QC-LDPC codes from various Golomb Rulers

Daekyeong Kim, Hyojeong Choi and Hong-Yeop Song
School of Electrical and Electronic Engineering
Yonsei University
Seoul, South Korea
{daky33, hjchoi3022, hysong}@yonsei.ac.kr

***Abstract*—In this paper, we analyze the girth of QC-LDPC codes constructed using a special type of Golomb rulers called B_h sequences and a well-known multiplication table method. We investigate the condition for the existence of 8-cycles and we are able to count the exact number of 8-cycles in the QC-LDPC codes using B_h sequences. The analysis focuses on the case $h = 3$. By computer simulation, we show that the resulting codes for $h = 3$ have a better performance than those from general Golomb rulers (non-B_3 sequences) and have a comparable performance to the modified LDPC codes from basegraph2 in 5GNR spec. As h increases, the result could have higher girth but the performance improvement is only marginal.**

***Index Terms*—Golomb ruler, B_3 sequence, QC-LDPC codes, girth**

I. Introduction

A Golomb ruler [2] is a set of s marks of integers $\{g_1, g_2, ..., g_s\}$ with $g_1 < g_2 < ... < g_s$ such that

$$g_j - g_i \tag{1}$$

are all distinct for all $i < j$. The distance $L = g_n - g_1$ is the length of the above s-mark Golomb ruler. An s-mark Golomb ruler is called optimal if it has the shortest length. One example of an optimal 6-mark Golomb ruler is $\{0, 1, 8, 12, 14, 17\}$ [8]. When $\{g_1 = 0, g_2, ..., g_{s-1}, g_s\}$ is a Golomb ruler, replacing g_s with $g > 2g_{s-1}$, in general, gives a new Golomb ruler [8].

A sequence $a_1 < a_2 < ... < a_n$ is called B_h sequence [11] if the h-fold sums

$$a_{j_1} + a_{j_2} + ... + a_{j_h} \tag{2}$$

are all distinct for all $j_1 \leq j_2 \leq ... \leq j_h$. Note that $j_1 = j_2$, etc, and some or all of these j_l's can be the same. The difference $L = a_s - a_1$ is the length of the B_h sequence. A B_h sequence is optimal if it is of the shortest length among those with the same number of elements. A. W. Lam in [11] tabulated some optimal B_h sequences they found. See Table I.

A 3-free set [12] $\{a_1, a_2, ..., a_s\}$ with $a_1 < a_2 < ... < a_s$ is a set of non-negative integers such that any three elements $a_i < a_j < a_k$ do not satisfy the condition

$$2a_j = a_i + a_k. \tag{3}$$

This work was supported by the National Research Foundation of Korea (NRF) Grant by the Korean Government through Ministry of Sciences and ICT (MSIT) under Grant RS-2023-00209000.

TABLE I
OPTIMAL B_h SEQUENCES [11]

h	n	Optimal sequences
3	3	$\{0, 1, 4\}$
	4	$\{0, 1, 7, 11\}$
		$\{0, 1, 8, 11\}$
	5	$\{0, 1, 15, 18, 23\}$
		$\{0, 1, 15, 20, 23\}$
	6	$\{0, 2, 11, 26, 42, 45\}$
	7	$\{0, 1, 7, 50, 59, 78, 82\}$
		$\{0, 6, 7, 50, 59, 78, 82\}$
		$\{0, 2, 23, 45, 72, 79, 82\}$
4	4	$\{0, 1, 11, 15\}$
		$\{0, 2, 12, 15\}$
	5	$\{0, 1, 24, 37, 41\}$
	6	$\{0, 1, 17, 70, 95, 100\}$
5	5	$\{0, 1, 16, 66, 72\}$

Relations between 3-free sets, Golomb rulers and B_h sequences are described in [3], [8]. Every Golomb ruler is a 3-free set but not conversely. An integer sequence is a Golomb ruler if and only if it is a B_2 sequence. Every B_{h+1} sequence is a B_h sequence but not conversely. The optimal 4-mark Golomb ruler $\{0, 1, 4, 6\}$ is an example of a B_2 sequence but not a B_3 sequence, since

$$1 + 1 + 4 = 0 + 0 + 6.$$

A quasi-cyclic low-density parity-check (QC-LDPC) code [4] is an LDPC code with quasi-cyclic property. With simple encoding scheme and parallel decoding, QC-LDPC codes can be used in wireless communications for forward error correction. One can construct a QC-LDPC code using the following algorithm [5]–[10]. Here, we use the following notation:

- $E = [e(i, j)]$ is a $3 \times s$ exponent matrix of integers
- I is the identity matrix of size $P \times P$
- $I^{(t)}$ is the identity matrix I circularly shifted to the right t times. It is called circular permutation matrix (CPM)

Algorithm 1 Main Construction Platform [5]–[10]

Input: A positive integer P and two integer sequences

$$a = (a_1, a_2, a_3) \quad \text{and} \quad b = (b_1, b_2, ..., b_s)$$

Output: Binary $3P \times sP$ matrix H

Step 1: Construct $E = [e(i,j)]$ by $e(i,j) = a_i \cdot b_j$ for all i, j
Step 2: Construct H by replacing each element of E by an appropriate CPM:

$$H = \begin{bmatrix} I^{(e(1,1))} & I^{(e(1,2))} & \dots & I^{(e(1,s))} \\ I^{(e(2,1))} & I^{(e(2,2))} & \dots & I^{(e(2,s))} \\ I^{(e(3,1))} & I^{(e(3,1))} & \dots & I^{(e(3,s))} \end{bmatrix}$$

Then, H as a parity check matrix defines a QC-LDPC code of length sP.

Girth is the minimum length of cycles in Tanner graph (bipartite graph) of a parity check matrix H. It is obvious that any cycle in this case has even length. With some abuse of notation, we say simply H has girth g when the Tanner graph of H has girth g. According to [4], there exist cycles of length $2c$ in H if and only if

$$\sum_{l=0}^{c-1} a_{i_l}(b_{j_l} - b_{j_{l+1}}) \equiv 0 \pmod{P} \tag{4}$$

for some $i_0, i_1, ..., i_{c-1}$ and $j_0, j_1, ..., j_c = j_0$ such that $i_l \neq i_{l+1}$ and $j_l \neq j_{l+1}$ for $0 \leq l < c$. Thus, if E avoids the condition for the existence of a cycle lengths up to $2c$, the resulting code from Algorithm 1 has girth $2(c+1)$.

Majdzade in [12] constructs the girth-8 QC-LDPC codes using $a = (0, 1, 2)$ and some 3-free sets as b in Algorithm 1. Kim in [8] constructs the codes using $a = (1, 2, 3)$ and some Golomb rulers as b in Algorithm 1. This construction is further analyzed by D. Kim in [9], [10]. It is proved in [8] that the resulting code has girth 8 if the size P of CPM in Algorithm 1 is larger than twice of the length L of the Golomb ruler when $a = (1, 2, 3)$.

D. Kim in [9], [10] constructed the QC-LDPC codes of girth 8 where $a = (1, 2, 3)$ and $b = (b_1, b_2, ..., b_s)$ is an integer sequence from the optimal 6-mark Golomb ruler $\{0, 1, 8, 12, 14, 17\}$ or other 6-mark Golomb rulers $\{0, 1, 8, 12, 14, g_6\}$ with $g_6 = 29, 30, 31, ..., 99$ in Algorithm 1. Here, the size P of CPM was set to be 200 for the length 1200. By simulation, the E_b/N_0 at Frame Error Rate (FER) 10^{-3} are compared for all these g_6 values as in Fig. 1.

There exists distinct performance degradation of the codes with $g_6 = 50, 51, 58, 62, 64$. In theses cases, the Golomb rulers $\{0, 1, 8, 12, 14, g_6\}$ with $g_6 = 50, 51, 58, 62, 64$ cover the distance of $\frac{P}{4} = 50$ as follows.

$$50 - 0 = 51 - 1 = 58 - 8 = 62 - 12 = 64 - 14 = 50$$

But in all other cases, the Golomb rulers don't cover the distance of $\frac{P}{4} = 50$. D. Kim in [9], [10] analyzed that this difference makes the separation of the performance between suggested codes as shown in Fig. 1. And they suspect that

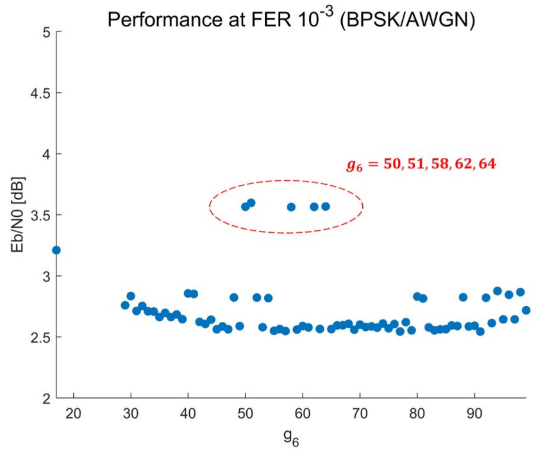

Fig. 1. Performance of the half-rate codes from Golomb rulers [9]

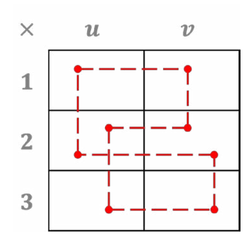

Fig. 2. 8-cycle pattern in Lemma 1

the extra covered distance 50 above causes a very distinctive group of 8-cycles which behave as stopping sets or trapping sets [13].

This paper is organized as follows. In Section II, We prove and verify some properties about the number of cycles of the codes constructed using some $B_h (h \geq 3)$ sequences. In Section III, we simulate and analyze the performance of the codes in Section II. Finally in Section IV, we summarize and conclude the paper.

II. Some New Construction from B_h Sequences

With some abuse of notation, we use the integer sequence $b = (b_1, b_2, ..., b_s)$ and the s-mark Golomb ruler or B_h sequence $\{b_1, b_2, ..., b_s\}$ interchangeably.

B_3 sequences are special case of Golomb rulers. We construct the QC-LDPC codes using $a = (1, 2, 3)$ and B_3 sequences as b in Algorithm 1. Eventually we will show that the codes constructed using B_3 sequences have better performance than the codes constructed using general Golomb rulers. By exactly counting the number of 8-cycles of the resulting codes from B_3 sequences, we check that the number of 8-cycles is significantly decreased, and we are sure that this is the main reason of the performance improvement.

When $a = \{1, 2, 3\}$ is used in Algorithm 1, the pattern in

Fig. 2 must causes 8-cycles for any $u < v$ since

$$\sum_{l=0}^{3}(e(i_l, j_l) - e(i_l, j_{l+1})) \\ = u - v + 2v - 2u + 3u - 3v + 2v - 2u = 0.$$

Note that Fig. 2 shows two columns of E from Algorithm 1. The pattern in Fig. 2 causes 8-cycles P times which are all distinct, since every 1 within a CPM causes a cycle and there are P 1's in it. Since this pattern occurs whenever 2 columns are chosen from s columns of exponent matrix, this type of 8-cycles appear $\binom{s}{2} \times P$ times.

Lemma 1: Assume that $a = (1, 2, 3)$ is used with any integer sequence b in Algorithm 1. The 8-cycles in Fig. 2 must appear $\binom{s}{2} \times P$ times. Therefore, the total number 8-cycles is at least this much in H.

Lemma 2: Assume $\{b_1, b_2, ..., b_s\}$ is a length-L B_h sequence. If $P > hL$, then h-fold sums from the sequence $b = (b_1, b_2, ..., b_s)$,

$$b_{j_1} + b_{j_2} + ... + b_{j_h}$$

are all distinct mod P for any $j_1 \leq j_2 \leq ... \leq j_h$.

Proof: Any h-fold sum can not be more than hL. ■

Lemma 3: Assume that $a = (1, 2, 3)$, any integer sequence $b = (b_1, b_2, ..., b_s)$ and $P \times P$ CPMs are used in Algorithm 1. Then, the condition for the existence of an 8-cycle becomes

$$b_{j_0} + b_{j_1} - b_{j_2} - b_{j_3} \equiv 0 \pmod P \tag{5}$$

or

$$b_{j_0} - b_{j_1} + b_{j_2} - b_{j_3} \equiv 0 \pmod P \tag{6}$$

or

$$b_{j_0} - 2b_{j_1} + 2b_{j_2} - b_{j_3} \equiv 0 \pmod P \tag{7}$$

or

$$2b_{j_0} - 2b_{j_1} + 2b_{j_2} - 2b_{j_3} \equiv 0 \pmod P \tag{8}$$

for some j_0, j_1, j_2, j_3 such that $j_0 \neq j_1,\ j_1 \neq j_2,\ j_2 \neq j_3$ and $j_3 \neq j_0$.

Proof: The condition for the existence of an 8-cycle in (4) becomes

$$\sum_{l=0}^{3} a_{i_l}(b_{j_l} - b_{j_{l+1}}) \equiv 0 \pmod P \tag{9}$$

for some i_0, i_1, i_2, i_3 and $j_0, j_1, j_2, j_3, j_4 = j_0$ such that $i_l \neq i_{l+1}$ and $j_l \neq j_{l+1}$ for $0 \leq l < 4$. Suppose we arrange all conditions for the existence of an 8-cycle by substituting 1, 2, 3 for i_l's in possible combinations. The rotations of i_l's ($i_l \to i_{l+1}$) make any difference in the resulting expressions. Therefore, we don't need to consider any cyclic permutations of i_l's and it is enough to consider the following six cases of (i_0, i_1, i_2, i_3):

$$\begin{aligned} &(1,2,1,2), \quad &&(1,2,1,3), \\ &(2,3,2,3), \quad &&(2,3,2,1), \\ &(3,1,3,1), \quad &&(3,1,3,2). \end{aligned} \tag{10}$$

From the first case of $(i_0, i_1, i_2, i_3) = (1, 2, 1, 2)$ and since $a = (a_1, a_2, a_3) = (1, 2, 3)$, the condition (9) becomes

$$b_{j_0} - b_{j_1} + 2b_{j_1} - 2b_{j_2} + b_{j_2} - b_{j_3} + 2b_{j_3} - 2b_{j_0} \equiv 0 \pmod P$$

which reduces to

$$b_{j_0} - b_{j_1} + b_{j_2} - b_{j_3} \equiv 0 \pmod P$$

as the condition (6).

From $(i_0, i_1, i_2, i_3) = (2, 3, 2, 1)$, we get the condition

$$2b_{j_0} - 2b_{j_1} + 3b_{j_1} - 3b_{j_2} + 2b_{j_2} - 2b_{j_3} + b_{j_3} - b_{j_0} \equiv 0 \pmod P$$

which reduces to

$$b_{j_0} + b_{j_1} - b_{j_2} - b_{j_3} \equiv 0 \pmod P$$

as the condition (5).

Similarly, we can get the remaining conditions from the other cases in (10). ■

Theorem 1: Assume that the sequence $a = (1, 2, 3)$, $b = (b_1, b_2, ..., b_s)$ and $P \times P$ CPMs are used in Algorithm 1. Let b be a B_3 sequence of length L. Then, the resulting QC-LDPC code has girth 8 and 8-cycles appear exactly $\binom{s}{2} \times P$ times if $P > 4L$ in general or if $P > 3L$ when P is odd.

Proof: Since $P > 2L$ and B_3 sequence is a Golomb ruler, the code has girth 8 [8].

We will show that all other 8-cycles are impossible in H except for the special type of 8-cycles in Fig. 2. From Lemma 1, such an 8-cycle appears exactly $\binom{s}{2} \times P$ times inevitably. We note that this pattern of an 8-cycle corresponds to the condition (5) with $j_0 = j_2$ and $j_1 = j_3$.

We now distinguish the following 3 remaining cases from Lemma 3:

(A) 8-cycles from (5) except for $j_0 = j_2$ and $j_1 = j_3$
(B) 8-cycles from (6) or (7)
(C) 8-cycles from (8)

For (A) and (B), it is straightforward that the condition cannot be satisfied, since B_3 sequence is used with $P > 3L$, and the conditions (5), (6), or (7) check whether some 2-fold sums or 3-fold sums repeat in the B_3 sequence.

For (C), we use the following relation.

$$\begin{aligned} &2b_{j_0} - 2b_{j_1} + 2b_{j_2} - 2b_{j_3} \equiv 0 \pmod P \\ \Leftrightarrow\ &b_{j_0} - b_{j_1} + b_{j_2} - b_{j_3} \equiv 0 \left(\bmod \frac{P}{gcd(2,P)}\right) \end{aligned}$$

If P is odd, then $gcd(2, P) = 1$, and the above becomes

$$b_{j_0} - b_{j_1} + b_{j_2} - b_{j_3} \equiv 0 \pmod P,$$

which is the condition (6).

If $P > 4L$ and P is even, the above becomes

$$b_{j_0} - b_{j_1} + b_{j_2} - b_{j_3} \equiv 0 \pmod{P/2}.$$

Since $P/2 > 2L$ and B_3 sequence is a Golomb ruler, it is straightforward that the condition cannot be satisfied by Lemma 2. ■

Tables II and III show the number of cycles when the codes are constructed using an optimal Golomb ruler, an optimal B_3

sequence. $P = 181 = 4 \cdot 45 + 1$ is used for Table II and an odd $P = 137 = 4 \cdot 45 + 2$ is used for Table III. In both case, the code from B_3 sequence has not only less 8-cycles but also less 10-,12-cycles than the code from the Golomb ruler.

TABLE II
COMPARISON OF THE NUMBER OF CYCLES ($P = 181$)

	Golomb Ruler [8] $\{0, 1, 8, 12, 14, 17\}$	B_3 sequence [11] $\{0, 2, 11, 26, 42, 45\}$
4-cycles	0	0
6-cycles	0	0
8-cycles	5249	2715 = $\binom{6}{2} \times 181$
10-cycles	27512	3982
12-cycles	255572	102989

TABLE III
COMPARISON OF THE NUMBER OF CYCLES ($P = 137$)

	Golomb Ruler [8] $\{0, 1, 8, 12, 14, 17\}$	B_3 sequence [11] $\{0, 2, 11, 26, 42, 45\}$
4-cycles	0	0
6-cycles	0	0
8-cycles	3973	2055 = $\binom{6}{2} \times 137$
10-cycles	20824	4110
12-cycles	193444	97681

Similarly, we can construct the girth-10 code using B_5 sequences and the girth-12 code using B_6 sequences as following Theorem 2. But we omit the detailed proof of Theorem 2 in this paper due to space limitation.

Theorem 2: Assume that the sequence $a = (1, 2, 4)$, $b = (b_1, b_2, ..., b_s)$ and $P \times P$ CPMs are used in Algorithm 1. Let b be a B_h sequence of length L. Then the resulting QC-LDPC code from Algorithm 1 has 1) girth at least 10 if $h = 5$ and $P > 5L$ and P is not a multiple of 3, 2) girth 12 if $h = 6$ and $P > 6L$.

III. SIMULATION

In this section, we simulate the FER performances of the QC-LDPC codes from various Golomb rulers. We also simulate the FER performances of the modified LDPC codes from 5GNR basegraph2 [1] of similar length and rate for comparison. Assuming BPSK modulation and AWGN channel, we use sum-product decoding with maximum 50 iterations.

Figure 3 shows the FER performances of the codes of P = 137. The code from optimal B_3 sequence shows additional coding gain about 0.6 dB over the code from optimal Golomb ruler and about 0.1 dB difference with 5GNR LDPC code of length 880, all at FER 10^{-3}.

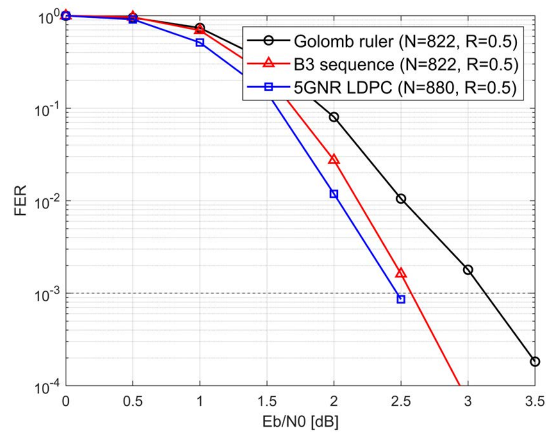

Fig. 3. Performance of the half-rate codes of length 822 using $P = 137$

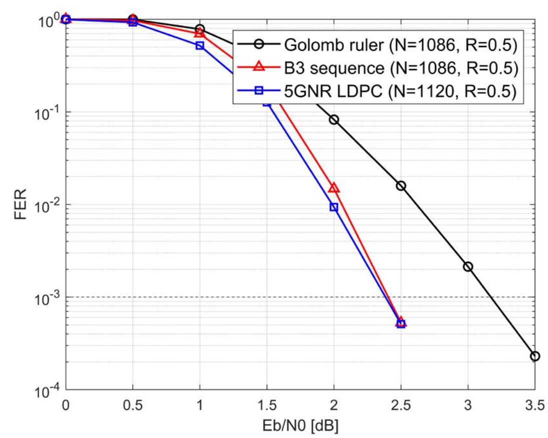

Fig. 4. Performance of the half-rate codes of length 1086 using $P = 181$

Figure 4 shows the FER performances of the codes of P = 181. The code from optimal B_3 sequence shows additional coding gain about 0.7 dB over the code from optimal Golomb ruler and almost same performance with 5GNR LDPC code of length 1120, all at FER 10^{-3}.

We have checked by computer the performance of the codes from Theorem 2 but confirmed some marginal improvement over the code from general Golomb rulers but not as good as those from 5GNR spec, and we skip the curve due to the space limitation.

IV. CONCLUDING REMARKS

In this paper, we constructed and analyzed the QC-LDPC codes using various Golomb rulers in Algorithm 1. From the conditions for the existence of an 8-cycle, we proved that using B_3 sequence of proper length in the construction makes the codes have girth 8 and leaves 8-cycles of some special case only. We simulated the performance of the codes from B_3

sequences and checked that it has similar performance with the modified LDPC codes from 5GNR basegraph2.

We now have examples of optimal B_h sequences only from [11]. Some more investigation on the constructing these sequences could be an interesting future work.

However, it is noted that as h increases, the length of an optimal sequence increases rapidly, and it makes the rate of the resulting code to be low, and it could be much lower than the half. Therefore, we may have only a marginal interest of using B_h sequences with large h in this construction for QC-LDPC codes. This could be another problem to be solved for the design of QC-LDPC codes of various rates (high or low) using this technique.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) Grant by the Korean Government through Ministry of Sciences and ICT (MSIT) under Grant RS-2023-00209000.

REFERENCES

[1] 3GPP TS 38.212, NR; Multiplexing and Channel Coding (Release 17), 2022.

[2] G. S. Bloom and S. W. Golomb, "Applications of numbered undirected graphs," *Proceedings of the IEEE*, 65(4), pp. 562-570, 1977.

[3] A. Dimitromanolakis, "Analysis of the Golomb Ruler and the Sidon Set Problems, and Determination of Large, Near-Optimal Golomb Rulers (Master's thesis)," Department of Electronic and Computer Engineering, Technical University of Crete, 2002.

[4] M. P. C. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *IEEE Transactions on Information Theory*, 50(8), pp. 1788-1793, 2004.

[5] I. Kim and H.-Y. Song, "A simple construction for qc-ldpc codes of short lengths with girth at least 8," *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1462–1465, 2020.

[6] I. Kim and H.-Y. Song, "Some new constructions of girth-8 qc-ldpc codes for future gnss," *IEEE Communications Letters*, vol. 25, no. 12, pp. 3780–3784, 2021

[7] I. Kim, T. Kojima and H. -Y. Song, "Some Short-Length Girth-8 QC-LDPC Codes From Primes of the Form $t^2 + 1$," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1211-1215, 2022

[8] I. Kim and H.-Y. Song, "A construction for girth-8 QC-LDPC codes using Golomb rulers," *Electronics Letters*, 58(15), pp. 582-584, 2022.

[9] D. Kim, I. Kim, H. Cho, H. Choi and H. -Y. Song, "Performance Analysis of QC-LDPC codes constructed by using Golomb rulers," *2022 27th Asia Pacific Conference on Communications (APCC),* pp. 301-302, 2022.

[10] D. Kim, "Performance analysis and new construction of QC-LDPC codes from Golomb ruler (Master's thesis)," Department of Electrical and Electronic Engineering, The Graduate School Yonsei University, 2023.

[11] A. W. Lam and X. Duan, "Optimal Bh(n) sequences," *Electronics Letters*, 25(6), pp. 477–478, 1989.

[12] M. Majdzade and M. Gholami, "On the Class of High-Rate QC-LDPC Codes With Girth 8 From Sequences Satisfied in GCD Condition," *IEEE Communications Letters*, 24(7), pp. 1391-1394, July 2020.

[13] A. Price and J. Hall, "A survey on trapping sets and stopping sets," *arXivpreprint arXiv:1705.05996*, May 2017.