J. Algebra Comb. Discrete Appl.
12(3) • 175–180

Received: 23 March 2024
Accepted: 7 March 2025

Journal of Algebra Combinatorics Discrete Structures and Applications

On generator polynomial matrices of quasi-cyclic codes with linear complementary duals

Research Article

Norifumi Ojiro, Hajime Matsui

Abstract: Using notion of generator polynomial matrices of quasi-cyclic codes, we show a necessary and sufficient condition for these codes to be linear complementary dual. This extends the well-known result by Yang and Massey on cyclic codes to quasi-cyclic codes. As an application we present various examples of optimal binary LCD quasi-cyclic codes.

2020 MSC: 94B60, 94B15, 94B05, 11T71

Keywords: LCD code, Quasi-cyclic code, Reversible code, Optimal code, Generator polynomial matrix

1. Introduction

A linear code C with $C \cap C^{\perp} = \{0\}$ is called a linear complementary dual (LCD) code, where $C^{\perp}$ is the dual code of C. The following theorem gives a necessary and sufficient condition for cyclic codes to be LCD:

Theorem 1.1 ([11, Lemma]). *Let g be a generator polynomial of a cyclic code C over a finite field $\mathbb{F}_q$ of length m. Then*

$$C \text{ is LCD if and only if } \gcd(\widetilde{a}, g) = 1,$$

where $a \in \mathbb{F}_q[x]$ with $ag = 1 - x^m$ and $\widetilde{a}$ is the monic reciprocal polynomial of a.

We denote by ${}^{\mathrm{r}}C$ the reversed code of a code C which is obtained by reversing all codewords of C with respect to coordinate order. A code C is reversible if $C = {}^{\mathrm{r}}C$. As a corollary of Theorem 1.1, it was shown that linear complementary duality and reversibility of certain cyclic codes are equivalent:

Norifumi Ojiro, Hajime Matsui; Toyota Technological Institute, 2–12–1 Hisakata, Tempaku, Nagoya, Aichi, 468-8511, Japan, (email:norifumi.ojiro@gmail.com, matsui@sci.kagoshima-u.ac.jp).

Corollary 1.2 ([11, Corollary]). *Let C be an $\mathbb{F}_q$-cyclic code of length m. Suppose* $\gcd(m,q)=1$. *Then, C is LCD if and only if C is reversible.*

A linear code in $\mathbb{F}_q^{m\ell}$ is said to be quasi-cyclic with ℓ cyclic blocks if it is invariant under the cyclic shift:

$$\mathbb{F}_q^{m\ell} \ni (c_{1,0}, c_{1,1}, \cdots, c_{1,m-1}, \cdots, c_{\ell,0}, c_{\ell,1} \cdots, c_{\ell,m-1}) \longmapsto (c_{1,1}, \cdots, c_{1,m-1}, c_{1,0}, \cdots, c_{\ell,1}, \cdots, c_{\ell,m-1}, c_{\ell,0}) \in \mathbb{F}_q^{m\ell},$$

cf. [2],[4],[9],[10],[12]. When $\ell = 1$, it is equal to a cyclic code.

Let $R = \mathbb{F}_q[x]$ and $\mathbb{L} = R^\ell$. Let $M_{\ell,\ell'}(R)$ be the set of $(\ell \times \ell')$-matrices with entries in R, which is abbreviated to $M_\ell(R)$ if $\ell = \ell'$, and $GL_\ell(R)$ the set of invertible elements of $M_\ell(R)$.

The map $\rho : \mathbb{F}_q^{m\ell} \to \mathbb{L}/(1-x^m)\mathbb{L}$ defined by

$$(c_{1,0}, \cdots, c_{1,m-1}, \cdots, c_{\ell,0}, \cdots, c_{\ell,m-1}) \longmapsto \left(\sum_{k=0}^{m-1} c_{1,k}x^k, \cdots, \sum_{k=0}^{m-1} c_{\ell,k}x^k \right)$$

gives an $\mathbb{F}_q$-linear isomorphism, which sends quasi-cyclic codes in $\mathbb{F}_q^{m\ell}$ to R-modules in $\mathbb{L}/(1-x^m)\mathbb{L}$. This implies that any quasi-cyclic code C in $\mathbb{F}_q^{m\ell}$ is represented by a matrix $G \in M_\ell(R)$ such that $\rho(C) = \mathbb{L}G/(1-x^m)\mathbb{L}$. The matrix G satisfies $AG = GA = (1-x^m)I$ for some $A \in M_\ell(R)$, where I is the identity matrix of $M_\ell(R)$. We call such G a generator polynomial matrix, and denote by C_G the quasi-cyclic code with G as a generator polynomial matrix. Note that $C_G = C_{MG}$ for any $M \in GL_\ell(R)$. By applying row transformations over R, the matrix G can be uniquely transformed to a reduced matrix, that is, we can assume that $G = (g_{i,j})$ is upper triangular, $g_{i,i}$ are monic polynomials and $\deg(g_{i,j}) < \deg(g_{j,j})$ for any $i < j$. If G is reduced, $A = (a_{i,j})$ is automatically an upper triangular matrix with monic diagonal entries and satisfies $\deg(a_{i,j}) < \deg(a_{i,i})$ for any $i < j$.

The dual code and the reversed code of a quasi-cyclic code in $\mathbb{F}_q^{m\ell}$ are again quasi-cyclic codes in $\mathbb{F}_q^{m\ell}$. Put

$$G^\perp = \mathrm{diag}\left(x^{m+\deg(a_{i,i})}\right) {}^{\mathrm{t}}A(x^{-1}) + (1-x^m)\mathrm{diag}(a^*_{i,i}),$$
$${}^{\mathrm{r}}G = \left\{\mathrm{diag}\left(x^{m+\deg(g_{i,i})}\right) G(x^{-1}) + (1-x^m)\mathrm{diag}(g^*_{i,i})\right\} J,$$

where $\mathrm{diag}(a^*_{i,i})$ is the diagonal matrix with $a^*_{i,i}$ as (i,i)-entries, $a^*_{i,i} = x^{\deg(a_{i,i})}a_{i,i}(x^{-1})$ is the reciprocal polynomial of $a_{i,i}$, ${}^{\mathrm{t}}A(x^{-1})$ is the transposed matrix of $A(x^{-1})$ and J is the backward identity matrix of $M_\ell(R)$. Then ${C_G}^\perp = C_{G^\perp}$ and ${}^{\mathrm{r}}C_G = C_{{}^{\mathrm{r}}G}$, and C_G is reversible (resp. self-dual) if and only if $\mathbb{L}{}^{\mathrm{r}}G = \mathbb{L}G$ (resp. $\mathbb{L}G^\perp = \mathbb{L}G$), cf. [6],[7],[9],[10], where these facts are proven using the same techniques in [9]. Note that $|G^\perp| = \prod_{i=1}^\ell a^*_{i,i} = |A|^*$ and $|{}^{\mathrm{r}}G| = \pm\prod_{i=1}^\ell g^*_{i,i} = \pm|G|^*$, where $|A|$ is the determinant of A. For $\ell = 1$ we have $A = a$ and $a^* = c\,\widetilde{a}$ for some $c \in \mathbb{F}_q \setminus \{0\}$.

Using the decomposition via Chinese remainder theorem, the characterization of LCD quasi-cyclic codes was investigated in [4],[12]. For 1-generator quasi-cyclic codes, some analogies of Theorem 1.1 were given in [2],[3],[12]. For general quasi-cyclic codes, only a sufficient condition for the codes to be LCD was given in [2]. In the next section, we will extend Theorem 1.1 and Corollary 1.2 to the case of quasi-cyclic codes.

2. Results

Theorem 2.1. *Let $G \in M_\ell(R)$ be the reduced generator polynomial matrix of a quasi-cyclic code of length $m\ell$. Then*

$$C_G \text{ is LCD if and only if there exists } P \in GL_{2\ell}(R) \text{ such that } P\begin{pmatrix} G \\ G^\perp \end{pmatrix} = \begin{pmatrix} I \\ O \end{pmatrix}.$$

Proof. We will prove the following equivalences:

$$\begin{aligned} C_G \cap {C_G}^\perp = \{0\} &\iff C_G + {C_G}^\perp = \mathbb{F}_q^{m\ell} && (1)\\ &\iff \mathbb{L}G + \mathbb{L}G^\perp = \mathbb{L} && (2)\\ &\iff \text{There exist } X, Y \in M_\ell(R) \text{ such that } XG + YG^\perp = I && (3)\\ &\iff \text{There exists } P \in GL_{2\ell}(R) \text{ such that } P\begin{pmatrix} G \\ G^\perp \end{pmatrix} = \begin{pmatrix} I \\ O \end{pmatrix}. && (4) \end{aligned}$$

Proof of (1): Since $\dim_{\mathbb{F}_q}(C_G) + \dim_{\mathbb{F}_q}({C_G}^\perp) = \dim_{\mathbb{F}_q}(\mathbb{F}_q^{m\ell})$, we have

$$\begin{aligned} \dim_{\mathbb{F}_q}(C_G + {C_G}^\perp) &= \dim_{\mathbb{F}_q}(C_G) + \dim_{\mathbb{F}_q}({C_G}^\perp) - \dim_{\mathbb{F}_q}(C_G \cap {C_G}^\perp) \\ &= \dim_{\mathbb{F}_q}(\mathbb{F}_q^{m\ell}) - \dim_{\mathbb{F}_q}(C_G \cap {C_G}^\perp), \end{aligned}$$

this implies (1).
Proof of (2): Since ρ is an $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_q^{m\ell}$ to $\mathbb{L}/(1-x^m)\mathbb{L}$, we have

$$\begin{aligned} C_G + {C_G}^\perp = \mathbb{F}_q^{m\ell} &\iff \rho(C_G) + \rho({C_G}^\perp) = \rho(\mathbb{F}_q^{m\ell}) \\ &\iff \mathbb{L}G/(1-x^m)\mathbb{L} + \mathbb{L}G^\perp/(1-x^m)\mathbb{L} = \mathbb{L}/(1-x^m)\mathbb{L} \\ &\iff (\mathbb{L}G + \mathbb{L}G^\perp)/(1-x^m)\mathbb{L} = \mathbb{L}/(1-x^m)\mathbb{L} \\ &\iff \mathbb{L}G + \mathbb{L}G^\perp = \mathbb{L}. \end{aligned}$$

Proof of (3): Obvious.
Proof of (4): For "⇒", put $P = \begin{pmatrix} X & Y \\ A & -B \end{pmatrix}$, where B is the matrix in $M_\ell(R)$ such that $B\,G^\perp = (1-x^m)I$, see [6, Section 5]. Then we have

$$P\begin{pmatrix} G \\ G^\perp \end{pmatrix} = \begin{pmatrix} I \\ O \end{pmatrix}.$$

Let us prove that P belongs to $GL_{2\ell}(R)$. Note that $\dim_{\mathbb{F}_q}(C_G) = m\ell - \deg|G|$ for any code C_G in $\mathbb{F}_q^{m\ell}$. Since $m\ell = \dim_{\mathbb{F}_q}(C_G) + \dim_{\mathbb{F}_q}({C_G}^\perp)$, one has $m\ell - \deg|G| - \deg|G^\perp| = 0$, or equivalently $\deg\left(|(1-x^m)I||G|^{-1}|G^\perp|^{-1}\right) = 0$, and so $|A| = c\,|G^\perp|$ for some $c \in \mathbb{F}_q \setminus \{0\}$. On the other hand, we have

$$P\begin{pmatrix} G & O \\ O & G^\perp \end{pmatrix}\begin{pmatrix} I & I \\ O & I \end{pmatrix}\begin{pmatrix} I & O \\ -XG & I \end{pmatrix} = \begin{pmatrix} O & I \\ AG & O \end{pmatrix}.$$

Therefore $|P||G||G^\perp| = -|A||G|$, that is, $|P| = -c$, this means $P \in GL_{2\ell}(R)$. The converse is obvious. □

When $\ell = 1$ we have $G = g$, $G^\perp = a^*$ and $\gcd(a^*, g) = 1 \iff \gcd(\widetilde{a}, g) = 1$, thus our theorem agrees with Theorem 1.1.

Remark 2.2. Let $\mathcal{J} = \{j \in \mathbb{Z} \mid 1 \le j \le 2\ell\}$ and $\mathcal{I}$ a subset of ℓ elements of $\mathcal{J}$, especially, $\mathcal{I}_0 = \{j \in \mathbb{Z} \mid 1 \le j \le \ell\}$. Let $|M_{\mathcal{I},\mathcal{I}_0}|$ denote the $(\ell \times \ell)$-minor of $M \in M_{2\ell,\ell}(R)$ determined by $(\mathcal{I}, \mathcal{I}_0)$, that is, the determinant of the $(\ell \times \ell)$-submatrix of M obtained by taking rows in $\mathcal{I}$ in regular order.

Since $GL_{2\ell}(R)$ is generated by row transformations over R and such transformations leave

$$\gcd\{|M_{\mathcal{I},\mathcal{I}_0}| \mid \text{for all } \mathcal{I} \subset \mathcal{J}\}$$

invariant, we have by Theorem 2.1 the following equivalent:

$$\begin{aligned} C_G \textit{ is LCD} &\iff \begin{pmatrix} G \\ G^\perp \end{pmatrix} \textit{ can be transformed by row transformations over } R \textit{ to } \begin{pmatrix} I \\ O \end{pmatrix} \\ &\iff \gcd\left\{ \left| \begin{pmatrix} G \\ G^\perp \end{pmatrix}_{\mathcal{I},\mathcal{I}_0} \right| \;\middle|\; \text{for all } \mathcal{I} \subset \mathcal{J} \right\} = 1. \end{aligned}$$

Therefore if $\gcd(|A|^*, |G|) = 1$ then C_G is LCD. But the converse is generally not true except for $\ell = 1$.

Example 2.3. Let $q = 2$, $\ell = 2$, $m = 4$,

$$G = \begin{pmatrix} 1+x^2 & x \\ 0 & 1+x^2 \end{pmatrix} \text{ and } G^{\perp} = \begin{pmatrix} 1+x^2 & 0 \\ x^5 & 1+x^2 \end{pmatrix}.$$

Then

$$\begin{pmatrix} G \\ G^{\perp} \end{pmatrix} = \begin{pmatrix} 1+x^2 & x \\ 0 & 1+x^2 \\ 1+x^2 & 0 \\ x^5 & 1+x^2 \end{pmatrix}.$$

Putting

$$P = \begin{pmatrix} x^2+x^4 & x+x^3 & 1 & x \\ x & 1 & x & 0 \\ 1+x^2 & x & 1+x^2 & 0 \\ 0 & 1+x^2 & x^5 & 1+x^2 \end{pmatrix},$$

we have $P \in GL_4(R)$ and $P \begin{pmatrix} G \\ G^{\perp} \end{pmatrix} = \begin{pmatrix} I \\ O \end{pmatrix}$, and by Theorem 2.1, C_G is LCD.

Of course, it can be verified by the equivalent of Remark 2.2. For simplicity, denoting $\left| \begin{pmatrix} G \\ G^{\perp} \end{pmatrix}_{\{i,j\},\mathcal{I}_0} \right|$ by $\{i,j\}$, we have

$$\{1,2\} = |G| = (1+x)^4,\ \{1,3\} = \begin{vmatrix} 1+x^2 & x \\ 1+x^2 & 0 \end{vmatrix} = x(1+x)^2,$$
$$\{1,4\} = \begin{vmatrix} 1+x^2 & x \\ x^5 & 1+x^2 \end{vmatrix} = 1+x^4+x^6,\ \{2,3\} = \begin{vmatrix} 0 & 1+x^2 \\ 1+x^2 & 0 \end{vmatrix} = (1+x)^4,$$
$$\{2,4\} = \begin{vmatrix} 0 & 1+x^2 \\ x^5 & 1+x^2 \end{vmatrix} = x^5(1+x)^2,\ \{3,4\} = |G^{\perp}| = (1+x)^4.$$

Since $\gcd(\{1,2\},\dots,\{3,4\}) = 1$, C_G is LCD.

In [11], Yang and Massey gave the following theorem equivalent with Theorem 1.1:

Theorem 1.1′ ([11, Theorem]). *Let $g \in R$ be the reduced generator polynomial of a cyclic code of length m. Then*

$$C_g \text{ is LCD if and only if } g = cg^* \text{ for } c \in \mathbb{F}_q \setminus \{0\} \text{ and } \gcd(a, g) = 1.$$

For quasi-cyclic codes, the straightforward generalization of this theorem is not true. Indeed, for G of Example 2.3 we have $A = G$, and so $XA + YG \neq I$ for all $X, Y \in M_\ell(R)$.

Remark 2.4. Because the gcd of two polynomials in $\mathbb{F}_q[x]$ of degree $\leq m$ can be computed in $O(m \log^2 m)$ [8, Corollary 2], the confirmation of LCD property by checking $P \begin{pmatrix} G \\ G^{\perp} \end{pmatrix} = \begin{pmatrix} I \\ O \end{pmatrix}$ for some $P \in GL_{2\ell}(R)$ through elementary row operations over R can be done with $O(\ell^2 m \log^2 m) = O(\ell n \log^2 m)$. This indicates that our method has less computational complexity than the conventional method shown by [5, Proposition 1], since the complexity of computing $\mathcal{G}\,({}^{\mathrm{t}}\mathcal{G})$ is $O(nk^2) = O(n^3)$, where $\mathcal{G} \in M_{k,n}(\mathbb{F}_q)$ is a generator matrix. Further, since our method treats $G \in M_\ell(R)$ instead of $\mathcal{G} \in M_{k,n}(\mathbb{F}_q)$, the data size is reduced by ℓ/k times for $\ell/k < 1$ in many important cases.

Corollary 2.5. *Let G be as in Theorem 2.1. Suppose that there exists $P \in GL_{2\ell}(R)$ such that $P \begin{pmatrix} {}^{\mathrm{r}}G \\ G^{\perp} \end{pmatrix} = \begin{pmatrix} I \\ O \end{pmatrix}$. Then, C_G is LCD if and only if C_G is reversible.*

Proof. By the same argument as in the proof of Theorem 2.1, we have

$$\begin{aligned}\text{there exists } P \in GL_{2\ell}(R) \text{ such that } P\begin{pmatrix}{}^{\mathrm{r}}G\\ G^{\perp}\end{pmatrix} = \begin{pmatrix}I\\ O\end{pmatrix} &\iff \mathbb{L}\,{}^{\mathrm{r}}G + \mathbb{L}G^{\perp} = \mathbb{L}\\ &\iff {}^{\mathrm{r}}C_G + {C_G}^{\perp} = \mathbb{F}_q^{m\ell}\\ &\iff {}^{\mathrm{r}}C_G \cap {C_G}^{\perp} = \{0\}.\end{aligned}$$

Combining with the proof of Theorem 2.1, we have the desired assertion. □

Remark 2.6. When $\ell = 1$, C_G is a cyclic code of length m, $A = a$ and $G = g$ with $ag = 1 - x^m$. If $\gcd(m, q) = 1$ then $1 - x^m$ decomposes into different irreducible polynomials in $\mathbb{F}_q[x]$, and so $\gcd(a, g) = \gcd(a^*, g^*) = 1$. Then there exists $P \in GL_2(R)$ such that $P\begin{pmatrix}g^*\\ a^*\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix}$ by the same argument as in the proof for "⇒" of (4). Since ${}^{\mathrm{r}}G = g^*$ and $G^{\perp} = a^*$, Corollary 2.5 induces Corollary 1.2.

In the following table, we will give various examples of binary LCD quasi-cyclic codes with $\ell = 2$ which are obtained by applying our theorem and attain the bounds in [1, Tables 1,2]. In the table, n, k and d mean length, dimension and minimum weight, respectively, and we write e.g. $[0, 2, 3, 8]$ to mean $1 + x^2 + x^3 + x^8 \in \mathbb{F}_2[x]$.

References

[1] S. Bouyuklieva, Optimal binary LCD codes, Designs, Codes and Cryptography, 89(11) (2021) 2441–2461.

[2] M. Esmaeili, S. Yari, On complementary-dual quasi-cyclic codes, Finite Fields and Their Applications,15(3) (2009) 375–386.

[3] C. Guan, R. Li, Z. Ma, On Euclidean, Hermitian and symplectic quasi-cyclic complementary dual codes, Preprint: arXiv:2301.00945 (2023).

[4] C. Güneri, B. Özkaya, P. Solé, Quasi-cyclic complementary dual codes, Finite Fields and Their Applications, 42 (2016) 67–80.

[5] J. L. Massey, Linear codes with complementary duals, Discrete Mathematics, 106/107 (1992) 337–342.

[6] H. Matsui, On generator and parity-check polynomial matrices of generalized quasi-cyclic codes, Finite Fields and Their Applications, 34 (2015) 280–304 .

[7] H. Matsui, A modulus factorization algorithm for self-orthogonal and self-dual quasi-cyclic codes via polynomial matrices, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 104(11) (2021) 1649–1653.

[8] R. T. Moenck, Fast computation of GCDs, Proceedings of the Fifth Annual ACM Symposium on Theory of Computing (1973).

[9] N. Ojiro, K. Kaneko, H. Matsui, An efficient algorithm for constructing reversible quasi-cyclic codes via Chinese remainder theorem, Finite Fields and Their Applications, 89 (2023) 102204.

[10] R. Taki Eldin,, H. Matsui, Linking reversed and dual codes of quasi-cyclic codes, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 105(3) (2022) 381–388.

[11] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Mathematics, 12 (1994) 391–393 .

[12] M. Zeraatpisheh, M. Esmaeili, T. A. Gulliver, Quasi-cyclic codes: algebraic properties and applications, Computational and Applied Mathematics 39(96) (2020).

Table 1. Binary LCD quasi-cyclic codes with good and optimal parameters

n	k	d	$G = \begin{pmatrix} g_{1,1} & g_{1,2} \\ 0 & g_{2,2} \end{pmatrix}$
20	8	6	$g_{1,1} = [0, 2]$, $g_{1,2} = [0, 3, 4, 5, 6, 7, 8, 9]$, $g_{2,2} = [0, 10]$.
22	11	6	$g_{1,1} = [0, 1]$, $g_{1,2} = [0, 2, 3, 8]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10]$.
24	8	8	$g_{1,1} = [0, 1, 2, 4, 5, 6]$, $g_{1,2} = [0, 4]$, $g_{2,2} = [0, 1, 3, 4, 6, 7, 9, 10]$.
24	12	6	$g_{1,1} = [0, 1, 2, 3]$, $g_{1,2} = [0, 4, 5]$, $g_{2,2} = [0, 1, 4, 5, 8, 9]$.
26	12	8	$g_{1,1} = [0, 1]$, $g_{1,2} = [0, 1, 3, 7, 9, 10, 11, 12]$, $g_{2,2} = [0, 13]$.
26	13	7	$g_{1,1} = [0, 1]$, $g_{1,2} = [0, 2, 3, 4, 5, 6, 7, 9]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]$.
26	14	6	$g_{1,1} = [0]$, $g_{1,2} = [0, 3, 4, 5, 6, 9, 11]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]$.
28	14	7	$g_{1,1} = [0, 2, 3]$, $g_{1,2} = [0, 2, 4, 9]$, $g_{2,2} = [0, 2, 3, 4, 7, 9, 10, 11]$.
30	11	9	$g_{1,1} = [0, 2, 3, 4, 6]$, $g_{1,2} = [0, 3, 5, 8]$, $g_{2,2} = [0, 1, 3, 4, 6, 7, 9, 10, 12, 13]$.
30	12	8	$g_{1,1} = [0, 4, 6, 7]$, $g_{1,2} = [0, 2, 5, 7, 9, 10]$, $g_{2,2} = [0, 3, 4, 6, 8, 9, 10, 11]$.
30	15	7	$g_{1,1} = [0, 1, 3, 5]$, $g_{1,2} = [0, 3, 6, 9]$, $g_{2,2} = [0, 1, 2, 4, 5, 8, 10]$.
32	16	8	$g_{1,1} = [0, 1, 2, 3]$, $g_{1,2} = [0, 1, 7, 8, 12]$, $g_{2,2} = [0, 1, 4, 5, 8, 9, 12, 13]$.
34	9	13	$g_{1,1} = [0, 1, 3, 6, 8, 9]$, $g_{1,2} = [0, 2, 7, 8, 9, 10, 11, 12]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]$.
34	17	8	$g_{1,1} = [0, 1]$, $g_{1,2} = [0, 1, 2, 3, 4, 5, 6, 7, 10, 13, 14, 15]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]$.
34	18	7	$g_{1,1} = [0]$, $g_{1,2} = [0, 1, 4, 5, 6, 7, 8, 9, 11, 13, 14]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]$.
36	14	10	$g_{1,1} = [0, 1, 2, 3, 4, 5]$, $g_{1,2} = [0, 1, 2, 6, 7, 8, 9, 10, 11, 13, 16]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]$.
36	16	9	$g_{1,1} = [0, 2, 4]$, $g_{1,2} = [0, 1, 2, 3, 6, 7, 9, 14]$, $g_{2,2} = [0, 2, 4, 6, 8, 10, 12, 14, 16]$.
36	18	8	$g_{1,1} = [0, 1, 2]$, $g_{1,2} = [0, 2, 6, 7, 8, 11, 14, 15]$, $g_{2,2} = [0, 1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16]$.
36	20	6	$g_{1,1} = [0, 1, 2]$, $g_{1,2} = [0, 1, 4, 5, 6]$, $g_{2,2} = [0, 1, 2, 6, 7, 8, 12, 13, 14]$.
36	22	6	$g_{1,1} = [0]$, $g_{1,2} = [0, 1, 2, 3, 4, 5, 6, 9, 10, 11]$, $g_{2,2} = [0, 2, 6, 8, 12, 14]$.
38	18	8	$g_{1,1} = [0, 1]$, $g_{1,2} = [0, 1, 4, 5, 11, 12, 14, 15]$, $g_{2,2} = [0, 19]$.
38	19	8	$g_{1,1} = [0, 1]$, $g_{1,2} = [0, 3, 7, 8, 10, 14, 15]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]$.
38	20	7	$g_{1,1} = [0]$, $g_{1,2} = [0, 5, 7, 11, 12, 15]$, $g_{2,2} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]$.
40	16	10	$g_{1,1} = [0, 4]$, $g_{1,2} = [0, 1, 3, 8, 9, 11, 12, 16]$, $g_{2,2} = [0, 20]$.
40	20	9	$g_{1,1} = [0, 1, 2, 3]$, $g_{1,2} = [0, 4, 5, 7, 10, 13, 15]$, $g_{2,2} = [0, 1, 4, 5, 8, 9, 12, 13, 16, 17]$.
40	24	5	$g_{1,1} = [0]$, $g_{1,2} = [0, 1, 3, 4, 5, 7, 12]$, $g_{2,2} = [0, 4, 8, 12, 16]$.