分类号：O157.2　　单位代码：10335

学　　号：11106053

浙江大学

博士学位论文

中文论文题目：组合构型、格镶嵌及其在信息科学中的应用

英文论文题目：**Combinatorial configurations, lattice tilings and their applications in information science**

申请人姓名：张韬

指导教师：葛根年　教授

专业名称：应用数学

研究方向：组合数学与编码理论

所在学院：数学科学学院

论文提交日期　2017年3月30日

组合构型、格镶嵌
及其在信息科学中的应用

论文作者签名： _____

指导教师签名： _____

论文评阅人1：_____

评阅人2：_____

评阅人3：_____

评阅人4：_____

评阅人5：_____

答辩委员会主席：范更华　教授　福州大学

委员1：范更华　教授　福州大学

委员2：宗传明　教授　天津大学

委员3：符方伟　教授　南开大学

委员4：吴佃华　教授　广西师范大学

委员5：葛根年　教授　浙江大学

答辩日期：2017年5月19日

Combinatorial configurations, lattice tilings

and their applications in information science

Author's signature: _____

Supervisor's signature: _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committee Chairperson:

Prof. Genghua Fan, Fuzhou University

Examining Committee Members:

Prof. Genghua Fan, Fuzhou University

Prof. Chuanming Zong, Tianjin University

Prof. Fangwei Fu, Nankai University

Prof. Dianhua Wu, Guangxi Normal University

Prof. Gennian Ge, Zhejiang University

Date of oral defence: May 19th, 2017

浙江大学研究生学位论文独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。除了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或撰写过的研究成果，也不包含为获得浙江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。

学位论文作者签名：　　签字日期： 2017 年 5 月 19 日

学位论文版权使用授权书

本学位论文作者完全了解浙江大学有权保留并向国家有关部门或机构送交本论文的复印件和磁盘，允许论文被查阅和借阅。本人授权浙江大学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和传播，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：　　导师签名：

签字日期： 2017 年 5 月 19 日　　签字日期： 2017 年 5 月 19 日

致　　谢

首先我要感谢我的导师葛根年教授。自我进入浙江大学读博以来，葛老师在科研和生活上都给与了我很多的指导和建议。葛老师鼓励我去开阔视野，将研究主题扩展到更广的方向上，这极大地培养了我的独立科研能力。葛老师精深的理论知识，广阔的学科视野，严谨的治学态度更是为我树立了榜样，而这将使我终身受益。

其次我要感谢浙江大学的冯涛博士。冯老师在科研上给予了我很多具体的指导，让我学会了如何做科研。

另外我还要感谢这五年中在学习和生活上给予过我指导的各位老师，特别是特拉华大学的向青教授和清华大学的冯克勤教授。在他们到浙江大学访问和教学期间，我从他们那里学到了许多的新课题和新方法。

感谢我的同门对我的帮助和照顾。

感谢我的家人。

由于作者水平有限，加之时间和篇幅所限，文中难免有谬误和不详之处，敬请各位专家学者不吝批评指正！

摘　　要

本学位论文涉及了代数编码，代数组合，格镶嵌中的若干问题及其在信息论中的应用。本文的主旨是利用组合观点，应用抽象代数，代数数论和特征理论来研究这些问题。

在第2 章，我们考虑了两种形状的镶嵌问题。其中一个是十字形，半十字形和准十字形。由于一些物理原因，闪存在电荷写入与电荷擦除这两个过程中的不对称性导致了某个特定区块会产生显著的错误。这种错误让我们有理由去把有限量级错误模型应用到闪存上，而有限量级纠错码等价于十字形，半十字形和准十字形的镶嵌问题。对于这一问题，我们推广了原来绝大部分的构造，给出了一类准完美码的构造。同时，我们还给了一个一般的完美码的构造，得到了一些新的完美码。另外，我们还证明了一些完美码的不存在性结果。特别地，我们完全解决了Schwartz (European J. Combin., vol. 36, pp.130-142, Feb. 2014) 留下来的问题。另一个是在l_p 度量下的球。在1970 年，Golomb 和Welch 给了一个著名的猜想：当$n \geq 3$，$r > 1$，不存在长为n 半径为r 的完美Lee 码。我们证明了一些在l_p 度量下的完美码的不存在性结果。特别地，我们的结果进一步证实了Golomb-Welch 猜想。另一方面，由于大家都相信Golomb-Welch 猜想是对的，那么构造接近完美的码就有意义了，我们给出了一个准完美l_p 码的代数构造。

在第3 章，我们考虑自正交码及其在量子码中的应用。自对偶码是一类特殊的自正交码，它是线性码中最重要的一类码字，和很多其他领域有重要的联系，比如：格，设计，射影平面和不变理论。一般来说，构造极小距离相对较大的自对偶码是困难的。我们利用双循环构型和四次剩余构造了几类新的自对偶码，它们是二次双循环自对偶码的推广。数据说明我们的码比之前已知的最好码的参数要好。量子码主要用于在量子计算和量子通信中保护量子信息的脱散。构造量子码的一个有力方法是通过经典自正交码。我们利用常循环码，广义Reed-Solomon 码构造了几类新的量子极大距离可分码。同时，利用一些多项式，我们给出了一类经典线性码的构造。通过这些线性码，我们得到了一些比已知结果参数更好的量子码。

在第4 章，我们考虑了两个其他与信息论相关的问题。一个是半正则相对差集。由于与两两无偏基的联系，半正则相对差集最近被广泛研究。半正则相对差集的研究主要

集中在差集的存在性问题上。目前有大量的结果是关于(p^a, p^b, p^a, p^{a-b}) 相对差集，其中p是一个素数；然而只有很少的结果是关于(mn, n, mn, m) 相对差集，其中gcd$(m, n) = 1$。当gcd$(m, n) = 1$ 时，(mn, n, mn, m) 相对差集的不存在性只在下面5 种情形被考虑过：(1) $m = p$, $n = q$, $p > q$；(2) $m = pq$, $n = 3$, $p, q > 3$；(3) $m = 4$, $n = p$；(4) $m = 2$ 和(5) $n = p$，其中p，q 是不同的奇素数。对于存在性结果，当群的大小不是素数幂且禁止子群的大小大于2 时，有关半正则相对差集的构造只有4 类。本文给出了一些新的(mn, n, mn, m)相对差集的不存在性结果，其中gcd$(m, n) = 1$。特别地，我们的结果是Hiramine 工作(J. Combin. Theory Ser. A, 117(7):996–1003, 2010) 的一个推广。另外，我们还给出了一类非交换$(16q, q, 16q, 16)$ 相对差集的构造，其中q 是一个素数幂，$q \equiv 1 \pmod 4$ 和$q > 4.2 \times 10^8$。另一个是Grassmannian 填充。在1996 年，Conway，Hardin 和Sloane 提出了$\mathbb{R}^m$ 上的n 维子空间的填充问题。该问题的目标是寻找一个n 维子空间集合，使得它们两两之间离得尽可能地远。这个问题可以看成是球码或者等角线问题的推广。我们利用差集和拉丁方给出了三类最优Grassmannian 填充。

在第5 章中对其他工作做了简要汇报。

关键词： 完美码，闪存，自对偶码，量子码，半正则相对差集，Grassmannian 填充

Abstract

This thesis involves various problems in the area of algebraic coding theory, algebraic combinatorics, lattice tilings and their applications in information theory. This dissertation aims to investigate these problems via a combinatorial perspective, with applications of tools from abstract algebra, algebraic number theory and character theory.

In Chapter 2, two special shapes for tilings are considered. One includes the cross, semi-cross and quasi-cross. Some physical effects that limit the reliability and performance of multilevel flash memories induce errors that have low magnitudes and are dominantly asymmetric. This motivated the application of the asymmetric limited magnitude error model in flash memory, and the asymmetric limited magnitude codes are equivalent to the lattice tiling problems by cross, semi-cross and quasi-cross. For this problem, we present a new construction of quasi-perfect codes, which generalizes most of the previously known constructions. We also give a new general construction of perfect codes, and obtain some new parameters of perfect codes. Meanwhile, we prove some nonexistence results for perfect codes. In particular, we have completely solved the problems left by Schwartz (European J. Combin., vol. 36, pp.130-142, Feb. 2014). The other is the sphere under l_p metric. In 1970, Golomb and Welch posed the long standing conjecture which states that there is no perfect r error correcting Lee codes of length n for $n \geq 3$ and $r > 1$. We prove some nonexistence results for perfect codes in $\mathbb{Z}^n$ under the l_p metric. In particular, our results further substantiate the Golomb-Welch conjecture. Since it is widely believed that the Golomb-Welch conjecture is true, constructing codes close to perfect makes sense. We then give an algebraic construction of quasi-perfect l_p codes.

In Chapter 3, we consider the theory of self-orthogonal codes and their applications in quantum codes. Self-dual codes are special classes of self-orthogonal codes, and they are one of the most interesting classes of linear codes, since they have strong connections with several other areas including lattices, designs, projective planes and invariant theory. Generally, it is hard to construct self-dual codes with relatively large minimum distance. We construct several classes of self-dual

codes by using double circulant configuration and fourth power residues, which are a generalization of the quadratic double circulant self-dual codes. Numerical experiments show that some of our codes have better parameters than previously known codes. Quantum codes were introduced to protect quantum information from decoherence during quantum computations and quantum communications. A powerful construction of quantum codes is employing classical codes with certain self-orthogonality. We use classical constacyclic codes and generalized Reed-Solomon codes to construct several classes of quantum MDS codes. We also present a construction of classical linear codes based on certain classes of polynomials. Through these classical linear codes, we obtain some new quantum codes which have better parameters than the ones available in the literature.

In Chapter 4, we consider two other problems related to information theory. One is semi-regular relative difference sets. Semi-regular relative difference sets have been extensively studied due to their close connections with mutually unbiased bases. The research is concentrated on two aspects — non-existence and existence results. There has been much research on (p^a, p^b, p^a, p^{a-b}) relative difference sets with p a prime, while there are only a few results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$. The nonexistence results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$ have only been obtained for the following five cases: (1) $m = p,\ n = q,\ p > q$; (2) $m = pq,\ n = 3,\ p, q > 3$; (3) $m = 4,\ n = p$; (4) $m = 2$ and (5) $n = p$, where p, q are distinct odd primes. For the existence results, there are only four constructions of semi-regular relative difference sets in groups of size not a prime power with the forbidden subgroup having size larger than 2. We present some more non-existence results on (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$. In particular, our result is a generalization of the main result of Hiramine's work (J. Combin. Theory Ser. A, 117(7):996–1003, 2010). Meanwhile, we give a construction of non-abelian $(16q, q, 16q, 16)$ relative difference sets, where q is a prime power with $q \equiv 1 \pmod 4$ and $q > 4.2 \times 10^8$. The other is Grassmannian packings. The problem of packing n-dimensional subspaces of $\mathbb{R}^m$ was introduced by Conway, Hardin and Sloane in 1996. The goal is to find a set of n-dimensional subspaces such that they are as far apart as possible. It can be seen as a generalization of the problem of spherical codes or equiangular lines. We present three constructions of optimal packings in Grassmannian spaces from difference sets and latin squares.

In Section 5, we briefly introduce some other works.

Keywords: Perfect code, flash memory, self-dual code, quantum code, semi-regular relative difference set, Grassmannian packing

表　格

目　　次

1 绪论

1.1 镶嵌及其在信息论中的应用

设V 是$\mathbb{Z}^n$ 的一个子集，V 的一个平移是$V+x=\{v+x : v\in V\}$。如果$\mathfrak{T}=\{V+l : l\in L\}$, $L\subseteq\mathbb{Z}^n$ 形成$\mathbb{Z}^n$ 的一个分割，那么我们称$\mathfrak{T}$ 是$\mathbb{Z}^n$ 的一个镶嵌。如果L 还是一个格，我们则称$\mathfrak{T}$是一个格镶嵌。在第2章，我们将研究两种形状的镶嵌。一种是十字形，半十字形和准十字形，另一种是Lee 球。

设m,k_1,k_2 为满足$0\le k_1\le k_2$ 的整数。如果大小为n的集合$B\subseteq\mathbb{Z}_m$满足：所有的集合

$$\{ab \pmod m : a\in[-k_1,k_2]^*\},\ b\in B,$$

有k_1+k_2 个非零元，且它们两两不交，我们则称B是一个分解集。我们记这样的分解集为$B[-k_1,k_2](m)$集。一个$B[-k_1,k_2](m)$ 集称为完美的，如果$n=\frac{m-1}{k_1+k_2}$。如果$q\not\equiv 1 \pmod{k_1+k_2}$ 且$n=\lfloor\frac{q-1}{k_1+k_2}\rfloor$，则称$B$ 是准完美的。十字形，半十字形和准十字形的格镶嵌存在性问题等价于完美分解集的存在性问题。

另一方面，闪存是一种非易失性存储器，即断电数据也不会丢失。由于它的可靠性，存储密度高且有相对较高的性价比，因而当前越来越被广泛应用于日常生活中。闪存的主要缺点是其固有的电荷写入与电荷擦除这两个过程的不对称性。写入电荷的过程可以在单个存储单元上进行，但是如果想擦除一个存储单元上的电荷的话，需要对其所在的整个区块进行电荷擦除才行。这个不对称性导致在某个特定的区块上产生显著的错误。并且，报告显示一般闪存错误的量级较小且与字母集的大小无关，但错误会显著大于经典错误量级。因此，我们有理由去把有限量级错误模型应用到闪存上，而利用分解集可以构造有限量级错误码。在这里，利用一个分解集$B[-k_1,k_2](n)$得到的码可以纠正符号$a\in\{0,1,\ldots,n-1\}$ 在传输中变成$a+e$的错，其中$-k_1\le e\le k_2$。

在分解集问题上。首先，利用分圆的思想，我们给出了下面的准完美分解集的构造。

定理1.1. 设p 是一个素数，k_1,k_2,t 是满足$0\le k_1\le k_2$，$t|\gcd(k_1,k_2)$ 和$\frac{k_1+k_2}{t}|(p-1)$ 的整数。对于$0\le i\le t-1$，设$T_i=\{x|x\equiv i \pmod t,\ x\in[-k_1,k_2]^*\}$，则$|T_i|=\frac{k_1+k_2}{t}$。设$g$ 是模p 原

根且$g \equiv 1 \pmod{t}$，设$\theta = \gcd\{\mathrm{ind}_g(k) \mid k \in [-k_1, k_2]^*\}$。如果对于$0 \le i \le t-1$，

$$|\{\frac{\mathrm{ind}_g(k)}{\theta} \pmod{\frac{k_1+k_2}{t}} \mid k \in T_i\}| = \frac{k_1+k_2}{t}$$

且v是满足$v|\theta$，$\frac{v(k_1+k_2)}{t}|(p-1)$以及$\gcd(\frac{\theta}{v}, \frac{k_1+k_2}{t}) = 1$的正整数，则

$$\left\{ g^{\frac{v(k_1+k_2)}{t}i+j} \pmod{tp} \mid i \in [0, \frac{t(p-1)}{v(k_1+k_2)} - 1],\ j \in [0, v-1] \right\}$$

是一个准完美$B[-k_1, k_2](tp)$集。特别地，如果$t = 1$，则上面的集合是完美$B[-k_1, k_2](p)$集。

同时，我们还给出了一些非奇异完美分解集的不存在性结果。这部分工作已经发表在《IEEE Transactions on Information Theory》。

其次，我们给出了下面的完美分解集的构造，我们的构造推广了目前已知的绝大部分构造。

定理1.2. 设$p = (k_1+k_2)nm+1$是一个素数以及g是模p原根。设

$$A = \{ind_g(i) \pmod{(k_1+k_2)n} : i \in [-k_1, k_2]^*\}.$$

如果存在一个大小为n的子集$A' \subseteq \mathbb{Z}_{(k_1+k_2)n}$满足$\mathbb{Z}_{(k_1+k_2)n} = A + A'$是一个1-折叠分解，则存在一个完美$B[-k_1, k_2](p)$集。

定理1.3. 设$p = 2knm+1$是一个素数且g是模p原根。设

$$A = \{ind_g(i) \pmod{kn} : i \in [1, k]\}.$$

如果存在一个大小为n的子集$A' \subseteq \mathbb{Z}_{kn}$满足$\mathbb{Z}_{kn} = A + A'$是一个1-折叠分解，则存在一个完美$B[-k, k](p)$集。

我们还继续研究了非奇异完美分解集的不存在性问题，解决了非奇异完美$B[-1, 3](m)$集在文献[134]中遗留下来的问题。我们还给出了一个分解集在冲突避免码上的应用。这部分工作已经被《IEEE Transactions on Information Theory》接收。

最后，注意到非奇异完美分解集与群的1-折叠分解之间的联系。我们完全解决了当k_1+k_2为奇数时，非奇异完美$B[-k_1, k_2](m)$集的存在性问题。即证明了

定理1.4. 当$1 \le k_1 < k_2$和k_1+k_2是奇数时，不存在非奇异完美分解集。

当k_1+k_2为偶数时，我们给出了非奇异完美$B[-k_1,k_2](m)$集存在的一些必要条件。我们还初步地研究了奇异完美$B[-k_1,k_2](m)$集的存在性问题。这部分工作已经投稿到《IEEE Transactions on Information Theory》。

在Lee 球的镶嵌问题上。Golomb 和Welch 猜想在Lee 范数下的完美码只存在于下列情况：球半径$r=1$ 或者Lee空间的维数$n=1,2$。在这个问题上，我们证明了下面的结果。

定理1.5. 设$r\le n$，$p_{n,r}=\sum_{t=1}^{r}2^t\sum_{j=1}^{r-t+1}j^2\binom{r-j}{t-1}\binom{n-1}{t-1}$，$k_{n,r}=|B_1^n(r)|=\sum_{i=0}^{min\{n,r\}}2^i\binom{n}{i}\binom{r}{i}$。如果$k_{n,r}\equiv 3$ 或$6\pmod 9$，$p_{n,r}\equiv 0\pmod 3$ 以及$k_{n,r}$ 无平方因子，则不存在一个线性完美(n,r) *Lee* 码。

由于大家都认为Golomb-Welch 猜想是对的，那么去构造接近完美的码就有意义了。我们给出了一个准完美l_p 码的代数构造，其中$p=1,r=2$ 以及$2\le p<\infty,r=2^{1/p}$。这部分工作已经被《IEEE Transactions on Information Theory》接收。

1.2 自正交码及其在量子码中的应用

自对偶码是线性码中最重要的一类码，它和很多其他领域有重要的联系，比如：格，设计，射影平面和不变理论。另一个有意思的码是高次剩余码，一般来说，它的码率比较大，极小距离比较大且有有效的译码方法。我们结合这两种码，利用双循环构型和四次剩余构造了几类自对偶码，它们是二次双循环自对偶码的推广。另外，数据表明我们构造的码比之前已知的最好码的参数要好。这部分工作已经发表在《IEEE Transactions on Information Theory》。

量子码在量子计算和量子通信中有重要的应用。自从Calderbank 等人发现可以利用$\mathbb{F}_2$ 或$\mathbb{F}_4$ 上的经典自正交码来构造量子码以来，很多量子码被构造出来了。下面的定理是最常用的一个量子码构造方法。

定理1.6. ([8] Hermitian 构造) 如果C 是一个满足$C^{\perp H}\subseteq C$ 的$[n,k,d]_{q^2}$ 线性码，则存在一个$[[n,2k-n,\ge d]]_q$ 量子码。

我们首先利用常循环码构造了几类新的量子极大距离可分码。这部分工作已经发表在《IEEE Transactions on Information Theory》。

其次，注意到广义Reed-Solomon 码一定是一个极大距离可分码。我们通过研究它的内

在结构，给出了几类新的量子极大距离可分码。这部分工作已经发表在《Designs, Codes and Cryptography》。

最后，为了改善广义Reed-Solomon 码的码长小于等于q 这一缺点，利用赋值法，可以推广广义Reed-Solomon 码的构造且得到的线性码的参数一般比较好。基于此，我们利用一些特殊的多项式，得到了一些比已知结果参数更好的量子码。这部分工作已经发表在《IEEE Transactions on Information Theory》。

1.3 其他与信息论相关的课题

在第4 章，我们考虑了两个其他与信息论相关的问题。一个是半正则相对差集，另一个是Grassmannian 填充。

设G 是阶为uv 的有限群，且设N 是G 的阶为v 的子群。G的一个大小为k 的子集D 称为是G中相对于N的(u, v, k, λ) 相对差集，如果差$r_1 r_2^{-1}$ 的多重集，其中$r_1, r_2 \in D$，$r_1 \neq r_2$，包含集合$G\backslash N$中每个元素恰好λ 次且不包含N中元素。如果群G 是交换群(非交换群)，则D 称为交换(非交换) 相对差集。如果$k = v\lambda$，则D 称为半正则相对差集。

最近，由于与两两无偏基之间的紧密联系，半正则相对差集被广泛地研究。目前关于(p^a, p^b, p^a, p^{a-b}) 相对差集有很多的研究，然而(mn, n, mn, m) 相对差集研究却比较少，其中gcd$(m, n) = 1$。在第4章，我们首先证明了下面的的不存在性结果。

定理1.7. *设m, n 是满足$gcd(m, n) = 1$ 的整数。如果m, n 满足下面的一个条件：*

1. *$m = 2^l m'$，l 和m' 是奇数，以及2 是模n 自共轭的。*
2. *$m = 2p$，$p = 1$ 或者p 是一个奇素数，以及pn 是模pn 自共轭的。*
3. *m 是一个奇素数且mn 是模mn 自共轭的。*

则在交换群$G = \mathbb{Z}_m \times H$中不存在$(mn, n, mn, m)$ 相对差集，其中H 是阶为n^2 的相对差集。特别地，如果m 是无平方因子的整数，则不存在交换(mn, n, mn, m)-相对差集。

我们还构造了一类非交换$(16q, q, 16q, 16)$ 相对差集，其中q 是一个素数幂满足$q \equiv 1 \pmod 4$ 和$q > 4.2 \times 10^8$。这部分工作已经投稿到《Journal of Algebraic Combinatorics》。

设$\mathbb{F}$ 表示域$\mathbb{R}$ 或者$\mathbb{C}$。$\mathbb{F}^m$中的通过原点的N 条不同线的集合，用等长向量$x_1, \cdots, x_N$ 表示，如果存在$a \in \mathbb{R}$ 使得

$$|\langle x_i, x_j \rangle| = a \text{ 对所有} i \neq j,$$

则集合是一个等角线集合，常数a 表示这些线之间的公共角。由于与量子信息论之间的关系，等角线问题最近得到了大量的关注。等角线问题的主要目的是构造具有较大大小的等角线。在第4章，我们利用直积差集给出一类$\mathbb{C}^d$ 中的大小为$O(d^2)$ 的等角线。

紧接着线，n-维子空间的填充也已被研究[34,42,130]。它的目的是在$\mathbb{F}^m$中找到一个n-维子空间集合$U_1,\ldots,U_N$，使得它们之间两两尽可能地远。这些填充问题在编码理论和量子信息理论都有应用。我们证明了任意的一个差集都可以导出一个单纯型填充。

定理1.8. *如果在群$(G,\cdot)$中存在一个参数为(v,k,λ)的差集D，则在实Grassmannian 空间$G_{\mathbb{R}}(v,k)$ 中存在v 个维数为k 的实子空间形成一个单纯型填充。*

由于差集有很多的构造，我们得到很多新的最优填充无穷类。另外，我们还利用差集给出了文献[21]中的构造一个新解释。同时，我们还利用Latin 方给出了一类最优填充。

定理1.9. *假设在字母集$\{0,1,\cdots,st-1\}$上存在一个阶为st的对称Latin 方L 满足下面的条件：*

(1) *对于$m=0,s,2s,\cdots,s(t-1)$，$L(x,x)=m$ 解的个数是s；*

(2) *对于$m=0,s,2s,\cdots,s(t-1)$，$i=0,1,\cdots,st-1$，设$u(i)$ 是$L(i,u(i))=m$ 的唯一解。则对某个$a|st$，$a\leq s$，我们有$\{(i-u(i)) \pmod{st} : i=0,1,\cdots,st-1\}=\{0,a,\cdots,st-a\}$ 且每个ja $(j=0,1,\cdots,\frac{st}{a}-1)$ 恰出现a 次。*

则在复Grassmannian 空间$G_{\mathbb{C}}(st,\frac{s(t+1)}{2})$ 中，存在t^2个维数为$\frac{s(t+1)}{2}$的复子空间形成一个单纯型填充。

这部分工作已经被《Designs, Codes and Cryptography》接收。

2 镶嵌及其在信息论中的应用

设V 是$\mathbb{Z}^n$ 的一个子集，V 的一个平移是$V+x=\{v+x : v \in V\}$。如果$\mathfrak{T}=\{V+l : l \in L\}$, $L \subseteq \mathbb{Z}^n$ 形成$\mathbb{Z}^n$ 的一个分割，那么我们称$\mathfrak{T}$ 是$\mathbb{Z}^n$ 的一个镶嵌。如果L 还是一个格，我们则称$\mathfrak{T}$是一个格镶嵌。文献[79]中有下面的定理。

定理2.1. *[79] 设$S \subseteq \mathbb{Z}^n$ 使得$|S|=m$。存在一个关于S的$\mathbb{Z}^n$ 格镶嵌当且仅当存在一个阶为m的Abel 群G 和一个同态$\phi : \mathbb{Z}^n \mapsto G$ 使得ϕ 限制在S 上是一个双射。*

因此，一个格镶嵌问题可以转化成一个有限群中的问题。在这一章，我们将学习两种形状的镶嵌。一种是十字形，半十字形和准十字形，基于上面的定理，十字形，半十字形和准十字形镶嵌问题可以转化成分解集问题。我们将在2.1节学习分解集的构造和存在性。另一种是Lee 球，Lee 球镶嵌问题等价于完美Lee 码的存在性。我们将在2.2节学习Lee 码。

2.1 分解集

2.1.1 介绍

闪存是一种非易失性存储器，即断电数据也不会丢失。由于它的可靠性，存储密度高且有相对较高的性价比，因而当前越来越被广泛应用于日常生活中，比如个人计算机，数字音频播放器，移动电话等。

为了测量闪存的存储密度，多层记忆单元被用来增加每个单元的存储比特的数量。因此，每个多层记忆单元存储$\log_2(q)$个比特作为一个大小为q的离散字母集上的一个符号。闪存的主要缺点是其固有的电荷写入与电荷擦除这两个过程的不对称性。写入电荷的过程可以在单个存储单元上进行，但是如果想擦除一个存储单元上的电荷的话，需要对其所在的整个区块进行电荷擦除才行。这个不对称性导致在某个特定的区块上产生显著的错误。并且，报告显示一般闪存错误的量级较小且与字母集的大小无关，但错误会显著大于经典错误量级。因此，我们有理由去把有限量级错误模型应用到闪存上[28,94]。

分解集最早出现在研究格镶嵌的时候[74,142–144,147,148]。由于它们在非易失性编码上的

应用（参见文献[20,46,94–96,133,134,160]），它们又得到了广泛的关注。在这里，利用一个分解集$B[-k_1,k_2](n)$得到的码可以纠正符号$a \in \{0,1,\ldots,n-1\}$ 在传输中变成$a+e$的错，其中$-k_1 \le e \le k_2$。

完美分解集的研究主要包括存在性和不存在性结果。对于存在性，文献[95]给出了一个$k_1 = 0$的完美分解集的构造。在文献[96]中，Kløve 等人给出了一个对于$k_1 = k_2$的完美分解集构造。文献[133,160]研究了对于$1 \le k_1 < k_2$的分解集的构造。对于不存在性结果，Woldar[156]给出了一些对于$k_1 = 0$的纯奇异的完美分解集存在的必要条件。在文献[133,134]中，Schwartz给出了一些对于$1 \le k_1 < k_2$的完美分解集存在的必要条件。

在这部分，我们首先给出一类新的准完美分解集和一些新的完美分解集的构造，我们的构造推广了目前已知的绝大部分构造。对于不存在性，我们完全解决了当k_1+k_2 为奇数时，非奇异完美$B[-k_1,k_2](m)$集的存在性问题。当k_1+k_2为偶数时，我们给出了非奇异完美$B[-k_1,k_2](m)$集存在的一些必要条件。我们还初步地研究了奇异完美$B[-k_1,k_2](m)$集的存在性问题。特别地，我们完全解决了完美$B[-1,3](m)$集在文献[134]中遗留下来的问题。

2.1.2 准备工作

在这个小节，我们给出一些定义和一些定理。下面的定义将在这个部分一直使用。

- 对于一个奇素数p，一个模p原根g，和一个不能被p 整除的整数b ，存在一个唯一的整数$l \in [0,p-2]$ 使得$g^l \equiv b \pmod p$。事实上，它是b 对应于基底g 的指数，并且记作$\mathrm{ind}_g(b)$。
- 对于任意的正整数m，设$\mathbb{Z}_m$ 为模m 整数环且$\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$。
- 设a,b 为满足$a \le b$ 的整数，记

$$[a,b] = \{a, a+1, a+2, \ldots, b\} \text{ 以及}$$
$$[a,b]^* = \{a, a+1, a+2, \ldots, b\} \setminus \{0\}.$$

2.1.2.1 分解集

设m,k_1,k_2 为满足$0 \le k_1 \le k_2$ 的整数。如果大小为n的集合$B \subseteq \mathbb{Z}_m$ 满足：所有的集合

$$\{ab \pmod m : a \in [-k_1,k_2]^*\},\ b \in B,$$

有k_1+k_2 个非零元，且它们两两不交，那么我们称B为一个分解集。我们记这样的分解集为$B[-k_1,k_2](m)$集。如果存在一个大小为n 的$B[-k_1,k_2](m)$ 集，则有$n \le \frac{m-1}{k_1+k_2}$。

一个$B[-k_1,k_2](m)$ 集称为完美的，如果$n=\frac{m-1}{k_1+k_2}$。显然，一个完美集只有在$m\equiv 1 \pmod{k_1+k_2}$ 时存在。如果$m\not\equiv 1 \pmod{k_1+k_2}$ 且$n=\lfloor\frac{m-1}{k_1+k_2}\rfloor$，则称$B$ 是准完美的。

一个完美$B[-k_1,k_2](m)$ 集称为非奇异的 如果$\gcd(m,k_2!)=1$。否则的话，集合称为奇异的。如果对于任意的素数$p|m$，存在某个满足$0<k\leq k_2$的整数k 使得$p|k$，则完美$B[-k_1,k_2](m)$ 集称为纯奇异的。文献[73]中证明了，研究完美分解集只需研究非奇异完美分解集和纯奇异完美分解集。

我们将用到下面两个完美分解集的构造。

定理2.2. [134] 如果存在一个完美$B[-k_1,k_2](m)$ 集和某个正整数$d|m$，$\gcd(d,k_2!)=1$，则$(k_1+k_2)d|(m-d)$，且存在一个完美$B[-k_1,k_2](m/d)$ 集。

定理2.3. [160] 设B_1 是一个$B[-k_1,k_2](m_1)$ 集和B_2 是一个$B[-k_1,k_2](m_2)$ 集，其中$\gcd(m_2,k_2!)=1$。设

$$B_1\odot B_2=\{c+rm_1 : c\in B_1, r\in[0,m_2-1]\}\cup\{m_1c : c\in B_2\}.$$

则

1. $B_1\odot B_2$ 是一个$B[-k_1,k_2](m_1m_2)$ 集；
2. $|B_1\odot B_2|=m_2|B_1|+|B_2|$；
3. 如果B_1 和B_2 都是完美的，则$B_1\odot B_2$ 是完美的。

根据上面两个定理，容易看出存在一个非奇异完美$B[-k_1,k_2](m)$ 集当且仅当对任意整除m的素数p，存在一个非奇异完美$B[-k_1,k_2](p)$集。

下面的引理是文献[73]中定理1.2.1的特殊情形。

引理2.4. [73] 如果$m|n$ 且存在一个完美$B[-k_1,k_2](m)$ 和一个完美$B[-k_1,k_2](n)$ 集，则存在一个完美$B[-k_1,k_2](n/m)$ 集。

2.1.2.2 群的1-折叠分解

设G 是一个有限群且设A 和B 为G 的子集，如果对于G中任意元素g，存在唯一的元素$a\in A$ 和$b\in B$ 使得$g=a+b$，则我们称$G=A+B$ 是群G 的一个1-折叠分解。

一个子集$A\subseteq\mathbb{Z}_m$ 称为是周期的，如果稳定集$N(A)=\{g\in\mathbb{Z}_m : A+g=A\}$ 是$\mathbb{Z}_m$ 的一个非平凡子群。我们需要文献[149]中的下面两个引理。

引理2.5. [149] 如果$G = A + B$是一个1-折叠分解且$gcd(k, |A|) = 1$，则$G = kA + B$是一个1-折叠分解。

引理2.6. [149] 假设$\mathbb{Z}_n = A + B$是一个1-折叠分解。如果

1. $|A|$是一个素数幂，或者
2. n是下面某个数的因子：$u^e v,\ u^2v^2,\ u^2vw,\ uvwz$，其中$u, v, w, z$是素数和$e$是正整数，

则A或B是周期的。

我们有下面的引理。

引理2.7. 假设$\mathbb{Z}_m = A + B$是一个1-折叠分解。如果$|A| = q$是一个素数幂，则存在某个$l|\frac{m}{q}$使得$A \pmod{lq}$是$\mathbb{Z}_{lq}$中大小为q的周期子集。

证明. 设$n = \frac{m}{q}$，我们对n的因子用归纳法。

如果A是$\mathbb{Z}_{nq}$中的周期子集，则证明结束。否则，由于$|A|$是素数幂，根据引理2.6，B在$\mathbb{Z}_{nq}$中是周期的。则存在一个元素$e \in \mathbb{Z}_{nq}^*$使得$B + e = B$，因此B是$\langle e\rangle$的一些陪集的并，其中$\langle e\rangle$是$\mathbb{Z}_{nq}$中由e生成的子群。我们可以把B写作$B = \langle e\rangle + C$，其中C是陪集代表元，则$\mathbb{Z}_{nq} = A + \langle e\rangle + C$。假设$|\langle e\rangle| = s$，由于$s|C| = n$，我们有$s|n$。则$\mathbb{Z}_{\frac{n}{s}q} = A + C$，这里集合$A$和$C$是模$\frac{n}{s}q$的。如果$A$在$\mathbb{Z}_{\frac{n}{s}q}$是周期的，则我们只需取$l = \frac{n}{s}$。否则的话，我们重复上面的步骤直到停止。由于$n$有限，存在$l|n$使得$A \pmod{lq}$是$\mathbb{Z}_{lq}$中大小为$q$的周期子集。

□

2.1.3 分解集的构造

2.1.3.1 准完美分解集

下面的构造是对文献[160]中构造的推广且证明是类似的。为读者方便，我们给出证明。

定理2.8. 设p是一个素数，k_1, k_2, t是满足$0 \le k_1 \le k_2$，$t|\gcd(k_1, k_2)$和$\frac{k_1+k_2}{t}|(p-1)$的整数。对于$0 \le i \le t-1$，设$T_i = \{x|x \equiv i \pmod{t},\ x \in [-k_1, k_2]^*\}$，则$|T_i| = \frac{k_1+k_2}{t}$。设$g$是模$p$原

根且$g \equiv 1 \pmod{t}$，设$\theta = \gcd\{\mathrm{ind}_g(k) \mid k \in [-k_1, k_2]^*\}$。如果对于$0 \le i \le t-1$，

$$|\{\frac{\mathrm{ind}_g(k)}{\theta} \pmod{\frac{k_1+k_2}{t}} \mid k \in T_i\}| = \frac{k_1+k_2}{t}$$

且v 是满足$v|\theta$，$\frac{v(k_1+k_2)}{t}|(p-1)$ 以及$\gcd(\frac{\theta}{v}, \frac{k_1+k_2}{t}) = 1$ 的正整数，则

$$\left\{g^{\frac{v(k_1+k_2)}{t}i+j} \pmod{tp} \mid i \in [0, \frac{t(p-1)}{v(k_1+k_2)} - 1],\ j \in [0, v-1]\right\}$$

是一个准完美$B[-k_1, k_2](tp)$ 集。特别地，如果$t = 1$，则上面的集合是完美$B[-k_1, k_2](p)$ 集。

证明. 假设

$$rg^{\frac{v(k_1+k_2)}{t}i_1+j_1} \equiv sg^{\frac{v(k_1+k_2)}{t}i_2+j_2} \pmod{tp},$$

其中$r, s \in [-k_1, k_2]^*$, $i_1, i_2 \in [0, \frac{t(p-1)}{v(k_1+k_2)} - 1]$ 和$j_1, j_2 \in [0, v-1]$。注意到$g \equiv 1 \pmod{t}$，我们有$r \equiv s \pmod{t}$，因此存在$0 \le l \le t-1$ 使得$r, s \in T_l$ 。

由于

$$rg^{\frac{v(k_1+k_2)}{t}i_1+j_1} \equiv sg^{\frac{v(k_1+k_2)}{t}i_2+j_2} \pmod{p},$$

我们有

$$\mathrm{ind}_g(r) + \frac{v(k_1+k_2)}{t}i_1 + j_1 \equiv \mathrm{ind}_g(s) + \frac{v(k_1+k_2)}{t}i_2 + j_2 \pmod{p-1}.$$

对上式模v，我们得到

$$j_1 \equiv j_2 \pmod{v},$$

由于$j_1, j_2 \in [0, v-1]$，从而$j_1 = j_2$ 。因此，我们有

$$\mathrm{ind}_g(r) \equiv \mathrm{ind}_g(s) \pmod{\frac{v(k_1+k_2)}{t}}$$

且

$$\frac{\mathrm{ind}_g(r)}{v} \equiv \frac{\mathrm{ind}_g(s)}{v} \pmod{\frac{(k_1+k_2)}{t}}.$$

注意到$\gcd(\frac{\theta}{v}, \frac{k_1+k_2}{t}) = 1$，我们有$r = s$，且$i_1 = i_2$。 □

下面，我们举一些例子。

例2.9. 设$p = 73$，$k_1 = 2$，$k_2 = 2$ 和$t = 2$。则$g = 5$ 是模p 原根。计算可得$\mathrm{ind}_g(1) = 0$，$\mathrm{ind}_g(2) = 8$，$\mathrm{ind}_g(-1) = 36$ 和$\mathrm{ind}_g(-2) = 44$。因此$\theta = 4$ 且我们有

$$\frac{\mathrm{ind}_g(-1)}{4} \equiv 1 \pmod{2},\ \frac{\mathrm{ind}_g(1)}{4} \equiv 0 \pmod{2},$$

和

$$\frac{\text{ind}_g(-2)}{4} \equiv 1 \pmod 2,\ \frac{\text{ind}_g(2)}{4} \equiv 0 \pmod 2.$$

则在定理2.8中取$v=4$，集合

$$\{5^{8i+j} \pmod{146} \mid i \in [0,8],\ j \in [0,3]\}$$

是一个准完美$B[-2,2](146)$集。

例2.10. 设$p=557$，$k_1=2$，$k_2=6$和$t=2$。则$g=3$是模p原根。计算可得$\text{ind}_g(1)=0$，$\text{ind}_g(2)=363$，$\text{ind}_g(3)=1$，$\text{ind}_g(4)=170$，$\text{ind}_g(5)=207$，$\text{ind}_g(6)=364$，$\text{ind}_g(-1)=278$和$\text{ind}_g(-2)=85$。因此$\theta=1$且我们有

$$\text{ind}_g(-1) \equiv 2 \pmod 4,\ \text{ind}_g(1) \equiv 0 \pmod 4,$$

$$\text{ind}_g(3) \equiv 1 \pmod 4,\ \text{ind}_g(5) \equiv 3 \pmod 4,$$

和

$$\text{ind}_g(-2) \equiv 1 \pmod 4,\ \text{ind}_g(2) \equiv 3 \pmod 4,$$

$$\text{ind}_g(4) \equiv 2 \pmod 4,\ \text{ind}_g(6) \equiv 0 \pmod 4.$$

则在定理2.8中取$v=1$，集合

$$\{3^{4i} \pmod{1114} \mid i \in [0,138]\}$$

是准完美$B[-2,6](1114)$集。

表2-1 列出了一些满足定理2.8 条件的参数。从数据来看，当$\frac{k_1+k_2}{t}$ 是偶数时，有无穷多个素数p 满足定理2.8的条件。

我们还发现当$0<k_1\le k_2$，$k_1+k_2\le 12$，$t|\gcd(k_1,k_2)$ 和$\frac{k_1+k_2}{t}$ 是奇数时，对任意的素数$p\le 5000$ 均不满足定理2.8 的条件。因此我们给出下面的猜想。

猜想2.11. 设p 是素数，k_1,k_2,t 是满足$0<k_1\le k_2$，$t|\gcd(k_1,k_2)$ 和$\frac{k_1+k_2}{t}|(p-1)$ 的整数。对于$0\le i\le t-1$，设$T_i=\{x|x\equiv i \pmod t,\ x\in[-k_1,k_2]^*\}$。设$g$ 是模p 的原根且$g\equiv 1 \pmod t$，设$\theta=\gcd\{\text{ind}_g(k) \mid k\in[-k_1,k_2]^*\}$。如果对于$0\le i\le t-1$，$|\{\frac{\text{ind}_g(k)}{\theta} \pmod{\frac{k_1+k_2}{t}} \mid k\in T_i\}|=\frac{k_1+k_2}{t}$，则$\frac{k_1+k_2}{t}$ 是偶数。

表 2-1　利用定理2.8构造的准完美$B[-k_1,k_2](tp)$ 集，其中$t\geq 2$

k_1	k_2	t	p
2	2	2	$7,11,19,23,31,43,47,59,67,71$
2	6	2	$557,653,677,1373,1733,1877,1997,2237,2693,3413$
4	4	2	$5,29,53,101,149,173,197,269,293,317$
4	8	2	$1171,3511,4003,9319,12907,15031,17851,21787,22051,24223$
3	3	3	$23,31,47,71,79,103,127,151,167,191$
3	9	3	$941,5981,6221,12941,18749,19421,26669,27509,28901,29021$

2.1.3.2　完美分解集

我们首先给出两个简单的一般构造。

定理2.12. 设$p=(k_1+k_2)nm+1$ 是一个素数以及g 是模p 原根。设

$$A=\{ind_g(i) \pmod{(k_1+k_2)n} : i\in[-k_1,k_2]^*\}.$$

如果存在一个大小为n的子集$A'\subseteq\mathbb{Z}_{(k_1+k_2)n}$ 满足$\mathbb{Z}_{(k_1+k_2)n}=A+A'$ 是一个1-折叠分解，则存在一个完美$B[-k_1,k_2](p)$ 集。

证明. 设

$$B=\{g^{b+(k_1+k_2)ni} :\ b\in A',\ i\in[0,m-1]\}.$$

则$|B|=mn$ 且容易看出$B\cdot[-k_1,k_2]^*=\mathbb{Z}_p^*$。因此$B$ 是一个完美$B[-k_1,k_2](p)$ 集。 □

定理2.13. 设$p=2knm+1$ 是一个素数且g 是模p 原根。设

$$A=\{ind_g(i) \pmod{kn} : i\in[1,k]\}.$$

如果存在一个大小为n 的子集$A'\subseteq\mathbb{Z}_{kn}$ 满足$\mathbb{Z}_{kn}=A+A'$ 是一个1-折叠分解，则存在一个完美$B[-k,k](p)$ 集。

证明. 设

$$B = \{g^{b+kni} : b \in A',\ i \in [0, m-1]\}.$$

我们断言B 是一个完美$B[-k,k](p)$ 集。

假设

$$rg^{kni_1+j_1} \equiv sg^{kni_2+j_2} \pmod{p},$$

其中$r, s \in [-k,k]^*$，$i_1, i_2 \in [0, m-1]$ 和$j_1, j_2 \in A'$。则我们有

$$\mathrm{ind}_g(r) + kni_1 + j_1 \equiv \mathrm{ind}_g(s) + kni_2 + j_2 \pmod{p-1}.$$

将上式模kn，我们得到

$$\mathrm{ind}_g(r) + j_1 \equiv \mathrm{ind}_g(s) + j_2 \pmod{kn}.$$

由于$kn|\frac{p-1}{2}$，$j_1, j_2 \in A'$ 和$\mathbb{Z}_{kn} = A + A'$ 是一个1-折叠分解，我们有$j_1 = j_2$ 和$r = s$ 或者$r = -s$。

如果$r = s$，则$i_1 \equiv i_2 \pmod{2m}$ 且$i_1 = i_2$。如果$r = -s$，则$kni_1 \equiv kni_2 + \frac{p-1}{2} \pmod{p-1}$，从而$\frac{p-1}{2}|kn(i_1 - i_2)$ 且$i_1 \neq i_2$。也就是$m|(i_1 - i_2)$ 且$i_1 \neq i_2$，矛盾。 □

评论2.14. *在定理2.12中，如果$A = \{0, n, 2n, \ldots, (k_1+k_2-1)n\}$，为满足1-折叠分解条件，我们可以取$A' = [0, n-1]$。这就是文献[95,160]中的构造。对于定理2.13也是类似的。*

为了得到新的完美分解集，我们定义集合

$$S(2k, 2^{m+1}k) := \{\{0, 2j, 4j, \ldots, 2(k-1)j, 2^m kj, (2^m k+2)j, \ldots, (2^m k+2(k-1))j\} : j \in [1, 2^m k],\ \gcd(j, 2^{m+1}k) = 1\}.$$

引理2.15. *对于任意的$A \in S(2k, 2^{m+1}k)$，存在大小为2^m的集合$A' \subset \mathbb{Z}_{2^{m+1}k}$ 满足$A + A' = \mathbb{Z}_{2^{m+1}k}$ 是一个1-折叠分解。*

证明. 设$A = \{0, 2j, 4j, \ldots, 2(k-1)j, 2^m kj, (2^m k+2)j, \ldots, (2^m k+2(k-1))j\}$，其中$j \in [1, 2^m k]$ 且$\gcd(j, 2^{m+1}k) = 1$。则我们可以取

$$A' = \{2kji_1 + i_2 : i_1 \in [0, 2^{m-1}-1],\ i_2 \in [0,1]\}.$$

□

结合定理2.12，2.13 和引理2.15，我们有下面两个推论。

推论2.16. 设$p = 2^m(k_1 + k_2)n + 1$ 是一个素数，$k_1 + k_2$ 是偶数且g 是模p 的一个原根。如果

$$\{ind_g(i) \pmod{(k_1 + k_2)2^m} : i \in [-k_1, k_2]^*\} \in S(k_1 + k_2, (k_1 + k_2)2^m),$$

则存在一个完美$B[-k_1, k_2](p)$ 集。

表 2-2　利用推论2.16得到的完美$B[-k_1, k_2](p)$ 集的一些例子

k_1	k_2	m	p
1	3	2	$241, 1489, 3793, 17041, 22993, 26161, 33457, 35569, 39313, 45553$
1	3	3	$19681, 29473, 34273, 79777, 88609, 88801, 96097, 97441, 142369, 155809$
1	3	4	$577, 13249, 20161$
1	5	2	34729
2	4	2	$313, 6073, 11497, 12889, 23497, 34057, 36313, 42409, 46633, 49081$
2	4	3	$38449, 77041, 79633$
3	5	2	78241
2	6	3	307009

推论2.17. 设$p = 2^{m+1}kn + 1$ 是一个素数，k 是一个偶数且g 是模p 原根。如果

$$\{ind_g(i) \pmod{2^m k} : i \in [1, k]\} \in S(k, 2^m k),$$

则存在一个完美$B[-k, k](p)$ 集。

表2-2 和2-3 分别列出了一些满足推论2.16 和2.17 中条件的一些参数。结合定理2.3，表2-2 和2-3，我们可以得到无穷多个新的完美分解集。

2.1.4　完美分解集的不存在性结果

在这个小节，我们将给出一些新的非奇异完美分解集和纯奇异完美分解集的不存在性

表 2-3　利用推论2.17得到的完美$B[-k,k](p)$ 集的一些例子

k	m	p
6	2	$134161, 189169$
6	3	86689

结果。

2.1.4.1　非奇异完美分解集

定理2.18. *当$1 \le k_1 < k_2$ 和$k_1 + k_2$ 是奇数时，不存在非奇异完美分解集。*

证明. 根据定理2.2，我们只需证明对于素数$p \equiv 1 \pmod{k_1 + k_2}$，不存在完美分解集$B[-k_1, k_2](p)$。设$g$ 是一个模p本原元。如果存在一个完美$B[-k_1, k_2](p)$ 集B，设$A = \{\mathrm{ind}_g(i) : i \in [-k_1, k_2]^*\}$，$C = \{\mathrm{ind}_g(i) : i \in B\}$，则$\mathbb{Z}_{p-1} = A + C$。由于$|A| = k_1 + k_2$ 是奇数，根据引理2.5，我们有$\mathbb{Z}_{p-1} = 2A + C$。则$|2A| = |A|$。注意到$0, \frac{p-1}{2} \in A$，我们有$|2A| < |A|$，矛盾。 □

对于$k_1 = 0$ 或者$1 \le k_1 \le k_2$ 且$k_1 + k_2$ 是偶数，看起来总是存在某个n，使得存在非奇异完美$B[-k_1, k_2](n)$ 集[95,96,133,160]。接下来，我们将对某些k_1 ，k_2，给出一些非奇异完美$B[-k_1, k_2](n)$ 集存在的条件。

定理2.19. *设k, p 是奇素数，g 是一个模p 本原元以及$\mu = gcd\{ind_g(j) : j \in [-1, k]^*\}$。则存在一个完美$B[-k, k](p)$ 集当且仅当*

$$p \equiv 1 \pmod{2\mu k} \text{ 且} |\{\frac{ind_g(j)}{\mu} \pmod{k} : j \in [1, k]\}| = k.$$

证明. 如果$p \equiv 1 \pmod{2\mu k}$ 且$|\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod{k} : j \in [1, k]\}| = k$，则结果可从文献[96]中得到。

如果B 是一个完美$B[-k, k](p)$ 集，设$A = \{\mathrm{ind}_g(j) : j \in [-k, k]^*\}$，$A' = \{\mathrm{ind}_g(j) : j \in [1, k]\}$ 和$C = \{\mathrm{ind}_g(j) : j \in B\}$。则$\mathbb{Z}_{p-1} = A + C$ 和$A = A' + \{0, \frac{p-1}{2}\}$。因此$\mathbb{Z}_{p-1} = A' + \{0, \frac{p-1}{2}\} + C$。从而$\mathbb{Z}_{\frac{p-1}{2}} = A' + C$。注意到$|A'| = k$ 是一个奇素数，根据引理2.7，存在一个整数l 使得$kl | \frac{p-1}{2}$ 且A' 在$\mathbb{Z}_{kl}$是周期的。由于$\mathrm{ind}_g(1) = 0$，我们有$A' \pmod{kl} = \{il :$

$i \in [0, k-1]\}$。则$l = \mu$，

$$p \equiv 1 \pmod{2\mu k} \text{ 且} |\{\frac{\text{ind}_g(j)}{\mu} \pmod{k} : j \in [1,k]\}| = k.$$

□

类似地，我们有下面的结果。

定理2.20. 设k, p 是奇素数，g 是模p 本原元以及$\mu = gcd\{ind_g(j) : j \in [1,k]\}$。则存在一个完美$B[1,k](p)$ 集当且仅当

$$p \equiv 1 \pmod{\mu k} \text{ 且} |\{\frac{ind_g(j)}{\mu} \pmod{k} : j \in [1,k]\}| = k.$$

评论2.21. 在定理*2.19* 和*2.20*中，数μ 不依赖于g 的选择[95,96]。

下面的定理是对于任意k_1, k_2 的一般结果。

定理2.22. 设p 是一个奇素数，k_1, k_2 是满足$gcd(k_1 + k_2, \frac{p-1}{k_1+k_2}) = 1$ 的整数。设g 是模p 本原元以及$\mu = gcd\{ind_g(j) : j \in [-1, k_2]^*\}$。则存在一个完美$B[-k_1, k_2](p)$ 集当且仅当

$$p \equiv 1 \pmod{\mu(k_1+k_2)} \text{ 且} |\{\frac{ind_g(j)}{\mu} \pmod{k_1+k_2} : j \in [-k_1, k_2]^*\}| = k_1 + k_2.$$

证明. 如果$p \equiv 1 \pmod{\mu(k_1+k_2)}$ 且$|\{\frac{\text{ind}_g(j)}{\mu} \pmod{k_1+k_2} : j \in [-k_1, k_2]^*\}| = k_1 + k_2$，则存在性结果可由文献[95,96,160]得。

如果B 是一个完美$B[-k_1, k_2](p)$ 集，设$A = \{\text{ind}_g(j) : j \in [-k_1, k_2]^*\}$ 和$C = \{\text{ind}_g(j) : j \in B\}$。则$\mathbb{Z}_{p-1} = A + C$。由于$\gcd(k_1 + k_2, \frac{p-1}{k_1+k_2}) = 1$，根据引理2.5，我们有$\mathbb{Z}_{p-1} = \frac{p-1}{k_1+k_2}A + C$，则$|A| = |\frac{p-1}{k_1+k_2}A|$。如果$\gcd(\mu,\ k_1 + k_2) > 1$，则$\frac{p-1}{k_1+k_2}A$ 中所有元素都是$\frac{p-1}{k_1+k_2}\gcd(\mu,\ k_1 + k_2)$ 的倍数。因此

$$|\frac{p-1}{k_1+k_2}A| \le \frac{p-1}{\frac{p-1}{k_1+k_2}\gcd(\mu,\ k_1+k_2)} = \frac{k_1+k_2}{\gcd(\mu,\ k_1+k_2)} < k_1 + k_2 = |A|,$$

矛盾。从而$\gcd(\mu, k_1 + k_2) = 1$。注意到$\mu|(p-1)$，我们有$p \equiv 1 \pmod{\mu(k_1+k_2)}$。

由于$|A| = |\frac{p-1}{k_1+k_2}A|$，则对于任意的$a, b \in A$, $\frac{p-1}{k_1+k_2}a \not\equiv \frac{p-1}{k_1+k_2}b \pmod{p-1}$，也就是$a \not\equiv b \pmod{k_1+k_2}$。由于$\gcd(\mu, k_1+k_2) = 1$，则$\frac{a}{\mu} \not\equiv \frac{b}{\mu} \pmod{k_1+k_2}$。因此我们有

$$|\{\frac{\text{ind}_g(j)}{\mu} \pmod{k_1+k_2} : j \in [-k_1, k_2]^*\}| = k_1 + k_2.$$

□

下面的引理是推导完美$B[-k_1,k_2](p)$集存在性条件的一个有力工具。

引理2.23. 设p是素数，k_1,k_2是满足$1\le k_1\le k_2$的整数，设$M=[-k_1,k_2]^*$。如果B是完美$B[-k_1,k_2](p)$集，则B满足下面的条件：

1. 对于任意的$a\in\mathbb{Z}_p^*$，$|B\cap aM|=1$；

2. 如果$i\in B$，则$-i,\pm 2i,\cdots,\pm k_2 i\notin B$。

证明. 注意到B是完美的当且仅当$|B|(k_1+k_2)=p-1$个乘积$bm,\ b\in B,m\in M$是不同且非零的。

(i) 我们只需证明对每一个$a\in\mathbb{Z}_p^*$存在唯一的一对(b,m)满足$b=am$，其中$b\in B$和$m\in M$。

如果存在$b_1,b_2\in B$，$m_1,m_2\in M$使得$b_1=am_1$和$b_2=am_2$，则$m_2b_1=m_2am_1=m_1b_2$。由于B是完美的，我们断言$b_1=b_2$且$m_1=m_2$。从而我们有唯一性。

对于任意的$b\in B$，$m\in M$，存在一个唯一的$a\in\mathbb{Z}_p^*$使得$b=am$。由于$|B|(k_1+k_2)=p-1$，这证明了对任意的$a\in\mathbb{Z}_p^*$存在唯一一对(b,m)使得$b=am$，其中$b\in B$和$m\in M$。

(ii) 设$i\in B$和$m\in[2,k_2]$，则$m\cdot i=1\cdot(mi)$。根据完美集B的乘积的唯一性，我们断言$mi\notin B$。类似地，对于$i\in B$和$m\in[1,k_2]$，我们有$m\cdot i=(-1)\cdot(-mi)$，因此$-mi\notin B$。

□

下面的两个定理给出了完美$B[-1,3](q)$和$B[-2,4](q)$集存在的一个必要条件。

定理2.24. 设p是形如$4n+1$的素数，设$\langle 4,6\rangle$是$\mathbb{Z}_p^*$中由4和6生成的子群。如果$\langle 4,6\rangle\bigcap\{\pm 2,\pm 3\}\neq\emptyset$，则不存在一个完美$B[-1,3](p)$集。

证明. 设p是形如$4n+1$的素数，B是一个完美$B[-1,3](p)$集和$M=\{-1,1,2,3\}$。设$\pm B=B\cup -B$。假设$1\in B$，则$-1,\pm 2,\pm 3\notin B$，从而$\pm 2,\pm 3\notin\pm B$。如果$r\in B$则$-r,\pm 2r,\pm 3r\notin B$。因此$6r\in B$或者$-6r\in B$。

如果$6r\in B$，计算可得$-4r,-9r\in B$。类似地，如果$-6r\in B$，则$4r,9r\in B$。从而，$\langle 6,4,9\rangle=\langle 6,4\rangle\subseteq\pm B$。因此$\langle 4,6\rangle\cap\{\pm 2,\pm 3\}\subseteq\pm B\cap\{\pm 2,\pm 3\}=\emptyset$，这与我们的假设矛盾。 □

在文献[134]中，作者证明了，对于$q \leq 1000$，除了已知的构造[160]，和除了可能的

$$q = 81, 89, 97, 241, 405, 445, 457, 485, 577, 729, 881, 937, 941,$$

不存在完美$B[-1, 3](q)$集。对于$q = 941$，我们可以通过定理2.8构造完美$B[-1, 3](q)$集。对于剩下的12 个情形，我们可以利用定理2.24排除掉4 个。也就是，我们有下面的推论。

推论2.25. *对于$q \leq 1000$，除了已知的构造[160]，和除了可能的*

$$q = 81, 97, 241, 405, 457, 485, 577, 729,$$

不存在完美$B[-1, 3](q)$ 集。

证明. 我们只需证明对于$q = 89, 445, 881, 937$，不存在完美$B[-1, 3](q)$ 集。

对于$q = 89, 881, 937$，结论直接由定理2.24可得，对于$q = 445 = 5 \times 89$，结论由定理2.24 和2.2可得。 □

定理2.26. *设p 是形如$6n + 1$ 的奇素数，设$\langle 6, 8\rangle$ 是$\mathbb{Z}_p^*$ 中由6 和8 生成的子群。如果$\langle 6, 8\rangle \bigcap \{\pm 2, \pm 3, \pm 4\} \neq \emptyset$，则不存在完美$B[-2, 4](p)$ 集。*

证明. 设p 是形如$6n + 1$ 的素数，B 是一个完美$B[-2, 4](p)$ 集和$M = \{-2, -1, 1, 2, 3, 4\}$。设$\pm B = B \cup -B$。假设$1 \in B$，则$-1, \pm 2, \pm 3, \pm 4 \notin B$ ，以及$\pm 2, \pm 3, \pm 4 \notin \pm B$。如果$r \in B$则$-r, \pm 2r, \pm 3r, \pm 4r \notin B$。根据引理2.23，集合$\{6r, 8r\}$ 中恰好有一个元素包含在B 中且集合$\{-6r, -8r\}$ 中恰好有一个元素包含在B 中。则我们有$\langle 6, 8\rangle \subseteq \pm B$。从而$\langle 6, 8\rangle \bigcap \{\pm 2, \pm 3, \pm 4\} \subseteq \pm B \cap \{\pm 2, \pm 3, \pm 4\} = \emptyset$，这与我们的假设矛盾。 □

根据定理2.26，对于形如$6n + 1$ 以及$p \leq 1000$的素数p，除了已知的构造[160]，和除了可能的

$$p = 37, 181, 241, 313, 337, 349, 409, 421, 541, 877, 919, 937,$$

不存在完美$B[-2, 4](p)$集。

定理2.27. *设$p = (k_1 + k_2)m + 1$ 是一个素数且g 是模p 原根。假设*

1. $k_1 + k_2$ 是素数幂，或者

2. $p-1$ 是下面数的一个因子：$u^e v,\ u^2v^2,\ u^2vw,\ uvwz$，其中$u,v,w,z$ 是素数且e 是正整数。

设$A=\{ind_g(i):\ i\in[-k_1,k_2]^*\}$。如果存在一个完美$B[-k_1,k_2](p)$ 集，则存在$l|m$使得$A \pmod{(k_1+k_2)l}$ 是$\mathbb{Z}_{(k_1+k_2)l}$ 中大小为(k_1+k_2) 的周期子集。

证明. 我们对m 的因子用归纳法。

如果A 在$\mathbb{Z}_{(k_1+k_2)m}$ 是周期的，则证明结束。否则的话，由于存在一个完美$B[-k_1,k_2](p)$集，则存在一个大小为m的集合C 使得$A+C=\mathbb{Z}_{p-1}$。注意到$|A|=k_1+k_2$ 是素数幂或者$p-1$ 是下面数的一个因子：$u^e v,\ u^2v^2,\ u^2vw,\ uvwz$，其中$u,v,w,z$ 是素数且e 是正整数。则根据引理2.6，C 在$\mathbb{Z}_{(k_1+k_2)m}$ 中是周期的。因此存在一个元素$e\in\mathbb{Z}^*_{(k_1+k_2)m}$ 使得$C+e=C$，从而C 是$\langle e\rangle$ 的一些陪集的并，其中$\langle e\rangle$ 是$\mathbb{Z}_{(k_1+k_2)m}$ 中由e 生成的子群。我们可以把C 写成$C=\langle e\rangle+D$，其中D 是陪集代表元。则$\mathbb{Z}_{(k_1+k_2)m}=A+\langle e\rangle+D$。假设$|\langle e\rangle|=s$，由于$s|D|=m$我们有$s|m$。则$\mathbb{Z}_{(k_1+k_2)\frac{m}{s}}=A+D$，其中$A$ 和D 是模$(k_1+k_2)\frac{m}{s}$的。如果A 在$\mathbb{Z}_{(k_1+k_2)\frac{m}{s}}$ 中周期，则我们取$l=\frac{m}{s}$ 即可。否则，我们继续上面的步骤。由于m 是有限的，存在$l|m$ 使得$A \pmod{(k_1+k_2)l}$是$\mathbb{Z}_{(k_1+k_2)l}$ 中大小为(k_1+k_2) 的周期子集。 □

根据定理2.27 和计算机搜索，我们有下面的结果。

定理2.28. *1.* 对于$n=97,457$ 和485，不存在一个完美$B[-1,3](n)$ 集。

2. 对于$n=37,349$ 和877，不存在一个完美$B[-2,4](n)$ 集。

对于完美$B[-1,3](n)$ 集，结合表2-2，推论2.25 和定理2.28，我们完全解决了文献[134]中剩下的非奇异情形。

2.1.4.2 奇异完美分解集

下面的引理是文献[58]中结果的推广且证明是类似的。为读者方便，我们给出证明。

引理2.29. 设k_1,k_2 是整数，$1\le k_1<k_2$，$k_2\ge 3$，$n=k_1+k_2+1$。如果n 不是素数，则不存在一个完美$B[-k_1,k_2](n^2)$ 集。

证明. 假设$\mathbb{Z}^*_{n^2}=[-k_1,k_2]^*S$。$S$ 中与n 互素的元素个数是$\varphi(n^2)/\varphi(n)=n$。因此$S=\{x,a_1,a_2,\cdots,a_n\}$，其中$\gcd(x,n)>1$ 且$\gcd(a_i,n)=1$ 对于$i=1,\cdots,n$。

如果$jn \in \mathbb{Z}_{n^2}^*$，$1 \le j \le n-1$具有形式$ia_k$，其中$i \in [-k_1, k_2]^*$，则$jn \equiv ia_k \pmod{n^2}$。因此$n|i$，与$|i| \le k_2 < n$矛盾。从而$n, 2n, \cdots, (n-1)n$是$-k_1 x \pmod{n^2}, \cdots, -x \pmod{n^2}, x \pmod{n^2}, \cdots, k_2 x \pmod{n^2}$的一个置换。因此存在$1 \le i \le n-1$使得$x = in$。由于存在一个整数$j$，$1 \le j \le n-1$，使得$jin \equiv n \pmod{n^2}$，也就是$ji \equiv 1 \pmod{n}$，我们可以假设$x = n$。因此我们将假设$S = \{n, a_1, a_2, \cdots, a_n\}$。接下来，我们的证明分成三种情况。

情形1: $n = pqm$，**其中**p **和**q **是不同素数，**$p < q$，**且**$m \in \mathbb{Z}$。

设$d = q^2 m$。由于$n \nmid d$，所以$n < d < n^2$，$d|n^2$。容易看出$d \not\equiv in \pmod{n^2}$。因此假设$d \equiv ia_j \pmod{n^2}$对于某个$i \in [-k_1, k_2]^*$。设$l = \frac{n^2}{d}$，显然$l < n$。则我们有$0 \equiv ld \equiv lia_j \pmod{n^2}$。由于$\gcd(a_j, n) = 1$，则$li \equiv 0 \pmod{n^2}$，与$|i|, l < n$矛盾。

情形2: $n = 2^k$，**其中**$k \ge 3$。

假设$[-k_1, k_2]^*\{2^k, a_1, \cdots, a_{2^k}\} = \mathbb{Z}_{2^{2k}}^*$。则$[-k_1, k_2]^*\{a_1, \cdots, a_{2^k}\} = P$，其中$P = \mathbb{Z}_{2^{2k}} \backslash (2^k\{0, 1, \cdots, 2^k - 1\})$，$\mathbb{Z}_{2^{2k}}$中不是$2^k$倍数的那些元素。设$A = \{a_1, \cdots, a_{2^k}\}$。

设$p = t2^{k-1} \in P$。则t是奇数。注意到t有$\varphi(2^{k+1}) = 2^k$种选取方法。记$p = ma$，其中$m \in [-k_1, k_2]^*$且$a \in A$。由于a是奇数，则m是2^{k-1}的倍数。注意到$|m| \le k_2 < 2^k$，则$m = 2^{k-1}$。因此，对于奇数t，存在$a \in A$使得$t2^{k-1} \equiv 2^{k-1}a \pmod{2^{2k}}$，也就是$t \equiv a \pmod{2^{k+1}}$。由于$t$恰好有$2^k$种选择和$A$中有$2^k$个元素，模$2^{k+1}$的每个奇同余类恰包含$A$中一个元素。

设$q = u2^{k-2} \in P$，其中u是奇数。记$q = u2^{k-2} = ma$，其中$m \in [-k_1, k_2]^*$且$a \in A$。则m一定是2^{k-2}的奇数倍，由于$5 \cdot 2^{k-2} > 2^k$，则要么$m = 2^{k-2}$，要么$m = 3 \cdot 2^{k-2}$。

设a_0是A中任意元素。考虑P中元素$9 \cdot 2^{k-2}a_0 \pmod{2^{2k}}$。这个元素具有形式$2^{k-2}a_1$或$3 \cdot 2^{k-2}a_1$对于某个$a_1 \in A$。对于第二种情形$9 \cdot 2^{k-2}a_0 \equiv 3 \cdot 2^{k-2}a_1 \pmod{2^{2k}}$，因此$3a_0 \equiv a_1 \pmod{2^{k+2}}$。因此元素$2^{k-2}a_1$有两种表示形式，矛盾。

对于第一种情形，$9 \cdot 2^{k-2}a_0 \equiv 2^{k-2}a_1 \pmod{2^{2k}}$，意味着$9a_0 \equiv a_1 \pmod{2^{k+2}}$。我们用$a_1$代替$a_0$重复上面的讨论。对于每个正整数$r$，存在$a_r \in A$使得$9^r a_0 \equiv a_r \pmod{2^{k+2}}$。

对于每个k，$q^{2^{k-2}} \equiv 2^{k+1} + 1 \pmod{2^{k+2}}$。因此对于$r = 2^{k-2}$，我们有$9^r a_0 \equiv a_r \pmod{2^{k+2}}$和$a_0 \equiv a_r \pmod{2^{k+1}}$。由于$A$中不同的元素模$2^{k+1}$是不同的，我们有$a_0 = a_r$，则$9^r a_0 \equiv a_0 \pmod{2^{k+2}}$，与$q^r \equiv 2^{k+1} + 1 \pmod{2^{k+2}}$矛盾。

情形3: $n = p^k$，**其中**p **是奇素数且**$k \ge 2$。

对于这种情形，见文献[148] Theorem 3.2。 □

引理2.30. *如果存在完美*$B[-1, k](m)$*集且假设存在一个整数*$a > 0$*和素数*p*满足*$p|m$*，*

$p|a(1+k)+1$ 和$a|p-1$，则$a(k+1)+1|m$。

证明. 设$S=\{s_1,\cdots,s_n\}$ 是一个完美$B[-1,k](m)$ 集，假设对于$1\le i\le t$, $p|s_i$ 和对于$t+1\le i\le n, p\not|s_i$。我们断言对于$t+1\le i\le n$，$|\{j:p|js_i\}|=\frac{a(k+1)-(p-1)}{ap}$。这只需要证明$\alpha=\frac{a(k+1)-(p-1)}{a}$ 是最大的被p 整除的小于等于k 的整数。由于$a|p-1$，α 是整数。根据$p|a(1+k)+1$ 和gcd$(a,p)=1$，我们有$p|\alpha$。容易看出$\alpha<k$ 且下一个被p 整除的数是$\alpha+p>k$。因此$\langle p\rangle=\{0\}\cup\{js_i:j\in[-1,k]^*,i\in[1,t]\}\cup\{(hp)s_i:h\in[1,\frac{a(k+1)-(p-1)}{ap}],i\in[t+1,n]\}$，从而

$$\frac{n(k+1)+1}{p}=|\langle p\rangle|=1+(k+1)t+\frac{a(k+1)-(p-1)}{ap}(n-t).$$

所以$(a+a(k+1)t+t-n)(1-p)=0$。我们有$n-t=a+a(k+1)t$。因此$m=1+n(k+1)=(a(k+1)+1)(t(k+1)+1)$。 □

类似地，我们有下面的引理。

引理2.31. 如果存在完美$B[-2,k](m)$ 集且假设存在整数$a>0$ 和奇素数p 使得$p|m$，$p|a(2+k)+1$，$a|p-1$ 和$a<p-1$。则$a(k+2)+1|m$。

引理2.32. 如果存在一个完美$B[-1,k](m)$ 集，其中$k+2$ 是合数。则

- $gcd(k+2,m)=1$，或者
- $k+2|m$ 且$gcd(k+2,\frac{m}{k+2})=1$。

证明. 假设gcd$(k+2,m)>1$。根据引理2.30，取$a=1$ 和p 是gcd$(k+2,m)$ 的任意素因子，我们有$k+2|m$。由于存在完美$B[-1,k](m)$ 集和完美$B[-1,k](k+2)$ 集，根据引理2.4，存在完美$B[-1,k](\frac{m}{k+2})$集。如果gcd$(k+2,\frac{m}{k+2})>1$，我们重复上面的讨论，得到完美$B[-1,k](\frac{m}{(k+2)^2})$ 集。则根据引理2.4，我们有完美$B[-1,k]((k+2)^2)$ 集，与引理2.29矛盾。 □

引理2.33. 设n,k_1,k_2 是满足$1\le k_1<k_2$ 的整数。如果B 是一个完美$B[-k_1,k_2](n)$集。设$\mathbb{Z}_n'=\{i:i\in\mathbb{Z}_n,gcd(i,n)=1\}$，$M(n)=\{i:i\in[-k_1,k_2]^*,gcd(i,n)=1\}$ 且$B(n)=\{i:i\in B,gcd(i,n)=1\}$。则$\mathbb{Z}_n'=M(n)\cdot B(n)$ 且对于任意的$a\in\mathbb{Z}_n'$，$|B(n)\cap aM(n)|=1$。

证明. 容易看出$\mathbb{Z}_n' = M(n) \cdot B(n)$ 且$\varphi(n) = |M(n)||B(n)|$。我们只需证明对每一个$a \in \mathbb{Z}_n'$，存在唯一的一对$(b, m)$ 满足$b = am$，其中$b \in B(n)$ 和$m \in M(n)$。

如果存在$b_1, b_2 \in B(n)$，$m_1, m_2 \in M(n)$ 使得$b_1 = am_1$ 且$b_2 = am_2$，则$m_2 b_1 = m_2 a m_1 = m_1 b_2$。由于$\mathbb{Z}_n' = M(n) \cdot B(n)$，我们有$b_1 = b_2$ 且$m_1 = m_2$。我们证明了唯一性。

对于任意的$b \in B(n)$，$m \in M(n)$，存在唯一的$a \in \mathbb{Z}_n'$ 使得$b = am$。由于$|M(n)||B(n)| = \varphi(n)$，这证明了任意的$a \in \mathbb{Z}_n'$ 存在唯一一对(b, m)，其中$b \in B(n)$ 和$m \in M(n)$ 使得$b = am$。 □

现在我们把上面的一般方法应用到纯奇异完美$B[-1, k](m)$ 和$B[-2, k](m)$ 集上。

定理2.34. *如果$k = 3, 4, 5, 6, 8, 9, 10$，则除了可能的$m = k+2$，不存在纯奇异完美$B[-1, k](m)$集。*

证明. 我们分情况证明。

- $k = 3$。对于这种情形，见文献[73] Theorem 2.0.5。
- $k = 4$。对于这种情形，我们有$m = 2^u 3^v$，其中u 和v 是非负整数。由于$k + 2 = 6$，根据引理2.32 可知$m = 1$ 或6。
- $k = 5$。对于这种情形，我们有$m = 5^u$，其中u 是非负整数满足$5^u \equiv 1 \pmod 6$。如果$u \geq 1$，根据引理2.33，存在$B \subseteq \mathbb{Z}_{5^u}'$ 使得$\mathbb{Z}_{5^u}' = B \cdot M$ 和$|B \cap M| = 1$，其中$\mathbb{Z}_{5^u}' = \{i : i \in \mathbb{Z}_{5^u}, \gcd(i, 5) = 1\}$ 和$M = \{-1, 1, 2, 3, 4\}$。不失一般性，假设$1 \in B$，则$-1, \pm 2, \pm 3, \pm 4 \notin B$。在引理2.33中取$a = 2, -2, 3, -3, 4, -4$，我们有：

$$\begin{aligned}
&\{6, 8\} \text{ 中恰好有一个包含在} B \text{ 中},\\
&\{-6, -8\} \text{ 中恰好有一个包含在} B \text{ 中},\\
&\{6, 9, 12\} \text{ 中恰好有一个包含在} B \text{ 中},\\
&\{-6, -9, -12\} \text{ 中恰好有一个包含在} B \text{ 中},\\
&\{8, 12, 16\} \text{ 中恰好有一个包含在} B \text{ 中},\\
&\{-8, -12, -16\} \text{ 中恰好有一个包含在} B \text{ 中}.
\end{aligned}$$

如果$6 \in B$，则$-6, 8, 9, 12 \notin B$，因此$-8, 16 \in B$，这与$|B \cap 8M| = 1$ 矛盾。

类似的，如果$8 \in B$，则$6, -8, 12, 16 \notin B$，因此$-6 \in B$。从而$-12 \notin B$，$-16 \in B$，这与$|B \cap -8M| = 1$矛盾。因此不存在纯奇异完美$B[-1, 5](m)$集。

- $k = 6$。对于这种情形，我们有$m = 2^u 3^v 5^w$，其中u, v, w非负。由于$k + 2 = 8$，根据引理2.32，我们有$2^u = 1$或8。根据引理2.4，存在完美$B[-1, 6](3^v 5^w)$集。如果$v \geq 1$，则在$\mathbb{Z}_{3^v 5^w}$中存在$2 \cdot 3^{v-1} 5^w$个元素与3互素而在$[-1, 6]^*$中有5个元素与3互素，因此$w \geq 1$。如果$w \geq 1$，则在$\mathbb{Z}_{3^v 5^w}$中存在$4 \cdot 3^v 5^{w-1}$个元素与5 in 互素而在$[-1, 6]^*$中有6个元素与5互素，因此$v \geq 1$。从而$v = w = 0$或$v, w \geq 1$。如果$v, w \geq 1$，则根据引理2.33，存在$B \subseteq \mathbb{Z}'_{3^v 5^w}$使得$\mathbb{Z}'_{3^v 5^w} = B \cdot M$和$|B \cap M| = 1$，其中$\mathbb{Z}'_{3^v 5^w} = \{i : i \in \mathbb{Z}_{3^v 5^w}, \gcd(i, 15) = 1\}$和$M = \{-1, 1, 2, 4\}$。不失一般性，假设$1 \in B$，则$-1, \pm 2, \pm 4 \notin B$。由于$|B \cap 2M| = 1$，则$8 \in B$。类似的，由于$|B \cap (-2)M| = 1$，我们有$-8 \in B$。这与$|B \cap 8M| = 1$矛盾。因此不存在纯奇异完美$B[-1, 6](m)$集，除了$m = 8$。

- $k = 8$。对于这种情形，由于$m \equiv 1 \pmod 9$，我们有$m = 2^u 5^v 7^w$，其中u, v, w是非负整数。由于$k + 2 = 10$，根据引理2.32，我们有$2^u 5^v = 1$或10。由引理2.4，存在完美$B[-1, 8](7^w)$集。如果$w \geq 1$，则在$\mathbb{Z}_{7^w}$中存在$6 \cdot 7^{w-1}$个元素与7互素而在$[-1, 8]^*$中有8个元素与7互素，则$8|6 \cdot 7^{w-1}$，矛盾。因此除了$m = 10$，不存在纯奇异完美$B[-1, 8](m)$集。

- $k = 9$。对于这种情形，由于$m \equiv 1 \pmod{10}$，我们有$m = 3^u 7^v$，其中u, v非负。如果$u \geq 1$，则在$\mathbb{Z}_{3^u 7^v}$中存在$2 \cdot 3^{u-1} 7^v$个元素与3互素而在$[-1, 9]^*$中有7个元素与3互素，因此$v \geq 1$。如果$v \geq 1$，则在$\mathbb{Z}_{3^u 7^v}$中有$6 \cdot 3^u 7^{v-1}$个元素与7互素而在$[-1, 9]^*$中有9个元素与7互素，因此$u \geq 1$。从而$u = v = 0$或$u, v \geq 1$。如果$u, v \geq 1$，根据引理2.33，存在$B \subseteq \mathbb{Z}'_{3^u 7^v}$使得$\mathbb{Z}'_{3^u 7^v} = B \cdot M$和$|B \cap M| = 1$，其中$\mathbb{Z}'_{3^u 7^v} = \{i : i \in \mathbb{Z}_{3^u 7^v}, \gcd(i, 21) = 1\}$和$M = \{-1, 1, 2, 4, 5, 8\}$。不失一般性，假设$1 \in B$，则$-1, \pm 2, \pm 4, \pm 5, \pm 8 \notin B$。在引理2.33中取$a = 2, -2, 4, -4$，我们有：

$$\{10, 16\} \text{ 中恰好有一个包含在} B \text{ 中},$$
$$\{-10, -16\} \text{ 中恰好有一个包含在} B \text{ 中},$$
$$\{16, 20, 32\} \text{ 中恰好有一个包含在} B \text{ 中},$$
$$\{-16, -20, -32\} \text{ 中恰好有一个包含在} B \text{ 中}.$$

如果$10 \in B$，则$-10, 16 \notin B$，因此$-16 \in B$。则$-20, 32, -32 \notin B$，从而$20 \in B$，这与$|B \cap 10M| = 1$矛盾。

对于情形$16 \in B$可类似讨论。因此不存在纯奇异完美$B[-1,9](m)$ 集。

- $k=10$。对于这种情形，我们有$m=2^u3^v5^w7^x$ ，其中u,v,w,x 非负。由于$k+2=12$，由引理2.32 可知$2^u3^v=1$ 或12。根据引理2.4，存在完美$B[-1,10](5^w7^x)$ 集。如果$w \geq 1$，在$\mathbb{Z}_{5^w7^x}$中存在$4\cdot 5^{w-1}7^x$ 个元素与5 互素而在$[-1,10]^*$中存在9 个元素与5 互素，因此$9|4\cdot 5^{w-1}7^x$，矛盾。从而$w=0$。如果$x \geq 1$，则在$\mathbb{Z}_{7^x}$中存在$6\cdot 7^{x-1}$ 个元素与7 互素而在$[-1,10]^*$中有10 个元素与7 互素，所以$10|6\cdot 7^{x-1}$，矛盾。因此除了$m=12$，不存在纯奇异完美$B[-1,10](m)$ 集。

□

定理2.35. *如果$k=3,4,6$，则除了可能的$m=k+3$，不存在纯奇异完美$B[-2,k](m)$ 集。*

证明. 我们分情况证明。

- $k=3$。如果存在一个纯奇异完美$B[-2,3](m)$ 集，则$m=2^u3^v$。如果$v \geq 1$，根据引理2.31，取$a=1$ 和$p=3$，我们有$6|m$。利用与引理2.32类似讨论可得$v=0$ 或1。如果$v \neq u$，则$u>v$。根据引理2.4，存在一个纯奇异完美$B[-2,3](2^{u-v})$ 集。注意到在$\mathbb{Z}_{2^{u-v}}$中有2^{u-v-1} 个元素与2 互素而在$[-2,3]^*$中有3 个元素与2 互素。我们有$3|2^{u-v-1}$，矛盾。因此除了$m=6$，不存在纯奇异完美$B[-2,3](m)$ 集。

- $k=4$。由于$m \equiv 1 \pmod 6$，因此不存在纯奇异完美$B[-2,4](m)$ 集。

- $k=6$。如果存在一个纯奇异完美$B[-2,6](m)$集，则$m=3^u5^v$。如果$u \geq 1$，根据引理2.31，取$a=1$ 和$p=3$，我们有$9|m$。利用与引理2.32类似讨论可得$u=0$ 或2。如果$v \geq 1$，根据引理2.4，存在一个纯奇异完美$B[-2,6](5^v)$ 集。注意到在$\mathbb{Z}_{5^v}$中有$4\cdot 5^{v-1}$ 个元素与5 互素而在$[-2,6]^*$中有7 个元素与5 互素，我们有$7|4\cdot 5^{v-1}$，矛盾。因此除了$m=9$，不存在纯奇异完美$B[-2,6](m)$ 集。

□

评论2.36. *在文献[134]中，除了有限几个情形，作者决定了所有的完美$B[-1,3](n)$ 集对于$n \leq 1001$ 和完美$B[-2,3](n)$ 集对于$n \leq 1251$ 。结合定理2.18，2.34 和2.35，我们证明了不存在纯奇异完美$B[-1,3](n)$ 集和除了$n=6$，不存在完美$B[-2,3](n)$ 集。*

注意到Schwartz[133] 构造了一类纯奇异完美$B[-1,2](4^l)$ 集。基于上面的结果，我们给出下面的猜想。

猜想2.37. 设k_1,k_2 是满足$1 \le k_1 < k_2$ 和$k_1+k_2 \ge 4$ 的整数，则除了可能的$m=k_1+k_2+1$，不存在纯奇异完美$B[-k_1,k_2](m)$ 集。

2.1.5 在冲突避免码上的应用

冲突避免码主要应用于无反馈的多址冲突信道。一个码字就是$\mathbb{Z}_n$的一个子集I，I 的重量就是大小$|I|$。对于一个码字I，设

$$d(I)=\{a-b \pmod n:\ a,b\in I\}$$

为I中两个元素的差的集合。注意到$0\in d(I)$。设$d^*(I)$为$d(I)$的非零差，也就是I中不同元素的差的集合

$$d^*(I)=d(I)\backslash\{0\}.$$

M 个码字的集合

$$C=\{I_1,I_2,\ldots,I_M\}$$

称为长为n重量为ω的冲突避免码，如果对所有的$j\neq k$，

$$d^*(I_j)\cap d^*(I_k)=\emptyset$$

和对所有的$j\in[1,M]$有$|I_j|=\omega$。我们记这样的码为(n,ω)-冲突避免码。

例2.38. 设$n=15$，$\omega=3$。四个码字$\{0,5,10\}$，$\{0,1,2\}$，$\{0,7,11\}$，$\{0,6,12\}$ 形成一个$(15,3)$-冲突避免码。我们可以验证

$$\begin{aligned}
d^*(\{0,5,10\})&=\{5,10\},\\
d^*(\{0,1,2\})&=\{1,2,13,14\},\\
d^*(\{0,7,11\})&=\{4,7,8,11\},\\
d^*(\{0,6,12\})&=\{3,6,9,12\},
\end{aligned}$$

是不交的。

给定正整数n 和ω，考虑所有的长为n 重量为ω 的冲突避免码。其中具有最多码字数量的冲突避免码称为是最优的，且码字数量记做$M(n,\omega)$。冲突避免码的主要问题就是对所有的n 和ω，决定$M(n,\omega)$ 。例子2.38 表明$M(15,3)\geq 4$。

一个码字I 称为是等差的 如果I 中的元素在$\mathbb{Z}_n$中形成等差数列，也就是存在某个$i\in\mathbb{Z}_n$，

$$I=\{0,i,2i,\ldots,(\omega-1)i\}.$$

元素i 称为这个码字的生成元 。对于一个由i生成的等差码字I，它的差的集合为

$$d(I)=\{0,\pm i,\pm 2i,\ldots,\pm(\omega-1)i\}.$$

元素$\pm i,\pm 2i,\ldots,\pm(\omega-1)i$ 在$\mathbb{Z}_n$ 中不一定不同。因此$|d^*(I)|\leq 2\omega-2$，如果$\pm i,\pm 2i,\ldots,\pm(\omega-1)i$ 是不同的，则等式成立。一个重量为ω的码字I 是异常的如果$|d^*(I)|<2\omega-2$。如果一个冲突避免码C 的所有码字都是等差的，则我们说C 是等差的，且它的生成元集合记作$\Gamma(C)$。

如果C 是一个长为n，重量为ω，且无异常码字的等差冲突避免码，则C 的生成元集合形成一个$B[-(\omega-1),\omega-1](n)$ 集。反过来，如果存在一个$B[-k,k](n)$ 集，取它为某个码C 的生成元集合，则对应的码C 是一个长为n，重量为$k+1$，且无异常码字的等差冲突避免码。因此，我们有下面的结果。

定理2.39. 如果存在一个大小为m的$B[-k,k](n)$ 集，则$M(n,k+1)\geq m$。

下面的结果和定理2.3类似，是冲突避免码的一个递归构造。

定理2.40. [119] 设$\omega\geq 3$，且n_1,n_2 和s 是满足$s|n_1$，和对所有的$l\in[2,\omega-1]$有$gcd(l,n_2)=1$的正整数。设C_1 是一个包含m_1 个异常码字$I_1,\ldots,I_{m_1}$ 的等差(n_1,ω)-冲突避免码且满足

$$\mathbb{Z}_{n_1}\setminus\cup_{j=1}^{m_1}d^*(I_j)\supseteq\frac{n_1}{s}\mathbb{Z}_{n_1}.$$

设C_2 是有m_2个码字的(sn_2,ω)-冲突避免码。则由

$$\Gamma(C)=\{i+jn_1:i\in\Gamma(C_1),\ j\in[0,n_2-1]\}\cup\{(n_1/s)k:k\in\Gamma(C_2)\}$$

生成的长为n_1n_2的码C是一个有$m_1n_2+m_2$个码字的等差(n_1n_2,ω)-冲突避免码。

给定一个子集$I\subseteq\mathbb{Z}_n$，注意到稳定集$N(I)=\{g\in\mathbb{Z}_n:I+g=I\}$ 是$\mathbb{Z}_n$ 的一个子群。文献[138] 证明了对任意的子集$I\subseteq\mathbb{Z}_n$ 有$d(I)\supseteq N(d(I))$。在同一篇文章中，它们还给出了$M(n,\omega)$ 的一个一般上界。

定理2.41. [138] 设C 是一个(n,ω)-冲突避免码。如果C中存在E 个异常码字$I_1, I_2, \ldots, I_E$，则

$$|C| \leq \frac{n-1+\sum_{j=1}^{E}(|N(d(I_j))|-1)}{2\omega-2}.$$

另外，他们决定了很多个$M(n,\omega)$ 的值。利用类似的想法，我们得到下面的定理。为读者方便，我们给出证明。

定理2.42. 设$\omega \geq 3$。假设n 是满足$(2\omega-2)|(n-1)$ 和$gcd(n,(2\omega-2)!)=1$ 的整数。如果存在一个完美$B[-(\omega-1),\omega-1](n)$ 集和一个整数t 满足$\omega \leq t \leq 2\omega-2$ 且$gcd(t,(\omega-1)!)=1$，则$M(tn,\omega)=t\frac{n-1}{2\omega-2}+1$。

证明. 如果存在一个完美$B[-(\omega-1),\omega-1](n)$ 集，则存在一个有$\frac{n-1}{2\omega-2}$个非异常码字的等差(n,ω)-冲突避免码C_1 。设C_2 是一个只包含一个由1生成的码字的(t,ω)-冲突避免码。应用定理2.40，其中$s=1$，$n_1=n$，$n_2=t$，我们得到一个有$t\frac{n-1}{2\omega-2}+1$个码字的(tn,ω)-冲突避免码。

下面只需证明任意的(tn,ω)-冲突避免码至多包含$t\frac{n-1}{2\omega-2}+1$ 个码字。设C 是一个(tn,ω)-冲突避免码。假设C中有E 个异常码字$I_j,\ j\in[1,E]$。对任意的j，设N_j 是$d(I_j)$ 的稳定集。则由于$|N_j| \leq |d(I_j)| \leq 2\omega-2$，$N_j$ 的大小严格小于$2\omega-1$。

我们断言$\mathbb{Z}_{tn}$的大小小于$2\omega-1$ 的子群G是

$$\langle n\rangle = \{0, n, 2n, \ldots, (t-1)n\}$$

的子群。否则的话，存在$a\in G$，它不能被n整除。则由于$\gcd(n,(2\omega-2)!)=1$，a 在$\mathbb{Z}_{tn}$ 中的阶大于$2\omega-2$，这与$|G|<2\omega-1$ 矛盾。

因此对任意的j，我们有$N_j \subset \langle n\rangle$。根据定理2.41，我们得到

$$\begin{aligned}|C| &\leq \frac{tn-1+\sum_{j=1}^{E}(|N_j|-1)}{2\omega-2}\\ &\leq \frac{tn-1+t-1}{2\omega-2}\\ &\leq t\frac{n-1}{2\omega-2}+\frac{t-1}{\omega-1}.\end{aligned}$$

由于$\omega \leq t \leq 2\omega-2$，我们有$M(tn,\omega)=t\frac{n-1}{2\omega-2}+1$。 □

由于我们在2.1.3.2小节得到了无穷多个新的完美分解集，则根据定理2.42，我们决定了无穷多个$M(n,\omega)$ 的值。

2.2 l_p 范数下的完美和准完美码

2.2.1 介绍

Lee 范数的概念最早是在处理带噪音的信道问题时引入的[104,151]。紧接着，几类Lee 范数意义下的码被广泛研究（参见文献[2,6,13,25,47,48,62,78]）。在这部分，我们将只关注在$\mathbb{Z}^n$上的完美和准完美l_p码。在文献[62]中，Golomb 和Welch 猜想在Lee 范数下的完美码只存在于下列情况：球半径$r = 1$ 或者Lee空间的维数$n = 1, 2$。除了实际应用，Golomb-Welch 猜想是过去45 年这个领域研究的主要动力。尽管在这个领域有很多文章，但这个猜想还远未解决。

在文献[67] 中，Gravier 等人解决了Golomb-Welch 猜想的3 维Lee 空间情形。4维情形被Špacapan[140] 在计算机的帮助下解决。文献[77] 证明了对于$3 \le n \le 5$ 和$r > 1$，不存在完美Lee 码。Horak[76] 证明了完美Lee 码在$n = 6$ 和$r = 2$ 下的不存在性。在文献[80]中，Horak 和Grošek 给出了一个新的处理这个猜想的工具，并且证明了对于$7 \le n \le 11$ 和$r = 2$，线性完美Lee 码不存在。

还有一些研究人员考虑了这个猜想的大维数情形。在文献[62]中，Golomb 和Welch证明了当$r \ge r_n$时，完美Lee 码不存在，其中r_n 没有具体给出来。后来，Post[124] 证明了当$r \ge \frac{\sqrt{2}}{2}n - \frac{1}{4}(3\sqrt{2} - 2)$ 和$n \ge 6$ 时，不存在线性完美码。在文献[107]中，Lepistö证明了一个完美Lee码必须满足$n \ge (r + 2)^2/2.1$，其中$r \ge 285$。

尽管Golomb-Welch猜想还没有被完全解决，但大家都认为它是正确的。因此，去构造那些接近完美的码就有意义了[2]。在文献[80]中，Horak 和Grošek 构造了一些$n = 3$时的准完美Lee 码。他们还证明了至多有有限个r，使得在$\mathbb{Z}^n$中存在一个准完美r纠错Lee码。

最近，完美Lee码的概念被推广到完美l_p码，其中$p \ge 2$[26]。可以证明对于$n = 2, 3$和$p = 2$，只有在$n = 2$ 以及$r = 1, \sqrt{2}, 2, 2\sqrt{2}$ 和$n = 3$ 以及$r = 1, \sqrt{3}$ 时，存在线性完美码。还可以证明对于$n = 2$ 和r 是整数时，如果$r > 2$ 以及$2 \le p < \infty$，不存在一个完美l_p码。后来Strapasson 等人[146]考虑了准完美码，并且决定了对于$p = 2$ 和$n = 2, 3$ 时，线性准完美码存在的所有半径。

在这部分，我们将继续上面的研究。我们证明了线性完美l_p 码的一些不存在性结果，其中$p = 1$ 或者$2 \le p < \infty, r = 2^{1/p}, 3^{1/p}$。同时，我们还给出了一个准完美$l_p$ 码的代数构造，其中$p = 1, r = 2$ 以及$2 \le p < \infty, r = 2^{1/p}$。

2.2.2 准备工作

$\mathbb{Z}^n$ 上的一个码C 是$\mathbb{Z}^n$的一个子集。如果码C 还同时是一个格，则C称为一个线性码。由于线性码更有可能有一个有效的译码算法，因此线性码具有重要的作用。两个点$x=(x_1,x_2,\cdots,x_n)\in\mathbb{Z}^n, y=(y_1,y_2,\cdots,y_n)\in\mathbb{Z}^n$ 的l_p距离定义为

$$d_p(x,y):=(\sum_{i=1}^{n}|x_i-y_i|^p)^{\frac{1}{p}},$$

其中$1\leq p<\infty$。如果$p=1$，则l_1 距离也称为Lee 距离，并且相应的码称为Lee 码。$\mathbb{Z}^n$上的码C的极小距离$d_p(C)$定义为

$$d_p(C):=\min\{d_p(x,y):\ x,y\in C,\ x\neq y\}.$$

$\mathbb{Z}^n$ 上中心为$x=(x_1,x_2,\cdots,x_n)$，半径为r 的球定义为

$$B_p^n(x,r):=\{z\in\mathbb{Z}^n:\ d_p(x,z)\leq r\}.$$

当$x=0$时，我们把$B_p^n(0,r)$ 记做$B_p^n(r)$。

为了定义$C\subseteq\mathbb{Z}^n$在l_p范数下的填充半径和覆盖半径，其中$1\leq p<\infty$，我们首先定义$\mathbb{Z}^n$上l_p范数下的距离集合

$$D_{p,n}=\{d\in\mathbb{R}:\ \text{存在}z_1,z_2\in\mathbb{Z}^n\ \text{使得}d_p(z_1,z_2)=d\}.$$

容易看出来$D_{p,n}\subseteq\{0,1,2^{1/p},3^{1/p},\cdots\}$ 以及$D_{1,n}=\{0,1,2,3,\cdots\}$。$D_{2,n}$ 已经被文献[26]完全决定出来了，但一般来说，并不容易去决定集合$D_{p,n}$。接下来，我们将把集合$D_{p,n}$ 中的元素记作

$$D_{p,n}=\{d_{p,n,i}:\ i=0,1,2,\cdots,\ \text{和}d_{p,n,0}<d_{p,n,1}<d_{p,n,2}<\cdots\}.$$

码$C\subset\mathbb{Z}^n$ 在l_p 范数下的填充半径是最大的$r\in D_{p,n}$ 使得对任意的$x,y\in C$，$B_p^n(x,r)\bigcap B_p^n(y,r)=\emptyset$成立。码$C\subset\mathbb{Z}^n$ 在l_p 范数下的填充半径将记作$r_p(C)$。

码$C\subset\mathbb{Z}^n$ 在l_p 范数下的覆盖半径是最小的$r\in D_{p,n}$ 使得$\bigcup_{c\in C}(c+B_p^n(r))=\mathbb{Z}^n$。码$C\subset\mathbb{Z}^n$ 在l_p 范数下的覆盖半径将记作$R_p(C)$。

一个l_p范数下的(n,r) 码$C\subseteq\mathbb{Z}^n$ 称为是完美的如果$r_p(C)=R_p(C)=r$。一个l_p范数下的(n,r) 码$C\subseteq\mathbb{Z}^n$ 称为是准完美的如果存在整数i 使得$r_p(C)=r=d_{p,n,i}$ 且$R_p(C)=d_{p,n,i+1}$。

另一个定义l_p 完美码的方式是镶嵌。设V 是$\mathbb{Z}^n$ 的一个子集。V 的一个复制指的是V的一个平移$V+x=\{v+x:\ v\in V\}$，其中$x\in\mathbb{Z}^n$。如果V 的复制的集合$\mathfrak{T}=\{V+l:\ l\in L\}$,

$L \subseteq \mathbb{Z}^n$，形成$\mathbb{Z}^n$ 的一个划分，则$\mathfrak{T}$称为一个关于V的$\mathbb{Z}^n$ 镶嵌。$\mathfrak{T}$ 称为一个格镶嵌如果L 形成一个格。显然，码C 是l_p 完美码当且仅当$\{B_p^n(r_p(C)) + c : \ c \in C\}$ 形成一个关于$B_p^n(r_p(C))$ 的$\mathbb{Z}^n$ 镶嵌。

注意到如果存在$V \subseteq \mathbb{Z}^n$ 和$C \subseteq \mathbb{Z}^n$ 使得对于某个i，$B_p^n(d_{p,n,i}) \subsetneqq V \subsetneqq B_p^n(d_{p,n,i+1})$成立以及$\{V + c : \ c \in C\}$ 形成一个关于V的$\mathbb{Z}^n$ 镶嵌，则集合C 是$\mathbb{Z}^n$ 上的准完美l_p码，且我们把这样的码记作l_p范数下准完美$(n, d_{p,n,i}, |V|)$ 码。

下面的定理是l_p 版本的[80] Theorem 11，它也可视为定理2.1的一个推论。

定理2.43. *对于整数i，如果存在一个阶为M的Abel 群G 满足$|B_p^n(d_{p,n,i})| < M < |B_p^n(d_{p,n,i+1})|$和一个同态$\phi : \mathbb{Z}^n \mapsto G$ 使得ϕ 限制在$B_p^n(d_{p,n,i})$ 是一个单设以及ϕ 限制在$B_p^n(d_{p,n,i+1})$ 是一个满射，则存在一个l_p范数下准完美$(n, d_{p,n,i}, M)$ 码。*

2.2.3 不存在性结果

2.2.3.1 $p = 1$

在这个小节，我们考虑完美Lee码的不存在性。$B_1^n(r)$ 的大小是众所周知的[62]，我们把它记作$k_{n,r}$:

$$k_{n,r} := |B_1^n(r)| = \sum_{i=0}^{\min\{n,r\}} 2^i \binom{n}{i}\binom{r}{i}.$$

为了得到我们的主要结果，我们需要下面的引理。

引理2.44. [152] $x_1 + x_2 + \cdots + x_k \le n$ 在$\mathbb{Z}_{>0}$ 中解的个数是$\binom{n}{k}$。

引理2.45. $\sum_{i=1}^{t} \sum_{\substack{x_i \ge 1 \\ \sum_{i=1}^{t} x_i \le r}} x_i^2 y_i = \sum_{j=1}^{r-t+1} j^2 \binom{r-j}{t-1} \sum_{i=1}^{t} y_i$。

证明. 由于$x_i \ge 1$ 且$\sum_{i=1}^{t} x_i \le r$，则对于$1 \le i \le t$有$1 \le x_i \le r - t + 1$。对于每个$1 \le j \le r - t + 1$，根据引理2.44，$x_i = j$ 及$\sum_{\substack{1 \le k \le t \\ k \ne i}} x_k \le r - j$ 在$\mathbb{Z}_{>0}$ 中解的个数是$\binom{r-j}{t-1}$。因此$\sum_{i=1}^{t} \sum_{\substack{x_i \ge 1 \\ \sum_{i=1}^{t} x_i \le r}} x_i^2 y_i = \sum_{j=1}^{r-t+1} j^2 \binom{r-j}{t-1} \sum_{i=1}^{t} y_i$。 □

引理2.46. $\sum_{c_1,\cdots,c_n \in \{\pm 1\}} (\sum_{i=1}^{n} c_i b_i)^2 = 2^n \sum_{i=1}^{n} b_i^2.$

证明.

$$\begin{aligned}
&\sum_{c_1,\cdots,c_n\in\{\pm1\}}(\sum_{i=1}^{n}c_ib_i)^2\\
&=\sum_{c_1,\cdots,c_n\in\{\pm1\}}(\sum_{i=1}^{n}b_i^2+2\sum_{1\le i<j\le n}c_ib_ic_jb_j)\\
&=2^n\sum_{i=1}^{n}b_i^2+2\sum_{c_1,\cdots,c_n\in\{\pm1\}}\sum_{1\le i<j\le n}c_ic_jb_ib_j\\
&=2^n\sum_{i=1}^{n}b_i^2+2\sum_{1\le i<j\le n}(1\cdot1\cdot b_ib_j+1\cdot(-1)\cdot b_ib_j+(-1)\cdot1\cdot b_ib_j+(-1)\cdot(-1)\cdot b_ib_j)\\
&=2^n\sum_{i=1}^{n}b_i^2.
\end{aligned}$$

□

引理2.47. $\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{i=1}^{t}x_{l_i}=\binom{n-1}{t-1}\sum_{i=1}^{n}x_i$.

证明. 由于$1\le l_1<l_2<\cdots<l_t\le n$，如果$i\in\{l_1,l_2,\cdots,l_t\}$，则对其他$t-1$个数存在$\binom{n-1}{t-1}$种选择。因此对于$1\le i\le n$, x_i在等式左边出现$\binom{n-1}{t-1}$次，结论成立。 □

我们有下面的定理。

定理2.48. *设$r\le n$，$p_{n,r}=\sum_{t=1}^{r}2^t\sum_{j=1}^{r-t+1}j^2\binom{r-j}{t-1}\binom{n-1}{t-1}$。如果$k_{n,r}\equiv3$ 或$6\pmod 9$，$p_{n,r}\equiv0\pmod 3$ 以及$k_{n,r}$ 无平方因子，则不存在一个线性完美(n,r) Lee 码。*

证明. 如果$k_{n,r}=|B_1^n(r)|\equiv3\text{ or }6\pmod 9$，$p_{n,r}\equiv0\pmod 3$ 以及$k_{n,r}$ 无平方因子。那么每个阶为$k_{n,r}$ 的Abel 群均同构于循环群$\mathbb{Z}_{k_{n,r}}$。根据定理2.1，我们需要证明不存在同态$\phi:\mathbb{Z}^n\mapsto\mathbb{Z}_{k_{n,r}}$ 使得ϕ 限制在$B_1^n(r)$ 上是一个双射。注意到每个同态$\phi:\mathbb{Z}^n\mapsto\mathbb{Z}_{k_{n,r}}$都由值$\phi(e_i),\ i=1,\cdots,n$完全决定，其中$e_i,\ i=1,\cdots,n,$ 是$\mathbb{Z}^n$ 的一组标准基。另外如果$\{\sum_{i=1}^{t}\pm b_{l_i}\phi(e_{l_i}):\ 1\le t\le r,\ 1\le l_1<l_2<\cdots<l_t\le n,\ b_{l_i}\ge1,\ \sum_{i=1}^{t}b_{l_i}\le r\}\ne\mathbb{Z}_{k_{n,r}}\backslash\{0\}$，则$\phi$ 限制在$B_1^n(r)$上不是一个双射。因此，我们只需证明对$\mathbb{Z}_{k_{n,r}}$的每个n元集$(a_1,\cdots,a_n)$，有

$$\Big\{\sum_{i=1}^{t}\pm b_{l_i}a_{l_i}:\ 1\le t\le r,\ 1\le l_1<l_2<\cdots<l_t\le n,\ b_{l_i}\ge1,\ \sum_{i=1}^{t}b_{l_i}\le r\Big\}\ne\mathbb{Z}_{k_{n,r}}\backslash\{0\}.$$

否则的话，我们有

$$\sum_{t=1}^{r}\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{\substack{b_{l_i}\ge 1\\ \sum_{i=1}^{t} b_{l_i}\le r}}(\sum_{i=1}^{t}\pm b_{l_i}a_{l_i})^2\equiv\sum_{i=1}^{k_{n,r}-1} i^2 \pmod{k_{n,r}}. \tag{2-1}$$

上式的左边可以写成

$$\begin{aligned}
&\sum_{t=1}^{r}\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{\substack{b_{l_i}\ge 1\\ \sum_{i=1}^{t} b_{l_i}\le r}}\sum_{c_{l_1},\cdots,c_{l_t}\in\{\pm 1\}}(\sum_{i=1}^{t} c_{l_i}b_{l_i}a_{l_i})^2\\
=&\sum_{t=1}^{r}2^t\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{\substack{b_{l_i}\ge 1\\ \sum_{i=1}^{t} b_{l_i}\le r}}\sum_{i=1}^{t} b_{l_i}^2a_{l_i}^2\\
=&\sum_{t=1}^{r}2^t\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{i=1}^{t}\sum_{\substack{b_{l_i}\ge 1\\ \sum_{i=1}^{t} b_{l_i}\le r}} b_{l_i}^2a_{l_i}^2\\
=&\sum_{t=1}^{r}2^t\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{j=1}^{r-t+1} j^2\binom{r-j}{t-1}\sum_{i=1}^{t} a_{l_i}^2\\
=&\sum_{t=1}^{r}2^t\sum_{j=1}^{r-t+1} j^2\binom{r-j}{t-1}\sum_{1\le l_1<l_2<\cdots<l_t\le n}\sum_{i=1}^{t} a_{l_i}^2\\
=&\sum_{t=1}^{r}2^t\sum_{j=1}^{r-t+1} j^2\binom{r-j}{t-1}\binom{n-1}{t-1}(\sum_{i=1}^{n} a_i^2)\\
=&p_{n,r}(\sum_{i=1}^{n} a_i^2),
\end{aligned}$$

其中第一个等式根据引理2.46，第三个根据引理2.45，第五个根据引理2.47。根据平方和公式，我们有$\sum_{i=1}^{k_{n,r}-1} i^2=\frac{(k_{n,r}-1)k_{n,r}(2k_{n,r}-1)}{6}$。从我们的假设可知$3\mid k_{n,r}$，$3\mid p_{n,r}$，且容易看出如果$k_{n,r}\equiv 3$或$6 \pmod 9$，有$3\nmid\frac{(k_{n,r}-1)k_{n,r}(2k_{n,r}-1)}{6}$，这与式子(2-1)矛盾，也就是$p_{n,r}(\sum_{i=1}^{n} a_i^2)\equiv\frac{(k_{n,r}-1)k_{n,r}(2k_{n,r}-1)}{6} \pmod{k_{n,r}}$。 □

通过考虑上面定理在半径为$r=3$和$r=4$的情形，我们有下面的推论。

推论2.49. *如果$n\equiv 12$或$21 \pmod{27}$以及$k_{n,3}$无平方因子，则不存在线性完美$(n,3)$ Lee码。*

证明. 根据定理2.48，我们需要证明$k_{n,3} \equiv 3$或$6 \pmod 9$以及$p_{n,3} \equiv 0 \pmod 3$。根据定义，我们有

$$\begin{aligned} k_{n,3} &= \sum_{i=0}^{3} 2^i \binom{n}{i}\binom{3}{i} \\ &= 1 + 6n + 4\binom{n}{2}\binom{3}{2} + 8\binom{n}{3} \\ &= 1 + 6n^2 + \frac{4n(n-1)(n-2)}{3}. \end{aligned}$$

那么$k_{n,3} \equiv 3$或$6 \pmod 9$等价于$3 + 18n^2 + 4n(n-1)(n-2) \equiv 9$或$18 \pmod{27}$。因此$k_{n,3} \equiv 3$或$6 \pmod 9$当且仅当$n \equiv 1, 11, 12, 19, 20$或$21 \pmod{27}$。

类似地，我们有

$$\begin{aligned} p_{n,3} &= \sum_{t=1}^{3} 2^t \sum_{j=1}^{4-t} j^2 \binom{3-j}{t-1}\binom{n-1}{t-1} \\ &= 2\sum_{j=1}^{3} j^2 + 4\sum_{j=1}^{2} j^2 \binom{3-j}{1}\binom{n-1}{1} + 8\binom{n-1}{2} \\ &= 28 + 24(n-1) + 4(n-1)(n-2). \end{aligned}$$

则$p_{n,3} \equiv 0 \pmod 3$当且仅当$n \equiv 0 \pmod 3$。

从而只有当$n \equiv 12$或$21 \pmod{27}$时，我们有$k_{n,3} \equiv 3$或$6 \pmod 9$以及$p_{n,3} \equiv 0 \pmod 3$。 □

推论2.50. *如果$n \equiv 3, 5, 21$或$23 \pmod{27}$，$n \geq 4$且$k_{n,4}$无平方因子，则不存在线性完美$(n, 4)$ Lee码。*

证明. 根据定理2.48，我们只需证明$k_{n,4} \equiv 3$或$6 \pmod 9$和$p_{n,4} \equiv 0 \pmod 3$。根据定义，我们有

$$\begin{aligned} k_{n,4} &= \sum_{i=0}^{4} 2^i \binom{n}{i}\binom{4}{i} \\ &= 1 + 8n + 4\binom{n}{2}\binom{4}{2} + 8\binom{n}{3}\binom{4}{3} + 16\binom{n}{4} \\ &= 1 + 8n + 12n(n-1) + \frac{16n(n-1)(n-2)}{3} + \frac{2n(n-1)(n-2)(n-3)}{3}. \end{aligned}$$

则$k_{n,4} \equiv 3$或$6 \pmod 9$等价于$3 + 24n + 36n(n-1) + 16n(n-1)(n-2) + 2n(n-1)(n-2)(n-3) \equiv 9$或$18 \pmod{27}$。因此$k_{n,4} \equiv 3$或$6 \pmod 9$当且仅当$n \equiv 3, 4, 5, 13, 21, 22$或$23 \pmod{27}$。

类似地，我们有

$$\begin{aligned}
p_{n,4} &= \sum_{t=1}^{4} 2^t \sum_{j=1}^{5-t} j^2 \binom{4-j}{t-1}\binom{n-1}{t-1} \\
&= 2\sum_{j=1}^{4} j^2 + 4\sum_{j=1}^{3} j^2 \binom{4-j}{1}\binom{n-1}{1} + 8\sum_{j=1}^{2} j^2 \binom{4-j}{2}\binom{n-1}{2} + 16\binom{n-1}{3} \\
&= 60 + 4(n-1)\sum_{j=1}^{3} j^2(4-j) + 4(n-1)(n-2)\sum_{j=1}^{2} j^2 \binom{4-j}{2} + \frac{8(n-1)(n-2)(n-3)}{3} \\
&= 60 + 80(n-1) + 28(n-1)(n-2) + \frac{8(n-1)(n-2)(n-3)}{3}.
\end{aligned}$$

则$p_{n,4} \equiv 0 \pmod 3$ 等价于$180 + 240(n-1) + 84(n-1)(n-2) + 8(n-1)(n-2)(n-3) \equiv 0 \pmod 9$。因此$p_{n,4} \equiv 0 \pmod 3$ 当且仅当$n \equiv 1, 3$ 或$5 \pmod 9$。

因此只有当$n \equiv 3, 5, 21$ 或$23 \pmod{27}$ 时，我们有$k_{n,4} \equiv 3$ 或$6 \pmod 9$ 和$p_{n,4} \equiv 0 \pmod 3$。 □

评论2.51. 当$r = 2$ 时，$k_{n,2} = 2n^2 + 2n + 1$ 且$p_{n,2} = 4n + 6$，不存在整数n 满足定理*2.48*中的条件。因此我们无法利用定理*2.48*得到关于线性完美$(n, 2)$ *Lee* 码的不存在性结果。

表2-4 给出了一些满足定理2.48条件的一些整数。事实上，我们发现当$r = 3$ 和$n \leq 5000$时，有265 个整数满足定理2.48 的条件，以及当$r = 4$ 和$n \leq 5000$ 时，有734 个整数满足定理2.48中的条件。看起来，有很多参数(n, r) 满足定理2.48中的条件。

表 2-4　线性完美(n, r) Lee 码的不存在结果

r	n
3	$21, 39, 48, 66, 75, 93, 120, 129, 156, 174, 183, 201, 210, 228, 255, 291$
4	$5, 21, 23, 32, 48, 50, 59, 75, 77, 84, 86, 102, 104, 111, 113, 129, 131, 138$

评论2.52. 在*[80], Horak* 和*Grošek* 猜想，对于任意的$n \geq 2$ 和$r > 0$ 如果存在阶为$|B_1^n(r)|$的群G 和一个同态$\phi : \mathbb{Z}^n \mapsto G$ 满足ϕ 限制在$B_1^n(r)$ 上是双射，则存在一个同态$\phi : \mathbb{Z}^n \mapsto \mathbb{Z}_{|B_1^n(r)|}$ 使得ϕ 限制在$B_1^n(r)$ 上是一个双射。如果猜想是正确的，则在定理*2.48* 中，$k_{n,r}$ 无平方因子的条件就不需要了。

2.2.3.2 $2 \le p < \infty$

与Lee 范数不同，存在无穷多个半径和维数，使得完美l_p $(2 \le p < \infty)$码存在。例如对于$n < (1+1/r)^p$，存在完美$(n, n^{\frac{1}{p}}r)$ l_p 码[26]。在这个小节，我们研究对于半径较小的完美l_p $(2 \le p < \infty)$ 码的不存在性。注意到对于一般的n 和r ，球$B_p^n(r)$ 的大小我们知道的比较少，但是半径$2^{\frac{1}{p}}$ 和$3^{\frac{1}{p}}$ 非常的特殊。由于当维数n 固定时，在l_p范数下，这些半径的球的大小都是相同的（即与p 无关），且容易得出

$$k_{n,2,p} := |B_p^n(2^{\frac{1}{p}})| = 2n^2 + 1 \text{ 和} k_{n,3,p} := |B_p^n(3^{\frac{1}{p}})| = 1 + 2n^2 + \frac{4n(n-1)(n-2)}{3}.$$

定理2.53. *如果$n \equiv 5$ 或$8 \pmod 9$ 和$k_{n,2,p}$ 无平方因子，则不存在线性完美$(n, 2^{1/p})$ l_p 码。*

证明. 证明与定理2.48类似，我们只需证明$\mathbb{Z}_{k_{n,2,p}}$中任意n元集合$(a_1, \cdots, a_n)$ 有

$$\left\{ \pm a_i, \pm a_j \pm a_k : 1 \le i \le n,\ 1 \le j < k \le n \right\} \ne \mathbb{Z}_{k_{n,2,p}} \backslash \{0\}.$$

否则的话，我们有

$$2\sum_{i=1}^{n} a_i^2 + 2 \sum_{1 \le i < j \le n} ((a_i + a_j)^2 + (a_i - a_j)^2) \equiv \sum_{i=1}^{k_{n,2,p}-1} i^2 \pmod{k_{n,2,p}}.$$

也就是

$$(4n-2)\sum_{i=1}^{n} a_i^2 \equiv \frac{(k_{n,2,p}-1)k_{n,2,p}(2k_{n,2,p}-1)}{6} \pmod{k_{n,2,p}}.$$

如果$n \equiv 5$ 或$8 \pmod 9$，则$k_{n,2,p} \equiv 3$ 或$6 \pmod 9$ 且$3 \mid (4n-2)$。因此$3 \mid k_{n,2,p}$ 且$3 \nmid \frac{(k_{n,2,p}-1)k_{n,2,p}(2k_{n,2,p}-1)}{6}$，矛盾。 □

定理2.54. *如果$n \equiv 11, 12, 20$ 或$21 \pmod{27}$ 和$k_{n,3,p}$ 无平方因子，则不存在线性完美$(n, 3^{1/p})$ l_p 码。*

证明. 证明与定理2.48类似，我们只需证明对于$\mathbb{Z}_{k_{n,3,p}}$的任意n元集合$(a_1, \cdots, a_n)$ 有

$$\left\{ \pm a_i, \pm a_{j_1} \pm a_{j_2}, \pm a_{l_1} \pm a_{l_2} \pm a_{l_3} : 1 \le i \le n,\ 1 \le j_1 < j_2 \le n,\ 1 \le l_1 < l_2 < l_3 \le n \right\} \ne \mathbb{Z}_{k_{n,3,p}} \backslash \{0\}.$$

否则的话，我们有

$$2\sum_{i=1}^{n} a_i^2 + 2 \sum_{1 \le i < j \le n} ((a_i + a_j)^2 + (a_i - a_j)^2) + 2 \sum_{1 \le i < j < k \le n} ((a_i + a_j + a_k)^2 + (a_i + a_j - a_k)^2 +$$

$$(a_i - a_j + a_k)^2 + (a_i - a_j - a_k)^2) \equiv \sum_{i=1}^{k_{n,3,p}-1} i^2 \pmod{k_{n,3,p}}.$$

也就是

$$(4n^2-8n+6)\sum_{i=1}^{n}a_i^2 \equiv \frac{(k_{n,3,p}-1)k_{n,3,p}(2k_{n,3,p}-1)}{6} \pmod{k_{n,3,p}}.$$

如果$n \equiv 11,12,20$ 或$21 \pmod{27}$，则$k_{n,3,p} \equiv 3$ 或$6 \pmod 9$ 和$3 \mid (4n^2-8n+6)$。因此$3 \mid k_{n,3,p}$ 和$3 \nmid \frac{(k_{n,3,p}-1)k_{n,3,p}(2k_{n,3,p}-1)}{6}$，矛盾。 □

表2-5 列出了一些线性完美l_p 码的一些不存在结果，其中$2 \le p < \infty$。事实上，我们发现当$r = 2^{1/p}$ 和$n \le 5000$，有1073个数满足定理2.53的条件，以及当$r = 3^{1/p}$ 和$n \le 5000$，有701个数满足定理2.54的条件。

表 2-5　线性完美(n,r) l_p 码的不存在结果，其中$2 \le p < \infty$

r	n
$2^{1/p}$	$5,8,14,17,23,26,32,35,41,44,50,53,59,62,68,71,77,80,86,89,95,98$
$3^{1/p}$	$11,12,20,21,38,39,47,48,65,66,74,75,92,93$

评论2.55. 注意到对于其他半径，我们可以得到类似的结果。但是由于我们对集合$D_{p,n}$和$B_p^n(r)$的结构知道的较少，其中$2 \le p < \infty$，我们很难得到一般结果。

评论2.56.　*1.* 如果我们记环$\mathbb{Z}_m$ 的乘法半群为R_m，则上面两个小节我们用的主要技巧是选取一个同态$\chi : R_m \to R_m$，其中$\chi(a) = a^2$。选取其他同态可能可以得到其他结果。

2. 我们之前在评论*2.51*中指出我们的方法无法得到线性完美$(n,2)$ *Lee* 码的不存在性结果。最近，*Kim*[93] 利用选取$\chi(a) = a^{2k}$证明了一些关于线性完美$(n,2)$ *Lee* 码的不存在性结果。

2.2.4　准完美l_p 码

在这个小节，我们给出准完美$(n,2,q)$ Lee 码和准完美$(n,2^{1/p},q)$ l_p 码的一个代数构造。根据定理2.43，如果$|B_1^n(2)| < q < |B_1^n(3)|$且存在一个阶为$q$ 的Abel 群G和一个同态$\phi : \mathbb{Z}^n \mapsto G$使得$\phi$ 限制在$B_1^n(2)$上是一个单射，ϕ 限制在$B_1^n(3)$上是一个满射，则存在一个准完美$(n,2,q)$ Lee 码。类似地，如果$|B_p^n(2^{\frac{1}{p}})| < q < |B_p^n(3^{\frac{1}{p}})|$ 且存在一个阶为q 的Abel

群G和一个同态$\phi:\mathbb{Z}^n\mapsto G$使得$\phi$ 限制在$B_p^n(2^{\frac{1}{p}})$ 上是一个单射，ϕ 限制在$B_p^n(3^{\frac{1}{p}})$上是一个满射，则存在一个准完美$(n,2^{1/p},q)$ l_p 码。我们指出对于准完美$(n,2,q)$ Lee 码，如果维数n是固定的，则q 越小，码越接近完美。对于准完美$(n,2^{1/p},q)$ l_p 码也是类似的。

2.2.4.1 p=1

定理2.57. 设$q=2nm+1$ 是一个素数且n,m 是满足$n\equiv 1 \pmod 6$, $n\geq 7$ 和$n+1<m<3n+\frac{2(n-1)(n-2)}{3}$ 的整数。设g 是模q 的原根，记

$$
\begin{aligned}
S :=&\{1,2\}\bigcup\{1+g^{2mk},1-g^{2mk}:\ 1\leq k\leq\frac{n-1}{2}\},\\
T :=&\{1,2,3\}\bigcup\{1+g^{2mk},1-g^{2mk},1+2g^{2mk},1-2g^{2mk},2+g^{2mk},2-g^{2mk}:\ 1\leq k\leq\frac{n-1}{2}\}\\
&\bigcup\{1+g^{2mk}+g^{2ml},1+g^{2mk}-g^{2ml},1-g^{2mk}+g^{2ml},1-g^{2mk}-g^{2ml}:\ 1\leq k\leq\frac{n-1}{3},\\
&2k\leq l\leq n-1-k\}.
\end{aligned}
$$

如果$|\{ind_g(i) \pmod m : i\in S\}|=n+1$ 且$|\{ind_g(i) \pmod m : i\in T\backslash\{0\}\}|=m$，则存在一个准完美$(n,2,q)$ *Lee* 码。

证明. 容易看出$|B_1^n(2)|<q<|B_1^n(3)|$。接下来，我们将证明存在一个同态$\phi:\mathbb{Z}^n\mapsto\mathbb{Z}_q$ 使得ϕ 限制在$B_1^n(2)$ 上是一个单射以及ϕ 限制在$B_1^n(3)$ 上是一个满射。我们只需证明在$\mathbb{Z}_q$ 中存在n元集$(a_1,\cdots,a_n)$ 使得

$$
\begin{aligned}
&|\{0,\pm a_i,\pm 2a_i,\pm a_j\pm a_k:\ 1\leq i\leq n,\ 1\leq j<k\leq n\}|=k_{n,2},\ \text{(单射)}\\
&\{0,\pm a_i,\pm 2a_i,\pm 3a_i,\pm a_{j_1}\pm a_{j_2},\pm 2a_{j_1}\pm a_{j_2},\pm a_{j_1}\pm 2a_{j_2},\pm a_{k_1}\pm a_{k_2}\pm a_{k_3}:\ 1\leq i\leq n,\\
&1\leq j_1<j_2\leq n,\ 1\leq k_1<k_2<k_3\leq n\}=\mathbb{Z}_q\ \text{(满射)}.
\end{aligned}
$$

设$a_i=g^{2mi}, i=1,2,\cdots,n$。则我们有

$$
\begin{aligned}
&\{\pm g^{2mi},\pm 2g^{2mi},\pm g^{2mj}\pm g^{2mk}:\ 1\leq i\leq n,\ 1\leq j<k\leq n\}\\
&=S\cdot\{\pm g^{2mi}:\ 1\leq i\leq n\}\\
&=S\cdot\{g^{mi}:\ 1\leq i\leq 2n\}.
\end{aligned}
$$

由于$|S|=n+1$ 和$|\{\text{ind}_g(i) \pmod m : i\in S\}|=n+1$，则$|S\cdot\{g^{mi}:\ 1\leq i\leq 2n\}|=2n(n+1)=k_{n,2}-1$。注意到$0\notin S\cdot\{g^{mi}:\ 1\leq i\leq 2n\}$，因此$|\{0,\pm g^{2mi},\pm 2g^{2mi},\pm g^{2mj}\pm g^{2mk}:$

$1 \le i \le n,\ 1 \le j < k \le n\}| = k_{n,2}$。由于$|\{\text{ind}_g(i) \pmod m : i \in T\backslash\{0\}\}| = m$，我们有

$$\begin{aligned}
&\{\pm g^{2mi}, \pm 2g^{2mi}, \pm 3g^{2mi}, \pm g^{2mj_1} \pm g^{2mj_2}, \pm 2g^{2mj_1} \pm g^{2mj_2}, \pm g^{2mj_1} \pm 2g^{2mj_2},\\
&\pm g^{2mk_1} \pm g^{2mk_2} \pm g^{2mk_3} :\ 1 \le i \le n,\ 1 \le j_1 < j_2 \le n,\ 1 \le k_1 < k_2 < k_3 \le n\}\\
&\supseteq (T\backslash\{0\}) \cdot \{\pm g^{2mi} :\ 1 \le i \le n\}\\
&\supseteq (T\backslash\{0\}) \cdot \{g^{mi} :\ 1 \le i \le 2n\}\\
&\supseteq \mathbb{Z}_q\backslash\{0\},
\end{aligned}$$

因此

$$\begin{aligned}
&\big\{0, \pm g^{2mi}, \pm 2g^{2mi}, \pm 3g^{2mi}, \pm g^{2mj_1} \pm g^{2mj_2}, \pm 2g^{2mj_1} \pm g^{2mj_2}, \pm g^{2mj_1} \pm 2g^{2mj_2},\\
&\pm g^{2mk_1} \pm g^{2mk_2} \pm g^{2mk_3} :\ 1 \le i \le n, 1 \le j_1 < j_2 \le n,\ 1 \le k_1 < k_2 < k_3 \le n\big\} = \mathbb{Z}_q.
\end{aligned}$$

□

评论2.58. 在文献[25]中，对于任意的满足$p \ge 7$和$p \equiv \pm 5 \pmod{12}$的素数，作者构造了一个准完美$(2[\frac{p}{4}], 2, p^2)$ *Lee* 码。由于定理*2.57*中的准完美*Lee* 码的维数都是奇数，因此定理*2.57* 给出了一类具有新参数的准完美*Lee* 码。

表2-6 列出了一些准完美$(n, 2, q)$ Lee 码。我们来分析下我们构造的这些准完美Lee 码的品质。

例2.59. 设$n = 7,\ q = 197,\ g = 2$，根据定理*2.57*，我们得到一个准完美$(7, 2, 197)$ *Lee* 码C，其中$|V| = 197$。注意到$|B_1^7(2)| = 113$ 以及$|B_1^7(3)| = 575$，则$|V| = 197$ 更接近填充球而不是覆盖球，因此码很接近完美。

例2.60. 设$n = 31,\ q = 4093,\ g = 2$，根据定理*2.57*，我们得到一个准完美$(31, 2, 4093)$ *Lee* 码C，其中$|V| = 4093$。注意到$|B_1^{31}(2)| = 1985$ 以及$|B_1^{31}(3)| = 41727$，则$|V| = 4093$ 更接近填充球而不是覆盖球，因此码很接近完美。

表 2-6　准完美$(n,2,q)$ Lee 码

n	7	7	19	19	25	25	25	25	31	31	31
q	197	211	2129	2357	5651	5701	5851	6451	4093	5333	7937
g	2	2	3	2	2	2	2	3	2	2	3

2.2.4.2　$2 \le p < \infty$

定理2.61. 设$q = 2nm+1$ 是一个素数且n, m 是满足$n \equiv 1 \pmod 6$, $n \ge 7$ 和$n+1 \le m < n + \frac{2(n-1)(n-2)}{3}$的整数。设$g$ 是模q 原根，记

$$S := \{1\} \bigcup \{1+g^{2mk}, 1-g^{2mk} : 1 \le k \le \frac{n-1}{2}\},$$

$$T := \{1\} \bigcup \{1+g^{2mk}, 1-g^{2mk} : 1 \le k \le \frac{n-1}{2}\} \bigcup \{1+g^{2mk}+g^{2ml}, 1+g^{2mk}-g^{2ml},$$
$$1-g^{2mk}+g^{2ml}, 1-g^{2mk}-g^{2ml} : 1 \le k \le \frac{n-1}{3},\ 2k \le l \le n-1-k\}.$$

如果$|\{ind_g(i) \pmod m : i \in S\}| = n$ 和$|\{ind_g(i) \pmod m : i \in T\backslash\{0\}\}| = m$，则存在一个准完美$(n, 2^{1/p}, q)$ l_p 码。

证明. 证明与定理2.57的证明类似，我们只需证明在$\mathbb{Z}_q$中存在n 元集$(a_1, \cdots, a_n)$ 使得

$$|\{0, \pm a_i, \pm a_j \pm a_k, : 1 \le i \le n,\ 1 \le j < k \le n\}| = k_{n,2,p},$$

$$\{0, \pm a_i, \pm a_{j_1} \pm a_{j_2}, \pm a_{k_1} \pm a_{k_2} \pm a_{k_3} : 1 \le i \le n,\ 1 \le j_1 < j_2 \le n,\ 1 \le k_1 < k_2 < k_3 \le n\} = \mathbb{Z}_q.$$

设$a_i = g^{2mi}$, $i = 1, 2, \cdots, n$。则

$$\begin{aligned}
&\{\pm g^{2mi}, \pm g^{2mj} \pm g^{2mk} : 1 \le i \le n,\ 1 \le j < k \le n\} \\
&= S \cdot \{\pm g^{2mi} : 1 \le i \le n\} \\
&= S \cdot \{g^{mi} : 1 \le i \le 2n\}.
\end{aligned}$$

由于$|S| = n$ 和$|\{\text{ind}_g(i) \pmod m : i \in S\}| = n$，则$|S \cdot \{g^{mi} : 1 \le i \le 2n\}| = 2n^2 = k_{n,2,p} - 1$。注意到$0 \notin S \cdot \{g^{mi} : 1 \le i \le 2n\}$，因此$|\{0, \pm g^{2mi}, \pm g^{2mj} \pm g^{2mk}, : 1 \le i \le n,\ 1 \le j < k \le n\}| = k_{n,2,p}$。由于$|\{\text{ind}_g(i) \pmod m : i \in T\backslash\{0\}\}| = m$，我们有

$$\begin{aligned}
&\{\pm g^{2mi}, \pm g^{2mj_1} \pm g^{2mj_2}, \pm g^{2mk_1} \pm g^{2mk_2} \pm g^{2mk_3} : 1 \le i \le n,\ 1 \le j_1 < j_2 \le n,\ 1 \le k_1 < k_2 < k_3 \le n\} \\
&\supseteq (T\backslash\{0\}) \cdot \{\pm g^{2mi} : 1 \le i \le n\} \\
&\supseteq (T\backslash\{0\}) \cdot \{g^{mi} : 1 \le i \le 2n\} \\
&\supseteq \mathbb{Z}_q\backslash\{0\},
\end{aligned}$$

因此

$$\{0, \pm g^{2mi}, \pm g^{2mj_1} \pm g^{2mj_2}, \pm g^{2mk_1} \pm g^{2mk_2} \pm g^{2mk_3} : 1 \le i \le n,\ 1 \le j_1 < j_2 \le n,$$
$$1 \le k_1 < k_2 < k_3 \le n\} = \mathbb{Z}_q.$$

□

表2-7 列出了一些准完美$(n, 2^{1/p}, q)$ l_p 码，其中$2 \le p < \infty$。下面我们来分析下我们构造的准完美l_p 码的品质。

例2.62. 设$n = 31,\ q = 4093,\ g = 2$，根据定理*2.61*，我们有一个准完美$(31, 2^{1/p}, 4093)$ l_p 码C，其中$|V| = 4093$。注意到$|B_p^{31}(2^{1/p})| = 1923$ 和$|B_p^{31}(3^{\frac{1}{p}})| = 37883$，则$|V| = 4093$ 更接近填充球而不是覆盖球，因此码很接近完美。

表 2-7　准完美$(n, 2^{1/p}, q)$ l_p 码，其中$2 \le p < \infty$

n	19	19	25	31	31	31	31	31
q	2129	2357	5651	4093	5333	6883	7937	8123
g	3	2	2	2	2	2	3	2

3 自正交码及其在量子码中的应用

3.1 四次剩余双循环自对偶码

3.1.1 介绍

自对偶码是最有意思的一类线性码，它包含很多著名的纠错码，比如扩展Hamming码，扩展Golay 码，以及某些扩展二次剩余码。这些码在数据传输中有重要的应用[60,121,150]。自对偶码还与很多其他领域有很强的联系，包括加性量子码[23]，设计[9,10]，射影几何[103]，格[35]，不变量理论[120]。因此，构造好的自对偶码是一个重要的研究问题。目前有很多文章致力于分类或者构造自对偶码（参见文献[5,17,19,57,69,71,81,82,128]）。

另一类有趣的码是二次剩余码。它的码率接近$1/2$且有很大的极小距离。它还有一个很有效的译码方法—-置换译码，置换译码主要是基于这种码具有很大的自同构群。最初的研究者主要关注二次剩余码，而现在已经有一些高次剩余码的研究了[30,43,136]。

Karlin[91] 建立了自对偶码与二次剩余码的联系。他利用二次剩余来构造二元双循环码。后来，Pless[123]利用二次剩余来构造三元双循环码，给出了著名的Pless 对称码。在2002 年，Gaborit[55]提出了二次剩余双循环码，它包含了Karlin 的构造以及Pless 对称码。Gaborit同时还构造了GF(4)，GF(5)，GF(7) 和GF(9) 上的新的自对偶码无穷类。

我们的目标是利用高次剩余，特别是四次剩余，来构造双循环自对偶码。我们给出了在GF(2)，GF(3)，GF(4)，GF(8) 和GF(9) 上新的自对偶码无穷类，其中有些码具有比以前更好的参数。比如三元$[124, 62, 24]$ 自对偶码, 四元$[76, 38, 19]$ 自对偶码, GF(8) 上的$[58, 29, 18]$ 自对偶码以及GF(9) 上的$[58, 29, 18]$ 自对偶码。我们还考虑了这些码的自同构群。本部分的所有计算都是在3.40 GHz CPU 上用MAGMA V2.20-4[16] 完成的。

3.1.2 定义和一般结果

3.1.2.1 自对偶码

有限域GF(q) 上长为n，维数为k 的线性码C 指的是GF$(q)^n$ 上的k-维子空间，其中q 是

一个素数幂。码C 的一个生成矩阵G 是一个$k \times n$ 的矩阵且它的行张成整个码。Euclidean 内积定义为

$$(x, y) = \sum_{i=1}^{n} x_i y_i,$$

其中$x = (x_1, \ldots, x_n)$ 和$y = (y_1, \ldots, y_n)$。对于一个长为n 的线性码C，码

$$C^{\perp} = \{x \in \text{GF}(q)^n | (x, c) = 0 \text{ 对所有} c \in C\}$$

被称为它的Euclidean 对偶码。$C^{\perp}$ 是一个线性码，并且我们有$\dim(C) + \dim(C^{\perp}) = n$。$C$ 称为Euclidean 自正交如果$C \subseteq C^{\perp}$，和Euclidean 自对偶如果$C = C^{\perp}$。在这个部分，我们说自对偶都表示Euclidean 自对偶。注意到一个自对偶码的码长n 总是偶数以及维数是$n/2$。因此，我们一般不把一个自对偶码的维数写出来。

两个码字$x = (x_1, \ldots, x_n)$ 和$y = (y_1, \ldots, y_n)$ 之间的（Hamming）距离，记作$d(x, y)$，是x 与y 的具有不同数字的位置的个数。一个码字$x = (x_1, \ldots, x_n)$ 的（Hamming）重量$w(x)$ 是$w(x) = d(x, 0)$，一个码C 的极小距离$d(C)$ 定义为$d(C) = \min\{d(x, y) | x \neq y \in C\}$。那么对于自对偶码，我们有下面的结果。

定理3.1. [82,117,126,128] 设C 是GF(q) 上的码长为n，极小距离为$d(C)$ 的自对偶码。那么我们有

(i) 如果$q = 2$，则

$$d(C) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4; \text{ 如果} n \not\equiv 22 \pmod{24}, \\ 4\lfloor \frac{n}{24} \rfloor + 6; \text{ 如果} n \equiv 22 \pmod{24}. \end{cases}$$

(ii) 如果$q = 3$，则$d(C) \leq 3\lfloor \frac{n}{12} \rfloor + 3$。

(iii) 如果$q = 4$，则$d(C) \leq 4\lfloor \frac{n}{12} \rfloor + 4$。

(iv) $d(C) \leq \lfloor \frac{n}{2} \rfloor + 1$ 对于$q \neq 2, 3, 4$。

码C 被称为极值的如果上面的等式成立。一个自对偶码称为是最优的如果它具有该码长的最大可能的极小距离。一个极值码自然是一个最优码。

3.1.2.2 高次剩余，分圆，分圆数

设p 是一个奇素数，γ 是GF(p) 中的本原元。设$N > 1$ 是$p - 1$ 的因子。我们定义GF(p) 的N 阶分圆类$C_0, C_1, \ldots, C_{N-1}$：

$$C_i = \left\{ \gamma^{jN+i} | 0 \leq j \leq \frac{p-1}{N} - 1 \right\},$$

其中$0 \le i \le N-1$。也就是说C_0 是模p 的N 次剩余类，且$C_i = \gamma^i C_0$，$1 \le i \le N-1$。对于满足$0 \le m, n < N$ 的整数m, n，N 阶分圆数定义为

$$(m,n)_N = |(C_m + 1) \bigcap C_n|.$$

下面的引理总结了分圆数的一些基本性质。

引理3.2. [12] 设$p = ef + 1$ 为奇素数。则

1. 当$i \equiv i' \pmod e$ 且$j \equiv j' \pmod e$时，$(i,j)_e = (i',j')_e$。

2.

$$\begin{aligned}(i,j)_e &= (e-i, j-i)_e \\ &= \begin{cases} (j,i)_e; & \text{如果} f \text{ 是偶数}, \\ (j+e/2, i+e/2)_e; & \text{如果} f \text{ 是奇数}. \end{cases}\end{aligned}$$

3. $\sum_{i=0}^{e-1}(i,j)_e = f - \delta_j$，其中如果$j \equiv 0 \pmod e$，则$\delta_j = 1$，否则$\delta_j = 0$。

在下文，我们需要下面的由一个固定的原根决定的4 阶分圆数的精确值。

定理3.3. [12] 设p 是一个形如$p = 8l + 5$ 的素数。设g 是p 的一个原根。则4阶分圆数为

$$\begin{aligned}&(0,0)_4 = (2,0)_4 = (2,2)_4 = \frac{p-7+2x}{16}, \\ &(0,1)_4 = (1,3)_4 = (3,2)_4 = \frac{p+1+2x-4y}{16}, \\ &(0,2)_4 = \frac{p+1-6x}{16}, \\ &(0,3)_4 = (1,2)_4 = (3,1)_4 = \frac{p+1+2x+4y}{16}, \\ &(1,0)_4 = (1,1)_4 = (2,1)_4 = (2,3)_4 = (3,0)_4 = (3,3)_4 = \frac{p-3-2x}{16},\end{aligned}$$

其中x 和y 由下式唯一决定

$$p = x^2 + y^2,\ x \equiv 1 \pmod 4,\ y \equiv g^{\frac{p-1}{4}} x \pmod p.$$

评论3.4. 为了方便，在接下来的章节中，我们记$A := (0,0)_4$, $B := (0,1)_4$, $C := (0,2)_4$, $D := (0,3)_4$ 以及$E := (1,0)_4$。

3.1.2.3 一般结果

设p是形如$4k+1$的奇素数，它所对应的4阶分圆类为C_0, C_1, C_2和C_3。设m_0，m_1，m_2，m_3和m_4是GF(q)中的元素。我们下面定义GF(q)上的$p \times p$阶矩阵$C_p(m_0, m_1, m_2, m_3, m_4)$，它由$c_{ij}$, $1 \le i, j \le p$组成，其中

$$c_{ij} = \begin{cases} m_0; \text{ 如果} j = i, \\ m_1; \text{ 如果} j - i \in C_0, \\ m_2; \text{ 如果} j - i \in C_1, \\ m_3; \text{ 如果} j - i \in C_2, \\ m_4; \text{ 如果} j - i \in C_3. \end{cases}$$

我们定义I_n和J_n分别为$n \times n$阶单位矩阵和全1矩阵。则$C_p(1,0,0,0,0) = I_p$和$C_p(1,1,1,1,1) = J_p$。记$A_1 := C_p(0,1,0,0,0)$，$A_2 := C_p(0,0,1,0,0)$，$A_3 := C_p(0,0,0,1,0)$和$A_4 := C_p(0,0,0,0,1)$。注意到4阶分圆类形成一个4类的结合方案[40]，我们有下面的结果。

引理3.5. *如果p是形如$8l+5$的奇素数，则*

$$\begin{aligned} & A_1 = A_3^t \text{ 且} A_2 = A_4^t, \\ & A_1^2 = AA_1 + BA_2 + CA_3 + DA_4, \\ & A_2^2 = DA_1 + AA_2 + BA_3 + CA_4, \\ & A_3^2 = CA_1 + DA_2 + AA_3 + BA_4, \\ & A_4^2 = BA_1 + CA_2 + DA_3 + AA_4, \\ & A_1A_2 = A_2A_1 = AA_1 + EA_2 + DA_3 + BA_4, \\ & A_1A_3 = A_3A_1 = (2l+1)I_p + AA_1 + EA_2 + AA_3 + EA_4, \\ & A_1A_4 = A_4A_1 = EA_1 + DA_2 + BA_3 + EA_4, \\ & A_2A_3 = A_3A_2 = BA_1 + EA_2 + EA_3 + DA_4, \\ & A_2A_4 = A_4A_2 = (2l+1)I_p + EA_1 + AA_2 + EA_3 + AA_4, \\ & A_3A_4 = A_4A_3 = DA_1 + BA_2 + EA_3 + EA_4. \end{aligned}$$

证明. 结论可直接从A_i的定义和定理3.3得到。 □

在下文我们还需要下面的结果。

引理3.6. 如果p是形如$8l+5$的奇素数，则

$$\begin{aligned}&(m_0I_p+m_1A_1+m_2A_2+m_3A_3+m_4A_4)(m_0I_p+m_1A_1+m_2A_2+m_3A_3+m_4A_4)^t\\&=a_0I_p+a_1A_1+a_2A_2+a_3A_3+a_4A_4,\end{aligned}$$

其中

$$\begin{aligned}a_0=&m_0^2+(\frac{p-1}{4})(m_1^2+m_2^2+m_3^2+m_4^2),\\a_1=a_3=&m_0m_3+m_0m_1+(m_1m_3+m_1^2+m_3^2)A+(m_2m_4+m_1m_2+m_3m_4)B+m_1m_3C+\\&(m_2m_4+m_2m_3+m_1m_4)D+(m_1m_2+m_3m_4+m_1m_4+m_2m_3+m_2^2+m_4^2)E,\\a_2=a_4=&m_0m_4+m_0m_2+(m_2^2+m_4^2+m_2m_4)A+(m_1m_3+m_2m_3+m_1m_4)B+m_2m_4C+\\&(m_1m_2+m_3m_4+m_1m_3)D+(m_1m_4+m_2m_3+m_1m_2+m_3m_4+m_1^2+m_3^2)E.\end{aligned}$$

证明. 结果可直接由引理 3.5 得到。 □

为方便，我们记

$$\begin{aligned}\overrightarrow{m}:=&(m_0,m_1,m_2,m_3,m_4)\in \mathrm{GF}(q)^5,\\D_0(\overrightarrow{m}):=&m_0^2+(\frac{p-1}{4})(m_1^2+m_2^2+m_3^2+m_4^2),\\D_1(\overrightarrow{m}):=&m_0m_3+m_0m_1+(m_1m_3+m_1^2+m_3^2)A+(m_2m_4+m_1m_2+m_3m_4)B+m_1m_3C+\\&(m_2m_4+m_2m_3+m_1m_4)D+(m_1m_2+m_3m_4+m_1m_4+m_2m_3+m_2^2+m_4^2)E,\\D_2(\overrightarrow{m}):=&m_0m_4+m_0m_2+(m_2^2+m_4^2+m_2m_4)A+(m_1m_3+m_2m_3+m_1m_4)B+m_2m_4C+\\&(m_1m_2+m_3m_4+m_1m_3)D+(m_1m_4+m_2m_3+m_1m_2+m_3m_4+m_1^2+m_3^2)E.\end{aligned}$$

定义3.7. 设$P_n(R)$和$B_n(\alpha,R)$是分别对应于下面形式的生成矩阵的码：

$$\begin{pmatrix} I_n & R \end{pmatrix},$$

和

$$\begin{pmatrix} & \alpha & 1 & \cdots & 1 \\ & -1 & & & \\ I_{n+1} & \vdots & & R & \\ & -1 & & & \end{pmatrix},$$

其中$\alpha\in \mathrm{GF}(q)$以及R是一个$n\times n$的循环矩阵。码$P_n(R)$和$B_n(\alpha,R)$分别称为**纯双循环码**和**带边双循环码**。

设

$$P_p(\overrightarrow{m}) := P_p(m_0 I_p + m_1 A_1 + m_2 A_2 + m_3 A_3 + m_4 A_4),$$
$$B_p(\alpha, \overrightarrow{m}) := B_p(\alpha, m_0 I_p + m_1 A_1 + m_2 A_2 + m_3 A_3 + m_4 A_4).$$

则以$P_p(\overrightarrow{m})$和$B_p(\alpha, \overrightarrow{m})$为生成矩阵的码称之为**四次剩余双循环码**。

这个小节的主要结果是:

定理3.8. 设p是形如$8l+5$的奇素数，q是一个素数幂。设$\alpha \in \mathrm{GF}(q)$，$\overrightarrow{m} \in \mathrm{GF}(q)^5$。则

1. 以$P_p(\overrightarrow{m})$为生成矩阵的码是$\mathrm{GF}(q)$上的自对偶码当且仅当:
   (a) $D_0(\overrightarrow{m}) = -1$,
   (b) $D_1(\overrightarrow{m}) = 0$,
   (c) $D_2(\overrightarrow{m}) = 0$;
2. 以$B_p(\alpha, \overrightarrow{m})$为生成矩阵的码是$\mathrm{GF}(q)$上的自对偶码当且仅当:
   (a) $\alpha + p = -1$,
   (b) $-\alpha + m_0 + \frac{p-1}{4}(m_1 + m_2 + m_3 + m_4) = 0$,
   (c) $D_0(\overrightarrow{m}) = -2$,
   (d) $D_1(\overrightarrow{m}) = -1$,
   (e) $D_2(\overrightarrow{m}) = -1$.

证明. 结果可由

$$P_p(\overrightarrow{m}) P_p(\overrightarrow{m})^t = I_p + D_0(\overrightarrow{m}) I_p + D_1(\overrightarrow{m}) A_1 + D_2(\overrightarrow{m}) A_2 + D_1(\overrightarrow{m}) A_3 + D_2(\overrightarrow{m}) A_4,$$

以及

$$B_p(\alpha, \overrightarrow{m}) B_p(\alpha, \overrightarrow{m})^t = I_{p+1} + \begin{pmatrix} \alpha + p & S \cdots S \\ S & \\ \vdots & X \\ S & \end{pmatrix},$$

得到，其中$X = J_p + D_0(\overrightarrow{m}) I_p + D_1(\overrightarrow{m}) A_1 + D_2(\overrightarrow{m}) A_2 + D_1(\overrightarrow{m}) A_3 + D_2(\overrightarrow{m}) A_4$和$S = -\alpha + m_0 + \frac{p-1}{4}(m_1 + m_2 + m_3 + m_4)$。 □

3.1.3　特征2的域上的四次剩余双循环自对偶码

3.1.3.1　GF(2)上的自对偶码

在这个小节，我们在GF(2)上构造两个自对偶码无穷类。我们先给出下面两个引理。

引理3.9. 设p是形如$16k+5$的奇素数，其中k是一个非负整数。设g是p的一个固定的原根。如果$p=x^2+y^2,\ x\equiv 1\pmod 4,\ y\equiv g^{\frac{p-1}{4}}x\pmod p$。那么存在$t$，$s$使得$x=8t+1$，$y=4s+2$且$k\equiv t\pmod 2$。特别地，我们有下面的等式中的一个成立：

1. $A\equiv C\equiv D\equiv E\equiv 0\pmod 2,\ B\equiv 1\pmod 2$，
2. $A\equiv B\equiv C\equiv E\equiv 0\pmod 2,\ D\equiv 1\pmod 2$。

证明. 设$p=16k+5=x^2+y^2,\ x\equiv 1\pmod 4,\ y\equiv g^{\frac{p-1}{4}}x\pmod p$。则$x^2\equiv 1\pmod 8$，且$y^2\equiv 4\pmod 8, y\equiv 2\pmod 4$。

假设$x=4m+1$和$y=4s+2$，那么

$$16k+5=16m^2+8m+1+16s^2+16s+4,$$

也就是，

$$2k=2m^2+m+2s^2+2s,$$

所以$m\equiv 0\pmod 2$，那么存在t使得$m=2t$。

因此

$$2k=8t^2+2t+2s^2+2s,$$

也就是，

$$k-t=4t^2+s^2+s,$$

我们有$k\equiv t\pmod 2$。

从而，根据定理 3.3，如果$y\equiv 2\pmod 8$，那么

$$A\equiv C\equiv D\equiv E\equiv 0\pmod 2,\ B\equiv 1\pmod 2.$$

如果$y\equiv 6\pmod 8$，那么

$$A\equiv B\equiv C\equiv E\equiv 0\pmod 2,\ D\equiv 1\pmod 2.$$

□

引理3.10. 设p是一个形如$16k+13$的奇素数，其中k是一个非负整数。假设g是p的一个原根。如果$p=x^2+y^2$, $x\equiv 1 \pmod 4$, $y\equiv g^{\frac{p-1}{4}}x \pmod p$。那么存在整数$t, s$使得$x=8t+5$, $y=4s+2$且$k+t\equiv 1 \pmod 2$。特别地，我们有下面的等式中的一个成立：

1. $A\equiv C\equiv D\equiv 0 \pmod 2$, $B\equiv E\equiv 1 \pmod 2$，
2. $A\equiv B\equiv C\equiv 0 \pmod 2$, $D\equiv E\equiv 1 \pmod 2$。

证明. 设$p=16k+13=x^2+y^2$, $x\equiv 1 \pmod 4$, $y\equiv g^{\frac{p-1}{4}}x \pmod p$。我们有$x^2\equiv 1 \pmod 8$，所以$y^2\equiv 4 \pmod 8$, $y\equiv 2 \pmod 4$。

假设$x=4m+1$和$y=4s+2$，那么

$$16k+13=16m^2+8m+1+16s^2+16s+4,$$

从而有

$$2k+1=2m^2+m+2s^2+2s,$$

所以$m\equiv 1 \pmod 2$，从而存在整数t使得$m=2t+1$。

因此，

$$2k+1=8t^2+8t+2+2t+1+2s^2+2s,$$

也就是说，

$$k=4t^2+5t+s^2+s+1,$$

所以$k+t\equiv 1 \pmod 2$。

因此根据定理 3.3，如果$y\equiv 2 \pmod 8$，那么

$$A\equiv C\equiv D\equiv 0 \pmod 2,\ B\equiv E\equiv 1 \pmod 2.$$

如果$y\equiv 6 \pmod 8$，那么

$$A\equiv B\equiv C\equiv 0 \pmod 2,\ D\equiv E\equiv 1 \pmod 2.$$

□

现在我们有下面的定理：

定理3.11. 设p是一个奇素数，则下面的结论成立：

1. 如果p形如$16k+5$，则在GF(2)上以$B_p(0,1,0,1,1,1)$为生成矩阵的码是长为$2p+2$的自对偶码；

2. 如果p形如$16k+13$，则在GF(2)上以$P_p(0,0,1,1,1)$为生成矩阵的码是长为$2p$的自对偶码。

证明. 如果p形如$16k+5$，则由引理 3.9，我们有

$$\begin{aligned}
&\alpha + p = 16k+5 \equiv 1 \pmod 2,\\
&-\alpha + m_0 + (\frac{p-1}{4})(m_1+m_2+m_3+m_4) \equiv 0 \pmod 2,\\
&D_0(1,0,1,1,1) = 1 + (4k+1)(1+1+1) \equiv 0 \pmod 2,\\
&D_1(1,0,1,1,1) = 1 + A + 2B + 2D + 4E \equiv 1 \pmod 2,\\
&D_2(1,0,1,1,1) = 2 + 3A + B + C + D + 3E \equiv 1 \pmod 2.
\end{aligned}$$

由定理 3.8，在GF(2)上以$B_p(0,1,0,1,1,1)$为生成矩阵的码是长为$2p+2$的自对偶码。

若p形如$16k+13$，则由引理 3.10，我们有

$$\begin{aligned}
&D_0(0,0,1,1,1) = (4k+3)(1+1+1) \equiv 1 \pmod 2,\\
&D_1(0,0,1,1,1) = A + 2B + 2D + 4E \equiv 0 \pmod 2,\\
&D_2(0,0,1,1,1) = 3A + B + C + D + 3E \equiv 0 \pmod 2.
\end{aligned}$$

由定理 3.8，在GF(2)上以$P_p(0,0,1,1,1)$为生成矩阵的码是长为$2p$的自对偶码。 □

由Dirichlet定理知，存在无穷多个形如$16k+5$或$16k+13$的素数，因此定理 3.11中的两个类是无穷类。由这些构造得到的码大部分是极值的，最优的或者目前已知最好参数的码（见表 3-1）。特别地，码$[12,6,4]$和$[122,61,20]$同时还达到了已知最好参数的一般线性码[63]。表3-1列出了一些由定理 3.11构造的码。

评论3.12. 在下面的表中，我们将用**已知最好**来表示码在相应参数下达到了已知最好的极小距离，并且用**超越以前**来表示码的极小距离比已知结果更好。

3.1.3.2　GF(4)上的自对偶码

在这个小节，我们给出GF(4)上自对偶码的四个无穷类构造。设ζ是GF(4)的本原元，满足$\zeta^2+\zeta+1=0$，那么我们有下面的定理。

表 3-1　GF(2) 上由$P_p(0,0,1,1,1)$ 和$B_p(0,1,0,1,1,1)$ 构造的码

码	构造	评论
$[12,6,4]$	$B_5(0,1,0,1,1,1)$	极值的
$[26,13,6]$	$P_{13}(0,0,1,1,1)$	最优的[56]
$[58,29,10]$	$P_{29}(0,0,1,1,1)$	最优的[56]
$[108,54,16]$	$B_{53}(0,1,0,1,1,1)$	已知最好[56]
$[122,61,20]$	$P_{61}(0,0,1,1,1)$	已知最好[72]

定理3.13. 设p 是形如$16k+5$ 的素数，则在GF(4)上以$P_p(0,1,\zeta^2,1,\zeta)$ 为生成矩阵的码是长为$2p$的自对偶码。

证明. 如果p 是形如$16k+5$的素数，则由引理 3.9知

$$\begin{aligned}
&D_0(0,1,\zeta^2,1,\zeta) = (4k+1)(1+\zeta+1+\zeta^2) \equiv 1 \pmod 2,\\
&D_1(0,1,\zeta^2,1,\zeta) = 3A + C + (3\zeta^2+3\zeta)E \equiv 0 \pmod 2,\\
&D_2(0,1,\zeta^2,1,\zeta) = C \equiv 0 \pmod 2.
\end{aligned}$$

通过定理 3.8，我们得到在GF(4)上以$P_p(0,1,\zeta^2,1,\zeta)$ 为生成矩阵的码是长为$2p$的自对偶码。

□

定理3.14. 设p 是形如$16k+5$的素数。假设分圆数$(0,1)_4$ 是奇的。则在GF(4)上以$B_p(0,\zeta,1,\zeta^2,0,0)$ 为生成矩阵的码是长为$2p+2$ 的自对偶码。

证明. 如果p 是形如$16k+5$ 的奇素数且分圆数$(0,1)_4$ 是奇的，也就是$B = (0,1)_4 \equiv 1 \pmod 2$。那么根据引理3.9，我们有

$$\begin{aligned}
&\alpha + p = 16k+5 \equiv 1 \pmod 2,\\
&-\alpha + m_0 + (\frac{p-1}{4})(m_1+m_2+m_3+m_4) \equiv 0 \pmod 2,\\
&D_0(\zeta,1,\zeta^2,0,0) = -4k\zeta^2 \equiv 0 \pmod 2,\\
&D_1(\zeta,1,\zeta^2,0,0) = \zeta + A + \zeta^2 B + E \equiv 1 \pmod 2,\\
&D_2(\zeta,1,\zeta^2,0,0) = 1 + \zeta A + \zeta^2 D + \zeta E \equiv 1 \pmod 2.
\end{aligned}$$

由定理 3.8，在GF(4)上以$B_p(0,\zeta,1,\zeta^2,0,0)$ 为生成矩阵的码是长为$2p+2$ 的自对偶码。　□

定理3.15. 设p是形如$16k+13$的奇素数。假设分圆数$(0,1)_4$是奇的，则在GF(4)上以$P_p(\zeta,\zeta,\zeta,\zeta^2,0)$和$B_p(0,\zeta,1,\zeta,\zeta,\zeta^2)$为生成矩阵的码分别是长为$2p$和$2p+2$的自对偶码。

证明. 如果p是形如$16k+13$的奇素数以及分圆数$(0,1)_4$是奇的，也就是$B=(0,1)_4\equiv 1 \pmod 2$。由引理 3.10，我们得到

$$\begin{aligned}
&D_0(\zeta,\zeta,\zeta,\zeta^2,0)=\zeta^2+(4k+3)(2\zeta^2+\zeta)\equiv 1 \pmod 2,\\
&D_1(\zeta,\zeta,\zeta,\zeta^2,0)=\zeta+\zeta^2B+C+D+E\equiv 0 \pmod 2,\\
&D_2(\zeta,\zeta,\zeta,\zeta^2,0)=\zeta^2+\zeta^2A+2B+\zeta D+\zeta^2E\equiv 0 \pmod 2.
\end{aligned}$$

根据定理 3.8，在GF(4)上以$P_p(\zeta,\zeta,\zeta,\zeta^2,0)$为生成矩阵的码分别是长为$2p$的自对偶码。

由于我们有

$$\begin{aligned}
&\alpha+p=16k+13\equiv 1 \pmod 2,\\
&-\alpha+m_0+(\frac{p-1}{4})(m_1+m_2+m_3+m_4)\equiv 0 \pmod 2,\\
&D_0(\zeta,1,\zeta,\zeta,\zeta^2)=(4k+4)\zeta^2\equiv 0 \pmod 2,\\
&D_1(\zeta,1,\zeta,\zeta,\zeta^2)=-1+(2+\zeta)B+\zeta C+(1+2\zeta^2)D+(2\zeta^2+\zeta)E\equiv 1 \pmod 2,\\
&D_2(\zeta,1,\zeta,\zeta,\zeta^2)=-\zeta+(\zeta+2\zeta^2)B+C+(1+2\zeta)D+(1+2\zeta^2)E\equiv 1 \pmod 2.
\end{aligned}$$

根据定理 3.8，在GF(4)上以$B_p(0,\zeta,1,\zeta,\zeta,\zeta^2)$为生成矩阵的码分别是长为$2p+2$的自对偶码。 □

表3-2 列出了一些由上面的三个定理生成的码的例子，所有的码都是极值的或者已知最好参数的码。特别地，码$[76,38,19]$具有比以前更好的参数[65]。另外，码$[74,37,18]$和$[76,38,19]$还达到了一般线性码的最好参数[63]。

3.1.3.3　GF(8)上的自对偶码

在这个小节，我们给出GF(8)上自对偶码的一个构造。设ζ是GF(8)上的本原元，满足$\zeta^3+\zeta+1=0$，那么我们有下面的定理。

定理3.16. 设p是形如$16k+13$的奇素数，那么GF(8)上以$P_p(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$为生成矩阵的码是长为$2p$的自对偶码。

表 3-2　GF(4) 上由$P_p(0,1,\zeta^2,1,\zeta)$, $P_p(\zeta,\zeta,\zeta,\zeta^2,0)$, $B_p(0,\zeta,1,\zeta^2,0,0)$ 和$B_p(0,\zeta,1,\zeta,\zeta,\zeta^2)$构造的码

码	构造	评论
$[10,5,4]$	$P_5(0,1,\zeta^2,1,\zeta)$	极值的
$[26,13,8]$	$P_{13}(\zeta,\zeta,\zeta,\zeta^2,0)$	已知最好[56]
$[58,29,15]$	$P_{29}(\zeta,\zeta,\zeta,\zeta^2,0)$	已知最好[56]
$[60,30,16]$	$B_{29}(0,\zeta,1,\zeta,\zeta,\zeta^2)$	已知最好[65]
$[74,37,18]$	$P_{37}(0,1,\zeta^2,1,\zeta)$	已知最好[65]
$[76,38,19]$	$B_{37}(0,\zeta,1,\zeta^2,0,0)$	超越以前[65]

证明. 如果$p=16k+13$，那么由引理 3.10得

$$
\begin{aligned}
&D_0(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)=(4k+2)\zeta+1\equiv 1 \pmod 2,\\
&D_1(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)=\zeta^2+A+\zeta^2B+\zeta^3C+\zeta^2D\equiv 0 \pmod 2,\\
&D_2(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)=\zeta^6A+\zeta B+\zeta^6C+\zeta D+\zeta E\equiv 0 \pmod 2.
\end{aligned}
$$

根据定理 3.8，我们得到GF(8)上以$P_p(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$ 为生成矩阵的码是长为$2p$ 的自对偶码。 □

表3-3 列出了一些这种码的例子。其中码$[26,13,10]$ 达到了一般线性码的最好参数[63]，并且码长为58 的码是新的。

表 3-3　GF(8)上由$P_p(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$ 构造的码

码	构造	评论
$[26,13,10]$	$P_{13}(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$	已知最好[65]
$[58,29,18]$	$P_{29}(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$	

3.1.4　特征为3的域上的四次剩余双循环自对偶码

3.1.4.1　GF(3)上的自对偶码

在这个小节，我们给出GF(3)上自对偶码的两个构造：$B_p(1,1,0,1,2,1)$ 和$B_p(1,1,0,0,1,1)$，我们还列出了一些这些构造的例子。我们首先给出下面的引理。

引理3.17. 设p是形如$24k+13$的奇素数，其中k是非负整数。假设g是p的原根。如果$p=x^2+y^2,\ x\equiv 1\pmod 4,\ y\equiv g^{\frac{p-1}{4}}x\pmod p$。则存在整数$m,\ n$满足$m\equiv 2\pmod 3$或者$n\equiv 1\pmod 3$，使得$x=4m+1$，$y=4n+2$。并且有

1. 如果$m\equiv 2\pmod 3$，则$A\equiv 0\pmod 3$，$C+1\equiv 0\pmod 3$和$2B+C+2D+2E\equiv 0\pmod 3$；

2. 如果$n\equiv 1\pmod 3$，则$2+A+B+2E\equiv 0\pmod 3$和$2+A+D+2E\equiv 0\pmod 3$。

证明. 假设$m\not\equiv 2\pmod 3$，则

$$24k+13=16m^2+8m+1+16n^2+16n+4,$$

也就是说

$$3k+1=2m^2+m+2n^2+2n.$$

由于

$$2m^2+m=\begin{cases}0;\ \text{如果}m\equiv 0,1\pmod 3,\\ 1;\ \text{如果}m\equiv 2\pmod 3,\end{cases}$$

且

$$2n^2+2n=\begin{cases}0;\ \text{如果}n\equiv 0,2\pmod 3,\\ 1;\ \text{如果}n\equiv 1\pmod 3.\end{cases}$$

因此$n\equiv 1\pmod 3$。

如果$m\equiv 2\pmod 3$，则$4A=\frac{p-7+2x}{4}=\frac{24k+13-7+8m+2}{4}\equiv 0\pmod 3$且$16(C+1)=24k+13+1-6x+16\equiv 0\pmod 3$。由于$A$和$C+1$是整数，我们有$A\equiv 0\pmod 3$和$C+1\equiv 0\pmod 3$。并且

$$\begin{aligned}&2(2B+C+2D+2E)\\&=\frac{2p+2+4x}{4}+\frac{p+1-6y}{8}+\frac{p-3-2x}{4}\\&=21k-m+11\\&\equiv 0\pmod 3,\end{aligned}$$

以及$2B+C+2D+2E$是整数，从而$2B+C+2D+2E\equiv 0\pmod 3$。

如果$n \equiv 1 \pmod 3$，则

$$\begin{aligned}
&2(2+A+B+2E)\\
&=4+\frac{p-7+2x}{8}+\frac{p+1+2x-4y}{8}+\frac{p-3-2x}{4}\\
&=12k-2n+8\\
&\equiv 0 \pmod 3,
\end{aligned}$$

且

$$\begin{aligned}
&2(2+A+D+2E)\\
&=4+\frac{p-7+2x}{8}+\frac{p+1+2x+4y}{8}+\frac{p-3-2x}{4}\\
&=12k+2n+10\\
&\equiv 0 \pmod 3.
\end{aligned}$$

由于$2+A+B+2E$ 和$2+A+D+2E$ 是整数，我们有$2+A+B+2E \equiv 0 \pmod 3$ 和$2+A+D+2E \equiv 0 \pmod 3$。 □

作为上面引理的一个应用，我们有下面的定理。

定理3.18. 设p 是形如$24k+13$的整数。那么$p = x^2+y^2$，其中$x = 4m+1$，$y = 4n+2$ 且m, n 是满足$m \equiv 2 \pmod 3$ 或者$n \equiv 1 \pmod 3$的整数。并且我们有

1. 如果$m \equiv 2 \pmod 3$，那么GF(3)上以$B_p(1,1,0,1,2,1)$ 为生成矩阵的码是自对偶码；
2. 如果$n \equiv 1 \pmod 3$，那么GF(3)上以$B_p(1,1,0,0,1,1)$ 为生成矩阵的码是自对偶码。

证明. 设p 是形如$24k+13$ 的奇素数。假设$m \equiv 2 \pmod 3$，则由引理 3.17，我们有

$$\begin{aligned}
&\alpha+p = 24k+14 \equiv 2 \pmod 3,\\
&-\alpha+m_0+(\frac{p-1}{4})(m_1+m_2+m_3+m_4) \equiv 0 \pmod 3,\\
&D_0(1,0,1,2,1) = 36k+19 \equiv 1 \pmod 3,\\
&D_1(1,0,1,2,1) = 2+4A+3B+3D+6E \equiv 2 \pmod 3,\\
&D_2(1,0,1,2,1) = 2+3A+2B+C+2D+8E \equiv 2 \pmod 3.
\end{aligned}$$

根据定理 3.8，GF(3)上以$B_p(1,1,0,1,2,1)$ 为生成矩阵的码是自对偶码。

假设$n \equiv 1 \pmod 3$，那么由引理 3.17，我们有

$$\begin{aligned}
&\alpha + p = 24k + 14 \equiv 2 \pmod 3,\\
&-\alpha + m_0 + (\frac{p-1}{4})(m_1 + m_2 + m_3 + m_4) \equiv 0 \pmod 3,\\
&D_0(1,0,0,1,1) = 12k + 7 \equiv 1 \pmod 3,\\
&D_1(1,0,0,1,1) = 1 + A + B + 2E \equiv 2 \pmod 3,\\
&D_2(1,0,0,1,1) = 1 + A + D + 2E \equiv 2 \pmod 3.
\end{aligned}$$

根据定理 3.8，GF(3)上以$B_p(1,1,0,0,1,1)$ 为生成矩阵的码是自对偶码。 □

表3-4 列出了这些码的一些例子。注意到表3-4中所有的码都达到了一般线性码的最好参数[63]。

表 3-4　GF(3)上由$B_p(1,1,0,1,2,1)$ 和$B_p(1,1,0,0,1,1)$ 构造的码

码	构造	评论
$[28,14,9]$	$B_{13}(1,1,0,1,2,1)$	极值的
$[76,38,18]$	$B_{37}(1,1,0,0,1,1)$	已知最好[56]
$[124,62,24]$	$B_{61}(1,1,0,0,1,1)$	已知最好[63]

3.1.4.2　GF(9)上的自对偶码

在这个小节，我们给出GF(9)上自对偶码的两个无穷类的构造。设ζ 是GF(9) 中的本原元，满足$\zeta^2 + 2\zeta + 2 = 0$，则我们有下面的引理。

引理3.19. *设p 是形如$24k+5$ 的奇素数，其中k 是非负整数。则$C \equiv 0 \pmod 3$ 且$2 + B + D + 2E \equiv 0 \pmod 3$。*

证明. 设$p = x^2 + y^2$ 且$x \equiv 1 \pmod 4$。假设存在整数m使得$x = 4m + 1$ 。如果$p = 24k + 5$，那么根据定理 3.3有

$$16C = p + 1 - 6x = 24k + 6 - 6x \equiv 0 \pmod 3.$$

由于C 是整数，则$C \equiv 0 \pmod 3$。类似的，我们有

$$\begin{aligned}
&2 + B + D + 2E \\
&= 2 + \frac{p+1+2x}{8} + \frac{p-3-2x}{8} \\
&= 2 + \frac{p-1}{4} \\
&= 6k + 3 \\
&\equiv 0 \pmod 3.
\end{aligned}$$

□

那么我们有下面的定理

定理3.20. 设p 是形如$24k+5$的奇素数，其中k 是非负整数。则在GF(9)上以$P_p(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7)$ 为生成矩阵的码是长为$2p$的自对偶码。

证明. 如果$p = 24k + 5$，由引理 3.19 我们有，

$$\begin{aligned}
&D_0(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7) = 2, \\
&D_1(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7) = \zeta^7 + \zeta^3 B + \zeta^2 C + \zeta^3 D + \zeta^7 E \equiv 0 \pmod 3, \\
&D_2(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7) = \zeta^5 + \zeta B + \zeta^6 C + \zeta D + \zeta^5 E \equiv 0 \pmod 3.
\end{aligned}$$

根据定理 3.8，GF(9)上以$P_p(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7)$ 为生成矩阵的码是长为$2p$的自对偶码。 □

对于p 是形如$24k + 13$的奇素数，我们有下面的定理。

定理3.21. 设p 是形如$24k + 13$的奇素数。那么$p = x^2 + y^2$，其中$x = 4m + 1$，$y = 4n + 2$，m, n 是满足$m \equiv 2 \pmod 3$ 或者$n \equiv 1 \pmod 3$的整数。如果$m \equiv 2 \pmod 3$ 则在GF(9)上以$P_p(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7)$ 为生成矩阵的码是长为$2p$ 的自对偶码。

证明. 如果$p = 24k + 13$ 且$m \equiv 2 \pmod 3$，根据引理 3.17有

$$\begin{aligned}
&D_0(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7) = 2 + (6k + 3)\zeta^5 \equiv 2 \pmod 3, \\
&D_1(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7) = \zeta^5 + 2A + \zeta^5 C \equiv 0 \pmod 3, \\
&D_2(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7) = \zeta^5 + B + \zeta^6 C + D + E \equiv 0 \pmod 3.
\end{aligned}$$

由定理 3.8，我们有GF(9)上以$P_p(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7)$ 为生成矩阵的码是长为$2p$ 的自对偶码。□

表3-5 列出了上面两个构造的一些例子。其中码$[10, 5, 6]$ 和$[58, 29, 18]$ 达到了一般线性码的最好参数[63]。

表 3-5　GF(9)上由$P_p(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7)$ 和$P_p(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7)$ 构造的码

码	构造	评论
$[10, 5, 6]$	$P_5(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7)$	极值的
$[26, 13, 10]$	$P_{13}(\zeta^2, 1, \zeta^7, \zeta^5, \zeta^7)$	已知最好[65]
$[58, 29, 18]$	$P_{29}(\zeta^2, \zeta, \zeta^7, \zeta, \zeta^7)$	已知最好[63]

评论3.22. 对于$p = 24k + 13 = x^2 + y^2$，其中$x = 4m + 1$，$y = 4n + 2$，m, n 是满足$n \equiv 1 \pmod 3$的整数。我们相信也能给出相应的双循环码的构造。但是满足这个条件的最小的数是37，且在GF(9)上决定$[74, 37]$自对偶码的极小距离是困难的。

评论3.23. 我们还可能得到GF(2)，GF(3)，GF(4)，GF(8) 和GF(9)上的其他纯双循环（带边双循环）码，在这里我们只列出那些具有好的极小距离的码。

3.1.5　自同构群

在这个章节，我们证明一些关于双循环码的自同构群的结果。我们首先考虑GF(q)上以$B_p(0, m_0, m_1, m_2, m_3, m_4)$为生成矩阵的码的自同构群，其中$p$ 是形如$8k + 5$的素数且q 是一个素数幂。由文献[55]，我们考虑GF(q)上维数为$p + 1$的线性空间V_{p+1} 和它的一组基向量：$e_\infty = (1, 0, \ldots, 0)$, $e_0 = (0, 1, \ldots, 0), \ldots,$ $e_{p-1} = (0, 0, \ldots, 1)$。设$g$ 是GF(p) 的本原元且

$$\chi(a) = \begin{cases} m_0; \text{ 如果} a = 0, \\ m_1; \text{ 如果} a = g^{4i} \text{ 对于某个} i, \\ m_2; \text{ 如果} a = g^{4i+1} \text{ 对于某个} i, \\ m_3; \text{ 如果} a = g^{4i+2} \text{ 对于某个} i, \\ m_4; \text{ 如果} a = g^{4i+3} \text{ 对于某个} i. \end{cases}$$

我们定义作用在V_{p+1}上的变换S_p：

$$e_\infty S_p = \sum_{j=0}^{p-1} e_j,\ e_i S_p = \sum_{j=0}^{p-1} \chi(j-i)e_j,\ i = 0, \ldots, p-1.$$

对于GF(p)中任意的元素b，我们定义位移变换$S(b)$：

$$e_\infty S(b) = e_\infty,\ e_i S(b) = e_{i+b},\ i = 0, \ldots, p-1.$$

对于$s \neq 0$，我们定义四次变换$T(s^4)$：

$$e_\infty T(s^4) = e_\infty,\ e_i T(s^4) = e_{is^4},\ i = 0, \ldots, p-1.$$

则我们有下面的命题。

命题3.24. *对于任意的$b \in$ GF(p)，$0 \neq s \in$ GF(p) 以及GF(q)上的变换S_p有：*

$$S_p S(b) = S(b) S_p \text{ 和} S_p T(s^4) = T(s^4) S_p.$$

证明. 为了证明等式，我们只需要分别计算等式的左边和等式的右边作用在基向量上的结果：

$$e_\infty S_p S(b) = \sum_{j=0}^{p-1} e_j S(b) = \sum_{j=0}^{p-1} e_{j+b},$$

$$e_\infty S(b) S_p = e_\infty S_p = \sum_{j=0}^{p-1} e_j.$$

由于当j遍历GF(p)时，$j+b$遍历整个GF(p)，上面两个等式相等。对于$i = 0, \ldots, p-1$，

$$e_i S_p S(b) = \sum_{j=0}^{p-1} \chi(j-i) e_j S(b) = \sum_{j=0}^{p-1} \chi(j-i) e_{j+b},$$

$$e_i S(b) S_p = e_{i+b} S_p = \sum_{j=0}^{p-1} \chi(j-i-b) e_j,$$

这两个向量也相等。因此$S_p S(b) = S(b) S_p$。

由于

$$e_\infty S_p T(s^4) = \sum_{j=0}^{p-1} e_j T(s^4) = \sum_{j=0}^{p-1} e_{js^4},$$

$$e_\infty T(s^4) S_p = e_\infty S_p = \sum_{j=0}^{p-1} e_j,$$

并且对于$i = 0, \ldots, p-1$，

$$e_i S_p T(s^4) = \sum_{j=0}^{p-1} \chi(j-i) e_j T(s^4) = \sum_{j=0}^{p-1} \chi(j-i) e_{js^4},$$

$$e_i T(s^4) S_p = e_{is^4} S_p = \sum_{j=0}^{p-1} \chi(j - is^4 - b) e_j,$$

因此$S_p T(s^4) = T(s^4) S_p$。 □

下面我们定义由下面的变换生成的群$R(p)$ (p 具有形式$8k+5$)：

1. 循环位移：$x \mapsto x + b$，其中b 在GF(p)中，
2. 四次变换：$x \mapsto s^4 x$，其中$s \neq 0$ 在GF(p)中。

那么我们有下面的结果：

定理3.25. GF(q)上任意以$B_p(0, m_0, m_1, m_2, m_3, m_4)$为生成矩阵的码在群$R(p)$同时作用在生成矩阵$B_p(0, m_0, m_1, m_2, m_3, m_4)$两部分是不变的。

证明. 由于$B_p(0, m_0, m_1, m_2, m_3, m_4) = \begin{pmatrix} I & S_p \end{pmatrix}$. 那么作用任意的$S(b)$和$T(s^4)$中的变换$M$，根据命题 3.24我们有

$$\begin{pmatrix} I & S_p \end{pmatrix} \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix} = \begin{pmatrix} M & S_p M \end{pmatrix} = \begin{pmatrix} M & M S_p \end{pmatrix} = M \begin{pmatrix} I & S_p \end{pmatrix}.$$

这就证明了结论。 □

定理3.26. GF(q)上以$P_p(m_0, m_1, m_2, m_3, m_4)$为生成矩阵的码的自同构群包含一个大小为$\frac{p(p-1)}{4}$的群。

证明. 根据循环位移：$x \to x + b$ 和四次变换：$x \to s^4 x$ 的构造，其中b 在GF(p)中，$s \neq 0$ 在GF(p)中。他们可以同时作用在生成矩阵的两部分且不变，并且他们形成一个大小为$\frac{p(p-1)}{4}$的群。从而结论成立。 □

3.1.6　二元四次剩余四循环自对偶码

在这个章节，我们定义四次剩余四循环码。同时我们还得到一个二元自对偶码的无穷类。

定义3.27. 设$F_n(R_1, R_2)$是以形如

$$\begin{pmatrix} & R_1 & R_2 \\ I_{2n} & & \\ & R_2^t & R_1^t \end{pmatrix},$$

为生成矩阵的码，其中R_1, R_2是$n \times n$循环矩阵。码$F_n(R_1, R_2)$称为**四循环码**。假设p是一个形如$8k+5$的奇素数，R_1和R_2形如$m_0 I_p + m_1 A_1 + m_2 A_2 + m_3 A_3 + m_4 A_4$，其中$m_i \in \mathrm{GF}(q)$，$i = 0, 1, 2, 3, 4, 5$。那么码$F_p(R_1, R_2)$称为**四次剩余四循环码**。

我们有下面的定理。

定理3.28. 设p是形如$16k+13$的奇素数，则$\mathrm{GF}(2)$上以$F_p(A_4, I_p + A_2 + A_3 + A_4)$为生成矩阵的码是长为$4p$的自对偶码。

证明. 如果p具有形式$16k+13$，则

$$F_p(A_4, I_p + A_2 + A_3 + A_4) F_p(A_4, I_p + A_2 + A_3 + A_4)^t = I_{2p} + \begin{pmatrix} X & Y \\ Y & X \end{pmatrix},$$

其中$X = (1+A+2B+2D+5E)(A_1+A_3)+(2+4A+B+C+D+3E)(A_2+A_4)+(16k+13)I_p$以及$Y = 2A_4(I_p + A_2 + A_3 + A_4)$。那么根据引理 3.10，在$\mathrm{GF}(2)$上$F_p(A_4, I_p + A_2 + A_3 + A_4) F_p(A_4, I_p + A_2 + A_3 + A_4)^t = 0$。所以$\mathrm{GF}(2)$上以$F_p(A_4, I_p + A_2 + A_3 + A_4)$为生成矩阵的码是长为$4p$的自对偶码。 □

例3.29. 设$p = 13$。应用定理 *3.28*我们得到二元$[52, 26, 10]$自对偶码，且它是最优的*[56]*。

3.1.7 总结

自对偶码在数据传输中有重用应用，但是去构造一个具有大的极小距离的自对偶码是不容易的。我们甚至没发现一个渐进好的自对偶码无穷类，即使它已经被证明存在[112,116]。最有名的自对偶码是二次剩余双循环自对偶码，它的极小距离有一个平方根界[24]。在这个章节，我们利用四次剩余构造了几个自对偶码的无穷类。它们中有些码的参数比已知结果更好。数据显示它的极小距离可能有一个类似与二次剩余双循环自对偶码的界。

我们知道最有效的译二次剩余码的方法是置换译码，它是利用这个码具有大的自同构群来译码的[115]。在3.1.5节，我们证明了我们构造的码也具有大的自同构群。所以很可能

我们的码也有一个很好的译码方法。

另一个值得指出来的是在3.1.6节，我们用四次剩余给了一个二元四循环自对偶码的一个无穷类。当然我们还可以在其他域上给出类似的构造。由于码长会变得很大，我们没法给出任何的例子，但我们仍相信这些构造能够得到好的自对偶码。

3.2　量子码

3.2.1　介绍

量子纠错码在量子计算和量子通信中有重要作用。在文献[22,23]中，Calderbank 等人发现可以利用$\mathbb{F}_2$ 或$\mathbb{F}_4$ 上的经典自正交码来构造量子码。而这很快被推广到非二元情形[8,127]。自此之后，利用经典Euclidean 自正交码或Hermitian 自正交码，很多量子码已经被构造出来了[3,32,141]。

设q 是一个素数幂，一个$[[n,k,d]]_q$ 量子码是指$\mathbb{C}^{q^n}$ 上极小距离为d 的q^k 维子空间，它能发现$d-1$ 个量子错误和纠正至多$\lfloor\frac{d-1}{2}\rfloor$ 个量子错误。与经典编码理论类似，量子编码理论的一个核心任务是构造具有好的参数的量子码。下面的定理给出了量子码极小距离的下界。

定理3.30. ([92,97] 量子*Singleton* 界) 具有参数$[[n,k,d]]_q$ 的量子码满足

$$2d \leq n-k+2.$$

一个达到量子Singleton 界的量子码称为量子极大距离可分码。就像经典线性码一样，量子极大距离可分码也是一类重要的量子码。构造量子极大距离可分码已经成为近几年量子码理论的一个中心课题。目前有很多方法去构造量子码，而下面的定理是最常用一个的构造方法。

定理3.31. ([8] Hermitian 构造) 如果C 是一个$[n,k,d]_{q^2}$线性码满足$C^{\perp H} \subseteq C$，则存在一个$[[n,2k-n,\geq d]]_q$量子码。

与经典线性码类似，量子码也有繁衍原则。

定理3.32. ([51] 繁衍原则) 假设存在一个$[[n,k,d]]_q$ 量子码。那么

1. (子码) 存在一个$[[n, k-1, \geq d]]_q$ 量子码；

2. (加长) 存在一个$[[n+1, k, \geq d]]_q$ 量子码；

3. (刺穿) 存在一个$[[n-1, k, \geq d-1]]_q$ 量子码；

4. 存在一个$[[n, k, d-1]]_q$ 量子码。

对于量子极大距离可分码，我们有下面的推论。

推论3.33. *如果存在一个Hermitian 自正交$[n, k, n-k+1]_{q^2}$极大距离可分码，则存在一个$[[n, n-2k, k+1]]_q$ 量子极大距离可分码。*

目前，关于量子极大距离可分码有很多的研究工作（参见文献[14,31,50,64,66,86,88–90,101,102,110,162]）。然而，去构造具有码长$n > q+1$和极小距离$d > \frac{q}{2}$的量子极大距离可分码是不容易的。在这部分，我们将分别利用常循环码和广义Reed-Solomon码去构造量子极大距离可分码。

基于Reed-Solomon码，可以构造一个好的Hermitian自正交码类。但是一个q元Reed-Solomon码的码长是小于等于q。利用赋值的想法，人们成功推广了Reed-Solomon码并构造了几类码长大于q的好的线性码（参见文献[49,87,111,145,158]）。然而，这些码一般来说并不是Hermitian自正交的。在这部分，我们首先利用赋值的想法给出一个线性码的构造，然后决定它们的对偶码。这样，我们得到Hermitian自正交码和新的量子码。有些量子码的参数比已知的在线表格[45,63]中的参数好。

3.2.2 准备工作

记$\mathbb{F}_q$ 为q阶有限域，其中q 是一个素数幂。$\mathbb{F}_q$上长为n 的线性码是$\mathbb{F}_q^n$的子空间。给定两个向量$x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_q^n$，我们对两种内积感兴趣。一种是Euclidean 内积，定义为

$$\langle x, y\rangle_E = \sum_{i=0}^{n-1} x_i y_i.$$

当$q = l^2$，其中l 是一个素数幂，则我们可以考虑它们的Hermitian 内积，定义为

$$\langle x, y\rangle_H = x_0 y_0^l + x_1 y_1^l + \cdots + x_{n-1} y_{n-1}^l.$$

码C 的Euclidean 对偶码定义为

$$C^{\perp E} = \{x \in \mathbb{F}_q^n |\ \langle x, y\rangle_E = 0 \text{ 对任意的} y \in C\}.$$

类似的，码C 的Hermitian 对偶码定义为

$$C^{\perp H}=\{x\in\mathbb{F}_q^n|\langle x,y\rangle_H=0\text{ 对任意的}y\in C\}.$$

一个线性码C 称为Euclidean (Hermitian) 自正交如果$C\subseteq C^{\perp E}$ ($C\subseteq C^{\perp H}$)。

对于向量$x=(x_1,\cdots,x_n)\in\mathbb{F}_{q^2}^n$，设$x^i=(x_1^i,\cdots,x_n^i)$。对于$\mathbb{F}_{q^2}^n$的子集合$S$，定义$S^q$ 为集合$\{x^q|\ x\in S\}$。那么容易得到对于$\mathbb{F}_{q^2}$上的线性码C ，我们有$C^{\perp H}=(C^q)^{\perp E}$。因此，$C$ 是Hermitian 自正交当且仅当$C\subseteq(C^q)^{\perp E}$，也就是说，$C^q\subseteq C^{\perp E}$。

3.2.2.1　常循环码

假设$\gcd(n,q)=1$。对于$\eta\in\mathbb{F}_{q^2}^*$，一个长为$n$的$q^2$元线性码$C$ 称为是η 常循环的如果它在η常循环位移变换下是不变的：

$$(c_0,c_1,\cdots,c_{n-1})\to(\eta c_{n-1},c_0,\cdots,c_{n-2}).$$

如果我们把码字$c=(c_0,c_1,\cdots,c_{n-1})$ 等价于它的多项式表示$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，那么一个$\mathbb{F}_{q^2}$上长为$n$ 的η 常循环码C 等价于商环$\mathbb{F}_{q^2}[x]/\langle x^n-\eta\rangle$的一个理想，其中$xc(x)$ 对应于$c(x)$的η常循环位移。此外$\mathbb{F}_{q^2}[x]/\langle x^n-\eta\rangle$ 是一个主理想整环，并且C 由$x^n-\eta$的首一因子$g(x)$生产。在这种情况下，$g(x)$ 称为C 的生成多项式且记$C=\langle g(x)\rangle$。如果$\eta=-1$，我们称这样的码为亚循环码。

设$\eta\in\mathbb{F}_{q^2}$ 是一个本原r次单位根。由于$\gcd(n,q)=1$，那么在$\mathbb{F}_{q^2}$的某个扩域中存在一个本原(rn)次单位根ω 满足$\omega^n=\eta$。容易验证下式

$$x^n-\eta=\prod_{i=0}^{n-1}(x-\omega^{1+ir}).$$

设$\Omega=\{1+ir|0\le i\le n-1\}$。对于每一个$j\in\Omega$，设$C_j$ 是包含j的模rn的q^2分圆陪集。设C是$\mathbb{F}_{q^2}$上长为n由$g(x)$生成的η常循环码。那么集合$Z=\{j\in\Omega|g(\omega^j)=0\}$ 称为C 的定义集。容易看出C 的定义集是模rn的q^2分圆陪集的一些并，且$\dim(C)=n-|Z|$。容易计算出$C^{\perp H}$ 的定义集是$Z^{\perp H}=\{j\in\Omega|-qj\pmod{rn}\notin Z\}$。

类似于循环码，常循环码也有BCH 界。

定理3.34. ([11,159] 常循环码的*BCH* 界) 设C 是$\mathbb{F}_{q^2}$上的长为n的η常循环码，其中η 是本原r次单位根。设ω是$\mathbb{F}_{q^2}$的某个扩域中的一个本原(rn)次单位根满足$\omega^n=\eta$。假设C的生成多项式的根包含在集合$\{\omega^{1+ri}|i_1\le i\le i_1+d-2\}$中。那么$C$的极小距离至少是$d$。

下面的引理给出了一个方法判别一个$\mathbb{F}_{q^2}$上长为n的η常循环码是否包含它的Hermitian对偶码。

引理3.35. [90] 设r 是$q+1$ 的正因子且$\eta \in \mathbb{F}_{q^2}^*$ 的阶为r。设C 是$\mathbb{F}_{q^2}$上长为n，定义集为$Z \subseteq \Omega$的η常循环码，那么C 包含它的Hermitian 对偶码当且仅当$Z \bigcap (-qZ) = \emptyset$，其中$-qZ = \{-qz \pmod{rn} | z \in Z\}$。

3.2.2.2 广义Reec-Solomon码

下面我们介绍广义Reed-Solomon 码的基本概念和性质。取$\mathbb{F}_q$ 中的n 个不同元素$a_1, \cdots, a_n$ 以及$\mathbb{F}_q$中的n 个非零元$v_1, \cdots, v_n$ 。对于$1 \leq k \leq n$，我们定义码

$$\text{GRS}_k(\mathbf{a}, \mathbf{v}) := \{(v_1 f(a_1), \cdots, v_n f(a_n)) |\ f(x) \in \mathbb{F}_q[x] \text{ 和} \deg(f(x)) < k\},$$

其中$\mathbf{a} = (a_1, \cdots, a_n)$ 和$\mathbf{v} = (v_1, \cdots, v_n)$。码$\text{GRS}_k(\mathbf{a}, \mathbf{v})$ 称为$\mathbb{F}_q$上的广义Reed-Solomon 码。众所周知一个广义Reed-Solomon 码$\text{GRS}_k(\mathbf{a}, \mathbf{v})$ 是具有参数$[n, k, n-k+1]_q$的极大距离可分码。下面的引理给出了一个方法判别一个广义Reed-Solomon 码是否是Hermian 自正交的。

引理3.36. 设$\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_{q^2}^n$ 和$\mathbf{v} = (v_1, \cdots, v_n) \in (\mathbb{F}_{q^2}^*)^n$，则$\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ 当且仅当$\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E = 0$ 对所有$0 \leq j, l \leq k-1$。

证明. 注意到$\text{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$ 当且仅当$\text{GRS}_k(\mathbf{a}, \mathbf{v})^q \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_E}$。显然$\text{GRS}_k(\mathbf{a}, \mathbf{v})^q$ 有一组基$\{(v_1^q a_1^{iq}, \cdots, v_n^q a_n^{iq}) | 0 \leq i \leq k-1\}$，和$\text{GRS}_k(\mathbf{a}, \mathbf{v})$ 有一组基$\{(v_1 a_1^i, \cdots, v_n a_n^i) | 0 \leq i \leq k-1\}$。所以$\text{GRS}_k(\mathbf{a}, \mathbf{v})^q \subseteq \text{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_E}$ 当且仅当$\sum_{i=1}^n v_i^{q+1} a_i^{qj+l} = 0$ 对所有$0 \leq j, l \leq k-1$。 □

注意到引理3.36是Rains[127]引入的刺穿码的特例，但是对于我们下面的构造来说，引理3.36已经足够了。

3.2.3 利用常循环码构造量子极大距离可分码

3.2.3.1 长为$\frac{q^2+1}{5}$的量子极大距离可分码

设q 是形如$10m+3$ 或$10m+7$的奇素数幂，其中m 是一个正整数。设$n = \frac{q^2+1}{5}$，$r = q+1$ 且$\eta \in \mathbb{F}_{q^2}$ 是一个本原r次单位根。下面，我们用$\mathbb{F}_{q^2}$上的长为n的η常循环码去构造量子码。首先，我们需要下面的引理。

引理3.37. [90] 设$n=\frac{q^2+1}{5}$，$s=\frac{q^2+1}{2}$ 且$r=q+1$。那么$\Omega=\{1+ri|0\leq i\leq n-1\}$ 是q^2分圆陪集的不交并：

$$\Omega=C_s\bigcup C_{s+n(q+1)/2}\bigcup(\bigcup_{j=1}^{n/2-1}C_{s-(q+1)j}),$$

其中$C_s=\{s\}$，$C_{s+n(q+1)/2}=\{s+n(q+1)/2\}$ 且对于$1\leq j\leq n/2-1$，$C_{s-(q+1)j}=\{s-(q+1)j,s+(q+1)j\}$。

引理3.38. *1. 假设q 是形如$10m+3$的奇素数幂，其中m 是正整数。如果C 是$\mathbb{F}_{q^2}$上长为$n=\frac{q^2+1}{5}$，定义集是$Z=\bigcup_{j=0}^{\delta}C_{s-(q+1)j}$的$\eta$常循环码，其中$\eta$ 是本原r次单位根，$0\leq\delta\leq 3m$，则$C^{\perp H}\subseteq C$。*

2. 假设q 是形如$10m+7$的奇素数幂，其中m 是正整数。如果C 是$\mathbb{F}_{q^2}$上长为$n=\frac{q^2+1}{5}$，定义集是$Z=\bigcup_{j=0}^{\delta}C_{s-(q+1)j}$的$\eta$ 常循环码，其中η 是本原r次单位根，$0\leq\delta\leq 3m+1$，则$C^{\perp H}\subseteq C$。

证明. 我们将只证明第一部分，第二部分可以类似的证明。我们固定$q=10m+3$和$0\leq\delta\leq 3m$。根据引理 3.35，我们只需证明$Z\bigcap(-qZ)=\emptyset$。假设存在整数$0\leq i\leq j\leq\delta$使得$C_{s-(q+1)i}=-qC_{s-(q+1)j}$。

情形1: $s-(q+1)i\equiv -q(s-(q+1)j)\pmod{(q+1)n}$。

通过计算可得

$$\frac{q^2+1}{2}\equiv i+qj\pmod{\frac{q^2+1}{5}}.$$

由于$q=10m+3$，我们有

$$10m^2+6m+1\equiv i+(10m+3)j\pmod{20m^2+12m+2}.$$

注意到$0\leq i+(10m+3)j\leq 3m+30m^2+9m<3(10m^2+6m+1)$，我们有

$$10m^2+6m+1=i+(10m+3)j,$$

也就是

$$i=10m^2+6m+1-(10m+3)j.$$

如果$j\leq m$，那么$i\geq 3m+1$，矛盾。

如果$j\geq m+1$，那么$i\leq -7m-2$，矛盾。

情形2: $s-(q+1)i\equiv -q(s+(q+1)j)\pmod{(q+1)n}$.

对于这种情形，我们有

$$\frac{q^2+1}{2} \equiv i - qj \pmod{\frac{q^2+1}{5}}.$$

由于$q = 10m+3$，我们有

$$10m^2+6m+1 \equiv i-(10m+3)j \pmod{20m^2+12m+2}.$$

容易验证$3m \geq i-(10m+3)j \geq -30m^2-9m > -3(10m^2+6m+1)$，从而

$$-(10m^2+6m+1) = i-(10m+3)j,$$

因此

$$i = (10m+3)j-(10m^2+6m+1).$$

如果$j \leq m$，则$i \leq -3m-1$，矛盾。

如果$j \geq m+1$，则$i \geq 7m+2$，矛盾。 □

定理3.39. *(1)* 设q 是形如$10m+3$的奇素数，则存在q 元$[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq 6m+2$ 是偶数。

(2) 设q 是形如$10m+7$的奇素数，则存在q 元$[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq 6m+4$ 是偶数。

证明. 注意到除了C_s 和$C_{s+n(q+1)/2}$，每个q^2分圆陪集有两个元素，则根据Hermitian 构造和引理3.38，结论成立。 □

评论3.40. 在文献[90]中, *Kai* 等人构造了下面两类量子极大距离可分码。

1. 如果q 是形如$20m+3$ 或$20m+7$的奇素数幂，则存在一个q 元$[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq \frac{q+5}{2}$是偶数。

2. 如果q 是形如$20m-3$ 或$20m-7$的奇素数幂，则存在一个q 元$[[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq \frac{q+3}{2}$ 是偶数。

显然，我们的结果有更大的极小距离。

3.2.3.2　长为$\frac{q^2-1}{2t}$的量子极大距离可分码

设q是形如$2tm+1$的奇素数幂。设$n=\frac{q^2-1}{2t}$和$r=2$。由于$2n|(q^2-1)$，那么对每个满足$1\leq i\leq 2n$的奇数i，模$2n$的q^2分圆陪集C_i为$C_i=\{i\}$。

引理3.41. 设q是形如$2tm+1$的奇素数幂和$n=\frac{q^2-1}{2t}$。如果C是一个长为n，定义集为$Z=\bigcup_{j=0}^{\delta}C_{1+2j}$的$q^2$元亚循环码，其中$0\leq\delta\leq(t+1)m-1$，那么$C^{\perp H}\subseteq C$。

证明. 根据引理3.35，我们只需证明$Z\bigcap(-qZ)=\emptyset$。假设存在整数$0\leq i\leq j\leq\delta$满足$C_{1+2i}=-qC_{1+2j}$，也就是

$$1+2i\equiv -q(1+2j)\pmod{\frac{q^2-1}{t}}.$$

由于$q=2tm+1$，我们有

$$(2tm+1)(1+2j)+1+2i\equiv 0\pmod{4tm^2+4m}.$$

注意到$0<(2tm+1)(1+2j)+1+2i<(t+1)(4tm^2+4m)$，我们有

$$(2tm+1)(1+2j)+1+2i=x(4tm^2+4m),$$

其中$1\leq x\leq t$。上式等价于

$$1+2i=x(4tm^2+4m)-(2tm+1)(1+2j).$$

如果$j\geq mx$，则$1+2i\leq 2mx-2mt-1<0$，矛盾。

如果$j\leq mx-1$，则$1+2i\geq 2mx+2mt+1$，矛盾。 □

定理3.42. 设q是形如$2tm+1$的奇素数幂，则存在一个q元$[[\frac{q^2-1}{2t},\frac{q^2-1}{2t}-2d+2,d]]$量子极大距离可分码，其中$2\leq d\leq(t+1)m+1$。

证明. 注意到每个q^2-分圆陪集只有一个元素，根据Hermitian 构造和引理3.41，结论成立。 □

评论3.43. 设$t=1$和$q=2m+1$。利用定理 *3.42*，存在一个q元$[[\frac{q^2-1}{2},\frac{q^2-1}{2}-2d+2,d]]$量子极大距离可分码，其中$2\leq d\leq q$。这个结果已经在文献[90]中出现。

评论3.44. 设m是一个奇数以及$q=2tm+1$。利用定理*3.42*，存在一个q元$[[m(q+1),m(q+1)-2d+2,d]]$量子极大距离可分码，其中$2\leq d\leq(t+1)m+1$这个结果已经在文献[90]中出现。

评论3.45. 设$q\equiv 1 \pmod 4$。假设m是一个奇数以及$q=4tm+1$。根据定理*3.42*，存在一个q元$[[2m(q+1),2m(q+1)-2d+2,d]]$量子极大距离可分码，其中$2\leq d\leq 2(t+1)m+1$。这个结果也在文献[90]中出现。

评论3.46. 定理*3.42*也被文献[31]独立的得到。

3.2.3.3 长为$\frac{q^2-1}{2t_1t_2}$的量子极大距离可分码

在这个章节，我们构造一些长为$\frac{q^2-1}{2t_1t_2}$的q元量子极大距离可分码，其中q是奇素数幂，$(2t_1)|(q-1)$，$t_2|(q+1)$以及t_2是奇数。设$n=\frac{q^2-1}{2t_1t_2}$和$r=2$。由于$2n|(q^2-1)$，则对每个满足$1\leq i\leq 2n$的奇数i，模$2n$的q^2分圆陪集C_i为$C_i=\{i\}$。

引理3.47. *1.* 设q是形如$30m+11$的奇素数幂和$n=\frac{q^2-1}{30}$。如果C是一个长为n，定义集为$Z=\bigcup_{j=2m+1}^{\delta}C_{1+2j}$的$q^2$元亚循环码，其中$2m+1\leq\delta\leq 10m+2$，则$C^{\perp H}\subseteq C$。

2. 设q是形如$30m+19$的奇素数幂和$n=\frac{q^2-1}{30}$。如果C是一个长为n，定义集为$Z=\bigcup_{j=m+1}^{\delta}C_{1+2j}$的$q^2$元亚循环码，其中$m+1\leq\delta\leq 9m+4$，则$C^{\perp H}\subseteq C$。

3. 设q是形如$12m+5$的奇素数幂和$n=\frac{q^2-1}{12}$。如果C是一个长为n，定义集为$Z=\bigcup_{j=2m+1}^{\delta}C_{1+2j}$的$q^2$元亚循环码，其中$2m+1\leq\delta\leq 7m+1$，则$C^{\perp H}\subseteq C$。

证明. 我们将只证明第一部分，其他部分可类似可得。我们固定$q=30m+11$和$2m+1\leq\delta\leq 10m+2$。根据引理3.35，我们只需证明$Z\bigcap(-qZ)=\emptyset$。假设存在整数$2m+1\leq i\leq j\leq\delta$使得$C_{1+2i}=-qC_{1+2j}$，也就是

$$1+2i\equiv -q(1+2j) \pmod{\frac{q^2-1}{15}}.$$

如果$q=30m+11$，我们有

$$(30m+11)(1+2j)+1+2i\equiv 0 \pmod{60m^2+44m+8}.$$

注意到$2(60m^2+44m+8)<(30m+11)(1+2j)+1+2i<10(60m^2+44m+8)$, 则

$$(30m+11)(1+2j)+1+2i=x(60m^2+44m+8),$$

其中$3 \leq x \leq 9$。注意到$4m+3 \leq 1+2i \leq 20m+5$。上式等价于

$$1+2i = x(60m^2+44m+8) - (30m+11)(1+2j),\ 3 \leq x \leq 9.$$

对于情形$3 \leq x \leq 4$。如果$j \geq mx+1$，则$1+2i \leq -2m-1$。如果$j \leq mx$，则$1+2i \geq 36m+13$。矛盾。

对于情形$5 \leq x \leq 7$。如果$j \geq mx+2$，则$1+2i \leq 4m+1$。如果$j \leq mx+1$，则$1+2i \geq 20m+7$。矛盾。

对于情形$8 \leq x \leq 9$。如果$j \geq mx+3$，则$1+2i \leq -12m-5$。如果$j \leq mx+2$，则$1+2i \geq 26m+9$。矛盾。 □

定理3.48. *(1)* 设q是形如$30m+11$的奇素数幂，则存在一个q元$[[\frac{q^2-1}{30}, \frac{q^2-1}{30}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq 8m+3$。

(2) 设q是形如$30m+19$的奇素数幂，则存在一个q元$[[\frac{q^2-1}{30}, \frac{q^2-1}{30}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq 8m+5$。

(3) 设q是形如$12m+5$的奇素数幂，则存在一个q元$[[\frac{q^2-1}{12}, \frac{q^2-1}{12}-2d+2, d]]$量子极大距离可分码，其中$2 \leq d \leq 5m+2$。

证明. 注意到每个q^2分圆陪集只有一个元素，根据Hermitian 构造和引理3.47，结论成立。 □

3.2.4　利用广义Reed-Solomon码构造量子极大距离可分码

3.2.4.1　q 元量子极大距离可分码，其中$q = 2am+1$

在这个章节，我们考虑q 元量子极大距离可分码，其中$q = 2am+1$。我们首先需要下面的引理。

引理3.49. 设q是形如$2am+1$的奇素数幂，ω是$\mathbb{F}_{q^2}$中的一个固定的本原元以及$n = \frac{q^2-1}{2a}$。设$\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \cdots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$和$\mathbf{u} = (1, \omega^a, \cdots, \omega^{(n-1)a}) \in \mathbb{F}_{q^2}^n$。那么对任意的$0 \leq j, l \leq (a+1)m-1$，我们有$\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E = 0$。

证明. 对任意的$0 \le j,l \le (a+1)m-1$，我们有

$$\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E = \sum_{i=0}^{n-1} \omega^{[2a(i+1)+t](qj+l)} \omega^{ia(q+1)} = \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{2ai(qj+l+\frac{q+1}{2})}.$$

我们断言$2a(qj+l+\frac{q+1}{2}) \not\equiv 0 \pmod{q^2-1}$。否则的话$qj+l = r\frac{q+1}{2}$，我们有$m(q+1)|\frac{r+1}{2}(q+1)$。则存在一个整数$r_1$使得$r = 2mr_1 - 1$。因此$qj+l = (2mr_1-1)\frac{q+1}{2} = mr_1q + (r_1-a)m - 1 = (mr_1-1)q + (a+r_1)m$，与$0 \le j,l \le (a+1)m-1$矛盾。从而我们有

$$\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E = \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{2ai(qj+l+\frac{q+1}{2})} = 0.$$

□

现在我们证明下面的定理。

定理3.50. *设q是形如$2am+1$的奇素数幂。则对每个$1 \le b \le 2a$，存在一个$[[bm(q+1), bm(q+1)-2d+2, d]]_q$量子极大距离可分码，其中$2 \le d \le (a+1)m+1$。*

证明. 设$\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \cdots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$和$\mathbf{u} = (1, \omega^a, \cdots, \omega^{(n-1)a}) \in \mathbb{F}_{q^2}^n$，其中$n = m(q+1) = \frac{q^2-1}{2a}$。取$\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_b)$以及$\mathbf{v} = (\underbrace{\mathbf{u}, \mathbf{u}, \cdots, \mathbf{u}}_{b \text{ times}})$。

注意到如果$\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$，其中$1 \le i_1, i_2 \le n$和$1 \le j_1, j_2 \le b$，则$i_1 = i_2$和$j_1 = j_2$。因此向量$\mathbf{a}$中的元素是两两不同的。

那么对于$0 \le j,l \le (a+1)m-1$，根据引理3.49，我们有

$$\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E = \sum_{i=1}^{b} \langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \rangle_E = 0.$$

因此对于$1 \le k \le (a+1)m$，$\mathbf{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathbf{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$。从而根据推论3.33，结论成立。

□

特别地，取$b=1$，我们得到下面的推论，它也是文献[31,163]中的主要结果。

推论3.51. *设q是形如$2am+1$的奇素数幂。那么存在一个$[[m(q+1), m(q+1)-2d+2, d]]_q$量子极大距离可分码，其中$2 \le d \le (a+1)m+1$。*

引理3.49中的向量$\mathbf{a}_t$中的元素形成$\mathbb{F}_{q^2}^*$的子群的一个陪集。下面的引理和引理3.49类似，不过选取的向量是去掉$\mathbf{a}_t$中$q+1$个元素。

引理3.52. 设q 是形如$2am+1$ 的奇素数幂，ω 是$\mathbb{F}_{q^2}$ 中固定的本原元以及$n=\frac{q^2-1}{2a}-q-1$。设$\mathbf{b}_t=(\omega^{2a+t},\omega^{4a+t},\cdots,\omega^{q-1-2a+t},\omega^{q-1+2a+t},\cdots,\omega^{2q-2-2a+t},\cdots,\omega^{q^2-q+2a+t},\cdots,\omega^{q^2-1-2a+t})\in\mathbb{F}_{q^2}^n$。则存在向量$\mathbf{w}\in(\mathbb{F}_{q^2}^*)^n$ 使得对任意$0\le j,l\le(a+1)m-2$，有$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=0$。

证明. 设A 是一个$(m-2)\times(m-1)$ 的矩阵，其中$A_{ij}=\omega^{aj(q+1)(2i-1)}\in\mathbb{F}_q$ 对于$1\le i\le m-2$和$1\le j\le m-1$。那么存在$\mathbf{c}\in\mathbb{F}_q^{m-1}$ 使得$A\cdot\mathbf{c}^t=0$。注意到通过删除矩阵A 的第j'列，剩余的矩阵乘以$\prod_{j\neq j'}\omega^{aj(q+1)}$ 是一个Vandermonde 矩阵，因此向量$\mathbf{c}$ 的所有元素非零。从而我们可以把$\mathbf{c}$ 表示成$\mathbf{c}=(\omega^{a_1(q+1)},\cdots,\omega^{a_{m-1}(q+1)})$。

下面设$\mathbf{w}_i=(\omega^{a_1+i\frac{q-1}{2}},\cdots,\omega^{a_{m-1}+i\frac{q-1}{2}})$ 和$\mathbf{w}=(\mathbf{w}_0,\mathbf{w}_1,\cdots,\mathbf{w}_q)$。那么对于$0\le j,l\le(a+1)m-2$，我们有

$$\begin{aligned}
&\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E\\
=&\sum_{i=1}^{m-1}\omega^{a_i(q+1)}\sum_{s=0}^{\frac{q-1}{2}}\omega^{[2s(q-1)+t+2ai](qj+l)}-\sum_{i=1}^{m-1}\omega^{a_i(q+1)}\sum_{s=0}^{\frac{q-1}{2}}\omega^{[2s(q-1)+q-1+t+2ai](qj+l)}\\
=&\omega^{t(qj+l)}(1-\omega^{(q-1)(qj+l)})\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}\sum_{s=0}^{\frac{q-1}{2}}\omega^{2s(q-1)(qj+l)}.
\end{aligned}$$

注意到

$$\sum_{s=0}^{\frac{q-1}{2}}\omega^{2s(q-1)(qj+l)}=\begin{cases}0; & \text{如果}\frac{q+1}{2}\nmid(qj+l),\\ \frac{q+1}{2}; & \text{如果}\frac{q+1}{2}|(qj+l).\end{cases}$$

假设$qj+l=r\frac{q+1}{2}$。如果r 是偶数，则$\omega^{(q-1)(qj+l)}=1$，因此$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=0$。

如果r 是奇数，我们断言$r\neq 2m-1\pmod{2m}$。否则的话，设$r=2mx+2m-1$，那么$qj+l=(2mx+2m-1)\frac{q+1}{2}=[(x+1)m-1]q+(a+x+1)m$，这与$0\le j,l\le(a+1)m-2$矛盾。因此$2a(qj+l)\pmod{q^2-1}\in\{ar(q+1)|1\le r\le 2m-3,\ r\text{ 是奇数}\}$。我们有

$$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=\frac{q+1}{2}\omega^{t(qj+l)}(1-\omega^{(q-1)(qj+l)})\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}=0,$$

其中最后的等式是根据向量$\mathbf{c}$ 的定义。 □

根据引理3.49 和3.52，我们有下面的定理。

定理3.53. 设q 是一个形如$2am+1$ 的奇素数幂。那么对于满足$b,c\ge 0$，$1\le b+c\le 2a$ 以及$b\ge 1$ 或者$m\ge 2$ 的整数b,c，存在一个$[[(bm+c(m-1))(q+1),(bm+c(m-1))(q+1)-2d+2,d]]_q$ 量子极大距离可分码，其中$2\le d\le(a+1)m$。

证明. 设$\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \cdots, \omega^{2n_1a+t}) \in \mathbb{F}_{q^2}^{n_1}$，$\mathbf{u} = (1, \omega^a, \cdots, \omega^{(n_1-1)a}) \in \mathbb{F}_{q^2}^{n_1}$，$\mathbf{b}_t = (\omega^{2a+t}, \omega^{4a+t}, \cdots, \omega^{q-1-2a+t}, \omega^{q-1+2a+t}, \cdots, \omega^{2q-2-2a+t}, \cdots, \omega^{q^2-q+2a+t}, \cdots, \omega^{q^2-1-2a+t}) \in \mathbb{F}_{q^2}^{n_2}$，和$\mathbf{w}$ 是引理3.52 中定义的长为n_2 的向量，其中$n_1 = m(q+1) = \frac{q^2-1}{2a}$ 和$n_2 = (m-1)(q+1) = \frac{q^2-1}{2a} - q - 1$。取$\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_b, \mathbf{b}_{b+1}, \mathbf{b}_{b+2}, \cdots, \mathbf{b}_{b+c})$ 以及$\mathbf{v} = (\underbrace{\mathbf{u}, \mathbf{u}, \cdots, \mathbf{u}}_{b \text{ times}}, \underbrace{\mathbf{w}, \mathbf{w}, \cdots, \mathbf{w}}_{c \text{ times}})$。

注意到如果$\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$，其中$1 \le i_1, i_2 \le n_1$ 和$1 \le j_1, j_2 \le b$，那么$i_1 = i_2$ 且$j_1 = j_2$。因此向量$\mathbf{a}$ 中的元素是两两不同的。

那么对于$0 \le j, l \le (a+1)m - 2$，根据引理3.49 和3.52，我们有

$$\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E = \sum_{i=1}^{b} \langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \rangle_E + \sum_{i=b+1}^{b+c} \langle \mathbf{b}_i^{qj+l}, \mathbf{w}^{q+1} \rangle_E = 0.$$

因此对于$1 \le k \le (a+1)m - 1$，$\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$。从而根据推论3.33，结论成立。 □

3.2.4.2 q 元量子极大距离可分码，其中$q = 2am - 1$

在这个章节，我们考虑q 元量子极大距离可分码，其中$q = 2am - 1$。我们首先证明下面的引理。

引理3.54. 设q 是形如$2am - 1$ 的奇素数幂，ω 是$\mathbb{F}_{q^2}$ 中固定的本原元以及$n = \frac{q^2-1}{2a}$。设$\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \cdots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$ 和$\mathbf{u} = (1, \omega^{2a-1}, \omega^{2(2a-1)}, \cdots, \omega^{(n-1)(2a-1)}) \in \mathbb{F}_{q^2}^n$。那么对于$0 \le j, l \le (a+1)m - 3$，我们有$\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E = 0$。

证明. 对于$0 \le j, l \le (a+1)m - 3$，我们有

$$\begin{aligned} & \langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E \\ =& \sum_{i=0}^{n-1} \omega^{(2a-1)i(q+1)} \omega^{[t+2a(i+1)](qj+l)} \\ =& \omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{i[(q+1)(2a-1)+2a(qj+l)]}. \end{aligned}$$

我们断言$(q+1)(2a-1) + 2a(qj+l) \not\equiv 0 \pmod{q^2-1}$。否则的话，$\frac{q+1}{2a} | (qj+l)$，设$qj + l = r\frac{q+1}{2a}$。我们有$(q^2-1) | (q+1)(r+2a-1)$，从而$(q-1) | (r+2a-1)$。则存在整数$r_1$ 使得$r = r_1(q-1) - 2a + 1$。那么我们有$qj + l = rm = [r_1(q-1) - 2a + 1]m = (r_1m - 2)q +$

$(2a+1-r_1)m-2$，这与$0 \le j,l \le (a+1)m-3$矛盾。因此

$$\begin{aligned}
&\langle \mathbf{a}_t^{qj+l}, \mathbf{u}^{q+1} \rangle_E \\
=&\omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{i[(q+1)(2a-1)+2a(qj+l)]} \\
=&\omega^{(t+2a)(qj+l)} \sum_{i=0}^{n-1} \omega^{2ai[\frac{(q+1)(2a-1)}{2a}+(qj+l)]} \\
=&0.
\end{aligned}$$

□

现在我们证明下面的定理。

定理3.55. 设q是形如$2am-1$的奇素数幂。则对每个$1 \le b \le 2a$，存在一个$[[bm(q-1), bm(q-1)-2d+2, d]]_q$量子极大距离可分码，其中$2 \le d \le (a+1)m-1$。

证明. 设$\mathbf{a}_t = (\omega^{2a+t}, \omega^{4a+t}, \cdots, \omega^{2na+t}) \in \mathbb{F}_{q^2}^n$和$\mathbf{u} = (1, \omega^{2a-1}, \omega^{2(2a-1)}, \cdots, \omega^{(n-1)(2a-1)}) \in \mathbb{F}_{q^2}^n$，其中$n = m(q-1) = \frac{q^2-1}{2a}$。取$\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_b)$和$\mathbf{v} = (\underbrace{\mathbf{u}, \mathbf{u}, \cdots, \mathbf{u}}_{b \text{ times}})$。

注意到如果$\omega^{2ai_1+j_1} = \omega^{2ai_2+j_2}$，其中$1 \le i_1, i_2 \le n$和$1 \le j_1, j_2 \le b$，那么$i_1 = i_2$且$j_1 = j_2$。因此向量$\mathbf{a}$中的元素是两两不同的。

那么对于$0 \le j,l \le (a+1)m-3$，根据引理3.54，我们有

$$\langle \mathbf{a}^{qj+l}, \mathbf{v}^{q+1} \rangle_E = \sum_{i=1}^{b} \langle \mathbf{a}_i^{qj+l}, \mathbf{u}^{q+1} \rangle_E = 0.$$

因此对于$1 \le k \le (a+1)m-2$，$\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{v})^{\perp_H}$。则根据推论3.33，结论成立。

□

特别地，取$b=1$或者让a是个奇数和$b=2$，我们有下面两个推论，它们是文献[153]中的主要结果。

推论3.56. 设q是形如$2am-1$的奇素数幂。那么存在一个$[[m(q-1), m(q-1)-2d+2, d]]_q$量子极大距离可分码，其中$2 \le d \le (a+1)m-1$。

推论3.57. 设q是形如$2am-1$的奇素数幂，其中a是一个奇数。那么存在一个$[[2m(q-1), 2m(q-1)-2d+2, d]]_q$量子极大距离可分码，其中$2 \le d \le (a+1)m-1$。

为了构造更多的量子极大距离可分码，我们需要下面的引理[88]。

引理3.58. [88] 设A 是$\mathbb{F}_{q^2}$ 上秩为$n-1$ 的$(n-1)\times n$ 矩阵。方程$Ax=0$ 在$\mathbb{F}_q$ 有一个非零解当且仅当$A^{(q)}$ 和A 是行等价的，其中$A^{(q)}$ 是把A 的所有元素作q 次幂。

则我们有下面的引理。

引理3.59. 设q 是形如$2am-1$ 的奇素数幂以及$n=\frac{q^2-1}{2a}-q+1$。设$\mathbf{b}_t=(\omega^{2a+t},\omega^{4a+t},\cdots,\omega^{q+1-2a+t},\omega^{q+1+2a+t},\cdots,\omega^{2q+2-2a+t},\cdots,\omega^{q^2-q-2+2a+t},\cdots,\omega^{q^2-1-2a+t})\in\mathbb{F}_{q^2}^n$。那么存在$\mathbf{w}\in(\mathbb{F}_{q^2}^*)^n$ 使得对于$0\le j,l\le(a+1)m-4$，有$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=0$。

证明. 设ω 是$\mathbb{F}_{q^2}$ 中固定的本原元。设A 是$(m-2)\times(m-1)$ 矩阵且$A_{ij}=\omega^{2aj(m-3+(q-1)(i-1))}$ 对于$1\le i\le m-2,\ 1\le j\le m-1$。

由于对于$1\le i\le m-2$，有$(m-3+(q-1)(i-1))q\equiv(m-3+(q-1)(m-i-2))\pmod{q^2-1}$，那么$A^{(q)}$ 和A 是行等价的。根据引理3.58，存在$\mathbf{c}\in\mathbb{F}_q^{m-1}$ 使得$A\cdot\mathbf{c}^t=0$。注意到通过删除矩阵A 中任意一行，剩下的矩阵是Vandermonde 矩阵，因此向量$\mathbf{c}$ 的所有元素非零。因此我们可以把$\mathbf{c}$ 表示成$\mathbf{c}=(\omega^{a_1(q+1)},\cdots,\omega^{a_{m-1}(q+1)})$。

设$\mathbf{w}=(\omega^{a_1},\cdots,\omega^{a_{m-1}},\omega^{a_1-(m-3)},\cdots,\omega^{a_{m-1}-(m-3)},\cdots,\omega^{a_1-(m-3)(q-2)},\cdots,\omega^{a_{m-1}-(m-3)(q-2)})\in(\mathbb{F}_{q^2}^*)^n$. 则对于$0\le j,l\le k-1\le(a+1)m-4$，我们有

$$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l-m+3)s}.$$

注意到

$$\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l-m+3)s}=\begin{cases}0; & \text{如果}(q-1)\nmid(qj+l-m+3),\\ q-1; & \text{如果}(q-1)|(qj+l-m+3).\end{cases}$$

假设$qj+l-m+3=t(q-1)$，我们断言$t\not\equiv m-2,m-1\pmod m$。否则的话，如果$t\equiv m-2\pmod m$，设$t=rm+m-2$,，则$0\le r\le a$。如果$r\le a-1$，则$qj+l=t(q-1)+m-3=(mr+m-3)q+(q-mr-1)=(mr+m-3)q+(2a-r)m-2$ 以及$(2a-r)m-2>(a+1)m-4$，矛盾。如果$r=a$，则$qj+l=t(q-1)+m-3=(am+m-3)q+(am-2)$ 且$am+m-3>(a+1)m-4$，矛盾。类似的，$t\not\equiv m-1\pmod m$。因此$qj+l\pmod{\frac{q^2-1}{2a}}\in\{t(q-1)+m-3|0\le t\le m-3\}$。从而

$$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=(q-1)\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}=0,$$

其中最后的等式由向量$\mathbf{c}$ 的定义可得。 □

现在，我们证明下面的定理。

定理3.60. 设q 是形如$2am-1$ 的奇素数幂。那么对于满足$b,c\geq 0$，$1\leq b+c\leq 2a$ 以及$b\geq 1$ 或$m\geq 2$ 的整数b,c，存在一个$[[(bm+c(m-1))(q-1),(bm+c(m-1))(q-1)-2d+2,d]]_q$ 量子极大距离可分码，其中$2\leq d\leq (a+1)m-2$。

证明. 设$\mathbf{a}_t=(\omega^{2a+t},\omega^{4a+t},\cdots,\omega^{2n_1a+t})\in\mathbb{F}_{q^2}^{n_1}$，$\mathbf{u}=(1,\omega^{2a-1},\omega^{2(2a-1)},\cdots,\omega^{(n_1-1)(2a-1)})\in\mathbb{F}_{q^2}^{n_1}$，$\mathbf{b}_t=(\omega^{2a+t},\omega^{4a+t},\cdots,\omega^{q+1-2a+t},\omega^{q+1+2a+t},\cdots,\omega^{2q+2-2a+t},\cdots,\omega^{q^2-q-2+2a+t},\cdots,\omega^{q^2-1-2a+t})\in\mathbb{F}_{q^2}^{n_2}$ 和$\mathbf{w}$ 是由引理3.59 定义的长为n_2 的向量，其中$n_1=\frac{q^2-1}{2a}$ 和$n_2=\frac{q^2-1}{2a}-q+1$。取$\mathbf{a}=(\mathbf{a}_1,\mathbf{a}_2,\cdots,\mathbf{a}_b,\mathbf{b}_{b+1},\mathbf{b}_{b+2},\cdots,\mathbf{b}_{b+c})$ 和$\mathbf{v}=(\underbrace{\mathbf{u},\mathbf{u},\cdots,\mathbf{u}}_{b\text{ times}},\underbrace{\mathbf{w},\mathbf{w},\cdots,\mathbf{w}}_{c\text{ times}})$。

注意到如果$\omega^{2ai_1+j_1}=\omega^{2ai_2+j_2}$，其中$1\leq i_1,i_2\leq n_1$ 和$1\leq j_1,j_2\leq b$，则$i_1=i_2$ 且$j_1=j_2$。因此向量$\mathbf{a}$ 中的元素两两不同。

那么对于$0\leq j,l\leq (a+1)m-4$，根据引理3.54 和3.59，我们有

$$\langle\mathbf{a}^{qj+l},\mathbf{v}^{q+1}\rangle_E=\sum_{i=1}^{b}\langle\mathbf{a}_i^{qj+l},\mathbf{u}^{q+1}\rangle_E+\sum_{i=b+1}^{b+c}\langle\mathbf{b}_i^{qj+l},\mathbf{w}^{q+1}\rangle_E=0.$$

因此对于$1\leq k\leq (a+1)m-3$，$\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp_H}$。从而根据推论3.33，结论成立。 □

下面的引理是和引理3.59类似的结果。

引理3.61. 设q 是形如$2am-1$ 的奇素数幂，其中a 是奇数以及$n=\frac{q^2-1}{a}-q+1$。设$\mathbf{b}_t=(\omega^{a+t},\omega^{2a+t},\cdots,\omega^{q-a+1+t},\omega^{q+a+1+t},\cdots,\omega^{2q+2-a+t},\cdots,\omega^{q^2-q-2+a+t},\cdots,\omega^{q^2-1-a+t})\in\mathbb{F}_{q^2}^{n}$。那么存在$\mathbf{w}\in(\mathbb{F}_{\mathbf{q^2}}^{*})^{\mathbf{n}}$ 使得$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=0$ 对于$0\leq j,l\leq (a+1)m-3$。

证明. 设ω 是$\mathbb{F}_{q^2}$ 的一个固定的本原元。设A 是$(2m-2)\times(2m-1)$ 矩阵且$A_{ij}=\omega^{a(i(q-1)-1)j}$ 对于$1\leq i\leq 2m-2,\ 1\leq j\leq 2m-1$。

由于对于$1\leq i\leq 2m-1$，有$a(i(q-1)-1)q\equiv a((2m-1-i)(q-1)-1)\pmod{q^2-1}$，那么$A^{(q)}$ 和A 是行等价的。根据引理3.58，存在$\mathbf{c}\in\mathbb{F}_q^{2m-1}$ 使得$A\cdot\mathbf{c}^t=0$。由于删除掉矩阵A 的任何一列，剩下的矩阵是一个Vandermonde 矩阵，则向量$\mathbf{c}$ 的所有元素非零。因此我们可以把$\mathbf{c}$ 表示成$\mathbf{c}=(\omega^{a_1(q+1)},\cdots,\omega^{a_{2m-1}(q+1)})$。

设$\mathbf{v}=(\omega^{a_1},\cdots,\omega^{a_{2m-1}},\omega^{a_1+1},\cdots,\omega^{a_{2m-1}+1},\cdots,\omega^{a_1+q-2},\cdots,\omega^{a_{2m-1}+q-2})\in(\mathbb{F}_{q^2}^*)^n$。则对$0\le j,l\le k-1\le(a+1)m-3$，我们有

$$\langle\mathbf{b}_t^{qj+l},\mathbf{w}^{q+1}\rangle_E=\sum_{i=1}^{2m-1}\omega^{a_i(q+1)+ia(qj+l)}\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l+1)s}.$$

注意到

$$\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l+1)s}=\begin{cases}0; & \text{如果}(q-1)\nmid(qj+l+1),\\ q-1; & \text{如果}(q-1)|(qj+l+1).\end{cases}$$

假设$qj+l+1=t(q-1)$，则$t\not\equiv 0,2m-1\pmod{2m}$。否则的话，如果$t\equiv 0\pmod{2m}$，设$t=2rm$。则$qj+l=t(q-1)-1=(2rm-1)q+(2a-2r)m-2$且$\min\{2rm-1,(2a-2r)m-2\}>(a+1)m-3$，矛盾。类似的，$t\not\equiv 2m-1\pmod{2m}$。因此

$$\sum_{i=1}^{n}v_i^{q+1}a_i^{qj+l}=(q-1)\sum_{i=1}^{m-1}\omega^{a_i(q+1)+ia(qj+l)}=0,$$

其中最后的等式由向量$\mathbf{c}$的定义可得。 □

那么我们可以得到下面的定理。

定理3.62. 设q是形如$2am-1$的奇素数幂，其中a是奇数。则对于满足$c_1,c_2,c_3\ge 0$，$0\le c_1+c_2\le a$，$0\le c_1+c_3\le a$和$c_1+c_2+c_3\ge 1$的整数c_1,c_2,c_3，存在一个$[[(c_1(2m-1)+(c_2+c_3)m)(q-1),(c_1(2m-1)+(c_2+c_3)m)(q-1)-2d+2,d]]_q$量子极大距离可分码，其中$2\le d\le(a+1)m-1$。

证明. 设$\mathbf{a}_t=(\omega^{2a+t},\omega^{4a+t},\cdots,\omega^{2n_1a+t})\in\mathbb{F}_{q^2}^{n_1}$，$\mathbf{u}=(1,\omega^{2a-1},\omega^{2(2a-1)},\cdots,\omega^{(n_1-1)(2a-1)})\in\mathbb{F}_{q^2}^{n_1}$，$\mathbf{b}_t=(\omega^{a+t},\omega^{2a+t},\cdots,\omega^{q-a+1+t},\omega^{q+a+1+t},\cdots,\omega^{2q+2-a+t},\cdots,\omega^{q^2-q-2+a+t},\cdots,\omega^{q^2-1-a+t})\in\mathbb{F}_{q^2}^{n_2}$和$\mathbf{w}$是由引理3.61定义的长度为$n_2$的向量，其中$n_1=m(q-1)=\frac{q^2-1}{2a}$和$n_2=(m-1)(q-1)=\frac{q^2-1}{a}-q+1$。取$\mathbf{a}=(\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_{c_1},\mathbf{a}_{c_1+1},\mathbf{a}_{c_1+2},\cdots,\mathbf{a}_{c_1+c_2},\mathbf{a}_{c_1+a+1},\mathbf{a}_{c_1+a+2},\cdots,\mathbf{a}_{c_1+a+c_3})$和$\mathbf{v}=(\underbrace{\mathbf{w},\mathbf{w},\cdots,\mathbf{w}}_{c_1\text{ times}},\underbrace{\mathbf{u},\mathbf{u},\cdots,\mathbf{u}}_{c_2+c_3\text{ times}})$。

注意到如果$\omega^{2ai_1+j_1}=\omega^{2ai_2+j_2}$，其中$1\le i_1,i_2\le n_1$和$1\le j_1,j_2\le b$，则$i_1=i_2$且$j_1=j_2$。因此向量$\mathbf{a}$中的元素两两不同。

对于$0\le j,l\le(a+1)m-3$，根据引理3.54和3.61，我们有

$$\langle\mathbf{a}^{qj+l},\mathbf{v}^{q+1}\rangle_E=\sum_{i=1}^{c_1}\langle\mathbf{b}_i^{qj+l},\mathbf{w}^{q+1}\rangle_E+\sum_{i=c_1+1}^{c_1+c_2}\langle\mathbf{a}_i^{qj+l},\mathbf{u}^{q+1}\rangle_E+\sum_{i=c_1+a+1}^{c_1+a+c_3}\langle\mathbf{a}_i^{qj+l},\mathbf{u}^{q+1}\rangle_E=0.$$

因此对于$1 \le k \le (a+1)m-2$，$\mathrm{GRS}_k(\mathbf{a},\mathbf{v}) \subseteq \mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp_H}$。从而根据推论3.33，结论成立。 □

3.2.4.3　q 元量子极大距离可分码，其中$q=2am-1$ 且$\gcd(a,m)=1$

在这个章节，我们考虑q 元量子极大距离可分码，其中$q=2am-1$ 且$\gcd(a,m)=1$。首先，我们证明下面的引理。

引理3.63. 设q 是形如$q=2am-1$的奇素数幂，其中$\gcd(a,m)=1$。设ω 是$\mathbb{F}_{q^2}$ 中固定的本原元，$f \in \{0,1\}$且s,t 是满足$0 \le s \le m,\ 0 \le t \le a-1$ 和$s+t \ge 1$ 的整数。设$\mathbf{b}_{i,f} = (\omega^{2a+i(q+1)+f}, \omega^{4a+i(q+1)+f}, \cdots, \omega^{2as+i(q+1)+f})$, $\mathbf{c}_{i,f} = (\omega^{2m+i(q+1)+f}, \omega^{4m+i(q+1)+f}, \cdots, \omega^{2mt+i(q+1)+f})$ 以及$\mathbf{a}_f = (\mathbf{b}_{0,f}, \mathbf{c}_{0,f}, \mathbf{b}_{1,f}, \mathbf{c}_{1,f}, \cdots, \mathbf{b}_{q-2,f}, \mathbf{c}_{q-2,f})$，则存在$\mathbf{v} \in (\mathbb{F}_{q^2}^*)^{(s+t)(q-1)}$ 使得对于$0 \le j,l \le am+s+t-3$，$\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \rangle_E = 0$。

证明. 设ω 是$\mathbb{F}_{q^2}$ 中固定的本原元。令A 是$(s+t-1)\times(s+t)$ 的矩阵，其中对于$1 \le i \le s+t-1,\ 1 \le j \le s$，$A_{ij} = \omega^{2aj(s+t-2+(q-1)(i-1))}$ 和对于$1 \le i \le s+t-1,\ s+1 \le j \le s+t$，$A_{ij} = \omega^{2mj(s+t-2+(q-1)(i-1))}$。

由于对于$1 \le i \le s+t-1$，有$(s+t-2+(q-1)(i-1))q \equiv (s+t-2+(q-1)(s+t-1-i)) \pmod{q^2-1}$，则$A^{(q)}$ 和A 是行等价的。根据引理3.58，存在$\mathbf{c} \in \mathbb{F}_q^{s+t}$ 使得$A \cdot \mathbf{c}^t = 0$。注意到删除A 的任意第j'列，剩下的矩阵乘以$\prod_{j_1 \ne j'} \omega^{2aj_1(s+t-2)} \prod_{j_2 \ne j'} \omega^{2mj_2(s+t-2)}$是一个Vandermonde 矩阵，因此向量$\mathbf{c}$ 所有坐标非零。从而我们可以把$\mathbf{c}$ 表示成$\mathbf{c} = (\omega^{e_1(q+1)}, \cdots, \omega^{e_{s+t}(q+1)})$。

现在设$\mathbf{u}_i = (\omega^{e_1+i}, \cdots, \omega^{e_{s+t}+i})$ 和$\mathbf{v} = (\mathbf{u}_0, \mathbf{u}_{-(s+t-2)}, \cdots, \mathbf{u}_{-(s+t-2)(q-2)})$，那么对于任意的$0 \le j,l \le am+s+t-3$，我们有

$$
\begin{aligned}
&\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \rangle_E \\
=&\sum_{i=1}^{s}\sum_{k=0}^{q-2} \omega^{(2ai+k(q+1)+f)(qj+l)} \omega^{(e_i-(s+t-2)k)(q+1)} + \sum_{i=1}^{t}\sum_{k=0}^{q-2} \omega^{(2mi+k(q+1)+f)(qj+l)} \omega^{(e_{s+i}-(s+t-2)k)(q+1)} \\
=&\omega^{f(qj+l)} \Big(\sum_{i=1}^{s} \omega^{2ai(qj+l)+e_i(q+1)} + \sum_{i=1}^{t} \omega^{2mi(qj+l)+e_{s+i}(q+1)}\Big) \sum_{k=0}^{q-2} \omega^{k(q+1)(qj+l-s-t+2)}.
\end{aligned}
$$

注意到

$$
\sum_{k=0}^{q-2} \omega^{k(q+1)(qj+l-s-t+2)} = \begin{cases} 0; & \text{如果} (q-1) \nmid (qj+l-s-t+2), \\ q-1; & \text{如果} (q-1) \mid (qj+l-s-t+2). \end{cases}
$$

如果$qj+l-s-t+2=r(q-1)$，我们断言$0\le r\le s+t-2$或者$am\le r\le am+s+t-2$。否则的话，如果$r>s+t-2$，则$qj+l=r(q-1)+s+t-2=(r-1)q+q+s+t-r-2=(r-1)q+2am+s+t-r-3$。由于$0\le j,l\le am+s+t-3$，我们有$am\le r\le am+s+t-2$。注意到$\omega^{2ai(am(q-1))}=\omega^{2mi(am(q-1))}=1$，我们有

$$\begin{aligned}&\langle \mathbf{a}_f^{qj+l},\mathbf{v}^{q+1}\rangle_E\\ =&\omega^{f(qj+l)}(q-1)(\sum_{i=1}^{s}\omega^{2ai(r(q-1)+s+t-2)+e_i(q+1)}+\sum_{i=1}^{t}\omega^{2mi(r(q-1)+s+t-2)+e_{s+i}(q+1)})\\ =&0,\end{aligned}$$

其中最后的等式由向量$\mathbf{c}$的定义可得。 □

从而我们有下面的定理。

定理3.64. 设q是形如$q=2am-1$的奇素数幂，其中$\gcd(a,m)=1$。那么对于满足$1\le c\le 2(a+m-1)$的整数c，存在一个$[[c(q-1),c(q-1)-2d+2,d]]_q$量子极大距离可分码，其中$2\le d\le am+c_1-1$,

$$c_1=\begin{cases}c; & \text{如果}1\le c\le a+m-1,\\ \lfloor\frac{c}{2}\rfloor; & \text{如果}a+m\le c\le 2(a+m-1).\end{cases}$$

证明. 如果$1\le c\le a+m-1$，令$c=s+t$使得$0\le s\le m,\ 0\le t\le a-1$。设$\mathbf{b}_i=(\omega^{2a+i(q+1)},\omega^{4a+i(q+1)},\cdots,\omega^{2as+i(q+1)})$，$\mathbf{c}_i=(\omega^{2m+i(q+1)},\omega^{4m+i(q+1)},\cdots,\omega^{2mt+i(q+1)})$。取$\mathbf{a}=(\mathbf{b}_0,\mathbf{c}_0,\mathbf{b}_1,\mathbf{c}_1,\cdots,\mathbf{b}_{q-2},\mathbf{c}_{q-2})$。

如果$a+m\le c\le 2(a+m-1)$, $c_1=\lfloor\frac{c}{2}\rfloor$，设$c_1=s_1+t_1$以及$c-c_1=s_2+t_2$使得$0\le s_1,s_2\le m,\ 0\le t_1,t_2\le a-1$。设$\mathbf{b}_{i,0}=(\omega^{2a+i(q+1)},\omega^{4a+i(q+1)},\cdots,\omega^{2as_1+i(q+1)})$，$\mathbf{c}_{i,0}=(\omega^{2m+i(q+1)},\omega^{4m+i(q+1)},\cdots,\omega^{2mt_1+i(q+1)})$，$\mathbf{b}_{i,1}=(\omega^{2a+i(q+1)+1},\omega^{4a+i(q+1)+1},\cdots,\omega^{2as_2+i(q+1)+1})$和$\mathbf{c}_{i,1}=(\omega^{2m+i(q+1)+1},\omega^{4m+i(q+1)+1},\cdots,\omega^{2mt_2+i(q+1)+1})$。取$\mathbf{a}=(\mathbf{b}_{0,0},\mathbf{c}_{0,0},\mathbf{b}_{1,0},\mathbf{c}_{1,0},\cdots,\mathbf{b}_{q-2,0}\mathbf{c}_{q-2,0},\mathbf{b}_{0,1},\mathbf{c}_{0,1},\mathbf{b}_{1,1},\mathbf{c}_{1,1},\cdots,\mathbf{b}_{q-2,1},\mathbf{c}_{q-2,1})$。

如果$\omega^{2ai_1+j_1(q+1)}=\omega^{2mi_2+j_2(q+1)}$，其中$1\le i_1\le m$，$1\le i_2\le a-1$和$0\le j_1,j_2\le q-2$。那么$\omega^{2ai_1-2mi_2+(j_1-j_2)(q+1)}=1$，因此$(q+1)|(2ai_1-2mi_2)$，也就是$(2am)|(2ai_1-2mi_2)$。从而$a|mi_2$，这与$\gcd(a,m)=1$矛盾。因此向量$\mathbf{a}$的元素两两不同。

从而根据推论3.33和引理3.63，结论成立。 □

3.2.4.4　q 元量子极大距离可分码，其中$q=2am+1$ 和$\gcd(a,m)=1$

在这个章节，我们考虑q 元量子极大距离可分码，其中$q=2am+1$ 和$\gcd(a,m)=1$。

引理3.65. 设q 是形如$q=2am+1$的奇素数幂，其中$\gcd(a,m)=1$。设ω 是$\mathbb{F}_{q^2}$ 中的固定本原元，$f\in\{0,1\}$，且s,t 是满足$0\le s\le m,\ 0\le t\le a-1$ 和$s+t\ge 1$的整数。设$\mathbf{b}_{i,f}=(\omega^{2a+i(q-1)+f},\omega^{4a+i(q-1)+f},\cdots,\omega^{2as+i(q-1)+f})$，$\mathbf{c}_{i,f}=(\omega^{2m+i(q-1)+f},\omega^{4m+i(q-1)+f},\cdots,\omega^{2mt+i(q-1)+f})$ 以及$\mathbf{a}_f=(\mathbf{b}_{0,f},\mathbf{c}_{0,f},\mathbf{b}_{1,f},\mathbf{c}_{1,f},\cdots,\mathbf{b}_{q,f},\mathbf{c}_{q,f})$。那么存在$\mathbf{v}\in(\mathbb{F}_{q^2}^*)^{(s+t)(q+1)}$ 使得对于$0\le j,l\le am+s+t-1$，$\langle\mathbf{a}_f^{qj+l},\mathbf{v}^{q+1}\rangle_E=0$。

证明. 设ω 是$\mathbb{F}_{q^2}$ 中的固定本原元。令A 是$(s+t-1)\times(s+t)$ 的矩阵，其中对于$1\le i\le s+t-1,\ 1\le j\le s$，$A_{ij}=\omega^{2aj((q+1)i-\frac{q+1}{2})}\in\mathbb{F}_q$ 和对于$1\le i\le s+t-1,\ s+1\le j\le s+t$，$A_{ij}=\omega^{2mj((q+1)i-\frac{q+1}{2})}\in\mathbb{F}_q$。那么存在$\mathbf{c}\in\mathbb{F}_q^{s+t}$ 使得$A\cdot\mathbf{c}^t=0$。注意到当删除矩阵A的第j'列时，剩下的矩阵乘以$\prod_{j_1\neq j'}\omega^{aj_1(q+1)}\prod_{j_2\neq j'}\omega^{mj_2(q+1)}$是一个Vandermonde 矩阵，因此向量$\mathbf{c}$ 的所有坐标非零。从而我们可以把$\mathbf{c}$ 表示成$\mathbf{c}=(\omega^{e_1(q+1)},\cdots,\omega^{e_{s+t}(q+1)})$。

设$\mathbf{u}_i=(\omega^{e_1+i\frac{q-1}{2}},\cdots,\omega^{e_{s+t}+i\frac{q-1}{2}})$ 和$\mathbf{v}=(\mathbf{u}_0,\mathbf{u}_1,\cdots,\mathbf{u}_q)$，那么对于任意的$0\le j,l\le am+s+t-1$，我们有

$$\begin{aligned}
&\langle\mathbf{a}_f^{qj+l},\mathbf{v}^{q+1}\rangle_E\\
=&\sum_{i=1}^{s}\sum_{k=0}^{q}\omega^{(2ai+k(q-1)+f)(qj+l)}\omega^{(e_i+k\frac{q-1}{2})(q+1)}+\sum_{i=1}^{t}\sum_{k=0}^{q}\omega^{(2mi+k(q-1)+f)(qj+l)}\omega^{(e_{s+i}+k\frac{q-1}{2})(q+1)}\\
=&\omega^{f(qj+l)}\Big(\sum_{i=1}^{s}\omega^{2ai(qj+l)+e_i(q+1)}+\sum_{i=1}^{t}\omega^{2mi(qj+l)+e_{s+i}(q+1)}\Big)\sum_{k=0}^{q}\omega^{k(q-1)(qj+l+\frac{q+1}{2})}.
\end{aligned}$$

注意到

$$\sum_{k=0}^{q}\omega^{k(q-1)(qj+l+\frac{q+1}{2})}=\begin{cases}0; & \text{如果}(q+1)\nmid(qj+l+\frac{q+1}{2}),\\ q+1; & \text{如果}(q+1)|(qj+l+\frac{q+1}{2}).\end{cases}$$

如果$qj+l+\frac{q+1}{2}=r(q+1)$，我们断言$1\le r\le s+t-1$ 或者$am+1\le r\le am+s+t-1$。如果$r<am+1$，则$qj+l=r(q+1)-\frac{q+1}{2}=(r-1)q+r+am$。由于$0\le j,l\le am+s+t-1$，我们有$1\le r\le s+t-1$。如果$r\ge am+1$，则$qj+l=r(q+1)-\frac{q+1}{2}=rq+r-am-1$，

因此$am+1 \le r \le am+s+t-1$。注意到$\omega^{2ai(am(q-1))} = \omega^{2mi(am(q-1))} = 1$，我们有

$$\begin{aligned}
&\langle \mathbf{a}_f^{qj+l}, \mathbf{v}^{q+1} \rangle_E \\
=&\omega^{f(qj+l)}(q+1)(\sum_{i=1}^{s} \omega^{2ai(r(q+1)-\frac{q+1}{2})+e_i(q+1)} + \sum_{i=1}^{t} \omega^{2mi(r(q+1)-\frac{q+1}{2})+e_{s+i}(q+1)}) \\
=&0,
\end{aligned}$$

其中最后的等式由$\mathbf{c}$ 的定义可得。 □

结合引理3.36，3.65 和Hermitian 构造，我们有下面的定理。

定理3.66. 设q 是形如$q = 2am+1$ 的奇素数幂，其中$\gcd(a,m) = 1$。那么对于满足$1 \le c \le 2(a+m-1)$ 的整数c，存在一个$[[c(q+1), c(q+1)-2d+2, d]]_q$ 量子极大距离可分码，其中$2 \le d \le am + c_1 + 1$,

$$c_1 = \begin{cases} c; & \text{如果} 1 \le c \le a+m-1, \\ \lfloor \frac{c}{2} \rfloor; & \text{如果} a+m \le c \le 2(a+m-1). \end{cases}$$

3.2.4.5 总结

量子极大距离可分码是一类重要的量子码。在这部分，利用广义Reed-Solomon 码和Hermitian 构造，我们构造了许多新的具有较大极小距离的量子极大距离可分码。在表3-6，我们列出了我们这部分构造的量子极大距离可分码。 从下面的评论中可以看到，我们构造的量子极大距离可分码包含很多以前的结果，也产生了很多新的量子极大距离可分码。

评论3.67. *(1)* 考虑形如$[[a(q+1), a(q+1)-2d+2, d]]_q$ 的具有较大极小距离的量子极大距离可分码。在文献[31,90] 中，作者构造了一类量子极大距离可分码，其中$a = \frac{q-1}{\lambda}$，极小距离是$2 \le d \le \frac{q+1}{2} + \frac{q-1}{\lambda}$，以及$\lambda$ 是$q-1$ 的偶因子。在我们的构造中，类*1* 不仅可以取$a = \frac{q-1}{\lambda}$，其中λ 是$q-1$ 的偶因子(取$b=1$)，同时还可以取$a = \frac{q-1}{\lambda}$，其中λ 是$q-1$ 的奇因子(取$b=2$ 和m 使得$\frac{q-1}{2m}$ 是奇数)。更进一步，a 还可以是不整除$q-1$ 的整数(取$b \nmid (q-1)$)。

(2) 类2 给出了更多形如$[[a(q+1), a(q+1)-2d+2, d]]_q$ 的具有较大极小距离的量子极大距离可分码。

表 3-6　量子极大距离可分码

类	码长	极小距离
1	$n=bm(q+1)$, $m\|\frac{q-1}{2}, bm\le q-1$	$2\le d\le \frac{q+1}{2}+m$
2	$n=(bm+c(m-1))(q+1)$, $m\|\frac{q-1}{2}, b,c\ge 0, (b+c)m\le q-1$ 和$b\ge 1$ or $m\ge 2$	$2\le d\le \frac{q-1}{2}+m$
3	$n=bm(q-1)$, $m\|\frac{q+1}{2}, bm\le q+1$	$2\le d\le \frac{q-1}{2}+m$
4	$n=(bm+c(m-1))(q-1)$, $m\|\frac{q+1}{2}, b,c\ge 0, (b+c)m\le q+1$ 和$b\ge 1$ or $m\ge 2$	$2\le d\le \frac{q-3}{2}+m$
5	$n=(c_1(2m-1)+(c_2+c_3)m)(q-1)$, $m\|\frac{q+1}{2}, c_1,c_2,c_3\ge 0, 0\le c_1+c_2\le \frac{q+1}{2m}$, $0\le c_1+c_3\le \frac{q+1}{2m}$ 和$c_1+c_2+c_3\ge 1$	$2\le d\le \frac{q-1}{2}+m$
6	$n=c(q-1)$, $q=2am-1, \gcd(a,m)=1$, $1\le c\le 2(a+m-1)$	$2\le d\le \frac{q-1}{2}+c_1$, $c_1=\begin{cases} c; & \text{如果} 1\le c\le a+m-1, \\ \lfloor\frac{c}{2}\rfloor; & \text{如果} a+m\le c\le 2(a+m-1). \end{cases}$
7	$n=c(q+1)$, $q=2am+1, \gcd(a,m)=1$, $1\le c\le 2(a+m-1)$	$2\le d\le \frac{q+1}{2}+c_1$, $c_1=\begin{cases} c; & \text{如果} 1\le c\le a+m-1, \\ \lfloor\frac{c}{2}\rfloor; & \text{如果} a+m\le c\le 2(a+m-1). \end{cases}$

(3) 考虑形如$[[a(q-1), a(q-1)-2d+2, d]]_q$的具有较大极小距离的量子极大距离可分码。在文献[90,153]中，作者考虑了一类量子极大距离可分码，其中$a|(q+1)$。在我们的构造类*3* 中，整数a 不仅可以是$q+1$ 的因子，也可以不是$q+1$ 的因子。

(4) 类*4* 和*5* 给出了更多形如$[[a(q-1), a(q-1)-2d+2, d]]_q$的具有较大极小距离的量子极大距离可分码。

(5) 类6 (类7) 是一类形如$[[c(q-1), c(q-1)-2d+2, d]]_q$ *(相对应的*$[[c(q+1), c(q+1)-2d+2, d]]_q$*)的具有较大极小距离的量子极大距离可分码。对任意的*$1 \leq c \leq 2(a+m-1)$*，其中*$q = 2am-1$ *(相对应的*$q = 2am+1$*)* $\gcd(a, m) = 1$*。尽管对于某些*c*，得到的量子码可能被包含在类3, 4 和5 (相应的类1 和2)中，但依然还是能得到很多新的量子码。*

3.2.5 利用某些多项式类构造量子码

在这个小节，我们将给出一个新的经典线性码的构造和一类量子码。在这整个小节，我们将固定下面的概念。

- 设$q = p^{\alpha_1}$，其中p 是一个素数以及α_1 是正整数。
- 设m 是一个正整数满足$\gcd(q, m) = 1$ 和$\text{ord}_m(q) = p^{\alpha_2}$，也就是说，$p^{\alpha_2}$ 是最小的正整数l 使得$m|(q^l - 1)$。
- 设$t = p^{\alpha_2}$ 和$s = p^{\alpha_2 - 1}$。

3.2.5.1 多项式码

注意到$\text{ord}_m(q) = t$。对任意的$a \in \mathbb{Z}_m = \{0, 1, \cdots, m-1\}$，包含$a$的$q$分圆陪集$C_a$ 定义为

$$C_a := \{aq^j \pmod m \mid 0 \leq j \leq t-1\}.$$

下面我们选取具有最长长度的q 分圆陪集的代表元:

$$A := \{\max(C_a) \mid 0 \leq a \leq m-1, |C_a| = t\},$$

其中$\max(C_a)$ 是集合C_a 中的最大元。我们定义下面的多项式。

定义3.68. *对于每个*$a \in A$ *和每个满足*$0 \leq k \leq s-1$*的整数*k*，定义*

$$e_{a,k}(x) = \sum_{j=0}^{t-1} \gamma^{q^{j+k}} x^{q^j a},$$

其中γ *是*$\mathbb{F}_{q^s}/\mathbb{F}_q$ *固定的正则元，也就是，集合*$\{\gamma, \gamma^q, \cdots, \gamma^{q^{s-1}}\}$ *形成*$\mathbb{F}_{q^s}$*的一组*$\mathbb{F}_q$ *基。*

设U_m 是由$\mathbb{F}_{q^t}^*$ 的m次单位根形成的子群。接下来，我们假设上面的多项式都是定义在U_m 上。设$P := \{e_{a,k}(x) \mid a \in A, 0 \leq k \leq s-1\}$。我们有下面的结果。

引理3.69. 多项式$e_{a,k}(x)$ 具有下面的性质：

(i) 对于$a \in A$ 和$0 \le k \le s-1$，多项式$e_{a,k}(x)$ 的系数在$\mathbb{F}_{q^s}$ 中且次数等于a。

(ii) 对于$a \in A$ 和$0 \le k \le s-1$，多项式$e_{a,k}(x)$ 在$\mathbb{F}_q$ 上线性无关。

(iii) 对于所有的$\beta \in U_m$，$e_{a,k}(\beta) \in \mathbb{F}_q$。

(iv) 对于所有的$u \in (\mathbb{F}_{q^s} \bigcap U_m) \bigcup \{0\}$，$e_{a,k}(u) = 0$。

(v) $|P| = \frac{m-\gcd(m,q^s-1)}{p}$。

证明. (i). 结论显然。

(ii). 假设$\sum_{a\in A}\sum_{k=0}^{s-1} c_{a,k}e_{a,k}(x) = 0$，其中$c_{a,k} \in \mathbb{F}_q$。则$x^a$ 的系数是$\sum_{k=0}^{s-1} c_{a,k}\gamma^{q^k} = 0$，由于集合$\{\gamma, \gamma^q, \cdots, \gamma^{q^{s-1}}\}$ 形成$\mathbb{F}_{q^s}$的一组$\mathbb{F}_q$基，因此$c_{a,k} = 0$ $(0 \le k \le s-1)$。因此对于$a \in A$ 和$0 \le k \le s-1$，多项式$e_{a,k}(x)$ 在$\mathbb{F}_q$ 上线性无关。

(iii). 设$\beta \in U_m$，则

$$(e_{a,k}(\beta))^q = (\sum_{j=0}^{t-1} \gamma^{q^{j+k}}\beta^{q^j a})^q = \sum_{j=0}^{t-1} \gamma^{q^{j+k+1}}\beta^{q^{j+1}a} = \sum_{j=1}^{t-1} \gamma^{q^{j+k}}\beta^{q^j a} + \gamma^{q^{t+k}}\beta^{q^t a} = \sum_{j=0}^{t-1} \gamma^{q^{j+k}}\beta^{q^j a},$$

因此$e_{a,k}(\beta) \in \mathbb{F}_q$。

(iv). 显然$e_{a,k}(0) = 0$。设$u \in \mathbb{F}_{q^s} \bigcap U_m$，则

$$e_{a,k}(u) = \sum_{j=0}^{t-1} \gamma^{q^{j+k}}u^{q^j a} = \frac{t}{s}\sum_{j=0}^{s-1} \gamma^{q^{j+k}}u^{q^j a} = p\sum_{j=0}^{s-1} \gamma^{q^{j+k}}u^{q^j a} = 0.$$

(v). 容易验证$|C_a| < t$ 当且仅当$m|a(q^s-1)$，也就是说，$\frac{m}{\gcd(m,q^s-1)}|a$。由于每个具有$t$个元素的$q$分圆陪集对应于$s$个多项式，我们有$|P| = \frac{m-\gcd(m,q^s-1)}{p}$。 □

为了给出我们的构造，设

- $L \subseteq A$, $S := \bigcup_{a\in L} C_a$, $\mathfrak{A} := \bigcup_{a\in A} C_a$,
- $P(S) := \{e_{a,k}(x) \mid a \in (S \bigcap A), 0 \le k \le s-1\}$,
- $V(S) := \text{span}_{\mathbb{F}_q}(P(S))$,
- $\{\beta_1, \beta_2, \cdots, \beta_n\}$ 是$U_m \backslash (U_m \bigcap \mathbb{F}_{q^s}^*)$在$\mathbb{F}_{q^s}$ 上两两不共轭的完全代表系。

显然$n=\frac{m-\gcd(m,q^s-1)}{p}$。

评论3.70. 对于我们特殊选择的多项式和点，我们给出一些解释。

1. 我们希望构造把U_m 映射到$\mathbb{F}_q$的多项式。根据上面的引理，多项式$e_{a,k}(x)$ $(a \in A, 0 \le k \le s-1)$ 满足这些条件。这些多项式也可在文献[87,145]中发现。

2. 由于对于所有的$u \in (\mathbb{F}_{q^s} \bigcap U_m) \bigcup \{0\}$，$e_{a,k}(u)=0$，为了构造好的线性码，我们把点集选在$U_m \backslash (U_m \bigcap \mathbb{F}_{q^s}^*)$ 中。根据多项式$e_{a,k}(x)$ 的定义，我们有$e_{a,k}(u)=e_{a,k}(u^{q^s})$ 对于所有的$u \in U_m \backslash (U_m \bigcap \mathbb{F}_{q^s}^*)$。因此我们选择的点是$U_m \backslash (U_m \bigcap \mathbb{F}_{q^s}^*)$在$\mathbb{F}_{q^s}$ 上两两不共轭的完全代表系。

3. 注意到我们已经构造了$\frac{m-\gcd(m,q^s-1)}{p}$ 个多项式和$\frac{m-\gcd(m,q^s-1)}{p}$ 个点。

我们的构造是：

命题3.71. 设

$$C(S) := \{(f(\beta_1), f(\beta_2), \cdots, f(\beta_n)) \mid f \in V(S)\}.$$

则$C(S)$ 是一个$[n,k,d]_q$ 码，其中$n=\frac{m-\gcd(m,q^s-1)}{p}$，$k=|P(S)|$，$d \ge \lceil \frac{m+1-c}{p} \rceil$，$c$ 是集合S中的最大元。

证明. 我们只需证明$d \ge \lceil \frac{m+1-c}{p} \rceil$。一方面，根据引理3.69，$f(u)=0$ 对于所有的$u \in (\mathbb{F}_{q^s} \bigcap U_m) \bigcup \{0\}$。另一方面，如果$\beta_i$ 是$f(x)$ 的一个根，则它所有的p 共轭元$\beta_i, \cdots, \beta_i^{q^{s(p-1)}}$ 也是$f(x)$的根。因此$f(x)$ 在$\{\beta_1, \beta_2, \cdots, \beta_n\}$中至多有$\frac{\deg(f(x))-\gcd(m,q^s-1)-1}{p}$ 个根。从而它的Hamming 重量至少是$n-\frac{c-\gcd(m,q^s-1)-1}{p}=\frac{m+1-c}{p}$。 □

评论3.72. 上面的线性码构造是文献[145] 中构造*IV* 的一个推广。

3.2.5.2 新的量子码

在这个小节，我们将利用多项式码构造新的量子码。首先，我们决定码$C(S)$ 的对偶码。设$\overline{C_a}=\{m-i \mid i \in C_a\}$ 和$\overline{S}=\bigcup_{a \in S} \overline{C_a}$，我们有

命题3.73. $C(S)$ 的*Euclidean* 对偶码是$C(R)$，其中$R=\mathfrak{A} \backslash \overline{S}$。

证明. 由于$\dim(C(S))+\dim(C(R))=n$，我们只需要证明$C(S)$ 的每个码字与$C(R)$ 的每个码字是正交的。

对于$a\in S$，$b\in R$ 和$0\le k_1,k_2\le s-1$，我们有

$$\begin{aligned}
&\sum_{i=1}^{n} e_{a,k_1}(\beta_i)e_{b,k_2}(\beta_i)\\
=&\sum_{i=1}^{n}(\sum_{j=0}^{t-1}\gamma^{q^{j+k_1}}\beta_i^{q^j a})(\sum_{l=0}^{t-1}\gamma^{q^{l+k_2}}\beta_i^{q^l b})\\
=&\sum_{i=1}^{n}\sum_{j=0}^{t-1}\sum_{l=0}^{t-1}\gamma^{q^{j+k_1}+q^{l+k_2}}\beta_i^{q^j a+q^l b}\\
=&\sum_{j=0}^{t-1}(\sum_{l=0}^{t-1}(\sum_{i=1}^{n}\gamma^{q^{j+k_1}+q^{k_2}}\beta_i^{q^j a+b})^{q^l})\\
=&\sum_{j=0}^{t-1}(\sum_{l_1=0}^{s-1}\sum_{l_2=0}^{p-1}(\sum_{i=1}^{n}\gamma^{q^{j+k_1}+q^{k_2}}\beta_i^{q^j a+b})^{q^{l_1+l_2 s}})\\
=&\sum_{j=0}^{t-1}\sum_{l_1=0}^{s-1}\gamma^{q^{j+k_1+l_1}+q^{k_2+l_1}}(\sum_{l_2=0}^{p-1}(\sum_{i=1}^{n}\beta_i^{q^j a+b})^{q^{l_1+l_2 s}}).
\end{aligned}$$

注意到

$$\begin{aligned}
&\sum_{l_2=0}^{p-1}(\sum_{i=1}^{n}\beta_i^{q^j a+b})^{q^{l_1+l_2 s}}\\
=&\sum_{\beta\in U_m}\beta^{q^j a+b}-\sum_{\beta\in\mathbb{F}_{q^s}\bigcap U_m}\beta^{q^j a+b}\\
=&\begin{cases}0; & \text{如果}\gcd(m,q^s-1)\nmid q^j a+b,\\ -\gcd(m,q^s-1); & \text{如果}\gcd(m,q^s-1)|q^j a+b,\end{cases}
\end{aligned}$$

我们有

$$\begin{aligned}
&\sum_{i=1}^{n} e_{a,k_1}(\beta_i)e_{b,k_2}(\beta_i)\\
=&-\gcd(m,q^s-1)\sum_{\substack{j=0\\ \gcd(m,q^s-1)|q^j a+b}}^{t-1}\sum_{l_1=0}^{s-1}\gamma^{q^{j+k_1+l_1}+q^{k_2+l_1}}\\
=&-\gcd(m,q^s-1)p\sum_{\substack{j=0\\ \gcd(m,q^s-1)|q^j a+b}}^{s-1}\sum_{l_1=0}^{s-1}\gamma^{q^{j+k_1+l_1}+q^{k_2+l_1}}\\
=&0.
\end{aligned}$$

□

为了应用我们的结果去构造量子码，我们还需要考虑$C(S)$的Hermitian对偶。

命题3.74. 设$q = l^2$，则$C(S)$ 的*Hermitian*对偶码是$C(R)$，其中$R = \mathfrak{A}\backslash\overline{lS}$，$lS = \{ls \mid s \in S\}$。

证明. 显然$C(S)$的Hermitian对偶码是$C(lS)$的Euclidean对偶码。根据命题3.73可知结论成立。 □

下面我们给出我们的主要结果

定理3.75. 设$q = p^{2e}$ 是一个素数幂，其中p 是素数以及e 是一个正整数。如果存在整数m 和一个集合S 满足下面的条件：

1. $\gcd(q, m) = 1$ 且$\mathrm{ord}_m(q) = p^b$，其中$b \geq 1$ 是一个正整数；

2. $L \subseteq A$，$S = \bigcup_{a\in L} C_a$, $\mathfrak{A} = \bigcup_{a\in A} C_a$，$S \bigcup \overline{p^e S} \supseteq \mathfrak{A}$，其中$C_a$ 是模m的q分圆陪集和$A = \{\max(C_a) \mid 0 \leq a \leq m-1, |C_a| = p^b\}$，

则存在一个$[[n, k, d]]_{p^e}$ 量子码，其中$n = \frac{m-\gcd(m,q^{p^b-1}-1)}{p}$，$k = \frac{2|S|-m+\gcd(m,q^{p^b-1}-1)}{p}$，$d \geq \lceil\frac{m+1-c}{p}\rceil$，和$c$ 是集合S中的最大元。

证明. 根据命题3.74，我们有$C(\mathfrak{A}\backslash\overline{p^e S}) = C(S)^{\perp H}$。如果$S \bigcup \overline{p^e S} \supseteq \mathfrak{A}$，则$C(S)^{\perp H} \subseteq C(S)$。应用定理3.33 和命题3.71，结论成立。 □

表3-7 列出了一些由定理3.75得到的量子码，其中$\max(S)$ 是集合S中的最大元。在表3-8中，我们利用繁衍原则(定理3.32) 去与在线的表[45]中的量子码进行比较。表3-8 和3-9显示了我们得到的量子码比之前的参数要好。

评论3.76. 对于固定的p 和e，定理*3.75*中的m 有无穷多种选择*(*比如，取$m = q^{p^b} - 1$ 对于某个*b)*。但是，一般来说，我们无法决定是否存在非平凡的S *(*$S \neq \mathfrak{A}$*)* 使得$S \bigcup \overline{p^e S} \supseteq \mathfrak{A}$。表*3-7* 显示对于每个$m$，$S$有很多种选择，且对应的量子码的参数比以前的结果要好。

下面我们给出一个例子来解释我们的构造。

例3.77. 取$q=4$，$m=15$。则$\mathrm{ord}_{15}(4)=2$，因此$t=2$和$s=1$。模15 的4分圆陪集为

$$C_0=\{0\},\ C_1=\{1,4\},\ C_2=\{2,8\},\ C_3=\{3,12\},\ C_5=\{5\},$$
$$C_6=\{6,9\},\ C_7=\{7,13\},\ C_{10}=\{10\},\ C_{11}=\{11,14\}.$$

那么$A=\{4,8,9,12,13,14\}$，我们有下面的六个多项式：

$$e_4(x)=x^4+x,\qquad e_8(x)=x^8+x^2,\qquad e_9(x)=x^9+x^6,$$
$$e_{12}(x)=x^{12}+x^3,\qquad e_{13}(x)=x^{13}+x^7,\qquad e_{14}(x)=x^{14}+x^{11}.$$

设γ 是$\mathbb{F}_{16}$ 中的一个固定的本原元。我们取$\{\gamma,\gamma^2,\gamma^3,\gamma^6,\gamma^7,\gamma^{11}\}$ 作为$U_{15}\backslash\mathbb{F}_4^*$ 在$\mathbb{F}_4$上的两两不共轭的一个完全代表系。

如果我们取$S=C_1\bigcup C_2\bigcup C_6$，则$\overline{2S}=C_7\bigcup C_{11}\bigcup C_3$。设$V(S)$ 是由多项式$e_4(x),e_8(x),e_9(x)$生成的一个$\mathbb{F}_4$ 向量空间，则码$\{(f(\gamma),f(\gamma^2),f(\gamma^3),f(\gamma^6),f(\gamma^7),f(\gamma^{11}))\mid f\in V(S)\}$ 是一个$[6,3,4]_4$ *Hermitian* 对偶包含码。因此我们得到一个$[[6,0,\geq 4]]_2$ 量子码。

3.2.5.3 总结

在这个章节，利用多项式码，我们构造了一些参数比以前好的量子码。多项式码的一般框架为：

1. 设$F=\mathbb{F}_q,\ K=\mathbb{F}_{q^s},\ E=\mathbb{F}_{q^t}$；
2. 取$\mathfrak{S}=\{a_1,...,a_n\}$ 作为E 的一个子集；
3. 选取$f_i(x)\in K[x],\ 1\leq i\leq k$，使得$f_i(a_j)\in F$ 对于所有的i,j，以及$f_i(x)\ (1\leq i\leq k)$在F 上线性无关；
4. 设$V=\mathrm{span}\langle f_i(x):1\leq i\leq k\rangle_F$；
5. 则$C:=\{(f(a_1),\cdots,f(a_n))\mid f\in V\}$ 是一个F 上的$[n,k]$ 线性码。

利用多项式码去构造量子码的主要难点是一般不容易决定它的对偶码。

表 3-7　新的量子码

q	m	$\max(S)$	量子码	q	m	$\max(S)$	量子码
4	15	9	$[[6,0,\geq 4]]_2$	4	15	13	$[[6,4,\geq 2]]_2$
4	255	226	$[[120,40,\geq 15]]_2$	4	255	229	$[[120,48,\geq 14]]_2$
4	255	230	$[[120,52,\geq 13]]_2$	4	255	233	$[[120,60,\geq 12]]_2$
4	255	234	$[[120,64,\geq 11]]_2$	4	255	237	$[[120,72,\geq 10]]_2$
4	255	241	$[[120,80,\geq 8]]_2$	4	255	242	$[[120,84,\geq 7]]_2$
4	255	245	$[[120,92,\geq 6]]_2$	4	255	246	$[[120,96,\geq 5]]_2$
4	255	249	$[[120,104,\geq 4]]_2$	4	255	250	$[[120,108,\geq 3]]_2$
4	255	253	$[[120,116,\geq 2]]_2$	9	104	90	$[[32,12,\geq 5]]_3$
9	104	94	$[[32,16,\geq 4]]_3$	9	104	98	$[[32,22,\geq 3]]_3$
9	104	101	$[[32,28,\geq 2]]_3$	9	728	704	$[[240,198,\geq 9]]_3$
9	728	707	$[[240,204,\geq 8]]_3$	9	728	709	$[[240,208,\geq 7]]_3$
9	728	713	$[[240,214,\geq 6]]_3$	9	728	716	$[[240,220,\geq 5]]_3$
9	728	718	$[[240,224,\geq 4]]_3$	9	728	722	$[[240,230,\geq 3]]_3$
9	728	725	$[[240,236,\geq 2]]_3$	16	85	67	$[[40,12,\geq 10]]_4$
16	85	71	$[[40,16,\geq 8]]_4$	16	85	73	$[[40,20,\geq 7]]_4$
16	85	75	$[[40,22,\geq 6]]_4$	16	85	77	$[[40,26,\geq 5]]_4$
16	85	79	$[[40,30,\geq 4]]_4$	16	85	81	$[[40,34,\geq 3]]_4$
16	85	83	$[[40,38,\geq 2]]_4$	16	255	203	$[[120,36,\geq 27]]_4$
16	255	209	$[[120,40,\geq 24]]_4$	16	255	211	$[[120,44,\geq 23]]_4$
16	255	213	$[[120,48,\geq 22]]_4$	16	255	215	$[[120,52,\geq 21]]_4$
16	255	217	$[[120,56,\geq 20]]_4$	16	255	219	$[[120,60,\geq 19]]_4$
16	255	220	$[[120,62,\geq 18]]_4$	16	255	225	$[[120,66,\geq 16]]_4$
16	255	227	$[[120,70,\geq 15]]_4$	16	255	229	$[[120,74,\geq 14]]_4$
16	255	231	$[[120,78,\geq 13]]_4$	16	255	233	$[[120,82,\geq 12]]_4$
16	255	235	$[[120,86,\geq 11]]_4$	16	255	237	$[[120,90,\geq 10]]_4$
16	255	241	$[[120,94,\geq 8]]_4$	16	255	243	$[[120,98,\geq 7]]_4$
16	255	245	$[[120,102,\geq 6]]_4$	16	255	247	$[[120,106,\geq 5]]_4$
16	255	249	$[[120,110,\geq 4]]_4$	16	255	251	$[[120,114,\geq 3]]_4$
16	255	253	$[[120,118,\geq 2]]_4$				

表 3-8　量子码比较

表3-7中的量子码	利用繁衍原则	表[45]中的量子码
$[[240,220,\geq 5]]_3$	$[[238,220,\geq 3]]_3$	$[[238,216,3]]_3$
$[[40,16,\geq 8]]_4$		$[[40,2,8]]_4$
$[[40,20,\geq 7]]_4$		$[[40,8,7]]_4$
$[[40,22,\geq 6]]_4$		$[[40,14,6]]_4$
$[[40,26,\geq 5]]_4$		$[[40,20,5]]_4$
$[[40,30,\geq 4]]_4$		$[[40,26,4]]_4$
$[[40,34,\geq 3]]_4$		$[[40,32,3]]_4$
$[[120,52,\geq 21]]_4$	$[[117,52,\geq 18]]_4$	$[[117,49,14]]_4$
$[[120,56,\geq 20]]_4$	$[[117,56,\geq 17]]_4$	$[[117,49,14]]_4$
$[[120,60,\geq 19]]_4$	$[[117,60,\geq 16]]_4$	$[[117,49,14]]_4$
$[[120,62,\geq 18]]_4$	$[[117,62,\geq 15]]_4$	$[[117,49,14]]_4$

表 3-9　量子码比较

表3-7中的量子码	表[63]中的量子码
$[[120,40,\geq 15]]_2$	$[[120,40,14]]_2$
$[[120,48,\geq 14]]_2$	$[[120,48,13]]_2$
$[[120,52,\geq 13]]_2$	$[[120,52,12]]_2$
$[[120,60,\geq 12]]_2$	$[[120,60,11]]_2$
$[[120,64,\geq 11]]_2$	$[[120,64,10]]_2$
$[[120,72,\geq 10]]_2$	$[[120,72,9]]_2$

4 其他与信息论相关的课题

4.1 (mn, n, mn, m) 相对差集，其中$\gcd(m, n) = 1$

4.1.1 介绍

设G 是阶为uv 的有限群，且设N 是G 的阶为v 的子群。G的一个大小为k 的子集D 称为是G中相对于N的(u, v, k, λ) 相对差集如果差$r_1 r_2^{-1}$ 的多重集，其中$r_1, r_2 \in D$，$r_1 \neq r_2$，包含集合$G\backslash N$中每个元素恰好λ 次且不包含N中元素。如果群G 是交换群(非交换群)，则D 称为交换(非交换) 相对差集。如果$k = v\lambda$，则D 称为半正则相对差集。

最近，文献[61]在半正则交换相对差集与两两无偏基之间建立了联系。文章证明了如果存在一个半正则交换(mn, n, mn, m) 相对差集，则在$\mathbb{C}^{mn}$中存在$n + 1$ 个两两无偏正交基。出于这个联系，我们学习半正则(mn, n, mn, m) 相对差集。对于(p^a, p^b, p^a, p^{a-b}) 相对差集有很多的研究，其中p 是一个素数，参见文献[114,125,131]。在这个章节，我们主要关注(mn, n, mn, m) 相对差集，其中$\gcd(m, n) = 1$。

半正则相对差集的研究主要集中在差集的存在性问题上。对于不存在性结果，Ma在文献[113]中证明了不存在交换(pq, q, pq, p) 相对差集，其中p, q 是不同的素数且$p > q$。在文献[109]中，Leung，Ma 和Tan 证明了不存在交换$(3pq, 3, 3pq, pq)$ 相对差集，其中p, q是大于3 的不同素数。在文献[54] 中，Feng 和Xiang 证明了不存在$(2p, p, 2p, 2)$ 相对差集，其中p 是奇素数，以及不存在交换$(4p, p, 4p, 4)$ 相对差集其中$p > 4$ 是奇素数。后来，Hiramine[75] 推广了Feng–Xiang 工作的一个结果，证明了如果一个交换$(2n, n, 2n, 2)$ 相对差集存在，则n 除了一些情形外一定是2 的幂次。在文献[52]中，Feng 通过群环给出了一些关于(pm, p, pm, m)相对差集的不存在性和结构性结果，其中p 是一个奇素数和$\gcd(p, m) = 1$。对于存在性结果，大部分已知的半正则相对差集都具有参数(p^a, p^b, p^a, p^{a-b})，其中p 是一个素数。据我们所知，只有四类构造的半正则相对差集所在的群的大小不是素数幂且禁止群的大小大于2。在文献[38,108]中，作者构造了一类具有参数$(p^{2t}(p + 1), p + 1, p^{2t}(p + 1), p^{2t})$的相对差集，其中$t$ 是一个正整数且$p = 2$ 或p 是一个Mersenne 素数。在文献[54]中，Feng和Xiang 构造了一类具有参数$(4q, q, 4q, 4)$ 的非交换相对差集，其中q 是一个奇素数幂，

且$q \equiv 1 \pmod 4$ 和$q > 9$。在文献[52]中，Feng 给出了一个$(p(p+1), p, p(p+1), p+1)$ 相对差集的构造，其中p 是一个Mersenne 素数。

这个章节的主要目的是继续这个研究。我们将给出一些关于(mn, n, mn, m) 相对差集的不存在性结果，其中$\gcd(m, n) = 1$。我们还将构造一类非交换$(16q, q, 16q, 16)$ 相对差集，其中q 是一个素数幂满足$q \equiv 1 \pmod 4$ 和$q > 4.2 \times 10^8$。

4.1.2 准备工作

4.1.2.1 相对差集和群环

下面的引理在研究半正则相对差集时是非常有用。

引理4.1. [125] 设R 是G中相对于N的一个交换$(m, n, m, m/n)$ 相对差集。则$exp(G)|m$ 或者$G = \mathbb{Z}_4$，$n = 2$。

设G 是一个有限群。群环$\mathbb{Z}[G]$ 是一个具有基$\{g \mid g \in G\}$ 的自由交换群。对于任意的集合A，A中元素属于G (A 可能是一个多重集)，我们把A 等价于群环中的一个元素$\sum_{g\in G} d_g g$，其中d_g 是g 在A 中出现的次数。给任意的$A = \sum_{g\in G} d_g g \in \mathbb{Z}[G]$，我们定义$A^{(-1)} = \sum_{g\in G} d_g g^{-1}$，其中$g^{-1}$ 是g 在群G 中的逆元。群环的加法和乘法分别定义为:

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

和

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

利用群环语言，一个群G中相对于子群N 的(m, n, k, λ) 相对差集D 可以表示成:

$$DD^{(-1)} = k1_G + \lambda(G - N),$$

其中1_G 是群G 的恒等元。

对于一个有限交换群G，它的特征群记作$\widehat{G}$。对任意的$A = \sum_{g\in G} d_g g$ 和$\chi \in \widehat{G}$，定义$\chi(A) = \sum_{g\in G} d_g \chi(g)$。下面的反演公式表明$A$ 完全由它的特征值$\chi(A)$ 决定，其中χ 遍历$\widehat{G}$。

引理4.2. 设G 是一个交换群。如果$A = \sum_{g\in G} d_g g \in \mathbb{Z}[G]$，则

$$d_h = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(A)\chi(h^{-1}),$$

对所有的$h \in G$。

4.1.2.2　数论知识

对于一个正整数m，我们用ζ_m 表示$\mathbb{C}$中的一个本原m-次单位根。

定义4.3. 设$m = p^a m'$，其中$gcd(p, m') = 1$。则p 称为是模m 自共轭如果存在一个整数j 使得$p^j \equiv -1 \pmod{m'}$。一个合数n 称为是模m 自共轭如果n 的每个素因子都是模m 自共轭的。

下面的引理可参见文献[132]。

引理4.4. 设p 是一个素数，$m = p^a m'$ 是满足$p \nmid m'$ 的整数。设P 是$\mathbb{Z}[\zeta_m]$ 中p 的素理想因子。如果$\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$，存在某个正整数$j$，满足$\sigma(\zeta_{m'}) = \zeta_{m'}^{p^j}$，则$\sigma(P) = P$。

我们有下面的推论。

推论4.5. 设p 是一个素数，$m = p^a m'$ 是满足$p \nmid m'$ 的整数。如果p 是模m 自共轭的，则p 在$\mathbb{Q}(\zeta_m)/Q$ 中的分解群包含$\overline{\sigma_m} : \zeta_m \to \zeta_m^{-1}$。

下面的引理可参见文献[132]。

引理4.6. 设$a \in \mathbb{Z}[\zeta_m]$ 是方程$x\overline{x} = n$ 的一个解，其中n 是一个正整数。如果$\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ 固定n 在$\mathbb{Q}(\zeta_m)$ 中的所有素理想因子，则存在某个单位根ε 使得$\sigma(a) = \varepsilon a$。

设τ 是$x\overline{x} = 2$ 在$\mathbb{Z}[\zeta_n]$ 的一个解，其中n 是奇数。设ρ 是τ 的任意一个素理想因子，则$\rho|\tau$ 且$\overline{\rho}|\overline{\tau}$。如果$\rho = \overline{\rho}$，则2 在$\mathbb{Z}[\zeta_n]$ 中分歧，矛盾。因此$\rho \neq \overline{\rho}$，我们有一个分解$(2) = \rho_1 \cdots \rho_r \overline{\rho_1} \cdots \overline{\rho_r}$。设$\overline{\rho_i} = \rho_{i+r}$。则$(\tau) = \rho_{i_1} \cdots \rho_{i_r}$ 且$(\overline{\tau}) = \rho_{i_1+r} \cdots \rho_{i_r+r}$，集合$\{i_1, \cdots, i_r\}$ 称为元素τ 的形式。我们有下面的引理。

引理4.7. [83] 设τ_1 和τ_2 是$x\overline{x} = 2$ 在$\mathbb{Z}[\zeta_n]$ 中的两个解，其中n 是奇数。则它们具有相同的形式当且仅当它们相差一个单位根。

4.1.3 半正则相对差集的不存在性结果

在这个小节，我们将证明一些关于(mn, n, mn, m) 相对差集的不存在性结果，其中gcd$(m, n) = 1$。

定理4.8. 设m, n 是满足$gcd(m, n) = 1$ 的整数。如果m, n 满足下面的一个条件：

1. $m = 2^l m'$，l 和m' 是奇数，以及2 是模n 自共轭的。

2. $m = 2p$，$p = 1$ 或者p 是一个奇素数，且pn 是模pn 自共轭的。

3. m 是一个奇素数且mn 是模mn 自共轭的。

则在交换群$G = \mathbb{Z}_m \times H$中不存在$(mn, n, mn, m)$ 相对差集，其中H 是阶为n^2 的相对差集。特别地，如果m 是无平方因子的整数，则不存在交换(mn, n, mn, m)-相对差集。

证明. 设$G = \langle g\rangle \times H$，其中$|H| = n^2$ 和$g^m = 1$。假设D 是交换群G中相对于大小为n的子群N的一个(mn, n, mn, m) 相对差集。由于gcd$(m, n) = 1$，我们可以假设$N \subseteq H$。则

$$DD^{(-1)} = mn + m(G - N). \tag{4-1}$$

记$D = D_0 + D_1 g + \cdots + D_{m-1} g^{m-1} \in \mathbb{Z}[G]$，其中$D_i \subseteq H$，$0 \le i \le m - 1$。注意到$|D||N| = |G|$ 且如果存在$d_1, d_2 \in D$ 和$n_1, n_2 \in N$ 使得$d_1 n_1 = d_2 n_2$，由于N是一个子群，则$n_1/n_2 = d_2/d_1 \in N$。因此$d_1 = d_2$ 和$n_1 = n_2$。从而$DN = G$。也就是$(D_0 + D_1 g + \cdots + D_{m-1} g^{m-1})N = H + Hg + \cdots + Hg^{m-1}$。则我们得到

$$D_0 N = D_1 N = \cdots = D_{m-1} N = H, \tag{4-2}$$

$$|D_0| = |D_1| = \cdots = |D_{m-1}| = n. \tag{4-3}$$

根据式子(4-1)，我们得到

$$\begin{aligned} DD^{(-1)} &= (D_0 + D_1 g + \cdots + D_{m-1} g^{m-1})(D_0^{(-1)} + D_1^{(-1)} g^{m-1} + \cdots + D_{m-1}^{(-1)} g) \\ &= mn + m(H - N) + mHg + \cdots + mHg^{m-1}. \end{aligned}$$

也就是

$$\sum_{i=0}^{m-1} D_i D_i^{(-1)} = mn + m(H - N), \tag{4-4}$$

$$\sum_{i=0}^{m-1} D_i D_{i+k}^{(-1)} = mH, \text{ 对于} 1 \le k \le m - 1, \tag{4-5}$$

其中下标是模m的。

设χ 是群H 的一个非平凡特征。如果$\chi|_N = 1$，则根据式子(4-2)，$\chi(D_0) = \chi(D_1) = \cdots = \chi(D_{m-1}) = 0$。

接下来，我们假设$\chi|_N \neq 1$。设$\chi(D_i) = \eta_i$ $(0 \leq i \leq m-1)$。根据引理4.1，$\exp(G)|mn$，则$\exp(H)|n$，所以$\eta_i \in \mathbb{Z}[\zeta_n]$。根据式子(4-4) 和(4-5)，下式成立。

$$\sum_{i=0}^{m-1} \eta_i \overline{\eta_i} = mn, \tag{4-6}$$

$$\sum_{i=0}^{m-1} \eta_i \overline{\eta_{i+k}} = 0, \text{ 对于} 1 \leq k \leq m-1, \tag{4-7}$$

其中下标是模m的。对于$0 \leq j \leq m-1$，计算等式(4-6)+$\zeta_m^{-j} \cdot$(式子(4-7)的第一个等式) + $\cdots + \zeta_m^{-j(m-1)} \cdot$(式子(4-7)的第$(m-1)$个等式)，我们有

$$\Big(\sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i\Big)\Big(\overline{\sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i}\Big) = mn, \ 0 \leq j \leq m-1.$$

记$A_j = \sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i$，则对于$0 \leq j \leq m-1$，$A_j \overline{A_j} = mn$ 和$A_j \in \mathbb{Z}[\zeta_{mn}]$。下面，我们根据我们定理的条件分成三种情况讨论。

情形1: $m = 2^l m'$，l **和**m' **是奇数，以及**2 **是模**n **自共轭的。**

注意到$A_0 \in \mathbb{Z}[\zeta_n]$。设$P$ 是2 在$\mathbb{Z}[\zeta_n]$ 中任意的素理想因子。由于2 是模n 自共轭的，根据推论4.5，我们有$\sigma_{-1}(P) = P$。设$v_P(a)$ 是最大的满足$P^i|a$ 的整数i 。设$v_P(A_0) = t$，则$v_P(\overline{A_0}) = t$。因此$v_P(mn) = v_P(A_0) + v_P(\overline{A_0}) = 2t$。注意到$2$ 在$\mathbb{Q}(\zeta_n)$ 中不分歧，我们有$v_P(mn) = v_P(2^l) = l$ 是奇数，矛盾。

情形2: $m = 2p$，$p = 1$ **或**p **是一个奇素数，且**pn **是模**pn **自共轭的。**

由于pn 是模pn 自共轭的。根据引理4.5，$\sigma_{-1} : \zeta_{pn} \to \zeta_{pn}^{-1}$ 固定pn 的所有素理想因子。设$pn = \prod_{i=1}^r p_i^{e_i}$，其中$p_i$，$1 \leq i \leq r$ 是素数。设$\omega_{pn} = \prod_{i=1}^r (\sqrt{(-1)^{\frac{p_i-1}{2}} p_i})^{e_i}$，则$\omega_{pn} \in \mathbb{Z}[\zeta_{pn}] = \mathbb{Z}[\zeta_{2pn}]$ 和$\overline{\omega_{pn}} \omega_{pn} = pn$。对于任意的$i \in \{1, 2, \cdots, r\}$，主理想$(1 - \zeta_{p_i^{e_i}})$ 是$\mathbb{Z}[\zeta_{p_i^{e_i}}]$ 中的素理想且$(p_i) = (1 - \zeta_{p_i^{e_i}})^{\varphi(p_i^{e_i})}$，$(\sqrt{(-1)^{\frac{p_i-1}{2}} p_i}) = (1 - \zeta_{p_i^{e_i}})^{\frac{\varphi(p_i^{e_i})}{2}}$。由于素理想$(1 - \zeta_{p_i^{e_i}})$ 是p_i 在$\mathbb{Z}[\zeta_{p_i^{e_i}}]$ 的因子且它在$\mathbb{Z}[\zeta_{pn}]$ 中不分歧，我们可以把p_i 在$\mathbb{Z}[\zeta_{pn}]$ 中的素理想分解写作：$(p_i) = (\prod_\lambda \varrho_{i,\lambda})^{\varphi(p_i^{e_i})}$，其中所有的素理想$\varrho_{i,\lambda}$ 都是不同的且$\overline{\varrho_{i,\lambda}} = \varrho_{i,\lambda}$。则我们有$(pn) = \prod_{i=1}^r (\prod_\lambda \varrho_{i,\lambda})^{\varphi(p_i^{e_i}) e_i}$ 且$(\omega_{pn}) = \prod_{i=1}^r (\prod_\lambda \varrho_{i,\lambda})^{\frac{\varphi(p_i^{e_i}) e_i}{2}}$。

由于$A_j \overline{A_j} = mn = 2pn$ 且$A_j \in \mathbb{Z}[\zeta_{pn}]$ 对于$0 \leq j \leq m-1$。比较两边的素理想分解，考虑到pn在$\mathbb{Z}[\zeta_{pn}]$的一个素理想如果整除A_j ，则它也整除$\overline{A_j}$ 且有相同的指数，我们有$A_j \in (\omega_{pn})$。因此存在一个代数整数$B_j \in \mathbb{Z}[\zeta_{pn}]$ 使得$A_j = B_j \omega_{pn}$ 且$B_j \overline{B_j} = 2$.

注意到对于$0 \le j \le m-1$，$A_j = \sum_{i=0}^{m-1} \zeta_m^{ij}\eta_i$。则

$$A_j + A_{j+p} = 2\sum_{i=0}^{p-1} \zeta_m^{2ij}\eta_{2i} = \omega_{pn}(B_j + B_{j+p}).$$

如果B_j和B_{j+p}不具有相同形式，则存在一个2的素理想因子整除B_j但不整除B_{j+p}，矛盾。因此对任意的$0 \le j \le p-1$，B_j和B_{j+p}具有相同形式。根据引理4.7，它们相差一个单位根。假设$B_{j+p} = \mu_j B_j$，其中$\mu_j \in \mathbb{Z}[\zeta_{pn}]$是一个单位根。注意到

$$A_j - A_{j+p} = 2\sum_{i=0}^{p-1} \zeta_m^{(2i+1)j}\eta_{2i+1} = \omega_{pn}B_j(1-\mu_j).$$

则

$$\overline{B_j}\sum_{i=0}^{p-1} \zeta_m^{(2i+1)j}\eta_{2i+1} = \omega_{pn}(1-\mu_j),$$

所以$\overline{B_j}|(1-\mu_j)$。假设μ_j是一个本原l-次单位根。如果l至少有两个不同的素因子，则$1-\mu_j$是一个单位，矛盾。如果l是一个素数幂$q|(pn)$，则$(1-\mu_j)|q$，矛盾。因此$l = 1$或2。也就是对于$0 \le j \le p-1$，$A_{j+p} = A_j$或$A_{j+p} = -A_j$。

如果$p = 1$，容易得到$\eta_0 = 0$或$\eta_1 = 0$。

如果$p > 1$，记

$$S_1 = \{j : 0 \le j \le p-1, A_{j+p} = A_j\},$$
$$S_2 = \{j : 0 \le j \le p-1, A_{j+p} = -A_j\}.$$

注意到$S_1 \bigcup S_2 = \{0, 1, \cdots, p-1\}$。如果$S_1 = \{0\}$，则$A_0 = A_p$且$A_1 = -A_{p+1}$。我们有

$$\sum_{i=0}^{p-1} \eta_{2i+1} = 0 \text{ 和 } \sum_{i=0}^{p-1} \zeta_m^{2i}\eta_{2i} = 0.$$

由于$m = 2p$且p是一个奇素数，我们有$\eta_0 = \eta_2 = \cdots = \eta_{2p-2}$。则$A_0 = p\eta_0$。因此$A_0\overline{A_0} = p^2\eta_0\overline{\eta_0} = 2pn$，这与$\gcd(p, 2n) = 1$矛盾。对于情形$S_2 = \{0\}$是类似的。因此如果$0 \in S_i$，则$|S_i| \ge 2$。

如果对于某个$1 \le t \le p-1$，$0, t \in S_1$，则

$$\sum_{i=0}^{p-1} \eta_{2i+1} = 0,$$
$$\sum_{i=0}^{p-1} \zeta_{2p}^{t(2i+1)}\eta_{2i+1} = 0.$$

这给出了$\eta_1 = \eta_3 = \cdots = \eta_{m-1} = 0$。类似地，如果$0, t \in S_2$ 对某个$1 \le t \le p-1$，我们有$\eta_0 = \eta_2 = \cdots = \eta_{m-2} = 0$。

从而我们证明了对任意的$i \in \{0, 2, \cdots, 2p-2\}$，$j \in \{1, 3, \cdots, 2p-1\}$ 和任意H上的特征χ，$\chi(D_i D_j) = 0$。根据引理4.2，计算可得$D_i D_j = H$。设$W_k = \text{supp}(D_k D_k^{(-1)})$，$k = 0, 1, \cdots, m-1$，其中对于$\sum_{h\in H} a_h h \in \mathbb{Z}[H]$，$\text{supp}(\sum_{h\in H} a_h h) = \{h : a_h \neq 0\}$。假设存在一个非恒等元$h \in W_i \cap W_j$。则存在$a, b \in D_i$ 和$c, d \in D_j$ 使得$h = ab^{-1} = cd^{-1}$。由于$ad = bc$ 和$D_i D_j = H$，我们有$a = b$ 和$c = d$，这与h 的选择矛盾。因此$W_i \cap W_j = \{1\}$。根据式子(4-4)，存在一个分割$H - N = T_1 \cup T_2$ 满足$\sum_{i=0}^{p} D_{2i} D_{2i}^{(-1)} = pn + mT_1$ 和$\sum_{i=0}^{p} D_{2i+1} D_{2i+1}^{(-1)} = pn + mT_2$。由于存在某个$H$上的特征$\chi$ 满足$\chi(D_i) = 0$ 对于$i = 0, 2, \cdots, 2m-2$ 或者$\chi(D_i) = 0$ 对于$i = 1, 3, \cdots, 2m-1$，我们有$pn = -m\chi(T_i)$ 对于某个$i \in \{1, 2\}$。从而$n = -2\chi(T_i)$，矛盾。

情形3: m **是奇素数且**mn **是模**mn **自共轭的**

与情形2类似的讨论，我们有$\omega_n \in \mathbb{Z}[\zeta_n]$ 使得$\omega_n \overline{\omega_n} = n$ 和$A_j \in (\omega_n)$ $(0 \le j \le m-1)$。注意到$A_j = \sum_{i=0}^{m-1} \zeta_m^{ij} \eta_i$，我们有$m\eta_i \in (\omega_n)$ $(0 \le i \le m-1)$。由于$\gcd(m, n) = 1$，则$\eta_i \in (\omega_n)$ $(0 \le i \le m-1)$。假设$\eta_i = \omega_n \tau_i$，其中$\tau_i \in \mathbb{Z}[\zeta_n]$。根据式子(4-6) 和(4-7)，我们有

$$\sum_{i=0}^{m-1} \tau_i \overline{\tau_i} = m,$$
$$\sum_{i=0}^{m-1} \tau_i \overline{\tau_{i+k}} = 0, \text{ 对于} 1 \le k \le m-1,$$

其中下标是模m的。对于$0 \le j \le m-1$，设$B_j = \sum_{i=0}^{m-1} \zeta_m^{ij} \tau_i$。则对于$0 \le j \le m-1$，$B_j \overline{B_j} = m$。对于$0 \le k \le m-1$，设$\sigma_k : \zeta_n \to \zeta_n, \zeta_m \to \zeta_m^k$。根据引理4.4，$\sigma_k$ 固定m在$\mathbb{Q}(\zeta_{mn})$ 中的所有素理想。根据引理4.6，存在某个单位根$\varepsilon \in \mathbb{Q}(\zeta_{mn})$使得

$$\sigma_0(B_1) = \varepsilon B_1. \tag{4-8}$$

注意到$B_1 = \sum_{i=0}^{m-1} \zeta_m^i \tau_i = \sum_{i=0}^{m-2} \zeta_m^i (\tau_i - \tau_{m-1})$ 和$\{\zeta_m^i : i = 0, 1, \cdots, m-2\}$ 形成$\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)$的一组基。记$\varepsilon = \zeta_m^a \zeta_n^b$，根据式子(4-8)，我们有

$$\sum_{i=0}^{m-1} \tau_i - m\tau_{m-1} = \zeta_m^a \zeta_n^b (\sum_{i=0}^{m-1} \zeta_m^i \tau_i),$$

也就是$\zeta_m^{m-a} (\sum_{i=0}^{m-1} \tau_i - m\tau_{m-1}) = \zeta_n^b (\sum_{i=0}^{m-1} \zeta_m^i \tau_i)$。由于$m$ 是素数，我们有$\zeta_n^b \tau_0 = \zeta_n^b \tau_1 = \cdots = \zeta_n^b \tau_{m-a-1} = \zeta_n^b \tau_{m-a+1} = \cdots = \zeta_n^b \tau_{m-1}$。因此$\tau_0 = \tau_1 = \cdots = \tau_{m-a-1} = \tau_{m-a+1} = \cdots = \tau_{m-1}$。则$B_1 = \zeta_m^{m-a} (\tau_{m-a} - \tau_0)$ 和$B_0 = (m-1)\tau_0 + \tau_{m-a}$。设$\omega_m = \sqrt{(-1)^{\frac{m-1}{2}} m}$。

注意到$\omega_m\overline{\omega_m} = m$，$B_j\overline{B_j} = m$ 和m 是模mn 自共轭的，则与情形2类似讨论，存在单位根$\alpha, \alpha_1 \in \mathbb{Z}[\zeta_{mn}]$ 使得$B_0 = \omega_m\alpha$，$B_1 = \omega_m\alpha_1$。定义$\beta = \alpha_1\zeta_m^a$，则

$$B_0 = \tau_{m-a} + (m-1)\tau_0 = \omega_m\alpha,$$
$$B_1\zeta_m^a = \tau_{m-a} - \tau_0 = \omega_m\alpha_1\zeta_m^a = \omega_m\beta.$$

因此$m\tau_0 = \omega_m(\alpha - \beta)$，所以$\overline{\omega_m}|(\alpha - \beta)$。注意到$(\omega_m) = (1-\zeta_m)^{\frac{m-1}{2}}$，以及$\alpha$ 和β 是单位根。这给出了$\alpha = \beta$，因此$\tau_0 = 0$。

因此我们证明了对任意的H上的特征χ，至多存在一个$0 \le i \le m-1$ 满足$\chi(D_i) \neq 0$。则对任意的$0 \le i \neq j \le m-1$ 我们有$\chi(D_iD_j) = 0$。根据与情形2类似的讨论，存在一个分割$H - N = S_0 \cup \cdots \cup S_{m-1}$，且对于$0 \le i \le m-1$，$D_iD_i^{(-1)} = n + mS_i$。由于存在某个$H$上的特征$\chi$ 满足$\chi(D_i) = 0$ 对某个$0 \le i \le m-1$，我们有$n = -m\chi(S_i)$，矛盾。 □

评论4.9. 设$m = 2$，$n = p^r$ 是一个奇素数幂。应用定理*4.8 (*条件*2)*，不存在一个交换$(2p^r, p^r, 2p^r, 2)$-相对差集。这个结果出现在文献*[75]*中。

4.1.4 一类非交换$(16q, q, 16q, 16)$ 相对差集

在这个小节，我们构造一类在大小为$16q^2$的非交换群里的$(16q, q, 16q, 16)$ 相对差集，其中q 是奇素数幂，$q \equiv 1 \pmod 4$ 且$q > 4.2 \times 10^8$。

我们的构造基于Weil 定理。给定一个素数幂$q \equiv 1 \pmod r$ 和一个本原元$g \in \mathbb{F}_q$，我们用C_0^r 来表示乘法子群$\{g^{ir} : 0 \le i < (q-1)/r\}$，和$C_j^r$ 来表示C_0^r 在$\mathbb{F}_q$ 中的陪集，也就是，$C_j^r = g^j \cdot C_0^r$，$0 \le j < r$。下面的结果出现在文献[18,29]中，是Weil 定理的一个应用。

引理4.10. 设$q \equiv 1 \pmod r$ 是一个满足不等式

$$q - \left[\sum_{i=0}^{l-2}\binom{l}{i}(l-i-1)(r-1)^{l-i}\right]\sqrt{q} - lr^{l-1} > 0$$

的素数幂。则，对任意给定的l-元集$(j_1, j_2, \ldots, j_l) \in [0, r-1]^l$ 和给定的$\mathbb{F}_q$中两两不同的l-元集$(c_1, c_2, \ldots, c_l)$，存在一个元素$x \in \mathbb{F}_q$ 使得对每个$i \in [1, l]$，$x + c_i \in C_{j_i}^r$。

对于素数幂$q = p^n$，$n \ge 1$，p 是奇素数，设$\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$，$\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ 是绝对迹函数。

$\mathbb{F}_q$上的二次特征η 定义为

$$\eta(x)=\begin{cases}1, \text{ 如果}x \text{ 是}\mathbb{F}_q \text{ 中非零平凡元;}\\ 0, \text{ 如果}x=0;\\ -1, \text{ 如果}x \text{ 是}\mathbb{F}_q \text{ 中非平方元.}\end{cases}$$

对于$u\in\mathbb{F}_q^*$，我们定义

$$S(u):=\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}(ux^2)}.$$

则容易看出$S(u)=\eta(u)S(1)$ 和$S(1)\overline{S(1)}=q$。

接下来，我们假设$q\equiv 1 \pmod 4$，$e\in\mathbb{F}_q$ 满足$e^2=-1$。给定元素$s_2,s_8\in\mathbb{F}_q^*$，我们定义

$$\begin{aligned}
&s_1=\frac{1+e}{2}+\frac{1-e}{2}s_2, && s_3=\frac{1-e}{2}+\frac{1+e}{2}s_2, && s_4=\frac{1+e}{2}+\frac{1-e}{2}s_8,\\
&s_5=\frac{1-e}{2}s_2+\frac{1+e}{2}s_8, && s_6=\frac{1-e}{2}+s_2+\frac{e-1}{2}s_8, && s_7=1+\frac{1+e}{2}s_2+\frac{-1-e}{2}s_8,\\
&s_9=\frac{1-e}{2}+\frac{1-e}{2}s_2+es_8, && s_{10}=1+s_2-s_8, && s_{11}=\frac{1+e}{2}+\frac{1+e}{2}s_2-es_8,\\
&s_{12}=\frac{1-e}{2}+\frac{1+e}{2}s_8, && s_{13}=1+\frac{1-e}{2}s_2+\frac{e-1}{2}s_8, && s_{14}=\frac{1+e}{2}+s_2+\frac{-1-e}{2}s_8,\\
&s_{15}=\frac{1+e}{2}s_2+\frac{1-e}{2}s_8.
\end{aligned}$$

引理4.11. 如果$q>4.2\times 10^8$，则存在$s_2,s_8\in\mathbb{F}_q^*$ 满足

$$\begin{aligned}
&\eta(s_1)=\eta(s_2)=\eta(s_4)=\eta(s_5)=\eta(s_6)=\eta(s_8)=\eta(s_9)=\eta(s_{10})=\eta(s_{15})=1,\\
&\eta(s_3)=\eta(s_7)=\eta(s_{11})=\eta(s_{12})=\eta(s_{13})=\eta(s_{14})=-1.
\end{aligned}$$

证明. 如果$\frac{1-e}{2},\frac{1+e}{2},e\in C_0^2$，则条件$\eta(s_1)=1,\eta(s_3)=-1$ 等价于$\frac{2}{1-e}s_1=\frac{1+e}{1-e}+s_2\in C_0^2$和$\frac{2}{1+e}s_3=\frac{1-e}{1+e}+s_2\in C_1^2$。由于$0,\frac{1+e}{1-e},\frac{1-e}{1+e}$ 是$\mathbb{F}_q^*$ 中不同元素，根据引理4.10，我们可以找到$s_2\in\mathbb{F}_q^*$ 使得$s_1,s_2\in C_0^2$ 和$s_3\in C_1^2$。对任意的奇素数幂$q>4.2\times 10^8$，一旦元素s_2 被决定了，我们再次利用引理4.10 去得到我们所需要的元素s_8。对于$\frac{1-e}{2},\frac{1+e}{2},e$ 的其他情形，证明是类似的。 □

利用上面的$e,s_i\in\mathbb{F}_q^*,(1\le i\le 15)$。设$H=\mathbb{F}_q\times\mathbb{F}_q$，$N=\{0\}\times\mathbb{F}_q\le H$，和

$G=\langle x,y,H:\ x^4=y^4=1,xy=yx,(u,v)^x=(u,ev),(u,v)^y=(u,ev)$ 对任意的$(u,v)\in H\rangle$,

其中$(u,v)^x$表示$x^{-1}(u,v)x$。设$s_0 := 1$，定义

$$D := \sum_{i=0}^{3}\sum_{j=0}^{3} D_{4j+i}x^i y^j \in \mathbb{Z}[G],$$

其中$D_i = \{(z, \frac{1}{s_i}z^2) : z \in \mathbb{F}_q\}$。

定理4.12. 设q是素数幂满足$q \equiv 1 \pmod 4$和$q > 4.2 \times 10^8$。则D是一个G中相对于N的$(16q, q, 16q, 16)$相对差集。

证明. 为了证明定理，我们将证明

$$DD^{(-1)} = 16q + 16(G - N). \tag{4-9}$$

定义$D_i^{(-x^j y^k)} = \sum_{d\in D_i} x^{-j}y^{-k}d^{-1}x^j y^k$。注意到对任意的$h \in H$，应用$h \to h^{-1}$，我们有

$$\begin{aligned}
&D_iD_j^{(-x)} \to x^3D_jD_i^{(-x^3)}x^3, && D_iD_j^{(-y)} \to y^3D_jD_i^{(-y^3)}y^3,\\
&D_iD_j^{(-xy)} \to x^3y^3D_jD_i^{(-x^3y^3)}x^3y^3, && D_iD_j^{(-x^2y)} \to x^2y^3D_jD_i^{(-x^2y^3)}x^2y^3,\\
&D_iD_j^{(-x^3y)} \to xy^3D_jD_i^{(-xy^3)}xy^3, && D_iD_j^{(-xy^2)} \to x^3y^2D_jD_i^{(-x^3y^2)}x^3y^2.
\end{aligned}$$

则等式(4-9)等价于下面的群环$\mathbb{Z}[H]$中的等式：

$$\sum_{i=0}^{15} D_iD_i^{(-1)} = 16q + 16(H - N), \tag{4-10}$$

$$\begin{aligned}
&D_0D_1^{(-x)} + D_1D_2^{(-x)} + D_2D_3^{(-x)} + D_3D_0^{(-x)} + D_4D_5^{(-x)} + D_5D_6^{(-x)} + D_6D_7^{(-x)} +\\
&D_7D_4^{(-x)} + D_8D_9^{(-x)} + D_9D_{10}^{(-x)} + D_{10}D_{11}^{(-x)} + D_{11}D_8^{(-x)} + D_{12}D_{13}^{(-x)} + D_{13}D_{14}^{(-x)} +\\
&D_{14}D_{15}^{(-x)} + D_{15}D_{12}^{(-x)} = 16H,
\end{aligned} \tag{4-11}$$

$$\begin{aligned}
&D_0D_2^{(-x^2)} + D_1D_3^{(-x^2)} + D_2D_0^{(-x^2)} + D_3D_1^{(-x^2)} + D_4D_6^{(-x^2)} + D_5D_7^{(-x^2)} + D_6D_4^{(-x^2)} +\\
&D_7D_5^{(-x^2)} + D_8D_{10}^{(-x^2)} + D_9D_{11}^{(-x^2)} + D_{10}D_8^{(-x^2)} + D_{11}D_9^{(-x^2)} + D_{12}D_{14}^{(-x^2)} + D_{13}D_{15}^{(-x^2)} +\\
&D_{14}D_{12}^{(-x^2)} + D_{15}D_{13}^{(-x^2)} = 16H,
\end{aligned} \tag{4-12}$$

$$\begin{aligned}
&D_0D_4^{(-y)} + D_1D_5^{(-y)} + D_2D_6^{(-y)} + D_3D_7^{(-y)} + D_4D_8^{(-y)} + D_5D_9^{(-y)} + D_6D_{10}^{(-y)} + D_7D_{11}^{(-y)} +\\
&D_8D_{12}^{(-y)} + D_9D_{13}^{(-y)} + D_{10}D_{14}^{(-y)} + D_{11}D_{15}^{(-y)} + D_{12}D_0^{(-y)} + D_{13}D_1^{(-y)} + D_{14}D_2^{(-y)} +\\
&D_{15}D_3^{(-y)} = 16H,
\end{aligned} \tag{4-13}$$

$$\begin{aligned}
&D_0D_5^{(-xy)} + D_1D_6^{(-xy)} + D_2D_7^{(-xy)} + D_3D_4^{(-xy)} + D_4D_9^{(-xy)} + D_5D_{10}^{(-xy)} + D_6D_{11}^{(-xy)} +\\
&D_7D_8^{(-xy)} + D_8D_{13}^{(-xy)} + D_9D_{14}^{(-xy)} + D_{10}D_{15}^{(-xy)} + D_{11}D_{12}^{(-xy)} + D_{12}D_1^{(-xy)} + D_{13}D_2^{(-xy)} +\\
&D_{14}D_3^{(-xy)} + D_{15}D_0^{(-xy)} = 16H,
\end{aligned} \tag{4-14}$$

$$D_0D_6^{(-x^2y)}+D_1D_7^{(-x^2y)}+D_2D_4^{(-x^2y)}+D_3D_5^{(-x^2y)}+D_4D_{10}^{(-x^2y)}+D_5D_{11}^{(-x^2y)}+D_6D_8^{(-x^2y)}+$$
$$D_7D_9^{(-x^2y)}+D_8D_{14}^{(-x^2y)}+D_9D_{15}^{(-x^2y)}+D_{10}D_{12}^{(-x^2y)}+D_{11}D_{13}^{(-x^2y)}+D_{12}D_2^{(-x^2y)}+D_{13}D_3^{(-x^2y)}+$$
$$D_{14}D_0^{(-x^2y)}+D_{15}D_1^{(-x^2y)}=16H, \tag{4-15}$$
$$D_0D_7^{(-x^3y)}+D_1D_4^{(-x^3y)}+D_2D_5^{(-x^3y)}+D_3D_6^{(-x^3y)}+D_4D_{11}^{(-x^3y)}+D_5D_8^{(-x^3y)}+D_6D_9^{(-x^3y)}+$$
$$D_7D_{10}^{(-x^3y)}+D_8D_{15}^{(-x^3y)}+D_9D_{12}^{(-x^3y)}+D_{10}D_{13}^{(-x^3y)}+D_{11}D_{14}^{(-x^3y)}+D_{12}D_3^{(-x^3y)}+D_{13}D_0^{(-x^3y)}+$$
$$D_{14}D_1^{(-x^3y)}+D_{15}D_2^{(-x^3y)}=16H, \tag{4-16}$$
$$D_0D_8^{(-y^2)}+D_1D_9^{(-y^2)}+D_2D_{10}^{(-y^2)}+D_3D_{11}^{(-y^2)}+D_4D_{12}^{(-y^2)}+D_5D_{13}^{(-y^2)}+D_6D_{14}^{(-y^2)}+$$
$$D_7D_{15}^{(-y^2)}+D_8D_0^{(-y^2)}+D_9D_1^{(-y^2)}+D_{10}D_2^{(-y^2)}+D_{11}D_3^{(-y^2)}+D_{12}D_4^{(-y^2)}+D_{13}D_5^{(-y^2)}+$$
$$D_{14}D_6^{(-y^2)}+D_{15}D_7^{(-y^2)}=16H, \tag{4-17}$$
$$D_0D_9^{(-xy^2)}+D_1D_{10}^{(-xy^2)}+D_2D_{11}^{(-xy^2)}+D_3D_8^{(-xy^2)}+D_4D_{13}^{(-xy^2)}+D_5D_{14}^{(-xy^2)}+D_6D_{15}^{(-xy^2)}+$$
$$D_7D_{12}^{(-xy^2)}+D_8D_1^{(-xy^2)}+D_9D_2^{(-xy^2)}+D_{10}D_3^{(-xy^2)}+D_{11}D_0^{(-xy^2)}+D_{12}D_5^{(-xy^2)}+D_{13}D_6^{(-xy^2)}+$$
$$D_{14}D_7^{(-xy^2)}+D_{15}D_4^{(-xy^2)}=16H, \tag{4-18}$$
$$D_0D_{10}^{(-x^2y^2)}+D_1D_{11}^{(-x^2y^2)}+D_2D_8^{(-x^2y^2)}+D_3D_9^{(-x^2y^2)}+D_4D_{14}^{(-x^2y^2)}+D_5D_{15}^{(-x^2y^2)}+$$
$$D_6D_{12}^{(-x^2y^2)}+D_7D_{13}^{(-x^2y^2)}+D_8D_2^{(-x^2y^2)}+D_9D_3^{(-x^2y^2)}+D_{10}D_0^{(-x^2y^2)}+D_{11}D_1^{(-x^2y^2)}+$$
$$D_{12}D_6^{(-x^2y^2)}+D_{13}D_7^{(-x^2y^2)}+D_{14}D_4^{(-x^2y^2)}+D_{15}D_5^{(-x^2y^2)}=16H. \tag{4-19}$$

为了证明这些等式，我们将证明当作用H上的任意一个特征，这些等式的左边和右边具有相同的值。容易验证对于H的平凡特征是正确的。接下来，我们考虑H 的非平凡特征。注意到H 的任一个非平凡特征χ 可以写作

$$\chi_{g,h}(g',h')=\zeta_p^{\mathrm{Tr}(gg'+hh')},\ \text{对任意的}(g',h')\in H,$$

对于某个$(g,h)\in H$，$(g,h)\neq(0,0)$。

如果$h=0$，则$\chi_{g,0}(D_i)=0$ 和$\chi_{g,0}$ 是在N 上平凡的。容易看出此时所有的等式成立。

如果$h\neq 0$，则$\chi_{g,h}$ 在N 上非平凡，计算可得

$$\chi_{g,h}(D_i)=\sum_{y\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}(gy+\frac{h}{s_i}y^2)}=\eta(h)\eta(s_i)S(1)\zeta_p^{-\mathrm{Tr}(\frac{g^2s_i}{4h})}.$$

容易验证此时等式(4-10)成立。对于等式(4-11)–(4-19)，我们将只证明等式(4-11)，其他等式的证明是类似的。注意到$\chi_{g,h}(16H)=0$，我们只需证明$\chi_{g,h}$(等式(4-11)的左边)$=0$。根

据s_i，$0 \le i \le 15$ 的选择，容易得到下式

$$\eta(s_0s_1s_2s_3) = \eta(s_4s_5s_6s_7) = \eta(s_8s_9s_{10}s_{11}) = \eta(s_{12}s_{13}s_{14}s_{15}) = -1,$$
$$\frac{s_0 - s_2}{s_1 - s_3} = \frac{s_1 - s_3}{s_2 - s_0} = \frac{s_4 - s_6}{s_5 - s_7} = \frac{s_5 - s_7}{s_6 - s_4} = \frac{s_8 - s_{10}}{s_9 - s_{11}} = \frac{s_9 - s_{11}}{s_{10} - s_8} = \frac{s_{12} - s_{14}}{s_{13} - s_{15}} = \frac{s_{13} - s_{15}}{s_{14} - s_{12}} = \frac{1}{e}.$$

由于$\chi_{g,h}(D_i^{-x}) = \overline{\chi_{g,eh}(D_i)} = \eta(eh)\eta(s_i)\overline{S(1)}\zeta_p^{\mathrm{Tr}(\frac{g^2 s_i}{4eh})}$ 和$\frac{g^2 s_1}{4eh} - \frac{g^2 s_0}{4h} = \frac{g^2 s_3}{4eh} - \frac{g^2 s_2}{4h}$，我们有

$$\begin{aligned}
&\chi_{g,h}(D_0D_1^{(-x)}) + \chi_{g,h}(D_2D_3^{(-x)}) \\
=&\eta(h)\eta(s_0)S(1)\zeta_p^{-\mathrm{Tr}(\frac{g^2 s_0}{4h})}\eta(eh)\eta(s_1)\overline{S(1)}\zeta_p^{\mathrm{Tr}(\frac{g^2 s_1}{4eh})} + \eta(h)\eta(s_2)S(1)\zeta_p^{-\mathrm{Tr}(\frac{g^2 s_2}{4h})}\eta(eh)\eta(s_3)\overline{S(1)}\zeta_p^{\mathrm{Tr}(\frac{g^2 s_3}{4eh})} \\
=&\eta(es_0s_1)q\zeta_p^{\mathrm{Tr}(\frac{g^2 s_1}{4eh} - \frac{g^2 s_0}{4h})} + \eta(es_2s_3)q\zeta_p^{\mathrm{Tr}(\frac{g^2 s_3}{4eh} - \frac{g^2 s_2}{4h})} \\
=&0.
\end{aligned}$$

类似的，我们可以证明

$$\begin{aligned}
&\chi_{g,h}(D_1D_2^{(-x)}) + \chi_{g,h}(D_3D_0^{(-x)}) = 0, && \chi_{g,h}(D_4D_5^{(-x)}) + \chi_{g,h}(D_6D_7^{(-x)}) = 0, \\
&\chi_{g,h}(D_5D_6^{(-x)}) + \chi_{g,h}(D_7D_4^{(-x)}) = 0, && \chi_{g,h}(D_8D_9^{(-x)}) + \chi_{g,h}(D_{10}D_{11}^{(-x)}) = 0, \\
&\chi_{g,h}(D_9D_{10}^{(-x)}) + \chi_{g,h}(D_{11}D_8^{(-x)}) = 0, && \chi_{g,h}(D_{12}D_{13}^{(-x)}) + \chi_{g,h}(D_{14}D_{15}^{(-x)}) = 0, \\
&\chi_{g,h}(D_{13}D_{14}^{(-x)}) + \chi_{g,h}(D_{15}D_{12}^{(-x)}) = 0.
\end{aligned}$$

证明结束。 □

评论4.13. *利用MAGMA[16]，我们发现对于所有的素数幂$q \equiv 1 \pmod 4$ 且$353 \le q < 1.2 \times 10^6$，存在$s_2, s_8 \in \mathbb{F}_q^*$ 满足引理4.11 中的条件，从而存在相应的相对差集。实验表明对所有的素数幂$q \equiv 1 \pmod 4$ 且$q \ge 353$，可能存在$s_2, s_8 \in \mathbb{F}_q^*$ 满足引理4.11中的条件。*

4.2 Grassmannian空间填充的组合构造

4.2.1 介绍

设$\mathbb{F}$ 表示域$\mathbb{R}$ 或者$\mathbb{C}$。$\mathbb{F}^m$中的通过原点的N 条不同线的集合，用等长向量$x_1, \cdots, x_N$ 表示，如果存在$a \in \mathbb{R}$ 使得

$$|\langle x_i, x_j\rangle| = a \text{ 对所有的} i \ne j,$$

则这个集合称为一个等角线集合，常数a 指的是这些线之间的公共角。

等角线最早是由Haantjes[70] 在1948 年引入的。由于与量子信息建立了联系[4,135]，尽管等角线已经被研究了很多年，最近等角线又引起了大量的关注。

$\mathbb{C}^m$ 中等角线的数量最多是m^2[41]，而当向量限制到$\mathbb{R}^m$ 上时，这个数量最多是$\frac{m(m+1)}{2}$[106]。不论是在复数或实数情形，一个公开问题是：这个上界能否被无穷多个m 取到。在文献[99]中，König 在$\mathbb{C}^m$上构造了m^2-m+1 个等角线，其中$m-1$ 是素数幂。de Caen[39] 在$\mathbb{R}^m$ 上构造了$2(m+1)^2/9$ 个等角线，其中$(m+1)/3$ 是4 的幂次的两倍。最近，Jedwab 等人[84,85] 和Greaves 等人[68] 利用两两无偏基集合给出了一些具有较大数量的等角线的构造。

紧接着线，n-维子空间的填充也已被研究[34,42,130]。它的目的是在$\mathbb{F}^m$中找到一个n-维子空间集合$U_1,\ldots,U_N$，使得它们尽可能的远。这些填充问题在编码理论[7] 和量子信息理论[161] 都有应用。

Grassmannian 空间$G_{\mathbb{F}}(m,n)$ 是$\mathbb{F}^m$ 的所有n-维子空间集合。对于$\mathbb{F}^m$的一个n-维子空间U，设A 是U的一个$n\times m$ 生成矩阵，其中它的行扩充成整个U。则从$\mathbb{F}^m$ 到U 的一个射影可以表示成矩阵$P_U=A^*A$，其中A^* 表示A 的共轭转置或者在实数情形下就是A 的转置。对于$\mathbb{F}^m$中两个n-维子空间U,V，它们的弦距离定义为

$$d^2(U,V)=n-\mathrm{tr}(P_UP_V).$$

把子空间表示成射影矩阵并不依赖于子空间的基的选择，且我们可以把Grassmannian包含映射到Hilbert-Schmidt范数下的对称或Hermitian $m\times m$矩阵空间。结果矩阵将对应于以$\frac{1}{2}I$为心，$\frac{\sqrt{m}}{2}$ 为半径的球上。因此，每一个弦距离下的Grassmannian填充都对应于一个球码。从而球码的单纯型和正多面体Rankin界可以转移到Grassmannian 填充上。记

$$d_{\mathbb{F}}(m)=\begin{cases}\frac{(m+2)(m-1)}{2}, & \text{如果}\mathbb{F}=\mathbb{R};\\ m^2-1, & \text{如果}\mathbb{F}=\mathbb{C}.\end{cases}$$

则对于$N\le d_{\mathbb{F}}(m)+1$，我们有单纯型界：

$$\min_{i\neq j}d^2(U_i,U_j)\le\frac{n(m-n)}{m}\frac{N}{N-1},$$

其中等式在单纯型时成立，即，任意两个子空间的距离是一个常数。

对于$N>d_{\mathbb{F}}(m)+1$，我们有正多面体界：

$$\min_{i\neq j}d^2(U_i,U_j)\le\frac{n(m-n)}{m}.$$

如果等式成立，则$N\le 2d_{\mathbb{F}}(m)$。我们把上面的讨论总结如下。

定义4.14. 设$\mathcal{U}$是$\mathbb{F}^m$ ($\mathbb{F}=\mathbb{C}$ *or* $\mathbb{R}$) 中n-维子空间$U_1,\ldots,U_N$集合。则$\mathcal{U}$称为$G_{\mathbb{F}}(m,n)$的单纯型填充，如果$N\leq d_{\mathbb{F}}(m)+1$且$min_{i\neq j}d^2(U_i,U_j)=\frac{n(m-n)}{m}\frac{N}{N-1}$。$\mathcal{U}$称为$G_{\mathbb{F}}(m,n)$的正多面体填充，如果$N>d_{\mathbb{F}}(m)+1$且$min_{i\neq j}d^2(U_i,U_j)=\frac{n(m-n)}{m}$。单纯型填充和正多面体填充都称为最优填充。

尽管Grassmannian 填充已经被研究了20 年，但仍然只有很少的最优填充被构造出来。文献[34]给出了一些最优填充的例子。在文献[21,137]中，作者利用Clifford 群和Barnes-Wall 格给出了一些最优填充的构造。在文献[98]中，Kocák 和Niepel 利用Hadamard 矩阵给出了几类最优填充。最近Bodmann 和Haas[15] 利用两两无偏基和区块设计构造了一类正多面体填充。

在文献[99]中，作者利用差集去构造等角线，而且文献[84,85]中的结果可以利用相对差集得到。利用差集来构造等角线的一个主要思想是利用$|\{|\chi(D)|:\chi\in\widehat{G}\backslash\{\chi_0\}\}|=1$ (或者2)。在这部分，我们将推广这个想法并且利用直积差集给出一类$\mathbb{C}^d$ 中的大小为$O(d^2)$ 的等角线。接着，我们考虑高维子空间。我们利用差集给出单纯型填充的两个构造。由于差集有很多的构造，我们得到很多新的最优填充无穷类。特别地，我们给出了文献[21]中的构造的一个新解释。同时，我们还利用Latin 方给出了一类最优填充。

4.2.2 准备知识

设G 是一个有限群。群环$\mathbb{Z}[G]$ 是一个具有基$\{g\mid g\in G\}$ 的自由交换群。对于任意的集合A，A中元素属于G (A 可能是一个多重集)，我们把A 等价于群环中的一个元素$\sum_{g\in G}d_gg$，其中d_g 是g 在A 中出现的次数。给任意的$A=\sum_{g\in G}d_gg\in\mathbb{Z}[G]$，我们定义$A^{(-1)}=\sum_{g\in G}d_gg^{-1}$，其中$g^{-1}$ 是g 在群G 中的逆元。群环的加法和乘法分别定义为:

$$\sum_{g\in G}a_gg+\sum_{g\in G}b_gg=\sum_{g\in G}(a_g+b_g)g,$$

和

$$\sum_{g\in G}a_gg\sum_{g\in G}b_gg=\sum_{g\in G}(\sum_{h\in G}a_hb_{h^{-1}g})g.$$

对于一个有限群G，定义它的特征群为$\widehat{G}$。$\widehat{G}$ 的恒等元称为主特征，记作χ_0。对任意的$A=\sum_{g\in G}d_gg$ 和$\chi\in\widehat{G}$，定义$\chi(A)=\sum_{g\in G}d_g\chi(g)$。下面的性质是众所周知的。

定理4.15. *(正交关系)* 设G 是阶为v，单位元为e 的交换群。则

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}0,\ \text{如果}g\neq e;\\ v,\ \text{如果}g=e,\end{cases}$$

以及

$$\sum_{g\in G}\chi(g)=\begin{cases}0,\ \text{如果}\chi\neq\chi_0;\\ v,\ \text{如果}\chi=\chi_0.\end{cases}$$

大小为v的群$(G,\cdot)$的一个大小为k的子集D 称为$(G,\cdot)$ 中的一个(v,k,λ) 差集，如果乘积$d_1\cdot d_2^{-1}$ 包含G中每个非单位元恰好λ次，其中$d_1,d_2\in D$。用群环的语言，我们有

$$DD^{(-1)}=(k-\lambda)1_G+\lambda G,$$

其中1_G 是G 的单位元。

根据定义，如果D 是$(G,\cdot)$中的一个(v,k,λ) 差集，则对任意的非单位元$x\in G$，有

$$|D\cap(D\cdot x)|=\lambda$$

且

$$k(k-1)=\lambda(v-1).$$

交换群$(G,+)$ 中的一个差集D 称为一个斜Hadamard 差集如果它具有参数$(q,\frac{q-1}{2},\frac{q-3}{4})$且$G$ 是D，$-D$ 和$\{0_G\}$ 的并，其中0_G 是交换群G 的单位元。可以证明一个斜Hadamard 差集存在当且仅当$q\equiv 3\pmod 4$ 是一个素数幂。

设$G=A\times B$ 是两个群A 和B 的直积，其中$|A|=a$ 和$|B|=b$ $(a,b\geq 2)$。设大小为k的集合$D\subseteq G$ 满足$G\backslash\{A\cup B\}$ 中每个元素恰好可以用λ (≥ 1) 种方式表示成$d_1^{-1}d_2$，其中$d_1,d_2\in D$。更进一步，假设$A\cup B$ 中没有非单位元可以这么表示。则我们称D 是G 中的一个(a,b,k,λ) 直积差集。用群环的语言，G 中的一个(a,b,k,λ) 直积差集可以表示成：

$$DD^{(-1)}=(k+\lambda)1_G+\lambda(G-A-B).$$

直积差集可以看成是差集的推广。对于更多的这些组合对象知识，可参见文献[125]。

4.2.3　等角线的一个构造

在这个小节，我们利用差集给出等角线的一个构造。我们首先给出一个一般构造。

定理4.16. 设$B_i = (b_{i1}, \cdots, b_{im})$ $(1 \le i \le s)$ 是$n \times m$ 矩阵，其中$b_{ij} \in \mathbb{F}^n$ $(\mathbb{F} = \mathbb{C}\ or\ \mathbb{R})$。假设存在$a, d, e, f \in \mathbb{R}$ 和$b, c \in \mathbb{F}$ 使得下面的条件成立：

1. 对于任意的$1 \le i \le s,\ 1 \le j \le m$，$\langle b_{ij}, b_{ij} \rangle = a$。
2. 对于任意的$1 \le i \le s,\ 1 \le j \ne k \le m$，$\langle b_{ij}, b_{ik} \rangle = b$。
3. 对于任意的$1 \le i \ne k \le s,\ 1 \le j \le m$，$\langle b_{ij}, b_{kj} \rangle = c$。
4. 对于任意的$1 \le i \ne k \le s,\ 1 \le j \ne l \le m$，$|\langle b_{ij}, b_{kl} \rangle| = d$。
5. $|b + f^2| = |c + e^2| = d$。

则在$\mathbb{F}^{n+m+s}$中存在大小为ms 的等角线。

证明. 我们构造下面的矩阵，其中它的列将构成所需要的等角线。

$$M = \begin{pmatrix} B_1 & B_2 & \cdots & B_s \\ eI_m & eI_m & \cdots & eI_m \\ fJ_m & \overrightarrow{0} & \cdots & \overrightarrow{0} \\ \overrightarrow{0} & fJ_m & \cdots & \overrightarrow{0} \\ \vdots & \vdots & \ddots & \vdots \\ \overrightarrow{0} & \overrightarrow{0} & \cdots & fJ_m \end{pmatrix},$$

其中I_m 是$m \times m$ 单位矩阵，$\overrightarrow{0} = (\underbrace{0, 0, \cdots, 0}_{m})$ 和$J_m = (\underbrace{1, 1, \cdots, 1}_{m})$。 □

下面我们给出一个满足定理4.16条件的矩阵的构造。设$G = \mathbb{F}_q^+ \times \mathbb{F}_q^*$，则集合$D = \{(x, x) \in \mathbb{F}_q^+ \times \mathbb{F}_q^* | x \in \mathbb{F}_q^*\}$ 是G 上相对于$N_1 = \{(0, x) | x \in \mathbb{F}_q^*\}$ 和$N_2 = \{(x, 1) | x \in \mathbb{F}_q^+\}$ 的$(q, q-1, q-1, 1)$ 直积差集[59]。用群环的语言，我们有

$$DD^{(-1)} = q \cdot 1_G + G - N_1 - N_2,$$

其中$D^{(-1)}$ 表示对应于集合$\{(-x, y^{-1}) : (x, y) \in D\}$ 的群环中的元素。

如果χ 是交换群的一个特征，根据定理4.15，我们有

$$\chi(DD^{(-1)}) = \begin{cases} (q-1)^2, & \text{如果} \chi = \chi_0; \\ 1, & \text{如果} \chi|_{N_1} = \chi_0 \text{ 和} \chi \ne \chi_0; \\ 0, & \text{如果} \chi|_{N_2} = \chi_0 \text{ 和} \chi \ne \chi_0; \\ q, & \text{如果} \chi|_{N_1} \ne \chi_0 \text{ 和} \chi|_{N_2} \ne \chi_0. \end{cases}$$

进一步，我们计算可得

$$\chi(D)=\begin{cases}-1, & \text{如果}\chi|_{N_1}=\chi_0\text{和}\chi\neq\chi_0;\\ 0, & \text{如果}\chi|_{N_2}=\chi_0\text{和}\chi\neq\chi_0.\end{cases}$$

定理4.17. 设q是一个素数幂且$s\leq q$是一个正整数。则在$\mathbb{C}^{2q-2+s}$中存在大小为$(q-1)s$的等角线。

证明. 接着上面的记号，容易看出$\widehat{G}\cong\widehat{\mathbb{F}_q^+}\times\widehat{\mathbb{F}_q^*}$。设$\widehat{\mathbb{F}_q^+}=\{\psi_1,\cdots,\psi_q\}$，$\widehat{\mathbb{F}_q^*}=\{\chi_1,\cdots,\chi_{q-1}\}$以及记$D=\{d_1,d_2,\cdots,d_{q-1}\}$。对于$1\leq i\leq s$，设$B_i=(\psi_i\chi_k(d_j))_{\substack{1\leq j\leq q-1\\1\leq k\leq q-1}}$，则$b_{ij}=(\psi_i\chi_j(d_1),\cdots,\psi_i\chi_j(d_{q-1}))^\top$，其中$A^\top$表示$A$的转置。我们有$\langle b_{ij},b_{rt}\rangle=\psi_i\psi_r^{-1}\chi_j\chi_t^{-1}(D)$，则矩阵$B_i$满足定理4.16中的条件，其中$a=q-1,\ b=-1,\ c=0,\ d=\sqrt{q},\ f=\sqrt{1+\sqrt{q}}$和$e=\sqrt[4]{q}$。因此结论成立。 □

特别地，我们有下面的推论。

推论4.18. 在$\mathbb{C}^{3q-2}$中存在大小为q^2-q的等角线，其中q是一个素数幂。

4.2.4　单纯型Grassmannian 填充的三个构造

4.2.4.1　第一个构造

定理4.19. 如果在群$(G,\cdot)$中存在一个参数为(v,k,λ)的差集D，则在实*Grassmannian* 空间$G_{\mathbb{R}}(v,k)$中存在v个维数为k的实子空间形成一个单纯型填充。

证明. 设$e_g\ (g\in G)$是$\mathbb{R}^v$的一组标准正交基。设U_1是由

$$e_d,\ d\in D$$

张成的k-维子空间。则通过置换$e_g\mapsto e_{g\cdot h}\ (h\in G)$，我们还能得到另外$v-1$个子空间$U_h$。

设$D=\{d_1,\cdots,d_k\}$，P_h是U_h的射影矩阵且$E_h=(e_{d_1\cdot h},\cdots,e_{d_k\cdot h})$。则$E_h^*$是$U_h$的生成矩阵，它的行是$U_h$的正交基。因此$P_h=E_hE_h^*$。

对于两个不同的子空间U_g和U_h，我们计算可得

$$\begin{aligned} d^2(U_g, U_h) &= k - \mathrm{tr}(P_g P_h) \\ &= k - \mathrm{tr}(E_g E_g^* E_h E_h^*) \\ &= k - \mathrm{tr}((E_g^* E_h E_h^*) E_g) \\ &= k - \mathrm{tr}((E_g^* E_h)(E_g^* E_h)^*) \\ &= k - |(D \cdot g) \cap (D \cdot h)| \\ &= k - \lambda. \end{aligned}$$

注意到$k(k-1) = \lambda(v-1)$，$\mathbb{R}^v$中v个k-维子空间的单纯型界为：

$$\min_{U \neq V} d^2(U, V) \leq \frac{k(v-k)}{v} \frac{v}{v-1} = k - \lambda.$$

□

我们给个例子来说明我们的构造

例4.20. 设$v = 7$和$D = \{1, 2, 4\}$。则D是$(\mathbb{Z}_7, +)$中的一个$(7, 3, 1)$差集。子空间U_0由

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

生成且其他子空间通过循环坐标可得。容易验证每对子空间有相同的距离。

下面，我们通过已知的差集，给出几类最优填充。

例4.21 (斜Hadamard 差集[122]). 斜*Hadamard* 差集是具有参数$(q, \frac{q-1}{2}, \frac{q-3}{4})$的差集且$G$是$D$, $-D$和1_G的并，其中$q \equiv 3 \pmod 4$是一个素数幂。根据定理*4.19*，对每个素数幂$q \equiv 3 \pmod 4$，在实*Grassmannian* 空间$G_{\mathbb{R}}(q, \frac{q-1}{2})$中存在$q$个维数为$\frac{q-1}{2}$的实子空间形成一个单纯型填充。

例4.22 (具有Singer 参数的差集[139]). 一个差集称为具有*Singer* 参数如果它的参数具有形式$(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}, \frac{q^{m-2}-1}{q-1})$，其中$q$是一个素数幂和$m$是一个正整数。目前有很多具有*Singer* 参数的差集的构造。根据定理*4.19*，对任意的素数幂q和正整数m，在实*Grassmannian* 空间$G_{\mathbb{R}}(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1})$中存在$\frac{q^m-1}{q-1}$个维数为$\frac{q^{m-1}-1}{q-1}$的实子空间形成一个单纯型填充。

例4.23 (McFarland 差集[118]). *McFarland* 差集是具有参数$(q^{m+1}(1+\frac{q^{m+1}-1}{q-1}), q^m\frac{q^{m+1}-1}{q-1}, q^m\frac{q^m-1}{q-1})$的差集，其中$q$是一个素数幂且$m$是一个正整数。则根据定理*4.19*，对任意的素数幂q和正整数m，在实*Grassmannian* 空间$G_{\mathbb{R}}(q^{m+1}(1+\frac{q^{m+1}-1}{q-1}), q^m\frac{q^{m+1}-1}{q-1})$中存在$q^{m+1}(1+\frac{q^{m+1}-1}{q-1})$个维数为$q^m\frac{q^{m+1}-1}{q-1}$的实子空间形成一个单纯型填充。

最后，我们给出一些评论。

评论4.24. *1.* 由于有很多差集，比如：*Menon* 差集[37]，分圆差集[105]，孪生素数差集[155]等等，利用定理*4.19*，我们可以得到更多的最优填充。

2. 斜*Hadamard* 差集有很多不等价构造[154]，因此对相同参数我们有很多选择。对其他差集也是类似的。

4.2.4.2　第二个构造

在这个小节，我们给出第二个最优填充的构造。我们首先给出下面的定义。

定义4.25. 一个$N\times N$矩阵H称为复*Hadamard* 矩阵，如果对任意$j,k=1,2,\cdots,N$，$|H_{jk}|=1$且$HH^*=NI_N$，其中I_N是单位矩阵。

对任意自然数N，复Hadamard 矩阵均存在。例如：$H=(e^{2\pi i(j-1)(k-1)/N})_{j,k=0,\cdots,N-1}$是一个$N\times N$复Hadamard 矩阵。

定理4.26. 对任意素数幂$q\equiv 3 \pmod 4$，在复*Grassmannian* 空间$G_{\mathbb{C}}(q,\frac{q-1}{2})$中，存在$\frac{q(q+1)}{2}$个维数为$\frac{q-1}{2}$的复子空间形成一个单纯型填充。

证明. 设$q\equiv 3 \pmod 4$是一个素数幂，$k=\frac{q-1}{2}$，$(G,+)$是阶为q的交换群以及$D=\{d_1,d_2,\cdots,d_{\frac{q-1}{2}}\}$是$(G,+)$中参数为$(q,\frac{q-1}{2},\frac{q-3}{4})$的斜Hadamard 差集。则$-D$也是一个差集

且$D\cup(-D)\cup\{0_G\}=G$。对任意的非恒等元$x\in G$，我们有

$$\begin{aligned}&|D\cap(-D+x)|+|(D+x)\cap -D|\\=&|(D\cup -D)\cap((D\cup -D)+x)|-|D\cap(D+x)|-|-D\cap(-D+x)|\\=&q-2-\frac{q-3}{4}-\frac{q-3}{4}\\=&\frac{q-1}{2}.\end{aligned}$$

设$C=\frac{1+\sqrt{q+2}}{\sqrt{q+1}}$ 且e_g $(g\in G)$ 是$\mathbb{C}^q$ 的标准正交基。设$H=(H_{ij})_{0\le i,j\le\frac{q-1}{2}}$ 是一个复Hadamard 矩阵，我们假设对任意i,j，$H_{i0}=H_{0j}=1$。设U_{t0} $(0\le t\le\frac{q-1}{2})$ 是由

$$e_{d_i}+\overline{H_{it}}Ce_{-d_i},\ d_i\in D$$

张成的$\frac{q-1}{2}$-维子空间。对每个U_{t0}，通过置换$e_g\mapsto e_{g+h}$ $(h\in G)$，我们还得到$q-1$ 个子空间U_{th}。

设P_{th} 是U_{th} 的射影矩阵以及$A_{th}=(\frac{e_{d_1+h}+H_{1t}Ce_{-d_1+h}}{\sqrt{1+C^2}},\cdots,\frac{e_{d_k+h}+H_{kt}Ce_{-d_k+h}}{\sqrt{1+C^2}})$。则$A_{th}^*$ 是U_{th} 的生成矩阵，其中它的行是U_{th} 的标准正交基。因此$P_{th}=A_{th}A_{th}^*$。

由于$D\cap(-D)=\emptyset$，对任意的$t\neq s$，我们有$A_{th}^*A_{sh}=\mathrm{diag}(\frac{1+C^2\overline{H_{1t}}H_{1s}}{1+C^2},\cdots,\frac{1+C^2\overline{H_{kt}}H_{ks}}{1+C^2})$。则对两个子空间$U_{tg}$ 和U_{sg} $(t\neq s)$，我们有

$$\begin{aligned}d^2(U_{tg},U_{sg})&=\frac{q-1}{2}-\mathrm{tr}(P_{tg}P_{sg})\\&=\frac{q-1}{2}-\mathrm{tr}(A_{tg}A_{tg}^*A_{sg}A_{sg}^*)\\&=\frac{q-1}{2}-\mathrm{tr}((A_{tg}^*A_{sg}A_{sg}^*)A_{tg})\\&=\frac{q-1}{2}-\mathrm{tr}((A_{tg}^*A_{sg})(A_{tg}^*A_{sg})^*)\\&=\frac{q-1}{2}-\frac{1}{(1+C^2)^2}\sum_{i=1}^{k}(1+C^2\overline{H_{it}}H_{is})(1+C^2H_{it}\overline{H_{is}})\\&=\frac{q-1}{2}-\frac{1}{(1+C^2)^2}\sum_{i=1}^{k}(1+C^2\overline{H_{it}}H_{is}+C^2H_{it}\overline{H_{is}}+C^4)\\&=\frac{q-1}{2}-\frac{q-1}{2}\frac{1+C^4}{(1+C^2)^2}+\frac{2C^2}{(1+C^2)^2}\\&=\frac{(q+1)^2}{4(q+2)}.\end{aligned}$$

设$E_{th1}=(\frac{e_{d_1+h}}{\sqrt{1+C^2}},\cdots,\frac{e_{d_k+h}}{\sqrt{1+C^2}})$ 和$E_{th2}=(\frac{H_{1t}Ce_{-d_1+h}}{\sqrt{1+C^2}},\cdots,\frac{H_{kt}Ce_{-d_k+h}}{\sqrt{1+C^2}})$，则$A_{th}=E_{th1}+E_{th2}$。由于$D\cap(-D)=\emptyset$，我们有$E_{th1}^*E_{th2}=0$。对任意的$g\neq h$，$A_{tg}^*A_{sh}=E_{tg1}^*E_{sh1}+$

$E_{tg1}^*E_{sh2}+E_{tg2}^*E_{sh1}+E_{tg2}^*E_{sh2}$。则

$$\begin{aligned}
&\mathrm{tr}((A_{tg}^*A_{sh})(A_{tg}^*A_{sh})^*)\\
=&\mathrm{tr}((E_{tg1}^*E_{sh1})(E_{tg1}^*E_{sh1})^*+(E_{tg1}^*E_{sh2})(E_{tg1}^*E_{sh2})^*+(E_{tg2}^*E_{sh1})(E_{tg2}^*E_{sh1})^*+(E_{tg2}^*E_{sh2})(E_{tg2}^*E_{sh2})^*).
\end{aligned}$$

对两个子空间U_{tg} 和U_{sh} ($g\neq h$)，利用斜Hadamard 差集的性质，我们有

$$\begin{aligned}
&d^2(U_{tg},U_{sh})\\
=&\frac{q-1}{2}-\mathrm{tr}(P_{tg}P_{sh})\\
=&\frac{q-1}{2}-\mathrm{tr}(A_{tg}A_{tg}^*A_{sh}A_{sh}^*)\\
=&\frac{q-1}{2}-\mathrm{tr}((A_{tg}^*A_{sh}A_{sh}^*)A_{tg})\\
=&\frac{q-1}{2}-\mathrm{tr}((A_{tg}^*A_{sh})(A_{tg}^*A_{sh})^*)\\
=&\frac{q-1}{2}-\mathrm{tr}((E_{tg1}^*E_{sh1})(E_{tg1}^*E_{sh1})^*+(E_{tg1}^*E_{sh2})(E_{tg1}^*E_{sh2})^*+(E_{tg2}^*E_{sh1})(E_{tg2}^*E_{sh1})^*+\\
&(E_{tg2}^*E_{sh2})(E_{tg2}^*E_{sh2})^*)\\
=&\frac{q-1}{2}-|(D+g)\cap(D+h)|\frac{1+C^4}{(1+C^2)^2}-(|(D+g)\cap(-D+h)|+|(D+h)\cap(-D+g)|)\frac{C^2}{(1+C^2)^2}\\
=&\frac{q-1}{2}-\frac{q-3}{4}\frac{1+C^4}{(1+C^2)^2}-\frac{q-1}{2}\frac{C^2}{(1+C^2)^2}\\
=&\frac{(q+1)^2}{4(q+2)}.
\end{aligned}$$

对于$\mathbb{C}^q$中的$\frac{q(q+1)}{2}$ 个$\frac{q-1}{2}$维子空间，我们计算可得它的单纯型界：

$$\min_{U\neq V}d^2(U,V)\leq\frac{\frac{q-1}{2}(q-\frac{q-1}{2})}{q}\frac{\frac{q(q+1)}{2}}{\frac{q(q+1)}{2}-1}=\frac{(q+1)^2}{4(q+2)}.$$

□

评论4.27. *1.* 与定理*4.26* 类似的结果已经出现在文献[21,98]中。在这个小节，我们利用斜*Hadamard* 差集给出一个新的这种最优填充的构造。

2. 事实上，假设$(G,+)$中有两个具有相同参数(v,k,λ)的差集满足下面条件：

(a) $D_1\cap D_2=\emptyset$；

(b) 对任意的非恒等元$x\in G$，存在某个常数μ，$|D_1\cap(D_2+x)|+|(D_1+x)\cap D_2|=\mu$；

(c) 存在$\sigma\in Aut(G)$，$D_2=\sigma(D_1)$。

则把D和$-D$改成D_1和D_2，则上面的构造也有效。不幸的是，如果差集D_1, D_2满足上面的条件，则D_1, D_2一定具有斜*Hadamard*参数的差集。这一点可通过下面的分析得到。

如果D_1, D_2是满足上面条件的两个差集，则对任意的非恒等元$x \in G$，$|(D_1 \cup D_2) \cap ((D_1 \cup D_2) + x)| = \mu + 2\lambda$。因此$D_1 \cup D_2$也是一个差集。通过差集的基本等式，我们有

$$k(k-1) = \lambda(v-1),$$
$$2k(2k-1) = (\mu + 2\lambda)(v-1).$$

因此$(v-1)|gcd(k(k-1), 2k(2k-1))$，从而$v-1 \leq 2k \leq v$。因此$k = \frac{v-1}{2}$，且$D_1, D_2$是具有参数$(v, \frac{v-1}{2}, \frac{v-3}{4})$的差集。

4.2.4.3 第三个构造

在这个小节，我们通过Latin方给出一个最优填充的构造。

定义4.28. 一个阶为n，字母集为$\{0, 1, \cdots, n-1\}$的*Latin*方L是一个$n \times n$阵列满足每个字母在每行每列均恰好出现一次。一个阶为n的*Latin*方L是对称的如果对任意的$0 \leq i, j \leq n-1$，$L(i,j) = L(j,i)$。

关于Latin方已经有很多的研究。相关进展可参考文献[33]。下面我们给出我们的主要构造。

定理4.29. 假设在字母集$\{0, 1, \cdots, st-1\}$上存在一个阶为st的对称*Latin*方L满足下面的条件：

(1) 对于$m = 0, s, 2s, \cdots, s(t-1)$，$L(x,x) = m$解的个数是$s$；

(2) 对于$m = 0, s, 2s, \cdots, s(t-1)$，$i = 0, 1, \cdots, st-1$，设$u(i)$是$L(i, u(i)) = m$的唯一解。则对某个$a|st$，$a \leq s$，我们有$\{(i - u(i)) \pmod{st} : i = 0, 1, \cdots, st-1\} = \{0, a, \cdots, st-a\}$且每个$ja$ $(j = 0, 1, \cdots, \frac{st}{a} - 1)$恰出现$a$次。

则在复*Grassmannian*空间$G_{\mathbb{C}}(st, \frac{s(t+1)}{2})$中，存在$t^2$个维数为$\frac{s(t+1)}{2}$的复子空间形成一个单纯型填充。

证明. 根据对称Latin 方的性质和第一个条件，我们有$2|s(t+1)$。

设ω 是一个本原st-次单位根。对于$m=0,s,2s,\cdots,s(t-1)$ 和$l=0,1,\cdots,t-1$，我们定义矩阵

$$(R_{m,l})_{i,j}=\begin{cases}\omega^{(i-j)l}, & \text{如果}L(i,j)=m;\\ 0, & \text{其他情形,}\end{cases}$$

其中$0\le i,j\le st-1$。

容易验证$R_{m,l}$ 满足下面的条件：

(1) $R_{m,l}^*=R_{m,l}$；

(2) $\mathrm{tr}(R_{m,l})=s$；

(3) $R_{m,l}^2=I$。

接下来，我们计算当$(m,l)\neq(m',l')$时，$\mathrm{tr}(R_{m,l}R_{m',l'})$ 的值。如果$m\neq m'$，则由于$R_{m,l}$ 和$R_{m',l'}$ 的非零位置不交，$\mathrm{tr}(R_{m,l}R_{m',l'})=0$。如果$m=m'$，根据第二个性质，我们有

$$\mathrm{tr}(R_{m,l}R_{m',l'})=\sum_{i=0}^{st-1}\omega^{(i-u(i))(l-l')}=a\sum_{i=0}^{\frac{st}{a}-1}\omega^{ai(l-l')}=0.$$

设$P_{m,l}=\frac{1}{2}(R_{m,l}+I)$，由$R_{m,l}$ 的性质可知

(1) $P_{m,l}^*=P_{m,l}$；

(2) $\mathrm{tr}(P_{m,l})=\frac{s(t+1)}{2}$；

(3) $P_{m,l}^2=P_{m,l}$；

(4) 对于$(m,l)\neq(m',l')$，我们有$\mathrm{tr}(P_{m,l}P_{m',l'})=\frac{s}{2}+\frac{st}{4}$。

设$U_{m,l}$ 是对应于射影矩阵$P_{m,l}$ 的子空间，则两个子空间之间的距离是

$$d^2(U_{m,l},U_{m',l'})=\frac{s(t+1)}{2}-\mathrm{tr}(P_{m,l}P_{m',l'})=\frac{st}{4}.$$

对于$\mathbb{C}^{st}$中t^2 个$\frac{s(t+1)}{2}$维子空间的极小距离的单纯型界是：

$$\min_{U\neq V}d^2(U,V)\le\frac{\frac{s(t+1)}{2}(st-\frac{s(t+1)}{2})}{st}\frac{t^2}{t^2-1}=\frac{st}{4}.$$

因此，在复Grassmannian 空间$G_{\mathbb{C}}(st,\frac{s(t+1)}{2})$ 中，t^2 个矩阵$P_{m,l}$ $(m=0,s,2s,\cdots,s(t-1),$ $l=0,1,\cdots,t-1)$ 形成一个单纯型填充。 □

评论4.30. 设$s=1$，t 是一个奇数，$L(i,j)=(i+j) \pmod t$。根据定理*4.29*，在复*Grassmannian* 空间$G_{\mathbb{C}}(t,\frac{t+1}{2})$ 中，存在t^2 个维数为$\frac{t+1}{2}$ 的复子空间单纯型填充。这个结果已经出现在文献[98] 中。

现在我们给出一个满足定理4.29的对称Latin 方的构造。设$G(n)=\{0,1,\cdots,n-1\}$，s 是一个正偶数且t 是一个正奇数。定义$f_s(x,y):\ G(s)\times G(s)\to G(s)$ 为

$$f_s(x,y)=\begin{cases}0, & \text{如果}x=y;\\ a+1, & \text{如果}a\in G(s-1),\ \{x,y\}=\{a,s-1\};\\ a+1, & \text{如果}a,x,y\in G(s-1),\ x\neq y,\ x+y\equiv 2a \pmod{s-1}.\end{cases}$$

设$g_t(x,y)=(x+y) \pmod t$ 是从$G(t)\times G(t)$ 到$G(t)$ 的映射。则我们定义$L_{s,t}(x,y):\ G(st)\times G(st)\to G(st)$：

$$L_{s,t}(sx_1+x_2,sy_1+y_2)=sg_t(x_1,y_1)+f_s(x_2,y_2) \text{ 对于} x_1,y_1\in G(t),x_2,y_2\in G(s).$$

容易验证$L_{s,t}(x,y)$ 满足下面的条件：

(1) $L_{s,t}(x,y)=L_{s,t}(y,x)$;

(2) 对于$m=0,s,2s,\cdots,s(t-1)$，$L_{s,t}(x,x)=m$ 的解的个数是s;

(3) 对任意的$i,k\in G(st)$，存在唯一的$j\in G(st)$ 使得$L_{s,t}(i,j)=k$。

则对于$m=0,s,2s,\cdots,s(t-1)$，$i\in G(t)$ 和$j\in G(s)$，存在唯一的$u(i)\in G(t),\ u(j)\in G(s)$ 使得$L_{s,t}(si+j,su(i)+u(j))=m$。根据$L_{s,t}(x,y)$ 的定义，我们有$u(i)=(\frac{m}{s}-i) \pmod t$ 且$u(j)=j$。因此$\{(si+j-su(i)-u(j)) \pmod{st}:i\in G(t),j\in G(s)\}=\{0,s,2s,\cdots,s(t-1)\}$ 且每个ks $(k=0,1,\cdots,t-1)$ 出现s 次。从而，$L_{s,t}(x,y)$ 形成一个满足定理4.29中条件的对称Latin 方。我们有下面的推论。

推论4.31. 对任意的正偶数s和正奇数t，在复*Grassmannian* 空间$G_{\mathbb{C}}(st,\frac{s(t+1)}{2})$ 中，存在t^2 个维数为$\frac{s(t+1)}{2}$ 的复子空间形成一个单纯型填充。

4.2.5 总结

在文献[99] 中，König 利用差集，在$\mathbb{C}^d$中构造了大小为d^2-d+1 的等角线，其中$d-1$ 是素数幂。最近，Jedwab 等人[84,85] 利用两两无偏基构造了具有较大大小的等角线集

合。它们的结果可以像4.2.3小节那样利用相对差集得到。这一工具的本质是$|\{|\chi(D)|:\chi\in\widehat{G}\backslash\{\chi_0\}\}|=1$ (或者2) 如果D 是群G 中的差集(或者相对差集)。注意到如果D 是一个直积差集，则$|\chi(D)|$ $(\chi\in\widehat{G}\backslash\{\chi_0\})$ 取三个值。在这部分，我们在$\mathbb{C}^d$中给出了一个大小为$O(d^2)$ 的等角线。这一方法也可以推广，如果我们可以找到交换群G 中的一个子集D 满足$|\chi(D)|$ $(\chi\in\widehat{G}\backslash\{\chi_0\})$ 取较少的值。

在4.2.4小节中，我们给出了三个单纯型Grassmannian 填充。基于第一个构造，任意的一个差集均可自动给出一个单纯型Grassmannian 填充。第二个构造是利用斜Hadamard 差集给出了文献[21]中的构造的一个新解释。第三个构造是利用特殊的Latin 方给出很多新的单纯型Grassmannian 填充。

5 其他工作

本章节概述了作者的其他一些工作。限于篇幅，只对这些课题的进展做简要介绍而不再展开论述。

5.1 伪平面函数的构造和相关的结合方案

奇特征的有限域上的平面函数可用来构造射影平面。而在偶特征的有限域上，并不存在平面函数。为了克服这个问题，Zhou[164] 在偶特征的有限域上提出了伪平面函数的概念，并利用伪平面函数构造了射影平面。这个令人兴奋的发现促使我们考虑伪平面函数的构造。我们构造了三类新的伪平面二项式函数。同时，我们证明了任意一个伪平面函数都可以给出一个5-类的结合方案。这部分工作已经发表在《Designs, Codes and Cryptography》。

5.2 b-字符码

b-字符码的研究背景源于高密度存储设备的兴起。虽然编码过程仍同于往常，但在高密度存储设备上，读取信息时只对单个位置读取时不便的，自然的推广是将码元成批次的读取。纠错方式也从原先对单个位置的纠错变成对这样一个读取的b长码字进行纠错。对此问题的最早研究来自Cassuto 和Blaum[27]。

我们对此问题的贡献为，在极小结对距离$d = 5$ 时，完整地对所有可行的码长n 构造了极大距离可分字符结对码。另分别通过有限几何的工具和代数曲线的工具，对于极小结对距离d 取6 和7 时也给出了一类新的极大距离可分字符结对码的构造。本工作已被《Designs, Codes and Cryptography》接收。

另外，对于$b \geq 3$的情形，我们建立了Singleton 型界，并利用有限几何的方法，给出了几类达到Singleton 型界的b-字符码的构造。这部分工作已投稿到《Finite Fields and Their Applications》。

5.3 长度在74 和116 之间的某些最优自对偶码的存在性

长期以来，最优二元自对偶码的存在性一直是一个重要的问题。我们通过选取合适的自同构群，构造了很多新的长度在74 和116 之间的最优自对偶码。这部分工作已经发表在《The Electronic Journal of Combinatorics》。

5.4 有限域上的置换多项式

由于在密码，编码和组合设计理论的应用，置换多项式最近被广泛地研究。我们构造了四类单项完全置换多项式和一类三项完全置换多项式，特别地，我们解决了一个Wu 等人[157]提出的猜想。进一步的，我们还给出了两类三项置换多项式。这部分工作已经发表在《Designs, Codes and Cryptography》。

5.5 m-序列的互相关性

在码分多址系统中，一个流行的扩频方法是利用序列。利用低自相关和低互相关的序列，可以降低通行过程中不同用户之间的干扰。因而，低相关序列成为了一个深受关注的研究课题。由于一个m-序列拥有理想的两值自相关。许多研究者考虑了一对m-序列的互相关值分布。我们考虑周期为$3^{3r}-1$的三元m-序列和它的d-采样的互相关，其中$d=3^r+2$或$d=3^{2r}+2$，且$(r,3)=1$。借鉴Dobbertin[44] 和Feng 等人[53]的思想，我们完全决定了互相关分布。这部分工作已经发表在《IEEE Transactions on Information Theory》。

5.6 分组密码的预处理—AONT 变换

AONT 变换最早由图灵奖得主Ron Rivest[129] 提出，以作为使用分组密码之前的预处理步骤，为分组密码提供了一层额外的安全性。在二元域上，完全符合AONT 变换要求的矩阵并不存在。如何构造一个尽量接近AONT 变换要求的二元矩阵? Stinson 等人[36]将此问题转化为下面的等价问题：怎样的一个可逆矩阵中有最大比例的可逆2×2 子矩阵，这个最大的比例值为多少? 我们证明了此最大的比例为0.5。并且还给出了具体构作矩阵的方案。这部分工作已经发表在《Discrete Mathematics》。

5.7 常维子空间码的构造

网络编码由Ahlswede[1] 等人于2000年引入。Koetter 和Kschischang[100] 证明了最为适用于随机网络编码纠错机制的编码方案是子空间码，即有限域上的n维空间的一族子空间。这激发了对常维码的研究。目前，常维码的研究主要有两种方法，一种是利用极大秩码，另一种是利用自同构群。Ferrers 表上的最优秩码可以用来构造子空间码，我们给出了一类Ferrers 表上的最优秩码的构造。这部分工作还在整理中。

參考文獻

[1] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian. On perfect codes and related concepts. *Des. Codes Cryptogr.*, 22(3):221–237, 2001.

[2] B. F. AlBdaiwi and B. Bose. Quasi-perfect Lee distance codes. *IEEE Trans. Inform. Theory*, 49(6):1535–1539, 2003.

[3] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, 2007.

[4] D. M. Appleby. Symmetric informationally complete-positive operator valued measures and the extended Clifford group. *J. Math. Phys.*, 46(5):052107, 29, 2005.

[5] K. T. Arasu and T. A. Gulliver. Self-dual codes over $\mathbb{F}_p$ and weighing matrices. *IEEE Trans. Inform. Theory*, 47(5):2051–2055, 2001.

[6] C. Araujo, I. Dejter, and P. Horak. A generalization of Lee codes. *Des. Codes Cryptogr.*, 70(1-2):77–90, 2014.

[7] A. Ashikhmin and A. R. Calderbank. Grassmannian packings from operator Reed-Muller codes. *IEEE Trans. Inform. Theory*, 56(11):5689–5714, 2010.

[8] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.

[9] E. F. Assmus, Jr. and J. D. Key. *Designs and their codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1992.

[10] E. F. Assmus, Jr. and H. F. Mattson, Jr. New 5-designs. *J. Combin. Theory*, 6:122–151, 1969.

[11] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri. The structure of 1-generator quasi-twisted codes and new linear codes. *Des. Codes Cryptogr.*, 24(3):313–326, 2001.

[12] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[13] K. Bibak, B. M. Kapron, and V. Srinivasan. The cayley graphs associated with some quasi-perfect lee codes are ramanujan graphs. *IEEE Trans. Inform. Theory*, 62(11):6355–6358, 2016.

[14] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

[15] B. G. Bodmann and J. I. Haas. Maximal orthoplectic fusion frames from mutually unbiased bases and block designs. arXiv: 1607.04546.

[16] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[17] S. Bouyuklieva and I. Bouyukliev. An algorithm for classification of binary self-dual codes. *IEEE Trans. Inform. Theory*, 58(6):3933–3940, 2012.

[18] M. Buratti. Cyclic designs with block size 4 and related optimal optical orthogonal codes. *Des. Codes Cryptogr.*, 26(1-3):111–125, 2002.

[19] S. Buyuklieva. On the binary self-dual codes with an automorphism of order 2. *Des. Codes Cryptogr.*, 12(1):39–48, 1997.

[20] S. Buzaglo and T. Etzion. Tilings with n-dimensional chairs and their applications to asymmetric codes. *IEEE Trans. Inform. Theory*, 59(3):1573–1582, 2013.

[21] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor, and N. J. A. Sloane. A group-theoretic framework for the construction of packings in Grassmannian spaces. *J. Algebraic Combin.*, 9(2):129–140, 1999.

[22] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, 1997.

[23] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $\mathrm{GF}(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[24] R. Calderbank. A square root bound on the minimum weight in quasicyclic codes. *IEEE Trans. Inform. Theory*, 29(3):332–337, 1983.

[25] C. Camarero and C. Martínez. Quasi-perfect Lee codes of radius 2 and arbitrarily large dimension. *IEEE Trans. Inform. Theory*, 62(3):1183–1192, 2016.

[26] A. Campello, G. C. Jorge, J. E. Strapasson, and S. I. R. Costa. Perfect codes in the l_p metric. *European J. Combin.*, 53:72–85, 2016.

[27] Y. Cassuto and M. Blaum. Codes for symbol-pair read channels. *IEEE Trans. Inform. Theory*, 57(12):8011–8020, 2011.

[28] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck. Codes for asymmetric limited-magnitude errors with application to multilevel flash memories. *IEEE Trans. Inform. Theory*, 56(4):1582–1595, 2010.

[29] Y. Chang and L. Ji. Optimal $(4up, 5, 1)$ optical orthogonal codes. *J. Combin. Des.*, 12(5):346–361, 2004.

[30] P. Charters. Generalizing binary quadratic residue codes to higher power residues over larger fields. *Finite Fields Appl.*, 15(3):404–413, 2009.

[31] B. Chen, S. Ling, and G. Zhang. Application of constacyclic codes to quantum MDS codes. *IEEE Trans. Inform. Theory*, 61(3):1474–1484, 2015.

[32] H. Chen, S. Ling, and C. Xing. Quantum codes from concatenated algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 51(8):2915–2920, 2005.

[33] C. J. Colbourn and J. H. Dinitz, editors. *Handbook of combinatorial designs*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[34] J. H. Conway, R. H. Hardin, and N. J. A. Sloane. Packing lines, planes, etc.: packings in Grassmannian spaces. *Experiment. Math.*, 5(2):139–159, 1996.

[35] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[36] P. D'Arco, N. N. Esfahani, and D. R. Stinson. All or nothing at all. *arXiv:1510.03655*, 2015.

[37] J. A. Davis and J. Jedwab. A survey of Hadamard difference sets. In *Groups, difference sets, and the Monster (Columbus, OH, 1993)*, volume 4 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 145–156. de Gruyter, Berlin, 1996.

[38] J. A. Davis, J. Jedwab, and M. Mowbray. New families of semi-regular relative difference sets. *Des. Codes Cryptogr.*, 13(2):131–146, 1998.

[39] D. de Caen. Large equiangular sets of lines in Euclidean space. *Electron. J. Combin.*, 7:R55, (3 pages), 2000.

[40] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[41] P. Delsarte, J. M. Goethals, and J. J. Seidel. Bounds for systems of lines, and jacobi polynomials. *Philips Res. Rep.*, 30:91–105, 1975.

[42] I. S. Dhillon, R. W. Heath, Jr., T. Strohmer, and J. A. Tropp. Constructing packings in Grassmannian manifolds via alternating projection. *Experiment. Math.*, 17(1):9–35, 2008.

[43] C. Ding. Cyclic codes from cyclotomic sequences of order four. *Finite Fields Appl.*, 23:8–34, 2013.

[44] H. Dobbertin. One-to-one highly nonlinear power functions on $\mathrm{GF}(2^n)$. *Appl. Algebra Engrg. Comm. Comput.*, 9(2):139–152, 1998.

[45] Y. Edel. Some good quantum twisted codes. Online available at `https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html`. Accessed on 2014-12-21.

[46] N. Elarief and B. Bose. Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude. *IEEE Trans. Inform. Theory*, 56(3):979–983, 2010.

[47] T. Etzion. Product constructions for perfect Lee codes. *IEEE Trans. Inform. Theory*, 57(11):7473–7481, 2011.

[48] T. Etzion, A. Vardy, and E. Yaakobi. Coding for the Lee and Manhattan metrics with weighing matrices. *IEEE Trans. Inform. Theory*, 59(10):6712–6723, 2013.

[49] M. F. Ezerman, S. Jitman, and P. Solé. Xing-Ling codes, duals of their subcodes, and good asymmetric quantum codes. *Des. Codes Cryptogr.*, 75(1):21–42, 2015.

[50] K. Feng. Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ $(p \geq 3)$ exist. *IEEE Trans. Inform. Theory*, 48(8):2384–2391, 2002.

[51] K. Feng, S. Ling, and C. Xing. Asymptotic bounds on quantum codes from algebraic geometry codes. *IEEE Trans. Inform. Theory*, 52(3):986–991, 2006.

[52] T. Feng. Relative (pn, p, pn, n)-difference sets with $\mathrm{GCD}(p, n) = 1$. *J. Algebraic Combin.*, 29(1):91–106, 2009.

[53] T. Feng, K. Leung, and Q. Xiang. Binary cyclic codes with two primitive nonzeros. *Sci. China Math.*, 56(7):1403–1412, 2013.

[54] T. Feng and Q. Xiang. Semi-regular relative difference sets with large forbidden subgroups. *J. Combin. Theory Ser. A*, 115(8):1456–1473, 2008.

[55] P. Gaborit. Quadratic double circulant codes over fields. *J. Combin. Theory Ser. A*, 97(1):85–107, 2002.

[56] P. Gaborit and A. Otmani. Tables of self-dual codes. Online available at `http://www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html`.

[57] P. Gaborit and A. Otmani. Experimental constructions of self-dual codes. *Finite Fields Appl.*, 9(3):372–394, 2003.

[58] S. Galovich and S. Stein. Splittings of abelian groups by integers. *Aequationes Math.*, 22(2-3):249–267, 1981.

[59] M. J. Ganley. Direct product difference sets. *J. Combin. Theory Ser. A*, 23(3):321–332, 1977.

[60] M. Garcia-Rodriguez, Y. Yañez, M. J. Garcia-Hernandez, J. Salazar, A. Turo, and J. A. Chavez. Application of Golay codes to improve the dynamic range in ultrasonic lamb waves air-coupled systems. *NDT & E International*, 43(8):677–686, 2010.

[61] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European J. Combin.*, 30(1):246–262, 2009.

[62] S. W. Golomb and L. R. Welch. Perfect codes in the Lee metric and the packing of polyominoes. *SIAM J. Appl. Math.*, 18:302–317, 1970.

[63] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2015-03-09.

[64] M. Grassl, T. Beth, and M. Roetteler. On optimal quantum codes. *Int. J. Quantum Inf.*, 2(01):55–64, 2004.

[65] M. Grassl and T. A. Gulliver. On circulant self-dual codes over small fields. *Des. Codes Cryptogr.*, 52(1):57–81, 2009.

[66] M. Grassl and M. Rotteler. Quantum MDS codes over small fields. In *Proc. Int. Symp. Inf. Theory*, pages 1104–1108, 2015.

[67] S. Gravier, M. Mollard, and C. Payan. On the non-existence of 3-dimensional tiling in the Lee metric. *European J. Combin.*, 19(5):567–572, 1998.

[68] G. Greaves, J. H. Koolen, A. Munemasa, and F. Szöllősi. Equiangular lines in Euclidean spaces. *J. Combin. Theory Ser. A*, 138:208–235, 2016.

[69] T. A. Gulliver and M. Harada. Classification of extremal double circulant self-dual codes of lengths 74–88. *Discrete Math.*, 306(17):2064–2072, 2006.

[70] J. Haantjes. Equilateral point-sets in elliptic two- and three-dimensional spaces. *Nieuw Arch. Wiskunde (2)*, 22:355–362, 1948.

[71] M. Harada. The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes. *Finite Fields Appl.*, 3(2):131–139, 1997.

[72] M. Harada, M. Kiermaier, A. Wassermann, and R. Yorgova. New binary singly even self-dual codes. *IEEE Trans. Inform. Theory*, 56(4):1612–1617, 2010.

[73] D. Hickerson. Splittings of finite groups. *Pacific J. Math.*, 107(1):141–171, 1983.

[74] D. Hickerson and S. Stein. Abelian groups and packing by semicrosses. *Pacific J. Math.*, 122(1):95–109, 1986.

[75] Y. Hiramine. On abelian $(2n, n, 2n, 2)$-difference sets. *J. Combin. Theory Ser. A*, 117(7):996–1003, 2010.

[76] P. Horak. On perfect Lee codes. *Discrete Math.*, 309(18):5551–5561, 2009.

[77] P. Horak. Tilings in Lee metric. *European J. Combin.*, 30(2):480–489, 2009.

[78] P. Horak and B. AlBdaiwi. Non-periodic tilings of $\mathbb{R}^n$ by crosses. *Discrete Comput. Geom.*, 47(1):1–16, 2012.

[79] P. Horak and B. F. AlBdaiwi. Diameter perfect Lee codes. *IEEE Trans. Inform. Theory*, 58(8):5490–5499, 2012.

[80] P. Horak and O. Grošek. A new approach towards the Golomb-Welch conjecture. *European J. Combin.*, 38:12–22, 2014.

[81] W. C. Huffman. Automorphisms of codes with applications to extremal doubly even codes of length 48. *IEEE Trans. Inform. Theory*, 28(3):511–521, 1982.

[82] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11(3):451–490, 2005.

[83] M. Ikeda. A remark on the non-existence of generalized bent functions. In *Number theory and its applications (Ankara, 1996)*, volume 204 of *Lecture Notes in Pure and Appl. Math.*, pages 109–119. Dekker, New York, 1999.

[84] J. Jedwab and A. Wiebe. Large sets of complex and real equiangular lines. *J. Combin. Theory Ser. A*, 134:98–102, 2015.

[85] J. Jedwab and A. Wiebe. Constructions of complex equiangular lines from mutually unbiased bases. *Des. Codes Cryptogr.*, 80(1):73–89, 2016.

[86] L. Jin, S. Ling, J. Luo, and C. Xing. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. *IEEE Trans. Inform. Theory*, 56(9):4735–4740, 2010.

[87] L. Jin and C. Xing. A construction of quantum codes via a class of classical polynomial codes. In *Proc. IEEE Int. Symp. Information Theory (ISIT)*, pages 339–342, 2012.

[88] L. Jin and C. Xing. A construction of new quantum MDS codes. *IEEE Trans. Inform. Theory*, 60(5):2921–2925, 2014.

[89] X. Kai and S. Zhu. New quantum MDS codes from negacyclic codes. *IEEE Trans. Inform. Theory*, 59(2):1193–1197, 2013.

[90] X. Kai, S. Zhu, and P. Li. Constacyclic codes and some new quantum MDS codes. *IEEE Trans. Inform. Theory*, 60(4):2080–2086, 2014.

[91] M. Karlin. New binary coding results by circulants. *IEEE Trans. Inform. Theory*, IT-15:81–92, 1969.

[92] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[93] D. Kim. Nonexistence of perfect 2-error correcting Lee codes in certain dimensions. arXiv: 1701.08412.

[94] T. Kløve, B. Bose, and N. Elarief. Systematic, single limited magnitude error correcting codes for flash memories. *IEEE Trans. Inform. Theory*, 57(7):4477–4487, 2011.

[95] T. Kløve, J. Luo, I. Naydenova, and S. Yari. Some codes correcting asymmetric errors of limited magnitude. *IEEE Trans. Inform. Theory*, 57(11):7459–7472, 2011.

[96] T. Kløve, J. Luo, and S. Yari. Codes correcting single errors of limited magnitude. *IEEE Trans. Inform. Theory*, 58(4):2206–2219, 2012.

[97] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A (3)*, 55(2):900–911, 1997.

[98] T. Kocák and M. Niepel. Families of optimal packings in real and complex grassmannian spaces. *J. Algebraic Combin.* to appear. Doi:10.1007/s10801-016-0702-x.

[99] H. König. Cubature formulas on spheres. In *Advances in multivariate approximation (Witten-Bommerholz, 1998)*, volume 107 of *Math. Res.*, pages 201–211. Wiley-VCH, Berlin, 1999.

[100] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[101] G. G. La Guardia. New quantum MDS codes. *IEEE Trans. Inform. Theory*, 57(8):5551–5554, 2011.

[102] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77(1):198, 1996.

[103] C. W. H. Lam, L. Thiel, and S. Swiercz. The nonexistence of finite projective planes of order 10. *Canad. J. Math.*, 41(6):1117–1123, 1989.

[104] C. Y. Lee. Some properties of nonbinary error-correcting codes. *IRE Trans.*, IT-4:77–82, 1958.

[105] E. Lehmer. On residue difference sets. *Canadian J. Math.*, 5:425–432, 1953.

[106] P. W. H. Lemmens and J. J. Seidel. Equiangular lines. *J. Algebra*, 24:494–512, 1973.

[107] T. Lepistö. A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric. *Inform. and Control*, 49(2):109–124, 1981.

[108] K. H. Leung, S. Ling, and S. L. Ma. Constructions of semi-regular relative difference sets. *Finite Fields Appl.*, 7(3):397–414, 2001.

[109] K. H. Leung, S. L. Ma, and V. Tan. Planar functions from Z_n to Z_n. *J. Algebra*, 224(2):427–436, 2000.

[110] Z. Li, L. Xing, and X. Wang. Quantum generalized Reed-Solomon codes: unified framework for quantum maximum-distance-separable codes. *Phys. Rev. A (3)*, 77(1):012308, 4, 2008.

[111] S. Ling, H. Niederreiter, and C. Xing. Symmetric polynomials and some good codes. *Finite Fields Appl.*, 7(1):142–148, 2001. Dedicated to Professor Chao Ko on the occasion of his 90th birthday.

[112] S. Ling and P. Solé. Good self-dual quasi-cyclic codes exist. *IEEE Trans. Inform. Theory*, 49(4):1052–1053, 2003.

[113] S. L. Ma. Planar functions, relative difference sets, and character theory. *J. Algebra*, 185(2):342–356, 1996.

[114] S. L. Ma and B. Schmidt. Relative (p^a, p^b, p^a, p^{a-b})-difference sets: a unified exponent bound and a local ring construction. *Finite Fields Appl.*, 6(1):1–22, 2000.

[115] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II*. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[116] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson. Good self dual codes exist. *Discrete Math.*, 3:153–162, 1972.

[117] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes. *Information and Control*, 22:188–200, 1973.

[118] R. L. McFarland. A family of difference sets in non-cyclic groups. *J. Combin. Theory Ser. A*, 15:1–10, 1973.

[119] K. Momihara, M. Müller, J. Satoh, and M. Jimbo. Constant weight conflict-avoiding codes. *SIAM J. Discrete Math.*, 21(4):959–979, 2007.

[120] G. Nebe, E. M. Rains, and N. J. A. Sloane. *Self-dual codes and invariant theory*, volume 17 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006.

[121] T. L. O'Donovan, P. A. Contla, and D. K. Das-Gupta. Application of Golay codes and piezoelectric ultrasound transducer to biomedical noninvasive measurement. *IEEE Trans. Electr. Insul.*, 28(1):93–100, 1993.

[122] R. E. A. C. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.

[123] V. Pless. Symmetry codes over $\mathrm{GF}(3)$ and new five-designs. *J. Combin. Theory Ser. A*, 12:119–142, 1972.

[124] K. A. Post. Nonexistence theorems on perfect Lee codes over large alphabets. *Information and Control*, 29(4):369–380, 1975.

[125] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.

[126] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44(1):134–139, 1998.

[127] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[128] E. M. Rains and N. J. A. Sloane. Self-dual codes. In *Handbook of coding theory, Vol. I, II*, pages 177–294. North-Holland, Amsterdam, 1998.

[129] R. L. Rivest. All-or-nothing encryption and the package transform. In *Fast Software Encryption*, pages 210–218. Springer, 1997.

[130] A. Roy. Bounds for codes and designs in complex subspaces. *J. Algebraic Combin.*, 31(1):1–32, 2010.

[131] B. Schmidt. On (p^a, p^b, p^a, p^{a-b})-relative difference sets. *J. Algebraic Combin.*, 6(3):279–297, 1997.

[132] B. Schmidt. *Characters and cyclotomic fields in finite geometry*, volume 1797 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.

[133] M. Schwartz. Quasi-cross lattice tilings with applications to flash memory. *IEEE Trans. Inform. Theory*, 58(4):2397–2405, 2012.

[134] M. Schwartz. On the non-existence of lattice tilings by quasi-crosses. *European J. Combin.*, 36:130–142, 2014.

[135] A. J. Scott and M. Grassl. Symmetric informationally complete positive-operator-valued measures: a new computer study. *J. Math. Phys.*, 51(4):042203, 16, 2010.

[136] D. N. Semënovykh. A generalization of quadratic residue codes to the case of residues of degrees three and four. *Diskret. Mat.*, 17(4):143–149, 2005.

[137] P. W. Shor and N. J. A. Sloane. A family of optimal packings in Grassmannian manifolds. *J. Algebraic Combin.*, 7(2):157–163, 1998.

[138] K. W. Shum, W. S. Wong, and C. S. Chen. A general upper bound on the size of constant-weight conflict-avoiding codes. *IEEE Trans. Inform. Theory*, 56(7):3265–3276, 2010.

[139] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.

[140] S. Špacapan. Nonexistence of face-to-face four-dimensional tilings in the Lee metric. *European J. Combin.*, 28(1):127–133, 2007.

[141] A. M. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.

[142] S. Stein. Factoring by subsets. *Pacific J. Math.*, 22:523–541, 1967.

[143] S. Stein. Packings of $\mathbf{R}^n$ by certain error spheres. *IEEE Trans. Inform. Theory*, 30(2, part 2):356–363, 1984.

[144] S. Stein and S. Szabó. *Algebra and tiling*, volume 25 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1994.

[145] M. Steinbach and D. Hachenberger. A class of quaternary linear codes improving known minimum distances. *Des. Codes Cryptogr.*, 78(3):615–627, 2016.

[146] J. E. Strapasson, G. C. Jorge, A. Campello, and S. I. R. Costa. Quasi-perfect codes in the l_p metric. *Comp. Appl. Math.* to appear. [Online]. Availabel: http://dx.doi.org/10.1007/s40314-016-0372-2.

[147] S. Szabó. Some problems on splittings of groups. *Aequationes Math.*, 30(1):70–79, 1986.

[148] S. Szabó. Some problems on splittings of groups. II. *Proc. Amer. Math. Soc.*, 101(4):585–591, 1987.

[149] S. Szabó and A. D. Sands. *Factoring groups into subsets*, volume 257 of *Lecture Notes in Pure and Applied Mathematics*. CRC Press, Boca Raton, FL, 2009.

[150] I. Trots, Y. Tasinkevych, A. Nowicki, and M. Lewandowski. Golay coded sequences in synthetic aperture imaging systems. *Arch. Acoust.*, 36(4):913–926, 2011.

[151] W. Ulrich. Non-binary error correction codes. *Bell Syst. Tech. J.*, 36:1341–1387, 1957.

[152] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, Cambridge, second edition, 2001.

[153] L. Wang and S. Zhu. New quantum MDS codes derived from constacyclic codes. *Quantum Inf. Process.*, 14(3):881–889, 2015.

[154] G. Weng, W. Qiu, Z. Wang, and Q. Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Des. Codes Cryptogr.*, 44(1-3):49–62, 2007.

[155] A. L. Whiteman. A family of difference sets. *Illinois J. Math.*, 6:107–121, 1962.

[156] A. J. Woldar. A reduction theorem on purely singular splittings of cyclic groups. *Proc. Amer. Math. Soc.*, 123(10):2955–2959, 1995.

[157] G. Wu, N. Li, T. Helleseth, and Y. Zhang. Some classes of complete permutation polynomials over $\mathbb{F}_q$. *Sci. China Math.*, 58(10):2081–2094, 2015.

[158] C. Xing and S. Ling. A class of linear codes with good parameters. *IEEE Trans. Inform. Theory*, 46(6):2184–2188, 2000.

[159] Y. Yang and W. Cai. On self-dual constacyclic codes over finite fields. *Des. Codes Cryptogr.*, pages 1–10, 2013.

[160] S. Yari, T. Kløve, and B. Bose. Some codes correcting unbalanced errors of limited magnitude for flash memories. *IEEE Trans. Inform. Theory*, 59(11):7278–7287, 2013.

[161] G. Zauner. Quantum designs: foundations of a noncommutative design theory. *Int. J. Quantum Inf.*, 9(1):445–507, 2011.

[162] G. Zhang and B. Chen. New quantum MDS codes. *Int. J. Quantum Inf.*, 12(4):1450019, 10, 2014.

[163] T. Zhang and G. Ge. Some new classes of quantum MDS codes from constacyclic codes. *IEEE Trans. Inform. Theory*, 61(9):5224–5228, 2015.

[164] Y. Zhou. $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations. *J. Combin. Designs.*, 21(12):563–584, 2013.

作者简历

- 张韬，男，浙江大学数学科学学院博士生，导师：葛根年.
- 通信地址：中国浙江省杭州市浙江大学玉泉校区数学科学学院，310027.
- 联系方式：(+86)13240948312，zhant220@163.com
- 教育经历：

  2004.9–2008.6，苏州大学数学科学学院，数学与应用数学（基地），理学学士.

  2012.9–今，浙江大学数学科学学院，应用数学专业，理学博士，研究方向：组合数学与编码密码学.
- 研究兴趣：代数组合学，组合设计，编码理论.

攻读博士学位期间主要研究成果

1. Baokun Ding, Gennian Ge, Jun Zhang, Tao Zhang and Yiwei Zhang, "New constructions of MDS symbol-pair codes", *Designs, Codes and Cryptography*, to appear. DOI: 10.1007/s10623-017-0365-1.

2. Tao Zhang and Gennian Ge, "Combinatorial constructions of packings in Grassmannian spaces", *Designs, Codes and Cryptography*, to appear. DOI: 10.1007/s10623-017-0362-4.

3. Tao Zhang, Xiande Zhang and Gennian Ge, "Splitter sets and k-radius sequences", *IEEE Transactions on Information Theory*, to appear. DOI: 10.1109/TIT.2017.2695219.

4. Tao Zhang and Gennian Ge, "Perfect and quasi-perfect codes under the l_p metric", *IEEE Transactions on Information Theory*, to appear. DOI: 10.1109/TIT.2017.2685424.

5. Jingxue Ma, Tao Zhang, Tao Feng and Gennian Ge, "Some new results on permutation polynomials over finite fields", *Designs, Codes and Cryptography*, vol. 83, no. 2, pp. 425–443, 2017.

6. Tao Zhang and Gennian Ge, "Quantum MDS codes with large minimum distance", *Designs, Codes and Cryptography*, vol. 83, no. 3, pp. 503–517, 2017.

7. Yiwei Zhang, Tao Zhang, Xin Wang and Gennian Ge, "Invertible binary matrix with maximum number of 2-by-2 invertible submatrices", *Discrete Mathematics*, vol. 340, no. 2, pp. 201–208, Feb. 2017.

8. Tao Zhang and Gennian Ge, "Quantum codes derived from certain classes of polynomials", *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6638–6643, Nov. 2016.

9. Tao Zhang and Gennian Ge, "New results on codes correcting single error of limited magnitude for flash memory", *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4494–4500, Aug. 2016.

10. Tao Zhang, Jerod Michel, Tao Feng, and Gennian Ge, "On the existence of certain optimal self-dual codes with lengths between 74 and 116", *The Electronic Journal of Combinatorics*, vol. 22, no. 4, P4.33, Nov. 2015.

11. Tao Zhang and Gennian Ge, "Some new classes of quantum MDS codes from constacyclic codes", *IEEE Transactions on Information Theory*, vol. 61, no. 9, pp. 5224–5228, Sept. 2015.

12. Tao Zhang and Gennian Ge, "Fourth power residue double circulant self-dual codes", *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4243–4252, Aug. 2015.

13. Sihuang Hu, Shuxing Li, Tao Zhang, Tao Feng, and Gennian Ge, "New pseudo-planar binomials in characteristic two and related schemes", *Designs, Codes and Cryptography*, vol. 76, no. 2, pp. 345–360, 2015.

14. Tao Zhang, Shuxing Li, Tao Feng, and Gennian Ge, "Some new results on the cross correlation of m-sequences", *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 3062–3068, May 2014.

15. Tao Zhang and Gennian Ge, "On (mn, n, mn, m) relative difference sets with $\gcd(m, n) = 1$", submitted.

16. Baokun Ding, Tao Zhang and Gennian Ge, "Maximum distance separable codes for b-symbol read channels", submitted.

17. Tao Zhang and Gennian Ge, "On the nonexistence of perfect splitter sets", submitted.

18. Tao Zhang and Gennian Ge, "Constructions of constant dimension codes", in manuscript.