分类号 TP957 学号 19010029

UDC 51 密级 公开

理学硕士学位论文

三类交换凯莱图的存在性及相关编码问题

硕士生姓名 何玮

学科专业 数学

研究方向 组合编码

指导教师 周悦 副研究员

国防科技大学研究生院

二〇二一年十二月

Existence of three types of abelian Cayley graphs and related coding problems

Candidate: Wei He

Supervisor: Associate Prof. Yue Zhou

A dissertation

Submitted in partial fulfillment of the requirements

for the degree of Master of Science

in Mathematics

Graduate School of National University of Defense Technology

Changsha, Hunan, P. R. China

December, 2021

独 创 性 声 明

本人声明所呈交的学位论文是我本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写过的研究成果，也不包含为获得国防科技大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文题目：三类交换凯莱图的存在性及相关编码问题

学位论文作者签名：何沛　　日期：2021 年 10 月 13 日

学位论文版权使用授权书

本人完全了解国防科技大学有关保留、使用学位论文的规定。本人授权国防科技大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档，允许论文被查阅和借阅；可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密学位论文在解密后适用本授权书。）

学位论文题目：三类交换凯莱图的存在性及相关编码问题

学位论文作者签名：何沛　　日期：2021 年 10 月 13 日

作者指导教师签名：周士飞　　日期：2021 年 10 月 13 日

目　录

表 目 录

图 目 录

摘　要

交换凯莱图是一类特殊的正则图，是代数图论中一类重要的研究对象，与编码学、密码学有着紧密的联系，具有重要的研究意义. 给定度和直径，交换凯莱图的顶点个数 (阶) 存在一个上界——交换凯莱摩尔界. 顶点数达到该上界的图被称为交换凯莱摩尔图. 这类图的构造和分类，是“度——直径”问题中的一个核心研究内容，同时对应于编码理论中完美线性李码的存在性问题. 当图的直径等于 2 时，度为 $2n$ 的交换凯莱摩尔图有 $2n^2+2n+1$ 个顶点，而满足这一参数的图直到最近才被完全分类. 基于该结果，本文主要研究顶点个数与交换凯莱摩尔界相差 1 的图的分类问题，以及相关的编码问题. 具体研究对象包括：

1) 度为 $2n$，直径为 2 的 $2n^2+2n$ 阶交换凯莱图；

2) 度为 $2n$，直径为 3 且生成集 S 满足 $|\tilde{S}^2|=2n^2+2n+1$ ($\tilde{S}=S\cup\{e\}$，$|\cdot|$ 表示多重集中不同元素的个数) 的 $2n^2+2n+2$ 阶交换凯莱图；

3) 顶点集为初等 2 群，生成集 S 的阶为 d，直径为 k 且图的阶达到上界 $\sum_{i=0}^{k}\binom{d}{i}$ 的交换凯莱图.

关于前两类图，通过使用代数数论、有限域、群特征标、对称多项式等数学工具，本文证明当参数满足一定的初等数论条件时，这两类图不存在. 并根据这些结论用程序分别计算出 10^5 以内，n 有多少种取值情况使得第一、二类图不存在. 对于第三类图，本文证明其与汉明距离下的二元完美线性码是等价的，并根据完美码的已有分类结果，给出了这类图的完全分类.

关键词: **凯莱图**; **度——直径问题**; **摩尔界**; **李码**; **纠错码**

ABSTRACT

Abelian Cayley graphs are important research objects in the study of algebraic graph theory. They also have strong connections with coding theory and cryptography. For a given valency and a given diameter, there is an upper bound on the cardinality of the vertex set of an abelian Cayley graph. We call it the abelian-Cayley-Moore bound, and the graphs meeting this bound abelian-Cayley-Moore graphs. The classification of abelian-Cayley-Moore graphs plays a central role in the study of Degree/Diameter problems of graph theory, and it also corresponds to the existence problem of linear perfect Lee codes which is important in coding theory. In particular, when the diameter of the graph equals 2 and the valency is $2n$, an abelian-Cayley-Moore graph has exactly $2n^2+2n+1$ vertices, for which the classification has been recently obtained. Based on the results, we mainly investigate abelian Cayley graphs whose numbers of vertices differ from $2n^2+2n+1$ by 1, and the related coding theory problems. Precisely speaking, they are:

1) Abelian Cayley graphs of degree $2n$ and diameter 2 with exactly $2n^2+2n$ vertices;

2) Abelian Cayley graphs of degree $2n$ and diameter 3 whose order is $2n^2+2n+2$ such that their generating set denoted by S satisfies $|\tilde{S}^2| = 2n^2+2n+1$ where $\tilde{S} = S \cup \{e\}$;

3) The abelian Cayley graphs of degree d and diameter k whose vertex set consists of $\sum_{i=0}^{k} \binom{d}{i}$ elements of order 2.

For the first two types of graphs, by applying various tools from algebraic number theory, finite fields, characters of groups, symmetric polynomials, etc., we show their nonexistence under certain elementary number theoretic conditions on n. According to these results, we calculate the number of values of n within 10^5 in which the first two types of graphs do not exist by computer programs. For the last type of graphs, we prove that they are equivalent to binary linear perfect codes under the Hamming-metric. By the known results on the classification of perfect codes, we present a complete classification of the third type of graphs.

Key Words: Cayley graph; degree-diameter problem; Moore bound; Lee code; error-correcting code

符号使用说明

$\mathbb{F}_q$	含有 q 个元素的有限域
$\mathbb{Z}$	整数环
$\mathbb{Q}$	有理数域
$\lvert\cdot\rvert$	多重集中不考虑重复时元素的个数
$d_L(x,y)$	两个码字的 Lee 距离
C_p	p 阶循环群
ζ_ω	ω 次本原单位根
(p)	p 生成的理想
$N(d,k)$	度为 d，直径为 k 的图的最大阶
$AC_{d,k}$	度为 d，直径为 k 的交换凯莱图的最大阶
$M_C(2n,k)$	度为 $2n$，直径为 k 的交换凯莱摩尔界

第一章　绪论

1.1　研究背景与意义

凯莱图是代数图论中一类重要的图，其广泛的应用及与其他数学领域的相关性吸引了很多专家学者的关注. 凯莱图的定义为：假设 G 是一个乘法群，其单位元为 e，S 是 G 的一个子集，$S = S^{-1}$ 且 $e \notin S$，则 $\Gamma(G, S)$ 是以 G 为顶点集的**凯莱图** (Cayley graph)，G 中任意两点 g，h 连边当且仅当 $g^{-1}h \in S$. 特别地，若 G 是交换群，则称 $\Gamma(G, S)$ 为**交换凯莱图** (abelian Cayley graph). 当度为 $2n$，直径为 $k(k > 1)$ 时，Dougherty 和 Faber[1] 证明了一个界，交换凯莱图 $\Gamma(G, S)$ 满足

$$|G| \leq \sum_{i=0}^{\min\{n,k\}} 2^i \binom{n}{i} \binom{k}{i}.$$

不等式的右边就是**交换凯莱摩尔界** (abelian Cayley Moore bound)，记为 $M_C(2n, k)$，顶点数等于交换凯莱摩尔界的图称为**交换凯莱摩尔图** (abelian Cayley Moore graph). 术语“摩尔界”源自 Moore[3] 在研究“度——直径”问题时提出的一个上界. “度——直径”问题的内容为：在给定图的最大度和直径的前提下，求图顶点个数的最大值. 对于度为 d，直径为 k 的图，记图的阶的最大值为 $N(d, k)$，Moore 给出了如下上界：

$$N(d, k) \leq 1 + d\sum_{i=0}^{k-1}(d-1)^i.$$

该界又被称为**摩尔界** (Moore bound).

构造这种高阶的图主要用于设计并行处理器的互联网络. 互联网络的设计存在两个基本限制：可以连接到任何一个节点的连接数量有限，并且两个节点之间的通信路由上的中间节点数量必须较少. 在满足这些约束条件的同时，人们希望最大化参与这种网络的节点数量，用图论的语言表达就是“度——直径”问题. 该网络被期望在任何处理器上都相同. 这意味着使用的图应该是顶点传递的，顶点传递指的是对于任意两个顶点 x 和 y，都存在一个图上的自同构将 x 映射到 y. 在这里，通常会考虑一类特殊的顶点传递图，即凯莱图. 在线表格[1]给出了某些度和直径下已经找到的阶数最大的图，其中有相当大一部分是凯莱图 [1, 4-5].

“度——直径”问题的一种解决思路是在给定度的前提下，找到直径尽可能小的高阶凯莱图，最直接的方法是将所有的群都尝试一次，找出群中所有的目标大

[1]http://combinatoricswiki.org/wiki/The Degree Diameter Problem for General Graphs

小的生成集，并检验是否能生成出整个群，如果可以，则算出图的直径. 然而，即使对于相对较小的群和生成集来说，运算量也非常的大. 目前，在计算机的辅助下，凯莱图被用于度 $d \leq 16$ 且直径 $k \leq 10$ 的高阶图的搜索，以确定 $N(d,k)$ 的下界 [4].

凯莱图和李码之间有着密切联系，李码在受限和局部响应通道、闪存、交织方案、多维突发错误校正和闪存秩调制方案中的错误校正等领域都有广泛应用 [1, 4-6].

Golomb–Welch 猜想是李码中的一个重要猜想，其内容为 $n \geq 3$ 且 $r \geq 2$ 时，$\mathbb{Z}^n$ 上不存在完美 r- 纠错李码. 2019 年，Leung 和周悦 [2] 证明了当 $n \geq 3$ 时，$\mathbb{Z}^n$ 上不存在线性完美 2- 纠错李码，由此可以推出当李球的半径为 2 且 $2n^2+2n+1$ 是素数时，Golomb-Welch 猜想是正确的. 本文研究的前两类图的存在性，可以视为在 [2] 研究成果基础上的推广.

1.2 国内外研究进展

Hoffman 和 Singleton 最早开始摩尔图的研究，他们在文献 [7] 中开创性的研究了直径为 2 和 3 的摩尔图. 在直径为 2 的情况下，证明了摩尔图只可能存在于度等于 2，3，7 和 57 的情况，不可能存在于其他情况，而且对前 3 种情况，图是唯一存在的，对于直径为 3，度为 2 的情况，他们利用图的邻接矩阵 (及其主子矩阵) 的特征值和特征向量证明了唯一的摩尔图是 7 循环图. 已知的摩尔图都是顶点传递的，目前尚未找到度为 57，直径为 2 的摩尔图的具体例子，只能说明它在理论上是可能存在的.

Damerell 在 [8] 中通过将距离正则图理论应用于摩尔图的分类证明了：当度不小于 3 且直径不小于 3 时不存在摩尔图. Bannai 和 Ito 在 [9] 中给出了独立证明，Plesník[10] 也给出了不存在性的部分结果 (度不超过 100 且直径不超过 100) 的另一个独立证明. 下面是摩尔图存在性结果的总结并附有表格：

1) 直径 $k=1$，度 $d \geq 1$ 的摩尔图是完全图 K_{d+1}；

2) 直径 $k=2$，当度 $d=2$ 时，摩尔图是 5 循环图；当度 $d=3$ 时，摩尔图是 Petersen 图；当度 $d=7$ 时，摩尔图是 Hoffman-Singleton 图；

3) 直径 $k \geq 3$，度 $d=2$ 时，摩尔图是 $2d+1$ 循环图.

由于摩尔图只存在于仅有的几种情况，所以目前的研究思路是研究给定的直径和最大度时构造尽可能接近摩尔界的图，即阶为 $M(d,k)-\delta$ 的图，其中 δ 足够小，参数 δ 称为**缺陷** (defect). 通过比较 δ 和度 d 的大小来判断 δ 是否足够小，若 $\delta \leq d$，则认为 δ 足够小.

表 1.1　摩尔图

最大度 d	直径 k	摩尔图
≥ 2	1	完全图 K_{d+1}
2	≥ 2	$2d+1$ 循环图
3	2	Peterson 图
7	2	Hoffman-Singleton 图
57	2	?

Erdős，Fajtlowitcz 和 Hoffman 在 [11] 中证明了除了 4 循环图外，没有直径为 2，缺陷为 1 的图. 这一结果被 Bannai 和 Ito[12] 以及 Kurosowa 和 Tsujii[13] 进一步推广：对任意的直径，只要度 $d \geq 3$，则不存在缺陷为 1 的图，特别地，当 $d = 2$ 时，只存在唯一的情况，即 $2k$ 循环图. 对于缺陷为 2 的图，Elspas 等人也有研究，详见 [14-15].

对于交换凯莱图的“度——直径”问题，2004 年，Dougherty 和 Faber[1] 提出了交换凯莱摩尔界. 他们在 [1] 中提出了研究交换凯莱图的一个巧妙的方法. 对于任意有限交换群 G，设生成集为 S，将 S 中互逆的一对元中任取一个组成新的集合，称为**简化生成集** (reduced generating set)，记为 S'. 若 S' 中含有 d 个元，将 $\mathbb{Z}^d$ 中的 d 个单位向量 $e_i (i = 1, ..., d)$ 一一映射成 S' 中的 d 个元，则可得到一个 $\mathbb{Z}^d$ 到 G 的同态, 将同态的核记为 N. 对任何给定的直径 k，定义

$$W_{d,k} = \{(x_1, .., x_d) \in \mathbb{Z}^d : |x_1| + \cdot + |x_d| \leq k\}.$$

则交换凯莱图 $\Gamma(G, S)$ 的直径为 k 当且仅当 $W_{d,k} + N = \mathbb{Z}^d$. 通过构造这个同态，交换凯莱图上的“度——直径”问题可转化为组合几何学中的问题处理.

设度为 d，直径为 k 的交换凯莱图的最高阶为 $AC_{d,k}$，Dougherty 和 Faber[1] 通过对格铺砌的深入研究，得到了 $AC_{2n,k}$ 的一般下界，结合交换凯莱摩尔界，则有如下结论：存在一个与 n，k 无关的常数 c 使得对任何 $d \geq 2$ 和 k，有

$$\frac{c \times 2^n}{n! n (\ln n)^{1+\log_2 e}} \leq AC_{2n,k} \leq \sum_{i=0}^{\min\{n,k\}} 2^i \binom{n}{i} \binom{k}{i}.$$

若 n 固定且 $k \to \infty$，则不等式最右边的摩尔界等于 $2^n \frac{k^n}{n!} + O(k^{n-1})$. $AC_{2n,k}$ 的具体值是很难确定的，他们 [1] 利用格铺砌得到了如下结论：当 $n = 2$ 时，交换凯莱摩尔图存在，即 $AC_{4,k} = W_{2,k} = 2k^2 + 2k + 1$，对于 $n = 3$，可由同样的方法得到

$$AC_{6,k} \geq \frac{32k^3 + 48k^2}{27} + f(k).$$

其中 $f(k)$ 是一个与 k 的模 3 剩余类有关的线性函数，交换凯莱摩尔界为

$$AC_{6,k} \leq |W_{3,k}| = \frac{4k^3+6k^2+8k+3}{3}.$$

文献 [1] 中给出了 $k \leq 14$ 时的所有 $AC_{6,k}$.

对于直径 k 给定的情况，也已经有了很多结论. 当 $k=2$ 时，有

$$AC_{d,2} \geq \left\lfloor \frac{d+2}{2} \right\rfloor \left\lceil \frac{d+2}{2} \right\rceil.$$

顶点集 G 为 $\mathbb{Z}_{\lfloor \frac{d+2}{2} \rfloor} \times \mathbb{Z}_{\lceil \frac{d+2}{2} \rceil}$，生成集为 $\{(x_1,0) : x_1 \in \mathbb{Z}_{\lfloor \frac{d+2}{2} \rfloor} \setminus \{0\}\} \cup \{(0,x_2) : x_2 \in \mathbb{Z}_{\lfloor \frac{d+2}{2} \rfloor} \setminus \{0\}\}$ 的交换凯莱图达到该下界. 由于该下界比上界小很多，所以有猜想认为对任意的 d，都有 $AC_{d,2} \approx \frac{d^2}{2}$. 2016 年以前，关于 $AC_{d,2}$ 的下界的最好的结果是 Sirán，Siagiová 和 Ždímalová[16] 在 Macbeth，Siagiová 和 Sirán[4] 的研究结果的基础上得到的. Macbeth，Siagiová 和 Sirán[4] 得到的结论是：对所有的 $d=4q-2$，q 为奇素数的幂，$AC_{d,2} \geq \frac{3}{8}(d^2-4)$. [16] 的结果为：对足够大的 d，$AC_{d,2} \geq \frac{3}{8}d^2 - 1.45d^{1.525}$. 这方面的另一个结果 [4] 是：对所有的 $d=3q-1$，q 为奇素数的幂，$AC_{d,2} \geq \frac{(d+1)^2}{3}$. 2016 年，周悦与 Pott[17] 证明了对足够大的 d，$AC_{d,2} \geq \frac{25}{64}d^2 - 2.1d^{1.525}$，还证明了当 $d=3q$，$q=2^m$，m 是奇数时，$AC_{d,2} \geq \frac{4}{9}d^2$，提高了 $AC_{d,k}$ 的下界. 后来，对于 q 是奇素数幂，张韬和葛根年 [18] 证明了更好的结果：对于足够大的 d，$AC_{d,2} \geq \frac{27}{64}d^2 - 3.9d^{1.525}$，$AC_{d,k} \geq (\frac{3}{3k-1})^k d^k + O(d^{k-0.475})$.

由于交换凯莱图和李码有关而且本文中有两类图的证明方法是李码文章中的方法，因此对李码的研究进展也做简单的介绍. 1970 年，Golomb 和 Welch[19] 证明了在 $\mathbb{Z}^2$ 上对于任意的 $e \geq 1$，都存在 e- 完美李码；对任意的 $n \geq 2$，都存在 $\mathbb{Z}^n$ 的 1- 完美李码. 他们还证明，对于大于 3 的固定维数，存在某个正整数 e_n，使得对于 $e \geq e_n$，$\mathbb{Z}^n$ 中不存在 e- 完美李码. 并且推测 e_n 可能为 2，这就是著名的 Golomb-Welch 猜想.

在 [20] 中，Horak 和 Grošek 证明了：当 $7 \leq n \leq 12$ 时，$\mathbb{Z}^n$ 上不存在线性完美 r- 纠错李码. 张韬和葛根年 [21] 证明了半径等于 3 和 4 时部分维数下线性完美李码的不存在性.

1975 年，Post[22] 得到了 e_n 的部分显式表示：

$$e_n = \begin{cases} n-1, & 3 \leq n \leq 5; \\ \frac{\sqrt{2}}{2}n - \frac{1}{4}(3\sqrt{2}-2), & n \geq 6. \end{cases}$$

后来，Lepistö[23] 证明了当 $e \geq 285$ 时，e- 完美李码的维度一定满足 $n \geq \frac{(e+2)^2}{2}$. 最近，Horak 和 Kim[6] 证明了上述结论在一般情况下也成立. 此外，Horak 等人 [24-27] 还证明当 $3 \leq n \leq 5$ 且 $e \geq 2$，和 $n=6$ 且 $e=2$ 时猜想成立.

2016 年，Kim[28] 在假设 $p=2n^2+2n+1$ 是素数的前提下，利用对称多项式证明了当 n 满足 $a(x+1)+by=n$ 没有非负整数解 (a，b 分别是满足 $p \mid 4^a+4n+2$ 和 $p \mid 4^b-1$ 的最小正整数，若不存在这样的 a，则令 $a=\infty$) 时，2- 纠错码不存在，证明运用了反证法，先构造一个多项式，通过将该多项式用对称多项式的一种基表示，然后证明基中某些对称多项式的系数为零，最后导出矛盾. 该结果进一步证实了 Golomb-Welch 猜想的正确性. 2018 年，Qureshi[29] 运用更全面的对称多项式知识证明了 $\mathbb{Z}^n$ 上不存在格铺砌的一种充分条件，他的证明过程中用到了两种不同的对称多项式的基，通过将所研究的多项式用不同的基表示，从基的系数上找规律，最终得到充分条件. 这一结果排除了一部分参数下线性完美李码的存在性.

2018 年，周悦和张韬 [30] 用群环语言来处理这一类问题. 考虑乘法群，以群中的元为基，将元素都属于 G 的多重集表示成各个不同元相加的形式和，系数为该元在集合中出现的次数. 这样不同的形式和做乘法运算的结果就相当于是多重集中的元素相互做乘法运算后对应集合的群环表示，而后又引入群特征，将问题转化为代数整数环上的某个多项式是否有根的问题. 某些时候，该问题可以直接利用代数数论知识直接求解；否则还可以通过局部化方法，转化为有限域上多项式的求解问题. 结合 MAGMA 计算，得出结论. 该结论能够排除维数满足一定条件、半径为 2 的线性完美李码的存在性. 文中还说明了 Golomb-Welch 猜想与交换凯莱图上的“度——直径”问题之间的紧密联系. 2019 年，Leung 和周悦 [2] 合作证明了当李球的半径为 2 时，对任意维度 n，$\mathbb{Z}^n$ 上的格铺砌都不存在，由此可以推出当李球的半径为 2 且 $2n^2+2n+1$ 是素数时，Golomb-Welch 猜想是正确的. 论文 [28] 和 [30] 的方法将在第三章和第四章被用于处理本文研究的问题.

1.3 论文的安排

上一节内容表明：直径为 2 且度为 $2n$ 的交换凯莱摩尔图 (阶为 $2n^2+2n+1$) 只存在于 $n=1,2$ 的情况. 第二章介绍完交换凯莱图，李码及代数数论等相关基础知识后，受该结论启发，本文将在第三章研究度为 $2n$ 且直径为 2 的 $2n^2+2n$ 阶交换凯莱图的不存在性并证明：设 G 是一个 $2n^2+2n$ 阶的交换群. 若 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，以及下面三个条件满足其中之一

1) $3,7,11$ 或 $19 \mid n(n+1)$;

2) 对 $v=5$或13，$v \mid n(n+1)$ 且 $8n+5 \notin \{vk^2 : k \in \mathbb{Z}\}$;

3) $17 \mid n(n+1)$ 且 $8n+9 \notin \{17k^2 : k \in \mathbb{Z}\}$.

则不存在以 G 为顶点集的该类图.

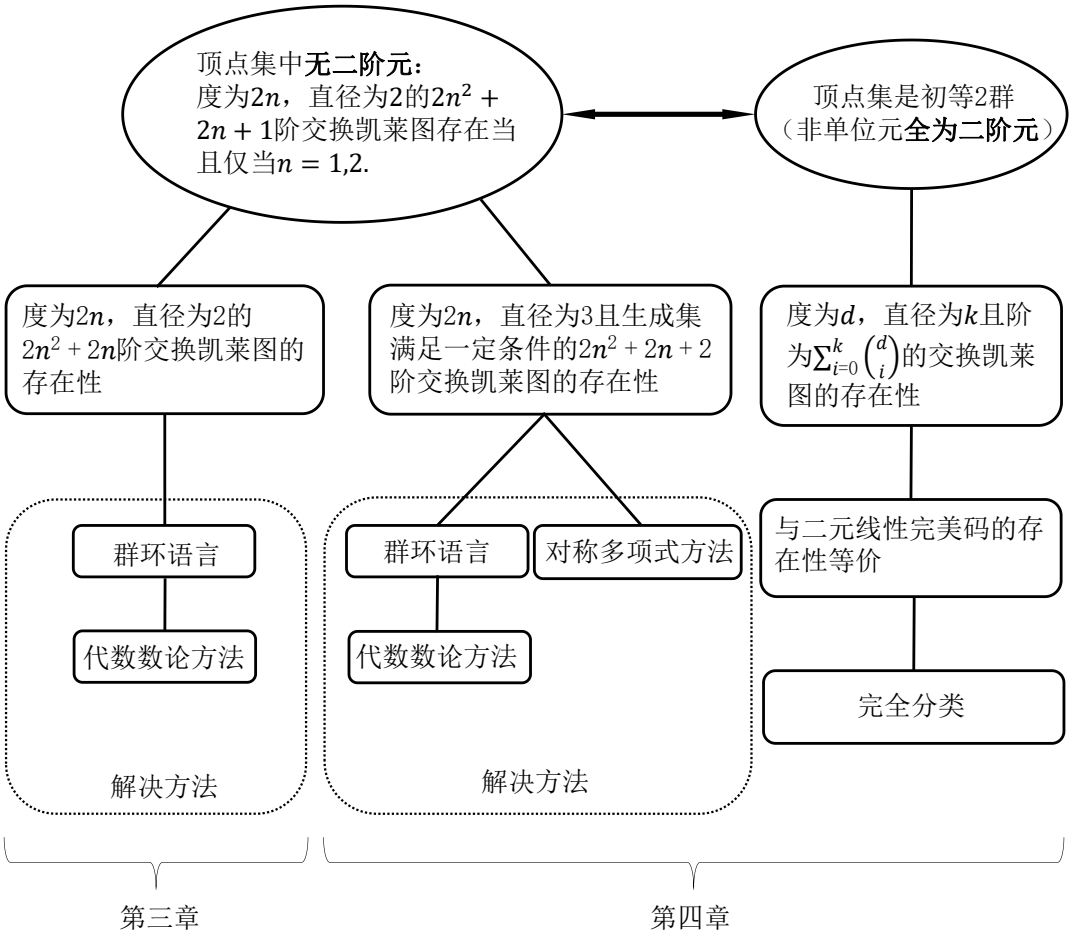

图 1.1　内容关系图

第四章分为两节，首节研究度为 $2n$，直径为 3 且生成集 S 满足 $|\tilde{S}^2| = 2n^2+2n+1$ 的 $2n^2+2n+2$ 阶交换凯莱图的不存在性 ($\tilde{S}=S\cup\{e\}$，$|\cdot|$ 表示多重集中不同元素的个数) 并证明：

一、 设 G 是阶为 $2n^2+2n+2$ 的交换群，$8n-7$ 不是 $\mathbb{Z}$ 上的平方元，若下列条件满足其中之一：

1) 3，7，19 或 $31 \mid n^2+n+1$；

2) $13 \mid n^2+n+1$ 且 $8n-11 \notin \{13k^2 : k\in\mathbb{Z}\}$.

则不存在以 G 为顶点集的该类图.

二、 假设 $2n^2+2n+2=mv(n>1)$，v 是素数且 $v>2n+1$. 设 G 是一个阶为 $2n^2+2n+2$ 的加法交换群. 设 a 是满足 $v \mid 4^a+4n+2$ 的最小正整数，b 是满足 $v \mid 4^b-1$ 的最小正整数 (若不存在 a 使得 $v \mid 4^a+4n+2$，则令 $a=\infty$). 若对 $\forall l \in \{0,1,\cdots,\lfloor\frac{m-1}{4}\rfloor\}$，$a(x+1)+by=n-l$ 都不存在非负整数解，则不存在以 G 为顶点集的第二类图.

第四章第二节研究顶点集为初等 2 群，生成集 S 的阶为 d，直径为 k 且阶达到上界 $\sum_{i=0}^{k}\binom{d}{i}$ 的交换凯莱图，证明其与汉明距离下的二元完美线性码的等价性. 并根据已有的完美码分类结果给出了这类图的完全分类：设 $G=(\mathbb{F}_2^m,+)$，则以 G 为顶点集的第三类图只存在如下几类：

1) $S=\{s:s\in G\setminus\{0,0,\cdots,0\}\}$，直径 $k=1$；

2) $2 \mid m$ 且 $S=\{e_1,e_2,\cdots,e_m,l_m\}$，直径 $k=\frac{m}{2}$；

   其中 $e_i(i=1,2,\cdots,m)$ 为标准基, l_m 为全 1 向量.

3) 当 $m=11$ 时，取 S 是由二元格雷码的校验矩阵全体列向量构成的集合. 此时，$|S|=23$，$\Gamma(G,S)$ 的直径 $k=3$.

第三、四章的内容关系如图1.1所示. 为了方便叙述，后续内容分别简称该三类图为第一、二、三类图.

最后一章是对研究生期间工作的总结，以及对未来研究的展望.

第二章　基础知识

2.1　李码与交换凯莱图

图中一个顶点的**度** (degree) 是指与该顶点连边的顶点个数，一个图的**最大度** (maximum degree) 和**最小度** (minimum degree) 指的是所有顶点的度的最大值和最小值. 两点间的**距离** (distance) 由连接两点的最短路径的长度表示，长度是指路径中包含除起始点之外的顶点个数. 一个图的**直径** (diameter) 指的是图中两个不同顶点间距离的最大值. 第一章提到了凯莱图的定义为：假设 G 是一个以 e 为单位元的乘法群，S 是 G 的一个子集，$S = S^{-1}$ 且 $e \notin S$，则**凯莱图** $\Gamma(G, S)$ 是以 G 为顶点集的无向图，G 中任意两点 g，h 相连当且仅当 $g^{-1}h \in S$. 当 G 为交换群时，$\Gamma(G, S)$ 为**交换凯莱图**. 由此可知，交换凯莱图 $\Gamma(G, S)$ 中每个点的度都等于 $|S|$，直径为 $\min\{l : \{s_1, ..., s_l : s_i \in S \cup \{e\}, i = 1, ..., l\} = G\}$.

令 $\mathbb{Z}$ 表示整数环，对 $\mathbb{Z}^n$ 中的两个码字 $x = (x_1, ..., x_n)$，$y = (y_1, ..., y_n)$，定义 x，y 的**李距离** (Lee distance) 为：

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

李码 (Lee code) 是定义了李距离的一个 $\mathbb{Z}^n$ 的子集. 若该集合有群结构，则称该码为**线性李码** (linear Lee code).

李码中任意两个不同的码字之间的距离的最小值称为码的**极小距离** (minimum distance)，当一个李码的极小距离不小于 $2r + 1$ 时，称该李码为 ***r*- 纠错码** (r-error-correcting code)，r 是**纠错半径** (error-correcting radius). 当 $\mathbb{Z}^n$ 中任意一个元都存在唯一一个码字与其距离不超过 r，则称该码是**完美码** (perfect code). $\mathbb{Z}^n$ 中的完美 r-纠错李码记作 *PL(n,r)*. 若还是线性码，则记作 *LPL(n,r)*.

令 V 表示 $\mathbb{Z}^n$ 中的一个子集，可以通过平移得到新集合 $V+x = \{v+x : v \in V\}$，其中 $x \in \mathbb{Z}^n$，若 $E = \{V + l : l \in L\}(L \in \mathbb{Z}^n)$ 中的集合互不相交且并集为 $\mathbb{Z}^n$，则称 E 是 $\mathbb{Z}^n$ 的一个**铺砌** (tiling). 若 L 是一个格，则称 E 是 $\mathbb{Z}^n$ 的一个**格铺砌** (lattice tiling). 球心在原点的**李球** (Lee sphere) 定义如下：

$$S(n, r) = \{x \in \mathbb{Z}^n : d_L(x, 0) = |x_1| + \cdots + |x_n| \leq r\}.$$

因此 C 是 $\mathbb{Z}^n$ 上的完美李码当且仅当 $\{S(n, r) + c : c \in C\}$ 构成 $\mathbb{Z}^n$ 的一个铺砌；C 是 $\mathbb{Z}^n$ 上的线性完美李码当且仅当 $\{S(n, r) + c : c \in C\}$ 构成 $\mathbb{Z}^n$ 的一个格铺砌.

Horák 等在 [31] 中建立了有限交换群与 $\mathbb{Z}^n$ 上的格铺砌的如下关系.

定理 2.1 ([31]): 设 $S \subseteq \mathbb{Z}^n$ 且 $|S| = m$，则 $\mathbb{Z}^n$ 上关于 S 的格铺砌存在当且仅当存在一个阶为 m 的交换群 G 和一个同态：$\phi : \mathbb{Z}^n \mapsto G$，且该同态在 S 上是双射.

如果 m 是素数，则有如下定理.

定理 2.2 ([31]): 设 $S \subseteq \mathbb{Z}^n$，$|S| = p$ 且 p 是素数，则 $\mathbb{Z}^n$ 上关于 S 的格铺砌存在当且仅当存在一个同态：$\phi : \mathbb{Z}^n \mapsto C_p$，且该同态在 S 上是双射.

由定理2.1和2.2容易得到如下推论.

推论 2.3 ([31]): $LPL(n, r)$ 存在当且仅当存在一个交换群 G 和一个同态：$\phi : \mathbb{Z}^n \mapsto G$，且该同态在 $S(n, r)$ 上是双射.

下面证明线性完美李码 $LPL(n, r)$ 与度为 $2n$，直径为 r 的交换凯莱摩尔图的存在性等价.

定理 2.4: 线性完美李码 $LPL(n, r)$ 存在性与度为 $2n$，直径为 r 的交换凯莱摩尔图存在性等价.

证明： 根据 [1] 可知，

$$|S(n, r)| = \sum_{i=0}^{\min\{n,r\}} 2^i \binom{n}{i}\binom{r}{i}.$$

由推论2.3可得，$LPL(n, r)$ 存在意味着存在一个满足 $|G| = \sum_{i=0}^{\min\{n,r\}} 2^i \binom{n}{i}\binom{r}{i}$ 的交换群 G(不妨设为加法群) 和一个同态 $\phi : \mathbb{Z}^n \mapsto G$，且该同态在 $S(n, r)$ 上是双射. 设 $e_1, \cdots, e_n$ 是 $\mathbb{Z}^n$ 上的标准基，则 $S(n, r)$ 可写成如下形式.

$$\begin{aligned} S(n, r) = \{0\} \cup \{\pm e_i : i = 1, \cdots, n\} \cup \{\pm e_{i_1} \pm e_{i_2} : 1 \le i_1 \le i_2 \le n\} \cup \\ \cdots \cup \{\pm e_{i_1} \pm \cdots \pm e_{i_r} : 1 \le i_1 \le \cdots \le i_r \le n\}. \end{aligned}$$

因为 ϕ 在 $S(n, r)$ 上是双射，则

$$\begin{aligned} G = \{0\} \cup \{\pm\phi(e_i) : i = 1, \cdots, n\} \cup \{\pm\phi(e_{i_1}) \pm \phi(e_{i_2}) : 1 \le i_1 \le i_2 \le n\} \cup \\ \cdots \cup \{\pm\phi(e_{i_1}) \pm \cdots \pm \phi(e_{i_r}) : 1 \le i_1 \le \cdots \le i_r \le n\}. \end{aligned} \tag{2.1}$$

这说明以 G 为顶点集，$S = \{\pm\phi(e_1), \cdots, \pm\phi(e_n)\}$ 为生成集可构成一个交换凯莱图 $\Gamma(G, S)$，并且 $\Gamma(G, S)$ 达到了交换凯莱摩尔界，因此，$\Gamma(G, S)$ 是一个度为 $2n$，直径为 r 的交换凯莱摩尔图.

相反，若度为 $2n$，直径为 r 的交换凯莱摩尔图 $\Gamma(G,S)$ 存在. 不妨设 $S=\{\pm s_i : i=1,\cdots,n\}$，$\phi$ 是 $\mathbb{Z}^n$ 到 G 的映射. 令 $\phi(e_i)=s_i, i=1,\cdots,n$，则 ϕ 是一个同态. 由于 $\Gamma(G,S)$ 是交换凯莱摩尔图，则 $|S(n,r)|=|G|=\sum_{i=0}^{\min\{n,r\}} 2^i\binom{n}{i}\binom{r}{i}$ 且 ϕ 在 $S(n,r)$ 上是双射. 根据推论2.3得 $LPL(n,r)$ 存在. □

例如，当 $n=2$，$r=2$ 时交换凯莱图如图2.1，对应的线性完美李码如图2.2.

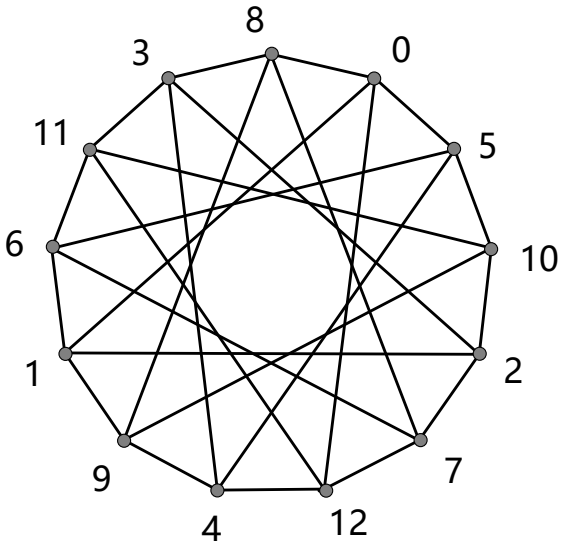

图 2.1　顶点集为 C_{13}，生成集为 $\{\pm1,\pm5\}$ 的交换凯莱摩尔图

9	10	11	12	0	1	2	3	4	5	6	7	8
4	5	6	7	8	9	10	11	12	0	1	2	3
12	0	1	2	3	4	5	6	7	8	9	10	11
7	8	9	10	11	12	0	1	2	3	4	5	6
2	3	4	5	6	7	8	9	10	11	12	0	1
10	11	12	0	1	2	3	4	5	6	7	8	9
5	6	7	8	9	10	11	12	0	1	2	3	4
0	1	2	3	4	5	6	7	8	9	10	11	12
8	9	10	11	12	0	1	2	3	4	5	6	7
3	4	5	6	7	8	9	10	11	12	0	1	2

图 2.2　$LPL(2,2)$

对于第一、二类图，按照定理2.4的证明过程中的方法也可以构造出对应的线

性李码. 两类图所对应的线性李码与完美线性李码很接近. 对于第一类图对应的线性码，若分别以每个码字为球心，2 为半径构造李球，则部分相邻的李球之间存在且仅存在一个交叉点. 对于第二类图对应的线性码，若分别以每个码字为球心，2 为半径构造李球，则部分相邻的李球之间会存在一个不属于任何李球的点. 将上述两种情况一般化，考虑 $\mathbb{Z}^n$ 上的线性李码，若存在 $r \in \mathbb{Z}$ 使得以 r 为半径构造李球满足上述性质，则称之为**几乎完美线性李码**，分别记为 $\mathrm{APLL}^+(n,r)$ 和 $\mathrm{APLL}^-(n,r)$.

2.2 群环与预备代数数论知识

后续的推导和证明过程涉及群环语言. 群环以及相关的特征被广泛应用于差集相关问题的研究，差集中很多重要的不存在性结果都是利用群环语言得到的，具体参考 [32-33] 及其中所引用的文献. 设 G 是以 e 为单位元的乘法群，**群环** $\mathbb{Z}[G]$ 指的是以 $\{g : g \in G\}$ 为基的交换群. 对任意一个多重集 A(A 中的元素都属于 G)，将 A 写成 $\sum_{g\in G} a_g g$，其中 a_g 等于 g 在 A 中出现的次数. $\mathbb{Z}[G]$ 中元素的加法和乘法分别定义如下：

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g.$$

$$(\sum_{g\in G} a_g g) \cdot (\sum_{g\in G} b_g g) := \sum_{g\in G} (\sum_{h\in G} a_h b_{h^{-1}g}) g.$$

另外，对任意的 $\lambda \in \mathbb{Z}$，

$$\lambda \cdot (\sum_{g\in G} a_g g) := \sum_{g\in G} (\lambda a_g) g.$$

对任意的 $A = \sum_{g\in G} a_g g$ 和 $t \in \mathbb{Z}$，定义

$$A^{(t)} := \sum_{g\in G} a_g g^t.$$

记 G 的特征群为 $\widehat{G}$. 对任意的 $A = \sum_{g\in G} a_g g$ 和 $\chi \in \widehat{G}$，定义 $\chi(A) = \sum_{g\in G} a_g \chi(g)$.

引理 2.1 ([30]): 设 G 是一个交换群. 若 $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$，则对所有 $h \in G$，

$$a_h := \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(A)\chi(h^{-1}). \tag{2.2}$$

(2.2)表明 A 完全由 $\chi(A)$ 决定，其中 χ 取遍 $\widehat{G}$ 中所有元.

第三章和第四章的推导证明中将用到关于包含 $\mathbb{Q}(\sqrt{m})$ 的最小分圆域和 $\mathbb{Z}[\zeta_\omega]$ 中的素理想分解的如下两个引理. 设 ζ_ω 是 $\mathbb{C}$ 中的 ω 次本原单位根，$\mathbb{Q}(\zeta_\omega)$ 表示同时包含 $\mathbb{Q}$ 和 ζ_ω 的最小的域，被称为 ω 次本原单位根**分圆域** (cyclotomic fields). 包含 $\mathbb{Q}(\sqrt{m})$ 的分圆域有多个，最小的域称为包含 $\mathbb{Q}(\sqrt{m})$ 的**最小分圆域**. **素理想分解** (prime ideal decomposition) 指的是将一个理想分解为有限个素理想的乘积. 素数 p 的主理想 (p) 在 $\mathbb{Z}$ 中是素理想，但在 $\mathbb{Z}[\zeta_\omega]$ 中有可能进一步分解.

引理 2.2 ([34]): *若 m 是非平方元整数，m 的素数分解如下*

$$m = 2^t \prod_j p_j,$$

其中 p_j 是 m 的奇素数因子，$t = 0$ 或 1. 设 $m' = \prod_j p_j$，则包含 $\mathbb{Q}(\sqrt{m})$ 的最小分圆域为

$$\begin{cases} \mathbb{Q}(\zeta_{m'}), & 若 m \equiv 1 \pmod 4; \\ \mathbb{Q}(\zeta_{4m'}), & 若 m \equiv -1 \pmod 4; \\ \mathbb{Q}(\zeta_{8m'}), & 若 m \equiv 2 \pmod 4. \end{cases}$$

引理 2.3 ([30]): *设 p 为一个素数，ζ_ω 是 $\mathbb{C}$ 中的 ω 次本原单位根. 若 $\omega = p^r\omega'$，其中 $\gcd(\omega', p) = 1$，则 (p) 在 $\mathbb{Z}[\zeta_\omega]$ 中的素理想分解为*

$$(p) = (P_1 P_2 ... P_d)^e,$$

其中 $P_i (i = 1, \cdots, d)$ 是不同的素理想，$e = \varphi(p^r)$，$d = \varphi(\omega')/f$，f 是 p 模 ω' 的乘法阶. 若 t 是一个不能被 p 整除的整数，且对某个整数 s，$t \equiv p^s \pmod{\omega'}$，则域的自同构 $\sigma_t : \zeta_{\omega'} \mapsto \zeta_{\omega'}^t$ 在 $P_i (i = 1, \cdots, d)$ 上是恒等映射.

2.3 对称多项式

在第四章证明第二类图时，需要用到对称多项式方法，本节介绍文中涉及的对称多项式知识.

对称函数理论在代数组合学、群论、李代数和代数几何等其他数学分支都有广泛的应用，是一项重要的研究工具.

考虑 n 维整系数多项式 $\mathbb{Q}[x_1, \cdots, x_n]$，定义对称群 S_n 通过排列 $x_i (i = 1, \cdots, n)$ 的顺序作用于该环中的元素. 若一个多项式在 S_n 所有元素的作用下保持不变，则称之为**对称多项式**. 根据对称多项式的性质不难发现全体 n 元对称多项式构成 $\mathbb{Q}[x_1, \cdots, x_n]$ 的一个子环，记为 Λ_n. 显然 $\Lambda_n = \bigoplus_{k \geq 0} \Lambda_n^k$，其中 Λ_n^k 是所有次数为 k 的齐次对称多项式和零多项式组成的集合.

定义一个非负整数 n 的一个划分 λ 为满足 $\lambda_1 \geq \cdots \geq \lambda_k$ 和 $\sum \lambda_i = n$ 的序列 $(\lambda_1, \cdots, \lambda_k) \in \mathbb{N}^k$. λ 中非零元的数量称为 λ 的长度. n 的全部划分组成的集合记为 $Par(n)$.

关于对称多项式，目前证明了一个重要的结论：Λ_n 共有 6 种基，第四章的对称多项式方法涉及了其中两种，具体定义如下：

1) **初等对称多项式** (elementary symmetric polynomials)，记为 e_λ，其中 $\lambda \in Par(n)$；

$$e_n = \sum_{i_1 < \cdots < i_n} x_{i_1} \cdots x_{i_n}, n \geq 1 \quad (e_0 = 1),$$
$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}, \quad \text{其中} \lambda = (\lambda_1, \cdots, \lambda_k).$$

2) **幂和对称多项式** (power sum symmetric polynomials)，记为 p_λ，其中 $\lambda \in Par(n)$；

$$p_n = \sum_i x_i^n, n \geq 1 \quad (p_0 = 1),$$
$$p_\lambda = p_{\lambda_1} p_{\lambda_2} \cdots p_{\lambda_k}, \quad \text{其中} \lambda = (\lambda_1, \cdots, \lambda_k).$$

第三章　第一类图的存在性问题

根据交换凯莱摩尔界可知，一个度为 $2n$ 和直径为 2 的交换凯莱图的阶不超过 $2n^2+2n+1$. 而且已有的研究结果表明：直径为 2 的交换凯莱摩尔图存在当且仅当 $n=1,2$[2]. 本章研究的问题是当 n 取何值时，不存在阶等于 $2n^2+2n$ 的交换凯莱图.

本章将运用代数数论、有限域和群特征标等数学工具证明结论：设 G 是一个 $2n^2+2n$ 阶的交换群. 若 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，以及下面三个条件满足其中之一：

1) $3,7,11$ 或 $19 \mid n(n+1)$;

2) 对 $v=5$或13，$v \mid n(n+1)$ 且 $8n+5 \notin \{vk^2 : k \in \mathbb{Z}\}$;

3) $17 \mid n(n+1)$ 且 $8n+9 \notin \{17k^2 : k \in \mathbb{Z}\}$.

则不存在以 G 为顶点集的该类图. 根据上述结论，可以排除 10^5 以内，91741 个 n 取值情况下第一类图的存在性.

3.1　充要条件

首先，对于 $n=1,2$ 的情况，可找到如下例子.

例 3.1: 设 C_m 为阶为 m 的循环群，其生成元为 g.

1) 当 $n=1$，$|G|=4$ 时，定义

$$S=\begin{cases}\{g^{\pm 1}\}, & G=C_4;\\ \{f_1,f_2\}, & G=C_2\times C_2=\langle f_1\rangle\times\langle f_2\rangle.\end{cases}$$

则交换凯莱图 $\Gamma(G,S)$ 是一个 4 循环图. 当 $G=C_4$ 时，$\Gamma(G,S)$ 对应的几乎完美线性李码如图3.1所示. 当 $G=C_2\times C_2$ 时不存在几乎完美线性李码与之对应.

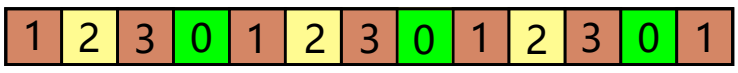

图 3.1　$G=C_4$，$S=\{\pm 1\}$ 时 $\Gamma(G,S)$ 对应的几乎完美线性李码

2) 当 $n=2$ 时，令 $G=C_{12}$，$S=\{g^{\pm 2},g^{\pm 3}\}$. 则交换凯莱图 $\Gamma(G,S)$ 如图所示3.2. 对应的几乎完美线性李码如图3.3所示.

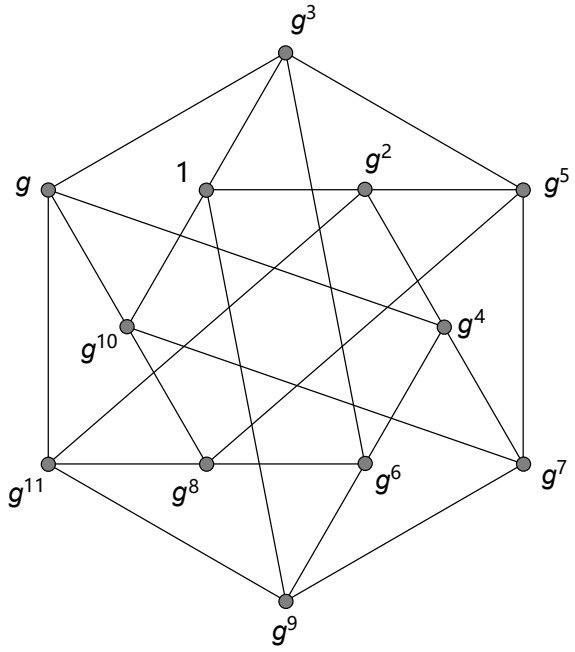

图 3.2　顶点集为 C_{12}，由 $\{g^{\pm 2}, g^{\pm 3}\}$ 生成的交换凯莱图

6	9	0	3	6	9	0	3	6	9	0	3	6
4	7	10	1	4	7	10	1	4	7	10	1	4
2	5	8	11	2	5	8	11	2	5	8	11	2
0	3	6	9	0	3	6	9	0	3	6	9	0
10	1	4	7	10	1	4	7	10	1	4	7	10
8	11	2	5	8	11	2	5	8	11	2	5	8
6	9	0	3	6	9	0	3	6	9	0	3	6
4	7	10	1	4	7	10	1	4	7	10	1	4
2	5	8	11	2	5	8	11	2	5	8	11	2

图 3.3　$G = C_{12}$，$S = \{g^{\pm 2}, g^{\pm 3}\}$ 时 $\Gamma(G, S)$ 对应的几乎完美线性李码

接下来将证明对于第一类图的顶点集 G 只可能包含一个或三个二阶元，而且，若包含一个二阶元 f，则存在 $a \in S$，使得 $a^2 = f$；若包含三个二阶元，则生成集 S 中包含两个二阶元.

引理 3.1: 设 G 是一个 $2n^2 + 2n$ 阶乘法群，$\Gamma(G, S)$ 是一个直径为 2 的交换凯莱图，其中 $|S| = 2n$. 则 G 中包含一个或三个二阶元，而且，当 G 只包含一个二阶元 f 时, $f \in \{a^2 : a \in S\}$.

证明：因为 S 是逆运算封闭的且 $|S|=2n$，则可以假设 S 由 S_0 和 S_1 两部分组成，其中 $S_0=\{f: f\in S, \mathrm{ord}(f)=2\}$，$S_1=\{a,a^{-1}: a\in S, \mathrm{ord}(a)\neq 2\}$. 设 $|S_1|=2m$，则 $|S_0|=2(n-m)$.

令 $T=S\cup\{e\}$，$\{*\ *\}$ 表示元素可重复的多重集，则 T^2 可写成如下并集形式

$$\{e\}\cup S\cup\{*\ ab: a,b\in S_0, a\neq b\ *\}\cup\{*\ cd: c,d\in S_1, c\neq d, d^{-1}\ *\} \tag{3.1}$$
$$\cup\{*\ a^2: a\in S_1\ *\}\cup\{*\ ac: a\in S_0, c\in S_1\ *\}.$$

(3.1)中包含的不同的元素个数最多为

$$\begin{aligned}&1+2n+\binom{2(n-m)}{2}+\frac{2m(2m-2)}{2}+2m+2(n-m)\cdot 2m\\ =&2n^2+n+m+1.\end{aligned}$$

由于 $\Gamma(G,S)$ 的直径为 2，因此 G 中所有的元素均在(3.1)中出现，所以 $2n^2+2n\leq 2n^2+n+m+1$，即 $n-m\leq 1$.

情况 **1**：$m=n$.

该情况意味着 $S_0=\varnothing$，$S=S_1$. 通过计算(3.1)中元素的个数可知，G 中恰好存在一个元素 f 在(3.1)中出现了两次. 下面证明 f 是 G 中唯一的二阶元且 $f\in\{*\ a^2: a\in S_1\ *\}$.

由于 $|G|$ 为偶数，则 G 中至少有一个二阶元. 令 h 为 G 中任意一个二阶元. 因为 $h\notin S$ 且 $\Gamma(G,S)$ 的直径为 2，则一定存在 $x,y\in S$ 使得 $xy=h$. 因此 $x^{-1}y^{-1}=h$，这意味着 h 是唯一一个在(3.1)中出现两次的元. 所以 G 只包含一个二阶元.

此外，由 $xy=f=x^{-1}y^{-1}$ 可以推出 $x^2=y^{-2}$. 若 $x\neq y$，则 f 在(3.1)的 $\{*\ cd: c,d\in S_1, c\neq d, d^{-1}\ *\}$ 中出现两次，x^2 在 $\{*\ a^2: a\in S_1\ *\}$ 中也出现了两次，与前面的结论相矛盾. 所以 $x=y$ 且 $f\in\{*\ a^2: a\in S_1\ *\}$.

情况 **2**：$m=n-1$.

该情况下 S_0 有两个元素，S_1 有 $2n-2$ 个元素且每个 G 中的元素恰好只在(3.1)中出现一次. 记 $S_0=\{f_1,f_2\}$，则 G 中至少有 f_1, f_2, f_1f_2 这三个二阶元. 下面证明 G 中不存在其他的二阶元.

首先 $\{*\ cd: c,d\in S_1, c\neq d, d^{-1}\ *\}\cup\{*\ a^2: a\in S_1\ *\}$ 中不可能有二阶元，否则该二阶元在(3.1)中出现偶数次，与前面结论相矛盾. 其次，若 $\{ac: a\in S_0, c\in S_1\}$ 中有二阶元，不失一般性，将其记为 ac，其中 $a\in S_0$，$c\in S_1$. 因此 c 是一个二阶元，与假设相矛盾.

因此，G 中没有除 f_1, f_2, f_1f_2 之外的二阶元. □

由引理3.1可以将第一类图分为如下两类：

I: G 中只有一个二阶元.

II: G 有三个二阶元.

根据前述例子，不难发现 **I** 类图存在几乎完美线性李码与之对应，而 **II** 类图不存在对应的几乎完美线性李码. 在证明该结论之前，首先证明如下定理.

定理 3.1: $\mathrm{APLL}^+(n,r)$ 存在当且仅当存在一个阶为 $\sum_{i=0}^{\min\{n,r\}} 2^i\binom{n}{i}\binom{r}{i}-1$ 的交换群 G 和一个同态：$\phi:\mathbb{Z}^n\mapsto G$，且该同态在 $S(n,r)\setminus\{\pm re_{i_0}\}$ 上是单射，$\phi(\pm re_{i_0})=f$，其中 e_i 是 $\mathbb{Z}^n$ 标准基中的一个元，$\{\pm re_{i_0}\}$ 分别是 $S(n,r)$ 与邻球的唯一交叉点，f 是 G 中的唯一二阶元.

证明： 首先证明必要性.

设 C 是 $\mathrm{APLL}^+(n,r)$，w 是 $\mathbb{Z}^n$ 中 $\bigcup_{c\in C}(S(n,r)+c)$ 任意一个重复的元素. 根据 $\mathrm{APLL}^+(n,r)$ 的定义可知，C 是 $\mathbb{Z}^n$ 的子群，且 $\mathbb{Z}^n$ 作为多重集有如下等式

$$\mathbb{Z}^n\bigcup(w+C)=\bigcup_{c\in C}(S(n,r)+c). \tag{3.2}$$

考虑商群 $G=\mathbb{Z}^n/C$. 取 ϕ 为 $\mathbb{Z}^n$ 到 G 的典型同态. 若存在 $x,y\in S(n,r)\setminus\{\pm re_i\}$，使得 $\phi(x)=\phi(y)$，则 $z=x-y\in C$. 因为 $y\in S(n,r)\setminus\{\pm re_i\}$，则 $x\in S(n,r)\setminus\{\pm re_i\}+z$. 这意味着 x 同时被 $S(n,r)\setminus\{\pm re_i\}+z$ 和 $S(n,r)\setminus\{\pm re_i\}$ 覆盖. 由 $APLL_1$ 的定义，$S(n,r)\setminus\{\pm re_i\}$ 与其余李球都不相交，所以 $z=0$，即 $x=y$. 因此 ϕ 在 $S(n,r)\setminus\{\pm re_i\}$ 上是单射.

下面说明 $\phi(re_i)=\phi(-re_i)=f$. 若存在 $x_0\in S(n,r)\setminus\{\pm re_i\}$ 使得 $\phi(re_i)=\phi(x_0)$. 因此 $x_0-re_i\in C$，即 $x_0\in re_i+C$，这与 $x_0\in S(n,r)\setminus\{\pm re_i\}$ 矛盾! 因此 $\phi(re_i)\in G\setminus\phi(S(n,r)\setminus\{\pm re_i\})$. 因为 G 的阶为 $\sum_{i=0}^{\min\{n,r\}} 2^i\binom{n}{i}\binom{r}{i}-1$ 且 ϕ 在 $S(n,r)\setminus\{\pm re_i\}$ 上是单射，所以 $\phi(re_i)=f$. 又 f 是二阶元，因此 $\phi(re_i)=\phi(-re_i)=f$.

对于充分性，只需定义 $C=ker(\phi)$，容易验证 C 是 $\mathrm{APLL}^+(n,r)$. □

若生成集 S 中不存在二阶元，则可令 $S=\{\pm\phi(e_i),i=1,\cdots,n\}$，$G$ 如定理2.4证明过程中的(2.1)式所示，则类似定理2.4的证明，由定理3.1可得如下推论.

推论 3.2: 若交换群 G 中只有一个二阶元，$|G|=\sum_{i=0}^{\min\{n,r\}} 2^i\binom{n}{i}\binom{r}{i}-1$，则度为 $2n$，直径为 r 的交换凯莱图 $\Gamma(G,S)$ 存在等价于 $\mathrm{APLL}^+(\mathrm{n},\mathrm{r})$ 存在.

对于 **II** 类图，生成集 S 中包含两个二阶元 (记为 f_1 和 f_2)，其余都是成对出现的互逆非二阶元. 在类似定理2.4证明过程中构造同态 $\phi:\mathbb{Z}^n\mapsto G$ 时，一定存在一个 e_i 使得 $\phi(e_i)=f_1$，$\phi(-e_i)=f_2$. 于是 $\phi(0)=f_1+f_2$，因此 ϕ 不是同态. 这表明 **II** 类图不存在对应的几乎完美线性李码.

利用群环语言可以推导 **I**，**II** 类图存在的充要条件.

定理 3.3: 设 G 是一个单位元为 e 的 $2n^2+2n$ 阶交换乘法群，S 是一个 G 的逆运算封闭的子集，$|S|=2n$ 且 $e\notin S$，则交换凯莱图 $\Gamma(G,S)$ 的直径为 2 当且仅当存在 T 满足

(a) $e\in T$,

(b) $T=T^{(-1)}$,

(c) $T^2=\begin{cases}2G-T^{(2)}+2ne+2f, & G\text{为第 I 类;}\\ 2G-T^{(2)}+2(n+1)e, & G\text{为第 II 类.}\end{cases}$

证明: 先证明必要性. 假设 $\Gamma(G,S)$ 的直径是 2，G 为第 I 类. 根据引理3.1，G 中的唯一二阶元 f 不在 S 中. 令 $S=\{a_1,\cdots,a_n\}\bigcup\{a_1^{-1},\cdots,a_n^{-1}\}$. 令 $T=e+\sum_{i=1}^n(a_i+a_i^{-1})$. (a) 和 (b) 显然满足.

根据引理3.1证明过程中对(3.1)的分析可知，运用群环语言可得如下等式

$$G+f=e+\sum_{i=1}^n(a_i+a_i^{-1}+a_i^2+a_i^{-2})+\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1}).$$

根据 T^2 的展开式可得

$$\begin{aligned}T^2=&\left(e+\sum_{i=1}^n(a_i+a_i^{-1})\right)^2\\ =&e+2\sum_{i=1}^n(a_i+a_i^{-1})+\left(\sum_{i=1}^n(a_i+a_i^{-1})\right)^2\\ =&e+2\sum_{i=1}^n(a_i+a_i^{-1})+\sum_{i=1}^n(a_i^2+a_i^{-2})+2\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1})+2ne\\ =&2e+2\sum_{i=1}^n(a_i+a_i^{-1})+2\sum_{i=1}^n(a_i^2+a_i^{-2})+2\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1})\\ &+(2n-1)e-\sum_{i=1}^n(a_i^2+a_i^{-2})\\ =&2G-T^{(2)}+2ne+2f.\end{aligned}$$

因此，当 G 属于第 I 类时，也满足 (c).

若 G 为第 II 类. 根据引理3.1，可以假设 $S=\{f_1,f_2\}\bigcup\{a_3,a_3^{-1},\cdots,a_{n+1},a_{n+1}^{-1}\}$，其中 f_1 和 f_2 都是 G 的二阶元. 令 $T=e+f_1+f_2+\sum_{i=3}^{n+1}(a_i+a_i^{-1})$，则 T 满足 (a) 和 (b). 通过计算可得，

$$\begin{aligned}T^2=&\left(e+f_1+f_2+\sum_{i=3}^{n+1}(a_i+a_i^{-1})\right)^2\\=&e+e+e+\left(\sum_{i=3}^{n+1}(a_i+a_i^{-1})\right)^2+2f_1+2f_2+2\sum_{i=3}^{n+1}(a_i+a_i^{-1})\\&+2f_1\sum_{i=3}^{n+1}(a_i+a_i^{-1})+2f_2\sum_{i=3}^{n+1}(a_i+a_i^{-1})\\=&3e+\sum_{i=3}^{n+1}(a_i^2+a_i^{-2})+2\sum_{3\leqslant i<j\leqslant n+1}(a_i+a_i^{-1})(a_j+a_j^{-1})+2(n-1)e+2f_1\\&+2f_2+2\sum_{i=3}^{n+1}(a_i+a_i^{-1})+2f_1\sum_{i=3}^{n+1}(a_i+a_i^{-1})+2f_2\sum_{i=3}^{n+1}(a_i+a_i^{-1}).\end{aligned}$$

根据引理3.1中对(3.1)的分析可知，G 的群环语言表示如下：

$$\begin{aligned}G=&e+f_1+f_2+\sum_{i=3}^{n+1}(a_i+a_i^{-1}+a_i^2+a_i^{-2})+\sum_{3\leqslant i<j\leqslant n+1}(a_i+a_i^{-1})(a_j+a_j^{-1})+\\&f_1f_2+f_1\sum_{i=3}^{n+1}(a_i+a_i^{-1})+f_2\sum_{i=3}^{n+1}(a_i+a_i^{-1}).\end{aligned}$$

将其代入到 T^2 中可得

$$T^2=2G-T^{(2)}+2(n+1)e.$$

因此，当 G 属于第 II 类时，也满足 (c).

从上述证明中可知，设 $S=T\setminus\{e\}$，条件 (a)、(b) 和 (c) 只是用群环语言解释了 $\Gamma(G,S)$ 直径为 2 时的性质. 因此，充分性部分的证明是显然的. □

3.2 主要结论的证明

在 [28] 中，Kim 使用对称多项式方法证明了一定维数下完美 2- 纠错李码的不存在性. 不过该方法适用的前提是 $|G|$ 必须存在大于 $2n+1$ 的素因子. 然而，$|G|=2n(n+1)$ 的所有素因子都不超过 $n+1$. 因此，[28] 中的方法不适用于本章的问题. 但在证明第二类图时，$|G|$ 可能存在大于 $2n+1$ 的素因子，因此适用，详

见第四章. 文献 [30] 用代数数论方法证明了线性完美李码的不存在性，该方法适用于本章研究的问题，本文称之为**代数数论和有限域方法**.

由引理3.1可知，该情况下 G 包含一个或三个二阶元. 因此，对任意子群 H，若满足 $|G/H|$ 是一个奇素数，则 H 一定包含 G 中所有的二阶元. 用 $\overline{(\cdot)} : G \to G/H$ 表示典型同态，则 G 中所有二阶元都将映射为 G/H 的单位元. 另外，对任意 $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, 定义 $\overline{A} = \sum_{g\in G} a_g \bar{g}$.

对一个 m 阶的子群 H，其中 m 为偶数，且 $|G/H|$ 是奇素数，若 T 满足定理3.3中的三个条件，则必然满足如下两个等式.

(b') $\overline{T} = \overline{T}^{(-1)}$,

(c') $\overline{T}^2 = 2mG/H - \overline{T}^{(2)} + (2n+2)$.

另外，为了方便书写，记 G/H 的单位元 $\bar{e}$ 为 1，因此 $(2n+2)\bar{e}$ 可以简化地写作 $(2n+2)$.

首先，考虑满足条件 (b') 和 (c') 的一个特殊情况.

引理 3.2: 设 K 为一个 v 阶的交换群，单位元为 e_K，$S = a \cdot e_K + bK \in \mathbb{Z}[K]$. 若 v 和 m 是满足 $a + vb = 2n+1$ 和 $mv = 2n^2 + 2n$ 的正整数，且 S 满足

$$S^2 = 2mK - S + (2n+2)e_K. \tag{3.3}$$

则 $8n+9$ 是 $\mathbb{Z}$ 的一个平方元.

证明: 经计算可得

$$\begin{aligned} S^2 &= (ae_K + bK)^2 \\ &= a^2 e_K + 2abK + b^2 vK \\ &= a^2 e_K + (ab + b(2n+1))K. \end{aligned}$$

通过比较 e_K 在(3.3)中的系数可得

$$a^2 + a - 2n - 2 = 0.$$

这表明 $8n+9$ 是 $\mathbb{Z}$ 中的一个平方元. □

先考虑 $G/H \cong C_3$ 时，满足条件 (b') 和 (c') 的 $\overline{T}$ 的存在性.

命题 3.1: 假设 $G/H \cong C_3$ 且 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元. 则不存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_3]$.

证明：运用反证法，假设存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_3]$. 因为 $\overline{T}^{(2)} = \overline{T}^{(-1)} = \overline{T}$，所以存在 $a, b \in \mathbb{Z}_{\geq 0}$ 使得 $\overline{T} = a + bG/H$，由条件 (c') 可得

$$\overline{T}^2 = 2mG/H - \overline{T} + 2n + 2.$$

由引理3.2，$8n+9$ 是 $\mathbb{Z}$ 中的一个平方元，这与假设条件相矛盾. 因此，不存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_3]$. □

下一个可能整除 $|G|$ 的奇素数是 5，因此接下来考虑 $G/H \cong C_5$ 的情况.

定理 3.4: 假设 $G/H \cong C_5$，$8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，对任意的 $k \in \mathbb{Z}$，$8n+5 \neq 5k^2$. 则不存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_5]$.

证明：用反证法，假设存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_5]$. 由条件 (c') 可得

$$\overline{T}^2 \equiv -\overline{T}^{(2)} + 2n + 2 \pmod{G/H}.$$

将等式两边的 T 用 T^2 替换得

$$(\overline{T}^{(2)})^2 \equiv -\overline{T}^{(4)} + 2n + 2 = -\overline{T} + 2n + 2 \pmod{G/H}.$$

第二个等号成立是因为 $\overline{T}^{(4)} = \overline{T}$.

联立上面两式消元得

$$\overline{T}^4 - 4(n+1)\overline{T}^2 + \overline{T} + 4n^2 + 6n + 2 \equiv 0 \pmod{G/H}.$$

经计算，

$$\overline{T}^4 - 4(n+1)\overline{T}^2 + \overline{T} + 4n^2 + 6n + 2 = (\overline{T}^2 - \overline{T} - 2n - 1)(\overline{T}^2 + \overline{T} - 2n - 2). \quad (3.4)$$

因为剩余类环 $\mathbb{Z}[G/H]/(G/H)$ 中没有零因子 (因为该商环同构于 $\mathbb{Z}[X]/(\sum_{i=0}^{4} X^i)$). 所以(3.4)式中的两个因子必有一个模 G/H 同余 0. 若 $\overline{T}^2 + \overline{T} - 2n - 2 \equiv 0 \pmod{G/H}$，则通过简单的计数可得

$$\overline{T}^2 = 2mG/H - \overline{T} + 2n + 2.$$

联立条件 (c') 得 $\overline{T} = \overline{T}^{(2)}$. 因为 2 是模 5 的本原元，则一定存在 $a, b \in \mathbb{Z}$ 使得 $\overline{T} = a + bG/H$. 由引理3.2，可得 $8n+9$ 是 $\mathbb{Z}$ 中的一个平方元，这与假设条件相矛盾!

若 $\overline{T}^2-\overline{T}-2n-1\equiv 0 \pmod{G/H}$，令 $\chi\in\widehat{G/H}$，则 $\chi(\overline{T})\in\mathbb{Z}[\zeta_5]$ 满足

$$\chi(\overline{T})^2-\chi(\overline{T})-2n-1=0. \tag{3.5}$$

这意味着 $8n+5$ 是 $\mathbb{Z}[\zeta_5]$ 中的一个平方元. 通过观察 $8n+5 \pmod 8$，不难发现 $8n+5$ 有一个平方因子当且仅当 $8n+5=tk^2, t\equiv 5 \pmod 8$. 由条件 $8n+5\neq 5k^2$ 得，$t\neq 5$. 根据引理2.2，包含 $\mathbb{K}=\mathbb{Q}(\sqrt{8n+5})$ 的最小分圆域为 $\mathbb{Q}(\zeta_t)$，而不是 $Q(\zeta_5)$. 因此，不存在 $\chi(\overline{T})$ 使得 (3.5) 成立，即不存在满足条件 (b') 和 (c') 的 $\overline{T}\in\mathbb{Z}[C_5]$. □

利用引理2.3可以处理 $|G/H|$ 更大的情况，下面证明当 $|G/H|=7,11,13,17$ 和 19 时的结论.

定理 3.5: 假设 $G/H\cong C_7$，$8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元. 则不存在满足条件 (b') 和 (c') 的 $\overline{T}\in\mathbb{Z}[C_7]$.

证明： 同样利用反证法，假设存在满足条件 (b') 和 (c') 的 $\overline{T}\in\mathbb{Z}[C_7]$，这意味着对 $i=0,1,2$, 有

$$f_i=\overline{T}^{(2^i)}\overline{T}^{(2^i)}+\overline{T}^{(2^{i+1})}-2n-2\equiv 0 \pmod{G/H}. \tag{3.6}$$

将上述三个等式看作是以 $\overline{T}^{(2^i)}$ 为变量的多项式，由此可以联立 f_0 和 f_1，从而得到一个没有 $\overline{T}^{(2^1)}$ 的新多项式 h_1. 同样可以利用 h_1 和 f_2 通过消去 $\overline{T}^{(2^2)}$ 得到一个新多项式 h_2. 注意到 $\overline{T}^{(2^3)}=\overline{T}$，因此 h_2 只包含一个变量 $\overline{T}$. 这些都可以通过 MAGMA [35] 实现. 而且，$h_2 \pmod{G/H}$ 可以被因式分解成 2 个不可约因式

$$h_2\equiv(\overline{T}^2+\overline{T}-2n-2)l \pmod{G/H}.$$

其中

$$\begin{aligned} l=&\overline{T}^6-\overline{T}^5-(6n+5)\overline{T}^4+(4n+3)\overline{T}^3+(12n^2+18n+7)\overline{T}^2\\ &-(2n+1)^2\overline{T}-8n^3-16n^2-10n-1. \end{aligned}$$

因为 h_2 是由 $f_i(i=0,1,2)$ 得到的，所以 $h_2\equiv 0 \pmod{G/H}$. 由定理3.4的证明可知，商环 $\mathbb{Z}[G/H]/(G/H)$ 中没有零因子，该剩余类环同构于 $\mathbb{Z}[X]/(\sum_{i=0}^{6}X^i)$. 对于 h_2 的第一个不可约因式，因为 2 不是模 7 的本原元，定理3.4中证明 $\overline{T}^2+\overline{T}-2n-2 \pmod{G/H}$ 不同余 0 的方法不适用. 但是可仿照定理3.4中处理 $\overline{T}^2-\overline{T}-2n-1$ 的方法证明该因式不同余 0.

设 $\chi \in \widehat{G/H}$ 是一个非平凡特征. 则 $\chi(\overline{T}) \in \mathbb{Z}[\zeta_7]$ 满足

$$\chi(\overline{T})^2 + \chi(\overline{T}) - 2n - 2 = 0. \tag{3.7}$$

这意味着 $8n+9$ 在 $\mathbb{Z}[\zeta_7]$ 中是个平方元. 因为 $8n+9$ 不是 $\mathbb{Z}$ 中的平方元，假设 $8n+9$ 有一个平方因子，则 $8n+9 = tk^2$，其中 t 是个大于 1 的非平方元. 则 $t \equiv 1 \pmod 8$. 由此可得 $t > 7$. 根据引理2.2得，包含 $\mathbb{Q}(\sqrt{8n+9})$ 的最小分圆域为 $\mathbb{Q}(\zeta_t)$，而不是 $Q(\zeta_7)$，因此不存在满足 (3.7) 的 $\chi(\overline{T})$. 所以 h_2 的第一个不可约因子模 G/H 不同余 0，于是 $l \equiv 0 \pmod{G/H}$.

l 是一个以 $\overline{T}$ 为变量的 6 次多项式. 取一个素数 p 然后对 $\chi(l) = 0$ 进行模 p 处理. 设 p 是模 $v = 7$ 的本原元，即 $p = 3, 5 \pmod v$. 由引理2.3得，(p) 是 $\mathbb{Z}[\zeta_v]$ 中的一个素理想. 用 X 代替 $\chi(l) \equiv 0 \pmod p$ 中的 $\chi(\overline{T}) \pmod p$ 且将其系数都模 p，则得到 $\mathbb{F}_p[X]$ 中的如下多项式

$$\begin{aligned}\bar{l}(X) = {} & X^6 - X^5 - (6n+5)X^4 + (4n+3)X^3 + (12n^2+18n+7)X^2 \\ & - (2n+1)^2 X - 8n^3 - 16n^2 - 10n - 1.\end{aligned}$$

假设 τ_1 是该多项式的根，即 $\bar{l}(\tau_1) = 0$ 且 $\tau_1 \equiv \chi(\overline{T}) \pmod p$.

假设 τ_1 的极小多项式的次数为 s，则 τ_1 的所有共轭元为：$\tau_1^p, \tau_1^{p^2}, \ldots, \tau_1^{p^{s-1}}$. 因为 p 是模 $v = 7$ 本原元，所以 $p^{\frac{v-1}{2}} \equiv -1 \pmod v$. 又 $\chi(\overline{T}^{(p)}) \equiv \chi(\overline{T})^p \pmod p$ 且 $\overline{T}^{(-1)} = \overline{T}$，因此

$$\chi(\overline{T}) = \chi(\overline{T}^{(-1)}) = \chi\left(\overline{T}^{(p^{\frac{v-1}{2}})}\right) \equiv \chi(\overline{T})^{p^{\frac{v-1}{2}}} \pmod p.$$

所以 $\tau_1^{p^3} = \tau_1^{p^{\frac{v-1}{2}}} = \tau_1$，这意味着 $s = 1$ 或 $s = 3$. 所以 $\bar{l}$ 的所有根 $\tau_1, \tau_1^p, \ldots, \tau_1^{p^{s-1}}$ 都属于 $\mathbb{F}_{p^3}$.

因为 τ_1 是 $\bar{l}$ 的一个根且 $\chi(\overline{T}^{(p)}) \equiv \chi(\overline{T})^p \pmod p$. 因此

$$\tau_i :\equiv \chi(\overline{T}^{(2^i)}) \equiv \begin{cases} \tau_1^{p^{3-i}} \pmod p, & 若 p \equiv 3 \pmod 7; \\ \tau_1^{p^i} \pmod p, & 若 p \equiv 5 \pmod 7. \end{cases} \tag{3.8}$$

注意 τ_1 一定要满足的必要条件. 首先，由 (3.6) 得对 $i = 0, 1, 2,$

$$\tau_i^2 + \tau_{i+1} - 2n - 2 \equiv 0 \pmod p. \tag{3.9}$$

其次，设 $\overline{T}=\sum_{\bar{g}\in G/H}a_{\bar{g}}\bar{g}$，可通过公式 (2.2) 计算 $a_{\bar{g}}$. 令 β 是 $\mathbb{F}_{p^{v-1}}$ 中一个阶数为 $v=7$ 的元. 对 $\bar{g}\in G/H$，假设 $\chi(\bar{g})\equiv\beta\pmod{p}$，则

$$\begin{aligned} a_{\bar{g}} &= \frac{1}{7}\left((2n+1)+\sum_{i=1}^{6}\chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right) \\ &= \frac{1}{7}\left((2n+1)+\sum_{i=1}^{3}\chi(\overline{T}^{(i)})\left(\chi(\bar{g}^{i})+\chi(\bar{g}^{-i})\right)\right) \\ &\equiv \frac{1}{7}\left((2n+1)+\sum_{j=0}^{2}\tau_1^{p^j}(\beta^{p^j}+\beta^{-p^j})\right) \pmod{p}. \end{aligned} \tag{3.10}$$

显然 $a_{\bar{g}}\pmod{p}$ 必须是 $\mathbb{F}_p$ 中的某个元. 而且，因为 $|\overline{T}|=|T|=2n+1$，因此所有的 $a_{\bar{g}}$ 也要满足

$$\sum_{\bar{g}\in G/H}a_{\bar{g}}\equiv 2n+1 \pmod{p}. \tag{3.11}$$

基于上述提到的所有必要条件，可以给出一个排除满足条件 (b') 和 (c') 的 $\overline{T}$ 的存在性的方法. 首先选定一个模 v 本原的素数 p，然后根据 n 模 p 的值，分成 p 种不同的情况. 为了检验这些必要条件，需要求出 $\bar{l}$ 在 $\mathbb{F}_{p^3}=\mathbb{F}_{p^{\frac{v-1}{2}}}$ 中的所有根，记 $\Omega=\{\bar{l}(x)=0:x\in\mathbb{F}_{p^3}\}$，且对 Ω 中的每个元素 τ_1，按如下 4 步计算：

(i) 将 τ_1 代入 (3.8) 求出 τ_i;

(ii) 检查 (3.9) 是否对每个 i 都成立;

(iii) 由 (3.10) 计算出 $a_{\bar{g}}$;

(iv) 检查是否 $a_{\bar{g}}$ 都满足 $a_{\bar{g}}\pmod{p}\in\mathbb{F}_p$ 和 (3.11).

利用 MAGMA 可以计算出当 $p=521$ 时，对 n 模 p 的每一个可能的值，都能找到至少一个必要条件不满足，因此，不存在满足条件 (b') 和 (c') 的 $\overline{T}$. □

后续的几种情况和 $G/H\cong C_7$ 的情况的方法类似，为了避免证明过程的重复叙述，下面对定理3.5的证明过程进行简单的总结，步骤如下：

步骤 1： 按照定理3.5的方法得到类似(3.6)的一系列 f_i，然后通过消元得到只包含一个变量 $\overline{T}$ 的 h，接着对 h 进行因式分解.

步骤 2： 对 h 的每个次数为 2 的不可约因式 q，通过添加的条件证明 q 模 G/H 不同余 0.

步骤 3： 对 h 的每个次数严格大于 2 的不可约因式 l，将 G/H 的特征 χ 作用到 l 上，得到一个单变量多项式 $\chi(l)$.

步骤 4： 选取一个模 v 本原的素数 p，用 X 代替 $\chi(l) \pmod p$ 中的 $\chi(\overline{T}) \pmod p$，得到 $\bar{l} \in \mathbb{F}_p[X]$.

步骤 5： 求出 $\Omega = \{\bar{l}(x) = 0 : x \in \mathbb{F}_{p^3}\}$，对 Ω 中的每个元素 τ_1，按照定理3.5中的步骤 (i) 至 (iv) 检验所有的必要条件.

下面按照这 5 个步骤处理余下四种情况.

定理 3.6: 假设 $G/H \cong C_{11}$ 且 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，则不存在满足条件 (b') 和 (c') 的子集 $\overline{T} \in \mathbb{Z}[C_{11}]$.

证明： 按照定理3.5的步骤证明该定理.

步骤 1：根据计算可以得到 $f_i(i = 0, 1, ..., 4)$，消元得到 h 并对其进行因式分解得到 $h \equiv (\overline{T}^2 + \overline{T} - 2n - 2)l \equiv 0 \pmod{G/H}$，其中 l 是 30 次的多项式.

步骤 2：根据引理3.2，在 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元的前提下，容易证明 q 模 G/H 不同余 0. 选取模 $v = 11$ 本原的素数 p，即 $p \equiv 2, 6, 7, 8 \pmod v$，经过步骤 3 和 4 后得到 $\bar{l} \in \mathbb{F}_p[X]$.

最后，根据步骤 5，求出 $\Omega = \{\bar{l}(x) = 0 : x \in \mathbb{F}_{p^3}\}$. 对 Ω 中的每个元素 τ_1，按照定理3.5中的步骤 (i) 至 (iv) 检验所有的必要条件. 需要特别指出的是由 τ_1 计算 $\chi(\overline{T}^{(2^i)})$ 的过程与定理3.5并不完全相同：

$$\tau_i :\equiv \chi(\overline{T}^{(2^i)}) \equiv \begin{cases} \tau_1^{p^i} \pmod p, & p \equiv 2 \pmod{11}; \\ \tau_1^{p^{2i}} \pmod p, & p \equiv 8 \pmod{11}; \\ \tau_1^{p^{3i}} \pmod p, & p \equiv 7 \pmod{11}; \\ \tau_1^{p^{5-i}} \pmod p, & p \equiv 6 \pmod{11}. \end{cases}$$

对任意 $\bar{g} \in G/H$，假设 $\chi(\bar{g}) \equiv \beta \pmod p$，则

$$\begin{aligned} a_{\bar{g}} &= \frac{1}{11}\left((2n+1) + \sum_{i=1}^{10} \chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right) \\ &= \frac{1}{11}\left((2n+1) + \sum_{i=1}^{5} \chi(\overline{T}^{(i)})(\chi(\bar{g}^{i}) + \chi(\bar{g}^{-i}))\right) \\ &\equiv \frac{1}{11}\left((2n+1) + \sum_{j=0}^{4} \tau_1^{p^j}(\beta^{p^j} + \beta^{-p^j})\right) \pmod p. \end{aligned}$$

利用 MAGMA 可以计算出当取 $p = 173$ 时，对 n 模 p 的每一个可能的值，都能找到至少一个必要条件不满足，因此，不存在满足条件 (b') 和 (c') 的 $\overline{T}$. □

定理 3.7: 假设 $G/H \cong C_{13}$ 且 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，对所有的 $k \in \mathbb{Z}$，$8n+5 \neq 13k^2$. 则不存在满足条件 (b') 和 (c') 的子集 $\overline{T} \in \mathbb{Z}[C_{13}]$.

证明： 按照定理3.5的步骤证明该定理.

步骤 1：计算得到 $f_i (i = 0, 1, ..., 5)$，消元得到 h 并对其进行因式分解得到

$$h \equiv (\overline{T}^2 - \overline{T} - 2n - 1)(\overline{T}^2 + \overline{T} - 2n - 2) l_1 l_2 \pmod{G/H}.$$

其中

$$\begin{aligned} l_1 = {} & \overline{T}^6 - \overline{T}^5 - (6n+5)\overline{T}^4 + (4n+3)\overline{T}^3 + (12n^2 + 18n + 7)\overline{T}^2 \\ & - (2n+1)^2 \overline{T} - 8n^3 - 16n^2 - 10n - 1. \end{aligned}$$

l_2 是 54 次多项式.

步骤 2：根据引理3.2，在 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元的前提下，容易证明 $q_1 := \overline{T}^2 + \overline{T} - 2n - 2$ 模 G/H 不同余 0. 对 $q_2 := \overline{T}^2 - \overline{T} - 2n - 1$，根据定理3.4中的方法，在对所有的 $k \in \mathbb{Z}$，$8n+5 \neq 13k^2$ 的条件下可以证明，q_2 模 G/H 不同余 0. 选取模 $v = 13$ 本原的素数 p，即 $p \equiv 2, 6, 7, 11 \pmod{v}$，记 $l = l_1 l_2$，经过步骤 3 和 4 得到 $\bar{l} \in \mathbb{F}_p[X]$.

最后，根据步骤 5，求出 $\Omega = \{\bar{l}(x) = 0 : x \in \mathbb{F}_{p^3}\}$. 对 Ω 中的每个元素 τ_1，按照定理3.5中的步骤 (i) 至 (iv) 检验所有的必要条件. 由 τ_1 计算 $\chi(\overline{T}^{(2^i)})$ 的过程与定理3.5也不同，具体公式如下：

$$\tau_i :\equiv \chi(\overline{T}^{(2^i)}) \equiv \begin{cases} \tau_1^{p^i} \pmod{p}, & p \equiv 2, 11 \pmod{13}; \\ \tau_1^{p^{6-i}} \pmod{p}, & p \equiv 6, 7 \pmod{13}. \end{cases}$$

对任意的 $\bar{g} \in G/H$，假设 $\chi(\bar{g}) \equiv \beta \pmod{p}$，则

$$\begin{aligned} a_{\bar{g}} = & \frac{1}{13}\left((2n+1) + \sum_{i=1}^{12} \chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right) \\ = & \frac{1}{13}\left((2n+1) + \sum_{i=1}^{6} \chi(\overline{T}^{(i)})(\chi(\bar{g}^{i}) + \chi(\bar{g}^{-i}))\right) \\ \equiv & \frac{1}{13}\left((2n+1) + \sum_{j=0}^{5} \tau_1^{p^j}(\beta^{p^j} + \beta^{-p^j})\right) \pmod{p}. \end{aligned}$$

取 $p=227$，对 n 模 p 的每一个可能的值，利用 MAGMA 程序都能找到至少一个必要条件不满足，因此，不存在满足条件 (b') 和 (c') 的 $\overline{T}$. □

定理 3.8: 假设 $G/H \cong C_{17}$ 且 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，对所有 $k \in \mathbb{Z}$，$8n+9 \neq 17k^2$. 则不存在满足条件 (b') 和 (c') 的子集 $\overline{T} \in \mathbb{Z}[C_{17}]$.

证明：按照定理3.5的步骤证明：

步骤 1：计算得到 $f_i(i=0,1,2,3)$，消元得到 h 并对其进行因式分解得到

$$h \equiv (\overline{T}^2+\overline{T}-2n-2)(\overline{T}^2-\overline{T}-2n-1)l \pmod{G/H}.$$

其中 l 是 12 次多项式.

步骤 2：根据定理3.5，在 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元和对所有的 $k \in \mathbb{Z}$，$8n+9 \neq 17k^2$ 的前提下，容易证明 $q_1 := \overline{T}^2+\overline{T}-2n-2$ 模 G/H 不同余 0. 对 $q_2 := \overline{T}^2-\overline{T}-2n-1$，按照定理3.4的证明过程中的方法可得，$q_2$ 模 G/H 不同余 0. 需要特别指出的是这里不需要增加条件 $8n+5 \neq 17k^2$，因为 $17 \not\equiv 5 \pmod 8$，这意味着包含 $\mathbb{Q}(\sqrt{8n+5})$ 不可能是 $\mathbb{Q}(\zeta_{17})$. 取模 $v=17$ 本原的素数 p，即 $p \equiv 3,5,6,7,10,11,12,14 \pmod v$，经过步骤 3 和 4 后得到 $\bar{l} \in \mathbb{F}_p[X]$.

最后，根据步骤 5，求出 $\Omega = \{\bar{l}(x)=0 : x \in \mathbb{F}_{p^3}\}$. 对 Ω 中的每个元素 τ_1，按照定理3.5中的步骤 (i) 至 (iv) 检验所有的必要条件. 其中 $\chi(\overline{T}^{(2^i)})$ 的计算公式如下：

$$\tau_i :\equiv \chi(\overline{T}^{(2^i)}) \equiv \begin{cases} \tau_1^{p^{8-2i}} \pmod p, & p \equiv 3,5,12,14 \pmod{17}; \\ \tau_1^{p^{2i}} \pmod p, & p \equiv 6,7,10,11 \pmod{17}. \end{cases}$$

对任意的 $\bar{g} \in G/H$，假设 $\chi(\bar{g}) \equiv \beta \pmod p$,

$$\begin{aligned} a_{\bar{g}} &= \frac{1}{17}\left((2n+1)+\sum_{i=1}^{16}\chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right) \\ &= \frac{1}{17}\left((2n+1)+\sum_{i=1}^{8}\chi(\overline{T}^{(i)})(\chi(\bar{g}^{i})+\chi(\bar{g}^{-i}))\right) \\ &\equiv \frac{1}{17}\left((2n+1)+\sum_{j=0}^{7}\tau_1^{p^j}(\beta^{p^j}+\beta^{-p^j})\right) \pmod p. \end{aligned}$$

利用 MAGMA 计算出当取 $p=37$ 时，对 n 模 p 的每一个可能的值，都能找到至少一个必要条件不满足，因此，不存在满足条件 (b') 和 (c') 的 $\overline{T}$. □

定理 3.9: 假设 $G/H \cong C_{19}$ 且 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，则不存在满足条件 (b') 和 (c') 的子集 $\overline{T} \in \mathbb{Z}[C_{19}]$.

证明：按照定理3.5步骤得：

步骤 1：计算得到 $f_i(i=0,1,\ldots,8)$，消元得到 h，对其进行因式分解得

$$h \equiv (\overline{T}^2+\overline{T}-2n-2)l_1l_2 \pmod{G/H}.$$

其中

$$\begin{aligned} l_1 = {} & \overline{T}^6-\overline{T}^5-(6n+5)\overline{T}^4+(4n+3)\overline{T}^3+(12n^2+18n+7)\overline{T}^2 \\ & -(2n+1)^2\overline{T}-8n^3-16n^2-10n-1. \end{aligned}$$

l_2 是 504 次多项式.

步骤 2：根据引理3.2，因为 $8n+9$ 是 $\mathbb{Z}$ 中的非平方元，容易证明 $q_1 := \overline{T}^2+\overline{T}-2n-2$ 模 G/H 不同余 0. 接着选取一个模 $v=19$ 本原的素数 p，即 $p \equiv 2,3,10,13,14,15 \pmod{v}$，记 $l=l_1l_2$，经过步骤 3 和 4 后得到 $\bar{l} \in \mathbb{F}_p[X]$.

最后，根据步骤 5，求出 $\Omega=\{\bar{l}(x)=0 : x \in \mathbb{F}_{p^3}\}$. 对 Ω 中的每个元素 τ_1，按照定理3.5中的步骤 (i) 至 (iv) 检验所有的必要条件. 其中 $\chi(\overline{T}^{(2^i)})$ 的计算公式如下：

$$\tau_i :\equiv \chi(\overline{T}^{(2^i)}) \equiv \begin{cases} \tau_1^{p^i} \pmod{p}, & p \equiv 2 \pmod{19}; \\ \tau_1^{p^{2i}} \pmod{p}, & p \equiv 13 \pmod{19}; \\ \tau_1^{p^{4i}} \pmod{p}, & p \equiv 14 \pmod{19}; \\ \tau_1^{p^{5i}} \pmod{p}, & p \equiv 15 \pmod{19}; \\ \tau_1^{p^{7i}} \pmod{p}, & p \equiv 3 \pmod{19}; \\ \tau_1^{p^{9-i}} \pmod{p}, & p \equiv 10 \pmod{19}. \end{cases}$$

对任意的 $\bar{g} \in G/H$，假设 $\chi(\bar{g}) \equiv \beta \pmod{p}$，则

$$\begin{aligned} a_{\bar{g}} &= \frac{1}{19}\left((2n+1)+\sum_{i=1}^{18}\chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right) \\ &= \frac{1}{19}\left((2n+1)+\sum_{i=1}^{9}\chi(\overline{T}^{(i)})(\chi(\bar{g}^{i})+\chi(\bar{g}^{-i}))\right) \\ &\equiv \frac{1}{19}\left((2n+1)+\sum_{j=0}^{8}\tau_1^{p^j}(\beta^{p^j}+\beta^{-p^j})\right) \pmod{p}. \end{aligned}$$

利用 MAGMA 计算出当取 $p=241$ 时，对 n 模 p 的每一个可能的值，都能找到至少一个必要条件不满足，因此，不存在满足条件 (b') 和 (c') 的 $\overline{T}$. □

在上述所有定理的证明中，需要多次在 $\overline{T}^2 \equiv -\overline{T}^{(2)}+2n+2 \pmod{G/H}$ 中将 $\overline{T}$ 替换为 $\overline{T}^{(2)}$，这只有当 2 是 $C_v \cong G/H$ 的生成元时替换后得到的新的等式才成立，因此该方法不能处理 G/H 的阶是偶数的情况. 假设 $|G/H|=\prod_{i=1}^{k}p_i$，其中

$p_i(i=1,\cdots,k)$ 全是奇素数，若能证明阶数为 $p_i(i\in\{1,\ldots,k\})$ 的群 G/H' 中 $\overline{T}$ 的不存在性，则也说明了 G/H 中不存在符合的 $\overline{T}$. 因此，只需要考虑 $|G/H|$ 是奇素数的情况.

定理3.9证明了 $|G/H|=19$ 时的不存在性结果. 下一个整除 $|G|$ 的奇素数是 23，然而由于运算量太大，计算机无法因式分解单变元多项式 h. 因此处理不了该情况以及 $|G/H|$ 更大的情况.

综合命题3.1和定理3.4, 3.5, 3.6, 3.7, 3.8, 3.9，可得到如下结果.

推论 3.10: 设 G 是一个 $2n^2+2n$ 阶的交换群. 若 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，以及下列三个条件满足其中之一：

1) $3,7,11$ 或 $19\mid n(n+1)$;

2) 对 $v=5$或13，$v\mid n(n+1)$ 且 $8n+5\notin\{vk^2:k\in\mathbb{Z}\}$;

3) $17\mid n(n+1)$ 且 $8n+9\notin\{17k^2:k\in\mathbb{Z}\}$.

则不存在满足定理3.3中的三个条件的 $T\subseteq G$，因此不存在以 G 为顶点集的第一类图.

表 3.1　推论3.10排除的 n 的数目，其中 $v=|G/H|$

v	N	10	10^2	10^3	10^4	10^5
3	$n\le N$ 时被命题3.1排除的数目	3	54	623	6527	66221
5	$n\le N$ 时被定理3.4排除的数目	2	27	349	3830	39449
7	$n\le N$ 时被定理3.5排除的数目	2	22	261	2777	28317
11	$n\le N$ 时被定理3.6排除的数目	1	14	166	1770	18021
13	$n\le N$ 时被定理3.7排除的数目	0	11	141	1498	15248
17	$n\le N$ 时被定理3.8排除的数目	0	10	108	1144	11660
19	$n\le N$ 时被定理3.9排除的数目	0	10	96	1024	10434
合计	$n\le N$ 时被推论3.10排除的数目	6	81	876	9084	91741

由于第一类图在满足顶点集只包含一个二阶元的情况下才存在与之对应的几乎完美线性李码，所以当 n 满足推论3.10中的条件时 $\mathbb{Z}^n$ 上也不存在相应的几乎完美线性李码.

在表格3.1中，列出了能够被推论3.10排除的 n 的数目. 在 3 到 100 之间只有 17 种情况不能被推论3.10排除，分别为 5, 9, 14, 20, 27, 31, 35, 44, 46, 54, 58, 61, 65, 73, 77, 82, 90. 通过使用 MAGMA 穷搜，可以排除 $n = 5$ 的情况.

从表格3.1中可以看出，$n \leq 10^5$ 中超过 90% 的 n 可以被推论3.10排除. 因为目前只找到了 $n = 1, 2$ 时满足条件 (a)，(b) 和 (c) 的 $T \subseteq G$. 因此可以合理猜想：对于阶为 $2n^2 + 2n$ 的交换群 G，除了 $n = 1$ 和 2 外，不存在以 G 为顶点集的第一类图.

本章内容已撰写学术论文，于 2021 年 7 月投稿至 SCI 期刊 Journal of Algebraic Combinatorics.

第四章　两种特殊交换凯莱图的存在性问题

上一章研究的交换凯莱图阶 $2n^2+2n$ 比交换凯莱摩尔界 $M_C(2n,2)$ 小 1；本章第一节研究阶为 $2n^2+2n+2$ 的第二类图, 即它的阶比交换凯莱摩尔界 $M_C(2n,2)$ 大 1，同样可视为在 [2] 研究结果基础上的推广. 该类图的直径为 3，其生成集 S 还需满足 $|\tilde{S}^2| = M_C(2n,2)(\tilde{S} = S \cup \{e\})$.

第二节研究第三类图，证明其与汉明距离下的二元完美线性码的等价性，并根据已有的二元完美线性码分类结果对其进行完全分类.

关于第二类图，分别运用代数数论、有限域、群特征标和对称多项式等数学工具证明第二类图不存在性问题的如下两个结论：

一、 设 G 是阶为 $2n^2+2n+2$ 的交换群，$8n-7$ 不是 $\mathbb{Z}$ 上的平方元，若下列三个条件满足其中之一：

1) 3，7，19 或 $31 \mid n^2+n+1$；

2) $13 \mid n^2+n+1$ 且 $8n-11 \notin \{13k^2 : k \in \mathbb{Z}\}$，

则不存在以 G 为顶点集的第二类图.

二、 假设 $2n^2+2n+2 = mv(n>1)$，v 是素数且 $v > 2n+1$. 设 G 是一个阶为 $2n^2+2n+2$ 的加法交换群. 设 a 是满足 $v \mid 4^a+4n+2$ 的最小正整数，b 是满足 $v \mid 4^b-1$ 的最小正整数 (若不存在 a 使得 $v \mid 4^a+4n+2$，则令 $a=\infty$). 若对 $\forall l \in \{0,1,\cdots,\lfloor\frac{m-1}{4}\rfloor\}$，$a(x+1)+by = n-l$ 都不存在非负整数解，则不存在以 G 为顶点集的第二类图.

根据上述两个结论，可以排除 10^5 以内 92524 个 n 取值情况下的第二类图的存在性.

关于第三类图，根据其与汉明距离下的二元完美线性码的等价性，及二元完美线性码的存在性情况，证明如下结论：设 $G = (\mathbb{F}_2^m, +)$，则以 G 为顶点集的第三类图只存在如下几类：

1) $S = \{s : s \in G \setminus \{0,0,\cdots,0\}\}$，直径 $k=1$；

2) $2 \mid m$ 且 $S = \{e_1, e_2, \cdots, e_m, l_m\}$，直径 $k = \frac{m}{2}$；

其中 $e_i(i=1,2,\cdots,m)$ 为标准基, l_m 为全 1 向量.

3) 当 $m=11$ 时，取 S 是由二元格雷码的校验矩阵全体列向量构成的集合. 此时，$|S|=23$，$\Gamma(G,S)$ 的直径 $k=3$.

4.1 第二类图的存在性问题

本节先介绍第二类图已有的实例，再分别利用代数数论和有限域方法、对称多项式方法研究该问题. 对于 $n=1,2$ 的情况，容易找到如下例子.

例 4.1: 记生成元为 g 的 m 阶循环群为 C_m.

1) 当 $n=1$ 时，令 $G=C_6$，$S=\{g^{\pm 1}\}$. 则交换凯莱图 $\Gamma(G,S)$ 是一个 6 循环图. $\Gamma(G,S)$ 对应的几乎完美线性李码如图4.1所示.

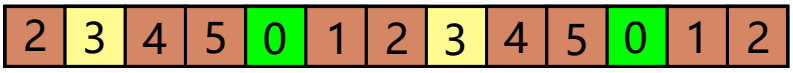

图 4.1 $G=C_6$，$S=\{\pm 1\}$ 时 $\Gamma(G,S)$ 对应的几乎完美线性李码

2) 当 $n=2$ 时，令 $G=C_{14}$，$S=\{g^{\pm 1},g^{\pm 4}\}$. 则交换凯莱图 $\Gamma(G,S)$ 如图4.2. 对应的几乎完美线性李码如图4.3所示.

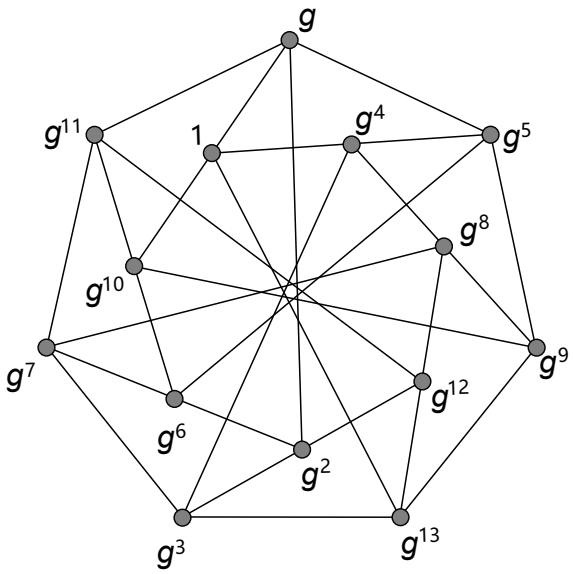

图 4.2 顶点集为 C_{14}，由 $\{g^{\pm 1},g^{\pm 4}\}$ 生成的交换凯莱图

对该类交换凯莱图 $\Gamma(G,S)$，可以证明 G 中只有一个二阶元.

引理 4.1: 设 G 是一个以 e 为单位元的 $2n^2+2n+2$ 阶群 (为了方便证明叙述，令其为乘法群). $\Gamma(G,S)$ 是一个度为 $2n$，直径为 3 的交换凯莱图，且满足 $|\tilde{S}^2|=M_C(2n,2)(\tilde{S}=S\cup\{e\})$，则 G 中只有一个二阶元 f 且 $f\notin\tilde{S}^2$.

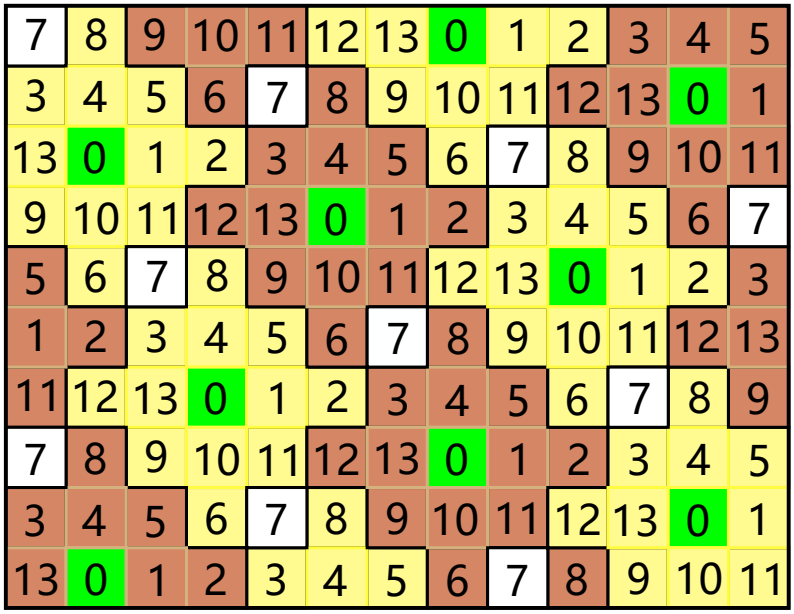

图 4.3　$G = C_{14}$，$S = \{g^{\pm 1}, g^{\pm 4}\}$ 时 $\Gamma(G, S)$ 对应的几乎完美线性李码

证明：因为 $2 \mid |G|$ 且 $4 \nmid |G|$，则 G 中只有一个二阶元 f. 因为 $|S|$ 是偶数且 S 是逆运算封闭的，所以 $f \notin S$. 另外，若 $f \in \tilde{S}^2$，则存在 $a, b \in S$ 使得 $f = ab = a^{-1}b^{-1}$，这意味着 $|\tilde{S}^2| < 2n^2 + 2n + 1$. 然而，$|\tilde{S}^2| = M_C(2n, 2) = 2n^2 + 2n + 1$，矛盾！因此 $f \notin \tilde{S}^2$. □

第二章提到了第二类图与几乎完美线性李码存在性的等价关系，上述例子对此也有体现，下面通过证明如下定理详细论证这一结论.

定理 4.1: $\mathrm{APLL}^-(n, r)$ 存在当且仅当存在一个交换群 G 和一个同态：$\phi : \mathbb{Z}^n \mapsto G$，且该同态在 $S(n, r)$ 上是单射，且 $G \setminus \phi(S(n, r))$ 只有一个元素.

证明：首先证明必要性.

设 C 是 $\mathrm{APLL}^-(n, r)$，w 是 $\mathbb{Z}^n$ 中不被格铺砌 $\dot{\bigcup}_{c \in C}(S(n, r) + c)$ 覆盖的任意一个元素. 根据 $\mathrm{APLL}^-(n, r)$ 的定义可知，C 是 $\mathbb{Z}^n$ 的子群，且

$$\mathbb{Z}^n = \left(\dot{\bigcup}_{c \in C}(S(n, r) + c)\right) \dot{\bigcup} (w + C). \tag{4.1}$$

考虑商群 $G = \mathbb{Z}^n / C$. 取 ϕ 为 $\mathbb{Z}^n$ 到 G 的典型同态. 若存在 $x, y \in S(n, r)$，使得 $\phi(x) = \phi(y)$，则 $z = x - y \in C$. 因为 $y \in S(n, r)$，则 $x \in S(n, r) + z$. 这意味着 x 同时被 $S(n, r) + z$ 和 $S(n, r)$ 两个李球覆盖. 由(4.1)式得 $z = 0$，即 $x = y$. 因此 ϕ 是单射且 $\phi(w)$ 是 G 中唯一不属于 $\phi(S(n, r))$ 中的元.

对于充分性，只需定义 $C = ker(\phi)$，容易验证 C 是 $\mathrm{APLL}^-(n, r)$. □

由于生成集 S 中不存在二阶元，则可令 $S=\{\pm\phi(e_i), i=1,\cdots,n\}$，$G$ 如定理2.4证明过程中的(2.1)式所示，同样类似定理2.4的证明，由定理4.1可得如下推论.

推论 4.2: 设 G 为交换群，$|G|=\sum_{i=0}^{\min\{n,r\}}2^i\binom{n}{i}\binom{r}{i}+1$. S 为 G 中满足 $|S|=2n$，$e\notin S$ 和 $|\tilde{S}^r|=M_C(2n,r)$ 的子集，则交换凯莱图 $\Gamma(G,S)$ 存在等价于 $\mathrm{APLL}^-(n,r)$ 存在.

4.1.1 代数数论和有限域方法

本节首先利用群环语言推导第二类图存在的另一个充要条件，然后根据这一条件推导出第二类图不存在的一系列必要条件.

定理 4.3: 设 G 是一个以 e 为单位元的 $2n^2+2n+2$ 阶乘法交换群，G 中存在满足 $|S|=2n$，$e\notin S$ 且 $|\tilde{S}^2|=M_C(2n,2)$ 的逆运算封闭子集 S 当且仅当存在 T 满足

(a) $e\in T$,

(b) $T=T^{(-1)}$,

(c) $T^2=2G-T^{(2)}+2ne-2f$.

证明: 必要性：假设 $S=\{a_1,\cdots,a_n\}\cup\{a_1^{-1},\cdots,a_n^{-1}\}$. 令 $T=S\cup\{e\}$，群环语言的表示为：$T=e+\sum_{i=1}^n(a_i+a_i^{-1})$. 条件 (a) 和 (b) 显然满足.

因为 $|T^2|=M_C(2n,2)$，所以 G 可用群环语言如下表示.

$$G=e+f+\sum_{i=1}^n(a_i+a_i^{-1}+a_i^2+a_i^{-2})+\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1}).$$

经计算，

$$\begin{aligned}T^2=&\left(e+\sum_{i=1}^n(a_i+a_i^{-1})\right)^2\\=&e+2\sum_{i=1}^n(a_i+a_i^{-1})+\left(\sum_{i=1}^n(a_i+a_i^{-1})\right)^2\\=&e+2\sum_{i=1}^n(a_i+a_i^{-1})+\sum_{i=1}^n(a_i^2+a_i^{-2})+2\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1})+2ne\\=&2e+2\sum_{i=1}^n(a_i+a_i^{-1})+2\sum_{i=1}^n(a_i^2+a_i^{-2})+2\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1})\end{aligned}$$

$$
\begin{aligned}
&+(2n-1)e-\sum_{i=1}^{n}(a_i^2+a_i^{-2})\\
=&2(G-f)+2ne-T^{(2)}\\
=&2G-T^{(2)}+2ne-2f.
\end{aligned}
$$

因此，(c) 也满足.

充分性：设 $T=e+\sum_{i=1}^{n}(a_i+a_i^{-1})$，令 $S=T\setminus\{e\}$. 显然 $|S|=2n$ 且逆运算封闭. 由 $T^2=2G-T^{(2)}+2ne-2f$ 得 $|\tilde{S^2}|=|T^2|=M_C(2n,2)$，所以满足条件的 S 存在. □

定理4.3说明第二类图存在当且仅当顶点集 G 中存在满足条件 (a)，(b) 和 (c) 的 T.

由引理4.1可知，G 中只有一个二阶元，记为 f. 因此，对 G 的任意子群 H，若 $|H|$ 是偶数，则 H 必定包含 f. 令 $\overline{(\cdot)}:G\to G/H$ 是一个同态，则 $\bar{f}$ 是 G/H 的单位元.

假设 $H\leq G$，且阶为偶数 m，则满足条件 (b) 和 (c) 的 T 一定满足如下条件.

(b') $\overline{T}=\overline{T}^{(-1)}$,

(c') $\overline{T}^2=2mG/H-\overline{T}^{(2)}+2n-2$.

为了方便叙述，用 1 代替 G/H 的单位元 $\bar{e}$. 于是 $(2n-2)\bar{e}$ 可以简写为 $(2n-2)$.

先考虑满足条件 (b') 和 (c') 的一个特殊情况.

引理 4.2: 设 K 是一个单位元为 e_K，阶为 v 的交换群，$S=a\cdot e_K+bK\in\mathbb{Z}[K]$. 若 v 和 m 是满足 $a+vb=2n+1$ 和 $mv=2n^2+2n+2$ 的正整数且 S 满足

$$
S^2=2mK-S+(2n-2)e_K, \tag{4.2}
$$

则 $8n-7$ 是 $\mathbb{Z}$ 中的一个平方元.

证明：通过计算，可以得到

$$
\begin{aligned}
S^2&=(ae_K+bK)^2\\
&=a^2e_K+2abK+b^2vK\\
&=a^2e_K+(ab+b(2n+1))K.
\end{aligned}
$$

通过比较 e_K 在(4.2)中的系数，可以得到

$$
a^2+a-2n+2=0,
$$

这表明 $8n-7$ 是 $\mathbb{Z}$ 中的一个平方元. □

根据 $|G/H|$ 的大小，从小到大依次证明满足条件 (b') 和 (c') 的 $\overline{T}$ 的不存在性. 首先是 $G/H \cong C_3$ 的情况.

命题 4.1: 假设 $G/H \cong C_3$ 且 $8n-7$ 是非平方元，则不存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_3]$.

证明: 用反证法证明，假设存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_3]$. 因为 $\overline{T}^{(2)} = \overline{T}^{(-1)} = \overline{T}$，所以存在 $a, b \in \mathbb{Z}_{\geq 0}$ 使得 $\overline{T} = a + bG/H$，且由条件 (c') 得

$$\overline{T}^2 = 2mG/H - \overline{T} + 2n - 2.$$

根据引理3.2得，$8n-7$ 是 $\mathbb{Z}$ 中的一个平方元，与假设条件相矛盾. 因此，不存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_3]$. □

由于对任意的 $n \in \mathbb{Z}$，$5 \nmid 2n^2+2n+2$，所以不必考虑 $G/H \cong C_5$ 的情况. 下面研究 $G/H \cong C_7$ 的情况.

定理 4.4: 假设 $G/H \cong C_7$ 且 $8n-7$ 是 $\mathbb{Z}$ 中的一个非平方元. 则不存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_7]$.

证明: 用反证法证明，假设存在满足条件 (b') 和 (c') 的 $\overline{T} \in \mathbb{Z}[C_7]$，则对 $i = 0, 1, 2,$

$$f_i = \overline{T}^{(2^i)}\overline{T}^{(2^i)} + \overline{T}^{(2^{i+1})} - 2n + 2 \equiv 0 \pmod{G/H}. \tag{4.3}$$

将它们看作以 $\overline{T}^{(2^i)}$ 为变量的多项式. 通过联立 f_0, f_1 和 f_2 消元可以得到一个只包含一个变量 $\overline{T}$ 的多项式 h. 然后，再对 $h \pmod{G/H}$ 进行因式分解，得到两个不可约因子

$$h \equiv (\overline{T}^2 + \overline{T} - 2n + 2)l \pmod{G/H}.$$

其中

$$\begin{aligned} l = {} & \overline{T}^6 - \overline{T}^5 - (6n-7)\overline{T}^4 + (4n-5)\overline{T}^3 + (12n^2 - 30n + 19)\overline{T}^2 \\ & - (4n^2 - 12n + 9)\overline{T} - 8n^3 + 32n^2 - 42n + 19. \end{aligned}$$

由于 h 是联立 f_0, f_1 和 f_2 消元得到，所以 h 模 G/H 同余 0. 因为剩余类环 $\mathbb{Z}[G/H]/(G/H)$ 没有零因子 (该环与 $\mathbb{Z}[X]/(\sum_{i=0}^{6} X^i)$ 同构)，因此 h 至少存在一个因式模 G/H 同余 0.

假设 $\overline{T}^2+\overline{T}-2n+2$ 模 G/H 同余 0. 令 $\chi\in\widehat{G/H}$ 为一个特征，则 $\chi(\overline{T})\in\mathbb{Z}[\zeta_7]$ 满足

$$\chi(\overline{T})^2+\chi(\overline{T})-2n+2=0. \tag{4.4}$$

由此推出 $8n-7$ 在 $\mathbb{Z}[\zeta_7]$ 中是一个平方元. 又因为 $8n-7$ 在 $\mathbb{Z}$ 中是非平方元. 假设 $8n-7$ 有一个整数平方因子，即存在 $t,k\in\mathbb{Z}$ 且 $t>1$ 是个非平方元，$8n-7=tk^2$，则 $t\equiv 1 \pmod 8$. 显然 $t>7$. 由引理2.2得，包含 $\mathbb{Q}(\sqrt{8n-7})$ 的最小分圆域为 $\mathbb{Q}(\zeta_t)$ 而不是 $Q(\zeta_7)$，因此不存在满足(4.4)的 $\chi(\overline{T})$. 因此，$\overline{T}^2+\overline{T}-2n+2$ 模 G/H 不同余 0，则 $l\equiv 0 \pmod{G/H}$.

因为 l 是一个 6 次多项式，选一个素数 p 来对 $\chi(l)=0$ 进行模 p 处理. 要求 p 是模 $v=7$ 的本原元，即 $p=3,5 \pmod v$. 根据引理2.3，(p) 是 $\mathbb{Z}[\zeta_v]$ 中的素理想. 用 X 代替 $\chi(l)\equiv 0 \pmod p$ 中的 $\chi(\overline{T}) \pmod p$ 且将其系数都模 p，则得到一个 $\mathbb{F}_p[X]$ 中的多项式 $\bar{l}(X)$.

假设 τ_1 是该多项式的根，即 $\bar{l}(\tau_1)=0$ 且 $\tau_1\equiv\chi(\overline{T}) \pmod p$. 假设 τ_1 的极小多项式的次数为 s，则 τ_1 的所有共轭元为：$\tau_1^p,\tau_1^{p^2},\ldots,\tau_1^{p^{s-1}}$. 因为 p 是模 $v=7$ 本原元，所以 $p^{\frac{v-1}{2}}\equiv -1 \pmod v$. 又 $\chi(\overline{T}^{(p)})\equiv\chi(\overline{T})^p \pmod p$ 且 $\overline{T}^{(-1)}=\overline{T}$，因此

$$\chi(\overline{T})=\chi(\overline{T}^{(-1)})=\chi\left(\overline{T}^{(p^{\frac{v-1}{2}})}\right)\equiv\chi(\overline{T})^{p^{\frac{v-1}{2}}} \pmod p.$$

所以 $\tau_1^{p^3}=\tau_1^{p^{\frac{v-1}{2}}}=\tau_1$，这意味着 $s=1$ 或 $s=3$. 因此 $\bar{l}$ 的所有根 $\tau_1,\tau_1^p,\ldots,\tau_1^{p^{s-1}}$ 都属于 $\mathbb{F}_{p^3}$.

因为 τ_1 是 $\bar{l}$ 的一个根且 $\chi(\overline{T}^{(p)})\equiv\chi(\overline{T})^p \pmod p$. 因此

$$\tau_i:\equiv\chi(\overline{T}^{(2^i)})\equiv\begin{cases}\tau_1^{p^{3-i}} \pmod p, & 若 p\equiv 3 \pmod 7;\\ \tau_1^{p^i} \pmod p, & 若 p\equiv 5 \pmod 7.\end{cases} \tag{4.5}$$

注意 τ_1 一定要满足的必要条件. 首先，由 (4.3) 得

$$\tau_i^2+\tau_{i+1}-2n+2\equiv 0 \pmod p. \tag{4.6}$$

其中 $i=0,1,2$. 其次，设 $\overline{T}=\sum_{\bar{g}\in G/H}a_{\bar{g}}\bar{g}$，可通过反推公式 (2.2) 计算 $a_{\bar{g}}$. 令 β 是 $\mathbb{F}_{p^{v-1}}$ 中一个阶数为 $v=7$ 的元. 对 $\bar{g}\in G/H$，假设 $\chi(\bar{g})\equiv\beta \pmod p$，则

$$\begin{aligned} a_{\bar{g}} &= \frac{1}{7}\left((2n+1)+\sum_{i=1}^{6}\chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right) \\ &= \frac{1}{7}\left((2n+1)+\sum_{i=1}^{3}\chi(\overline{T}^{(i)})\left(\chi(\bar{g}^{i})+\chi(\bar{g}^{-i})\right)\right) \\ &\equiv \frac{1}{7}\left((2n+1)+\sum_{j=0}^{2}\tau_1^{p^j}(\beta^{p^j}+\beta^{-p^j})\right) \pmod{p}. \end{aligned} \tag{4.7}$$

显然 $a_{\bar{g}} \pmod p$ 必须是 $\mathbb{F}_p$ 中的某个元. 而且，因为 $|\overline{T}| = |T| = 2n+1$，因此所有的 $a_{\bar{g}}$ 满足

$$\sum_{\bar{g}\in G/H} a_{\bar{g}} \equiv 2n+1 \pmod{p}. \tag{4.8}$$

基于上述提到的所有必要条件，可以给出一个排除满足条件 (b') 和 (c') 的 $\overline{T}$ 的存在性的方法. 首先选定一个模 v 本原元素数 p，然后根据 n 模 p 的值，分成 p 种不同的情况. 为了检验这些必要条件，需要求出 $\bar{l}$ 在 $\mathbb{F}_{p^3} = \mathbb{F}_{p^{\frac{v-1}{2}}}$ 中的所有根，记 $\Omega = \{\bar{l}(x) = 0 : x \in \mathbb{F}_{p^3}\}$，且对 Ω 中的每个元素 τ_1，按如下 4 步计算：

(i) 将 τ_1 代入 (4.5) 求出 τ_i;

(ii) 检查 (4.6) 是否对每个 i 都成立;

(iii) 由 (4.7) 计算出 $a_{\bar{g}}$;

(iv) 检查是否 $a_{\bar{g}}$ 都满足 $a_{\bar{g}} \pmod p \in \mathbb{F}_p$ 和 (4.8).

利用 MAGMA 可以计算出当取 $p = 101$ 时，对 n 模 p 的每一个可能的值，都能找到至少一个必要条件满足不了，因此，不存在满足条件 (b') 和 (c') 的 $\overline{T}$. □

与第三章的的情况一样，我们只需要关注 $|G/H|$ 是奇素数的情况. 定理4.4的证明方法还可以运用到 $|G/H|$ 更大的情况. 接下来 5 个可能的整除 n^2+n+1 的整数依次为 13, 19, 31, 37 和 43. 利用 MAGMA 可以得到：对 $G/H \cong C_{13}, G/H \cong C_{19}$ 和 $G/H \cong C_{31}$ 的情况，分别取 $p = 227, p = 241$ 以及 $p = 881$，按照定理4.4的方法可以证明不存在满足条件 (b') 和 (c') 的 $\overline{T}$. 由于过程与定理4.4类似，所以不再重复叙述. 对下一个整除 $|G|$ 的奇素数 37，由于运算量太大，计算机无法消元得到单变元多项式 h. 因此处理不了该情况以及 $|G/H|$ 更大的情况.

综合上述结论，可以得到以下推论.

推论 4.5: 设 G 是阶为 $2n^2+2n+2$ 的交换群，$8n-7$ 是 $\mathbb{Z}$ 中的非平方元，若下列条件满足其中之一

1) $3, 7, 19$ 或 $31 \mid n^2+n+1$;

2) $13 \mid n^2+n+1$ 且 $8n-11 \notin \{13k^2 : k \in \mathbb{Z}\}$.

则不存在满足定理4.3中的三个条件的 $T \subseteq G$，因此不存在以 G 为顶点集的第二类图.

4.1.2 对称多项式方法

由于 $|G| = 2n^2+2n+2$ 可能存在大于 $2n+1$ 的素因子，因此可以利用 Kim[28] 的对称多项式方法. 这里用到的方法是参考 [30] 中对 Kim 的对称多项式方法的推广得到的.

定理 4.6: 假设 $2n^2+2n+2 = mv(n>1)$,v 是素数且 $v > 2n+1$. 设 G 是一个阶为 $2n^2+2n+2$ 的加法交换群. 设 a 是满足 $v \mid 4^a+4n+2$ 的最小正整数，b 是满足 $v \mid 4^b-1$ 的最小正整数 (若不存在 a 使得 $v \mid 4^a+4n+2$，则令 $a=\infty$). 若对 $\forall l \in \{0,1,\cdots,\lfloor\frac{m-1}{4}\rfloor\}$，$a(x+1)+by = n-l$ 都不存在非负整数解，则 G 中不存在满足 $e \notin S$，$|S| = 2n$ 且 $|\tilde{S}^2| = 2n^2+2n+1(\tilde{S} = S \cup \{e\})$ 的逆运算封闭子集 S.

证明: 反证法，假设存在这样的 S.

将 S 分为 $R = \{r_i : i = 1,\cdots,n\}$ 和 $-R = \{-r_i : r_i \in R\}$ 两部分. 因为 $|\tilde{S}^2| = 2n^2+2n+1$，则根据引理4.1，

$$\{0\}, \{\pm r_i : i = 1,\cdots,n\}, \{\pm 2r_i : i = 1,\cdots,n\}, \{\pm r_i \pm r_j : 1 \le i < j \le n\}.$$

组成 $G \setminus \{f\}$ 的一个划分，其中 f 是 G 中唯一的二阶元.

假设 H 是 G 的一个子群，且 $|G/H| = v$. 令 $\rho : G \to G/H$ 是一个同态，且 $x_i = \rho(r_i)$. 则

$$\{0\}, \{* \pm x_i : i = 1,\cdots,n*\}, \{* \pm 2x_i : i = 1,\cdots,n*\}, \{* \pm x_i \pm x_j : 1 \le i < j \le n*\}$$

组成了 $mG/H \setminus \{0\}$ 的一个划分. 对一个整数 k，通过计算得

$$\begin{aligned}
&\sum_{i=1}^{n}(x_i^{2k} + (-x_i)^{2k} + (2x_i)^{2k} + (-2x_i)^{2k}) \\
&+ \sum_{1\le i<j\le n}((x_i+x_j)^{2k} + (x_i-x_j)^{2k} + (-x_i+x_j)^{2k} + (-x_i-x_j)^{2k}) \\
=&(4^k+4n+2)S_{2k} + 2\sum_{t=1}^{k-1}\binom{2k}{2t}S_{2t}S_{2(k-t)}.
\end{aligned}$$

其中 $S_t := \sum_{i=1}^{n} x_i^t$. 因为这也是对 $mG/H \setminus \{0\}$ 中每个元的 $2k$ 次方求和，所以

$$(4^k + 4n + 2)S_{2k} + 2\sum_{t=1}^{k-1} \binom{2k}{2t} S_{2t}S_{2(k-t)} = \begin{cases} 0, & v-1 \nmid 2k; \\ -m, & v-1 \mid 2k. \end{cases} \tag{4.9}$$

令 a 和 b 分别为满足 $v \mid 4^a + 4n + 2$ 和 $v \mid 4^b - 1$ 的最小正整数. 定义

$$X = \{ax + by : x \geq 1, y \geq 0\}.$$

首先证明如下两个命题.

命题 **1**：假设 $1 \leq k < \frac{v-1}{2}$，若 $k \notin X$，则 $S_{2k} = 0$.

使用归纳法，假设对任意 $k \leq k_0 - 1$ 且 $k \notin X$，$S_{2k} = 0$. 若 $k_0 \notin X$，由于 X 是加法封闭的，则对每个 t，t 和 $k_0 - t$ 至少有一个不属于 X.

因为任意满足 $v \mid 4^k + 4n + 2$ 的 k 一定是 $a + by$ 的形式，即 $k \in X$. 由此可得 $v \nmid 4^{k_0} + 4n + 2$. 根据(4.9)和归纳假设，

$$0 = (4^{k_0} + 4n + 2)S_{2k_0} + 2\sum_{t=1}^{k_0-1} \binom{2k_0}{2t} S_{2t}S_{2(k_0-t)} = (4^{k_0} + 4n + 2)S_{2k_0}.$$

因此，$S_{2k_0} = 0$.

设 $e_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1}^2 x_{i_2}^2 \cdots x_{i_k}^2$.

命题 **2**：假设 $1 \leq k \leq n < \frac{v-1}{2}$，若 $k \notin X$，则 $e_k = 0$.

同样使用归纳法，假设对任意 $k \leq k_0 - 1$ 且 $k \notin X$，$e_k = 0$. 若 $k_0 \notin X$，由于 X 是加法封闭的，则对每个 $0 < t < k_0$，t 和 $k_0 - t$ 至少有一个不属于 X. 根据命题 **1** 和归纳假设得，$e_t = 0$ 或 $S_{2(k_0-t)} = 0$. 根据关于 $x_1^2, x_2^2, \cdots, x_n^2$ 的牛顿恒等式 (Newton identities) 得

$$k_0 e_{k_0} = e_{k_0-1}S_2 - e_{k_0-2}S_4 + \cdots + (-1)^{k_0-1}S_{2k_0} = (-1)^{k_0-1}S_{2k_0} = 0.$$

于是，$e_{k_0} = 0$.

易知，若 $x_i = 0$，则 $-x_i = 2x_i = -2x_i = 0$. 因为 0 在 $mG/H \setminus \{0\}$ 中恰好出现 $m - 1$ 次. 因此 0 在 $\{x_i : i = 1, \cdots, n\}$ 中最多出现 $\lfloor \frac{m-1}{4} \rfloor$ 次. 假设 0 在其中出现 l 次 ($l \leq \lfloor \frac{m-1}{4} \rfloor$)，则 e_{n-l} 为所有非零 x_i^2 的乘积. 因此 $e_{n-l} \neq 0$. 由命题 **2** 得 $n - l \in X$，因此方程 $a(x+1) + by = n - l$ 存在非负整数解，与条件相矛盾！

□

综上所述，若 n 满足推论4.5或定理4.6中的条件，$\mathbb{Z}^n$ 上不存在几乎完美线性李码. 表格4.1中列出了能被推论4.5和定理4.6排除的 n 的个数，最后一行是综合二

者后的结果.

表 4.1　推论4.5和定理4.6排除的 n 的个数，其中 $v=|G/H|$.

条件	10	10^2	10^3	10^4	10^5
$3 \mid n^2+n+1$	1	25	304	3240	33036
$7 \mid n^2+n+1$	1	21	260	2778	28316
$13 \mid n^2+n+1$	1	10	133	1469	15161
$19 \mid n^2+n+1$	0	8	96	1022	10432
$31 \mid n^2+n+1$	1	5	59	627	6394
推论 4.5	3	52	620	6486	65826
定理 4.6	5	67	715	7072	70290
合计	6	84	910	9286	92524

从表格4.1中可以看出，$n \leq 10^5$ 中超过 90% 的 n 可以被推论4.5或定理4.6排除. 因为目前只找到了 $n=1,2$ 时的第二类图. 因此可以合理猜想：对于阶为 $2n^2+2n+2$ 的交换群 G，除了 $n=1$ 和 2 外，不存在以 G 为顶点集的第二类图.

本节部分内容已撰写学术论文于 2021 年 7 月在期刊 Discrete Mathematics Letters 上发表.

4.2　第三类图的存在性问题

本节研究第三类图与汉明距离下的二元完美线性码存在性的等价关系，首先介绍线性码的有关知识.

设 $\mathbb{F}_q^n$ 是有限域 $\mathbb{F}_q$ 上的 n 维向量空间，$\mathbb{F}_q$ 上的 (n, M) **码 C** 指的是 $\mathbb{F}_q^n$ 上包含 M 个向量的子集. C 中元素就是 C 的**码字** (codeword). 当 $q=2$ 时，称该码为**二元码** (binary code). 若 C 为 $\mathbb{F}_q^n$ 上的 k 维子空间，则称 C 为 $\mathbb{F}_q$ 上的 $[n, k]$ **线性码**. 若一个 $k \times n$ 矩阵的所有行向量构成 $[n,k]$ 线性码 C 的一组基，则称该矩阵为 C 的**生成矩阵** (generator matrix). 若一个 $(n-k) \times n$ 矩阵 H 满足所有行向量线性无关且

$$C=\{x \in \mathbb{F}_q^n | Hx^T=0\}.$$

则称 H 为 $[n,k]$ 线性码 C 的**校验矩阵** (parity check matrix)，以 H 为生成矩阵的线性码被称为 C 的**对偶码** (dual code).

两个码字不同坐标的个数称为它们之间的**汉明距离** (Hamming-metric，以下简称距离). 码 C 的**极小距离** (minimum distance) 是指 C 中所有不同码字间距离的最

小值. 当一个码的极小距离不小于 $2r+1$ 时，称该码为 ***r*- 纠错码** (r-error-correcting code)，r 为**纠错半径** (error-correcting radius). 用 $[n,k,w]$ 码表示极小距离为 w 的 $[n,k]$ 线性码.

记 $t=\lfloor\frac{w-1}{2}\rfloor$，当一个码的极小距离为 w 时，以其中码字为中心，t 为半径的球是互不相交的，而一个球中包含 $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i$ 个点. 设 $\mathbb{F}_q$ 中长度为 n，极小距离为 w 的码最多包含 $A_q(n,w)$ 个码字，易知 $A_q(n,w)$ 满足

$$A_q(n,w)\leq\frac{q^n}{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i}.$$

不等式的右边就是**汉明界** (Hamming bound). 当 C 的码字的个数达到汉明界时，则称 C 为**完美码** (perfect code).

下面证明第三类图与二元完美线性码存在性的等价关系.

定理 4.7: 设 k，d 为正整数，$G=(\mathbb{F}_2^m,+)$ 且 $|G|=\sum_{i=0}^{k}\binom{d}{i}$. 下列两个命题等价：

1) G 中存在满足 $|S|=d$ 且不含零向量的子集 S，使得交换凯莱图 $\Gamma(G,S)$ 的直径为 k;

2) $\mathbb{F}_2$ 上存在 $[d,d-m,2k+1]$ 完美码.

证明：先证必要性. 因为 $G=(\mathbb{F}_2^m,+)$，由 $|G|=\sum_{i=0}^{k}\binom{d}{i}$ 可得 $2^m=\sum_{i=0}^{k}\binom{d}{i}$. 交换凯莱图 $\Gamma(G,S)$ 的直径为 k 和 $|G|=\sum_{i=0}^{k}\binom{d}{i}$ 意味着 S 中任意不超过 k 个向量相加得到的结果都不同，并且

$$G=\left\{\sum_{0\leq i\leq l}s_i : l\leq k, s_i\in S\text{且两两不同}\right\}. \tag{4.10}$$

因为 G 是 $\mathbb{F}_2$ 的 n 维空间，所以 S 中任意 $2k$ 个向量相加都不等于零向量，即任意 $2k$ 个向量都线性无关. 关于 S 中 $2k+1$ 个向量的线性相关性，有如下命题.

命题 **1**：S 中存在 $2k+1$ 个向量线性相关.

由(4.10)式可知，对任意 $k+1$ 个向量之和，必定存在 a 个向量使得该 $a+k+1$ 个向量之和等于零向量，其中 $a\leq k$. 若 a 不等于 k，则 $a\leq k-1$. 因此 $a+k+1\leq 2k$，与 S 中任意 $2k$ 个向量相加都不等于零向量相矛盾. 因此 $a=k$. 由此可知 S 中存在 $2k+1$ 个向量之和等于零向量，即存在 $2k+1$ 个向量线性相关.

将 $s_1,\cdots,s_d$ 以列向量的形式组成一个矩阵 H，易知 H 是一个 $m\times d$ 矩阵.

命题 **2**：H 是行满秩矩阵.

假设 H 不是行满秩，不妨设 H 的行秩为 $m-\alpha$，$\alpha \in \mathbb{Z}^+$，则 H 中存在 $m-\alpha$ 个线性无关的行向量. 将其组成新矩阵 H'. 以 H' 为生成矩阵的线性码是 $[d, m-\alpha]$ 线性码. 因为 H 中任意 $2k$ 个向量都线性无关且存在 $2k+1$ 个向量线性相关，所以其对偶码的极小距离等于 $2k+1$，因此该对偶码是一个 $[d, d-m+\alpha, 2k+1]$ 码，由汉明界，

$$2^{d-N+\alpha} \leq \frac{2^d}{\sum_{i=0}^{k}\binom{d}{i}}.$$

因此 $2^{m-\alpha} \geq \sum_{i=0}^{k}\binom{d}{i}$，这与 $2^m = \sum_{i=0}^{k}\binom{d}{i}$ 相矛盾. 因此 H 是行满秩的.

因为 H 行满秩，则以 H 为生成矩阵的线性码是 $[d, m]$ 线性码. 其对偶码是 $[d, d-m, 2k+1]$ 码，由于线性码的极小距离为 w 当且仅当其校验矩阵存在 w 个线性相关的列向量，并且不存在 $w-1$ 个线性相关的列向量. 所以由命题 **1** 可知，该对偶码的极小距离为 $2k+1$. 由 $2^m = \sum_{i=0}^{k}\binom{d}{i}$ 得

$$2^{d-m} = \frac{2^d}{\sum_{i=0}^{k}\binom{d}{i}}.$$

因此，该对偶码是完美码.

下面证明充分性. 若 $\mathbb{F}_2$ 上存在 $[d, d-m, 2k+1]$ 完美码，则其对偶码为 $\mathbb{F}_2$ 上的 $[d, m]$ 线性码. 假设对偶码的生成矩阵为 L，因为原码的极小距离为 $2k+1$，则 L 的 d 个列向量中任意 $2k$ 个向量都是线性无关的. 将 L 的 d 个 m 维列向量视为集合 S，显然 S 是 G 中不含零向量的子集. 因为 S 中任意 $2k$ 个向量都是线性无关的，所以 S 中任意不超过 k 个向量相加得到的结果都不同，共有 $\sum_{i=0}^{k}\binom{d}{i}$ 种不同的元素. 因为 S 是 G 中的子集，$|G| = \sum_{i=0}^{k}\binom{d}{i}$，所以交换凯莱图 $\Gamma(G, S)$ 的直径为 k. □

由上述定理可知，每个第三类图都存在一个二元完美线性码与之对应. 因为 k 是正整数，所以 $[d, d-m, 2k+1]$ 完美码的极小距离 $2k+1 \geq 3$. 极小距离大于 3 的二元完美线性码只有码长为奇数的重复码和二元格雷码；极小距离等于 3 的二元完美线性码只有汉明码 [36-37]. 下面介绍这三种码的定义.

在 $\mathbb{F}_2^n$ 中，**重复码** (repetition code) 是只包含 $0\cdots00$ 和 $1\cdots11$ 两个码字的 $[n, 1, n]$ 码.

将 1，2，$\cdots$，2^r-1 写成 r 位 2 进制的形式，位数不够的用 0 在左边补齐. 若把该 2^r-1 个 2 进制数看作 2^r-1 个 r 维向量，则按列向量的形式可以组成一个 $r \times (2^r-1)$ 矩阵 H_r，以该矩阵为校验矩阵的码是一个 $[n=2^r-1, n-r]$ 码，无论将 H_r 的列向量如何置换得到的都是等价的码，该码被称为**汉明码** (Hamming

code). 由于汉明码的校验矩阵任意 2 列线性无关，存在 3 列线性相关，则汉明码的极小距离为 3.

定义 $G_{24} = [I_{12}|A]$，其中 I_{12} 是 12 阶单位矩阵，

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

以 G_{24} 为生成矩阵的线性码是 $[24, 12, 8]$ 码. 由 [37] 得，以删除 G_{24} 任何一列后为生成矩阵的线性码都是等价的，是 $[23, 12, 7]$ 码，被称为**二元格雷码** (binary Golay code).

设 $n > 1$ 为奇数，n 长的重复码，$[2^r - 1, 2^r - r - 1, 3]$ 汉明码和二元格雷码分别对应如下等式：

1) $2^{n-1} = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i}$;

2) $2^r = \sum_{i=0}^{1} \binom{2^r-1}{i}$;

3) $2^{11} = \sum_{i=0}^{3} \binom{23}{i}$.

根据上述二元完美线性码的存在性情况，可得到关于第三类图存在性的如下定理.

定理 4.8: 设 $G = (\mathbb{F}_2^m, +)$，则以 G 为顶点集的第三类图只存在如下几类：

1) $S = \{s : s \in G \setminus \{0, 0, \cdots, 0\}\}$，直径 $k = 1$;

2) $2 \mid m$ 且 $S = \{e_1, e_2, \cdots, e_m, l_m\}$，直径 $k = \frac{m}{2}$;

其中 $e_i (i = 1, 2, \cdots, m)$ 为标准基, l_m 为全 1 向量.

3) 当 $m = 11$ 时，取 S 是由二元格雷码的校验矩阵全体列向量构成的集合. 此时，$|S| = 23$，$\Gamma(G, S)$ 的直径 $k = 3$.

第五章　结论与展望

5.1　主要研究工作

图论中的“度——直径”问题以其广阔的研究背景和应用，备受专家学者的关注. 关于该问题，最理想的情况显然是完成摩尔图或者交换凯莱摩尔图的分类. 但经过长时间的研究，摩尔图的分类问题已基本解决，但交换凯莱图的分类还远未达成.

本文共研究了三类交换凯莱图，第一类图是直径为 2，度为 $2n$ 的情况下阶比交换凯莱摩尔界小 1 的交换凯莱图. 通过运用代数数论、有限域和群特征标等数学工具得到了如下结论：设 G 是一个 $2n^2+2n$ 阶的交换群. 若 $8n+9$ 是 $\mathbb{Z}$ 中的一个非平方元，以及下面三个条件满足任意至少一个

1) $3,7,11$ 或 $19 \mid n(n+1)$;

2) 对 $v=5$或13，$v \mid n(n+1)$ 且 $8n+5 \notin \{vk^2 : k \in \mathbb{Z}\}$;

3) $17 \mid n(n+1)$ 且 $8n+9 \notin \{17k^2 : k \in \mathbb{Z}\}$.

则不存在以 G 为顶点集的第一类图.

对于第二类图除运用第一类图中提到的方法外，还利用对称多项式等数学工具得到如下两个结论：

1、 设 G 是阶为 $2n^2+2n+2$ 的交换群，$8n-7$ 不是 $\mathbb{Z}$ 上的平方元，若下列条件满足至少一个：

   1) 3，7，19 或 $31 \mid n^2+n+1$；

   2) $13 \mid n^2+n+1$ 且 $8n-11 \notin \{13k^2 : k \in \mathbb{Z}\}$，

   则不存在以 G 为顶点集的第二类图.

2、 假设 $2n^2+2n+2=mv(n>1)$，v 是素数且 $v>2n+1$. 设 G 是一个阶为 $2n^2+2n+2$ 的加法交换群. 设 a 是满足 $v \mid 4^a+4n+2$ 的最小正整数，b 是满足 $v \mid 4^b-1$ 的最小正整数 (若不存在 a 使得 $v \mid 4^a+4n+2$，则令 $a=\infty$). 若对 $\forall l \in \{0,1,\cdots,\lfloor\frac{m-1}{4}\rfloor\}$，$a(x+1)+by=n-l$ 都不存在非负整数解，则不存在以 G 为顶点集的第二类图.

第三类图是顶点群为初等 2 群的交换凯莱图. 对第三类图，本文证明第三类图与汉明距离下的二元完美线性码存在性的等价关系. 并根据完美码的已有分类结果，给出了第三类图的完全分类：设 $G=(\mathbb{F}_2^m,+)$，则以 G 为顶点集的第三类图只存在如下几类：

1) $S=\{s:s\in G\setminus\{0,0,\cdots,0\}\}$，直径 $k=1$；

2) $2\mid m$ 且 $S=\{e_1,e_2,\cdots,e_m,l_m\}$，直径 $k=\frac{m}{2}$；

   其中 $e_i(i=1,2,\cdots,m)$ 为标准基, l_m 为全 1 向量.

3) 当 $m=11$ 时，取 S 是由二元格雷码的校验矩阵全体列向量构成的集合. 此时，$|S|=23$，$\Gamma(G,S)$ 的直径 $k=3$.

5.2 未来研究展望

第三章末尾提出了阶为 $2n^2+2n$ 情况下的猜想：除了 $n=1$ 和 $n=2$ 的情况，其余情况下都不存在第一类图. 对于推论3.10不能排除的情况，需要寻找新的方法将其排除. 对于阶为 $2n^2+2n+2$ 的情况，本文利用两种方法排除了部分情况，其余情况的存在性有待于进一步研究.

本文研究的前两类图都是直径为 2 的交换凯莱图，对于直径更大的图，可以尝试利用 Qureshi 在 [38] 中使用的对称多项式方法研究其分类问题. 由于解决方法尚不成熟，出于学位论文的严谨性，未在文中给出.

由于交换凯莱摩尔图与线性完美李码的存在性等价. Golomb-Welch 猜想等价于当 $n\geq 3$ 且 $r\geq 2$ 时，$\mathbb{Z}^n$ 中不存在完美 r- 纠错李码. 因此，若能证明 Golomb-Welch 猜想的正确性，交换凯莱摩尔图的分类问题也随之解决. 目前作者正在学习离散几何以及调和分析 [6] 中的一些方法，改进并应用到 Golomb-Welch 猜想的证明中.

致　谢

回想起第一次来国防科大参加保研面试，已是三年以前，那时本科毕业论文还未开始，转眼间硕士毕业论文已经接近尾声. 两年半的军校生活改变了我很多，以前作为地方大学国防生，没有真正接触部队，对部队的很多东西都不了解，这两年半的军校生活让我养成了一个军人该有的生活习惯，明白了自己的使命和担当.

作为一名研究生，学习的任务不同于本科生，在这两年半内不仅需要完成规定的学分任务，还要发表论文. 对于如何完成研究生阶段的学业，也有过迷茫. 非常幸运能遇到尽职尽责的周悦老师，周老师对学生很负责，一开始便规划好了我的研究生阶段的学术任务，正是因为一切都能按部就班地进行，如今才能顺利达到毕业要求. 在带学生的过程中，周老师既严格，又很有耐心. 让我记忆深刻的是在第一次撰写学术论文的时候，由于从未写过学术论文，很多地方都很不规范，达不到一篇学术论文应有的标准. 周老师没有过多的苛责，而是手把手耐心地指导. 除此之外，周老师对学术的专注和对卓越的追求为实验室的学生树立了良好的榜样，让我们不敢放松对自己的要求. 生活中周老师也很关心学生，在学校取消寒假就地过年时，还暖心地请我们一起吃饭. 衷心祝福周老师婚后生活幸福美满，身体健康，在学术上取得更高的成就.

在实验室的两年半里，我获得过很多来自老师和同学们的帮助. 感谢李超教授对实验室的辛苦付出，领导实验室向着更强大的方向发展，祝福李老师身体健康，阖家幸福. 感谢实验室的屈龙江、海昕、李瑞林、付绍静、孙兵、刘国强、周子健和刘韵雯等老师，感谢您们在科研学术上给我的指导和生活上的帮助. 感谢杨智超师兄，智超师兄是实验室的加班常客，在我为发论文焦虑的时候，经常能和智超师兄一起坐班车回一号院，在车上和师兄交流自己的烦恼，师兄给了我很多指导. 还要感谢李康荃师兄，康荃师兄是我们讨论班的大师兄，自身学术上的成绩很出色，指导过众多师弟师妹. 此外还要感谢李宇玻师兄，在众多师兄中，我跟李宇玻师兄的交流最多. 师兄不但学术实力过硬，对实验室的师弟师妹也很照顾，乐于助人是同学们对他的第一印象. 另外还要感谢万前红老师，第一次见万老师时我称呼她师姐，当时我不清楚博后是什么，也不了解万老师的情况，就往年轻了称呼. 不过万老师确实像师姐一样，跟我们有商有量，在学习和生活上都给了我们很多帮助. 万老师教会了我很多为人处世的道理，胜似生活中的导师，祝万老师家庭幸福，工作顺利，永远开心. 感谢实验室的张毅师兄、刘佳杰师兄、陆金玉师姐、史佳丽师姐、靳仁杰师兄、孙明豪师兄，感谢你们在学习生活方面给我的帮

助. 还要特别感谢计算机学院的张璋师兄在我撰写毕业论文时提供的帮助. 感谢杨云霄同学、姜沙同学、张维师弟、于博师弟、张翰丰师妹、唐薇师妹、胡禹佳师妹在生活上给我的帮助，感谢实验室李红艳秘书为实验室的辛苦付出. 非常荣幸能和你们相处这两年半，不管是学习科研还是家庭生活都祝愿大家越来越好，感谢帮助过我的每一位同学和老师，你们教会了我待人真诚，热心地为他人提供力所能及的帮助，这样才能拥有愉快的工作氛围. 最后要感谢我的家人们，我的今天离不开你们坚定的支持.

参考文献

[1] Dougherty R, Faber V. The Degree-Diameter Problem for Several Varieties of Cayley Graphs I: The Abelian Case[J]. SIAM Journal on Discrete Mathematics, 2004, 17(3): 478~519.

[2] Leung K H, Zhou Y. No lattice tiling of $\mathbb{Z}^n$ by Lee sphere of radius 2[J]. Journal of Combinatorial Theory, Series A, 2020, 171.

[3] Miller M, Sirán J. Moore graphs and beyond: A survey of the degree/diameter problem[J]. The Electronic Journal of Combinatorics, 2013, 20(2): DS14.

[4] Macbeth H, Siagiová J, Sirán J. Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups[J]. Discrete Mathematics, 2012, 312(1): 94~99.

[5] Dinneen M J, Hafner P R. New results for the degree/diameter problem[J]. Networks, 1994, 24(7): 359~367.

[6] Horak P, Kim D. 50 Years of the Golomb–Welch Conjecture[J]. IEEE Transactions on Information Theory, 2018, 64(4): 3048~3061.

[7] Hoffman A J, Singleton R R. On Moore Graphs with Diameters 2 and 3[J]. IBM Journal of Research and Development, 1960, 4(5): 497~504.

[8] Damerell R M. On Moore graphs[J]. Mathematical Proceedings of the Cambridge Philosophical Society, 1973, 74(2): 227~236.

[9] Bannai E, Ito T. On finite Moore graphs[J]. Journal of the Faculty of Science the University of Tokyo.sect A Mathematics, 1973, 20: 191~208.

[10] Plesník J. One method for proving the impossibility of certain Moore graphs[J]. Discrete Mathematics, 1974, 8(4): 363~376.

[11] Erdös P, Fajtlowicz S, Hoffman A J. Maximum degree in graphs of diameter 2[J]. Networks, 1980, 10(1): 87~90.

[12] Bannai E, Ito T. Regular graphs with excess one[J]. Discrete Mathematics, 1981, 37(2-3): 147~158.

[13] Kurosawa K, Tsujii S. Considerations on diameter of communication networks[J]. Electronics & Communications in Japan, 1981, 64(4).

[14] Elspas B. Topological constraints on interconnection-limited logic[C]//5th Annual Symposium on Switching Circuit Theory and Logical Design, Princeton, New Jersey, USA, November 11-13, 1964. IEEE Computer Society, 1964: 133~137.

[15] Bermond J, Delorme C, Farhi G. Large graphs with given degree and diameter. II[J]. Journal of Combinatorial Theory, Series B, 1984, 36(1): 32~48.

[16] Sirán J, Siagiová J, Ždímalová M. Large graphs of diameter two and given degree[J]. In Proc. IWONT 2010, 2011: 379~382.

[17] Pott A, Zhou Y. Cayley graphs of diameter two from difference sets[J]. Journal of graph theory, 2015, 85(2).

[18] Zhang T, Ge G. Improved lower bounds on the degree–diameter problem[J]. Journal of Algebraic Combinatorics, 2019, 49(3): 1~12.

[19] Golomb S W, Welch L R. Perfect codes in the Lee metric and the packing of polyominoes[J]. SIAM Journal on Applied Mathematics, 1970, 18: 302~317.

[20] Horák P, Grosek O. A new approach towards the Golomb-Welch conjecture[J]. European Journal of Combinatorics, 2014, 38: 12~22.

[21] Zhang T, Ge G. Perfect and Quasi-Perfect Codes Under the l_p Metric[J]. IEEE Transactions on Information Theory, 2017, 63(7): 4325~4331.

[22] Post K A. Nonexistence theorems on perfect Lee codes over large alphabets[J]. Information & Control, 1975, 29(4): 369~380.

[23] Lepistö T. A modification of the elias-bound and nonexistence theorems for perfect codes in the Lee-metric[J]. Information & Control, 1981, 49(2): 109~124.

[24] Horak P. On perfect Lee codes - ScienceDirect[J]. Discrete Mathematics, 2009, 309(18): 5551~5561.

[25] Horak P. Tilings in Lee metric[J]. European Journal of Combinatorics, 2009, 30(2): 480~489.

[26] Špacapan S. Nonexistence of face-to-face four-dimensional tilings in the Lee metric[J]. European Journal of Combinatorics, 2007, 28(1): 127~133.

[27] Gravier S, Mollard M, Payan C. On the Non-existence of 3-Dimensional Tiling in the Lee Metric[J]. European Journal of Combinatorics, 1998, 19(5): 567~572.

[28] Kim D. Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions[J]. European Journal of Combinatorics, 2017, 63: 1~5.

[29] Qureshi C. On the non-existence of linear perfect Lee codes: The Zhang-Ge condition and a new polynomial criterion[J]. European Journal of Combinatorics, 2020, 83.

[30] Zhang T, Zhou Y. On the nonexistence of lattice tilings of $\mathbb{Z}^n$ by Lee spheres[J]. Journal of Combinatorial Theory, Series A, 2019, 165: 225~257.

[31] Horák P, AlBdaiwi B F. Diameter Perfect Lee Codes[J]. IEEE Transactions on Information Theory, 2012, 58(8): 5490~5499.

[32] Beth T, Jungnickel D, Lenz H. Design Theory. Vol. I.[J]. Cambridge University Press Cambridge, Mar.1999.

[33] Pott A. Finite Geometry and Character Theory[M]. Springer Verlag, Berlin, 1995.

[34] Weiss E. Algebraic number theory[M]. unabridged. Mineola, N.Y.: Dover Publications, Jan.1998.

[35] Bosma W, Cannon J, Playoust C. The Magma Algebra System I: The User Language[J]. Journal of Symbolic Computation, 1997.

[36] Van Lint J H. Introduction to special section on coding theory[J]. IEEE Transactions on Information Theory, 1988, 34(5): 1274~1275.

[37] Huffman W C, Pless V. Fundamentals of Error-Correcting Codes[M]. Cambridge University Press, 2003.

[38] Qureshi C M. On the non-existence of linear perfect Lee codes: The Zhang-Ge condition and a new polynomial criterion[J]. European Journal of Combinatorics, 2020, 83.

作者在学期间取得的学术成果

发表的学术论文

[1] He W. On the non-existence of Abelian Moore Cayley graphs with excess one. Discrete Mathematics Letters, 2021, (7):58-65.

已投稿的学术论文

[1] He W, Zhou Y. On abelian Cayley graphs of diameter two and defect one. Submitted to Journal of Algebraic Combinatorics.