Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 7468792, 10 pages
https://doi.org/10.1155/2019/7468792

Research Article

A Construction of High Performance Quasicyclic LDPC Codes: A Combinatoric Design Approach

Muhammad Asif,[1] **Wuyang Zhou**,[1] **Muhammad Ajmal**,[2] **Zain ul Abiden Akhtar**,[3] **and Nauman Ali Khan**[1]

[1]*Key Laboratory of Wireless-Optical Communication, University of Science and Technology China, Hefei, 230027, China*
[2]*School of Mathematical Science, University of Science and Technology China, Hefei, 230027, China*
[3]*Department of Telecommunication Engineering, The Islamia University of Bahawalpur, Bahawalpur, Pakistan*

Correspondence should be addressed to Wuyang Zhou; wyzhou@ustc.edu.cn

Received 11 July 2018; Revised 5 November 2018; Accepted 10 December 2018; Published 3 February 2019

Academic Editor: Michael McGuire

This correspondence presents a construction of quasicyclic (QC) low-density parity-check (LDPC) codes based on a special type of combinatorial designs known as block disjoint difference families (BDDFs). The proposed construction of QC-LDPC codes gives parity-check matrices with column weight three and Tanner graphs having a girth lower-bounded by 6. The proposed QC-LDPC codes provide an excellent performance with iterative decoding over an additive white Gaussian-noise (*AWGN*) channel. Performance analysis shows that the proposed short and moderate length QC-LDPC codes perform as well as their competitors in the lower signal-to-noise ratio (SNR) region but outperform in the higher SNR region. Also, the codes constructed are quasicyclic in nature, so the encoding can be done with simple shift-register circuits with linear complexity.

1. Introduction

Low-density parity-check codes [1] are of vital importance for many modern communication systems because of their capacity-approaching performance and low-complexity iterative decoding over noisy information channels. LDPC codes were first discovered by Robert Gallager in the early 1960's and rediscovered by Mackay [2] in 1990's. LDPC codes provide many advantages over other error correction codes in terms of error performance, low-cost encoding and decoding, and a flexible scale for code length and rate selection. Therefore, LDPC codes have become a focal choice for many advanced communication standards such as Wi-Fi (802.11n/ac/ad), WiMAX (802.16e), and 10 Gigabit Ethernet (802.3an). After several rounds of discussions, LDPC codes have been determined for 5G communications. LDPC codes have been adopted by an important scenario of 5G communications known as enhanced mobile broadband (eMBB). The most promising error correction codes for 5G communications are polar codes, spatially coupled LDPC codes, binary/nonbinary LDPC codes, block Markov superposition transmission (BMST), and turbo codes. Recently, in literature [3, 4], low-complexity decoding algorithms have been presented for LDPC codes. Because of these significant efforts, LDPC codes have been adopted for many next-generation communication systems.

A binary (w_c, w_r)-regular LDPC code is defined by the null space of a parity-check matrix H having constant column-weight w_c and constant row-weight w_r. The null space of a parity-check matrix having variable column and/or variable row weights gives an irregular LDPC code. If the parity-check matrix consists of an array circulant permutation matrices of same size over a finite field $GF(q)$, the null space of this parity-check matrix gives a QC-LDPC code over $GF(q)$ [5–7]. An important constraint on parity-check matrix that any two rows or columns of H can agree in at most one position, called Row-Column (RC)-constraint. The RC-constraint on parity-check matrix H guarantees that the Tanner graph of an LDPC code has no length-4 cycles.

Based on the major construction methods, LDPC codes are categorized into two classes: (1) random-like LDPC codes are designed based on computer search, the most

well-known random-like constructions are based on PEG [8] and protograph-based methods [9–11]; (2) structured LDPC codes are constructed based on algebraic techniques such as finite fields [5, 6, 12–20], finite geometries [21, 22], and combinatorial structures [23–32]. The QC-LDPC codes, also known as architecture-aware codes, are one of the most studied LDPC codes because their parity-check matrices have a special structure which facilitates the hardware implementations of an encoder and decoder. Compared to random-like LDPC codes, the QC-LDPC codes have generator matrices which are quasicyclic in nature, so encoding can be done with shift register circuits having linear complexity.

Recently, some researchers have focused on a special class of regular QC-LDPC codes with parity-check matrices composed of an array of circulant permutation matrices and proved that the minimum distance of any (w_c, w_r)-regular QC-LDPC code is lower-bounded by $w_c + 1$ and a girth of at most 12 [33, 34]. In literature [23–32], QC-LDPC codes have been constructed based on the different combinatorial structures. In this correspondence, a construction method for binary QC-LDPC codes based on block disjoint difference families [35, 36] is presented. The proposed construction scheme gives length-4 cycles free QC-LDPC codes. The proposed QC-LDPC codes constructed for short and moderate length applications provide excellent error-correcting performance with iterative decoding over an *AWGN* channel. Based on numerical testing, the proposed QC-LDPC codes perform as well as their competitors in the lower SNR region but outperform in the higher SNR region. Also, the codes constructed are quasicyclic in nature, so the encoding can be done with simple shift-register circuits with linear complexity.

The remainder of this correspondence is arranged as follows: in Section 2, the basic concepts about design theory and cyclic difference families (CDFs) are given. The existence and construction of block disjoint difference families based on Skolem and Rosa Triple systems are given in Section 3. Section 4 presents the construction of QC-LDPC codes based on BDDFs for $v = 1, 3 \bmod 6$. Performance analysis based on numerical results is presented in Section 5, and the conclusion of this correspondence is presented in Section 6.

2. Basic Concepts and Definitions

In this section, we discuss some basic concepts of design theory such as balanced incomplete block design (BIBD), cyclic difference families, and block disjoint difference families.

Definition 1 (see [37]). A design is a pair (X, A), where X is a set of elements called points and A is a collection of nonempty subsets of X called blocks. Let v, k, and λ be positive integers such that $v > k \geq 2$. A (v, k, λ)-BIBD is a design (X, A) such that the following properties hold:

(i) $|X| = v$,

(ii) each block contains exactly k points, and

(iii) every pair of points appear in exactly λ blocks.

Definition 2 (see [37]). Let $Z_v = \{0, 1, \ldots, v-1\}$ be an additive group. The ω k-element subsets of Z_v, $A_i = \{a_{i1}, a_{i2}, \ldots, a_{ik}\}$, $i = 1, 2, \ldots, \omega$, $a_{i1} < a_{i2} < \cdots < a_{ik}$, give a cyclic difference family represented as (v, k, λ) if all nonzero elements appear λ times among the differences $a_{ix} - a_{iy}$, $i = 1, 2, \ldots, \omega$, $x \neq y$, $x, y = 1, 2, \ldots, k$. This (v, k, λ)-CDF is called a planar CDF if $\lambda = 1$.

In [26–30], $(k(k-1)\omega+1, k, 1)$-CDFs are used to construct QC-LDPC having a girth lower bounded by 6. The existences of $(k(k-1)\omega + 1, k, 1)$-CDFs are given in Theorem 3.

Theorem 3. *Under any of the following conditions, a* $(v, k, 1)$*-CDF exists:*

(i) *A* $(6\omega + 1, 3, 1)$ *cyclic difference family exists for all* $\omega \geq 1$ *[38].*

(ii) *A* $(12\omega + 1, 4, 1)$ *cyclic difference family exists for all* $1 \leq \omega \leq 1000$ *[39].*

(iii) *A* $(20\omega + 1, 5, 1)$ *cyclic difference family exists for* $1 \leq \omega \leq 50$ *and* $\omega \neq 16, 25, 31, 34, 40, 45$ *[40].*

In this correspondence, regular QC-LDPC codes of short and moderate lengths are constructed using a special class of cyclic difference families, called block disjoint difference families.

Definition 4 (see [36]). If Z_v is an additive group, then a family of k-tuples of elements from Z_v is a (v, k, λ)-CDF if the collection of blocks of k-tuples form a (v, k, λ) balanced incomplete block design. If this collection of blocks is disjoint, the family (v, k, λ) is known as a block disjoint difference family.

In next section, we review some constructions of $(v, 3, 1)$-BDDFs based on Skolem Triple System and Rosa Triple System for $v = 1 \bmod 6$ and $v = 3 \bmod 6$, respectively. Finally, we will use $(v, 3, 1)$-BDDFs, $v = 1, 3 \bmod 6$, to desing lenght-4 cycles free binary QC-LDPC codes.

3. Block Disjoint Difference Families (BDDFs)

3.1. Construction of (v, 3, 1)-BDDFs for v= 1 mod 6. Based on Skolem Triple System, a class of $(v, 3, 1)$-CDFs is used to construct $(v, 3, 1)$-BDDFs for $v = 1 \bmod 6$. First, we construct $(v, 3, 1)$-CDFs based on Skolem Triple Systems, and then a linear translation of $(v, 3, 1)$-CDFs gives $(v, 3, 1)$-BDDFs for $v = 1 \bmod 6$.

Definition 5 (see [37]). A sequence $S = (s_1, s_2, \ldots, s_{2\omega})$ of 2ω elements taken from $\{1, 2, \ldots, \omega\}$ is known as a Skolem sequence of order ω if

(i) every $s_m \in \{1, \ldots, \omega\}$ appears exactly twice in S, and

(ii) if $s_m = s_n = \mu$ for $n > m$, then $n - m = \mu$.

Skolem sequences can also be represented as collections of ordered pairs $\{(x_j, y_j) : 1 \leq j \leq \omega, y_j - x_j = j\}$ with $\bigcup_{j=1}^{\omega} \{x_j, y_j\} = \{1, 2, \ldots, 2\omega\}$. Skolem sequences of order ω exist if and only if $\omega = 0, 1 \bmod 4$. Skolem sequences of order ω are constructed by a method given in [37].

(i) $\omega = 1; (1, 1)$

(ii) $\omega = 4; (1, 1, 3, 4, 2, 3, 2, 4)$

(iii) $\omega = 5; (2, 4, 2, 3, 5, 4, 3, 1, 1, 5)$

(iv) $\omega = 4\alpha; \alpha \geq 2$

$$\begin{gathered}(2\alpha, 4\alpha - 1), (2\alpha + 1, 6\alpha)\\ (\alpha - 1, 3\alpha), (\alpha, \alpha + 1)\\ (4\alpha + \psi - 1, 8\alpha - \psi + 1) \quad \psi = 1, \ldots, 2\alpha\\ (\alpha + \psi + 1, 3\alpha - \psi) \quad \psi = 1, \ldots, \alpha - 2\\ (\psi, 4\alpha - \psi - 1) \quad \psi = 1, \ldots, \alpha - 2\end{gathered} \tag{1}$$

(v) $\omega = 4\alpha + 1; \alpha \geq 2$

$$\begin{gathered}(\alpha + 1, \alpha + 2), (2\alpha + 1, 6\alpha + 2), (2\alpha + 2, 4\alpha + 1)\\ (4\alpha + \psi + 1, \psi\alpha - \psi + 3), \quad \psi = 1, \ldots, 2\alpha\\ (\alpha + \psi + 2, 3\alpha - \psi + 1), \quad \psi = 1, \ldots, \alpha - 2\\ (\psi, 4\alpha - \psi + 1), \quad \psi = 1, \ldots, \alpha\end{gathered} \tag{2}$$

Example 6. We construct a Skolem sequence of order 8

$$S = (4, 1, 1, 5, 4, 7, 8, 3, 5, 6, 3, 2, 7, 2, 8, 6) \tag{3}$$

A Skolem sequence of order ω can be used to generate a Steiner Triple System (STS) of order $6\omega + 1$ using following construction:

(i) for each $s_i = s_j \in S$, form pairs (i, j).

(ii) transform each pair into triples $(\mu, i + \omega, j + \omega)$, where $s_i = s_j = \mu$.

(iii) transform each triple $(\mu, i + \omega, j + \omega)$ into base blocks $\{0, \mu, j + \omega\}$.

(iv) each base block in (iii) is developed by adding 1 under $Z_{6\omega+1}$ to generate an STS of order $(6\omega + 1)$.

Example 7. We construct an STS(25). First, construct a skolem sequence of order 4, $S = (1, 1, 4, 2, 3, 2, 4, 3)$. From step (i), we obtain the pairs $(1, 2), (4, 6), (5, 8), (3, 7)$. Based on step (ii), we then convert these pairs into triples $(1, 5, 6), (2, 8, 10), (3, 9, 12), (4, 7, 11)$. Using transformation in step (iii), we construct the sets $\{0, 1, 6\}, \{0, 2, 10\}, \{0, 3, 12\}, \{0, 4, 11\}$. We then add 1 to each of these sets mod 25 to obtain a STS of size $4 \times 25 = 100$.

From a STS of order $(6\omega + 1)$, a $(6\omega + 1, 3, 1)$-CDF can be obtained by letting $A_i = \{0, \mu, j + \omega\}$, for $1 \leq i \leq \omega$, where A_i's denote the base blocks of a $(6\omega + 1, 3, 1)$-CDF. A construction of $(6\omega + 1, 3, 1)$-BDDFs using a linear translation of $(6\omega + 1, 3, 1)$-CDFs based on Skolem Triple System can be found in [35].

Theorem 8 (see [35]). *There exists a block disjoint* $(24\omega + 1, 3, 1)$ *difference family for* $\omega \geq 1$.

Proof. Beginning with a $(24\omega + 1, 3, 1)$-CDF based on a Skolem Triple System of order 4ω that does not have disjoint blocks, the idea is to linearly translate the blocks such that no two blocks intersect. This construction requires that $\omega \geq 3$. The cases for smaller values of ω are treated separately.

$$\begin{gathered}a_1\colon (0, 1, 12\omega)\\ b_1\colon (0, 4\omega - 1, 9\omega - 1)\\ c_1\colon (0, 2\omega, 10\omega - 1)\\ d_1\colon (0, 4\omega, 10\omega)\\ e_1\colon (0, 2\omega - 2r - 1, 7\omega + r - 1), \quad 1 \leq r \leq \omega - 1\\ f_1\colon (0, 2\omega + 2r, 11\omega + r - 1), \quad 1 \leq r \leq \omega - 1\\ g_1\colon (0, 2r + 1, 10\omega + r), \quad 1 \leq r \leq \omega - 1\\ h_1\colon (0, 2r, 6\omega + r), \quad 1 \leq r \leq \omega - 1\end{gathered} \tag{4}$$

By linear translation of above cyclic difference family, we can obtain the following block disjoint difference family:

$$\begin{gathered}a_{11}\colon (7\omega - 1, 7\omega, 19\omega - 1), \quad \omega = 0 \bmod 2\\ a_{12}\colon (7\omega, 7\omega + 1, 19\omega), \quad \omega = 1 \bmod 2\\ b_{11}\colon (2\omega + 2, 6\omega + 1, 11\omega + 1)\\ c_{11}\colon (0, 2\omega, 10\omega - 1)\\ d_{11}\colon (6\omega, 10\omega, 16\omega)\\ e_{11}\colon (2r, 2\omega + 4r - 1, 7\omega + 3r - 1)\\ f_{11}\colon (2r + 1, 2\omega + 4r + 1, 11\omega + 3r)\\ g_{11}\colon (17\omega + 4r, 17\omega + 2r - 1, \omega + 3r)\\ h_{11}\colon (21\omega + r + 1 + s_\omega, 21\omega + 3r + 1 + s_\omega, 3\omega + 2r + s_\omega), \quad r \not\equiv 0 \bmod 3\\ h_{12}\colon (13\omega + r - l_r + 5, 13\omega + 3r - l_r + 5, 19\omega + 2r - l_r + 5) \quad r \equiv 0 \bmod 3 \text{ and } r \not\equiv \omega - 1\\ h_{13}\colon (10\omega + 13, 12\omega + 1, 17\omega + 2), \quad \omega \equiv 1 \bmod 3\end{gathered} \tag{5}$$

where $1 \leq r \leq \omega - 1, s_\omega = \omega \bmod 2$, and l_r is defined as

For $\omega \equiv 0 \bmod 3$: if $r \neq 3r' - l_{r'}$ for all $r' < r$ then $l_r = 0$; otherwise $l_r = 4$.

For $\omega \equiv 1 \bmod 3$: if $r \neq 3r' - l_{r'}$ for all $r' < r$ then $l_r = 0$; otherwise $l_r = 2$.

For $\omega \equiv 2 \bmod 3$: if $r \neq 3r' - l_{r'} + 2$ for all $r' < r$ then $l_r = 2$; otherwise $l_r = 4$.

Since by linear translation (and one flip) of cyclic difference family based on Skolem Triple Systems a block disjoint difference family is obtained, clearly, the new set of triples is also a difference family with disjoint blocks. The linear translation from cyclic difference family to block disjoint

Table 1: Linear translation from CDFs to BDDFs for $v = 1 \bmod 6$.

CDF	BDDF	Add	Comments
a_1	a_{11}	$7\omega - 1$	if $\omega \equiv 0 \bmod 2$
a_1	a_{12}	7ω	if $\omega \equiv 1 \bmod 2$
b_1	b_{11}	$2\omega + 2$	
c_1	c_{11}	0	
d_1	d_{11}	6t	
e_1	e_{11}	$2r$	for $1 \le r \le \omega - 1$
f_1	f_{11}	$2r + 1$	for $1 \le r \le \omega - 1$
g_1	g_{11}	$17\omega + 4r$	to $\{0, -(2r+1), -(10\omega + r)\}$ for $1 \le r \le \omega - 1$
h_1	h_{11}	$21\omega + r + s_\omega$	$1 \le r \le \omega - 1$ if $r \not\equiv 0 \bmod 3$
h_1	h_{12}	$13\omega + r - l_r + 5$	$1 \le r \le \omega - 2$ if $r \equiv 0 \bmod 3$
h_1	h_{13}	$10\omega + 3$	if $r \equiv 0 \bmod 3$

difference family is summarized in Table 1. In the following cases for small values of ω, $1 \le \omega \le 2$:

$v = 25$ ($\omega = 1$): (0,2,9), (6,10,16), (7,8,19), (12,15,20).

$v = 49$ ($\omega = 2$): (0,4,19), (2,7,16), (3,9,25), (6,13,23), (8,44,46), (12,20,32), (17,35,37), (21,22,45).

It is relatively easy to verify that the triples are all disjoint which complete the proof. □

3.2. Construction of (v, 3, 1)-BDDFs for v=3 mod 6. This subsection gives a construction of $(v, 3, 1)$-BDDFs for $v = 3 \bmod 6$. A class of $(v, 3, 1)$-CDFs based on Rosa Triple Systems is used to construct $(v, 3, 1)$-BDDFs for $v = 3 \bmod 6$. First, we construct $(v, 3, 1)$-CDFs based on Rosa Triple System, then by a linear translation of $(v, 3, 1)$-CDFs we obtain $(v, 3, 1)$-BDDFs for $v = 3 \bmod 6$.

Definition 9 (see [37]). A sequence $S = (s_1, \ldots, s_\omega, 0, s_{\omega+2}, \ldots, s_{2\omega+1})$ of $2\omega + 1$ elements taken from $\{1, 2, \ldots, \omega\}$ is said to be a Rosa sequence of order ω if all of the following hold:

(i) every $s_i \in \{1, \ldots, \omega\}$ appears exactly twice in S.

(ii) if $s_m = s_n = \mu$ for $n > m$, then $n - m = \mu$.

(iii) a hook or zero is inserted at position $\omega + 1$.

Rosa sequences can also be expressed as collections of ordered pairs $\{(x_i, y_i) : 1 \le i \le \omega, y_i - x_i = i\}$ with $\bigcup_{i=1}^{\omega} \{x_i, y_i\} = \{1, 2, \ldots, 2\omega\}$. Rosa sequences of order ω exist if and only if $\omega = 0, 3 \bmod 4$. A Rosa sequence of order ω can be constructed by a method given in [37].

(1) $\omega = 2; \{(1, 2), (4, 6)\}$

(2) $\omega = 5; \{(1, 5), (2, 7), (3, 4), (8, 10), (9, 12))\}$

(3) $\omega = 4\alpha; \alpha \ge 1$

$$\begin{gathered} (2\alpha - 1, 2\alpha), (3\alpha, 5\alpha + 1) \\ (3\alpha + 1, 7\alpha + 1), (6\alpha + 1, 8\alpha + 1) \\ (4\alpha + \psi + 1, 8\alpha - \psi + 1) \quad \psi = 1, \ldots, \alpha - 1 \\ (5\alpha + \psi + 1, 7\alpha - \psi + 1) \quad \psi = 1, \ldots, \alpha - 1 \\ (\alpha + \psi - 1, 3\alpha - \psi) \quad \psi = 1, \ldots, \alpha - 1 \\ (\psi, 4\alpha - \psi + 1) \quad \psi = 1, \ldots, \alpha - 1 \end{gathered} \tag{6}$$

(4) $\omega = 4\alpha - 1; \alpha \ge 2$

$$\begin{gathered} (6\alpha - 1, 2\alpha), (5\alpha, 7\alpha + 1) \\ (4\alpha + 1, 6\alpha), (7\alpha - 1, 7\alpha) \\ (5\alpha + \psi, 7\alpha - \psi - 1) \quad \psi = 1, \ldots, \alpha - 2 \\ (4\alpha + \psi + 1, 8\alpha - \psi) \quad \psi = 1, \ldots, \alpha - 2 \\ (\psi, 4\alpha - \psi) \quad \psi = 1, \ldots, \alpha - 2 \end{gathered} \tag{7}$$

Example 10. We construct a Rosa sequence of order 8

$$S = (3, 1, 1, 3, 6, 7, 5, 8, 0, 4, 6, 5, 7, 4, 2, 8, 2) \tag{8}$$

Rosa sequences of order ω can be used to generate Steiner Triple System of order $6\omega + 3$ using following construction [37]:

(i) for each $s_i = s_j \in S$, form pairs (i, j).

(ii) Transform each pair into triples $(\mu, i+\omega, j+\omega)$, where $s_i = s_j = \mu$.

(iii) Transform each triple $(\mu, i+\omega, j+\omega)$ into sets $\{0, \mu, j+\omega\}$.

(iv) each base block in (iii) is developed by adding 1 under $Z_{6\omega+3}$.

(v) Add triples of the form $\{0, 2\omega + 1, 4\omega + 2\}$.

(vi) Add 1 to this triple mod $6\omega + 3$ to generate the STS of order $6\omega + 3$.

It is important to note that, from step (i) to step (iv), the construction of STS of order $6\omega + 3$ is same as the construction of STS of order $6\omega + 1$. But, step (v) and step (vi) are additionally added in the construction of STS of order $6\omega + 3$. Since, the differences between elements of base blocks must exist in the difference set $\{1, 2, \ldots, 6\omega + 2\}$. Each base block of STS of order $6\omega + 3$ in step (iii) covers six differences of the difference set. Then, all the base blocks of STS of order $6\omega + 3$ cover 6ω differences of the difference set $\{1, 2, \ldots, 6\omega + 2\}$. So, there are two differences which are not covered by the base blocks in step (iii). To obtain the two missing differences, from step (v), a short block of the form $\{0, 2\omega + 1, 4\omega + 2\}$ is added. Finally, from step (vi), the short block $\{0, 2\omega + 1, 4\omega + 2\}$ is developed by adding 1 of order $v/3$ which gives the missing $v/3$ blocks of STS of order $6\omega + 3$.

Example 11. We construct an STS of order 27. First, construct a Rosa sequence of order 4, $S = (1, 1, 3, 4, 0, 3, 2, 4, 2)$. From step (i), we obtain the pairs $(1, 2), (7, 9), (3, 6), (4, 8)$. Based on step (ii), we convert these pairs into triples $(1, 5, 6), (2, 11, 13), (3, 7, 10), (4, 8, 12)$. Using transformation in step (iii), we construct the base blocks $\{0, 1, 6\}, \{0, 2, 13\}, \{0, 3, 10\}, \{0, 4, 12\}$. From step (iv), each base block obtained from step (iii) is developed by adding 1 under Z_{27}. If we develop all base blocks in (iii) under mod 27, we obtain 108 blocks. But, we know however that this is a BIBD and total number of blocks must be equal to $n = v(v-1)/k(k-1) = 27(27-1)/3(3-1) = 117$. Also, the differences between elements of four base blocks in step (iii) cover 24 differences of the difference set $\{1, 2, \ldots, 26\}$ and two differences, $\{9, 18\}$, are missing. To obtain the two missing differences, from step (v), a short block of the form $\{0, 9, 18\}$ is added. Finally, from step (vi), the short block $\{0, 9, 18\}$ is developed by adding 1 of order 9 which gives the missing 9 blocks of STS of order 27.

From a STS of order $(6\omega + 3)$, a $(6\omega + 3, 3, 1)$-CDF can be constructed by letting $A_i = \{0, \mu, j + \omega\}$, for $1 \le i \le \omega$, where A_i's are called the base blocks of a $(6\omega + 3, 3, 1)$-CDF. Theorem 12 gives the construction of $(6\omega + 3, 3, 1)$-BDDFs by linear translation of $(6\omega + 3, 3, 1)$-CDFs based on Rosa Triple System.

Theorem 12 (see [36]). *There exists a block disjoint* $(24\omega + 3, 3, 1)$ *difference family for* $\omega \ge 0$.

Beginning with a $(24\omega+3, 3, 1)$*-CDF based on a Rosa Triple System of order* 4ω *that does not have disjoint blocks, the idea is to linearly translate the blocks such that no two blocks intersect. A detailed construction of* $(v, 3, 1)$*-BDDFs based on Rosa Triple System can be found in [36].*

In next section, we construct two classes of binary QC-LDPC codes based on $(v, k, 1)$-BDDFs for $v = 1, 3 \bmod 6$.

4. BDDFs-Based Construction of QC-LDPC Codes

Consider a parity-check matrix $\mathbf{H}^{(1)}$ consisting of an $1 \times \omega$ array of $k \times k$ circulant matrices given as follows:

$$\mathbf{H}^{(1)} = [\mathbf{Q}_1, \mathbf{Q}_2, \ldots, \mathbf{Q}_\omega] \tag{9}$$

Based on the block disjoint difference families for $v = 1, 3 \bmod 6$ given in Sections 3.1 and 3.2, we construct a parity-check matrix $\mathbf{H}^{(1)}$ where each $\mathbf{Q}_i$, $1 \le i \le \omega$, represents a $k \times k$ circulant permutation matrix whose each row is obtained from the right cyclic shift of the row above it. The first row of $\mathbf{Q}_i$ is obtained from one of the ω k-element base blocks of the $(v, k, 1)$-BDDFs for $v = 1, 3 \bmod 6$. The null space of $\mathbf{H}^{(1)}$ gives a QC-LDPC code of rate $\omega - 1/\omega$ and a girth of at least 6.

To make the idea more clear, a detailed construction of parity-check matrices based on the $(v, k, 1)$-BDDFs is given in Example 13, as follows

Example 13. Consider a $(25, 3, 1)$-BDDF with base blocks $A_i = \{a_{i1}, a_{i2}, \ldots, a_{ik}\}$, $i = 1, \ldots, 4$, and $k = 3$ for Z_{25}. The base blocks for a $(6 \times 4 + 1, 3, 1)$-BDDF are

$$\begin{aligned} A_1 &= \{0, 2, 9\}, \\ A_2 &= \{6, 10, 16\}, \\ A_3 &= \{12, 15, 20\}, \\ A_4 &= \{7, 8, 19\}. \end{aligned} \tag{10}$$

Based on above construction, we can construct a matrix $\mathbf{B}$ using a $(25, 3, 1)$-BDDF for $v = 1 \bmod 6$:

$$\mathbf{B} = \begin{bmatrix} 0 & 2 & 9 & 6 & 10 & 16 & 12 & 15 & 20 & 7 & 8 & 19 \\ 9 & 0 & 2 & 16 & 6 & 10 & 20 & 12 & 15 & 19 & 7 & 8 \\ 2 & 9 & 0 & 10 & 16 & 6 & 15 & 20 & 12 & 8 & 19 & 7 \end{bmatrix} \tag{11}$$

Theorem 14. *The parity-check matrix* $\mathbf{H}^{(1)}$ *based on BDDFs for* $v = 1, 3 \bmod 6$ *given in (9) has no length-4 cycles.*

Proof. To prove this theorem, we have to prove that $\mathbf{Q}_i$'s, for $1 \le i \le \omega$, of $\mathbf{H}^{(1)}$ have no length-4 cycles.

Consider a submatrix W given as

$$W = \begin{pmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{pmatrix}. \tag{12}$$

where $\lambda_1, \lambda_2 \in \mathbf{Q}_i$ and $\mu_1, \mu_2 \in \mathbf{Q}_j$, $1 \le i, j \le \omega$. The submatrix W has cycles of length 4 if and only if $\lambda_1 - \lambda_2 = \mu_1 - \mu_2 \bmod v$. Due to the property of BDDFs, all the elements of $\mathbf{Q}_i$ and $\mathbf{Q}_j$ are distinct. So, both of the differences $\lambda_1 - \lambda_2$ *and* $\mu_1 - \mu_2$ satisfy the relation that $\lambda_1 - \lambda_2 \ne \mu_1 - \mu_2$. Therefore, the matrix $\mathbf{H}^{(1)}$ has no length-4 cycles and provides a girth of at least 6. □

4.1. A Class of Binary QC-LDPC Codes: Method I. In this subsection, we give a construction of binary QC-LDPC codes based on the BDDFs for $v = 1, 3 \bmod 6$. Let $GF(q)$ be a finite field. For each nonzero element δ^i in $GF(q)$, $0 \le i < q - 1$, form a $(q-1)$-tuple over $GF(2)$, $\mathbf{u}_b(\delta^i) = (u_0, u_1, \ldots, u_{q-2})$, where all the components of $\mathbf{u}_b$ are equal to zero except the i*th* component $u_i = 1$. Subscript "b" stands for binary. This

$(q-1)$-tuple over $GF(2)$ is referred to as the binary location-vector of δ^i. The binary location-vector of additive identity of $GF(q)$ is an all-zero $(q-1)$-tuple, $\mathbf{u}_b(0) = (0, 0, 0, \ldots, 0)$.

Let α be an element of $GF(q)$. The right cyclic-shift of binary location vector $\mathbf{u}_b(\alpha)$ of field element α gives the binary location vector $\mathbf{u}_b(\alpha\delta)$ of field element $\alpha\delta$. If δ is a primitive element of $GF(q)$, then the $(q-1)$-tuples of $\alpha, \delta\alpha, \delta^2\alpha, \ldots, \delta^{q-2}\alpha$, give a $(q-1) \times (q-1)$ circular permutation matrix $\mathbf{W}_b(\alpha)$ over $GF(2)$. The matrix $\mathbf{W}_b(\alpha)$ is called a $(q-1)$-fold binary dispersion of α over $GF(2)$. If $\alpha = 0$, then the $(q-1)$-fold binary dispersion of 0-element $\mathbf{W}_b(0)$ is a $(q-1) \times (q-1)$ all-zero matrix over $GF(2)$.

Next, replacing each element of $\mathbf{H}^{(1)}$ given in (9) by its $(q-1)$-fold binary matrix dispersion $\mathbf{W_b}$ over $GF(2)$. We obtain an $k \times k\omega$ array $\mathbf{H}_b^{(1)}$ over $GF(2)$:

$$\mathbf{H}_b^{(1)} = \begin{bmatrix} \mathbf{W}_{0,0} & \mathbf{W}_{0,1} & \cdots & \mathbf{W}_{0,k\omega-1} \\ \mathbf{W}_{1,0} & \mathbf{W}_{1,1} & \cdots & \mathbf{W}_{1,k\omega-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{W}_{k-1,0} & \mathbf{W}_{k-1,1} & \cdots & \mathbf{W}_{k-1,k\omega-1} \end{bmatrix} \tag{13}$$

where $\mathbf{W}_{i,j}$ is an $(q-1) \times (q-1)$ circular permutation matrix over $GF(2)$, for $0 \le i < k$ and $0 \le j < k\omega$. Array $\mathbf{H}_b^{(1)}$ gives an $k(q-1) \times k\omega(q-1)$ matrix over $GF(2)$. Since the matrix $\mathbf{H}_b^{(1)}$ satisfies the RC-constraint, so the null space of $\mathbf{H}_b^{(1)}$ gives an LDPC code whose Tanner graph has a girth of at least 6.

For any pair of integers w_c and w_r, for $1 \le w_c \le k$ and $1 \le w_r \le k\omega$. Let $\mathbf{H}_b^{(1)}(w_c, w_r)$ be a $w_c \times w_r$ subarray of $\mathbf{H}_b^{(1)}$ and give a $w_c(q-1) \times w_r(q-1)$ matrix over $GF(2)$. The null space of $\mathbf{H}_b^{(1)}(w_c, w_r)$ over $GF(2)$ gives a binary QC-LDPC code $C_{qc}^{(1)}$ of length $w_r(q-1)$ with rate at least $(w_r - w_c)/w_r$ and minimum distance lower bounded by w_c+1. Since $\mathbf{H}_b^{(1)}(w_c, w_r)$ satisfies the RC-constraint, the Tanner graph of $C_{qc}^{(1)}$ has a girth of at least 6. For different choices of w_c and w_r, the above construction method gives a class binary QC-LDPC codes for various lengths and rates.

4.2. A Class of Binary QC-LDPC Codes: Method II. In this subsection, we use the concept of incidence matrices to construct QC-LDPC codes based on the $(v, 3, 1)$-BDDFs. Let $X = Z_v$ be a set of v varieties or elements. A design (X, B) with n k-subsets of X, $B_1, B_2, \ldots, B_n$, called blocks, is known as (v, n, r, k, λ)-BIBD if the following properties hold: (1) each element appears in exactly r blocks; (2) each pair of elements appears in exactly λ blocks; and (3) the block size k is small compared to the cardinality of X. A (v, n, r, k, λ)-BIBD can also be described by a $v \times n$ matrix $\mathbf{M} = (m_{i,j})$ over $GF(2)$ defined by the following rule:

$$m_{i,j} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j. \end{cases} \tag{14}$$

where matrix $\mathbf{M}$ is called the incidence matrix. The incidence matrix of a (v, n, r, k, λ)-BIBD satisfies the following properties: (1) each column of $\mathbf{M}$ contains exactly k 1's; (2) each row of $\mathbf{M}$ contains exactly r 1's; and (3) two distinct rows of $\mathbf{M}$ can agree at most λ positions.

Example 15. Let (X, B) be the following $(7, 7, 3, 3, 1)$-BIBD:

$$\begin{aligned} X &= \{1, 2, 3, 4, 5, 6, 7\}, \\ \text{and } B &= \{124, 235, 346, 457, 561, 672, 713\}. \end{aligned} \tag{15}$$

The incidence matrix of this $(7, 7, 3, 3, 1)$-BIBD is given as follows:

$$\mathbf{M} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{16}$$

It is important to note that each row of $\mathbf{M}$ is a right cyclic shift of the previous row and the right cyclic shift of last row returns the first row. Also, each column of $\mathbf{M}$ is a downward cyclic shift of a column on its left. Therefore, $\mathbf{M}$ is a 7×7 circulant permutation matrix.

Consequently, for a (v, k, λ)-BDDF with $\lambda = 1$, the incidence matrix $\mathbf{M}$ satisfies all the required properties of a parity-check matrix. Therefore, the null space of $\mathbf{M}$ gives a (w_c, w_r)-LDPC code of length n. Also, the incidence matrix $\mathbf{M}$ satisfies the *RC*-constraint with $\lambda = 1$. So, the Tanner graph of $\mathbf{M}$ has a girth of at least 6.

Based on $(v, k, 1)$-BDDFs for $v = 1, 3 \bmod 6$, consider a parity-check matrix $\mathbf{H}^{(2)}$ consisting of an $1 \times \omega$ array of circulant matrices given as follows:

$$\mathbf{H}^{(2)} = [\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_\omega] \tag{17}$$

where each $\mathbf{M}_i$, $1 \le i \le \omega$, represents a $v \times n$ incidence matrix over $GF(2)$. Clearly, the matrix $\mathbf{H}^{(2)}$ satisfies all the required properties of a parity-check matrix. The matrix $\mathbf{H}^{(2)}$ is a $v \times \omega n$ matrix over $GF(2)$ with row and column weights 3ω and 3, respectively. The null space of $\mathbf{H}^{(2)}$ gives a binary regular QC-LDPC with minimum distance at least 4, rate lower bounded by $(\omega - 1)/\omega$, and a girth of at least 6.

5. Numerical Results

In this section, the error correction performance of two proposed classes of binary QC-LDPC codes, given in the Sections 4.1 and 4.2, is compared with randomly constructed LDPC codes and QC-LDPC codes obtained from design theoretic techniques. Simulation results are obtained by *BP* iterative decoding with maximum number of iterations equal to 50. Also, Binary-phase-shift-keying(*BPSK*) transmission is assumed over an *AWGN* channel.

Firstly, suppose we have a $(73, 3, 1)$-BDDF for $v = 1 \bmod 6$ and $GF(73)$ is the code construction field. Choosing

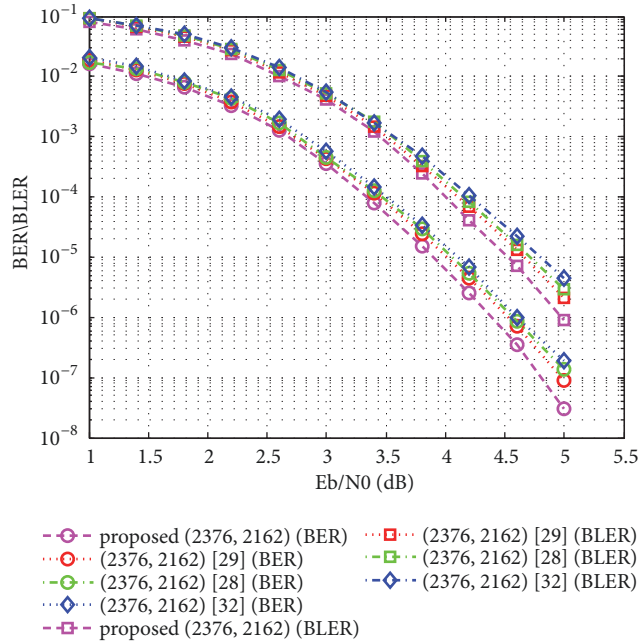

FIGURE 1: Error-correcting performance of proposed (2376, 2162) QC-LDPC code, a (2376, 2162) QC-LDPC code based on cyclic difference families [29], a (2376, 2162) QC-LDPC code obtained from cyclic difference families [28], and a (2376, 2162) QC-LDPC code constructed based on the subsets with distinct differences between the elements [32].

$w_c = 3$ and $w_r = 33$, we construct a 3×33 subarray of $\mathbf{H}_b^{(1)}$ of 72×72 circular permutation matrices over $GF(2)$. Subarray $\mathbf{H}_b^{(1)}(3, 33)$ is a 216×2376 matrix with row-weight 33 and column-weight 3. The null space of $\mathbf{H}_b^{(1)}(3, 33)$ gives a (2376, 2162) binary QC-LDPC code of rate 0.9110. Assuming *BPSK* transmission over *AWGN* channel, the bit-error rate (*BER*) and block-error rate (*BLER*) performance of proposed code decoded with Sum-product algorithm (*SPA*) are shown in Figure 1. Also shown in Figure 1 are the error correcting performances of (2376, 2162) QC-LDPC codes constructed from design theoretic techniques in literature [28, 29] and a (2376, 2162) QC-LDPC code constructed based on the subsets with distinct differences between the elements [32]. Based on the numerical results, the proposed QC-LDPC codes perform almost the same or better than their competitors in the waterfall region but outperform in the higher SNR region.

Secondly, suppose we have a $(81, 3, 1)$-BDDF for $\nu = 3 \bmod 6$ and $GF(81)$ is the code construction field. Choosing $w_c = 3$ and $w_r = 18$, we construct a 3×18 subarray of $\mathbf{H}_b^{(1)}$ of 80×80 circular permutation matrices over $GF(2)$. Subarray $\mathbf{H}_b^{(1)}(3, 18)$ is a 240×1440 matrix with row-weight equal to 18, column-weight 3. The null space of $\mathbf{H}_b^{(1)}(3, 18)$ gives a (1440, 1202) binary QC-LDPC code of rate 0.8347. The *BER* and *BLER* performance of this code decoded with *SPA* is shown in Figure 2. Also shown in Figure 2 are the error correcting performances of a (1440, 1202) PEG-LDPC code [8], a (1440, 1202) QC-LDPC code obtained from cyclic difference families [28], and a (1440, 1202) QC-LDPC code constructed from t-designs [31]. Based on the simulation results, the proposed QC-LDPC codes perform as well as their counterparts in the waterfall region but outperform in the higher SNR region.

Finally, suppose we have a $(133, 3, 1)$-BDDF for $\nu = 1 \bmod 6$. For $\omega = 20$, we have the following parameters: $\nu = 133$, $n = 2660$, $w_c = 3$, $w_r = 60$, and $\lambda = 1$. Based on this design, the parity-check matrix $\mathbf{H}^{(2)}$ consists of an array of 20 133×133 circulant matrices over $GF(2)$. $\mathbf{H}^{(2)}$ is a 133×2660 matrix over $GF(2)$ whose null space gives a (2660, 2532) binary regular QC-LDPC code with rate 0.9518 and a girth of at least 6. The *BER* and *BLER* performance of this code decoded with *SPA* is shown in Figure 3. Also shown in Figure 3 are the error correcting performances of a (2660, 2532) PEG-LDPC code [8], and a (2660, 2532) QC-LDPC code constructed based on the subsets with distinct differences between the elements [32] and a (2660, 2532) QC-LDPC code obtained from cyclic difference families [28]. Based on the simulation results, the proposed QC-LDPC codes perform as well as their counterparts in the waterfall region but outperform in the higher SNR region.

6. Conclusion

In this correspondence, two classes of binary QC-LDPC codes have been constructed based on a special type of combinatorial designs known as block disjoint difference families (BDDFs). Firstly, binary QC-LDPC codes are constructed using binary matrix dispersion of finite field elements based on BDDFs for $\nu = 1, 3 \bmod 6$. Secondly, binary QC-LDPC are constructed based on the incidence matrices obtained

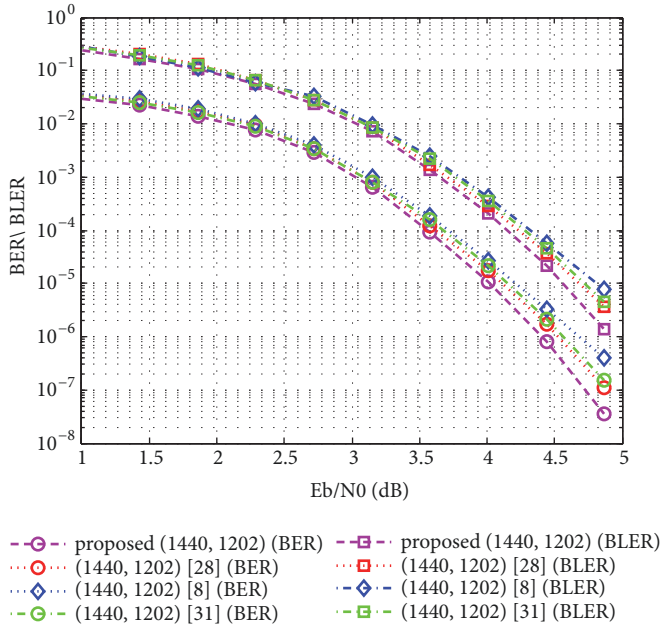

Figure 2: Error-correcting performance of proposed (1440, 1202) QC-LDPC code, a (1440, 1202) PEG-LDPC code [8], a (1440, 1202) QC-LDPC code constructed from t-designs [31], and a (1440, 1202) QC-LDPC code obtained from cyclic difference families [28].

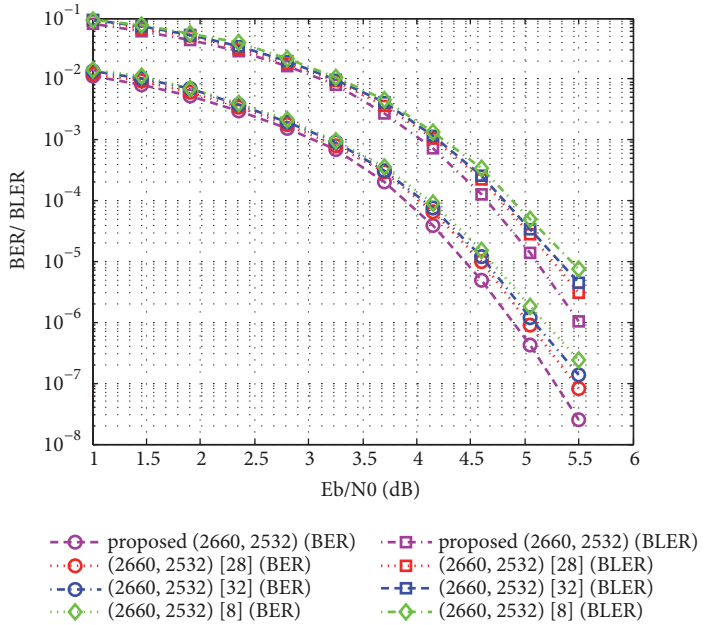

Figure 3: Error-correcting performance of proposed (2660, 2532) QC-LDPC code, a (2660, 2532) PEG-LDPC code [8], a (2660, 2532) QC-LDPC code constructed constructed based on the subsets with distinct differences between the elements [32], and a (2660, 2532) QC-LDPC code obtained from cyclic difference families [28].

from $(v, 3, 1)$-BDDFs for $v = 1, 3 \bmod 6$. The proposed QC-LDPC codes have parity-check matrices with column-weight three and their Tanner graphs provide a girth of at least 6. Also, the proposed QC-LDPC codes provide an excellent error performance with iterative decoding over an *AWGN* channel. Based on the simulation results, the performance analysis shows that the proposed QC-LDPC codes of short and moderate length perform as well as their competitors in lower SNR region but outperform in the higher SNR region. Also, the codes constructed are quasicyclic in nature, so the encoding can be done with simple shift-register circuits with linear complexity.

Data Availability

No data were used to support this study.

Disclosure

The current address of Muhammad Asif, Wuyang Zhou, Muhammad Ajmal, and Nauman Ali Khan is No. 96, JinZhai Road Baohe District, Hefei, Anhui, 230026, PR China.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication this work.

Authors' Contributions

Muhammad Asif, Wuyang Zhou, Muhammad Ajmal, Zain ul Abiden Akhtar, and Nauman Ali Khan conceived and designed this research work; Muhammad Asif and Wuyang Zhou participated in construction and performance analysis of this work. Muhammad Ajmal and Zain ul Abiden Akhtar participated in numerical analysis of this work; Muhammad Asif wrote the paper and Nauman Ali Khan technically reviewed the paper.

Acknowledgments

This work was partially supported by Natural Science Foundation of China under Grant number: 61461136002, Key Program of National Natural Science Foundation of China under Grant number: 61631018, and Fundamental Research Funds for the Central Universities and Huawei Innovation Research Program. Author Muhammad Asif acknowledges the support of the Chinese Academy of Sciences (CAS) and TWAS for his PhD studies at the University of Science and Technology, China, as a 2016 CAS-TWAS President's Fellowship Awardee (CAS-TWAS No. 2016-48).

References

[1] R. G. Gallager, "Low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 8, pp. 21–28, 1962.

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

[3] S. Wang, Q. Huang, and Z. Wang, "Symbol flipping decoding algorithms based on prediction for non-binary LDPC codes," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 1913–1924, 2017.

[4] Q. Huang, L. Song, and Z. Wang, "Set Message-Passing Decoding Algorithms for Regular Non-Binary LDPC Codes," *IEEE Transactions on Communications*, vol. 65, pp. 5110–5122, 2017.

[5] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2711–2736, 2001.

[6] L. Chen, J. Xu, I. Djurdjevic, and S. Lin, "Near-Shannon-limit quasi-cyclic low-density parity-check codes," *IEEE Transactions on Communications*, vol. 52, no. 7, pp. 1038–1042, 2004.

[7] W. Ryan and S. Lin, *Channel Codes: Classical and Modern*, Cambridge University Press, Cambridge, 2009.

[8] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, 2005.

[9] D. Divsalar, S. Dolinar, and C. Jones, "Construction of Protograph LDPC Codes with Linear Minimum Distance," in *Proceedings of the 2006 IEEE International Symposium on Information Theory*, pp. 664–668, Seattle, WA, USA, July 2006.

[10] D. Divsalar, S. Dolinar, C. R. Jones, and K. Andrews, "Capacity-approaching protograph codes," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 6, pp. 876–888, 2009.

[11] S. Abu-Surra, D. Divsalar, and W. E. Ryan, "Enumerators for protograph-based ensembles of LDPC and generalized LDPC codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 858–886, 2011.

[12] I. Djurdjevic, J. Xu, K. Abdel-Ghaffar, and S. Lin, "A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols," *IEEE Communications Letters*, vol. 7, no. 7, pp. 317–319, 2003.

[13] Y. Y. Tai, L. Lan, L. Zeng, S. Lin, and K. A. S. Abdel-Ghaffar, "Algebraic construction of quasi-cyclic LDPC codes for the AWGN and erasure channels," *IEEE Transactions on Communications*, vol. 54, no. 10, pp. 1765–1774, 2006.

[14] 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 Transactions on Information Theory*, vol. 53, no. 7, pp. 2429–2458, 2007.

[15] S. Song, B. Zhou, S. Lin, and K. Abdel-Ghaffar, "A unified approach to the construction of binary and nonbinary quasi-cyclic LDPC codes based on finite fields," *IEEE Transactions on Communications*, vol. 57, no. 1, pp. 84–93, 2009.

[16] J. Y. Kang, Q. Huang, L. Zhang, B. Zhou, and S. Lin, "Quasi-cyclic LDPC codes: an algebraic construction," *IEEE Transactions on Communications*, vol. 58, no. 5, pp. 1383–1396, 2010.

[17] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. F. Blake, "Quasi-cyclic LDPC Codes: An algebraic construction, rank analysis, and codes on latin squares," *IEEE Transactions on Communications*, vol. 58, no. 11, pp. 3126–3139, 2010.

[18] L. Zhang, S. Lin, K. Abdel-Ghaffar, Z. Ding, and B. Zhou, "Quasi-cyclic LDPC codes on cyclic subgroups of finite fields," *IEEE Transactions on Communications*, vol. 59, no. 9, pp. 2330–2336, 2011.

[19] Q. Diao, Q. Huang, S. Lin, and K. Abdel-Ghaffar, "A matrix-theoretic approach for analyzing quasi-cyclic low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 4030–4048, 2012.

[20] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Algebraic quasi-cyclic ldpc codes: Construction, low error-floor, large girth and a reduced-complexity decoding scheme," *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2626–2637, 2014.

[21] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: Geometry decomposition and masking," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 121–134, 2007.

[22] Q. Diao, Y. Y. Tai, S. Lin, and K. Abdel-Ghaffar, "LDPC codes on partial geometries: construction, trapping set structure, and puncturing," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 59, no. 12, pp. 7898–7914, 2013.

[23] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 6, pp. 1156–1176, 2004.

[24] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, "Construction of low-density parity-check codes based on balanced incomplete block designs," *IEEE Transactions on Information Theory*, vol. 50, no. 6, pp. 1257–1268, 2004.

[25] S. J. Johnson and S. R. Weller, "Regular low-density parity-check codes from combinatorial designs," in *Proceedings of the 2001 IEEE Information Theory Workshop, ITW 2001*, pp. 90–92, Australia, September 2001.

[26] S. J. Johnson and S. R. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Transactions on Communications*, vol. 51, no. 9, pp. 1413–1419, 2003.

[27] S. J. Johnson and S. R. Weller, "A family of irregular LDPC codes with low encoding complexity," *IEEE Communications Letters*, vol. 7, no. 2, pp. 79–81, 2003.

[28] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Construction of high-rate regular quasi-cyclic LDPC codes based on cyclic difference families," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3108–3113, 2013.

[29] M. Fujisawa and S. Sakata, "A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E90-A, no. 5, pp. 1055–1061, 2007.

[30] S. M. Ibraheem, M. M. A. Elrazzak, S. M. S. Eldin, W. Saad, and A. E. Aboelazm, "A class of structured quasi-cyclic LDPC codes based on planar difference families," in *Proceedings of the 2013 International Conference on Advanced Technologies for Communications, ATC 2013*, pp. 614–619, Viet Nam, October 2013.

[31] H. Falsafain and M. Esmaeili, "Construction of structured regular LDPC codes: a design-theoretic approach," *IEEE Transactions on Communications*, vol. 61, no. 5, pp. 1640–1647, 2013.

[32] S. Vafi and N. Rezvani Majid, "A New Scheme of High Performance Quasi-Cyclic LDPC Codes with Girth 6," *IEEE Communications Letters*, vol. 19, no. 10, pp. 1666–1669, 2015.

[33] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1788–1793, 2004.

[34] J. L. Fan, "Array codes as low-density parity-check codes," in *Proceedings of the 2nd International Symposium on Turbo Codes*, pp. 543–546, 2000.

[35] J. H. Dinitz and P. Rodney, "Disjoint difference families with block size 3," *Utilitas Mathematica*, vol. 52, pp. 153–160, 1997.

[36] J. H. Dinitz and N. Shalaby, "Block disjoint difference families for Steiner triple systems: v≡3mod6," *Journal of Statistical Planning and Inference*, vol. 106, no. 1-2, pp. 77–86, 2002.

[37] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC, 1996.

[38] R. Peltesohn, "Eine Losung der beiden Heffterschen Differenzenprobleme," *Compositio Mathematica*, vol. 6, pp. 251–257, 1939.

[39] G. Ge, Y. Miao, and X. Sun, "Perfect difference families, perfect difference matrices, and related combinatorial structures," *Journal of Combinatorial Designs*, vol. 18, no. 6, pp. 415–449, 2010.

[40] R. Julian, R. Abel, S. Costa, and N. J. Finizio, "Directed-ordered whist tournaments and (v,5,1) difference families: Existence results and some new classes of Z -cyclic solutions," *Discrete Applied Mathematics*, vol. 143, no. 1-3, pp. 43–53, 2004.