Some variations of Tanner's construction for short length QC-LDPC codes

Wonjun Kim,[1] Hyunwoo Cho,[1] Hong-Yeop Song,[1,✉] and Min Kyu Song[2]

[1] *Department of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea*

[2] *Advanced Defense Science and Technology Research Institute (ADSTRI), Agency for Defense Development, Daejeon, South Korea*

✉ E-mail: hysong@yonsei.ac.kr

This paper proposes a modification to Tanner's work for constructing girth-8 quasi-cyclic low-density parity-check codes. The main contribution of this paper is to use an arithmetic sequence at the leftmost column for the exponent matrix so that the lifting size is not necessarily restricted to the prime numbers. Two theorems on the lifting sizes that achieve girth at least 8 using this approach is also provided. This construction exhibits better frame error rate results to the modified 5G new radio (NR) low-density parity-check codes for lengths around 500. Also, this construction achieves better frame error rate performance results than the recently proposed one using the Golomb rulers at around frame error rate of 10^{-6}.

Introduction: Low-density parity-check (LDPC) codes are one of the most widely used error-correcting codes in modern communication systems, such as the data channel of the 5G NR standard, Wi-Fi, and video communication standards [1, 2]. These codes are known for their ability to achieve near-Shannon limit under iterative decoding [3].

As low-latency communication systems, like vehicle-to-vehicle and Internet of Things, become more prevalent, the demand for error-correcting codes with shorter lengths is increasing. That is why our construction efforts are focused on short-length LDPC codes. It is well known that algebraically constructed LDPC codes tend to perform better than randomly constructed ones (e.g. by PEG algorithms) for lengths shorter than 1000 bits [4, 5].

Quasi-cyclic low-density parity-check (QC-LDPC) codes are a family of LDPC codes that exhibit a property: cyclically shifting a codeword for some fixed integer number of times produces another valid codeword. This property makes QC-LDPC codes an attractive option for high-speed communication systems, as they enable simple encoding methods with low required memory [6, 7] and low complexity decoding techniques [8].

The construction of QC-LDPC codes can be achieved using an exponent matrix [4, 9]. The exponent matrix E is an $m \times n$ matrix with elements denoted by $e(i, j)$, where i is the row index and j is the column index. To construct the H matrix, one can replace the (i, j) position of the exponent matrix E with $I_P(e(i, j))$, where $I_P(e(i, j))$ is a $P \times P$ identity matrix cyclically shifted $e(i, j)$ times. This process results in an H matrix of size $mP \times nP$, where P is referred to as the lifting size. The H matrix constructed with this method is regular, meaning that it has a constant column weight and a constant row weight.

The girth of LDPC codes is a crucial criterion for evaluation, referring to the shortest cycle lengths in the Tanner graph of the H matrix. Short cycle lengths can adversely affect belief-propagation(BP) decoding, making it essential for the H matrix to have a large girth [5]. Fossorier [4] established the conditions for cycles in the H matrix constructed from an exponent matrix. Fossorier made a proposition that H matrix has a cycle of length $2c$ if and only if

$$\sum_{k=0}^{c-1} (e(i_k, j_k) - e(i_{k+1}, j_k)) \equiv 0 \pmod{P}, \tag{1}$$

for some $i_0 = i_c$, $1 \le i_k \ne i_{k+1} \le m$ and $1 \le j_k \ne j_{k+1} \le n$.

Tanner et al. proposed a method for constructing an exponent matrix exploiting the multiplicative structure of integers [5]. Specifically,

$$e(i, j) = a^{j-1} b^{i-1} \pmod{P},$$

for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. It was proved that the H matrix has a girth ranging from at least 6 to at most 12 with a prime integer P. An $m \times n$ exponent matrix has a form:

$$E = \begin{bmatrix} 1 & a & a^2 & \ldots & a^{n-1} \\ b & ab & a^2 b & \ldots & a^{n-1} b \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ b^{m-1} & ab^{m-1} & a^2 b^{m-1} & \ldots & a^{n-1} b^{m-1} \end{bmatrix}.$$

For convenience, we will denote this construction by Tanner(m, n), where the top row and leftmost column of the exponent matrix are both geometric sequences of some integers a and b, respectively. Numerous research studies have been conducted to investigate the girth of Tanner's constructions with specific parameters. Kim et al. analysed and provided a proof for girth of Tanner(3,5) for lifting sizes of primes in a form of $P = 15k + 1$ [10]. The girths of Tanner(3,7) [11], Tanner(3,11) [12], and Tanner(3,13) [13] were analysed and determined using a similar approach as Kim's. These girths were determined for lifting sizes of primes in the form of $P = 21k + 1$, $P = 33k + 1$, and $P = 39k + 1$, respectively. Most of the girths analysed in these results were found to be 12. It is important to note that achieving such high girths requires a crucial restriction on the lifting size: the integer $P = mn + 1$ is a prime. An algorithm was employed in a computer search to derive the girth distribution for general Tanner(m, n) for various lifting sizes in reference [14].

Many studies have been conducted on constructing girth-8 QC-LDPC codes with various lifting sizes, which are not necessarily limited to prime numbers. Reference [15] describes another variation of Tanner's construction that uses geometric sequences in both the top row and leftmost column of an exponent matrix to create girth-8 QC-LDPC codes, subject to the conditions that $P \le M \le T$. Here, P is a prime of the form $P = t^2 + 1$, $M = KP$ is the modulus used to calculate the values of the exponent matrix, and T is the lifting size. A bound for T was given to achieve girth-8. In reference [16], some conditions were proposed for achieving girth-8 by using an exponent matrix consisting of two arbitrary sequences a_i and b_j for the top row and leftmost column, respectively, and $e(i, j) = a_i b_j$.

The Golomb ruler has been applied to construct girth-8 QC-LDPC codes. Specifically, the Golomb ruler marks were used to generate the first row of the exponent matrix, while consecutive integers were used for the leftmost column of the exponent matrix [9]. The authors of the paper [17] employed a modified Golomb ruler construction technique to increase the length of the codes by multiplying the last element of the Golomb ruler marks. Exploiting the Golomb ruler structure even further, the authors of the paper [18] employed a Golomb ruler that satisfies the B_3 property. Moreover, the results indicated that the proposed method outperformed the Golomb rulers that lacked the B_3 property in terms of frame error rate (FER).

This paper presents a modified structure of the exponent matrix, which is based on Tanner's construction. Unlike Tanner's approach, which employs geometric sequences for both the top row and the leftmost column, our construction employs a geometric sequence for the top row and an arithmetic sequence for the leftmost column of length up to 3. We provide a proof for the girth-8 conditions of our construction (Theorems 1 and 2), and compare the FER of the codes generated using our approach with those produced by the original Tanner's construction, the modified version of 5G NR standard [2], and the Golomb ruler [9] construction. By allowing lifting sizes that are not necessarily prime and ensuring that the girth is at least 8, we can provide a wide range of options for code lengths.

Main result – construction of ***H*** *and some properties:* **Main construction**

Let n, d, q, P be integers with $n > 3$, $d \ge 1$, $q > 1$, $gcd(q, P) = 1$, and $gcd(d, P) = 1$, where gcd is the greatest common divisor. Let N be the order of q modulo P, where we require that $N > n$.

(Step 1) From the set $S_N = \{0, 1, 2, \ldots, N-1\}$, take arbitrary n distinct elements $0 = a_1 < a_2 < \cdots < a_n$.

(Step 2) Define

$$e(i, j) = diq^{a_j} \tag{2}$$

for $i = 1, 2, 3$ and $j = 1, 2, \ldots, n$. Then, $E = (e(i, j))$ is a $3 \times n$ exponent matrix.

(Step 3) Replace the (i, j) position of E with $I_P(e(i, j))$, where $I_P(e(i, j))$ is the $P \times P$ identity matrix cyclically shifted $e(i, j)$ times. The result is an H matrix of size $3P \times nP$.

The QC-LDPC code defined as a null space of H above has length nP and code rate at least $(n - 3)/n$. We note that the exponent matrix E in Step 1 of the above is a multiplication table with an arithmetic sequence on the leftmost column and a geometric sequence (or its some subsequence) at the top row. We will identify the range of the lifting size P so that the code has neither 4-cycle nor 6-cycle in the theorems below.

Theorem 1. *Assume all the notations in the main construction. If* $P > 2q^{a_n} - 2$, *then H matrix from the main construction has girth at least 8.*

Proof. For a 4-cycle, (1) with (2) substituted becomes

$$(i_0 - i_1)q^{a_{j_0}} \equiv (i_0 - i_1)q^{a_{j_1}} \pmod{P},$$

where d was cancelled since it is relatively prime to P. Since $i_0 - i_1$ can only be any one of $\pm 1, \pm 2$. This gives

$$2(q^{a_{j_0}} - q^{a_{j_1}}) \equiv 0 \quad \text{or} \quad (q^{a_{j_0}} - q^{a_{j_1}}) \equiv 0 \pmod{P}. \tag{3}$$

Since $j_0 \neq j_1$ and we have

$$1 - q^{a_n} \leq q^{a_{j_0}} - q^{a_{j_1}} \leq q^{a_n} - 1,$$

any of the relations in (3) is impossible. Hence, a 4-cycle does not exist.

For a 6-cycle, (1) with (2) substituted becomes

$$q^{a_{j_0}}(i_0 - i_1) + q^{a_{j_1}}(i_1 - i_2) + q^{a_{j_2}}(i_2 - i_0) \equiv 0 \pmod{P},$$

where d is cancelled. Possible cases for the 3-tuple $((i_0 - i_1), (i_1 - i_2), (i_2 - i_0))$ are $(\pm 1, \pm 1, \mp 2)$, $(\pm 1, \mp 2, \pm 1)$, and $(\mp 2, \pm 1, \pm 1)$, double signs in the same order. All eight cases can be simplified to

$$q^{a_{j_0}} + q^{a_{j_2}} - 2q^{a_{j_1}} \equiv 0 \pmod{P}. \tag{4}$$

Since we have assumed that $P > 2q^{a_n} - 2$ and

$$2 - 2q^{a_n} < q^{a_{j_0}} + q^{a_{j_2}} - 2q^{a_{j_1}} < 2q^{a_n} - 2,$$

LHS of (4) cannot be a multiple of P. It is easy to see that it cannot be zero either. Therefore, the relation (4) is impossible, and hence, a 6-cycle does not exist. □

Theorem 2. *Assume that* $q^{a_n} < P \leq 2q^{a_n} - 2$. *Then, we have*

(4-cycles): H matrix from the main construction has no 4-cycle if and only if $P \neq 2q^l - 2$ *for the integers l with* $\log_q(q^{a_n} + 2)/2 < l \leq a_n$.

(6-cycles): H matrix from the main construction has no 6-cycle if and only if $P \neq q^{a_n} + q^l - 2$ *and* $P \neq 2q^{a_n} - q^l - 1$ *both for* $l = 1, 2, \ldots, a_n - 1$.

Proof. For 4-cycles, we will continue from (3) where P is now larger than q^{a_n}. This immediately rules out the second relation in (3). The first one can also be ruled out easily except for the values of $P = 2q^l - 2$ where l is in the range $\log_q(q^{a_n} + 2)/2 < l \leq a_n$. The other direction is obvious.

The condition for 6-cycles can be verified similarly. □

Remark 1. Two theorems will remain true when diq^{a_j} for $e(i, j)$ in the main construction is replaced with $(a + di)(q^{a_j} + h)$ with any positive integers a and h.

Remark 2. Two theorems will remain true when $a_0 \neq 0$ in Step 1 of the main construction. Here, the value a_n in both theorems must be replaced with $a_n - a_0$.

Table 1. Values of P that guarantees girth at least 8 for $q = 2$

a_n	$2^{a_n} < P \leq 2^{a_n+1} - 2$	$2^{a_n+1} - 2 < P$
	all the odd values in the range	all the odd values
4	Except for 23, 27, 29	No exceptions
5	Except for 47,55,59,61	
6	Except for 95,111,119,123,125	
7	Except for 191,223,239,247,251,253	

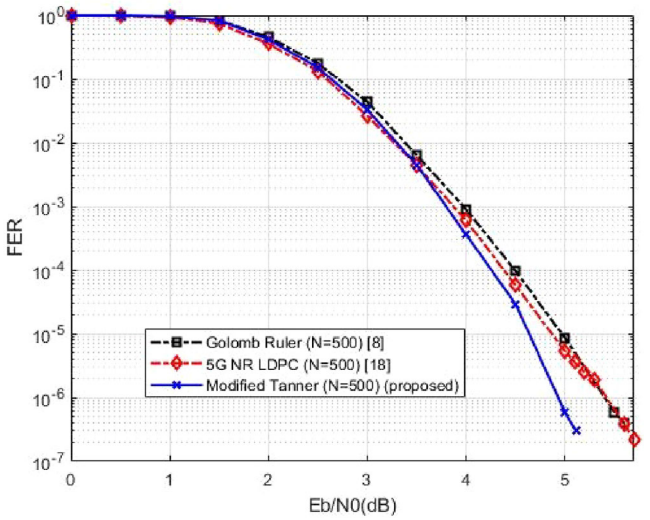

Fig. 1 *Performance comparison with length 500*

Remark 3. Two theorems will remain true when E is row permuted and/or column permuted with any permutations.

Remark 4. In Theorem 2, when $q = 2$, the value $q^{a_n} + q^l - 2$ must be even and cannot be equal to P which must be odd. Table 1 shows all the odd values of P that guarantees girth at least 8 from the main construction when $q = 2$ is used. There is no exception when $2^{a_n+1} - 2 < P$ but there are some exceptions in the odd integers P when $2^{a_n} < P \leq 2^{a_n+1} - 2$.

Performance analysis: Here, we compare simulation results of proposed construction with previous works, namely the Golomb ruler construction and original Tanner's construction. All three constructions have exponent matrices of the same size 3×6 and the code rate close to $1/2$. Lengths of interest here for simulation are short around 500. In addition to the constructions previously mentioned, we also include LDPC codes from the 5G NR standard in our comparison. We use the standard sum–product decoding with a maximum of eight iterations. The environment is set to additive white gaussian noise (AWGN) with binary phase shift keying (BPSK) modulation. FER performances of three codes of length 500 are depicted in Figure 1. Ruler set (0,1,4,10,12,17) is chosen to construct Golomb Ruler LDPC codes. The proposed construction (modified Tanner) uses $(a_1, a_2, \ldots, a_6) = (0, 1, 2, 3, 4, 5)$ with $q = 2$. The 5G NR's base graph 2 is truncated to match the rate and desired lengths for comparison. As shown in Figure 1, the proposed code has coding gain about 0.7 dB over those from 5G NR variation [2] and also over the Golomb ruler's [9] at FER 10^{-6}.

Initially, Tanner's research focused on constructing codes with lifting sizes that were prime numbers. In his paper, he mentioned that for non-prime lifting sizes, the girth could be as low as 4. This provides a motivation for comparing our construction for prime and non-prime lifting sizes, as our main contribution involves modifying the original work to achieve girth-8 even for non-prime lifting sizes. The number of cycles presented in Tables 2 and 3 have been determined through an exhaustive search by a computer program. As can be seen from Table 2, all of the original codes by Tanner have 6-cycles and non-prime lifting sizes have significantly more cycles in terms of either length 6 or length 8. Table 3 shows that proposed codes do not contain any 4-cycles and 6-cycles as

Table 2. Number of cycles of original codes by Tanner in Figure 2

P	4-cycle	6-cycle	8-cycle	10-cycle
Prime $P = 53$	0	53	954	10,653
Non-prime $P = 57$	0	228	1197	9633
Prime $P = 83$	0	166	830	9628
Non-prime $P = 87$	0	174	1653	9483

Table 3. Number of cycles of proposed codes in Figure 2

P	4-cycle	6-cycle	8-cycle	10-cycle
Prime $P = 53$	0	0	2067	9964
Non-prime $P = 57$	0	0	2223	9690
Prime $P = 83$	0	0	2905	9628
Non-prime $P = 87$	0	0	3219	9396

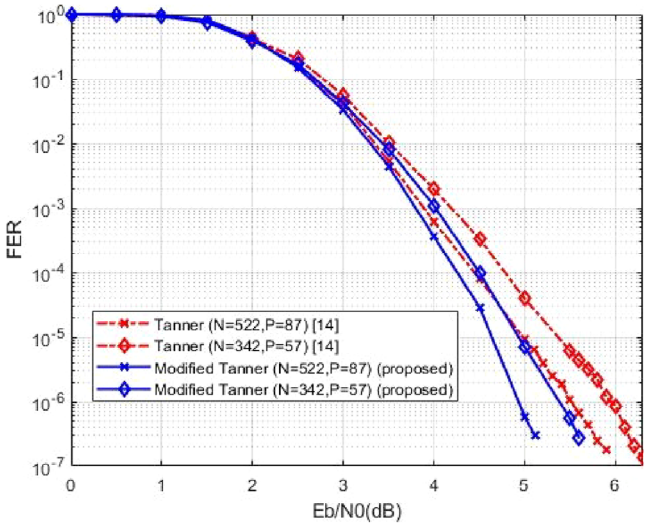

Fig. 2 *Comparison with original codes for NON-prime lifting sizes*

proved. There is not a significant difference in the number of cycles between proposed codes, regardless of whether the lifting size is prime or not. The occurrence of length 10-cycles is somewhat consistent across all the analysed codes in two tables. Figure 2 demonstrates the significance of modifying the code to achieve girth-8 for non-prime lifting sizes, as this modification is an important contribution to the observed performance improvements.

Concluding remarks: This paper presents a modification of Tanner's exponent row structure that allows for the construction of girth-8 LDPC codes with various lifting sizes not restricted to prime numbers. We provide a proof for the values of the lifting size P that induce girth at least 8. Compared to the Golomb ruler construction and truncated version of 5G NR, our modified version of Tanner's work yields some non-trivial coding gain for lengths around 500.

The proposed construction results in the codes with H matrix of size $3P \times nP$ whose column weight is 3, which limits its code rate to be around $\frac{n-3}{n}$, and possibly limits the error performance as well, that could be a good topic of future research especially for short lengths.

The proposed construction itself on the other hand is very simple and clear with H matrix of constant column weight 3. In addition, by allowing its lifting size to be non-prime integers, the proposed code will have all the more options for the code length.

Author contributions: **Wonjun Kim**: Conceptualization; investigation; software; writing—original draft. **Hyunwoo Cho**: Investigation; visualization. **Hong—Yeop Song**: Conceptualization; formal analysis; investigation; methodology; project administration; software; supervision; writing—original draft; writing—review and editing. **Min Kyu Song**: Conceptualization; funding acquisition; investigation; methodology; project administration.

Acknowledgements: This work was supported by the Agency For Defense Development Grant funded by the Korean Government (UD210005SD).

Conflict of interest statement: The authors declare no conflicts of interest.

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

Received: *7 July 2023* Accepted: *4 January 2024*
doi: 10.1049/ell2.13088

References

1 Kabakulak, B., Taşkin, Z.C., Pusane, A.E.: Optimization–based decoding algorithms for LDPC convolutional codes in communication systems. *IISE Trans.* **51**(10), 1061–1074 (2019)
2 3GPP TS 38.212 v16.7.0 release 16, NR; multiplexing and channel coding. https://www.etsi.org/deliver/etsits/138200138299/138212/16.07.0060/ts138212v160700p.pdf (2021)
3 MacKay, D.J.: Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory* **45**(2), 399–431 (1999)
4 Fossorier, M.P.: Quasicyclic low-density parity-check codes from circulant permutation matrices. *IEEE Trans. Inf. Theory* **50**(8), 1788–1793 (2004)
5 Tanner, R.M., Sridhara, D., Sridharan, A., Fuja, T.E., Costello, D.J.: LDPC block and convolutional codes based on circulant matrices. *IEEE Trans. Inf. Theory* **50**(12), 2966–2984 (2004)
6 Li, Z., Chen, L., Zeng, L., Lin, S., Fong, W.H.: Efficient encoding of quasi-cyclic low-density parity-check codes. *IEEE Trans. Commun.* **54**(1), 71–81 (2006)
7 Peterson, W.W., Weldon, E.J.: *Error-Correcting Codes*, 256 pp., 2nd ed. MIT Press, Cambridge, MA (1972)
8 Nguyen, T.B., Nguyen, T.T., Lee, H.: Low-complexity high-throughput QC-LDPC decoder for 5G new radio wireless communication. *Electronics* **10**(4), 516 (2021)
9 Kim, I., Song, H.-Y.: A construction for girth-8 QC-LDPC codes using Golomb rulers. *Electron. Lett.* **58**(15), 582–584 (2022)
10 Kim, S., No, J.-S., Chung, H., Shin, D.-J.: On the girth of Tanner (3,5) quasi-cyclic LDPC codes. *IEEE Trans. Inf. Theory* **52**(4), 1739–1744 (2006)
11 Gholami, M., Mostafaiee, F.: On the girth of Tanner (3,7) quasi-cyclic LDPC codes. *Trans. Comb.* **1**(2), 1–16 (2012)
12 Xu, H., Bai, B., Feng, D., Sun, C.: On the girth of Tanner (3, 11) quasi-cyclic LDPC codes. *Finite Fields Appl.* **46**, 65–89 (2017)
13 Xu, H., Li, H., Feng, D., Zhang, B., Zhu, H.: On the girth of Tanner (3, 13) quasi-cyclic LDPC codes. *IEEE Access* **7**, 5153–5179 (2018)
14 Xu, H., Li, H., Bai, B., Zhu, M., Zhang, B.: Tanner (J, L) quasi-cyclic LDPC codes: Girth analysis and derived codes. *IEEE Access* **7**, 944–957 (2018)
15 Kim, I., Kojima, T., Song, H.-Y.: Some short-length girth-8 QC-LDPC codes from primes of the form $t^2 + 1$. *IEEE Commun. Lett.* **26**(6), 1211–1215 (2022)
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 Kim, D., Kim, I., Cho, H., Song, H.-Y.: Performance of QC-LDPC codes from some new Golomb rulers. In: The 32nd Joint Conference on Communications and Information, Sokcho, Korea (2022)
18 Kim, D., Cho, H., Kim, W., Song, H.-Y.: Analysis of girth and performance of QC-LDPC codes from various Golomb rulers. In: The 33rd Joint Conference on Communications and Information, Yeosu, Korea (2023)