On Almost Perfect Linear Lee Codes of Packing Radius 2

Xiaodong Xu\textsuperscript{a} and Yue Zhou\textsuperscript{a}

Abstract—More than 50 years ago, Golomb and Welch conjectured that there is no perfect Lee codes $C$ of packing radius $r$ in $\mathbb{Z}^n$ for $r \geq 2$ and $n \geq 3$. Recently, Leung and the second author proved that if $C$ is linear, then the Golomb-Welch conjecture is valid for $r = 2$ and $n \geq 3$. In this paper, we consider the classification of linear Lee codes with the second-best possibility, that is the density of the lattice packing of $\mathbb{Z}^n$ by Lee spheres $S(n, r)$ equals $\frac{|S(n, r)|}{|\mathbb{Z}^n|}$. We show that, for $r = 2$ and $n \equiv 0, 3, 4 \pmod{6}$, this packing density can never be achieved.

Index Terms—Lee code, perfect code, Cayley graph, Golomb-Welch conjecture.

I. INTRODUCTION

Let $\mathbb{Z}$ denote the ring of integers. For two words $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n) \in \mathbb{Z}^n$, the Lee distance (also known as $\ell_1$-norm, taxicab metric, rectilinear distance or Manhattan distance) between them is defined by

$$d_L(x, y) = \sum_{i=1}^{n} |x_i - y_i| \text{ for } x, y \in \mathbb{Z}^n.$$  

A Lee code $C$ is just a subset of $\mathbb{Z}^n$ endowed with the Lee distance. If $C$ further has the structure of an additive group, i.e. $C$ is a lattice in $\mathbb{Z}^n$, then we call $C$ a linear Lee code. Lee codes have many practical applications, for example, constrained and partial-response channels [2], flash memory [3] and interleaving schemes [4].

The minimum distance between any two distinct elements in $C$ is called the minimum distance of $C$. Given a Lee code of minimum distance $2r + 1$, for any $x \in \mathbb{Z}^n$, if one can always find a unique $c \in C$ such that $d_L(x, c) \leq r$, then $C$ is called a perfect code. This is equivalent to

$$\mathbb{Z}^n = \bigcup_{c \in C} (S(n, r) + c),$$

where

$$S(n, r) := \{ (x_1, \cdots, x_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} |x_i| \leq r \}$$

and $S(n, r) + c := \{ v + c : v \in S(n, r) \}$. Thus, the existence of a perfect Lee code implies a tiling of $\mathbb{Z}^n$ by Lee spheres of radius $r$.

Perfect Lee codes exist for $n = 1, 2$ and any $r$, and for $n \geq 3$ and $r = 1$. Golomb and Welch [5] conjectured that there are no more perfect Lee codes for other choices of $n$ and $r$. This conjecture is still far from being solved, despite many efforts and various approaches applied on it. We refer the reader to the recent survey [6] and the references therein. For perfect codes with respect to other metrics, see the very recent monograph [7] by Etzion.

Let $L(n, r)$ denote the union of $n$-cubes centered at each point of $S(n, r)$ in $\mathbb{R}^n$. It is not difficult to see that there is a tiling of $\mathbb{Z}^n$ by $S(n, r)$ if and only if there is a tiling of $\mathbb{R}^n$ by $L(n, r)$. Figure 1 shows a (lattice) tiling of $\mathbb{R}^2$ by $L(2, 2)$. As the shape of $L(n, r)$ is close to a cross-polytope when $r$ is large enough, one can use the cross-polytope packing density to prove the Golomb-Welch conjecture provided that $r$ is large enough compared with $n$. In fact, this idea was first applied by Golomb and Welch themselves in [5]. There are some other geometric approaches, including the analysis of some local configurations of the boundary of Lee spheres in a tiling by Post [8], and the density trick by Astola [9] and Lepistö [10].

Fig. 1. Tiling of $\mathbb{R}^2$ by $L(2, 2)$. 

Manuscript received 5 August 2021; revised 26 December 2022; accepted 2 June 2023. Date of publication 19 June 2023; date of current version 15 September 2023. The work of Xiaodong Xu was supported in part by the Natural Science Foundation of China under Grant 71471176. The work of Yue Zhou was supported in part by the Natural Science Foundation of Hunan Province under Grant 2019RS2031 and in part by the Training Program for Excellent Young Innovators of Changsha under Grant kq2106006. An earlier version of this paper was presented at the 12th International Workshop on Coding and Cryptography [1]. (Corresponding author: Yue Zhou.) 

Xiaodong Xu is with the Guangxi Academy of Sciences, Nanning 530007, China. 

Yue Zhou is with the Department of Mathematics, National University of Defense Technology, Changsha 410073, China (e-mail: yue.zhou.ovgu@gmail.com).

Communicated by C. Xing, Associate Editor for Coding and Decoding. 
Val color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2023.3287222. 
Digital Object Identifier 10.1109/TIT.2023.3287222
A Lee code is called \textit{t-quasi-perfect} if its packing radius and covering radius are \( t \) and \( t+1 \), respectively. Note that an APLL code is a quasi-perfect Lee code, but a quasi-perfect Lee code is not necessarily almost perfect. For instance, two families of 2-quasi-perfect codes in \( \mathbb{Z}^n \) are constructed in \cite{18} and the packing density equals \( \frac{2n+1}{2(n+1)^2} \), where \( n = 2 \left( \frac{t}{2} \right) \) for a prime \( p \) satisfying \( p \geq 7 \) and \( p \equiv \pm 5 \pmod{12} \). In particular, the packing density equals \( \frac{41}{60} \) when \( n = 4 \), and it tends to \( \frac{1}{2} \) for big \( n \). We refer to \cite{18, 20}, and \cite{21} for more constructions and other results on quasi-perfect Lee codes.

About the existence of APLL codes of packing radius 2, one can apply the symmetric polynomial method in \cite{11} and the algebraic number theory approach in \cite{16} to derive some partial results. For \( n \leq 10^5 \), one can exclude the existence of APLL codes of packing radius 2 for 76,573 choices of \( n \). For more details, see \cite{22}.

The main result of this paper is the following one.

\textbf{Theorem 1:} Let \( n \) be a positive integer. If \( n \equiv 0, 3, 4 \pmod{6} \), then there exists no almost perfect linear Lee code of packing radius 2.

As in \cite{17}, our proof is given by investigating group ring equations in \( \mathbb{Z}[G] \) where \( G \) is of order \( |S(n,2)| = 2(n^2 + n + 1) \). However, the situation here is different from the one appeared in \cite{17}. We consider a special subset \( T \subseteq G \) and show that \( T \) splits into two disjoint subsets \( T_0 \subseteq H \) and \( fT_1 \subseteq fH \) where \( H \) is the unique subgroup of \( G \) of index 2 and \( f \) is the unique involution in \( G \). Then, we analyze the elements appearing in \( (T_0^{(2)} + T_1^{(2)})T_0 \) and \( (T_0^{(2)} + T_1^{(2)})T_1 \). Unfortunately, we could not get any contradiction when \( n \equiv 1, 2, 5 \pmod{6} \). But we conjecture that there is no APLL code for this case when \( n > 2 \).

The rest part of this paper consists of three sections. In Section II, we convert the existence of an almost perfect linear Lee code of packing radius 2 into some conditions in group ring. Then we prove Theorem 1 in Section III. In Section IV, we conclude this paper with several remarks and research problems.

\section{Necessary and Sufficient Conditions in Group Ring}

Let \( \mathbb{Z}[G] \) denote the set of formal sums \( \sum_{g \in G} a_g g \), where \( a_g \in \mathbb{Z} \) and \( G \) is a finite multiplicative group. The addition and the multiplication on \( \mathbb{Z}[G] \) are defined by

\[
\sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g) g,
\]

and

\[
\left( \sum_{g \in G} a_g g \right) \cdot \left( \sum_{g \in G} b_g g \right) := \sum_{g \in G} \left( \sum_{h \in G} a_h b_{h^{-1}g} \right) g,
\]

for \( \sum_{g \in G} a_g g, \sum_{g \in G} b_g g \in \mathbb{Z}[G] \). Moreover,

\[
\lambda \cdot \left( \sum_{g \in G} a_g g \right) := \sum_{g \in G} (\lambda a_g) g
\]

for \( \lambda \in \mathbb{Z} \) and \( \sum_{g \in G} a_g g \in \mathbb{Z}[G] \).

However, it seems that the geometric approaches do not work for small \( r \) and large \( n \). In the past several years, algebraic approaches have been proposed and applied on the existence of perfect linear Lee code for small \( r \). In \cite{11}, Kim introduced a symmetric polynomial method to study this problem for sphere radius \( r = 2 \). This approach has been extended by Zhang and Ge \cite{12}, and Qureshi \cite{13} for \( r \geq 3 \). See \cite{6}, \cite{14}, \cite{15}, and \cite{16} for other related results.

In particular, Leung and the second author \cite{17} succeeded in getting a complete solution to the case with \( r = 2 \): there is no perfect linear Lee code of minimum distance 5 in \( \mathbb{Z}^n \) for \( n \geq 3 \).

It is worth pointing out that the existence of a perfect linear Lee code of minimum distance \( 2r+1 \) in \( \mathbb{Z}^n \) is equivalent to an abelian Cayley graph of degree \( 2n \) and diameter \( r \) whose number of vertices meets the so-called \textit{abelian Cayley Moore bound}; see \cite{16} and \cite{18}. For more results about the degree-diameter problems in graph theory, we refer to the survey \cite{19}.

It is clear that a perfect Lee code \( C \) means the packing density of \( \mathbb{Z}^n \) by \( S(n,r) \) with centers consisting of all the elements in \( C \) is 1. If there is no perfect linear Lee code for \( r \geq 2 \) and \( n \geq 3 \), one may wonder whether the second best is possible, which is about the existence of a lattice packing of \( \mathbb{Z}^n \) by \( S(n,r) \) with density \( \frac{|S(n,r)|}{|S(n,2)|+1} \). We call such a linear Lee code \textit{almost perfect}. In Figure 2, we present a lattice packing of \( \mathbb{Z}^2 \) by \( S(2,2) \), and its packing density is \( \frac{|S(2,2)|}{|S(2,2)|+1} = \frac{13}{14} \). This example and the numbers labeled on the cubes will be explained later in Example 4. For convenience, we abbreviate the term almost perfect linear Lee code to \textit{APLL}

The \textit{packing radius} of a Lee code \( C \) is defined to be the largest integer \( r' \) such that for any element \( w \in \mathbb{Z}^n \) there exists at most one codeword \( c \in C \) with \( d_L(w,c) \leq r' \). The \textit{covering radius} of a Lee code \( C \) is the smallest integer \( r'' \) such that for any element \( w \in \mathbb{Z}^n \) there exists at least one codeword \( c \in C \) with \( d_L(w,c) \leq r'' \). It is clear that a Lee code is perfect if and only if its packing radius and covering radius are the same. For an APLL code with packing density \( \frac{|S(n,r)|}{|S(n,2)|+1} \), its packing radius and covering radius are \( r \) and \( r+1 \), respectively.
For an element $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$ and $t \in \mathbb{Z}$, we define
\[ A^{(t)} := \sum_{g \in G} a_g g^t. \]
A multi-subset $D$ of $G$ can be viewed as an element $\sum_{g \in D} g \in \mathbb{Z}[G]$. In the rest of this paper, by abuse of notation, we will use the same symbol to denote a multi-subset of $G$ and the associated element in $\mathbb{Z}[G]$. Moreover, $|D|$ denotes the number of distinct elements in $D$.

The following result converts the existence of APLL codes into an algebraic combinatorics problem on abelian groups. Its proof is not difficult, and more or less the same as the proof of Theorem 8 in [23].

**Lemma 2:** There is an APLL code of packing radius $r$ in $\mathbb{Z}^n$ if and only if there is an abelian group $G$ and a homomorphism $\varphi : \mathbb{Z}^n \rightarrow G$ such that the restriction of $\varphi$ to $S(n, r)$ is injective and $G \setminus \varphi(S(n, r))$ has only one element.

**Proof:** First, let us prove the necessary part of the condition. Assume that $C$ is an APLL code of packing radius $r$ and $w \in \mathbb{Z}^n$ is an arbitrary element which is not covered by the lattice packing $\bigcup_{c \in C}(S(n, r) + c)$. Then, by the definition of APLL codes, $C$ is a subgroup of $\mathbb{Z}^n$ and
\[ \mathbb{Z}^n = \left( \bigcup_{c \in C}(S(n, r) + c) \right) \cup (w + C). \tag{1} \]
Consider the quotient group $G = \mathbb{Z}^n / C$ and take $\varphi$ to be the canonical homomorphism from $\mathbb{Z}^n$ to $G$. If there are $x, y \in S(n, r)$, such that $\varphi(x) = \varphi(y)$, then $z = x - y \in C$. Since $S(n, r)$ contains $y, x \in S(n, r)$, $z$ must be 0 which implies $x = y$. Therefore, $\varphi$ is injective and $\varphi(w)$ is the unique element not in $\varphi(S(n, r))$.

To prove the sufficient part, one only has to define $C = \ker(\varphi)$. The verification of the almost perfect property of $C$ is straightforward.

The number of elements in a Lee sphere
\[ |S(n, r)| = \sum_{i=0}^{\min\{n, r\}} 2^i \binom{n}{i} \binom{r}{i}, \]
which can be found in [5] and [24].

In particular, when $r = 2$, $|S(n, r)| = 2n^2 + 2n + 1$ and the group $G$ considered in Lemma 2 is of order $2n^2 + 2n + 2$.

The next result translates the existence of an APLL code into a group ring condition. The same result has been proved in [22] in the context of the existence of abelian Moore Cayley graphs with excess one. For completeness, we include a proof here.

**Lemma 3:** There exists an APLL code of packing radius 2 in $\mathbb{Z}^n$ if and only if there is an abelian group $G$ of order $2(n^2 + n + 1)$ and an inverse-closed subset $T \subseteq G$ containing $e$ with $|T| = 2n + 1$ such that
\[ T^2 = 2(G - f) - T^{(2)} + 2ne, \tag{2} \]
where $e$ is the identity element in $G$ and $f$ is the unique element of order 2 in $G$.

**Proof:** The proof of (2) is similar to the proof of Lemma 2.3 in [16]. Suppose that there exists an APLL code of packing radius 2. By Lemma 2, we have a homomorphism $\varphi : \mathbb{Z}^n \rightarrow G$. Define $a_i = \varphi(e_i)$ for $i = 1, \cdots, n$. As the radius equals 2, by definition, $G$ has the following partition
\[ G = \{e, f\} \cup \{a_i^{\pm 1}, a_i^{\pm 2} : i = 1, \cdots, n\} \]
\[ \cup \{a_i^{\pm 1}a_j^{\pm 1} : 1 \leq i < j \leq n\} \]
where $f$ is the unique element of $G$ not in $\varphi(S(n, 2))$.

Let $T = e + \sum_{i=1}^n a_i + \sum_{i=1}^n a_i^{-1}$. Hence $|T| = 2n + 1$. Moreover,
\[ T^2 = e + 2\sum_{i=1}^n a_i + 2\sum_{i=1}^n a_i^{-1} + (\sum_{i=1}^n a_i^2) + (\sum_{i=1}^n a_i^{-2}) \]
\[ + 2 \left( \sum_{i=1}^n a_i \right) \left( \sum_{i=1}^n a_i^{-1} \right) \]
\[ = (2n + 1) + 2\sum_{i=1}^n a_i + \sum_{i=1}^n a_i^{-1} + \sum_{i=1}^n (a_i^2 + a_i^{-2}) \]
\[ + 2 \sum_{1 \leq i < j \leq n} a_i^{\pm 1}a_j^{\pm 1} \]
\[ = 2ne + 2(G - f) - T^{(2)}. \]
Therefore (2) is proved.

Applying the map $x \rightarrow x^{(-1)}$ on the both sides of (2), we get
\[ T^2 = 2(G - f) - T^{(2)} + 2ne, \]
because $T$ is inverse-closed. By comparing this equation with (2), we see $f = f^{-1}$. As $n^2 + n + 1$ is always odd, there is only one involution in $G$ which is $f$.

Next we prove the sufficiency part. Given an inverse-closed subset $T \subseteq G$ containing $e$ with $|T| = 2n + 1$ satisfying (2), we define a homomorphism $\varphi : \mathbb{Z}^n \rightarrow G$ by $\varphi(e_i) = a_i$. It is clear that $\varphi$ is completely determined by the value of all $a_i$’s. As $T$ is inverse-closed and $|T| = 2n + 1$, the restriction of $\varphi$ to $S(n, 1)$ is injective. Furthermore, by checking the coefficients of elements in (2) as in the necessity part of the proof, we see that
\[ G \setminus \{f\} = \{e\} \cup \{a_i^{\pm 1}, a_i^{\pm 2} : i = 1, \cdots, n\} \]
\[ \cup \{a_i^{\pm 1}a_j^{\pm 1} : 1 \leq i < j \leq n\}, \]
that is $G \setminus \{f\} = \varphi(S(n, 2))$. By Lemma 2, $C = \ker(\varphi)$ is an APLL code of packing radius 2.

**Remark 1:** Similar to the alternative proof of the uniqueness of $f \in G$ in Lemma 3, we can show that if there is an APLL code of packing radius 2, then there is a group $G$ of even order with a unique involution in $G$ by checking $a_i \cdots a_j = a_i^{-1} \cdots a_j^{-1}$ for $j \leq r$. However, the corresponding group ring equations become more complicated, and we are not going to investigate them in this paper.

The following two examples show that for $n = 1, 2$, there do exist APLL codes of packing radius 2. The corresponding result of Example 4 (b) has been already depicted in Figure 2.
Example 4: Let $C_m$ denote the cyclic group generated by $g$ of order $m$.
(a) $n = 1$, $G = C_6$ and $T = \{e, g^{\pm 1}\}$.
(b) $n = 2$, $G = C_{14}$ and $T = \{e, g^{\pm 2}, g^{\pm 3}\}$.

In Figure 2, we label each element in $\mathbb{Z}^2$ which is mapped to $\varphi(e_1) = g^2$ by 2 and those mapped to $\varphi(e_2) = g^3$ by 3. The center of every Lee sphere is labeled by 0. The holes are all labeled by 7 which corresponds to the unique involution $g^7$ in $G$.

In (a) and (b), $G$ has a unique subgroup $H$ of order $n^2 + n + 1$. We will obtain further necessary and sufficient conditions in terms of subsets in $H$ in the later part, and the corresponding results for (a) and (b) will be given in Example 6.

Remark 2: It is easy to check that $\{e, g^{\pm 3}, g^{\pm 2}\} \subseteq C_{13}$ defines a perfect linear code in $\mathbb{Z}^2$ as a lattice with basis $\{(2, 3), (-3, 2)\}$; see Figure 1. Accordingly the basis of the APLL code in Figure 2 generated by $\{e, g^{\pm 3}, g^{\pm 2}\} \subseteq C_{14}$ is $\{(4, 2), (3, 3)\}$.

It is obvious that $6\mathbb{Z}$ is the unique APLL code of packing radius 2 in $\mathbb{Z}$. In fact, we can further prove that all APLL codes of packing radius 2 in $\mathbb{Z}$ are Lee-isometric as follows.

First, if $T \subseteq C_{14} = G$ satisfies (2), $T$ must contain a primitive element of $C_{14}$. Moreover, it is easy to check that if we assume that $e, g^{\pm 1} \in T$, then $T$ must be $\{e, g, g^2, g^3\}$. Thus, all $T$ satisfying Lemma 2.2 must be of the shape $\{e, g^{\pm 3}, g^{\pm 2}\}$ for some $\psi$ in the automorphism group $\text{Aut}(C_{14})$ of $C_{14}$.

Second, for any homomorphism $\varphi: \mathbb{Z}^n \to G$, set $t_i = \varphi(e_i)$ and $T := \{e\} \cup \{t_i^{\pm 1}: i = 1, \ldots, n\}$. For any $\psi \in \text{Aut}(G)$, define a homomorphism $\varphi': \mathbb{Z}^n \to G$ by $\varphi'(e_i) = \psi(t_i)$ and $T' = \{e\} \cup \{\psi(t_i)^{\pm 1}: i = 1, \ldots, n\}$. Then

$$\ker(\varphi') = \left\{ \sum_{i=1}^n a_ie_i : \prod_{i=1}^n \psi(t_i)^{a_i} = e \right\} = \left\{ \sum_{i=1}^n a_ie_i : \prod_{i=1}^n t_i^{a_i} = e \right\} = \ker(\varphi),$$

which means that $\varphi$ and $\varphi'$ define exactly the same Lee code. In particular, $\varphi$ defined by $\varphi(e_1) = \psi(g)$ and $\varphi(e_2) = \psi(g^2)$ provides the same Lee code in $\mathbb{Z}^2$ for every $\psi \in \text{Aut}(C_{14})$.

Finally, we consider different homomorphisms $\varphi: \mathbb{Z}^n \to G$ with the same $T = \{e\} \cup \{t_i^{\pm 1}: i = 1, \ldots, n\}$. Now we must have $\varphi(e_i) = t_i^{p_i}$ where $(p_1, p_2, \ldots, p_n)$ is a permutation of $(1, 2, \ldots, n)$ and $c_i \in \{-1, 1\}$. Let $\varphi_0$ be defined by $\varphi_0(e_i) = t_i$ for $i = 1, \ldots, n$. Then we can obtain $C_0 = \ker(\varphi_0)$ from $C = \ker(\varphi)$ through the linear map $\tau$ defined by $e_i \mapsto t_i^{c_i}$ for $i = 1, \ldots, n$. As $\tau$ is a combination of permutatation of axes and reflections, it is a Lee-isometry of $\mathbb{Z}^2$.

Therefore, there are exactly four APLL codes of packing radius 2 in $\mathbb{Z}^2$, they are all Lee-isometric and their bases are $\{(4, 2), (3, -2)\}$ and its images under the maps in $\mathbb{Z}^2$ defined by $t_1(x, y) = (-x, y)$, $t_2(x, y) = (y, x)$ and $t_3(x, y) = (-y, x)$, respectively.

In Lemma 3, we have obtained some necessary and sufficient condition for the existence of APLL codes of packing radius 2 in terms of a subset $T$ in an abelian group $G$ of order $2(n^2 + n + 1)$. We can further split $T$ into subsets in a subgroup $H$ and its coset $fH$.

Let $H$ denote the unique subgroup of order $n^2 + n + 1$ in $G$. Define $T_0 = T \cap H$ and $T_1 = fT \cap H$. Thus

$$T = T_0 + fT_1.$$ 

By (2),

$$T_0^2 + T_1^2 + 2fT_0T_1 = 2(G - f) - T_0^{(2)} - T_1^{(2)} + 2n \cdot e.$$ 

By considering the above equation intersecting $H$ and $fH$, respectively, we obtain

$$T_0T_1 = H - e, \quad (3)$$

$$T_0^2 + T_1^2 = 2H - T_0^{(2)} - T_1^{(2)} + 2ne. \quad (4)$$

Therefore, we have proved the following result.

Lemma 5: Let $T = T_0 + fT_1 \subseteq G$ with $T_0$ and $T_1 \subseteq H$.

Then the subset $T$ satisfies that $e \in T$, $T^{(-1)} = T$ and (2) if and only if $e \in T_0$, $T_0^{(-1)} = T_0$, $T_1^{(-1)} = T_1$, (3) and (4) hold.

Example 6: The following examples of $T_0$ and $T_1$ are derived from $T$ in Example 4 (a) and (b), respectively. It is easy to check that $T_0$ and $T_1$ satisfy (3) and (4).

(a) For $n = 1$, $G = C_6 = \{g\}$ and $H = 2C_6 = \{g^2\} \cong C_3$. Let $T = \{e, g^{\pm 1}\}$.

Then $T_0 = \{e\}$ and $T_1 = \{g^2, g^4\}$.

(b) For $n = 2$, $G = C_{14} = \{g\}$ and $H = 2C_{14} = \{g^2\} \cong C_7$.

From $T = \{e, g^{\pm 2}, g^{\pm 3}\}$, one gets

$$T_0 = \{e, g^2, g^{12}\} \quad \text{and} \quad T_1 = \{g^4, g^{10}\}.$$ 

Remark 3: A near-factorization of a group $H$ is a pair of (not necessarily inverse-closed) subsets $T_0$ and $T_1$ such that (3) holds. There are very little known results on them. However, it has been proved that, up to translate, $T_0$ and $T_1$ must be inverse-closed; see [25].

The following result is a collection of obvious necessary conditions for $T_0$ and $T_1$, which will be intensively used in Section III.

Lemma 7: Suppose that $T = T_0 + fT_1 \subseteq G$ satisfying $e \in T$, $T^{(-1)} = T$, $|T| = 2n + 1$, (3) and (4). Then the following statements hold.

(a) $e \in T_0$, $e \notin T_1$;

(b) $T_0 \cap T_1 = \emptyset$ and $T_0^{(2)} \cap T_1^{(2)} = \emptyset$;

(c) $T_0 \cap (T_0^{(2)} \setminus \{e\}) = T_0 \cap T_1^{(2)} = \emptyset$;

(d) $\{ab : a \neq b, a, b \in T_0 \cap T_0^{(2)} = \{e\}$;

(e) When $n$ is odd, $|T_0| = n$ and $|T_1| = n + 1$;

(f) When $n$ is even, $|T_0| = n + 1$ and $|T_1| = n$;

(g) There is no common non-identity element in $T_0^2$ and $T_1^2$;

(h) $T_0 \cap T_0^{(3)} = \{e\}$.

Proof: By the definition of $T$ and $T_0$, we have (a). From (3) and the inverse-closed property of $T_1$, we derive $T_0 \cap T_1 = \emptyset$. As gcd(2, |$H$|) = 1, the map $x \mapsto x^2$ on $H$ is a group automorphism. Thus $T_0^{(2)} \cap T_1^{(2)} = \emptyset$ and (b) is proved.

Note that $T_0, T_0^{(2)} \setminus \{e\}$ and $T_1^{(2)}$ are all subsets in $H$. By checking (4), we know that they cannot share any common element. By the same reason, we also prove (d).

From (3), we get $|T_0| \cdot |T_1| = n(n + 1)$. Notice that $|T_0|$ must be odd because it has an involution $x \mapsto x^{-1}$ with a unique fixed element $e$. Together with $|T_0| + |T_1| = 2n + 1$, we derive (e) and (f). By checking the elements appeared in $T_0^2 + T_1^2$ in (4), we get (g).
Finally, we prove (h). It is clear that \( e \in T_0 \cap T_0^{(3)} \). Assume to the contrary that there exists \( b \in T_0 \setminus \{e\} \) such that \( b = a^2 \) for some \( a \in T_0 \). Then \( a^2 = a^{-1}b \in T_0^2 \). As \( a^{-1} \neq b \), this is a contradiction to (d).

In [22], several different approaches have been applied to derive various nonexistence results. In particular, we need the following one in the next section.

Proposition 8 (Corollary 3.1 in [22]): Suppose that \( 8n - 7 \) is not a square in \( \mathbb{Z} \) and one of the following conditions are satisfied:

- \( 3, 7, 19 \) or \( 31 \) divides \( n^2 + n + 1 \);
- \( 13 \mid n^2 + n + 1 \) and \( 8n - 11 \notin \{13k^2 : k \in \mathbb{Z}\} \).

Then there is no inverse-closed subset \( T \subseteq G \) satisfying Lemma 3.

Although Proposition 8 does not work for \( n = 3 \), this situation can be excluded by a direct verification because the group \( G \) is small.

The symmetric polynomial method applied by Kim [11] on the existence of perfect linear Lee codes can be used directly here to derive strong nonexistence results; see Theorem 3.1 in [22]. In particular, it leads to the following results appeared in [22].

Result 9: For \( 3 < n \leq 10^5 \), if \( n^2 + n + 1 \) is a prime, then there is no inverse-closed subset \( T \subseteq G \) satisfying Lemma 3.

III. PROOF OF THE MAIN RESULT

In this section, we are going to prove Theorem 1 by showing the nonexistence of inverse-closed subsets \( T_0, T_1 \subseteq H \) satisfying \( e \in T_0, |T_0| + |T_1| = 2n + 1, (3) \) and (4).

Define \( \hat{T} = T_0 + T_1 \in \mathbb{Z}[H] \). Write \( \hat{T}^{(2)} = \sum_{i=0}^{2n} a_i \) where \( a_0 = e, a_i \in T_0^{(2)} \) for \( i = 0, \ldots, |T_0| - 1 \) and \( a_i \in T_1^{(2)} \) for \( i = |T_0|, \ldots, 2n \). Let \( k_0 = |T_0| \) and \( k_1 = |T_1| \).

By multiplying \( T_0 \) and \( T_1 \) on the both sides of (4), respectively, and rearranging the terms, we get

\[
\hat{T}^{(2)} T_0 = (2k_0 - k_1)H + T_1 - T_0^{(3)} + 2nT_0,
\]

\[
\hat{T}^{(2)} T_1 = (2k_1 - k_0)H + T_0 - T_1^{(3)} + 2nT_1.
\]

Consider the above two equations modulo 3

\[
\hat{T}^{(2)} T_0 \equiv (2k_0 - k_1)H + T_1 - T_0^{(3)} + 2nT_0 \pmod{3},
\]

\[
\hat{T}^{(2)} T_1 \equiv (2k_1 - k_0)H + T_0 - T_1^{(3)} + 2nT_1 \pmod{3}.
\]

Note that \( T_0^{(3)} \equiv T_0^{(3)} \pmod{3} \). If \( 3 \nmid |H| \), then \( T_0^{(3)} \) is a subset; for \( 3 
mid |H| \), we will show that there are only very few elements in \( T_0^{(3)} \) appearing more than once in \( T_0^{(3)} \). Thus, we can derive some strong conditions on the coefficients of most of the elements in the right-hand side of the above two equations. For instance, when \( n \equiv 1 \pmod{3} \) and \( n \) is odd, the first equation becomes

\[
\hat{T}^{(2)} T_0 \equiv T_1 - T_0^{(3)} + 2T_0 \pmod{3}.
\]

As \( T_1, T_0^{(3)} \) and \( T_0 \) are approximately of size \( n \), most of the elements in \( H \) appear in \( T_0^{(3)} T_0 \) for \( 3k \) times, \( k = 0, 1, \ldots \).

Let \( X_i, (Y_i, \text{resp.)} \) be the subset of elements of \( H \) appearing in \( T_0^{(3)} T_0 \) (\( T_0^{(3)} T_1 \), resp.) exactly \( i \) times for \( i = 0, 1, \ldots, M_0 \) (\( M_1 \), resp.), which means \( X_i \)’s (\( Y_i \)’s, resp.) form a partition of the group \( H \). In particular, we define \( M_0 \) and \( M_1 \) to be the largest integers such that \( X_{M_0} \) and \( Y_{M_1} \) are non-empty sets.

Then

\[
\hat{T}^{(2)} T_0 = \sum_{i=0}^{M_0} i X_i,
\]

\[
\hat{T}^{(2)} T_1 = \sum_{i=0}^{M_1} i Y_i.
\]

By (5) and (6), we have the following three conditions on the value of \( |X_i|’s \) and \( |Y_i|’s \):

\[
\sum_{i=0}^{M_0} i |X_i| = (2n + 1)k_0,
\]

\[
\sum_{i=0}^{M_1} i |Y_i| = (2n + 1)k_1,
\]

\[
\sum_{i=0}^{M_0} |X_i| = \sum_{i=0}^{M_1} |Y_i| = n^2 + n + 1.
\]

Some extra conditions are given by the following Lemma.

Lemma 10: For \( X_i \) and \( Y_i \) defined in (5) and (6),

\[
\sum_{i=1}^{M_0} |X_i| = (2n + 1)k_0 - 2(k_0 - 1)k_0
\]

\[
+ \theta_0 + \sum_{s \geq 3} \frac{(s - 1)(s - 2)}{2} |X_s|,
\]

\[
\sum_{i=1}^{M_1} |Y_i| = (2n + 1)k_1 - 2(k_1 - 1)k_1
\]

\[
+ \theta_1 + \sum_{s \geq 3} \frac{(s - 1)(s - 2)}{2} |Y_s|,
\]

\[
\theta_0 = |(T_0^{(2)} \setminus T_0^{(3)}) \cap \hat{T}^{(4)}| \quad \text{and}
\]

\[
\theta_1 = |\left( T_1 \cap \hat{T}^{(2)} \right) \setminus \left( T_1^{(2)} \cup \{e\} \right) \cap \hat{T}^{(4)}|.
\]

Note that \( |X_i|’s \) and \( |Y_i|’s \) are nonnegative integers. Our main idea is to use (7), (8), (9), (10) and (11) together with \( \hat{T}^{(2)} T_0 \) and \( \hat{T}^{(2)} T_1 \) (mod 3) to determine \( |X_i|’s \) and \( |Y_i|’s \). For some cases, we will end up with a contradiction which means there is no \( T_0 \) and \( T_1 \) satisfying (3) and (4), for example, see Theorem 14; for the other cases, the value of \( |X_i|’s \) and \( |Y_i|’s \) together with a careful analysis of (3) and (4) also lead to contradictions, for instance, see Theorems 15 and 16.

To prove Lemma 10, we need the following fact.

Lemma 11: For \( X_i \)’s defined by (5), \( e \in X_1, |X_1| \) is even for \( i \neq 1 \) and \( |X_1| \) is odd.

Proof: The identity element \( e \) is in \( X_1 \) for the following reasons: First, \( e \notin T_0^{(2)} T_0 \), otherwise \( T_0 \cap T_0^{(2)} \neq \emptyset \) which contradicts Lemma 7 (c); second, \( e \) appears in \( T_0^{(2)} T_0 \) exactly once which also follows from \( T_0^{(2)} \cap T_0 = \{e\} \) by Lemma 7 (c).

Note that \( X_i = X_i^{(e)} \) for \( i \geq 1 \). Hence \( |X_i| \) is even for \( i \geq 2 \), and \( |X_1| \) is odd because \( e \in X_1 \). Moreover, as \( |H| = n^2 + n + 1 \) is odd and \( X_i \)’s form a partition of \( H \), \( |X_0| \) is even.

Recall that we have defined \( k_0 = |T_0| \) and \( k_1 = |T_1| \) at the beginning of this section.
Lemma 12: Denote the elements in $T_1^{(2)}$ by $a_i$ with $i = 0, \cdots, k_0 - 1$ and the elements in $T_1^{(2)}$ by $a_i$ with $i = k_0, \cdots, 2n$. In particular, let $a_0 = e$. Then

$$|a_i T_k \cap a_j T_k| \in \{0, 1, 2\},$$

for any $i < j$ and $k = 0, 1$. For $\ell = 0, 1, 2$, define

$$C_{k, \ell} = \# \{ (a_i, a_j) : i < j, |a_i T_k \cap a_j T_k| = \ell \}.$$

Then

$$C_{k, 1} = \begin{cases} 2k_0 - 2, & k = 0; \\ 2k_1 - \frac{|T_1 \cap T_1^{(2)}|}{2}, & k = 1, \\ \end{cases}$$

and

$$C_{k, 2} = \begin{cases} (k_0 - 1)^2 - \frac{|T_0 \cap T_1^{(2)}| + |T_1 \cap T_1^{(2)}|}{2}, & k = 0; \\ k_1^2 - 2k_1 - \frac{|T_1^{(2)} \cap (T_1^{(2)} \cup \{e\}) \cap T_1^{(2)}|}{2}, & k = 1. \\ \end{cases}$$

Proof: An element $a_i a_j = a_j a_i = a_i T_k \cap a_j T_k$ for some $x, y \in T_k$ if and only if

$$a_i a_j^{-1} = x^{-1} y \in T_2^{(2)}.$$

By (4), there exist at most two possible choices of $(x, y)$. Moreover, if $(x, y)$ is such that $a_i x = a_j y$, then $a_i y^{-1} = a_j x^{-1}$ which also provides a solution $(y^{-1}, x^{-1})$. Thus $|a_i T_k \cap a_j T_k| = 1$ if and only if $x = y^{-1}$, which is equivalent to $a_i a_j^{-1} \in T_2^{(2)}$.

Next let us determine the value of $C_{k, \ell}$ for $\ell = 1, 2$.

Calculation of $C_{0, 1}$: By the previous analysis, for $i < j$, $|a_i T_0 \cap a_j T_0| = 1$ if and only if $a_i a_j^{-1} \in T_0^{(2)} \setminus \{e\}$, which is equivalent to $\sqrt[2]{a_i} \notin T_0^{(2)} \setminus \{e\}$.

If $0 \leq i < j \leq k_0$, i.e., $\sqrt[2]{a_i} \notin T_0^{(2)} \setminus \{e\}$, then $\sqrt[2]{a_j}$ must be $e$ because $e \in T_0 = e T_0$ which is a subset of $T_0^{(2)}$, and Lemma 7 (c) and (4) tell us that $T_0 \cap \{a : a, b \in T_0 \setminus \{e\}, a \neq b\} = 0$. If $k_0 \geq i < j \leq 2n$, then by Lemma 7 (g) and $T_0 \subseteq T_0^{(2)}$, $\sqrt[2]{a_i} \notin T_0^{(2)} \setminus \{e\}$ cannot belong to $T_1$. Therefore, we have proved that for $i < j$, $|a_i T_0 \cap a_j T_0| = 1$ if and only if one of the following cases happens:

(a) $a_i = e$ and $\sqrt[2]{a_j} \notin T_0 \setminus \{e\}$; 

(b) $\sqrt[2]{a_i} \in T_0$ and $\sqrt[2]{a_j} \in T_1$ such that $\sqrt[2]{a_i a_j^{-1}} \in T_0$.

By (3), there are totally $k_0 - 1$ ordered pairs $(a_i, a_j)$ satisfying (b). Thus, $C_{0, 1} = 2(k_0 - 1)$.

Calculation of $C_{1, 1}$: Similarly, for $i < j$, $|a_i T_1 \cap a_j T_1| = 1$ if and only if $a_i a_j^{-1} \in T_1^{(2)}$, which is equivalent to one of the following cases:

(a) $a_i = e$ and $\sqrt[2]{a_j} \in T_1$; 

(b) $\sqrt[2]{a_i}, \sqrt[2]{a_j} \in T_k$ for the same $k = 0$ or 1 such that $\sqrt[2]{a_i a_j^{-1}} \in T_1$.

The first case is obtained by checking the coefficients of elements in $T_0 T_1$ via (3) and the second case is from (4). It is clear that Case (a) provides $k_1$ ordered pairs $(a_i, a_j)$ with $i < j$.

To count this number for Case (b), without loss of generality, we order the elements in $T_0$ and $T_1$ such that $a_i^{-1} = a_{k_0-i}$ for $i = 1, \cdots, k_0$ and $a_{k_0+i}^{-1} = a_{2n-i}$ for $i = 0, \cdots, k_1 - 1$.

Given an element $c \in T_1$, by (4), there always exists exactly one unordered pair $\{a, b\} \subseteq T_0$ or $T_1$ such that $ab = c$. Suppose that $a = \sqrt[2]{a_i}$, $b = \sqrt[2]{a_j}$ and $a, b \in T_0$. As $c \neq e$, $u$ and $v$ must be different. Consequently,

$$c = ab = \sqrt[2]{a_i} \sqrt[2]{a_j} = \sqrt[2]{a_{k_0-i}} \sqrt[2]{a_{k_0+i}}.$$ 

Note that $u < v$ implies $k_0 - v < k_0 - u$. Thus, if $a_u \neq a_{k_0-v}$, then

$$\# \{ (\sqrt[2]{a_i}, \sqrt[2]{a_j}) : c = \sqrt[2]{a_i a_j^{-1}}, i < j \} = \begin{cases} 2, & u < v; \\ 0, & u > v. \end{cases}$$

If $a_u = a_{k_0-v}$, then $a_u = a_{k_0-1}$ and $c$ is represented by exactly one ordered pair which implies $c = a_u \in T_0^{(2)}$.

Therefore, there are totally

$$\frac{2}{2} \left| T_1 \cap T_0^{(2)} \right| + \frac{1}{2} \left| T_1 \cap T_1^{(2)} \right|$$

ordered pair $\{\sqrt[2]{a_i}, \sqrt[2]{a_j}\} \in T_0 \times T_0$ with $i < j$ such that $\sqrt[2]{a_i a_j^{-1}} \in T_1$. A similar analysis for $a, b \in T_1$ leads to

$$\frac{2}{2} \left| T_1 \cap T_1^{(2)} \right| + \frac{1}{2} \left| T_1 \cap T_1^{(2)} \right|$$

ordered pair $\{\sqrt[2]{a_i}, \sqrt[2]{a_j}\} \in T_1 \times T_1$ with $i < j$ such that $\sqrt[2]{a_i a_j^{-1}} \in T_1$. As (4) tells us that $T_1$ is covered by the elements in $T_0^{(2)}$ and $T_1^{(2)}$, by the above counting results,

$$C_{1, 1} = k_1 + \left( \left| T_1 \right| - \frac{\left| T_1 \cap T_0^{(2)} \right|}{2} - \frac{\left| T_1 \cap T_1^{(2)} \right|}{2} \right)$$

$$= 2k_1 - \left| T_1 \cap T_1^{(2)} \right| + \frac{1}{2} \left| T_0^{(2)} \setminus T_0 \right|$$

Calculation of $C_{0, 2}$: For $i < j$, $|a_i T_0 \cap a_j T_0| = 2$ if and only if $a_i a_j^{-1} \in T_0^{(2)} \setminus T_0^{(2)}$, which is equivalent to one of the following cases:

(a) $\sqrt[2]{a_i} \in T_0$ and $\sqrt[2]{a_j} \in T_1$ such that $a_i a_j^{-1} \in T_0^{(2)} \setminus T_0^{(2)}$; 

(b) $\sqrt[2]{a_i}, \sqrt[2]{a_j} \in T_k$ for the same $k = 0$ or 1 such that $a_i a_j^{-1} \in T_0^{(2)} \setminus T_0^{(2)}$.

By (3), $T_0^{(2)} \setminus T_0^{(2)} = H - e$. Thus the cardinality of the ordered pairs $(a_i, a_j)$ satisfying (a) and $i < j$ is

$$\left| T_0^{(2)} \setminus T_0^{(2)} \right| = \frac{1}{2} \left( \# \{ (a, b) : a, b \in T_0 \} - \# \{ (a, a) : a \in T_0, a \neq e \} \right)$$

$$= \frac{1}{2} \left( k_0^2 - k_0 - (k_0 - 1) \right)$$

$$= \frac{1}{2} \left( k_0 - 1 \right)^2.$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
For (b), we follow the argument in the calculation of $C_{1,1}$. For any $c \in T_0^2 \setminus T_0(2)$, suppose that $a = \sqrt{a_{i-1}}$, $b = \sqrt{a_{j-1}}$ and $a, b \in T_0$ such that $c = a_i a_{j-1} = (ab) \in (T_0(2))^2$. As $c \neq e$, $u$ and $v$ must be different. Consequently,

$$c = a_u a_v^{-1} = a_{k_v - u} a_{k_u - v}^{-1}.$$ 

It follows that

$$\# \{ (\sqrt{a_i}, \sqrt{a_j}) \in T_0 \times T_0 : c = a_i a_j^{-1}, i < j \} = \begin{cases} 2, & a_u \neq a_{k_v - u}, u < v; \\ 0, & a_u \neq a_{k_v - u}, u > v; \\ 1, & a_u = a_{k_v - u}. \end{cases}$$

Therefore, there are totally

$$2 \cdot \left( \left| T_0^2 \setminus T_0(2) \right| \cap \left( (T_0(2))^2 \setminus T_0(4) \right) \right) \cup \left( \left| T_0^2 \setminus T_0(2) \right| \cap T_0(4) \right) = 2 \cdot \left( \left| T_0^2 \setminus T_0(2) \right| \cap (T_0(2))^2 \right) - \left| T_0^2 \setminus T_0(2) \right| \cap T_0(4)$$

ordered pair $\sqrt{a_i}, \sqrt{a_j} \in T_0 \times T_0$ with $i < j$ such that $a_i a_j^{-1} \in T_0^2 \setminus T_0(2)$.

A similar analysis for $a, b \in T_1$ leads to

$$2 \cdot \left( \left| T_0^2 \setminus T_0(2) \right| \cap (T_1(2))^2 \right) - \left| T_0^2 \setminus T_0(2) \right| \cap T_0(4)$$

ordered pair $\sqrt{a_i}, \sqrt{a_j} \in T_1 \times T_1$ with $i < j$ such that $a_i a_j^{-1} \in T_0^2 \setminus T_0(2)$. As (4) tells us that

$$(T_0(2))^2 + (T_1(2))^2 = 2H - T_0(4) - T_1(4) + 2ne,$$

which means that $T_0^2 \setminus T_0(2)$ is covered by the elements in $(T_0(2))^2$ and $(T_1(2))^2$. By the counting results for cases (a) and (b),

$$C_{0,2} = \left| T_0^2 \setminus T_0(2) \right| + \left( \left| T_0^2 \setminus T_0(2) \right| - \left| T_0^2 \setminus T_0(2) \right| \cap T_0(4) \right) = (k_0 - 1)^2 - \frac{\left| T_0^2 \setminus T_0(2) \right| \cap T_0(4)}{2}.$$

**Calculation of $C_{1,2}$:** For $i < j$, $|a_i T_1 \cap a_j T_1| = 2$ if and only if $a_i a_j^{-1} \in T_1^2 \setminus (T_1(2) \cup \{ e \})$, which is equivalent to one of the following cases:

(a) $\sqrt{a_i} \in T_0$ and $\sqrt{a_j} \in T_1$ such that $a_i a_j^{-1} \in T_1^2 \setminus (T_1(2) \cup \{ e \})$;

(b) $\sqrt{a_i}, \sqrt{a_j} \in T_k$ for the same $k = 0$ or $1$ such that $a_i a_j^{-1} \in T_k^2 \setminus (T_k(2) \cup \{ e \})$.

For Case (a), (3) tells us that each element in $T_0^2 \setminus (T_1(2) \cup \{ e \})$ is covered by elements in $T_0 T_1$ exactly once. As a consequence, the cardinality of ordered pairs $(a_i, a_j)$ satisfying (a) and $i < j$ is

$$\left| T_0^2 \setminus (T_1(2) \cup \{ e \}) \right| = \frac{1}{2} \left( \# \{(a, b) : a, b \in T_1 \} - \# \{(a, a^{-1}) : a \in T_1 \} \right)$$

For Case (b), we follow the same argument for Case (b) of $C_{0,2}$. Consequently,

$$C_{1,2} = 2 \left| T_1^2 \setminus (T_1(2) \cup \{ e \}) \right| - \frac{\left| T_1^2 \setminus (T_1(2) \cup \{ e \}) \cap T_1(4) \right|}{2} = k_1^2 - 2k_1 - \frac{\left| T_1^2 \setminus (T_1(2) \cup \{ e \}) \cap T_1(4) \right|}{2}.$$

By Lemma 12, it is straightforward to get

$$\sum_{i < j} |a_i T_0 \cap a_j T_0| = 2k_0(k_0 - 1) - \left| \left( T_0^2 \setminus T_0(2) \right) \cap T_0(4) \right|, \quad (12)$$

and

$$\sum_{i < j} |a_i T_1 \cap a_j T_1| = 2k_1(k_1 - 1) - \left| \left( T_1^2 \setminus (T_1(2) \cup \{ e \}) \cap T_1(4) \right) \cap T_1(4) \right|.$$ 

**Recall that** $\theta_0 = \left| \left( T_0^2 \setminus T_0(2) \right) \cap T_0(4) \right|$ Let $\theta_{1,1} = \left| \left( T_0^2 \setminus (T_1(2) \cup \{ e \}) \cap T_0(4) \right) \cap T_1(4) \right|$ and $\theta_{1,2} = \left| T_1^2 \setminus T_1(2) \right|$ which equals $\left| T_1^2 \setminus T_1(4) \right|$.

**By (4) and** $T_1(4) \cap T_0(2) = \{ e \}$,

$$\theta_0 + \theta_{1,1} + \theta_{1,2} = \left| T_0^2 \setminus (T_1(2) \cup \{ e \}) \cap T_0(4) \right| = 2n.$$

Hence

$$\theta_0 + \theta_{1,1} + \theta_{1,2} = 2n.$$

Now we are ready to prove Lemma 10.

**Proof of Lemma 10:** We only prove the result for $T_0$. The proof of (11) is the same.

By the inclusion–exclusion principle, we count the distinct elements in $T_0(2)/T_0$.

$$|T_0(2)/T_0| = \sum_{i=0}^{2n} |a_i T_0| - \sum_{i<j} |a_i T_0 \cap a_j T_0| + \sum_{r \geq 3} (-1)^{r-1} |a_i T_0 \cap a_{i+1} T_0 \cap \cdots \cap a_{i+r-1} T_0|,$$

where $i_1 < i_2 < \cdots < i_r$ cover all the possible values. By the definition of $X_i$'s, the left-hand side of (14) equals $\sum_{i=1}^{M_0} |X_i|$.

Now we determine the value of the different sums in (14).

First, $\sum_{i=0}^{2n} |a_i T_0| = (2n + 1)k_0$. Second, (12) tells us the value of $\sum_{i<j} |a_i T_0 \cap a_j T_0|$.

Finally, suppose that $g \in a_{i_1} T_0 \cap a_{i_2} T_0 \cap \cdots \cap a_{i_r} T_0$ with $r \geq 3$. Then the contribution for $g$ in the sum $\sum_{r \geq 3} (-1)^{r-1} |a_i T_0 \cap a_{i+1} T_0 \cap \cdots \cap a_{i+r-1} T_0|$ is

$$\left( -1 \right)^{r-1} \left( \frac{s}{3} \right) + \left( -1 \right)^{r-1} \left( \frac{s}{4} \right) + \cdots = \left( \frac{s}{3} \right) - \left( \frac{s}{2} \right) + \left( \frac{s}{1} \right) = \frac{(s-1)(s-2)}{2}.$$

Therefore,

$$\sum_{r \geq 3} (-1)^{r-1} |a_i T_0 \cap a_{i+1} T_0 \cap \cdots \cap a_{i+r-1} T_0| = \sum_{s \geq 3} |X_s| \frac{(s-1)(s-2)}{2}.$$
Plugging them all into (14), we get (10).

Recall that at the very beginning of this section we have obtained

\[
\begin{align*}
\hat{T}^{(2)}T_0 &= (2k_0 - k_1)H + T_1 - T_0^3 + 2nT_0, \quad (15) \\
\hat{T}^{(2)}T_1 &= (2k_1 - k_0)H + T_0 - T_1^3 + 2nT_1. \quad (16)
\end{align*}
\]

In the following, we investigate (15) and (16) separately in different cases depending on the value of \( n \) modulo 3.

**A. Case: \( n \equiv 1 \) (mod 3)**

First we need to prove the following observation.

**Lemma 13:** When \( n \equiv 1 \) (mod 3),

(a) there is no element in \( T_j^{(3)} \) appearing more than 2 times for \( j = 0, 1 \),

(b) \( e \) appears only once in \( T_0^{(3)} \), and

(c) there are \( 0 \) or \( 2 \) elements appearing twice in \( T_0^{(3)} \), and there are at most 2 elements appearing twice in \( T_j^{(3)} \).

**Proof:** Recall that \( |H| = n^2 + n + 1 \). By the assumption, \( 3 \mid |H| \) but \( 9 \not| |H| \). Thus there are exactly two elements in \( H \) of order 3. We denote one of them by \( h \), which means the other one is \( h^{-1} \).

(a) For fixed \( j = 0 \) or \( 1 \), suppose that there exist distinct elements \( a, b \) in \( T_j \) such that \( a^3 = b^3 \). Then \( ab^{-1} \) must be of order 3 in \( H \). Without loss of generality, assume \( ab^{-1} = h \).

Toward a contradiction, suppose that there exists \( c \neq a, b \) in \( T_j \) such that \( c^3 = a^3 = b^3 \) which means \( ac^{-1} \) or \( bc^{-1} \) equals \( h \). By (4), there are at most one unsorted pair \( \{u, v\} \) with \( u, v \in T_j \) such that \( uv = h \). It follows that the unsorted pairs \( \{a, b^{-1}\} \) and \( \{a, c^{-1}\} \) (or \( \{b, c^{-1}\} \)) must be equal. However, this is impossible.

(b) Note that \( e = a^3 \) for some \( a \in T_0 \) if and only if \( a = e, h \) or \( h^{-1} \). Hence, \( e \) appears more than once in \( T_0^{(3)} \), then it appears for at least three times in \( T_0^{(3)} \) which contradicts (a).

(c) For \( j = 1 \) or \( 2 \), if \( g = t_1^{(3)} = t_2^{(3)} \) appears twice in \( T_j^{(3)} \), then \( t_1t_2^{-1} \) has to be of order 3. By (4), the unsorted pair \( \{t_1, t_2^{-1}\} \) must be \( \{a, b^{-1}\} \) or \( \{b, a^{-1}\} \) which are given in (a). Therefore, there is no element different from \( a^3 \) and \( a^{-3} \) appearing twice in \( T_j^{(3)} \).

In particular, for \( j = 0, 1 \), (b) tells us that \( a^3 \neq e \). Hence \( a^3 \neq a^{-3} \in T_0^{(3)} \).

By Lemma 7 (e) and (f), \( 2k_0 - k_1 = 2k_1 - k_0 = 0 \) (mod 3). Using (15), (16) and (11),

\[
\begin{align*}
\hat{T}^{(2)}T_0 &\equiv T_0 - T_0^{(3)} + 2T_0 \quad \text{(mod 3)}, \quad (17) \\
\hat{T}^{(2)}T_1 &\equiv T_0 - T_1^{(3)} + 2T_1 \quad \text{(mod 3)}. \quad (18)
\end{align*}
\]

By Lemma 7 (b) and (h),

\[ T_0 \cap T_1 = \emptyset, \text{ and } T_0 \cap T_0^{(3)} = \{e\}. \]

Let \( \Delta_i \) be the set of elements appearing twice in \( T_i^{(3)} \) for \( i = 1, 2 \). By Lemma 13, \( |\Delta_0|, |\Delta_1| \leq 2 \) and there is no element appearing more than 2 times in \( T_i^{(3)} \) for \( i = 1, 2 \). Note that

\[ |T_0^{(3)}| = k_0 - |\Delta_0|, \text{ and } |T_1^{(3)}| = k_1 - |\Delta_1|. \]

Depending on the parity of \( n \), we investigate (18) and (17), respectively.

**Theorem 14:** For \( n \equiv 4 \) (mod 6) and \( n > 2 \), there is no inverse-closed subsets \( T_0 \) and \( T_1 \subseteq H \) with \( e \in T_0 \) and \( k_0 + k_1 = 2n + 1 \) satisfying (3) and (4).

**Proof:** Suppose to the contrary that there exist \( T_0 \) and \( T_1 \) satisfying (3) and (4).

As \( 2 \mid n \), \( k_0 = n + 1 \) and \( k_1 = n \). We concentrate on (18).

Let \( u_0 = |T_1^{(3)} \cap T_0| \) and \( u_1 = |T_0^{(3)} \cap T_1| \). By Lemma 7, \( T_0 \cap T_1 = \emptyset \). Furthermore, we separate \( \Delta_i \) into three disjoint parts \( \Delta_0^1 = \Delta_1 \cap T_0, \Delta_1^1 = \Delta_1 \cap T_1 \) and \( \Delta_2^1 = \Delta_1 \setminus (T_0 \cup T_1) \).

By comparing the coefficients of elements in (18), we get

\[ \bigcup_{i \geq 0} Y_{3i+2} = (T_1 \setminus T_1^{(3)}) \cup \left(T_0^{(3)} \setminus (T_0 \cup T_1 \cup \Delta_1)\right) \cup \Delta_1^0. \]

Note that \( |T_0^{(3)}| = k_1 - |\Delta_1| \). It follows that

\[ \sum_{i \geq 0} |Y_{3i+2}| = (n - u_1) + (n - |\Delta_1| - (u_0 + u_1) - |\Delta_1^2|) + |\Delta_1^0|. \]

Similarly,

\[ \sum_{i \geq 0} |Y_{3i+1}| = (n + 1 - u_0) + |\Delta_1^2| + u_1 - |\Delta_1^1|. \]

To summarize, we have proved

\[ \sum_{i \geq 0} |Y_{3i+2}| = 2n - 2u_1 - u_0 - 2|\Delta_1^2| - |\Delta_1^1|, \quad (19) \]

\[ \sum_{i \geq 0} |Y_{3i+1}| = n + 1 - u_0 + u_1 + |\Delta_1^2| - |\Delta_1^1|. \quad (20) \]

Now (11) becomes

\[
\sum_{i=1}^{M_1} |Y_i| = (2n + 1)n - 2(n-1)n + \theta_1 + \sum_{s \geq 3} \frac{(s-1)(s-2)}{2} |Y_s| \\
= 3n + \theta_1 + \sum_{s \geq 3} \frac{(s-1)(s-2)}{2} |Y_s|. \quad (21)
\]

Plugging (19) and (20) into it to replace \( 3n \), we get

\[
\sum_{i=1}^{M_1} |Y_i| = \sum_{i \geq 0} |Y_{3i+1}| + \sum_{i \geq 0} |Y_{3i+2}| + 2u_0 + u_1 + |\Delta_1^2| \\
+ 2|\Delta_1^1| - 1 + \theta_1 + \sum_{s \geq 3} \frac{(s-1)(s-2)}{2} |Y_s|,
\]

which implies

\[
1 = 2u_0 + u_1 + |\Delta_1^2| + 2|\Delta_1^1| + \theta_1 \\
+ \sum_{s \geq 3} \left( \frac{(s-1)(s-2)}{2} - 1 \right) |Y_s| \\
+ \sum_{s \geq 3} \left( \frac{(s-1)(s-2)}{2} \right) |Y_s|. \quad (22)
\]

As \( |Y_i|, u_0, u_1, |\Delta_1^2|, |\Delta_1^1| \) and \( \theta \) are all nonnegative integers, (22) implies that \( u_0 = 0 \) and each \( |Y_i| = 0 \) for \( i \geq 4 \). Recall that \( u_1 \) is the cardinality of the inverse-closed subset \( T_1^{(3)} \cap T_1 \) which does not contain the identity element \( e \) of \( H \). Hence
$u_1$ must be even. Similarly, $|\Delta_1^3|$ and $|\Delta_2^3|$ are also even. Thus, by (22),
\[ u_1 = |\Delta_1^3| = |\Delta_2^3| = 0, \]
and $\theta_1 = 1$. Plugging them into (19) and (20), we get
\[ |Y_1| = n + 1, \quad |Y_2| = 2n. \]

By (8),
\[ 3|Y_3| = (2n + 1)n - (n + 1) - 4n = 2n^2 - 4n - 1 \equiv 3 \pmod{6}. \]
Consequently, $|Y_1|$ and $|Y_3|$ are both odd. As $Y_i$'s form a partition of the group $H$ and each $Y_i$ is inverse-closed, there exists only one of them of odd size. We get a contradiction.

Therefore, we have excluded the existence of $|Y_i|$'s which means there do not exist inverse-closed subsets $T_0$ and $T_1 \subset H$ with $e \in T_0$ and $k_0 + k_1 = 2n + 1$ satisfying (3) and (4).

For $n$ odd and $n \equiv 1 \pmod{3}$, we could not derive any contradiction by analyzing the value of $|X_i|$'s and $|Y_i|$'s.

**B. Case: $n \equiv 0 \pmod{3}$**

We separate the proof into two cases according to the parity of $n$.

**Theorem 15:** For $n \equiv 3 \pmod{6}$, there is no inverse-closed subsets $T_0$ and $T_1 \subset H$ with $e \in T_0$ and $k_0 + k_1 = 2n + 1$ satisfying (3) and (4).

*Proof:* As $n$ is odd, $|T_0| = k_0 = n$ and $|T_1| = k_1 = n + 1$. Toward a contradiction, suppose that $T_0$ and $T_1$ exist such that (3) and (4) hold.

First Lemma 7 tells us that $2k_0 - k_1 \equiv 2k_1 - k_0 \equiv 2 \pmod{3}$. Under the assumption that $3 \mid n$
\[ T^{(2)}_0 = 2H + T_1 - T^{(3)}_0 \equiv 2 \pmod{3}, \]
\[ T^{(2)}_1 = 2H + T_0 - T^{(3)}_1 \equiv 2 \pmod{3}. \]

Moreover, as $3 \mid |H|$, there is no repeating element in $T^{(3)}_0$ and $T^{(3)}_1$.

Assume that there are $\ell_0$ elements in $T_1 \cap T^{(3)}_0$ and $\ell_1$ elements in $T_0 \cap T^{(3)}_1$. It follows that
\[ \sum_{i \geq 0} |X_{3i+1}| = k_0 - \ell_0, \quad \sum_{i \geq 0} |Y_{3i+1}| = k_1 - \ell_1, \]
\[ \sum_{i \geq 0} |X_{3i+2}| = n^2 - n + 2\ell_0, \quad \sum_{i \geq 0} |Y_{3i+2}| = n^2 - n + 2\ell_1, \]
\[ \sum_{i \geq 0} |X_{3i}| = k_0 - \ell_0, \quad \sum_{i \geq 0} |Y_{3i}| = k_0 - \ell_1. \]

In particular, for $2 \mid n$,
\[ \sum_{i \geq 0} |X_{3i+1}| = n - \ell_0, \]
\[ \sum_{i \geq 0} |X_{3i+2}| = n^2 - n + 2\ell_0, \]
\[ \sum_{i \geq 0} |X_{3i}| = n + 1 - \ell_0. \]

The strategy of our proof is as follows: First we consider the possible nonnegative integer solutions for $|X_i|$’s satisfying (24). Several inequalities will provide us
\[ \begin{cases} |X_0| = n + 1, & \text{or} & |X_0| = n - 1, \\ \ell_0 = 0, & & \ell_0 = 0 \text{ or } 2. \end{cases} \]

Then, we will show that such $X_0$ cannot exist.

Next we provide the details of the proof of (25). Now (10) becomes
\[ \sum_{i=1}^{M_0} |X_i| = 3n + \theta_0 + \sum_{s \geq 3} \frac{(s-1)(s-2)}{2} |X_s|. \]
Subtract (9) from (10),
\[ -|X_0| = -n^2 + 2n - 1 + \theta_0 + \sum_{s \geq 3} \frac{(s-1)(s-2)}{2} |X_s|, \]
which means
\[ n^2 - |X_0| - 2n - \theta_0 + 1 \]
\[ = \sum_{s \geq 3} \frac{(s-1)(s-2)}{2} |X_s| \leq \frac{M_0 - 1}{2} \sum_{s \geq 3} (s-2) |X_s|. \]

On the other hand, by (7), (9) and (24),
\[ \sum_{i \geq 1} 3i(|X_{3i+1}| + |X_{3i+2}|) + \sum_{i \geq 1} (3i - 2) |X_{3i}| = \sum_{i \geq 0} i |X_i| - \sum_{i \geq 0} |X_{3i+1}| - 2 \sum_{i \geq 0} |X_{3i+2}| - \sum_{i \geq 0} 2 |X_{3i}| + 2 |X_0| \]
\[ = 2 |X_0| - \ell_0 - 2. \]

As $M_0 > 1$, by Lemma 11, $|X_{M_0}|$ is even, and $|X_{M_0}| \geq 2$. By (27),
\[ (M_0 - 2) \leq 2 |X_0| - \ell_0 - 2, \]
which means
\[ M_0 \leq |X_0| + 1 - \frac{\ell_0}{2}. \]

Moreover, by (27), we also have
\[ \sum_{s \geq 3} (s-2) |X_s| \leq 2 |X_0| - \ell_0 - 2. \]
Plugging it and (28) into (26), we have
\[ n^2 - |X_0| - 2n - \theta_0 + 1 \]
\[ \leq M_0 - 1 - 2 |X_0| - \ell_0 - 2 \]
\[ \leq (|X_0| - \ell_0/2) (|X_0| - \ell_0/2 - 1) \]
\[ \leq |X_0|/(|X_0| - 1). \]

By $|X_0| \leq \sum_{i \geq 0} |X_{3i}| = k_0 - \ell_0 \leq n + 1$ and a direct computation with the above inequality using $\theta_0 \leq 2n$, we derive that $|X_0| = n + 1, n, n - 1$ or $n - 2$. Moreover, $|X_1|$ is odd by Lemma 11. Consequently, by (24), $\ell_0$ must be even for odd $n$. Taking (29) and $\sum_{i \geq 0} |X_{3i}| = n + 1 - \ell_0$ into account, we get four possible cases.
and Case (IV) are impossible, because \( n \) is assumed to be odd. Hence, we have proved (25).

**Determination of \( X_0 \):** Next we show that

\[
X_0 = \begin{cases} 
T_1, & |X_0| = n + 1; \\
T_1 \setminus \{\gamma, \gamma^{-1}\}, & |X_0| = n - 1, 
\end{cases}
\]

(30)

where \( \gamma \) is an element in \( T_1 \). Afterwards we will finish the whole proof by getting some contradiction from (30).

Recall

\[
\hat{T}^{(2)} T_0 = (n - 1) H + T_1 - T_0^3 + 2n T_0.
\]

(15)

First we consider the case with \( \ell_0 = 0 \). For an arbitrary element \( t \in T_1 \), since \( \ell_0 = |T_1 \cap T_0^{(3)}| = 0 \), \( t \) can only be represented as

\[
abc \text{ for some pairwise distinct } a, b, c \in T_0
\]

or

\[
aab \text{ for some distinct } a, b \in T_0
\]

in \( T_0^3 \).

Taking account of the ordering of the elements in the representations, the coefficient of \( t \) in \( T_0^3 \in \mathbb{Z}[H] \) is divisible by 3. Together with \( n = 0 \) (mod 3) and \( T_1 \cap T_0 = \emptyset \), the coefficient of \( t \) in the right-hand side of (15) must be congruent to 0 modulo 3. Since \( \sum_{i \geq 0} |X_{3i}| = n + 1 \) and \( |T_1| = n + 1 \),

\[
X_0 = \begin{cases} 
T_1, & |X_0| = n + 1; \\
T_1 \setminus \{\gamma, \gamma^{-1}\}, & |X_0| = n - 1, 
\end{cases}
\]

for some \( \gamma \in T_1 \).

When \( \ell_0 = 2 \), by (25), \( |X_0| = n - 1 \). By our definition of \( \ell_0 \), there exist exactly two elements \( \gamma \) and \( \gamma^{-1} \in T_1 \) such that \( \gamma, \gamma^{-1} \in T_0^{(3)} \). The coefficients of them in the right-hand side of (15) must be congruent to 1 modulo 3, and the coefficient of any element in \( T_1 \setminus \{\gamma, \gamma^{-1}\} \) is still congruent to 0 modulo 3. Thus \( X_0 = T_1 \setminus \{\gamma, \gamma^{-1}\} \).

Therefore, we have obtained (30).

In the final step, we show that (30) cannot hold which concludes the proof of Theorem 15.

If \( T_1 = X_0 \), then (15) tells us

\[
(T_0^{(2)} + T_1^{(2)}) T_0 \cap T_1 = \emptyset,
\]

which cannot hold, because \( T_0 T_1 = H - e \) means for any non-identity \( a \in T_0^{(2)} + T_1^{(2)} \) there always exist \( t_0 \in T_0 \) and \( t_1 \in T_1 \) such that \( t_0 t_1 = a \).

If \( T_1 \setminus \{\gamma, \gamma^{-1}\} = X_0 \), then (15) tells us \( t \notin (T_0^{(2)} + T_1^{(2)}) T_0 \) for any \( t \in T_1 \setminus \{\gamma, \gamma^{-1}\} \). By (3),

\[
(T_1 - \gamma - \gamma^{-1}) T_0 = H - e - (\gamma T_0 + \gamma^{-1} T_0).
\]

For any \( x \in T_0 \), if \( tx = y \), then \( t = x^{-1} y \) which means \( y \notin T_0^{(2)} + T_1^{(2)} \). Thus the above equation implies

\[
\gamma T_0 + \gamma^{-1} T_0 + e = T_0^{(2)} + T_1^{(2)}.
\]

(31)

As \( \gamma^2 \in T_1^{(2)} \),

\[
\gamma^2 = \gamma a \quad \text{or} \quad \gamma^2 = \gamma^{-1} a
\]

for some \( a \in T_0 \setminus \{e\} \). The first case is impossible because \( T_0 \cap T_1 = \emptyset \). The second case implies that \( a = \gamma^3 \in T_0 \cap T_1^{(3)} \).

By (31), \( a = \gamma^4 \) belongs to \( T_0^{(2)} + T_1^{(2)} \).

If \( \gamma^4 \in T_0^{(2)} \), then \( \gamma^2 \in T_0 \) which means \( T_0 \cap T_1^{(2)} \neq \emptyset \).

It contradicts Lemma 7 (c).

For \( \gamma^4 \in T_1^{(2)} \), we need more detailed analysis. As \( a^2 \in T_0^{(2)} \), by (31) there exists \( b \in T_0 \) such that

\[
a^2 = \gamma^6 = \gamma b, \quad \text{or} \quad \gamma^{-1} b,
\]

which means \( b = \gamma^5 \) or \( \gamma^7 \in T_0 \). If \( b = \gamma^5 \in T_0 \), then

\[
T_1^{(2)} \ni \gamma^2 = \gamma^5 \gamma^{-3} = b \cdot a^{-1} \in T_0^3
\]

whence \( \gamma^2 \in T_0^3 \cap T_1^{(2)} \) which is not possible by Lemma 7 (g); if \( b = \gamma^7 \in T_0 \), then \( \gamma^4 = b \gamma^{-3} = b a^{-1} \in T_0^3 \). Recall that \( \gamma^4 \in T_1^{(2)} \). Hence \( \gamma^4 \in T_0^3 \cap T_1^{(2)} \) which contradicts Lemma 7 (g) again.

To summarize, we have proved that there exist no \( T_0 \) and \( T_1 \) satisfying (3) and (4).

The proof for even \( n \) which is congruent to 0 modulo 3 is similar, but we have to handle some extra problems.

*Theorem 16:* For \( n = 0 \) (mod 6), there is no inverse-closed subsets \( T_0 \) and \( T_1 \subseteq H \) with \( e \in T_0 \) and \( k_0 + k_1 = 2n + 1 \) satisfying (3) and (4).

*Proof:* Now \( n \) is divisible by 2 and 3, \( |T_0| = k_0 = n + 1 \) and \( |T_1| = k_1 = n \). Toward a contradiction, suppose that \( T_0 \) and \( T_1 \) exist such that (3) and (4) hold. The smallest possible value of \( n \) equals 6. However, throughout the rest part of the proof, we can always assume that

\[
n \geq 30.
\]

(32)

The reason is as follows: for \( n = 6, 12 \) and 24, \( n^2 + n + 1 \) is prime which means the nonexistence result is already covered by Result 9. For \( n = 18 \), it can be excluded by Proposition 8.

Instead of looking at \( X_1 \)'s as in the proof of Theorem 15, we consider \( Y_1 \)'s. By (16),

\[
\hat{T}^{(2)} T_1 \equiv 2 H + T_0 - T_1^{(3)} \pmod{3}.
\]

(33)

It follows that

\[
\sum_{i \geq 0} |Y_{3i+1}| = n - \ell_1,
\]

(34)

\[
\sum_{i \geq 0} |Y_{3i+2}| = n^2 - n + 2 \ell_1,
\]

\[
\sum_{i \geq 0} |Y_{3i}| = n + 1 - \ell_1,
\]

where \( \ell_1 \) is defined to be the cardinality of \( T_0 \cap T_1^{(3)} \), and (11) becomes

\[
\sum_{i=1}^{M_1} |Y_i| = 3n + \theta_1 + \sum_{s \geq 3} \frac{(s - 1)(s - 2)}{2} |Y_s|.
\]

By subtracting (9) from (11), we get

\[
n^2 - |Y_0| - 2n + 1 - \theta_1 = \sum_{s \geq 3} \frac{(s - 1)(s - 2)}{2} |Y_s|.
\]

(35)
On the other hand, by (8), (9) and (34),
\[ \sum_{i \geq 1} 3i(|Y_{3i+1}| + |Y_{3i+2}|) + \sum_{i \geq 1} (3i - 2)|Y_{3i}| = \sum_{i \geq 0} |Y_i| - \sum_{i \geq 0} |Y_{3i+1}| - 2 \sum_{i \geq 0} |Y_{3i+2}| - 2|Y_{3|} + 2|Y_0| \]
\[ = 2|Y_0| - \ell_1 - 2. \quad (36) \]

It is easy to check that (36) is the same as (27) by replacing \( X_i \) with \( Y_i \), and \( \ell \) with \( \ell_1 \).

As we do not know whether \(|Y_{M_1}| \geq 2\), we cannot immediately follow the proof of Theorem 15 to determine the possible value of \(|Y_i|\)'s. Next we concentrate on the proof of the following claim.

**Claim 1:** \(|Y_{M_1}| \geq 2\).

Toward a contradiction, suppose that \(|Y_{M_1}| = 1\) which is equivalent to \(Y_{M_1} = \{e\}\).

\[ \hat{T}'(2)T_1 = \sum_{i=1}^{M_1} iY_i, \]

we know that \(M_1 = |\hat{T}'(2) \cap T_1| = |\hat{T}'(2) \cap T_1| + |\hat{T}'(2) \cap T_1| \leq k_1 = n\), and \(2 | M_1 \) because \(|\hat{T}'(2) \cap T_1|\) and \(|\hat{T}'(2) \cap T_1|\) are both even. Moreover, by (33), \(e \in T_0\) and \(e \notin T_1\), we see that \(3 | M_1\). Therefore, we have obtained the following restriction on \(M_1\):

\[ 6 \leq M_1 \leq n, \quad \text{and} \quad 6 | M_1. \quad (37) \]

By (36), we obtain \(M_1 - 2 \leq 2|Y_0| - \ell_1 - 2\), which means
\[ M_1 \leq 2|Y_0| - \ell_1. \quad (38) \]

Let \(M_1' = \max\{i < M_1 : |Y_i| > 0\}\). If \(M_1' < 3\), then by (34), (37) and \(|Y_{M_1}| = 1\), we have
\[ |Y_0| = n - \ell_1, \]
\[ |Y_1| = n - \ell_1, \]
\[ |Y_2| = n^2 - n + 2\ell_1. \]

Plugging them in to (35), we get
\[ n^2 - 3n + \ell_1 + 1 - \theta_1 = \frac{(M_1 - 1)(M_1 - 2)}{2} \leq \frac{n^2 - 3n + 2}{2}, \]
where the last inequality comes from (37). Recall that \(\theta_1 \leq 2n\). Thus
\[ n^2 - 3n + \ell_1 + 1 - 2n \leq \frac{n^2 - 3n + 2}{2}. \]

It implies that \(n \leq 7\) which contradicts our assumption (32). Therefore \(M_1' \geq 3\).

As \(e \notin Y_{M_1} \), by the inverse-closed property of \(\hat{T}'(2)\) and \(T_1\), \(|Y_{M_1'}|\) must be even. In particular, \(|Y_{M_1'}| \geq 2\). By (36), we get
\[ (M_1' - 2) \cdot 2 + (M_1 - 2) \leq 2|Y_0| - \ell_1 - 2, \]
which means
\[ M_1' \leq \frac{|Y_0| - \ell_1 + M_1}{2} + 2. \quad (39) \]

By (36), we also get
\[ 2|Y_0| - \ell_1 - 2 \geq \sum_{3 \leq s \leq M_1'} (s - 2)|Y_s| + (M_1 - 2). \quad (40) \]

By (35),
\[ n^2 - |Y_0| - 2n + 1 - \theta_1 \leq \frac{M_1 - 1}{2} \sum_{3 \leq s \leq M_1'} (s - 2)|Y_s| + \frac{(M_1 - 1)(M_1 - 2)}{2}. \]

Plugging (40) and (39) into it, we get
\[ n^2 - |Y_0| - 2n + 1 - \theta_1 \leq \frac{M_1 - 1}{2} (2|Y_0| - \ell_1 - M_1) + \frac{(M_1 - 1)(M_1 - 2)}{2} \]
\[ \leq \left( \frac{|Y_0| - M_1 + \ell_1}{2} + 1 \right) \left( \frac{|Y_0| - M_1 + \ell_1}{2} \right) + \frac{(M_1 - 1)(M_1 - 2)}{2}. \]

We add \(|Y_0|\) on both sides of the above inequality and get
\[ n^2 - 2n + 1 - \theta_1 \leq F(|Y_0|, M_1), \quad (41) \]
where
\[ F(x, y) := x^2 + \frac{3}{4}y^2 - xy + 2x - 2y + 1. \]

Recall that \(|Y_0| \leq n - \ell_1\) by the third equation in (34) and (37), we only have to consider the value of \(F(x, y)\) for \((x, y) \in [0, n] \times [6, n]\). Our goal is to show that the value of \(F(x, y)\) is always smaller than \(n^2 - 2n + 1 - \theta_1\) which means (41) cannot hold.

It is easy to see that \(F\) defines an elliptic paraboloid and the minimum value is attained at point \((-1/2, 1)\). Hence, the maximum value of \(F(x, y)\) for \((x, y) \in [0, n] \times [6, n]\) can be obtained only if \(x = n\) or \(y = n\).

For \(x = n\),
\[ F(n, y) = \frac{3}{4}y^2 - (n + 2)y + n^2 + 2n + 1. \]

Its maximum value for \(y \in [6, n]\) with \(6 | y\) is
\[ F(n, 6) = n^2 - 4n + 16, \]
and \(F(n, 12) = n^2 - 10n + 85\) is the second largest value under the assumption (32).

First, we can simply check that \(y = 6\) is impossible: Now \(M_1 = 6\) and \(|Y_0| = n\), which means \(\ell_1 = 0\) and \(|Y_3| = 0\). By (34), (11) and (35),
\[ |Y_1| + |Y_4| = n, \]
\[ |Y_2| + |Y_5| = n^2 - n, \]
\[ |Y_1| + 2|Y_2| + 4|Y_4| + 5|Y_5| = 2n^2 + n - 6, \]
\[ 3|Y_4| + 6|Y_5| = n^2 - 3n + 1 - \theta_1 - 10. \]
Consequently, $|Y_1| = \frac{n^2}{3} - \frac{4n}{3} - \frac{\theta_1}{3} + 1$ which must be smaller than or equal to $n$ by the first equation. Recall that $\theta_1 \leq 2n$. Thus
$$\frac{n^2}{3} - 2n + 1 \leq n,$$
which implies $n < 0$. It contradicts our assumption (32).

For the second largest value $F(n, 12)$, as $\theta_1 \leq 2n$, if (41) holds, then
$$n^2 - 4n + 1 \leq n^2 - 2n + 1 - \theta_1 \leq n^2 - 10n + 85,$$
which means $n \leq 14$. But these value have already been excluded by (32). Therefore,
$$n^2 - 2n + 1 - \theta_1 > F(n, y),$$
for any $y \in [6, n]$ with $6 \mid y$.

For $y = n$,
$$F(x, n) = x^2 - (n - 2)x + \frac{3}{4}n^2 - 2n + 1.$$
Its maximum value for $x \in [0, n]$ is
$$F(n, n) = \frac{3}{4}n^2 + 1.$$
It is larger than or equal to $n^2 - 4n + 1$ if and only if $n \leq 16$, which again contradicts (32).

Therefore, (41) cannot hold which means that we have proved Claim 1.

Following the proof of Theorem 15, our next goal is to show that the only possible value of $|Y_0|$ are as follows:

$$\begin{align*}
|Y_0| &= n + 1, \quad \text{or} \quad |Y_0| = n - 1, \quad \text{or} \quad |Y_0| = n - 2 + \ell_1, \quad \ell_1 = 1.
\end{align*}$$

(42)

By replacing $Y_i$’s with $X_i$’s, one can get (24) and (27) from (34) and (36), respectively. Moreover, (26) becomes (35) if we change $X_i$’s to $Y_i$’s and change $\theta_0$ to $\theta_1$.

Hence, by the same argument for (29), we get
$$\begin{align*}
n^2 - |Y_0| - 2n + 1 - \theta_1 &\leq M_1 - \frac{1}{2} - (2|Y_0| - \ell_1 - 2) \\
&\leq (|Y_0| - \ell_1/2)(|Y_0| - \ell_1/2 - 1) \\
&\leq |Y_0|/2 - 1 - |Y_0| - 1.
\end{align*}$$

(43)

Taking account of $\theta_1 \leq 2n$, we get $|Y_0| = n - 1, n$ or $n + 1$ under the assumption (32). Note that $\ell_1 = |T_0 \cap T_1^{(3)}|$ must be even, because $T_0$ and $T_1$ are inverse-closed and $e \notin T_1^{(3)}$. Taking (43) and $|Y_0| \leq \sum_{i \geq 0} |Y_3i| = n + 1 - \ell_1$ into account, we get four possible cases

(I) $|Y_0| = n + 1$ and $\ell_1 = 0$;

(II) $|Y_0| = n - 1$ and $\ell_1 = 0$ or 2;

(III) $|Y_0| = n$, $\ell_1 = 0$;

(IV) $|Y_0| = n - 2$, $\ell_1 = 0$.

To prove (42), we only have to exclude Case (IV).

Case (IV): By (36) and Claim 1,
$$(M_1 - 2)2 \leq 2|Y_0| - \ell_1 - 2,$$
which implies
$$M_1 \leq |Y_0| + 1 - \frac{\ell_0}{2} = n - 2 + 1 = n - 1.$$

On the other hand, by (43),
$$M_1 \geq 1 + \frac{n^2 - (n - 2) - 2n + 1 - \theta_1}{(n - 2) - 1} \geq n - 1.$$

Therefore $M_1$ must be $n - 1$. Plugging $\ell_1 = 0$ into the last equation of (34), we get
$$\sum_{i \geq 0} |Y_{3i}| = n + 1.$$  (44)

By (36) and $M_1 = n - 1 \equiv 2 \pmod{3}$,
$$2n - 6 = 2|Y_0| - \ell_1 - 2$$
$$= \sum_{i \geq 1} 3i|Y_{3i+1}| + \sum_{i \geq 1, 3i+2 \neq M_1} 3i|Y_{3i+2}|$$
$$+ 2(n - 1 - 2) + \sum_{i \geq 1} (3i - 2)|Y_{3i}|.$$

As a consequence, $|Y_3| = |Y_4| = \ldots = |Y_{M_1-1}| = 0$. However, it means $\sum_{i \geq 0} |Y_{3i}| = |Y_0| = n - 2$ which contradicts (44).

Therefore, we have proved (42).

**Determination of $Y_0$**: We basically follow the argument used in the proof of Theorem 15. Our goal is to prove

$$\begin{align*}
Y_0 &= \begin{cases}
T_0, & \text{if } |Y_0| = n + 1; \\
T_0 \setminus \{\ell_1\}, & \text{if } |Y_0| = n; \\
T_0 \setminus \{\gamma, \gamma^{-1}\}, & \text{if } |Y_0| = n - 1,
\end{cases}
\end{align*}$$

(45)

for some $\gamma \in T_0$.

Recall
$$T^{(2)} T_1 = (n - 1)H + T_0 - T_1^3 + 2nT_1.$$  (16)

First let us consider the case with $\ell_1 = 0$. For an arbitrary element $t \in T_0$, as $\ell_1 = |T_0 \cap T_1^{(3)}| = 0$, $t$ can only be represented as

- $abc$ for some pairwise distinct $a, b, c \in T_1$,

- $aab$ for some distinct $a, b \in T_1$,

in $T_1^3$.

Taking account of the ordering of the elements in the representations, the coefficient of $t$ in $T_1^3 \in \mathbb{Z}[H]$ is divisible by 3. Together with $n \equiv 0 \pmod{3}$ and $T_1 \cap T_0 = \emptyset$, the coefficient of $t \in T_0$ in the right-hand side of (16) must be congruent to 0 modulo 3. Since $\sum_{i \geq 0} |Y_{3i}| = n + 1$, $|Y_0| = n + 1$ and $Y_0$ is inverse-closed, we obtain (45).

When $\ell_1 = 2$ which happens only if $|Y_0| = n - 1$ by (42), there exist exactly two elements $\gamma, \gamma^{-1} \in T_0 \cap T_1^{(3)}$. The coefficients of $\gamma$ or $\gamma^{-1}$ in the right-hand side of (16) must be congruent to 1 modulo 3, and the coefficient of any element in $T_0 \setminus \{\gamma, \gamma^{-1}\}$ is still congruent to 0 modulo 3. Thus $Y_0 = T_0 \setminus \{\gamma, \gamma^{-1}\}$ which corresponds to the last case in (45).

The final part of our proof is to show that (45) cannot hold which concludes the proof of Theorem 16.
If \( T_0 = Y_0 \), then (16) tells us

\[
(T_0^{(2)} + T_1^{(2)}) T_1 \cap T_0 = \emptyset,
\]

which cannot hold, because \( T_0 T_1 = H - e \) means for any non-identity \( a \in T_0^{(2)} + T_1^{(2)} \) there always exist \( t_0 \in T_0 \) and \( t_1 \in T_1 \) such that \( t_0 t_1 = a \).

If \( T_0 \setminus \{ e \} = Y_0 \), then \( t \notin (T_0^{(2)} + T_1^{(2)}) T_1 \) for any \( t \in T_0 \setminus \{ e \} \). By (3),

\[
Y_0 T_1 = (T_0 - e) T_1 = H - e - T_1.
\]

As \( Y_0 \cap (T_0^{(2)} + T_1^{(2)}) T_1 = \emptyset \) implies \( Y_0 T_1 \cap (T_0^{(2)} + T_1^{(2)}) = \emptyset \),

\[
T_0^{(2)} + T_1^{(2)} \subseteq e + T_1,
\]

which is impossible by the sizes of them.

If \( T_0 \setminus \{ \gamma, \gamma^{-1} \} = Y_0 \) for some \( \gamma 
eq e \), then \( t \notin (T_0^{(2)} + T_1^{(2)}) T_1 \) for any \( t \in T_0 \setminus \{ \gamma, \gamma^{-1} \} \). By (3),

\[
Y_0 T_1 = (T_0 - \gamma - \gamma^{-1}) T_1 = H - e - (\gamma T_1 + \gamma^{-1} T_1).
\]

As \( Y_0 \cap (T_0^{(2)} + T_1^{(2)}) T_1 = \emptyset \) implies \( Y_0 T_1 \cap (T_0^{(2)} + T_1^{(2)}) = \emptyset \), the above equation and the sizes of \( T_0 \) and \( T_1 \) lead to

\[
\gamma T_1 + \gamma^{-1} T_1 + e = T_0^{(2)} + T_1^{(2)}, \tag{46}
\]

Since \( \gamma^2 \in T_0^{(2)} \),

\[
\gamma^2 = \gamma \alpha \quad \text{or} \quad \gamma^2 = \gamma^{-1} \alpha
\]

for some \( \alpha \in T_1 \). The first case is impossible because \( T_0 \cap T_1 = \emptyset \). The second case implies that \( \alpha = \gamma^3 \in T_1 \cap T_0^{(3)} \). By (46), \( \gamma \alpha = \gamma^4 \) belongs to \( T_0^{(2)} \) or \( T_1^{(2)} \).

If \( \gamma^4 \in T_1^{(2)} \), then \( \gamma^2 \in T_1 \) which means \( \gamma^2 \in T_1 \cap T_0^{(2)} \). It follows that the coefficient of \( e \) in \( T_1^{(2)} \) is larger than 0. However, \( e \notin Y_0 = T_0 \setminus \{ \gamma, \gamma^{-1} \} \). This is a contradiction.

If \( \gamma^4 \in T_0^{(2)} \), then \( \gamma^2 \in T_0 \cap T_0^{(2)} \). It contradicts Lemma 7 (c).

Therefore, we have finished the proof that there exist no \( T_0 \) and \( T_1 \) satisfying (3) and (4).

The main result, i.e. Theorem 1 is a simple combination of Theorems 14, 15 and 16.

IV. Concluding Remarks

In this paper, we investigate the classification of linear Lee codes of packing radius 2 and packing density \( \frac{|S(n,2)| + 1}{|S(n,2)|} \) in \( \mathbb{Z}^n \). We call linear Lee codes with this density almost perfect. There are still several cases remaining open.

Problem 17: For \( n \equiv 1, 2, 5 \pmod{6} \), show that there is an almost perfect linear Lee code of packing radius 2 if and only if \( n = 2 \).

If this problem is solved, then we get the complete nonexistence proof of APL codes of packing radius 2, for \( n \geq 3 \). As a direct consequence, we obtain a complete list of APL codes of packing radius 2 in \( \mathbb{Z}^n \): 6Z for \( n = 1 \) and the four codes in \( \mathbb{Z}^2 \) listed in Remark 2.

To solve Problem 17, one may try to follow the approach in [17] to investigate the coefficients of the elements in \( T(4) T_0 \) and \( T(4) T_1 \) modulo 5. In a very recent work [26], this approach has been applied and Problem 17 has been solved except for only a finite number of \( n \).

One may naturally expect a similar classification result provided that the packing density equals \( \frac{|S(n,2)| + \epsilon}{|S(n,2)|} \), where \( \epsilon \) is a small integer compared with \( n \). However, it seems not an easy task, because the order of the group \( G \) equals \( |S(n,2)| + \epsilon = 2n^2 + 2n + 1 + \epsilon \) which is determined by \( \epsilon \) and some key steps of the proof should rely on the structure of \( G \). One may compare the proof for \( \epsilon = 0 \) and for \( \epsilon = 1 \) with \( n \equiv 0 \pmod{3} \) in [17, Proposition3.3] and Theorems 15, 16. The first one consists of only a half-page proof and the second one is much more complicated. Therefore, a small change of the order of \( G \) could lead to a big change of the proof.

Another interesting question is about quasi-perfect linear Lee codes. As we have mentioned in the introduction, the packing density of the 2-quasi-perfect Lee codes constructed in [18] and [21] tends to \( \frac{1}{2} \) when \( n \to \infty \). However, to the best of our knowledge, there is no construction with packing density tending to 1 when \( n \to \infty \). Therefore, we propose the following open problem.

Problem 18: Find better upper and lower bounds of the packing density of 2-quasi-perfect linear Lee codes in \( \mathbb{Z}^n \) for infinitely many \( n \).

ACKNOWLEDGMENT

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement the presentation of this article.

REFERENCES

[1] X. Xu and Y. Zhou, “On almost perfect linear Lee codes of packing radius 2,” 2022, arXiv:2210.03361.

[2] R. M. Roth and P. H. Siegel, “Lee–metric BCH codes and their application to constrained and partial-response channels,” IEEE Trans. Inf. Theory, vol. 40, no. 4, pp. 1083–1096, Jul. 1994.

[3] M. Schwartz, “Quasi-cross lattice tilings with applications to flash memory,” IEEE Trans. Inf. Theory, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.

[4] M. Blaum, J. Bruck, and A. Vardy, “Interleaving schemes for multidimensional cluster errors,” IEEE Trans. Inf. Theory, vol. 44, no. 2, pp. 730–743, Mar. 1998.

[5] S. W. Golomb and L. R. Welch, “Perfect codes in the Lee metric and the packing of polynomials,” SIAM J. Appl. Math., vol. 18, no. 2, pp. 302–317, Mar. 1970. [Online]. Available: http://www.jstor.org/stable/2199465

[6] P. Horak and D. Kim, “50 years of the Golomb–Welch conjecture,” IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 3048–3061, Apr. 2018.

[7] T. Etzion, Perfect Codes and Related Structures. Singapore: World Scientific, Mar. 2022.

[8] K. A. Post, “Nonexistence theorems on perfect Lee codes over large alphabets,” Inf. Control, vol. 29, no. 4, pp. 369–380, Dec. 1975. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S00199958575800052

[9] J. Astola, “An Elias-type bound for Lee codes over large alphabets and its application to perfect codes (corresp.),” IEEE Trans. Inf. Theory, IT-28, no. 1, pp. 111–113, Jan. 1982.

[10] T. Lepistö, “A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric,” Inf. Control, vol. 49, no. 2, pp. 109–124, May 1981. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S001999581904617

[11] D. Kim, “Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions,” Eur. J. Combinatorics, vol. 63, pp. 1–5, Jun. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0195669817300070

[12] T. Zhang and G. Ge, “Perfect and quasi-perfect codes under the \( \ell_p \) metric,” IEEE Trans. Inf. Theory, vol. 63, no. 7, pp. 4325–4331, Jun. 2017.
[13] C. Qureshi, “On the non-existence of linear perfect Lee codes: The Zhang–Ge condition and a new polynomial criterion,” *Eur. J. Combinatorics*, vol. 83, Jan. 2020, Art. no. 103022. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0195669819301234

[14] P. Horak and D. Kim, “Algebraic method in tilings,” 2016, arXiv:1603.00051.

[15] C. Qureshi, A. Campello, and S. I. R. Costa, “Non-existence of linear perfect Lee codes with radius 2 for infinitely many dimensions,” *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3042–3047, Apr. 2018.

[16] T. Zhang and Y. Zhou, “On the nonexistence of lattice tilings of \( Z^n \) by Lee spheres,” *J. Combinat. Theory A*, vol. 165, pp. 225–257, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0097316519300238

[17] K. H. Leung and Y. Zhou, “No lattice tiling of \( Z^n \) by Lee sphere of radius 2,” *J. Combinat. Theory A*, vol. 171, Apr. 2020, Art. no. 105157. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0097316519301384

[18] C. Camarero and C. Martínez, “Quasi-perfect Lee codes of radius 2 and arbitrarily large dimension,” *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1183–1192, Mar. 2016.

[19] M. Miller and J. Širáň, “Moore graphs and beyond: A survey of the degree/diameter problem,” *Electron. J. Combinatorics*, vol. 20, no. 2, p. DS14, May 2013. [Online]. Available: http://www.combinatorics.org/ojs/index.php/eljc/article/view/DS14

[20] B. F. AlBdaiwi and B. Bose, “Quasi-perfect Lee distance codes,” *IEEE Trans. Inf. Theory*, vol. 49, no. 6, pp. 1535–1539, Jun. 2003.

[21] S. Mesnager, C. Tang, and Y. Qi, “2-correcting Lee codes: (Quasi)-perfect spectral conditions and some constructions,” *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3031–3041, Apr. 2018.

[22] W. He, “On the nonexistence of Abelian Moore Cayley graphs with excess one,” *Discrete Math. Lett.*, vol. 7, pp. 58–65, Jul. 2021.

[23] P. Horak and B. F. AlBdaiwi, “Diameter perfect Lee codes,” *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5490–5499, Aug. 2012.

[24] R. G. Stanton and D. D. Cowan, "Note on a ‘square’ functional equation," *SIAM Rev.*, vol. 12, no. 2, pp. 277–279, Apr. 1970.

[25] D. de Caen, D. A. Gregory, I. G. Hughes, and D. L. Kreher, “Near-factors of finite groups,” *ARS Combinatoria*, vol. 29, pp. 53–63, Jun. 1990. [Online]. Available: https://www.combinatorialmath.ca/arscombinatoria/

[26] Z. Zhou and Y. Zhou, “Almost perfect linear Lee codes of packing radius 2 only exist for small dimension,” 2022, arXiv:2210.04550.