be a set of positive integers such that \( 1 \leq w_1,w_2,...,w_t \leq w \), and \( w_1 + w_2 + ... + w_t = w \). Then we can decompose \( B_1 \) into \( t \) \( v \times v \) circulants with weights \( w_1,w_2,...,w_t \), respectively. Let \( b_1 \) be the first column of \( B_1 \). We split \( b_1 \) into \( t \) columns of the same length \( v \), denoted by \( b_1^{(1)},b_1^{(2)},...,b_1^{(t)} \), such that the first \( w_1 \) 1-components of \( b_1 \) are put in \( b_1^{(1)} \), the next \( w_2 \) 1-components of \( b_1 \) are put in \( b_1^{(2)} \),..., and the last \( w_t \) 1-components of \( b_1 \) are put in \( b_1^{(t)} \). For each new column \( b_1^{(i)} \), we form a \( v \times v \) circulant \( B_1^{(i)} \) by cyclically shifting \( b_1^{(i)} \).
downward \( v \) times. This results in \( t \times v \times v \) circulants, \( B_1, B_2, \ldots, B_t \), with weights \( w_1, w_2, \ldots, w_t \) respectively. These circulants are called the descendants of \( B_1 \). Such a decomposition of \( B_1 \) is called column decomposition of \( B_1 \). Column decomposition of \( B_1 \) results in a \( v \times tv \) matrix

\[
B_1 = \begin{bmatrix} B_{11} & B_{12} & \cdots & B_{1t} \end{bmatrix},
\]

which is a row of \( t \times v \times v \) circulants. The parameter \( t \) is called the column splitting factor. If \( t = w \) and \( w_1 = w_2 = \ldots = w(t) = 1 \) then each descendant circulant \( B_{1i} \) of \( B \) is a permutation matrix and \( B \) is a row of \( t \) permutation matrices.

Figure 1 shows a column decomposition of a \( 5 \times 5 \) circulant of weight 3 into two descendants with weights 2 and 1, and descendant matrices can be described by

\[
1 + x^2, x^4, \text{respectively.}
\]

\[
B_i = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}
\]

Fig 1 A column decomposition of a circulant of weight 3

If no two columns in \( B_1 \) have more than one 1-component in common, then no two columns in \( B_1 \) have more than one 1-component in common.

In this case the null space of \( B_1 \) gives a quasi-cyclic LDPC code whose Tanner graph is free of cycles of length 4. If \( B_1 \) is a sparse matrix, \( B_{11} \) is also a sparse matrix with smaller density than \( B_1 \). So after decomposing we extended the H matrix to get the smaller density matrix with a minimum distance of at least 4.

V. Conclusion

Using the \((101,5,1)\) difference family from [2],

\[
\begin{align*}
D_1 &= \{0,14,42,47,55\}, D_2 = \{0,95,83,52,63\} \\
D_3 &= \{0,17,51,21,74\}, D_4 = \{0,36,79,26\} \\
D_5 &= \{0,100,98,76,71\}
\end{align*}
\]

the quasi-cyclic irregular LDPC codes have been constructed:

a rate-2/3,\([303,202]\) code with \( a_1 = x^{D_3} \) decomposing to descendant matrices expressed by

\[
b_{11} = 1 + x^{17}, b_{12} = x^{21} + x^{51}, b_{13} = x^{74}
\]

a rate-3/4,\([404,303]\) code with \( a_1 = x^{D_3} \) decomposing to descendant matrices expressed by

\[
b_{11} = 1 + x^{51}, b_{12} = x^{17}, b_{13} = x^{21}, b_{14} = x^{74}
\]

a rate-6/7,\([707,606]\) code with \( a_1 = x^{D_3} \) decomposing to descendant matrices expressed by

\[
b_{21} = 1 + x^{92}, b_{22} = x^{7}, b_{23} = x^{26}, b_{24} = x^{36}, \\
b_{21} = 1 + x^{52}, b_{22} = x^{21}, b_{23} = x^{63} + x^{83}, b_{31} = x^{95}
\]

where \( x^{D_j} = x^{d_{j,1}} + \cdots + x^{d_{j,t}} \).
Fig 2. Error correction performance of LDPC codes on an AWGN channel. The rate-2/3 \[303,202\] irregular quasi-cyclic code with \(W=[2,2,1]\), the rate-3/4 \[404,303\] irregular quasi-cyclic code with \(W=[2,1,1,1]\) and the rate-6/7 \[707,606\] irregular quasi-cyclic code with \(W=[2,1,1,1,2,2,1]\) These new codes are compared to regular quasi-cyclic codes based on difference family. The decoding performance of the quasi-cyclic codes shown in Fig2, Fig 3 presents that it is a modest performance gain to be made over the regular quasi-cyclic codes by using column decomposition method to get irregular quasi-cyclic LDPC codes. Further it has the advantage of a reduced encoding complexity.

Fig 3 Error correction performance of LDPC codes on an AWGN channel. The rate-2/3 \[303,202\] irregular quasi-cyclic code with \(W=[2,2,1]\) and the rate-3/4 \[404,303\] irregular quasi-cyclic code with \(W=[2,1,1,1]\) compared regular quasi-cyclic LDPC codes.

References