This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2019.2940977, IEEE Communications Letters

Design of High-Rate LDPC Codes Based on Matroid Theory

Guangfu Wu, Yijie Lv, Jiguang He

***Abstract*—In this letter, sufficient conditions for the determination of the girth are studied from the perspective of matroid theory. The girth of a Tanner graph is at least $2(t_1 + 2)$ if t_1 specific conditions are simultaneously met. A novel method of constructing high-rate low-density parity-check (LDPC) codes is proposed based on the matroid theory. The parity-check matrices of the constructed LDPC codes are in the form of $\mathbf{H} = [\mathbf{I}|\mathbf{H}_2]$ with $\mathbf{H}_2$ constructed under the conditions of a given girth and a fixed column weight (e.g., $W_c = 4$ or $W_c = 6$). Simulation results verify that the proposed LDPC codes outperform those in the literature over additive white Gaussian noise channels in terms of bit error rate performance.**

***Index Terms*—Girth condition, high rate, matroid theory, parity-check matrix, Bit error rate**

I. Introduction

In the pioneering paper *A Mathematical Theory of Communication*, Shannon proved the existence of a channel code which ensures reliable communications provided that the information rate for the given code does not exceed the capacity of the channel. Several decades since Shannon's paper was published, great efforts were devoted to finding the practical capacity-achieving error correction codes. Until the 1990s, the invention of turbo codes and rediscovery of low-density parity-check (LDPC) codes make approaching Shannon's theoretical performance limits practically feasible.

LDPC codes were initially invented by Gallager in 1960. Tanner further introduced a graphical representation for the LDPC codes, well-known as Tanner graph. LDPC codes belong to the class of linear block codes with implementable decoders, which bring near-capacity performance on a variety of channels, e.g., binary-input additive white Gaussian noise (AWGN) channels in [1]. In [2], a novel family of protograph LDPC codes has been proposed, which can achieve not only linear complexity encoding and high-speed decoding by means of a quasi-cyclic (QC) structure but also near-interruption performance over different block fading channels. LDPC codes was also used to design bit-interleaved coded modulation (BICM) with iterative demapping and decoding functions, which bring improved throughput under the constraints of limited bandwidth [3].

In the literature, there exist two major construction methods for LDPC codes: 1) random construction approach, e.g., random or semi-random methods in [4], 2) algebraic construction approach, e.g., algebraic construction of geometric LDPC codes and quasi-cyclic LDPC codes in [5]–[9]. However, when constructing short- or medium-length high-rate LDPC codes, the two aforementioned construction methods can not bring satisfactory performance in terms of bit error rate (BER). The research on short-length error correction codes primarily concentrates on the algebraic codes, such as Golay codes and quadratic residue (QR) codes. Their minimum Hamming distances can be equivalent to the theoretical maximum, but they are not tailored for low- and medium-complexity decoding algorithms, e.g., iterative message passing algorithm and its variants. These motivates the study of construction of short- or medium-length high-rate LDPC codes by leveraging other novel construction methods in this letter.

Matroid theory was first proposed by Whitney, and the relationship between matroids and graphs was built by. Edmonds and Fulkerson realized that matroids play an critical role in the transversal theory. Greene derived the MacWilliams identities from matroid theory, which are now widely used in the fields of combinatorial optimization, network theory [10], and coding theory [11]. In the letter, we study the construction of LDPC codes with a given girth, which is well interpreted by the matriod theory.

II. Preliminaries

A. Fundamentals of LDPC Codes

LDPC codes fall into the category of linear block codes with their parity-check matrices being sparse. The parity-check matrix of a LDPC code (n, k) is defined as $\mathbf{H} \in \mathbb{B}^{(n-k)\times n}$ with $\mathbb{B} = \{0, 1\}$. A regular LDPC code has fixed column weight W_c and row weight W_r, where $W_r = W_c \cdot (n/(n-k))$, $W_c \ll n - k$, and $W_r \ll n$. The code rate R for a regular LDPC code is

$$R = \frac{k}{n} = 1 - \frac{W_c}{W_r}. \quad (1)$$

Unlike regular LDPC codes, an irregular LDPC code has more than one column weights and row weights. Usually, the irregular LDPC code is characterized by the degree distribution (i.e., distribution of column weights and row weights) [12].

This work was supported by the National Natural Science Foundation of China (Grant No. 11461031), Science and Technology key Project of the Education Department of Jiangxi Province (Grant GJJ170492), Natural Science Foundation of Jiangxi Provincial (Grant 20181BBE58018), Science and Technology Project of the Education Department of Jiangxi Province (GJJ180442). The corresponding author is G. Wu.

G. Wu and Y. Lv are with the Dept. of Information Engineering, Jiangxi University of Science and Technology, Jiangxi, China (e-mail: wuguangfu@126.com, lvsejianke@126.com).

J. He is with Centre for Wireless Communications, University of Oulu, FI-90014, Finland (e-mail: jiguang.he@oulu.fi).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2019.2940977, IEEE Communications Letters

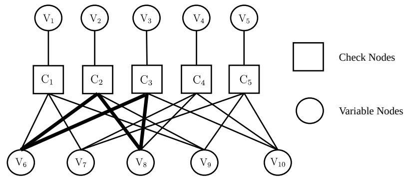

Fig. 1: Tanner graphical representation of $\mathbf{H}$.

B. Graphical Representation of LDPC Codes

The parity-check matrix of LDPC codes can be represented by a bipartite Tanner graph, composed of two kinds of nodes, i.e., variable nodes (VNs) and the check nodes (CNs), denoted by V_j and C_i, respectively, for $i = 1, \cdots, n-k$, and $j = 1, \cdots, n$. If $h_{i,j} = 1$, the i-th check node (C_i) is connected to the j-th variable node (V_j) in the associated Tanner graph. For the purpose of better illustration, an example of $\mathbf{H}$ with $n = 8$ and $k = 3$ is provided as

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad (2)$$

with its corresponding Tanner graph shown in Fig. 1.

C. Cycles in Tanner Graphs

A cycle in a Tanner graph refers to a trajectory that begins with one of the vertices, traverses through several vertices, and finally returns to the original vertice [13]. For instance, the four tandem connected thick edges in Fig. 1 form a cycle of length 4. The girth is defined as the length of the shortest cycle in the Tanner graph (e.g., the girth is 4 for Fig. 1), which has a great impact on the performance of iterative messaging passing decoding. Therefore, in the construction process of a parity-check matrix, great efforts should be put on maximizing the girth. In this letter, we construct short-length high-rate LDPC codes with enhanced performance through the matroid theory.

III. Novel Construction of High-Rate LDPC Codes

In principle, short cycles should be avoided in the process of constructing the parity-check matrix. In the literature, the theorems on the girth are proposed from the perspective of matrix or graph theory. In this letter, matrix and graph theory are transformed into set problem via matroid theory, and the theorems on determining the girth are provided from the perspective of matroid theory.

A. Definition and Theorems

Each column of the parity-check matrix can be represented by a set. The support of non-zero elements in vector $\mathbf{h}_i$ (i.e., the i-th column of $\mathbf{H}$) is represented by the set $\mathbb{L}_i$, for $i = 1, \cdots, n$. For example, the parity-check matrix in (2) can be represented by the following sets: $\mathbb{L}_1 = \{1\}$, $\mathbb{L}_2 = \{2\}$, $\mathbb{L}_3 = \{3\}$, $\mathbb{L}_4 = \{4\}$, $\mathbb{L}_5 = \{5\}$, $\mathbb{L}_6 = \{1,2,3\}$, $\mathbb{L}_7 = \{1,4,5\}$, $\mathbb{L}_8 = \{2,3,4\}$, $\mathbb{L}_9 = \{1,2,5\}$, $\mathbb{L}_{10} = \{3,4,5\}$. Equivalently, the corresponding parity-check matrix can be constructed according to $\mathbb{L}_i$, for $i = 1, \cdots, n$.

Definition 1. A matroid M is an ordered pair of $(\mathbb{E}, \mathcal{I})$, where $\mathbb{E}$ is a finite set, and $\mathcal{I}$ is a collection of subsets of $\mathbb{E}$. They satisfy the following three conditions [14]:

1) $\emptyset \in \mathcal{I}$.
2) If $\mathbb{E}_1 \in \mathcal{I}$, and $\mathbb{E}_2 \subseteq \mathbb{E}_1 \subseteq \mathbb{E}$, then $\mathbb{E}_2 \in \mathcal{I}$.
3) If $\mathbb{E}_1 \in \mathcal{I}$, $\mathbb{E}_2 \in \mathcal{I}$ and $|\mathbb{E}_1| < |\mathbb{E}_2|$, then there exists $e \in \mathbb{E}_2 \setminus \mathbb{E}_1$ such that $\mathbb{E}_1 \cup \{e\} \in \mathcal{I}$.

Following the matroid theory, we first construct a matroid with all sets whose cardinalities are less than or equal to W_c, and then select parts of the sets which satisfy the pre-determined conditions to form a parity-check matrix. The matroid theory is leveraged for analyzing the relationship among sets, which represent the columns of the corresponding parity-check matrix.

A series of theorems on the girth of the LDPC code, listed in the sequel, are obtained by transforming the relationship among columns into that among sets based on the matroid theory [6], [15].

Theorem 1. *If $\exists$ $|\mathbb{L}_i \cap \mathbb{L}_j| \geq 2$ for $\forall i, j$, where $i \neq j$, then the girth of the LDPC code is 4.*

Proof. It can be easily seen from the relationship between the parity-check matrix and its corresponding Tanner graph in the previous example. If $|\mathbb{L}_i \cap \mathbb{L}_j| = 2$, e.g., $|\mathbb{L}_6 \cap \mathbb{L}_8| = 2$ for $\mathbf{H}$ in (2), a length-4 cycle exists. □

Theorem 2. *If $\mathbb{L}_i$, for $i = 1, \cdots, n$, satisfies the following two conditions, then the girth of the LDPC code is greater than or equal to 8.*

Condition 1: $|\mathbb{L}_i \cap \mathbb{L}_j| < 2, i \neq j, \forall i, j \in \{1, 2, \cdots, n\}$.
Condition 2: $|(\mathbb{L}_i \cap \mathbb{L}_j) \cup (\mathbb{L}_i \cap \mathbb{L}_k) \cup (\mathbb{L}_j \cap \mathbb{L}_k)| < 3, i \neq j \neq k, \forall i, j, k \in \{1, 2, \cdots, n\}$.

Proof. If there exists a Tanner graph with girth 6, there exist 3 sets and the unions of intersections of every 2 sets out of the 3 sets must have no less than 3 elements, e.g., $|(\mathbb{L}_6 \cap \mathbb{L}_8) \cup (\mathbb{L}_6 \cap \mathbb{L}_{10}) \cup (\mathbb{L}_8 \cap \mathbb{L}_{10})| = 3$ for $\mathbf{H}$ in (2). Therefore, the girth of the LDPC code is at least 8. □

Theorem 3. *Let $\mathbb{L}(n) = \{1, 2, \cdots, n\}$ denote a set having n elements, and $\mathbb{T}(t)$ represent a subset of $\mathbb{L}(n)$ with t elements ($t \leq n$). If $\mathbb{L}_i$, for $i = 1, \cdots, n$, satisfies the following t_1 conditions, the girth of the Tanner graph is at least $2(t_1 + 2)$.*

Conditions: $| \cup_{\forall i,j \in \mathbb{T}(t) \subseteq \mathbb{L}(n)} (\mathbb{L}_i \cap \mathbb{L}_j)| < t$, $t = 2, 3, \cdots, t_1 + 1$.

Proof. The proof can be done by the method *proof by contradiction*. If there exists a length-4 cycle, $\exists i, j \in \mathbb{T}(2) \subseteq \mathbb{L}(n), |\mathbb{L}_i \cap \mathbb{L}_j| = 2$, which contradicts with the first condition when $t = 2$. If there exists a length-6 cycle, $\exists i, j, k \in \mathbb{T}(3) \subseteq \mathbb{L}(n), |(\mathbb{L}_i \cap \mathbb{L}_j) \cup (\mathbb{L}_i \cap \mathbb{L}_k) \cup (\mathbb{L}_j \cap \mathbb{L}_k)| = 3$, which contradicts with the second condition when $t = 3$. By analogy, if there exists a length-$2(t_1 + 1)$ cycle, $\exists i_1, \ldots, i_{t_1+1} \in \mathbb{T}(t_1 + 1) \subseteq \mathbb{L}(n), |(\mathbb{L}_{i_1} \cap \mathbb{L}_{i_2}) \cup (\mathbb{L}_{i_1} \cap \mathbb{L}_{i_3}) \cup \cdots \cup (\mathbb{L}_{i_{t_1}} \cap \mathbb{L}_{i_{t_1+1}})| = t_1 + 1$, which contradicts with the last condition when $t = t_1 + 1$. In other words, if all the t_1 conditions in Theorem 3 are simultaneously satisfied, there does not exist any cycles with length less than or equal to $2(t_1 + 1)$, i.e., the girth of the Tanner graph is at least $2(t_1 + 2)$. □

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2019.2940977, IEEE Communications Letters

B. Construction of High-Rate LDPC Codes

Algorithm 1 CONSTRUCTION OF $\mathbf{H}_2$

Input:
r, W_c; ▷ row number and column weight of $\mathbf{H}_2$.
Output:
$\mathbf{H}_2$: initialized as $\mathbf{H}_2 = [\,]$.
Begin
$\mathbb{L}_1 = \{l_{1,1}, \cdots, l_{1,W_c}\} \subset \{1, \cdots, r\}$;
$\mathbf{H}_2 = [\mathbf{h}_{\mathbb{L}_1}]$; ▷ $\mathbf{h}_{\mathbb{L}_1}$ is the first column with 1 indexed by $\mathbb{L}_1$.
for $j = 2 : 1 : \binom{r}{W_c}$ **do**
  $\mathbb{L}_j = \{l_{j,1}, \cdots, l_{j,W_c}\} \subset \{1, \cdots, r\}$;
  if $\tilde{c}_{\mathbf{H}_2} < 2$ **then** ▷ $\tilde{c}_{\mathbf{H}_2}$ is the column number of current $\mathbf{H}_2$.
    for $m = 1 : 1 : \tilde{c}_{\mathbf{H}_2}$ **do**
      $q(m) = cal(\mathbb{L}_j, \mathbb{L}_m)$; ▷ $cal(\mathbb{L}_j, \mathbb{L}_m)$ calculates $|\mathbb{L}_j \cap \mathbb{L}_m|$.
    end for
    if $\max(\mathbf{q}) < 2$ **then** ▷ $\max(\mathbf{q})$ returns the maximum value in the vector $\mathbf{q}$.
      $\mathbf{H}_2 = [\mathbf{H}_2 | \mathbf{h}_{\mathbb{L}_j}]$;
    else
      $\mathbf{H}_2 = [\mathbf{H}_2]$;
    end if
  else
    for $s = 1 : 1 : \tilde{c}_{\mathbf{H}_2}$ **do**
      $q(s) = cal(\mathbb{L}_j, \mathbb{L}_s)$;
      for $t = s + 1 : 1 : \tilde{c}_{\mathbf{H}_2}$ **do**
        $Q(s,t) = cal(\mathbb{L}_j, \mathbb{L}_s, \mathbb{L}_t)$; ▷ $cal(\mathbb{L}_j, \mathbb{L}_s, \mathbb{L}_t)$ calculates $|(\mathbb{L}_j \cap \mathbb{L}_s) \cup (\mathbb{L}_j \cap \mathbb{L}_t) \cup (\mathbb{L}_s \cap \mathbb{L}_t)|$.
      end for
    end for
    if $(\max(\mathbf{Q}) < 3) \&\& (\max(\mathbf{q}) < 2)$ **then** ▷ $\max(\mathbf{Q})$ returns the maximum value in the matrix $\mathbf{Q}$.
      $\mathbf{H}_2 = [\mathbf{H}_2 | \mathbf{h}_{\mathbb{L}_j}]$;
    else
      $\mathbf{H}_2 = [\mathbf{H}_2]$;
    end if
  end if
end for
End

Given W_c and r (i.e., $r = n - k$), the maximum number of columns of $\mathbf{H}_2$ can be roughly determined by **Theorem 4**, shown in the sequel.

Theorem 4. *The parity-check matrix of the LDPC code is assumed to be in the form of* $\mathbf{H} = [\mathbf{I} | \mathbf{H}_2]$[1]*, where* $\mathbf{H}_2$ *is a submatrix with column weight being* W_c *without length-4 and length-6 cycles. The column number of* $\mathbf{H}_2$ *is upper bounded as*

$$c_{\mathbf{H}_2} \leq \lfloor \frac{r-1}{W_c - 1} \rfloor \cdot \frac{r}{W_c} \tag{3}$$

Proof. If $|\mathbb{L}_i^{\mathbf{H}_2} \cap \mathbb{L}_j^{\mathbf{H}_2}| < 2, i \neq j, \forall i, j \in \{1, 2, \cdots, c_{\mathbf{H}_2}\}$, the weight of each row in $\mathbf{H}_2$ is less than or equal to $\lfloor \frac{r-1}{W_c-1} \rfloor$, where $\mathbb{L}_i^{\mathbf{H}_2}$ denotes the set representation for the i-th column of $\mathbf{H}_2$ and $\lfloor x \rfloor$ returns the greatest integer less than or equal to x. The total number of 1's in $\mathbf{H}_2$ can be expressed as $W_c \cdot c_{\mathbf{H}_2}$, so we get:

$$\lfloor \frac{r-1}{W_c - 1} \rfloor \cdot r \geq W_c \cdot c_{\mathbf{H}_2}. \tag{4}$$

□

This letter focuses on the construction of high-rate LDPC codes, which avoid length-4 and length-6 cycles in the Tanner graphs. The algorithm for constructing $\mathbf{H}_2$ is presented as follows:[2]

Step 1: List $\binom{r}{W_c}$ sets with each set containing W_c elements out of $\{1, \cdots, r\}$.

Step 2: Randomly select one set out of the $\binom{r}{W_c}$ sets as the first column of $\mathbf{H}_2$.

Step 3: Select another set as the second column of $\mathbf{H}_2$ by following Condition 1 of **Theorem 2**.

Step 4: Construct the remaining columns of $\mathbf{H}_2$ according to Condition 1 and Condition 2 of **Theorem 2**

The pseudocode for constructing $\mathbf{H}_2$ is provided in **Algorithm 1**.

The algorithm does not have a pre-fixed row weight and column number for $\mathbf{H}_2$. Nevertheless, the proposed algorithm can guarantee the girth of constructed LDPC codes is at least 8.

IV. SIMULATION RESULTS

In the simulations, we set $W_c = 4$ and $W_c = 6$ and evaluate the BER performance over AWGN channels with binary phase shift keying (BPSK) modulation and sum-product iterative decoding algorithm. The maximum number of iterations is set to 100 and the maximum erroneous bits are set 3000 for all the signal-to-noise ratios (SNRs). Simulation results for the LDPC codes constructed by **Algorithm 1** are shown in Fig. 2 with different code rates and lengths. The code $(774, 672)$ with $W_c = 4$ has the best BER performance due to its lowest code rate (even though it also has the shortest length), while the three LDPC codes with $W_c = 6$ have similar BER performance.

The construction methods from [16]–[18] are taken as the benchmark schemes. Fig. 3 shows the BER performance between our constructed LDPC codes and those from [16]–[18]. The code rates of our constructed LDPC codes are slightly lower than those from [16]–[18], while the code lengths are (almost) the same. Our constructed LDPC codes outperform those from [16]–[18] in terms of BER performance. When the BER is at the level of 10^{-4}, there exist an approximate 0.25 dB gain between our constructed LDPC code and that from [16] and an approximate 0.7 dB gain between our constructed LDPC code and that from [17]. When the BER is at the level of 10^{-7}, there exists an approximate 0.25 dB gain between our constructed LDPC code and that from [18].

[1]The structure is favorable since the generator matrix can be easily obtained. Moreover, we only need to focus on the construction of a smaller matrix $\mathbf{H}_2$ instead of $\mathbf{H}$.

[2]In practice, the number of columns constructed by the proposed algorithm is difficult to reach the theoretical upper bound, shown in (3).

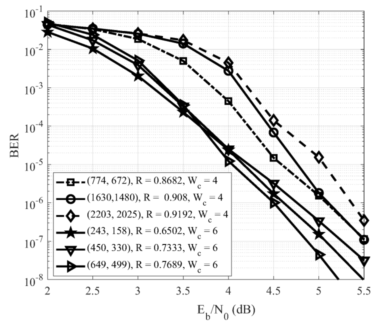

Fig. 2: Our constructed LDPC codes with $W_c = 4$ and $W_c = 6$.

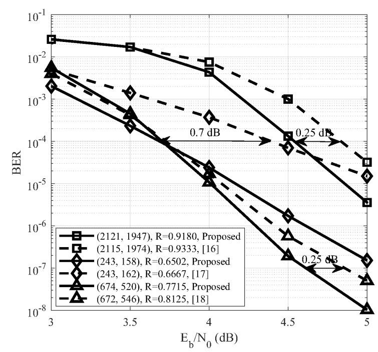

Fig. 3: Comparison between our constructed LDPC codes and those from [16]–[18].

The degree distributions of our constructed LDPC codes are shown in Tables I, II, and III, respectively. The complexity of constructing them based on Algorithm 1 are $O(r^4)$, $O(r^6)$, and $O(r^6)$, respectively.

TABLE I: The degree distribution of our constructed $(2121, 1974)$ LDPC code

Degree of CNs	25	26	27	29	30	31	33	34
Number of CNs	2	1	1	1	3	2	2	2
Degree of CNs	35	36	37	38	39	40	41	42
Number of CNs	2	3	8	2	3	6	5	5
Degree of CNs	43	44	45	46	47	48	49	50
Number of CNs	5	9	11	15	15	11	9	11
Degree of CNs	51	52	53	54	55	56	57	58
Number of CNs	5	6	4	9	4	3	6	6

TABLE II: The degree distribution of our constructed $(243, 158)$ LDPC code

Degree of CNs	6	8	9	10	11	12
Number of CNs	2	2	3	4	20	24
Degree of CNs	13	14	15	16	17	
Number of CNs	11	9	2	5	3	

TABLE III: The degree distribution of our constructed $(674, 520)$ LDPC code

Degree of CNs	12	13	14	15	16	17	18
Number of CNs	1	2	6	3	2	5	15
Degree of CNs	19	20	21	22	23	24	25
Number of CNs	11	12	27	31	10	5	2
Degree of CNs	26	27	28	29	30	31	
Number of CNs	4	5	3	3	5	2	

V. Conclusions

In the paper, a novel high-rate LDPC code (including short- and medium-length) construction scheme has been proposed based on the matroid theory. Simulation results have shown that the BER performance of the constructed LDPC codes is better than those constructed in the literature over AWGN channels with avoidance of length-4 and length-6 cycles. It would be of great interest to study the avoidance of length-8 cycles in order to construct even better LDPC codes as our future investigation.

References

[1] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58–60, Feb 2001.

[2] Y. Fang, P. Chen, G. Cai, F. C. Lau, S. C. Liew, and G. Han, "Outage-limit-approaching channel coding for future wireless communications: Root-protograph low-density parity-check codes," *IEEE Vehicular Technology Magazine*, vol. 14, no. 2, pp. 85–93, 2019.

[3] Y. Fang, G. Zhang, G. Cai, F. C. M. Lau, P. Chen, and G. Han, "Root-protograph-based BICM-ID: A reliable and efficient transmission solution for block-fading channels," *IEEE Trans. Commun.*, pp. 1–1, 2019.

[4] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[5] G. Zhang, Y. Hu, Y. Fang, and J. Wang, "Constructions of type-II QC-LDPC codes with girth eight from sidon sequence," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 3865–3878, Jun 2019.

[6] A. Tasdighi, A. H. Banihashemi, and M. Sadeghi, "Symmetrical constructions for regular girth-8 QC-LDPC codes," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 14–22, Jan. 2017.

[7] 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 Trans. Commun.*, vol. 62, no. 8, pp. 2626–2637, Aug. 2014.

[8] F. Amirzade and M. Sadeghi, "Lower bounds on the lifting degree of QC-LDPC codes by difference matrices," *IEEE Access*, vol. 6, pp. 23 688–23 700, 2018.

[9] X. Xiao, W. E. Ryan, B. Vasi, S. Lin, and K. Abdel-Ghaffar, "Reed-solomon-based quasi-cyclic LDPC codes: Designs, cycle structure and erasure correction," in *Proc. of Information Theory and Applications Workshop (ITA)*, Feb 2018, pp. 1–10.

[10] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 1949–1969, Jun. 2007.

[11] J. Feldman, M. J. Wainwright, and D. R. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 954–972, Mar. 2005.

[12] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb 2001.

[13] A. Dehghan and A. H. Banihashemi, "On the tanner graph cycle distribution of random LDPC, random protograph-based LDPC, and random quasi-cyclic LDPC code ensembles," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4438–4451, Jun. 2018.

[14] G. Wu, L. Wang, and T. Truong, "Use of matroid theory to construct a class of good binary linear codes," *IET Communications*, vol. 8, no. 6, pp. 893–898, Apr. 2014.

[15] G. Wu, H. C. Chang, L. Wang, and T. K. Truong, "Constructing rate 1/p systematic binary quasi-cyclic codes based on the matroid theory," *Designs, Codes and Cryptography*, vol. 71, no. 1, pp. 47–56, 2014.

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

[17] M. Polak and E. Zhupa, "Graph based linear error correcting codes," *CoRR*, vol. abs/1612.03279, 2016. [Online]. Available: http://arxiv.org/abs/1612.03279

[18] X. Wu, M. Jiang, and C. Zhao, "Construction of high-rate QC-LDPC codes with multi-weight circulants," in *proc. of ISTC*, Sep. 2016, pp. 21–25.