SCIENCE CHINA
Information Sciences

• Supplementary File •

Two classes of QC-LDPC cycle codes approaching Gallager lower bound

Hengzhou XU[1,2*], Huaan LI[2], Mengmeng XU[1], Dan FENG[2] & Hai ZHU[1*]

[1] *School of Network Engineering, Zhoukou Normal University, Zhoukou* 466001*, China;*
[2] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China*

Appendix A Some examples of difference sets

Example 1. Let $G = \{0, 1, 2, 3, 4, 5, 6\}$ be the additive group under modulo-7 addition. Consider $D = \{0, 1, 3\}$. The following equations hold:

$$1 = 1 - 0, \quad 2 = 3 - 1, \quad 3 = 3 - 0, \quad 4 = 0 - 3, \quad 5 = 1 - 3, \quad 6 = 0 - 1.$$

Hence, the 3-subset D of G is a $(7, 3, 1)$-difference set (or planar difference set).

Example 2. Let $G = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ be the additive group under modulo-11 addition. Consider $D = \{1, 3, 4, 5, 9\}$. The following equations hold:

$$\begin{array}{lllll} 1 = 4 - 3 = 5 - 4, & 2 = 3 - 1 = 5 - 3, & 3 = 4 - 1 = 1 - 9, & 4 = 5 - 1 = 9 - 5, & 5 = 9 - 4 = 3 - 9, \\ 6 = 4 - 9 = 9 - 3, & 7 = 1 - 5 = 5 - 9, & 8 = 1 - 4 = 9 - 1, & 9 = 1 - 3 = 3 - 5, & 10 = 3 - 4 = 4 - 5. \end{array}$$

Therefore, the 5-subset D of G is a $(11, 5, 2)$-difference set.

Example 3. Let $G = \{0, 1, 2, 3, 4, \ldots, 380\}$ be the additive group under modulo-381 addition. Consider $D = \{$0, 1, 19, 28, 96, 118, 151, 153, 176, 202, 240, 254, 290, 296, 300, 307, 337, 361, 366, 369$\}$. It can be found that the following equations are satisfied.

$$\begin{array}{lllll}
1 = 1 - 0, & 2 = 153 - 151, & 3 = 369 - 366, & 4 = 300 - 296, & 5 = 366 - 361, \\
6 = 296 - 290, & 7 = 307 - 300, & 8 = 369 - 361, & 9 = 28 - 19, & 10 = 300 - 290, \\
11 = 307 - 296, & 12 = 0 - 369, & 13 = 1 - 369, & 14 = 254 - 240, & 15 = 0 - 366, \\
16 = 1 - 366, & 17 = 307 - 290, & 18 = 19 - 1, & 19 = 19 - 0, & 20 = 0 - 361, \\
21 = 1 - 361, & 22 = 118 - 96, & 23 = 176 - 153, & 24 = 361 - 337, & 25 = 176 - 151, \\
26 = 202 - 176, & 27 = 28 - 1, & 28 = 28 - 0, & 29 = 366 - 337, & 30 = 337 - 307, \\
31 = 19 - 369, & 32 = 369 - 337, & 33 = 151 - 118, & 34 = 19 - 366, & 35 = 153 - 118, \\
36 = 290 - 254, & 37 = 337 - 300, & 38 = 240 - 202, & 39 = 19 - 361, & 40 = 28 - 369, \\
41 = 337 - 296, & 42 = 296 - 254, & 43 = 28 - 366, & 44 = 0 - 337, & 45 = 1 - 337, \\
46 = 300 - 254, & 47 = 337 - 290, & 48 = 28 - 361, & 49 = 202 - 153, & 50 = 290 - 240, \\
51 = 202 - 151, & 52 = 254 - 202, & 53 = 307 - 254, & 54 = 361 - 307, & 55 = 151 - 96, \\
56 = 296 - 240, & 57 = 153 - 96, & 58 = 176 - 118, & 59 = 366 - 307, & 60 = 300 - 240, \\
61 = 361 - 300, & 62 = 369 - 307, & 63 = 19 - 337, & 64 = 240 - 176, & 65 = 361 - 296, \\
66 = 366 - 300, & 67 = 307 - 240, & 68 = 96 - 28, & 69 = 369 - 300, & 70 = 366 - 296, \\
71 = 361 - 290, & 72 = 28 - 337, & 73 = 369 - 296, & 74 = 0 - 307, & 75 = 1 - 307, \\
76 = 366 - 290, & 77 = 96 - 19, & 78 = 254 - 176, & 79 = 369 - 290, & 80 = 176 - 96, \\
81 = 0 - 300, & 82 = 1 - 300, & 83 = 337 - 254, & 84 = 202 - 118, & 85 = 0 - 296, \\
86 = 1 - 296, & 87 = 240 - 153, & 88 = 290 - 202, & 89 = 240 - 151, & 90 = 118 - 28,
\end{array}$$

[*] Corresponding author (email: hzxu@zknu.edu.cn, zhu_sea@163.com)

$91 = 0 - 290$, $92 = 1 - 290$, $93 = 19 - 307$, $94 = 296 - 202$, $95 = 96 - 1$,
$96 = 96 - 0$, $97 = 337 - 240$, $98 = 300 - 202$, $99 = 118 - 19$, $100 = 19 - 300$,
$101 = 254 - 153$, $102 = 28 - 307$, $103 = 254 - 151$, $104 = 19 - 296$, $105 = 307 - 202$,
$106 = 202 - 96$, $107 = 361 - 254$, $108 = 96 - 369$, $109 = 28 - 300$, $110 = 19 - 290$,
$111 = 96 - 366$, $112 = 366 - 254$, $113 = 28 - 296$, $114 = 290 - 176$, $115 = 369 - 254$,
$116 = 96 - 361$, $117 = 118 - 1$, $118 = 118 - 0$, $119 = 28 - 290$, $120 = 296 - 176$,
$121 = 361 - 240$, $122 = 240 - 118$, $123 = 151 - 28$, $124 = 300 - 176$, $125 = 153 - 28$,
$126 = 366 - 240$, $127 = 0 - 254$, $128 = 1 - 254$, $129 = 369 - 240$, $130 = 118 - 369$,
$131 = 307 - 176$, $132 = 151 - 19$, $133 = 118 - 366$, $134 = 153 - 19$, $135 = 337 - 202$,
$136 = 254 - 118$, $137 = 290 - 153$, $138 = 118 - 361$, $139 = 290 - 151$, $140 = 96 - 337$,
$141 = 0 - 240$, $142 = 1 - 240$, $143 = 296 - 153$, $144 = 240 - 96$, $145 = 296 - 151$,
$146 = 19 - 254$, $147 = 300 - 153$, $148 = 176 - 28$, $149 = 300 - 151$, $150 = 151 - 1$,
$151 = 151 - 0$, $152 = 153 - 1$, $153 = 153 - 0$, $154 = 307 - 153$, $155 = 28 - 254$,
$156 = 307 - 151$, $157 = 176 - 19$, $158 = 254 - 96$, $159 = 361 - 202$, $160 = 19 - 240$,
$161 = 337 - 176$, $162 = 118 - 337$, $163 = 151 - 369$, $164 = 366 - 202$, $165 = 153 - 369$,
$166 = 151 - 366$, $167 = 369 - 202$, $168 = 153 - 366$, $169 = 28 - 240$, $170 = 96 - 307$,
$171 = 151 - 361$, $172 = 290 - 118$, $173 = 153 - 361$, $174 = 202 - 28$, $175 = 176 - 1$,
$176 = 176 - 0$, $177 = 96 - 300$, $178 = 296 - 118$, $179 = 0 - 202$, $180 = 1 - 202$,
$181 = 96 - 296$, $182 = 300 - 118$, $183 = 202 - 19$, $184 = 337 - 153$, $185 = 361 - 176$,
$186 = 337 - 151$, $187 = 96 - 290$, $188 = 176 - 369$, $189 = 307 - 118$, $190 = 366 - 176$,
$191 = 176 - 366$, $192 = 118 - 307$, $193 = 369 - 176$, $194 = 290 - 96$, $195 = 151 - 337$,
$196 = 176 - 361$, $197 = 153 - 337$, $198 = 19 - 202$, $199 = 118 - 300$, $200 = 296 - 96$,
$201 = 202 - 1$, $202 = 202 - 0$, $203 = 118 - 296$, $204 = 300 - 96$, $205 = 0 - 176$,
$206 = 1 - 176$, $207 = 28 - 202$, $208 = 361 - 153$, $209 = 118 - 290$, $210 = 361 - 151$,
$211 = 307 - 96$, $212 = 240 - 28$, $213 = 366 - 153$, $214 = 202 - 369$, $215 = 366 - 151$,
$216 = 369 - 153$, $217 = 202 - 366$, $218 = 369 - 151$, $219 = 337 - 118$, $220 = 176 - 337$,
$221 = 240 - 19$, $222 = 202 - 361$, $223 = 96 - 254$, $224 = 19 - 176$, $225 = 151 - 307$,
$226 = 254 - 28$, $227 = 153 - 307$, $228 = 0 - 153$, $229 = 1 - 153$, $230 = 0 - 151$,
$231 = 1 - 151$, $232 = 151 - 300$, $233 = 28 - 176$, $234 = 153 - 300$, $235 = 254 - 19$,
$236 = 151 - 296$, $237 = 96 - 240$, $238 = 153 - 296$, $239 = 240 - 1$, $240 = 240 - 0$,
$241 = 337 - 96$, $242 = 151 - 290$, $243 = 361 - 118$, $244 = 153 - 290$, $245 = 118 - 254$,
$246 = 202 - 337$, $247 = 19 - 153$, $248 = 366 - 118$, $249 = 19 - 151$, $250 = 176 - 307$,
$251 = 369 - 118$, $252 = 240 - 369$, $253 = 254 - 1$, $254 = 254 - 0$, $255 = 240 - 366$,
$256 = 28 - 153$, $257 = 176 - 300$, $258 = 28 - 151$, $259 = 118 - 240$, $260 = 240 - 361$,
$261 = 176 - 296$, $262 = 290 - 28$, $263 = 0 - 118$, $264 = 1 - 118$, $265 = 361 - 96$,
$266 = 254 - 369$, $267 = 176 - 290$, $268 = 296 - 28$, $269 = 254 - 366$, $270 = 366 - 96$,
$271 = 290 - 19$, $272 = 300 - 28$, $273 = 369 - 96$, $274 = 254 - 361$, $275 = 96 - 202$,
$276 = 202 - 307$, $277 = 296 - 19$, $278 = 151 - 254$, $279 = 307 - 28$, $280 = 153 - 254$,
$281 = 300 - 19$, $282 = 19 - 118$, $283 = 202 - 300$, $284 = 240 - 337$, $285 = 0 - 96$,
$286 = 1 - 96$, $287 = 202 - 296$, $288 = 307 - 19$, $289 = 290 - 1$, $290 = 290 - 0$,
$291 = 28 - 118$, $292 = 151 - 240$, $293 = 202 - 290$, $294 = 153 - 240$, $295 = 296 - 1$,
$296 = 296 - 0$, $297 = 118 - 202$, $298 = 254 - 337$, $299 = 300 - 1$, $300 = 300 - 0$,
$301 = 96 - 176$, $302 = 290 - 369$, $303 = 176 - 254$, $304 = 19 - 96$, $305 = 290 - 366$,
$306 = 307 - 1$, $307 = 307 - 0$, $308 = 296 - 369$, $309 = 337 - 28$, $310 = 290 - 361$,
$311 = 296 - 366$, $312 = 300 - 369$, $313 = 28 - 96$, $314 = 240 - 307$, $315 = 300 - 366$,
$316 = 296 - 361$, $317 = 176 - 240$, $318 = 337 - 19$, $319 = 307 - 369$, $320 = 300 - 361$,
$321 = 240 - 300$, $322 = 307 - 366$, $323 = 118 - 176$, $324 = 96 - 153$, $325 = 240 - 296$,
$326 = 96 - 151$, $327 = 307 - 361$, $328 = 254 - 307$, $329 = 202 - 254$, $330 = 151 - 202$,
$331 = 240 - 290$, $332 = 153 - 202$, $333 = 361 - 28$, $334 = 290 - 337$, $335 = 254 - 300$,
$336 = 337 - 1$, $337 = 337 - 0$, $338 = 366 - 28$, $339 = 254 - 296$, $340 = 296 - 337$,
$341 = 369 - 28$, $342 = 361 - 19$, $343 = 202 - 240$, $344 = 300 - 337$, $345 = 254 - 290$,

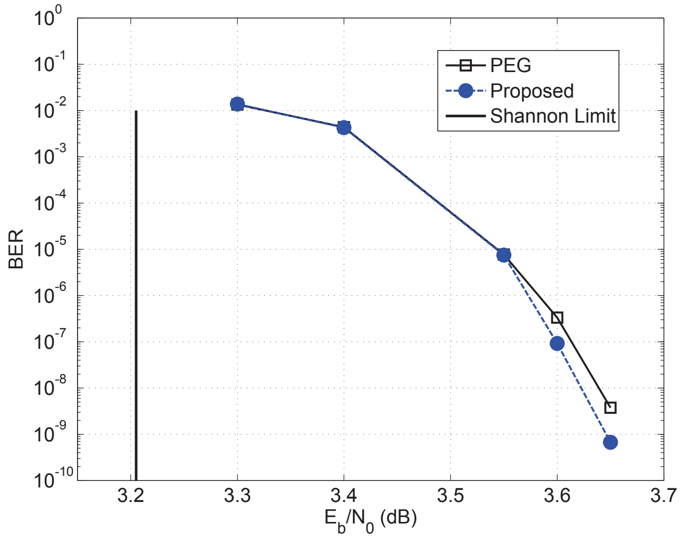

Figure B1 The error performance of the proposed $(7620, 6858)$ LDPC cycle code over GF(64) and the comparable $(7620, 6858)$ LDPC cycle code over GF(64) constructed based on the progressive-edge-growth (PEG) algorithm [1].

$$\begin{array}{lllll}
346 = 118 - 153, & 347 = 366 - 19, & 348 = 118 - 151, & 349 = 337 - 369, & 350 = 369 - 19, \\
351 = 307 - 337, & 352 = 337 - 366, & 353 = 0 - 28, & 354 = 1 - 28, & 355 = 176 - 202, \\
356 = 151 - 176, & 357 = 337 - 361, & 358 = 153 - 176, & 359 = 96 - 118, & 360 = 361 - 1, \\
361 = 361 - 0, & 362 = 0 - 19, & 363 = 1 - 19, & 364 = 290 - 307, & 365 = 366 - 1, \\
366 = 366 - 0, & 367 = 240 - 254, & 368 = 369 - 1, & 369 = 369 - 0, & 370 = 296 - 307, \\
371 = 290 - 300, & 372 = 19 - 28, & 373 = 361 - 369, & 374 = 300 - 307, & 375 = 290 - 296, \\
376 = 361 - 366, & 377 = 296 - 300, & 378 = 366 - 369, & 379 = 151 - 153, & 380 = 0 - 1.
\end{array}$$

Therefore, the 20-subset D of G is a $(381, 20, 1)$-difference set (or planar difference set).

Appendix B Numerical results and analysis

In this section, we will compare some proposed nonbinary LDPC cycle codes with the existing large-girth codes constructed based the methods in [1–4].

First, the comparable code is constructed based on the progressive-edge-growth (PEG) algorithm [1].

Example 4. Consider the $(381, 20, 1)$-planar difference set in Example 3 of **Appendix A**. According to the 20-subset $D = \{0, 1, 19, 28, 96, 118, 151, 153, 176, 202, 240, 254, 290, 296, 300, 307, 337, 361, 366, 369\}$, we can construct a 2×20 exponent matrix

$$\mathbf{P}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 19 & 28 & 96 & 118 & 151 & 153 & 176 & 202 & 240 & 254 & 290 & 296 & 300 & 307 & 337 & 361 & 366 & 369 \end{bmatrix}.$$

By replacing the elements of $\mathbf{P}_1$ with the corresponding circulant permutation matrices (CPMs) of size 381×381, we can obtain the parity-check matrix $\mathbf{H}_1$ of a binary QC-LDPC cycle code. We randomly replace 1's in $\mathbf{H}_1$ with nonzero elements of finite field GF(q), and a matrix $\mathbf{H}_{\mathrm{NB}}$ over GF(q) is obtained. The null space over GF(q) of $\mathbf{H}_{\mathrm{NB}}$ gives a $(7620, 6858)$ LDPC cycle code over GF(q). Consider $q = 64$. We can construct a $(7620, 6858)$ LDPC cycle code over GF(64) with code rate 0.9. For comparison, we also construct a $(7620, 6858)$ LDPC cycle code over GF(64) based on the progressive-edge-growth (PEG) algorithm [1]. Notice that the nonzero field elements of these two nonbinary LDPC cycle codes are randomly chosen. The bit error rates (BERs) of these two $(7620, 6858)$ LDPC cycle codes over GF(64) are shown in Fig. B1. In the simulations, the BPSK modulated additive white gaussian noise (AWGN) channel and the fast-Fourier-transform (FFT) based q-ary sum-product algorithm (QSPA) with 50 iterations are assumed. It can be seen from Fig. B1 that at the BER of 10^{-8}, the proposed code outperforms about 0.02 dB than the PEG-LDPC cycle code, and the coding gain gap will be larger and larger with the increase of SNR. Furthermore, at a BER of 10^{-9}, the proposed code performs 0.45 dB from the Shannon limit.

Second, we construct a $(456, 342)$ LDPC cycle code over GF(64) to compare with the $(448, 336)$ LDPC cycle code over GF(64) constructed based on the method in [2].

Example 5. Consider the $(57, 8, 1)$-planar difference set whose 8-subset D is $\{1, 6, 7, 9, 19, 38, 42, 49\}$. According to the 8-subset D, we can construct a 2×8 exponent matrix

$$\mathbf{P}_2' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 6 & 7 & 9 & 19 & 38 & 42 & 49 \end{bmatrix}.$$

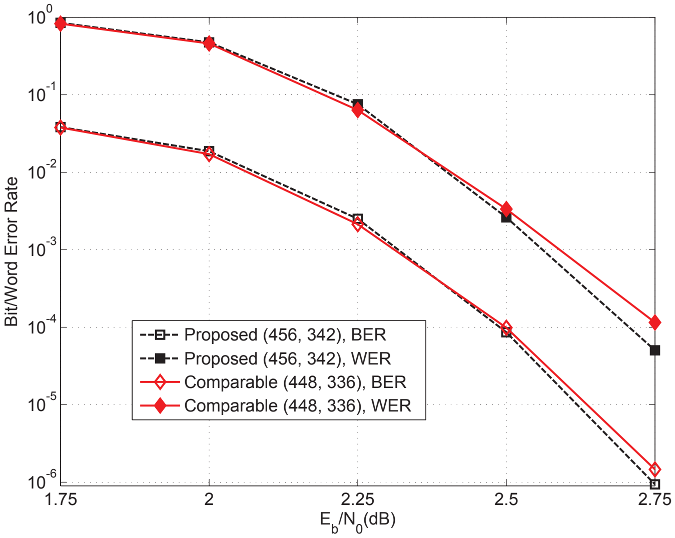

Figure B2 The error performance of the proposed $(456, 342)$ LDPC cycle code over GF(64) and the comparable $(448, 336)$ LDPC cycle code over GF(64) constructed based on the method in [2].

The simplified isomorphic form of $\mathbf{P}'_2$ is

$$\mathbf{P}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 6 & 8 & 18 & 37 & 41 & 48 \end{bmatrix}.$$

In other words, $\mathbf{P}'_2$ is isomorphic to $\mathbf{P}_2$, i.e., $\mathbf{P}'_2 \cong \mathbf{P}_2$. By replacing the elements of $\mathbf{P}_2$ with the corresponding CPMs of size 57×57, we can obtain a matrix $\mathbf{H}_2$ of size 114×456. We randomly replace 1's in $\mathbf{H}_2$ with nonzero elements of finite field GF(64), and a matrix $\mathbf{H}_{2,64}$ over GF(64) is obtained. The null space over GF(64) of $\mathbf{H}_{2,64}$ gives a $(456, 342)$ LDPC cycle code over GF(64) of code rate 0.75. For comparison, we also construct a $(448, 336)$ LDPC cycle code over GF(64) of code rate 0.75 based on the method in [2]. Notice that the nonzero field elements of these two nonbinary LDPC cycle codes are randomly chosen. The bit/word error rate (BER/WER) performance of these two codes decoded with iterative decoding using the QSPA (50 iterations) is shown in Fig. B2. Note that the transmitted channel is the BPSK modulated AWGN channel. At a WER of 10^{-4}, the proposed $(456, 342)$ LDPC cycle code over GF(64) outperforms the comparable $(448, 336)$ LDPC cycle code over GF(64) by about 0.05 dB.

Next, in order to show the good performance of the LDPC codes with large girths, the performance of several LDPC codes over different finite fields is given as follows.

Example 6. In [3], a $(228, 114)$ LDPC code over GF(8) was constructed. The WER performance of this code decoded with iterative decoding using the QSPA (80 iterations) is shown in Fig. 2 of [3], and the used channel is the BPSK modulated AWGN channel. For comparison, we also plot it in Fig. B3. We accordingly construct a $(112, 56)$ LDPC cycle code over GF(64) whose exponent matrix is

$$\mathbf{P}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 6 & 9 \end{bmatrix}.$$

Note that its lifting size is 28. The nonzero field elements in the parity-check matrix of the proposed $(112, 56)$ LDPC cycle code over GF(64) are randomly chosen. Under the same simulation conditions with the $(228, 114)$ LDPC code over GF(8) in [3], the BER/WER performance of the $(112, 56)$ LDPC cycle code over GF(64) is also shown in Fig. B3. We can see that, at a WER of 1.4×10^{-4}, the proposed $(112, 56)$ LDPC cycle code over GF(64) achieves a coding gain of 0.4 dB over the comparable $(228, 114)$ LDPC cycle code over GF(8) in [3].

According to the exponent matrix

$$\mathbf{P}_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 3 & 4 & 13 \end{bmatrix},$$

we can obtain a 82×164 matrix $\mathbf{H}_3$ by replacing the elements of $\mathbf{P}_4$ with the corresponding CPMs of size 41×41. We randomly replace 1's in $\mathbf{H}_3$ with nonzero elements of finite field GF(64), and a matrix $\mathbf{H}_{3,64}$ over GF(64) is obtained. The null space over GF(64) of $\mathbf{H}_{3,64}$ gives a $(164, 82)$ LDPC cycle code over GF(64) of code rate 0.5. For comparison, we choose the $(1000, 500)$ LDPC code over GF(2) in [4], and the BER/WER performance is given in Fig. 4 in [4]. We plot it in Fig. B4. Also shown in Fig. B4 is the BER/WER performance of the proposed $(164, 82)$ LDPC cycle code over GF(64). The simulation conditions are the QSPA with 50 iterations and the BPSK modulated AWGN channel. We can see from Fig. B4 that, at a BER of 10^{-5}, the proposed $(164, 82)$ LDPC cycle code over GF(64) outperforms the $(1000, 500)$ LDPC code over GF(2) by about 0.2 dB.

Finally, we employ an example to illustrate the effect of nonzero finite field elements and also to show the performance of the proposed LDPC cycle codes.

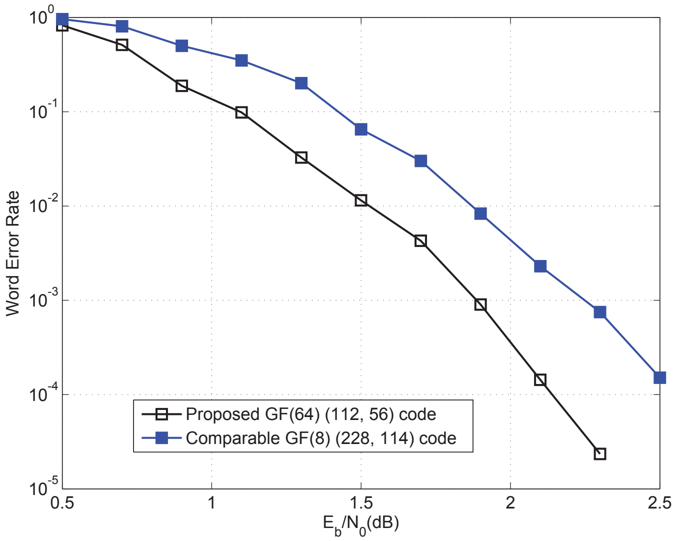

Figure B3 The error performance of the proposed $(112, 56)$ LDPC cycle code over GF(64) and the comparable $(228, 114)$ LDPC code over GF(8) constructed based on the method in [3].

Table B1 The nonzero field elements in the parity-check matrix $\mathbf{H}_{4,256}$ of the proposed $(16, 8)$ LDPC cycle code over GF(256) in Example 7

Row index	Nonzero field elements			
1	92	246	238	121
2	44	223	5	225
3	186	43	99	37
4	196	26	95	16
5	231	228	89	250
6	161	17	179	55
7	170	82	24	89
8	92	59	220	141

Example 7. Consider a girth-8 exponent matrix

$$\mathbf{P}_5 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \end{bmatrix}.$$

By replacing the elements of $\mathbf{P}_5$ with the corresponding CPMs of size 4×4, we can obtain a matrix $\mathbf{H}_4$ of size 8×16. We replace 1's in $\mathbf{H}_4$ with nonzero elements of finite field GF(256), and a matrix $\mathbf{H}_{4,256}$ over GF(256) is obtained. In order to improve the performance of the $(16, 8)$ LDPC cycle code over GF(256), we optimize the nonzero fields in $\mathbf{H}_{4,256}$ by employing the cycle cancellation method [6,7]. The optimized nonzero field elements in $\mathbf{H}_{4,256}$ are recorded in Table B1. In Table B1, the nonzero elements are represented by the powers of α, where α is a primitive element of GF(256) created by using the primitive polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^8$. The null space over GF(256) of $\mathbf{H}_{4,256}$ gives a $(16, 8)$ LDPC cycle code over GF(256) of code rate 0.5. For comparison, we also construct a $(16, 8)$ LDPC cycle code over GF(256) in the *Consultative Committee for Space Data System* (CCSDS) standard [5], denoted by the $(16, 8)$ CCSDS-LDPC cycle code over GF(256). Actually, for the lifting size 4, there is only one isomorphic class of exponent matrices of size 2×4, and then the proposed exponent $\mathbf{P}_5$ is isomorphic to one of the $(16, 8)$ CCSDS-LDPC cycle code over GF(256). Hence, the code gain gap between the proposed code and the CCSDS-LDPC cycle code originates from the difference of nonzero field elements in their parity-check matrices. The BER/WER performance of these two codes decoded with iterative decoding using the QSPA (50 iterations) is shown in Fig. B5. Assume that the transmitted channel is the BPSK modulated AWGN channel. It can be seen that the proposed $(16, 8)$ LDPC cycle code over GF(256) performs much better than the comparable $(16, 8)$ CCSDS-LDPC cycle code over GF(256).

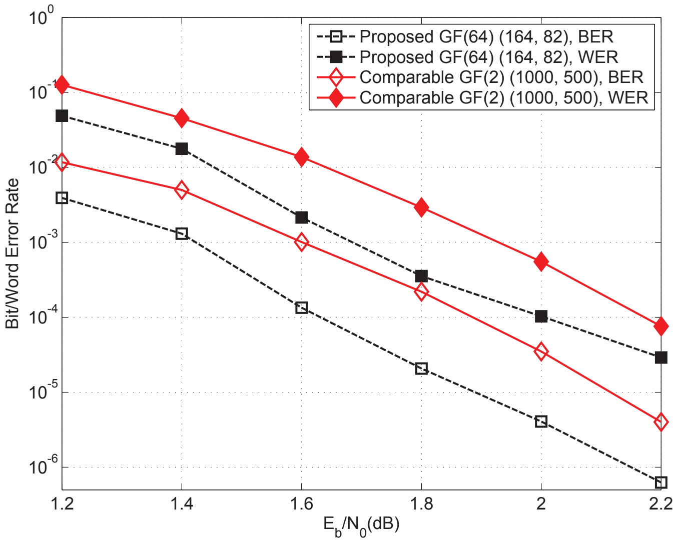

Figure B4 The error performance of the proposed $(164, 82)$ LDPC cycle code over GF(64) and the comparable $(1000, 500)$ LDPC code over GF(2) constructed based on the method in [4].

Appendix C Some lower bounds on code length (or lifting size) of QC-LDPC cycle codes

Based on two classes of the proposed QC-LDPC cycle codes, some tight lower bounds on code length (or lifting size) of QC-LDPC cycle codes are recorded in Table C1. This table is organized as follows:

- First column: the column number ρ of the exponent matrix $\mathbf{P}$;
- Second column: the tight lower bounds on lifting size L_8 of QC-LDPC cycle codes of girth 8;
- Third column: the tight lower bounds on lifting size L_{12} of QC-LDPC cycle codes of girth 12;
- Fourth column: the second row $(p_1, p_2, \ldots, p_\rho)$ in the exponent matrix $\mathbf{P}$ of QC-LDPC cycle codes with girth 12;
- Fifth column: the row $(p_1, p_2, \ldots, p_\rho)$ in [8] which is isomorphic to the one in the corresponding fourth column. Since Singer perfect difference, as a subclass of difference sets, had been used to construct QC-LDPC cycle codes in [8].

The tight lower bounds in Table C1 will be helpful for constructing nonbinary LDPC cycle codes with large girths. It is noticeable that Table C1 provides a constructive proof of the lower bounds on the lifting size, and a theoretical analysis results on the lower bounds for lifting sizes were also presented in [9]. For example, we need to construct a QC-LDPC cycle code with the exponent matrix $\mathbf{P}$ of size 2×4, i.e., $\rho = 4$. Assume that the lifting size L is less than 4, the maximum girth of the constructed LDPC cycle codes is 4. When $4 \leqslant L < 13$, the maximum girth can achieve 8, and 12 while $L \geqslant 13$. In order to facilitate understanding, some examples of QC-LDPC cycle codes with girth 8 are recorded in Tables C2, C3, and Tables C4 and C5 provide some QC-LDPC cycle codes with girth 12. These four tables are organized as follows:

1. Table C2 and Table C3:
   - First column: the row weight ρ of the constructed QC-LDPC cycle codes with girth 8;
   - Second column: lower bounds on lifting size L_8 of QC-LDPC cycle codes of girth 8;
   - Third column: lower bounds on lifting size L_{12} of QC-LDPC cycle codes of girth 12;
   - Fourth column: the lifting size L of the constructed QC-LDPC cycle codes with girth 8;
   - Fifth column: the second row $(p_1, p_2, \ldots, p_\rho)$ in the exponent matrix $\mathbf{P}$ of QC-LDPC cycle codes with girth 8.
2. Table C4 and Table C5:
   - First column: the row weight ρ of the constructed QC-LDPC cycle codes with girth 12;
   - Second column: lower bounds on lifting size L_{12} of QC-LDPC cycle codes of girth 12;
   - Third column: the lifting size L of the constructed QC-LDPC cycle codes with girth 12;
   - Fourth column: the second row $(p_1, p_2, \ldots, p_\rho)$ in the exponent matrix $\mathbf{P}$ of QC-LDPC cycle codes with girth 12.

References

1 Hu X Y, Eleftheriou E, Arnold D. Regular and irregular progressive edge-growth Tanner graphs. IEEE Trans Inf Theory, 2005, 51: 386–398

2 Tao X, Zheng L, Liu W, et al. Recurisive design of high girth $(2, k)$ LDPC codes from (k, k) LDPC codes. IEEE Commun Letters, 2011, 15: 70–72

3 Huang J, Liu L, Zhou W, et al. Large-girth nonbinary QC-LDPC codes of various lengths. IEEE Trans Commun, 2010, 58: 3436–3447

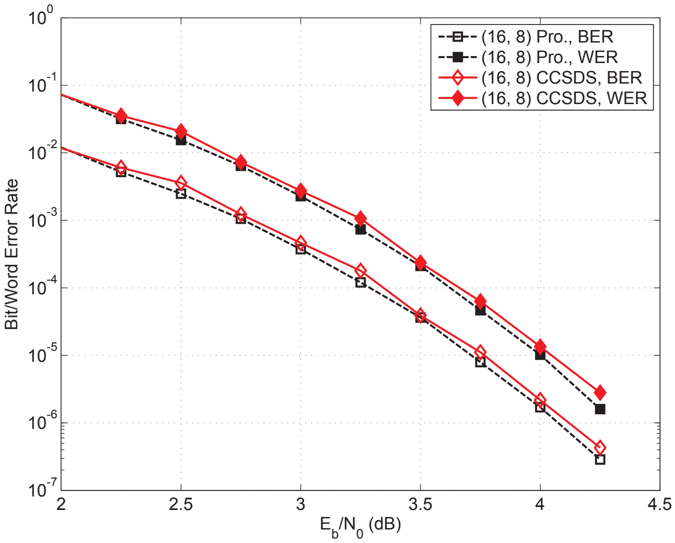

Figure B5 The error performance of the proposed $(16, 8)$ LDPC cycle code over GF(256) and the comparable $(16, 8)$ LDPC cycle code over GF(256) in the CCSDS standard.

4 Myung S, Yang K, Kim J. Quasi-cyclic LDPC codes for fast encoding. IEEE Trans Inf Theory, 2005, 51: 2894–2901

5 Short Block Length LDPC Codes for TC Synchronization and Channel Coding, CCSDS 231.1-O-1, 2015.

6 Poulliat C, Fossorier M, Declercq D. Design of regular $(2, d_c)$-LDPC codes over GF(q) using their binary images. IEEE Trans Commun, 2008, 56: 1626–1635

7 Chen C, Bai B, Shi G, et al. Nonbinary LDPC codes on cages: structural property and code optimization. IEEE Trans Commun, 2015, 63: 364–375

8 Chen C, Bai B M, Wang X M. Construction of nonbinary quasi-cyclic LDPC cycle codes based on singer perfect difference set. IEEE Commun Letters, 2010, 14: 181–183

9 Amirzade F, Sadeghi M R. Lower bounds on the lifting degree of QC-LDPC codes by difference matrices. IEEE Access, 2018, 6: 23688–23700

Table C1 Some tight lower bound on the lifting sizes of QC-LDPC cycle codes

ρ	L_8	L_{12}	$(p_1, p_2, \ldots, p_\rho)$	Isomorphic $(p_1, p_2, \ldots, p_\rho)$ in [8]
3	3	7	$(1, 2, 4)$	$(0, 1, 3)$
4	4	13	$(0, 1, 3, 9)$	$(0, 1, 4, 6)$
5	5	21	$(3, 6, 7, 12, 14)$	$(0, 2, 7, 8, 11)$
6	6	31	$(1, 5, 11, 24, 25, 27)$	$(0, 1, 4, 10, 12, 17)$
7	7	48	$(0, 1, 15, 26, 36, 43, 45)$	None
8	8	57	$(1, 6, 7, 9, 19, 38, 42, 49)$	$(0, 1, 3, 13, 32, 36, 43, 52)$
9	9	73	$(1, 2, 4, 8, 16, 32, 37, 55, 64)$	$(0, 1, 3, 7, 15, 31, 36, 54, 63)$
10	10	91	$(0, 1, 3, 9, 27, 49, 56, 61, 77, 81)$	$(0, 1, 6, 10, 23, 26, 34, 41, 53, 55)$
12	12	133	$(1, 11, 16, 40, 41, 43, 52, 60, 74, 78, 121, 128)$	$(0, 2, 6, 24, 29, 40, 43, 55, 68, 75, 76, 85)$
14	14	183	$(0, 2, 3, 10, 26, 39, 43, 61, 109, 121, 130, 89, 99, 136, 141, 155)$	$(0, 4, 6, 20, 35, 52, 59, 77, 78, 86, 122, 127)$
17	17	273	$(1, 2, 4, 8, 16, 32, 64, 91, 117, 128, 137, 182, 195, 205, 234, 239, 256)$	None
18	18	307	$(0, 1, 3, 30, 37, 50, 55, 76, 98, 117, 129, 133, 157, 189, 199, 222, 293, 299)$	None
20	20	381	$(0, 1, 19, 28, 96, 118, 151, 153, 176, 202, 240, 254, 290, 296, 300, 307, 337, 361, 366, 369)$	None
24	24	553	$(1, 23, 52, 90, 108, 120, 152, 163, 173, 178, 186, 223, 232, 272, 359, 407, 411, 431, 438, 512, 513, 515, 529, 548)$	None
26	26	651	$(1, 5, 25, 42, 71, 107, 125, 201, 210, 217, 354, 355, 357, 387, 399, 412, 434, 462, 468, 473, 483, 521, 535, 561, 625, 633)$	None
28	28	757	$(0, 1, 3, 9, 27, 43, 81, 129, 173, 220, 243, 310, 387, 404, 409, 445, 455, 466, 470, 505, 519, 578, 608, 641, 653, 660, 673, 729)$	None
30	30	871	$(1, 24, 29, 69, 151, 167, 216, 234, 259, 263, 295, 321, 329, 414, 488, 543, 582, 599, 645, 659, 683, 689, 696, 716, 731, 819, 820, 822, 831, 841)$	None

Table C2 Some $(2,\rho)$-regular girth-8 QC-LDPC codes with lifting sizes L for $3 \leqslant \rho \leqslant 5$ and $3 \leqslant L \leqslant 20$

Row weight ρ	Low bound on lifting size L_8 with girth 8	Low bound on lifting size L_{12} with girth 12	Lifting size L	$(p_1, p_2, \ldots, p_\rho)$
3	3	7	3	$(0,1,2)$
3	3	7	4	$(0,1,2)$
3	3	7	5	$(0,1,2)$
3	3	7	6	$(0,1,6)$
4	4	13	4	$(0,1,2,3)$
4	4	13	5	$(0,1,2,3)$
4	4	13	6	$(0,1,2,3)$
4	4	13	7	$(0,2,5,6)$
4	4	13	8	$(1,2,4,5)$
4	4	13	9	$(3,4,5,8)$
4	4	13	10	$(1,6,7,9)$
4	4	13	11	$(4,5,7,9)$
4	4	13	12	$(2,3,6,8)$
5	5	21	5	$(0,1,2,3,4)$
5	5	21	6	$(0,1,2,3,4)$
5	5	21	7	$(0,1,2,3,4)$
5	5	21	8	$(0,2,5,6,7)$
5	5	21	9	$(0,1,2,3,5)$
5	5	21	10	$(1,4,5,6,7)$
5	5	21	11	$(0,4,7,9,10)$
5	5	21	12	$(1,4,8,9,10)$
5	5	21	13	$(2,5,10,11,12)$
5	5	21	14	$(3,6,10,11,12)$
5	5	21	15	$(5,8,10,11,12)$
5	5	21	16	$(1,6,9,10,11)$
5	5	21	17	$(3,4,6,9,13)$
5	5	21	18	$(3,5,10,11,14)$
5	5	21	19	$(3,4,10,14,17)$
5	5	21	20	$(0,1,8,10,16)$

Table C3 Some $(2,\rho)$-regular girth-8 QC-LDPC codes with lifting sizes L for $\rho = 6$ and $6 \leqslant L \leqslant 30$

Row weight ρ	Low bound on lifting size L_8 with girth 8	Low bound on lifting size L_{12} with girth 12	Lifting size L	$(p_1, p_2, \ldots, p_\rho)$
6	6	31	6	$(0, 1, 2, 3, 4, 5)$
6	6	31	7	$(0, 1, 2, 3, 4, 5)$
6	6	31	8	$(0, 1, 2, 3, 4, 5)$
6	6	31	9	$(0, 1, 2, 4, 5, 8)$
6	6	31	10	$(2, 4, 5, 7, 8, 9)$
6	6	31	11	$(0, 4, 6, 7, 9, 10)$
6	6	31	12	$(1, 2, 3, 4, 6, 10)$
6	6	31	13	$(1, 5, 6, 7, 8, 11)$
6	6	31	14	$(0, 5, 6, 9, 10, 12)$
6	6	31	15	$(0, 4, 9, 10, 11, 12)$
6	6	31	16	$(0, 3, 4, 5, 6, 12)$
6	6	31	17	$(0, 2, 6, 11, 15, 16)$
6	6	31	18	$(5, 6, 7, 11, 13, 16)$
6	6	31	19	$(1, 5, 8, 14, 15, 16)$
6	6	31	20	$(3, 9, 10, 14, 17, 19)$
6	6	31	21	$(3, 6, 12, 16, 17, 19)$
6	6	31	22	$(4, 10, 13, 14, 16, 21)$
6	6	31	23	$(6, 8, 11, 14, 15, 19)$
6	6	31	24	$(3, 4, 7, 8, 20, 22)$
6	6	31	25	$(7, 9, 10, 13, 18, 20)$
6	6	31	26	$(6, 8, 12, 13, 21, 24)$
6	6	31	27	$(3, 7, 8, 9, 16, 19)$
6	6	31	28	$(1, 4, 6, 12, 24, 25)$
6	6	31	29	$(3, 8, 10, 11, 17, 21)$
6	6	31	30	$(7, 8, 10, 14, 18, 23)$

Table C4 Some $(2,\rho)$-regular girth-12 QC-LDPC codes with lifting sizes L

Row weight ρ	Low bound on lifting size L_{12} with girth 12	Lifting size L	$(p_1, p_2, \ldots, p_\rho)$
3	7	8	$(0,1,3)$
3	7	9	$(0,1,3)$
3	7	12	$(0,1,4)$
3	7	15	$(0,1,4)$
3	7	18	$(0,1,4)$
3	7	21	$(0,1,5)$
4	13	14	$(0,1,4,6)$
4	13	15	$(0,1,3,7)$
4	13	16	$(0,2,3,7)$
4	13	20	$(0,2,3,9)$
4	13	24	$(0,1,3,10)$
4	13	28	$(0,1,6,9)$
4	13	32	$(0,1,5,12)$
4	13	36	$(0,1,7,11)$
4	13	40	$(0,5,6,14)$
4	13	44	$(0,1,4,13)$
4	13	48	$(0,1,9,12)$
4	13	52	$(0,1,11,15)$
4	13	56	$(0,2,11,14)$
4	13	60	$(0,1,10,16)$
4	13	64	$(0,1,11,15)$
5	21	22	None
5	21	23	$(0,2,7,8,11)$
5	21	24	$(0,1,4,9,11)$
5	21	25	$(0,1,4,9,11)$
5	21	26	$(0,1,4,9,11)$
5	21	27	$(0,1,7,9,12)$
5	21	28	$(0,1,7,9,12)$
5	21	29	$(0,1,7,10,12)$
5	21	30	$(0,1,7,9,12)$
5	21	31	$(0,1,3,7,15)$
5	21	32	$(0,1,5,11,13)$

Table C5 Some $(2, \rho)$-regular girth-12 QC-LDPC codes with lifting sizes L

Row weight ρ	Low bound on lifting size L_{12} with girth 12	Lifting size L	$(p_1, p_2, \ldots, p_\rho)$
6	31	32	None
6	31	33	None
6	31	34	None
6	31	35	$(0, 1, 3, 7, 12, 20)$
6	31	36	$(0, 1, 3, 8, 23, 27)$
6	31	37	$(0, 1, 3, 7, 16, 26)$
6	31	38	$(0, 1, 3, 7, 17, 30)$
6	31	39	$(0, 1, 3, 7, 12, 22)$
6	31	40	$(0, 1, 3, 7, 17, 28)$
7	48	49	$(0, 1, 3, 7, 27, 35, 40)$
7	48	50	$(0, 1, 3, 8, 14, 18, 30)$
7	48	51	$(0, 1, 3, 7, 12, 20, 30)$
7	48	52	$(0, 1, 3, 7, 12, 22, 35)$
7	48	53	$(0, 1, 3, 7, 12, 22, 40)$
7	48	54	$(0, 1, 3, 7, 16, 26, 37)$
7	48	55	$(0, 1, 3, 7, 12, 20, 30)$
7	48	56	$(0, 1, 3, 7, 12, 20, 41)$
8	57	58	None
8	57	59	None
8	57	60	None
8	57	61	None
8	57	62	None
8	57	63	$(0, 1, 3, 7, 15, 20, 31, 41)$
8	57	64	$(0, 1, 3, 8, 19, 25, 29, 52)$
8	57	65	$(0, 1, 3, 8, 19, 25, 29, 52)$
8	57	66	$(0, 1, 3, 8, 19, 25, 29, 52)$
8	57	67	$(0, 1, 3, 8, 19, 25, 29, 52)$
8	57	68	$(0, 1, 3, 8, 19, 25, 29, 52)$
9	73	84	None
9	73	85	$(0, 1, 3, 8, 14, 29, 33, 49, 76)$
9	73	86	$(0, 1, 3, 8, 17, 36, 42, 63, 74)$
9	73	87	$(0, 1, 3, 7, 17, 36, 49, 67, 79)$
9	73	88	$(0, 1, 3, 7, 27, 41, 52, 60, 73)$
9	73	89	$(0, 1, 3, 7, 12, 20, 35, 49, 65)$
9	73	90	$(0, 1, 3, 7, 20, 28, 51, 61, 75)$
10	91	130	$(0, 1, 3, 7, 12, 20, 30, 46, 78, 93)$
10	91	132	$(0, 1, 3, 7, 12, 20, 30, 44, 65, 93)$
11	Unkown	133	$(0, 26, 38, 48, 73, 81, 109, 113, 115, 118, 132)$