A construction for girth-8 QC-LDPC codes using Golomb rulers

Inseon Kim and Hong-Yeop Song✉
School of Electrical and Electronics Engineering, Yonsei University, Seoul, Korea
✉Email: hysong@yonsei.ac.kr

In this paper, an algebraic construction of regular QC-LDPC codes by using the modular multiplication table mod P and Golomb rulers are proposed. It is proved that the proposed QC-LDPC codes based on a Golomb ruler of length L have girth at least 8 if $P > 2L$. The error performance of the proposed QC-LDPC codes are simulated with various Golomb rulers. The proposed codes of length around 300 from the optimal 6-mark Golomb ruler have an additional coding gain of at least 0.1 dB over 5G NR LDPC codes, 0.5 dB over those given earlier by others, both at FER 10^{-3}. Some non-trivial techniques to increase the length of a given Golomb ruler with and without an additional mark for improving the performance of the codes from Golomb rulers up to 0.7 dB are also found.

Introduction: A Golomb ruler is a set of marks at integer positions along a ruler such that no two pairs of marks are the same distance apart [1, 2]. It was first studied by Babcock to find solutions for selecting radio frequencies to diminish the interference between communication channels in 1953 [3], and was fully studied mathematically in terms of their constructions and applications [4] and many new applications in radioastornomy [5], coding theory [6, 7], and sequences design [8].

Quasi-cyclic low-density parity-check (QC-LDPC) codes [9] are getting more and more attention because of the simple encoding scheme and parallel decoding. The QC-LDPC code $\mathcal{C}$ is an LDPC code such that, for some fixed integer i dividing the code length, $\hat{S}^i\mathbf{c} \in \mathcal{C}$ whenever $\mathbf{c} \in \mathcal{C}$ where $\hat{S}$ is the cyclic shift operator. It is a cyclic LDPC code when $i = 1$. A typical description of a QC-LDPC code uses a parity-check matrix which is partitioned by some circular permutation matrices (CPM) of the same size [9].

The multiplication table methods for structured QC-LDPC codes have been proposed in various different forms [9–16]. They follow some universal scheme of first constructing an $m \times n$ exponent matrix $\mathbf{E} = [e(i, j)]$ as a multiplication $e(i, j) = e(i, 0)e(0, j)$ and then determining the parity-check matrix $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ by substituting some appropriately-shifted CPM of size P into the position (i, j) of $\mathbf{E}$ for all i, j. The resulting code is the null space of $\mathbf{H}$, of length nP. The differences are (i) choice of the top-row and the left-most column sequences of $\mathbf{E}$ so that some girth condition is satisfied and (ii) choice of the multiplication (ordinary or modular).

A universal condition to guarantee some girth of the proposed codes is from ref. [9] or its variation (some sufficient conditions). Here, the two sequences $\{e(i, 0)|i = 0, 1, \ldots, m-1\}$ and $\{e(0, j)|j = 0, 1, \ldots n-1\}$ should satisfy the non-existence condition [9] of a $2c$-cycle in the Tanner graph of $\mathbf{H}$:

$$\sum_{l=0}^{c-1} (e(i_l, 0)e(0, j_l) - e(i_l, 0)e(0, j_{l+1})) \not\equiv 0 \pmod{P}$$

for all $i_0, i_1, \ldots, i_{c-1}$ and $j_0, j_1, \ldots, j_c = j_0$ such that $i_l \neq i_{l+1}$ and $j_l \neq j_{l+1}$ for $0 \leq l < c$.

A greatest common divisor (GCD) constraint on the finite integer sequences is one sufficient condition that guarantees the girth-8 when the sequence with GCD constraint is used as top-row of $\mathbf{E}$ and the left-most column is given as $\{0, 1, \ldots, m-1\}$ [12]. A 3-free-set condition is another such condition [15]. It is known that any 3-free-set condition implies the GCD constraints but not conversely [15]. These two constructions [12, 15] have the properties that (i) the left-most columns are $\{0, 1, \ldots, m-1\}$ and the top-rows are either the sequences with GCD constraints or 3-free-set condition in order to guarantee the girth-8 property and (ii) multiplication is ordinary and hence the CPM size is determined by the largest element in $\mathbf{E}$. On the other hand, in ref. [16], (i) they have to search for the top-row integer sequence that satisfies the condition from ref. [9] and then (ii) the multiplication is modular. All three constructions have to search for the top-row sequences to guarantee the girth-8 property in some exhaustive ways.

A set of positive integers $\{g_1, g_2, \ldots, g_n\}$ where $g_1 < g_2 < \ldots < g_n$ is called a Golomb ruler if the differences $g_j - g_i$'s, for $i < j$, are all distinct [2]. Usually, the first mark is placed in position $g_1 = 0$. In this case, the length of the ruler is equal to the maximum difference, $L = g_n - g_1 = g_n$. An optimal Golomb ruler is the Golomb ruler of the smallest possible length when the number of marks is fixed to be n. We note that all distinct differences $g_j - g_i$'s implies that $g_j - g_i \neq g_k - g_j$ for any $g_i < g_j < g_k$. Therefore, a Golomb ruler is always a 3-free set, but not conversely.

In this paper, we propose an algebraic construction of regular QC-LDPC codes by using the modular multiplication table mod P and Golomb rulers. The multiplication is done mod P and hence we prove that $P > 2L$ guarantees the girth-8 property, where L is the length of the Golomb ruler. We simulate the error performance of the proposed QC-LDPC codes with various Golomb rulers. The proposed codes of length around 300 from the optimal 6-mark Golomb ruler have an additional coding gain of 0.1 dB over those from 5G NR LDPC code [17], 0.5 dB over those from ref. [13] and at least 2.0 dB over those from ref. [15], all at FER 10^{-3}. We also find some non-trivial techniques to increase the length of a given Golomb ruler with and without an additional mark for improving the performance of the codes up to 0.7 dB.

Properties of Golomb rulers: We will describe some techniques of getting a new Golomb ruler from any given one. The proposed construction in this paper will use any Golomb ruler regardless of its optimality. We note that when $\{g_1, g_2, \ldots, g_n\}$ is an n-mark Golomb ruler, any subset of size $m \leq n$ is also an m-mark Golomb ruler.

Theorem 1. *Let $\{g_1, g_2, \ldots, g_{n-1}, g_n\}$ be an n-mark Golomb ruler. Then, $\{g_1, g_2, \ldots, g_{n-1}, g\}$ is also an n-mark Golomb ruler if $g > 2g_{n-1}$.*

Proof. To prove that $\{g_1, g_2, \ldots, g_{n-1}, g\}$ is an n-mark Golomb ruler, we have to check the differences with g and g_i for $1 \leq i \leq n-1$, since $\{g_1, g_2, \ldots, g_{n-1}\}$ is an $(n-1)$-mark Golomb ruler. If $g - g_i = g - g_j$ for some $i \neq j$, then $g_i = g_j$, which is impossible. If $g - g_i = g_j - g_k$ for some $j > k$ and some i, then $g = g_i + g_j - g_k \leq g_i + g_j \leq 2g_{n-1}$, which is impossible since $g > 2g_{n-1}$. □

Construction of QC-LDPC codes using Golomb ruler: We will describe the main construction and the proof that it gives a girth-8 QC-LDPC code.

Main construction:

(Step 1) Choose an n-mark Golomb ruler $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ of length $L = b_{n-1} - b_0$, where $n > 3$.

(Step 2) Construct a $3 \times n$ exponent matrix $\mathbf{E} = [e(i, j)]$ where $e(i, j) = ib_j \pmod{P}$ for $i = 1, 2, 3$ and $j = 0, 1, \ldots n-1$, where $P > 2L$. The integer $e(i, j)$ must be in the range $0 \leq e(i, j) \leq P - 1$.

(Step 3) Finally construct the parity-check matrix $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ by substituting an appropriate CPM of size P. For the position (i, j), the appropriate CPM is the identity matrix of size P circularly shifted by $e(i, j)$.

The binary QC-LDPC code from main construction is the null space of the parity-check matrix $\mathbf{H}$. The length becomes nP and the code rate is at least $(n-3)/n$. We want to check whether the proposed QC-LDPC codes have girth-8 or not.

Theorem 2. *The QC-LDPC codes from main construction have girth-8 if $P > 2L$, where P is the modulus in the construction of the exponent matrix as in (Step 2) and L is the length the Golomb ruler.*

Proof. We have to show that the Tanner graph of $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ from main construction does not have 4-cycles and 6-cycles. Main construction uses the multiplication table method with left-most column (1,2,3) and the top-row $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ for the exponent matrix $\mathbf{E} = [e(i, j)]$. It is easy to see from the non-existence condition in Introduction that there is no 4-cycle if $b_i - b_j \not\equiv 0 \pmod{P}$ and $2(b_i - b_j) \not\equiv 0 \pmod{P}$ for all $0 \leq i \neq j < n$. Since the length of the Golomb ruler is L, we have $-L \leq b_i - b_j \leq L$ for any $i \neq j$. Therefore, the condition is satisfied since $P > 2L$.

Table 1. *Golomb rulers [2] and CPM size P in main construction*

# marks	Golomb rulers	L	P
4	(0,1,4,6)	6	$P > 12$
5	(0,1,4,9,11)	11	$P > 22$
	(0,2,7,8,11)		
6	(0,1,4,10,12,17)	17	$P > 34$
	(0,1,4,10,15,17)		
	(0,1,8,11,13,17)		
	(0,1,8,12,14,17)		
7	(0,1,4,10,18,23,25)	25	$P > 50$
	(0,1,7,11,20,23,25)		
	(0,1,11,16,19,23,25)		
	(0,2,3,10,16,21,25)		
	(0,2,7,13,21,22,25)		

Now, consider the case of 6-cycles. The non-existence condition for 6-cycles can be rewritten as

$$(2-1)b_i - (3-1)b_j + (3-2)b_k \neq 0 \pmod P$$

or

$$b_i - b_j \neq b_j - b_k \pmod P,$$

for any three distinct indices i, j and k. Since the length of the Golomb ruler is L, the difference $b_i - b_j$ for any $i \neq j$ is in the range between $-L$ and L, and these differences $(b_i - b_j)$'s for all $i \neq j$ are all distinct. Therefore, the condition is satisfied since $P > 2L$. □

It is noticed that one can add a constant to the left-most column or to the top-row of the multiplication table in main construction without changing the girth-8 property.

Therefore, one can use $(i, i+1, i+2)$ instead of (1,2,3) for the left-most column, and similarly, one can use $(b_0 + j, b_1 + j, \ldots, b_{n-1} + j)$ for the top-row of the multiplication table, for any integers i and j.

Table 1 shows that the n-mark optimal Golomb rulers and corresponding CPM sizes of girth-8 QC-LDPC codes from main construction. In the table, we present only the optimal Golomb rulers whose number of marks are between 4 and 7 [2]. According to ref. [1], the researchers found optimal Golomb rulers up to 27 marks.

From any n-mark Golomb ruler, one can find the smaller number of mark ruler by taking its subset. For example, let us consider the 7-mark Golomb ruler in Table 1. It gives the QC-LDPC code of length $7P$ and of rate $4/7$. By taking its subsets for 6-marks, 5-marks, and 4-marks, one can construct QC-LDPC codes of lengths $6P$, $5P$, and $4P$ and of rates $3/6$, $2/5$, and $1/4$, respectively.

Performance of QC-LDPC codes from main construction with various Golomb rulers: We now analyse the performance of the proposed girth-8 QC-LDPC codes from main construction using sum-product decoding and max 50 iterations under the assumption of AWGN channel and BPSK modulation.

Fig. 1 shows the FER performance of the proposed half-rate codes of length $6P = 312$ from two different 6-mark Golomb rulers: one is an optimal 6-mark Golomb ruler and the other is a subset of size 6 from the 7-mark Golomb ruler both in Table 1. Note that $P = 52 > 2L$ for using the Golomb ruler of length L so that both codes have girth-8. For comparison, we select three other half-rate QC-LDPC codes: 5G NR LDPC code of length 308 [17], the code by symmetrical construction [13] and the code from the 3-free set (0,2,3,7,8,10) [15]. The two proposed codes have almost the same performance. They have an additional coding gain of about 0.1 dB over 5G NR LDPC code, 0.5 dB over the code from [13], and more than 2.0 dB over the code from ref. [15], all at FER 10^{-3}.

We also simulated the FER performance of all the codes from five different 7-mark optimal Golomb rulers in Table 1 of length $7P = 357$ and of rate $4/7$. It turned out that their performances are very much the same. Here, the size $P = 51$ is used.

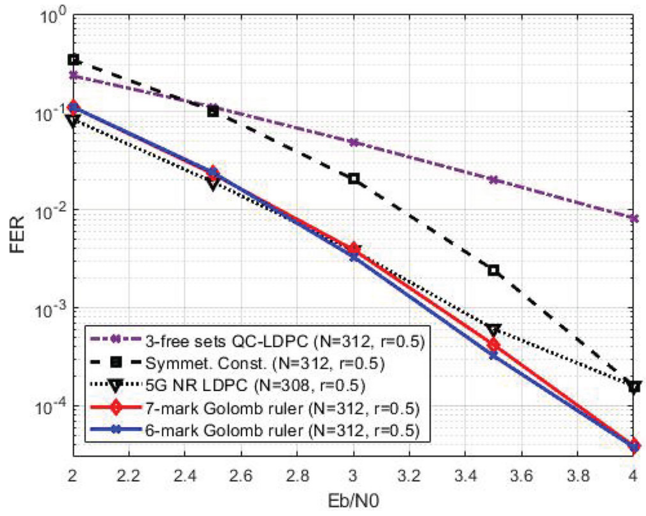

Fig. 1 *Performance comparison of various half-rate codes*

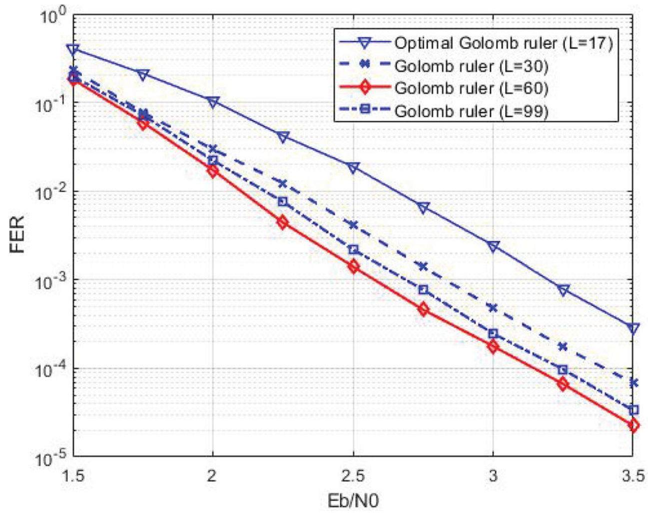

Fig. 2 *Performance of the codes using four 6-mark Golomb rulers*

In general, one can use the $(n-1)$-mark Golomb ruler obtained from n-mark one by taking a subset of size $n-1$. There are n ways of doing this. We check the case $n = 7$ and some extensive computing simulations show that all they have some similar performance.

Given an n-mark Golomb ruler, one can obtain many others of longer length by Theorem 1. The longer ones obtained by Theorem 1 are further away from the optimal Golomb ruler, but they construct the QC-LDPC codes with the same length nP.

In the hope of improving the performance, we simulate four half-rate codes from 6-mark Golomb rulers. The result is shown in Fig. 2.

We take the last optimal 6-mark Golomb ruler of length 17 in Table 1: (0, 1, 8, 12, 14, 17). From Theorem 1, we change the last mark 17 to 30, 60, and 99 to obtain longer length 6-mark rulers of lengths 30, 60, and 99, respectively. We use the CPM size $P = 200$ so that the code length is 1200 and the rate $3/6$.

The QC-LDPC codes using the ruler of length 60 shows the best performance among them. This code has an additional coding gain about 0.7 dB at FER 10^{-3} over those using the optimal ruler of length 17.

This shows an interesting trend of performance of the codes from the n-mark rulers when the last mark g_n increases. The performance increases as g_n increases up to some threshold value g^* and then decreases as the value g_n further increases beyond g^*. We now propose an interesting open problem: given an n-mark (optimal) Golomb ruler of length $L = g_n$, find the value g^* for the final mark g_n so that the performance of the code from main construction using the n-mark Golomb ruler of length g^* is the best.

Concluding remarks: In this paper, we propose an algebraic construction of regular QC-LDPC codes by using the modular multiplication table mod P and Golomb rulers. We prove that the proposed QC-LDPC codes based on a Golomb ruler of length L have girth at least 8 if $P > 2L$. We also proposed some deterministic ways to make some n-mark Golomb rulers (and also $n+1$-mark Golomb rulers) from a given n-mark Golomb ruler without any exhaustive search.

One interesting open problem is to find a new final mark g^* of a given n-mark optimal Golomb ruler so that the performance of the proposed QC-LDPC code is best. We currently do not have any idea except that it must be a function of the modulus P since $2g^* < P$ must be satisfied for the girth-8 property.

One final comment on the relation between the Golomb rulers and the 3-free sets. Every Golomb ruler is a 3-free set but not conversely. For example, a 3-free set (0,2,3,7,8,10) fails to be a Golomb ruler by the relations; $3-2=8-7$ of four different terms 2,3,7,8; or $2-0=10-8$ of another four terms 0,2,8,10; and many more. It may require further research for any theoretical support but now we just guess that the existence or non-existence of such violations in 3-free sets makes performance difference between the codes from 3-free sets and from Golomb rulers.

Acknowledgment: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A2C2011969).

Conflict of interest: The authors declare no conflict of interest.

Data availability statement: Data sharing not applicable - no new data generated, or the article describes entirely theoretical research.

Received: *15 January 2022* Accepted: *14 March 2022*
doi: 10.1049/ell2.12531

REFERENCES

1 Golomb ruler From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Golomb_ruler (2021). Accessed 11 Jan 2022

2 Dimitromanolakis, A.: Analysis of the golomb ruler and the sidon set problems, and determination of large, near-optimal golomb rulers. Master's Thesis, Technical University of Crete, Chania (2002)

3 Babcock, W.C.: Intermodulation interference in radio systems frequency of occurrence and control by channel selection. *Bell Syst. Tech. J.* **32**(1), 63–73 (1953)

4 Bloom, G.S., Golomb, S.W.: Applications of numbered undirected graphs. *Proc. IEEE* **65**(4), 562–570 (1977)

5 Blum, E.J., Ribes, J.C., Biraud, F.: Some new possibilities of optimum synthetic linear arrays for radioastronomy. *Astron. Astrophys.* **41**(3-4), 409–411 (1975)

6 Robinson, J., Bernstein, A.: A class of binary recurrent codes with limited error propagation. *IEEE Trans. Info. Theory* **13**(1), 106–113 (1967)

7 Chen, C., Bai, B., Li, Z., Yang, X., Li, L.: Nonbinary cyclic LDPC codes derived from idempotents and modular Golomb rulers. *IEEE Trans. Commun.* **60**(3), 661–668 (2012)

8 Urbano, D.F.D., Ojeda, C.A.M., Solarte, C.A.T.: Almost difference sets from singer type Golomb rulers. *IEEE Access* **10**, 1132–1137 (2022)

9 Fossorier, M.P.C.: Quasicyclic low-density parity-check codes from circulant permutation matrices. *IEEE Trans. Info. Theory* **50**, 1788–1793 (2004)

10 Tanner, R.M., Sridhara, D., Sridharan, A., Fuja, T.E., Costello, D.J.: LDPC block and convolutional codes based on circulant matrices. *IEEE Trans. Info. Theory* **50**(12), 2966–2984 (2004)

11 Zhang, G., Hu, Y., Ren, D., Liu, Y., Yang, Y.: Type-II QC-LDPC codes from multiplicative subgroup of prime field. *IEEE Access* **8**, 142459–142467 (2020)

12 Zhang, G., Sun, R., Wang, X.: Construction of girth-eight QC-LDPC codes from greatest common divisor. *IEEE Commun. Lett.* **17**(2), 369–372 (2013)

13 Tasdighi, A., Banihashemi, A.H., Sadeghi, M.-R.: Symmetrical constructions for regular girth-8 QC-LDPC codes. *IEEE Trans. Comm.* **65**(1), 14–22 (2017)

14 Xiao, X., Ryan, W.E., Vasic, B., Lin, S., Abdel-Ghaffar, K.: Reed-Solomon-based quasi-cyclic LDPC codes: designs, cycle structure and erasure correction. In: *Proceedings of Information Theory and Application Workshop*, pp. 1–10. IEEE, Piscataway, NJ (2018)

15 Majdzade, M., Gholami, M.: On the class of high-rate QC-LDPC codes with girth-8 from sequences satisfied in GCD condition. *IEEE Commun. Lett.* **24**(7), 1391–1394 (2020)

16 Kim, I., Song, H.-Y.: Some new constructions of girth-8 QC-LDPC codes for future GNSS. *IEEE Commun. Lett.* **25**(12), 3780–3784 (2021)

17 3GPP TS 38.212 v16.7.0 Release 16, NR; Multiplexing and Channel Coding. https://www.etsi.org/deliver/etsi_ts/138200_138299/138212/16.07.00_60/ts_138212v160700p.pdf (2021). Accessed 29 May 2022