Some New Constructions of Girth-8 QC-LDPC Codes for Future GNSS

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

***Abstract*— In this letter, we propose a new construction of girth-8 Quasi-Cyclic Low-Density Parity-Check codes (QC-LDPC) with various lengths for the global navigation satellite systems (GNSS). This scheme combines two steps. The first is the construction of a family of regular girth-8 QC-LDPC codes of various lengths and rates with two designed sequences. The second is the performance improvement of those from the first construction of half-rate cases using a proposed weight matrix so that the result becomes type-II QC-LDPC codes. This results in some final codes with short lengths of 600, 1200, and 1800, especially for future GNSS. We performed a simulation and confirmed that the proposed QC-LDPC codes of lengths 600 and 1200 have an additional coding gain about 0.3 dB at frame error rate 10^{-5} over the LDPC codes used in the Global Positioning System.**

***Index Terms*— QC-LDPC codes, protograph, Type-II QC-LDPC codes, GNSS.**

I. Introduction

THE reliable transmission of the global navigation satellite system (GNSS) message is an essential requirement affecting the service quality of the GNSS receivers. The Global Positioning System (GPS) is a representative of GNSS, and it has three message types; legacy navigation (LNAV), civil navigation (CNAV) and CNAV-2. CNAV is a message structure proposed for civilian L2C and L5 signals in the modernized GPS [1]. The CNAV message format is known to be more flexible than that of LNAV [16].

Various types of error-correcting codes (ECC) were adopted to increase the reliability of GNSS signal transmission and reception. The half-rate $(171, 133)_8$ convolutional code is the most widely used in the GNSS standards [6]. In addition, Reed-Solomon (RS) codes as well as low-density parity-check (LDPC) codes were also applied to some GNSS standards [2], [3]. Recently, some RS codes combined with orthogonal modulations are designed for future GNSS [5]. Quasi-cyclic LDPC (QC-LDPC) codes [8] have attracted the attention from many researchers in mobile communications in large because the decoder can be implemented with parallel operations.

For QC-LDPC codes, one famous approach is to construct first an $M \times N$ exponent matrix $\mathbf{E} = [e(i,j)]$ and then to substitute some circulant permutation matrices (CPM) into $e(i,j)$ for the final parity check matrix of size $MP \times NP$, where P is the size of the CPM. The multiplication table method is generally used for the shape of the exponent matrix $\mathbf{E} = [e(i,j)] = [a_i b_j]$, where the sequences a_i and b_j should be appropriately designed [4], [9], [10], [14], [15], [17], [18], [20]. A series of constructions [18], [20] for two sequences a_i's and b_j's using the greatest common divisor (gcd) constraint were proposed for girth 8. A construction for girth-8 QC-LDPC codes with column multiplier was proposed [15]. The construction of RS based QC-LDPC codes was proposed [17]. Their exponent matrices are also some multiplication tables. [14] and [4] obtained some QC-LDPC codes with girth 8 using the multiplication table approach with additional all-zero left-most column and all-zero top-row, which is called 'sequentially multiplied columns' (SMC) method. Another simple construction of QC-LDPC codes of girth 8 was also proposed [10]. Here, a $3 \times t$ exponent matrix is constructed over $GF(P)$ with a prime $P = t^2 + 1$.

A protograph is a bipartite graph allowing some multiple edges. The QC-LDPC codes can be treated as a special case of protograph LDPC codes [7]. In this sense, we could construct type-II QC-LDPC codes with at most double edges [19]. Construction of type-II RS-based QC-LDPC codes (girth-8) was proposed for better performance [9]. Type-II means that at most double edges can appear in its protographs. Constructing type-II QC-LDPC codes with cyclic difference set sequences was proposed [19]. The conditions for the non-existence of 4-cycles and 6-cycles for type-II or multi-edge type QC-LDPC codes are considered in [12], [13], and [19].

In this letter, we propose a new construction of girth-8 QC-LDPC codes for CNAV message structure. This scheme combines two steps. The first is the construction of a family of regular girth-8 QC-LDPC codes of various lengths and rates with two designed sequences. The second is the performance improvement of those from the first construction of half-rate cases using a proposed weight matrix so that the result becomes type-II QC-LDPC codes. This results in some final codes with short lengths of 600, 1200, and 1800. We performed a simulation and confirmed that the proposed QC-LDPC codes of lengths 600 and 1200 have an additional coding gain about 0.3 dB at FER 10^{-5} over the LDPC codes used in the GPS.

This letter is organized as follows. Section II describes the main construction for girth-8 QC-LDPC codes in two steps. Section III shows the proposed QC-LDPC codes for future GNSS and their simulation results. Final section concludes the letter with some interesting open problems.

II. Proposed Construction for QC-LDPC Codes

We propose a combined approach of the construction for QC-LDPC codes as discussed in Introduction. We

Manuscript received August 15, 2021; revised September 15, 2021; accepted October 7, 2021. Date of publication October 14, 2021; date of current version December 10, 2021. This work was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea Government (MSIT) (No. 2020R1A2C201196912). The associate editor coordinating the review of this letter and approving it for publication was K. Niu. *(Corresponding author: Hong-Yeop Song.)*

The authors 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).

Digital Object Identifier 10.1109/LCOMM.2021.3120106

Fig. 1. Patterns of a cycle of length 4 and length 6 in construction 1.

designed two sequences satisfying some specific conditions for avoiding 4-cycles and 6-cycles to construct an exponent matrix. Then, the parity-check matrices of QC-LDPC codes will be obtained by substituting some appropriate CPMs. The resulting QC-LDPC codes of girth 8 still have to be modified for better performance. We extend our methods to construction final girth-8 type-II QC-LDPC codes.

A. The First Step: Construction With Girth at Least 8

Let M, N and P be some integers with $M < N < P$. We consider an exponent matrix $\mathbf{E} = [e(i,j)]$ of size $M \times N$. Then, a binary QC-LDPC code is the null space of an $MP \times NP$ parity-check matrix $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$, where $\mathbf{H}_{e(i,j)}$ is the $P \times P$ identity matrix cyclically shifted by $e(i,j)$ for $i = 0, 1, \ldots, M-1$ and $j = 0, 1, \ldots, N-1$. Here, $\mathbf{H}_{e(i,j)}$ is called a CPM. The resulting QC-LDPC code will have the rate at least $\frac{N-M}{N}$ and the length NP.

There have been several approaches to design $\mathbf{E} = [e(i,j)]$. We use $e(i,j) = a_i b_j$ with some pre-designed integer sequences a_i's and b_j's for $i = 0, 1, \ldots, M-1$ and $j = 0, 1, \ldots, N-1$. In this case, we take the remainder after $a_i b_j$ is divided by P so that $0 \le e(i,j) < P$ for all i, j.

For the constructed QC-LDPC codes from $\mathbf{E}$ with CPM's of size P, the necessary and sufficient condition for the existence of a cycle of length $2c$ [8] becomes

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

for some sequences $a_{i_0}, a_{i_1}, \ldots, a_{i_{c-1}}$ and $b_{j_0}, b_{j_1}, \ldots, b_{j_c}$, where $b_{j_0} = b_{j_c}$, $a_{i_l} \neq a_{i_{l+1}}$ and $b_{j_l} \neq b_{j_{l+1}}$ for $0 \le l \le c-1$.

For the case of cycles of length 4 in Tanner graph of $\mathbf{H}$, the condition for the existence becomes $(a_i - a_j)(b_x - b_y) \equiv 0 \pmod{P}$ for some a_i, a_j, b_x and b_y where $0 \le i < j < M$ and $0 \le x < y < N$. Therefore, it would be a good initial choice for a_i's all distinct mod P and b_j's all distinct mod P as well. We note that this is not sufficient for the non-existence of a 4-cycle. The sufficient condition is the negation of (1) when $c = 2$ for all a_i's and b_j's.

The second figure of Figure 1 shows a possible pattern of a cycle of length 6 in a $3P \times 3P$ submatrix of the parity-check matrix $\mathbf{H}$. For the case of cycles of length 6 in Tanner graph of $\mathbf{H}$, the condition for the existence of a 6-cycle becomes (1) when $c = 3$ for all a_i's and b_j's. The final result contains six relations, one of which is given as $(a_i - a_j)(b_x - b_y) + (a_j - a_k)(b_x - b_z) \equiv 0 \pmod{P}$ for some a_i, a_j, a_k and b_x, b_y, b_z.

Construction 1: For any positive integers M, N and P with $M < N < P$, we proceed as follows:

1) *Find two integer sequences* $\mathbf{a} = (a_0, a_1, \ldots, a_{M-1})$ *and* $\mathbf{b} = (b_0, b_1, \ldots, b_{N-1})$ *satisfying the conditions which are negations of* (1) *for* $c = 2$ *and 3, and also* $a_0 < a_1 < \cdots < a_{M-1}$ *and* $b_0 < b_1 < \cdots < b_{N-1}$.
2) *Choose* m *and* n *with* $1 \le m \le M$ *and* $m < n \le N$.
3) *Pick up* m *terms from* $\mathbf{a}$ *and* n *terms from* $\mathbf{b}$ *with order preserved (and re-index the terms if it is necessary) and obtain two sequences* $(a_0, a_1, \ldots, a_{m-1})$ *and* $(b_0, b_1, \ldots, b_{n-1})$, *which become also increasing sequences of integers.*
4) *Choose a positive integer* K, *and construct* $\mathbf{E} = [e(i,j)]$ *with*

$$e(i,j) = a_i b_j \pmod{KP}. \tag{2}$$

and $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ *by substituting CPM's of size* KP *appropriately.*

Then we have a regular rate $(n-m)/n$ *girth-8 QC-LDPC code of length* nKP *and dimension* mKP *as a null space of* $\mathbf{H}$.

Remark 1: Note that the exponent matrix $\mathbf{E} = [e(i,j)]$ *will result in a QC-LDPC code of girth at least* 8 *when* $K = 1$. *It seems to be not obvious to check that* $\mathbf{E} = [e(i,j)]$ *with* $K > 1$ *also result in those of girth at least 8. We would like to emphasize that the above two exponent matrices are different since* $e(i,j) = a_i b_j$ *is now computed mod* KP. *We claim that if* $\mathbf{E} = [e(i,j)]$ *computed mod* P *satisfies the condition in Step 1) of the construction, then those computed mod* KP *also satisfies the similar condition mod* KP.

Proof: If $(a_i - a_j)(b_k - b_l) \equiv 0 \pmod{KP}$ *for some* a_i, a_j, b_k *and* b_l, *then* $(a_i - a_j)(b_k - b_l) = KPq \equiv 0 \pmod{P}$. *This takes care of the non-existence of 4-cycles. The 6-cycles can be treated similarly.*

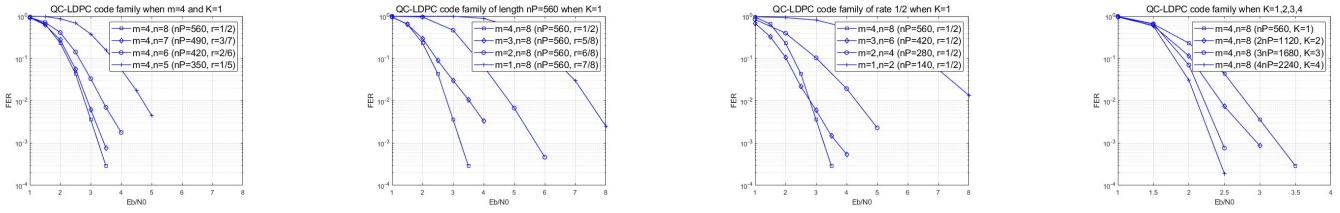
Example 1: For $M = 4$, $N = 8$ *and* $P = 70$, *we found* $\mathbf{a} = (1, 2, 3, 4)$ *and* $\mathbf{b} = (2, 9, 17, 22, 26, 31, 39, 46)$ *according to Step 1) of Construction 1. Table I shows the rates and lengths of constructed girth-8 QC-LDPC codes family using* $\mathbf{a}$ *and* $\mathbf{b}$ *and various shortened sequences of length* m *and* n *when* $P = 70$ *(*$K = 1$*). Another family can also be obtained from Step 4) of Construction 1 when* $K = 1, 2, 3, 4$.

TABLE I
RATES AND LENGTHS OF CODE FAMILY IN EXAMPLE 1

length	560	490	420	350	280	210	140
m \ n	8	7	6	5	4	3	2
4	4/8	3/7	2/6	1/5			
3	5/8	4/7	3/6	2/5	1/4		
2	6/8	5/7	4/6	3/5	2/4	1/3	
1	7/8	6/7	5/6	4/5	3/4	2/3	1/2

Figure 2 shows the performance of some selected girth-8 QC-LDPC codes family of Example 1. Figure 2a shows the FER performance of the codes with $m = 4$ fixed and n taking values from 8 to 5 so that the rate changes from $1/2$ to $1/5$. Observe that the length becoming shorter affects more than the rate becoming smaller in this case. Figure 2b shows the FER performance of the codes with $n = 8$ fixed and m taking values from 4 to 1 so that the rate changes from $1/2$ to $7/8$. Here, the length is fixed to be $nP = 560$. As m gets smaller, the rate gets higher and the performance becomes worse as expected. Figure 2c shows the FER performance of the codes of rate $1/2$ fixed with various combinations of m and n. As m and n get smaller, the performance becomes worse, and we guess it is because the code length becomes smaller.

Remark 2: We would like to note that the performance remains the same for any selection of $m < M$ *terms from* $\mathbf{a} = (1, 2, 3, 4)$. *For example, for* $m = 2$, *the selections are* $(1, 2)$, $(1, 3)$ *or* $(1, 4)$, *etc. We have checked by simulation that*



(a) (b) (c) (d)

Fig. 2. Performance of some selected cases in example 1 from construction 1.

all these have the same or similar performance. We believe that the same is true for any selection of $n < N$ terms from $\mathbf{b}$.

Figure 2d shows the FER performance of the codes with $\mathbf{a}$ and $\mathbf{b}$ designed in Example 1 with KP when $P = 70$ and $K = 1, 2, 3$, and 4. As the value of KP becomes larger, the length gets larger. Therefore, it would be reasonable to suspect that the performance gets better as K gets larger. We discuss this in the following remark.

Remark 3: We have checked by simulation that the performance gets better as K gets larger until $K = 4$ and then it gets worse for $k = 5, 6$ and 9. This made us to wonder if one can conclude that there exists a value K such that the FER performance is the best for given $\mathbf{a}$ *and* $\mathbf{b}$ *in Step 3) of the construction with P. We guess that such a value might be around the minimum of a_{m-1} and b_{n-1} in Step 3) of the construction.*

B. The Second Step: Construction of Half-Rate Type-II QC-LDPC Codes With Girth 8

The proposed girth-8 QC-LDPC codes using two designed sequences in Section II-A are (m, n) regular LDPC codes. In the sense that (m, n) regular QC-LDPC codes can be treated as all-1 protograph of size $m \times n$, we could construct a protograph with at most double edges for a girth-8 type-II QC-LDPC codes in order to improve the error performance. For this, the weight matrix of a protograph should be the same as the size of the exponent matrix constructed in the previous section.

A weight matrix $\mathbf{W} = [w(i, j)]$ of a protograph for type-II QC-LDPC codes is an $m \times n$ matrix of $0, 1$ or 2. We propose the weight matrix $\mathbf{W} = [w(i, j)]$ for half-rate type-II QC-LDPC codes with $n = 2m$ as follows;

$$\mathbf{W} = \begin{bmatrix} 1 & 1 & & & 2 & 1 & \cdots & 1 \\ & 1 & 1 & & 1 & 2 & \cdots & 1 \\ & & \ddots & & \vdots & \vdots & \ddots & \vdots \\ 1 & & \cdots & 1 & 1 & 1 & \cdots & 2 \end{bmatrix} \tag{3}$$

where the blank represents 'zero.' Note that every variable node on the left-half side has degree 2. The right-half side has 2 on the diagonal and 1 otherwise. Thus, every variable node on the right-half side has degree $m + 1$.

It is well-known that the error performance of the QC-LDPC codes can be improved by the graphical shape of the protograph. If a QC-LDPC code is generated by the protograph whose subgraph of all degree-2 variable nodes are cycle-free, then it has error performance that falls double exponentially [11]. For this, we design the length of the walk composed of degree-2 nodes as large as possible in designing the weight matrix in (3).

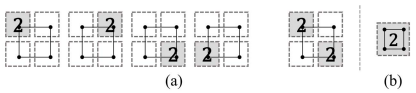


Fig. 3. Additional 4-cycle patterns in construction 2.

Construction 2: We start from the $[2mKP, mKP]$ QC-LDPC code from Construction 1 with the parity-check matrix $\mathbf{H} = [\mathbf{H}_{e(i,j)}]$ and $m \geq 3$. The proposed type-II QC-LDPC code will have the parity-check matrix $\mathbf{H} = [\mathbf{P}_{i,j}]$ where $\mathbf{P}_{i,j}$ is now determined by the weight matrix $\mathbf{W} = [w(i, j)]$ in (3) *as follows: for $0 \leq i < m$ and $0 \leq j < 2m$,*

$$\mathbf{P}_{i,j} = \begin{cases} \mathbf{0}, & \text{if } w(i,j) = 0 \\ \mathbf{H}_{e(i,j)}, & \text{if } w(i,j) = 1 \\ \mathbf{H}_{e(i,j)} + \mathbf{H}_{e(i,i+2 \pmod m)}, & \text{if } w(i,j) = 2. \end{cases}$$

Recall that $e(i, j) = a_i b_j \pmod{KP}$. Two sequences $\mathbf{a}$ and $\mathbf{b}$ from Construction 1 maintain the non-existence conditions for 4-cycles and 6-cycles when $w(i, j) = 0$ or 1. When $w(i, j) = 2$, two CPMs of size KP are added, and now we have to check whether there are any additional 4- or 6-cycles. In the following, we consider only the cases with $K = 1$. The general case will be treated in Remark 4 following the discussion.

Figures 3 and 4 show the additional patterns of 4-cycle and 6-cycle due to the newly introduced term $\mathbf{H}_{e(i,i+2 \pmod m)}$. For the cycle of length 4, we need to consider 2 sizes of submatrices which are 2×2 and 1×1 shown in Fig. 3 (a) and (b). For the case of 2×2 submatrix, there are $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ (4 subcases) and $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right]$ (1 case). In any of such cases, a condition for the existence of a 4-cycle with a single participation of the term $\mathbf{H}_{e(i,i+2 \pmod m)}$ is

$$a_i(b_{i+2 \pmod m} - b_y) - a_j(b_x - b_y) \equiv 0 \pmod P,$$

for some $a_i, a_j, b_x, b_y, b_{i+2 \pmod m}$. The condition with double participations of this term becomes

$$a_i(b_{i+2 \pmod m} - b_y) - a_j(b_x - b_{j+2 \pmod m}) \equiv 0 \pmod P,$$

for some $a_i, a_j, b_x, b_y, b_{i+2 \pmod m}, b_{j+2 \pmod m}$.

For the subcase of 1×1 submatrix, the condition becomes

$$2a_i(b_x - b_{i+2 \pmod m}) \equiv 0 \pmod P, \tag{4}$$

for some $a_i, b_x, b_{i+2 \pmod m}$.

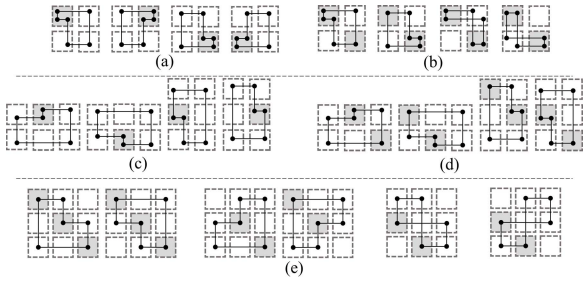


Fig. 4. Additional 6-cycle patterns in construction 2.

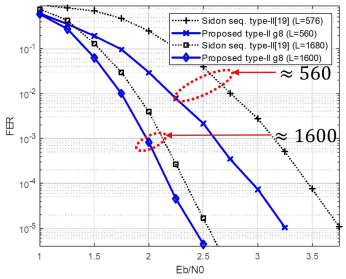


Fig. 5. Performance of the proposed codes from example 2.

For the cycle of length 6, we need to consider 4 sizes of submatrices which are 2×2, 2×3, 3×2 and 3×3 shown in Fig. 4 (a), (b), (c), (d) and (e). For the case of 2×2 submatrix, there are $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ (4 subcases in Fig. 4(a)) and $\left[\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right]$ (4 subcases in Fig. 4(b)). A condition for the existence of 6-cycles with a single participation of the term $\mathbf{H}_{e(i,i+2 \pmod m))}$ is $a_i(b_x - b_{i+2 \pmod m)}) + (a_i - a_j)(b_x - b_y) \equiv 0 \pmod P$, for some $a_i, a_j, b_x, b_y, b_{i+2 \pmod m)}$. The condition with double participations of the term becomes $a_i(b_x - b_{i+2 \pmod m)}) + a_j(b_y - b_{j+2 \pmod m)}) \equiv 0 \pmod P$, for some $a_i, a_j, b_x, b_y, b_{i+2 \pmod m)}, b_{j+2 \pmod m)}$.

For the case of 2×3 submatrix, there are $\left[\begin{smallmatrix} 1 & 2 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right]$ (2 subcases) and $\left[\begin{smallmatrix} 1 & 2 & 1 \\ 1 & 1 & 2 \end{smallmatrix}\right]$ (2 subcases), both are shown on the left of Fig. 4 (c) and (d). In any of such cases, a condition for the existence of a 6-cycle with a single participation of the term $\mathbf{H}_{e(i,i+2 \pmod m))}$ is $a_i(b_y - b_{i+2 \pmod m)}) + (a_i - a_j)(b_x - b_z) \equiv 0 \pmod P$, for some $a_i, a_j, b_x, b_y, b_{i+2 \pmod m)}, b_z$. The condition with double participations becomes $a_i(b_x - b_y + b_{i+2 \pmod m)} - b_z) + a_j(b_{j+2 \pmod m)} - b_x) \equiv 0 \pmod P$, for some $a_i, a_j, b_x, b_y, b_{i+2 \pmod m)}, b_z, b_{j+2 \pmod m)}$. The case of 3×2 submatrix can be treated similarly.

For the case of 3×3 submatrix, there are basically six types shown in Fig. 4(e). Consider for example the very first group (two left-most) shown in Fig. 4(e). Each dot can correspond to the value 1 or the value 2, and there are 13 possibilities for this group. Note that the multiple occurrence of the value 2 is restricted so that they cannot come to the same row, the same column, and on the positive-slope lines. In any of such cases, a condition for the existence of a 6-cycle with a single participation of the term $\mathbf{H}_{e(i,i+2 \pmod m))}$ is $a_i b_{i+2 \pmod m)} - a_i b_y + a_j b_y - a_j b_z + a_k b_z - a_k b_x \equiv 0 \pmod P$, for some $a_i, a_j, a_k, b_x, b_{i+2 \pmod m)}, b_y, b_z$. The conditions with double or triple participations of the terms can be similarly treated. For the second group (next two left-most), there are 9 possibilities. For the third and fourth (one in each group), there are 13 and 8 possibilities, respectively. The condition for the existence of a 6-cycle can be found similarly according to the single or double participations of the new term.

Two sequences $\mathbf{a}$ and $\mathbf{b}$ in Step 1) of Construction 1 have to satisfy the additional conditions that are negations of all the conditions discussed just above in order to construct type-II codes in Construction 2. We now take care of the cases $K > 1$ as a remark.

Remark 4: Let $\mathbf{E} = [a_i b_j]$ *be the result of Construction 1 and computed mod* P*. If it satisfies the additional non-existence conditions for 4-cycles and 6-cycles, then the same matrix computed mod* KP *also satisfies the similar conditions mod* KP*. This must be obvious by the proof similar to those at the end of Remark 1.*

Example 2: We choose $M = m = 4$, $N = n = 8$ *and two choices of* P *in the following with* $K = 1$.

- *We choose* $P = 70$ *and obtain two sequences* $\mathbf{a} = (1, 2, 3, 4)$ *and* $\mathbf{b} = (2, 8, 15, 21, 26, 32, 39, 45)$ *from Construction 1 and satisfying the additional non-existence conditions. Then we apply Construction 2 to obtain a girth-8 type-II QC-LDPC codes with length 560.*
- *We choose* $P = 200$ *and obtain two sequences* $\mathbf{a} = (1, 2, 3, 4)$ *and* $\mathbf{b} = (1, 2, 6, 7, 24, 26, 31, 67)$ *from Construction 1 and satisfying the additional non-existence conditions. Then we apply Construction 2 to obtain a girth-8 type-II QC-LDPC codes with length 1600.*

Figure 5 shows the error performance of the proposed $[560, 280]$ and $[1600, 800]$ girth-8 type-II QC-LDPC codes, respectively, in Example 2. It also shows the $[576, 288]$ and $[1680, 840]$ type-II QC-LDPC codes from Sidon sequences [19]. We use sum-product decoding with the maximum number of iteration as 50 under assumption of AWGN channel and BPSK modulation. We observe that the proposed girth-8 type-II QC-LDPC codes outperform the ones from [19] for both cases, even though the lengths are slightly smaller.

III. Girth-8 Type-II QC-LDPC Codes for GNSS

In the remaining of this letter, we consider the CNAV message structure for various message lengths: 300, 600 and 900 bits to be applicable for legacy systems and future message length modifications. This gives the codes of lengths 600, 1200 and 1800, respectively. We design three different QC-LDPC codes with the proposed scheme based on Constructions 1 and 2 as follows:

We choose $M = 4$, $N = 8$ *and* $P = 75$*. We obtain two sequences* $\mathbf{a} = (1, 2, 3, 4)$ *and* $\mathbf{b} = (1, 4, 18, 39, 56, 61, 63, 69)$ *from Construction 1 and satisfying the additional non-existence conditions. We now use* $K = 1, 2, 3$ *for the exponent matrix* $\mathbf{E}$ *for three different parameters. Then we apply Construction 2 to obtain a family of three different half-rate girth-8 type-II QC-LDPC codes. We obtain the code of length 600 for* $K = 1$*, and those of lengths 1200 and 1800 for* $K = 2$ *and* $K = 3$*, respectively.*

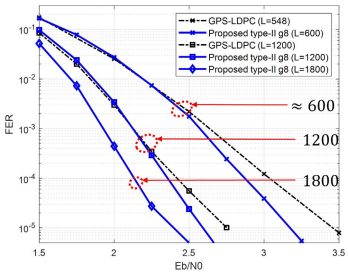


Fig. 6. Performance of the proposed codes from Section III.

We observe that the condition (4) can never be satisfied when P is odd. Note that three exponent matrices above can differ with each other depending on the CPM size KP even they are from the same sequences $\mathbf{a}$ and $\mathbf{b}$. Here, we achieve various lengths by changing the value only of K.

The FER performance of the proposed half-rate girth-8 type-II QC-LDPC codes is shown in Fig. 6. We assume the BPSK modulation and transmission over AWGN channels. For decoding, we use the conventional sum-product algorithm with at most 50 iterations. For the comparison, we also simulated the two half-rate LDPC codes with lengths 548 and 1200, which are currently used in the GPS L1C signals [2]. It is clear from the figure that the proposed codes are slightly better. The improvement is about $0.2 \sim 0.3$ dB at FER of 10^{-5} for the lengths 600 and 1200. We note that one of the current LDPC codes in the GPS has length 548 which is slightly shorter than 600. We also note that the proposed code of length 1800 can also be a good candidate for the future use in the GPS.

IV. Concluding Remark

We proposed in this letter a family of girth-8 QC-LDPC codes of various lengths and rates in Construction 1 and half-rate type-II codes of lengths 600, 1200, and 1800 for the future GNSS in Construction 2. We would like to conclude this letter by mentioning some interesting open problems in this process.

The first is the question of the existence of two increasing integer sequences $\mathbf{a}$ and $\mathbf{b}$ of length M and N, respectively, satisfying various conditions for ruling out the existence of 4- and 6-cycles in Step 1) of Construction 1. We guess initially that such sequences are abundant for any modulus P, but an exhaustive search by computation shows that no such $\mathbf{b}$ of length $N = 10$ exists for $\mathbf{a} = (1, 2, 3, 4, 5)$ and $P = 60$. For which parameters $M < N < P$ and why do such integer sequences $\mathbf{a}$ of length M and $\mathbf{b}$ of length N satisfying the conditions mod P exist?

Two other open problems are essentially mentioned in Remark 2 and Remark 3. Due to the space limitation, we will stop here.

References

[1] (2019). *IS-GPS-200 NAVSTAR GPS Space Segment/Navigation User Segment, Revision K*. [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-200K.pdf

[2] (2020). *IS-GPS-800 NAVSTAR GPS Space Segment/User Segment L1C Interfaces, Revision G*. [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-800G.pdf

[3] Japan Aerospace Exploration Agency. (2020). *Performance Standard (PS-QZSS) and Interface Specification (IS-QZSS)*. [Online]. Available: https://qzss.go.jp/en/technical/ps-is-qzss/ps-is-qzss.html

[4] M. Battaglioni, A. Tasdighi, M. Baldi, M. H. Tadayon, and F. Chiaraluce, "Compact QC-LDPC block and SC-LDPC convolutional codes for low-latency communications," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2018, pp. 1–5.

[5] H. Cho, H.-Y. Song, J. M. Ahn, and D. W. Lim, "Some new RS-coded orthogonal modulation schemes for future GNSS," *ICT Exp.*, May 2021, doi: 10.1016/j.icte.2021.04.004.

[6] J. T. Curran, M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger, "Coding aspects of secure GNSS receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1271–1287, Jun. 2016.

[7] L. Dai, Y. Fang, Z. Yang, P. Chen, and Y. Li, "Protograph LDPC-coded BICM-ID with irregular CSK mapping in visible light communication systems," *IEEE Trans. Veh. Technol.*, early access, Aug. 19, 2021, doi: 10.1109/TVT.2021.3106053.

[8] 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.

[9] I. Kim and H.-Y. Song, "Construction of Reed–Solomon based quasi-cyclic LDPC codes based on protograph," in *Proc. 24th Asia–Pacific Conf. Commun. (APCC)*, Nov. 2018, pp. 397–400.

[10] 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)*, Jeju, South Korea, Oct. 2020, pp. 1462–1465.

[11] A. K. Pradhan, A. Thangaraj, and A. Subramanian, "Construction of near-capacity protograph LDPC code sequences with block-error thresholds," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 27–37, Jan. 2016.

[12] M.-R. Sadeghi and F. Amirzade, "Analytical lower bound on the lifting degree of multiple-edge QC-LDPC codes with girth 6," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1528–1531, Aug. 2018.

[13] M.-R. Sadeghi, "Optimal search for girth-8 quasi cyclic and spatially coupled multiple-edge LDPC codes," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1466–1469, Sep. 2019.

[14] M. H. Tadayon, A. Tasdighi, M. Battaglioni, M. Baldi, and F. Chiaraluce, "Efficient search of compact QC-LDPC and SC-LDPC convolutional codes with large girth," *IEEE Commun. Lett.*, vol. 22, no. 6, pp. 1156–1159, Jun. 2018.

[15] 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.

[16] A. Wang, J. Chen, Y. Zhang, J. Wang, and B. Wang, "Performance evaluation of the CNAV broadcast ephemeris," *J. Navigat.*, vol. 72, no. 5, pp. 1331–1344, Apr. 2019, doi: 10.1017/S037346331900016X.

[17] 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)*, San Diego, CA, USA, Feb. 2018, pp. 1–10.

[18] G. Zhang *et al.*, "Construction of girth-eight QC-LDPC codes from greatest common divisor," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 369–372, Feb. 2013.

[19] 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.

[20] J. Zhang and G. Zhang, "Deterministic girth-eight QC-LDPC codes with large column weight," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 656–659, Apr. 2014.