Some Short-Length Girth-8 QC-LDPC Codes From Primes of the Form $t^2 + 1$

Inseon Kim, *Graduate Student Member, IEEE*, Tetsuya Kojima, *Member, IEEE*, and Hong-Yeop Song, *Senior Member, IEEE*

***Abstract*— We propose a simple algebraic construction for girth-8 regular QC-LDPC codes of short lengths, a few hundreds, based on the square matrix from some prime integers of the form $t^2 + 1 = P$ and a multiplication table method. We generalize the conventional multiplication table method in a way that the size T of the circular permutation matrix (CPM) can be different from the modulus M in the calculation of the exponent matrix. We classify and suggest the parameters $P \leq M \leq T$ with $M = kP$ so that the resulting codes have girth 8. In particular, we prove the existence of a threshold T_0 so that the resulting code will always have girth 8 if $T > T_0$ is used, given that $M = kP$. Finally, we present various simulation results and theoretical analysis, one of which shows that the proposed codes of length around 250 have an additional coding gain of about 0.4 dB over the 5G NR LDPC codes.**

***Index Terms*— Regular LDPC codes, QC-LDPC codes, Girth-8 codes, 5G NR channel codes, Algebraic constructions.**

I. Introduction

THE Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) codes is one of the important family of LDPC codes [1] since they have simple encoding and parallel decoding implementation. They were recently adopted as various communications standards for the error-correcting codes, in particular, 5G NR [2], etc. Wireless communication systems such as global navigation satellite systems (GNSS) and 5G ultra-reliable and low latency communication (URLLC) require transmission and reception of short data packets for the reliable and low-latency communications [3], [4]. In this letter, we would like to focus on constructing QC-LDPC codes of short lengths about a few hundreds.

5G NR communication system uses two types of error correcting codes; QC-LDPC codes for the data channel and polar codes for the control channel [2]. For 5G NR LDPC codes, various lengths and rates can be obtained by selecting some submatrices of a given parity-check matrix. For 5G NR polar codes, it is known that some good decoding performance can be obtained if CRC-aided successive cancellation list (CA-SCL) decoding with list size up to 8 [5], [6]. We will compare in this letter the error performance of the proposed codes with some of 5G NR codes (both LDPC and polar) of similar parameters.

Tanner graph is an important tool for design and analysis of QC-LDPC codes. The length of the shortest cycle in its Tanner graph, called girth, is closely related with its error performance. One of the popular constructions for the codes with large girth has been the multiplication table methods [7]–[12]. Tanner proposed constructions using the multiplicative table for the first time [7] and it was verified much later [8] that QC-LDPC codes using Tanner's construction have girth 6. Regular QC-LDPC codes of girth 8 were proposed in [9] and the symmetrical structure was utilized to reduce the search space. Xiao et. al. proposed QC-LDPC codes using Reed-Solomon (RS) parity-check matrix [10] which was using also a multiplication table method. Recently, [11], [12] proposed constructions for girth-8 QC-LDPC codes using a multiplication table and [12] further expanded it into the construction for type-II QC-LDPC codes.

This letter is organized as follows. Section II introduces the square matrix from the primes of the form $t^2 + 1$ and the multiplication table method. Section III describes the proposed construction for girth-8 regular QC-LDPC codes of short lengths, a few hundreds, based on the square matrix from some prime integers of the form $t^2 + 1$ and a multiplication table method. We generalize the conventional multiplication table method in a way that the size T of circular permutation matrix (CPM) can be different from the modulus M in the calculation of the exponent matrix. We present all possible parameters for the proposed QC-LDPC codes for some short lengths up to 500. We also prove the existence of a threshold T_0 on the size T of CPM so that the resulting code will have girth 8 if $T > T_0$ is used. In Section IV, we present various simulation results, one of which shows that the proposed codes of length around 250 have an additional coding gain of about 0.4 dB over the 5G NR LDPC codes of comparable parameters. Section V discusses some concluding remarks.

II. Preliminaries

Let $t \geq 3$ be an integer such that $t^2 + 1 = P$ is a prime. Let α be a primitive root mod P. Then, we may construct a square matrix of size $t \times t$ over the integers mod P as follows:

$$\begin{bmatrix} 1 & \alpha^{t} & \alpha^{2t} & \cdots & \alpha^{(t-1)t} \\ \alpha & \alpha^{t+1} & \alpha^{2t+1} & \cdots & \alpha^{(t-1)t+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{t-1} & \alpha^{2t-1} & \alpha^{3t-1} & \cdots & \alpha^{t^2-1} \end{bmatrix} \tag{1}$$

In this matrix, all the elements are distinct mod P. In our main construction later, we will use its $3 \times n$ submatrix

Manuscript received February 21, 2022; accepted March 6, 2022. Date of publication March 14, 2022; date of current version June 10, 2022. This work was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea Government (MSIT) (No. 2020R1A2C2011969). The associate editor coordinating the review of this letter and approving it for publication was K. Niu. *(Corresponding author: Hong-Yeop Song.)*

Inseon Kim and Hong-Yeop Song are with the School of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, Republic of Korea (e-mail: is.kim@yonsei.ac.kr; hysong@yonsei.ac.kr).

Tetsuya Kojima is with the National Institute of Technology, Tokyo College, Hachioji 193-0942, Japan (e-mail: kojt@tokyo-ct.ac.jp).

Digital Object Identifier 10.1109/LCOMM.2022.3159560

for $P \geq 17$. It is an open problem that there exist an infinitely many primes of the form $t^2 + 1$ [13], [14]. Some known primes P of the form $t^2 + 1$ for small values of t are the followings [13]:

$$(t, P) = (4, 17), (6, 37), (10, 101), (14, 197), (16, 257), \ldots$$

We would like to briefly review the construction for QC-LDPC codes using the multiplication table methods [7], [11]. For some integer P, the first step is to choose two integer sequences $\mathbf{a} = (a_0, a_1, \ldots, a_{m-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$. Next is to construct an exponent matrix $\mathbf{E} = [e(i, j)]$ with $e(i, j) = a_i b_j \pmod{P}$. Finally, a parity-check matrix $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ is obtained by substituting CPM shifted by $e(i, j)$ into $\mathbf{E}$. Usually the size of CPM has been selected to be P which is the modulus in the calculation of $e(i, j)$ above. The condition for the existence of a $2c$-cycle [1] now becomes

$$\sum_{l=0}^{c-1} (e(i_l, j_l) - e(i_l, j_{l+1})) \equiv 0 \pmod{P} \tag{2}$$

for some $i_0, i_1, \ldots, i_{c-1}$ and $j_0, j_1, \ldots, j_c$ where $j_0 = j_c$, $i_l \neq i_{l+1}$ and $j_l \neq j_{l+1}$ for $0 \leq l \leq c - 1$. We note here that the modulus must be the same as the size of CPM.

In 2004 [7], Tanner *et al.* have used $\mathbf{a} = (1, c, c^2, \ldots, c^{m-1})$ and $\mathbf{b} = (1, d, d^2, \ldots, d^{n-1})$ where c and d are elements of order m and n, respectively, where m and n are some divisors of $P - 1$ for some prime P. Recently, Kim and Song [11] have used top three rows of the matrix (1) with CPM size $T = P, P + 1, \ldots$ and constructed some QC-LDPC codes of girth 8. The girth property was checked only by computer in a case-by-case manner. In this letter, we will use some $3 \times n$ submatrix of (1) and generalize the calculation of the exponent matrix using modulus $M = kP$ for some positive integer k, further generalize the construction of $\mathbf{H}$ by using the CPM of size $T \geq M$ and finally investigate the girth property of the resulting codes in detail. In some sense, therefore, this letter is a full generalization of [11] in the construction steps as well as in the investigation of their girth property.

III. Main Constructions and Girth Property

We first propose an algebraic construction for QC-LDPC codes based on the square matrix (1). Then, we discuss various parameters of the resulting codes, and investigate various conditions for girth-8 in detail. In the following, $(x)_K$ is the unique integer in the range from 0 to $K - 1$ that is congruent to x mod K.

Main construction:

1) Let $P = t^2 + 1$ be a prime with $t \geq 3$, α be a primitive root mod P and consider the square matrix of size $t \times t$ as shown in (1).
2) For some $n \leq t$, choose any $3 \times n$ submatrix of (1) consisting of three consecutive rows, and denote it by $\mathbf{D} = [d(i, j)]$, where $i = 0, 1, 2$ and $j = 0, 1, \ldots, n - 1$.
3) Construct the $3 \times n$ exponent matrix $\mathbf{E} = [e(i, j)]$ by keeping the left-most column and the top row of $\mathbf{D}$ and then using the multiplication table method. That is, for all i and j we use $e(i, 0) = (d(i, 0))_P$ and $e(0, j) = (d(0, j))_P$, and finally
$$e(i, j) = (e(i, 0)e(0, j))_M$$
for $M = kP$ for some integer $k > 0$.
4) The parity-check matrix $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ is now obtained by substituting $e(i, j)$-shifted CPM of size T, for some $T \geq M$.

TABLE I

Some Parameters of Main Construction

target rate	target length	(n, T)	(t, P)	$M = kP \leq T$
1/4	$200 = 2^3 5^2$	(4,50)	(4,17)	17,34
			(6,37)	37
	$300 = 2^2 3 5^2$	(4,75)	(4,17)	17,34,51,68
			(6,37)	37,74
	$400 = 2^4 5^2$	(4,100)	(4,17)	17,34,51,68,85
			(6,37)	37,74
	$500 = 2^2 5^3$	(4,125)	(4,17)	17,34,..., 119
			(6,37)	37,74,111
			(10,101)	101
2/5	$200 = 2^3 5^2$	(5,40)	(6,37)	37
	$250 = 2 5^3$	(5,50)	(6,37)	37
	$300 = 2^2 3 5^2$	(5,60)	(6,37)	37
	$350 = 2 5^2 7$	(5,70)	(6,37)	37
	$400 = 2^4 5^2$	(5,80)	(6,37)	37,74
	$450 = 2 3^2 5^2$	(5,90)	(6,37)	37,74
	$500 = 2^3 5^3$	(5,100)	(6,37)	37,74
1/2	$300 = 2^2 3 5^2$	(6,50)	(6,37)	37
	$450 = 2 3^2 5^2$	(6,75)	(6,37)	37,74

TABLE II

Threshold E_b/N_0 of the Proposed Codes by Density Evolution

$(3, n)$	target rate	threshold E_b/N_0
(3,4)	1/4	1.07 dB
(3,5)	2/5	0.97 dB
(3,6)	1/2	1.16 dB

Theorem 1: Main construction above gives a parity-check matrix $\mathbf{H}$ *of a* $(3, n)$ *regular QC-LDPC code of length* nT *and rate* $\geq (n - 3)/n$.

The regular QC-LDPC codes of various lengths and rates can be obtained by selecting the parameters (P, M, T). In the rest of this letter, we will consider the first three rows and first n columns of (1) in Step 2) of Main construction without loss of generality.

The target length must be of the form $L = nT$ where n is the number of columns of $\mathbf{E}$ and T is the size of CPM. We have the target rate $\approx (n - 3)/n$ and we must find an integer $t \geq n$ such that $t^2 + 1 = P$ is a prime and $P \leq T$. Divide T by P and obtain $T = qP + r$. Then $M = kP$ for $k = 1, 2, \ldots, q$ are all possible values of M. We list all these cases for the target lengths $L = 200, 250, 300, 350, 400, 450$ and 500 in Table I. We note that only three pairs $(t, P) = (4, 17), (6, 37)$ and $(10, 101)$ are used in the table.

Remark 1: In all cases shown in Table I, the codes are $(3, n)$ *regular, with values of* n *equals to only* $4, 5,$ *or 6, which* *are in fact the constant degrees of check-nodes. Together with the target rate, this determines threshold value of E_b/N_0 (from density evolution) shown in Table II. [15]*

We will now investigate various conditions for the resulting codes to have girth 8. We have checked by computer the girth of all the codes in Table I and those of lengths less than 200 mentioned above. As we have noted earlier, when $n < t$, we use the left-most n columns and top 3 rows in Step 2). Further, we use $\alpha = 5$ for $P = 17$ and $\alpha = 2$ for $P = 37$ and 101. First, all the codes in Table I turn out to have girth at least 8. For the lengths less than 200, lots (but not all) of cases have girth 8, which will be described in the remaining of this section.

Remark 2: Let $P = t^2 + 1$ be a prime with some $t = n \geq 3$ and α be a primitive root mod P. Assume that $T = M = P$ in Main construction. Then, $\mathbf{E} = \mathbf{D}$ and the elements are all distinct mod M. This rules out the existence of a 4-cycle. Furthermore, when

$$(P, \alpha) = (17, 5), (37, 2), (101, 2), (197, 2), (257, 13), \quad (3)$$

we check that all the regular QC-LDPC codes from Main construction do not have a 6-cycle. This takes care of the cases when $T = M = P$.

The next case is when $T = M = kP$ for some positive integer $k > 1$. It is obvious that if $x \not\equiv 0 \pmod{P}$ then $x \not\equiv 0 \pmod{kP}$. This gives the following:

Remark 3: For the parameters (P, α) listed in (3), it is not difficult to show that, when we change the parameters $T = M = kP$ for any positive integer $k \geq 1$, the resulting code of Main construction does not have 4-cycles and 6-cycles.

In the remaining of this section, we consider the final and most general case when $T \geq M = kP$.

Remark 4: Main construction is a generalized version of the multiplication table method in that the modulus M in the calculation of $\mathbf{E}$ and the size T of CPM in $\mathbf{H}$ can be different. When they are different, the condition (2) has to be computed mod T (instead of mod M or P).

Note that it is enough to consider the case of $n = t$ as long as the girth of the resulting code is concerned. For the parameters $(t, P) = (4, 17)$, the lengths of the resulting codes are multiples of 4 from 68, corresponding to the CPM size $T = 17, 18, \ldots$. Among these, we check that the cases of $T = 17, 21, 25, 26$ and all $28 \leq T \leq 10000$ have girth at least 8. For the parameters $(t, P) = (6, 37)$, the lengths of the resulting codes are multiples of 6 from 222, corresponding to the CPM size $T = 37, 38, \ldots$. Surprisingly, we found that the cases of all $37 \leq T \leq 10000$ have girth at least 8. From these results, we are able to prove that there exists a lower bound T_0 such that the resulting codes all have girth at least 8 whenever $T > T_0$ for (t, P) if (P, α) listed in (3) is used.

Lemma 1: Let $P = t^2 + 1$ be a prime with $t \geq 3$, and let α be a primitive root mod P. For (P, α) listed in (3), the QC-LDPC codes from Main construction have girth 8 if

$$T > T_0 = \left(2 \max\{(\alpha)_P, (\alpha^2)_P\} + 1\right)(P - 1), \quad (4)$$

where $0 \leq (x)_K < K$ is the integer congruent to x mod K, which are shown in Table III.

TABLE III
SOME THRESHOLD VALUES T_0 FROM LEMMA 1

(P, α)	(17, 5)	(37, 2)	(101, 2)	(197, 2)	(257, 13)
T_0	272	324	900	1764	86784

We recall that the cases of $28 \leq T \leq 272$ for $(P, \alpha) = (17, 5)$ and $37 \leq T \leq 324$ for $(P, \alpha) = (37, 2)$ have been checked by computer. This computer check and Lemma 1 gives the following:

Theorem 2: Assume that we use (P, α) in (3) and let T_0 be the integer given in (4). Then, Main construction with $(P, M = kP, T > T_0)$ gives a QC-LDPC code of girth at least 8. Furthermore, it gives a girth-8 code when $T \geq 28$ for $(P, \alpha) = (17, 5)$ and $T \geq 37$ for $(P, \alpha) = (37, 2)$.

Now, we will prove Lemma 1. We have to show that Tanner graph of $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ from Main construction does not have 4-cycles and 6-cycles.

Consider the case of 4-cycles. We know that there exists a 4-cycle if

$$\begin{aligned} & e(0,i) - e(0,j) + e(1,j) - e(1,i) \equiv 0 \pmod{T}, \\ \text{or } & e(0,i) - e(0,j) + e(2,j) - e(2,i) \equiv 0 \pmod{T}, \\ \text{or } & e(1,i) - e(1,j) + e(2,j) - e(2,i) \equiv 0 \pmod{T} \quad (5) \end{aligned}$$

for some $0 \leq i \neq j < n$.

We will concentrate on the first relation in (5). Its LHS can be easily upper-bounded by $2(M - 1)$ since every term is an integer less than $M = kP$.

$$\begin{aligned} e(0,i) - e(0,j) + e(1,j) - e(1,i) &< e(0,i) + e(1,j) \\ &< 2(M - 1). \quad (6) \end{aligned}$$

In fact, we note that $e(0, i)$ is an integer less than P. Note also that $e(1, j) = (\alpha e(0, j))_M$ and the product of $(\alpha)_P$ and $e(0, j)$ cannot be bigger than $M = kP$ if k is large enough. In this case, we may have

$$e(1, j) \leq (\alpha)_P e(0, j) \leq (\alpha)_P (P - 1).$$

Combining these two upper-bounds, if k is large enough,

$$\begin{aligned} & e(0,i) - e(0,j) + e(1,j) - e(1,i) \\ & \quad < e(0,i) + e(1,j) \\ & \quad < P - 1 + (\alpha)_P(P - 1) = ((\alpha)_P + 1)(P - 1). \end{aligned}$$

Similarly, by upper-bounding the LHS of the second and third relations in (5), we have

$$\begin{aligned} e(0,i) - e(0,j) + e(2,j) - e(2,i) &< ((\alpha^2)_P + 1)(P - 1), \\ e(1,i) - e(1,j) + e(2,j) - e(2,i) &< ((\alpha)_P + (\alpha^2)_P)(P - 1), \end{aligned}$$

for any $i \neq j$ and if k is large enough. Finally, combining all three together, we have the overall upper-bound T_0 in (4) of the LHS of any of the three relations in (5).

How large is the value k for the above bounds? It is not difficult to show that the upper-bound is true when

$$k \geq \max\{(\alpha)_P, (\alpha^2)_P\}.$$

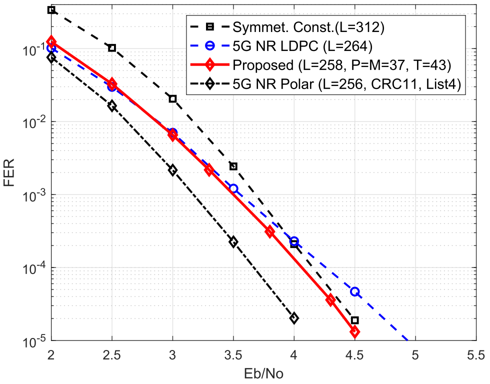

Fig. 1. Performance comparison of some half-rate codes.

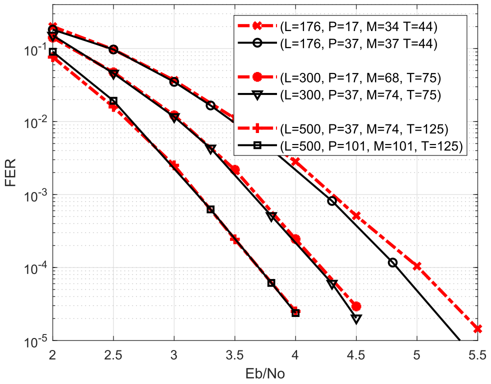

Fig. 2. Performance of some proposed codes of target rate $1/4$.

For k less than this value, we simply use the upper bound $2(M-1)$ in (6). Now, it is straightforward to show that $2(M-1)$ is less than T_0 in this case.

Finally, Remark 3 in which $T = M = kP$ implies that, for any $i \neq j$, the LHS of the relations in (5) cannot be 0 mod T or mod kP. This implies that the LHS of the relations in (5) cannot be 0.

Therefore, all three relations (5) cannot be satisfied if $T > T_0$ where T_0 is given in (4). This takes care of the non-existence of a 4-cycle.

Now, consider the case of 6-cycles. We know that there exists a 6-cycle if

$$e(0,i) - e(0,j) + e(2,j) - e(2,l) + e(1,l) - e(1,i) \equiv 0 \pmod{T}$$

for some three distinct indices i, j and l. This case can be taken care of easily and in the same manner as the case of 4-cycles. This finishes the proof of Lemma 1.

Remark 5: The complexity of Main construction with Theorem 2 is very low in that one has to calculate $3n$ elements $\mathbf{E}$ *and $3n$ substitutions of CPMs for* $\mathbf{H}$*. Therefore, the computational complexity is almost negligible compared with the cases in which* one has to check in addition the girth conditions exhaustively *when constructing the exponent matrix* $\mathbf{E}$ *in most of the previous reports [7]–[12], without which there is no guarantee of girth at least 8.*

IV. Performance of the Proposed Codes

In this section, we analyze the performance of the proposed codes using sum-product decoding with the maximum 50 iterations under the additive white Gaussian noise (AWGN) channel and binary phase shift keying (BPSK) modulation.

We first compare the performance of the proposed code of length around 250 with some other LDPC codes and a polar code in Fig.1. The half-rate 5G NR QC-LDPC code has length 264 [2] and it shows an error-floor after FER $< 10^{-3}$. It is also known that it has girth 6 [16]. The proposed code of girth 8 and target rate $1/2$ with $(P, M, T) = (37, 37, 43)$ has length 258 (the exact rate 0.508) and shows no error-floor until FER $> 10^{-5}$ and an additional coding gain of about 0.4 dB over the 5G NR LDPC code at FER 10^{-5}. The half-rate girth-8 QC-LDPC code from the symmetrical construction [9] has length 312 that is much larger than 258, but with much worse performance than the proposed code. The half-rate 5G NR polar code with CA-SCL decoding [5] has comparable length 256 with the proposed code and performs well better with a coding gain of 0.4 dB relative to the proposed code at FER 10^{-5}. It would be an interesting future work to investigate further this comparison of LDPC codes and polar codes, both of short lengths.

TABLE IV
Cycle Distribution, Minimum Distance and Rate

L	Opt.d_{min}	P	rate	$\hat{d}_{\text{min}}$	Cycle Distribution
500	< 192	37	0.262	112	$125x^8 + 500x^{10} + 5000x^{12}$
		101*	0.254	120	$500x^{10} + 5625x^{12}$
300	< 116	17	0.277	50	$225x^8 + 300x^{10} + 4500x^{12}$
		37*	0.277	54	$75x^8 + 450x^{10} + 4150x^{12}$
176	46-62	17	0.295	8	$242x^8 + 704x^{10} + 3080x^{12}$
		37*	0.272	24	$176x^8 + 572x^{10} + 3256x^{12}$

We simulate the performance of the proposed codes of lengths 176, 300 and 500. For each of these lengths, multiples parameters can be selected with target rate $1/4$, and selected the best two choices as shown in Fig. 2. We have determined the cycle distributions, minimum distances and the exact rates of all these six codes and presented in Table IV. Here, the code with bigger P (with * in the table) becomes slightly better.

In Table IV, $\sum_{i \geq i_0} g_i x^i$ implies that the code has g_i i-cycles in its Tanner graph for $i \geq i_0$. Due to the space limitation we show only the terms for $i \leq 12$ here. Note that the code of length 500 constructed with $P = 101$ has girth 10. The minimum distance was estimated by calculating some small but random portions of the codewords. It is interesting that the values here are much less than those of the optimal linear codes reported in various sources. For example, the minimum distance of an optimum $[176, 44]$ linear code is known to be $46 \sim 62$ [17, p.336]. For the lengths 300 and 500, we were able to find only an upper bound using MAGMA. It seems that the performance is not much related with the minimum distance considering the decoding algorithm. The exact rate turned out be slightly increased from the target rate. For practical application, this will not be any problem since, for

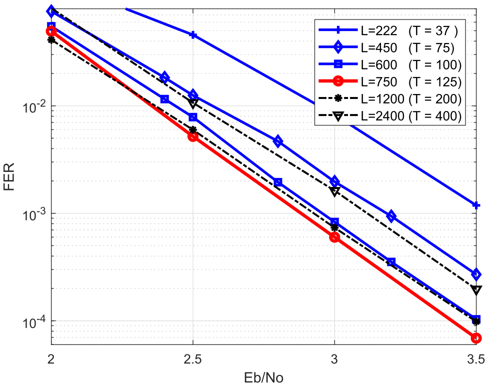

Fig. 3. Performance of QC-LDPC codes for $M = P = 37$ as T increases.

example, some number of zero-padding or puncturing can be used.

Remark 6: We present in Figs. 1 and 2 the performance of those codes with FER $> 10^{-5}$. *It is evident to see that the proposed codes show no error floor phenomenon in this range.*

Finally, we would like to discuss and present some trend of Main construction for given parameters P and M as T gets larger and larger. This is one key contribution of this letter that T can be any larger than M or P for large lengths, hoping that the performance gets better and better. It turned out that it is NOT true that increasing T gives better and better performance. On the other hand, we found that the performance increases for a while and then decreases after some value of T. We may conjecture that there exists an optimal value of T for the best performance. The evidence is shown in Fig. 3. All these curves are the performance of the half-rate and girth-8 codes with parameters $M = P = 37$ ($t = n = 6$) and 3×6 exponent matrices. Therefore, the length is given as $L = 6T$ for each T in the figure. It would be interesting to find the optimal value of T for the performance and its relation with the lower bound T_0 for girth-8 as in Lemma 1 and Theorem 2.

V. Concluding Remarks

In this letter, we propose a simple algebraic construction for girth-8 regular QC-LDPC codes of short lengths, a few hundreds, based on the square matrix from some prime integers of the form $t^2 + 1$ and a multiplication table method. We generalize the conventional multiplication table method in a way that the size T of CPM can be much larger than the modulus M in the calculation of the exponent matrix. Various parameters of the resulting codes are determined and the performance of some example codes are simulated and compared with various other codes with FER up to 10^{-5}. Threshold E_b/N_0, minimum distance, cycle distribution and exact rates of these codes are investigated.

We note that one could choose M as any integer between P and T. In fact, [11] uses $M = P$ and $T = P, P+1, P+2, \ldots$ without any guarantee that the girth of the resulting code is at least 8, except for the case-by-case computer check. We didn't mention in this letter, but we have also constructed lots of codes for some values of $P < M < T$, with values of M other than kP, and found that the performances are very much similar whenever the girth is at least 8. The choice $T = M = kP$ gives an advantage that the resulting code is easily shown to have girth at least 8 if the code from $T = M = P$ has girth at least 8 (Remark 3). Finally, we choose $M = kP$ with (P, α) in (3) and $T > T_0$ for the guarantee of the girth 8 (Theorem 2).

The performance of the proposed regular QC-LDPC code is slightly worse than those of 5G NR polar code (Figure 1). Various efforts to improve the performance of the QC-LDPC codes would be also an interesting future work.

References

[1] M. P. C. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[2] *NR: Multiplexing Channel Coding (Release16)*, document TS 38.212 v16.7.0, 3GPP, 2021.

[3] G. Durisi *et al.*, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[4] B. Li, Z. Zhang, N. Zang, and S. Wang, "High-precision GNSS ocean positioning with BeiDou short-message communication," *J. Geodesy*, vol. 93, no. 2, pp. 125–139, Feb. 2019.

[5] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.

[6] S. Nagata, *Final Report of 3GPP TSG RAN WG1 AH1 NR v1.0.0*, document R1-1701553, 3GPP, Jan. 2017, p. 80.

[7] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, Jr., "LDPC block and convolutional codes based on circulant matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

[8] G. Zhang, Y. Hu, D. Ren, Y. Liu, and Y. Yang, "Type-II QC-LDPC codes from multiplicative subgroup of prime field," *IEEE Access*, vol. 8, pp. 142459–142467, 2020.

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

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

[11] I. Kim and H.-Y. Song, "A simple construction for QC-LDPC codes of short lengths with girth at least 8," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 1462–1465.

[12] I. Kim and H.-Y. Song, "Some new constructions of Girth-8 QC-LDPC codes for future GNSS," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 3780–3784, Dec. 2021.

[13] *The On-Line Encyclopedia Integer Sequences: Primes Form* k^{2+1}. Accessed: Nov. 7, 2021. [Online]. Available: https://oeis.org/A002496

[14] P. Ribenboim, *The Little Book of Bigger Primes*, 2nd ed. New Work, NY, USA: Springer, 2004.

[15] S. J. Johnson, "Reported thresholds and BER performance for LDPC and LDPC-like codes," Dept. Elect. Comput. Eng., Univ. Newcastle, Tyne, U.K., Tech. Rep. SPM855, 2012.

[16] H. Li, B. Bai, X. Mu, J. Zhang, and H. Xu, "Algebra-assisted construction of quasi-cyclic LDPC codes for 5G new radio," *IEEE Access*, vol. 6, pp. 50229–50244, 2018.

[17] V. Pless, R. A. Brualdi, and W. C. Huffman, *Handbook Coding Theory*, vol. 1. Amsterdam, The Netherlands: Elsevier, 1998, p. 336.