分类号：O157.2　　单位代码：10335

密　级：　　学　　号：11006057

浙江大学

博士学位论文

中文论文题目：组合构型、指数和及其在信号处理、编码设计中的应用

英文论文题目：**Combinatorial Configurations, Exponential Sums and Their Applications in Signal Processing and the Design of Codes**

申请人姓名：李抒行

指导教师：葛根年　教授

合作导师：

专业名称：应用数学

研究方向：代数编码、组合设计与代数组合

所在学院：数学科学学院

论文提交日期：二〇一六年四月

组合构型、指数和及其在信号处理、编码设计中的应用

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：冯克勤\教授\清华大学

委员 1：冯克勤\教授\清华大学

委员 2：宗传明\教授\北京大学

委员 3：林东岱\研究员\中科院信息工程研究所

委员 4：胡磊\研究员\中科院信息工程研究所

委员 5：葛根年\教授\浙江大学

委员 6：_____

答辩日期：二〇一六年五月

致　谢

首先感谢我的导师葛根年教授。葛老师的悉心关怀和指导一直激励着我不断努力。葛老师的耐心教导使我从一个新手开始慢慢体会到应该如何做研究。对我的研究工作，葛老师一直从多方面予以大力的支持。他的言传身教更是令我受益匪浅。

其次感谢冯涛博士对我无微不至的关怀、鼓励和指导。冯老师带领我进入了代数编码和代数组合的领域。他在我身上花费了大量的时间，带我走过了从一无所知到略窥门径的艰难的日子。

感谢香港科技大学的丁存生教授和熊茂胜教授。他们慷慨资助了我在香港科技大学的访问。在香港期间同他们展开了愉快的合作, 获益良多。特别感谢丁老师不辞辛劳为我撰写了若干推荐信。

感谢特拉华大学的向青教授。向老师在访问浙大期间带来的讲座让我第一次感受到代数设计领域的魅力。

感谢清华大学的冯克勤教授帮我撰写推荐信。冯老师的学识修养令人钦佩。

感谢我的同门张会、高斐、朱明志、胡思煌、魏恒嘉、林浩、张一炜、上官冲、汪馨、张韬、顾玉杰、丁报昆、马景学，特别是胡思煌、魏恒嘉、林浩、张一炜、上官冲对我的帮助、鼓励和照顾。感谢马景学、丁报昆、钱昺辰、李伟聪在我不在杭州期间帮助处理各种杂事。

感谢我的亲人。

感谢所有帮助我的人。

摘 要

这篇论文考虑了代数编码, 组合设计和代数组合领域的若干理论问题. 同时, 也考虑了包括数字通信, 信号处理和数据存储等实际应用中提出的若干基础性问题. 本文的主旨在于利用包括代数数论, 特征理论, 指数和及代数函数域在内的多种数学工具, 去考察这些理论和实际问题.

在第 2 章, 我们考虑压缩传感矩阵的确定性构造. 由 Candès, Donoho 和 Tao 首倡, 压缩传感的理论已成为信号处理领域过去十年来最重大的进展. 压缩传感的一个核心问题是传感矩阵的构造. 注意到低相关值的矩阵给出性能良好的传感矩阵, 我们从编码理论, 组合设计和其它组合构型的角度出发, 构造了许多确定性传感矩阵的无穷类. 这些工作给出了基于相关值的最优或近似最优的传感矩阵.

在代数编码和序列设计领域, 许多问题可归结为某些指数和及其值分布的计算. 尽管这些计算总的来说是非常困难的, 在第 3 章, 我们通过引入新的思想取得了新的进展. 具体来讲, 我们得到了一类 Niho 指数的循环码的重量分布. 我们计算了一个 m-序列和它的特定的采样序列的互相关分布. 我们得到一类有任意多个非零点的循环码的重量分层.

在第 4 章, 我们考虑一些组合设计的构造. 划分式差族是很多最优构型背后的组合结构. 我们提出一个组合的递归构造, 统一了若干利用广义分圆的代数构造. 我们的新构造为推广已有构造和生成新的划分式差族的无穷类提供了很大的灵活性. 可分组设计是组合设计理论的基本内容. 由于缺乏合适的代数和几何结构, 型不一致的可分组设计的构造是一个非常具有挑战性的问题. 我们提出了一个新的构造, 得到了型不一致可分组设计的若干新的无穷类.

在第 5 章, 我们考虑循环码的理论和应用. 作为实际中广泛使用的循环码, BCH 码是最重要的纠错码之一. 注意到关于 BCH 码的经典结果绝大部分考虑的是本原的 BCH 码, 我们首次系统研究了非本原的 BCH 码. 我们确定了几类非本原 BCH 码的参数. 作为量子信息处理的基础, 量子码可由经典的纠错码导出. 我们用伪循环码构造了量子极大距离可分码, 统一了许多之前的构造且得到了新的无穷类. 字符结对码是用来纠正字符对读取信道中错误的一种新的编码方案. 利用循环码和拟循环码, 我们构

造了三类极小结对距离为五或六的极大距离可分字符结对码. 此外, 我们提出一个算法, 得到了许多极小结对距离为七的极大距离可分字符结对码.

一个代数编码和两个代数组合领域的问题被收录在附录中. 值得一提地, 即使直接的计算看起来是不可能的, 我们仍得出了一类有任意多个非零点的循环码的重量分布. 我们通过建立特定的指数和与一类图的谱之间令人惊讶的联系做到了这一点. 此外, 我们在一个有关差集的经典问题和一个有关伪平面函数的新兴问题上取得了进展. 前一个问题研究了不具有特征整除性质的差集, 这是 Jungnickel 和 Schmidt 在 1997 年提出的公开问题. 我们得到了不具备特征整除性质的差集的一些必要条件. 后一个问题涉及与有限射影平面相关的一个新概念. 这个工作丰富了伪平面函数的已知结果并建立了伪平面函数和结合方案之间的一个联系.

关键词： BCH 码, 压缩传感矩阵, 循环码, 差集, 指数和, 广义汉明重量, 可分组设计, 划分式差族, 伪平面函数, 量子码, 字符结对码, 重量分布, 重量分层

Abstract

This thesis concerns various theoretical problems in the area of algebraic coding theory, combinatorial design theory and algebraic combinatorics. Meanwhile, it concerns some fundamental problems arising from many practical applications such as digital communication, signal processing and data storage. The substance is to investigate these problems by employing various mathematical tools, including algebraic number theory, character theory, exponential sums and the theory of algebraic function fields.

In Chapter 2, we consider the deterministic constructions of compressed sensing matrices. Initiated by Candès, Donoho and Tao, the theory of compressed sensing has seen the most significant progress in the area of signal processing in the last decade. A central problem in compressed sensing is the construction of sensing matrices. Noticing that matrices with small coherence values give rise to favorable sensing matrices, we succeed in constructing many infinite families of deterministic sensing matrices, from the viewpoints of coding theory, combinatorial design theory and other combinatorial configurations. These works present many optimal or near optimal coherence-based constructions of sensing matrices.

In the area of algebraic coding theory and sequence design, many problems can be reduced to the computation of certain exponential sums and their value distributions. Although these computations are very difficult in general, in Chapter 3, we make some progress by introducing fresh ideas to deal with exponential sums. More specifically, we obtain the weight distribution of a class of cyclic codes with Niho exponent. We compute the cross-correlation distribution of an m-sequence and its certain decimated sequence. We obtain the weight hierarchy of a class of cyclic codes with arbitrarily many nonzeroes.

In Chapter 4, we consider the construction of some combinatorial designs. Partitioned difference families are the underlying structures of many optimal configurations. We present a combinatorial recursive construction to unify several algebraic constructions that employ generalized cyclotomy. Our new construction provides much flexibility for generalizing the

existing constructions and for producing new series of partitioned difference families. Group divisible designs are a fundamental building block in combinatorial design theory. The construction of nonuniform group divisible designs is a very challenging problem since no proper algebraic or geometric structures are available. We present a new construction to generate several new classes of nonuniform group divisible designs.

In Chapter 5, we consider the theory of cyclic codes and its applications. As widely-used cyclic codes in practical applications, the Bose-Chaudhuri-Hocquenghem (BCH) codes are one of the most important error-correcting codes. While classical results mainly concern the primitive BCH codes, we start the first systematic study of non-primitive BCH codes. We determine the fundamental parameters for several classes of non-primitive BCH codes. Quantum codes, which are a foundation of quantum information processing, can be derived from classical error-correcting codes. We use pseudo-cyclic codes to construct quantum maximum distance separable codes, which unifies many previous constructions and produces new classes of such codes. The symbol-pair code is a new coding framework which is proposed to correct errors in the symbol-pair read channel. Employing cyclic and constacyclic codes, we construct three new classes of maximum distance separable symbol-pair codes with minimum pair-distance five or six. Moreover, we propose an algorithm which produces many maximum distance separable symbol-pair codes with minimum pair-distance seven.

The appendix involves one problem in the area of algebraic coding theory and two problems in the area of algebraic combinatorics. Remarkably, we obtain the weight distributions of a class of cyclic codes with arbitrarily many nonzeroes, even though direct computation seems hopeless. We achieve this by establishing an unexpected and beautiful connection between the exponential sums concerned and the spectra of graphs. In addition, we make progress in a classical problem related to difference sets and an emerging problem concerning pseudo-planar functions. The former problem studies difference sets that do not possess the character divisibility property, as proposed by Jungnickel and Schmidt in 1997. We provide some necessary conditions for the possible candidates lacking the character divisibility property. The latter problem concerns a new concept related to finite projective planes. This work enriches the known constructions of pseudo-planar functions and builds a connection between pseudo-planar functions and association schemes.

Keywords: **BCH code, compressed sensing matrix, cyclic code, difference set, exponential sum, generalized Hamming weight, group divisible design, partitioned difference family, pseudo-planar function, quantum code, symbol-pair code, weight distribution, weight hierarchy**

目 次

图 目 录

表 目 录

1 绪论

1.1 确定性传感矩阵的构造

给定一个信号 $x \in \mathbb{R}^n$ 和一个传感矩阵 $A \in \mathbb{R}^{m\times n}$, 采样的过程即是取乘积 $y = Ax$, 其中 $y \in \mathbb{R}^m$ 是测量到的向量. 信号处理中一个根本性的问题是从 y 中可靠地恢复 x, 并且希望测量次数 m 尽可能小. 一个信号 x 被称为是稀疏的如果 x 只含有少量非零分量. 压缩传感的理论保证, 只要传感矩阵 A 满足限制等距性质, 任何稀疏信号 x 可以被可靠和高效地恢复出来, 即使 m 远小于 n[41,99]. 因此, 构造满足限制等距性质的传感矩阵成为压缩传感的一个中心问题.

一个矩阵 A 有列 $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$, 它的相关值定义为

$$\mu(A) = \max_{1\le i<j\le n} \frac{|\langle \mathbf{a}_i, \mathbf{a}_j\rangle|}{||\mathbf{a}_i||_2 \cdot ||\mathbf{a}_j||_2},$$

其中 $\langle\cdot,\cdot\rangle$ 是通常的内积且 $||\cdot||_2$ 是2-范数. 绝大多数确定性构造着眼于生成相关值较小的矩阵, 从而满足限制等距性质.

在基于相关值的传感矩阵的构造方面, 我们的贡献在于建立了传感矩阵和其它许多构型的联系. 首先, 注意到 DeVore[76] 的构造本质上利用了 Reed-Solomon 码, 而 Reed-Solomon 码是一种特殊的代数几何码. 基于这个联系, 我们利用更一般的代数几何码生成了传感矩阵的无穷类, 我们得到的矩阵优于DeVore 的矩阵. 这部分工作已经发表在《IEEE Transactions on Information Theory》.

其次, 我们注意到 Steiner 系的关联矩阵是潜在的传感矩阵. 特别地, 所需要的 Steiner 系可由有限几何导出. 通过建立有限几何和传感矩阵的联系, 我们得到了一系列新的传感矩阵. 这部分工作已经发表在《IEEE Transactions on Signal Processing》.

最后, 注意到低相关值的实矩阵和复矩阵事实上在包括序列设计和量子信息处理等多个领域都有过研究. 许多达到或近似达到著名的 Welch 界或 Levenstein 界的构造已经知道. 这些矩阵是最优或近似最优的基于相关值的传感矩阵. 我们给出了一个全面的综述总结了这些已知的构造并强调了它们在压缩传感中的重要性. 这部分工作已经发表在《IEEE Transactions on Information Theory》.

1.2 指数和及其值分布在代数编码中的应用

指数和及其值分布的计算是许多源于编码理论和序列设计的问题背后的核心数学问题. 这个问题总的来讲是非常困难的, 只能期待在某些特殊的情形下得到确切的值和值分布.

循环码是一类具有良好代数性质的线性码. 循环码拥有高效的编码与译码算法, 已被广泛应用于通信与数据存储领域. 重量分布是编码理论中一个重要的研究课题. 我们考虑了 Niho 指数循环码的重量分布. 基于 Delsarte 定理, 确定重量分布可以转化为确定某些指数和的值分布. 同时, Niho 指数使得我们可以通过 Niho 定理建立这些指数和与某些方程的界的个数之间一个美妙的联系. 因此, 我们可以通过分析某些方程来确定指数和的值. 我们得到了两类二元的三重和四重循环码和一类非二元的四重循环码. 通过一些例子, 我们说明了这三类码中包含了最优的或具有已知最好参数的码. 这部分工作已经发表在《IEEE Transactions on Information Theory》.

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, 可以降低通信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[134]. 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[96] 和 Feng 等人[106] 的思想, 我们完全决定了互相关分布. 此外, 对周期为 $2^{2lm}-1$ 的二元 m-序列和采样 $d=\frac{2^{2lm}-1}{2^m+1}+2^s$, 其中 $l\geq 2$ 为偶数且 $0\leq s\leq 2m-1$, 我们证明了对这个采样互相关值至少取四个值. 虽然确定互相关分布看起来非常困难, 我们验证了由 Sarwate 等人[240] 和 Helleseth[130] 提出的两个著名猜想的正确性. 这部分工作已经发表在《IEEE Transactions on Information Theory》.

广义汉明重量是线性码的基本参数. 广义汉明重量包含了线性码的结构信息并在很多应用中刻画了线性码的表现. 然而, 线性码的广义汉明重量的计算一般而言是困难的. 在最近的一篇有趣的文章中[297], 作者利用数论方面的新想法研究了不可约循环码的广义汉明重量且在某些情况下得到了重量分层. 受此启发, 我们考察了文献[295] 中引入的一族可约循环码的广义汉明重量. 这类循环码有任意多个非零点, 包含许多之前文献中研究过的循环码作为其中的子类. 特别地, 它包含文献[297] 研究的不可约循环码. 通过将文献[297] 中的思想拓展到高维并利用一些组合的技巧, 我们在

一些情况下确定了这类循环码的重量分层. 这部分工作已投稿至《IEEE Transactions on Information Theory》.

Delsarte 定理[72] 给出了循环码的一个迹表示. 研究循环码的重量分布, 往往从这个迹表示出发, 利用指数和的工具加以分析. 然而, 当循环码有较多个非零点时, 它的迹表示变得非常复杂, 以上方法就失效了. 因此, 关于具有多个非零点的循环码的重量分布的结果极其稀少. 为了求得有多个非零点的循环码的重量分布, 必须要引入新的思想和方法. 通过建立一类具有任意多个非零点的循环码的重量分布, 和 Hermitian 型图的谱之间意外的联系，我们求出了这类循环码的重量分布. 这个出人意料的突破展现了循环码的重量分布与图的谱理论, 以结合方案为核心的代数组合理论之间美妙的联系. 这部分工作已经发表在《IEEE Transactions on Information Theory》.

1.3 组合设计的构造

划分式差族在文献[85] 中被明确引入, 用以构造最优的常重复合码. 它在多种离散构型的构造中发挥了重要作用, 包括最优常重码[278,309], 最优常重复合码[33,80,84,303,309], 最优跳频序列[82,86,117,278] 和最优集合差系[33,81,84,279,303,309]. 最近, 划分式差族在零差平衡函数 (zero-difference balanced functions) 的名义下受到了集中的研究[33,80,83,84,278,303,309]. 我们从组合的角度考察了划分式差族的构造. 我们引入一个划分式相对差族的概念, 作为我们构造的核心. 我们提出了划分式差族的两个一般的递归构造. 这些构造为之前从分圆导出了几个无穷类提供了一个简单的解释. 此外, 我们得到了若干类新的划分式差族. 这些划分式差族可以导出最优的常重复合码. 这部分工作已被《Designs, Codes and Cryptography》录用.

自从 Wilson 基本构造法提出以来[284], 可分组设计在其它组合构型的构造中起到了重要的作用. 此外, 可分组设计在编码领域也有很多重要的应用. 因此, 可分组设计的构造是组合设计领域的一个中心问题. 特别地, 由于缺乏合适的代数和几何结构, 型不一致可分组设计的构造是一个非常具有挑战性的问题. 我们提出一个构造型如 $g^k m^1$ 的 $\{k\}$-可分组设计的新方法, 其中广义差集, 一个截断技巧和一个差方法起到了关键作用. 利用这个一般构造, 导出了型不一致的可分组设计的若干新的无穷类和许多新例子. 这部分工作已被《Journal of Combinatorial Designs》录用.

1.4 循环码及其应用

作为实际中广泛使用的循环码, BCH 码是最重要的纠错码之一. 已知的关于 BCH 码的结果几乎都考虑本原的长度 $n = q^m - 1$. 据我们所知, 文献中只有很少的文章考虑了非本原长度的 BCH 码. 这是因为处理非本原长度的 BCH 码更加困难. 我们开启了对长为 $n = (q^m - 1)/(q - 1)$ 的狭义射影 BCH 码的研究, 确定了一些大维数狭义射影 BCH 码的参数, 确定了一些三元小维数狭义射影 BCH 码的参数和重量分布, 确定了有某些特殊设计距离的狭义射影 BCH 码的参数. 如许多例子所示, 狭义射影 BCH 码包含了很多最优的线性码. 这为我们提供了强大的动力去进一步研究狭义射影 BCH 码. 这部分工作已投稿至《IEEE Transactions on Information Theory》.

量子纠错码在量子计算和量子通信中有重要作用. 量子极大距离可分码是一类最优的量子码, 它的构造在近年来受到了很大的关注. 构造新的量子极大距离可分码的一个非常有效的办法是利用拟循环码. 作为拟循环码的自然推广, 伪循环码已在文献[228]的 8.10 节中被研究过. 我们利用伪循环码统一了之前的许多利用拟循环码的构造并得到了新的量子极大距离可分码. 相比之下, 伪循环码为构造提供了更多的灵活性，使得我们对这些新的构造有了更好的理解. 这部分工作已经发表在《IEEE Transactions on Information Theory》.

受高密度存储的应用所启发,一个被称为字符结对码的新的编码框架被提出[43,44], 用来纠正字符对读取信道中发生的错误. 借鉴文献[166] 中的思想, 我们利用循环和拟循环吗构造了极小结对距离 $d_p \in \{5, 6\}$ 的极大距离可分字符结对码的若干无穷类. 我们的构造推广了文献[166] 中的结果. 此外, 我们得到了保证一类循环码成为极大距离可分字符结对码的充要条件. 这个条件和一类特殊的分式线性变换的性质有关. 我们仔细研究了这一类特殊的分式线性变换, 提出了对以上充要条件的一个更精确的刻画. 由这个刻画得到了一个 $d_p = 7$ 的极大距离可分字符结对码的构造算法. 这部分工作已投稿至《Designs, Codes and Cryptography》.

1.5 代数组合

给定群 G 中的一个 (v, k, λ) 差集 D, D 的阶定义为 $n = k - \lambda$. 我们称 D 满足特征整除性质 (character divisibility property), 如果对 G 的任意一个非平凡特征 χ, 均

有 $\sqrt{n} \mid \chi(D)$. 注意到所有满足 $\gcd(v,n) > 1$ 的差集都具有这个性质, Jungnickel 和 Schmidt 在 1997 年提出了以下的公开问题[163]:

问题： 构造 $\gcd(v,n) > 1$ 的不具有特征整除性质的差集.

近二十年来, 关于这个问题的进展非常缓慢. 我们以有三个非平凡特征值的差集为候选, 得出了这类差集不具有特征整除性质的一些必要条件, 为推进这个问题做出了初步的探索. 这部分工作已经发表在《Designs, Codes and Cryptography》.

平面函数是出现在许多不同数学分支的不同对象的一个精炼的表示. 它与差集, 半域和有限几何都有着密切的联系. 此外, 平面函数在编码和密码领域的许多应用已被发掘出来. 特别地, 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 在偶特征的有限域上提出了伪平面函数 (pseudo-planar function) 的概念[306], 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, 这推广了 Bonnecaze 和 Duursma 的一个结果[23]. 这部分工作已经发表在《Designs, Codes and Cryptography》.

2 确定性传感矩阵的构造

2.1 压缩传感的背景

压缩传感 (Compressed sensing) 是一种利用信号的稀疏性或可压缩性的一种新的数据采样理论. 它指出了一个稀疏的或可压缩的信号可以通过与传统采样理论相比少得多的采样次数恢复出来[39,99]. 我们可将压缩传感视为一个两阶段的方案. 首先, 一个稀疏或近似稀疏的信号可通过非适定的线性投射加以采样. 这个过程集合了采样和压缩的过程. 其次, 信号可通过求解一个优化问题恢复出来.

考虑一个时间离散的信号 $x \in \mathbb{R}^n$, 我们在采样过程中使用 m 次测量. 用矩阵的符号,

$$y = \Phi x + e,$$

其中 Φ 是一个 $m \times n$ 的*传感矩阵* (Sensing matrix) 满足 $m < n$ 且 e 是一个未知的噪声项. 当 $m < n$, 这个问题通常是没有意义的. 然而, Donoho[99] 和 Candès 等人[39] 开创性的工作充分利用了信号的稀疏性, 使得一个稀疏信号可通过非常少的测量次数恢复出来. 这个问题被描述为求解线性方程 $y = \Phi x$ 最稀疏的解:

$$\min_{x \in \mathbb{R}^n} \|x\|_0 \quad \text{满足} \Phi x = y. \tag{2.1}$$

这个 ℓ_0-优化是一个组合优化问题, 总的来说是 NP-难的[214]. 然而, 压缩传感提出了一个强有力的方法, 在测量次数 $m \ll n$ 的情况下, 仍然可以通过有效的算法恢复稀疏信号.

一个信号 x 被称为 k-*稀疏* (k-sparse) 如果 x 有至多 k 个非零分量. 选择一个 $m \times n$ 随机高斯矩阵 (Gaussian matrix) Φ, 它的元素服从相互独立的高斯分布, 作为传感矩阵. 考虑 (2.1) 的一个凸松弛. 如果 $m \geq Ck \log(n/m)$, 其中 C 是一个常数, 我们可以通过 ℓ_1-优化:

$$\min_{x \in \mathbb{R}^n} \|x\|_1 \quad \text{满足} \Phi x = y \tag{2.2}$$

以很高的概率精确的恢复 x[41]. 事实上, 当 x 是稀疏或近似稀疏时, 压缩传感理论表明, 利用一个合适的传感矩阵 Φ, y 实质上包含了足够的信息去恢复 x, 即使 $m \ll n$.

为了确定什么样的矩阵是合适的, 我们需要一些准则. 限制等距性质 (Restricted isometry property) 是一个熟知的准则[40]. 一个矩阵 Φ 满足 k 阶限制等距性质, 如果存在一个常数 $0 \leq \delta_k < 1$, 使得

$$(1-\delta_k)\|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1+\delta_k)\|x\|_2^2 \tag{2.3}$$

对任意 k-稀疏信号 x 成立. 最小的使得 (2.3) 对每个 k-稀疏信号成立的常数 δ_k 被称为 k 阶限制等距常数 (Restricted isometry constant). 限制等距性质是一个保证稀疏或近似稀疏的信号可由 ℓ_1-优化恢复的充分条件[38]. 如果一个传感矩阵满足限制等距性质且它的限制等距常数足够小, 例如迭代阈值 (Iterative Thresholding)[22,108], 正交匹配追踪 (Orthogonal Matching Pursuit)[199,260] 和它的各种改进算法[70,215,216] 可确保恢复稀疏或近似稀疏的信号. 总之, 选取合适的传感矩阵, 我们可将稀疏或近似稀疏的信号的恢复归结为存在有效算法的优化问题.

传感矩阵的构造是压缩传感的一个中心问题. 假设一个 k-稀疏信号 $x \in \mathbb{R}^n$ 可以稳定地从 m 次测量中恢复. 稀疏度的一个上界是

$$k \leq Cm/\log(n/k),$$

其中 C 是一个常数[62]. 达到这个上界的随机矩阵已被研究过[41], 保证能以很大概率恢复稀疏信号. 事实上, 如果一个随机矩阵的元素均服从某些概率分布, 那么这个矩阵以很高的概率满足 k 阶限制等距性质, 其中 $k \leq Cm/\log(n/k)$ 对某个常数 C[12]. 尽管随机矩阵是很好的候选, 有一些理由使得我们更青睐确定性的传感矩阵. 首先, 尚无有效的算法测试一个随机矩阵满足限制等距性质, 即使它确实以很高的概率满足. 其次, 当信号长度很长时, 随机矩阵要求很多的存储空间. 与随机矩阵相比, 确定性矩阵可以克服这些缺陷. 确定性矩阵的限制等距性质由它们的构造所保证. 利用确定性矩阵的结构, 可以用更加节省空间的方式存储矩阵. 此外, 确定性矩阵的结构有利于设计快速的恢复算法, 这在实时的应用中至关重要. 因此, 我们专注于确定性传感矩阵的构造.

对一个矩阵 A, 它的列为 $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$, A 的相关值 (coherence) 定义为

$$\mu(A) = \max_{i \neq j} \frac{|\langle \mathbf{a}_i, \mathbf{a}_j \rangle|}{\|\mathbf{a}_i\|_2 \cdot \|\mathbf{a}_j\|_2}, \quad \text{对} 1 \leq i, j \leq n.$$

相关值在确定性构造中起到了核心的作用, 因为低相关矩阵满足限制等距性质.

引理 2.1 (命题 1[27]): *Φ 是一个相关值为 μ 的矩阵. 那么 Φ 满足 k 阶限制等距性质, 其中 $\delta_k \leq \mu(k-1)$, 如果 $k < 1/\mu + 1$.*

引理 2.1 说明低相关矩阵是传感矩阵的自然候选. 另一方面, 对一个 $m \times n$ 矩阵 Φ, 我们有著名的 Welch 界[283]:

$$\mu(\Phi) \geq \sqrt{\frac{n-m}{m(n-1)}}. \tag{2.4}$$

这个界蕴含了基于相关值的确定性构造只能得到满足 k 阶限制等距性质的传感矩阵, 其中 $k = O(m^{\frac{1}{2}})$.

近年来, 利用限制等距性质作为准则的若干确定性构造已被提出. 他们中绝大部分基于相关值. DeVore 利用有限域 $\mathbb{F}_p$ 上的多项式构造了 $p^2 \times p^{r+1}$ 二元传感矩阵, 其中 p 是一个素数幂[76]. 这些矩阵的相关值为 r/p 且满足阶为 $k < p/r+1$ 的限制等距性质. 有很大的极小距离的 Bose-Chaudhuri-Hocquenghem (BCH) 码被用作构造相关值为 $\mu \leq (2^{l-j}-1)/(2^l-1)$ 且满足阶为 $k \leq 2^j + 1$ 的限制等距性质的 $(2^l-1) \times 2^{O(2^{(l-j)}\frac{\ln j}{j})}$ 矩阵[4]. 利用 p-元 BCH 码, 这个构造被推广到构造复数域上的矩阵[5], 得出了相关值为 $\mu \leq p(p^{l-r}-1)/(2(p-1)(p^l-1))$ 的 $(p^l-1) \times p^{\mathcal{O}(p^{(l-r)}\frac{\log_p r}{r})}$ 复矩阵. 加法组合的方法导出了 $m \times n$ 矩阵满足阶为 $k \geq m^{\frac{1}{2}+\epsilon}$ 的限制等距性质, 其中 $\epsilon > 0$ 且 $n^{1-\epsilon} \leq m \leq n$[27]. 值得一提的是, 这个构造克服了基于相关值的构造的 $k = O(m^{\frac{1}{2}})$ 的瓶颈.

另一方面, 一些不基于限制等距性质的确定性构造也被提出. chirp 序列被用作构造复传感矩阵且一个快速恢复算法被提出[6]. 注意到压缩传感和编码理论的联系, 实传感矩阵由二阶 Reed-Muller 码和它的子码构造出来[147]. Calderbank 等人[35] 总结了这两个构造, 证明这些传感矩阵满足*统计限制等距性质* (statistical RIP). 统计限制等距性质比限制等距性质要弱, 保证除了极少的例外, 能恢复所有的稀疏信号. 限制等距性质的一个被称为限制等距性质-1 (RIP-1) 的变形被提出[16]. 非平衡的扩展图 (unbalanced expanders), 作为有好的扩展性质的二部图, 生成满足限制等距性质-1 的矩

阵. 在文献[152] 中, hash 函数和提取图 (extractor graphs) 被用来构造二元传感矩阵. 一个利用 hash 族的递归构造已被提出[66].

2.2 利用代数曲线构造确定性压缩传感矩阵

2.2.1 引言

在本节中, 我们利用有限域上的代数曲线构造确定性压缩传感矩阵. 这个构造是 DeVore 构造[76] 的一个推广. 我们借鉴了由 Goppa[125] 提出的用有限域上的代数曲线构造线性码的思想. 这个思想已被充分地推广, 由代数曲线构造的码被称为*代数几何码* (Algebraic geometry code)[21,261,293]. 关于代数曲线和它们的函数域的知识[220,252] 为传感矩阵的构造提供了很大的灵活性. 通过选取合适的曲线, 我们得到了优于 DeVore 矩阵的二元传感矩阵.

2.2.2 背景知识

2.2.2.1 代数曲线的背景知识

关于代数曲线的基本符号, 我们遵循文献[293] 中的惯例. 令 $\mathbb{F}_q$ 为 q 阶的有限域, 其中 q 是一个素数幂. $\mathbb{F}_q$ 上一个绝对不可约曲线 $\mathcal{X}$ 被记做 $\mathcal{X}/\mathbb{F}_q$. $\mathcal{X}/\mathbb{F}_q$ 的亏格被记做 $g = g(\mathcal{X})$. $\mathcal{X}/\mathbb{F}_q$ 上一个 $\mathbb{F}_{q^r}$-有理点 P 是一个点 $P \in \mathcal{X}$, 它的元素均落在 $\mathbb{F}_{q^r}$ 中. 通常, 一个 $\mathbb{F}_q$-有理点被称为 $\mathcal{X}/\mathbb{F}_q$ 的一个*有理点* (rational point).

$\mathcal{X}$ 的一个*除子* (divisor) D 是一个形式和

$$D = \sum_{P \in \mathcal{X}} n_P P,$$

其中对每个 $P \in \mathcal{X}$, 系数 n_P 是一个整数且只有有限多个非零. 如果每个 n_P 是非负的, 我们称 D 为一个*有效* (effective) 除子并记 $D \geq 0$. D 的一个*支撑集* (support set) 是一个点 P 的集合满足 n_P 非零, 并记做 $\mathrm{supp}(D)$. D 的*次数* (degree) 定义做

$$\deg(D) = \sum_{P \in \mathcal{X}} n_P \deg(P).$$

注意到 $\deg(P) = 1$ 对每个有理点 $P \in \mathcal{X}$.

用 $\mathbb{F}_q(\mathcal{X})$ 记 $\mathcal{X}$ 的函数域. $\mathbb{F}_q(\mathcal{X})$ 的元素被称作函数 (function). 对一个函数 $x \in \mathbb{F}_q(\mathcal{X})$, x 的主除子 (principle divisor) 是

$$\text{div}(x) = \sum_{P \in \mathcal{X}} \nu_P(x) P,$$

其中 ν_P 对应于点 P 的正规离散赋值. 可以证明对每个函数 x 只有有限多个 $\nu_P(x)$ 非零. 赋值 $\nu_P(x) \geq 0$ 蕴含了 $x(P) \in \overline{\mathbb{F}}_q$, 其中 $\overline{\mathbb{F}}_q$ 是 $\mathbb{F}_q$ 的代数闭包. 此外, 如果 P 是一个有理点, $x(P) \in \mathbb{F}_q$.

给定 $\mathcal{X}/\mathbb{F}_q$ 的一个除子 G, Riemann-Roch 空间 (Riemann-Roch space) $\mathcal{L}(G)$ 定义为:

$$\mathcal{L}(G) = \{x \in \mathbb{F}_q(\mathcal{X}) \backslash \{0\} \mid \text{div}(x) + G \geq 0\} \cup \{0\}.$$

$\mathcal{L}(G)$ 是 $\mathbb{F}_q$ 上有限维向量空间且它的维数记做 $\ell(G)$. 由 Riemann-Roch 定理,

$$\ell(G) \geq \deg(G) - 1 + g$$

且等式成立如果 $\deg(G) \geq 2g - 1$.

2.2.2.2 代数几何码

我们回顾之前文献中对代数几何码的描述[252]. 令 $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 为 $\mathbb{F}_q$ 的一个子集. 令 $\mathcal{P}_k$ 为 $\mathbb{F}_q$ 上一个 k-维线性空间, 包含了 $\mathbb{F}_q$ 上次数不超过 $k-1$ 的多项式:

$$\mathcal{P}_k = \{f \in \mathbb{F}_q[x] \mid \deg f \leq k - 1\}.$$

定义一个赋值映射 $\phi : \mathcal{P}_k \to \mathbb{F}_q^n$ 为

$$\phi(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \in \mathbb{F}_q^n.$$

ϕ 的像是一个长度为 n, 维数为 k 的 $[n, k]$ 线性码:

$$\mathcal{C}_k = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f \in \mathcal{P}_k\}$$

被称为一个 RS 码 (Reed-Solomon code). 由于 $f \in \mathcal{P}_k$ 至多有 $k-1$ 个零点, 极小距离 $d \geq n+1-k$. 另一方面, 由 Singleton 界有 $d \leq n+1-k$. 因而 RS 码是 $\mathbb{F}_q$ 上的极大距离可分码, 满足 $d = n+1-k$.

代数几何码是 RS 码的一个自然推广. 对以上构造做出一些微小的改动即可得到代数几何码. 更确切地, 有限域里的元素被替换为一条代数曲线上的有理点, 向量空间 $\mathcal{P}_k$ 被替换为 Riemann-Roch 空间 $\mathcal{L}(G)$, 其中 G 是一个除子.

考虑一条亏格为 g 的代数曲线 $\mathcal{X}/\mathbb{F}_q$, 令 $P_1, P_2, \ldots, P_n$ 为$\mathcal{X}$ 的 n 个不同的有理点. 假设 G 是一个除子满足次数 $g \leq \deg(G) < n$ 且支撑集 $\mathrm{supp}(G) \cap \{P_1, P_2, \ldots, P_n\} = \emptyset$. 因而 $\nu_{P_i}(f) \geq 0$ 对任意 $f \in \mathcal{L}(G)$ 和 $1 \leq i \leq n$. 因此, $f(P_i) \in \mathbb{F}_q$ 对任意 $f \in \mathcal{L}(G)$ 且 $1 \leq i \leq n$. 定义一个赋值映射 $\psi : \mathcal{L}(G) \to \mathbb{F}_q^n$ 为

$$\psi(f) = (f(P_1), f(P_2), \ldots, f(P_n)) \in \mathbb{F}_q^n.$$

ψ 的像被记为 $C(P_1, P_2, \ldots, P_n; G)$, 被称作一个代数几何码 (Algebraic geometry code). 以下的定理给出了它的参数.

定理 2.1 (定理 3.1.1[261]): $C(P_1, P_2, \ldots, P_n; G)$ 是 $\mathbb{F}_q$ 上一个 $[n, k, d]$ 线性码, 满足

$$k \geq \deg(G) - g + 1, \quad d \geq n - \deg(G).$$

此外, 维数 k 等于 $\deg(G) - g + 1$ 如果 $\deg(G) \geq 2g - 1$.

2.2.3 主要结果

2.2.3.1 DeVore 构造的回顾

在文献[76] 中, DeVore 利用有限域上的多项式给出了传感矩阵的一个确定性构造. 为了方便, 我们仅考虑素数阶的有限域. 令 $\mathbb{F}_p$ 为一个有限域, 其中 p 是一个素数. 令 $\mathcal{P}_r$ 为 $\mathbb{F}_p$ 上次数不超过 r 的多项式的集合. $\mathcal{P}_r$ 包含 p^{r+1} 个多项式.

将 $\mathbb{F}_p \times \mathbb{F}_p$ 的元素按照字典序排为 $(0,0), (0,1), \ldots, (p-1, p-1)$. 对任意 $f \in \mathcal{P}_r$, 定义一个列向量 v_f, 它的行由 $\mathbb{F}_p \times \mathbb{F}_p$ 的元素标记. 二元向量 v_f 形如

$$(f_{0,0}, \ldots, f_{0,p-1}, f_{1,0}, \ldots, f_{1,p-1}, \ldots, f_{p-1,0}, \ldots, f_{p-1,p-1})^T,$$

其中

$$f_{i,j} = \begin{cases} 1, & \text{如果 } f(i) = j \\ 0, & \text{其它} \end{cases}$$

对 $0 \le i \le p-1$ 和 $0 \le j \le p-1$. 因此, 对任意 $f \in \mathcal{P}_r$, v_f 是一个恰包含 p 个 1 的二元向量. 事实上, f 可被视为一个从 $\mathbb{F}_p$ 到 $\mathbb{F}_p$ 的映射. v_f 以二元向量的形式记录了映射 f 的像. 列向量 $\{v_f \mid f \in \mathcal{P}_r\}$ 组成了一个 $p^2 \times p^{r+1}$ 矩阵 Φ_0.

定理 2.2 (定理 3.1[76]): 假设 $\Phi = \frac{1}{\sqrt{p}}\Phi_0$, 那么 Φ 是一个传感矩阵, 相关值 $\mu(\Phi) \le r/p$.

注意到这个方法可被应用于任何有限域 $\mathbb{F}_q$, 其中 q 是一个素数幂. 在这个构造中, 每个多项式给出传感矩阵的一列. 回顾每个多项式给出 RS 码的一个码字. 这个类似暗示了传感矩阵的一种新的构造, 因为 RS 码已被推广为代数几何码. 以下, 我们给出利用有限域上代数曲线的构造.

2.2.3.2 主要构造

假设 q 是一个素数幂且 $\mathcal{X}$ 是 $\mathbb{F}_q$ 上一条代数曲线. 令 $\mathcal{P}$ 为 $\mathcal{X}/\mathbb{F}_q$ 上的有理点组成的集合. 选取 $\mathcal{X}$ 的一个除子 G 满足 $\deg(G) < |\mathcal{P}|$ 且$\text{supp}(G) \cap \mathcal{P} = \emptyset$. Riemann-Roch 空间 $\mathcal{L}(G)$ 是 $\mathbb{F}_q$ 上一个线性空间, 维数为 $\ell(G)$. 由于 $\text{supp}(G) \cap \mathcal{P} = \emptyset$, 我们有 $f(P) \in \mathbb{F}_q$ 对任意 $P \in \mathcal{P}$ 和 $f \in \mathcal{L}(G)$. 函数 f 可用一个二元列向量 v_f 表示, 它的分量由 $\mathcal{P} \times \mathbb{F}_q$ 中的元素标记. 假设由 $(P, a) \in \mathcal{P} \times \mathbb{F}_q$ 标记的分量记做 $f_{P,a}$, 那我们取

$$f_{P,a} = \begin{cases} 1, & \text{如果 } f(P) = a \\ 0, & \text{其它.} \end{cases}$$

注意到对每个 $f \in \mathcal{L}(G)$, 恰好有 $|\mathcal{P}|$ 个 1 在 v_f 中.

令 $m = |\mathcal{P}| \times q$ 且 $n = q^{\ell(G)}$. 列向量 $\{v_f \mid f \in \mathcal{L}(G)\}$ 形成一个 $m \times n$ 矩阵 Φ_0. 我们有以下的定理.

定理 2.3: 假设 $\Phi = \frac{1}{\sqrt{|\mathcal{P}|}}\Phi_0$, 那么 Φ 是一个传感矩阵, 相关值 $\mu(\Phi) \le \deg(G)/|\mathcal{P}|$.

证明. 对 $\mathcal{L}(G)$ 中任意两个不同的函数 f 和 g, $\frac{1}{\sqrt{|\mathcal{P}|}}v_f$ 和 $\frac{1}{\sqrt{|\mathcal{P}|}}v_g$ 是 Φ 的两个不同列.

假设 z 是 v_f 和 v_g 的内积. 注意到

$$z = |\{P \in \mathcal{P} : f(P) = g(P)\}| = |\{P \in \mathcal{P} : (f-g)(P) = 0\}|$$

. 对函数 $f-g$, 假设它在 $\mathcal{P}$ 中的 z 个不同零点为 $P_{i_1}, P_{i_2}, \ldots, P_{i_z}$. 我们有

$$0 \neq f - g \in \mathcal{L}(G - P_{i_1} - \cdots - P_{i_z}),$$

这蕴含了

$$0 \leq \deg(G - P_{i_1} - \cdots - P_{i_z}) = \deg(G) - z.$$

因此,

$$\frac{1}{\sqrt{|\mathcal{P}|}} v_f \cdot \frac{1}{\sqrt{|\mathcal{P}|}} v_g = \frac{z}{|\mathcal{P}|} \leq \frac{\deg(G)}{|\mathcal{P}|}.$$

所以, 相关值 $\mu(\Phi) \leq \deg(G)/|\mathcal{P}|$. □

注： 这个定理可被视为 DeVore 构造的推广. 如果代数曲线 $\mathcal{X}$ 选作 $\mathbb{F}_q$ 上的射影直线, 相应的函数域 $\mathbb{F}_q(\mathcal{X})$ 同构于有理函数域 $\mathbb{F}_q(x)$. $\mathcal{X}$ 包含 $q+1$ 个有理点, 其中有一个无穷远点 ∞ 和 q 个仿射点. 存在一个从 $\mathcal{X}$ 的仿射有理点到有限域 $\mathbb{F}_q$ 的元素的一一映射. 选取除子 $G = r\infty$, Riemann-Roch 空间 $\mathcal{L}(G) = \mathcal{L}(r\infty)$ 即是向量空间 $\mathcal{P}_r$. 在这种情况下, 我们得到了 DeVore 矩阵. 由于相关值的上界是 $\deg(G)/|\mathcal{P}|$, 当 $\deg(G)$ 给定时, 我们希望 $|\mathcal{P}|$ 越大越好. 因此选取有理点个数较多的曲线时, 可以期待得出由于 DeVore 构造的矩阵.

我们的构造需要的信息包括一条代数曲线上的有理点和某个除子的 Riemann-Roch 空间. 对代数曲线上的有理点, 包括 `Magma` 和 `Sage` 在内的软件提供了内置函数去计算它们. 同时, 对于 Riemann-Roch 空间的计算, 一个简单有效的算法已被提出[142]. 总之, 构造所需的信息不难得到, 构造的实现也是简单的.

2.2.4 例子

2.2.4.1 椭圆曲线

有限域上的椭圆曲线广为人知, 原因之一是基于椭圆曲线上的有理点的优美的

密码系统[182]. 对一条椭圆曲线 $\mathcal{X}/\mathbb{F}_q$, 记 $\mathcal{X}$ 上 $\mathbb{F}_{q^r}$-有理点的个数为 N_r. 由 Schoof 算法[243], N_1 可以被有效的计算出来. 此外, N_r 可由以下引理容易的计算出来.

引理 2.2 (定理 4.12[280]): 令 $N_1 = q + 1 - a$. 记 $X^2 - aX + q = (X - \alpha)(X - \beta)$. 那么 $N_r = q^r + 1 - (\alpha^r + \beta^r)$.

我们可用 $\mathcal{X}$ 上的 $\mathbb{F}_{q^r}$-有理点构造传感矩阵. 例如, 给定 $\mathbb{F}_2$ 上一条椭圆曲线 $\mathcal{X}$:

$$y^2 + y = x^3 + x, \tag{2.5}$$

亏格 $g = g(\mathcal{X}) = 1$. $\mathbb{F}_{2^r}$-有理点的个数 N_r 已被计算出[252]:

$$N_r = \begin{cases} 2^r + 1, & \text{当 } r \equiv 2, 6 \pmod 8 \\ 2^r + 1 + 2 \cdot 2^{r/2}, & \text{当 } r \equiv 4 \pmod 8 \\ 2^r + 1 - 2 \cdot 2^{r/2}, & \text{当 } r \equiv 0 \pmod 8 \\ 2^r + 1 + 2^{(r+1)/2}, & \text{当 } r \equiv 1, 7 \pmod 8 \\ 2^r + 1 - 2^{(r+1)/2}, & \text{当 } r \equiv 3, 5 \pmod 8. \end{cases}$$

令 ∞ 为无穷远处的有理点且 $\mathcal{P}$ 为 $\mathcal{X}$ 上余下的有理点的集合, 满足 $|\mathcal{P}| = N_r - 1$. 对整数 s 满足 $1 = 2g - 1 \leq s < N_r - 1$, 令 $G = s\infty$. 由定理 2.3, 我们有一个 $m_0 \times n_0$ 传感矩阵 Φ_0 满足

$$m_0 = 2^r \cdot (N_r - 1), \;\; n_0 = 2^{r\ell(G)} = 2^{rs}, \;\; \mu(\Phi_0) \leq s/(N_r - 1).$$

Φ_0 满足阶 $k_0 < (N_r - 1)/s + 1$ 的限制等距性质.

特别地, 如果 $r \equiv 4 \pmod 8$, 我们有一个 $m \times n$ 传感矩阵 Φ 满足

$$m = 2^r(2^r + 2^{\frac{r}{2}+1}), \quad n = 2^{rs}, \quad \mu(\Phi) \leq s/(2^r + 2^{\frac{r}{2}+1}),$$

其中 $1 \leq s < 2^r + 2^{\frac{r}{2}+1}$. Φ 满足阶 $k < (2^r + 2^{\frac{r}{2}+1})/s + 1$ 的限制等距性质. 注意到

$\log_2 m = \frac{3r}{2} + \log_2(2^{\frac{r}{2}} + 2) \approx 2r$ 且 $\log_2 n = rs$, Φ 可用来恢复稀疏度

$$k \leq \frac{(\sqrt{m} + 2\sqrt[4]{m}) \log m}{2 \log n}$$

的信号. 回顾 DeVore 构造[76] 给出的矩阵可恢复稀疏度

$$k \leq \frac{\sqrt{m} \log m}{2 \log(n/m)}$$

的信号. 给定测量次数 m, 当 n 充分大时, 我们的构造略微占优. 此外, 通过调整 r 和 s 的值, 我们可得到一批不同的传感矩阵.

现在我们通过数值实验比较由椭圆曲线得到的传感矩阵和随机高斯矩阵. 对一个信号 x, 我们利用正交匹配追踪求解 ℓ_0-优化 (2.1) 并将解记为 x^*. 定义 x 的恢复信噪比 (signal-to-noise ratio)[215] 为

$$\text{SNR}(x) = 10 \cdot \log_{10}\big(\frac{\|x\|_2}{\|x - x^*\|_2}\big)\text{dB}.$$

如果 SNR(x) 不低于 100 dB, 我们称 x 的恢复是完美的.

将椭圆曲线 (2.5) 写作射影形式:

$$y^2 z + y z^2 = x^3 + x z^2. \tag{2.6}$$

令 $r = 2$, (2.6) 的所有 $\mathbb{F}_4$-有理点为

$$\{[0,0,1], [0,1,1], [1,0,1], [1,1,1]\}$$

且无穷 $\mathbb{F}_4$-有理点 ∞ 为 $[0,1,0]$. 假设 $s = 3$, $\mathcal{L}(3\infty)$ 是 $\mathbb{F}_4$ 上一个三维向量空间, 有一组基 $\{1, x, y\}$. 由定理 2.3, 我们得到一个由椭圆曲线 (2.5) 导出的 16×64 传感矩阵. 图 2.1 展现了这个矩阵和一个 16×64 随机高斯矩阵的完美恢复百分比(perfect recovery percentage). 对每个稀疏度 k, 输入了 5000 个信号测试完美恢复百分比. 由椭圆曲线 (2.5) 构成的矩阵优于高斯矩阵.

类似地, 令 $r = 3$ 且 $s = 3$, 我们得到一个 32×512 传感矩阵. 图 2.2 展现了这个矩

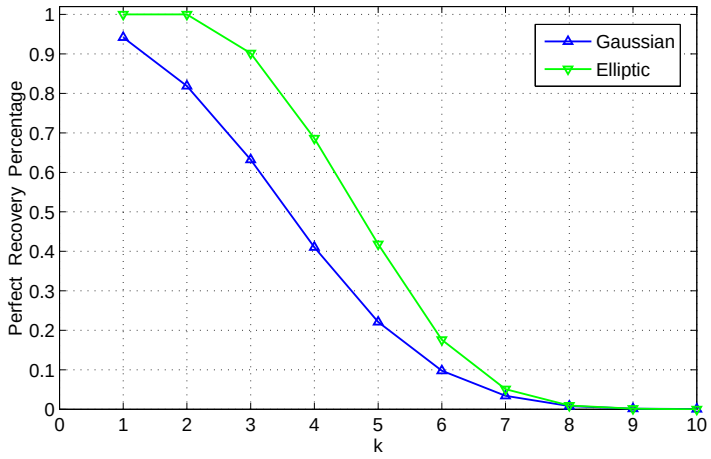

图 2.1　由椭圆曲线 $y^2 + y = x^3 + x$ 得出的矩阵和 16×64 随机高斯矩阵的完美恢复百分比

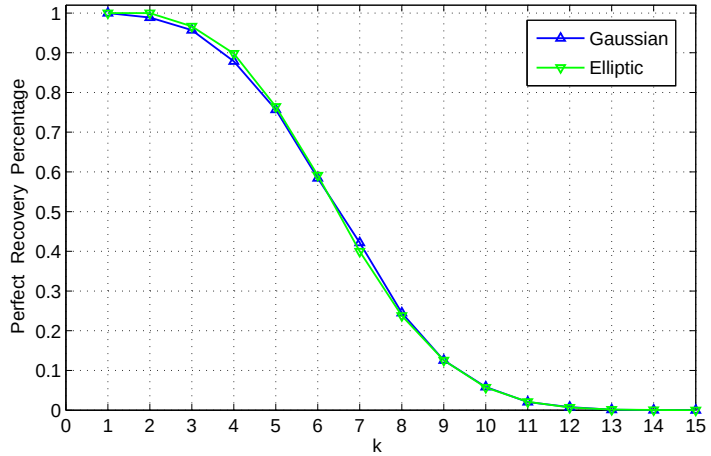

图 2.2　由椭圆曲线 $y^2 + y = x^3 + x$ 得出的矩阵和 32×512 随机高斯矩阵的完美恢复百分比

阵和一个 32×512 随机高斯矩阵的完美恢复百分比. 在这个例子中, 由椭圆曲线 (2.5) 构成的矩阵与高斯矩阵表现相当. 考虑到确定性构造的优点, 椭圆曲线构成的矩阵在实际应用中比随机高斯矩阵更受欢迎.

2.2.4.2　Hermitian 曲线

由定理 2.3, 我们得到相关值 $\mu \leq \deg(G)/|\mathcal{P}|$ 的矩阵, 其中 $\mathcal{P}$ 是曲线 $\mathcal{X}$ 上一些有理点的集合. 为了让这个相关值的上界尽可能小, 我们对具有很多有理点的曲线感兴趣. 一般的, 一条曲线上有理点的个数有以下的界.

定理 2.4 (Hasse-Weil 定理): 令 $\mathcal{X}$ 为 $\mathbb{F}_q$ 上一条代数曲线, 亏格为 g. $\mathcal{X}$ 上有理点个数

$N(\mathcal{X})$ 满足

$$|N(\mathcal{X}) - q - 1| \leq 2g\sqrt{q}.$$

一族达到以上的界的曲线是 Hermitian 曲线. 令 q 为一个素数幂的平方. $\mathbb{F}_q$ 上的 Hermitian 曲线 H_q 由以下仿射方程定义

$$y^{\sqrt{q}} + y = x^{\sqrt{q}+1}.$$

曲线的亏格 $g = g(H_q) = (q - q^{1/2})/2$ 且 H_q 上有理点的个数 $N(H_q) = q^{3/2} + 1$[252]. 注意到 $N(H_q)$ 达到 Hasse-Weil 定理中的上界.

令 Q 为 H_q 中和 $\mathbb{F}_q(x)$ 中的无穷远点相关的有理点. 令 $\mathcal{P}$ 为 H_q 上剩余有理点的集合, 满足 $|\mathcal{P}| = N(H_q) - 1 = q^{3/2}$. 对一个整数 s 满足 $q - q^{1/2} - 1 = 2g - 1 \leq s < q^{3/2}$, 我们令 $G = sQ$. 由定理 2.3, 我们有一个 $m \times n$ 传感矩阵Φ 满足

$$m = q^{5/2}, \quad n = q^{s+1-(q-q^{1/2})/2}, \quad \mu(\Phi) \leq s/q^{3/2},$$

其中 $q - q^{1/2} - 1 \leq s < q^{3/2}$. Φ 满足阶 $k < q^{3/2}/s + 1$ 的限制等距性质. 因此, Φ 可被用来恢复稀疏度

$$k \leq \frac{m^{3/5}}{\log_q n + \frac{1}{2}(m^{2/5} - m^{1/5})}$$

的信号.

以下我们比较由 Hermitian 曲线得到的矩阵和 DeVore 矩阵. 假设 $q = p^4$, 其中 p 是一个素数幂. 由 Hermitian 曲线 H_q 我们得到一个 $m_H \times n_H$ 矩阵 Φ_H 满足

$$\begin{aligned} m_H &= p^{10}, \\ n_H &= p^{4(s+1-g)}, \\ \mu_H &= s/p^6, \end{aligned}$$

其中 $p^4 - p^2 - 1 \leq s < p^6$, $g = (p^4 - p^2)/2$ 且相关值 $\mu(\Phi_H) \leq \mu_H$. 由 DeVore 构造, 我

们有一个 $m_D \times n_D$ 矩阵 Φ_D 满足

$$\begin{aligned} m_D &= p^{10}, \\ n_D &= p^{5(t+1)}, \\ \mu_D &= t/p^5, \end{aligned}$$

其中 $1 \le t < p^5$ 且相关值 $\mu(\Phi_D) \le \mu_D$. 当

$$4(s+1-g) = 5(t+1),$$

Φ_H 和 Φ_D 有同样的规模. 我们比较可达到的相关值的上界, 即 μ_H 和 μ_D.

$$\begin{aligned} \frac{\mu_H}{\mu_D} &= \frac{1}{p} \cdot \frac{s}{t} \\ &= \begin{cases} \Theta(p^{3-\eta}), & \text{如果 } t = \Theta(p^\eta), 0 \le \eta < 3 \\ \frac{1}{2c}, & \text{如果 } t = \Theta(p^3) = cp^3 + o(p^3), c \ne 0 \\ \Theta(p^{-\epsilon}), & \text{如果 } t = \Theta(p^{3+\epsilon}), 0 < \epsilon \le 2. \end{cases} \end{aligned}$$

从相关值的来看, 当 $t = \Theta(p^{3+\epsilon})$, 我们的矩阵在渐近意义上远远优于 DeVore 矩阵. 事实上, 对二元矩阵, 当 $t = o(p^{2.5})$, DeVore 构造是渐近最优的[4]. 我们的构造给出了当 $t > p^3/2$ 时渐近意义下优于 DeVore 构造的矩阵.

2.2.5 总结

在本节中, 我们利用有限域上的代数曲线构造了二元传感矩阵. 我们的构造可视为 DeVore 利用有限域上多项式的构造的自然推广. 通过选取合适的曲线, 我们得到了优于 DeVore 矩阵的传感矩阵.

代数曲线和它们的函数域的丰富资源为传感矩阵的构造提供了很大的灵活性. 文献[41]用压缩传感的理论框架导出一个加密方案, 其中一个传感矩阵作为一个加密密钥. 我们的构造为传感矩阵提供了更多的选择, 亦即为加密方案中的密钥提供了更多的选择, 因为不同的曲线得出不同的矩阵. 这对传感矩阵在密码学领域的潜在应用有很高的价值.

历史上, Goppa 的想法启发了关于代数几何码的研究, 得出了很多具有好的参数的线性码. 我们相信我们的构造仍然有很大的潜力. 一般的, 二元传感矩阵在压缩传感中不是好的候选矩阵, 因为所有的矩阵元素都是非负的. 利用 p-元 BCH 码, 非二元传感矩阵的构造取得了一些进展[5]. 因此, 利用代数曲线构造非二元传感矩阵是一个有趣的问题.

2.3 利用有限几何构造确定性稀疏传感矩阵

2.3.1 引言

目前, 关于随机的稀疏传感矩阵已经有了很多的研究, 可见综述文献[113]. 在本节中, 我们考虑确定性稀疏传感矩阵的构造.

在本节中, 我们利用填充设计的关联矩阵去生成低相关的二元矩阵. 特别地, 我们对一类被称为 Steiner 系的特殊的填充设计感兴趣. 一系列 Steiner 系可从有限几何得到. 利用这些 Steiner 系, 我们构造了四类基于相关值的二元稀疏传感矩阵. 更确切地, 我们得到了 $m \times n$ 确定性二元稀疏矩阵满足稀疏度 $k = \Theta(m^{1/2})$ 或 $k = \Theta(m^{1/3})$.

我们同时利用文献[5] 中提出的嵌入操作将我们的二元矩阵与 Hadamard 矩阵 (Hadamard matrices) 或离散傅立叶变换矩阵 (Discrete Fourier Transform) 融合. 这个操作给出了改进的传感矩阵. 它扩展了初始二元矩阵的列数且保持相关值不变. 注意到二元矩阵只含有非负的元素 0 和 1, 嵌入操作为传感矩阵添加了很多其它元素, 使得每一次测量包含了比之前更多的信息. 因此, 嵌入操作提高了传感矩阵的恢复效果. 此外, 嵌入操作后得到的改进矩阵保留了原矩阵稀疏的性质.

数据实验表明我们的二元和改进矩阵具有很好的恢复效果. 与高斯矩阵, Devore 矩阵[76], 由代数曲线得到的矩阵[188] 和由 BCH 码得到的矩阵相比[4,5], 我们的矩阵在数值实验中表现更好. 此外, 我们矩阵的稀疏性质有利于缩短利用正交匹配追踪等算法恢复信号时所花费的时间.

2.3.2 填充设计和 Steiner 系的背景知识

填充设计 (packing design) 在组合设计领域是一个长期的研究课题. 某些填充设计的关联矩阵自然地给出低相关的二元矩阵. 我们首先给出填充设计和它的关联矩阵的定义.

定义 2.1: 令 $m \geq s \geq t$. 一个 t-(m, s, λ) 填充设计是一个对 $(X, \mathcal{B})$, 其中 X 是一个 m-元集合, 集合元素称为点 (points) 且 $\mathcal{B}$ 是一个 X 的 s-子集组成的集合, 集合元素称为区组 (blocks), 使得每个点的 t-元子集至多出现在 λ 个 $\mathcal{B}$ 中的区组中. λ 被称为填充设计 $(X, \mathcal{B})$ 的指数.

定义 2.2: 令 $(X, \mathcal{B})$ 为一个填充设计, 其中 $X = \{x_1, \ldots, x_m\}$ 且 $\mathcal{B} = \{B_1, \ldots, B_n\}$. $(X, \mathcal{B})$ 的关联矩阵是一个 $m \times n$ 二元矩阵 M 满足

$$M_{i,j} = \begin{cases} 1 & \text{如果 } x_i \in B_j, \\ 0 & \text{如果 } x_i \notin B_j. \end{cases}$$

更多关于填充设计的背景, 可参见文献[206]. 此后, 我们仅考虑指数 $\lambda = 1$ 的填充设计. 以下定理表明填充设计可以得出低相关的矩阵.

定理 2.5: 令 $(X, \mathcal{B})$ 为一个 t-$(m, s, 1)$ 填充设计, 有 n 个区组. 假设 Φ 是关联矩阵, 那么 Φ 是一个 $m \times n$ 矩阵, 相关值 $\mu(\Phi) \leq \frac{t-1}{s}$.

证明. 假设 Φ 由 n 列 $\phi_1, \phi_2, \ldots, \phi_n$, 那么 $\|\phi_i\|_2 = \sqrt{s}$ 对 $1 \leq i \leq n$. 由于 $(X, \mathcal{B})$ 是一个 t-$(m, s, 1)$ 填充设计, 对 X 的任意 t 个点, 存在至多一个区组属于 $\mathcal{B}$ 包含这些点. 因此, 每两个 $\mathcal{B}$ 中的区组由不超过 $t-1$ 个公共点. 等价地, 内积 $\langle \phi_i, \phi_j \rangle \leq t-1$ 对 $1 \leq i, j \leq n, i \neq j$. 因此, 我们有

$$\mu(\Phi) = \max_{i \neq j} \frac{|\langle \phi_i, \phi_j \rangle|}{\|\phi_i\|_2 \cdot \|\phi_j\|_2} \leq \frac{t-1}{s}.$$

□

Steiner 系 (Steiner systems) 的研究可追溯到十九世纪中叶, 是组合设计理论中的一个中心问题. Steiner 系是一种特殊的填充设计.

定义 2.3: 令 $m \geq s \geq t \geq 2$. 一个 Steiner 系 $S(t, s, m)$ 是一个 t-$(m, s, 1)$ 填充设计, 使得每个点的 t-子集恰好出现在一个区组中.

对一个 Steiner 系 $S(t, s, m)$, 区组个数 $n = \binom{m}{t} / \binom{s}{t}$. 因此, 我们有以下的推论.

推论 2.1: 令 $(X, \mathcal{B})$ 为一个 Steiner 系 $S(t, s, m)$. 假设 Φ 是一个关联矩阵, 那么 Φ 是一个 $m \times n$ 矩阵, 相关值 $\mu(\Phi) \leq \frac{t-1}{s}$, 其中 $n = \binom{m}{t} / \binom{s}{t}$.

关于 Steiner 系的存在性结果, 可参见综述[67]. 以下, 我们考虑由有限几何导出的 Steiner 系, 导出我们二元传感矩阵的构造.

2.3.3 由有限几何得出的二元矩阵

由定理 2.5, 我们知道低相关矩阵可由具有较大区组大小的填充设计得出. 一系列区组大小很大的 Steiner 系可从有限几何得出.

定义 2.4: 一个有限关联结构, 或有限几何, 是一个三元组 $(\mathcal{P}, \mathcal{L}, I)$, 其中 $\mathcal{P}$ 是一个点的有限集, $\mathcal{L}$ 是线的有限集且 I 是它们之间的一个关联关系.

以下, 我们列举四类从有限几何得出的二元传感矩阵.

2.3.3.1 射影空间

定义 2.5: 一个有限射影空间 (projective space) 是一个有限关联结构满足:

1. 任两个点恰好在一条直线上.
2. 令 A,B,C,D 为四个不同的点且任三个不共线. 如果 AB 和 CD 相交, 则 AD 和 BC 也相交.
3. 任意线至少有三个点.

假设 $d \geq 2$ 是一个整数且 q 是一个素数幂. 经典的 d-维射影空间 $PG(d, q) = (\mathcal{P}, \mathcal{L}, I)$ 可以如下构造. 令 V 为 $\mathbb{F}_q$ 上一个 $d+1$-维线性空间. 对任意 $(a_0, a_1, \ldots, a_d) \in V \setminus \{(0, 0, \ldots, 0)\}$, 一个点 $(a_0 : a_1 : \cdots : a_d)$ 定义为

$$\{(\lambda a_0, \lambda a_1, \ldots, \lambda a_d) \mid \lambda \in \mathbb{F}_q \setminus \{0\}\}.$$

亦即, $\mathcal{P}$ 的一个点是 V 中一个 1-维子空间除去原点. 因此, $(a_0 : a_1 : \cdots : a_d)$ 和 $(\lambda a_0 : \lambda a_1 : \ldots : \lambda a_d)$ 对任意 $\lambda \in \mathbb{F}_q \setminus \{0\}$ 是相同的. 我们有 $|\mathcal{P}| = \frac{q^{d+1}-1}{q-1}$. 对任意 $(b_0, b_1, \ldots, b_d) \in V \setminus \{(0, 0, \ldots, 0)\}$, $\mathcal{L}$ 的一条线是 V 中一个 2-维子空间除去原点. 亦即, $\mathcal{L}$ 的一条线是 $\mathcal{P}$ 中一些点的集合, 这些点的坐标是以下 $d-1$ 个线性齐次方程的

非零公共解

$$\begin{cases} c_{00}x_0 + c_{01}x_1 + & \cdots & +c_{0d}x_d = 0 \\ c_{10}x_0 + c_{11}x_1 + & \cdots & +c_{1d}x_d = 0 \\ & \cdots & \\ c_{d-2,0}x_0 + c_{d-2,1}x_1 + & \cdots & +c_{d-2,d}x_d = 0, \end{cases}$$

其中 $c_{ij} \in \mathbb{F}_q$ 且矩阵 $C = (c_{ij})$ 的秩为 $d-1$. 另一个描述一条线 $\mathcal{L}$ 的简单方法是它的参数表示. 经过 $(a_0 : a_1 : \cdots : a_d)$ 和 $(b_0 : b_1 : \cdots : b_d)$ 的线是以下点的集合

$$\{(b_0 : b_1 : \cdots : b_d)\} \cup \{(a_0 + \lambda b_0 : a_1 + \lambda b_1 : \cdots : a_d + \lambda b_d)\},$$

其中 $\lambda \in \mathbb{F}_q$. 由于每两个点确定一条直线且每条线包含 $q+1$ 个点, $|\mathcal{L}| = \binom{\frac{q^{d+1}-1}{q-1}}{2} / \binom{q+1}{2} = \frac{(q^{d+1}-1)(q^d-1)}{(q+1)(q-1)^2}$. 对任意 $p \in \mathcal{P}$ 和 $l \in \mathcal{L}$, p 和 l 是相关联的当且仅当 p 包含在 l 中.

射影空间 $PG(d,q)$ 给出一个 Steiner 系 $S(2, q+1, \frac{q^{d+1}-1}{q-1})$[256]. 特别地, 二元传感矩阵可从 3-维射影空间 $PG(3,q) = (\mathcal{P}_1, \mathcal{L}_1, I_1)$ 中得出. 在这种情况下, 点集是

$$\mathcal{P}_1 = \{(a_0 : a_1 : a_2 : a_3) \mid (a_0, a_1, a_2, a_3) \in \mathbb{F}_q^4 \setminus \{(0,0,0,0)\}\}.$$

线的集合 $\mathcal{L}_1$ 由以下直线组成

$$\left\{ (x_0 : x_1 : x_2 : x_3) \middle| \begin{cases} c_{00}x_0 + c_{01}x_1 + c_{02}x_2 + c_{03}x_3 = 0 \\ c_{10}x_0 + c_{11}x_1 + c_{12}x_2 + c_{13}x_3 = 0 \end{cases} \right\},$$

其中

$$C = \begin{pmatrix} c_{00} & c_{01} & c_{02} & c_{03} \\ c_{10} & c_{11} & c_{12} & c_{13} \end{pmatrix}$$

跑遍 $\mathbb{F}_q^4$ 中所有的 2-维线性空间的矩阵表示. 以下, 我们称一个射影空间的关联矩阵为射影矩阵 (projective matrix).

构造 2.1: *令 q 为一个素数幂. 存在一个由射影空间 $PG(3,q)$ 导出的 Steiner 系 $S(2, q+1, q^3+q^2+q+1)$. 假设 Φ 是关联矩阵. 那么 Φ 是一个 $(q^3+q^2+q+1) \times (q^2+1)(q^2+q+1)$ 射影矩阵, 相关值 $\mu(\Phi) \leq \frac{1}{q+1}$.*

2.3.3.2 仿射空间

定义 2.6: 一个有限仿射空间 (affine space) 是一个有限关联结构满足:

1. 任两个点恰好在一条直线上.
2. 两条直线 l 和 l' 是平行的如果 $l = l'$ 或 l 与 l' 不相交. 对任意点 A 和任意线 l, 恰好存在一条经过 A 的线 l' 平行于 l.
3. 如果 A, B, C 是三个不共线的点且 A', B' 是两个相异的点使得 $A'B'$ 平行于 AB, 那么经过 A' 与 AC 平行的直线与经过 B' 与 BC 平行的直线交于某个点 C'.
4. 存在三个不共线的点.

假设 $d \geq 2$ 是一个整数且 q 是一个素数幂. 经典的 d-维仿射空间 $AG(d, q) = (\mathcal{P}, \mathcal{L}, I)$ 可以如下构造. 令 V 为 $\mathbb{F}_q$ 上一个 d-维线性空间. 点集 $\mathcal{P}$ 是 V 中的点且 $|\mathcal{P}| = q^d$. 线的集合 $\mathcal{L}$ 是 V 中 1-维子空间的陪集构成的集合. 亦即, $\mathcal{L}$ 是 $\mathcal{P}$ 中点的集合, 这些点的坐标是以下 $d-1$ 个线性方程的公共解

$$\begin{cases} c_{11}x_1 + c_{12}x_2 + \quad \cdots \quad + c_{1d}x_d = f_1 \\ c_{21}x_1 + c_{22}x_2 + \quad \cdots \quad + c_{2d}x_d = f_2 \\ \qquad\qquad\qquad \cdots \\ c_{d-1,1}x_1 + c_{d-1,2}x_2 + \quad \cdots \quad + c_{d-1,d}x_d = f_{d-1}, \end{cases}$$

其中 $c_{ij}, f_i \in \mathbb{F}_q$ 且矩阵

$$C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1d} \\ c_{21} & c_{22} & \cdots & c_{2d} \\ & & \cdots & \\ c_{d-1,1} & c_{d-1,2} & \cdots & c_{d-1,d} \end{pmatrix}$$

和

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1d} & f_1 \\ c_{21} & c_{22} & \cdots & c_{2d} & f_2 \\ & & \cdots & & \\ c_{d-1,1} & c_{d-1,2} & \cdots & c_{d-1,d} & f_{d-1} \end{pmatrix}$$

的秩为 $d-1$. 另一个描述 $\mathcal{L}$ 中一条线的简单方法是它的参数表示. 经过 $(a_1, a_2, \cdots, a_d)$ 和 $(b_1, b_2, \cdots, b_d)$ 的一条线是以下点的集合:

$$\{\lambda(a_1, a_2, \cdots, a_d) + (1-\lambda)(b_1, b_2, \cdots, b_d) \mid \lambda \in \mathbb{F}_q\}.$$

由于任意两个点确定一条直线且每条直线包含 q 个点, $|\mathcal{L}| = \binom{q^d}{2}/\binom{q}{2} = \frac{q^{d-1}(q^d-1)}{q-1}$. 对任意 $p \in \mathcal{P}$ 和 $l \in \mathcal{L}$, p 和 l 相关联当且仅当 p 包含在 l 中.

仿射空间 $AG(d,q)$ 给出一个 Steiner 系 $S(2,q,q^d)$[256]. 特别地, 二元传感矩阵可由 3-维仿射空间 $AG(3,q) = (\mathcal{P}_1, \mathcal{L}_1, I_1)$ 导出. 在这种情况下, 点集是

$$\mathcal{P}_1 = \{(a_1, a_2, a_3) \in \mathbb{F}_q^3\}.$$

线的集合 $\mathcal{L}_1$ 包含线

$$\left\{(x_1,x_2,x_3)\middle|\begin{cases} c_{11}x_1 + c_{12}x_2 + c_{13}x_3 = f_1 \\ c_{21}x_1 + c_{22}x_2 + c_{23}x_3 = f_2 \end{cases}\right\},$$

其中

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix}$$

跑遍 $\mathbb{F}_q^3$ 中 2-维子空间的矩阵表示且 (f_1, f_2) 跑遍 $\mathbb{F}_q^2$, 使得矩阵

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} & f_1 \\ c_{21} & c_{22} & c_{23} & f_2 \end{pmatrix}$$

的秩为 2. 以下, 我们称一个仿射空间的关联矩阵为一个仿射矩阵 (affine matrix).

构造 2.2: *令 q 为一个素数幂. 存在一个由仿射空间 $AG(3,q)$ 生成的 Steiner 系 $S(2,q,q^3)$. 假设 Φ 是关联矩阵. 那么 Φ 是一个 $q^3 \times q^2(q^2+q+1)$ 仿射矩阵, 相关值 $\mu(\Phi) \leq \frac{1}{q}$.*

2.3.3.3 Unital

定义 2.7: *一个 unital 是一个有限关联结构满足:*

1. *包含 n^3+1 个点.*
2. *每条线有 $n+1$ 个点.*
3. *任意两个相异的点恰在一条直线上.*

假设 q 是一个素数幂. 令 $(\mathcal{P}_1, \mathcal{L}_1, I_1)$ 为阶为 q 的 Hermitian unital, 可如下构造. 这

个 unital 属于一个 2-维射影空间 $PG(2,q^2)=(\mathcal{P},\mathcal{L},I)$. 点集是

$$\mathcal{P}_1=\{(a_0:a_1:a_2)\in\mathcal{P}\mid a_0^{q+1}+a_1^{q+1}+a_2^{q+1}=0\}.$$

亦即, Hermitian unital 的点是 $PG(2,q^2)$ 中落在曲线 $\mathcal{C}: x^{q+1}+y^{q+1}+z^{q+1}=0$ 上的点. 易知 $|\mathcal{P}_1|=q^3+1$. 假设 $l\in\mathcal{L}$ 与直线 $\mathcal{C}$ 相交于两个点 $(a_0:a_1:a_2)$ 和 $(b_0:b_1:b_2)$. 那么 l 是点的集合

$$\{(b_0:b_1:b_2)\}\cup\{(a_0+\lambda b_0:a_1+\lambda b_1:a_2+\lambda b_2)\},$$

其中 $\lambda\in\mathbb{F}_{q^2}$. 令 Tr 记从 $\mathbb{F}_{q^2}$ 到 $\mathbb{F}_q$ 的迹函数, 其中 $\mathrm{Tr}(x)=1+x^q$ 对任意 $x\in\mathbb{F}_{q^2}$. 迹函数的核 $\{x\in\mathbb{F}_{q^2}\mid x^q=-1\}$ 包含 q 个元素. 由于

$$\begin{aligned}
&(a_0+\lambda b_0)^{q+1}+(a_1+\lambda b_1)^{q+1}+(a_2+\lambda b_2)^{q+1}\\
=\;&\lambda a_0^q b_0+\lambda a_0 b_0^q+\lambda a_1^q b_1+\lambda a_1 b_1^q+\lambda a_2^q b_2+\lambda a_2 b_2^q\\
&+(a_0^{q+1}+a_1^{q+1}+a_2^{q+1})+\lambda^{q+1}(b_0^{q+1}+b_1^{q+1}+b_2^{q+1})\\
=\;&\mathrm{Tr}(\lambda(a_0^q b_0+a_1^q b_1+a_2^q b_2)),
\end{aligned}$$

恰好存在 q 个 $\lambda\in\mathbb{F}_{q^2}$ 使得 $(a_0+\lambda b_0)^{q+1}+(a_1+\lambda b_1)^{q+1}+(a_2+\lambda b_2)^{q+1}=0$. 因此, 如果一条线 $l\in\mathcal{L}$ 与曲线 $\mathcal{C}$ 交于两个点, 那它必须与 $\mathcal{C}$ 交于 $q+1$ 个点. 事实上, $\mathcal{L}$ 的每条线交 $\mathcal{C}$ 于 1 个或 $q+1$ 个点[256]. $\mathcal{L}_1$ 是所有与 $\mathcal{C}$ 交于 $q+1$ 个点的直线组成的集合, 亦即,

$$\mathcal{L}_1=\{l\cap\mathcal{C}\mid l\in\mathcal{L},|l\cap\mathcal{C}|=q+1\}.$$

对任意 $p\in\mathcal{P}_1$ 和 $l\in\mathcal{L}_1$, p 和 l 相关联当且仅当 p 包含在 l 中.

由定义 2.7, 阶为 q 的 Hermitian unital 给出一个 Steiner 系 $S(2,q+1,q^3+1)$. 因此, 我们得到二元传感矩阵. 以下, 我们称一个 unital 的关联矩阵为一个 unital 矩阵 (unital matrix).

构造 2.3: *令 q 为一个素数幂. 存在一个从 q 阶 Hermitian unital 导出的 Steiner 系 $S(2,q+1,q^3+1)$. 假设 Φ 是关联矩阵. 那么 Φ 是一个 $(q^3+1)\times q^2(q^2-q+1)$ unital 矩阵, 相关值 $\mu(\Phi)\le\frac{1}{q+1}$.*

2.3.3.4 逆平面

定义 2.8：一个逆平面 (inversive plane) 是一个满足以下条件的有限关联结构. 注意到一个逆平面中的线被称为一个圈 (circle).

1. 任意三个不同的点恰在一个圈上.
2. 如果 A, B 是两个点且 C 是一个包含 A 且不包含 B 的圈, 那么恰存在一个圈 C' 包含 B 使得 $C \cap C' = \{A\}$.
3. 存在四个点不在同一个圈上.

假设 q 是一个素数幂. 一个逆平面 $(\mathcal{P}, \mathcal{L}, I)$ 可如下构造. 点集是 $\mathcal{P} = \mathbb{F}_{q^2} \cup \{\infty\}$, 其中 ∞ 代表一个无限元. 对 $a \in \mathbb{F}_{q^2}, a \neq 0$, 我们定义 $\infty = \frac{a}{0}$. 假设 $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^2}$, 令 G 为一个群包含所有如下形式的分式线性变换

$$t_{\alpha\beta\gamma\delta} : a \to \frac{\alpha a + \beta}{\gamma a + \delta}, \quad \forall\, a \in \mathbb{F}_{q^2}, \alpha\delta - \beta\gamma \neq 0,$$

其中 $t_{\alpha\beta\gamma\delta}(\infty) = \alpha\gamma^{-1}$ 且 $t_{\alpha\beta\gamma\delta}(-\delta\gamma^{-1}) = \infty$. 因而, G 是作用在 $\mathcal{P}$ 上的一个置换群且是严格 3-传递的 (习题 2.8.4[95]). 事实上, 群 G 同构于射影一般线性群 $\mathrm{PGL}(2, \mathbb{F}_{q^2})$ (习题 2.8.7[95]). 令 $S = \mathbb{F}_q \cup \{\infty\}$ 为 $\mathcal{P}$ 的一个子集, 圈的集合 $\mathcal{L}$ 由 S 在 G 的作用下的轨道生成. 对任意 $p \in \mathcal{P}$ 和 $l \in \mathcal{L}$, p 和 l 是相关联的当且仅当 p 包含在 l 中. 由 G 的严格 3-传递性质, $(\mathcal{P}, \mathcal{L}, I)$ 是一个 Steiner 系 $S(3, q+1, q^2+1)$ (例子 4.30[177]). 因此, 我们得到了二元传感矩阵. 以下, 我们将逆平面的关联矩阵称为一个逆矩阵 (inversive matrix).

构造 2.4：令 q 为一个素数幂. 存在一个由逆平面导出的 Steiner 系 $S(3, q+1, q^2+1)$. 假设 Φ 是关联矩阵. 那么 Φ 是一个 $(q^2+1) \times q(q^2+1)$ 逆矩阵, 相关值 $\mu(\Phi) \leq \frac{2}{q+1}$.

对以上有限几何的系统处理, 可参见文献[73,273]. 值得一提的是所有这些有限几何均可由 Magma[25] 的内置函数生成. 因此, 二元传感矩阵的构造是容易的.

2.3.4 嵌入操作

我们回顾文献[5] 中提出的嵌入操作. 嵌入操作将二元矩阵与其它低相关矩阵融合起来.

定义 2.9: 假设 A 是一个 $m \times n_1$ 二元矩阵, 它的列为 $u_1, u_2, \ldots, u_{n_1}$ 且每列的列和为常数 w. 令 B 为一个 $w \times n_2$ 矩阵, 它的列为 $v_1, v_2, \ldots, v_{n_2}$. c_{ij} 是一个将 u_i 中 w 个 1 替换为 v_j 中相应的 w 个元素后得到的列向量. 定义 $A \odot B$ 为一个 $m \times n_1 n_2$ 矩阵, 它的列为 c_{ij}, 其中 $1 \leq i \leq n_1$ 且 $1 \leq j \leq n_2$.

以下引理说明, $A \odot B$ 的相关值由 A 和 B 的相关值决定.

引理 2.3 (**引理** 2[5]): 假设 $C = A \odot B$, 那么 $\mu(C) = max\{\mu(A), \mu(B)\}$.

总之, 如果我们有一个合适的二元矩阵 A 和矩阵 B, 两个矩阵都具有低相关值, 那么嵌入操作生成一个低相关矩阵 $A \odot B$. 嵌入操作是非常有用的. 一方面, 给定一个二元传感矩阵, 嵌入操作生成了一个有更多列的改进矩阵. 由于改进矩阵包括除了 0 和 1 之外的其它元素, 每次测量包含了比之前更多的信息. 因此, 改进矩阵的恢复效果优于原二元矩阵. 另一方面, 给定一个稠密的传感矩阵, 嵌入操作将它的元素融入一个二元矩阵, 生成了一个具有更多列的稀疏的传感矩阵. 稀疏矩阵有利于节省存储空间和加快恢复进程, 因而更受欢迎.

以下, 通过将 Hadamard 矩阵或离散傅立叶变换矩阵嵌入我们的二元矩阵, 得到一系列改进矩阵. 更一般地, 许多低相关矩阵, 例如会议矩阵 (conference matrices)[153], 签名集 (signature sets)[169], Grassmannian 框架 (Grassmannian frames)[257] 和相互无偏基 (mutually unbiased bases)[289], 已在不同的背景和应用中得到了研究. 嵌入操作也可被用于这些矩阵. 这为低相关矩阵的构造提供了极大的灵活性. 在这个意义下, 我们的二元矩阵的构造在嵌入操作中起到了作为基础结构的重要作用.

2.3.5 数值实验

本小节将我们的二元矩阵, 改进矩阵与其它几种典型的矩阵进行了比较. 其中, 高斯 (Gaussian) 和复值高斯 (complex-valued Gaussian) 矩阵是广泛应用的随机稠密矩阵. 由 BCH 码[4] 和 p-元 BCH 码[5] 得到的矩阵是确定性的稠密矩阵. 后者有相对于 Welch 界的接近最优的相关值. DeVore 矩阵[76] 和由代数曲线得到的矩阵[188] 是二元的稀疏矩阵. 数值实验表明我们的矩阵优于这些矩阵. 对我们的稀疏矩阵, 绝大多数的矩阵元素是零. 通过删除关于零元素的运算, 信号恢复过程的计算复杂度可被降低. 与稠密矩阵相比, 我们的稀疏矩阵要求更少的存储空间和恢复时间.

在数值实验中, 我们利用 k-稀疏向量作为测试信号, 其中 k 个非零分量服从标准

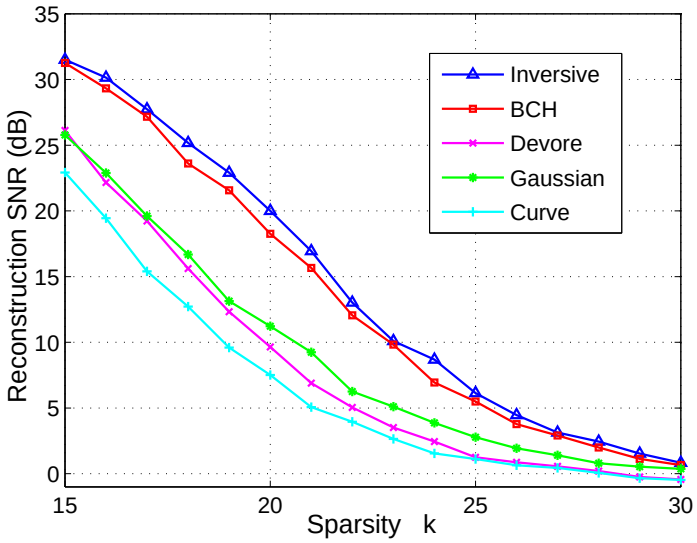

图 2.3　有噪声信号的恢复信噪比. BCH 矩阵规模为 63×512. DeVore 矩阵和由代数曲线得出的矩阵规模为 64×512. 其它矩阵规模为 65×512.

的高斯分布. 如果传感矩阵是复值的, 我们利用 k-稀疏的复值向量作为稀疏信号, 其中每个非零分量的实部与虚部服从标准的高斯分布. 对有噪声的恢复, 一个信号 x 掺入了加性的高斯噪声 e, 其中信噪比是 30 dB. 因而, 给定一个传感矩阵 Φ, 我们有测量向量 $y = \Phi(x + e)$. 对每个稀疏度 (sparsity) k, 我们用正交匹配追踪作为恢复算法测试 1000 个 k-稀疏信号. 对一个信号 x, 假设 x^* 是由正交匹配追踪恢复出的信号. x 的恢复信噪比 (reconstruction SNR) 定义为

$$\text{SNR}(x) = 20 \cdot \log_{10}\big(\frac{\|x\|_2}{\|x - x^*\|_2}\big)\text{dB}.$$

图 2.3 展现了有噪声的 k-稀疏 512×1 信号的恢复信噪比, 其中 $15 \le k \le 30$. 由代数曲线构造的传感矩阵是由有限域 $\mathbb{F}_8$ 上的椭圆曲线 $y^2 + y = x^3$ 导出的. 此处使用的逆矩阵是从 65×520 逆矩阵中随机选取 512 列构成的. 逆矩阵的恢复效果优于其它矩阵.

图 2.4 展现了有噪声的 k-稀疏 775×1 信号的恢复信噪比, 其中 $20 \le k \le 55$. 此处的BCH 矩阵是从 127×16384 BCH 矩阵中选取前 775 列构成的. 仿射矩阵的恢复效果优于高斯矩阵且与 BCH 矩阵相仿. 有一种观点认为这个比较对 BCH 矩阵不公平, 因为它被设计为去采样长度的大得多的信号. 然而, 确定性构造总是得出一系列有固定规模的矩阵. 一般地, 很难让我们构造的矩阵与其它方法构造的矩阵具有相近的规模.

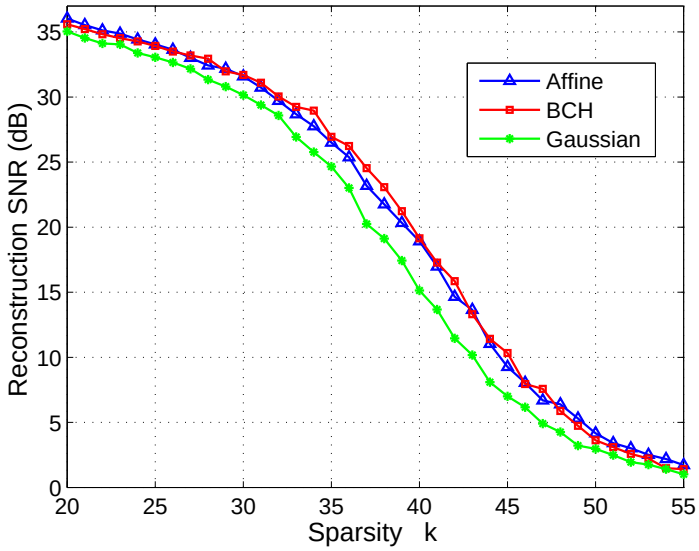

图 2.4　有噪声信号的恢复信噪比. BCH 矩阵规模为 127×775. 其它矩阵规模为 125×775.

此外, 在实际应用中, 一个确定性矩阵的某些列总是被删去, 以适应信号的长度. 因此, 我们认为实验中使用从原矩阵中挑选一些列构成 BCH 矩阵是一个合理的折衷. 以下, 当类似情况发生时, 我们都将明确声明.

对一个信号 x, 如果它的恢复信噪比不低于 100 dB, 我们称 x 的恢复是完美的. 图 2.5 展现了无噪声 k-稀疏 250×1 信号的完美恢复百分比 (perfect recovery percentage), 其中 $1 \leq k \leq 15$. 假设 H 是一个 4×4 Hadamard 矩阵. H' 是一个由 H 添加一行得到的 5×4 矩阵. 这一行的每个元素以等概率取值 1 或 -1. 将 H 嵌入 28×63 unital 矩阵, 我们得到一个 28×252 矩阵. 在图中, 我们用 'Unital + Hada' 代表改进的 unital 矩阵, 它是从这个 28×252 矩阵中随机选取 250 列构成. 改进的 DeVore 矩阵是由将 H' 的前两列嵌入 25×125 DeVore 矩阵得出. 嵌入操作方便我们采样长度更大的信号. 改进的 unital 矩阵的恢复效果优于其它矩阵.

图 2.6 展现了无噪声 k-稀疏 1458×1 信号的完美恢复百分比, 其中 $10 \leq k \leq 40$. 假设 w 是有限域 $\mathbb{F}_9$ 的一个本原元. 一个二元 81×729 矩阵可由有限域 $\mathbb{F}_9$ 上的椭圆曲线 $y^2 = x^3 + wx + 1$ 生成. 由代数曲线得出的矩阵的改进矩阵可由将 9×9 离散傅立叶变换矩阵嵌入到这个二元矩阵中生成. 类似地, 改进的 DeVore 矩阵可从 81×729 DeVore 矩阵得到. 将 5×5 离散傅立叶变换矩阵嵌入到射影矩阵, 我们得到一个 85×1785 矩阵. 改进的射影矩阵由从这个 85×1785 矩阵中随机选取 1458 列生成.

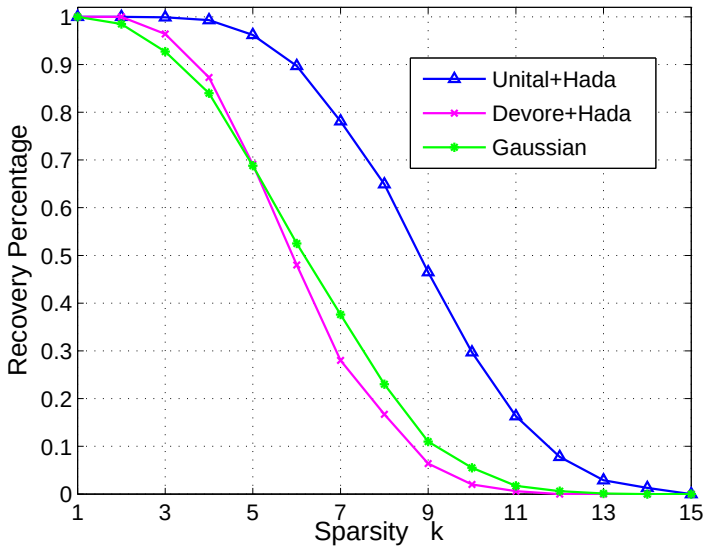

图 2.5　无噪声信号的完美恢复百分比. 改进的 DeVore 矩阵的规模为 25×250. 其它矩阵规模为 28×250.

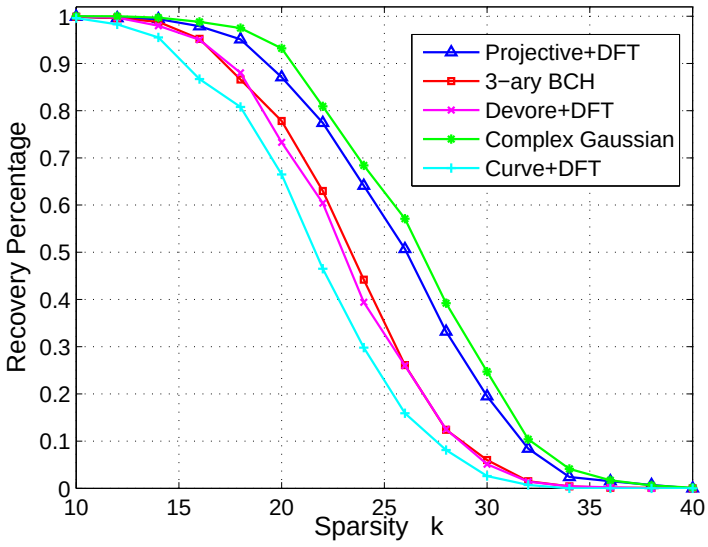

图 2.6　无噪声信号的完美恢复百分比. 3-元 BCH 矩阵的规模为 80×1458. 改进的 DeVore 矩阵和改进的由代数曲线得到的矩阵规模为 81×1458. 其它矩阵规模为 85×1458.

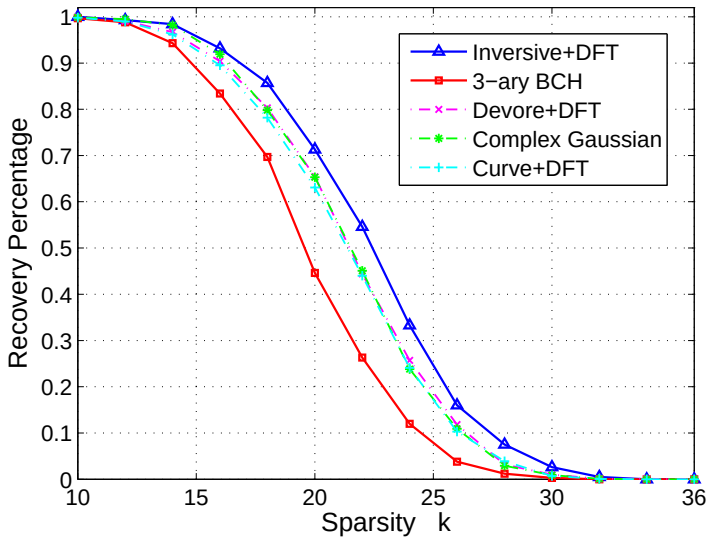

图 2.7　无噪声信号的完美恢复百分比. 3-元 BCH 矩阵的规模为 80×6561. 改进的 DeVore 矩阵和改进的由代数曲线得到的矩阵规模为 81×6561. 其它矩阵规模为 82×6561.

此处用到的 3-元 BCH 矩阵由 80×14348907 3-元 BCH 矩阵中选取前 1458 列生成. 改进的射影矩阵恢复效果略次于复值高斯矩阵, 优于其它矩阵.

图 2.7 展现了无噪声 k-稀疏 6561×1 信号的完美恢复百分比, 其中 $10 \leq k \leq 36$. 二元 DeVore 矩阵和由代数曲线导出的二元矩阵与图 2.6 的相同. 将 9×9 离散傅立叶变换矩阵嵌入其中, 我们得到改进的 81×6561 矩阵. 将 10×10 离散傅立叶变换矩阵嵌入到逆矩阵中, 我们得到一个 82×7380 矩阵. 改进的逆矩阵由从这个 82×7380 矩阵中随机选取 6561 列生成. 此处用到的 3-元BCH 矩阵从一个 80×14348907 3-元 BCH 矩阵选取前 6561 列生成. 改进的逆矩阵的恢复效果优于其它矩阵.

我们的二元和改进的矩阵都非常稀疏, 绝大部分的矩阵元素都是零. 通过删去和零元素相关的运算, 我们矩阵的稀疏性质有助于加快恢复过程. 传感矩阵中的零元素并不包含信息, 因此在计算过程中可忽略. 因此, 我们矩阵的稀疏性质对降低计算复杂度有本质的意义. 图 2.8 展现了无噪声 k-稀疏 3648×1 信号的完美恢复百分比和恢复时间, 其中 $80 \leq k \leq 210$. 基于文献[5] 的作者提供的 MATLAB 代码, 我们可以构造一个 255×4096 BCH 矩阵理论上保证恢复 8-稀疏信号, 或一个 1023×32768 BCH 矩阵理论上保证恢复 9-稀疏信号. 作为替代, 此处使用的 BCH 矩阵从一个 511×262144 BCH 矩阵中选取了前 3648 列. 此处, 很多列被删去了. 要点在于, 当 255 次测量太少而

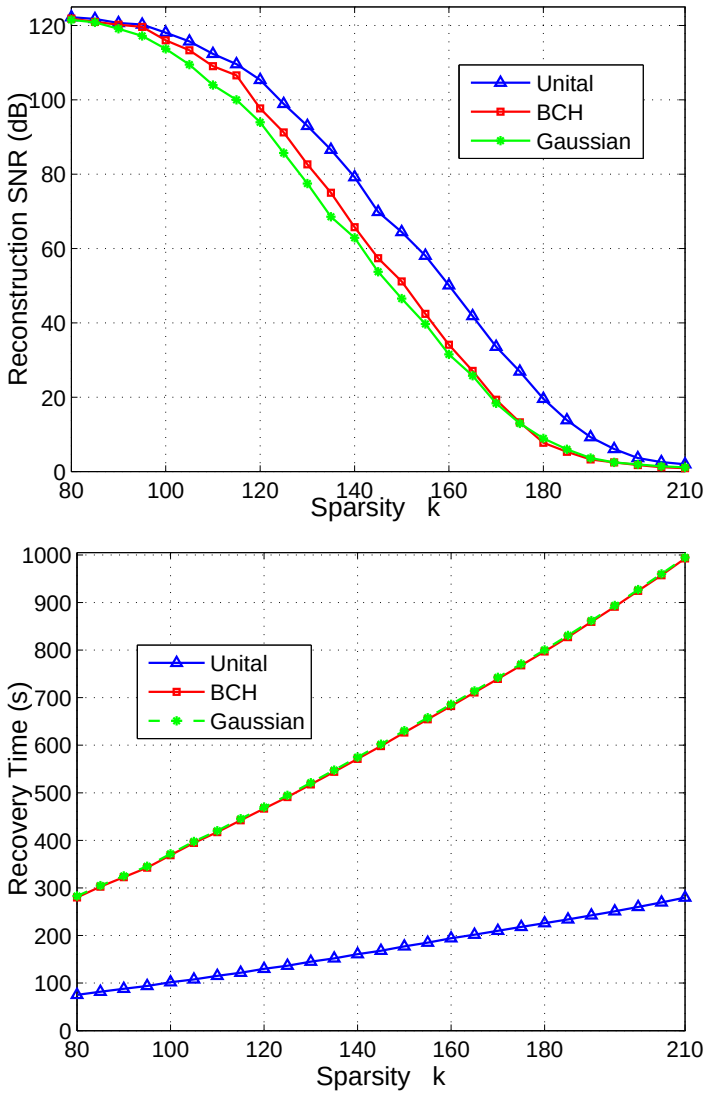

图 2.8　无噪声信号的恢复信噪比和恢复时间. BCH 矩阵规模为 511×3648. 其它矩阵规模为 513×3648.

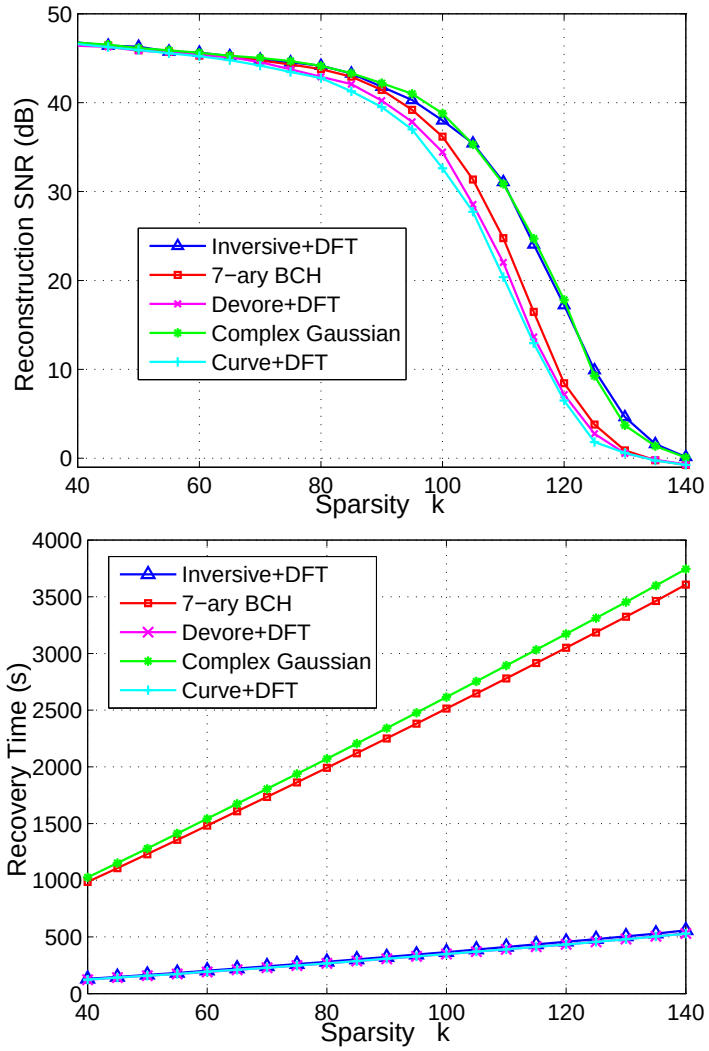

图 2.9　无噪声信号的恢复信噪比和恢复时间. BCH 矩阵规模为 342×13718. 改进的 DeVore 矩阵和改进的由代数曲线得到的矩阵规模为 361×13718. 其它矩阵规模为 362×13718.

1023 测量太多时, 我们的 unital 矩阵提供了另外的选择. unital 矩阵的不仅恢复效果优于其它矩阵, 且花费了最少的恢复时间.

图 2.9 展现了有噪声 k-稀疏 13718×1 信号的完美恢复百分比和恢复时间, 其中 $40 \leq k \leq 140$. 一个二元 361×6859 由有限域 $\mathbb{F}_{19}$ 上的椭圆曲线 $y^2 = x^3 + x + 8$ 导出. 由代数曲线导出的矩阵的改进矩阵可由将一个 19×19 离散傅立叶变换矩阵的前两列嵌入到这个二元矩阵中生成. 类似地, 改进的 DeVore 矩阵可由 361×6859 DeVore 矩阵得出. 将 20×20 离散傅立叶矩阵的前两列嵌入到一个逆矩阵中, 我们得到一个 362×13756 矩阵. 改进的逆矩阵可从这个 362×13756 矩阵中随机选取 13718 列生成. 此处用到的 7-元 BCH 矩阵从一个 342×823543 7-元 BCH 矩阵中选取前 13718 列生

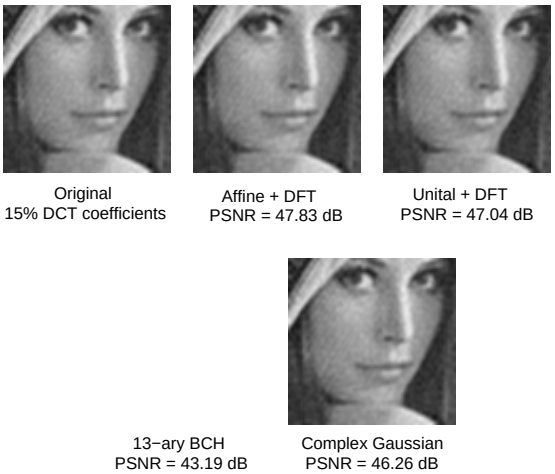

图 2.10　恢复一个 80×80 的图片, 其中仅有最大的 15% 的离散傅立叶变换系数被保留下来. 13-元 BCH 矩阵规模为 2196×6400, 改进的仿射矩阵的规模为 2197×6400. 其它的矩阵规模为 2198×6400.

成. 改进的逆矩阵的恢复效果与复值高斯矩阵相当, 优于其它矩阵. 改进的逆矩阵的恢复时间远少于稠密的矩阵.

在图 2.10 中, 我们恢复一个 80×80 的图片. 通过保留图片的离散傅立叶变换的前 15% 最大的系数并把其它系数置为零, 原始图片被稀疏化. 利用改进的仿射矩阵和改进的 unital 矩阵, 我们得到的恢复图片有更高的峰信噪比 (Peak Signal to Noise Ratios). 改进的矩阵的恢复效果优于 13-元BCH 矩阵和复值高斯矩阵.

2.3.6　总结

在本节中, 我们引入了确定性稀疏传感矩阵的一种新构造. 通过考察一系列由有限几何得出的 Steiner 系, 我们构造了四类二元稀疏矩阵. 文献[4] 指出光正交码 (Optical Orthogonal Codes) 导出了二元传感矩阵. 事实上, 一系列光正交码从有限几何中构造出来[2,20,207]. 在这个意义下, 我们的工作追溯到了光正交码背后的源头, 以 Steiner 系为桥梁, 建立了传感矩阵和有限几何之间的联系. 由于在有限几何领域有许多创造性的构造, 我们希望这个新观点可以刺激进一步的研究且得出传感矩阵的新的构造.

我们也利用嵌入操作改进我们的二元矩阵. 一方面, 嵌入操作增加了列数, 提升了恢复效果. 另一方面, 给定一个低相关的稠密矩阵, 嵌入操作给出一个稀疏矩阵. 稀疏性质有利于降低存储负担, 加快恢复过程. 在这种意义下, 我们的二元矩阵为嵌入操作

提供了基础架构. 嵌入操作是一个非常一般的框架, 因为任何基于相关值的构造可以用嵌入操作进行改进.

2.4 由近似正交系得到的确定性传感矩阵

2.4.1 引言

由于正交矩阵有零相关值, 我们称具有低相关值的矩阵为近似正交系 (near orthogonal system). 从不同的背景和动机出发, 近似正交系本质上以许多不同的名字居于许多不同场景的核心位置. 在本节中, 我们对源自于不同场景的近似正交系提供一个综述. 这些近似正交系的构造事实上就是确定性的低相关矩阵的构造. 更具体地, 我们得到了几类确定性的 $m \times n$ 矩阵满足稀疏度 $k = \Theta(m^{\frac{1}{2}})$ 或 $k = O\big((\frac{m}{\log m})^{\frac{1}{2}}\big)$.

许多数值实验表明我们的矩阵具有好的恢复效果. 与高斯矩阵 (Gaussian matrices), 随机离散傅立叶变换矩阵 (random Discrete Fourier Transform matrices), 伯努利矩阵 (Bernoulli matrices) 和由 BCH 码构成的矩阵[4,5] 相比, 我们的矩阵在许多数值实验中优于这些矩阵.

2.4.2 由 MWBE 序列集导出的传感矩阵

一个 MWBE 序列集 (Maximum Welch-Bound-Equality sequence set) 可被视为一个相关值达到 Welch 下界 (2.4) 的矩阵. 因而, 我们将一个 (N, K) MWBE 序列集视为一个 $K \times N$ 矩阵, 相关值为 $\sqrt{\frac{N-K}{K(N-1)}}$. MWBE 序列集也可被称作等角紧框架 (equiangular tight frames)[258] 或最优的 Grassmannian 框架 (optimal Grassmannian frames)[257]. MWBE 序列集在通信和编码理论中的应用可见[257]. 由于针对 MWBE 的存在性有很强的限制[258], 它的构造是很困难的[239]. 近年来, 新的 MWBE 序列集从差集[78,79,290] 和 Steiner 系中构造出来[107]. 以下, 我们考虑由这些新的 MWBE 序列导出的近似正交系. 由 MWBE 序列集得到传感矩阵的确定性构造是基于相关值的最优构造, 因为它们达到了 Welch 界 (2.4).

2.4.2.1 由差集得到的 MWBE 序列集

为了最大化不同信号的不相干性, 码本 (codebook) 被应用于码分多址系统中. 在文献[78,79,290]中的码本事实上就是由差集导出的 MWBE 序列集. 以下, 我们回顾文献[79] 中的构造.

假设 G 是一个阶为 v 的有限交换群. 一个大小为 k 的 G 的子集 D 被称为是一个 (v,k,λ) 差集如果 G 的每个非零元可被表为 $d_1-d_2, d_1,d_2\in D$ 恰好 λ 次. 有关差集的一个综述, 可参见文献[162] .

群 G 的一个特征 χ 是一个从群 G 到模长为 1 的复数组成的群 U 的一个群同态. 以下关于群特征的事实是熟知的:

1. $\chi(0)=1$;
2. $\chi(g)$ 是一个单位根;
3. $\chi(g^{-1})=\chi(g)^{-1}=\overline{\chi(g)}$, 其中上划线代表复数的共轭.

G 的所有特征形成一个群, 被称为 G 的特征群且记为 $\widehat{G}$.

对任意的有限交换群 G, 它的特征群可如下定义. 给定一个正整数 n, 令 ζ_n 为 n-次单位根 $e^{\frac{2\pi i}{n}}$. 对循环群 $\mathbb{Z}_n$, 我们有 $\widehat{\mathbb{Z}_n}=\{\chi_i \mid 0\le i\le n-1\}$, 其中

$$\chi_j(a)=\zeta_n^{ja},\ \forall a\in\mathbb{Z}_n.$$

注意到任意有限交换群是循环群的直积, 亦即, $G=\mathbb{Z}_{n_1}\bigoplus\mathbb{Z}_{n_2}\bigoplus\cdots\bigoplus\mathbb{Z}_{n_t}$. 那么, 特征群 $\widehat{G}=\{\chi_{j_1,j_2,\ldots,j_t}\mid j_i\in\mathbb{Z}_{n_i}, 1\le i\le t\}$, 其中

$$\chi_{j_1,j_2,\ldots,j_t}((a_1,a_2,\ldots,a_t))=\prod_{i=1}^{t}\zeta_{n_i}^{j_ia_i},\ \forall(a_1,a_2,\ldots,a_t)\in G.$$

因而, 我们有 $|\widehat{G}|=|G|$.

令 G 为一个阶为 N 的交换群且 $\widehat{G}=\{\chi_0,\chi_1,\ldots,\chi_{N-1}\}$. 假设 $D=\{d_1,d_2,\ldots,d_K\}$ 是 G 的一个 K 元子集. 我们定义一个 $K\times N$ 矩阵 $\Phi:=\Phi(G,D)$ 其中第 i 列为

$$\phi_i=(\chi_{i-1}(d_1),\chi_{i-1}(d_2),\ldots,\chi_{i-1}(d_K))^T.$$

Φ 是一个 MWBE 序列集, 如果 D 是 G 中的一个差集.

命题 2.1 (定理 3[79]): *Φ 是一个 (N,K) MWBE 序列集当且仅当 D 是 G 中一个 (N,K,λ) 差集, 其中 $K>1$.*

作为一个直接的结果, 确定性传感矩阵可由差集得到.

定理 2.6: 给定一个 n 阶交换群中的 (n, m, λ) 差集, 存在一个 $m \times n$ 矩阵 Φ 满足 $\mu(\Phi) = \sqrt{\frac{n-m}{m(n-1)}}$.

因而, 选定合适的差集, 就可以得到相应的传感矩阵. 第一个构造利用了 Singer 差集[162].

构造 2.5 (Singer **矩阵**): 假设 q 是一个素数幂且 d 是一个整数满足 $d \geq 3$. 令 α 为 $\mathbb{F}_{q^d}^*$ 的一个本原元且

$$tr_{q^d/q}(x) = \sum_{i=0}^{d-1} x^{q^i}$$

为 $\mathbb{F}_{q^d}$ 到 $\mathbb{F}_q$ 的迹函数. 那么集合 $\{i \mid 0 \leq i < (q^d-1)/(q-1), tr_{q^d/q}(\alpha^i) = 0\}$ 是群 $\mathbb{Z}_v$ 中的一个 (v, k, λ) Singer 差集, 其中

$$\begin{aligned} v &= \frac{q^d-1}{q-1}, \\ k &= \frac{q^{d-1}-1}{q-1}, \\ \lambda &= \frac{q^{d-2}-1}{q-1}. \end{aligned}$$

由定理 2.6, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= \frac{q^{d-1}-1}{q-1}, \\ n &= \frac{q^d-1}{q-1}, \\ \mu(\Phi) &= \frac{q^{\frac{d-2}{2}}(q-1)}{q^{d-1}-1}. \end{aligned}$$

我们称以上矩阵为一个 Singer 矩阵. 利用 McFarland 差集[204], 我们有以下类似的构造.

构造 2.6 (McFarland **矩阵**): 假设 q 是一个素数幂且 d 是一个正整数. 令 G 为一个阶为 $v = q^{d+1}(q^d + \cdots + q^2 + q + 2)$ 的群包含一个阶为 q^{d+1} 的基本交换子群 E 在它的中心中. 将 E 视作 $\mathbb{F}_q^{d+1}$ 的加法子群, 作为 $\mathbb{F}_q$ 上一个 $(d+1)$-维子空间. 令 $s = (q^{d+1}-1)/(q-1)$. 恰好存在 E 的 s 个 d-维子空间, 记做 $H_1, H_2, \ldots, H_s$. 如果 $g_0, \ldots, g_s$ 是 E 在 G 中不同的陪集代表元, 那么 $D = (g_1 + H_1) \cup (g_2 + H_2) \cup \cdots \cup (g_s + H_s)$ 是一个 (v, k, λ)

McFarland 差集满足

$$\begin{aligned} v &= q^{d+1}\left(\frac{q^{d+1}-1}{q-1}+1\right), \\ k &= q^{d}\left(\frac{q^{d+1}-1}{q-1}\right), \\ \lambda &= q^{d}\left(\frac{q^{d}-1}{q-1}\right). \end{aligned}$$

特别地, 我们选取一个正整数 d 满足 $\frac{q^{d+1}-1}{q-1}+1$ 是一个素数幂. 一般地, 确定 (q,d) 是否满足 $\frac{q^{d+1}-1}{q-1}+1$ 是一个素数幂是困难的. 数值实验表明集合 $\{(q,d) \mid 2 \leq q \leq 100, q$ 素数幂$, 1 \leq d \leq 10\}$ 中, 共有 350 个 (q,d) 对, 其中存在 41 个合适的 (q,d) 对. 现在, 我们假设 $\frac{q^{d+1}-1}{q-1}+1 = r^l$, 其中 r 是一个素数满足 $\gcd(r,q)=1$ 且 l 是一个正整数. 定义 $(G_1,+)=(\mathbb{F}_q^{d+1},+)$ 且 $(G_2,+)=(\mathbb{F}_r^{l},+)$. 那么 $(G,+)=(G_1\times G_2,+)$ 是一个阶为 v 的交换群且 $E=G_1\times\{0\}$ 是一个阶为 q^{d+1} 的初等交换子群. 由定理 2.6, 我们得到一个 $m\times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= q^{d}\left(\frac{q^{d+1}-1}{q-1}\right), \\ n &= q^{d+1}\left(\frac{q^{d+1}-1}{q-1}+1\right), \\ \mu(\Phi) &= \frac{q-1}{q^{d+1}-1}. \end{aligned}$$

我们称以上矩阵为一个 McFarland 矩阵.

2.4.2.2 Steiner MWBE 序列集

Steiner 系是组合设计领域的一个主要的研究课题[67]. 在文献[107] 中, 几个新的 MWBE 序列集的无穷类由 Steiner 系构造出来. 以下我们回顾这构造.

一个 $(2,k,v)$ Steiner 系 (Steiner system) 是一个对 $(X,\mathcal{B})$, 其中 X 一个 v 个元素(被称为点) 的集合, $\mathcal{B}$ 是一个 X 的 k-子集(被称为区组) 的集合, 使得每个点的 2-子集恰好出现在 $\mathcal{B}$ 的一个区组中.

令 $(X, \mathcal{B})$ 为一个 $(2, k, v)$ Steiner 系, 其中 $X = \{x_1, \ldots, x_v\}$ 和 $\mathcal{B} = \{B_1, \ldots, B_b\}$. 易知 $b = \frac{v(v-1)}{k(k-1)}$. $(X, \mathcal{B})$ 的关联矩阵是一个 $v \times b$ 二元矩阵 M 定义为

$$M_{i,j} = \begin{cases} 1 & \text{如果 } x_i \in B_j, \\ 0 & \text{如果 } x_i \notin B_j. \end{cases}$$

命题 2.2 (定理 1[107]): 每个 $(2, k, v)$ Steiner 系生成一个 (N, K) MWBE 序列集满足 $N = v(1 + \frac{v-1}{k-1})$ 和 $K = \frac{v(v-1)}{k(k-1)}$.

特别地, $K \times N$ 矩阵 Φ 可以如下构造:

1. 令 A 一个 $(2, k, v)$ Steiner 系的关联矩阵的转置, 规模为 $\frac{v(v-1)}{k(k-1)} \times v$.

2. 对每个 $j = 1, \ldots, v$, 令 H_j 为任意 $(1 + \frac{v-1}{k-1}) \times (1 + \frac{v-1}{k-1})$ 矩阵有正交的行和单位的元素, 例如一个复值 Hadamard 矩阵.

3. 对每个 $j = 1, \ldots, v$, 令 Φ_j 为 $\frac{v(v-1)}{k(k-1)} \times (1 + \frac{v-1}{k-1})$ 矩阵, 通过将 A 的第 j 列的非零元替换为 H_j 的不同行, 将零元替换为零行. 注意到 A 中每列存在 $\frac{v-1}{k-1}$ 个 1, 因此 H_j 中仅有 $\frac{v-1}{k-1}$ 行被选出去组成 Φ_j.

4. 将 Φ_j 合并起来生成 $\Phi = (\frac{k-1}{v-1})^{\frac{1}{2}}[\Phi_1 \cdots \Phi_v]$.

注: 以上构造可被视为文献[4,5] 中嵌入操作的一个特殊情况, 可由二元矩阵生成非二元的传感矩阵.

借助 Steiner 系, 我们有以下定理.

定理 2.7: 给定一个 $(2, k, v)$ Steiner 系, 存在一个 $\frac{v(v-1)}{k(k-1)} \times v(1 + \frac{v-1}{k-1})$ 矩阵 Φ 满足 $\mu(\Phi) = \frac{k-1}{v-1}$.

因此, 通过选择合适的 Steiner 系, 可得出传感矩阵. 特别地, 我们考虑以下四类 Steiner 系.

构造 2.7 (**仿射矩阵** (Affine matrix)): 令 q 为一个素数幂. 对 $d \geq 2$, 存在一个从仿射空间得到的 $(2, q, q^d)$ Steiner 系 [67]. 由定理 2.7, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= q^{d-1}\left(\frac{q^d-1}{q-1}\right), \\ n &= q^d\left(\frac{q^d-1}{q-1}+1\right), \\ \mu(\Phi) &= \frac{q-1}{q^d-1}. \end{aligned}$$

我们称以上矩阵为一个仿射矩阵.

构造 2.8 (**射影矩阵** (Projective matrix)): 令 q 为一个素数幂. 对 $d \geq 2$, 存在一个从射影空间得到的 $(2, q+1, \frac{q^{d+1}-1}{q-1})$ Steiner 系 [67]. 由定理 2.7, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= \frac{(q^d-1)(q^{d+1}-1)}{(q+1)(q-1)^2}, \\ n &= \frac{q^{d+1}-1}{q-1}\left(\frac{q^d-1}{q-1}+1\right), \\ \mu(\Phi) &= \frac{q-1}{q^d-1}. \end{aligned}$$

我们称以上矩阵为一个射影矩阵.

构造 2.9 (unital **矩阵**): 令 q 为一个素数幂. 对 $d \geq 2$, 存在一个从 unital 得到的 $(2, q+1, q^3+1)$ Steiner 系 [67]. 由定理 2.7, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= \frac{q^2(q^3+1)}{q+1}, \\ n &= (q^2+1)(q^3+1), \\ \mu(\Phi) &= \frac{1}{q^2}. \end{aligned}$$

我们称以上矩阵为一个 unital 矩阵.

构造 2.10 (Denniston 矩阵): 对任意 $2 \leq r < s$, 存在一个从 Denniston 设计得到的 $(2, 2^r, 2^{r+s} + 2^r - 2^s)$ Steiner 系[67]. 由定理 2.7, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= \frac{(2^s+1)(2^{r+s}+2^r-2^s)}{2^r}, \\ n &= (2^s+2)(2^{r+s}+2^r-2^s), \\ \mu(\Phi) &= \frac{1}{2^s+1}. \end{aligned}$$

我们称以上矩阵为一个 Denniston 矩阵.

2.4.3 由信号集导出的近似正交系

对一个 $m \times n$ 矩阵 Φ, 当 n 较大时, Welch 界 (2.4) 是不紧的. 更确切地, 若 Φ 是实矩阵, (2.4) 中等式仅当 $n \leq \frac{m(m+1)}{2}$ 时成立, 若 Φ 是复矩阵, (2.4) 中等式仅当 $n \leq m^2$ 时成立[257]. 当 n 较大时, 以下由 Levenstein[184] 提出的界优于 Welch 界.

如果 Φ 是一个实矩阵满足 $n > \frac{m(m+1)}{2}$, 那么

$$\mu(\Phi) \geq \sqrt{\frac{3n - m^2 - 2m}{(m+2)(n-m)}}. \tag{2.7}$$

如果 Φ 是一个复矩阵满足 $n > m^2$, 那么

$$\mu(\Phi) \geq \sqrt{\frac{2n - m^2 - m}{(m+1)(n-m)}}. \tag{2.8}$$

一个 (N, K) 信号集 (signal set) 可被视作一个 $K \times N$ 矩阵. 在同步码分多址应用中, 一个信号集被用来区分不同用户的信号. 为此, 矩阵的相关值应尽可能小. 达到 (或近似达到) Levenstein 界的信号集被称为最优的 (或近似最优) 的信号集. 在文献[91]中, 最优或近似最优的信号集由特殊的平面函数 (planar functions) 和几乎 bent 函数 (almost bent functions) 得出. 我们以下回顾这个构造.

假设 $q = p^t$, 其中 p 是一个素数且 t 是一个正整数. 我们用 $x_0, x_1, \ldots, x_{q-1}$ 记 $\mathbb{F}_q$ 的所有元素. 对任意的正整数 l, 令 ζ_l 为 l-次复单位根 $e^{\frac{2\pi i}{l}}$. 令 $tr_{q/p}$ 为 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的迹函数. 对任意 $x \in \mathbb{F}_q$, 定义

$$\psi(x) = \zeta_p^{tr_{q/p}(x)}.$$

那么 ψ 是一个 $\mathbb{F}_q$ 的加法特征.

令 $e_i^{(q)}$ 为 q-维希尔伯特空间中第 i 项为 1, 其它项为 0 的向量. 定义 $E^{(q)} = \{e_i^{(q)} \mid 1 \le i \le q\}$, 即由这些向量组成的标准正交基.

令 f 为一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的函数. 对每个对 $(a,b) \in \mathbb{F}_q^2$, 我们定义单位范数向量

$$C_f(a,b) = \frac{1}{\sqrt{q}}(\psi(af(x_0)+bx_0), \ldots, \psi(af(x_{q-1})+bx_{q-1})).$$

那么, 我们定义信号集

$$C_f = \{C_f(a,b) \mid (a,b) \in \mathbb{F}_q^2\} \cup E^{(q)}.$$

信号集 C_f 相对于 Levenstein 界是最优或近似最优的如果 f 是平面的或几乎 bent 的. 我们将在以下介绍这些概念.

2.4.3.1 由平面函数导出的最优信号集

假设 $q = p^t$, 其中 p 是一个奇素数且 t 是一个正整数. 假设 f 是一个从交换群 A 到交换群 B 的函数. f 的非线性度的度量定义如下

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \frac{|\{x \in A \mid f(x+a) - f(x) = b\}|}{|A|}.$$

显然, $P_f \ge \frac{1}{|B|}$. 一个函数 $f : A \to B$ 有完美非线性度 (perfect nonlinearity) 如果 $P_f = \frac{1}{|B|}$. 从一个有限交换群到另一个同阶的有限交换群的完美非线性函数被称为一个*平面函数* (planar function). 平面函数由 Dembowski 和 Ostrom 引入, 用于构造仿射平面[74]. 关于高非线性度函数的一个综述, 可参见[42].

以下, 我们列出一些已知的从 $\mathbb{F}_{p^t}$ 到 $\mathbb{F}_{p^t}$ 的平面函数.

1. $f(x) = x^2$;
2. $f(x) = x^{p^k+1}$, 其中 $t/\gcd(t,k)$ 为奇数[74];
3. $f(x) = x^{(3^k+1)/2}$, 其中 $p = 3$, k 为奇数且 $\gcd(t,k) = 1$[68];
4. $f(x) = x^{10} - ux^6 - u^2x^2$, 其中 $p = 3$, t 是奇数且 $u \in \mathbb{F}_{3^t}$[68,92].

关于平面函数的一个更完整的列举, 可参见[231]. 我们可以平面函数得出最优信号集.

命题 2.3 (定理 4[91]): 令 f 为一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 平面函数. 那么, C_f 是一个 (q^2+q, q) 最优信号集.

令 $m = q$, $n = q^2 + q$, Levenstein 界 (2.8) 是

$$\sqrt{\frac{2n - m^2 - m}{(m+1)(n-m)}} = \frac{1}{\sqrt{q}}.$$

因此, 我们有以下定理.

定理 2.8: 给定一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数, 存在一个 $q \times (q^2+q)$ 矩阵 Φ 满足 $\mu(\Phi) = \frac{1}{\sqrt{q}}$.

因此, 选取合适的平面函数即可得到传感矩阵.

构造 2.11 (由最优信号集导出的矩阵): 令 $q = p^t$ 其中 p 是一个奇素数且 t 是一个正整数. $f_1(x) = x^2$ 是一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数. 由定理 2.8, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= q, \\ n &= q^2 + q, \\ \mu(\Phi) &= \frac{1}{\sqrt{q}}. \end{aligned}$$

假设 k 是一个正整数满足 $t/\gcd(t,k)$ 为奇数. 那么 $f_2(x) = x^{p^k+1}$ 也是一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数. 我们可以类似得到一个相同参数的传感矩阵.

构造 2.12 (由最优信号集导出的矩阵): 令 $q = 3^t$ 其中 t 是一个正整数. 假设 k 是一个奇数且 $\gcd(t,k) = 1$. 那么 $f_3(x) = x^{(3^k+1)/2}$ 是一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数. 由定理 2.8, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= 3^t, \\ n &= 3^{2t} + 3^t, \end{aligned}$$

$$\mu(\Phi) \quad = \quad \frac{1}{\sqrt{3^t}}.$$

如果 t 是奇数, 对任意 $u \in \mathbb{F}_q$, $f_4(x) = x^{10} - ux^6 - u^2x^2$ 也是一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数. 我们可以类似得到一个相同参数的传感矩阵.

注意到由最优信号集导出的传感矩阵是基于相关值的最优的矩阵, 因为它们达到了 Levenstein 界 (2.8).

2.4.3.2　由几乎 bent 函数导出的近似最优信号集

假设 $q = 2^t$, 其中 t 是一个正整数. 此时, 不存在从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数. 对一个从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的函数 f, 我们定义

$$\lambda_f(a,b) = \sum_{x \in \mathbb{F}_q} (-1)^{tr_{2^t/2}(af(x)+bx)},$$

其中 $(a,b) \in \mathbb{F}_q^2$ 且 $tr_{2^t/2}$ 是从 $\mathbb{F}_{2^t}$ 到 $\mathbb{F}_2$ 的迹函数. f 被称为几乎 bent (almost bent) 如果 $\lambda_f(a,b) = 0$ 或 $\pm 2^{(t+1)/2}$ 对每个 (a,b) 满足 $a \neq 0$.

令 t 为奇数. 以下, 我们列举一些已知的从 $\mathbb{F}_{2^t}$ 到 $\mathbb{F}_{2^t}$ 的几乎 bent 函数.

1. Gold 函数: $f(x) = x^{2^i+1}$, 其中 $\gcd(i,t) = 1$[122,223];
2. Kasami 函数: $f(x) = x^{2^{2i}-2^i+1}$, 其中 $\gcd(i,t) = 1$[170];
3. Welch 函数: $f(x) = x^{2^{(t-1)/2}+3}$[34];
4. Niho 函数: 假设 $t = 2l+1$. $f(x) = x^{2^l+2^{l/2}-1}$, 如果 l 为偶数; $f(x) = x^{2^l+2^{(3l+1)/2}-1}$, 如果 l 为奇数[145].

我们可以由几乎 bent 函数得到近似最优信号集.

命题 2.4 (定理 4[91]): 令 f 为一个从 $\mathbb{F}_{2^t}$ 到 $\mathbb{F}_{2^t}$ 的几乎 bent 函数. 那么, C_f 是一个 $(2^{2t}+2^t, 2^t)$ 信号集, 相关值为 $\frac{1}{2^{(t-1)/2}}$.

取 $m = 2^t$, $n = 2^{2t} + 2^t$, Levenstein 界 (2.7) 为

$$\sqrt{\frac{3n - m^2 - 2m}{(m+2)(n-m)}} = \sqrt{\frac{2^{t+1}+1}{2^t(2^t+2)}} \approx \frac{1}{2^{(t-1)/2}}.$$

因此, 由几乎 bent 函数构造的信号集是近似最优的. 因此, 我们有以下定理.

定理 2.9: 给定一个从 $\mathbb{F}_{2^t}$ 到 $\mathbb{F}_{2^t}$ 的几乎 bent 函数, 存在一个 $2^t \times (2^{2t}+2^t)$ 矩阵 Φ 满足 $\mu(\Phi) = \frac{1}{2^{(t-1)/2}}$.

因此, 选取合适的几乎 bent 函数可得到传感矩阵.

构造 2.13 (**由近似最优信号集导出的矩阵**): 令 $q = 2^t$ 其中 t 是奇数. $f_1(x) = x^{2^{(t-1)/2}+3}$ 是一个从 $\mathbb{F}_{2^t}$ 到 $\mathbb{F}_{2^t}$ 的几乎 bent 函数. 由定理 2.9, 我们得到一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= 2^t, \\ n &= 2^{2t}+2^t, \\ \mu(\Phi) &= \frac{1}{2^{(t-1)/2}}. \end{aligned}$$

如果 $\gcd(i,k) = 1$, 那么 $f_2(x) = x^{2^{2i}+1}$ 和 $f_3(x) = x^{2^{2i}-2^i+1}$ 是从 $\mathbb{F}_{2^t}$ 到 $\mathbb{F}_{2^t}$ 的几乎 bent 函数. 我们可以类似得到一个相同参数的传感矩阵. 假设 $t = 2l+1$. 取 $f_4(x) = x^{2^l+2^{l/2}-1}$ 如果 l 是偶数, 取 $f_5(x) = x^{2^l+2^{(3l+1)/2}-1}$ 如果 l 是奇数. 我们可以类似得到一个相同参数的传感矩阵.

2.4.4 由相互无偏基和近似相互无偏基导出的近似正交系

相互无偏基 (mutually unbiased bases) 源自于 Schwinger 的工作[244]. 向量空间 $\mathbb{C}^d$ 的两组正交基 $\mathcal{B}$ 和 $\mathcal{B}'$ 被称为相互无偏的 (mutually unbiased) 当且仅当

$$|\langle b|b'\rangle|^2 = \frac{1}{d} \tag{2.9}$$

对任意 $b \in \mathcal{B}$ 和 $b' \in \mathcal{B}'$ 成立, 其中 $\langle\cdot|\cdot\rangle$ 是希尔伯特空间 $\mathbb{C}^d$ 中通常的内积. 对一个关于基 $\mathcal{B}'$ 的量子系统, 当我们用基 $\mathcal{B}$ 取测量它时, 不能得出任何的信息. 因此, 相互无偏基在量子信息论和量子密码中起到了重要的作用[14,15,30].

$\mathbb{C}^d$ 的任何一族相互无偏基的大小不超过 $d+1$[289]. 令 $N(d)$ 记 $\mathbb{C}^d$ 的一族相互无偏基的最大个数. 已知 $N(d) = d+1$ 当 d 是一个素数幂时成立[289]. 当 d 不是一个素数幂, 确定 $N(d)$ 是一个公开问题. 一般认为这种情况下 $d+1$ 组相互无偏基不存在[248].

因此, 通过将 (2.9) 放松到

$$|\langle b|b'\rangle|^2 = \frac{1+o(1)}{d}$$

或

$$|\langle b|b'\rangle|^2 = \frac{1+o(\log d)}{d},$$

近似相互无偏基 (approximately mutually unbiased bases) 的概念被提出[179]. 对任意非素数幂的整数 d, $d+1$ 组近似相互无偏基已被得到[179,248].

相应地, 相互无偏基和近似相互无偏基的构造给出近似正交系. 我们在以下回顾这些构造.

2.4.4.1 素数幂维希尔伯特空间中的相互无偏基

令 $\mathbb{F}_q$ 为 q 个元素的有限域, 有奇特征 p. 令 $tr_{q/p}$ 为 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的绝对迹函数. 以下命题构造了 $\mathbb{C}^q$ 中 $q+1$ 组相互无偏基, 其中 q 为一个素数幂.

命题 2.5 (定理 2[178]): 令 $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q\}$ 为一个向量的集合, 其中

$$v_{a,b} = q^{-1/2}\left(\zeta_p^{tr_{q/p}(ax^2+bx)}\right)_{x\in\mathbb{F}_q}.$$

标准基和 B_a, 其中 $a \in \mathbb{F}_q$, 形成 $\mathbb{C}^q$ 的 $q+1$ 组相互无偏基.

注: 以上得到的近似正交系是利用最优信号集的构造的特殊情况. 更确切地, 信号集 C_f 其中 $f(x) = x^2$ 是从 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的平面函数, 给出相同的近似正交系.

当 q 是一个偶素数幂, 即, $q = 2^t$ 对某个正整数 t, $q+1$ 组相互无偏基的构造利用了 Galois 环 (Galois rings). 我们简要介绍 Galois 环, 更多细节可参考[274]. 令 $\mathbb{Z}_4$ 为整数环模 4 的商环. 用 $\langle 2\rangle$ 记 $\mathbb{Z}_4[x]$ 中由 2 生成的理想. 一个首一多项式 $h(x) \in \mathbb{Z}_4[x]$ 被称为基础本原的 (basic primitive) 当且仅当典范映射下它在 $\mathbb{Z}_4[x]/\langle 2\rangle \cong \mathbb{Z}_2[x]$ 中的像是 $\mathbb{Z}_2[x]$ 中的本原多项式. 令 $h(x)$ 为一个 t 次的首一基础本原多项式. 环 $\mathrm{GR}(4,t) = \mathbb{Z}_4[x]/\langle h(x)\rangle$ 被称为 $\mathbb{Z}_4$ 上 t 次 Galois 环.

$\mathrm{GR}(4,t)$ 的构造保证了它有 4^t 个元素. 元素 $\xi = x + \langle h(x)\rangle$ 的阶为 $2^t - 1$. 定义 Teichmüller 系 (Teichmüller system) $\mathcal{T}_t = \{0, 1, \xi, \ldots, \xi^{2^t-2}\}$. 任意元素 $r \in \mathrm{GR}(4,t)$ 可被唯一的写作 $r = a + 2b$, 其中 $a, b \in \mathcal{T}_t$.

环自同构 σ: GR$(4,t) \to$ GR$(4,t)$ 定义为 $\sigma(a+2b) = a^2 + 2b^2$, 被称为 Frobenius 自同构 (Frobenius automorphism). 这个映射固定素环 $\mathbb{Z}_4$ 中的元素. GR$(4,t)$ 的所有自同构形如 σ^k, 其中 $k \geq 0$. 迹函数 Tr: GR$(4,t) \to \mathbb{Z}_4$ 定义为 $Tr(x) = \sum_{k=0}^{t-1} \sigma^k(x)$.

命题 2.6 (定理 3[178]): 令 GR$(4,t)$ 为一个 Galois 环, 有 Teichmüller 系 $\mathcal{T}_t$. 对 $a \in \mathcal{T}_t$, 记 $M_a = \{v_{a,b} \,|\, b \in \mathcal{T}_t\}$ 其中

$$v_{a,b} = 2^{-t/2} \left(i^{Tr((a+2b)x)}\right)_{x \in \mathcal{T}_t},$$

其中 $i = \sqrt{-1}$. 标准基和 M_a, 其中$a \in \mathcal{T}_t$, 形成 $\mathbb{C}^{2^t}$ 中 $2^t + 1$ 组相互无偏基.

因此, 我们有以下的构造.

构造 2.14 (由相互无偏基导出的矩阵): 令 q 为一个素数幂. 令 Φ 为命题 2.5 或命题 2.6中的 $q+1$ 个相互无偏基合并构成的矩阵. 那么 Φ 是一个 $m \times n$ 传感矩阵满足

$$\begin{aligned} m &= q, \\ n &= q^2 + q, \\ \mu(\Phi) &= \frac{1}{\sqrt{q}}. \end{aligned}$$

注: 当 q 是一个素数幂时, 构造 2.11 利用平面函数 $f_1(x) = x^2$ 构造了具有相同参数的传感矩阵. 这个构造同时包括了 q 是一个偶素数幂的情况.

注: 以上构造是 chirp 矩阵的构造[35] 的一个推广. 事实上, 对一个奇素数 p, 一个 chirp 矩阵是命题 2.5 中除去标准基的 p 组相互无偏基合并构成的矩阵.

2.4.4.2 非素数幂维希尔伯特空间中的近似相互无偏基

在希尔伯特空间 $\mathbb{C}^l$ 中, 其中 l 是一个非素数幂, $l+1$ 组近似相互无偏基已被构造出[248], 作为素数幂维中的相互无偏基的一个类似.

令 p 为最小的素数满足 $p \geq l$. 对每个 $a = 1, \ldots, l$, 我们考虑基 $\mathcal{B}_a = \{u_{a,1}, \ldots, u_{a,l}\}$, 其中

$$u_{a,b} = \frac{1}{\sqrt{l}} \left(\zeta_p^{ax^2} \zeta_l^{bx}\right)_{x=1}^{l}$$

对 $b = 1, \ldots, l$.

命题 2.7 (定理 1[248]): 标准基 $\mathcal{B}_0 = \{u_{0,1}, \ldots, u_{0,l}\}$ 和 l 组基 $\mathcal{B}_a$ 对 $a = 1, \ldots, l$ 是正交的且满足

$$|\langle u_{a,i} \mid u_{b,j} \rangle| \leq \Big(2\pi^{-\frac{1}{2}} + O\big(\frac{1}{\log l}\big)\Big)\Big(\frac{\log l}{l}\Big)^{\frac{1}{2}},$$

其中 $a, b = 0, \ldots, l$, $a \neq b$ 且 $1 \leq i, j \leq l$.

因此, 我们有以下的构造.

构造 2.15 (由近似相互无偏基导出的矩阵): 令 l 为一个非素数幂. 令 Φ 为命题 2.7 中 $l+1$ 组近似相互无偏基合并而成的矩阵. 那么 Φ 是一个 $m \times n$ 传感矩阵 Φ 满足

$$\begin{aligned} m &= l, \\ n &= l^2 + l, \\ \mu(\Phi) &= O\Big(\Big(\frac{\log l}{l}\Big)^{\frac{1}{2}}\Big). \end{aligned}$$

注意到如果 l 是一个素数幂, 这个构造与构造 2.14 相同. 由相互无偏基生成的传感矩阵的测量次数一定是一个素数幂, 相反, 由近似相互无偏基生成的传感矩阵则无此限制.

2.4.5 数值实验

在本小节中, 由近似正交系导出的传感矩阵与其它几类典型的传感矩阵进行了比较. 其中包括, 高斯 (Gaussian) 和复值高斯 (complex-valued Gaussian) 矩阵. 给定一个 $n \times n$ 离散傅立叶变换 (Discrete Fourier Transform) 矩阵, 一个 $m \times n$ 随机离散傅立叶变换 (random Discrete Fourier Transform) 矩阵由从一个离散傅立叶变换矩阵中随机抽取 m 行构成, 其中 $m < n$. 伯努利 (Bernoulli) 矩阵是一个随机矩阵其中每个元素以等概率取 1 或 -1. 由 BCH 码[4] 和 p-元 BCH 码导出的矩阵[5] 是确定性的传感矩阵. 我们的矩阵在很多数值实验中优于这些矩阵.

在实验中, 我们用 k-稀疏向量作为测试信号, 其中 k 个非零元满足标准的高斯分布. 如果传感矩阵是复值的, 我们利用 k-稀疏的复值向量作为稀疏信号, 其中每个非零分量的实部与虚部服从标准的高斯分布. 对有噪声的恢复, 一个信号 x 掺入了加

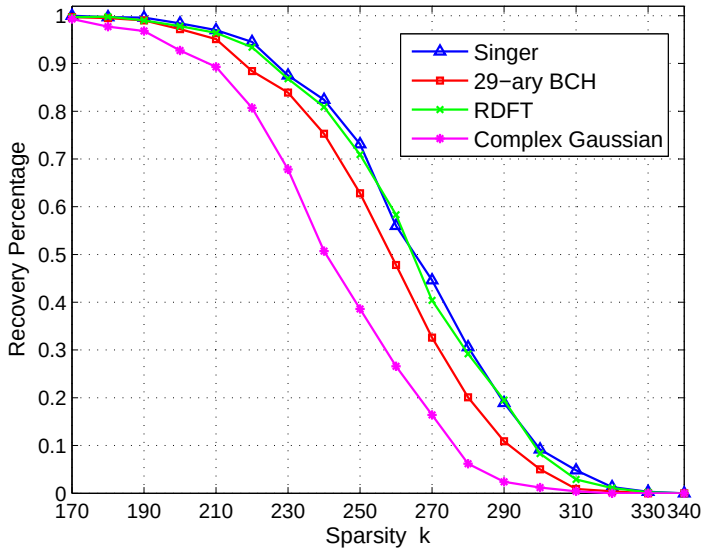

图 2.11　无噪声 7381×1 信号的完美恢复百分比. 29-元 BCH 矩阵的规模为 840×7381 且其它矩阵的规模为 820×7381.

性的高斯噪声 e, 其中信噪比是 30 dB. 因而, 给定一个传感矩阵 Φ, 我们有测量向量 $y = \Phi(x + e)$. 对每个稀疏度 (sparsity) k, 我们用正交匹配追踪作为恢复算法测试 1000 个 k-稀疏信号. 对一个信号 x, 假设 x^* 是由正交匹配追踪恢复出的信号. x 的恢复信噪比 (reconstruction SNR) 定义为

$$\text{SNR}(x) = 20 \cdot \log_{10}\big(\frac{\|x\|_2}{\|x - x^*\|_2}\big)\text{dB}.$$

首先, 我们考虑由 MWBE 序列解导出的传感矩阵. 对一个信号 x, 如果 SNR(x) 不小于 100 dB, 我们称 x 的恢复是完美的. 图 2.11 无噪声 k-稀疏 7381×1 信号的完美恢复百分比, 其中 $170 \le k \le 340$. 由构造 2.5, 一个 820×7381 Singer 矩阵可由 $(7381, 820, 91)$ Singer 差集导出. BCH 矩阵由一个 29-元 840×24389 BCH 矩阵选取前 7381 列构成. Singer 矩阵优于复值高斯和 BCH 矩阵, 和随机离散傅立叶变换矩阵相当. 有一种观点认为这个比较对 BCH 矩阵不公平, 因为它被设计为去采样长度的大得多的信号. 然而, 确定性构造总是得出一系列有固定规模的矩阵. 一般地, 很难让我们构造的矩阵与其它方法构造的矩阵具有相近的规模. 此外, 在实际应用中, 一个确定性矩阵的某些列总是被删去, 以适应信号的长度. 因此, 我们认为实验中使用从原矩阵中挑选一些列构成 BCH 矩阵是一个合理的折衷. 以下, 当类似情况发生时, 我们都将明确声明.

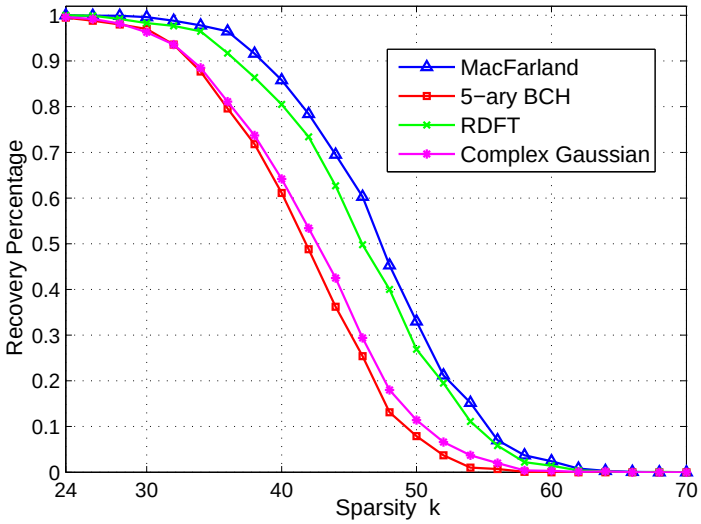

图 2.12　无噪声 1573×1 信号的完美恢复百分比. 5-元 BCH 矩阵的规模为 124×1573 且其它矩阵的规模为 132×1573.

类似地, 由构造 2.6, 一个 132×1573 McFarland 矩阵可由 $(1573, 132, 11)$ McFarland 差集导出. 此处使用的 BCH 矩阵由一个 5-元 124×78125 BCH 矩阵选取前 1573 列得出. 图 2.12 无噪声 k-稀疏 1573×1 信号的完美恢复百分比, 其中 $24 \leq k \leq 70$. McFarland 矩阵优于其它矩阵.

图 2.13 展现了有噪声 k-稀疏 1870×1 信号的恢复信噪比, 其中 $100 \leq k \leq 220$. 由构造 2.8, 一个 357×1870 射影矩阵可由 $(2, 5, 85)$ Steiner 系导出. 此处使用的 BCH 矩阵由一个 19-元 360×6859 BCH 矩阵选取前 1870 列得出. 射影矩阵优于复值高斯和 BCH 矩阵, 与随机离散傅立叶变换矩阵相当.

图 2.14 展现了无噪声 k-稀疏 3276×1 信号的完美恢复百分比, 其中 $110 \leq k \leq 250$. 由构造 2.9, 一个 525×3276 unital 矩阵可由 $(2, 6, 126)$ Steiner 系得到. BCH 矩阵由一个 23-元 528×12167 BCH 矩阵选取前 3276 列得到. unital 矩阵优于其它矩阵.

其次, 我们考虑由信号集得到的传感矩阵. 由构造 2.12, 一个 729×532170 传感矩阵可由从 $\mathbb{F}_{3^6}$ 到 $\mathbb{F}_{3^6}$ 的平面函数 $f_1(x) = x^{(3^5+1)/2}$ 导出. 我们生成前 6561 列构成传感矩阵. BCH 矩阵由一个 3-元 728×19873 BCH 矩阵选取前 6561 列得到. 图 2.15 展现了无噪声 k-稀疏 6561×1 信号的完美恢复百分比, 其中 $130 \leq k \leq 310$. 由最优信号集生成的传感矩阵优于复值高斯和 BCH 矩阵, 与随机离散傅立叶变换矩阵相当. 类似地, 一个 243×59292 传感矩阵可由从 $\mathbb{F}_{3^5}$ 到 $\mathbb{F}_{3^5}$ 的平面函数 $f_2(x) = x^{10} - x^6 - x^2$ 导出. 我们生成前 2187 列构成传感矩阵. BCH 矩阵由一个 3-元 242×59049 BCH 矩阵

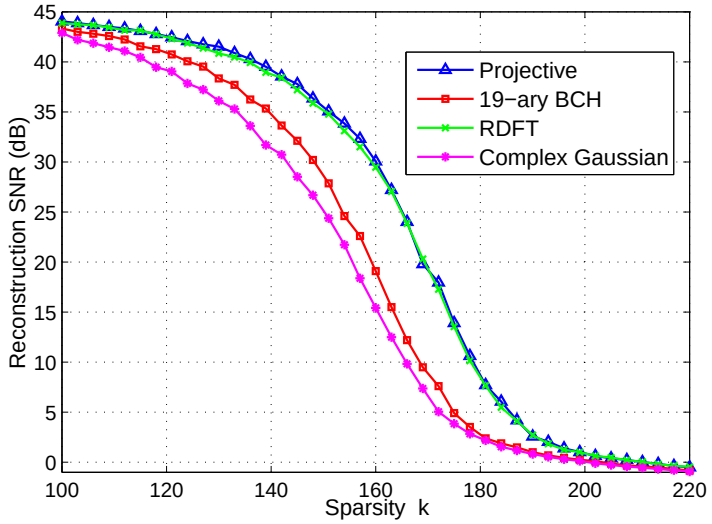

图 2.13　有噪声 1870×1 信号的恢复信噪比. 19-元 BCH 矩阵的规模为 360×1870 且其它矩阵的规模为 357×1870.

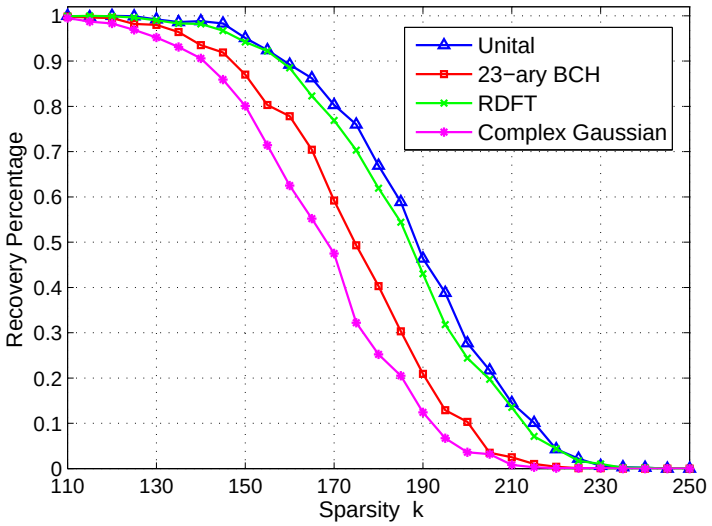

图 2.14　无噪声 3276×1 信号的完美恢复百分比. 23-元 BCH 矩阵的规模为 528×3276 且其它矩阵的规模为 525×3276.

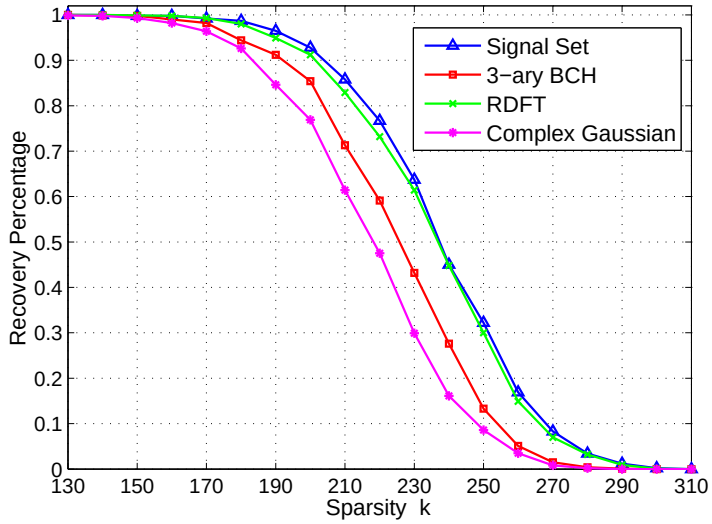

图 2.15　无噪声 6561×1 信号的完美恢复百分比. 3-元 BCH 矩阵的规模为 728×6561 且其它矩阵的规模为 729×6561.

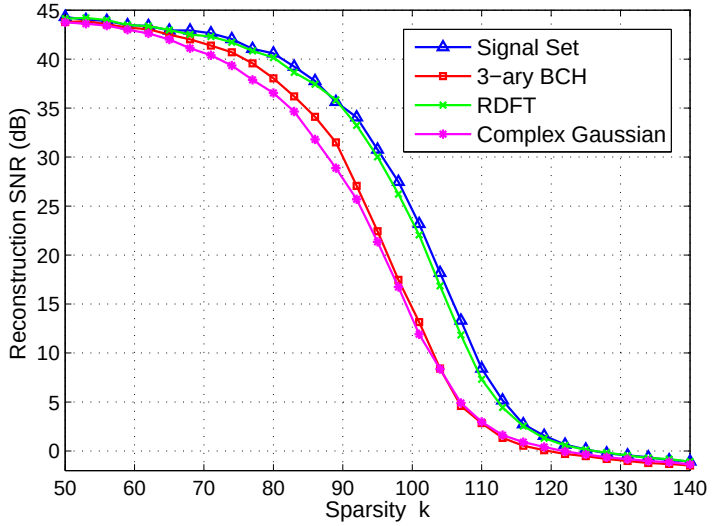

图 2.16　有噪声 2187×1 信号的恢复信噪比. 3-元 BCH 矩阵的规模为 242×2187 且其它矩阵的规模为 243×2187.

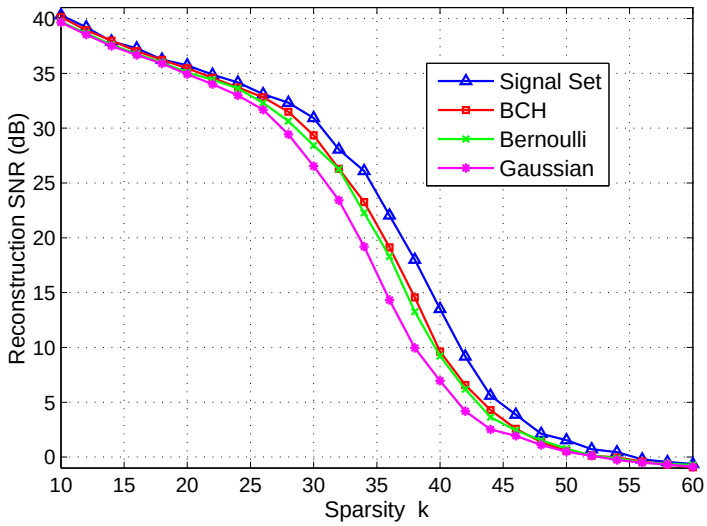

图 2.17　有噪声 1536×1 信号的恢复信噪比. BCH 矩阵的规模为 127×1536 且其它矩阵的规模为 128×1536.

选取前 2187 列得到. 图 2.16 展现了有噪声 k-稀疏 2187×1 信号的恢复信噪比, 其中 $50 \leq k \leq 140$. 由最优信号集生成的传感矩阵优于复值高斯和 BCH 矩阵, 与随机离散傅立叶变换矩阵相当.

由构造 2.12, 一个 128×16512 传感矩阵可由从 $\mathbb{F}_{2^7}$ 到 $\mathbb{F}_{2^7}$ 的 Gold 函数 $f_3(x) = x^{2^3+1}$ 导出. 我们生成前 1536 列构成传感矩阵. BCH 矩阵由一个 127×16384 BCH 矩阵选取前 1536 列得到. 图 2.17 展现了有噪声 k-稀疏 1536×1 信号的恢复信噪比, 其中 $10 \leq k \leq 60$. 由近似最优信号集生成的传感矩阵优于其它矩阵. 类似地, 一个 512×262656 传感矩阵可由从 $\mathbb{F}_{2^9}$ 到 $\mathbb{F}_{2^9}$ 的 Welch 函数 $f_4(x) = x^{2^{(9-1)/2}+3}$ 导出. 我们生成前 5120 列构成传感矩阵. BCH 矩阵由一个 511×262144 BCH 矩阵选取前 5120 列得到. 图 2.18 展现了无噪声 k-稀疏 5120×1 信号的恢复信噪比, 其中 $80 \leq k \leq 170$. 由近似最优信号集生成的传感矩阵优于其它矩阵.

最后, 我们考虑由相互无偏基和近似相互无偏基导出的传感矩阵. 由构造 2.14, 一个 169×28730 传感矩阵可由 $\mathbb{C}^{169}$ 中 170 个相互无偏基构成. 我们生成前 2197 列构成传感矩阵. 此处使用的 BCH 矩阵是一个 13-元 168×2197 BCH 矩阵. 图 2.19 展现了无噪声 k-稀疏 2197×1 信号的完美恢复百分比, 其中 $35 \leq k \leq 85$. 由相互无偏基生成的传感矩阵优于复值高斯和随机傅立叶变换矩阵矩阵, 与 BCH 矩阵相当.

由构造 2.15, 一个 324×105300 传感矩阵可由 $\mathbb{C}^{324}$ 中 325 个近似相互无偏基构成. 我们生成前 2916 列构成传感矩阵. 此处使用的 BCH 矩阵是由 7-元 342×823543

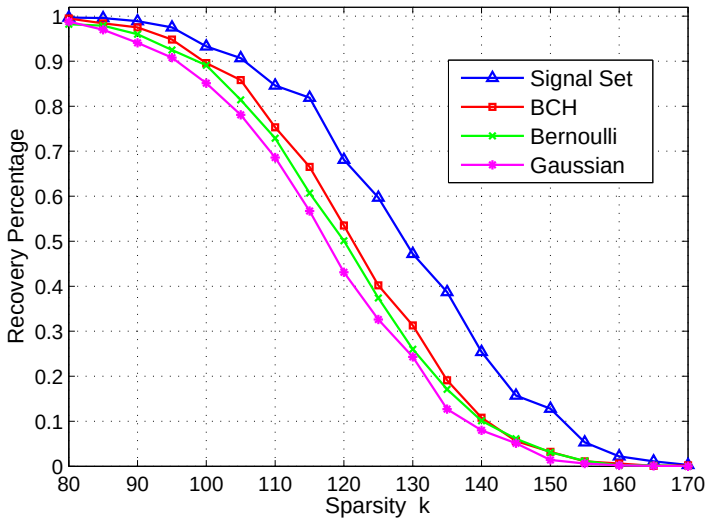

图 2.18　无噪声 5120×1 信号的完美恢复百分比. BCH 矩阵的规模为 511×5120 且其它矩阵的规模为 512×5120.

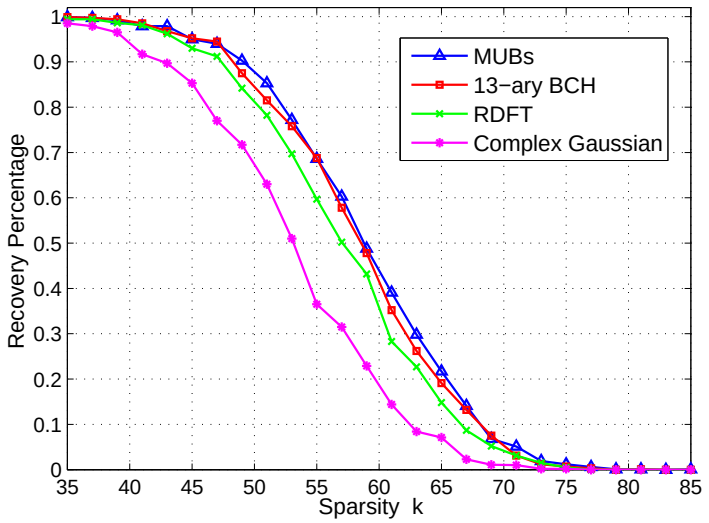

图 2.19　无噪声 2197×1 信号的完美恢复百分比. 13-元 BCH 矩阵的规模为 168×2197 且其它矩阵的规模为 169×2197.

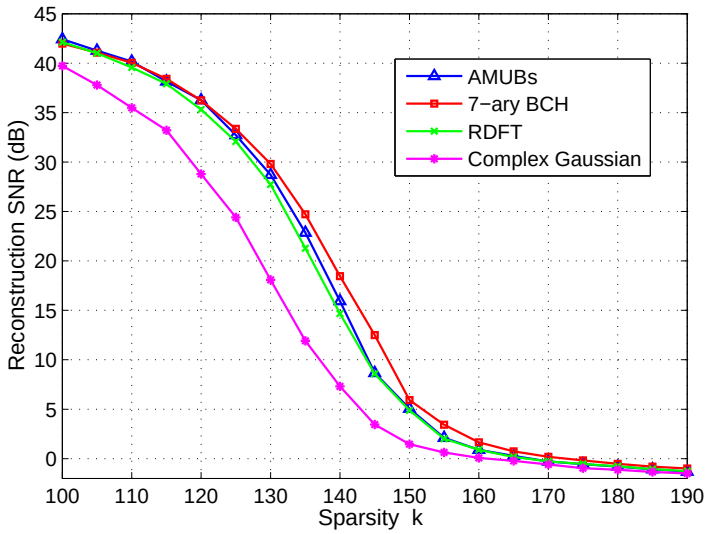

图 2.20　有噪声 2916×1 信号的恢复信噪比. 7-元 BCH 矩阵的规模为 342×2916 且其它矩阵的规模为 324×2916.

BCH 矩阵选取前 2916 列生成. 图 2.20 展现了有噪声 k-稀疏 2916×1 信号的恢复信噪比, 其中 $100 \leq k \leq 190$. 由相互无偏基生成的传感矩阵优于复值高斯矩阵, 和随机傅立叶变换矩阵相当. 同时, 它略次于 BCH 矩阵. 然而, 由于利用近似相互无偏基的构造生成了测量次数不是素数幂的传感矩阵, 它在实际中仍是有用的.

2.4.6　总结

传感矩阵的确定性构造是压缩传感中一个关键性的问题. 在本节中, 我们引进了近似正交系的概念, 这个概念事实上位于许多应用中的核心位置. 我们将近似正交系应用于压缩传感, 得到了许多类新的确定性传感矩阵. 特别地, 从 MWBE 序列集和最优信号集导出的构造得到了基于相关值的最好的确定性传感矩阵, 因为他们达到了 Welch 界或 Levenstein 界.

一系列数值实验证实了我们构造的矩阵具有良好的恢复性能. 在许多实验中, 我们的矩阵优于其它几类典型的传感矩阵. 作为确定性传感矩阵的一个优点, 特定的快速优化算法可以被设计来恢复信号. 在这个意义下, 为我们的矩阵设计比一般通用算法更有效的恢复算法是一个未来的研究课题.

3 指数和及其值分布在代数编码中的应用

3.1 Niho 指数循环码的重量分布

3.1.1 引言

循环码是一类具有良好代数性质的线性码. 循环码拥有便于实际应用的高效的编码与译码算法. 循环码已被广泛应用于通信与数据存储领域. 此外, 循环码被用来构造量子码[259] , 跳频序列[90] 等其它有趣的离散构型.

对有限域 $\mathbb{F}_p$ 上长为 l 的循环码 $\mathcal{C}$, 每个码字 $c = (c_0, \ldots, c_{l-1})$ 可被等同于一个多项式 $\sum_{i=0}^{l-1} c_i x^i \in \mathbb{F}_p[x]$. 事实上, $\mathcal{C}$ 是主理想整环 $\mathbb{F}_p[x]/(x^l - 1)$ 中的一个理想. 因此, 它可以被记做 $\mathcal{C} = (g(x))$, 其中 $g(x) \in \mathbb{F}_p[x]$ 满足 $g(x) \mid x^l - 1$ 被称为 $\mathcal{C}$ 的生成多项式 (generator polynomial). 一个循环码 $\mathcal{C}$ 被称为有 i 个零点 (zeros) 如果它的生成多项式可被分解为 $\mathbb{F}_p$ 上 i 个不可约多项式. 如果它的对偶码 $\mathcal{C}^\perp$ 有 i 个零点, 我们称 $\mathcal{C}$ 为一个有 i 个非零点 (nonzeros) 的循环码. 一个循环码 $\mathcal{C}$ 是不可约的如果它有一个非零点, 若不然, 则称之为可约的.

令 A_i 为 $\mathcal{C}$ 中汉明重量为 i 的码字个数, 其中 $0 \le i \le l$. 重量分布 $\{A_0, A_1, \ldots, A_l\}$ 是编码理论中一个重要的研究课题. 对不可约的循环码, McEliece[203] 指出它们的重量可由高斯和表出. 关于不可约循环码的重量分布已有大量文献, 可参阅一篇全面的综述[89] 和其中提到的文献.

在文献[87,88,105,106,144,185,192,193,195,196,208,271,272,275,288,292,301,302,308]中, 有少数非零点的可约循环码的重量分布已得到密集地研究. 一般地, 重量分布和一些指数和的值分布密切相关, 总的来说是很难计算的. 因而, 近年来, 关于重量分布的研究刺激了计算指数和的值分布的精妙技巧的发展. 例如, Luo 和 Feng[192,193] 提出了一个利用二次型计算值分布的方法. 他们的思想启发了一系列后续的研究工作[87,195,301,302,308]. 文献[88,196] 将循环码的重量由高斯周期表出. 这个观察引出了一系列的后续研究[105,271,272,275,292]. 总之, 受这些思想的启发, 重量分布的计算在最近取得了极大的进展.

在本节中, 我们考虑有某些有两个非零点的循环码的重量分布. 我们固定 $n = 2m$, 其中 m 是一个正整数. 令 p 为一个素数且 $q = p^n$ 为一个素数幂. 我们用 $\mathbb{F}_q$ 记 q 阶的

有限域且固定 θ 为 $\mathbb{F}_q$ 的一个本原元. 我们用 $\mathcal{C}_{q,d_1,d_2}$ 记长度为 $q-1$ 的有两个零点 θ^{d_1} 和 θ^{d_2} 的循环码. 亦即, $\mathcal{C}_{q,d_1,d_2}$ 的生成多项式为 $g_{d_1}(x)g_{d_2}(x)$, 其中 $g_i(x)$ 为 θ^i 在 $\mathbb{F}_p$ 上的极小多项式. 由 Pless 距等式[229] (Pless power moment identities), 确定 $\mathcal{C}_{q,d_1,d_2}$ 的重量分布等价于确定它的对偶码 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 的重量分布, 其中 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 是由两个非零点的可约循环码. 通常, 对偶码 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 更便于研究, 因为它有一个简单的迹表示[72].

给定一个素数 p, 一个正整数 d 是 Niho 指数 (Niho exponent) 如果 $d \equiv p^i \pmod{p^m-1}$ 对某个整数 i 成立. 不失一般性, 我们可假设 $d \equiv 1 \pmod{p^m-1}$. 对于两个 Niho 指数 $d = s(p^m-1)+1$ 和 $d' = s'(p^m-1)+1$, 称它们是等价的 (equivalent) 如果 $d' \equiv p^i d \pmod{p^n-1}$ 对某个整数 i 成立. 此外, $d' \equiv p^m d \pmod{p^n-1}$ 当且仅当 $s+s' \equiv 1 \pmod{p^m+1}$. 所以, 我们可以限制 s 在 $1 \le s \le p^{m-1}+1$ 中. 对一个 Niho 指数 $d = s(p^m-1)+1$ 满足 $(d, p^n-1) = 1$, 它的逆 $d^{-1} = s'(p^m-1)+1$ 也是一个 Niho 指数, 其中 $s' \equiv \frac{s}{2s-1} \pmod{p^m+1}$ 且 $\frac{1}{2s-1}$ 代表 $2s-1$ 模 p^m+1 的逆. Niho 指数的名称源自于 Niho 对 m-序列和它的采样序列的互相关值的研究[221]. 令 ζ_p 为 p 次复单位根. 如果 $(d_1, q-1) = (d_2, q-1) = 1$, $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 的重量分布可从以下指数和的值分布得到,

$$\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_n(ax+x^{d_1^{-1}d_2})}, \quad a \in \mathbb{F}_q.$$

这等价于一个 m-序列和它的采样为 Niho 指数 $d_1^{-1}d_2$ 的采样序列的互相关值分布.

值得注意的是, 有一些文献考虑了具有 Niho 指数的循环码. Charpin[49] 考虑了 $\mathcal{C}^{\perp}_{2^n,d_1,1}$ 的重量分布, 其中 $(d_1, 2^n-1) = 1$. 这个码至少有四个非零重量. Li 等人[185] 考虑了一类具有三个 Niho 指数非零点的循环码, 并得出了重量分布.

本节考虑循环码 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 的重量分布, 其中 d_1 和 d_2 均为 Niho 指数. 我们指出 Niho 指数 d_1 和 d_2 并不一定与 $q-1$ 互素. 通过对 d_1 和 d_2 提出具体的条件, 我们得到了两类二元码和一类非二元码的重量分布. 重量分布通过计算以下指数和的值分布得到:

$$S(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(ax^{2^m+1})+\mathrm{Tr}_n(bx^{d_2})}$$

和

$$T(a,b) = \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_n(ax^{d_1}+bx^{d_2})},$$

其中 Tr_m (或 Tr_n) 是从 $\mathbb{F}_{p^m}$ (或 $\mathbb{F}_q$) 到 $\mathbb{F}_p$ 的绝对迹函数. 此外, 我们列举了若干个例子说明我们得到的一些二元码是最优的或具有已知最好的参数.

3.1.2 预备知识

本小节中包括了一些预备知识. 在第一部分, 我们规定了一些符号. 在第二部分, 我们介绍了 Delsarte 和 Niho 定理. 基于 Delsarte 定理, 确定重量分布可以转化为确定某些指数和的值分布. 同时, Niho 定理建立了这些指数和与某些方程的界的个数之间一个美妙的联系. 因此, 我们可以通过分析某些方程来确定指数和的值. 在第三部分, 我们介绍一些距等式. 这些距等式用来确定这些值的次数.

3.1.2.1 一些符号

在本子节中, 我们确定一些本节中通篇使用的符号. 令 m 为一个正整数且 $n = 2m$. 令 p 为一个素数且 $q = p^n$. 令 $\mathbb{F}_q$ 为 q 阶的有限域且 θ 为 $\mathbb{F}_q$ 的一个本原元. 定义 $\mathbb{F}_q$ 中的非零平方元 (或非平方元) 的集合为 Q (或 NQ). 当 p 是一个奇素数, 对每个 $x \in Q$, $\mathbb{F}_q^*$ 存在恰好两个元素, 它们的平方等于 x. 记这两个元素为 $\pm x^{\frac{1}{2}}$.

定义 $S = \{x \in \mathbb{F}_q | x\bar{x} = 1\}$, 其中 $\bar{x} = x^{p^m}$. 因此, S 是一个阶为 $p^m + 1$ 的循环群. 此外, 对任意的正整数 l, 我们令 $S_l = \{x^l \mid x \in S\}$.

给定一个正整数 d, 我们用 $cl(d)$ 记最小的的正整数 k 使得 $2^k d \equiv d \pmod{2^n - 1}$.

我们用 Tr_n (或 Tr_m) 记从 $\mathbb{F}_q$ (或 $\mathbb{F}_{p^m}$) 到 $\mathbb{F}_p$ 的绝对迹函数. 令 ζ_p 记 p 次复单位根. 我们考虑以下的指数和:

$$S(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(ax^{2^m+1}) + \mathrm{Tr}_n(bx^{d_2})}$$

和

$$T(a,b) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_n(ax^{d_1} + bx^{d_2})}.$$

为了清楚起见, 我们记

$$T_1(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax^{d_1} + bx^{d_2})}$$

和

$$T_2(a,b) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_n(ax^{d_1} + bx^{d_2})},$$

其中 $T_2(a,b)$ 中 p 是一个奇素数.

3.1.2.2 Delsarte 定理和 Niho 定理

对一个循环码 $\mathcal{C}^{\perp}_{q,d_1,d_2}$, 它的码字有一个很好的迹表示. 更确切地, 由 Delsarte 定理[72], 我们有

$$\mathcal{C}^{\perp}_{q,d_1,d_2} = \{c(a,b) = (\mathrm{Tr}_n(a\theta^{id_1} + b\theta^{id_2}))_{i=0}^{q-2} \mid a,b \in \mathbb{F}_q\}.$$

一个码字 $c(a,b)$ 的汉明重量可表为

$$\begin{aligned} w_H(c(a,b)) &= (q-1) - \frac{1}{p}\sum_{x\in\mathbb{F}_q^*}\sum_{\lambda\in\mathbb{F}_p} \zeta_p^{\lambda \mathrm{Tr}_n(ax^{d_1}+bx^{d_2})} \\ &= (q-1)(1-\frac{1}{p}) - \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}_n(\lambda ax^{d_1}+\lambda bx^{d_2})}. \end{aligned}$$

因而, 重量分布可由以下指数和的值分布得到

$$\sum_{x\in\mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}_n(ax^{d_1}+bx^{d_2})}, \quad a,b \in \mathbb{F}_q.$$

下面, 我们将看到当 d_1 和 d_2 是 Niho 指数, 这个指数和可能的取值由某些方程的解的个数确定.

以下引理实质上由 Niho 在 $p=2$ 的情形下提出[221]. 它可被视作引理 2[186] 的一个特殊情形. 此处, 我们给出一个简短的证明.

引理 3.1: 令 p 为一个素数且 $q = p^n$.

1) 对 $p=2$, 如果 $d_2 = s_2(2^m-1)+1$, 我们有 $S(a,b) = (U(a,b)-1)2^m$, 其中 $U(a,b)$ 是 $z \in S$ 的个数满足

$$\bar{b}z^{2(2s_2-1)} + a^{\frac{1}{2}}z^{2s_2-1} + b = 0.$$

2) 对 $p=2$, 如果 $d_1 = s_1(2^m-1)+1$ 且 $d_2 = s_2(2^m-1)+1$, 我们有 $T_1(a,b) = (V(a,b)-1)2^m$, 其中 $V(a,b)$ 是$z \in S$ 的个数满足

$$\bar{b}z^{2s_2-1} + \bar{a}z^{s_1+s_2-1} + az^{s_2-s_1} + b = 0.$$

3) 令 p 为一个素数. 假设 $d_1 = s_1(p^m-1)+1$ 且 $d_2 = s_2(p^m-1)+1$. 那么对任意 $\lambda \in \mathbb{F}_p^*$, 我们有 $T_2(\lambda a, \lambda b) = (W(a,b)-1)p^m$, 其中 $W(a,b)$ 是 $z \in S$ 的个数满足

$$\bar{b}z^{2s_2-1} + \bar{a}z^{s_1+s_2-1} + az^{s_2-s_1} + b = 0.$$

证明. 这三个情况可以统一证明. 定义 $\Omega = \{\theta^i | 0 \le i \le p^m\}$. 每个 $x \in \mathbb{F}_{p^n}^*$, 可以唯一表为 $x = y\omega$, 其中 $y \in \mathbb{F}_{p^m}^*$ 且 $\omega \in \Omega$. 因而, 对任意的 $\lambda \in \mathbb{F}_p^*$, 我们有

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_n(\lambda a x^{d_1} + \lambda b x^{d_2})} \\
&= 1 + \sum_{y\in\mathbb{F}_{p^m}^*} \sum_{\omega\in\Omega} \zeta_p^{\mathrm{Tr}_n(\lambda(ay\omega^{d_1} + by\omega^{d_2}))} \\
&= 1 - |\Omega| + \sum_{\omega\in\Omega} \sum_{y\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_m((a\omega^{d_1} + \bar{a}\bar{\omega}^{d_1} + b\omega^{d_2} + \bar{b}\bar{\omega}^{d_2})\lambda y)} \\
&= (N(a,b)-1)p^m,
\end{aligned}$$

其中

$$N(a,b) = |\{\omega \in \Omega | a\omega^{d_1} + \bar{a}\bar{\omega}^{d_1} + b\omega^{d_2} + \bar{b}\bar{\omega}^{d_2} = 0\}|.$$

注意当 $\omega^{d_i-1} = \omega^{(p^m-1)s_i}$ 和 $\bar{\omega}^{d_i}/\omega = \omega^{(p^m-1)(1-s_i)}$. 令 $z = \omega^{p^m-1}$, 我们有

$$N(a,b) = |\{z \in S | az^{s_1} + \bar{a}z^{1-s_1} + bz^{s_2} + \bar{b}z^{1-s_2} = 0\}|.$$

因此, 一个简单的计算可得出结果. □

3.1.2.3 一些距等式

我们用 $N_2(q, d_1, d_2)$ 以下方程组解的个数

$$\begin{cases} x^{d_1} + y^{d_1} = 0 \\ x^{d_2} + y^{d_2} = 0 \end{cases}, \quad x, y \in \mathbb{F}_q. \tag{3.1}$$

类似地, 用 $N_3(q, d_1, d_2)$ 记以下方程组的解的个数

$$\begin{cases} x^{d_1} + y^{d_1} + z^{d_1} = 0 \\ x^{d_2} + y^{d_2} + z^{d_2} = 0 \end{cases}, \quad x, y, z \in \mathbb{F}_q. \tag{3.2}$$

下面的距等式在确定重量分布中起到重要的作用.

引理 3.2: 令 p 为一个奇素数且 $q = p^n$. 那么我们有

1) $\sum_{a\in\mathbb{F}_{2^m}} \sum_{b\in\mathbb{F}_{2^n}} S(a,b) = 2^{3m}$.

2) $\sum_{a\in\mathbb{F}_{2^m}} \sum_{b\in\mathbb{F}_{2^n}} S(a,b)^2 = 2^{3m} N_2(2^n, 2^m+1, d_2)$.

3) $\sum_{a,b\in\mathbb{F}_{2^n}} T_1(a,b) = 2^{2n}$.

4) $\sum_{a,b\in\mathbb{F}_{2^n}} T_1(a,b)^2 = 2^{2n} N_2(2^n, d_1, d_2)$.

5) $\sum_{a,b\in\mathbb{F}_{2^n}} T_1(a,b)^3 = 2^{2n} N_3(2^n, d_1, d_2)$.

6) $\sum_{a,b\in\mathbb{F}_q} T_2(a,b) = p^{2n}$.

7) $\sum_{a,b\in\mathbb{F}_q} T_2(a,b)^2 = p^{2n} N_2(q, d_1, d_2)$.

8) $\sum_{a,b\in\mathbb{F}_q} T_2(a,b)^3 = p^{2n} N_3(q, d_1, d_2)$.

证明. 证明是常规的, 类似于引理 4[195]. 我们在此略去. □

因此, 如果我们能计算某些方程组的界的个数, 就可以得到这些距等式的精确信息.

3.1.3 二元 Niho 指数的循环码

考虑一个 Niho 指数 $d = s(2^m-1)+1$, 容易验证

$$cl(d) = \begin{cases} m & \text{如果 } s \equiv \frac{1}{2} \pmod{2^m+1}, \\ n & \text{其它}, \end{cases}$$

其中 $\frac{1}{2}$ 代表 2 模 2^m+1 的逆.

本小节考虑二元 Niho 指数的循环码的重量分布. 第一部分研究 $\mathcal{C}^{\perp}_{2^n,d_1,d_2}$ 的重量分布, 其中 $cl(d_1) = m$ 且 $cl(d_2) = n$. 为此, 我们计算 $S(a,b)$ 的值分布. 第二部分, 我们考虑 $\mathcal{C}^{\perp}_{2^n,d_1,d_2}$ 的重量分布, 其中 $cl(d_1) = cl(d_2) = n$. 通过对 d_1 和 d_2 提出条件, 我们得到 $T_1(a,b)$ 的值分布. 因而, 相应的循环码的重量分布立即可得.

3.1.3.1 $S(a,b)$ 的值分布和相关的循环码

本子节中, 我们考虑 $S(a,b)$ 的值分布, 其中 $d_2 = s_2(2^m-1)+1$. 为了保证 2^m+1 和 d_2 不等价, 我们有 $s_2 \not\equiv \frac{1}{2} \pmod{2^m+1}$. 作为准备, 我们有以下的引理.

引理 3.3: 假设 $q = 2^n$ 和 $l = (2s_2-1, 2^m+1)$. 那么 $N_2(q, 2^m+1, d_2) = (2^n-1)l+1$.

证明. 由定义, $N_2(q, 2^m+1, d_2)$ 以下方程组的解的个数

$$\begin{cases} x^{2^m+1} + y^{2^m+1} = 0 \\ x^{d_2} + y^{d_2} = 0 \end{cases}, \quad x, y \in \mathbb{F}_q. \tag{3.3}$$

当 $y=0$, 我们有一个解 $(x,y)=(0,0)$. 当 $y \in \mathbb{F}_{2^n}^*$, 令 $z = \frac{x}{y}$, 我们只需考虑方程组

$$\begin{cases} z^{2^m+1} = 1 \\ z^{d_2} = 1 \end{cases}, \quad z \in \mathbb{F}_q. \tag{3.4}$$

(3.4) 的每个解对应于 (3.3) 的 2^n-1 个解. 由于 $l = (2s_2-1, 2^m+1) = (d_2, 2^m+1)$, (3.4) 等价于 $z^l = 1$, 在 $\mathbb{F}_q$ 中恰好有 l 个解. 因而我们得出 $N_2(q, 2^m+1, d_2) = (2^n-1)l+1$. □

我们现在决定以下指数和的值分布

$$S(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(ax^{2^m+1}) + \mathrm{Tr}_n(bx^{d_2})}.$$

定理 3.1: 假设 $n = 2m$, 其中 $m \geq 1$. 定义 $d_2 = s_2(2^m-1)+1$, 其中 $s_2 \not\equiv \frac{1}{2} \pmod{2^m+1}$. 令 $q = 2^n$ 和 $l = (2s_2-1, 2^m+1)$. 那么 $S(a,b)$ 的值分布列在表 3.1.

证明. 由引理 3.1 的 1), 我们有 $S(a,b) = (U(a,b)-1)2^m$, 其中 $U(a,b)$ 是 $z \in S$ 的个数满足

$$\bar{b} z^{2(2s_2-1)} + a^{\frac{1}{2}} z^{2s_2-1} + b = 0.$$

当 $(a,b) = (0,0)$, 易知 $U(a,b) = 2^m+1$ 且 $S(a,b)$ 取平凡的值 2^{2m}. 以下我们考虑 $(a,b) \neq (0,0)$ 的情形. 令 $u = z^{2s_2-1}$, 等式变为

$$\bar{b} u^2 + a^{\frac{1}{2}} u + b = 0,$$

表 3.1　定理 3.1 的值分布

值	次数
2^{2m}	1
$(2l-1)2^m$	$\frac{(2^{2m}-1)(2^m-l+1)}{2l^2}$
$(l-1)2^m$	$\frac{(2^{2m}-1)((2^m+2)l-2^m-1)}{l^2}$
-2^m	$2^{3m}-1+\frac{(2^{2m}-1)(2^m+1-(2^{m+1}+3)l)}{2l^2}$

表 3.2　定理 3.2 的重量分布

重量	次数
0	1
$2^{2m-1}-(2l-1)2^{m-1}$	$\frac{(2^{2m}-1)(2^m-l+1)}{2l^2}$
$2^{2m-1}-(l-1)2^{m-1}$	$\frac{(2^{2m}-1)((2^m+2)l-2^m-1)}{l^2}$
$2^{2m-1}+2^{m-1}$	$2^{3m}-1+\frac{(2^{2m}-1)(2^m+1-(2^{m+1}+3)l)}{2l^2}$

它有 $0,1$ 或 2 个根在 S_l 中. 由于 $l=(2s_2-1,2^m+1)$, 对任意 $u\in S_l$, 方程 $z^{2s_2-1}=u$ 恰有 l 个解在 S 中. 因而, 我们有 $U(a,b)\in\{0,l,2l\}$ 当 $(a,b)\neq(0,0)$. 所以, 当 $(a,b)\neq(0,0)$, $S(a,b)$ 取三个不同的值 $\{-2^m,(l-1)2^m,(2l-1)2^m\}$. 这些值的次数可由引理 3.2 和引理 3.3 得到. □

作为定理 3.1 的直接结果, 我们得到一类二元循环码的重量分布.

定理 3.2: 假设 $n=2m$ 其中 $m\geq 1$. 定义 $d_1=2^m+1$ 和 $d_2=s_2(2^m-1)+1$ 满足 $s_2\not\equiv\frac{1}{2}\pmod{2^m+1}$. 令 $q=2^n$ 且 $l=(2s_2-1,2^m+1)$. 那么 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 是一个 $[2^n-1,3m,2^{2m-1}-(2l-1)2^{m-1}]$ 二元码. 它的重量分布列在表 3.2.

给定 m, 上述的码由一个参数 s_2 确定. 我们称由 Grassl[119] 维护的线性码的表为码表. 我们给出一些例子展示上述的定理. 根据码表, 其中有一些码是最优的线性码.

例 3.1: 当 $m=2$, 我们有 $s_2\in\{1,2\}$. 那么 $l=(2s_2-1,2^m+1)=1$ 对 s_2 的两个选择

都成立. 相应的两个循环码为 $[15,6,6]$ 二元码, 有重量分布:

$$1+30x^6+15x^8+18x^{10}.$$

根据码表[119], 这些循环码是最优的.

例 3.2: 当 $m=3$, 我们有 $s_2\in\{1,2,3,4\}$. 进一步, 我们有 $l=(2s_2-1,2^m+1)=1$ 对 $s_2\in\{1,3,4\}$. 相应的三个循环码为 $[63,9,28]$ 二元码, 有重量分布:

$$1+252x^{28}+63x^{32}+196x^{36}.$$

根据码表[119], 这些循环码是最优的.

3.1.3.2 $T_1(a,b)$ 的值分布和相关的循环码

我们在一个特殊情形下计算 $T_1(a,b)$ 的值分布. 在本子节中, 我们固定 $d_1=s_1(2^m-1)+1$ 和 $d_2=s_2(2^m-1)+1$ 其中 $s_1=2^{k-1}t-\frac{t-1}{2}$, $s_2=2^{k-1}t+\frac{t+1}{2}$ 对某个正整数 k 和某个奇数 $t\geq 1$. 为了确保 d_1,d_2 不等价且 $cl(d_1)=cl(d_2)=n$, 我们有 $(2^k-1)t,(2^k+1)t\not\equiv 0 \pmod{2^m+1}$. 我们称两对 Niho 指数 (d_1,d_2) 和 (d_1',d_2') 等价 (equivalent) 如果 (d_1,d_1') 和 (d_2,d_2') 分别等价或 (d_1,d_2') 和 (d_2,d_1') 分别等价. 令 $s_1=2^{k-1}t-\frac{t-1}{2}$, $s_2=2^{k-1}t+\frac{t+1}{2}$, $s_1'=2^{k+m-1}t-\frac{t-1}{2}$ 且 $s_2'=2^{k+m-1}t+\frac{t+1}{2}$. 易知 $s_1+s_2'\equiv 1 \pmod{2^m+1}$ 且 $s_1'+s_2\equiv 1 \pmod{2^m+1}$. 亦即, k 和 $k+m$ 给出两对等价的 Niho 指数. 因而, 我们可将 k 限制在范围 $1\leq k\leq m$ 中. 通过类似的分析, 我们可以不失一般性地假设 $1\leq t\leq 2^m+1$. 以下, 我们将假设更多的条件以确定 $T_1(a,b)$ 的值分布.

作为一个准备, 我们有以下的引理.

引理 3.4: 假设 $q=2^n$ 且 $l=(t,2^m+1)$. 那么

1) $N_2(q,d_1,d_2)=(2^n-1)l+1$.

2) $N_3(q,d_1,d_2)=(2^m-2)(2^n-1)l^2+3(2^n-1)l+1$.

证明. 1) 注意到

$$(d_1,2^n-1)=((2^k-1)t,2^m+1)$$

和

$$(d_2, 2^n - 1) = ((2^k + 1)t, 2^m + 1).$$

那么, l 整除 $(d_1, 2^n-1)$ 和 $(d_2, 2^n-1)$. 进一步, 我们有 $(d_1, 2^n-1) = l$ 或 $(d_2, 2^n-1) = l$. 因此, 方程组

$$\begin{cases} u^{d_1} = 1 \\ u^{d_2} = 1 \end{cases}$$

恰有 l 个解. 用引理 3.3 的证明中的想法, 余下的证明是常规的.

2) 由定义, $N_3(q, d_1, d_2)$ 以下方程组的解的个数

$$\begin{cases} x^{d_1} + y^{d_1} + z^{d_1} = 0 \\ x^{d_2} + y^{d_2} + z^{d_2} = 0 \end{cases}, \quad x, y, z \in \mathbb{F}_q. \tag{3.5}$$

当 $z = 0$, 有 $N_2(q, d_1, d_2) = (2^n - 1)l + 1$ 个解.

当 $z \neq 0$, 情况更加复杂. 令 $u = \frac{x}{z}$ 和 $v = \frac{y}{z}$, 我们只需考虑方程组

$$\begin{cases} u^{d_1} + v^{d_1} = 1 \\ u^{d_2} + v^{d_2} = 1 \end{cases}, \quad u, v \in \mathbb{F}_q. \tag{3.6}$$

(3.6) 的每个解对应于 (3.5) 的 $2^n - 1$ 个解. 如果 $u = 0$ 或 $v = 0$, 由 1) 的证明, (3.6) 恰有 l 个解. 如果 $uv \neq 0$, 由极表示, u 和 v 可被唯一的表为 $u = \alpha\delta$ 和 $v = \beta\gamma$, 其中 $\alpha, \beta \in \mathbb{F}_{2^m}^*$ 且 $\delta, \gamma \in S$. 所以 (3.6) 等价于

$$\begin{cases} \alpha\delta^{-t(2^k-1)} + \beta\gamma^{-t(2^k-1)} = 1 \\ \alpha\delta^{-t(2^k+1)} + \beta\gamma^{-t(2^k+1)} = 1 \end{cases}. \tag{3.7}$$

注意到

$$\begin{aligned} \Delta &= \begin{vmatrix} \delta^{-t(2^k-1)} & \gamma^{-t(2^k-1)} \\ \delta^{-t(2^k+1)} & \gamma^{-t(2^k+1)} \end{vmatrix} \\ &= \delta^{-t(2^k-1)}\gamma^{-t(2^k+1)} - \delta^{-t(2^k+1)}\gamma^{-t(2^k-1)}. \end{aligned}$$

以下, 我们将分两种情况讨论.

如果 $\Delta = 0$, 我们有 $\delta^t = \gamma^t$. 与 (3.7) 比较, 我们有 $\delta^t = \gamma^t = 1$ 且 (3.7) 退化为 $\alpha + \beta = 1$. 注意到有 l^2 个对 (δ, γ) 满足 $\delta^t = \gamma^t = 1$. 进而, 对每个对 (δ, γ), 存在 $2^m - 2$ 个对 (α, β), 满足 $\alpha + \beta = 1$ 且 $\alpha\beta \neq 0$. 因此, 这个情况有 $(2^m - 2)l^2$ 个解.

如果 $\Delta \neq 0$, 亦即, $\delta^t \neq \gamma^t$, 解 (3.7) 得

$$\alpha = \frac{1+\gamma^{2t}}{\delta^{-t(2^k-1)}(1+\delta^{-2t}\gamma^{2t})},$$
$$\beta = \frac{1+\delta^{2t}}{\gamma^{-t(2^k-1)}(1+\delta^{2t}\gamma^{-2t})}.$$

我们将要证明这种情况没有解. 由于 $\alpha \in \mathbb{F}_{2^m}^*$, 我们有 $\alpha = \bar{\alpha}$, 这导出了 $\delta^t = 1$. 类似地, 由于 $\beta \in \mathbb{F}_{2^m}^*$, 我们得到 $\gamma^t = 1$. 因此, 我们有 $\delta^t = \gamma^t = 1$, 这和 $\Delta \neq 0$ 矛盾. 因此, 当 $\Delta \neq 0$ 时没有解.

总结一下, 我们推出了 $N_3(q, d_1, d_2) = (2^n-1)l + 1 + (2^n-1)((2^m-2)l^2 + 2l) = (2^m-2)(2^n-1)l^2 + 3(2^n-1)l + 1$. □

以下由 Dobbertin 等人[97] 提出的引理描述了某些方程可能的解的个数.

引理 3.5 (引理 22[97]): *对 $a, b, c \in \mathbb{F}_{2^n}$, 方程*

$$x^{2^r+1} + ax^{2^r} + bx + c = 0$$

有 $0, 1, 2$ 或 $2^{r_0}+1$ 个解在 $\mathbb{F}_{2^n}$ 中, 其中 $r_0 = (r, n)$.

对任意 $z \in S$ 和 $a, b \in \mathbb{F}_q$ 满足 $a\bar{a} + b\bar{b} \neq 0$, 我们定义 S 上的分式线性变换 (fractional linear transformation)

$$\Phi_{a,b}(z) = \frac{az+b}{\bar{b}z+\bar{a}}.$$

容易验证分式线性变换是良定的且在 S 上诱导了一个置换. 特别地, 两个分式线性变换的复合仍然是一个分式线性变换. 更确切地, 我们有

$$\Phi_{a_3,b_3} = \Phi_{a_1,b_1}\Phi_{a_2,b_2},$$

其中

$$\begin{pmatrix} a_3 & b_3 \\ \bar{b}_3 & \bar{a}_3 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ \bar{b}_1 & \bar{a}_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ \bar{b}_2 & \bar{a}_2 \end{pmatrix}$$

且

$$a_3\bar{a}_3 + b_3\bar{b}_3 = (a_1\bar{a}_1 + b_1\bar{b}_1)(a_2\bar{a}_2 + b_2\bar{b}_2) \neq 0.$$

现在我们考虑以下指数和的值分布

$$T_1(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax^{d_1}+bx^{d_2})}.$$

定理 3.3: 令 $p=2, q=2^n$ 且 $n=2m$ 满足 $m\geq 2$. 给定一个正整数 $1\leq k\leq m$, 令 $s_1 = 2^{k-1}t - \frac{t-1}{2}$ 和 $s_2 = 2^{k-1}t + \frac{t+1}{2}$ 其中 $1\leq t\leq 2^m+1$ 为奇数. 定义 $d_1 = s_1(2^m-1)+1$ 和 $d_2 = s_2(2^m-1)+1$. 假设 $(2^k-1)t, (2^k+1)t \not\equiv 0 \pmod{2^m+1}$ 且 $l=(t,2^m+1)$. 如果以下条件之一成立:

i) $m\equiv -1 \pmod{k}$,

ii) $(k,2m)=1$,

那么 $T_1(a,b)$ 的值分布列在表 3.3.

证明. 由引理 3.1 的 2), 我们有 $T_1(a,b) = (V(a,b)-1)2^m$, 其中 $V(a,b)$ 是 $z\in S$ 的个数满足

$$\bar{b}z^{(2^k+1)t} + \bar{a}z^{2^kt} + az^t + b = 0. \tag{3.8}$$

如果 $(a,b)=(0,0)$, 易知 $V(a,b)=2^m+1$ 且 $T_1(a,b)$ 取平凡值 2^{2m}. 我们将证明 $T_1(a,b)$ 取至多四个值, 如果 i) 或 ii) 成立.

令 $w=z^t$, (3.8) 成为

$$\bar{b}w^{2^k+1} + \bar{a}w^{2^k} + aw + b = 0. \tag{3.9}$$

由于 $l=(t,2^m+1)$, $w\in S_l$ 中 (3.9) 的每个解对应于 (3.8) 的 l 个解. 以下, 我们专注于 (3.9) 并研究它在 S_l 中的解的个数.

首先, 假设 i) 成立. 如果 $a\neq 0$ 且 $b=0$, 我们有 $\bar{a}w^{2^k-1}+a=0$, 蕴含了 $w^{2^k-1} =$

$\frac{a}{\bar{a}} \in S$. 注意到 $m \equiv -1 \pmod{k}$, 容易验证

$$(2^k - 1, 2^m + 1) = \begin{cases} 1 & \text{如果 } k \text{ 是奇数,} \\ 3 & \text{如果 } k \text{ 是偶数.} \end{cases}$$

因此, (3.9) 有不超过 3 个解在 S_l 中. 类似地可说明 (3.9) 有不超过 3 个解在 S_l 中, 当 $a = 0$ 且 $b \neq 0$. 如果 $ab \neq 0$, 我们将利用命题 1[96] 中的技巧进行分析. 假设 $a\bar{a} + b\bar{b} = 0$, 我们有 $(\bar{b}w^{2^k} + a)(w + \frac{b}{a}) = 0$, 它有不超过 2 个解在 S_l 中. 当 $a\bar{a} + b\bar{b} \neq 0$, 我们考虑以下的分式线性变换:

$$\Phi_{a,b}(w) = \frac{aw + b}{\bar{b}w + \bar{a}}.$$

由 (3.9), 我们有

$$w^{2^k} = \frac{aw + b}{\bar{b}w + \bar{a}} = \Phi_{a,b}(w).$$

由于 $m \equiv -1 \pmod{k}$, 存在一个整数 i 使得 $ki = m + 1$. 在上式两边作用变换 $\Phi_{a,b}$ $i - 1$ 次, 我们得到

$$w^{2^{ki}} = \Phi_{a',b'}(w),$$

其中

$$\begin{pmatrix} a' & b' \\ \bar{b}' & \bar{a}' \end{pmatrix} = \begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix}^i.$$

对 $w \in S$, 我们有 $w^{2^{ki}} = w^{2^{m+1}} = w^{-2}$. 因此

$$a'w^3 + b'w^2 + \bar{b}'w + \bar{a}' = 0.$$

所以, (3.9) 有不超过 3 个解在 S_l 中. 总结一下, 当 $(a, b) \neq (0, 0)$, (3.9) 有 $0, 1, 2$ 或 3 个解在 S_l 中. 这蕴含了 $V(a, b) \in \{0, l, 2l, 3l\}$ 当 $(a, b) \neq (0, 0)$.

其次, 假设 ii) 成立. 如果 $b = 0$, (3.9) 成为 $\bar{a}w^{2^k-1} + a = 0$. 由于 $(k, 2m) = 1$, 易知它有不超过 1 个解在 S_l 中. 如果 $b \neq 0$, 由引理 3.5, (3.9) 有 $0, 1, 2$ 或 3 个解在 S_l 中. 总结一下, 当 $(a, b) \neq (0, 0)$, (3.9) 有 $0, 1, 2$ 或 3 个解在 S_l 中. 这蕴含了 $V(a, b) \in \{0, l, 2l, 3l\}$ 当 $(a, b) \neq (0, 0)$.

表 3.3　定理 3.3 的值分布

值	次数
2^{2m}	1
$(3l-1)2^m$	$\frac{(2^{2m}-1)(2^m+1-2l)(2^m+1-l)}{6l^3}$
$(2l-1)2^m$	$\frac{(2^{2m}-1)((2^m+3)l-2^m-1)(2^m+1-l)}{2l^3}$
$(l-1)2^m$	$\frac{(2^{2m}-1)((2^{2m+1}+2^{m+2}+6)l^2-(2^{2m+1}+7\cdot 2^m+5)l+(2^m+1)^2)}{2l^3}$
-2^m	$\frac{(2^{2m}-1)(6(2^{2m}+1)l^3-(6\cdot 2^{2m}+9\cdot 2^m+11)l^2+(3\cdot 2^{2m}+9\cdot 2^m+6)l-(2^m+1)^2)}{6l^3}$

因此, 我们证明了 $T_1(a,b)$ 取至多四个非平凡的值 $\{-2^m,(l-1)2^m,(2l-1)2^m,(3l-1)2^m\}$ 如果 i) 或 ii) 成立. 这些值的次数由引理 3.2 和引理 3.4 易得. □

注：当 k 为奇数, 每个满足 i) 的对 (k,m) 总满足 ii).

以下定理是定理 3.3 的直接结果.

定理 3.4: 令 $p=2, q=2^n$ 且 $n=2m$ 满足 $m\geq 2$. 给定一个正整数 $1\leq k\leq m$, 令 $s_1=2^{k-1}t-\frac{t-1}{2}$ 且 $s_2=2^{k-1}t+\frac{t+1}{2}$, 其中 $1\leq t\leq 2^m+1$, t 为奇数. 定义 $d_1=s_1(2^m-1)+1$ 和 $d_2=s_2(2^m-1)+1$. 假设 $(2^k-1)t,(2^k+1)t\not\equiv 0 \pmod{2^m+1}$ 且 $l=(t,2^m+1)$. 假设以下条件有一个成立:

i) $m\equiv -1 \pmod{k}$,

ii) $(k,2m)=1$.

那么 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 是一个 $[2^n-1,4m,2^{2m-1}-(3l-1)2^{m-1}]$ 二元码. 它的重量分布列在表 3.4.

给定 m, 上述码由 k 和 t 决定. 以下, 我们给出一些例子说明定理中的重量分布. 根据码表, 其中有一些码有已知最好的参数.

例 3.3: 当 $m=3$, 根据 (d_1,d_2) 的等价性, 满足定理 3.4 中条件的一个对 (k,t) 属于 $\{(1,1),(1,5),(1,7)\}$. 对所有这三个对, $l=(t,2^m+1)=1$. 因而这三个循环码是 $[63,12,24]$ 二元码, 具有相同的重量分布:

$$1+588x^{24}+504x^{28}+1827x^{32}+1176x^{36}.$$

表 3.4　定理 3.4 的重量分布

重量	次数
0	1
$2^{2m-1}-(3l-1)2^{m-1}$	$\frac{(2^{2m}-1)(2^m+1-2l)(2^m+1-l)}{6l^3}$
$2^{2m-1}-(2l-1)2^{m-1}$	$\frac{(2^{2m}-1)((2^m+3)l-2^m-1)(2^m+1-l)}{2l^3}$
$2^{2m-1}-(l-1)2^{m-1}$	$\frac{(2^{2m}-1)((2^{2m+1}+2^{m+2}+6)l^2-(2^{2m+1}+7\cdot 2^m+5)l+(2^m+1)^2)}{2l^3}$
$2^{2m-1}+2^{m-1}$	$\frac{(2^{2m}-1)(6(2^{2m}+1)l^3-(6\cdot 2^{2m}+9\cdot 2^m+11)l^2+(3\cdot 2^{2m}+9\cdot 2^m+6)l-(2^m+1)^2)}{6l^3}$

根据码表[119], 已知最优的长度为 63, 维数为 12 的二元线性码有极小距离 24. 因而, 我们的循环码有已知最好的参数且在应用中优于一般线性码.

例 3.4: 当 $m=4$, 由 (d_1,d_2) 的等价性, 满足定理 3.4 中条件的一个对 (k,t) 属于 $\{(1,1),(1,3),(1,5),(1,7),(1,9),(1,11),(1,13),(1,15)\}$. 对所有这八个对, $l=(t,2^m+1)=1$. 因而这八个循环码是 $[255,16,112]$ 二元码, 具有相同的重量分布:

$$1+10200x^{112}+4080x^{120}+30855x^{128}+20400x^{136}.$$

根据码表[119], 已知最优的长度为 255, 维数为 16 的二元线性码有极小距离 112. 因而, 我们的循环码有已知最好的参数且在应用中优于一般线性码.

3.1.4　非二元 Niho 指数循环码

本小节计算某些非二元 Niho 指数循环码的重量分布. 相应地, 我们将考虑 $T_2(a,b)$ 的值分布. 本小节中, 我们固定 $d_1=s_1(p^m-1)+1$ 且 $d_2=s_2(p^m-1)+1$ 其中 $s_1=\frac{t+2}{4}$ 且 $s_2=\frac{3t+2}{4}$ 对某个 $t\equiv 2 \pmod 4$. 为了确保 d_1 和 d_2 不等价, 我们有 $t\not\equiv 0 \pmod{p^m+1}$. 更一般地, 令 $s_1=\frac{t+2}{4}$, $s_2=\frac{3t+2}{4}$, $s_1'=\frac{t'+2}{4}$ 且 $s_2'=\frac{3t'+2}{4}$. 假设 $s_1+s_1'\equiv 1 \pmod{p^m+1}$ 且 $s_2+s_2'\equiv 1 \pmod{p^m+1}$. 那么我们有 $t+t'\equiv 0 \pmod{4(p^m+1)}$. 亦即, 如果 $t+t'\equiv 0 \pmod{4(p^m+1)}$, 我们得到两对等价的 Niho 指数. 因此, 我们可以将 t 限制在范围 $1\le t\le 4(p^m+1)$ 中. 以下, 我们将确定 $T_2(a,b)$ 的值分布.

作为准备, 我们有以下引理.

引理 3.6: 令 p 为一个奇素数且 $q=p^n$. 如果 $l=(t,p^m+1)$, 那么

1) $N_2(q,d_1,d_2)=\frac{(p^n-1)}{2}l+1$.

2) $N_3(q,d_1,d_2)=\frac{(p^m-2)(p^n-1)}{4}l^2+\frac{3(p^n-1)}{2}l+1$.

证明. 1) 证明类似于引理 3.4的 1) 的证明, 在此略去.

2) 由定义, $N_3(q,d_1,d_2)$ 是以下方程组的解的个数

$$\begin{cases} x^{d_1}+y^{d_1}+z^{d_1}=0 \\ x^{d_2}+y^{d_2}+z^{d_2}=0 \end{cases}, \quad x,y,z\in\mathbb{F}_q. \tag{3.10}$$

当 $z=0$, 恰有 $N_2(q,d_1,d_2)=\frac{(p^n-1)}{2}l+1$ 个解.

当 $z\neq 0$, 情形更加复杂. 令 $u=-\frac{x}{z}$ 且 $v=-\frac{y}{z}$, 我们只需考虑方程组

$$\begin{cases} u^{d_1}+v^{d_1}=1 \\ u^{d_2}+v^{d_2}=1 \end{cases}, \quad u,v\in\mathbb{F}_q. \tag{3.11}$$

(3.11) 的每个解对应于 (3.10) 的 p^n-1 个解. 如果 $u=0$ 或 $v=0$, 易知 (3.11) 恰有 $\frac{l}{2}$ 个解.

如果 $uv\neq 0$, 我们分以下四种情况讨论:

i) $u\in Q$ 且$v\in Q$,

ii) $u\in Q$ 且$v\in NQ$,

iii) $u\in NQ$ 且$v\in Q$,

iv) $u\in NQ$ 且$v\in NQ$.

注意到每个 $x\in Q$ (或 $x\in NQ$) 可被表为 $x=yz$ 和 $x=(-y)(-z)$ (或 $x=\theta yz$ 和 $x=\theta(-y)(-z)$) 当 y 跑遍 $\mathbb{F}_{p^m}^*$, z 跑遍 S. 此外, $\mathbb{F}_{p^m}^*\cap S=\{\pm 1\}$. 我们将分别处理这四种情形.

对情形 i), 我们记 $u=\alpha\delta$ 和 $v=\beta\gamma$, 其中 $\alpha,\beta\in\mathbb{F}_{p^m}^*$ 且 $\delta,\gamma\in S$. 因而 (3.11) 可被重写为

$$\begin{cases} \alpha\delta^{-\frac{t}{2}}+\beta\gamma^{-\frac{t}{2}}=1 \\ \alpha\delta^{-\frac{3t}{2}}+\beta\gamma^{-\frac{3t}{2}}=1 \end{cases}. \tag{3.12}$$

注意到

$$\Delta = \begin{vmatrix} \delta^{-\frac{t}{2}} & \gamma^{-\frac{t}{2}} \\ \delta^{-\frac{3t}{2}} & \gamma^{-\frac{3t}{2}} \end{vmatrix} = \delta^{-\frac{t}{2}}\gamma^{-\frac{3t}{2}} - \delta^{-\frac{3t}{2}}\gamma^{-\frac{t}{2}}.$$

如果 $\Delta = 0$, 我们有 $\delta^t = \gamma^t$, 亦即, $\gamma^{\frac{t}{2}} = \pm\delta^{\frac{t}{2}}$. 当 $\gamma^{\frac{t}{2}} = \delta^{\frac{t}{2}}$, 与 (3.12) 相比较, 我们有 $\alpha + \beta = \delta^{\frac{t}{2}}$. 注意到 $\mathbb{F}_{p^m}^* \cap S = \{\pm 1\}$, 我们有 $\alpha + \beta = \delta^{\frac{t}{2}} = \pm 1$. 存在 $\frac{l^2}{4}$ 个 (δ, γ) 对使得 $\delta^{\frac{t}{2}} = \gamma^{\frac{t}{2}} = 1$ 或 $\delta^{\frac{t}{2}} = \gamma^{\frac{t}{2}} = -1$. 此外, 对每个 (δ, γ) 对, 存在 $p^m - 2$ 个 (α, β) 对, 使得 $\alpha + \beta = 1$ 且 $\alpha\beta \neq 0$. 因此, 当 $\gamma^{\frac{t}{2}} = \delta^{\frac{t}{2}}$, 存在 $\frac{(p^m-2)}{2}l^2$ 个 $(\alpha, \beta, \delta, \gamma)$ 四元组满足 (3.12). 类似地可证明存在 $\frac{(p^m-2)}{2}l^2$ 个 $(\alpha, \beta, \delta, \gamma)$ 四元组满足 (3.12) 当 $\gamma^{\frac{t}{2}} = -\delta^{\frac{t}{2}}$. 由于 u 和 v 被表出了两次, 当 $\Delta = 0$, 存在 $\frac{1}{4}(\frac{(p^m-2)}{2}l^2 + \frac{(p^m-2)}{2}l^2) = \frac{(p^m-2)}{4}l^2$ 个 (3.11) 的解.

如果 $\Delta \neq 0$, 亦即, $\delta^t \neq \gamma^t$, 解 (3.7) 得

$$\alpha = \frac{1 - \gamma^t}{\delta^{-\frac{t}{2}}(1 - \delta^{-t}\gamma^t)},$$
$$\beta = \frac{1 - \delta^t}{\gamma^{-\frac{t}{2}}(1 - \delta^t\gamma^{-t})}.$$

我们将要证明此时没有解存在. 由于 $\alpha, \beta \in \mathbb{F}_{p^m}^*$, 由 $\alpha = \bar{\alpha}$ 和 $\beta = \bar{\beta}$, 我们有 $\delta^{2t} = 1$ 且 $\gamma^{2t} = 1$. 由于 $\delta^t \neq \gamma^t$, 我们有 $\delta^t = 1, \gamma^t = -1$ 或 $\delta^t = -1, \gamma^t = 1$. 然而, $\delta^t = 1$ 蕴含了 $\beta = 0$ 且 $\gamma^t = 1$ 蕴含了 $\alpha = 0$. 因此, 没有解存在当 $\Delta \neq 0$. 在情况 i), 存在 $\frac{(p^m-2)}{4}l^2$ 个 (3.11) 的解.

对情况 ii), 我们记 $u = \alpha\delta$ 且 $v = \theta\beta\gamma$, 其中 $\alpha, \beta \in \mathbb{F}_{p^m}^*$ 且 $\delta, \gamma \in S$. 因而 (3.11) 可重写作

$$\begin{cases} \alpha\delta^{-\frac{t}{2}} + \theta^{d_1}\beta\gamma^{-\frac{t}{2}} = 1 \\ \alpha\delta^{-\frac{3t}{2}} + \theta^{d_2}\beta\gamma^{-\frac{3t}{2}} = 1 \end{cases}. \tag{3.13}$$

注意到

$$\Delta = \begin{vmatrix} \delta^{-\frac{t}{2}} & \theta^{d_1}\gamma^{-\frac{t}{2}} \\ \delta^{-\frac{3t}{2}} & \theta^{d_2}\gamma^{-\frac{3t}{2}} \end{vmatrix} = \theta^{d_2}\delta^{-\frac{t}{2}}\gamma^{-\frac{3t}{2}} - \theta^{d_1}\delta^{-\frac{3t}{2}}\gamma^{-\frac{t}{2}}.$$

如果 $\Delta = 0$, 我们推出 $\delta^t\theta^{\frac{t}{2}(p^m-1)} = \gamma^t$. 令 $\eta = \theta^{p^m-1}$, 那么 η 是 S 的一个生成元. 我们有 $\eta^{\frac{t}{2}} = (\frac{\gamma}{\delta})^t = \eta^{jt}$ 对某个整数 j. 这等价于 $jt \equiv \frac{t}{2} \pmod{p^m + 1}$. 而由于 $t \equiv 2 \pmod 4$, 后者是不可能的.

如果 $\Delta \neq 0$, 解 (3.13) 得

$$\alpha = \frac{\delta^{\frac{t}{2}}(1 - \theta^{-\frac{t}{2}(p^m-1)}\gamma^t)}{1 - \theta^{-\frac{t}{2}(p^m-1)}\delta^{-t}\gamma^t},$$

$$\beta=\frac{\gamma^{\frac{t}{2}}(1-\delta^t)}{\theta^{d_1}(1-\theta^{\frac{t}{2}(p^m-1)}\delta^t\gamma^{-t})}.$$

由 $\alpha=\bar{\alpha}$ 和 $\beta=\bar{\beta}$, 我们推出 $\delta^t\gamma^t=1$ 和 $\gamma^{2t}=\theta^{t(p^m-1)}$. 因此我们有 $\alpha=\frac{\delta^{\frac{t}{2}}(1-\theta^{-\frac{t}{2}(p^m-1)}\delta^{-t})}{1-\theta^{-\frac{t}{2}(p^m-1)}\delta^{-2t}}$. 由 $\alpha=\bar{\alpha}$, 我们有 $\delta^t=\pm1$. 因而, $\gamma^t=\pm1$. 然而, 这与 $\gamma^{2t}=\theta^{t(p^m-1)}$ 矛盾, 因此 $t\not\equiv 0 \pmod{p^m+1}$. 所以, (3.11) 在情况 ii) 无解.

对情形 iii), 与情形 ii) 类似, (3.11) 无解.

对情形 iv), 我们记 $u=\theta\alpha\delta$ 且 $v=\theta\beta\gamma$, 其中 $\alpha,\beta\in\mathbb{F}_{p^m}^*$ 且 $\delta,\gamma\in S$. 那么 (3.11) 可被重写作

$$\begin{cases}\alpha\delta^{-\frac{t}{2}}+\beta\gamma^{-\frac{t}{2}}=\theta^{-d_1}\\ \alpha\delta^{-\frac{3t}{2}}+\beta\gamma^{-\frac{3t}{2}}=\theta^{-d_2}\end{cases}.$$

注意到

$$\Delta=\begin{vmatrix}\delta^{-\frac{t}{2}} & \gamma^{-\frac{t}{2}}\\ \delta^{-\frac{3t}{2}} & \gamma^{-\frac{3t}{2}}\end{vmatrix}=\delta^{-\frac{t}{2}}\gamma^{-\frac{3t}{2}}-\delta^{-\frac{3t}{2}}\gamma^{-\frac{t}{2}}.$$

如果 $\Delta=0$, 类似情形 ii) 可证明没有解存在. 如果 $\Delta\neq 0$, 类似情形 i) 可证明没有解存在. 因此, (3.11) 在情形 iv) 没有解.

综合以上四种情形, 我们推出$N_3(q,d_1,d_2)=\frac{(p^n-2)}{2}l+1+(p^n-1)(\frac{(p^m-2)}{4}l^2+l)=\frac{(p^m-2)(p^n-1)}{4}l^2+\frac{3(p^n-1)}{2}l+1$. □

现在我们决定以下指数和的值分布

$$T_2(a,b)=\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_n(ax^{d_1}+bx^{d_2})},$$

其中 p 是一个奇素数.

定理 3.5: 假设 $n=2m$ 其中 $m\geq 1$. 令 p 为一个奇素数且 $q=p^n$ 为一个素数幂. 给定一个正整数 t 满足 $t\equiv 2 \pmod 4$ 且 $t\not\equiv 0 \pmod{p^m+1}$, 令 $s_1=\frac{t+2}{4}$ 且 $s_2=\frac{3t+2}{4}$. 定义$d_1=s_1(p^m-1)+1, d_2=s_2(p^m-1)+1$ 且 $l=(t,p^m+1)$. 那么 $T_2(a,b)$ 的值分布列在表 3.5.

证明. 由引理 3.1 的 3), 我们有 $T_2(a,b)=(W(a,b)-1)p^m$, 其中 $W(a,b)$ 是 $z\in S$ 的个数满足

$$\bar{b}z^{\frac{3t}{2}}+\bar{a}z^t+az^{\frac{t}{2}}+b=0.$$

表 3.5　定理 3.5 的值分布

值	次数
p^{2m}	1
$(\frac{3l}{2}-1)p^m$	$\frac{2(p^{2m}-1)(l-p^m-1)(l-2p^m-2)}{3l^3}$
$(l-1)p^m$	$\frac{(p^{2m}-1)(2p^m+2-(p^m+3)l)(l-2p^m-2)}{l^3}$
$(\frac{l}{2}-1)p^m$	$\frac{2(p^{2m}-1)((p^{2m}+2p^m+3)l^2-(2p^{2m}+7p^m+5)l+2(p^m+1)^2)}{l^3}$
$-p^m$	$\frac{(p^{2m}-1)(3(p^{2m}+1)l^3-(6p^{2m}+9p^m+11)l^2+6(p^{2m}+3p^m+2)l-4(p^m+1)^2)}{3l^3}$

表 3.6　定理 3.6 的重量分布

重量	次数
0	1
$(p^m-p^{m-1})(p^m+1-\frac{3l}{2})$	$\frac{2(p^{2m}-1)(l-p^m-1)(l-2p^m-2)}{3l^3}$
$(p^m-p^{m-1})(p^m+1-l)$	$\frac{(p^{2m}-1)(2p^m+2-(p^m+3)l)(l-2p^m-2)}{l^3}$
$(p^m-p^{m-1})(p^m+1-\frac{l}{2})$	$\frac{2(p^{2m}-1)((p^{2m}+2p^m+3)l^2-(2p^{2m}+7p^m+5)l+2(p^m+1)^2)}{l^3}$
$(p^m-p^{m-1})(p^m+1)$	$\frac{(p^{2m}-1)(3(p^{2m}+1)l^3-(6p^{2m}+9p^m+11)l^2+6(p^{2m}+3p^m+2)l-4(p^m+1)^2)}{3l^3}$

如果$(a,b)=(0,0)$, 我们有 $W(a,b)=p^m+1$ 且 $T_2(a,b)$ 取平凡值 p^{2m}. 如果 $(a,b)\neq(0,0)$, 由于 $(\frac{t}{2},p^m+1)=\frac{l}{2}$, 以上方程有 $0,\frac{l}{2},l$ 或 $\frac{3l}{2}$ 个解在 S 中. 亦即, $W(a,b)\in\{0,\frac{l}{2},l,\frac{3l}{2}\}$. 因此 $T_2(a,b)$ 取四个非平凡值 $\{-p^m,(\frac{l}{2}-1)p^m,(l-1)p^m,(\frac{3l}{2}-1)p^m\}$ 当 $(a,b)\neq(0,0)$. 这些值的次数可由引理 3.2 和引理 3.6 得到. □

由引理 3.1 的 3), $T_2(\lambda a,\lambda b)=T_2(a,b)$ 对任意 $\lambda\in\mathbb{F}_p^*$. 因此, 我们容易推出以下的定理.

定理 3.6: 假设 $n=2m$ 其中 $m\geq 1$. 令 p 为一个奇素数且 $q=p^n$ 为一个素数幂. 给定一个正整数 t 满足 $t\equiv 2 \pmod 4$ 且 $t\not\equiv 0 \pmod{p^m+1}$, 令 $s_1=\frac{t+2}{4}$ 且 $s_2=\frac{3t+2}{4}$. 定义 $d_1=s_1(p^m-1)+1$, $d_2=s_2(p^m-1)+1$ 且 $l=(t,p^m+1)$. 那么 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 是一个 $[p^n-1,4m,(p^m-p^{m-1})(p^m+1-\frac{3l}{2})]$ p 元码. 进一步, $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 的重量分布列在表3.6.

给定 p 和 m, 上述码由一个参数 t 确定. 以下, 我们给出几个关于以上定理的重量分布的例子.

例 3.5: 令 $p=3, m=3$ 且 $t=14$, 我们有 $q=729, d_1=105, d_2=287$ 且 $l=(t,p^m+1)=14$. 相应地循环码 $\mathcal{C}^{\perp}_{q,d_1,d_2}$ 是一个 $[728,12,126]$ 三元码, 重量分布为:

$$1+104x^{126}+4056x^{252}+70304x^{378}+456976x^{504}.$$

例 3.6: 对 $p=5, m=2$ 且 $2\leq t\leq 50$ 满足 $t\equiv 2 \pmod 4$ 且 $t\neq 26$, 我们得到十二个循环码满足 $q=625$ 且 $l=(t,p^m+1)=2$. 所有这些码是 $[624,8,460]$ 五元码, 重量分布为:

$$1+62400x^{460}+15600x^{480}+187824x^{500}+124800x^{520}.$$

3.1.5 总结

在本节中, 我们考虑了 Niho 指数循环码的重量分布. 熟知地, 重量分布的确定本质上依赖于对某些指数和的计算. 特别地, 我们完全确定了 $S(a,b)$ 的值分布并在某些情形下得到了 $T_1(a,b)$ 和 $T_2(a,b)$ 值分布. 因而, 我们得到了一些二元和非二元循环码的值分布. 更具体地, 我们得到了两类二元的三重和四重循环码和一类非二元的四重循环码. 通过一些例子, 我们说明了这三类码中包含了最优的或具有已知最好参数的码.

3.2 m-序列互相关的一些新结果

3.2.1 引言

过去几十年中, 低相关序列在密码, 雷达和无线通信系统中得到了广泛的应用[123]. 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, 可以降低通信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[134].

令 p 为一个素数. 令 $\{a_t\}$ 和 $\{b_t\}$ 为两个周期为 N 的有限域 GF(p) 上的序列. $\{a_t\}$

和 $\{b_t\}$ 在平移 τ 处的互相关值定义为

$$C_{a,b}(\tau) = \sum_{t=0}^{N-1} \omega^{a_{t+\tau} - b_t},$$

其中 $0 \leq \tau < N$ 且 ω 是一个复 p-次单位根.

至今, 关于极大长度线性序列 (m-序列) 已经有了很多的研究. 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(见文献[34,49,69,97,98,130,145,175] 及其中的参考文献).

回忆由 $E = \mathrm{GF}(p^n)$ 到它的子域 $F = \mathrm{GF}(p^r)$ 上的迹函数定义为

$$Tr_r^n(x) = x + x^{p^r} + x^{p^{2r}} + ... + x^{p^{n-r}}.$$

当 $r = 1$, 我们得到到素域 $GF(p)$ 上的绝对迹函数, 记做 Tr_n 或 Tr. 一个周期为 $p^n - 1$ 的 p-元 m-序列 $\{a_t\}$ 可被表为

$$a_t = \mathrm{Tr}(\beta\alpha^t), \quad 0 \leq t \leq p^n - 2,$$

其中 $\beta \in \mathrm{GF}(p^n)^*$ 且 α 是 $\mathrm{GF}(p^n)$ 的一个本原元.

假设 $(d, p^n - 1) = 1$. $\{a_t\}$ 的 d-采样, 记做 $\{a_{dt}\}$, 是一个有相同周期的 m-序列. 注意到如果 $d \in \{1, p, \ldots, p^{n-1}\}$, $\{a_{dt}\}$ 只是 $\{a_t\}$ 的循环移位. 此时, $\{a_t\}$ 和 $\{a_{dt}\}$ 的互相关仅取两值(见定理 3.1[130]). 以下, 我们总考虑非退化的采样 d 满足 $d \notin \{1, p, \ldots, p^{n-1}\}$. 一个周期为 $p^n - 1$ 的 m-序列和它的 d-采样的互相关值可表为

$$\begin{aligned} C_d(\tau) &= \sum_{t=0}^{p^n-2} \omega^{a_{t+\tau} - a_{dt}} \\ &= -1 + \sum_{x \in \mathrm{GF}(p^n)} \chi(\alpha^\tau x - x^d), \end{aligned}$$

其中 $\chi(x) = w^{\mathrm{Tr}(x)}$ 对任意 $x \in \mathrm{GF}(p^n)$ 且 $0 \leq \tau \leq p^n - 2$. 计算互相关值等价于计算

Weil 和

$$\mathrm{C}_d(z) = \sum_{x \in \mathrm{GF}(p^n)^*} \chi(zx - x^d),$$

其中 $z \in \mathrm{GF}(p^n)^*$. 因此, 计算互相关分布即是确定多重集

$$\{\mathrm{C}_d(z) \mid z \in \mathrm{GF}(p^n)\}.$$

注意到互相关分布在其它许多场景中以不同的名字出现, 可参见文献[175] 的附录.

对一个 m-序列和它的 d-采样的互相关函数, 已知结果的综述可见[60,97,130]. 此外, 有一些更进一步的工作研究了一个 m-序列和它的 d-采样的互相关函数, 其中 $\gcd(d, p^n - 1) > 1$ (参见文献[133,217–219,245,291]). 当 $p = 2$ 且 $(d, 2^n - 1) = 1$, 已知的关于一个 m-序列和它的采样的互相关分布的结果列在表 3.7, 其中 $v_2(k)$ 是最大的整除 k 的 2 的幂次. 同时, 表 3.8 总结了 p 为奇素数时互相关分布的结果.

在本节中, 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[96] 和 Feng 等人[106] 的思想, 我们完全决定了互相关分布. 此外, 对周期为 $2^{2lm} - 1$ 的二元 m-序列和采样 $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, 其中 $l \geq 2$ 为偶数且 $0 \leq s \leq 2m - 1$, 我们得到了一些互相关值的结果. 当 l 为奇数时, 采样 d 是 Niho 指数, 已得到了广泛的研究[49,97,98,135,145,221]. 回顾任何非退化的采样得出至少三个互相关值(见定理 4.1[130]). 我们进一步证明了对这个采样, 互相关值至少取四个值. 虽然确定互相关分布看起来非常困难, 我们验证了以下两个 Sarwate 等人[240] 和 Helleseth[130] 提出的著名猜想的正确性. 以下, 我们定义 $\mathrm{S}_d(z) = \mathrm{C}_d(z) + 1$.

猜想 (文献[240]): 令 $n = 2t$ 和 $p = 2$, 那么 $\max_{z \in \mathrm{GF}(2^n)} |\mathrm{S}_d(z)| \geq 2^{t+1}$.

猜想 (猜想 5.1[130]): 如果 $p^n > 2$ 和 $d \equiv 1 \pmod{p-1}$, 那么 $\mathrm{S}_d(z) = 0$ 对某个 $z \in \mathrm{GF}(p^n)^*$.

3.2.2 三元 m-序列的互相关分布

在本小节中, 对周期为 $3^{3r} - 1$ 的三元 m-序列, 我们对采样 $d = 3^r + 2$ 或 $d = 3^{2r} + 2$, 其中 $(r, 3) = 1$, 确定了互相关分布.

我们首先引入一些概念. 给定一个素数幂 $q = p^s$, 我们有有限域 GF(q). 令 ω

表 3.7　周期为 2^n-1 的二元 m-序列和它的 d-采样的互相关分布, $(d,2^n-1)=1$

文献	d	互相关值个数
Gold[122]	$d=2^k+1, \frac{n}{(n,k)}$ 为奇数	3
Kasami[170]	$d=2^{2k}-2^k+1, \frac{n}{(n,k)}$ 为奇数	3
Welch[34]	$d=2^k+3, n=2k+1$	3
Hollmann 和 Xiang[145]	$d=2^{2k}+2^k-1, k=\frac{n-1}{4}$ 如果 $n\equiv 1 \pmod 4$ $k=\frac{3n-1}{4}$ 如果 $n\equiv 3 \pmod 4$	3
Cusick 和 Dobbertin[69]	$d=2^k+2^{\frac{k+1}{2}}+1, n=2k, k$ 为奇数	3
Cusick 和 Dobbertin[69]	$d=2^{k+1}+3, n=2k, k$ 为奇数	3
Niho[221]	$d=2^{2k+1}-1, n=4k$	4
Niho[221]	$d=(2^{2k}+1)(2^k-1)+2, n=4k$	4
Dobbertin[96]	$\sum_{i=0}^{2k}2^{im}, n=4k, 0<m<n, \gcd(m,n)=1$	4
Helleseth 和 Rosendahl[135]	$d=(2^{2k}+2^{s+1}-2^{k+1}-1)/(2^s-1), n=2k, 2s\|k$	4
Dobbertin 等[97]	$d=(2^k-1)s+1, s\equiv 2^r(2^r\pm 1)^{-1} \pmod{2^k+1}$, $v_2(r)<v_2(k)$	4
Helleseth[130]	$d=2^k+3, n=2k$	5
Dobbertin[96]	$d=2^{2k}+2^k+1, n=4k, k$ 为奇数	5
Johansen 和 Helleseth[160]	$d=\frac{5}{3}, n$ 为奇数	5
Johansen 等[161]	$d=\frac{17}{5}, n$ 为奇数	5
Boston 和McGuire[26]	$d=11, n$ 为奇数	5
Helleseth[131]	$d=2^{2k}-2^k+1, n=4k, k$ 为偶数	6
Helleseth[130]	$d=\frac{1}{3}(2^n-1)+2^s, n$ 为偶数, $s<n$ 且 $\frac{1}{3}2^{-s}(2^n-1)\neq 2 \pmod 3$	6
Dobbertin 等[97]	$d=3\cdot 2^{k-1}-1, n=2k, k$ 为奇数	6
Feng 等[106]	$d=2^{t+1}+3, n=2t, t\equiv 2 \pmod 4$ 且$t\geq 6$	7

表 3.8　周期为 p^n-1 的非二元 m-序列和它的 d-采样的互相关分, $(d,p^n-1)\geq 1$

文献	p	n	d	互相关值个数
Helleseth[130]	奇素数	任意	$d=p^{2k}-p^k+1$ $\frac{n}{(n,k)}$ 为奇数	3
Helleseth[130]	奇素数	任意	$d=\frac{1}{2}(p^{2k}+1)$ $\frac{n}{(n,k)}$ 为奇数	3
Dobbertin 等[98]	3	奇数	$d=2\cdot 3^{\frac{n-1}{2}}+1$	3
Helleseth[130]	$p^{\frac{n}{2}}\not\equiv 2 \pmod 3$	偶数	$d=2p^{\frac{n}{2}}-1$	4
Helleseth[130]	$p^n\equiv 1 \pmod 4$	任意	$d=\frac{1}{2}(p^n-1)+p^i$ $0\leq i<n$	5
Helleseth[130]	$p\equiv 2 \pmod 3$	偶数	$d=\frac{1}{3}(p^n-1)+p^i$ $0\leq i<n$ $\frac{1}{2}p^{-i}(p^n-1)\not\equiv 2 \pmod 3$	6
Helleseth[132]	$p^m\not\equiv 2 \pmod 3$	$4\mid n$	$d=p^{2m}-p^m+1$ $n=4m$	6
Luo 和 Feng[192]	奇素数	任意	$d=\frac{p^k+1}{2}$, k/e 奇 $e=\gcd(n,k)$	可变
Seo 等[245]	奇素数	$4\mid n$	$d=(\frac{p^m+1}{2})^2$, $n=2m$	4
Choi 等[59]	$4\mid p+1$	奇数	$d=\frac{p^n+1}{p^k+1}+\frac{p^n-1}{2}$, $k\mid n$	9

为 p-次单位根. GF(q) 的二次特征记为 η. GF(q) 的典范的加法特征记为 χ, 其中 $\chi(x)=\omega^{Tr(x)}, \forall x \in \text{GF}(q)$. 关于 η 和 χ 的高斯和 $G(\eta,\chi)$ 定义为

$$G(\eta,\chi)=\sum_{x\in \text{GF}(q)^*}\eta(x)\chi(x).$$

以下是两个引理.

引理 3.7 (**定理** 5.15[190]): 假设 $q=p^s$, 其中 p 是一个奇素数且 s 是一个正整数. 那么

$$G(\eta,\chi)=\begin{cases}(-1)^{s-1}q^{\frac{1}{2}} & \text{如果 } p\equiv 1 \pmod 4,\\ (-1)^{s-1}i^s q^{\frac{1}{2}} & \text{如果 } p\equiv 3 \pmod 4.\end{cases}$$

引理 3.8 (**定理** 5.33[190]): 令 q 为一个奇素数幂且 $f(x)=a_2x^2+a_1x+a_0\in GF(q)[x]$ 满足 $a_2\neq 0$. 那么

$$\sum_{c\in GF(q)}\chi(f(c))=\chi(a_0-a_1^2(4a_2)^{-1})\eta(a_2)G(\eta,\chi).$$

以下熟知的等式可参见文献[130].

引理 3.9: 我们有

$$\sum_{z\in GF(p^n)}\mathsf{S}_d(z)=p^n,$$

$$\sum_{z\in GF(p^n)}\mathsf{S}_d(z)^2=p^{2n},$$

$$\sum_{z\in GF(p^n)}\mathsf{S}_d(z)^3=p^{2n}b_3,$$

其中 b_3 为以下方程组的解的个数

$$x+y+1=0,$$

$$x^d+y^d+1=0,$$

其中 $x,y\in GF(p^n)$.

作为准备, 我们有以下的引理.

引理 3.10: 给定一个整数 r 满足 $\gcd(r,3)=1$. 假设 $n=3r, d=3^r+2$ 或 $d=3^{2r}+2$. 那么对 $x,y\in GF(3^n)$,

$$x+y+1=0,$$

和

$$x^d+y^d+1=0,$$

的公共解的个数是 3^r.

证明. 我们考虑 $d=3^r+2$ 的情形. 当 $d=3^{2r}+2$, 证明是类似的. 以上等式等价于

$$(x+1)^d-x^d-1=0.$$

因此,

$$(x+1)^{3^r}(x+1)^2-x^{3^r+2}-1=0,$$

这可导出

$$(x-1)(x^{3^r}-x)=0.$$

所以, 我们推出 $x\in GF(3^r)$, 蕴含了有 3^r 个公共解. □

现在我们叙述主要的定理.

定理 3.7: 给定一个整数 $r\geq 2$ 满足 $\gcd(r,3)=1$. 令 $n=3r, d=3^r+2$ 或 $d=3^{2r}+2$. 对周期为 3^n-1 的三元 m-序列, 与它的 d-采样的互相关分布如下所示. 当 r 是偶数, 互相关分布为

-1	取	$\frac{3^{3r}+3^{2r}}{2}-3^r$	次
$3^{2r}-1$	取	3^r	次
$3^{\frac{3r}{2}}-1$	取	$\frac{3^{3r-1}-3^{2r-1}}{2}$	次
$-3^{\frac{3r}{2}}-1$	取	$\frac{3^{3r-1}-3^{2r-1}}{2}$	次
$2\cdot 3^{\frac{3r}{2}}-1$	取	$\frac{3^{3r-1}-3^{2r-1}}{4}$	次
$-2\cdot 3^{\frac{3r}{2}}-1$	取	$\frac{3^{3r-1}-3^{2r-1}}{4}$	次

当 r 为奇数, 互相关分布为

-1	取	$2\cdot 3^{3r-1}+3^{2r-1}-3^r$	次
$3^{2r}-1$	取	3^r	次
$3^{\frac{3r+1}{2}}-1$	取	$\frac{3^{3r-1}-3^{2r-1}}{2}$	次
$-3^{\frac{3r+1}{2}}-1$	取	$\frac{3^{3r-1}-3^{2r-1}}{2}$	次

证明. 以下, 我们仅证明 $d=3^r+2$ 的情形. $d=3^{2r}+2$ 的情形是类似的. 我们固定 $d=3^r+2, E=GF(3^n), F=GF(3^r)$ 且 $n=3r$. 容易验证 $\gcd(d,3^n-1)=1$.

令 a 为 $GF(27)$ 的一个本原元满足

$$a^3+2a+1=0.$$

由于 $\gcd(r,3)=1$, 我们有 $E=F(a)$. 对任意 $x\in E$, 可被表示为

$$x=x_0+x_1a+x_2a^2,$$

其中 $x_0,x_1,x_2\in F$.

由于 $\gcd(r,3)=1$, 我们首先考虑 $r\equiv 2 \pmod 3$ 的情形, 其中 $a^{3^r}=a^9$. 第一步是将 $Tr_n(x^d)$ 表为 x_0,x_1 和 x_2 的一个函数. 注意到 $Tr_r^n(1)=Tr_r^n(a)=0$ 且 $Tr_r^n(a^2)=2$. 经计算得

$$Tr_n(x^d)=Tr_r(x_1x_2^2+x_0x_2^2+2x_1^2x_2+2x_1).$$

接下来, 我们计算 $\mathbf{C}_d(z)$ 对某个固定的 $z\in E$. 令

$$z=z_0+z_1a+z_2a^2$$

其中 $z_0,z_1,z_2\in F$, 我们得到

$$Tr_n(xz)=Tr_r(2x_2z_2+2x_0z_2+2x_1z_1+2x_2z_0).$$

定义 F 的加法特征为 χ_F, 其中 $\chi_F(x)=\omega^{Tr_r(x)}, \forall x\in F$. 因此,

$$\begin{aligned}\mathrm{S}_d(z) &= \sum_{x_0,x_1,x_2\in F}\chi_F(2x_1x_2^2+2x_0x_2^2+x_1^2x_2+x_1+2x_2z_2+2x_0z_2+2x_1z_1+2x_2z_0)\\ &= \sum_{x_0,x_1,x_2\in F}\chi_F(x_0(2x_2^2+2z_2)+2x_1x_2^2+x_1^2x_2+x_1+2x_2z_2+2x_1z_1+2x_2z_0)\\ &= 3^r\sum_{x_1\in F,x_2\in M}\chi_F(2x_1x_2^2+x_1^2x_2+x_1+2x_2z_2+2x_1z_1+2x_2z_0)\end{aligned} \tag{3.14}$$

其中

$$M=\{x_2\in F|x_2^2=-z_2\}.$$

如果 $z_2=0$, 那么 $M=\{0\}$. 我们有

$$\begin{aligned}\mathrm{S}_d(z) &= 3^r\sum_{x_1\in F}\chi_F(x_1(1+2z_1))\\ &= \begin{cases}0 & \text{如果 } z_1\neq 1,\\ 3^{2r} & \text{如果 } z_1=1.\end{cases}\end{aligned}$$

如果 $-z_2$ 是 F 中一个非平方元, 那么 $M=\emptyset$ 且 $\mathrm{S}_d(z)=0$.

如果 $-z_2$ 是 F 中一个非零平方元, 令 $z_2=-b^2$, 那么 $M=\{\pm b\}$. 因此,

$$\begin{aligned}\mathrm{S}_d(z) &= 3^r\sum_{x_1\in F}\chi_F(bx_1^2+(2b^2+2z_1+1)x_1+2b^3+2bz_0)\\ &\quad+3^r\sum_{x_1\in F}\chi_F(2bx_1^2+(2b^2+2z_1+1)x_1+b^3+bz_0).\end{aligned}$$

由引理 3.7 和引理 3.8, 我们有

$$\mathrm{S}_d(z)=(-1)^{r-1}\cdot i^r\cdot 3^{\frac{3r}{2}}(\eta(b)\chi_F(c)+\eta(2b)\chi_F(-c)),$$

其中

$$c=2b^3+2bz_0-(2b^2+2z_1+1)^2b^{-1}.$$

注意到

$$\eta(2)=\begin{cases}1 & \text{如果 } r \text{ 为偶数,}\\ -1 & \text{如果 } r \text{ 为奇数.}\end{cases}$$

假设 $A=\eta(b)\chi_F(c)+\eta(2b)\chi_F(-c)$. 由于 $\chi_F(c)=\overline{\chi_F(-c)}$, 我们有

$$A=\begin{cases}\pm 1,\pm 2 & \text{如果 } r \text{ 为偶数,}\\ 0,\pm\sqrt{-3} & \text{如果 } r \text{ 为偶数.}\end{cases}$$

当 r 是偶数, $\mathrm{S}_d(z)$ 取六个值$0, 3^{2r}, 3^{\frac{3r}{2}}, -3^{\frac{3r}{2}}, 2\cdot 3^{\frac{3r}{2}}$ 和 $-2\cdot 3^{\frac{3r}{2}}$. 对 $1\le i\le 6$, 用 N_i 记这些值出现的次数. 由引理 3.9, 引理 3.10 和以上讨论, 我们有

$$N_1=\frac{3^{3r}}{2}+\frac{3^{2r}}{2}-3^r,$$

$$N_2=3^r,$$

$$N_1+N_2+N_3+N_4+N_5+N_6=3^{3r},$$

$$3^{2r}N_2+3^{\frac{3r}{2}}(N_3-N_4)+2\cdot 3^{\frac{3r}{2}}(N_5-N_6)=3^{3r},$$

$$3^{4r}N_2+3^{3r}(N_3+N_4)+4\cdot 3^{3r}(N_5+N_6)=3^{6r},$$

$$3^{6r}N_2+3^{\frac{9r}{2}}(N_3-N_4)+8\cdot 3^{\frac{9r}{2}}(N_5-N_6)=3^{7r}.$$

因此当 $r\equiv 2 \pmod 6$ 时结论成立.

当 r 是奇数, $\mathrm{S}_d(z)$ 取四个值 $0, 3^{2r}, 3^{\frac{3r+1}{2}}$ 和 $-3^{\frac{3r+1}{2}}$. 对 $1\le i\le 4$, 用 N_i 记这些值出现的次数. 用 N_i 记这些值出现的次数.

$$N_2=3^r,$$

$$N_1+N_2+N_3+N_4=3^{3r},$$

$$3^{2r}N_2+3^{\frac{3r+1}{2}}(N_3-N_4)=3^{3r},$$

$$3^{4r}N_2+3^{3r+1}(N_3+N_4)=3^{6r}.$$

因此当 $r \equiv 5 \pmod 6$ 时结论成立.

对余下的情形 $r \equiv 1 \pmod 3$, 类似的讨论可知

$$Tr_n(x^d) = Tr_r(2x_2 + x_0x_2^2 + 2x_1^2x_2 + 2x_1x_2^2 + x_1).$$

互相关分布可以类似地得出. □

注: 当 $r = 3$, 数据表明周期为 $3^9 - 1$ 的三元 m-序列和采样 $d = 3^3 + 2 = 29$ 或 $d = 3^6 + 2 = 731$ 的互相关分布为

-1	出现	13338	次
728	出现	27	次
242	出现	3159	次
-244	出现	3159	次

这个结果与定理 3.7 一致. 因此, 当 $(r, 3) = 3$, 我们猜想互相关分布与定理 3.7 一致.

3.2.3 二元 m-序列互相关值的一些结果

在本小节中, 我们考虑周期为 $2^{2lm}-1$ 的二元 m-序列和 d-采样序列的互相关值, 其中 $d = \frac{2^{2lm}-1}{2^m+1} + 2^s, 0 \le s \le 2m-1$ 且 $(2^{s-1} - l, 2^m + 1) = 1$. 注意到 $(2^{s-1} - l, 2^m + 1) = 1$ 等价于 $(d, 2^{2lm} - 1) = 1$. 这个形式的一些特殊情形此前已被研究过. 例如, 当 $m = 1$, 采样 $d = \frac{2^{2l}-1}{3} + 2^s$ 的互相关分布已被确定[130]. 如果 $l = 2$ 且 $s = 0$, 采样 $d = \frac{2^{4m}-1}{2^m+1} + 1$ 已被研究过[131]. 事实上, 当 l 为奇数时, 易知 d 是 Niho 指数. 由文献[49], 对 Nhio 指数的采样, 互相关至少取四个值. 因而, 我们考虑当 l 为偶数时相同的情况是否发生. 这种情况下, d 可能不是 Niho 指数. 我们将证明 $\mathrm{C}_d(z)$ 至少取四个值. 此外, 我们对这种形式的采样验证了猜想 3.2.1 和猜想 3.2.1.

在本小节中, 我们始终假设 $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, 其中 $0 \le s \le 2m-1$, $(2^{s-1} - l, 2^m + 1) = 1$ 且 l 为偶数. 令 α 为 $\mathrm{GF}(2^{2lm})$ 的一个本原元. 我们定义

$$\begin{aligned} C_\infty &= \{0\}, \\ C_0 &= \{\alpha^{j(2^m+1)} \mid 0 \le j \le \frac{2^{2lm}-1}{2^m+1} - 1\}, \\ C_1 &= \mathrm{GF}(2^{2lm}) \setminus (C_0 \cup C_\infty). \end{aligned}$$

以下引理是引理 3.5[130] 的一个特殊情形.

引理 3.11:

$$\sum_{x\in \mathrm{GF}(2^{2lm})} \chi(ax^{2^m+1}) = \begin{cases} 2^{2lm} & \text{如果 } a \in C_\infty, \\ -2^{(l+1)m} & \text{如果 } a \in C_0, \\ 2^{lm} & \text{如果 } a \in C_1. \end{cases}$$

我们有以下的定理.

定理 3.8: 假设 $d = \frac{2^{2lm}-1}{2^m+1} + 2^s$, 其中 $0 \le s \le 2m-1$, $(2^{s-1}-l, 2^m+1) = 1$ 且 l 为偶数. 那么

(i) $\mathrm{S}_d(z) = 0$ 对某个 $z \in \mathrm{GF}(2^{2lm})^*$;

(ii) $\mathrm{C}_d(z)$ 取至少四个值;

(iii) 存在一个 $z \in \mathrm{GF}(2^{2lm})$ 使得 $\mathrm{S}_d(z) \ge 2^{lm+1}$.

证明. 由定理 3.8[130], 我们有

$$\mathrm{C}_d(z) = -1 + \frac{1}{2^m+1} \sum_{j=0}^{2^m} \sum_{x\in \mathrm{GF}(2^{2lm})} \chi(x^{2^m+1}(z\alpha^j + \alpha^{dj2^{-s}})),$$

其中 2^{-s} 是 2^s 模 $2^{2lm}-1$ 的逆.

对任意 $z \in \mathrm{GF}(2^{2lm})$, 定义

$$n_i(z) = |\{j \mid 0 \le j \le 2^m, z\alpha^j + \alpha^{dj2^{-s}} \in C_i\}|,$$

其中 $i = 0, 1, \infty$. 因此,

$$\mathrm{C}_d(z) = -1 + \frac{1}{2^m+1}(2^{2lm}n_\infty(z) - 2^{(l+1)m}n_0(z) + 2^{lm}n_1(z)). \tag{3.15}$$

等价地, $\mathrm{S}_d(z) = \frac{2^{lm}}{2^m+1}(2^{lm}n_\infty(z) - 2^m n_0(z) + n_1(z))$ 且 $2^{lm} \mid \mathrm{S}_d(z)$. 直接应用引理 3[49] 得到 (i) 的证明.

令 $A = \{\alpha^j \mid 0 \le j \le 2^m\}$. 由 $n_i(z)$ 的定义可知

$$n_\infty(z) = |\{x \in A \mid zx + x^{d2^{-s}} = 0\}|,$$

$$n_0(z) = |\{x \in A \mid (zx + x^{d2^{-s}})^{\frac{2^{2lm}-1}{2^m+1}} = 1\}|,$$
$$n_\infty(z) + n_0(z) + n_1(z) = 2^m + 1.$$

进一步, 由于 $(d2^{-s} - 1, 2^{2lm} - 1) = \frac{2^{2lm}-1}{2^m+1}$, 恰好存在 $2^m + 1$ 个 $z \in \mathrm{GF}(2^{2lm})$ 的选择使得 $n_\infty(z) = 1$.

以下, 我们将证明 (ii) 和 (iii). 由于 $\mathrm{S}_d(z)$ 取 0 值且至少一个负值 (引理 1[49]), 只需说明 $\mathrm{S}_d(z)$ 可取两个不同的正值. 以下, 我们分别讨论 $l > 2$ 和 $l = 2$ 这两个情形.

情形 1: $l > 2$

注意到 $n_\infty(z) + n_0(z) + n_1(z) = 2^m + 1$. 当 $n_\infty(z) = 1$, 由 (3.15), 我们有 $\mathrm{S}_d(z) \geq \frac{1}{2^m+1}2^{2lm} - 2^{(l+2)m} = \frac{2^{(l+2)m}(2^{(l-2)m}-1)}{2^m+1} > 2^{lm+1}$.

以下, 我们证明 $\mathrm{C}_d(z)$ 至少取四个值. 若不然, 假设 $\mathrm{S}_d(z)$ 取三个值 $\{u, v, 0\}$, 其中 $u > 2^{lm+1}$ 且 $v < 0$. 如果 $n_\infty(z) = 0$, 由 (3.15), 我们有 $\mathrm{S}_d(z) \leq 2^{lm}$. 因此, $\mathrm{S}_d(z)$ 取不同的值当 $n_\infty(z) = 0$ 和 $n_\infty(z) = 1$. 因此, 给定 $z \in \mathrm{GF}(2^{2lm})$, $\mathrm{S}_d(z) = u$ 当且仅当 $n_\infty(z) = 1$. 我们定义

$$N_u = |\{z \in \mathrm{GF}(2^{2lm}) \mid \mathrm{S}_d(z) = u\}|,$$
$$N_v = |\{z \in \mathrm{GF}(2^{2lm}) \mid \mathrm{S}_d(z) = v\}|,$$
$$N_0 = |\{z \in \mathrm{GF}(2^{2lm}) \mid \mathrm{S}_d(z) = 0\}|.$$

注意到恰好有 $2^m + 1$ 个 z 的选择使得 $n_\infty(z) = 1$. 我们得到 $N_u = 2^m + 1$. 另一方面, 由引理 3.9 的前两个式子, 我们有

$$uN_u + vN_v = 2^{2lm},$$
$$u^2N_u + v^2N_v = 2^{4lm}.$$

直接的计算说明 $N_u = \frac{2^{2lm}(v-2^{2lm})}{uv-v^2}$. 用 $v_2(k)$ 记整除 k 的最大的 2 幂次. 由于 $v_2(v) < 2lm$, 我们有 $v_2(2^{2lm}(v - 2^{2lm})) = v_2(v) + 2lm$ 且 $v_2(uv - v^2) = v_2(v) + v_2(u - v)$.

以下, 我们证明 $v_2(u - v) < 2lm$. 假设 $z_1 \in N_u$. 那么 $n_\infty(z_1) = 1, n_0(z_1) + n_1(z_1) =$

2^m 且

$$\begin{aligned} u = S_d(z_1) &= \frac{2^{lm}}{2^m+1}(2^{lm} - 2^m n_0(z_1) + n_1(z_1)) \\ &= \frac{2^{lm}}{2^m+1}(2^{lm} + 2^m(1 - n_0(z_1)) - n_0(z_1)). \end{aligned}$$

假设 $z_2 \in N_v$. 那么 $n_\infty(z_2) = 0, n_0(z_2) + n_1(z_2) = 2^m + 1$ 且

$$\begin{aligned} v = S_d(z_2) &= \frac{2^{lm}}{2^m+1}(-2^m n_0(z_2) + n_1(z_2)) \\ &= \frac{2^{lm}}{2^m+1}(2^m(1 - n_0(z_2)) - n_0(z_2) + 1). \end{aligned}$$

因此,

$$u - v = \frac{2^{lm}}{2^m+1}(2^{lm} + 2^m(n_0(z_2) - n_0(z_1)) + n_0(z_2) - n_0(z_1) - 1).$$

如果 $n_0(z_2)-n_0(z_1)-1 = 0$, 那么 $u-v = \frac{2^{lm}}{2^m+1}(2^{lm}+2^m)$ 且 $v_2(u-v) = (l+1)m < 2lm$. 如果 $n_0(z_2) - n_0(z_1) - 1 \neq 0$, 由于 $0 \leq n_0(z_1) \leq 2^m$ 且 $0 \leq n_0(z_2) \leq 2^m + 1$, 我们有 $v_2(n_0(z_2)-n_0(z_1)) \leq m$ 且 $v_2(n_0(z_2)-n_0(z_1)-1) \leq m$. 容易验证 $2^m(n_0(z_2)-n_0(z_1))+n_0(z_2) - n_0(z_1) - 1 \neq 0$ 且 $v_2(2^m(n_0(z_2) - n_0(z_1)) + n_0(z_2) - n_0(z_1) - 1) \leq 2m$. 因此, $v_2(u - v) \leq (l + 2)m < 2lm$.

所以, 我们有 $v_2(2^{2lm}(v-2^{2lm})) > v_2(uv-v^2)$, 蕴含了 N_u 是偶数. 这与 $N_u = 2^m+1$ 矛盾.

情形 2: $l = 2$

在此情形, $d = \frac{2^{4m}-1}{2^m+1} + 2^s$. 令 $D_0 = \{\alpha^{j\frac{2^{4m}-1}{2^m+1}} \mid 0 \leq j \leq 2^m\}$. 假设 $a = \alpha^{2^m+1}$ 且 $b = \alpha^{\frac{2^{4m}-1}{2^m+1}}$. 那么 $C_0 = \langle a\rangle$ 和 $D_0 = \langle b\rangle$. 由于 $(\frac{2^{4m}-1}{2^m+1}, 2^m + 1) = (2, 2^m + 1) = 1$, 任意 $x \in \mathrm{GF}(2^{2m})^*$ 可被唯一表为 $a^i b^k$, 对某个 $0 \leq i \leq \frac{2^{4m}-1}{2^m+1} - 1$ 和 $0 \leq k \leq 2^m$. 由于

$$zx + x^{d2^{-s}} = za^i b^k + (a^i b^k)^{d2^{-s}} = a^i(zb^k + b^{kd2^{-s}}),$$

$zx + x^{d2^{-s}}$ 属于 C_∞ (或 C_0, C_1) 当且仅当 $zb^k + b^{kd2^{-s}}$ 属于 C_∞ (或 C_0, C_1). 此外, 给定两个相异的 $x_1, x_2 \in A$ 满足 $x_1 = a^{i_1}b^{k_1}$ 且 $x_2 = a^{i_2}b^{k_2}$, 我们有 $k_1 \neq k_2$. 若不然,

$x_1x_2^{-1} \in C_0$, 由 A 的定义这是不可能的. 那么, 对 $i = 0, 1, \infty$,

$$\begin{aligned} n_i(z) &= |\{x \in A \mid zx + x^{d2^{-s}} \in C_i\}| \\ &= |\{0 \le k \le 2^m \mid zb^k + b^{kd2^{-s}} \in C_i\}| \\ &= |\{x \in D_0 \mid zx + x^{d2^{-s}} \in C_i\}|. \end{aligned}$$

由于 $(d2^{-s} - 1, 2^{4m} - 1) = \frac{2^{4m}-1}{2^m+1}$, 易知 $n_\infty(z) = 1$ 当且仅当 $z \in D_0$. 此外, 我们有

$$n_0(z) = |\{x \in D_0 \mid (zx + x^{d2^{-s}})^{\frac{2^{4m}-1}{2^m+1}} = 1\}|.$$

此后, 我们将 x 和 z 视作 D_0 的元素. 回顾 $x \in D_0$ 当且仅当 $x^{2^m+1} = 1$, 方程

$$(zx + x^{d2^{-s}})^{\frac{2^{4m}-1}{2^m+1}} = 1 \tag{3.16}$$

等价于

$$\begin{cases} zx + x^{d2^{-s}} \neq 0, \\ 1 + \frac{1}{zx^{d2^{-s}+1}} = 0. \end{cases} \tag{3.17}$$

令 $u = (d2^{-s} + 1, 2^m + 1)$, $1 + \frac{1}{zx^{d2^{-s}+1}} = 0$ 恰有 u 个解在 D_0 中.

如果 $u < 2^m + 1$, 由于 u 是 $2^m + 1$ 的一个因子, $u \le \frac{2^m+1}{3}$. 易知 $zx + x^{d2^{-s}} = 0$ 和 $1 + \frac{1}{zx^{d2^{-s}+1}} = 0$ 有公共解当且仅当 $z = 1$. 因此, 我们有

$$n_\infty(1) = 1, \quad n_0(1) = u - 1, \quad n_1(1) = 2^m - u + 1,$$

导出了

$$\begin{aligned} S_d(1) &= \frac{1}{2^m+1}(2^{4m} - 2^{3m}(u-1) + 2^{2m}(2^m - u + 1)) \\ &= 2^{3m} + \frac{2^{3m}}{2^m+1} - 2^{2m}u \\ &\ge 2^{3m} + \frac{2^{3m}}{2^m+1} - 2^{2m} \cdot \frac{2^m+1}{3} \\ &\ge 2^{2m+1}. \end{aligned}$$

类似地, 如果 $z \neq 1$, 我们有

$$n_\infty(z) = 1, \quad n_0(z) = u, \quad n_1(z) = 2^m - u,$$

蕴含了

$$\begin{aligned} \mathrm{S}_d(z) &= \frac{1}{2^m+1}(2^{4m} - 2^{3m}u + 2^{2m}(2^m - u)) \\ &= 2^{3m} - 2^{2m}u \\ &> 0. \end{aligned}$$

因此, 当 $u < 2^m + 1$, $\mathrm{S}_d(z)$ 取至少两个正值且其中一个不小于 2^{2m+1}.

如果 $u = 2^m + 1$, 类似可得

$$n_\infty(1) = 1, \quad n_0(1) = 2^m, \quad n_1(1) = 0,$$

蕴含了 $S_d(1) = 0$. 同时, 对 $z \neq 1$, 我们有

$$n_\infty(z) = 1, \quad n_0(z) = 0, \quad n_1(z) = 2^m,$$

蕴含了 $\mathrm{S}_d(z) = 2^{3m} \geq 2^{2m+1}$. 易知 $\mathrm{S}_d(z) = 2^{3m}$ 当且仅当 $z \in D_0 \setminus \{1\}$. 假设 $\mathrm{S}_d(z)$ 取三个值. 那么 2^{3m} 是 $\mathrm{S}_d(z)$ 取的唯一的正值. 假设 $\mathrm{S}_d(z) \in \{2^{3m}, v, 0\}$ 其中 $v < 0$. 因而,

$$\sum_{z \in \mathbb{F}_{2^{4m}}} \mathrm{S}_d(z) = 2^{3m} \cdot 2^m + vN_v < 2^{4m},$$

与引理 3.9 的第一个等式矛盾. □

注： 当 $l = 2$ 且 $s = 1, d = (2^{2m} + 1)(2^m - 1) + 2$ 是 Niho 指数. 这个采样在文献[221] 中被研究过, 其中 $\mathrm{C}_d(z)$ 恰好取四个值.

3.2.4 总结

在本节中, 我们得到了一个 m-序列和它的采样序列的互相关值的一些新结果.

我们的贡献有以下两点. 第一是确定了周期为 $3^{3r}-1$ 的三元 m-序列和 $d=3^r+2$ 或$d=3^{2r}+2$, 其中 $(r,3)=1$ 的采样序列的互相关分布. 第二是对周期为 $2^{2lm}-1$ 的二元 m-序列和 $d=\frac{2^{2lm}-1}{2^m+1}+2^s$, 其中 $l\geq 2$ 为偶数且 $0\leq s\leq 2m-1$ 的采样序列的互相关值得到了初步的结果. 我们证明了互相关值至少取四个值. 此外, 我们验证了 Sarwate 等人和 Helleseth 提出的两个著名的猜想在这个情况下成立. 对互相关值分布, 数值实验表明互相关值可能取八或九个值. 因此, 确定互相关值分布是一个非常困难的问题.

3.3 一类可约循环码的重量分层

3.3.1 引言

令 $\mathcal{C}$ 为 q 阶有限域 $\mathbb{F}_q$ 上的一个 $[n,k]$ 线性码, 亦即, $\mathcal{C}\subset\mathbb{F}_q^n$ 是 $\mathbb{F}_q$ 上一个 k-维线性空间. 对任意子码 $\mathcal{D}\subset\mathcal{C}$, $\mathcal{D}$ 的支集 (support) 定义为

$$\text{supp}(\mathcal{D})=\{i:0\leq i\leq n-1, c_i\neq 0 \text{ 对某个}(c_0,c_1,\ldots,c_{n-1})\in\mathcal{D}\}.$$

对 $1\leq r\leq k$, $\mathcal{C}$ 的 r-阶广义汉明重量 (generalized Hamming weight) 为

$$d_r(\mathcal{C})=\min\left\{|\text{supp}(\mathcal{D})|:\mathcal{D}\subset\mathcal{C}\text{ 且 }\dim_{\mathbb{F}_q}(\mathcal{D})=r\right\}.$$

此处 $|\text{supp}(\mathcal{D})|$ 为集合 $\text{supp}(\mathcal{D})$ 的大小. 集合 $\{d_r(\mathcal{C}):1\leq r\leq k\}$ 被称为 $\mathcal{C}$ 的重量分层 (weight hierarchy). 注意到 $d_1(\mathcal{C})$ 即是 $\mathcal{C}$ 的极小距离.

广义汉明重量的概念由 Helleseth, Kløve 和 Mykkeltveit 提出[138,180] 并首先被 Wei[281] 使用在密码学中去完全刻画一个线性码用于 II 型 wire-tap 信道[224] 中或作为一个 t-resilient 函数时的表现. 广义汉明重量可以用来刻画某些基于线性码的秘密共享方案的表现[183]. 最近, 广义汉明重量的概念被推广到线性网络编码中[222], 被用来刻画 wire-tap 网络中一个线性网络编码的表现[237]. 除了这些密码学方面的应用, 广义汉明重量提供了线性码详细的结构信息, 可以用来

1). 计算线性码的状态和分支复杂度谱 (state and branch complexity profiles)[109,174];

2). 指出有效的缩短码的方式[140];

3). 导出关于线性码的覆盖半径的微妙的上界[155];

4). 确定线性码的删除表译码能力(erasure list-decodability)[128];

5). 为某些码的表译码的提供表大小的上界[124].

总之, 线性码的广义汉明重量提供了在很多应用中起重要作用的基础信息.

在过去二十年中, 广义汉明重量的研究引起了广泛的关注, 在文献中已得到了很多结果. 例如, 广义汉明重量一般的上下界被导出[7,63,137,139,281], 一个有效的计算循环码的广义汉明重量的算法被提出[154], 对包括汉明码[281], Reed-Muller 码[129,281], 二元 Kasami 码[140], Melas 和对偶 Melas 码[263], BCH 码和它的对偶[57,61,100,103,209,246,264,266,267,270], 迹码[58,127,253,265,268], 乘积码[136,202,225,241,242,282], 代数几何码[13,28,71,143,146,212,213,296] 在内的许多类线性码的广义汉明重量已被确定或得到了估计. 然而, 一般而言, 计算线性码的广义汉明重量是困难的, 且完全的重量分层只在少数情况下已知 (见文献[13,140,141,143,225,269,281,282,296,297]). 用几何方法处理广义汉明重量的一个综述可参见[262].

在最近的一篇有趣的文章中[297], 作者利用数论方面的新想法研究了不可约循环码的广义汉明重量且在某些情况下得到了重量分层. 他们的工作扩展了以前的一些结果[141,269]. 受此启发, 在本节我们研究文献[295] 中引入的一族可约循环码的广义汉明重量. 这类循环码有任意多个非零点, 包含许多之前文献中研究过的循环码作为其中的子类. 特别地, 它包含文献[297] 研究的不可约循环码. 通过将文献[297] 中的思想拓展到高维并利用一些组合的技巧, 我们在一些情况下确定了这类循环码的重量分层.

3.3.2 主要结果

令 $q=p^s, Q=q^m$ 其中 p 是一个素数, s,m 是正整数. 令 γ 为有限域 $\mathbb{F}_Q$ 的一个本原元. 我们有以下三个假设:

i) $e \mid (Q-1), a \not\equiv 0 \pmod{Q-1}, e \geq t \geq 1$;

ii) 对 $1 \leq i \leq t$, $a_i \equiv a + \frac{Q-1}{e}\Delta_i \pmod{Q-1}$. 当 $t \geq 2$ 时, $\Delta_i \not\equiv \Delta_j \pmod{e}$ 对 $1 \leq i,j \leq t, i \neq j$ 且 $\gcd(\Delta_2-\Delta_1,\ldots,\Delta_t-\Delta_1,e)=1$;

iii) $\deg h_{a_i}(x) = m$ 对 $1 \leq i \leq t$ 且 $h_{a_i}(x) \neq h_{a_j}(x)$ 对 $i \neq j$. 此处 $h_a(x)$ 为 γ^{-a} 在 $\mathbb{F}_q$ 上的极小多项式.

定义

$$\delta = \gcd(Q-1, a_1, a_2, \ldots, a_t),$$
$$n = \frac{Q-1}{\delta}, \qquad N = \gcd\left(\frac{Q-1}{q-1}, ae\right).$$

易知 $\delta \mid \frac{Q-1}{e}$ 且

$$e\delta \mid N(q-1). \tag{3.18}$$

在以上三个假设下, 我们定义 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上长为 n, 校验多项式为 $\prod_{i=1}^{t} h_{a_i}(x)$ 的循环码, 其中 a_i 由假设所给出. 可知 $\mathcal{C}$ 是一个有 t 个非零点的 $[n, tm]$ 循环码.

我们指出这类循环码首先在文献[295]中提出, 并在几种情况下得出了它的重量分布. 由于参数 e, t, Δ_i 的灵活性, 这一类包含了许多的循环码. 我们指出这里一类包含许多有趣的码. 例如, 当 $q=2$, $a=-3$, $e=\frac{Q-1}{2}$, $t=2$ 且 $\Delta_i = i$ 对 $i=1,2$, 我们得到双错纠正的 BCH 码的对偶码. 当 q 是奇数, $a=-1$, $e=\frac{Q-1}{2}$, $t=2$ 且 $\Delta_i = i$ 对 $i=1,2$, 我们得到 q-元 Melas 码的对偶码. 此外, 根据 Grassl 维护的码表[119], 这一类循环码包含了一些具有已知最优参数的循环码 (见表 3.9).

表 3.9　属于所考虑的循环码类的具有已知最优参数的循环码

$[n,k,d]$	q	m	e	t	a	Δ_i	N
[63,12,24]	2	6	7	2	1	$\{0,1\}$	7
[85,16,32]	2	8	5	2	3	$\{0,1\}$	15
[255,16,112]	2	8	15	2	1	$\{0,1\}$	15
[255,24,100]	2	8	15	3	9	$\{0,1,14\}$	15
[80,8,48]	3	4	16	2	2	$\{0,1\}$	8
[80,12,42]	3	4	16	3	4	$\{0,1,7\}$	8
[242,10,153]	3	5	22	2	1	$\{0,1\}$	11
[242,15,138]	3	5	22	3	2	$\{0,1,15\}$	11

在本节中, 我们考虑这类码中的几个子类, 其中 $N \in \{1,2\}$. 本文中所引入的数论的方法对研究较大的 N 的情形亦有帮助. 在引理 6[295] 中提到假设 iii) 成立当 $N \le \sqrt{Q}$, 这对 $N=1,2$ 总是成立的. 我们有以下的主要结果:

定理 3.9: 令 $\mathcal{C}$ 为以上定义的循环码满足 $e=t\ge 1$. 令 $d_r := d_r(\mathcal{C})$ 为 $\mathcal{C}$ 的 r-阶广义汉明重量.

(i). 如果 $N=1$, 我们有

$$d_r=\frac{q^m-1}{\delta}\left(1-\frac{s}{t}\right)-\frac{q^{(t-s)m-r}-1}{t\delta},\quad \text{如果 } (t-s-1)m<r\le(t-s)m,$$

其中$0\le s\le t-1$.

(ii). 如果 $N=2$, 我们有

$$d_r=\begin{cases}\frac{q^m-1}{\delta}(1-\frac{s}{t})-\frac{1}{t\delta}(q^{(t-s-\frac{1}{2})m-r}+1)(q^{\frac{m}{2}}-1) & \text{如果 } (t-s-1)m<r\le\left(t-s-\frac{1}{2}\right)m,\\ \frac{q^m-1}{\delta}\left(1-\frac{s}{t}\right)-\frac{2}{t\delta}(q^{(t-s)m-r}-1) & \text{如果 } \left(t-s-\frac{1}{2}\right)m<r\le(t-s)m,\end{cases}$$

其中 $0\le s\le t-1$.

定理 3.10: 令 $\mathcal{C}$ 为一个以上定义的循环码满足 $e>t\ge 1$ 且 $N=1$. 假设 $\{\Delta_1 \pmod e,\ldots,\Delta_t \pmod e\}$ 是一个等差数列. 令 $d_r:=d_r(\mathcal{C})$ 为 $\mathcal{C}$ 的 r-阶广义汉明重量. 那么

$$d_r=\begin{cases}\frac{q^m-1}{\delta}(1-\frac{t-1}{e})-\frac{e-t+1}{e\delta}(q^{m-r}-1) & \text{如果 } 1\le r\le m,\\ \frac{q^m-1}{\delta}(1-\frac{s}{e})-\frac{q^{(t-s)m-r}-1}{e\delta} & \text{如果 } (t-s-1)m<r\le(t-s)m,\end{cases}$$

其中 $0\le s\le t-2$.

我们指出当 $t=1$, 定理 3.9 和 3.10 分别退化为推论 3.2[297] 和定理 4.1[297]. 当 $t\ge 2$, 这些结果是新的.

接下来, 为了展示定理 3.9 和 3.10 正确性, 我们给出一些数值实验的例子.

例 3.7: 对 $q=3, m=3, e=t=2$ 和 $a=1$, 这是一个 $\mathbb{F}_3$ 上的 $[26,6,9]$ 循环码满足 $N=1$. 利用 **Magma** 我们得到

$$d_1=9, d_2=12, d_6=26,$$

与定理 3.9 的 (i) 一致. 注意到计算 d_3, d_4 和 d_5 会花费太多时间. 因此, 在这种情况下我们只能得到部分的重量分层.

例 3.8: 对 $q=5, m=2, e=t=2$ 和 $a=2$, 这是一个 $\mathbb{F}_5$ 上的 $[12,4,4]$ 循环码满足 $N=2$. 利用 **Magma** 我们得到

$$d_1=4, d_2=6, d_3=10, d_4=12,$$

与定理 3.9 的 (ii) 一致.

例 3.9: 对 $q=4, m=2, e=3, t=2, a=1, \Delta_1=0$ 和 $\Delta_2=1$, 这是一个 $\mathbb{F}_4$ 上的 $[15,4,8]$ 循环码满足 $N=1$. 利用 **Magma** 我们得到

$$d_1=8, d_2=10, d_3=14, d_4=15,$$

与定理 3.10 一致.

3.3.3 背景知识

在本小节中, 我们介绍一些背景知识.

3.3.3.1 循环码

令 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上一个 $[n,k]$ 线性码. 假设 $(n,q)=1$. $\mathcal{C}$ 被称为是循环的, 如果 $(c_{n-1},c_0,\ldots,c_{n-2})\in\mathcal{C}$ 当 $(c_0,c_1,\ldots,c_{n-1})\in\mathcal{C}$. 对循环码 $\mathcal{C}$, 每个码字 $c=(c_0,\ldots,c_{n-1})$ 可与主理想整环 $R_n:=\mathbb{F}_q[x]/(x^n-1)$ 中一个多项式 $\sum_{i=0}^{n-1}c_ix^i$ 相联系. 据此, $\mathcal{C}$ 可被等同于 R_n 中的一个理想. 那么, 存在一个唯一的首一多项式 $g(x)\in\mathbb{F}_q[x]$ 满足 $g(x)\mid x^n-1$, $\mathcal{C}=(g(x))R_n$ 且 $g(x)$ 在 $\mathcal{C}$ 的元素中有最小的次数. 这个 $g(x)$ 被称为 $\mathcal{C}$ 的生成多项式 (generator polynomial). $h(x)=\frac{x^n-1}{g(x)}$ 是 $\mathcal{C}$ 的校验多项式 (parity check polynomial). 当 R_n 固定时, 一个循环码可由生成多项式或校验多项式唯一确定. $\mathcal{C}$ 有 i 个零点 (zeroes) 如果它的生成多项式可被分解为 $\mathbb{F}_q$ 上 i 个不可约多项式的乘积. 当对偶码 $\mathcal{C}^\perp$ 有 i 个零点时, 我们称 $\mathcal{C}$ 有 i 个非零点 (nonzeroes). 因此, 小节 3.3.2 中定义的循环码有任意多个非零点.

3.3.3.2 群特征, 高斯和及高斯周期

令 $q=p^s$ 其中 p 是一个素数. $\mathbb{F}_q$ 的典范加法特征 (canonical additive character) ψ_q

定义做

$$\begin{aligned}\psi_q : \mathbb{F}_q &\longrightarrow \mathbb{C}\\ x &\mapsto \zeta_p^{\mathrm{Tr}_p^q(x)},\end{aligned}$$

其中 $\zeta_p = \exp\left(2\pi\sqrt{-1}/p\right)$ 是本原 p-次复单位根, 且 Tr_p^q 是从 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的迹函数. 如果 Q 是 q 的一个幂次, 由迹函数的传递性我们有 $\psi_Q = \psi_q \circ \mathrm{Tr}_q^Q$.

令 $\chi : \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \to \mathbb{C}$ 为一个乘法特征, 亦即, $\chi(xy) = \chi(x)\chi(y)$ 对任意 $x, y \in \mathbb{F}_q^*$. 令 $\chi(0) = 0$, 我们将 χ 的定义延拓至 $\mathbb{F}_q$. 相应的高斯和 (Gauss sum) $G(\chi)$ 定义做

$$G(\chi) = \sum_{x\in\mathbb{F}_q} \chi(x)\psi_q(x),$$

其中 ψ_q 是 $\mathbb{F}_q$ 上典范的加法特征. 如果 χ 的阶为 2, χ 被称为 $\mathbb{F}_q$ 的二次特征且相应的高斯和为二次高斯和. 二次高斯和的值是已知的.

引理 3.12 (**定理** 5.15[190]): 令 $q = p^s$ 且 χ 为 $\mathbb{F}_q$ 的二次特征 (因此 p 是奇数). 那么

$$G(\chi) = \begin{cases} (-1)^{s-1}\sqrt{q} & \text{如果 } p \equiv 1 \bmod 4,\\ (-1)^{s-1}\left(\sqrt{-1}\right)^s\sqrt{q} & \text{如果 } p \equiv 3 \bmod 4.\end{cases}$$

令 γ 为 $\mathbb{F}_Q$ 的一个本原元. 对 $N \mid (Q-1)$, 记 $\langle\gamma^N\rangle$ 为 γ^N 生成的循环群. 对任意 $0 \le i \le N-1$, $C_i^{(N,Q)} = \gamma^i\langle\gamma^N\rangle$ 被称为 $\mathbb{F}_Q$ 的 i-次分圆类. 对任意 $a \in \mathbb{F}_Q$, 定义高斯周期 (Gauss period) $\eta_a^{(N,Q)}$ 为

$$\eta_a^{(N,Q)} = \sum_{x\in C_0^{(N,Q)}} \psi_Q(ax).$$

3.3.4 广义汉明重量的一个表达式

令 $\mathcal{C}$ 为小节 3.3.2 中定义的循环码. 由 Delsarte 定理[72], $\mathcal{C}$ 的元素可被唯一表成 $c(\underline{x}) = (c_i(\underline{x}))_{i=1}^n$ 其中 $\underline{x} = (x_1, x_2, \ldots, x_t)$ 跑遍集合 $\mathbb{F}_Q^t$ 且

$$c_i(\underline{x}) = \mathrm{Tr}_q^Q\left(\sum_{j=1}^t x_j\gamma^{a_j i}\right), \quad 1 \le i \le n.$$

换言之, 映射

$$\Psi : \mathbb{F}_Q^t \longrightarrow \mathcal{C},$$
$$\underline{x} \mapsto c(\underline{x})$$

是两个 $\mathbb{F}_q$-向量空间 $\mathbb{F}_Q^t$ 和 $\mathcal{C}$ 的同构, 因而诱导了 $\mathbb{F}_Q^t$ 的 r-维 $\mathbb{F}_q$-子空间和 $\mathcal{C}$ 的 r-维子码之间的一个 1-1 映射, 其中 $1 \leq r \leq tm$. 对任意 $\mathbb{F}_q$-向量空间 M, 记 $\begin{bmatrix} M \\ r \end{bmatrix}$ 为 M 的 r-维 $\mathbb{F}_q$-子空间组成的集合.

对任意 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, 定义

$$N(H_r) = |\{i : 1 \leq i \leq n, c_i(\underline{b}) = 0, \forall \underline{b} \in H_r\}|,$$

且对任意 $1 \leq r \leq tm$, 定义

$$N_r = \max\left\{ N(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}.$$

由于 Ψ 是一个同构, 由定义, $\mathcal{C}$ 的 r-阶广义汉明重量可表为

$$d_r := d_r(\mathcal{C}) = n - N_r.$$

令 $\underline{\epsilon_1}, \ldots, \underline{\epsilon_r}$ 为 H_r 的一个 $\mathbb{F}_q$-基. 那么,

$$c_i(\underline{b}) = 0, \forall \underline{b} \in H_r \Longleftrightarrow c_i(\underline{\epsilon_j}) = 0, \forall 1 \leq j \leq r.$$

我们用 ψ_Q (或 ψ_q) 记 $\mathbb{F}_Q$ (或 $\mathbb{F}_q$) 的典范加法特征. 由 ψ_q 的正交性我们有

$$\begin{aligned} N(H_r) &= \sum_{i=1}^{n} \left\{ \frac{1}{q} \sum_{x_1 \in \mathbb{F}_q} \psi_q(x_1 c_i(\underline{\epsilon_1})) \right\} \cdots \left\{ \frac{1}{q} \sum_{x_r \in \mathbb{F}_q} \psi_q(x_r c_i(\underline{\epsilon_r})) \right\} \\ &= \frac{1}{q^r} \sum_{i=1}^{n} \sum_{x_1, \ldots, x_r \in \mathbb{F}_q} \psi_q(c_i(x_1\underline{\epsilon_1} + \cdots + x_r\underline{\epsilon_r})) \\ &= \frac{1}{q^r} \sum_{i=1}^{n} \sum_{\underline{b} \in H_r} \psi_q(c_i(\underline{b})) = \frac{n}{q^r} + \frac{1}{q^r} \sum_{i=1}^{n} \sum_{\underline{b} \in H_r^*} \psi_q(c_i(\underline{b})), \end{aligned}$$

其中 $H_r^* = H_r \setminus \{0\}$. 回顾 $\gamma^{a_j} = \gamma^{a+\frac{Q-1}{e}\Delta_j}$. 令 $\beta_j = \gamma^{\frac{Q-1}{e}\Delta_j}$, 我们有 $\gamma^{a_j} = \gamma^a\beta_j$. 那么,

$$\begin{aligned}(q-1)N(H_r) &= \frac{n(q-1)}{q^r} + \frac{1}{q^r}\sum_{i=1}^{n}\sum_{\underline{b}\in H_r^*}\sum_{x\in\mathbb{F}_q^*}\psi_q(c_i(x\underline{b})) \\ &= \frac{n(q-1)}{q^r} + \frac{1}{q^r}\sum_{i=1}^{n}\sum_{\underline{b}\in H_r^*}\sum_{x\in\mathbb{F}_q^*}\psi_q\left(x\mathrm{Tr}_q^Q\left(\sum_{j=1}^{t}b_j\gamma^{a_ji}\right)\right) \\ &= \frac{n(q-1)}{q^r} + \frac{1}{q^r}\sum_{\underline{b}\in H_r^*}\sum_{i=1}^{n}\sum_{x\in\mathbb{F}_q^*}\psi_Q\left(x\gamma^{ai}\sum_{j=1}^{t}b_j\beta_j^i\right).\end{aligned}$$

注意到 $e \mid \frac{Q-1}{\delta} = n$, 任意 $1 \le i \le n$ 可被表为 $i = ej + h$ 其中 $0 \le j \le \frac{n}{e} - 1$ 且 $1 \le h \le e$. 那么, 右边第二项可写做

$$\frac{1}{q^r}\sum_{\underline{b}\in H_r^*}\sum_{j=0}^{\frac{n}{e}-1}\sum_{h=1}^{e}\sum_{x\in\mathbb{F}_q^*}\psi_Q\left(x\gamma^{aej}\gamma^{ah}\sum_{j=1}^{t}b_j\beta_j^h\right).$$

注意到 $\mathbb{F}_q^* = \left\langle\gamma^{\frac{Q-1}{q-1}}\right\rangle$ 且 $N = \gcd\left(\frac{Q-1}{q-1}, ae\right)$, 容易验证

$$\left\{x\gamma^{aej} \mid x\in\mathbb{F}_q^*, 0\le j\le\frac{n}{e}-1\right\} = \frac{(q-1)N}{e\delta} * C_0^{(N,Q)},$$

其中我们用 $l * A$ 记一个 A 的每个元素出现 l 次的多重集. 因而, 我们有

$$\begin{aligned}&\frac{1}{q^r}\sum_{\underline{b}\in H_r^*}\sum_{j=0}^{\frac{n}{e}-1}\sum_{h=1}^{e}\sum_{x\in\mathbb{F}_q^*}\psi_Q\left(x\gamma^{aej}\gamma^{ah}\sum_{j=1}^{t}b_j\beta_j^h\right) \\ =&\frac{(q-1)N}{e\delta q^r}\sum_{\underline{b}\in H_r^*}\sum_{h=1}^{e}\sum_{y\in C_0^{(N,Q)}}\psi_Q\left(y\gamma^{ah}\sum_{j=1}^{t}b_j\beta_j^h\right).\end{aligned}$$

令 $g = \gamma^a$, 我们有

$$(q-1)N(H_r) = \frac{(q-1)n}{q^r} + \frac{(q-1)N}{e\delta q^r}\sum_{\underline{b}\in H_r^*}\sum_{h=1}^{e}\sum_{y\in C_0^{(N,Q)}}\psi_Q\left(yg^h\sum_{j=1}^{t}b_j\beta_j^h\right).$$

亦即,

$$N(H_r) = \frac{N}{e\delta q^r}\sum_{\underline{b}\in H_r}\sum_{h=1}^{e}\eta_{g^h\sum_{j=1}^{t}b_j\beta_j^h}^{(N,Q)}. \tag{3.19}$$

因此, 为了计算 $\mathcal{C}$ 的广义汉明重量, 只需对所有 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$ 确定以上高斯周期的和的最大值. 这个问题一般而言是困难的. 然而, 当和式中的高斯周期去少数几个值, 有希望完全确定广义汉明重量. 因而, N 的值是计算中的一个关键点. 以下我们将考虑最简单的情形 $N \in \{1, 2\}$. 我们首先处理 $e = t$ 的情况.

3.3.5 定理 3.9 (i) 的证明

回顾 $\beta_j = \gamma^{\frac{Q-1}{t}\Delta_j}$ 对 $1 \le j \le t$ 且 $g = \gamma^a$. 定义 $\beta = \gamma^{\frac{Q-1}{t}}$. 由于 $\beta_j^t = 1$ 对任意 $1 \le j \le t$ 且 β_j 互不相同, 我们可以不失一般性假设 $\beta_j = \beta^j$, $1 \le j \le t$. 将 $\underline{b} = (b_1, \ldots, b_t) \mapsto \underline{y} = (y_1, \ldots, y_t)$ 替换为 $y_i = g^i \sum_{j=1}^t b_j \beta^{ij}, 1 \le i \le t$. 这给出了一个 $\mathbb{F}_q$-同构 $\phi : \mathbb{F}_Q^t \longrightarrow \mathbb{F}_Q^t$. 因此 (3.19) 可以重写作

$$N(H_r) = \frac{N}{t\delta q^r} \sum_{\underline{y} \in \phi(H_r)} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)}.$$

定义

$$\widetilde{N}(H_r) = \frac{N}{t\delta q^r} \sum_{\underline{y} \in H_r} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)}.$$

显然,

$$\max\left\{ N(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\} = \max\left\{ \widetilde{N}(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}.$$

因此, 我们专注于考虑

$$\begin{aligned} N_r &= \max\left\{ \widetilde{N}(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\} \\ &= \frac{N}{t\delta q^r} \max\left\{ F(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix} \right\}, \end{aligned} \tag{3.20}$$

其中

$$F(H_r) = \sum_{\underline{y} \in H_r} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)}. \tag{3.21}$$

我们现在证明定理 3.9 的 (i).

证明. 由于 $N=1$, 由 (3.18), 我们有 $e\delta \mid (q-1)$ 且 $e=t\le q-1$. 回顾

$$\eta_a^{(1,Q)}=\begin{cases} Q-1 & \text{如果 } a=0,\\ -1 & \text{如果 } a\neq 0.\end{cases}$$

对任意 $H_r\in\begin{bmatrix}\mathbb{F}_Q^t\\ r\end{bmatrix}$ 且任意 $1\le h\le t$, 定义

$$V_h=\underbrace{\mathbb{F}_Q\times\cdots\times\mathbb{F}_Q}_{h-1}\times\underset{h}{\{0\}}\times\underset{h+1}{\mathbb{F}_Q}\times\ldots\times\underset{t}{\mathbb{F}_Q}$$

和

$$v_h:=v_h(H_r)=\dim_{\mathbb{F}_q}(H_r\cap V_h).$$

那么, 由 (3.21),

$$\begin{aligned}F(H_r)&=\sum_{h=1}^{t}(|H_r\cap V_h|(Q-1)-(q^r-|H_r\cap V_h|))\\&=\sum_{h=1}^{t}(q^{v_h}(Q-1)-(q^r-q^{v_h}))\\&=Q\sum_{h=1}^{t}q^{v_h}-tq^r.\end{aligned}$$

因此, 对任意 r-维子空间 H_r, $(v_1(H_r),\ldots,v_t(H_r))$ 完全决定了 $F(H_r)$.

为了找到 $\max\left\{F(H_r):H_r\in\begin{bmatrix}\mathbb{F}_Q^t\\ r\end{bmatrix}\right\}$, 我们假设 $v_1\ge v_2\ge\cdots\ge v_t$, 因为 v_h 的顺序不产生影响. 我们采用如下操作: 首先选取 H_r 最大化 $v_1=v_1(H_r)$; 一旦 $v_1,\ldots,v_i$ 对 $i\ge 1$ 被确定, 在这些 H_r 中我们选取最大化 v_{i+1} 的. 由于 $t\le q-1$, 易知这个操作将会得出最大化 $F(H_r)$ 的 H_r.

假设 $(t-s-1)m<r\le(t-s)m$ 对某个 s 属于 $0\le s\le t-1$. 注意到

$$\dim_{\mathbb{F}_q}\left(\bigcap_{i=1}^{s}V_i\right)=(t-s)m,\quad \dim_{\mathbb{F}_q}\left(\bigcap_{i=1}^{s+1}V_i\right)=(t-s-1)m,$$

我们取 $v_1=\ldots=v_s=r$, 这个取法显然是最大的. 这意味着 $H_r\subset\bigcap_{i=1}^{s}V_i$. 为了让 v_{s+1} 最大, 我们应取 $\bigcap_{i=1}^{s+1}V_i\subset H_r\subset\bigcap_{i=1}^{s}V_i$, 满足 $v_{s+1}=(t-s-1)m$. 在这样的条件下,

H_r 形如

$$H_r = \underbrace{\{0\} \times \cdots \times \{0\}}_{s} \times \underset{s+1}{H} \times \underset{s+2}{\mathbb{F}_Q} \times \ldots \times \underset{t}{\mathbb{F}_Q},$$

其中 $H \subset \mathbb{F}_Q$ 是任意的 $r-(t-s-1)m$-维 $\mathbb{F}_q$-线性空间, 我们得到

$$v_h = v_h(H_r) = \begin{cases} r & 1 \le h \le s, \\ (t-s-1)m & h = s+1, \\ r-m & s+2 \le h \le t. \end{cases}$$

因此我们有

$$\max\left\{F(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}\right\} = Q\left(sq^r + q^{(t-s-1)m} + (t-s-1)q^{r-m}\right) - tq^r,$$

且

$$\begin{aligned} d_r &= n - \frac{1}{t\delta q^r}\max\left\{F(H_r) \mid H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}\right\} \\ &= \frac{q^m-1}{\delta}(1-\frac{s}{t}) - \frac{q^{(t-s)m-r}-1}{t\delta}. \end{aligned}$$

□

3.3.6 定理 3.9 (ii) 的证明

对 $t = e \ge 1$ 且 $N = 2$, 情况更加复杂. 受文献[297] 启发, 我们采取一个适用于 $N \ge 2$ 的新策略.

3.3.6.1 一个新策略

令 $\langle \cdot, \cdot \rangle : \mathbb{F}_Q^t \times \mathbb{F}_Q^t \to \mathbb{F}_q$ 为非退化双线性型

$$\langle \underline{x}, \underline{y} \rangle = \mathrm{Tr}_q^Q\left(\sum_{i=1}^{t} x_i y_i\right), \quad \forall\, \underline{x} = (x_1, \ldots, x_t), \underline{y} = (y_1, \ldots, y_t) \in \mathbb{F}_Q^t.$$

对 $\mathbb{F}_Q^t$ 的任意 $\mathbb{F}_q$-子空间 H, 定义

$$H^\perp = \{y \in \mathbb{F}_Q^t \mid \langle \underline{x}, \underline{y} \rangle = 0, \forall \underline{x} \in H\}.$$

我们有以下引理.

引理 3.13: 假设 $H \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$. 那么 $\dim_{\mathbb{F}_q} H^\perp = tm - r$ 且

$$\frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^\perp} \psi_q\left(\langle \underline{x}, \underline{y} \rangle\right) = \begin{cases} 1 & \text{如果 } \underline{x} \in H, \\ 0 & \text{如果 } \underline{x} \notin H. \end{cases}$$

证明. 令 $A = \frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^\perp} \psi_q(\langle \underline{x}, \underline{y} \rangle)$. 如果 $\underline{x} \in H$, 那么 $\langle \underline{x}, \underline{y} \rangle = 0, \forall \underline{y} \in H^\perp$. 因此, $A = 1$. 如果 $\underline{x} \notin H$, 那么存在 $\underline{y} \in H^\perp$ 使得 $\langle \underline{x}, \underline{y} \rangle \neq 0$. 特别地, 存在 $\underline{y_0} \in H^\perp$, 使得 $\psi_q(\langle \underline{x}, \underline{y_0} \rangle) \neq 1$. 那么,

$$\begin{aligned} A \cdot \psi_q(\langle \underline{x}, \underline{y_0} \rangle) &= \frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^\perp} \psi_q(\langle \underline{x}, \underline{y} \rangle + \langle \underline{x}, \underline{y_0} \rangle) \\ &= \frac{1}{q^{tm-r}} \sum_{\underline{y} \in H^\perp} \psi_q(\langle \underline{x}, \underline{y} + \underline{y_0} \rangle) = A. \end{aligned}$$

因此 $A = 0$. □

由以上引理, 我们可以计算 (3.21) 中的 $F(H_r)$.

$$\begin{aligned} F(H_r) &= \sum_{\underline{y} \in H_r} \sum_{h=1}^{t} \eta_{y_h}^{(N,Q)} = \sum_{h=1}^{t} \sum_{\underline{y} \in \mathbb{F}_Q^t} \eta_{y_h}^{(N,Q)} \frac{1}{q^{tm-r}} \sum_{\underline{x} \in H_r^\perp} \psi_q(\langle \underline{x}, \underline{y} \rangle) \\ &= \frac{1}{q^{tm-r}} \sum_{h=1}^{t} \sum_{\underline{x} \in H_r^\perp} \sum_{z \in C_0^{(N,Q)}} \sum_{\underline{y} \in \mathbb{F}_Q^t} \psi_Q(z y_h) \psi_q\left(\mathrm{Tr}_q^Q\left(\sum_{i=1}^{t} x_i y_i\right)\right) \\ &= \frac{1}{q^{tm-r}} \sum_{h=1}^{t} \sum_{\underline{x} \in H_r^\perp} \sum_{z \in C_0^{(N,Q)}} \sum_{y_1, \ldots, y_t \in \mathbb{F}_Q} \psi_Q\left(z y_h + \sum_{i=1}^{t} x_i y_i\right) \\ &= q^r \sum_{h=1}^{t} \sum_{\underline{x} \in H_r^\perp} \sum_{\substack{z \in C_0^{(N,Q)} \\ z + x_h = 0 \\ x_i = 0, \forall\, i \neq h}} 1. \end{aligned}$$

对任意 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$ 且 $1 \leq h \leq t$, 定义

$$W_h := W_h(N) = \underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times (-C_0^{(N,Q)}) \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}}$$

且

$$U_h := U_h(H_r) = H_r^{\perp} \bigcap \Big(\underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underset{h}{\mathbb{F}_Q} \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}} \Big).$$

我们有

$$F(H_r) = q^r \sum_{h=1}^{t} |H_r^{\perp} \cap W_h| = q^r \sum_{h=1}^{t} |U_h \cap W_h|. \tag{3.22}$$

因此对 $t = e \geq 1$ 和 $N \geq 2$, 为了计算广义汉明重量, 只需确定 $\sum_{h=1}^{t} |U_h \cap W_h|$ 的最大值对所有 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$.

我们指出由于 $H_r^{\perp} = \bigoplus_{h=1}^{t} U_h$, 空间 $H_r^{\perp}$ 和 H_r 可由$(U_1, \ldots, U_t)$ 唯一恢复出来, 其中 U_h 是 $\underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underset{h}{\mathbb{F}_Q} \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}}$ 的一个子空间. 令 $r' = tm - r$ 且令 $u_h = \dim_{\mathbb{F}_q}(U_h)$, u_h 满足 $\sum_{h=1}^{t} u_h = r'$. 为了找到 $\sum_{h=1}^{t} |U_h \cap W_h|$ 的最大值, 我们考虑以下两步:

1). 对每个合理的 $(u_1, \ldots, u_h)$, 确定维数为 u_h 的子空间 U_h 使得 $|U_h \cap W_h|$ 对每个 h 是最大的;

2). 考虑所有合理的 $(u_1, \ldots, u_h)$ 并找出最大值.

现在我们专注于 $N = 2$ 的情形.

3.3.7 一个引理

由于 $N = 2$, q 是奇数且 m 是偶数. 注意到 $Q = q^m$. 我们需要以下的引理.

引理 3.14: 令 $0 \leq l \leq m$ 且 $H \subset \mathbb{F}_Q$ 为一个 l-维 $\mathbb{F}_q$-子空间. 令 γ 为 $\mathbb{F}_Q$ 的一个本原元. 定义函数

$$f(l) := \begin{cases} q^l - 1 & \text{如果 } 0 \leq l \leq \frac{m}{2}, \\ \frac{q^l - 1}{2} + \frac{q^{\frac{m}{2}} - q^{l - \frac{m}{2}}}{2} & \text{如果 } \frac{m}{2} \leq l \leq m. \end{cases}$$

那么, 对 $0 \leq l \leq m$,

$$\max \left\{ \left| H \cap C_i^{(2,Q)} \right| : H \subset \mathbb{F}_Q, \dim_{\mathbb{F}_q}(H) = l \right\} = f(l),$$

其中 $i \in \{0, 1\}$. 进一步, 达到最大值的子空间 $H \subset \mathbb{F}_Q$ 可以如下选取:

1) 如果 $0 \leq l \leq \frac{m}{2}$, 那么我们可以选取任意的 $H \subset \gamma^i \mathbb{F}_{q^{\frac{m}{2}}}$;

2) 如果 $\frac{m}{2} \leq l \leq m$, 假设 $G(\chi) = (-1)^j q^{\frac{m}{2}}$ 对某个 $j \in \{0,1\}$, 其中 χ 是 $\mathbb{F}_Q$ 的二次特征. 那么我们可以选取 H 满足 $H^\perp \subset C_{i+j}^{(2,Q)} \cup \{0\}$, 其中 $H^\perp$ 是 H 关于非退化双线性型$\langle \cdot, \cdot \rangle : \mathbb{F}_Q \times \mathbb{F}_Q \to \mathbb{F}_q$

$$\langle x, y \rangle = \mathrm{Tr}_q^Q (xy), \forall x, y \in \mathbb{F}_Q,$$

的正交补.

证明. 我们仅证明 $i = 0$ 的情况. $i = 1$ 的情况是类似的.

如果 $0 \leq l \leq \frac{m}{2}$, 那么 $\mathbb{F}^*_{q^{\frac{m}{2}}} \subset C_0^{(2,Q)}$. 注意到 $\dim_{\mathbb{F}_q} \left(\mathbb{F}_{q^{\frac{m}{2}}} \right) = \frac{m}{2}$. 对任意 $H \subset \mathbb{F}_{q^{\frac{m}{2}}}$, 我们有 $|H \cap C_0^{(2,Q)}| = q^l - 1$, 显然是最大值.

如果 $\frac{m}{2} \leq l \leq m$, 那么

$$|H \cap C_0^{(2,Q)}| = \sum_{a \in H \setminus \{0\}} \frac{1}{2}(1 + \chi(a)) = \frac{q^l - 1}{2} + \frac{1}{2} \sum_{a \in H} \chi(a).$$

注意到

$$\begin{aligned} \sum_{a \in H} \chi(a) &= \sum_{a \in \mathbb{F}_Q} \frac{\chi(a)}{q^{m-l}} \sum_{b \in H^\perp} \psi_q(\langle a, b \rangle) \\ &= \frac{1}{q^{m-l}} \sum_{b \in H^\perp} \chi(b) \sum_{a \in \mathbb{F}_Q} \chi(ab) \psi_q(\langle a, b \rangle) \\ &= \frac{G(\chi)}{q^{m-l}} \sum_{b \in H^\perp} \chi(b). \end{aligned}$$

由于 $\dim_{\mathbb{F}_q}(H^\perp) = m - l \leq \frac{m}{2}$, 我们可选择 $H^\perp$ 满足 $H^\perp \subset C_j^{(2,Q)} \cup \{0\}$. 因此, 我们有 $\chi(b) = (-1)^j, \forall b \in H^\perp \setminus \{0\}$. 所以,

$$\sum_{a \in H} \chi(a) = \frac{q^{\frac{m}{2}}}{q^{m-l}} \sum_{b \in H^\perp \setminus \{0\}} 1 = q^{\frac{m}{2}} - q^{l - \frac{m}{2}}.$$

这显然是 $\sum_{a\in H}\chi(a)$ 最大的值. 因此,

$$\left|H\cap C_0^{(2,Q)}\right| = \frac{q^l-1}{2} + \frac{q^{\frac{m}{2}} - q^{l-\frac{m}{2}}}{2} = f(l)$$

是最大值当 $\frac{m}{2} \le l \le m$. □

3.3.8 证明

我们现在叙述定理 3.9 的 (ii) 的证明. 回顾 H_r 可由 $(U_1,\ldots,U_t)$ 恢复, 其中 U_h 是 u_h-维子空间满足 $\sum_{h=1}^t u_h = r' = tm - r$. 对任意合理的 $(u_1,\ldots,u_t)$, 引理 3.14 说明了怎样选取 $(U_1,\ldots,U_t)$ 使得 $|U_h\cap W_h|$ 对每个 $1\le h\le t$ 达到最大值 $f(u_h)$. 因而只需决定能给出最大值 $\sum_{h=1}^t f(u_h)$ 的 $(u_1,\ldots,u_t)$, 其中 $(u_1,\ldots,u_t)$ 满足 $0\le u_h\le m, \forall h$ 和 $\sum_{h=1}^t u_h = r'$. 不失一般性, 假设 $u_1\ge\cdots\ge u_t$.

以下引理用于决定最大值 $\sum_{h=1}^t f(u_h)$. 定义有限集 $\mathcal{L} = \{(l_1,\ldots,l_t) \mid 0\le l_1,\ldots,l_t\le m, l_1\ge l_2\ge\cdots\ge l_t\}$ 且对每个 $0\le s\le tm$ 一个子集 $\mathcal{L}_s = \{(l_1,\ldots,l_t)\in\mathcal{L} \mid \sum_{i=1}^t l_i = s\}$. 我们在 $\mathcal{L}_s$ 上定义以下的偏序: 对任意 $\underline{l} = (l_1,\ldots,l_t), \underline{l'} = (l'_1,\ldots,l'_t)\in\mathcal{L}_s$, 我们说 $\underline{l}\succ\underline{l'}$ 如果存在一个整数 $i, 1\le i\le t$, 使得 $l_j = l'_j, \forall 1\le j\le i-1$ 且 $l_i > l'_i$. 易知 $\succ$ 给出 $\mathcal{L}_s$ 上一个全序.

引理 3.15: 对任意 $\underline{l},\underline{l'}\in\mathcal{L}_s$, 如果 $\underline{l}\succ\underline{l'}$, 那么 $\sum_{h=1}^t f(l_h)\ge\sum_{h=1}^t f(l'_h)$.

证明. 对任意 $\underline{l} = (l_1,\ldots,l_t)\in\mathcal{L}_s$, 定义 $f(\underline{l}) = \sum_{h=1}^t f(l_h)$. 为了简便定义 $l_0 := m$. 假设 $l_i < l_{i-1}$ 且 $l_j\ge 1$ 对某些 i,j 满足 $1\le i<j\le t$. 我们可以定义关于 $\underline{l}$ 的一个操作 $S_{i,j}$ 如下:

$$S_{i,j}(\underline{l}) = (l_1,\ldots,l_{i-1},l_i+1,l_{i+1},\ldots,l_{j-1},l_j-1,l_{j+1},\ldots,l_t).$$

显然 $S_{i,j}(\underline{l})\in\mathcal{L}_s$ 且 $S_{i,j}(\underline{l})\succ\underline{l}$. 我们声明 $f\left(S_{i,j}(\underline{l})\right)\ge f(\underline{l})$.

事实上, 只需证明

$$f(l_i+1) - f(l_i)\ge f(l_j) - f(l_j-1), \quad l_i\ge l_j\ge 1. \tag{3.23}$$

对 $1 \le l \le m$, 定义一个函数 $g(l) = f(l) - f(l-1)$. 直接的计算说明 g 是一个增函数. 因此, (3.23) 成立.

最后, 注意到对任意 $\underline{l} \succ \underline{l'}$, $\underline{l}$ 可以由 $\underline{l'}$ 经过一些列合适的操作 $S_{i,j}$ 得出, 引理得证. □

由引理 3.15, 我们可以如下证明定理 3.9 的 (ii): 假设 $(t-s-1)m < r \le (t-s)m$ 对某些 $0 \le s \le t-1$, 那么 $sm \le r' = tm - r < (s+1)m$. 我们可选择一个 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, 使得

$$H_r^\perp = \underbrace{\mathbb{F}_Q \times \cdots \times \mathbb{F}_Q}_{s} \times \underset{s+1}{T} \times \underset{s+2}{\{0\}} \times \cdots \times \underset{t}{\{0\}},$$

其中 T 是一个 $\mathbb{F}_Q$ 的 $(r'-sm)$-维 $\mathbb{F}_q$-子空间. 对 $1 \le h \le t$,

$$U_h = H_r^\perp \cap (\underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underset{h}{\mathbb{F}_Q} \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}})$$

形如

$$U_h = \underbrace{\{0\} \times \cdots \times \{0\}}_{h-1} \times \underset{h}{Y_h} \times \underset{h+1}{\{0\}} \times \cdots \underset{t}{\{0\}},$$

其中 Y_h 是 $\mathbb{F}_Q$ 的一个 $\mathbb{F}_q$-子空间. 我们可以进一步要求对每个 $1 \le h \le t$, $\left|Y_h \cap (-C_0^{(2,Q)})\right|$ 达到引理 3.14 中所述的最大值. 因此, 由 (3.22), $F(H_r) = \sum_{h=1}^t f(u_h)$, 其中 $u_1 = \cdots = u_s = m, u_{s+1} = r' - sm = (t-s)m - r$ 且 $u_{s+2} = \cdots = u_t = 0$. 显然 $\underline{u} = (u_1, \ldots, u_t) \in \mathcal{L}_{r'}$ 在全序 $\succ$ 的意义下是最大的. 由引理 3.15, $F(H_r)$ 是最大的, 亦即, 对所有 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, 这个 H_r 是使得 $F(H_r)$ 最大的一个 r-为子空间. 由 (3.20) 和引理 3.14, 可知

$$N_r = \frac{2}{t\delta}\left[\frac{s(q^m-1)}{2} + f((t-s)m - r)\right].$$

这完成了定理 3.9 的 (ii) 的证明.

3.3.9 定理 3.10 的证明

在本小节中, 我们考虑 $e > t$ 且 $N = 1$ 的情形. 如果 $t = 1$, $\mathcal{C}$ 是文献[297] 中考虑过的不可约循环码. 所以我们假设 $e > t \ge 2$. 回顾对 $1 \le r \le tm$ 和 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$, 由 (3.19)

我们有

$$N(H_r) = \frac{1}{e\delta q^r} \sum_{\underline{b} \in H_r} \sum_{h=1}^{e} \eta_{g^h \sum_{j=1}^{t} b_j \beta_j^h}^{(1,Q)},$$

其中 $g = \gamma^a$, $\beta = \gamma^{\frac{Q-1}{e}}$ 且 $\beta_j = \beta^{\Delta_j}$ 对 $1 \le j \le t$. 对 $1 \le h \le e$, 定义

$$W_h := \left\{ \underline{b} = (b_1, \ldots, b_t) \in \mathbb{F}_Q^t : \sum_{j=1}^{t} b_j \beta_j^h = 0 \right\}.$$

每个 W_h 是一个 $(t-1)m$-维 $\mathbb{F}_q$-线性空间. 令

$$w_h := \dim_{\mathbb{F}_q}(H_r \cap W_h).$$

由于 $\eta_0^{(1,Q)} = Q - 1$ 且 $\eta_y^{(1,Q)} = -1$ 如果 $y \in \mathbb{F}_Q^*$, 我们有

$$\begin{aligned} N(H_r) &= \frac{1}{e\delta q^r} \sum_{h=1}^{e} ((Q-1)q^{w_h} - (q^r - q^{w_h})) \\ &= \frac{1}{e\delta q^r} \left(Q \sum_{h=1}^{e} q^{w_h} - eq^r \right) = \frac{Q}{e\delta q^r} \sum_{h=1}^{e} q^{w_h} - \frac{1}{\delta}. \end{aligned} \tag{3.24}$$

为了找到 $\max\left\{N(H_r) : H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}\right\}$, 不失一般性假设 $w_1 \ge w_2 \ge \ldots \ge w_e$. 进行变量替换 $\underline{b} = (b_1, \ldots, b_t) \mapsto \underline{y} = (y_1, \ldots, y_t)$, 其中 $y_h = g^h \sum_{j=1}^{t} b_j \beta_j^h, 1 \le h \le t$. 这定义了一个 $\mathbb{F}_q$-同构 $\phi : \mathbb{F}_Q^t \to \mathbb{F}_Q^t$. 对 $t+1 \le h \le e$, 定义 $y_h := g^h \sum_{j=1}^{t} b_j \beta_j^h$. 由于 ϕ 是一个同构, 存在 $\lambda_{h,1}, \ldots, \lambda_{h,t} \in \mathbb{F}_Q$ 满足

$$y_h = \sum_{i=1}^{t} \lambda_{h,i}\, y_i, \quad t+1 \le h \le e.$$

由于 $\{\Delta_1 \pmod e, \ldots, \Delta_t \pmod e\}$ 是一个等差数列, 可知 $\lambda_{h,i} \ne 0, \forall\, h, i$ 其中 $t+1 \le h \le e, 1 \le i \le t$ (见文献[295]).

因此 (3.24) 可以写作

$$N(H_r) = \frac{Q}{e\delta q^r} \sum_{h=1}^{e} q^{\widetilde{w}_h} - \frac{1}{\delta},$$

其中

$$\widetilde{w}_h := \dim_{\mathbb{F}_q}\left(\widetilde{H}_r \cap \widetilde{W}_h\right) \text{ 和} \widetilde{w}_1 \geq \widetilde{w}_2 \geq \ldots \geq \widetilde{w}_e.$$

此处 $\widetilde{H}_r = \phi(H_r)$ 和 $\widetilde{W}_h = \phi(W_h)$ 形如

$$\widetilde{W}_h = \underbrace{\mathbb{F}_Q \times \cdots \mathbb{F}_Q}_{h-1} \times \underset{h}{\{0\}} \times \underset{h+1}{\mathbb{F}_Q} \times \cdots \times \underset{t}{\mathbb{F}_Q}, \quad 1 \leq h \leq t,$$

和

$$\widetilde{W}_h = \left\{(y_1, \cdots, y_t) \in \mathbb{F}_Q^t : y_h = \sum_{i=1}^{t} \lambda_{h,i} y_i = 0\right\}, \quad t+1 \leq h \leq e.$$

由于 $e \leq q-1$, 为了找到最大化 $N(H_r)$ 的 H_r, 类似于 $e = t$ 且 $N = 1$ 的情况, 首先是让 $\widetilde{w}_1$ 尽可能的大, 此外, 我们再令 $\widetilde{w}_2$ 尽可能的大, 等等, 最终我们令 $\widetilde{w}_e$ 尽可能的大.

假设 $(t-s-1)m < r \leq (t-s)m$ 对某些 $0 \leq s \leq t-1$. 由于 $\dim_{\mathbb{F}_q}\left(\bigcap_{h=1}^{s} \widetilde{W}_h\right) = (t-s)m$, 类似于 $e = t$ 且 $N = 1$ 的情形, 对 $H_r \in \begin{bmatrix} \mathbb{F}_Q^t \\ r \end{bmatrix}$ 满足 $\bigcap_{h=1}^{s+1} \widetilde{W}_h \subset \widetilde{H}_r \subset \bigcap_{h=1}^{s} \widetilde{W}_h$, $N(H_r)$ 达到最大值. 因此, $\widetilde{H}_r$ 形如

$$\widetilde{H}_r = \begin{cases} \underbrace{\{0\} \times \cdots \times \{0\}}_{s} \times \underset{s+1}{T} \times \underset{s+2}{\mathbb{F}_Q} \times \cdots \times \underset{t}{\mathbb{F}_Q} & \text{如果 } 0 \leq s \leq t-2, \\ \underbrace{\{0\} \times \cdots \times \{0\}}_{s} \times \underset{s+1}{T} & \text{如果 } s = t-1. \end{cases}$$

其中 T 是 $\mathbb{F}_Q$ 的一个 $r-(t-s-1)m$-维 $\mathbb{F}_q$-子空间.

如果 $0 \leq s \leq t-2$, 容易验证 $\widetilde{w}_1 = \cdots = \widetilde{w}_s = r$, $\widetilde{w}_{s+1} = (t-s-1)m$ 且 $\widetilde{w}_{s+2} = \cdots = \widetilde{w}_t = r-m$. 对 $t+1 \leq h \leq e$, $\widetilde{w}_h$ 是满足

$$\lambda_{h,s+1} y_{s+1} + \lambda_{h,s+2} y_{s+2} + \cdots + \lambda_{h,t} y_t = 0$$

的子空间 $(y_{s+1}, \ldots, y_t)$ 的 $\mathbb{F}_q$-维数, 其中 $y_{s+1} \in T$ 且 $y_{s+2}, \ldots, y_t \in \mathbb{F}_Q$. 由于 $\forall h, i$, $\lambda_{h,i} \neq 0$, 易知 $\widetilde{w}_h = r-m$ 对 $t+1 \leq h \leq e$. 因此这个 H_r 最大化 $\sum_{h=1}^{e} q^{\widetilde{w}_h}$, 最大值为

$$\sum_{h=1}^{e} q^{\widetilde{w}_h} = sq^r + q^{(t-s-1)m} + (e-s-1)q^{r-m}.$$

如果 $s = t-1$, 我们可知 $\widetilde{w}_1 = \cdots = \widetilde{w}_s = r$ 且 $\widetilde{w}_{s+1} = 0$. 因此对任意 $s+2 \leq h \leq e$,

由不等式 $0 \leq \widetilde{w}_h \leq \widetilde{w}_{s+1}$, 我们有 $\widetilde{w}_h = 0$ 对 $s+2 \leq h \leq e$. 亦即, 这个 H_r 最大化$\sum_{h=1}^{e} q^{\widetilde{w}_h}$, 最大值为

$$\sum_{h=1}^{e} q^{\widetilde{w}_h} = sq^r + e - s.$$

直接的计算可完成证明.

3.3.10 总结

广义汉明重量是线性码的基本参数. 广义汉明重量包含了线性码的结构信息并在很多应用中刻画了线性码的表现. 然而, 线性码的广义汉明重量的计算一般而言是困难的. 在本节中, 我们研究了文献[295] 提出的一类可约循环码的广义汉明重量并在某些情况下得出了重量分层. 这可通过将文献[297] 的思想拓展到高维并利用一些组合的技巧实现. 值得注意的是这些循环码有任意多个非零点.

本节中考虑的码是高度结构化的, 这使得重量分层的计算成为可能. 我们研究了 $N \in \{1, 2\}$ 的情形且此处采用的方法对研究更大的 N 亦有帮助. 我们指出当 $N = 1$, 许多码有两个非零重量且对偶码的极小距离至少为三. 我们事实上以文献[36] 提出的方式构造了很多强正则图.

4 组合设计的构造

4.1 划分式差族的一个统一的组合构造

4.1.1 引言

令 $(G,+)$ 为一个 v 阶的交换群. 令 $\mathcal{F}=\{D_i \mid 0\le i\le l-1\}$ 为 G 的一族子集, ΔD_i 为一个多重集 $\{a-b|a,b\in D_i, a\neq b\}$. $\mathcal{F}$ 被称为是一个*差族* (difference family), 如果群 G 的每个非零元在多重集的并 $\bigcup_{i=0}^{l-1}\Delta D_i$ 中恰好出现 λ 次. 令 K 为多重集 $\{|D_i| \mid 0\le i\le l-1\}$. 我们称 $\mathcal{F}$ 是一个 (G,K,λ)-DF. 进一步, 如果 G 是一个 v 阶的循环群, 我们记 $\mathcal{F}$ 为一个 (v,K,λ)-DF. 令 $\mathcal{F}$ 为一个 (G,K,λ)-DF, 如果 $\mathcal{F}$ 的元素形成 G 的一个划分, 那么 $\mathcal{F}$ 被称为一个*划分式差族* (partitioned difference family), 并记为一个 (G,K,λ)-PDF. 以下, 我们利用一个"指数式"符号描述多重集 K: 一个 $(G,[k_1^{u_1}k_2^{u_2}\dots k_s^{u_s}],\lambda)$-DF 是一个差族, 其中有 u_i 个大小为 k_i 的子集合, $1\le i\le s$.

划分式差族在文献[85] 中被明确引入, 用以构造最优的常重复合码. 它在多种组合的构造中发挥了重要作用, 包括最优常重码[278,309], 最优常重复合码[33,80,84,303,309], 最优跳频序列[82,86,117,278] 和最优集合差系[33,81,84,279,303,309]. 事实上, 划分式差族已经隐含在研究差族的文献中[287]. 最近, 划分式差族在*零差平衡函数* (zero-difference balanced functions) 的名义下受到了集中的研究[33,80,83,84,278,303,309]. 令 f 为从一个交换群 $(G,+)$ 到另一个交换群 $(H,+)$ 的函数, 其中 $|G|=n$, $|f(G)|=l$. f 是一个 (n,l,λ) 零差平衡函数, 如果对任意的 $a\in G\setminus\{0\}$, 我们有

$$|\{x\in G|f(x+a)-f(x)=0\}|=\lambda$$

对某个常数 λ 成立. 以下定理说明划分式差族和零差平衡函数是等价的.

定理 4.1 (定理 1[309]): *令 $(G,+)$ 和 $(H,+)$ 为两个交换群, 其中 $|G|=n$. 令 f 为一个从 G 到 H 的函数满足 $f(G)=\{h_0,h_1,\dots,h_{l-1}\}$. 对 $0\le i\le l-1$, 记 $D_i=\{x\in G \mid f(x)=h_i\}$. 那么 f 是一个 (n,l,λ) 零差平衡函数当且仅当 $\mathcal{F}=\{D_i \mid 0\le i\le l-1\}$ 是一个 (G,K,λ)-PDF, 其中 K 是多重集 $\{|D_i| \mid 0\le i\le l-1\}$.*

目前已经有很多方法构造划分式差族. 第一种是基于分圆的方法. 利用有限域上的经典分圆, 划分式差族在 Wilson[287] 的工作中已被构造出来. 这是一系列后续研究的源头[46,279,298]. Yin 等人[298] 提出了一个巧妙的方法修改了 Wilson 的构造并得到了新的划分式差族. 这个思想在[279] 中被推广, 并给出了划分式差族的两个递归构造. 最近, 几个基于循环群[33,84,303] 和有限域的直和[84] 上的广义分圆的构造被提出. 第二个方法基于有限域上的迹函数. 这个想法在文献[80] 中提出, 进一步的扩展和修改包括在文献[83,117,278,309] 中. 此外, 一些几何构造隐含在文献[110,116] 中. 一类特殊的划分式差族在文献[111] 中以不交差族的完全集 (complete sets of disjoint difference families) 的名义得到研究. 在文献[81] 中, 划分式差族由高非线性度函数和具有理想自相关的三元序列得到. 在文献[32] 证明了满足 $K = [k^m(k-1)^1]$ 的划分式差族可以由 1-旋转可分不完全区组设计 (1-rotational resolvable balanced incomplete block designs) 刻画, 并得到了一系列这样的划分式差族. 一个涉及严格不交差族 (strictly disjoint difference family) 的构造也被提出. 作为划分式差族及其应用的一个综述, 请参见文献[83].

我们将考虑从组合的角度构造可划分差族. 我们引入一个划分式相对差族 (partitioned relative difference family) 的概念, 作为我们构造的核心. 基于此, 我们得到了划分式差族的一个一般的递归构造. 一方面, 这个构造为基于分圆的一系列构造[33,84,303] 提供了一个统一的解释. 另一方面, 这个构造给出了许多新的划分式差族. 此外, 这个构造可以视为文献[32] 定理 6.2 和文献[279] 构造 5.2 的一个推广. 更进一步, 通过扩展划分式相对差族的概念, 我们提出了一个更一般的递归构造, 得到了划分式差族一个新的无穷类.

4.1.2 一些已知构造的回顾

在本小节中, 我们将回顾一些已知的划分式差族的构造. 这些构造将在接下来的递归构造中发挥作用. 我们首先引入一些记号. 令 q 为一个素数幂. 我们用 $\mathbb{F}_q^+$ 记有限域 $\mathbb{F}_q$ 的加法群. 模 n 的整数环被记做 $\mathbb{Z}_n$. 整数 $a_1, a_2, \ldots, a_l$ 的最大公因子被记做 $\gcd(a_1, a_2, \ldots, a_l)$. 对两个正整数 b 和 n, $\mathrm{ord}_n(b)$ 是最小的正整数 c 使得 $b^c \equiv 1 \pmod{n}$. 本节中, 每个集合的并被视为多重集的并. 一个多重集 A 的 μ 个复制的并被记为 A^μ.

4.1.2.1 Wilson 构造

我们描述利用有限域的分圆的 Wilson 构造和它在素数幂阶循环群上的一个类似构造.

命题 4.1 (文献[287]): 令 q 为一个素数幂且 $q-1=ef$. 对有限域 $\mathbb{F}_q$, 令 $C_i, 0 \le i \le e-1$ 为 e 阶的分圆陪集. 那么 $\mathcal{F}=\{\{0\}, C_0, C_1, \ldots, C_{e-1}\}$ 是一个 $(\mathbb{F}_q^+, [f^e 1^1], f-1)$-PDF.

一个类似的构造可在素数幂阶的循环群上得到.

命题 4.2: 令 p 为一个素数, n 为一个正整数. 令 b 为 $\mathbb{Z}_{p^n}$ 的一个元素满足 $\mathrm{ord}_{p^n}(b)=f$ 且 $\gcd(b^j-1,p)=1$ 对每个 $1 \le j \le f-1$ 成立. 那么 $\mathbb{Z}_{p^n} \setminus \{0\}$ 可被划分为 $\frac{p^n-1}{f}$ 个 b-分圆陪集 B_i, $1 \le i \le \frac{p^n-1}{f}$. 更进一步, $\mathcal{F}=\{\{0\}, B_1, \ldots, B_{\frac{p^n-1}{f}}\}$ 是一个 $(p^n, [f^{\frac{p^n-1}{f}} 1^1], f-1)$-PDF.

证明. 由于 $\mathrm{ord}_{p^n}(b)=f$ 且 $\gcd(b^j-1,p)=1$ 对 $1 \le j \le f-1$ 成立, 每个 b-分圆陪集形如 $\{x, bx, \ldots, b^{f-1}x\}$, 其中 $x \in \mathbb{Z}_{p^n} \setminus \{0\}$. 只需证明任意的 $a \in \mathbb{Z}_{p^n} \setminus \{0\}$, 在 $\cup_{i=1}^{\frac{p^n-1}{f}} \Delta B_i$ 中恰好出现 $f-1$ 次. 因而, 我们考虑以下 $f-1$ 个方程的解的总个数:

$$a \equiv b^j x - x \pmod{p^n}, 1 \le j \le f-1.$$

对每个 $1 \le j \le f-1$, 由于 $\gcd(b^j-1,p)=1$, 恰好存在一个解 x. 因而解的总个数是 $f-1$. □

4.1.2.2 Wilson 构造的变形

一些 Wilson 构造的变形在文献[298] 中提出并在文献[279] 中得到进一步推广. 我们仅列出文献[279] 中的以下结果.

命题 4.3:
1) 令 $q=25+4b^2$ 或 $q=49+4b^2$ 为一个素数幂满足 b 为奇数. 那么存在一个 $(\mathbb{F}_q^+, [2^{\frac{q-1}{4}}(\frac{q-1}{4})^1(\frac{q+3}{4})^1], \frac{q+3}{8})$-PDF.
2) 令 $q=1+8b^2=9+64c^2$ 为一个素数幂满足 b, c 为奇数. 那么存在一个 $(\mathbb{F}_q^+, [2^{3b^2}(b^2)^1(b^2+1)^1], 2c^2+1)$-PDF.

3) 令 $q = 4 + b^2$ 为一个素数幂满足 $b \equiv 1 \pmod 4$. 那么存在一个 $(\mathbb{F}_q^+, [(\frac{q-1}{4})^1(\frac{q+3}{4})^1(\frac{q-1}{2})^1], \frac{3q-7}{8})$-PDF.

4) 令 $q = 9 + 4b^2$ 为一个素数幂满足 b 为偶数. 那么存在一个 $(\mathbb{F}_q^+, [(\frac{q-1}{4})^2(\frac{q+1}{2})^1], \frac{3q-3}{8})$-PDF.

4.1.3 一些几何构造

我们描述两个隐含在文献中的划分式差族的几何构造. 第一个构造利用了仿射几何.

命题 4.4 (引理 3.2[110]): 令 $n \geq 2$ 且 $1 \leq t < n$. 仿射几何 $AG(n, q)$ 的点集可被视为 $\mathbb{Z}_{q^n-1} \cup \{\infty\}$. $AG(n, q)$ 中所有的 t-平面可被划分为平行类. 令 $\mathcal{F}$ 为 $\mathbb{Z}_{q^n-1} \cup \{\infty\}$ 的一族子集, 包含了一个平行类里的 q^{n-t} 个 t-平面. 注意到 $\mathcal{F}$ 恰有一个子集包含点 ∞. 将点 ∞ 由这个子集中删除, 我们有一族新的子集 $\mathcal{F}'$, 是一个 $(q^n - 1, [(q^t)^s(q^t - 1)^1], q^t - 1)$-PDF, 其中 $s = q^{n-t} - 1$.

以下的构造设计射影几何.

命题 4.5 (定理 3.1[116]): 令 $n \geq 2$. 射影几何 $PG(n, q)$ 的点集可被视为 $\mathbb{Z}_{\frac{q^{n+1}-1}{q-1}}$. 存在 $\frac{q^n-1}{q-1}$ 条直线 $l_i, 0 \leq i < \frac{q^n-1}{q-1}$ 经过一个固定点 a. 令 $\mathcal{F} = \{l_i \setminus \{a\} \mid 0 \leq i < \frac{q^n-1}{q-1}\} \cup \{\{a\}\}$. 那么 $\mathcal{F}$ 是一个 $(\frac{q^{n+1}-1}{q-1}, [q^s 1^1], q - 1)$-PDF 其中 $s = \frac{q^n-1}{q-1}$.

4.1.4 差矩阵和划分式相对差族

本小节中, 我们引入两个起重要作用的组合构型. 第一个是差矩阵.

令 $(G, +)$ 为一个阶为 g 的交换群. 一个 $(G, k; \lambda)$ 差矩阵 (difference matrix) 是一个 $k \times g\lambda$ 的由 G 中元素构成的矩阵 $D = (d_{ij})$, 满足对每个 $1 \leq i < j \leq k$, 差的多重集 $\{d_{il} - d_{jl} \mid 1 \leq l \leq g\lambda\}$ 包含 G 的每个元素恰好 λ 次.

我们记一个 $(G, k; \lambda)$ 差矩阵为一个 $(G, k; \lambda)$-DM. 更进一步, 如果 $G = \mathbb{Z}_v$, 我们记之为一个 $(v, k; \lambda)$-DM. 如果一个 $(G, k; \lambda)$-DM 存在, 则一个满足 $2 \leq k' < k$ 的 $(G, k'; \lambda)$-DM 存在.

以下是关于差矩阵的一些结果.

命题 4.6: 1) (定理 17.6[64]) 一个有限域 $\mathbb{F}_q$ 的乘法表是一个 $(\mathbb{F}_q^+, q; 1)$-DM.

2) (定理 17.18[64]) 令 G 为阶为 g 的任意群. 那么存在一个 $(G,p;1)$-DM 其中 p 是整除 g 的最小素数.

3) (推论 2.3[31]) 令 $G=\mathbb{F}_{q_1}^{+}\times\cdots\times\mathbb{F}_{q_n}^{+}$ 初等交换群的直积, 令 $k=\min\{q_i \mid 1\le i\le n\}$. 那么存在一个 $(G,k;1)$-DM.

4) (定理 2.1[31]) 令 $R=(G,+,\cdot)$ 为一个环, 令 I 为 G 的一个 k-子集满足 I 中任意非零差是 R 的一个单位. 那么矩阵 $M=(m_{ig})_{i\in I,g\in G}$, 其中 $a_{ig}=i\cdot g$, 是一个$(G,k;1)$-DM.

一个 $(G,k;1)$-DM 是齐性的 (homogeneous), 如果每一行是 G 中元素的一个排列. 如果一个 $(G,k;1)$-DM 包含一个全 0 行, 那么其余的行形成一个 $(G,k-1;1)$-DM, 反之亦然. 因而, 一个 $(G,k;1)$-DM 等价于一个齐性的 $(G,k-1;1)$-DM.

其次，我们引入划分式相对差族的概念.

定义 4.1: 令 $(G,+)$ 为一个交换群, N 为 G 的一个子群. 令 $\mathcal{F}=\{D_i \mid 0\le i\le l-1\}$ 为 G 的一族子集. $\mathcal{F}$ 被称为一个 (G,N,K,λ) 相对差族 (relative difference family) 如果每个 $G\setminus N$ 的元素在 $\bigcup_{i=0}^{l-1}\Delta D_i$ 中恰好出现 λ 次且每个 N 中元素出现 0 次, 其中 K 为多重集 $\{|D_i| \mid 0\le i\le l-1\}$. 进一步, 如果 $\mathcal{F}$ 中的子集 $G\setminus N$ 的一个划分, 那么 $\mathcal{F}$ 被称为划分式相对差族 (partitioned relative difference family), 记为一个 (G,N,K,λ)-PRDF.

以上定义中的子群 N 被称为禁止子群 (forbidden subgroup). 当 G 是一个循环子群 $\mathbb{Z}_v$, N 是一个阶为 n 的子群, 一个 (G,N,K,λ)-PRDF 也被记做 (v,n,K,λ)-PRDF. 以下, 我们列出一类在接下来构造中将要用到的划分式相对差族.

命题 4.7 (1703 **页**[116]): 射影几何 $PG(2t+1,q)$ 的点集可被视作 $\mathbb{Z}_{\frac{q^{2t+2}-1}{q-1}}$. 它包含一个形如 $S=\{0,s,2s,\ldots,(k-1)s\}$ 的 t-平面 S, 其中 $s=q^{t+1}+1$, $k=\frac{q^{t+1}-1}{q-1}$. 令 L_a 为PG$(2t+1,q)$ 经过一个固定点 $a\in S$ 的线的集合. 令 $L(S)$ 为包含在 S 中的线的集合. 那么

$$\mathcal{F}=\{\{l\setminus\{a\}\} \mid l\in L_a\setminus L(S)\}$$

是一个 $(\frac{q^{2t+2}-1}{q-1},\frac{q^{t+1}-1}{q-1},[q^{\frac{q^t(q^{t+1}-1)}{q-1}}],q-1)$-PRDF.

4.1.5 划分式差族的一个统一的递归构造

本小节中, 我们从划分式相对差族的角度考虑划分式差族的构造. 我们提出两个起重要作用的划分式相对差族的构造. 更具体的, 我们有以下的划分式相对差族的膨胀构造, 其中齐性的差矩阵是关键的元素.

构造 4.1 (膨胀构造): 假设存在一个 (G, N, K, λ)-PRDF. 如果同时存在一个 $(W, k^*; 1)$-DM 满足 $k^* = \max\{k \mid k \in K\}$, 那么存在一个 $(G \times W, N \times W, K^{|W|}, \lambda)$-PRDF.

证明. 令 $\mathcal{F}$ 为一个 (G, N, K, λ)-PRDF 且 $M = (m_{ij})$, $1 \le i \le k^*$, $1 \le j \le |W|$ 为一个齐性的 $(W, k^*; 1)$-DM. 每个子集 $\{b_1, \ldots, b_k\} \in \mathcal{F}$ 对应于 $|W|$ 个形如

$$\{(b_1, m_{1j}), \ldots, (b_k, m_{kj})\}, 1 \le j \le |W|$$

的子集. 假设 $\mathcal{F}'$ 由所有这些子集构成, 即,

$$\mathcal{F}' = \{\{(b_1, m_{1j}), \ldots, (b_k, m_{kj})\} \mid 1 \le j \le |W|, \{b_1, \ldots, b_k\} \in \mathcal{F}\}.$$

由于 $\mathcal{F}$ 的子集形成 $G \setminus N$ 的一个划分且 M 是齐性的, $\mathcal{F}'$ 的子集形成 $(G \setminus N) \times W$ 的一个划分. 容易验证 $\mathcal{F}'$ 是一个 $(G \times W, N \times W, K^{|W|}, \lambda)$-PRDF. □

其次，我们有以下的划分式相对差族的复合构造.

构造 4.2 (复合构造): 假设存在一个 (G, H, K_1, λ)-PRDF 和一个 (H, U, K_2, λ)-PRDF. 那么存在一个 $(G, U, K_1 \cup K_2, \lambda)$-PRDF.

证明. 令 $\mathcal{F}_1$ 为一个 (G, H, K_1, λ)-PRDF 且 $\mathcal{F}_2$ 为一个 (H, U, K_2, λ)-PRDF. 由定义易知 $\mathcal{F}_1 \cup \mathcal{F}_2$ 是一个 $(G, U, K_1 \cup K_2, \lambda)$-PRDF. □

我们可直接得出以下推论.

推论 4.1: 假设存在一个 (G, H, K_1, λ)-PRDF 和一个 (H, K_2, λ)-PDF. 那么存在一个 $(G, K_1 \cup K_2, \lambda)$-PDF.

以下我们描述划分式差族的递归构造.

构造 4.3 (主要构造): 假设以下的存在:

1. 一个 (G, N, K_1, λ)-PRDF;
2. 一个齐性的 $(W, k^*; 1)$-DM 满足 $k^* = \max\{k \mid k \in K_1\}$;
3. 一个 $(N \times W, K_2, \lambda)$-PDF.

那么存在一个 $(G \times W, K_1^{|W|} \cup K_2, \lambda)$-PDF.

证明. 假设存在一个 (G, N, K_1, λ)-PRDF 和一个齐性的 $(W, k^*; 1)$-DM. 应用膨胀构造, 我们得到一个 $(G \times W, N \times W, K_1^{|W|}, \lambda)$-PRDF. 注意到存在一个 $(N \times W, K_2, \lambda)$-PDF. 由推论 4.1, 我们有一个 $(G \times W, K_1^{|W|} \cup K_2, \lambda)$-PDF. □

注: 以上定理推广了文献[32] 的定理 6.2 和文献[279] 的构造 5.2 中的递归构造.

主要构造提供划分式差族构造的一个非常一般的框架. 它为几个利用分圆的划分式差族的构造[33,84,303] 提供了一个统一的解释. 这些利用分圆的构造可视为主要构造的特殊情况. 更具体地, 以下推论为文献[33] 定理 1 中利用广义分圆的构造提供了一个简单的解释 (另有一个简单的描述见文献[303] 构造 1).

推论 4.2: 令 v 为一个分解为 $v = \prod_{i=1}^{l} p_i^{m_i}$ 的正整数. 假设 $f \mid \gcd(p_1 - 1, p_2 - 1, \ldots, p_l - 1)$. 那么存在一个 $(v, [f^{\frac{v-1}{f}} 1^1], f-1)$-PDF.

证明. 令 $b_1 \in \mathbb{Z}_{p_1^{m_1}}$ 满足 $\mathrm{ord}_{p_1^{m_1}}(b_1) = f$ 且 $\gcd(b_1^i - 1, p_1) = 1$ 对每个 $1 \le i \le f-1$ 成立. 由命题 4.2, 存在一个 $(\mathbb{Z}_{p_1^{m_1}}, \{0\}, [f^{\frac{p_1^{m_1}-1}{f}}], f-1)$-PRDF $\mathcal{F}_1 = \{B_j \mid 1 \le j \le \frac{p_1^{m_1}-1}{f}\}$, 其中每个 B_j 是一个 b_1-分圆陪集. 由命题 4.6 的 2), 存在一个齐性的 $(\mathbb{Z}_{p_2^{m_2}}, f; 1)$-DM M. 特别地, 我们可以按以下方法选取 M. 令 $b_2 \in \mathbb{Z}_{p_2^{m_2}}$ 满足 $\mathrm{ord}_{p_2^{m_2}}(b_2) = f$ 且 $\gcd(b_2^i - 1, p_2) = 1$ 对每个 $1 \le i \le f-1$ 成立. 用元素 $\{1, b_2, \ldots, b_2^{f-1}\}$ 标记 M 的行, 用 $\mathbb{Z}_{p_2^{m_2}}$ 的元素标记列. 假设 M 是上述行和列的标记对应的乘法表. 那么由命题 4.6 的 4), M 是一个齐性的 $(\mathbb{Z}_{p_2^{m_2}}, f; 1)$-DM. 此外, 由命题 4.2, 存在一个 $(\mathbb{Z}_{p_2^{m_2}}, [f^{\frac{p_2^{m_2}-1}{f}} 1^1], f-1)$-PDF. 利用主要构造, 我们得到一个 $(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}}, [f^{\frac{p_1^{m_1} p_2^{m_2}-1}{f}} 1^1], f-1)$-PDF $\mathcal{F}_2$. 注意到 $\mathcal{F}_2 \setminus \{\{0\}\}$ 是一个 $(\mathbb{Z}_{p_1^{m_1} p_2^{m_2}}, \{0\}, [f^{\frac{p_1^{m_1} p_2^{m_2}-1}{f}}], f-1)$-PRDF. 重复这个步骤, 我们最终得到一个 $(\mathbb{Z}_v, [f^{\frac{v-1}{f}} 1^1], f-1)$-PDF. 这正是文献[33] 定理 1 和文献[303] 构造 1 所得到的划分式差族. □

更一般地, 我们可以进一步推广以上的推论.

定理 4.2: 对 $1 \le j \le t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的正整数. 假设对每个 $1 \le j \le t$, $f \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$. 那么存在一个 $(G, [f^{\frac{v-1}{f}}1^1], f-1)$-PDF, 其中 $G = \mathbb{Z}_{v_1} \times \cdots \times \mathbb{Z}_{v_t}$ 且 $v = \prod_{j=1}^{t} v_j$.

证明. 由推论 4.2 知存在一个 $(\mathbb{Z}_{v_1}, \{0\}, [f^{\frac{v_1-1}{f}}], f-1)$-PRDF 和一个 $(\{0\}\times\mathbb{Z}_{v_2}, [f^{\frac{v_2-1}{f}}1^1], f-1)$-PDF. 利用命题 4.6 的 2), 我们有一个齐性的 $(v_2, f; 1)$-DM. 应用主要构造, 我们有一个 $(\mathbb{Z}_{v_1} \times \mathbb{Z}_{v_2}, [f^{\frac{v_1v_2-1}{f}}1^1], f-1)$-PDF. 重复这个步骤, 我们最终得到一个 $(G, [f^{\frac{v-1}{f}}1^1], f-1)$-PDF. □

类似地, 我们可以为文献[84] 定理 1 中利用广义分圆的构造提供了一个简单的解释.

推论 4.3: 令 $q_1, q_2, \ldots, q_l$ 为素数幂且 $f \mid \gcd(q_1-1, q_2-1, \ldots, q_l-1)$. 假设 $q = \prod_{i=1}^{l} q_i$, $q_i = e_i f+1, 1 \le i \le l$ 且 $G = \mathbb{F}_{q_1}^+ \times \mathbb{F}_{q_2}^+ \times \cdots \times \mathbb{F}_{q_l}^+$. 那么存在一个 $(G, [f^{\frac{q-1}{f}}1^1], f-1)$-PDF.

证明. 我们用 $C_j^{e_i}$, $0 \le j \le e_i - 1$ 记 $\mathbb{F}_{q_i}$ 上阶为 e_i 的分圆类. 由命题 4.1, 存在一个 $(\mathbb{F}_{q_1}^+, \{0\}, [f^{\frac{q_1-1}{f}}], f-1)$-PRDF $\mathcal{F}_1 = \{C_j^{e_1} \mid 0 \le j \le e_1 - 1\}$. 由命题 4.6 的 1), 存在一个齐性的 $(\mathbb{F}_{q_2}^+, f; 1)$-DM M. 特别地, 我们可以用以下的方式选取 M. 用 $C_0^{e_2}$ 的元素标记 M 的行, 用 $\mathbb{F}_{q_2}$ 的元素标记列. 假设 M 是上述行和列的标记对应的乘法表. 那么由命题 4.6 的 4), M 是一个齐性的 $(\mathbb{F}_{q_2}^+, f; 1)$-DM. 此外, 由命题 4.1, 存在一个 $(\mathbb{F}_{q_2}^+, [f^{\frac{q_2-1}{f}}1^1], f-1)$-PDF. 利用主要构造, 我们得到一个 $(\mathbb{F}_{q_1}^+ \times \mathbb{F}_{q_2}^+, [f^{\frac{q_1q_2-1}{f}}1^1], f-1)$-PDF $\mathcal{F}_2$. 注意到 $\mathcal{F}_2 \setminus \{\{(0,0)\}\}$ 是一个 $(\mathbb{F}_{q_1}^+ \times \mathbb{F}_{q_2}^+, \{(0,0)\}, [f^{\frac{q_1q_2-1}{f}}], f-1)$-PRDF. 重复这个步骤, 我们最终得到一个 $(G, [f^{\frac{q-1}{f}}1^1], f-1)$-PDF. 这正是文献[84] 定理 1 所得到的划分式差族. □

注: 事实上, 文献[84] 定理 1 中的假设了所有素数幂 q_i 是两两不同的. 而这个假设是多余的. 特别地, 当 $l = 2$ 且 q_1, q_2 为相同的素数, 我们重新得到了文献[303] 定理 2 构造的划分式差族.

现在我们给出几类由主要构造得出的新的划分式差族. 对任意 $k \ge 2$, 集合 $D = \{1, \ldots, k\} \subset \mathbb{Z}_{k+1}$ 是一个平凡的 $(k+1, 1, [k^1], k-1)$-PRDF. 由这个划分式相对差族出发, 我们有以下的构造.

定理 4.3: 令 k 为一个正整数满足 $k \geq 2$. 对 $1 \leq j \leq t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的正整数. 假设对每个 $1 \leq j \leq t$, $k \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$. 那么存在一个 $(\mathbb{Z}_{k+1} \times G, [k^{v+\frac{v-1}{k}}1^1], k-1)$-PDF, 其中 $G = \mathbb{Z}_{v_1} \times \cdots \times \mathbb{Z}_{v_t}$ 且 $v = \prod_{j=1}^{t} v_j$.

证明. 注意到 $D = \{1, \ldots, k\} \subset \mathbb{Z}_{k+1}$ 是一个 $(k+1, 1, [k^1], k-1)$-PRDF. 由于 $k \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$ 对每个 $1 \leq j \leq t$ 成立, 由命题 4.6 的 2), 存在一个齐性的 $(G, k; 1)$-DM. 更进一步, 由推论 4.2, 存在一个 $(\{0\} \times G, [k^{\frac{v-1}{k}}1^1], k-1)$-PDF. 应用主要构造, 我们有一个 $(\mathbb{Z}_{k+1} \times G, [k^{v+\frac{v-1}{k}}1^1], k-1)$-PDF. □

定理 4.4: 令 k 为一个正整数满足 $k \geq 2$. 令 $G = \mathbb{F}_{p_1^{s_1}}^{+} \times \mathbb{F}_{p_2^{s_2}}^{+} \times \cdots \times \mathbb{F}_{p_l^{s_l}}^{+}$ 且 $v = \prod_{i=1}^{l} p_i^{s_i}$. 假设 $k \mid p_i^{s_i}-1$ 对每个 $1 \leq i \leq l$ 成立. 那么存在一个 $(\mathbb{Z}_{k+1} \times G, [k^{v+\frac{v-1}{k}}1^1], k-1)$-PDF.

证明. 注意到 $D = \{1, \ldots, k\} \subset \mathbb{Z}_{k+1}$ 是一个 $(k+1, 1, [k^1], k-1)$-PRDF. 由于 $k \mid p_i^{s_i}-1$ 对每个 $1 \leq i \leq l$ 成立, 由命题 4.6 的 3),存在一个齐性的 $(G, k; 1)$-DM. 更进一步, 由推论 4.3, 存在一个 $(\{0\} \times G, [k^{\frac{v-1}{k}}1^1], k-1)$-PDF. 利用主要构造, 我们有一个 $(\mathbb{Z}_{k+1} \times G, [k^{v+\frac{v-1}{k}}1^1], k-1)$-PDF. □

令 q 为一个素数幂且 $n \geq 2$. 命题 4.5 给出的划分式差族自然给出一个 $(\frac{q^{n+1}-1}{q-1}, 1, [q^s], q-1)$-PRDF, 其中 $s = \frac{q^n-1}{q-1}$. 从这个划分式相对差族出发, 我们可以用类似前两个定理的办法得到以下的定理.

定理 4.5: 令 q 为一个素数幂且 $n \geq 2$. 对 $1 \leq j \leq t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的正整数. 假设对每个 $1 \leq j \leq t$, $q \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$. 那么存在一个 $(\mathbb{Z}_{\frac{q^{n+1}-1}{q-1}} \times G, [q^s 1^1], q-1)$-PDF 满足 $G = \mathbb{Z}_{v_1} \times \cdots \times \mathbb{Z}_{v_t}$, $v = \prod_{j=1}^{t} v_j$ 且 $s = \frac{q^n-1}{q-1}v + \frac{v-1}{q}$.

定理 4.6: 令 q 为一个素数幂且 $n \geq 2$. 令 $v = \prod_{i=1}^{l} p_i^{s_i}$ 且 $G = \mathbb{F}_{p_1^{s_1}}^{+} \times \mathbb{F}_{p_2^{s_2}}^{+} \times \cdots \times \mathbb{F}_{p_l^{s_l}}^{+}$. 假设 $q \mid p_i^{s_i}-1$ 对 $1 \leq i \leq l$. 那么存在一个 $(\mathbb{Z}_{\frac{q^{n+1}-1}{q-1}} \times G, [q^s 1^1], q-1)$-PDF 满足 $s = \frac{q^n-1}{q-1}v + \frac{v-1}{q}$.

注意到之前构造中涉及的初始的划分式相对差族在禁止子群的意义下是平凡的. 接下来, 我们提出一个由命题 4.7 中非平凡的划分式相对差族出发的构造.

定理 4.7: 令 q 为一个素数幂. 对 $1 \leq j \leq t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的正整数. 假设对每个 $1 \leq j \leq t$, $q \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$. 那么存

在一个 $(\mathbb{Z}_{\frac{q^4-1}{q-1}} \times G, [q^s 1^1], q-1)$-PDF, 其中 $G = \mathbb{Z}_{v_1} \times \cdots \times \mathbb{Z}_{v_t}$, $v = \prod_{j=1}^{t} v_j$ 且 $s = q(q+1)v + v + \frac{v-1}{q}$.

证明. 给定一个素数幂 q, 在命题 4.7 中令 $t = 1$, 我们有一个 $(\frac{q^4-1}{q-1}, q+1, [q^{q(q+1)}], q-1)$-PRDF. 由于对每个 $1 \le j \le t, q \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$, 那么由命题 4.6 的 2), 存在一个齐性的 $(G, q; 1)$-DM. 进一步, 由定理 4.3, 存在一个 $(\mathbb{Z}_{q+1} \times G, [q^{v+\frac{v-1}{q}} 1^1], q-1)$-PDF. 利用主要构造, 我们有一个 $(\mathbb{Z}_{\frac{q^4-1}{q-1}} \times G, [q^s 1^1], q-1)$-PDF 满足 $s = q(q+1)v + v + \frac{v-1}{q}$. □

类似地, 我们有以下的定理.

定理 4.8: 令 q 为一个素数幂. 令 $v = \prod_{i=1}^{l} p_i^{s_i}$ 且 $G = \mathbb{F}^+_{p_1^{s_1}} \times \mathbb{F}^+_{p_2^{s_2}} \times \cdots \times \mathbb{F}^+_{p_l^{s_l}}$. 假设 $q \mid p_i^{s_i} - 1$ 对每个 $1 \le i \le l$ 成立. 那么存在一个 $(\mathbb{Z}_{\frac{q^4-1}{q-1}} \times G, [q^s 1^1], q-1)$-PDF 满足 $s = q(q+1)v + v + \frac{v-1}{q}$.

注: 注意到定理 4.7 (或定理 4.8) 中的划分式差族的参数已被定理 4.5 (或定理 4.6) 覆盖. 我们依然列出定理 4.7 和定理 4.8 来说明非平凡的划分式相对差族在构造划分式差族中的作用.

最后, 我们将命题 4.3 的划分式差族应用于主要构造, 得出几类新的划分式差族. 由于证明是直接的, 我们在此略去.

定理 4.9: 对 $1 \le j \le t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的正整数. 令 $G = \mathbb{Z}_{v_1} \times \cdots \times \mathbb{Z}_{v_t}$ 且 $v = \prod_{j=1}^{t} v_j$.

1) 令 $q = 25 + 4b^2$ 或 $q = 49 + 4b^2$ 为一个素数幂满足 b 是一个奇数. 假设对每个 $1 \le j \le t$, $\frac{q+11}{8} \mid \gcd(p_{j1} - 1, p_{j2} - 1, \ldots, p_{jl_j} - 1)$. 那么存在一个 $(G \times \mathbb{F}_q^+, [(\frac{q+11}{8})^s 2^{\frac{q-1}{4}} (\frac{q-1}{4})^1 (\frac{q+3}{4})^1], \frac{q+3}{8})$-PDF, 其中 $s = \frac{8q(v-1)}{q+11}$.

2) 令 $q = 1 + 8b^2 = 9 + 64c^2$ 为一个素数幂满足 b, c 是奇数. 假设对每个 $1 \le j \le t$, $2c^2 + 2 \mid \gcd(p_{j1} - 1, p_{j2} - 1, \ldots, p_{jl_j} - 1)$. 那么存在一个 $(G \times \mathbb{F}_q^+, [(2c^2+2)^s 2^{3b^2} (b^2)^1 (b^2+1)^1], 2c^2+1)$-PDF, 其中 $s = \frac{q(v-1)}{2c^2+2}$.

3) 令 $q = 4 + b^2$ 为一个素数幂满足 $b \equiv 1 \pmod 4$. 假设对每个 $1 \le j \le t$, $\frac{3q+1}{8} \mid \gcd(p_{j1} - 1, p_{j2} - 1, \ldots, p_{jl_j} - 1)$. 那么存在一个 $(G \times \mathbb{F}_q^+, [(\frac{3q+1}{8})^s (\frac{q-1}{4})^1 (\frac{q+3}{4})^1 (\frac{q-1}{2})^1], \frac{3q-7}{8})$-PDF, 其中 $s = \frac{8q(v-1)}{3q+1}$.

4) 令 $q = 9 + 4b^2$ 为一个素数幂满足 b 是一个偶数. 假设对每个 $1 \le j \le t$, $\frac{3q+5}{8} \mid \gcd(p_{j1}-1, p_{j2}-1, \ldots, p_{jl_j}-1)$. 那么存在一个 $(G \times \mathbb{F}_q^+, [(\frac{3q+5}{8})^s(\frac{q-1}{4})^2(\frac{q+1}{2})^1], \frac{3q-3}{8})$-PDF, 其中 $s = \frac{8q(v-1)}{3q+5}$.

定理 4.10: 令 $p_1, \ldots, p_l$ 为素数. 令 $v = \prod_{i=1}^{l} p_i^{s_i}$ 且 $G = \mathbb{F}_{p_1^{s_1}}^+ \times \mathbb{F}_{p_2^{s_2}}^+ \times \cdots \times \mathbb{F}_{p_l^{s_l}}^+$.

1) 令 $q = 25+4b^2$ 或 $q = 49+4b^2$ 为一个素数幂满足 b 是一个奇数. 假设 $\frac{q+11}{8} \mid p_i^{s_i}-1$ 对每个 $1 \le i \le l$ 成立. 那么存在一个 $(G \times \mathbb{F}_q^+, [(\frac{q+11}{8})^s 2^{\frac{q-1}{4}} (\frac{q-1}{4})^1 \ (\frac{q+3}{4})^1], \frac{q+3}{8})$-PDF, 其中 $s = \frac{8q(v-1)}{q+11}$.

2) 令 $q = 1+8b^2 = 9+64c^2$ 为一个素数幂满足 b, c 是奇数. 假设 $2c^2+2 \mid p_i^{s_i}-1$ 对每个 $1 \le i \le l$ 成立. 那么存在一个 $(G \times \mathbb{F}_q^+, [(2c^2+2)^s 2^{3b^2} (b^2)^1 (b^2+1)^1], 2c^2+1)$-PDF, 其中 $s = \frac{q(v-1)}{2c^2+2}$.

3) 令 $q = 4 + b^2$ 为一个素数幂满足 $b \equiv 1 \pmod 4$. 假设 $\frac{3q+1}{8} \mid p_i^{s_i} - 1$ 对每个 $1 \le i \le l$ 成立. 那么存在一个 $(G \times \mathbb{F}_q^+, [(\frac{3q+1}{8})^s (\frac{q-1}{4})^1 (\frac{q+3}{4})^1 (\frac{q-1}{2})^1], \frac{3q-7}{8})$-PDF, 其中 $s = \frac{8q(v-1)}{3q+1}$.

4) 令 $q = 9 + 4b^2$ 为一个素数幂满足 b 是一个偶数. 假设 $\frac{3q+5}{8} \mid p_i^{s_i} - 1$ 对每个 $1 \le i \le l$ 成立. 那么存在一个 $(G \times \mathbb{F}_q^+, [(\frac{3q+5}{8})^s (\frac{q-1}{4})^2 (\frac{q+1}{2})^1], \frac{3q-3}{8})$-PDF, 其中 $s = \frac{8q(v-1)}{3q+5}$.

4.1.6 一个更一般的递归构造

本小节的目标是推广上小节中的主要构造. 这个推广基于以下两点. 首先, 我们将划分式相对差族的概念推广到可有超过一个的禁止子群. 其次, 在递归构造中, 我们将用带洞的差矩阵来取代差矩阵.

我们首先介绍一个更一般的划分式相对差族的概念. 令 $(G, +)$ 为阶为 v 的交换群. 令 $H_1, H_2, \ldots, H_n$ 和 U 为 G 的 $(n+1)$ 个不同的子群, 对任意的 $1 \le i < j \le n$ 满足 $H_i \cap H_j = U$. 一个 $(G; H_1, H_2, \ldots, H_n; U, K, \lambda)$ 划分式相对差族 (partitioned relative difference family) 是 G 的一族子集 $\mathcal{F} = \{D_i \mid 0 \le i \le l-1\}$, 其中 $K = \{|D_i| \mid 0 \le i < l\}$ 且满足以下两个条件:

1. $G \setminus (\cup_{i=1}^{n} H_i)$ 的每个元素在多重集的并 $\bigcup_{i=0}^{l-1} \Delta D_i$ 中恰好出现 λ 次, 其中 $\cup_{i=1}^{n} H_i$ 的每个元素不出现;

2. $\{D_i \mid 0 \le i \le l-1\}$ 形成 $G \setminus (\cup_{i=1}^{n} H_i)$ 的一个划分.

注意到当 $n=1$, 一个 $(G; H_1; U, K, \lambda)$-PRDF 即是之前定义的一个 (G, H_1, K, λ)-PRDF.

其次, 我们给出带洞的差矩阵的定义. 令 G 为一个阶为 g 的交换群且 S 为 G 的一个阶为 s 的子群. 一个 G 上的关于 S 的*带洞的差矩阵* (holey difference matrix) 是一个 $k \times (g-s)$ 矩阵 $D=(d_{ij})$, $d_{ij} \in G$, 满足差 $\{d_{rj} - d_{tj} \mid 1 \le j \le g-s\}$ 遍历 $G \setminus S$ 的所有元素, 其中 $1 \le r < t \le k$. D 被记为一个 $(G, S, k; 1)$-HDM. 如果 D 每一行的元素遍历 $G \setminus S$ 的所有元素, 我们称 D 为一个*齐性的* (homogeneous) $(G, S, k; 1)$-HDM. 当 $S=\emptyset$, 一个 $(G, S, k; 1)$-HDM 即是一个 $(G, k; 1)$-DM. 如果一个 $(G, S, k; 1)$-HDM 包含一个全 0 行, 那么其余的行形成一个齐性的 $(G, S, k-1; 1)$-HDM, 反之亦然.

以下我们描述划分式相对差族的一个膨胀构造和一个递归构造. 它们分别推广了构造 4.1 和构造 4.2. 首先我们有以下利用带洞差矩阵的膨胀构造.

构造 4.4 (膨胀构造): *假设存在一个 (G, H, K, λ)-PRDF. 如果存在一个 $(W, S, k^*; 1)$-HDM 满足 $k^* = \max\{k \mid k \in K\}$, 那么存在一个 $(G \times W; G \times S, H \times W; H \times S, K^{|W \setminus S|}, \lambda)$-PRDF.*

证明. 令 $\mathcal{F}$ 为一个 (G, H, K, λ)-PRDF 且 $M=(m_{ij})$, $1 \le i \le k^*$, $1 \le j \le |W \setminus S|$ 为一个齐性的 $(W, S, k^*; 1)$-HDM. 每个子集 $\{b_1, \ldots, b_k\} \in \mathcal{F}$ 对应于以下形式的 $|W \setminus S|$ 个集合

$$\{(b_1, m_{1j}), \ldots, (b_k, m_{kj})\}, 1 \le j \le |W \setminus S|.$$

假设 $\mathcal{F}'$ 由所有这些子集构成, 即,

$$\mathcal{F}' = \{\{(b_1, m_{1j}), \ldots, (b_k, m_{kj})\} \mid 1 \le j \le |W \setminus S|, \{b_1, \ldots, b_k\} \in \mathcal{F}\}.$$

由于 $\mathcal{F}$ 的子集形成 $G \setminus H$ 的一个划分且 M 是 W 上相对于 S 的一个齐性的带洞差矩阵, $\mathcal{F}'$ 的子集形成 $(G \times W) \setminus ((G \times S) \cup (H \times W))$ 的一个划分. 易知 $\mathcal{F}'$ 是一个 $(G \times W; G \times S, H \times W; H \times S, K^{|W \setminus S|}, \lambda)$-PRDF. □

其次, 我们有以下的复合构造.

构造 4.5 (复合构造): *假设 n 是一个正整数. 假设存在一个 $(G; H_1, H_2, \ldots, H_n; U, K, \lambda)$-PRDF. 假设 t 满足 $1 \le t \le n$ 以及对每个 $1 \le i \le t$, 存在一个 (H_i, U, K_i, λ)-*

PRDF. 如果 $t \leq n-1$, 那么存在一个 $(G; H_{t+1}, H_{t+2}, \ldots, H_n; U, K', \lambda)$-PRDF 满足 $K' = K \bigcup (\cup_{i=1}^{t} K_i)$. 特别地, 如果 $t = n$, 那么存在一个 (G, U, K', λ)-PRDF 满足 $K' = K \bigcup (\cup_{i=1}^{n} K_i)$.

证明. 令 $\mathcal{F}$ 为给定的 $(G; H_1, H_2, \ldots, H_n; U, K, \lambda)$-PRDF. 对每个 $1 \leq i \leq t$, 令 $\mathcal{F}_i$ 为一个(H_i, U, K_i, λ)-PRDF. 易见 $\mathcal{F} \bigcup (\cup_{i=1}^{t} \mathcal{F}_i)$ 是一个 $(G; H_{t+1}, H_{t+2}, \ldots, H_n;\ U, K', \lambda)$-PRDF 满足 $K' = K \bigcup (\cup_{i=1}^{t} K_i)$. 当 $t = n$, $\mathcal{F} \bigcup (\cup_{i=1}^{n} \mathcal{F}_i)$ 是一个 (G, U, K', λ)-PRDF, 其中 $K' = K \bigcup (\cup_{i=1}^{n} K_i)$. □

结合以上两个构造, 我们有以下的主要构造的推广.

构造 4.6 (主要构造的推广): 假设有以下的存在:

1. 一个 (G, H, K_1, λ)-PRDF;
2. 一个齐性的 $(W, S, k^*; 1)$-HDM 满足 $k^* = \max\{k \mid k \in K_1\}$;
3. 一个 $(G \times S, H \times S, K_2, \lambda)$-PRDF;
4. 一个 $(H \times W, K_3, \lambda)$-PDF.

那么存在一个 $(G \times W, K, \lambda)$-PDF 满足 $K = K_1^{|W \setminus S|} \cup K_2 \cup K_3$.

证明. 令 $\mathcal{F}$ 为一个 (G, H, K_1, λ)-PRDF 且 D 为一个齐性的 $(W, S, k^*; 1)$-HDM. 由构造 4.4, 我们有一个 $(G \times W; G \times S, H \times W; H \times S, K^{|W \setminus S|}, \lambda)$-PRDF $\mathcal{F}_1$. 注意到存在一个 $(G \times S, H \times S, K_2, \lambda)$-PRDF $\mathcal{F}_2$ 和一个 $(H \times W, K_3, \lambda)$-PDF $\mathcal{F}_3$. 由构造 4.5, $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$ 是一个 $(G \times W, K, \lambda)$-PDF 满足 $K = K_1^{|W \setminus S|} \cup K_2 \cup K_3$. □

以下, 我们利用以上构造给出划分式差族的一个无穷类. 作为准备, 我们有以下的定义. 给定两个正整数 k 和 n, 一个横截设计 (transversal design) 是一个满足以下条件的三元组 $(X, \mathcal{G}, \mathcal{B})$:

1. X 是一个包含 kn 个元素 (称为点) 的集合;
2. $\mathcal{G}$ 是一个包含 X 的 n-子集 (称为组) 的集合, 这些 n-子集划分了 X;
3. $\mathcal{B}$ 是一个包含 X 的子集 (称为区组) 的集合. 每个区组与每个组恰好相交于一个点, 使得来自不同组的两个点恰好出现在 $\mathcal{B}$ 的一个区组中.

以上的横截设计被记做一个 TD(k,n). 由定义知 TD(k,n) 中每个区组包含 k 个点且共有 n^2 个区组. 以下的横截设计是熟知的.

命题 4.8 (文献[197]): *令 q 为一个素数幂. 那么存在一个* TD$(q+1,q)$.

进而, 我们可以从一个 TD$(q+1,q)$ 导出一个齐性的带洞差矩阵. 以下构造类似于文献[47]中带洞差矩阵的构造.

引理 4.1: *令 q 为一个素数幂. 存在一个齐性的 $(\mathbb{Z}_{q^2-1},(q+1)\mathbb{Z}_{q^2-1},q;1)$-HDM, 其中 $(q+1)\mathbb{Z}_{q^2-1}$ 是 $\mathbb{Z}_{q^2-1}$ 的形如 $\{0,q+1,2(q+1),\ldots,(q-2)(q+1)\}$ 的子群.*

证明. 记 $I_q=\{0,1,\ldots,q-1\}$. 由命题 4.8, 我们有一个三元组 $(X,\mathcal{G},\mathcal{B})$ 作为一个 TD$(q+1,q)$. 不失一般性, 我们可以假设 $X=I_q\times\{1,2,\ldots,q+1\}$, $\mathcal{G}=\{I_q\times\{i\}\mid 1\le i\le q+1\}$ 且 $\mathcal{B}$ 包含以下的 q 个区组

$$\{(s,1),(s,2),\ldots,(s,q),(q-1,q+1)\},s\in I_q.$$

这 q 个区组是所有的包含 $(q-1,q+1)$ 的区组. 令 $\mathcal{B}_0=\{B_j\mid 1\le j\le q(q-1)\}$ 不包含 $(q-1,q+1)$ 的区组的集合. 对于 $1\le j\le q(q-1)$, 令 $B_j=\{(b_{0j},1),(b_{1j},2),\ldots,(b_{qj},q+1)\}$. 那么, 对任意的 $0\le i<l\le q-1$, 我们有

$$\{(b_{ij},b_{lj})\mid 1\le j\le q(q-1)\}=(I_q\times I_q)\setminus\{(x,x)\mid x\in I_q\}.$$

同时, 对任意的 $0\le i\le q-1$, 我们有

$$\{(b_{ij},b_{qj})\mid 1\le j\le q(q-1)\}=I_q\times\{0,1,\ldots,q-2\}.$$

由文献[24], 存在一个 $(\mathbb{Z}_{q^2-1},(q+1)\mathbb{Z}_{q^2-1},[q^1],1)$-RDF $A=\{a_i\mid 0\le i\le q-1\}$. 易知存在 A 的一个适当的平移 $A+g$, 其中 $g\in\mathbb{Z}_{q^2-1}$ 且 $A+g=\{a_i+g\mid a_i\in A\}$, 满足 $(A+g)\cap(q+1)\mathbb{Z}_{q^2-1}=\emptyset$. 为了方便, 我们假设 $A\cap(q+1)\mathbb{Z}_{q^2-1}=\emptyset$.

令 $D=(d_{ij})$ 为一个 $\mathbb{Z}_{q^2-1}$ 上的 $q\times q(q-1)$ 矩阵, 其中 $d_{ij}\equiv a_{b_{ij}}+(q+1)b_{qj}\pmod{q^2-1}$, $0\le i\le q-1$, $1\le j\le q(q-1)$. 对任意 $0\le i<l\le q-1$, 注意到 $\{(b_{ij},b_{lj})\mid 1\le j\le q(q-1)\}=(I_q\times I_q)\setminus\{(x,x)\mid x\in I_q\}$. D 中第 $(i+1)$ 行和第 $(l+1)$

行的差构成多重集 $\{d_{ij}-d_{lj} \mid 1 \le j \le q(q-1)\}$, 亦即多重集 $\Delta A = \mathbb{Z}_{q^2-1} \setminus (q+1)\mathbb{Z}_{q^2-1}$. 所以, D 是 $\mathbb{Z}_{q^2-1}$ 上相对于 $(q+1)\mathbb{Z}_{q^2-1}$ 的一个带洞差矩阵.

由于 $A \cap (q+1)\mathbb{Z}_{q^2-1} = \emptyset$, D 的每个元素属于 $\mathbb{Z}_{q^2-1} \setminus (q+1)\mathbb{Z}_{q^2-1}$. 注意到 $\{(b_{ij}, b_{qj}) \mid 1 \le j \le q(q-1)\} = I_q \times \{0, 1, \ldots, q-2\}$ 对每个 $0 \le i \le q-1$ 成立且 A 的元素模 $q+1$ 两两不同. 那么, 对每个 $0 \le i \le q-1$,

$$\{d_{ij} \equiv a_{b_{ij}} + (q+1)b_{qj} \pmod{q^2-1} \mid 1 \le j \le q(q-1)\}$$

中的元素两两不同. 即, D 的每行由 $\mathbb{Z}_{q^2-1} \setminus (q+1)\mathbb{Z}_{q^2-1}$ 的元素构成. 因而, D 是一个齐性的 $(\mathbb{Z}_{q^2-1}, (q+1)\mathbb{Z}_{q^2-1}, q; 1)$-HDM. □

以下的划分式相对差族将在我们的构造中用到.

引理 4.2: *存在一个* $(\mathbb{Z}_{q^2-1}, (q+1)\mathbb{Z}_{q^2-1}, [q^{q-1}], q-1)$-PRDF.

证明. 如引理 4.1 的证明, 令 $A = \{a_0, a_1, \ldots, a_{q-1}\}$ 为一个 $(\mathbb{Z}_{q^2-1}, (q+1)\mathbb{Z}_{q^2-1}, [q^1], 1)$-RDF 满足 $A \cap (q+1)\mathbb{Z}_{q^2-1} = \emptyset$. 令

$$\mathcal{F} = \{\{(a_0+j(q+1)) \bmod (q^2-1), \ldots, (a_{q-1}+j(q+1)) \bmod (q^2-1)\} \mid 0 \le j \le q-2\}.$$

由于 A 的元素模 $q+1$ 两两不同, 易知 $\mathcal{F}$ 是一个 $(\mathbb{Z}_{q^2-1}, (q+1)\mathbb{Z}_{q^2-1}, [q^{q-1}], q-1)$-PRDF. □

以下, 我们将给出新的划分式差族的构造.

定理 4.11: *令* n *为一个正整数. 那么存在一个* $(\mathbb{Z}_{2^n+1} \times \mathbb{Z}_{2^{2n}-1}, [(2^n)^{2^{2n}+2^n-2}\ (2^n-1)^1], 2^n-1)$-PDF.

证明. 令 $\{1, 2, \ldots, 2^n\}$ 为一个 $(\mathbb{Z}_{2^n+1}, \{0\}, [(2^n)^1], 2^n-1)$-PRDF. 由引理 4.1, 存在一个齐性的 $(\mathbb{Z}_{2^{2n}-1}, (2^n+1)\mathbb{Z}_{2^{2n}-1}, 2^n; 1)$-HDM. 因为 $\mathbb{Z}_{2^{2n}-1} \cong \mathbb{Z}_{2^n+1} \times \mathbb{Z}_{2^n-1}$ 且子群 $(2^n+1)\mathbb{Z}_{2^{2n}-1} \cong \{0\} \times \mathbb{Z}_{2^n-1}$, 由引理 4.2, 存在一个 $(\mathbb{Z}_{2^n+1} \times \mathbb{Z}_{2^n-1}, \{0\} \times \mathbb{Z}_{2^n-1}, [(2^n)^{2^n-1}], 2^n-1)$-PRDF. 由命题 4.4, 存在一个 $(\{0\} \times \mathbb{Z}_{2^{2n}-1}, [(2^n)^{2^n-1}(2^n-1)^1], 2^n-1)$-PDF. 应用构造 4.6, 我们得到一个 $(\mathbb{Z}_{2^n+1} \times \mathbb{Z}_{2^{2n}-1}, [(2^n)^{2^{2n}+2^n-2}(2^n-1)^1], 2^n-1)$-PDF. □

最后, 我们在表 4.1 中总结新得到的划分式差族. 表中的一些符号定义如下.

令 q 记一个素数幂. 对 $1 \le j \le t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的整数. 记 $G_1 = \mathbb{Z}_{v_1} \times \cdots \times \mathbb{Z}_{v_t}$ 和 $v = \prod_{j=1}^{t} v_j$. 令$p_1, \ldots, p_l$ 为素数. 记 $G_2 = \mathbb{F}^+_{p_1^{s_1}} \times \mathbb{F}^+_{p_2^{s_2}} \times \cdots \times \mathbb{F}^+_{p_l^{s_l}}$ 且 $u = \prod_{i=1}^{l} p_i^{s_i}$.

表 4.1　新构造的(G, K, λ) 划分式差族

G	K	λ	限制
G_1	$[f^{\frac{v-1}{f}}1^1]$	$f-1$	$f \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$\mathbb{Z}_{k+1} \times G_1$	$[k^{v+\frac{v-1}{k}}1^1]$	$k-1$	$k \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$\mathbb{Z}_{k+1} \times G_2$	$[k^{u+\frac{u-1}{k}}1^1]$	$k-1$	$k \mid p_i^{s_i}-1, 1 \le i \le l$
$\mathbb{Z}_{\frac{q^{n+1}-1}{q-1}} \times G_1$	$[q^s 1^1], s=\frac{q^n-1}{q-1}v+\frac{v-1}{q}$	$q-1$	$q \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$\mathbb{Z}_{\frac{q^{n+1}-1}{q-1}} \times G_2$	$[q^s 1^1], s=\frac{q^n-1}{q-1}u+\frac{u-1}{q}$	$q-1$	$q \mid p_i^{s_i}-1, 1 \le i \le l$
$G_1 \times \mathbb{F}_q^+$	$[(\frac{q+11}{8})^s 2^{\frac{q-1}{4}}(\frac{q-1}{4})^1(\frac{q+3}{4})^1]$ $s=\frac{8q(v-1)}{q+11}$	$\frac{q+3}{8}$	$q=25+4b^2$ 或 $49+4b^2, b$ 奇数 $\frac{q+11}{8} \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$G_1 \times \mathbb{F}_q^+$	$[(2c^2+2)^s 2^{3b^2}(b^2)^1(b^2+1)^1]$ $s=\frac{q(v-1)}{2c^2+2}$	$2c^2+1$	$q=1+8b^2=9+64c^2, b, c$ 奇数 $2c^2+2 \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$G_1 \times \mathbb{F}_q^+$	$[(\frac{3q+1}{8})^s(\frac{q-1}{4})^1(\frac{q+3}{4})^1(\frac{q-1}{2})^1]$ $s=\frac{8q(v-1)}{3q+1}$	$\frac{3q-7}{8}$	$q=4+b^2, b \equiv 1 \pmod 4$ $\frac{3q+1}{8} \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$G_1 \times \mathbb{F}_q^+$	$[(\frac{3q+5}{8})^s(\frac{q-1}{4})^2(\frac{q+1}{2})^1]$ $s=\frac{8q(v-1)}{3q+5}$	$\frac{3q-3}{8}$	$q=9+4b^2, b$ 偶数 $\frac{3q+5}{8} \mid \gcd(p_{j1}-1, \ldots, p_{jl_j}-1), 1 \le j \le t$
$G_2 \times \mathbb{F}_q^+$	$[(\frac{q+11}{8})^s 2^{\frac{q-1}{4}}(\frac{q-1}{4})^1(\frac{q+3}{4})^1]$ $s=\frac{8q(u-1)}{q+11}$	$\frac{q+3}{8}$	$q=25+4b^2$ 或 $49+4b^2, b$ 奇数 $\frac{q+11}{8} \mid p_i^{s_i}-1, 1 \le i \le l$
$G_2 \times \mathbb{F}_q^+$	$[(2c^2+2)^s 2^{3b^2}(b^2)^1(b^2+1)^1]$ $s=\frac{q(u-1)}{2c^2+2}$	$2c^2+1$	$q=1+8b^2=9+64c^2, b, c$ 奇数 $2c^2+2 \mid p_i^{s_i}-1, 1 \le i \le l$
$G_2 \times \mathbb{F}_q^+$	$[(\frac{3q+1}{8})^s(\frac{q-1}{4})^1(\frac{q+3}{4})^1(\frac{q-1}{2})^1]$ $s=\frac{8q(u-1)}{3q+1}$	$\frac{3q-7}{8}$	$q=4+b^2, b \equiv 1 \pmod 4$ $\frac{3q+1}{8} \mid p_i^{s_i}-1$ 对 $1 \le i \le l$
$G_2 \times \mathbb{F}_q^+$	$[(\frac{3q+5}{8})^s(\frac{q-1}{4})^2(\frac{q+1}{2})^1]$ $s=\frac{8q(u-1)}{3q+5}$	$\frac{3q-3}{8}$	$q=9+4b^2, b$ 偶数 $\frac{3q+5}{8} \mid p_i^{s_i}-1, 1 \le i \le l$
$\mathbb{Z}_{2^n+1} \times \mathbb{Z}_{2^{2n}-1}$	$[(2^n)^{2^{2n}+2^n-2}(2^n-1)^1]$	2^n-1	$n \ge 1$

4.1.7　用划分式差族构造最优常重复合码

常重复合码 (Constant composition codes) 应用于电力线路通信的调制中[226]. 在本小节中, 我们应用新得到的划分式差族构造最优的常重复合码.

令 $\mathcal{A} = \{0, 1, \ldots, l-1\}$ 为一个有 l 个符号的字母表. 一个 $(n, M, d, [\omega_0, \ldots, \omega_{l-1}])_l$-CCC 是一个大小为 M, 极小汉明距离为 d 的子集$C \subset \mathcal{A}^n$, 满足符号 i 在 C 的每个码字中恰好出现 ω_i 次. 由于 $\mathcal{A}$ 中的符号并无本质区别, 我们将 $[\omega_0, \ldots, \omega_{l-1}]$ 视作一个多重集, 并记做 $[k_1^{u_1} k_2^{u_2} \ldots k_s^{u_s}]$, 其中 k_i 在 $[\omega_0, \ldots, \omega_{l-1}]$ 中恰好出现 u_i 次, $1 \le i \le s$.

给定长度 n, 极小距离 d 和类型 $[\omega_0, \ldots, \omega_{l-1}]$, 我们要构造一个 $(n, M, d, [\omega_0, \ldots, \omega_{l-1}])_l$-CCC 使得 M 尽可能的大. 令 $A_l(n, d, [\omega_0, \ldots, \omega_{l-1}])$ 为一个 $(n, M, d, [\omega_0, \ldots, \omega_{l-1}])_l$-CCC 最大可能的大小. 以下的界为 $A_l(n, d, [\omega_0, \ldots, \omega_{l-1}])$ 提供了基本的限制.

命题 4.9 (引理 3[194]): 如果 $nd - n^2 + (\omega_0^2 + \cdots + \omega_{l-1}^2) > 0$, 那么

$$A_l(n, d, [\omega_0, \ldots, \omega_{l-1}]) \leq \frac{nd}{nd - n^2 + (\omega_0^2 + \cdots + \omega_{l-1}^2)}. \tag{4.1}$$

一个达到 (4.1) 的常重复合码被称为是最优的. 以下的命题表明最优的常重复合码可由划分式差族导出.

命题 4.10 (构造 6[85]): 如果一个 (G, K, λ)-PDF 存在, 其中 $n = |G|$ 且 $K = [k_1^{u_1} k_2^{u_2} \ldots k_s^{u_s}]$, 那么存在一个最优的 $(n, n, n - \lambda, K)_l$-CCC 达到 (4.1), 其中 $l = \sum_{i=1}^{s} u_i$.

借助命题 4.10, 几类新的最优的常重复合码可由新得到的划分式差族导出. 这些结果整理在表 4.2. 其中用到的记号定义如下. 令 q 记一个素数幂. 对 $1 \leq j \leq t$, 令 v_j 为一个分解为 $v_j = \prod_{i=1}^{l_j} p_{ji}^{m_{ji}}$ 的整数. 我们令 $v = \prod_{j=1}^{t} v_j$. 令 $p_1, \ldots, p_l$ 为素数且 $u = \prod_{i=1}^{l} p_i^{s_i}$.

4.1.8 总结

本节考虑了划分式差族的组合构造. 我们提出了划分式相对差族的概念, 这个概念在我们的构造中起到了重要的作用. 我们提出了划分式差族的两个一般的递归构造. 这些构造为之前从分圆导出了几个无穷类提供了一个简单的解释. 此外, 我们得到了若干类新的划分式差族. 这些划分式差族可以导出最优的常重复合码.

我们指出划分式相对差族的概念和名为框架 (frame) 的组合构型密切相关[112]. 事实上, 一个划分式相对差族可以导出一个在点集上有正则自同构群的框架. 因此, 划分式相对差族在组合设计领域也拥有独立的研究兴趣.

4.2 型不一致的可分组设计的一个新构造

4.2.1 引言

一个集合系统 (set system) 是一个二元对 $(X, \mathcal{B})$, 其中 X 是一个点 (point) 的集合且 $\mathcal{B}$ 是一族被称为区组 (block) 的 X 的子集的集合. 令 $(X, \mathcal{B})$ 为一个集合系统且 $\mathcal{G}$ 为 X 的一个划分, 划分中的子集被称为组 (group), 三元对 $(X, \mathcal{G}, \mathcal{B})$ 被称为一个可分组设计 (group divisible design), 如果 X 的任意一个不同的点组成的点对或者出现在一个组中, 或者出现在恰好一个区组中, 但不会两者都满足. 一个型为 $g_1^{u_1} g_2^{u_2} \ldots g_s^{u_s}$ 的

表 4.2　由划分式差族导出的新的最优常重复合码

$(n, M, d, K)_l$-CCC	限制
$(v, v, v-f+1, [f^{\frac{v-1}{f}}1^1])_l$ $l=\frac{v-1}{f}+1$	$f \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1)$ $1\le j\le t$
$(v(k+1), v(k+1), v(k+1)-k+1, [k^{v+\frac{v-1}{k}}1^1])_l$ $l=\frac{v-1}{k}+v+1$	$k \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1)$ $1\le j\le t$
$(u(k+1), u(k+1), u(k+1)-k+1, [k^{u+\frac{u-1}{k}}1^1])_l$ $l=\frac{u-1}{k}+u+1$	$k \mid p_i^{s_i}-1$ $1\le i\le l$
$(\frac{v(q^{n+1}-1)}{q-1}, \frac{v(q^{n+1}-1)}{q-1}, \frac{v(q^{n+1}-1)}{q-1}-q+1, [q^s1^1])_{s+1}$ $s=\frac{q^n-1}{q-1}v+\frac{v-1}{q}$	$q \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1)$ $1\le j\le t$
$(\frac{u(q^{n+1}-1)}{q-1}, \frac{u(q^{n+1}-1)}{q-1}, \frac{u(q^{n+1}-1)}{q-1}-q+1, [q^s1^1])_{s+1}$ $s=\frac{q^n-1}{q-1}u+\frac{u-1}{q}$	$q \mid p_i^{s_i}-1$ $1\le i\le l$
$(qv, qv, qv-\frac{q+3}{8}, [(\frac{q+11}{8})^s 2^{\frac{q-1}{4}}(\frac{q-1}{4})^1(\frac{q+3}{4})^1])_l$ $s=\frac{8q(v-1)}{q+11}, l=s+\frac{q-1}{4}+2$	$q=25+4b^2$ 或 $49+4b^2$, b 奇数 $\frac{q+11}{8} \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1), 1\le j\le t$
$(qv, qv, qv-2c^2-1, [(2c^2+2)^s 2^{3b^2}(b^2)^1(b^2+1)^1])_l$ $s=\frac{q(v-1)}{2c^2+2}, l=s+3b^2+2$	$q=1+8b^2=9+64c^2$, b, c 奇数 $2c^2+2 \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1), 1\le j\le t$
$(qv, qv, qv-\frac{3q-7}{8}, [(\frac{3q+1}{8})^s(\frac{q-1}{4})^1(\frac{q+3}{4})^1(\frac{q-1}{2})^1])_l$ $s=\frac{8q(v-1)}{3q+1}, l=s+3$	$q=4+b^2, b\equiv 1 \pmod 4$ $\frac{3q+1}{8} \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1), 1\le j\le t$
$(qv, qv, qv-\frac{3q-3}{8}, [(\frac{3q+5}{8})^s(\frac{q-1}{4})^2(\frac{q+1}{2})^1])_l$ $s=\frac{8q(v-1)}{3q+5}, l=s+3$	$q=9+4b^2$, b 偶数 $\frac{3q+5}{8} \mid \gcd(p_{j1}-1,\ldots,p_{jl_j}-1), 1\le j\le t$
$(qu, qu, qu-\frac{q+3}{8}, [(\frac{q+11}{8})^s 2^{\frac{q-1}{4}}(\frac{q-1}{4})^1(\frac{q+3}{4})^1])_l$ $s=\frac{8q(u-1)}{q+11}, l=s+\frac{q-1}{4}+2$	$q=25+4b^2$ 或 $49+4b^2$, b 奇数 $\frac{q+11}{8} \mid p_i^{s_i}-1, 1\le i\le l$
$(qu, qu, qu-2c^2-1, [(2c^2+2)^s 2^{3b^2}(b^2)^1(b^2+1)^1])_l$ $s=\frac{q(u-1)}{2c^2+2}, l=s+3b^2+2$	$q=1+8b^2=9+64c^2$, b, c 奇数 $2c^2+2 \mid p_i^{s_i}-1, 1\le i\le l$
$(qu, qu, qu-\frac{3q-7}{8}, [(\frac{3q+1}{8})^s(\frac{q-1}{4})^1(\frac{q+3}{4})^1(\frac{q-1}{2})^1])_l$ $s=\frac{8q(u-1)}{3q+1}, l=s+3$	$q=4+b^2, b\equiv 1 \pmod 4$ $\frac{3q+1}{8} \mid p_i^{s_i}-1, 1\le i\le l$
$(qu, qu, qu-\frac{3q-3}{8}, [(\frac{3q+5}{8})^s(\frac{q-1}{4})^2(\frac{q+1}{2})^1])_l$ $s=\frac{8q(u-1)}{3q+5}, l=s+3$	$q=9+4b^2$, b 偶数 $\frac{3q+5}{8} \mid p_i^{s_i}-1, 1\le i\le l$
$(m, m, m-2^n+1, [(2^n)^{2^{2n}+2^n-2}(2^n-1)^1])_l$ $m=(2^n+1)(2^{2n}-1), l=2^{2n}+2^n-1$	—

K-GDD 是一个可分组设计, 其中每个区组的大小属于集合 K 且有 u_i 个大小为 g_i 的组, $1\le i\le s$. 一个可分组设计被称作是型一致的 (uniform) 如果所有的组有相同的大小. 否则, 它被称为型不一致的 (non-uniform).

在一个可分组设计 $(X, \mathcal{G}, \mathcal{B})$ 中, 区组的一个 α-平行类 (α-parallel class) 是一个子集 $\mathcal{B}'\subset\mathcal{B}$ 使得每个点 $x\in X$ 恰好包含在 $\mathcal{B}'$ 中 α 个区组中. 有时, 当 $\alpha=1$, 我们称之为一个平行类 (parallel class).

自从 Wilson 基本构造法 (Wilson's Fundamental Construction) 提出以来[284], 可分组设计在其它组合构型的构造中起到了重要的作用, 例如, 成对平衡设计 (pairwise balanced designs)[284–286], 填充 (packings)[29,118,211], 框架 (frames)[112,255] 等等. 可分组设计在编码领域也有很多重要的应用, 例如光正交码 (optical orthogonal codes)[104,276], 常

重码 (constant weight codes)[53,101,156] 和常重复合码 (constant composition codes)[53]. 可分组设计的构造在组合设计领域已成为一个中心问题.

关于可分组设计的构造, 已发展了许多方法. 在文献中, 主要有两种直接构造的方法. 第一是几何方法, 利用了有限几何中的关联结构. 一些型一致的可分组设计的无穷类可由诸如卵形 (ovals)[121], Baer 子平面 (Baer subplanes)[121,249], 椭圆半平面 (elliptic semiplanes)[11] 等等. 第二个方法基于差方法. 在此方法中, 我们需要选取一个自同构群作用到基区组上生成所有的区组. 有时, 选取合适的自同构群涉及精细的技巧. 关于递归构造, Wilson 基本构造是最重要的且已在一系列研究中被推广. 在文献[254] 中, Stinson 利用不完全可分组设计推广了 Wilson 基本构造法. Zhu[310] 利用双可分组设计的语言重述了 Stinson 的构造, 并大大简化了证明. 从那以后, 一些重要的不完全可分组设计和双可分组设计构造被提出[205,210,236]. 在文献[48] 中, Chang 和 Miao 得出了一个非常一般的构造, 统一了以上的构造.

基于这些成熟的方法, 得到了一系列关于型一致的可分组设计的构造. 感兴趣的读者可参考综述[115]. 值得注意的是, 除了从有限几何得到的可分组设计, 大部分结果中的去组大小都很小, 一般不超过五.

当我们利用可分组设计构造其它组合设计时, 我们偏好组有不同的大小, 以适应不同的情况[65]. 与型一致的可分组设计相比, 型不一致的构造的结果要少得多. 一个主要的原因是, 在型不一致的情形下, 缺乏合适的代数和几何结构. 因而, 型不一致可分组设计的构造是一个非常有挑战性的问题.

在本节中, 我们考虑仅有一个组有不同大小的型不一致的可分组设计的构造, 亦即, 考虑型为 $g^u m^1$ 的 $\{k\}$-GDD. 此外, 我们专注于 $u = k$ 的情形. 这个情形有着根本的重要性, 因为它的解决能够帮助我们处理更一般的 u 的情况. 同时, 这个情形也特别的困难, 因为区组的大小仅比组的个数小一这个条件就区组的安排施加了严格的限制.

为了克服前述的困难, 我们提出了如下的型不一致可分组设计的新构造. 首先, 给定一个具有特定参数的广义差集, 可以用一般方法生成一个初始的可分组设计. 其次, 最重要的, 我们提出一种截断的方法修改初始的可分组设计, 得到一个新的 $\{k-1, k\}$-GDD 满足所有大小为 $k-1$ 的区组形成一个 $(k-1)$-平行类. 最后, 我们将 $(k-1)$-平行类划分为 1-平行类. 之后, 一个 $\{k\}$-GDD 可由标准的方法得出.

我们的构造有两个关键点. 其一是选择合适的广义差集. 其二是将得到的 $(k-1)$-平行类划分为 1-平行类. 事实上, 将 $(k-1)$-平行类划分为 1-平行类通常是一个困难的

问题. 作为替代, 我们提出了一个变形的构造回避这个问题. 在变形的构造中, 为了避免直接去划分 $(k-1)$-平行类, 我们利用 Rees 乘积构造 (Rees' product constructions) 去膨胀带有一个 $(k-1)$-平行类的可分组设计, 其中这个 $(k-1)$-平行类给出一个新的具有更大组大小的可分组设计中的 1-平行类.

为了说明新构造和它的变形, 我们展示了型不一致可分组设计的一些新的具体构造. 在这些构造中, 我们利用了和有限射影平面密切相关的一些广义差集. 同时, 我们提出了一个差方法去直接划分 $(k-1)$-平行类. 因之, 我们得到了型不一致可分组设计的几个无穷类, 并得到了许多具有较大区组大小的型不一致可分组设计的例子.

4.2.2 广义差集和相应的可分组设计

本节中, 之后所有考虑的群都是交换群. 在本小节中, 我们介绍广义差集的概念并证明某些可分组设计可以由它们得到. 这些可分组设计是我们构造的出发点.

我们首先回顾相对差集的定义. 令 G 为一个阶为 mn 的群, N 为 G 的一个阶为 n 的子群. 一个 k 元子集 $D \subset G$ 被称为 G 中相对于 N 的一个 (m, n, k, λ) **相对差集** (relative difference set), 如果差 $d \cdot (d')^{-1}$, $d, d' \in D$, $d \neq d'$ 覆盖了 $G \setminus N$ 中每个元素恰好 λ 次且不覆盖 N 中的元素. 子群 N 被称为**禁止子群** (forbidden subgroup), 或**例外子群** (exceptional subgroup). 作为一个自然的推广, 以下我们将考虑一个相对于若干子群的推广的差集.

令 G 为一个阶为 v 的群. 对 $1 \leq i \leq r$, 令 N_i 为一个 G 的阶为 n_i 子群, 其中 $N_1, N_2, \ldots, N_r$ 的两两相交皆为平凡. 一个 G 中相对于子群 $N_1, N_2, \ldots, N_r$ 的 $(v; n_1, n_2, \cdots, n_r; k, \lambda)$ **广义差集** (generalized difference set) 是 G 的一个 k 元子集 D 满足差 $d \cdot (d')^{-1}$, $d, d' \in D$, $d \neq d'$ 覆盖 $G \setminus (\cup_{i=1}^{r} N_i)$ 中每个元素恰好 λ 次, 且不覆盖 $\cup_{i=1}^{r} N_i$ 中元素. 子群 $N_1, \ldots, N_r$ 被称为**禁止子群** (forbidden subgroup), 或**例外子群** (exceptional subgroup). 特别地, 当仅有一个禁止子群时, 亦即 $r = 1$ 时, 一个广义差集就是一个相对差集. 注意一个满足 $r = 1$ 的广义差集的符号与相对差集原本的符号并不一致. 以下, 当我们考虑相对差集时, 我们将使用原本的符号.

令 $gD = \{gd \mid d \in D\}$ 为集合 D 的一个平移, 其中 $g \in G$. 熟知 G 中相对于 N 的差集 D 的所有平移, 形成一个可分组设计的所有区组, 其中 G 的元素为点且 N 的所有陪集为组. 以下引理说明一个可分组设计也可从一个广义差集中得到.

引理 4.3：令 D 为 G 中相对于 $N_1, N_2, \ldots, N_r$ 的一个 $(v; n_1, n_2, \cdots, n_r; k, 1)$-GDS. 那么存在一个 K-GDD, 型为 $n_i^{v/n_i}, 1 \le i \le r$, 其中 $K = \{k\} \cup \{n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_r\}$.

证明. 证明同相对差集的情形类似，故在此略去. □

以下, 我们列举三类与射影平面密切相关的广义差集. 这些广义差集源自 Dembowski-Piper 对具有较大的拟正则自同构群的射影平面的分类[75]. 事实上, 对许多这样的射影平面, 它们的存在性可被归结为相应的广义差集的存在性 (见文献[307] 定理 1.55 和文献[230] 第 5 章). 以下, 我们用 $\mathbb{F}_q$ 记阶为 q 的有限域. 用 $\mathbb{F}_q^+$ 和 $\mathbb{F}_q^*$ 记 $\mathbb{F}_q$ 的加法和乘法子群. $\mathrm{Tr}_q^{q^2}$ 是从 $\mathbb{F}_{q^2}$ 到 $\mathbb{F}_q$ 的迹函数.

命题 4.11 (Bose[24])：集合

$$D = \{x \in \mathbb{F}_{q^2}^* \mid \mathrm{Tr}_q^{q^2}(x) = 1\}$$

是一个 $\mathbb{F}_{q^2}^*$ 中相对于 $\mathbb{F}_q^*$ 的 $(q+1, q-1, q, 1)$-RDS.

命题 4.12 (Ganley[114])：集合

$$D = \{(x, x) \in \mathbb{F}_q^+ \times \mathbb{F}_q^* \mid x \in \mathbb{F}_q^*\}$$

是一个 $G = \mathbb{F}_q^+ \times \mathbb{F}_q^*$ 中相对于 $N_1 = \{(0, x) \mid x \in \mathbb{F}_q^*\}$ 和 $N_2 = \{(x, 1) \mid x \in \mathbb{F}_q^+\}$ 的 $(q(q-1); q-1, q; q-1, 1)$-GDS.

命题 4.13 (Kantor[168])：集合

$$D = \{(x, 1-x) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \mid x \in \mathbb{F}_q^* \setminus \{1\}\}$$

是一个 $G = \mathbb{F}_q^* \times \mathbb{F}_q^*$ 中相对于 $N_1 = \{(1, x) \mid x \in \mathbb{F}_q^*\}$, $N_2 = \{(x, 1) \mid x \in \mathbb{F}_q^*\}$ 和 $N_3 = \{(x, x) \mid x \in \mathbb{F}_q^*\}$ 的 $((q-1)^2; q-1, q-1, q-1; q-2, 1)$-GDS.

4.2.3 一个新的构造

在本小节中, 我们提出型不一致可分组设计的一个新的构造. 首先, 利用一个截断

技巧, 我们从某些可分组设计导出型一致的 K-GDDs, 其中 $K = \{k-1, k\}$ 且大小为 $k-1$ 的区组形成一个 $(k-1)$-平行类. 这些型一致的可分组设计是我们构造的关键.

构造 4.7 (截断技巧): 令 G 为一个阶为 $m(n+1)$ 的群. 令 D 为 G 中相对于子群 $N_i, 1 \le i \le r$ 的一个 $(m(n+1); m, n+1, n+1, \cdots, n+1; n, 1)$-GDS. 令 $n+1$ 为一个正整数, 有分解 $n+1 = ab$. 假设存在 G 的一个阶为 bm 的子群 H 包含 N_1. 那么, 对每个 $1 \le s \le a$, 存在一个型为 m^{bs} 的 $\{bs-1, bs\}$-GDD, 使得大小为 $bs-1$ 的区组形成一个 $(bs-1)$-平行类.

证明. 对 $1 \le i \le r$, 令 Γ_i 为 N_i 在 G 中所有陪集构成的集合. 记 $\mathcal{A}_1 = \{gD \mid g \in G\}$, $\mathcal{A}_2 = \cup_{i=2}^{r}\Gamma_i$. 假设 X 是 G 中元素构成的集合且 $\mathcal{G} = \Gamma_1$. 那么, 由引理 4.3, $(X, \mathcal{G}, \mathcal{A}_1 \cup \mathcal{A}_2)$ 是一个型为 m^{n+1} 的 $\{n, n+1\}$-GDD. 这是我们初始的可分组设计, 我们将要用一个截断技巧去修改它.

令 $\{h_1H, h_2H, \ldots, h_aH\}$ 为 H 在 G 中所有的陪集. 对任意 $1 \le s \le a$, 令 Y 为任意 s 个陪集的并. 不失一般性, 我们可令

$$Y = h_1H \cup h_2H \cup \ldots \cup h_sH.$$

由定义, Y 可被划分为 bs 个 N_1 的不同的陪集, 我们将这个划分记做 $\mathcal{G}'$. 我们将之前的可分组设计的区组按以下的方式截断. 令

$$\mathcal{B}_1 = \{A \cap Y \mid A \in \mathcal{A}_1\} = \{gD \cap Y \mid g \in G\}.$$

且

$$\mathcal{B}_2 = \{A \cap Y \mid A \in \mathcal{A}_2\} = \{gN_i \cap Y \mid gN_i \in \Gamma_i, 2 \le i \le r\}.$$

因而, 我们有一个新的集合系统 $(Y, \mathcal{G}', \mathcal{B}_1 \cup \mathcal{B}_2)$, 作为原来集合系统 $(X, \mathcal{G}, \mathcal{A}_1 \cup \mathcal{A}_2)$ 的一个截断版本. 易知 $(Y, \mathcal{G}', \mathcal{B}_1 \cup \mathcal{B}_2)$ 形成一个型为m^{bs} 的 K-GDD. 需要证明 $K = \{bs-1, bs\}$ 且大小为 $bs-1$ 的区组形成一个 $(bs-1)$-平行类.

首先我们考虑属于 $\mathcal{B}_2 = \{gN_i \cap Y \mid gN_i \in \Gamma_i, 2 \le i \le r\}$ 的区组. 由于 $N_1, N_2, \ldots, N_r$ 的两两相交是平凡的, 对每个 $gN_i \in \Gamma_i$ 和 $2 \le i \le r$, gN_i 交 N_1 的每个陪集于至多一个元素. 注意到 $|N_i| = n+1$ 且 N_1 共有 $n+1$ 个陪集, gN_i 交 N_1 的

每个陪集于恰好一个元素. 注意到 Y 是 bs 个 N_1 的陪集的并, 我们有 $|gN_i \cap Y| = bs$ 对每个 $gN_i \in \Gamma_i$ 和 $2 \leq i \leq r$. 因而, $\mathcal{B}_2$ 包含 $m(r-1)$ 个大小为 bs 的区组.

其次, 我们考虑 $\mathcal{B}_1$ 中的区组. 对 $1 \leq i \leq a$, 定义 $D_i = h_i D \cap Y$. 那么

$$\begin{aligned}\mathcal{B}_1 &= \{gD \cap Y : g \in G\} \\ &= \bigcup_{i=1}^{a} \{gD \cap Y : g \in h_i H\} \\ &= \bigcup_{i=1}^{a} \{h_i h D \cap Y : h \in H\} \\ &= \bigcup_{i=1}^{a} \{hD_i : h \in H\}.\end{aligned}$$

因而, $\mathcal{B}_1$ 中区组的大小由 D_i 的大小决定, 其中 $1 \leq i \leq a$. 由定义, D 交 N_1 的每个陪集于至多一个元素. 更确切的, 由于 $|D| = n$, D 于 N_1 的一个陪集不相交(这个陪集记做 xN_1), 且与每个剩下的陪集交于恰好一个点. 注意到 N_1 是 H 的一个子群满足 $[H : N_1] = b$. 因而,

$$|D \cap (h_i H)| = \begin{cases} b & \text{如果 } x \notin h_i H, \\ b-1 & \text{如果 } x \in h_i H. \end{cases} \tag{4.2}$$

注意到

$$|D_i| = |h_i D \cap Y| = \sum_{j=1}^{s} |h_i D \cap h_j H| = \sum_{j=1}^{s} |D \cap h_i^{-1} h_j H|. \tag{4.3}$$

对每个 $1 \leq i \leq a$, 存在恰好一个 $1 \leq j \leq a$, 使得 $x \in h_i^{-1} h_j H$. 因而我们可以定义一个映射

$$\begin{aligned}\psi : \{1, \ldots, a\} &\longrightarrow \{1, \ldots, a\} \\ i &\longrightarrow \psi(i),\end{aligned}$$

使得 $x \in h_i^{-1} h_{\psi(i)} H$. 容易验证 ψ 是一个双射. 由 (4.2) 和 (4.3),

$$|D_i| = bs - 1 \Longleftrightarrow \psi(i) \in \{1, 2, \ldots, s\}.$$

因此在集合 $D_i, 1 \le i \le a$ 中, 存在 s 个集合, 即 $D_{\psi^{-1}(k)}, 1 \le k \le s$, 大小为 $bs-1$, 且存在 $a-s$ 个大小为 bs. 所以, $\mathcal{B}_1$ 包含 bms 个大小为 $bs-1$ 的区组和 $bm(a-s)$ 个大小为 bs 的区组.

记 $D_k^* = D_{\psi^{-1}(k)}, 1 \le k \le s$. 那么集合 $\{hD_k^* \mid h \in H, 1 \le k \le s\}$ 由 $\mathcal{B}_1$ 中所有的大小为 $bs-1$ 的区组组成. 对 s 个陪集 $h_1H, h_2H, \ldots, h_sH$, D_k^* 交 h_kH 于 $b-1$ 个元素且交剩下的陪集于 b 个元素. 回顾 Y 由 s 个陪集 $h_1H, h_2H, \ldots, h_sH$ 组成. 那么对 $1 \le k \le s$, $\{hD_k^* \mid h \in H\}$ 覆盖 h_kH 的元素恰好 $b-1$ 次且覆盖 $Y \setminus h_kH$ 的元素恰好 b 次. 因而, $\{hD_k^* \mid h \in H, 1 \le k \le s\}$ 中的区组是所有大小为 $bs-1$ 的区组, 形成一个 $(bs-1)$-平行类.

总之, $(Y, \mathcal{G}', \mathcal{B}_1 \cup \mathcal{B}_2)$ 是一个型为 m^{bs} 的 $\{bs-1, bs\}$-GDD, 其中大小为 $bs-1$ 的区组形成一个 $(bs-1)$-平行类. □

应用构造 4.7 于 Bose 相对差集, Ganley 广义差集和 Kantor 广义差集, 我们得到以下结果.

推论 4.4: *令 q 为一个素数幂. 令 $ab = q'$ 其中 $q' \in \{q-1, q, q+1\}$. 对每个 $1 \le s \le a$, 存在一个型为 $(q-1)^{bs}$ 的 $\{bs-1, bs\}$-GDD, 其中大小为 $bs-1$ 的区组形成一个 $(bs-1)$-平行类.*

证明. 令 $ab = q$, 我们从命题 4.12 的 $(q(q-1); q-1, q; q-1, 1)$-GDS 出发. 取 $\mathbb{F}_q^+$ 的一个阶为 b 的子群 L. 在构造 4.7 中令 $m = n = q-1$ 且 $H = L \times \mathbb{F}_q^*$. 那么我们得到一个型为 $(q-1)^{bs}$ 的 $\{bs-1, bs\}$-GDD.

对 $ab = q+1$ 或 $q-1$, 我们可以从 Bose 相对差集或 Kantor 广义差集出发, 类似地处理. □

一个型不一致的可分组设计可由构造 4.7 直接得到, 如果相应的 $(bs-1)$-平行类能够被划分为 $(bs-1)$ 个 1-平行类.

定理 4.12: *令 $(X, \mathcal{G}, \mathcal{B})$ 为一个由构造 4.7 的得到的可分组设计. 如果 $(bs-1)$-平行类能够被划分为 $(bs-1)$ 个 1-平行类, 那么存在一个型为 $m^{bs}(bs-1)^1$ 的 $\{bs\}$-GDD .*

证明. 假设 $(bs-1)$-平行类能够被划分为 $(bs-1)$ 个 1-平行类. 我们可以添加一个包含 $bs-1$ 个点的组, 并建立 $bs-1$ 个点和 $bs-1$ 个 1-平行类之间的一一映射. 将每个点添加到相应的 1-平行类中的每个区组, 我们得到型为 $m^{bs}(bs-1)^1$ 的 $\{bs\}$-GDD . □

4.2.4 直接划分 α-平行类的具体构造

在本小节中, 依照上节的提出的构造方法, 我们给出型不一致可分组设计的具体构造. 我们构造的关键一步是直接划分构造 4.7 中的 α-平行类. 首先, 我们利用 Ganley 广义差集得出型不一致可分组设计的一个无穷类.

定理 4.13: *令 p 为一个素数. 令 m 和 n 为正整数使得 $n \mid m$. 那么, 存在一个型为 $(p^m-1)^{p^n}(p^n-1)^1$ 的 $\{p^n\}$-GDD.*

证明. 令 $G = \mathbb{F}^+_{p^m} \times \mathbb{F}^*_{p^m}$, $N_1 = \{(0,x) \mid x \in \mathbb{F}^*_{p^m}\}$, $N_2 = \{(x,1) \mid x \in \mathbb{F}^+_{p^m}\}$. 由命题 4.12, $D = \{(x,x) \in \mathbb{F}^+_{p^m} \times \mathbb{F}^*_{p^m} \mid x \in \mathbb{F}^*_{p^m}\}$ 是 G 相对于 N_1 和 N_2 的一个 $(p^m(p^m-1); p^m-1, p^m; p^m-1, 1)$-GDS. 令 ξ 为 $\mathbb{F}^*_{p^m}$ 的一个本原元且 $\theta = \xi^{\frac{p^m-1}{p^n-1}}$ 为 $\mathbb{F}^*_{p^n}$ 的一个本原元. 在构造 4.7 中令 $H = \mathbb{F}^+_{p^n} \times \mathbb{F}^*_{p^m}$ 且 $s = 1$, 我们有一个型为 $(p^m-1)^{p^n}$ 的 $\{p^n-1, p^n\}$-GDD, 它的点集 Y 包含 H 的元素. 注意到 D 交 N_1 的每个陪集于恰好一个点, 除了 $D \cap N_1 = \emptyset$. 因此, $D^* = D \cap Y$ 的大小为 p^n-1, 并且所有大小为 p^n-1 的区组为 $\{hD^* \mid h \in H\}$.

注意到

$$D^* = D \cap H = \{(\theta^i, \theta^i) \mid 0 \le i < p^n - 1\}.$$

集合 $\{hD^* \mid h \in \{0\} \times \mathbb{F}^*_{p^m}\}$ 能够划分为 p^n-1 个子集族 $\mathcal{C}_l$, $0 \le l < p^n-1$, 其中

$$\mathcal{C}_l = \{\{(\theta^i, \xi^j\theta^{i+l}) \mid 0 \le i < p^n-1\} \mid 0 \le j < \frac{p^m-1}{p^n-1}\}.$$

对每个 $0 \le l < p^n-1$, 易知区组

$$\{hS \mid S \in \mathcal{C}_l, h \in \mathbb{F}^+_{p^n} \times \{1\}\}$$

形成一个 1-平行类. 注意到所有大小为 p^n-1 的区组形如 $\{hD^* \mid h \in H\}$, 其中

$$\{hD^* \mid h \in H\} = \bigcup_{l=0}^{p^n-2} \{hS \mid S \in \mathcal{C}_l, h \in \mathbb{F}^+_{p^n} \times \{1\}\}.$$

因而, 大小为 p^n-1 的区组形成 p^n-1 个 1-平行类. 由定理 4.12, 我们有一个型如 $(p^m-1)^{p^n}(p^n-1)^1$ 的 $\{p^n\}$-GDD. □

当用到的广义差集是 Bose 相对差集或 Kantor 广义差集时, 我们没有找到一个类似以上的一般方法划分 α-平行类. 然而, 我们可以利用以下的方法得到很多型不一致可分组设计的例子.

令 q 为一个素数幂且 D 为 $(q+1, q-1, q, 1)$ Bose 相对差集. 我们选择三个正整数 b, l, d, 满足

$$d \mid (b-1) \mid l \mid b(q-1) \mid q^2-1. \tag{4.4}$$

将 D 用到构造 4.7 中并令 $Y = H = \frac{q+1}{b}\mathbb{Z}_{q^2-1} \cong \mathbb{Z}_{b(q-1)}$, $s=1$, 我们有一个型如 $(q-1)^b$ 的 $\{b-1, b\}$-GDD. 特别地, 大小为 $b-1$ 的区组形如

$$\{hD^* \mid h \in H\},$$

其中 D^* 是 D 的一个平移和 H 的交, 大小为 $b-1$. 简单起见, 我们将 H 的元素等同于 $\mathbb{Z}_{b(q-1)}$ 的元素. 我们想要划分 $\{hD^* \mid h \in H\}$ 为 $b-1$ 个 1-平行类. 以下, 我们利用差方法在某些假设下得到一个划分. 取 $\mathbb{Z}_{b(q-1)}$ 的一个子群 $\mathbb{Z}_l$. 考虑 D^* 在 $\mathbb{Z}_l$ 上一族特殊的平移:

$$\{\{(r+di) \bmod l \mid r \in D^*\} \mid 0 \le i < \frac{l}{b-1}\}.$$

假设这族子集形成 $\mathbb{Z}_l$ 的一个划分. 那么区组 $\{D^* + di + lj, 0 \le i < \frac{l}{b-1}, 0 \le j < \frac{b(q-1)}{l}\}$ 形成一个 1-平行类, 记做 P. 那么

$$\{P + x + \frac{ld}{b-1}y, 0 \le x < d, 0 \le y < \frac{b-1}{d}\}$$

形成 $b-1$ 个 1-平行类. 由于集合

$$\{x + di + \frac{ld}{b-1}y + lj \mid 0 \le x < d, 0 \le i < \frac{l}{b-1}, 0 \le y < \frac{b-1}{d}, 0 \le j < \frac{b(q-1)}{l}\}$$

包含 H 的所有元素, 我们已将 $\{hD^* \mid h \in H\}$ 划分为 $b-1$ 个 1-平行类.

我们的差方法有两个关键点. 其一是我们首先选择 H 的一个子群 $\mathbb{Z}_l$ 并验证 D^* 的一族特殊的平移是否划分 $\mathbb{Z}_l$. 如果是, 我们可将这族平移扩展为一个 1-平行类. 其二, 这组特殊的平移由一个公差为 d 的等差数列决定. 这保证了之前构造的 1-平行类的一些平移生成所有的 1-平行类.

如果我们从 Kantor 广义差集出发, 以上的差方法同样有效. 令 q 为一个素数幂且 D 为 $((q-1)^2; q-1, q-1, q-1; q-2, 1)$ Kantor 广义差集. 令 L 为循环群 $\mathbb{F}_q^*$ 的阶为 b 的子群. 将 D 应用于构造 4.7, 令 $Y = H = L \times \mathbb{F}_q^*$ 且 $s = 1$, 我们有一个型如 $(q-1)^b$ 的 $\{b-1, b\}$-GDD. 特别地, 大小为 $b-1$ 的区组形如

$$\{hD^* \mid h \in H\},$$

其中 D^* 为 D 的一个平移和 H 的交, 大小为 $b-1$. 令

$$S^* = \{(1, r_2) \mid (r_1, r_2) \in D^*\}.$$

假设我们能划分 $\{lS^* \mid l \in \{1\} \times \mathbb{F}_q^*\}$ 为 $b-1$ 份 $\{1\} \times \mathbb{F}_q^*$, 例如 $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{b-1}$. 那么对每个 $1 \le i \le b-1$, $\{hC \mid h \in L \times \{1\}, C \in \mathcal{C}_i\}$ 形成一个 1-平行类. 那么, 我们可以将 $\{hD^* \mid h \in H\}$ 划分为 $b-1$ 个 1-平行类. 由于 $\mathbb{F}_q^*$ 是一个循环群, 划分 $\{lS^* \mid l \in \{1\} \times \mathbb{F}_q^*\}$ 为若干个 $\{1\} \times \mathbb{F}_q^*$ 与我们之前考虑 Bose 相对差集遇到的问题是一样的. 因此, 上述方法同样使用.

此处的差方法给出了一个明确的方法, 常常能将 α-平行类划分为 1-平行类. 利用这个方法连同 Bose 相对差集和 Kantor 广义差集, 我们用计算机搜索了点数不超过 5000 且 $6 \le k \le 13$ 的型不一致 $\{k\}$-GDDs. 搜索结果列在表 4.3. 之前对区组大小较小的可分组设计的研究主要集中于区组大小不超过五的情况, 我们成功得到了许多区组大小更大的型不一致可分组设计的例子.

4.2.5 新构造的变形

在本小节中, 我们利用 Rees 乘积构造[233–235] 给出之前新构造的一个变形. 与原构造相比, 这个变形采取了不同的策略去处理构造 4.7 中的 α-平行类. 不同于直接划分 α-平行类, 我们利用 Rees 构造去膨胀构造 4.7 中的可分组设计, 其中由 α-平行类得出一个组大小更大的可分组设计中的 1-平行类.

为了理解 Rees 构造, 我们需要以下的概念. 一个型为 m^k 的 $\{k\}$-GDD 被称为一个横截设计 (transversal design), 并记做 TD(k, m). 现在我们描述 Rees 乘积构造.

构造 4.8 (构造 2.1[234]): 假设存在一个型为 g^u 的 K-GDD, 其中有 l 个不同的大小为

表 4.3　从 Bose 相对差集和 Kantor 广义差集出发得到的型不一致可分组设计

q	k	组型	广义差集	q	k	组型	广义差集
181	7	$180^{7}6^{1}$	Bose	3067	7	$3066^{7}6^{1}$	Kantor
223	7	$222^{7}6^{1}$	Bose	3319	7	$3318^{7}6^{1}$	Kantor
337	7	$336^{7}6^{1}$	Kantor	3373	7	$3372^{7}6^{1}$	Bose
421	7	$420^{7}6^{1}$	Kantor	3529	7	$3528^{7}6^{1}$	Kantor
463	7	$462^{7}6^{1}$	Kantor	3583	7	$3582^{7}6^{1}$	Bose
811	7	$810^{7}6^{1}$	Bose	3613	13	$3612^{13}12^{1}$	Bose
853	7	$852^{7}6^{1}$	Bose	3823	7	$3822^{7}6^{1}$	Kantor
883	7	$882^{7}6^{1}$	Kantor	3907	7	$3906^{7}6^{1}$	Kantor
1021	7	$1020^{7}6^{1}$	Bose	3919	7	$3918^{7}6^{1}$	Bose
1117	13	$1116^{13}12^{1}$	Bose	4507	7	$4506^{7}6^{1}$	Bose
1723	7	$1722^{7}6^{1}$	Kantor	4591	7	$4590^{7}6^{1}$	Bose
1873	9	$1872^{9}8^{1}$	Kantor	4621	7	$4620^{7}6^{1}$	Kantor
2017	9	$2016^{9}8^{1}$	Kantor	4759	7	$4758^{7}6^{1}$	Bose
2029	7	$2028^{7}6^{1}$	Bose	4957	7	$4956^{7}6^{1}$	Kantor
2953	7	$2952^{7}6^{1}$	Bose	4969	7	$4968^{7}6^{1}$	Bose
3037	7	$3036^{7}6^{1}$	Bose				

$k \in K$ 的 α-平行类, 且存在一个 TD(u, α). 那么存在一个型如 $(\alpha g)^u$ 的 K-GDD, 其中有 $l\alpha^2$ 个区组大小为 k 的相异平行类.

这个构造说明, 利用一个合适的横截设计, 原本有相异 α-平行类的可分组设计能够被膨胀为一个组大小更大的可分组设计, 使得相异的 α-平行类导出相异的 1-平行类. 在以下的构造中, 我们也会利用以下的 Ree 构造的更精细的版本.

构造 4.9 (构造 4.2[234]): 令 $(X, \mathcal{G}, \mathcal{B})$ 为一个型为 g^u 的 $\{k_1, k_2\}$-GDD, 其中大小为 k_1 的区组可被划分为 l 个相异的 α-平行类. 对一个正整数 v, 假设存在一个 TD$(u, v\alpha)$ 包含一个自同构群 $\mathcal{H}$ 在横截设计每个组的点上的作用是传递的. 进一步假设 $\mathcal{H}$ 有一个阶为α 的子群 H. 那么存在一个型如 $(v\alpha g)^u$ 的 $\{k_1, k_2\}$-GDD, 其中大小为 k_1 的区组可被划分为 $lv\alpha^2$ 个相异平行类.

结合构造 4.7 和构造 4.8, 我们有以下定理.

定理 4.14: 令 $(X, \mathcal{G}, \mathcal{B})$ 为一个从构造 4.7 得到的可分组设计. 假设存在一个 TD$(bs, bs-1)$. 那么存在一个型为 $((bs-1)m)^{bs}((bs-1)^2)^1$ 的 $\{bs\}$-GDD .

证明. 将构造 4.8 应用于可分组设计 $(X, \mathcal{G}, \mathcal{B})$, 令 $g = m, u = bs, l = 1$ 且 $\alpha = bs - 1$, 我们有一个型如 $((bs-1)m)^{bs}$ 的 $\{bs-1, bs\}$-GDD 满足大小为 $bs-1$ 的区组形成 $(bs-1)^2$ 个 1-平行类. 那么, 我们用通常的方法得到一个型为 $((bs-1)m)^{bs}((bs-1)^2)^1$ 的 $\{bs\}$-GDD. □

类似地, 结合构造 4.7 和构造 4.9, 我们有以下的定理.

定理 4.15: 令 $(X, \mathcal{G}, \mathcal{B})$ 为一个从构造 4.7 得到的可分组设计. 对一个正整数 v, 假设存在一个 TD$(bs, v(bs-1))$ 包含一个自同构群 $\mathcal{H}$ 在横截设计每个组的点上的作用是传递的. 假设 $\mathcal{H}$ 有一个阶为 $bs-1$ 的子群 H. 那么存在一个型如 $((bs-1)vm)^{bs}(v(bs-1)^2)^1$ 的 $\{bs\}$-GDD.

4.2.6 利用 Rees 乘积构造的具体构造

在本小节中, 我们给出基于以上变形的几个具体构造, 其中 Rees 乘积构造起到了核心的作用. 为了利用 Rees 乘积构造, 我们首先需要考虑合适的横截设计的构造.

熟知, 一个横截设计等价于一个相互正交的拉丁方的集合(文献[1] 定理 3.18). 特别地, 我们有以下的结果.

引理 4.4 (定理 3.28[1]): 令 q 为一个素数幂. 那么存在一个 TD$(q+1,q)$.

考虑横截设计的另一个构造, 我们需要以下的结果.

引理 4.5: 令 q 为一个素数幂且 k 为一个整数满足 $k \leq q$. 那么存在一个 TD(k,q) 包含一个自同构群在横截设计每个组的点上的作用是传递的.

证明. 令 $A=(a_{ij}), 1 \leq i,j \leq q$, 为有限域 $\mathbb{F}_q$ 的乘法表. 令 A' 为 A 的前 k 行组成的子矩阵. 那么 $(a_{1j}, a_{2j}, \ldots, a_{kj})^T$ 是 A' 的第 j 列且我们定义

$$\mathcal{B}_j = \{\{(1, a_{1j}+g), (2, a_{2j}+g), \ldots, (k, a_{kj}+g)\}, g \in \mathbb{F}_q^+\},$$

对每个 $1 \leq j \leq q$. 令 $X = \{(i,x) \mid 1 \leq i \leq k, x \in \mathbb{F}_q^+\}$, $\mathcal{G} = \{\{(i,x) \mid x \in \mathbb{F}_q^+\} \mid 1 \leq i \leq k\}$ 且 $\mathcal{B} = \cup_{j=1}^{q} \mathcal{B}_j$. 容易验证 $(X, \mathcal{G}, \mathcal{B})$ 是一个 TD(k,q), 其中 $\mathbb{F}_q^+$ 在每个组的点上是传递的. □

我们利用 Rees 乘积构造给出一个型不一致可分组设计的具体构造.

定理 4.16: 令 q 为一个素数幂. 令 $ab = q'$ 其中 $q' \in \{q-1, q, q+1\}$. 假设存在某个正整数 $1 \leq s \leq a$, 使得 $bs-1$ 为一个素数幂, 例如, $bs-1 = p^t$. 那么存在一个型如 $((q-1)p^e)^{p^t+1}(p^{t+e})^1$ 的 $\{p^t+1\}$-GDD 对每个 $e \geq t$.

证明. 由推论 4.4, 存在一个型如 $(q-1)^{bs}$ 的 $\{bs-1, bs\}$-GDD, 其中大小为 $bs-1$ 的区组形成一个 $(bs-1)$-平行类.

对 $e=t$, 由于 $bs-1=p^t$ 是一个素数幂, 一个 TD(p^t+1, p^t) 由引理 4.4 存在. 利用定理 4.14, 存在一个型如 $((q-1)p^t)^{p^t+1}(p^{2t})^1$ 的 $\{p^t+1\}$-GDD.

对 $e \geq t+1$, 由引理 4.5, 存在一个 TD(p^t+1, p^e) 满足 $\mathbb{F}_{p^e}^+$ 在横截设计每个组的点上的作用是传递的. 注意到 $\mathbb{F}_{p^e}^+$ 有一个阶为 p^t 的子群. 在定理 4.15 中令 $v = p^{e-t}$ 导出一个型为 $((q-1)p^e)^{p^t+1}(p^{t+e})^1$ 的 $\{p^t+1\}$-GDD . □

由于参数 a, b, s 选择的灵活性, 以上定理可给出型不一致可分组设计的许多无穷类. 以下我们列举了一些.

推论 4.5：以下的可分组设计存在:

(1) 型如 $((2^n-1)7^e)^8(7^{e+1})^1$ 的 $\{8\}$-GDDs 其中 $n \geq 3$ 且 $e \geq 1$;

(2) 型如 $((5^n-1)7^e)^8(7^{e+1})^1$ 的 $\{8\}$-GDDs 其中 $n \geq 2$ 且 $e \geq 1$;

(3) 型如 $((q-1)2^e)^9(2^{e+3})^1$ 的 $\{9\}$-GDDs, 其中 q 素数幂满足 $q \geq 8$ 且 $e \geq 3$.

证明. 证明是定理 4.16 的直接应用. 对 (1), 取 $q = 2^n$, $a = 2^{n-2}$, $b = 4$ 和 $s = 2$. 对 (2), 取 $q = 5^n$, $a = \frac{5^n-1}{4}$, $b = 4$ 和 $s = 2$. 对 (3), 取 $b = 3$ 和 $s = 3$. □

4.2.7 总结

型不一致可分组设计的构造是一个非常具有挑战性的问题. 在本节中, 我们提出一个构造型如 $g^k m^1$ 的 $\{k\}$-GDDs 的新方法, 其中广义差集, 一个截断技巧和一个差方法起到了关键作用. 利用这个一般构造, 导出了型不一致的可分组设计的一个新的无穷类和许多新例子. 特别地, 这些具体构造依赖于和射影平面相关的广义差集和一个划分 α-平行类的差方法. 一般地, 将一个 α-平行类划分为 1-平行类是一个困难的问题. 为了避免这个问题, 我们提出了一个变形的构造, 利用了 Rees 乘积构造. 特别地, 几个型不一致可分组设计的无穷类可由这个变形得到. 我们指出这个新的构造是非常灵活的, 因为不同的广义差集和不同的划分 α-平行类的策略将导出许多不同的型不一致可分组设计.

5 循环码及其应用

5.1 $\mathrm{GF}(q)$ 上长为 $n=\frac{q^m-1}{q-1}$ 的狭义 BCH 码

5.1.1 引言

在本小节中, 令 q 为素数 p 的幂次. $\mathrm{GF}(q)$ 上一个线性 $[n,k,d]$ 码 $\mathcal{C}$ 是一个 $\mathrm{GF}(q)^n$ 的 k-维线性子空间, 其中极小汉明距离为 d. $\mathrm{GF}(q)$ 上长为 n 的线性码 $\mathcal{C}$ 被称为是循环的如果 $(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ 蕴含 $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in\mathcal{C}$. $\mathrm{GF}(q)$ 上的循环码也可被视为商环 $\mathrm{GF}(q)[x]/(x^n-1)$ 中的理想.

通过将向量 $(c_0,c_1,\cdots,c_{n-1})\in\mathrm{GF}(q)^n$ 与多项式

$$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in\mathrm{GF}(q)[x]/(x^n-1)$$

等同, 任意 $\mathrm{GF}(q)$ 上长为 n 的线性码 $\mathcal{C}$ 对应于商环 $\mathrm{GF}(q)[x]/(x^n-1)$ 的一个子集. 一个线性码 $\mathcal{C}$ 是循环的当且仅当 $\mathrm{GF}(q)[x]/(x^n-1)$ 中相应的子集是一个理想.

注意到 $\mathrm{GF}(q)[x]/(x^n-1)$ 的每个理想均是主理想. 令 $\mathcal{C}=\langle g(x)\rangle$ 为一个循环码, 其中 $g(x)$ 是首一的且在 $\mathcal{C}$ 的所有生成元中有最低次数. 那么 $g(x)$ 是唯一的且被称为**生成多项式** (generator polynomial), 且 $h(x)=(x^n-1)/g(x)$ **校验多项式** (parity-check polynomial). 在本节中, 我们仅考虑 $\mathrm{GF}(q)$ 上长为 n 的循环码, 其中 $\gcd(n,q)=1$, 这蕴含了码的生成多项式不含重根.

令 n 为一个正整数. 令 $m=\mathrm{ord}_n(q)$, 亦即, m 是最小的正整数满足 $n|q^m-1$. 令 α 为 $\mathrm{GF}(q^m)$ 的乘法群 $\mathrm{GF}(q^m)^*$ 的一个生成元, 记 $\beta=\alpha^{(q^m-1)/n}$. 那么 β 是 $\mathrm{GF}(q^m)$ 中一个本原 n-次单位根. 对任意 i 满足 $1\le i\le q^m-2$, 令 $m_i(x)$ 记 β^i 在 $\mathrm{GF}(q)$ 上的极小多项式. 对任意 $2\le\delta<n$, 定义

$$g_{(n,q,m,\delta)}(x)=\mathrm{lcm}(m_1(x),m_2(x),\cdots,m_{\delta-1}(x)),$$

其中 lcm 记这些多项式的最小公倍式. 此外, 我们定义

$$\tilde{g}_{(n,q,m,\delta)}(x) = (x-1)g_{(n,q,m,\delta)}(x).$$

令 $\mathcal{C}_{(n,q,m,\delta)}$ 且 $\tilde{\mathcal{C}}_{(n,q,m,\delta)}$ 为 $\mathrm{GF}(q)$ 上长为n 的循环码, 其中生成多项式分别为 $g_{(n,q,m,\delta)}(x)$ 和 $\tilde{g}_{(n,q,m,\delta)}(x)$. 那么 $\mathcal{C}_{(n,q,m,\delta)}$ 被称为一个*狭义 BCH 码* (narrow-sense BCH code), 其中*设计距离* (designed distance) 为 δ. $\tilde{\mathcal{C}}_{(n,q,m,\delta)}$ 是 $\mathcal{C}_{(n,q,m,\delta)}$ 的类偶 (even-like) 子码. 显然, 我们有

$$\dim(\tilde{\mathcal{C}}_{(n,q,m,\delta)}) = \dim(\mathcal{C}_{(n,q,m,\delta)}) - 1.$$

由定义, $g_{(n,q,m,\delta)}(x)$ 有 $\delta-1$ 个连续的根 β^i 对 $1 \le i \le \delta-1$, 且 $\tilde{g}_{(n,q,m,\delta)}(x)$ 有 δ 个连续的根 β^i 对 $0 \le i \le \delta-1$. 由 BCH 界可知 $\mathcal{C}_{(n,q,m,\delta)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta)}$ 的极小距离至少分别为 δ 和 $\delta+1$. 因此, δ 被称为 $\mathcal{C}_{(n,q,m,\delta)}$ 的设计距离.

熟知对两个不同的 δ 和 δ', 码 $\mathcal{C}_{(n,q,m,\delta)}$ 和 $\mathcal{C}_{(n,q,m,\delta')}$ 可能相同. 因此, 一个 BCH 码可能有许多不同的设计距离. $\mathcal{C}_{(n,q,m,\delta)}$ 的最大的设计距离被称为 Bose *距离* (Bose distance), 记做 d_B. 由定义, 一个 BCH 码的 Bose 距离可作为码的极小距离的一个下界. 因此当极小距离不能确定时, 考虑 Bose 距离是有意义的.

循环码 $\mathcal{C}_{(n,q,m,\delta)}$ 在每本关于编码理论的书中均有涉及. 当 $n = q^m - 1$, 码 $\mathcal{C}_{(n,q,m,\delta)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta)}$ 被称为*狭义本原 BCH 码* (narrow-sense primitive BCH codes), 已在很多文献中被研究过[3,9,10,17,50,51,77,94,171–173,200,201,227,299,300]. 特别地, 关于狭义本原 BCH 码的一个最近的总结, 可参见文献[94]. 当 $n = (q^m-1)/(q-1)$, 码 $\mathcal{C}_{(n,q,m,\delta)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta)}$ 被称为*狭义射影 BCH 码* (narrow-sense projective BCH codes), 当 $q > 2$ 时, 这类码在文献中没有研究过.

本小节将要研究几类特殊的狭义射影 BCH 码的参数. 包括分圆陪集, 定位多项式, 非减序列分解和有限域上和二次型相关的指数和在内的多种方法被利用来得到几类狭义射影 BCH 码的维数, Bose 距离, 极小距离和重量分布. 一类达到 Griesmer 界的三元 BCH 码被发掘了出来. 对本节考虑的一些 BCH 码一个应用也有讨论.

我们将会看到, 一些狭义射影 BCH 码有最优的参数. 为了研究一些码的最优性, 我们参考了由 Markus Grassl 维护的已知最优线性码的数据库 http://www.codetables.de, 在下文中被简称为*数据库*. 在一些情况下, 我们将利用专著[93] 中关于最优循环码的表作为标杆.

5.1.2 预备知识

在本小节中, 我们列举一些关于分圆陪集, 陪集代表元, 非减序列分解, 有限域上二次型和指数和的一些背景. 同时回顾了一些关于 BCH 码的已知结果.

5.1.2.1 分圆陪集

为了处理 GF(q) 上长为 n 的循环码, 我们需要研究 x^n-1 在 GF(q) 上的分解. 为此, 我们介绍模 n 的 q-分圆陪集.

回顾 $\mathbb{Z}_n$ 记模 n 的整数环. 令 s 为一个整数满足 $0 \le s < n$. s 模 n 的 q-分圆陪集 (q-cyclotomic coset of s modulo n) 定义为

$$C_s = \{s, sq, sq^2, \cdots, sq^{\ell_s-1}\} \bmod n \subseteq \mathbb{Z}_n,$$

其中 ℓ_s 是最小的正整数满足 $s \equiv sq^{\ell_s} \pmod n$, 与 q-分圆陪集 C_s 的大小相等. C_s 中最小的非负整数被称为 C_s 的陪集代表元 (coset leader). 令 $\Gamma_{(n,q)}$ 为所有陪集代表元组成的集合. 我们有 $C_s \cap C_t = \emptyset$ 对任意两个相异的 s 和 t 属于 $\Gamma_{(n,q)}$, 并且

$$\bigcup_{s\in\Gamma_{(n,q)}} C_s = \mathbb{Z}_n. \tag{5.1}$$

亦即, 模 n 的 q-分圆陪集形成 $\mathbb{Z}_n$ 的一个划分.

令 $m = \mathrm{ord}_n(q)$, 令 α 为 GF$(q^m)^*$ 的一个生成元. 记 $\beta = \alpha^{(q^m-1)/n}$. 那么 β 是 GF(q^m) 中一个本原 n-次单位根. $m_s(x)$ 是 β^s 在 GF(q) 上的极小多项式. 易知

$$m_s(x) = \prod_{i\in C_s}(x-\beta^i) \in \mathrm{GF}(q)[x], \tag{5.2}$$

它在 GF(q) 是不可约的. 由 (5.1) 可知

$$x^n - 1 = \prod_{s\in\Gamma_{(n,q)}} m_s(x), \tag{5.3}$$

亦即 x^n-1 分解为 GF(q) 上的不可约因子. 因而, 对任意循环码

$$\mathcal{C}=\langle g(x)\rangle \subset \mathrm{GF}(q)[x]/(x^n-1),$$

生成多项式 $g(x)$ 为若干 $m_s(x)$ 的乘积. 因此, $g(x)$ 的次数和 $\mathcal{C}$ 的维数由和 $g(x)$ 相关的分圆陪集的大小决定.

以下, 我们列举一些关于分圆陪集的有用结果. 对于分圆陪集的大小, 我们有以下引理.

引理 5.1 (定理 4.1.4[151]): 每个 q-分圆陪集 $\mathcal{C}_s$ 的大小 ℓ_s 是 ord$_n(q)$ 的一个因子. ord$_n(q)$ 等于 C_1 的大小 ℓ_1.

以下引理说明当 s 小时, q-分圆陪集 $\mathcal{C}_s \subset \mathbb{Z}_n$ 的大小总是等于 ord$_n(q)$.

引理 5.2 (引理 8[3]): 令 n 为一个正整数使得 $\gcd(n,q)=1$ 且 $q^{\lfloor m/2\rfloor}<n\le q^m-1$, 其中 $m=\mathrm{ord}_n(q)$. q-分圆陪集 C_s 大小为 m, 其中 s 属于 $1\le s\le nq^{\lceil m/2\rceil}/(q^m-1)$.

作为一个直接的结果, 我们可知一些 BCH 码的维数.

定理 5.1 (定理 10[3]): 令 n 为一个正整数使得 $\gcd(n,q)=1$ 且 $q^{\lfloor m/2\rfloor}<n\le q^m-1$, 其中 $m=\mathrm{ord}_n(q)$. 那么长为 n 且设计距离 δ 属于$2\le\delta\le\min\{\lfloor nq^{\lceil m/2\rceil}/(q^m-1)\rfloor, n\}$ 的狭义 BCH 码的维数为

$$k=n-m\lceil(\delta-1)(1-1/q)\rceil.$$

5.1.2.2 非减序列分解和陪集代表元

熟知 GF(q) 上长为 n 的一个狭义 BCH 码的 Bose 距离一定是 $\mathbb{Z}_n$ 中 q-分圆陪集的一个代表元. 当 $n=q^m-1$, 已有一些关于 q-分圆陪集的结果[94,200,299]. 特别地, 在文献[299] 提出了非减序列分解的概念, 讨论了它和模 q^m-1 的陪集代表元的密切联系. 在本小节中, 我们说明这个概念对确定某些特殊的模 $\frac{q^m-1}{q-1}$ 的 q-分圆陪集代表元也有帮助. 此处我们总假设 $q>2$ 是一个素数幂.

假设 $\underline{v}=(v_{n-1},v_{n-2},\ldots,v_0)$ 是一个长为 n 的序列, 每个分量 v_i 满足 $0\le v_i\le q-1$. 序列 $\underline{v}$ 被称为一个非减序列 (nondecreasing sequence) 如果 $v_{i+1}\le v_i$ 对 $0\le i\le n-1$. 任何序列有一个唯一的非减序列分解 (nondecreasing sequence decomposition) 形如

$\underline{V_1V_2}\dots\underline{V_r}$ 其中 $\underline{V_i}$ 是非减序列且 r 是最小的. 令 $\underline{v}=(v_{l-1},\dots,v_0)$ 且 $\underline{w}=(u_{k-1},\dots,u_0)$ 为两个非减序列. 我们说 $\underline{v}=\underline{w}$ 如果 $l=k$ 且 $v_{l-1-i}=w_{l-1-i}$ 对任意 $0\le i\le l-1$. 我们说 $\underline{v}>\underline{w}$, 如果 $l>k$ 且 $v_{l-1-i}=w_{k-1-i}$ 对 $0\le i\le k-1$ 或存在一个整数 $0\le j\le \min\{l,k\}-1$ 使得 $v_{l-1-j}>w_{k-1-j}$ 且 $v_{l-1-i}=w_{k-1-i}$ 对 $0\le i\le j-1$. 对两个长度相同且具有非减序列分解 $\underline{v}=\underline{V_1V_2}\dots\underline{V_r}$ 和 $\underline{w}=\underline{W_1W_2}\dots\underline{W_s}$ 的序列, 我们说 $\underline{v}=\underline{w}$ 如果 $\underline{v}$ 和 $\underline{w}$ 相同. 我们说 $\underline{v}>\underline{w}$ 如果存在一个整数 $0\le j\le \min\{r,s\}-1$ 使得 $\underline{V_{r-1-j}}>\underline{W_{s-1-j}}$ 且 $\underline{V_{r-1-i}}=\underline{W_{s-1-i}}$ 对 $0\le i\le j-1$. 我们指出以上的符号 "$\underline{v}>\underline{w}$" 与相应整数的排序 $\sum_i v_iq^i>\sum_i w_iq^i$ 是一致的.

给定一个正整数 s, 我们假设 $0<s<n$. 假设 s 唯一的 q-元分解是 $\sum_{i=0}^{m-1}s_iq^i$, 其中 $0\le s_i\le q-1$. 这定义了序列 $\overline{s}=(s_{m-1},s_{m-2},\dots,s_0)$. 用 $E(s)$ 记 $\overline{s}$ 的非减序列分解. 相反, 令 $\underline{V_1V_2}\dots\underline{V_r}$ 为 $\overline{s}$ 的非减序列分解. 那么定义

$$E^{-1}(\underline{V_1V_2}\dots\underline{V_r})=s.$$

C_s 模 n 的陪集代表元记做 s^*.

当 $n=q^m-1$ 且 $\overline{s}=(s_{m-1},s_{m-2},\dots,s_0)$, 注意到 $\overline{n}=(q-1,q-1,\cdots,q-1)$, $\overline{q^is}$ 是对应于 $q^is \bmod n$ 的序列

$$\overline{q^is}=(s_{m-1-i},\dots,s_0,s_{m-1},\dots,s_{m-i}),\ 1\le i\le m-1. \tag{5.4}$$

亦即, 当 $n=q^m-1$, 乘以 q 的一个幂次对应于 $\overline{s}$ 的一个循环移位. 这个关键的事实是[299] 中重要结果的基础. 当 $n=\frac{q^m-1}{q-1}$, 情况更加复杂. 虽然 (5.4) 仍然成立, 但当 $\overline{q^is}>\overline{n}$, 注意到 $\overline{n}=(1,1,\dots,1)$, 我们需要在 $\overline{q^is}$ 中减去 $(1,1,\dots,1)$ 的某个倍数, 使得最终的序列落在 $\overline{0}$ 和 $\overline{n}$ 之间. 根据这个观察, 我们可以容易的将文献[299] 中某些结果翻译到 $n=\frac{q^m-1}{q-1}$ 的情况中. 以下, 我们总是考虑 q-分圆陪集模 $n=\frac{q^m-1}{q-1}$.

引理 5.3: 令 $0\le s\le \frac{q^m-1}{q-1}-1$ 是一个整数满足 $\overline{s}$ 的分量为 0 或 1. 假设 $E(s)=\underline{V_1V_2}\dots\underline{V_r}$. 我们有以下结果.

i) $E(s^*)=\underline{V_jV_{j+1}}\dots\underline{V_rV_1}\dots\underline{V_{j-1}}$ 对某个 j 其中 $\underline{V_j}\le\underline{V_i}$ 对每个 $1\le i\le r$.

ii) 如果 $\underline{V_1}=\underline{V_2}=\cdots=\underline{V_r}$ 或 $\underline{V_1}=\underline{V_2}=\cdots=\underline{V_j}<\underline{V_k}$ 对所有 $k>j$, 那么 $s=s^*$.

iii) 如果 $r = 1$, 那么 $s = s^*$.

证明. 由于 $\overline{n} = (1, 1, \cdots, 1)$ 且 $\overline{s}$ 的分量为 0 或 1, $\overline{q^i s}$ 的分量同样为 0 或 1. 因而 $0 < \overline{q^i s} < \overline{n}$ 对任意 i. 因而从 $\overline{q^i s}$ 中减去 $\overline{n}$ 某个倍数的情况不会发生. 证明与定理 2.2[299] 中关于 $n = q^m - 1$ 的证明完全类似. □

令 $\underline{v} = (v_{l-1}, v_{l-2}, \ldots, v_0)$ 为一个非减序列. 定义截断操作 (truncating operator) T_k 为

$$T_k(\underline{v}) = (v_{l-1}, v_{l-2}, \ldots, v_{l-k}),\ 1 \leq k \leq l.$$

我们定义后继操作 (successor operator) S 使得 $S(\underline{v})$ 是大于 $\underline{v}$ 的最小的非减序列. 特别地, 如果$v_0 < q - 1$, 我们有

$$S(\underline{v}) = (v_{l-1}, v_{l-2}, \ldots, v_0 + 1),$$

对应于整数 $\sum_{i=0}^{l-1} v_i q^i$ 的后继. 以下引理考虑了在一个特殊情况下考虑了模 $\frac{q^m-1}{q-1}$ 的陪集代表元.

引理 5.4: 令 $0 \leq s \leq \frac{q^m-1}{q-1} - 1$ 为一个整数. 假设 $E(s) = \underline{V_1 V_2} \ldots \underline{V_r}$, 其中 $\underline{V_1} > \underline{V_2}$. 假设 $\underline{V_1}$ 有长度 l 且分量为 0 或 1. 令 $M(s)$ 为最小的大于或等于 s 的陪集代表元. 记 $m = al + b$, 其中 $0 \leq b \leq l - 1$. 如果 $b = 0$, 我们有

$$M(s) = E^{-1}(\underbrace{\underline{V_1 V_1} \ldots \underline{V_1}}_{a}).$$

如果 $1 \leq b \leq l - 1$, 我们有

$$M(s) \geq E^{-1}(\underbrace{\underline{V_1 V_1} \ldots \underline{V_1}}_{a} S(T_b(\underline{V_1}))).$$

特别地, 如果 $S(T_b(\underline{V_1}))$ 的最后一个分量为 1, 那么以上的式子等号成立.

证明. 证明与定理 2.5[299] 对 $n = q^m - 1$ 的证明相同, 因为不涉及从 $\overline{q^i s}$ 减去 $(1, 1, \ldots, 1)$ 的情况. □

5.1.2.3 与二次型相关的高斯和与指数和

在本小节中, 我们回顾一些与有限域上的二次型相关的高斯和与指数和的结果. 此处, 我们列出两个之后要用到的引理.

定义 5.1: 令 χ 为 $\mathrm{GF}(q)$ 上一个乘法特征且 Tr 为从 $\mathrm{GF}(q)$ 到 $\mathrm{GF}(p)$ 的迹函数. 高斯和 $G(\chi)$ 定义做

$$G(\chi)=\sum_{x\in \mathrm{GF}(q)} \chi(x)\zeta_p^{\mathrm{Tr}(x)},$$

其中 $\zeta_p := \exp(2\pi\sqrt{-1}/p)$ 是一个 p-次复单位根.

引理 5.5 (**定理** 5.15[190]): 令 $q=p^s$ 且 η 为 $\mathrm{GF}(q)$ 的二次特征 (因此p 为奇数). 那么二次高斯和满足

$$G(\eta)=\begin{cases}(-1)^{s-1}\sqrt{q} & \text{如果 } p\equiv 1 \bmod 4,\\ (-1)^{s-1}(\sqrt{-1})^s\sqrt{q} & \text{如果 } p\equiv 3 \bmod 4.\end{cases}$$

如果 η 是 $\mathrm{GF}(q)$ 的二次特征且 $G(\eta)$ 是二次高斯和, 以下的等式成立:

$$\sum_{x\in \mathrm{GF}(q)^*} \zeta_p^{\mathrm{Tr}(ax^2)}=\frac{\eta(a)G(\eta)-1}{2},\quad \forall\, a\in \mathrm{GF}(q)^*. \tag{5.5}$$

引理 5.6 (**引理** 1[193]): 令 q 为一个奇素数幂且 $Q(x)$ 为一个从 $\mathrm{GF}(q^m)$ 到 $\mathrm{GF}(q)$ 的二次型, 秩为 r. 那么

$$\sum_{x\in \mathrm{GF}(q^m)} \zeta_p^{\mathrm{Tr}_p^{q^m}(Q(x))}=\begin{cases}\pm q^{m-r/2} & \text{如果 } q\equiv 1 \bmod 4,\\ \pm(\sqrt{-1})^r q^{m-r/2} & \text{如果 } q\equiv 3 \bmod 4.\end{cases}$$

5.1.2.4 BCH 码的一些已知结果

我们首先回顾一个向量的定位多项式的定义. 定位多项式在 BCH 码的研究中非常有用[9,10].

定义 5.2: 令 $c=(c_0,c_1,\ldots,c_{n-1})\in \mathrm{GF}(q)^n$ 为一个向量有非零的分量 $c_{i_1},c_{i_2},\ldots,c_{i_w}$.

那么

$$X_1 = \beta^{i_1}, \ldots, X_w = \beta^{i_w}$$

被称为 c 的定位子 (locators). c 的定位多项式 (locator polynomial) 为

$$\sigma(z) = \prod_{i=1}^{w}(1 - X_i z) = \sum_{i=0}^{w} \sigma_i z^i,$$

其中 $\sigma_0 = 1$. 系数 σ_i 关于 X_i 的初等对称多项式:

$$\begin{aligned}
\sigma_1 &= -(X_1 + \cdots + X_w), \\
\sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_{w-1}X_w, \\
&\vdots \\
\sigma_w &= (-1)^w X_1 \cdots X_w.
\end{aligned}$$

以下引理描述了 $\mathrm{GF}(q^m)$ 上一个多项式是 BCH 码中一个码字的定位多项式的条件. 事实上, 这个引理包含了寻找 BCH 码中一个具有给定重量的码字的方式, 其中利用了定位多项式.

引理 5.7 (第 9 章, 引理 4[198]): 令

$$\sigma(z) = \sum_{i=0}^{w} \sigma_i z^i$$

为 $\mathrm{GF}(q^m)$ 上一个多项式. 那么 $\sigma(z)$ 是只有 0 和 1 分量的属于 $\mathcal{C}_{(n,q,m,\delta)}$ 的码字 c 的定位多项式当且仅当以下两个条件成立.

i) $\sigma(z)$ 的零点是相异的 n-次单位根.

ii) $\sigma_i = 0$ 对所有 $1 \le i \le \delta - 1$ 满足 $p \nmid i$, 其中 p 是 $\mathrm{GF}(q)$ 的特征.

以下引理说明在某些情况下, 极小距离等于设计距离.

引理 5.8 (定理 4.3.13[18]): 对一个 BCH 码 $\mathcal{C}_{(n,q,m,\delta)}$, 如果 $\delta \mid n$, 那么极小距离 $d = \delta$.

5.1.3 大维数狭义射影 BCH 码

此后, 我们总假设 $n = \frac{q^m-1}{q-1}$. 因而, 我们有 $\mathrm{ord}_n(q) = m$. 我们用 α 记 $\mathrm{GF}(q^m)$ 的一个本原元且 $\beta = \alpha^{q-1}$. $\mathcal{C}_{(q,m,\delta)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta)}$ 分别为狭义射影 BCH 码 $\mathcal{C}_{(\frac{q^m-1}{q-1},q,m,\delta)}$ 和 $\tilde{\mathcal{C}}_{(\frac{q^m-1}{q-1},q,m,\delta)}$. 本小节中, 我们考虑有少数几个零点的, 亦即维数较大的狭义射影 BCH 码.

设计距离为 2 的狭义射影 BCH 码仅有一个零点, 码的参数是已知的.

定理 5.2: *码 $\mathcal{C}_{(n,q,m,2)}$ 有参数 $[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, d]$, 其中*

$$d = \begin{cases} 3 & \text{如果 } \gcd(m, q-1) = 1, \\ 2 & \text{如果 } \gcd(m, q-1) \neq 1. \end{cases}$$

证明. 维数由 $|C_1| = m$ 易知. 由于 $\mathcal{C}_{(n,q,m,2)}$ 仅有一个零点 β, 它的校验矩阵为

$$H = (1, \beta, \ldots, \beta^{n-1}),$$

其中第 i-列是 $\mathrm{GF}(q)^m$ 中对应于 β^{i-1} 的向量. 当 $\gcd(n, q-1) = \gcd(m, q-1) = 1$, 易知 H 的任意两列是线性无关的. 因此, 码 $\mathcal{C}_{(n,q,m,2)}$ 是汉明码且 $d = 3$. 当 $\gcd(m, q-1) \neq 1$, 我们可以找到 H 的线性相关的两列, 蕴含了 $d = 2$. □

定理 5.3: *码 $\tilde{\mathcal{C}}_{(n,q,m,2)}$ 有参数 $[(q^m-1)/(q-1), (q^m-1)/(q-1)-m-1, d]$, 其中 $d \in \{3, 4\}$.*

证明. $\tilde{\mathcal{C}}_{(n,q,m,2)}$ 是 $\mathcal{C}_{(n,q,m,2)}$ 的类偶子码, 维数为 $(q^m-1)/(q-1)-m-1$. 极小距离 $2 \leq d \leq 4$, 其中下界由 BCH 界得出, 上界由球填充界导出. 注意到校验矩阵

$$\widetilde{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ & & H & & \end{pmatrix},$$

其中 H 是定理 5.2 中码 $\mathcal{C}_{(n,q,m,2)}$ 的校验矩阵. 易知 $\widetilde{H}$ 的秩大于 2. 因此, 我们有 $d \in \{3, 4\}$. □

对于设计距离为 3 的狭义射影 BCH 码, 参数在以下情形可以确定.

定理 5.4: 令 $q \geq 3$. 码 $\mathcal{C}_{(n,q,m,3)}$ 有参数 $[(q^m-1)/(q-1), (q^m-1)/(q-1)-2m, d]$, 其中 $d = 3$ 在以下情况:

i) $q \equiv 1 \mod 3$ 且 $3 \mid m$,

ii) $q \equiv 2 \mod 3$ 且 $2 \mid m$,

且 $d \leq 4$ 在以下情况:

iii) $q \equiv 1 \mod 4$ 且 $4 \mid m$,

iv) $q \equiv 3 \mod 4$ 且 $2 \mid m$.

特别地, 如果 $q = 3$ 且 $2 \mid m$, 我们有 $d = 4$.

证明. 维数由 $|C_1| = |C_2| = m$ 得出. 对于极小距离, 我们仅证明 $d \leq 4$. $d = 3$ 的情形是类似的. 为了证明 $d \leq 4$, 我们将要找到一个码字 $c \in \mathcal{C}_{(n,q,m,3)}$ 有重量 4. 由引理 5.7, 只需找到 c 的一个定位多项式 $\sigma(z) = \sum_{i=0}^{4} \sigma_i z^i$, 其中 $\sigma(z)$ 的所有根属于循环群 $\langle\beta\rangle$ 且 $\sigma_1 = \sigma_2 = 0$. 由定义 5.2, 亦即寻找 $X_1, X_2, X_3, X_4 \in \langle\beta\rangle$, 满足

$$\begin{cases} X_1 + X_2 + X_3 + X_4 = 0, \\ X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 = 0. \end{cases}$$

iii) 或 iv) 蕴含 $4 \mid \frac{q^m-1}{q-1}$ 且 $-1 \in \langle\beta\rangle$. 因此, 我们可以选取 $X_1 = 1, X_2 = -1, X_3 = \beta^{\frac{q^m-1}{4(q-1)}}, X_4 = -\beta^{\frac{q^m-1}{4(q-1)}}$, 满足 $X_1, X_2, X_3, X_4 \in \langle\beta\rangle$ 且以上两式成立. 亦即, 我们找到一个码字 $c \in \mathcal{C}_{(n,q,m,3)}$ 有重量 4, 分量为 0 或 1. 因此, 我们有 $d \leq 4$.

特别地, 如果 $q = 3$, 我们有 $3 \in C_1$, 蕴含了 Bose 距离 $d_B \geq 4$. 另一方面, 当 $q = 3$ 且 $2 \mid m$, 我们有 $d \leq 4$. 注意到 $4 \geq d \geq d_B \geq 4$, 我们有 $d = 4$. □

令 $q \geq 3$. 对 $\mathcal{C}_{(n,q,m,3)}$ 的极小距离, 数值实验说明 $d = 4$ 当 $q = 3$, $d \in \{3, 4\}$ 当 $q > 3$. 理论上, BCH 界和球填充界蕴含 $4 \leq d \leq 6$ 当 $q = 3$ 且 $3 \leq d \leq 6$ 当 $q > 3$. 如定理 5.4 所示, 我们可以利用定位多项式在某些情况下排除 $d \in \{5, 6\}$ 的可能. 然而, 我们不确定这个技巧是否可用于其它剩下的情形, 因为这个方法只能找到分量为 0 或 1 的码字.

5.1.4 小维数狭义射影 BCH 码

本小节, 我们研究小维数狭义射影 BCH 码. 我们的任务是找到模 $n = (q^m - 1)/(q-1)$ 的前几个最大的陪集代表元. 注意到狭义射影 BCH 码的 Bose 距离是一个陪集代表元. 这些陪集代表元的知识给出了狭义射影 BCH 码的 Bose 距离和维数, 其中这些狭义射影 BCH 码的零点包括了 $x^n - 1$ 的所有的根除了几个最大的陪集代表元. 我们记最大 (或次大) 模 n 的陪集代表元为 δ_1 (或 δ_2). 对所有 $q > 2$ 确定 δ_1 和 δ_2 似乎是一个困难的问题. 本小节余下的部分, 我们假设 $q = 3$ 且只研究 $q = 3$ 的情形.

5.1.4.1 两个陪集代表元 δ_1 和 δ_2

引理 5.9: 令 $q = 3$ 和 $m \geq 2$. 最大的陪集代表元模 $n = (q^m - 1)/(q-1)$ 是

$$\delta_1 = q^{m-1} - 1 - \frac{q^{\lfloor (m-1)/2 \rfloor} - 1}{q-1}$$

和

$$|C_{\delta_1}| = \begin{cases} m & \text{如果 } m \text{ is odd,} \\ \frac{m}{2} & \text{如果 } m \text{ is even.} \end{cases}$$

次大的陪集代表元模 n 是

$$\delta_2 = q^{m-1} - 1 - \frac{q^{\lfloor (m+1)/2 \rfloor} - 1}{q-1}$$

且 $|C_{\delta_2}| = m$.

证明. 当 $m \in \{2, 3\}$, 结论可容易直接验证. 以下, 我们考虑 $m \geq 4$. 假设 $0 < \delta < n$ 是一个形如 $\overline{\delta} = (a_{m-1}, a_{m-2}, \ldots, a_0)$ 的陪集代表元. 我们首先指出 $a_{m-1} = 0$. 若不然, 由于 $\delta < n$, 我们有 $a_{m-1} = 1$ 且有一个分量 a_i 满足 $a_i = 0$. 我们可以去一个循环移位 $\overline{q^j \delta}$ 对某个 j (见 (5.4)) 使得 $a_i = 0$ 为第一个分量, 因而 $\overline{q^j \delta} < \overline{\delta}$, 与 δ 是一个陪集代表元矛盾.

我们假设陪集代表元 δ 形如 $\overline{\delta} = (0, 2, a_{m-3}, \ldots, a_0)$. 与之前同样的论证, 00 和 01 不能出现在 $\overline{\delta}$ 中. 此外, 如果 12 出现, 取一个合适的循环移位, 我们有 $\overline{q^j \delta} =$

$(1,2,\ldots,0,2,\ldots)$ 对某个 j. 易知

$$0<\overline{q^j\delta}-\overline{n}=(1,2,\ldots,0,2,\ldots)-(1,1,\ldots,1)=(0,b_{m-1},\ldots,b_0)=\overline{v},$$

其中 $0\le b_{m-1}\le 1$, 因此 $\overline{v}<\overline{\delta}$, 与 δ 是一个陪集代表元矛盾. 因此 12 不出现在 $\overline{\delta}$ 中.

再次, 令

$$\overline{\delta}=(0,\underbrace{2,\ldots,2}_{u},\underbrace{1,\ldots,1}_{v}), \tag{5.6}$$

其中 $u+v+1=m$. 我们可以验证相应于 $q^i\delta \bmod n$ 的序列为

$$\begin{aligned}
\overline{q\delta}&=(\underbrace{1,\ldots,1}_{u-1},0,\underbrace{2,\ldots,2}_{v+1}),\\
\overline{q^i\delta}&=(\underbrace{1,\ldots,1}_{u-i},0,\underbrace{2,\ldots,2}_{v+1},\underbrace{1,\ldots,1}_{i-1}),\ 2\le i\le u-1,\\
\overline{q^u\delta}&=(0,\underbrace{2,\ldots,2}_{v+1},\underbrace{1,\ldots,1}_{u-1}),\\
\overline{q^{u+1}\delta}&=(\underbrace{1,\ldots,1}_{v},0,\underbrace{2,\ldots,2}_{u}),\\
\overline{q^{u+1+i}\delta}&=(\underbrace{1,\ldots,1}_{v-i},0,\underbrace{2,\ldots,2}_{u},\underbrace{1,\ldots,1}_{i}),\ 1\le i\le v-1.
\end{aligned}$$

因此, 形如 (5.6) 的 δ 是一个陪集代表元模 n 当且仅当 $u\le v+1$, 亦即, $u\le\frac{m}{2}$.

最后, 令 δ 为一个形如 $\overline{\delta}=(0,2,a_{m-3},\ldots,a_0)$ 的陪集代表系且没有 (5.6) 的形式. 由我们所证明的, $\overline{\delta}$ 必须形如

$$\overline{\delta}=(0,\underbrace{2,\ldots,2}_{u_1},\underbrace{1,\ldots,1}_{v_1},0,\underbrace{2,\ldots,2}_{u_2},\underbrace{1,\ldots,1}_{v_2},\ldots,0,\underbrace{2,\ldots,2}_{u_t},\underbrace{1,\ldots,1}_{v_t}),$$

其中 $t\ge 2$ 且 $u_1\le u_i$ 对所有 $2\le i\le u$. 特别地, 我们有 $u_1\le u_2$ 且 $u_1+u_2+2\le m$, 蕴含了 $u_1\le\frac{m}{2}-1$.

由以上论证, 易知最大的两个陪集代表元为 δ_1 和 δ_2 为:

$$\text{当 } m \geq 4 \text{ 为偶数: } \overline{\delta_1} = (0, \underbrace{2, \ldots, 2}_{\frac{m}{2}}, \underbrace{1, \ldots, 1}_{\frac{m}{2}-1}),\ \overline{\delta_2} = (0, \underbrace{2, \ldots, 2}_{\frac{m}{2}-1}, \underbrace{1, \ldots, 1}_{\frac{m}{2}}).$$

$$\text{当 } m \geq 4 \text{ 为奇数: } \overline{\delta_1} = (0, \underbrace{2, \ldots, 2}_{\frac{m-1}{2}}, \underbrace{1, \ldots, 1}_{\frac{m-1}{2}}),\ \overline{\delta_2} = (0, \underbrace{2, \ldots, 2}_{\frac{m-3}{2}}, \underbrace{1, \ldots, 1}_{\frac{m+1}{2}}).$$

易知它对应于

$$\delta_1 = q^{m-1} - 1 - \frac{q^{\lfloor (m-1)/2 \rfloor} - 1}{q-1}.$$

由于 $q^{\frac{m}{2}}\delta_1 \equiv \delta_1 \pmod{n}$ 当 m 为偶数. 我们有

$$|C_{\delta_1}| = \begin{cases} m & \text{如果 } m \text{ 是奇数,} \\ \frac{m}{2} & \text{如果 } m \text{ 是偶数.} \end{cases}$$

容易验证

$$\delta_2 = q^{m-1} - 1 - \frac{q^{\lfloor (m+1)/2 \rfloor} - 1}{q-1}.$$

也可证明 $|C_{\delta_2}| = m$. □

5.1.4.2 其它陪集代表元 δ_i

回顾 $q = 3$. 令 δ_i 为第 i 大的陪集代表元模 $n = (q^m - 1)/(q-1)$. 在本子节中, 我们指出在 $q = 3$ 的情形某些陪集代表元 δ_i 也可以被决定.

令 δ 为一个形如

$$\overline{\delta} = (0, \underbrace{2, \ldots, 2}_{u_1}, \underbrace{1, \ldots, 1}_{v_1}, \ldots, 0, \underbrace{2, \ldots, 2}_{u_t}, \underbrace{1, \ldots, 1}_{v_t}).$$

的陪集代表元, 其中 $\sum_{i=1}^{t}(u_i + v_i + 1) = m$. 此外,

$$\overline{q\delta} = (\underbrace{1, \ldots, 1}_{u_1-1}, 0, \underbrace{2, \ldots, 2}_{v_1+1}, \ldots, \underbrace{1, \ldots, 1}_{u_t-1}, 0, \underbrace{2, \ldots, 2}_{v_t+1}).$$

显然, δ 是一个陪集代表元仅当 $u_1 \leq u_2 \leq \cdots \leq u_t$ 且 $u_1 \leq v_i + 1$ 对任意 $1 \leq i \leq t$. 特别地, 如果 $t \geq 2$, 那么 $u_1 + v_1 + u_2 + v_2 + 2 \leq m$ 蕴含了 $u_1 \leq \frac{m}{4}$. 因此, 对 $1 \leq i \leq \lfloor \frac{m}{4} \rfloor$,

δ_i 形如

$$\overline{\delta_i} = (0, \underbrace{2, \ldots, 2}_{\lceil \frac{m+1}{2} \rceil - i}, \underbrace{1, \ldots, 1}_{m-1-\lceil \frac{m+1}{2} \rceil + i}).$$

因而

$$\delta_i = q^{m-1} - 1 - \frac{q^{\lfloor \frac{m-3}{2} + i \rfloor} - 1}{q-1}, \quad 1 \le i \le \lfloor \frac{m}{4} \rfloor.$$

我们可知 $q = 3$ 起到了重要作用, 因为乘以 3 的幂次之后的结果是可预料的. 然而, 对 $q > 3$, 我们没有得到类似的结果.

5.1.4.3 三元码 $\mathcal{C}_{(n,q,m,\delta_1)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$

现在我们研究三元码 $\mathcal{C}_{(n,q,m,\delta_1)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$. 再次回顾 $q = 3$.

定理 5.5: 令 $m \ge 3$ 且 $q = 3$. 那么三元码 $\mathcal{C}_{(n,q,m,\delta_1)}$ 有参数

$$\left[\frac{q^m - 1}{q-1}, \, k, \, \delta_1 \right],$$

其中

$$k = \begin{cases} m+1 & \text{如果 } m \text{ 是奇数}, \\ \frac{m+2}{2} & \text{如果 } m \text{ 是偶数}. \end{cases}$$

此外, $\mathcal{C}_{(n,q,m,\delta_1)}$ 是一个三重码如果 $m \ge 4$ 是偶数, 是一个四重码如果 $m \ge 3$ 是奇数. $\mathcal{C}_{(n,q,m,\delta_1)}$ 的重量分布列在表 5.1 和表 5.2.

证明. 我们仅考虑 $m \ge 3$ 是奇数的情况. $m \ge 4$ 是偶数的情况可以类似地处理. 由引理 5.9 可知码的维数. 注意到 $\frac{3^m-1}{2} - \delta_1 = \frac{3^{m-1}+3^{\frac{m-1}{2}}}{2}$. 由 Delsarte 定理[72],

$$\mathcal{C}_{(n,q,m,\delta_1)} = \{\tilde{c}(a,b) : a \in \mathrm{GF}(3^m), \, b \in \mathrm{GF}(3)\},$$

其中

$$\tilde{c}(a,b) = \left(\mathrm{Tr}_3^{3^m} \left(a\alpha^{j(3^{m-1}+3^{\frac{m-1}{2}})} \right) + b \right)_{j=0}^{n-1}.$$

此处 α 是 $\mathrm{GF}(3^m)^*$ 的一个生成元. 由于 $\gcd(3^{m-1} + 3^{\frac{m-1}{2}}, 3^m - 1) = 2$, 只需研究以下

码的重量分布

$$c(a,b)=\left(\mathrm{Tr}_3^{3^m}\left(a\alpha^{2j}\right)+b\right)_{j=0}^{n-1},\quad a\in \mathrm{GF}(3^m),\ b\in \mathrm{GF}(3). \tag{5.7}$$

码 (5.7) 的重量分布应该在文献中是已知的. 然而, 为了解释我们接下来将要用到的方法, 我们给出详细的计算.

如果 $a=0$ 且 $b\neq 0$, 易知 $w(c(a,b))$ 取 $\frac{3^m-1}{2}$ 共 2 次. 如果 $a\neq 0$, 一个常规的计算 (见文献[193]) 表明汉明重量

$$\begin{aligned} w(c(a,b)) &= n-\sum_{j=0}^{n-1}\frac{1}{3}\sum_{x\in \mathrm{GF}(3)}\zeta_3^{x\left(\mathrm{Tr}_3^{3^m}(a\alpha^{2j})+b\right)} \\ &= \frac{2}{3}n-\frac{1}{6}\sum_{x\in \mathrm{GF}(3)^*}\zeta_3^{bx}\sum_{y\in \mathrm{GF}(2^{2m})^*}\zeta_3^{\mathrm{Tr}_3^{3^m}(axy^2)}. \end{aligned}$$

此处 $\zeta_3=\frac{-1+\sqrt{-3}}{2}$ 是 3-次复单位根. 由 (5.5) 可得

$$\begin{aligned} w(c(a,b)) &= \frac{2}{3}n-\frac{1}{6}\sum_{x\in \mathrm{GF}(3)^*}\zeta_3^{bx}(\eta(ax)G(\eta)-1) \\ &= \frac{2}{3}n-\frac{1}{6}\eta(a)G(\eta)\left(\zeta_3^b+\eta(-1)\zeta_3^{-b}\right)+\frac{1}{6}\left(\zeta_3^b+\zeta_3^{-b}\right), \end{aligned}$$

其中 η 是二次特征且 $G(\eta)$ 是 $\mathrm{GF}(2^{2m})$ 上二次高斯和.

由于 m 是奇数, $\eta(-1)=-1$. 由引理 5.5, 可知如果 $a\neq 0$ 且 $b=0$, $w(c(a,b))$ 取值 3^{m-1} 共 3^m-1 次, 如果 $a,b\neq 0$, $w(c(a,b))$ 取值 $3^{m-1}-\frac{1+(-1)^{(m+1)/2}3^{(m-1)/2}}{2}$ 和 $3^{m-1}-\frac{1+(-1)^{(m-1)/2}3^{(m-1)/2}}{2}$ 各 3^m-1 次. 因而, 当 $m\geq 3$ 为奇数, 我们得到了重量分布. □

例 5.1: 令 $(q,m)=(3,4)$. 定理 5.5 的码 $\mathcal{C}_{(n,q,m,\delta_1)}$ 有参数 $[40,3,25]$, 和重量分布 $1+16z^{25}+8z^{30}+2z^{40}$. 这个码是最优的循环码 (305 页[93]).

例 5.2: 令 $(q,m)=(3,5)$. 定理 5.5 的码 $\mathcal{C}_{(n,q,m,\delta_1)}$ 有参数 $[121,6,76]$, 和重量分布 $1+242z^{76}+242z^{81}+242z^{85}+2z^{121}$.

表 5.1　$\mathcal{C}_{(n,q,m,\delta_1)}$ 的重量分布当 $m \geq 4$ 为偶数

重量	次数
0	1
$3^{m-1} - \frac{3^{m/2-1}+1}{2}$	$2(3^{m/2}-1)$
$3^{m-1} + 3^{m/2-1}$	$3^{m/2}-1$
$\frac{3^m-1}{2}$	2

表 5.2　$\mathcal{C}_{(n,q,m,\delta_1)}$ 的重量分布当 $m \geq 3$ 为奇数

重量	次数
0	1
3^{m-1}	3^m-1
$3^{m-1} - \frac{1+(-1)^{(m-1)/2}3^{(m-1)/2}}{2}$	3^m-1
$3^{m-1} - \frac{1+(-1)^{(m+1)/2}3^{(m-1)/2}}{2}$	3^m-1
$\frac{3^m-1}{2}$	2

定理 5.6: 令 $m \geq 3$ 且 $q = 3$. 三元码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$ 有参数

$$\left[\frac{q^m-1}{q-1},\, k,\, d\right],$$

其中

$$k = \begin{cases} m & \text{如果 } m \text{ 是奇数,} \\ \frac{m}{2} & \text{如果 } m \text{ 是偶数,} \end{cases}$$

且

$$d = \begin{cases} 3^{m-1} & \text{如果 } m \text{ 是奇数,} \\ 3^{m-1} + 3^{\frac{m}{2}-1} & \text{如果 } m \text{ 是偶数.} \end{cases}$$

此外, $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$ 是一重码.

证明. 由 Delsarte 定理[72],

$$\tilde{\mathcal{C}}_{(n,q,m,\delta_1)} = \{c(a) : a \in \mathrm{GF}(3^m)\},$$

其中

$$c(a) = \left(\mathrm{Tr}_3^{3^m}\left(a\alpha^{(3^{m-1}+3^{\lfloor\frac{m-1}{2}\rfloor})j}\right)\right)_{j=0}^{n-1}.$$

注意到 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$ 是 $\mathcal{C}_{(n,q,m,\delta_1)}$ 的一个子码, 重量分布由定理 5.5 易得. □

容易验证定理 5.6 的码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$ 达到 Griesmer 界, 因而是最优的. 当 m 是偶数, 码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$ 的参数也许是新的. 当 m 是奇数, 码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$ 的参数不是新的, 它等价于 $\mathrm{GF}(3)$ 上的 simplex 码. 当 m 为奇数, 以上定理证明了三元 simplex 码等价于三元狭义射影 BCH 码. 已知 $\mathrm{GF}(q)$ 上的 simplex 码置换等价于一个循环码当 $\gcd(m, q-1) = 1$. 然而, 不清楚 $\mathrm{GF}(q)$ 上的 simplex 码是否等价于一个 BCH 码当 $\gcd(m, q-1) = 1$.

5.1.4.4 三元码 $\tilde{\mathcal{C}}_{(n,3,m,\delta_2)}$ 和 $\mathcal{C}_{(n,3,m,\delta_2)}$

确定三元码 $\tilde{\mathcal{C}}_{(n,3,m,\delta_2)}$ 和 $\mathcal{C}_{(n,3,m,\delta_2)}$ 的重量分布依赖于有限域上二次型的理论. 我们首先做一些准备.

令 $m \geq 3$ 为奇数. 对 $a, b \in \mathrm{GF}(2^{2m})$, 定义二次型

$$Q(x) = \mathrm{Tr}_3^{3^m}\left(ax^{3^{\frac{m-1}{2}}+1} + bx^{3^{\frac{m-3}{2}}+1}\right).$$

令 $r_{a,b}$ 为以上二次型的秩.

引理 5.10: 令 m 为奇数, $a, b \in \mathrm{GF}(2^{2m})$ 且 $(a, b) \neq (0, 0)$. 二次型

$$Q(x) = \mathrm{Tr}_3^{3^m}\left(ax^{3^{\frac{m-1}{2}}+1} + bx^{3^{\frac{m-3}{2}}+1}\right)$$

有秩 $r_{a,b} \in \{m, m-1, m-2, m-3\}$.

证明. 令 $B(x, y)$ 为与二次型 $Q(x)$ 相关的对称双线性型, 亦即,

$$\begin{aligned} B(x, y) &= Q(x+y) - Q(x) - Q(y) \\ &= \mathrm{Tr}_3^{3^m}\left(\left(b^{3^{\frac{m+3}{2}}}x^{3^{\frac{m+3}{2}}} + a^{3^{\frac{m+1}{2}}}x^{3^{\frac{m+1}{2}}} + ax^{3^{\frac{m-1}{2}}} + bx^{3^{\frac{m-3}{2}}}\right)y\right). \end{aligned}$$

回顾方程

$$b^{3^{\frac{m+3}{2}}}x^{3^{\frac{m+3}{2}}} + a^{3^{\frac{m+1}{2}}}x^{3^{\frac{m+1}{2}}} + ax^{3^{\frac{m-1}{2}}} + bx^{3^{\frac{m-3}{2}}} = 0$$

有 3^r 个解 $x \in \mathrm{GF}(2^{2m})$ 当且仅当 $Q(x)$ 的秩为 $m - r$. 注意到以上方程解的个数等于以下方程的解的个数的个数:

$$b^{3^{\frac{m+3}{2}}}x^{3^3} + a^{3^{\frac{m+1}{2}}}x^{3^2} + ax^3 + bx = 0.$$

这个方程至多有 27 个解, 因此 $r \leq 3$ 且 $r_{a,b} \in \{m, m-1, m-2, m-3\}$. □

对 $a, b \in \mathrm{GF}(2^{2m})$, 定义

$$T(a, b) = \sum_{x \in \mathrm{GF}(2^{2m})} \zeta_3^{\mathrm{Tr}_3^{3^m}\left(ax^{3^{\frac{m-1}{2}}+1} + bx^{3^{\frac{m-3}{2}}+1}\right)}.$$

记 $r_{a,b}$ 为二次型 $Q(x) = \mathrm{Tr}_3^{3^m}\left(ax^{3^{\frac{m-1}{2}}+1} + bx^{3^{\frac{m-3}{2}}+1}\right)$ 的秩, 记 η_0 为 $\mathrm{GF}(3)$ 上的二次

特征. 那么

$$\begin{aligned} S(a,b) &:= \sum_{y\in \mathrm{GF}(3)^*} T(ya,yb) \\ &= \sum_{y\in \mathrm{GF}(3)^*} \eta_0(y^{r_{a,b}})T(a,b) = T(a,b)\left(1+(-1)^{r_{a,b}}\right). \end{aligned}$$

我们会用到以下关于距等式的结果.

引理 5.11: 对 $S(a,b)$, 我们有:

i) $\sum_{a,b\in \mathrm{GF}(2^{2m})} S(a,b) = 2\times 3^{2m}$.

ii) $\sum_{a,b\in \mathrm{GF}(2^{2m})} S(a,b)^2 = 4\times 3^{3m}$.

iii) $\sum_{a,b\in \mathrm{GF}(2^{2m})} S(a,b)^3 = 32\times 3^{3m} - 24\times 3^{2m}$.

iv) $\sum_{a,b\in \mathrm{GF}(2^{2m})} T(a,b)^2 = 3^{2m}$.

证明. i) 显然.

ii) 定义 N_2 为 $(u,v)\in \mathrm{GF}(3)^*\times \mathrm{GF}(3)^*$ 和 $(x,y)\in \mathrm{GF}(2^{2m})\times \mathrm{GF}(2^{2m})$ 的个数, 满足以下两个方程:

$$\begin{cases} ux^{3^{\frac{m-1}{2}}+1} + vy^{3^{\frac{m-1}{2}}+1} = 0, \\ ux^{3^{\frac{m-3}{2}}+1} + vy^{3^{\frac{m-3}{2}}+1} = 0. \end{cases}$$

易知 $\sum_{a,b\in \mathrm{GF}(2^{2m})} S(a,b)^2 = 3^{2m}N_2$. 因而, 只需确定 N_2.

当 $x=y=0$, (u,v) 有 4 种选择. 当 $x\neq 0, y\neq 0$, 以上方程组等价于

$$\begin{cases} (\frac{x}{y})^{3^{\frac{m-1}{2}}+1} = -\frac{v}{u}, \\ (\frac{x}{y})^{3^{\frac{m-3}{2}}+1} = -\frac{v}{u}. \end{cases}$$

注意到 $\gcd(3^{\frac{m-1}{2}}+1, 3^m-1) = \gcd(3^{\frac{m-3}{2}}+1, 3^m-1) = 2$. 我们可知 $-\frac{v}{u}\in \mathrm{GF}(3)^*$ 为一个平方元. 即, $-\frac{v}{u}=1$. 因而, (u,v) 有 2 个选择. 同时, $\frac{x}{y}=\pm 1$ 恰好是以下方程组的所有解:

$$\begin{cases} (\frac{x}{y})^{3^{\frac{m-1}{2}}+1} = 1, \\ (\frac{x}{y})^{3^{\frac{m-3}{2}}+1} = 1. \end{cases}$$

因此, (x,y) 有 $2(3^m-1)$ 个选择. 总之, (u,v) 和 (x,y) 有 $4(3^m-1)$ 个选择当 $x\neq 0$ 且 $y\neq 0$. 总计, 我们有 $N_2=4+4(3^m-1)=4\times 3^m$.

iii) 定义 N_3 为三元组 $(u,v,w)\in \mathrm{GF}(3)^*\times\mathrm{GF}(3)^*\times\mathrm{GF}(3)^*$ 和 $(x,y,z)\in \mathrm{GF}(2^{2m})\times \mathrm{GF}(2^{2m})\times \mathrm{GF}(2^{2m})$ 的个数满足:

$$\begin{cases} ux^{3^{\frac{m-1}{2}}+1}+vy^{3^{\frac{m-1}{2}}+1}+wz^{3^{\frac{m-1}{2}}+1}=0,\\ ux^{3^{\frac{m-3}{2}}+1}+vy^{3^{\frac{m-3}{2}}+1}+wz^{3^{\frac{m-3}{2}}+1}=0. \end{cases}$$

易知 $\sum_{a,b\in\mathrm{GF}(2^{2m})}S(a,b)^3=3^{2m}N_3$. 因此, 只需确定 N_3.

当 $x=y=z=0$, 三元组 (u,v,w) 有 8 种选择. 当 x,y,z 恰有一个为 0, 我们可利用 ii) 的结果. 例如, 如果 $x=0$, 那么 $u\in\{1,2\}$ 且方程组退化为

$$\begin{cases} vy^{3^{\frac{m-1}{2}}+1}+wz^{3^{\frac{m-1}{2}}+1}=0,\\ vy^{3^{\frac{m-3}{2}}+1}+wz^{3^{\frac{m-3}{2}}+1}=0. \end{cases}$$

由 ii), (v,w) 和 (y,z) 有 $4(3^m-1)$ 个选择. 因此, 三元组 (u,v,w) 和 $(0,y,z)$ 有 $8(3^m-1)$ 个选择. 总计, 当 x,y,z 恰有一个为 0, 我们有 $24(3^m-1)$ 个选择.

当 x,y,z 全部非零, 我们有

$$u(\frac{x}{z})^{3^{\frac{m-1}{2}}+1}+v(\frac{y}{z})^{3^{\frac{m-1}{2}}+1}+w=0, \tag{5.8}$$

$$u(\frac{x}{z})^{3^{\frac{m-3}{2}}+1}+v(\frac{y}{z})^{3^{\frac{m-3}{2}}+1}+w=0. \tag{5.9}$$

由 (5.8) 和 (5.9) 可得

$$(\frac{x}{y})^{3^{\frac{m+3}{2}}+1}=-\frac{v(y^2-z^2)}{u(x^2-z^2)}. \tag{5.10}$$

(5.9) 两边取三次幂得,

$$u(\frac{x}{z})^{3^{\frac{m-1}{2}}+3}+v(\frac{y}{z})^{3^{\frac{m-1}{2}}+3}+w=0. \tag{5.11}$$

联合 (5.11) 和 (5.8) 可得

$$(\frac{x}{y})^{3^{\frac{m-1}{2}}+1}=-\frac{v(y^2-z^2)}{u(x^2-z^2)}. \tag{5.12}$$

由 (5.10) 和 (5.12), 我们有 $(\frac{x}{y})^{3^{\frac{m+3}{2}}+1} = (\frac{x}{y})^{3^{\frac{m-1}{2}}+1}$, 等价于 $(\frac{x}{y})^8 = 1$. 由于 $\gcd(8, 3^m - 1) = 2$, 我们有 $(\frac{x}{y})^2 = 1$. 由 x, y, z 的对称性, 我们推出 $(\frac{x}{z})^2 = 1$ 且 $(\frac{y}{z})^2 = 1$. 因此, 原方程组退化为

$$u + v + w = 0, \ \ u, v, w \in \mathrm{GF}(3)^*.$$

易知三元组 (u, v, w) 有 2 个选择, 三元组 (x, y, z) 有 $4(3^m - 1)$ 个选择. 总计, 当 x, y, z 全部非零时有 $8(3^m - 1)$ 个选择. 因此, $N_3 = 8 + 24(3^m - 1) + 8(3^m - 1) = 32 \times 3^m - 24$.

iv) 证明完全类似于 ii), 故在此略去. □

对 $j \in \{0, 2\}$, 定义

$$n_j = \left| \left\{ (a, b) \in \mathrm{GF}(2^{2m}) \times \mathrm{GF}(2^{2m}) : T(a, b) = \pm 3^{\frac{m+j}{2}} \sqrt{-1} \right\} \right|.$$

对 $j \in \{1, 3\}$ 且 $\epsilon = \pm 1$, 定义

$$n_{\epsilon,j} = \left| \left\{ (a, b) \in \mathrm{GF}(2^{2m}) \times \mathrm{GF}(2^{2m}) : T(a, b) = \epsilon 3^{\frac{m+j}{2}} \right\} \right|.$$

在 $n_{1,3} = 0$ 的假设下, (这个假设将在后面证明, 见定理 5.7 的证明), 我们得到 $T(a, b)$ 和 $S(a, b)$ 的值分布.

引理 5.12: 令 $m \geq 3$ 为一个奇数. 假设 $n_{1,3} = 0$.

(i). $T(a, b)$ 的值分布如下:

秩 $r_{a,b}$	值 $T(a,b)$	次数
m	$3^{\frac{m}{2}}\sqrt{-1}$	$\frac{(3^m-1)(8\times 3^m-9\times 3^{m-1}+9)}{8}$
m	$-3^{\frac{m}{2}}\sqrt{-1}$	$\frac{(3^m-1)(8\times 3^m-9\times 3^{m-1}+9)}{8}$
$m-1$	$3^{\frac{m+1}{2}}$	$\frac{(3^{m-1}+3^{\frac{m-1}{2}})(3^m-1)}{2}$
$m-1$	$-3^{\frac{m+1}{2}}$	$\frac{(3^{m-1}-3^{\frac{m-1}{2}})(3^m-1)}{2}$
$m-2$	$3^{\frac{m}{2}+1}\sqrt{-1}$	$\frac{(3^m-1)(3^{m-1}-1)}{8}$
$m-2$	$-3^{\frac{m}{2}+1}\sqrt{-1}$	$\frac{(3^m-1)(3^{m-1}-1)}{8}$
0	3^m	1

(2). $S(a,b)$ 的值分布如下:

秩 $r_{a,b}$	值 $S(a,b)$	次数
$m, m-2$	0	$(3^m-3^{m-1}+1)(3^m-1)$
$m-1$	$2\times 3^{\frac{m+1}{2}}$	$\frac{(3^{m-1}+3^{\frac{m-1}{2}})(3^m-1)}{2}$
$m-1$	$-2\times 3^{\frac{m+1}{2}}$	$\frac{(3^{m-1}-3^{\frac{m-1}{2}})(3^m-1)}{2}$
0	2×3^m	1

证明. 由引理 5.11 的距等式, 我们有

$$n_0+n_2+n_{1,1}+n_{-1,1}+n_{1,3}+n_{-1,3}=3^{2m}-1,$$
$$n_{1,1}-n_{-1,1}+3(n_{1,3}-n_{-1,3})=3^{\frac{m-1}{2}}(3^m-1),$$

$$n_{1,1}+n_{-1,1}+9(n_{1,3}+n_{-1,3})=3^{m-1}(3^m-1),$$
$$n_{1,1}-n_{-1,1}+27(n_{1,3}-n_{-1,3})=3^{\frac{m-1}{2}}(3^m-1),$$
$$-n_0+3(n_{1,1}+n_{-1,1})-9n_2+27(n_{1,3}+n_{-1,3})=0.$$

连同 $n_{1,3}=0$, 可知 $T(a,b)$ 的值分布. 由于 $S(a,b)=0$ 如果 $r_{a,b}\in\{m,m-2\}$ 且 $S(a,b)=2T(a,b)$ 如果 $r_{a,b}\in\{m-1,m-3\}$, 易知 $S(a,b)$ 的值分布. □

定理 5.7: 令 $m\geq 3$ 且 $q=3$. 三元码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 有参数

$$\left[\frac{q^m-1}{q-1},\ k,\ d\right],$$

其中

$$k=\begin{cases}2m & \text{如果 } m \text{ 是奇数},\\ \frac{3m}{2} & \text{如果 } m \text{ 是偶数},\end{cases}$$

且 $d=3^{m-1}-3^{\lfloor\frac{m-1}{2}\rfloor}$. 此外, 重量分布列在表 5.3 当 m 是偶数, 列在表 5.4 当 m 是奇数.

证明. 码的维数可由引理 5.9 得出. 注意到

$$\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}=\{c_1(a,b):a,b\in \mathrm{GF}(2^{2m})\},$$

其中

$$c_1(a,b)=\left(\mathrm{Tr}_3^{3^m}\left(a\beta^{\frac{3^{m-1}+3^{\lfloor\frac{m-1}{2}\rfloor}}{2}j}+b\beta^{\frac{3^{m-1}+3^{\lfloor\frac{m+1}{2}\rfloor}}{2}j}\right)\right)_{j=0}^{n-1},$$

此处 $\beta=\alpha^2$ 且 α 是 $\mathrm{GF}(3^m)^*$ 的一个生成元.

当 m 是偶数, 由于 $\mathrm{Tr}_3^{3^m}(x)^{3^j}=\mathrm{Tr}_3^{3^m}(x)$ 对 $x\in\mathrm{GF}(2^{2m})$ 和任意 j, 确定 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 的重量分布归结于以下码 $\mathcal{C}$ 的重量分布

$$c_2(a,b)=\left(\mathrm{Tr}_3^{3^m}\left(a\alpha^{(3^{\frac{m}{2}}+1)j}+b\alpha^{(3^{\frac{m}{2}-1}+1)j}\right)\right)_{j=0}^{n-1},\quad a\in\mathrm{GF}(3^{\frac{m}{2}}),b\in\mathrm{GF}(3^m).$$

我们指出 $\mathcal{C}$ 的重量分布是已知的 (定理 2[195]). 因而可得 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 的重量分布, 列在表 5.3. 可知极小距离 $d=3^{m-1}-3^{\frac{m}{2}-1}$.

表 5.3 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 的重量分布当 $m \geq 4$ 是偶数

重量	次数
0	1
$3^{m-1}-3^{\frac{m}{2}-1}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{8}$
3^{m-1}	$3^{\frac{m}{2}-1}(3^m-1)$
$3^{m-1}+3^{\frac{m}{2}-1}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{m-1}+1)}{4}$
$3^{m-1}+3^{\frac{m}{2}}$	$\frac{(3^{\frac{m}{2}-1}-1)(3^m-1)}{8}$

当 m 为奇数时, 我们需要多一点工作. 对 $a,b \in \mathrm{GF}(2^{2m})$, 定义

$$c_3(a,b)=\left(\mathrm{Tr}_3^{3^m}\left(a\alpha^{(3^{\frac{m-1}{2}}+1)j}+b\alpha^{(3^{\frac{m-3}{2}}+1)j}\right)\right)_{j=0}^{n-1}.$$

这等价于考虑码

$$\mathcal{C}'=\left\{c_3(a,b):a,b\in\mathrm{GF}(2^{2m})\right\}.$$

直接的计算可知

$$w(c_3(a,b))=3^{m-1}-\frac{1}{6}S(a,b).$$

因此我们从引理 5.12 中 $S(a,b)$ 的值分布直接得到 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 的重量分布 (见表 5.4), 假设 $n_{1,3}=0$.

我们最后证明 $n_{1,3}=0$. 这是因为 $n_{1,3}$ 是 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 中重量为 $3^{m-1}-3^{\frac{m+1}{2}}$ 的码字的个数. 然而, $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 是 $\mathcal{C}_{(n,q,m,\delta_2)}$ 的一个子码, 其极小距离为 $d\geq\delta_2=3^{m-1}-1-\frac{3^{\frac{m+1}{2}}-1}{2}>3^{m-1}-3^{\frac{m+1}{2}}$. 所以 $n_{1,3}=0$. □

例 5.3: 令 $(q,m)=(3,4)$. 定理 5.7 的码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 有参数 $[40,6,24]$, 及重量分布 $1+300z^{24}+240z^{27}+168z^{30}+20z^{36}$. 这是最优的循环码和线性码 (305 页 [93]).

例 5.4: 令 $(q,m)=(3,5)$. 定理 5.7 的码 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 有参数 $[121,10,72]$, 及重量分布 $1+10890z^{72}+39446z^{81}+8712z^{90}$. 这个码与数据库中最优的三元线性码有相同的参数.

表 5.4 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 的重量分布当 $m \geq 3$ 是奇数

重量	次数
0	1
$3^{m-1}-3^{\frac{m-1}{2}}$	$\frac{(3^{m-1}+3^{\frac{m-1}{2}})(3^m-1)}{2}$
3^{m-1}	$(3^m-3^{m-1}+1)(3^m-1)$
$3^{m-1}+3^{\frac{m-1}{2}}$	$\frac{(3^{m-1}-3^{\frac{m-1}{2}})(3^m-1)}{2}$

定理 5.8: 令 $m \geq 3$ 且 $q=3$. 三元码 $\mathcal{C}_{(n,q,m,\delta_2)}$ 有参数

$$\left[\frac{q^m-1}{q-1},\, k,\, \delta_2\right],$$

其中

$$k=\begin{cases} 2m+1 & \text{如果 } m \text{ 是奇数,} \\ \frac{3m+2}{2} & \text{如果 } m \text{ 是偶数.} \end{cases}$$

此外, 重量分布列在表 5.5 当 m 是偶数, 列在表 5.6 当 m 是奇数.

证明. 由引理 5.9 可知码的维数. 注意到

$$\mathcal{C}_{(n,q,m,\delta_2)}=\left\{c_1(a,b,c): a,b\in \mathrm{GF}(2^{2m}), c\in \mathrm{GF}(3)\right\},$$

其中

$$c_1(a,b,c)=\left(\mathrm{Tr}_3^{3^m}\left(a\beta^{\frac{3^{m-1}+3^{\lfloor\frac{m-1}{2}\rfloor}}{2}j}+b\beta^{\frac{3^{m-1}+3^{\lfloor\frac{m+1}{2}\rfloor}}{2}j}\right)+c\right)_{j=0}^{n-1}.$$

此处 $\beta=\alpha^2$ 且 α 是 $\mathrm{GF}(3^m)^*$ 的一个生成元.

当 m 是偶数, 对 $a,b\in \mathrm{GF}(2^{2m})$, 定义

$$c_2(a,b,c)=\left(\mathrm{Tr}_3^{3^m}\left(a\alpha^{(3^{\frac{m}{2}}+1)j}+b\alpha^{(3^{\frac{m}{2}-1}+1)j}\right)+c\right)_{j=0}^{n-1}.$$

确定 $\mathcal{C}_{(n,q,m,\delta_2)}$ 的重量分布可归结为考虑码

$$\mathcal{C} = \left\{c_2(a,b,c) : a \in \mathrm{GF}(3^{\frac{m}{2}}), b \in \mathrm{GF}(2^{2m}), c \in \mathrm{GF}(3)\right\}$$

的重量分布. 直接计算可知

$$\begin{aligned} w(c_2(a,b,c)) &= 3^{m-1} + \frac{1}{2}\left(\delta_{0,c} - 1\right) - \frac{1}{6}\sum_{y\in \mathrm{GF}(3)^*} \zeta_3^{cy} U(ya, yb) \\ &= 3^{m-1} + \frac{1}{2}\left(\delta_{0,c} - 1\right) - \frac{1}{6}\sum_{y\in \mathrm{GF}(3)^*} \zeta_3^{cy} (-1)^{r'_{a,b}} U(a,b), \end{aligned}$$

其中

$$U(a,b) = \sum_{x\in \mathrm{GF}(2^{2m})} \zeta_3^{\mathrm{Tr}_3^{3^m}(ax^{3^{\frac{m}{2}}+1} + bx^{3^{\frac{m}{2}-1}+1})},$$

$$\delta_{0,c} = \begin{cases} 1 & \text{如果 } c = 0, \\ 0 & \text{如果 } c \neq 0, \end{cases}$$

且 $r'_{a,b}$ 是二次型 $\mathrm{Tr}_3^{3^m}(ax^{3^{\frac{m}{2}}+1} + bx^{3^{\frac{m}{2}-1}+1})$ 的秩. 由定理 1[195], $U(a,b)$ 的值分布已知, 并列在下表:

秩$r'_{a,b}$	值$U(a,b)$	次数
m	$3^{\frac{m}{2}}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{8}$
m	$-3^{\frac{m}{2}}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{m-1}+1)}{4}$
$m-1$	$3^{\frac{m+1}{2}}i$	$\frac{3^{\frac{m}{2}-1}(3^m-1)}{2}$
$m-1$	$-3^{\frac{m+1}{2}}i$	$\frac{3^{\frac{m}{2}-1}(3^m-1)}{2}$
$m-2$	$-3^{\frac{m}{2}+1}$	$\frac{(3^{\frac{m}{2}-1}-1)(3^m-1)}{8}$
0	3^m	1

当 m 为偶数, $\mathcal{C}$ 和 $\mathcal{C}_{(n,q,m,\delta_2)}$ 的重量分布 (见表 5.5) 可由 $U(a,b)$ 的值分布得出.

例如, 由上表, 当 $r'_{a,b} = m$, $U(a,b)$ 取 $3^{\frac{m}{2}}$ 共 $\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{8}$ 次. 因此, 如果 $c = 0$, $w(c_2(a,b,c))$ 取值 $3^{m-1} - 3^{\frac{m}{2}-1}$ 共 $\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{8}$ 次, 如果 $c = 1$ 或 2, $w(c_2(a,b,c))$ 取值 $3^{m-1} + \frac{1}{2}\left(3^{\frac{m}{2}-1} - 1\right)$ 共 $\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{4}$ 次.

当 m 为奇数, 对 $a, b \in \mathrm{GF}(2^{2m})$ 和 $c \in \mathrm{GF}(3)$, 定义

$$c_3(a,b,c) = \left(\mathrm{Tr}_3^{3^m}\left(a\alpha^{(3^{\frac{m-1}{2}}+1)j} + b\alpha^{(3^{\frac{m-3}{2}}+1)j}\right) + c\right)_{j=0}^{n-1}.$$

只需考虑码

$$\mathcal{C}' = \left\{c_3(a,b,c) : a, b \in \mathrm{GF}(2^{2m}), c \in \mathrm{GF}(3)\right\}.$$

直接计算可得

$$w(c_3(a,b,c)) = 3^{m-1} + \frac{1}{2}\left(\delta_{0,c} - 1\right) - \frac{1}{6}\sum_{y\in\mathrm{GF}(3)^*} \zeta_3^{cy}(-1)^{r_{a,b}}T(a,b),$$

其中 $T(a,b)$ 和 $r_{a,b}$ 与引理 5.12 中相同. 利用引理 5.12中 $T(a,b)$ 的值分布, 当 m 为奇数, 我们得到 $\mathcal{C}_{(n,q,m,\delta_2)}$ 的重量分布 (见表 5.6). □

例 5.5: 令 $(q,m) = (3,4)$. 定理 5.8 的码 $\mathcal{C}_{(n,q,m,\delta_2)}$ 有参数 $[40,7,22]$, 和重量分布

$$1 + 280z^{22} + 300z^{24} + 336z^{25} + 240z^{27} + 600z^{28} + 168z^{30} + 240z^{31} + 20z^{36} + 2z^{40}.$$

这是最好的三元循环码 (305 页[93]), 且与数据库中最好的三元线性码有相同的参数. 注意到对参数为 $[40,7,d]$ 的三元线性码, 我们有 $d \le 23$.

例 5.6: 令 $(q,m) = (3,5)$. 定理 5.8 的码 $\mathcal{C}_{(n,q,m,\delta_2)}$ 有参数 $[121,11,67]$, 和重量分布

$$1 + 2420z^{67} + 10890z^{72} + 54450z^{76} + 39446z^{81} + 58806z^{85} + 8712z^{90} + 2420z^{94} + 2z^{121}.$$

数据库中已知最好的三元线性码有参数 $[121,11,68]$, 这个码不是循环码.

5.1.5 有特殊设计距离的狭义射影 BCH 码

在本小节中, 我们研究长为 $n = \frac{q^m-1}{q-1}$ 的有特殊设计距离的狭义射影 BCH 码. 如

表 5.5 $\mathcal{C}_{(n,q,m,\delta_2)}$ 的重量分布当 $m \geq 4$ 为偶数

重量	次数
0	1
$\frac{3^m-3^{m-1}-3^{\frac{m}{2}}-1}{2}$	$\frac{(5\times 3^{\frac{m}{2}-1}-1)(3^m-1)}{4}$
$\frac{3^m-3^{m-1}-2\times 3^{\frac{m}{2}-1}}{2}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{8}$
$\frac{3^m-3^{m-1}-3^{\frac{m}{2}-1}-1}{2}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{m-1}+1)}{2}$
$\frac{3^m-3^{m-1}}{2}$	$3^{\frac{m}{2}-1}(3^m-1)$
$\frac{3^m-3^{m-1}+3^{\frac{m}{2}-1}-1}{2}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{\frac{m}{2}}+1)^2}{4}$
$\frac{3^m-3^{m-1}+2\times 3^{\frac{m}{2}-1}}{2}$	$\frac{3(3^{\frac{m}{2}}-1)(3^{m-1}+1)}{4}$
$\frac{3^m-3^{m-1}+3^{\frac{m}{2}}-1}{2}$	$3^{\frac{m}{2}-1}(3^m-1)$
$\frac{3^m-3^{m-1}+2\times 3^{\frac{m}{2}}}{2}$	$\frac{(3^{\frac{m}{2}-1}-1)(3^m-1)}{8}$
$\frac{3^m-1}{2}$	2

表 5.6 $\mathcal{C}_{(n,q,m,\delta_2)}$ 的重量分布当 $m \geq 3$ 为奇数

重量	次数
0	1
$\frac{3^m-3^{m-1}-3^{\frac{m+1}{2}}-1}{2}$	$\frac{(3^{m-1}-1)(3^m-1)}{8}$
$\frac{3^m-3^{m-1}-2\times 3^{\frac{m-1}{2}}}{2}$	$\frac{(3^{m-1}+3^{\frac{m-1}{2}})(3^m-1)}{2}$
$\frac{3^m-3^{m-1}-3^{\frac{m-1}{2}}-1}{2}$	$\frac{(8\times 3^m-3^{m-1}-8\times 3^{\frac{m-1}{2}}+9)(3^m-1)}{8}$
$\frac{3^m-3^{m-1}}{2}$	$(3^m-3^{m-1}+1)(3^m-1)$
$\frac{3^m-3^{m-1}+3^{\frac{m-1}{2}}-1}{2}$	$\frac{(8\times 3^m-3^{m-1}+8\times 3^{\frac{m-1}{2}}+9)(3^m-1)}{8}$
$\frac{3^m-3^{m-1}+2\times 3^{\frac{m-1}{2}}}{2}$	$\frac{(3^{m-1}-3^{\frac{m-1}{2}})(3^m-1)}{2}$
$\frac{3^m-3^{m-1}+3^{\frac{m+1}{2}}-1}{2}$	$\frac{(3^{m-1}-1)(3^m-1)}{8}$
$\frac{3^m-1}{2}$	2

前所述, 一些模 $\frac{q^m-1}{q-1}$ 的陪集代表元的信息可由非减序列分解得出. 注意到对于一个狭义的 BCH 码, 它的 Bose 距离为一个陪集代表元. 因此, 如果设计距离有某些特殊的形式, 我们可以得到 Bose 距离.

定理 5.9: 令 $2 \leq \delta \leq n$ 为一个整数. 假设 $E(\delta) = \underline{V_1 V_2} \dots \underline{V_r}$.

i) 假设 $\overline{\delta}$ 仅有 0 和 1 分量. 如果 $\underline{V_1} = \underline{V_2} = \cdots = \underline{V_r}$ 或 $\underline{V_1} = \underline{V_2} = \cdots = \underline{V_j} < \underline{V_k}$ 对所有 $j < k \leq r$, 那么 $\mathcal{C}_{(n,q,m,\delta)}$ 有 Bose 距离 $d_B = \delta$.

ii) 假设 $\underline{V_1}$ 长度为 l 且有分量 0 或 1. 令 $\underline{V_1} > \underline{V_2}$ 且 $m = al + b$, 其中 $0 \leq b \leq l-1$.

(a). 如果 $b = 0$, 那么 $\mathcal{C}_{(n,q,m,\delta)}$ 有 Bose 距离

$$d_B = E^{-1}(\underbrace{\underline{V_1 V_1} \dots \underline{V_1}}_{a}).$$

(b). 如果 $1 \leq b \leq l-1$, 那么 $\mathcal{C}_{(n,q,m,\delta)}$ 有 Bose 距离

$$d_B \geq E^{-1}(\underbrace{\underline{V_1 V_1} \dots \underline{V_1}}_{a} S(T_b(\underline{V_1}))).$$

特别地, 如果 $S(T_b(\underline{V_1}))$ 最后的一个分量为 1, 那么等式成立.

证明. 这些结果是引理 5.3 和引理 5.4 的直接推论. □

对某些特定的 δ, 以上定理在确定 $\mathcal{C}_{(n,q,m,\delta)}$ 的 Bose 距离时非常有用. 以下, 我们给出几个例子.

例 5.7: 对 $q = 3, m = 6$ 和 $\delta = 110$, 考虑码 $\mathcal{C}_{(364,3,6,110)}$. 注意到

$$\overline{\delta} = (0, 1, 1, 0, 0, 2) = \underline{V_1 V_2},$$

其中 $\underline{V_1} = (0, 1, 1)$ 且 $\underline{V_2} = (0, 0, 2)$. 由于 $\underline{V_1} > \underline{V_2}$, 由定理 5.9 的 ii), Bose 距离

$$d_B = E^{-1}(\underline{V_1 V_1}) = E^{-1}(0, 1, 1, 0, 1, 1) = 112.$$

事实上, 最小的不超过 $\delta = 110$ 的陪集代表元即 112, 其中 $C_{112} = \{112, 280, 336\}$.

例 5.8: 对 $q=3, m=5$ 和 $\delta=29$, 考虑码 $\mathcal{C}_{(121,3,5,29)}$. 注意到

$$\overline{\delta}=(0,1,0,0,2)=\underline{V_1V_2},$$

其中 $\underline{V_1}=(0,1), \underline{V_2}=(0,0,2)$. 由于 $\underline{V_1}>\underline{V_2}$, 由定理 5.9 的 ii), Bose 距离

$$d_B=E^{-1}(\underline{V_1V_1}S(T_1(\underline{V_1})))=E^{-1}(0,1,0,1,1)=31.$$

事实上, 最小的不超过 $\delta=29$ 的陪集代表元即 31, 其中 $C_{31}=\{31,37,91,93,111\}$.

例 5.9: 对 $q=7, m=5$ 和 $\delta=393$, 考虑码 $\mathcal{C}_{(2801,7,5,393)}$. 注意到

$$\overline{\delta}=(0,1,1,0,1)=\underline{V_1V_2},$$

其中 $\underline{V_1}=(0,1,1), \underline{V_2}=(0,1)$. 由于 $\underline{V_1}>\underline{V_2}$, 由定理 5.9 的 ii), Bose 距离

$$d_B\geq E^{-1}(\underline{V_1}S(T_2(\underline{V_1})))=E^{-1}(0,1,1,0,2)=394.$$

事实上, 最小的不超过 $\delta=393$ 的陪集代表元即 394, 其中 $C_{394}=\{394,694,2057,2500,2758\}$. 因此, 我们有 Bose 距离 $d_B=394$.

以下, 我们考虑两类特殊的设计距离. 首先, 我们考虑设计距离为 $\frac{q^i-1}{q-1}$, 其中 $1\leq i\leq m-1$ 的 BCH 码.

定理 5.10: 对 $1\leq i\leq m-1$, $\mathcal{C}_{(n,q,m,\frac{q^i-1}{q-1})}$ 有 Bose 距离 $d_B=\frac{q^i-1}{q-1}$. 进一步, 如果 $1\leq i\leq\lceil\frac{m}{2}\rceil$, 那么码 $\mathcal{C}_{(n,q,m,\frac{q^i-1}{q-1})}$ 有参数

$$\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1}-m(q^{i-1}-1), d\right],$$

其中 $d\geq\frac{q^i-1}{q-1}$. 特别地, 如果 $i\mid m$, 那么 $d=\frac{q^i-1}{q-1}$.

证明. 注意到

$$\overline{\frac{q^i-1}{q-1}}=(\underbrace{0,\ldots,0}_{m-i},1,\ldots,1).$$

由定理 5.9 的 i), $\frac{q^i-1}{q-1}$ 是一个陪集代表元. 因此 $d_B = \frac{q^i-1}{q-1}$. 当 $1 \le i \le \lceil \frac{m}{2} \rceil$, 维数由定理 5.1 可知. 如果 $i \mid m$, 由引理 5.8, 我们有 $d = \frac{q^i-1}{q-1}$. □

有以上定理和数值实验, 我们有以下的猜想.

猜想： *码 $\mathcal{C}_{(n,q,m,(q^i-1)/(q-1))}$ 有极小距离 $d = (q^i-1)/(q-1)$, 其中 $1 \le i \le m-1$.*

注意到定理 5.10 说明这个猜想是对的当 $i \mid m$.

接下来, 我们考虑设计距离为 $q^i + l$ 的 BCH 码, 其中 $1 \le i \le \lceil \frac{m}{2} \rceil - 1$ 且 $1 \le l \le q-1$.

定理 5.11: *对 $1 \le i \le \lceil \frac{m}{2} \rceil - 1$ 且 $1 \le l \le q-1$, $\mathcal{C}_{(n,q,m,q^i+l)}$ 有 Bose 距离 $d_B = q^i + l$. 进一步, 码 $\mathcal{C}_{(n,q,m,q^i+l)}$ 有参数*

$$\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m \left\lceil (q^i + l - 1)\left(1 - \frac{1}{q}\right) \right\rceil, d \right],$$

其中 $d \ge q^i + l$. 特别地, 如果 $(q^i + l) \mid n$, 那么 $d = q^i + l$.

证明. 维数由定理 5.1 可知. 对 $1 \le i \le \lceil \frac{m}{2} \rceil - 1$ 且 $1 \le l \le q-1$, 令 $\delta = q^i + l$. 为了证明 Bose 距离等于 δ, 只需说明 δ 是一个陪集代表元. 注意到

$$\overline{\delta} = (\underbrace{0, \ldots, 0}_{m-i-1}, 1, \underbrace{0, \ldots, 0}_{i-1}, l).$$

我们将通过分析 $\overline{\delta}$ 证明 δ 是一个陪集代表元. 直接计算表明对 $1 \le i \le m-2$, $\overline{q^i\delta} > \overline{\delta}$. 此外,

$$\overline{q^{m-1}\delta} = \begin{cases} (1, \underbrace{0, \ldots, 0}_{m-i-1}, 1, \underbrace{0, \ldots, 0}_{i-1}) & \text{如果 } l = 1, \\ (0, \underbrace{q-l, \ldots, q-l}_{m-i-1}, q-l+1, \underbrace{q-l, \ldots, q-l}_{i-2}, q-l+1) & \text{如果 } 2 \le l \le q-1, \end{cases}$$

蕴含了 $\overline{q^{m-1}\delta} > \overline{\delta}$. 因此, δ 是一个陪集代表元模 n. 此外, 如果 $(q^i + l) \mid n$, 由引理 5.8, 我们有 $d = q^i + l$. □

例 5.10: 令 $(q,m)=(3,3)$. 码 $\mathcal{C}_{(n,q,m,q+1)}$ 有参数 $[13,7,4]$. 数据库中最优线性码有参数 $[13,7,5]$, 这个码不是循环码.

例 5.11: 令 $(q,m)=(3,4)$. 码 $\mathcal{C}_{(n,q,m,q+1)}$ 有参数 $[40,32,4]$, 是最优的三元循环码 (306 页[93]). 数据库中最优线性码有参数 $[40,32,5]$, 这个码不是循环码.

例 5.12: 令 $(q,m)=(3,4)$. 码 $\mathcal{C}_{(n,q,m,q+2)}$ 有参数 $[40,28,5]$. 数据库中最优线性码有参数 $[40,28,6]$, 这个码不是循环码.

例 5.13: 令 $(q,m)=(3,5)$. 码 $\mathcal{C}_{(n,q,m,q+2)}$ 有参数 $[121,106,6]$. 数据库中最优线性码有同样参数, 但不是循环码.

由定理 5.11 和数值实验, 我们有以下猜想.

猜想: 码 $\mathcal{C}_{(n,q,m,q+1)}$ 有极小距离 $d=q+1$.

注意定理 5.11 说明猜想是对的当 m 是偶数.

5.1.6 总结

尽管 BCH 码在每本关于编码理论的书中都有介绍, 文献中仅有不多的已知的结果 (见文献[9,10,50,51,94]). 一般地, 确定一个 BCH 码的维数是困难的, 确定极小距离则更难.

已知的关于 BCH 码的结果几乎都考虑本原的长度 $n=q^m-1$. 据我们所知, 文献中只有很少的文章考虑了非本原长度的 BCH 码. 这是因为处理非本原长度的 BCH 码更加困难. 本节首先研究了长为 $n=(q^m-1)/(q-1)$ 的狭义射影 BCH 码, 做出了以下贡献:

- 确定了一些大维数狭义射影 BCH 码的参数.
- 确定了一些三元小维数狭义射影 BCH 码的参数. 特别地, 我们确定了三元 BCH 码 $\mathcal{C}_{(n,q,m,\delta_1)}$, $\tilde{\mathcal{C}}_{(n,q,m,\delta_1)}$, $\mathcal{C}_{(n,q,m,\delta_2)}$ 和 $\tilde{\mathcal{C}}_{(n,q,m,\delta_2)}$ 的重量分布.
- 确定了有某些特殊设计距离的狭义射影 BCH 码的参数.

本节开启了对狭义射影 BCH 码的研究. 回顾狭义本原 BCH 码包含很多好的

码[93,94], 如许多例子所示, 狭义射影 BCH 码也包含了很多最优的线性码. 这为我们提供了强大的动因去进一步研究狭义射影 BCH 码.

5.2 伪循环码和量子极大距离可分码的构造

5.2.1 引言

量子纠错码在量子计算和量子通信中有重要作用. 给定一个素数幂 q, 一个 $[[n,k,d]]_q$ 量子码是希尔伯特空间 $(\mathbb{C}^q)^{\otimes n}$ 中一个极小距离为 d 的 q^k 维子空间, 满足能够探测到 $d-1$ 个量子错误并纠正 $\lfloor \frac{d-1}{2} \rfloor$ 个量子错误. 量子纠错中的一个核心问题是构造具有好参数的量子码. 自从 Shor[247] 和 Steane[250] 开创性的工作以来, 利用经典的纠错码, 许多好的量子码已被构造出来 (参见文献[3,8,37,52,176,189,238,251]).

一个 $[[n,k,d]]_q$ 量子码的参数必须满足量子 Singleton 界 (见文献[176,181,232])

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

达到这个界的量子码被称为一个量子极大距离可分码. 类似于经典纠错码的情形, 量子极大距离可分码是一类最优的量子码, 它的构造在近年来受到了很大的关注 (见文献[19,56,102,120,126,148,150,157–159,164,165,167,187,189,238,277,304,305]). 构造新的量子极大距离可分码的一个非常有效的办法是利用拟循环码. 以下, 我们总结了一些由拟循环码得到的 $[[n,n-2d+2,d]]_q$ 量子极大距离可分码的参数, 其中 q 为一个素数幂:

- $n=(q^2-1)/h$ 其中

  (i). h 为偶数, $h|(q-1)$, 且 $2 \leq d \leq \frac{q+1}{2}+\frac{q-1}{h}$ (见文献[56]);

  (ii). h 为偶数, $h|(q+1)$, 且 $2 \leq d \leq \frac{q+1}{h}+\frac{q-1}{2}$ (见文献[277]);

  (iii). h 为奇数, $h|(q+1)$, 且 $2 \leq d \leq \frac{q+1}{2h}+\frac{q-1}{2}$ (见文献[277]);

- $n=(q^2+1)/h$ 其中

  (iv). $h=1$, 且 $2 \leq d \leq q+1$ (见文献[159]);

  (v). $h=2$, q 为奇数, 且 $3 \leq d \leq q$ 为奇数(见文献[164]);

  (vi). $h=5$, $q \equiv 3 \pmod{10}$, 且 $2 \leq d \leq \frac{3}{5}(q-3)+2$ 为偶数(见文献[305]);

(vii). $h=5, q\equiv 7 \pmod{10}$, 且 $2\le d\le \frac{3}{5}(q-7)+4$ 为偶数(见文献[305]).

在本节中, 我们构造以下新的量子极大距离可分码.

定理 5.12: 令 q 为一个素数幂.

(1) 存在一个 $\left[\left[\frac{q^2+1}{5}, \frac{q^2+1}{5}-2d+2, d\right]\right]_q$ 量子极大距离可分码, 对任意的 d 落在以下的范围中:

(1.1) 如果 $q\equiv 2 \pmod{10}$ 且 $q\neq 2$, 那么 $3\le d\le \frac{3}{5}(q-2)+1$ 为奇数;

(1.2) 如果 $q\equiv 8 \pmod{10}$, 那么 $3\le d\le \frac{3}{5}(q-8)+5$ 为奇数.

(2) 令 h 为 q^2-1 的一个因子. 令 $h_1=\gcd(h,q+1)$ 且 $h_2=\gcd(h,q-1)$. 则存在 $\left[\left[\frac{q^2-1}{h}, \frac{q^2-1}{h}-2d+2, d\right]\right]_q$ 量子极大距离可分码, 对任意的 d 落在以下的范围中:

(2.1) 如果 $h_1h_2=2h$, 那么 $2\le d\le \frac{q+1}{h_1}+\frac{q-1}{h_2}$;

(2.2) 如果 $h_1h_2=h$, 那么 $2\le d\le \min\left\{\frac{q-1}{h_2}, \frac{q+1}{2h_1}+\frac{q-1}{2h_2}\right\}$.

在此, 我们做出几个评论. 首先, 定理 5.12 的 (1.1) 和 (1.2) 考虑了 q 为偶数的情形, 补全了 (vi) 和 (vii). 这些结果优于 Jin 等人的存在 $[[n, n-2d+2, d]]$ 量子极大距离可分码, 其中 $4\le n\le q^2$ 且几乎所有的 d 略小于 $q/2$ 的结果 (参见定理 3.4[157]).

其次, (2.1) 和 (2.2) 包含了之前的许多结果 (见文献[56,126,150,164,165,277,304,305]). 例如, (i) 和 (ii) 是 (2.1) 和 (2.2) 的特殊情形, 其中 $h|(q-1)$ 或 $h|(q+1)$. 最近的四类构造也是 (2.1) 和 (2.2) 的特殊情况 (见情形 (3)–(6)[305]). 如果要求构造的量子极大距离可分码的极小距离 d 超过 $q/2$, 那么 (2.1) 和 (2.2) 就归结为 (i), (ii) 和 (iii).

再次, 与之前利用了拟循环码的工作相比 (见文献[56,126,150,164,165,277,304,305]), 我们对定理 5.12 的证明依赖于*伪循环码* (pseudo-cyclic codes) 的理论 (见文献[228] 8.10 节). 粗略地讲, 伪循环码自然推广了拟循环码, 提供了更多的灵活性，以及对这些新构造的更好的理解. 仅用拟循环码的理论证明定理 5.12 是可能的. 然而, 即使如此, 受拟循环码本身的限制, 我们预计这个证明会非常复杂.

最后, 引理 70[176] (亦见推论 4[120]) 表明如果存在一个 $[[n, n-2d+2, d]]_q$ 量子极大距离可分码, 那么存在一个 $[[n-s, n-2d+2+s, d-s]]_q$ 量子极大距离可分码对任意的 $0\le s<d$. 因此新参数的量子极大距离可分码可由定理 5.12 直接得出.

在本节中, 我们将利用具备特殊性质的纠错码去构造量子极大距离可分码. 以下, 我们简要回顾由经典的极大距离可分码构造量子极大距离可分码的 Hermitian 构造.

令 q 为一个素数幂且 $\mathbb{F}_{q^2}$ 为 q^2 个元素的有限域. $\mathbb{F}_{q^2}$ 上一个长度为 n 的线性码是 $\mathbb{F}_{q^2}^n$ 的一个子空间. 它被称为一个 $[n,k,d]_{q^2}$ 量子码如果它的维数为 k 且极小汉明距离为 d. 它是一个极大距离可分码如果 $k=n-d+1$.

对任意的 $\alpha \in \mathbb{F}_{q^2}$, 定义它的共轭 $\overline{\alpha}=\alpha^q$. 对任意向量 $\mathbf{x},\mathbf{y} \in \mathbb{F}_{q^2}^n$, 其中 $\mathbf{x}=(x_1,\ldots,x_n)$ 且 $\mathbf{y}=(y_1,\ldots,y_n)$, Hermitian 内积 $\langle \mathbf{x},\mathbf{y}\rangle_H$ 定义做

$$\langle \mathbf{x},\mathbf{y}\rangle_H = \sum_{i=1}^{n} x_i \overline{y_i}.$$

对 $\mathbb{F}_{q^2}$ 上的一个线性码 $\mathcal{C}$, 它的 Hermitian 对偶码 (Hermitian dual code) $\mathcal{C}^{\perp_H}$ 定义做

$$\mathcal{C}^{\perp_H} = \left\{ \mathbf{x} \in \mathbb{F}_{q^2}^n : \langle \mathbf{x},\mathbf{y}\rangle_H = 0, \forall\, \mathbf{y} \in \mathcal{C} \right\}.$$

我们采用文献[56] 的记号, 称 $\mathcal{C}$ 是包含对偶的 (dual-containing) 如果 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$. 量子码的 Hermitian 构造 (Hermitian construction) 如下 (见文献[8]).

命题 5.1 (Hermitian 构造): 如果存在一个 $[n,k,d]_{q^2}$ 线性码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$, 那么存在一个 $[[n,2k-n,d']]_q$ 量子码满足 $d' \geq d$. 特别地, 如果 $\mathcal{C}$ 是一个 $[n,n-d+1,d]_{q^2}$ 极大距离可分码, 满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$, 那么存在一个 $[[n,n-2d+2,d]]_q$ 量子极大距离可分码.

由这个命题, $\mathbb{F}_{q^2}$ 上每个包含对偶的极大距离可分码给出 $\mathbb{F}_q$ 上一个量子极大距离可分码. 这是我们构造的出发点.

5.2.2 伪循环码

在本小节中, 我们回顾伪循环码的理论并证明一些有用的性质. 伪循环码在文献[228] 8.10 节中已被研究过, 其中证明了伪循环码事实上等价于截短的循环码. 值得一提的是, 在文献[191] 中, 伪循环码的概念被推广到Galois 环上的多循环码 (polycyclic codes).

5.2.2.1 定义和基本性质

定义 5.3: 令 $0 \neq f(x) \in \mathbb{F}_q[x]$ 为一个首一多项式. 一个主理想整环 $\mathbb{F}_q[x]/(f(x))$ 的非零理想 $\mathcal{C}$ 被称为一个伪循环码, 或一个 f-循环码.

以下, 我们用 $f(x)$ (或 f) 表示一个定义在某个合适的有限域上的首一多项式.

伪循环码自然推广了循环码, 亚循环码和拟循环码的概念. 事实上, 一个 f-循环码 $\mathcal{C}$ 是循环的如果 $f(x) = x^n - 1$, 是亚循环的如果 $f(x) = x^n + 1$, 是 λ-拟循环的如果 $f(x) = x^n - \lambda$ 对某个 $\lambda \in \mathbb{F}_q^*$. 假设 $\deg f(x) = n \geq 1$ 且 $\mathcal{C}$ 是 f-循环码. 正如循环码的情况, 以下定义的映射 φ,

$$\begin{aligned} \varphi : \mathbb{F}_q[x]/(f(x)) &\longrightarrow \mathbb{F}_q^n \\ a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} &\longrightarrow (a_0, a_1, \ldots, a_{n-1}) \end{aligned}$$

是一个 $\mathbb{F}_q$-线性空间的同构. 因而 $\mathcal{C}$ 可以被等价于像 $\varphi(\mathcal{C})$. 它是 $\mathbb{F}_q^n$ 的一个子空间, 因而是 $\mathbb{F}_q$ 上长度为 n 的一个线性码. 我们首先由以下的性质.

定理 5.13: 令 $\mathcal{C} \subset \mathbb{F}_q[x]/(f(x))$ 为一个 f-循环码, 其中 $f(x) \in \mathbb{F}_q[x]$ 且 $\deg f(x) = n \geq 1$. 存在一个多项式 $g(x) \in \mathbb{F}_q[x]$ 满足以下性质.

(i) $g(x) \in \mathbb{F}_q[x]$ 是 $\mathcal{C}$中唯一的首一且次数最小的多项式,

(ii) $\mathcal{C} = \langle g(x) \rangle$,

(iii) $g(x) \mid f(x)$.

令$k = n - \deg g(x)$, 其中 $g(x) = \sum_{i=0}^{n-k} g_i x^i$ 满足 $g_{n-k} = 1$. 那么

(iv) $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$ 且 $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ 是 $\mathcal{C}$ 的一组 $\mathbb{F}_q$-基,

(v) $\mathcal{C}$ 的每个元素可以唯一表示为一个乘积 $g(x)a(x)$, 其中 $a(x) \in \mathbb{F}_q[x]$ 满足 $a(x) = 0$ 或 $\deg a(x) < k$.

证明. 由于 $\mathbb{F}_q[x]/(f(x))$ 是一个主理想整环, 定理 5.13 的证明与循环码的情形几乎完全一致 (参见文献[151] 定理 4.2.1). □

对一个 f-循环码 $\mathcal{C}$, $g(x)$ 被称为 $\mathcal{C}$ 的生成矩阵, 其中 $g(x)$ 是 $f(x)$ 的一个首一因子且 $\mathcal{C}=\langle g(x)\rangle$. 用 $Z(g)$ 记 g 的零点组成的集合, 即,

$$Z(g):=\{a\in F:g(a)=0\},$$

其中 F 作为 $\mathbb{F}_q$ 的扩张是 $g(x)$ 的一个分裂域. 如果 f 给定, 那么任意 f-循环码 $\mathcal{C}$ 由它的生成多项式 g 唯一决定, 并本质上由 $Z(g)$ 唯一决定. 现在我们阐述关于 $\mathcal{C}$ 的极小距离的一个 BCH 型下界.

5.2.3 BCH 型下界

回顾一个截短的循环码的极小距离不会小于原始码的极小距离 (文献[228] 241 页). 以下的 BCH 型下界是这一观察的直接推论.

定理 5.14 (BCH 型下界): 令 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上一个生成多项式为 $g(x)$ 的 f-循环码, 其中 $f\in\mathbb{F}_q[x]$ 没有重根且 $\deg f(x)=n\geq 1$. 假设 $f(x)\mid(x^N-1)$ 对某个整数 N 满足 $\gcd(N,q)=1$ 成立. 令 θ 为 $\mathbb{F}_q$ 的某个扩域中的一个 N 阶的本原元. 假设有整数 a,b,d 使得 $\left\{\theta^{a+bi}:0\leq i\leq d-2\right\}\subseteq Z(g)$ 且 $\frac{N}{\gcd(b,N)}\geq n\geq d-1$. 那么 $\mathcal{C}$ 的极小距离至少是 d.

作为一个直接的结果, 我们可以由某些f-循环码得到极大距离可分码.

推论 5.1: 在定理 5.14 的假设下, 如果我们有 $Z(g)=\left\{\theta^{a+bi}:0\leq i\leq d-2\right\}$ 且 $\frac{N}{\gcd(b,N)}\geq n\geq d-1$, 那么 $\mathcal{C}$ 是一个 $[n,n-d+1,d]_q$ 极大距离可分码.

5.2.3.1 对偶码和 Hermitian 对偶码

在本小节中, 我们考虑伪循环码的对偶码和 Hermitian 对偶码.

定理 5.15: 令 $\mathcal{C}$ 为 $\mathbb{F}_q$ 上一个 f-循环码, 其中 $g(x)$ 为生成多项式, $f\in\mathbb{F}_q[x]$ 是一个首一的无重根的多项式且 $\deg f=n\geq 1$. 假设 $g(x)=\prod_{i=1}^{b}p_i(x)$ 为 $g(x)$ 分解为不可约多项式 $p_i(x)\in\mathbb{F}_q[x]$ 的乘积. 对 $1\leq i\leq b$, 令 α_i 为 $p_i(x)$ 的一个根, 令 $\mathbb{F}_{q^{t_i}}$ 为 $p_i(x)$ 的

分裂域. 令 $\mathbb{F}_{q^t}$ 为 $g(x)$ 的分裂域. 那么对偶码 $\mathcal{C}^{\perp}$ 为

$$\mathcal{C}^{\perp}=\left\{(c_0,\ldots,c_{n-1}):c_k=\left(\sum_{i=1}^{b}\mathrm{Tr}_q^{q^{t_i}}(\beta_i\alpha_i^k)\right),\right.$$
$$\left.0\le k\le n-1,\forall\ \beta_i\in\mathbb{F}_{q^{t_i}},1\le i\le b\right\}.$$

此处 $\mathrm{Tr}_q^{q^{t_i}}$ 为标准的从 $\mathbb{F}_{q^{t_i}}$ 到 $\mathbb{F}_q$ 的迹函数.

证明. 定义

$$C^{\perp}=\left\{(c_0,\ldots,c_{n-1}):c_k=\sum_{i=1}^{b}\beta_i\alpha_i^k,\right.$$
$$\left.0\le k\le n-1,\forall\ \beta_1,\ldots,\beta_b\in\mathbb{F}_{q^t}\right\}.$$

这是一个 $\mathbb{F}_{q^t}$ 上的线性码. 易知 $C^{\perp}$ 的对偶码为

$$C=\left\{(a_0,\ldots,a_{n-1})\in\mathbb{F}_{q_t}^n:\sum_{k=0}^{n-1}a_k\alpha_j^k=0,\forall\ 1\le j\le b\right\}.$$

$a(x)=\sum_{k=0}^{n-1}a_kx^k\in\mathcal{C}$ 当且仅当存在 $c(x)\in\mathbb{F}_q[x]$ 满足 $c(x)=0$ 或 $\deg c(x)<n-\deg g(x)$, 使得 $a(x)=c(x)g(x)$. 因而, $\mathcal{C}$ 是 C 在 $\mathbb{F}_q$ 上子域子码, 即, $\mathcal{C}=C|_{\mathbb{F}_q}$. 由 Delsarte 定理[72], 易得结论. □

现在我们描述伪循环码的 Hermitian 对偶码.

定理 5.16: 令 $\mathcal{C}$ 为一个 $\mathbb{F}_{q^2}$ 上的 f-循环码其中 $g(x)$ 为生成多项式, $f\in\mathbb{F}_{q^2}[x]$ 是首一无重根的多项式且 $\deg f=n\ge 1$. 假设 $g(x)=\prod_{i=1}^{b}p_i(x)$ 是 $g(x)$ 分解为不可约多项式 $p_i(x)\in\mathbb{F}_{q^2}[x]$ 的分解. 对 $1\le i\le b$, 令 α_i 为 $p_i(x)$ 的一个根, $\mathbb{F}_{q^{2t_i}}$ 为 $p_i(x)$ 的分裂域. 那么 Hermitian 对偶码 $\mathcal{C}^{\perp_H}$ 为

$$\mathcal{C}^{\perp_H}=\left\{(c_0,\ldots,c_{n-1}):c_k=\left(\sum_{i=1}^{b}\mathrm{Tr}_{q^2}^{q^{2t_i}}(\beta_i\bar{\alpha_i}^k)\right),\right.$$
$$\left.0\le k\le n-1,\forall\ \beta_i\in\mathbb{F}_{q^{2t_i}},1\le i\le b\right\}.$$

此处 $\alpha_i \in \mathbb{F}_q^{2t_i}$, 且 $\bar{\alpha}_i := \alpha_i^q$.

证明. 证明类似定理 5.15 的证明, 故省略. □

5.2.4 包含对偶码的极大距离可分码的判断准则

我们现在描述两个含对偶码的极大距离可分码的判断准则. 这些准则对定理 5.12 的证明起关键作用.

定理 5.17: 令 $f \in \mathbb{F}_{q^2}[x]$ 为一个多项式, $\deg f = n \geq 1$ 且 $f(x) \mid \left(x^{q^2-1} - 1\right)$. 令 θ 为 $\mathbb{F}_{q^2}$ 的一个本原元. 令 $g(x) = \prod_{i=d_1}^{d_2}(x - \alpha_i)$, 其中 $\alpha_i = \theta^{a+bi}$, d_1, d_2, a, b 是一些给定的整数. 假设 $g(x)|f(x)$. 令 $\mathcal{C}$ 为一个 $\mathbb{F}_{q^2}$ 上的 f-循环码且生成多项式为 g. 如果

$$\frac{q^2-1}{\gcd(b, q^2-1)} \geq n \geq d_2 - d_1 + 1 \geq 1, \tag{5.13}$$

且下列条件对任意的 i, j 满足 $d_1 \leq i \leq j \leq d_2$ 都成立:

$$\begin{cases} (q+1)a + b(qi+j) & \not\equiv & 0 \pmod{q^2-1}, \\ ((q+1)a + b(qi+j))n & \equiv & 0 \pmod{q^2-1}, \end{cases} \tag{5.14}$$

那么 $\mathcal{C}$ 是一个 $[n, n-d_2+d_1-1, d_2-d_1+2]_{q^2}$ 极大距离可分码满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$.

证明. 由推论 5.1, $\mathcal{C}$ 是一个 $[n, n-d_2+d_1-1, d_2-d_1+2]_{q^2}$ 极大距离可分码. 我们只需证明 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$. 由定理 5.16, 我们有

$$\mathcal{C}^{\perp_H} = \left\{ \left(\sum_{i=d_1}^{d_2} \beta_i \bar{\alpha}_i^k \right)_{k=0}^{n-1} : \forall\, \beta_{d_1}, \ldots, \beta_{d_2} \in \mathbb{F}_{q^2} \right\}.$$

因而 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$ 等价于

$$g(x) \mid \sum_{k=0}^{n-1} \left(\sum_{i=d_1}^{d_2} \beta_i \bar{\alpha}_i^k \right) x^k, \forall\, \beta_{d_1}, \ldots, \beta_{d_2} \in \mathbb{F}_{q^2}.$$

亦即,

$$0 = \sum_{k=0}^{n-1} \sum_{i=d_1}^{d_2} \beta_i \bar{\alpha}_i^k \alpha_j^k = \sum_{i=d_1}^{d_2} \beta_i \sum_{k=0}^{n-1} (\bar{\alpha}_i \alpha_j)^k,$$

$$\forall\ \beta_{d_1},\ldots,\beta_{d_2}\in\mathbb{F}_{q^2},\forall\ d_1\le j\le d_2.$$

这等价于

$$\sum_{k=0}^{n-1}(\bar{\alpha}_i\alpha_j)^k=0,\forall\ d_1\le i,j\le d_2.$$

这就是说

$$\sum_{k=0}^{n-1}(\bar{\alpha}_i\alpha_j)^k=0,\forall\ d_1\le i\le j\le d_2.$$

利用 $\alpha_i=\theta^{a+bi}$, 我们得到

$$\mathcal{C}^{\perp_H}\subseteq\mathcal{C}\Longleftrightarrow\sum_{k=0}^{n-1}\theta^{((q+1)a+b(qi+j))k}=0,\forall\ d_1\le i\le j\le d_2.$$

右边是一个几何级数, 它的和数是零如果

$$\theta^{(q+1)a+b(qi+j)}\neq 1,\quad \theta^{((q+1)a+b(qi+j))n}=1.$$

这等价于条件

$$\begin{aligned}(q+1)a+b(qi+j)&\not\equiv 0 \mod q^2-1,\forall d_1\le i\le j\le d_2,\\ ((q+1)a+b(qi+j))n&\equiv 0 \mod q^2-1,\forall d_1\le i\le j\le d_2.\end{aligned}$$

□

定理 5.18: 令 $f\in\mathbb{F}_{q^2}[x]$ 为一个多项式, $\deg f=n\ge 1$ 且 $f(x)\mid\left(x^{q^4-1}-1\right)$. 令 θ 为 $\mathbb{F}_{q^4}$ 的一个本原元. 令 $g(x)=\prod_{i=d_1}^{d_2}(x-\alpha_i)$, 其中 $\alpha_i=\theta^{a+bi}$, 且 d_1,d_2,a,b 是一些给定的整数. 假设 $g(x)|f(x)$.

(i) $g\in\mathbb{F}_{q^2}[x]$ 当且仅当对任意的 i 满足 $d_1\le i\le d_2$, 存在一个 j 满足 $d_1\le j\le d_2$ 使得

$$q^2(a+bi)\equiv a+bj \pmod{q^4-1}. \tag{5.15}$$

(ii) 假设 $g \in \mathbb{F}_{q^2}[x]$. 令 $\mathcal{C}$ 为一个 $\mathbb{F}_{q^2}$上的 f-循环码, 其中生成多项式为 g. 如果

$$\frac{q^4-1}{\gcd(b, q^4-1)} \geq n \geq d_2 - d_1 + 1 \geq 1, \tag{5.16}$$

且下列条件对任意的 i, j 满足 $d_1 \leq i \leq j \leq d_2$ 都成立:

$$\begin{cases} (q+1)a + b(qi+j) & \not\equiv & 0 \pmod{q^4-1}, \\ (q^3+1)a + b(q^3 i+j) & \not\equiv & 0 \pmod{q^4-1}, \\ ((q+1)a + b(qi+j))n & \equiv & 0 \pmod{q^4-1}, \\ ((q^3+1)a + b(q^3 i+j))n & \equiv & 0 \pmod{q^4-1}, \end{cases} \tag{5.17}$$

那么 $\mathcal{C}$ 是一个 $[n, n-d_2+d_1-1, d_2-d_1+2]_{q^2}$ 极大距离可分码满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$.

证明. (i) 是容易的. 对于 (ii), 由推论 5.1, $\mathcal{C}$ 是一个 $[n, n-d_2+d_1-1, d_2-d_1+2]_{q^2}$ 极大距离可分码. 我们只需证明 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$. 由定理 5.16, 我们有

$$\mathcal{C}^{\perp_H} = \left\{ \left(\sum_{i=d_1}^{d_2} \beta_i \alpha_i^{qk} + \beta_i^{q^2} \alpha_i^{q^3 k} \right)_{k=0}^{n-1} : \forall\, \beta_{d_1}, \ldots, \beta_{d_2} \in \mathbb{F}_{q^4} \right\}.$$

因而 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$ 等价于

$$g(x) \mid \sum_{k=0}^{n-1} \left(\sum_{i=d_1}^{d_2} \beta_i \alpha_i^{qk} + \beta_i^{q^2} \alpha_i^{q^3 k} \right) x^k,$$
$$\forall\, \beta_{d_1}, \ldots, \beta_{d_2} \in \mathbb{F}_{q^4}.$$

亦即,

$$\sum_{k=0}^{n-1} \left(\sum_{i=d_1}^{d_2} \beta_i \alpha_i^{qk} + \beta_i^{q^2} \alpha_i^{q^3 k} \right) \alpha_j^k = 0, \tag{5.18}$$
$$\forall\, \beta_{d_1}, \ldots, \beta_{d_2} \in \mathbb{F}_{q^4}, \forall\, d_1 \leq j \leq d_2.$$

令 $\left\{\epsilon, \epsilon^{q^2}\right\}$ 为 $\mathbb{F}_{q^4}$ 在 $\mathbb{F}_{q^2}$ 上的一组基, 记 $\beta_i = u_i\epsilon + v_i\epsilon^{q^2}$ 对 $u_i, v_i \in \mathbb{F}_{q^2}$. 那么 $\beta_i^{q^2} = u_i\epsilon^{q^2} + v_i\epsilon$. 由于 (5.18) 对任意 $u_i, v_i \in \mathbb{F}_{q^2}$ 成立, 我们得到

$$\sum_{k=0}^{n-1} (\alpha_i^q \alpha_j)^k = 0, \forall\, d_1 \leq i, j \leq d_2,$$
$$\sum_{k=0}^{n-1} (\alpha_i^{q^3} \alpha_j)^k = 0, \forall\, d_1 \leq i, j \leq d_2.$$

由于 $\alpha_i = \theta^{a+bi}$ 且 $\theta^{q^4-1} = 1$, 易知上式在 (5.17) 满足时成立. □

我们指出定理 5.17 和定理 5.18 与判定 $\mathbb{F}_{q^2}$ 上的一个拟循环码是否包含对偶码的条件是一致的 (见文献[167] 引理 2.2). 例如, 当 $\mathcal{C}$ 是一个 λ-拟循环码对某个 $\lambda \in \mathbb{F}_{q^2}^*$, 即 $f(x) = x^n - \lambda$, 定理 5.17 的 (5.13) 和 (5.14) 分别归结为文献[56] 引理 2.7 和引理 3.3 (亦见文献[165] 定理 2.1 和引理 2.2). 定理 5.17 和定理 5.18 解释了我们构造量子极大距离可分码的策略. 对给定的长的 n 和字母表大小 q^2, 我们寻找整数 a, b, d_1, d_2 使得定理 5.17 的 (5.13)–(5.14) 或定理 5.18 的 (5.15)–(5.17) 满足. 我们同时尝试令 $d := d_2 - d_1 + 2$ 尽可能的大. 相较于拟循环码, 利用伪循环码的优势在于整个构造的数学机理更易理解且更具灵活度.

5.2.5 主要结果

5.2.5.1 定理 5.12 (2.1) 和 (2.2) 的证明

在本小节中我们应用定理 5.17 构造 $\mathbb{F}_{q^2}$ 上包含对偶的极大距离可分码. 以下将要证明的命题 5.1 和定理 5.19, 直接蕴含了定理 5.12 (2.1) 和 (2.2). 给定一个整数 v, 一个素数 p 和一个非负整数 a, 记号 $p^a \| v$ 表示 $p^a \mid v$ 且 $p^{a+1} \nmid v$.

定理 5.19: 令 q 为一个素数幂且 h 为 q^2-1 的一个因子. 定义

$$h_1' = \gcd(h, q+1),\ h_2' = \gcd(h, q-1),\ n = \frac{q^2-1}{h}.$$

那么我们总有 $h_1'h_2' = h$ 或 $h_1'h_2' = 2h$.

(i) 如果 $h_1'h_2' = 2h$, 那么我们有一个 $[n, n-d+1, d]_{q^2}$ 极大距离可分码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$ 且 d 满足 $2 \le d \le \frac{q+1}{h_1'} + \frac{q-1}{h_2'}$.

(ii) 如果 $h_1'h_2' = h$, 那么我们有一个 $[n, n-d+1, d]_{q^2}$ 极大距离可分码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$ 且 d 满足 $2 \le d \le \min\left\{\frac{q-1}{h_2'}, \frac{q+1}{2h_1'} + \frac{q-1}{2h_2'}\right\}$.

证明. 记 $h_1' = 2^r h_1, h_2' = 2^s h_2, h = 2^\tau h_1 h_2$, 其中 h_1, h_2 为奇数且整数 r, s, τ 是非负的. 易知 $r + s \ge \tau \ge \max\{r, s\}$ 且 $\min\{r, s\} \le 1$. 由定理 5.17, 我们需要找到 d_1, d_2 对任意

i, j 满足 $d_1 \le i \le j \le d_2$, 以下两个等式成立:

$$(q+1)a + b(qi+j) \not\equiv 0 \pmod{q^2-1}, \tag{5.19}$$

$$(q+1)a + b(qi+j) \equiv 0 \pmod{h}, \tag{5.20}$$

令 $b = h$ 且 $a = 2^{\tau-r}h_2a_0$, 其中 a_0 是一个之后将被确定的整数, 那么 (5.20) 对任意 i, j 成立. 因而我们只需考虑 (5.19). 假设

$$(q+1)a + h(qi+j) \equiv 0 \pmod{q^2-1} \tag{5.21}$$

对 $i \le j$ 成立. 两边同时模 $q+1$ 得

$$h(j-i) \equiv 0 \pmod{q+1}.$$

这导出了

$$j = i + u\frac{q+1}{2^r h_1} \tag{5.22}$$

对某个整数 $u \ge 0$. 将 j 代入 (5.21), 我们得到

$$2^\tau h_1 i + 2^{\tau-r}(a_0+u) \equiv 0 \pmod{\frac{q-1}{h_2}}. \tag{5.23}$$

我们将分别研究情形 (i) 和 (ii).

对情形 (i), $\tau = r+s-1$, 那么 q 是奇数且 h 是偶数. 我们取 $a_0 = 1$. (5.23) 两边同时除以 2^s 得

$$2^{r-1}h_1 i + \frac{1+u}{2} \equiv 0 \pmod{\frac{q-1}{2^s h_2}}.$$

显然 $u \equiv 1 \pmod 2$. 利用 $2^{r-1}h_1\frac{q+1}{2^r h_1} = \frac{q+1}{2} \equiv 1 \pmod{\frac{q-1}{2^s h_2}}$, 我们有 $i \equiv -\frac{1+u}{2}\frac{q+1}{2^r h_1} \pmod{\frac{q-1}{2^s h_2}}$. 因而, 从 (5.22) 我们得到

$$\begin{cases} i = -\frac{u+1}{2}\frac{q+1}{2^r h_1} + v\frac{q-1}{2^s h_2}, \\ j = \frac{u-1}{2}\frac{q+1}{2^r h_1} + v\frac{q-1}{2^s h_2}, \end{cases} \tag{5.24}$$

其中 v,u 满足 $u\geq 0$ 和 $u\equiv 1 \pmod 2$ 的整数.

令 v_0 为最小的正整数使得 $v_0\frac{q-1}{2^s h_2}\geq \frac{q+1}{2^r h_1}$ 且我们定义

$$\begin{cases} d_1=-\frac{q+1}{2^r h_1}+v_0\frac{q-1}{2^s h_2}+1,\\ d_2=(v_0+1)\frac{q-1}{2^s h_2}-1. \end{cases}$$

我们断言没有没有形如 (5.24) 的 (i,j) 对, 其中 $d_1\leq i\leq j\leq d_2$. 若不然, 由于 $u\geq 1$ 且 $i=-\frac{1+u}{2}\frac{q+1}{2^r h_1}+v\frac{q-1}{2^s h_2}\geq d_1$, 我们必然有 $v\geq v_0+1$. 然而, 相应的 j 满足 $j=\frac{u-1}{2}\frac{q+1}{2^r h_1}+v\frac{q-1}{2^s h_2}\geq (v_0+1)\frac{q-1}{2^s h_2}>d_2$, 导出矛盾. 这说明 (5.19) 对满足 $d_1\leq i\leq j\leq d_2$ 的 i,j 成立. 注意到 $d_2-d_1+2=\frac{q+1}{2^r h_1}+\frac{q-1}{2^s h_2}$. 由定理 5.17, 我们可以构造一个 $[n,n-d+1,d]_{q^2}$ 极大距离可分码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H}\subseteq\mathcal{C}$ 且 $2\leq d\leq \frac{q+1}{h_1'}+\frac{q-1}{h_2'}$.

对情形 (ii), h 可能为奇或偶. 我们选取 $a_0=0$. 我们首先考虑 h 为奇数的情形, 那么 $\tau=r=s=0$. 从 (5.23) 我们有

$$h_1 i+u\equiv 0 \pmod{\frac{q-1}{h_2}}. \tag{5.25}$$

由于 $q+1\equiv 2 \pmod{q-1}$, 我们有 $2i\equiv -u\frac{q+1}{h_1} \pmod{\frac{q-1}{h_2}}$. 因而 $i=-u\frac{q+1}{2h_1}+v\frac{q-1}{2h_2}$ 对某个整数 v 成立. 将 i 代入 (5.25) 得 $u\equiv v \pmod 2$. 因而从 (5.22) 我们得

$$\begin{cases} i=-u\frac{q+1}{2h_1}+v\frac{q-1}{2h_2},\\ j=u\frac{q+1}{2h_1}+v\frac{q-1}{2h_2}, \end{cases} \tag{5.26}$$

其中 u,v 是满足 $u\geq 0$ 和 $u\equiv v \pmod 2$ 的整数.

其次, 如果 h 为偶数, 那么 q 是奇数, 我们有 $\tau=r+s$ 且 $\min\{r,s\}=1$. 如果 $q\equiv 3 \pmod 4$, 那么 $s=1$, $\tau=r+1$ 蕴含 $2^r\|(q+1)$. 如果 $q\equiv 1 \pmod 4$, 那么 $r=1$ 且 $\tau=s+1$ 蕴含了 $2^s\|(q-1)$. 在这两种情况下我们有 $2^s\|(q-1)$ 且 $2^r\|(q+1)$. (5.23) 两边同时除以 2^s 得

$$2^r h_1 i+u\equiv 0 \pmod{\frac{q-1}{2^s h_2}}. \tag{5.27}$$

利用 $q+1\equiv 2 \pmod{q-1}$ 我们有 $i=-u\frac{q+1}{2^{r+1}h_1}+v\frac{q-1}{2^{s+1}h_2}$ 对某个整数 v 成立. 将 i 代

入 (5.27) 得 $u \equiv v \pmod 2$. 由 (5.22) 我们有

$$\begin{cases} i = -u\frac{q+1}{2^{r+1}h_1} + v\frac{q-1}{2^{s+1}h_2}, \\ j = u\frac{q+1}{2^{r+1}h_1} + v\frac{q-1}{2^{s+1}h_2}, \end{cases} \tag{5.28}$$

其中 u, v 是满足 $u \geq 0$ 和 $u \equiv v \pmod 2$ 的整数.

易知 (5.26) 和 (5.28) 可被总结为

$$\begin{cases} i = -u\frac{q+1}{2h_1'} + v\frac{q-1}{2h_2'}, \\ j = u\frac{q+1}{2h_1'} + v\frac{q-1}{2h_2'}, \end{cases} \tag{5.29}$$

其中 u, v 是满足 $u \geq 0$ 和 $u \equiv v \pmod 2$ 的整数.

令 v_0 为最小的正整数使得 $v_0\frac{q-1}{2h_2'} \geq \frac{q+1}{2h_1'}$ 且 $v_0 \equiv 1 \pmod 2$. 定义

$$\begin{cases} d_1 = 1, \\ d_2 = \min\left\{\frac{q-1}{h_2'}, \frac{q+1}{2h_1'} + v_0\frac{q-1}{2h_2'}\right\} - 1. \end{cases}$$

我们断言形如 (5.29) 的 (i, j) 对不存在, 其中 $d_1 \leq i \leq j \leq d_2$. 若不然, 如果 $u = 0$, 由于 $i = j = v\frac{q-1}{2h_2'} \geq d_1 = 1$ 且 $v \equiv 0 \pmod 2$, 我们必有 $v \geq 2$, 那么 $j = v\frac{q-1}{2h_2'} > d_2$. 如果 $u \geq 1$, 由于 $i \geq d_1$, 我们必有 $v \geq v_0$. 因而, 相应的 j 满足 $j = u\frac{q+1}{2h_1'} + v\frac{q-1}{2h_2'} \geq \frac{q+1}{2h_1'} + v_0\frac{q-1}{2h_2'} > d_2$, 导出矛盾. 这说明 (5.19) 对满足 $d_1 \leq i \leq j \leq d_2$ 的 i, j 成立. 因而 $d_2 - d_1 + 2 = \min\left\{\frac{q-1}{h_2'}, \frac{q+1}{2h_1'} + v_0\frac{q-1}{2h_2'}\right\}$ 且

$$\min\left\{\frac{q-1}{h_2'}, \frac{q+1}{2h_1'} + v_0\frac{q-1}{2h_2'}\right\} = \begin{cases} \frac{q+1}{2h_1'} + \frac{q-1}{2h_2'} & \text{如果 } h_1' > h_2', \\ \frac{q-1}{h_2'} & \text{如果 } h_1' < h_2'. \end{cases}$$

□

5.2.5.2 定理 5.12 (1.1) 和 (1.2) 的证明

在本小节中我们利用定理 5.18 构造 $\mathbb{F}_{q^2}$ 上包含对偶码的极大距离可分码. 这个结

果连同命题 5.1, 直接蕴含了定理 5.12 (1.1) 和 (1.2). 为了理清证明的思路, 我们首先考虑以下一般的情形.

在定理 5.18 的条件下, 我们取

$$n = \frac{q^2+1}{h}, \quad a = h(q-1)a_0, \quad b = h(q^2-1),$$

其中 h 是 q^2+1 的一个因子且 a_0 是一个整数. 因而, (5.15) 蕴含对任意的 i ($d_1 \le i \le d_2$), 存在一个 j ($d_1 \le j \le d_2$) 使得

$$i + j \equiv (q-1)a_0 \pmod{\frac{q^2+1}{h}}.$$

易知此式在下列条件下成立

$$d_1 + d_2 \equiv (q-1)a_0 \pmod{\frac{q^2+1}{h}}. \tag{5.30}$$

易知 (5.17) 的最后两个条件总是成立. 进一步, (5.17) 的前两个条件彼此等价. 如果其中一个不满足, 则存在 i, j ($d_1 \le i, j \le d_2$) 使得

$$j \equiv q(a_0 + i) \pmod{\frac{q^2+1}{h}}. \tag{5.31}$$

对任意给定的 h, 我们要找到整数 d_1, d_2 和 a_0 使得 (5.16) 和 (5.30) 满足且 (5.31) 对任意的 i, j, $d_1 \le i, j \le d_2$, 都不成立.

以下我们将要证明定理 5.12 (1.1) 和 (1.2), 它是命题 5.1 和定理 5.20 的直接结果.

定理 5.20: 令 q 为一个素数幂. 定义 $n = \frac{q^2+1}{5}$.

(i) 如果 $q \equiv 2 \pmod{10}$ 且 $q \neq 2$, 那么存在一个 $[n, n-d+1, d]_{q^2}$ 极大距离可分码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$, 其中 $3 \le d \le \frac{3}{5}(q-2)+1$ 为奇数.

(ii) 如果 $q \equiv 8 \pmod{10}$, 那么存在一个 $[n, n-d+1, d]_{q^2}$ 极大距离可分码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H} \subseteq \mathcal{C}$, 其中 $3 \le d \le \frac{3}{5}(q-8)+5$ 为奇数.

证明. 假设 $q \equiv c \pmod{10}$ 其中 $c \in \{2, 8\}$. 令 δ 为一个正整数满足

$$\delta \leq \begin{cases} \frac{3(q-2)}{10} - 1, & \text{如果 } c = 2, \\ \frac{3q-4}{10} - 1, & \text{如果 } c = 8. \end{cases}$$

我们取

$$h = 5,\ a_0 = \frac{q^2 - 5q - 4}{10},\ d_1 = -\delta,\ d_2 = \delta + 1.$$

显然, (5.16) 满足. 进一步, 容易验证

$$(q-1)a_0 \equiv 1 \pmod{n}.$$

因而 (5.30) 满足. (5.31) 成为

$$j \equiv q(a_0 + i) \equiv \frac{q^2 - 5q + 6}{10} + qi \pmod{n}. \tag{5.32}$$

我们现在验证 (5.32) 没有整数解 (i, j) 满足 $i, j \in [-\delta, \delta + 1]$. 此处 $[-\delta, \delta + 1]$ 从 $-\delta$ 到 $\delta + 1$ 的闭区间.

若不然, 令 (i, j) 为 (5.32) 的一个解满足 $i, j \in [-\delta, \delta + 1]$. 我们首先考虑 $i \geq 0$ 的情形.

1) $0 \leq i \leq \delta + 1$.

情形 0: $i = 0$. 我们有 $j \equiv \frac{q^2-5q+6}{10} \pmod{n}$. 显然 $j \notin [-\delta, \delta + 1]$.

情形 1: $1 \leq i \leq \frac{1}{10}(q - c)$. 我们有

$$j \equiv \frac{q^2 - 5q + 6}{10} + qi \pmod{n}, \quad 1 \leq i \leq \frac{1}{10}(q - c).$$

容易验证对 $i = 1$, 我们有 $j = \frac{q^2-5q+6}{10} + q \cdot 1 > \delta + 1$, 且对 $i = \frac{1}{10}(q - c)$, 我们有 $j = \frac{q^2-5q+6}{10} + q \cdot \frac{1}{10}(q - c) < n - \delta$. 这蕴含了 $j \notin [-\delta, \delta + 1]$.

情形 2: $\frac{1}{10}(q - c) + 1 \leq i \leq \frac{3}{10}(q - c)$. 记 $i = \tau + \frac{1}{10}(q - c)$, 由 (5.32) 我们得到

$$j \equiv q \cdot \tau - \frac{(5 + c)q - 4}{10} \pmod{n}, \quad 1 \leq \tau \leq \frac{1}{5}(q - c).$$

容易验证对 $\tau = \frac{1}{5}(q - c)$, 我们有 $j = q \cdot \frac{1}{5}(q - c) - \frac{(5+c)q-4}{10} < n - \delta$. 如果 $c = 2$, 那

么对 $\tau=1$ 我们有 $j=q\cdot 1-\frac{(5+c)q-4}{10}>\delta+1$. 如果 $c=8$, 那么对 $\tau=1$ 我们有 $n-\delta>j=q\cdot 1-\frac{(5+c)q-4}{10}+n>\delta+1$, 且对 $\tau=2$, 我们有 $j=q\cdot 2-\frac{(5+c)q-4}{10}>\delta+1$. 这蕴含了 $j\notin[-\delta,\delta+1]$.

情形 3. 最后, 如果 $c=2, i\leq\delta+1\leq\frac{3}{5}(q-2)$. 如果 $c=8$, 由于 $\delta+1\leq\frac{3}{10}(q-8)+2$, 我们需要考虑 $i=\frac{3}{10}(q-8)+1$ 和 $i=\frac{3}{10}(q-8)+2$. 对这两种情况, 由 (5.32) 容易验证相应的 j 满足 $1+\delta<j<n-\delta$. 所以 $j\notin[-\delta,\delta+1]$. 综合以上情形, (5.32) 没有解 (i,j) 满足 $i,j\in[-\delta,\delta+1]$ 且 $0\leq i\leq\delta+1$.

现在我们考虑情形 $i<0$.

2) $-\delta\leq i\leq -1$.

注意到

$$-qa_0\equiv a_0+q\pmod{n}.$$

(5.32) 两边同时乘以 q^2, 我们得到

$$-j\equiv a_0+q-q\cdot i\pmod{n}.$$

经变量替换 $j'=-j, i'=-i$, 我们需要验证

$$j'\equiv\frac{q^2+5q-4}{10}+q\cdot i'\pmod{n}\tag{5.33}$$

没有解 (i',j') 满足 $i'\in[1,\delta]$ 且 $j'\in[-\delta-1,\delta]$. 证明类似于 $0\leq i\leq\delta+1$ 的情形, 故略去.

由于定理 5.18 的条件都满足, 我们得到了一个 $[n,n-d+1,d]_{q^2}$ 极大距离可分码 $\mathcal{C}$ 满足 $\mathcal{C}^{\perp_H}\subseteq\mathcal{C}$, 其中 d 取值

$$d=d_2-d_1+2=2\delta+3\leq\begin{cases}\frac{3}{5}(q-2)+1; \text{如果 } c=2,\\ \frac{3}{5}(q-8)+5; \text{如果 } c=8.\end{cases}$$

□

5.2.6 总结

近来, 量子极大距离可分码的构造得到了很多的关注. 利用经典的循环, 亚循环和

拟循环码，量子极大距离可分码的构造取得了很大进展. 在本文中, 我们利用伪循环码统一了之前的许多构造并得到了新的量子极大距离可分码.

5.3 利用循环和拟循环码构造极大距离可分的字符结对码

5.3.1 引言

受高密度存储方面的应用所启发,一个被称为*字符结对码*的新的编码框架被提出[43,44],用来纠正字*字符对读取信道*中发生的错误.假设我们想要从某种存储介质上读取数据. 当数据排列非常紧密而数据读取装置的精度较低时,我们能读取到的是相互之间有重复的数据字符对,而不再是单个的数据字符. 假设数据字符属于一个字母表 Σ,那么我们读取的字符对属于一个不同的字母表 $\Sigma \times \Sigma$. 为了可靠的恢复原始的数据,我们需要一个新的、能够纠正字符对读取信道中的错误的编码方案.

Cassuto 和 Blaum 奠定了字符结对码作为字符对读取信道中的纠错码的理论基础[43,44].他们提出了字符结对码的一些界和构造,以及一个译码算法. 字符结对码的构造在接下来的一系列文章中被继续研究, 包括代数构造[45,54,166] 和组合构造[54]. 同时,针对循环的字符结对码的一个有效的译码算法也被提出[294].

Chee[54] 等人提出了字符结对码的一个类 Singleton 界,进而提出了极大距离可分的字符结对码的概念.由于极大距离可分的字符结对码具有最优的纠错能力,它的构造是很有意义的. 总而言之,目前有两种构造方法.其一是利用具有恰当性质的线性码的直接构造,例如极大距离可分码[54], 循环和拟循环码[166]. 其二是利用编织[54,55], 欧拉图[54,55,166] 和其它组合构型[54,55] 的递归构造.

特别地,我们着重考虑构造小结对距离 d_p 较小的 $(n, d_p)_q$ 极大距离可分字符结对码.已知的极小结对距离 d_p 较小的 $(n, d_p)_q$ 极大距离可分字符结对码的无穷类有：

a) $q \geq 2, n \geq 2, d_p \in \{2, 3\}$[54],

b) $q \geq 2, n \geq 4, d_p = 4$[54],

c) q 为偶素数幂, $n \leq q + 2, d_p = 5$[54],

d) q 为奇素数, $5 \leq n \leq 2q + 3, d_p = 5$[54],

e) q 为素数幂, $n \mid q^2 - 1, n > q + 1, d_p = 5$[166],

f) q 为素数幂, $n = q^2 + q + 1$, $d_p = 5$[166],

g) $q \equiv 1 \pmod 3$ 为素数幂, $n = \frac{q^2+q+1}{3}$, $d_p = 5$[166],

h) q 为素数幂, $n = q^2 + 1$, $d_p = 6$[166],

i) q 为奇素数幂, $n = \frac{q^2+1}{2}$, $d_p = 6$[166],

j) q 为奇素数幂, $n = 8$, $d_p = 7$[54].

在本文中,我们借鉴 Kai 等人[166] 的思想,利用循环和拟循环码构造极大距离可分字符结对码.我们得到了以下新的 $(n, d_p)_q$ 极大距离可分字符结对码,其中 $d_p \in \{5, 6\}$. 我们用 $v_p(n)$ 记最大的整数 a, 使得 $p^a \mid n$, 其中 p 是一个素数.

1) q 为素数幂, n 和 r 是两个整数满足

$$r \mid q-1,\ nr \mid q^3-1,\ nr \nmid q-1,\ (\frac{q-1}{r}, n) = 1.$$

且$d_p = 5$,

2) q 为素数幂, n 和 r 是两个整数满足

$$nr \mid (q-1)(q^2+1),\ nr \nmid q^2-1,\ (\frac{q-1}{r}, n) = 1,$$

且$d_p = 6$,

3) q 为素数幂, $n \mid q^2 - 1$, n 为奇或 n为偶并且 $v_2(n) < v_2(q^2 - 1)$, $d_p = 6$.

我们强调类 1) (类似地, 类 2)) 是类 f) 和 g) (类似地,类 h) 和 i)) 的一个扩展. 更有趣地, 对于一类循环码, 我们找到一个保证它成为极小结对距离 $d_p = 7$ 的极大距离可分字符结对码的充要条件. 我们观察到这个条件和一类特殊的分式线性变换有关. 进一步地, 我们对这一类分式线性变换做了仔细的分析, 得出了对这个条件的精确刻画. 利用这个刻画, 我们提出了一个算法, 生成了许多极小结对距离 $d_p = 7$ 的极大距离可分字符结对码.

5.3.2 拟循环码

在本节中,我们对拟循环码做一个简要介绍.

令 q 为一个素数幂, $\mathbb{F}_q$ 为一个有限域并且 $\omega \in \mathbb{F}_q^*$. 一个 ω-拟循环码 $\mathcal{C}$ 是一个在拟循环移位下不变的线性码. 亦即, 如果

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C},$$

那么

$$(\omega c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

一个有限域 $\mathbb{F}_q$ 上的 ω-拟循环码 $\mathcal{C}$ 等价于主理想环 $\mathbb{F}_q[x]/(x^n - \omega)$ 中的一个理想. 因而, $\mathcal{C}$ 可以由一个元素生成. 存在一个唯一的首一的次数最低的多项式 $g(x) \in \mathcal{C}$, 使得 $g(x) \mid x^n - \omega$, $\mathcal{C} = \langle g(x) \rangle$. 这个多项式被称为 $\mathcal{C}$ 的生成多项式. 给定环 $\mathbb{F}_q[x]/(x^n - \omega)$ 和一个生成多项式 $g(x)$, 一个长度为 n 的 ω-拟循环码 $\mathcal{C} = \langle g(x) \rangle$ 便给定了. 它是线性空间 $\mathbb{F}_q^n$ 的一个维数为 $n - \deg(g(x))$ 的子空间. 当 $\omega = 1$, 一个 ω-拟循环码即是一个通常的循环码.

对于一个拟循环码的极小距离，作为文献[166] 中定理 3 的一个直接推广，我们有以下的 BCH 型界，

命题 5.2: 令 q 为一个素数幂, n 为一个正整数满足 $(n, q) = 1$. 令 $\omega \in \mathbb{F}_q^*$ 为一个阶为 r 的元素. 令 m 为满足 $nr \mid q^m - 1$ 的最小的正整数. 则存在 $\delta \in \mathbb{F}_{q^m}^*$, 使得 δ 的阶数为 nr 以及 $\omega = \delta^n$. 定义 $\xi = \delta^r$. 令 $\mathcal{C} = \langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n - \omega)$ 为一个长度为 n 的 ω-拟循环码. 假设生成多项式 $g(x)$ 有元素 $\{\delta \xi^{li} \mid b \leq i \leq b + d - 1\}$ 为根, 其中 b 和 l 为正整数，满足 $(l, n) = 1$. 那么 $\mathcal{C}$ 的极小距离至少为 $d + 1$.

证明. 证明与循环码经典的 BCH 界类似 (见专著[151] 的定理 4.5.3). 因此, 证明在此省略. □

5.3.3 字符结对码和极大距离可分字符结对码

令 Σ 为一个包含 q 个元素的字母表. 对于 $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \in \Sigma^n$, $\mathbf{u}$ 的字符对

读取向量定义为

$$\pi(\mathbf{u}) = ((u_0, u_1), (u_1, u_2), \ldots, (u_{n-2}, u_{n-1}), (u_{n-1}, u_0)) \in (\Sigma \times \Sigma)^n.$$

令 $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \in \Sigma^n$, $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \Sigma^n$, $\mathbf{u}$ 和 $\mathbf{v}$ 的结对距离为

$$d_P(\mathbf{u}, \mathbf{v}) = |\{0 \le i \le n-1 \mid (u_i, u_{i+1}) \ne (v_i, v_{i+1})\}|,$$

其中下标视为模 n 的整数. 一个 $(n, M, d_p)_q$ 字符结对码是一个子集合 $\mathcal{C} \subset \Sigma^n$, 满足 $|\mathcal{C}| = M$ 及$d_p = \min\{d_P(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \ne \mathbf{v}\}$. 如果 Σ 是一个有限域 $\mathbb{F}_q$, 定义 $\mathbf{u} \in \mathbb{F}_q^n$ 的结对重量为

$$w_P(\mathbf{u}) = |\{0 \le i \le n-1 \mid (u_i, u_{i+1}) \ne (0, 0)\}|,$$

其中下标视为模 n 的整数. 特别地, 如果 $(n, M, d_p)_q$ 字符结对码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的一个线性子空间, 那么 $d_p = \min\{w_P(\mathbf{u}) \mid \mathbf{u} \ne (0, 0, \ldots, 0)\}$.

令 $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ 为初始的向量. 令

$$((u'_0, u'_1), (u'_1, u'_2), \ldots, (u'_{n-2}, u'_{n-1}), (u'_{n-1}, u'_0))$$

为通过字符对读取信道接收到的向量. 那么对错误的个数定义为

$$|\{0 \le i \le n-1 \mid (u_i, u_{i+1}) \ne (u'_i, u'_{i+1})\}|$$

其中下标视为模 n 的整数. 由文献[44]的命题 3，类似于经典的纠错码, 一个 $(n, M, d_p)_q$ 字符结对码可以纠正至多 $\lfloor \frac{d_p - 1}{2} \rfloor$ 个对错误. 因此, 给定 q, n 和 M, 我们想要构造字符结对码, 使得 d_p 尽可能的大. 为此, 我们想要利用和经典纠错码相关的丰富的结果. 作为第一步, 我们需要理解字符结对码和经典纠错码之间的联系.

结对距离在文献[43,44]中首先引入, 是一个良定义的度量. 回顾 $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ 和 $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ 之间的汉明距离定义为

$$d_H(\mathbf{u}, \mathbf{v}) = |\{0 \le i \le n-1 \mid u_i \ne v_i\}|.$$

为了建立结对距离和汉明距离之间的关系，我们需要以下的定义.

定义 5.4: 令 S 为 $\{0,1,\ldots,n-1\}$ 的一个子集. S 中的元素可以看作是模 n 的整数环 $\mathbb{Z}_n$ 中的元素. S 可被划分为一系列子集的并, 使得每个子集包含 $\mathbb{Z}_n$ 在通常意义下中连续的元素. 显然, S 的子集合个数最小的划分是唯一的. 因此, 我们定义 $L(S)$ 这个唯一的划分中子集合的个数.

以下的命题揭示了距离和汉明距离之间的关系.

命题 5.3 (**命题 1和定理 2**[44]): 令 $\mathbf{u}=(u_0,u_1,\ldots,u_{n-1})\in\Sigma^n$ 和 $\mathbf{v}=(v_0,v_1,\ldots,v_{n-1})\in\Sigma^n$ 满足 $0<d_H(\mathbf{u},\mathbf{v})<n$. 定义 $S=\{0\le i\le n-1\mid u_i\neq v_i\}$. 那么

$$d_P(\mathbf{u},\mathbf{v})=d_H(\mathbf{u},\mathbf{v})+L(S).$$

因此, 我们有 $L(S)=d_P(\mathbf{u},\mathbf{v})-d_H(\mathbf{u},\mathbf{v})\le n-d_H(\mathbf{u},\mathbf{v})$. 连同 $1\le L(S)\le d_H(\mathbf{u},\mathbf{v})$, 我们有

$$d_H(\mathbf{u},\mathbf{v})+1\le d_P(\mathbf{u},\mathbf{v})\le\min\{2d_H(\mathbf{u},\mathbf{v}),n\}.$$

此外,

$$d_P(\mathbf{u},\mathbf{v})=\begin{cases}0 & \text{如果 } d_H(\mathbf{u},\mathbf{v})=0,\\ n & \text{如果 } d_H(\mathbf{u},\mathbf{v})=n.\end{cases}$$

特别地, 对于线性的字符结对码, 我们有以下的关于一个码字的汉明重量和结对重量的联系的推论.

推论 5.2: 令 $\mathcal{C}$ 为一个 $(n,M,d_p)_q$ 字符结对码, 同时也是 $\mathbb{F}_q^n$ 的一个线性子空间. 对任意 $\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})\in\mathcal{C}$, 定义

$$I(\mathbf{c})=L(\{0\le i\le n-1\mid c_i\neq 0\}).$$

假设 $0<w_H(\mathbf{c})<n$, 其中 $w_H(\mathbf{c})$ 表示 $\mathbf{c}$ 的汉明重量. 那么

$$w_P(\mathbf{c})=w_H(\mathbf{c})+I(\mathbf{c}). \tag{5.34}$$

因而, 我们有 $I(\mathbf{c}) = w_P(\mathbf{c}) - w_H(\mathbf{c}) \leq n - w_H(\mathbf{c})$. 连同 $1 \leq I(\mathbf{c}) \leq w_H(\mathbf{c})$, 我们有

$$w_H(\mathbf{c}) + 1 \leq w_P(\mathbf{c}) \leq \min\{2w_H(\mathbf{c}), n\}.$$

特别地, 如果 $\mathcal{C}$ 的极小汉明距离 $d < n$, 那么极小结对距离

$$d + 1 \leq d_p \leq \min\{2d, n\}. \tag{5.35}$$

类似于经典的纠错码, 有若干个界对字符结对码的参数提出了根本性的限制. 其中之一就是以下的类 Singleton 界.

命题 5.4 (定理 2.1[54]): 令 $q \geq 2$ 及 $2 \leq d \leq n$. 如果 $\mathcal{C}$ 是一个 $(n, M, d_p)_q$ 字符结对码, 那么 $M \leq q^{n-d_p+2}$.

达到类 Singleton 界的字符结对码 $\mathcal{C}$ 被称为极大距离可分字符结对码. 我们把它记为一个 $(n, d_p)_q$ 极大距离可分字符结对码. 以下, 我们着重考虑极大距离可分字符结对码的构造. 事实上, 经典的极大距离可分码直接生成了极大距离可分字符结对码.

命题 5.5 (命题 3.1[54]): 如果 $\mathcal{C}$ 是一个极大距离可分码, 那么 $\mathcal{C}$ 是一个极大距离可分字符结对码. 进一步地, 如果 $\mathcal{C}$ 是一个 $[n, n-d+1, d]_q$ 极大距离可分码满足 $d < n$, 那么 $\mathcal{C}$ 是一个 $(n, d+1)_q$ 极大距离可分字符结对码.

由经典的极大距离可分码的知识, 以上命题说明对任意的素数幂 q, 满足 $2 \leq d_p \leq n \leq q+1$ 的 $(n, d_p)_q$ 极大距离可分字符结对码是已知的. 因此, 以下我们将在 q 为素数幂且 $n > q+1$ 的条件下考虑 $(n, d_p)_q$ 极大距离可分字符结对码的构造.

我们注意到如果 $\mathcal{C}$ 是一个拟循环码且不是极大距离可分的, 那么 (5.35) 中的下界可以改进.

命题 5.6: 令 $\mathcal{C}$ 为一个 $[n, k, d]_q$ 拟循环码, 满足生成多项式为 $g(x)$ 及 $d \leq n - k$. 令 $c(x) \in \mathcal{C}$ 为一个汉明重量为 $d' \leq n - k$ 的码字. 那么 $I(c(x)) \geq 2$ 及 $w_P(c(x)) \geq d' + 2$. 特别地, $\mathcal{C}$ 是一个 $(n, q^k, d_p)_q$ 字符结对码, 其中 $d_p \geq d + 2$.

证明. 只需证明 $I(c(x)) \geq 2$, 由 (5.34), 这蕴含了 $w_P(c(x)) \geq d' + 2$. 若不然, 则必有 $I(c(x)) = 1$. 这蕴含了 $c(x)$ 中非零元素所在的指数形成一个连续的子集合. 不

失一般性, 我们可以假设 $c(x) = \sum_{i=0}^{d'-1} c_i x^i$, 其中对每个 $0 \le i \le d'-1$, $c_i \in \mathbb{F}_q^*$. 注意到 $g(x) \mid c(x)$. 由于 $\deg(g(x)) = n-k \ge d' > \deg(c(x))$, 矛盾. 因此, 我们有 $w_P(c(x)) \ge d'+2$. 特别地, 由于 $\mathcal{C}$ 是一个线性码, $\mathcal{C}$ 的极小结对距离等于它的极小非零结对重量. 由于 $d \le n-k$, 由推论 5.2 易得 $d_p \ge d+2$. □

这个命题是文献[166] 中构造的关键点 (见引理 5[166]). 以下，我们将用循环和拟循环码构造极大距离可分字符结对码.

5.3.4 极大距离可分字符结对码的新构造

令 q 为一个素数幂, n 为一个正整数. 在这一节中, 我们将要构造 $(n, d_p)_q$ 极大距离可分字符结对码,其中 $d_p \in \{5, 6, 7\}$.

首先, 我们考虑 $d_p = 5$ 的极大距离可分字符结对码的构造. 我们的结果扩展了文献[166] 的定理 16 和定理 19.

定理 5.21: 令 q 为一个素数幂. 令 n 和 r 为两个正整数满足

$$r \mid q-1,\ nr \mid q^3-1,\ nr \nmid q-1,\ (\frac{q-1}{r}, n) = 1.$$

那么存在一个 $(n,5)_q$ 极大距离可分字符结对码.

证明. 令 $\omega \in \mathbb{F}_q^*$ 为一个阶为 r 的元素. 令 $\delta \in \mathbb{F}_{q^3}^*$ 为一个阶为 nr 的元素, 满足 $\delta^n = \omega$. 由于 $nr \nmid q-1$, 我们有 $\delta \in \mathbb{F}_{q^3}^* \setminus \mathbb{F}_q$ 并且多项式 $g(x) = (x-\delta)(x-\delta^q)(x-\delta^{q^2}) \in \mathbb{F}_q[x]$ 整除 $x^n - \omega$. 令 $\mathcal{C}$ 为 ω-拟循环码 $\langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n-\omega)$. 在命题 5.2 中令 $l = \frac{q-1}{r}$, 我们知道 $\mathcal{C}$ 的极小距离至少为三. 此外, 由 Singleton 界, $\mathcal{C}$ 是一个 $[n, n-3, d]_q$ 码满足 $3 \le d \le 4$. 由命题 5.5 和命题 5.6, $\mathcal{C}$ 是一个 $(n,5)_q$ 极大距离可分字符结对码. □

注： 由专著[151] 的推论 7.4.4, 若 $n > 2(q-1)$, 上述定理中的码 $\mathcal{C}$ 的极小距离为三. 此外，当 $n = q^2+q+1$, $\mathcal{C}$ 即是汉明码. 因而它的极小距离为 3. 在这种情况下, 由文献[44] 的定理 19, $\mathcal{C}$ 也达到了结对距离的球填充界.

以下，我们给出两个 $d_p = 6$ 的极大距离可分字符结对码的构造. 第一个构造推广了文献[166] 中的定理 12 和定理 13.

定理 5.22: 令 q 为一个素数幂. 令 n 和 r 为两个正整数满足

$$r \mid q-1,\ nr \mid (q-1)(q^2+1),\ nr \nmid q^2-1,\ (\frac{q-1}{r}, n) = 1.$$

那么存在一个 $(n,6)_q$ 极大距离可分字符结对码.

证明. 令 $\omega \in \mathbb{F}_q^*$ 为一个阶为 r 的元素. 令 $\delta \in \mathbb{F}_{q^4}^*$ 为一个阶为 nr 的元素, 使得 $\delta^n = \omega$. 由 $nr \nmid q^2-1$, 我们有 $\delta \in \mathbb{F}_{q^4}^* \backslash \mathbb{F}_{q^2}$, 并且多项式 $g(x) = (x-\delta)(x-\delta^q)(x-\delta^{q^2})(x-\delta^{q^3}) \in \mathbb{F}_q[x]$ 整除 $x^n-\omega$. 令 $\mathcal{C}$ 为 ω-拟循环码 $\langle g(x) \rangle \subset \mathbb{F}_q[x]/(x^n-\omega)$. 在命题 5.2 中令 $l = \frac{q-1}{r}$, 我们知道 $\mathcal{C}$ 的极小距离至少为三. 此外, 由 Singleton 界, $\mathcal{C}$ 是一个 $[n, n-4, d]_q$ 码满足 $3 \le d \le 5$. 以下, 我们将证明 $d \neq 3$.

假设 $\mathcal{C}$ 的极小距离为三. 不失一般性, 我们有一个码字 $1 + a_i x^i + a_j x^j$, 其中 $1 \le i, j \le n-1$, $i \neq j$ 及 $a_i, a_j \in \mathbb{F}_q^*$. 因而, 我们有 $1 + a_i\delta^i + a_j\delta^j = 0$. 由于 $nr \mid (q-1)(q^2+1)$, 我们得到

$$(1 + a_i\delta^i)^{(q-1)(q^2+1)} = (-a_j\delta^j)^{(q-1)(q^2+1)} = 1,$$

这蕴含了 $(1 + a_i\delta^i)^{q(q^2+1)} = (1 + a_i\delta^i)^{(q^2+1)}$. 经计算, $\delta^{qi} + \delta^{q^3 i} + a_i\delta^{(q^3+q)i} = \delta^i + \delta^{q^2 i} + a_i\delta^{(q^2+1)i}$. 由于$q^3 + q \equiv q^2 + 1 \pmod{nr}$, 我们有$\delta^{q^3+q} = \delta^{q^2+1}$. 因而, 我们有$\delta^{(q-1)i} + \delta^{(q^3-1)i} = 1 + \delta^{(q^2-1)i}$, 这蕴含了

$$(\delta^{(q-1)i} - 1)(\delta^{(q^2-q)i} - 1) = 0.$$

这要求对某个 $1 \le i \le n-1$, 我们有 $nr \mid (q-1)i$. 然而, 由于 $(\frac{q-1}{r}, n) = 1$, 这是不可能的.

因而, $\mathcal{C}$ 的极小距离是四或五. 由命题 5.5 和命题 5.6 易知 $\mathcal{C}$ 是一个 $(n,6)_q$ 极大距离可分字符结对码. □

当 $n \mid q^2-1$, 我们有以下的 $(n,6)_q$ 极大距离可分字符结对码的构造.

定理 5.23: 令 q 为一个素数幂, n 为一个整数满足 $n > q+1$ 和 $n \mid q^2-1$. 那么

1) 当 n 为奇数, 存在一个 $(n,6)_q$ 极大距离可分字符结对码.

2) 当 n 为偶数, 存在一个 $(\frac{n}{2},6)_q$ 极大距离可分字符结对码.

证明. 1) 令 $\delta \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q$ 为一个阶为 n 的元素, 其中 n 为奇数. 多项式 $g(x) = (x-\delta^{-q})(x-\delta^{-1})(x-\delta)(x-\delta^q) \in \mathbb{F}_q[x]$ 整除 x^n-1. 令 $\mathcal{C}_1$ 为循环码 $\langle g(x)\rangle \subset \mathbb{F}_q[x]/(x^n-1)$. 由于 n 为奇数, 易知 $\mathcal{C}_1$ 是一个 $[n,n-4,d]_q$ 码满足 $3 \le d \le 5$. 当 $4 \le d \le 5$, 由命题 5.5 和命题 5.6 易知 $\mathcal{C}_1$ 是一个 $(n,6)_q$ 极大距离可分字符结对码. 当 $d=3$, 由命题 5.5 和命题 5.6, 任何重量大于三的码字的结对重量至少为五. 因而, 由 (5.34), 只要证明对每个满足 $w_H(c(x))=3$ 的码字 $c(x) \in \mathcal{C}$, 我们有 $I(c(x)) \ge 3$. 为此, 我们将要证明没有形如 $1+a_1x+a_ix^i$, 其中 $2 \le i \le n-1$, $a_1, a_i \in \mathbb{F}_q^*$ 的码字. 以下，我们分两种情况讨论.

首先, 假设存在一个码字 $1+a_1x+a_2x^2$, 其中 $a_1, a_2 \in \mathbb{F}_q^*$. 那么我们有以下的方程组

$$\begin{cases} 1+a_1\delta+a_2\delta^2=0, \\ 1+a_1\delta^{-1}+a_2\delta^{-2}=0. \end{cases}$$

解方程组得 $a_1 = -(\delta+\frac{1}{\delta})$. 因而, 我们有 $\delta+\frac{1}{\delta} \in \mathbb{F}_q^*$, 这蕴含了 $n \mid q+1$ 或 $n \mid q-1$. 由于 $n > q+1$, 这是不可能的.

其次, 假设有一个码字 $1+a_1x+a_ix^i$, 其中 $3 \le i \le n-2$ 及 $a_1, a_i \in \mathbb{F}_q^*$. 那么我们有以下的方程组

$$\begin{cases} 1+a_1\delta+a_i\delta^i=0, \\ 1+a_1\delta^{-1}+a_i\delta^{-i}=0. \end{cases}$$

解方程组得 $a_1 = -\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta}$ 及 $a_i = \frac{\delta^{i+1}-\delta^{i-1}}{\delta^{2i-1}-\delta}$. 因而, 我们有 $\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta}, \frac{\delta^{i+1}-\delta^{i-1}}{\delta^{2i-1}-\delta} \in \mathbb{F}_q^*$. 由于

$$\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta} + \frac{\delta^{i+1}-\delta^{i-1}}{\delta^{2i-1}-\delta} = \frac{\delta^{i+1}-1}{\delta^i-\delta} \in \mathbb{F}_q^*,$$

及

$$\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta} - \frac{\delta^{i+1}-\delta^{i-1}}{\delta^{2i-1}-\delta} = \frac{\delta^{i+1}+1}{\delta^i+\delta} \in \mathbb{F}_q,$$

我们有

$$\frac{\delta^i-\delta}{\delta^{i+1}-1} + \frac{\delta^{i+1}+1}{\delta^i+\delta} = \frac{(\delta^{2i}-1)(\delta^2+1)}{(\delta^i+\delta)(\delta^{i+1}-1)} \in \mathbb{F}_q^*.$$

注意到 $\frac{\delta^{2i}-1}{\delta^{2i-1}-\delta} \in \mathbb{F}_q^*$ 及 $\frac{\delta^{i+1}-1}{\delta^i-\delta} \in \mathbb{F}_q^*$. 连同以上的等式, 我们有

$$\frac{(\delta^{2i-1}-\delta)(\delta^2+1)}{(\delta^i+\delta)(\delta^i-\delta)} = \delta + \frac{1}{\delta} \in \mathbb{F}_q^*.$$

然而, 如以上所述, $\delta + \frac{1}{\delta} \in \mathbb{F}_q^*$ 是不可能的.

2) 令 $\delta \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q$ 为一个阶为 n 的元素, 其中 n 是一个偶数. 由于 $\delta^{\frac{n}{2}} = -1$, 多项式 $g(x) = (x-\delta^{-q})(x-\delta^{-1})(x-\delta)(x-\delta^q) \in \mathbb{F}_q[x]$ 整除 $x^{\frac{n}{2}}+1$. 令 $\mathcal{C}_2$ 为 (-1)-拟循环码 $\langle g(x)\rangle \subset \mathbb{F}_q[x]/(x^{\frac{n}{2}}+1)$. 由命题 5.2 和 Singleton 界, $\mathcal{C}_2$ 是一个 $[\frac{n}{2}, \frac{n}{2}-4, d]_q$ 码满足 $3 \le d \le 5$. 余下的证明类似于 1), 我们在此略去. □

注： 对 $n \mid q^2-1$, 当 n 是奇数或 n 是偶数且 $v_2(n) < v_2(q^2-1)$ 时, 定理 5.23 构造了 $(n,6)_q$ 极大距离可分字符结对码. 若 n 是偶数且 $v_2(n) = v_2(q^2-1)$, 定理 5.23 的构造会生成极小距离为二的码. 这些码不是极大距离可分字符结对码.

注： 由专著[151]的推论 7.4.4, 以上定理中的码 $\mathcal{C}_1$ (或 $\mathcal{C}_2$) 有极小距离 $3 \le d \le 4$, 如果 $n > 2(q-1)$ (或 $n > 4(q-1)$). 进一步地, 在某些情况下, $\mathcal{C}_1$ 和 $\mathcal{C}_2$ 的极小距离是三. 例如, 如果 $3 \mid n$, $\mathcal{C}_1$ 包含一个重量为三的码字 $1 + x^{\frac{n}{3}} + x^{\frac{2n}{3}}$, 并且 $\mathcal{C}_2$ 包含一个重量为三的码字 $1 - x^{\frac{n}{6}} + x^{\frac{n}{3}}$.

在以下定理中, 我们将证明在某些条件下, 极小结对距离 $d_p = 7$ 的极大距离可分字符结对码可由某些循环码生成.

定理 5.24: 令 q 为一个素数幂, n 为一个正整数满足 $n \mid q^2-1$ 及 $n > q+1$. 令 $\delta \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q$ 为一个阶为 n 的元素. 令 $\mathcal{C} \subset \mathbb{F}_q[x]/(x^n-1)$ 为一个 $[n, n-5, d]_q$ 循环码, 它的生成多项式为 $g(x) = (x-\delta^{-q})(x-\delta^{-1})(x-1)(x-\delta)(x-\delta^q) \in \mathbb{F}_q[x]$. 那么

1) 当 $5 \le d \le 6$, $\mathcal{C}$ 是一个 $(n,7)_q$ 极大距离可分字符结对码.

2) 当 $d = 4$ 及 n 为奇数时, $\mathcal{C}$ 是一个 $(n,7)_q$ 极大距离可分字符结对码当且仅当对每个 $3 \le i \le n-3$, $\frac{\delta^{i+1}-1}{\delta^i-\delta} \notin \mathbb{F}_q^*$.

证明. 由 BCH 界和 Singleton 界, 极小距离 $4 \le d \le 6$. 我们只证明 2), 因为 1) 的证明是简单的. 当 $d = 4$ 时, 由命题 5.5 及命题 5.6, 任何重量大于四的码字的结对重量至少为七. 因而, 由 (5.34), 只需证明对任意满足 $w_H(c(x)) = 4$ 的码字 $c(x) \in \mathcal{C}$, 我们有 $I(c(x)) \ge 3$. 以下, 我们将研究确保这个性质成立的充要条件.

假设存在一个重量为四的码字 $c(x)$, 使得 $I(c(x))=1$. 不失一般性, 我们可以假设 $c(x)=1+a_1x+a_2x^2+a_3x^3$, 其中 $a_1,a_2,a_3\in\mathbb{F}_q^*$. 因而, 有以下的方程组:

$$\begin{cases}1+a_1+a_2+a_3=0,\\ 1+a_1\delta+a_2\delta^2+a_3\delta^3=0,\\ 1+a_1\delta^{-1}+a_2\delta^{-2}+a_3\delta^{-3}=0.\end{cases}$$

解方程组得 $a_2=1+\delta+\frac{1}{\delta}$. 然而, $\delta+\frac{1}{\delta}\in\mathbb{F}_q$ 蕴含了 $(\delta^{q+1}-1)(\delta^{q-1}-1)=0$. 这与 $n>q+1$ 矛盾.

假设存在一个重量为四的码字 $c(x)$, 使得 $I(c(x))=2$. 不失一般性, 我们有以下两种情况

i) 存在一个码字 $c(x)=1+a_1x+a_2x^2+a_ix^i$, 其中 $3\le i\le n-2$ 及 $a_1,a_2,a_i\in\mathbb{F}_q^*$.

ii) 存在一个码字 $c(x)=1+a_1x+a_ix^i+a_{i+1}x^{i+1}$, 其中 $3\le i\le n-3$ 及 $a_1,a_i,a_{i+1}\in\mathbb{F}_q^*$.

对情况 i), 我们有以下的方程组:

$$\begin{cases}1+a_1+a_2+a_i=0,\\ 1+a_1\delta+a_2\delta^2+a_i\delta^i=0,\\ 1+a_1\delta^{-1}+a_2\delta^{-2}+a_i\delta^{-i}=0.\end{cases}$$

解方程组得

$$\frac{a_1}{a_2}=-\frac{\delta^{i-2}-\delta}{\delta^{i-1}-1}-1,\quad a_2=\frac{\delta^i-1}{\delta^{i-1}-\delta},$$

这蕴含了

$$\frac{\delta^{i-2}-\delta}{\delta^{i-1}-1}\in\mathbb{F}_q^*,\quad \frac{\delta^i-1}{\delta^{i-1}-\delta}\in\mathbb{F}_q^*.$$

因而,

$$\begin{aligned}\frac{\delta^{i-1}-1}{\delta^{i-2}-\delta}-\frac{\delta^i-1}{\delta^{i-1}-\delta}&=\frac{\delta^{i-2}(\delta+1)(\delta-1)^2}{(\delta^{i-1}-\delta)(\delta^{i-2}-\delta)}\in\mathbb{F}_q^*,\\ \frac{\delta^{i-1}-\delta}{\delta^i-1}-\frac{\delta^{i-2}-\delta}{\delta^{i-1}-1}&=\frac{\delta^{i-1}(\delta-1)^2}{(\delta^i-1)(\delta^{i-1}-1)}\in\mathbb{F}_q^*.\end{aligned}$$

比较以上两式的右边, 我们有 $1+\frac{1}{\delta} \in \mathbb{F}_q^*$, 易见这是不可能的.

对情况 ii), 我们有以下的方程组:

$$\begin{cases} 1+a_1+a_i+a_{i+1}=0, \\ 1+a_1\delta+a_i\delta^i+a_{i+1}\delta^{i+1}=0, \\ 1+a_1\delta^{-1}+a_i\delta^{-i}+a_{i+1}\delta^{-(i+1)}=0. \end{cases}$$

如果 n 是偶数, 以上方程组在 $i=\frac{n}{2}$, $a_1=a_{\frac{n}{2}+1}=-1$ 及 $a_{\frac{n}{2}}=1$ 时有解. 因此, n 为奇数的条件是必要的. 解以上的方程组得

$$a_1=-\frac{\delta^{i+1}-1}{\delta^i-\delta}, \quad a_i=\frac{\delta^{i+1}-1}{\delta^i-\delta}, \quad a_{i+1}=-1.$$

因而, 之前的方程组不成立, 当且仅当对每个 $3 \le i \le n-3$, $\frac{\delta^{i+1}-1}{\delta^i-\delta} \notin \mathbb{F}_q^*$. 证毕. □

给定一个整数 $3 \le i \le n-3$, $\frac{\delta^{i+1}-1}{\delta^i-\delta}=\theta \in \mathbb{F}_q^*$ 等价于 $\delta^i=\frac{1-\theta\delta}{-\theta+\delta}$, 其中 $\theta \in \mathbb{F}_q^*$. 因而, 定理 5.24 2) 中的充要条件和关于 δ 的分式线性变换 $\frac{1-\theta\delta}{-\theta+\delta}$ 的性质相关, 其中 $\theta \in \mathbb{F}_q^*$. 这为我们去研究这一类特殊的分式线性变换提供了动力. 利用附录中得到的结果, 以下定理给出了上述充要条件的一个更准确的刻画.

定理 5.25: 令 q 为一个素数幂, n 为一个整数满足 $n \mid q^2-1$ 及 $n>q+1$. 令 $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 为一个阶为 n 的元素. 令 x^2-bx-c 为 δ 在 $\mathbb{F}_q$ 上的首一极小多项式. 对一个整数 $i \ge 2$, 定义

$$a_0^{(i)}=\sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j}c^{j+1}, \quad a_1^{(i)}=\sum_{j=0}^{\lfloor \frac{i-1}{2} \rfloor} \binom{i-1-j}{j} b^{i-1-2j}c^j. \tag{5.36}$$

令 $\mathcal{C} \subset \mathbb{F}_q[x]/(x^n-1)$ 为一个 $[n, n-5, d]_q$ 循环码, 有极小多项式 $g(x)=(x-\delta^{-q})(x-\delta^{-1})(x-1)(x-\delta)(x-\delta^q)$. 那么 $\mathcal{C}$ 是一个 $[n, n-5, d]_q$ 码满足 $4 \le d \le 6$. 当 $5 \le d \le 6$, $\mathcal{C}$ 是一个 $(n, 7)_q$ 极大距离可分字符结对码. 当 $d=4$ 且 n 为奇数, $\mathcal{C}$ 是一个 $(n, 7)_q$ 极大距离可分字符结对码当且仅当对每个 $3 \le i \le n-3$, 以下之一成立:

1) $a_1^{(i)}=0$,

或者当 $a_1^{(i)} \neq 0$,

2) 如果 $a_1^{(i)}=1$, 那么 $a_0^{(i)}\neq -b$ 或 $c=1$,

3) 如果 $a_0^{(i)}=0$, 那么 $a_1^{(i)}\neq \frac{1}{c}$ 或 $b=0$,

4) 如果 $a_0^{(i)}\neq 0$ 且 $a_1^{(i)}\neq 1$, 那么 $a_1^{(i)}c=1$ 或 $\frac{a_1^{(i)}b+a_0^{(i)}}{a_1^{(i)}-1}\neq \frac{a_1^{(i)}c-1}{a_0^{(i)}}$.

证明. 结论由定理 5.24 和推论 5.3 易得. □

注: 由球填充界, 当 $n(n-1)\geq \frac{2q^5}{(q-1)^2}$, 上述定理中的码 $\mathcal{C}$ 有极小距离 $d=4$.

以上的定理和注蕴含了一个构造 $(n,7)_q$ 极大距离可分字符结对码的算法, 其中 $n\mid q^2-1, n(n-1)\geq \frac{2q^5}{(q-1)^2}$ 及 n 为奇数.

算法

输入:
- 一个素数幂 q
- 一个正整数 n, 满足 $n\mid q^2-1, n(n-1)\geq \frac{2q^5}{(q-1)^2}$

输出:
- 如果算法成功, 一个 $(n,7)_q$ 极大距离可分字符结对码 $\mathcal{C}$
- 如果算法失败, 返回空

步骤:

令 $S=\{x\in \mathbb{F}_{q^2}^* \mid \text{ord}(x)=n\}$
当 S 为非空时**运行**
    选择 $\delta\in S$, 令 $b=\delta+\delta^q, c=-\delta^{q+1}$
    更新 $S:=S\setminus\{\delta,\delta^q\}$
    计算 $a_0^{(2)}$ 和 $a_1^{(2)}$
    对 每个 $3\leq i\leq n-3$ **运行**
        计算 $a_0^{(i)}=ca_1^{(i-1)}$ 和 $a_1^{(i)}$
        如果 定理 5.25 中的条件不成立**则**
            返回步骤2
        结束如果
    结束对
    用 δ 如定理 5.25构造$\mathcal{C}$
    输出 $\mathcal{C}$
结束当
返回空

回避了直接验证 $\frac{\delta^{i+1}-1}{\delta^i-\delta}\in\mathbb{F}_q^*$, 以上算法利用了定理 5.25 中提出的条件. 给定 b 和 c, 所有其它的计算都在较小的域 $\mathbb{F}_q$ 上, 而非在域 $\mathbb{F}_{q^2}$ 上. 因而, 当素数幂 q 很大时, 这个算法更有优势. 进而, 注意到 $a_0^{(i+1)}=ca_1^{(i)}$ 对任意 $i\geq 0$ 成立, 我们只需计算 $a_1^{(i)}$ 的值而 $a_0^{(i)}$ 的值即随之得出.

利用以上的算法, 我们对以下的例子进行了数值实验

$$\{(q,n)\mid q \text{ 素数幂}, q\leq 100, n\mid q^2-1, n \text{ 奇数}, n>q+1\}.$$

在这些例子中, 定理 5.25中相应的 $[n, n-5, d]_q$ 码 $\mathcal{C}$ 的极小距离 $d=4$. 当 q 为奇数, 除了$(q,n) \in \{(59,435),(67,561),(83,861)\}$, 码 $\mathcal{C}$ 是一个 $(n,7)_q$ 极大距离可分字符结对码. 进一步, 数值实验显示当 q 为偶数时, $\mathcal{C}$ 不是一个极大距离可分字符结对码. 然而, 要证明 q 为奇数是 $\mathcal{C}$ 为$(n,7)_q$ 极大距离可分字符结对码的必要条件, 似乎是困难的.

5.3.5 总结

借鉴文献[166] 中的思想, 我们利用循环和拟循环吗构造了极小结对距离 $d_p \in \{5,6,7\}$ 的极大距离可分字符结对码. 我们的构造推广了文献[166] 中的结果. 此外, 我们得到了保证一类循环码成为极大距离可分字符结对码的充要条件. 这个条件和一类特殊的分式线性变换的性质有关. 我们仔细研究了这一类特殊的分式线性变换, 提出了对以上充要条件的一个更精确的刻画. 由这个刻画得到了一个 $d_p=7$ 的极大距离可分字符结对码的构造算法. 我们认为对这个刻画更深入的理解可能带来新的极大距离可分字符结对码.

我们注意到绝大部分 $(n,d_p)_q$ 极大距离可分字符结对码的构造集中于 d_p 较小的情况. 在这种情况下, 如果我们用一个 $[n,k,d]_q$ 线性码构造一个字符结对码, 则差 d_p-d 必然较小. 因而, 证明能够达到相应的极小结对距离是容易的. 构造较大结对距离的极大距离可分字符结对码是一个有趣的研究课题.

附录

令 q 为一个素数幂. 对 $u,v,w,z \in \mathbb{F}_q$ 及 $\delta \in \mathbb{F}_{q^2}$, 定义一个从 $\mathbb{F}_{q^2}$ 到 $\mathbb{F}_{q^2}$ 的分式线性变换

$$f_{u,v,w,z}(\delta) = \frac{u+v\delta}{w+z\delta},$$

其中 $w+z\delta \neq 0$ 且 $uz-vw \neq 0$. 我们进一步假设 $z \neq 0$, 若不然, $f_{u,v,w,z}$ 退化为一个线性函数. 以下, 我们将研究这类特殊的分式线性变换. 特别地, 假设 $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, 我们将得到一个使得

$$\delta^i = \frac{u+v\delta}{w+z\delta},$$

对某个 i 成立的充要条件. 这个条件提供了一个准则去判断分式线性变换 $f_{u,v,w,z}$ 是否将 δ 映到由 δ 生成的循环群中.

命题 5.7: 令 $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. 令 x^2-bx-c 为 δ 在 $\mathbb{F}_q$ 上的首一极小多项式. 对一个正整

数 $i \geq 2$, 定义

$$a_0^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j} c^{j+1}, \quad a_1^{(i)} = \sum_{j=0}^{\lfloor \frac{i-1}{2} \rfloor} \binom{i-1-j}{j} b^{i-1-2j} c^j. \tag{5.37}$$

那么对 $i \geq 0$, $\delta^i = \frac{u+v\delta}{w+z\delta}$ 当且仅当以下之一成立:

1) 如果 $i = 0$, 那么 $u = w, v = z$.

2) 如果 $i = 1$, 那么 $b = \frac{v-w}{z}$ 且 $c = \frac{u}{z}$.

3) 如果 $i \geq 2$, 那么

$$a_1^{(i)} \neq 0, \quad b = -\frac{a_0^{(i)}}{a_1^{(i)}} + \frac{v}{z a_1^{(i)}} - \frac{w}{z}, \quad c = -\frac{w a_0^{(i)}}{z a_1^{(i)}} + \frac{u}{z a_1^{(i)}}.$$

证明. 1) 和 2) 是简单的. 以下我们只考虑 3). 由于 $\delta^i = \frac{u+v\delta}{w+z\delta}$ 及 $z \neq 0$, 我们有 $\delta^{i+1} + \frac{w}{z}\delta^i - \frac{v}{z}\delta - \frac{u}{z} = 0$. 因而, δ 是多项式 $x^{i+1} + \frac{w}{z}x^i - \frac{v}{z}x - \frac{u}{z}$ 的一个根且

$$x^{i+1} + \frac{w}{z}x^i - \frac{v}{z}x - \frac{u}{z} \equiv 0 \pmod{x^2 - bx - c}.$$

对一个整数 $i \geq 0$, 我们定义一个整数 $T_i(x) = x^{i+1} + \frac{w}{z}x^i$. 对任意 $i \geq 2$, 我们有以下的递归关系:

$$\begin{aligned} T_i(x) &\equiv x^{i+1} + \frac{w}{z}x^i \\ &\equiv bx^i + cx^{i-1} + \frac{w}{z}(bx^{i-1} + cx^{i-2}) \\ &\equiv b(x^i + \frac{w}{z}x^{i-1}) + c(x^{i-1} + \frac{w}{z}x^{i-2}) \\ &\equiv bT_{i-1}(x) + cT_{i-2}(x) \pmod{x^2 - bx - c}. \end{aligned}$$

反复应用这个递归关系, 我们有

$$\begin{aligned} T_i(x) &\equiv d_2^{(i)} T_2(x) + d_1^{(i)} T_1(x) \\ &\equiv e_1^{(i)} T_1(x) + e_0^{(i)} T_0(x) \pmod{x^2 - bx - c}, \end{aligned}$$

其中 $d_1^{(i)}, d_2^{(i)}, e_0^{(i)}, e_1^{(i)} \in \mathbb{F}_q$. 我们的目标是明确的决定 $e_0^{(i)}$ 和 $e_1^{(i)}$. 等价关系蕴含了 $T_0(x)$ 必须是由 $T_2(x)$ 减去某个 $x^2 - bx - c$ 的倍式所生成的. 由于 $T_2(x) \equiv bT_1(x) + cT_0(x) \pmod{x^2 - bx - c}$, 我们有 $e_0^{(i)} = cd_2^{(i)}$. 显然, $d_2^{(i)}$ 是一些关于 b 和 c 的单项式的和. 更确切的, 假设 $i-2$ 能表示成一个包含 $i-2-2j$ 个 1 和 j 个 2 的有序和. 那么这个有序和对应在和式 $d_2^{(i)}$ 中的一项 $b^{i-2-2j}c^j$. 一共有 $\binom{i-2-j}{j}$ 种方法将 $i-2$ 分解为 $i-2-2j$ 个 1 和 j 个 2 的有序和. 因而

$$d_2^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j} c^j,$$

且

$$e_0^{(i)} = cd_2^{(i)} = \sum_{j=0}^{\lfloor \frac{i-2}{2} \rfloor} \binom{i-2-j}{j} b^{i-2-2j} c^{j+1} = a_0^{(i)}.$$

类似的, 通过考察将 $i-1$ 分解为包含 1 和 2 的有序和的个数, 我们有

$$e_1^{(i)} = \sum_{j=0}^{\lfloor \frac{i-1}{2} \rfloor} \binom{i-1-j}{j} b^{i-1-2j} c^j = a_1^{(i)}.$$

因而,

$$\begin{aligned} x^{i+1} + \frac{w}{z}x^i - \frac{v}{z}x - \frac{u}{z} &\equiv T_i(x) - \frac{v}{z}x - \frac{u}{z} \\ &\equiv a_1^{(i)}T_1(x) + a_0^{(i)}T_0(x) - \frac{v}{z}x - \frac{u}{z} \\ &\equiv a_1^{(i)}x^2 + (a_0^{(i)} + \frac{wa_1^{(i)}}{z} - \frac{v}{z})x + \frac{wa_0^{(i)}}{z} - \frac{u}{z} \\ &\equiv 0 \pmod{x^2 - bx - c}. \end{aligned}$$

所以, 我们有 $a_1^{(i)} \neq 0$ 及$x^2 + (\frac{a_0^{(i)}}{a_1^{(i)}} + \frac{w}{z} - \frac{v}{za_1^{(i)}})x + \frac{wa_0^{(i)}}{za_1^{(i)}} - \frac{u}{za_1^{(i)}} = x^2 - bx - c$. 结论由比较系数即得. □

特别地, 给定 $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 和一个整数 $i \geq 2$, 我们有以下简单的准则去判断 $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$ 是否对某个 $\theta \in \mathbb{F}_q^*$ 成立.

推论 5.3: 令 $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. 令 $x^2 - bx - c$ 为 δ 在 $\mathbb{F}_q$ 上的首一极小多项式. 对一个整数 $i \geq 2$, $\delta^i = \frac{1-\theta\delta}{-\theta+\delta}$, 其中 $\theta \in \mathbb{F}_q^*$ 当且仅当 $a_1^{(i)} \neq 0$ 及以下之一的条件成立

1) 如果 $a_1^{(i)}=1$, 那么 $a_0^{(i)}=-b$ 及 $c\neq 1$,

2) 如果 $a_0^{(i)}=0$, 那么 $a_1^{(i)}=\frac{1}{c}$ 及 $b\neq 0$,

3) 如果 $a_0^{(i)}\neq 0$ 且 $a_1^{(i)}\neq 1$, 那么 $a_1^{(i)}c\neq 1$ 及 $\frac{a_1^{(i)}b+a_0^{(i)}}{a_1^{(i)}-1}=\frac{a_1^{(i)}c-1}{a_0^{(i)}}$.

其中 $a_0^{(i)}$ 及 $a_1^{(i)}$ 由 (5.37) 定义. 更进一步, 令 $\mathbb{F}_r$ 为 $\mathbb{F}_q$ 的一个子域. 如果 $b,c\in\mathbb{F}_r$, 那么 $\delta^i=\frac{1-\theta\delta}{-\theta+\delta}$ 对某个 $i\geq 2$ 成立仅当 $\theta\in\mathbb{F}_r$.

证明. 在命题 5.7 中令 $u=z=-1$ 及 $v=w=\theta$, 我们有 $\delta^i=\frac{1-\theta\delta}{-\theta+\delta}$ 对某个 $\theta\in\mathbb{F}_q^*$ 成立当且仅当

$$b=\frac{(a_1^{(i)}-1)\theta-a_0^{(i)}}{a_1^{(i)}},\quad c=\frac{a_0^{(i)}\theta+1}{a_1^{(i)}}.$$

如果 $a_0^{(i)}=0$ 及 $a_1^{(i)}=1$, 那我们有 $b=0$ 及 $c=1$, 由于 x^2-1 在 $\mathbb{F}_q$ 上可约, 这是不可能的. 若 $a_1^{(i)}=1$ 或 $a_0^{(i)}=0$, 那么条件 1) 或条件 2) 成立. 如果 $a_0^{(i)}\neq 0$ 及 $a_1^{(i)}\neq 1$, 条件 3) 可由 b 和 c 的表达式推出. 假设 b 和 c 属于一个子域 $\mathbb{F}_r$, 那么由定义知 $a_0^{(i)},a_1^{(i)}\in\mathbb{F}_r$. 由于我们有 $a_0^{(i)}\neq 0$ 或 $a_1^{(i)}\neq 1$, 易知 $\theta\in\mathbb{F}_r$. □

附录

本附录概述了作者的其它一些工作，它们已出现在胡思煌博士的论文中[149]，故在此不详述。

一类有任意多个非零点的循环码的重量分布与 Hermitian 型图

Delsarte 定理[72] 给出了循环码的一个迹表示. 研究循环码的重量分布, 往往从这个迹表示出发, 利用指数和的工具加以分析. 然而, 当循环码有较多个非零点时, 它的迹表示变得非常复杂, 以上方法就失效了. 因此, 关于具有多个非零点的循环码的重量分布的结果极其稀少. 为了求得有多个非零点的循环码的重量分布, 必须要引入新的思想和方法.

通过建立一类具有任意多个非零点的循环码的重量分布, 和 Hermitian型图的谱之间意外的联系，我们求出了这类循环码的重量分布. 这个出人意料的突破展现了循环码的重量分布与图的谱理论, 以结合方案为核心的代数组合理论之间美妙的联系. 关于这个工作的详细介绍已收录在胡思煌博士的论文的第 6 章.

有少数特征值的差集

给定群 G 中的一个 (v,k,λ) 差集 D, D 的阶定义为 $n=k-\lambda$. 我们称 D 满足特征整除性质 (character divisibility property), 如果对 G 的任意一个非平凡特征 χ, 均有 $\sqrt{n} \mid \chi(D)$. 注意到所有满足 $\gcd(v,n)>1$ 的差集都具有这个性质, Jungnickel 和 Schmidt 在 1997 年提出了以下的公开问题[163].

问题： 构造 $\gcd(v,n)>1$ 的不具有特征整除性质的差集.

近二十年来, 关于这个问题的进展非常缓慢. 我们以有三个非平凡特征值的差集为候选, 得出了这类差集不具有特征整除性质的一些必要条件, 为推进这个问题做出了初步的探索. 关于这个工作的详细介绍已收录在胡思煌博士的论文的第 3 章.

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 在偶特征的有限域上提出了伪平面函数 (pseudo-planar function) 的概念[306], 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. 关于这个工作的详细介绍已收录在胡思煌博士的论文的第 5 章.

参考文献

[1] R. J. R. Abel, C. J. Colbourn, and J. H. Dinitz. Mutully orthogonal latin squares. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 160–193. CRC Press, Boca Raton, second edition, 2007.

[2] T. Alderson and K. Mellinger, "Classes of optical orthogonal codes from arcs in root subspaces," *Discrete Math.*, vol. 308, no. 7, pp. 1093–1101, 2008.

[3] S. Aly, A. Klappenecker, and P. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.

[4] A. Amini and F. Marvasti, "Deterministic construction of binary, bipolar and ternary compressed sensing matrices," *IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 2360–2370, 2011.

[5] A. Amini, V. Montazerhodjat, and F. Marvasti, "Matrices with small coherence using p-ary block codes," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 172–181, 2012.

[6] L. Applebaum, S. Howard, S. Searle, and R. Calderbank, "Chirp sensing codes: deterministic compressed sensing measurements for fast recovery," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 2, pp. 283–290, 2009.

[7] A. Ashikhmin, A. Barg, and S. Litsyn, "New upper bounds on generalized weights," *IEEE Trans. Inform. Theory*, vol. 45, no. 4, pp. 1258–1263, 1999.

[8] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[9] D. Augot, P. Charpin and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 960–973, 1992.

[10] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Trans. Inform. Theory*, vol. 40, no. 1, pp. 204–207, 1994.

[11] R. D. Baker. "An elliptic semiplane," *J. Combin. Theory Ser. A*, vol. 25, no. 2, pp. 193–195, 1978.

[12] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constr. Approx.*, vol. 28, no. 3, pp. 253–263, 2008.

[13] A. I. Barbero and C. Munuera, "The weight hierarchy of Hermitian codes," *SIAM J. Discrete Math.*, vol. 13, no. 1, pp. 79–104, 2000.

[14] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Phys. Rev. A*, vol. 61, no. 6, pp. 062 308, 6, 2000.

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179.

[16] R. Berinde, A. Gilbert, P. Indyk, H.Karloff, and M. Strauss, "Combining geometry and combinatorics: a unified approach to sparse signal recovery," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 798–805.

[17] E. R. Berlekamp, "The enumeration of information symbols in BCH codes," *Bell System Tech. J.*, vol. 46, no. 8, pp. 1861–1880, 1967.

[18] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann, *Error-Correcting Linear Codes*, Springer-Verlag, Berlin, 2006.

[19] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Combin. Des.*, vol. 8, no. 3, pp. 174–188, 2000.

[20] C. Bird and A. Keedwell, "Design and applications of optical orthogonal codes—a survey," *Bull. Inst. Combin. Appl.*, vol. 11, pp. 21–44, 1994.

[21] I. Blake, C. Heegard, T. Høholdt, and V. Wei, "Algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2596–2618, 1998.

[22] T. Blumensath and M. E. Davies, "Iterative hard thresholding for compressed sensing," *Appl. Comput. Harmon. Anal.*, vol. 27, no. 3, pp. 265–274, 2009.

[23] A. Bonnecaze and I. M. Duursma. "Translates of linear codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 43, no. 4, pp. 1218–1230, 1997.

[24] R. C. Bose. "An affine analogue of Singer's theorem," *J. Indian Math. Soc. (N.S.)*, vol. 6, no. 1, pp. 1–15, 1942.

[25] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997.

[26] N. Boston and G. McGuire, "The weight distributions of cyclic codes with two zeros and zeta functions," *J. Symbolic Comput.*, vol. 45, no. 7, pp. 723–733, 2010.

[27] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, "Explicit constructions of RIP matrices and related problems," *Duke Math. J.*, vol. 159, no. 1, pp. 145–185, 2011.

[28] M. Bras-Amorós, K. Lee, and A. Vico-Oton, "New lower bounds on the generalized Hamming weights of AG codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 10, pp. 5930–5937, 2014.

[29] A. E. Brouwer. "Optimal packings of K_4's into a K_n," *J. Combin. Theory Ser. A*, vol. 26, no. 3, pp. 278–297, 1979.

[30] D. Bruss, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, 1998.

[31] M. Buratti. "Recursive constructions for difference matrices and relative difference families," *J. Combin. Des.*, vol. 6, no. 3, pp. 165–182, 1998.

[32] M. Buratti, J. Yan, and C. Wang. "From a 1-rotational RBIBD to a partitioned difference family," *Electron. J. Combin.*, vol. 17, no. 1, Research Paper 139, 23, 2010.

[33] H. Cai, X. Zeng, T. Helleseth, X. Tang, and Y. Yang. "A new construction of zero-difference balanced functions and its applications," *IEEE Trans. Inform. Theory*, vol. 59, no. 8, pp. 5008–5015, 2013.

[34] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 4–8, 2000.

[35] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE Trans. Inform. Theory*, vol. 4, no. 2, pp. 358–374, 2010.

[36] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.*, vol. 18, no. 2, pp. 97–122, 1986.

[37] R. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over $\mathrm{GF}(4)$," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[38] E. Candès, "The restricted isometry property and its implications for compressed sensing," *C. R. Math. Acad. Sci. Paris*, vol. 346, no. 9–10, pp. 589–592, 2008.

[39] E. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 489–509, 2006.

[40] E. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.

[41] E. Candès and T. Tao, "Near-optimal signal recovery from random projections: universal encoding strategies," *IEEE Trans. Inform. Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[42] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2-3, pp. 205–244, 2004.

[43] Y. Cassuto and M. Blaum. "Codes for symbol-pair read channels," In *Proc. Int. Symp. Inf. Theory*, pages 988–992, 2010.

[44] Y. Cassuto and M. Blaum. "Codes for symbol-pair read channels," *IEEE Trans. Inform. Theory*, vol. 57, no. 12, pp. 8011–8020, 2011.

[45] Y. Cassuto and S. Litsyn. "Symbol-pair codes: Algebraic constructions and asymptotic bounds," In *Proc. Int. Symp. Inf. Theory*, pages 2348–2352, 2011.

[46] Y. Chang and C. Ding. "Constructions of external difference families and disjoint difference families," *Des. Codes Cryptogr.*, vol. 40, no. 2, pp. 167–185, 2006.

[47] Y. Chang and Y. Miao. "Constructions for optimal optical orthogonal codes," *Discrete Math.*, vol. 261, no. 1-3, pp. 127–139, 2003.

[48] Y. Chang and Y. Miao. "General constructions for double group divisible designs and double frames," *Des. Codes Cryptogr.*, vol. 26, no. 1-3, pp. 155–168, 2002.

[49] P. Charpin, "Cyclic codes with few weights and Niho exponents," *J. Combin. Theory Ser. A*, vol. 108, no. 2, pp. 247–259, 2004.

[50] P. Charpin, "On a class of primitive BCH-codes," *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 222–228, 1990.

[51] P. Charpin, "Open problems on cyclic codes," In: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, vol. I, pp. 963–1063 (Chapter 11), Elsevier, Amsterdam, 1998.

[52] H. F. Chau, "Five quantum register error correction code for higher spin systems," *Phys. Rev. A*, vol. 56, pp. R1–R4, 1997.

[53] Y. M. Chee, G. Ge, and A. C. H. Ling. "Group divisible codes and their application in the construction of optimal constant-composition codes of weight three," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3552–3564, 2008.

[54] Y. M. Chee, L. Ji, H. M. Kiah, C. Wang, and J. Yin. "Maximum distance separable codes for symbol-pair read channels," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7259–7267, 2013.

[55] Y. M. Chee, H. M. Kiah, and C. Wang. "Maximum distance separable symbol-pair codes," In *Proc. Int. Symp. Inf. Theory*, pages 2886–2890, 2012.

[56] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 3, pp. 1474–1484, 2015.

[57] J. Cheng and C. Chao, "On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two," *IEEE Trans. Inform. Theory*, vol. 43, no. 1, pp. 294–299, 1997.

[58] J. P. Cherdieu, D. J. Mercier, and T. Narayaninsamy, "On the generalized weights of a class of trace codes," *Finite Fields Appl.*, vol. 7, no. 2, pp. 355–371, 2001.

[59] S. T. Choi, J. Y. Kim, and J. S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$," arXiv:1205.5959.

[60] S. T. Choi and J. S. No, "On the cross-correlation distributions between p-ary m-sequences and their decimated sequences," *IEICE Trans. Fundamentals.*, vol. E95-A, no. 11, pp. 1808–1818, 2012.

[61] H. Chung, "The 2-nd generalized Hamming weight of double-error correcting binary BCH codes and their dual codes," in *Applied algebra, algebraic algorithms and error-correcting codes*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 1991, vol. 539, pp. 118–129.

[62] A. Cohen, W. Dahmen, and R. DeVore, "Compressed sensing and best k-term approximation," *J. Amer. Math. Soc.*, vol. 22, no. 1, pp. 211–231, 2009.

[63] G. Cohen, S. Litsyn, and G. Zémor, "Upper bounds on generalized distances," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 2090–2092, 1994.

[64] C. J. Colbourn. Difference matrices. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 58–71. CRC Press, Boca Raton, second edition, 2007.

[65] C. J. Colbourn, D. G. Hoffman, and R. Rees. "A new class of group divisible designs with block size three," *J. Combin. Theory Ser. A*, vol. 59, no. 1, pp. 73–89, 1992.

[66] C. J. Colbourn, D. Horsley, and C. McLean, "Compressive sensing matrices and hash families," *IEEE Trans. Commun.*, vol. 59, no. 7, pp. 1840–1845, 2011.

[67] C. J. Colbourn and R. Mathon, "Steiner systems," in *The CRC Handbook of Combinatorial Designs*, 2nd ed. Boca Raton: CRC Press, 2007, pp. 58–71.

[68] R. Coulter and R. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des. Codes Cryptogr.*, vol. 10, no. 2, pp. 167–184, 1997.

[69] T. W. Cusick and H. Dobbertin, "Some new three-valued crosscorrelation functions for binary m-sequences," *IEEE Trans. Inform. Theory*, vol. 42, no. 4, pp. 1238–1240, 1996.

[70] W. Dai and O. Milenkovic, "Subspace pursuit for compressive sensing signal reconstruction," *IEEE Trans. Inform. Theory*, vol. 55, no. 5, pp. 2230–2249, 2009.

[71] M. Delgado, J. I. Farrán, P. A. García-Sánchez, and D. Llena, "On the weight hierarchy of codes coming from semigroups with two generators," *IEEE Trans. Inform. Theory*, vol. 60, no. 1, pp. 282–295, 2014.

[72] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 21, no. 5, pp. 575–576, 1975.

[73] P. Dembowski, *Finite geometries*, ser. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Berlin: Springer-Verlag, 1968.

[74] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2," *Math. Z.*, vol. 103, no. 3, pp. 239–258, 1968.

[75] P. Dembowski and F. Piper. "Quasiregular collineation groups of finite projective planes," *Math. Z.*, vol. 99, no. 1, pp. 53–75, 1967.

[76] R. DeVore, "Deterministic constructions of compressed sensing matrices," *J. Complexity*, vol. 23, no. 4–6, pp. 918–925, 2007.

[77] Y. Dianwu and H. Zhengming, "On the dimension and minimum distance of BCH codes over $\mathrm{GF}(q)$," *J. Electron.*, vol. 13, no. 3, pp. 216–221, 1996.

[78] C. Ding, "Complex codebooks from combinatorial designs," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4229–4235, 2006.

[79] C. Ding and T. Feng, "A generic construction of complex codebooks meeting the Welch bound," *IEEE Trans. Inform. Theory*, vol. 53, no. 11, pp. 4245–4250, 2007.

[80] C. Ding. "Optimal constant composition codes from zero-difference balanced functions," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5766–5770, 2008.

[81] C. Ding. "Optimal and perfect difference systems of sets," *J. Combin. Theory Ser. A*, vol. 116, no. 1, pp. 109–119, 2009.

[82] C. Ding, M. Moisio, and J. Yuan. "Algebraic constructions of optimal frequency-hopping sequences," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2606–2610, 2007.

[83] C. Ding and Y. Tan. "Zero-difference balanced functions with applications," *J. Stat. Theory Pract.*, vol. 6, no. 1, pp. 3–19, 2012.

[84] C. Ding, Q. Wang, and M. Xiong. "Three new families of zero-difference balanced functions with applications," *IEEE Trans. Inform. Theory*, vol. 60, no. 4, pp. 2407–2413, 2012.

[85] C. Ding and J. Yin. "Combinatorial constructions of optimal constant-composition codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3671–3674, 2005.

[86] C. Ding and J. Yin. "Sets of optimal frequency-hopping sequences," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3741–3745, 2008.

[87] C. Ding, Y. Gao, and Z. Zhou, "Five families of three-weight ternary cyclic codes and their duals," *IEEE Trans. Inform. Theory*, vol. 59, no. 12, pp. 7940–7946, 2013.

[88] C. Ding, Y. Liu, C. Ma, and L. Zeng, "The weight distributions of the duals of cyclic codes with two zeros," *IEEE Trans. Inform. Theory*, vol. 57, no. 12, pp. 8000–8006, 2011.

[89] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discr. Math.*, vol. 313, no. 4, pp. 434–446, 2013.

[90] C. Ding, Y. Yang, and X. Tang, "Optimal sets of frequency hopping sequences from linear cyclic codes," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3605–3612, 2010.

[91] C. Ding and J. Yin, "Signal sets from functions with optimum nonlinearity," *IEEE Trans. Commun.*, vol. 55, no. 5, pp. 936–940, 2007.

[92] C. Ding and J. Yuan, "A family of skew Hadamard difference sets," *J. Combin. Theory Ser. A*, vol. 113, no. 7, pp. 1526–1535, 2006.

[93] C. Ding, *Codes from Difference Sets*, World Scientific, Singapore, 2015.

[94] C. Ding, X. Du and Z. Zhou, "The Bose and minimum distance of a class of BCH codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 5, pp. 2351–2356, 2015.

[95] J. Dixon and B. Mortimer, *Permutation groups*, ser. Grad. Texts in Math. New York: Springer-Verlag, 1996, vol. 163.

[96] H. Dobbertin, "One-to-one highly nonlinear power functions on $\mathrm{GF}(2^n)$," *Appl. Algebra Engrg. Comm. Comput.*, vol. 9, no. 2, pp. 139–152, 1998.

[97] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 613–627, 2006.

[98] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, "Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1473–1481, 2001.

[99] D. Donoho, "Compressed sensing," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[100] I. Duursma, H. Stichtenoth, and C. Voß, "Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields," in *Arithmetic, geometry and coding theory (Luminy, 1993)*. Berlin: de Gruyter, 1996, pp. 53–65.

[101] T. Etzion. "Optimal constant weight codes over Z_k and generalized designs," *Discrete Math.*, vol. 169, no. 1-3, pp. 55–82, 1997.

[102] K. Feng, "Quantum codes $[[6, 2, 3]]_p$ and $[[7, 3, 3]]_p$ $(p \geq 3)$ exist," *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2384–2391, 2002.

[103] G. L. Feng, K. K. Tzeng, and V. K. Wei, "On the generalized Hamming weights of several classes of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 1125–1130, 1992.

[104] T. Feng and Y. Chang. "Combinatorial constructions for optimal two-dimensional optical orthogonal codes with $\lambda = 2$," *IEEE Trans. Inform. Theory*, vol. 57, no. 10, pp. 6796–6819, 2011.

[105] T. Feng and K. Momihara, "Evaluation of the weight distribution of a class of cyclic codes based on index 2 gauss sums," *IEEE Trans. Inform. Theory*, vol. 59, no. 9, pp. 5980–5984, 2013.

[106] T. Feng, K. Leung, and Q. Xiang, "Binary cyclic codes with two primitive nonzeros," *Sci. China Math.*, vol. 56, no. 7, pp. 1403–1412, 2013.

[107] M. Fickus, D. G. Mixon, and J. C. Tremain, "Steiner equiangular tight frames," *Linear Algebra Appl.*, vol. 436, no. 5, pp. 1014–1027, 2012.

[108] M. Fornasier and H. Rauhut, "Iterative thresholding algorithms," *Appl. Comput. Harmon. Anal.*, vol. 25, no. 2, pp. 187–208, 2008.

[109] G. D. Forney, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1741–1752, 1994.

[110] R. Fuji-Hara, Y. Miao, and M. Mishima. "Optimal frequency hopping sequences: a combinatorial approach," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2408–2420, 2004.

[111] R. Fuji-Hara, Y. Miao, and S. Shinohara. "Complete sets of disjoint difference families and their applications," *J. Statist. Plann. Inference*, vol. 106, no. 1-2, pp. 87–103, 2002.

[112] S. Furino, Y. Miao, and J. Yin. *Frames and resolvable designs: uses, constructions, and existence*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[113] A. Gilbert and P. Indyk, "Sparse recovery using sparse matrices," *Proceedings of The IEEE*, vol. 98, no. 6, pp. 937–947, 2010.

[114] M. J. Ganley. "Direct product difference sets," *J. Combin. Theory Ser. A*, vol. 23, no. 3, pp. 321–332, 1977.

[115] G. Ge. Group divisible designs. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 255–260. CRC Press, Boca Raton, second edition, 2007.

[116] G. Ge, R. Fuji-Hara, and Y. Miao. "Further combinatorial constructions for optimal frequency-hopping sequences," *J. Combin. Theory Ser. A*, vol. 113, no. 8, pp. 1699–1718, 2006.

[117] G. Ge, Y. Miao, and Z. Yao. "Optimal frequency hopping sequences: auto- and cross-correlation properties," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 867–879, 2009.

[118] G. Ge and A. C. H. Ling. "Some more 5-GDDs and optimal $(v, 5, 1)$-packings," *J. Combin. Des.*, vol. 12, no. 2, pp. 132–141, 2004.

[119] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2016.

[120] M. Grassl and M. Rötteler, "Quantum MDS codes over small fields," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2015, pp. 1104–1108.

[121] M. Greig. "Designs from projective planes and PBD bases," *J. Combin. Des.*, vol. 7, no. 5, pp. 341–374, 1999.

[122] R. Gold, "Maximal recursive seuqneces with 3-valued recursive cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[123] S. W. Golomb and G. Gong, *Signal design for good correlation: For wireless communication, cryptography, and radar*. Cambridge: Cambridge University Press, 2005.

[124] P. Gopalan, V. Guruswami, and P. Raghavendra, "List decoding tensor products and interleaved codes," *SIAM J. Comput.*, vol. 40, no. 5, pp. 1432–1462, 2011.

[125] V. D. Goppa, "Codes on algebraic curves," *Dokl. Akad. Nauk SSSR*, vol. 259, no. 6, pp. 1289–1290, 1981.

[126] G. G. L. Guardia, "New quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 5551–5554, 2011.

[127] C. Güneri and F. Özbudak, "Improvements on generalized Hamming weights of some trace codes," *Des. Codes Cryptogr.*, vol. 39, no. 2, pp. 215–231, 2006.

[128] V. Guruswami, "List decoding from erasures: bounds and code constructions," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2826–2833, 2003.

[129] P. Heijnen and R. Pellikaan, "Generalized Hamming weights of q-ary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 181–196, 1998.

[130] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, no. 3, pp. 209–232, 1976.

[131] T. Helleseth, "A note on the cross-correlation function between two binary maximal length linear sequences," *Discrete Math.*, vol. 23, no. 3, pp. 301–307, 1978.

[132] T. Helleseth, "Pairs of m-sequences with a six-valued crosscorrelation," in *Mathematical properties of sequences and other combinatorial structures (Los Angeles, CA, 2002)*. Boston, MA: Kluwer Acad. Publ., 2003, pp. 1–6.

[133] T. Helleseth, L. Hu, A. Kholosha, X. Zeng, N. Li, and W. Jiang, "Period-different m-sequences with at most four-valued cross correlation," *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 3305–3311, 2009.

[134] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of coding theory, Vol. I, II*. Amsterdam: North-Holland, 1998, pp. 1765–1853.

[135] T. Helleseth and P. Rosendahl, "New pairs of m-sequences with 4-level cross-correlation," *Finite Fields Appl.*, vol. 11, no. 4, pp. 674–683, 2005.

[136] T. Helleseth and T. Kløve, "The weight hierarchies of some product codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 3, pp. 1029–1034, 1996.

[137] T. Helleseth, T. Kløve, V. I. Levenshtein, and Ø. Ytrehus, "Bounds on the minimum support weights," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 432–440, 1995.

[138] T. Helleseth, T. Kløve, and J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block length $n_1((q^l-1)/N)$," *Discrete Math.*, vol. 18, no. 2, pp. 179–211, 1977.

[139] T. Helleseth, T. Kløve, and Ø. Ytrehus, "Generalized Hamming weights of linear codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 1133–1140, 1992.

[140] T. Helleseth and P. V. Kumar, "The weight hierarchy of the Kasami codes," *Discrete Math.*, vol. 145, no. 1-3, pp. 133–143, 1995.

[141] T. Helleseth and P. V. Kumar, "On the weight hierarchy of the semiprimitive codes," *Discrete Math.*, vol. 152, no. 1-3, pp. 185–190, 1996.

[142] F. Hess, "Computing Riemann-Roch spaces in algebraic function fields and related topics," *J. Symbolic Comput.*, vol. 33, no. 4, pp. 425–445, 2002.

[143] J. W. P. Hirschfeld, M. A. Tsfasman, and S. G. Vladut, "The weight hierarchy of higher dimensional Hermitian codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 1, pp. 275–278, 1994.

[144] H. D. L. Hollmann and Q. Xiang, "On binary cyclic codes with few weights," in *Finite fields and applications (Augsburg, 1999)*. Berlin: Springer, 2001, pp. 251–275.

[145] H. D. L. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences," *Finite Fields Appl.*, vol. 7, no. 2, pp. 253–286, 2001.

[146] M. Homma and S. J. Kim, "The second generalized Hamming weight for two-point codes on a Hermitian curve," *Des. Codes Cryptogr.*, vol. 50, no. 1, pp. 1–40, 2009.

[147] S. Howard, A. Calderbank, and J. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes," in *IEEE Conf. Inform. Sciences and Systems (CISS2008)*, 2008, pp. 11–15.

[148] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, "Graphical nonbinary quantum error-correcting codes," *Phys. Rev. A*, vol. 78, p. 012306, 2008.

[149] S. Hu. *Several Discrete Configurations in Algebraic Combinatorics and Algebraic Coding Theory*. PhD thesis, Zhejiang University, 2014.

[150] X. Hu, G. Zhang, and B. Chen, "Constructions of new nonbinary quantum codes," *Internat. J. Theoret. Phys.*, vol. 54, no. 1, pp. 92–99, 2015.

[151] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[152] P. Indyk, "Explicit constructions for compressed sensing matrices," in *Proc. 19th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, Jan. 2008, pp. 30–33.

[153] Y. J. Ionin and H. Kaharaghani, "Balanced generalized weighing matrices and conference matrices," in *The CRC Handbook of Combinatorial Designs*, 2nd ed. Boca Raton: CRC Press, 2007, pp. 306–313.

[154] H. Janwa and A. K. Lal, "On the generalized Hamming weights of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 1, pp. 299–308, 1997.

[155] H. Janwa and A. K. Lal, "On generalized Hamming weights and the covering radius of linear codes," in *Applied algebra, algebraic algorithms and error-correcting codes*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2007, vol. 4851, pp. 347–356.

[156] L. Ji, D. Wu, and L. Zhu. "Existence of generalized Steiner systems $\mathrm{GS}(2, 4, v, 2)$," *Des. Codes Cryptogr.*, vol. 36, no. 1, pp. 83–99, 2005.

[157] 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*, vol. 56, no. 9, pp. 4735–4740, 2010.

[158] L. Jin and C. Xing, "Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes," *IEEE Trans. Inform. Theory*, vol. 58, no. 8, pp. 5484–5489, 2012.

[159] L. Jin and C. Xing, "A construction of new quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 5, pp. 2921–2925, 2014.

[160] A. Johansen and T. Helleseth, "A family of m-sequences with five-valued cross correlation," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 880–887, 2009.

[161] A. Johansen, T. Helleseth, and A. Kholosha, "Further results on m-sequences with five-valued cross correlation," *IEEE Trans. Inform. Theory*, vol. 55, no. 12, pp. 5792–5802, 2009.

[162] D. Jungnickel, A. Pott, and W. E. Smith, "Difference sets," in *The CRC Handbook of Combinatorial Designs*, 2nd ed. Boca Raton: CRC Press, 2007, pp. 419–435.

[163] D. Jungnickel and B. Schmidt, "Difference sets: an update," *London Math. Soc. Lecture Note Ser.* **245**, Cambridge Univ. Press, Cambridge, 1997, pp. 89–112.

[164] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 2, pp. 1193–1197, 2013.

[165] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 4, pp. 2080–2086, 2014.

[166] X. Kai, S. Zhu, and P. Li. "A construction of new MDS symbol-pair codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 11, pp. 5828–5834, 2015.

[167] X. Kai, S. Zhu, and Y. Tang, "Quantum negacyclic codes," *Phys. Rev. A*, vol. 88, p. 012326, 2013.

[168] W. M. Kantor. "Projective planes of type $\mathrm{I}-4$," *Geometriae Dedicata*, vol. 3, no. 3, pp. 335–346, 1974.

[169] G. N. Karystinos and D. A. Pados, "New bounds on the total squared correlation and optimum design of DS-CDMA binary signature sets," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 48–51, 2003.

[170] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes," *Inf. Control*, vol. 18, pp. 369–394, 1971.

[171] T. Kasami and S. Lin, "Some results on the minimum weight of primitive BCH codes", *IEEE Trans. Inform. Theory*, vol. 18, no. 6, pp. 824–825, 1972.

[172] T. Kasami, S. Lin and W. W. Peterson, "Linear codes which are invariant under the affine group and some results on minimum weights in BCH codes", *Electron. Commun. Japan*, vol. 50, no. 9, pp. 100–106, 1967.

[173] T. Kasami and N. Tokura, "Some remarks on BCH bounds and minimum weights of binary primitive BCH codes", *IEEE Trans. Inform. Theory*, vol. 15, pp. 408–413, 1969.

[174] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 242–245, 1993.

[175] D. J. Katz, "Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth," *J. Combin. Theory Ser. A*, vol. 119, no. 8, pp. 1644–1659, 2012.

[176] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.

[177] G. Khosrovshahi and R. Laue, "t-designs with $t \geq 3$," in *The CRC Handbook of Combinatorial Designs*, 2nd ed. Boca Raton: CRC Press, 2007, pp. 79–97.

[178] A. Klappenecker and M. Rötteler, "Constructions of mutually unbiased bases," in *Finite fields and applications*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2004, vol. 2948, pp. 137–144.

[179] A. Klappenecker, M. Rötteler, I. E. Shparlinski, and A. Winterhof, "On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states," *J. Math. Phys.*, vol. 46, no. 8, pp. 082 104, 17, 2005.

[180] T. Kløve, "The weight distribution of linear codes over $\mathrm{GF}(q^l)$ having generator matrix over $\mathrm{GF}(q)$," *Discrete Math.*, vol. 23, no. 2, pp. 159–168, 1978.

[181] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A (3)*, vol. 55, no. 2, pp. 900–911, 1997.

[182] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Des. Codes Cryptogr.*, vol. 19, no. 2–3, pp. 173–193, 2000.

[183] J. Kurihara and T. Uyematsu, "Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight," in *49th Annual Allerton Conference on Communication, Control, and Computing*, Sep 2011, pp. 951–957.

[184] V. I. Levenshtein, "Bounds for packings of metric spaces and some of their applications," *Problemy Kibernet.*, no. 40, pp. 43–110, 1983.

[185] C. Li, X. Zeng, and L. Hu, "A class of binary cyclic codes with five weights," *Sci. China Math.*, vol. 53, no. 12, pp. 3279–3286, 2010.

[186] N. Li, T. Helleseth, A. Kholosha, and X. Tang, "On the Walsh transform of a class of functions from Niho exponents," *IEEE Trans. Inform. Theory*, vol. 59, no. 7, pp. 4662–4667, 2013.

[187] R. Li and Z. Xu, "Construction of $[\![n, n-4, 3]\!]_q$ quantum codes for odd prime power q," *Phys. Rev. A (3)*, vol. 82, no. 5, p. 052316, 2010.

[188] S. Li, F. Gao, G. Ge, and S. Zhang, "Deterministic construction of compressed sensing matrices via algebraic curves," *IEEE Trans. Inform. Theory*, vol. 58, no. 8, pp. 5035–5041, 2012.

[189] Z. Li, L. Xing, and X. Wang, "Quantum generalized Reed-Solomon codes: unified framework for quantum mds codes," *Phys. Rev. A (3)*, vol. 77, no. 1, p. 012308, 2008.

[190] R. Lidl and H. Niederreiter, *Finite fields*, ser. Encyclopedia of Mathematics and its Applications. Reading, MA: Addison-Wesley Publishing Company Advanced Book Program, 1983, vol. 20.

[191] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, "Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes," *Finite Fields Appl.*, vol. 19, pp. 16–38, 2013.

[192] J. Luo and K. Feng, "Cyclic codes and sequences from generalized Coulter-Matthews function," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5345–5353, 2008.

[193] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5332–5344, 2008.

[194] Y. Luo, F. Fu, A. J. H. Vinck, and W. Chen. "On constant-composition codes over Z_q," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3010–3016, 2003.

[195] J. Luo, Y. Tang, and H. Wang, "Cyclic codes and sequences: the generalized Kasami case," *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2130–2142, 2010.

[196] C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, "The weight enumerator of a class of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 397–402, 2011.

[197] H. F. MacNeish. "Euler squares," *Ann. of Math. (2)*, vol. 23, no. 3, pp. 221–227, 1922.

[198] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[199] S. Mallat and Z. Zhang, "Matching pursuits with time-frequence dictionaries," *IEEE Trans. Signal Process.*, vol. 41, no. 12, pp. 3397–3415, 1993.

[200] D. M. Mandelbaum, "Two applications of cyclotomic cosets to certain BCH codes," *IEEE Trans. Inform. Theory*, vol. 26, no. 6, pp. 737–738, 1980.

[201] H. B. Mann, "On the number of information symbols in Bose-Chaudhuri codes," *Inf. Control*, vol. 5, no. 2, pp. 153–162, 1962.

[202] C. Martínez-Pérez and W. Willems, "On the weight hierarchy of product codes," *Des. Codes Cryptogr.*, vol. 33, no. 2, pp. 95–108, 2004.

[203] R. J. McEliece, "Irreducible cyclic codes and Gauss sums," in *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory*. Amsterdam: Math. Centrum, 1974, pp. 179–196. Math. Centre Tracts, No. 55.

[204] R. L. McFarland, "A family of difference sets in non-cyclic groups," *J. Combin. Theory Ser. A*, vol. 15, no. 1, pp. 1–10, 1973.

[205] Y. Miao. "Some constructions and uses of double group divisible designs," *Bull. Inst. Combin. Appl.*, 10(1):66–72, 1994. vol. 10, no. 1, pp. 66–72, 1994.

[206] W. H. Mills and R. C. Mullin, "Coverings and packings," in *Contemporary design theory*, ser. Wiley-Intersci. Ser. Discrete Math. Optim. New York: Wiley, 1992, pp. 371–399.

[207] N. Miyamoto, H. Mizuno, and S. Shinohara, "Optical orthogonal codes obtained from conics on finite projective planes," *Finite Fields Appl.*, vol. 10, no. 3, pp. 405–411, 2004.

[208] M. Moisio, "Explicit evaluation of some exponential sums," *Finite Fields Appl.*, vol. 15, no. 6, pp. 644–651, 2009.

[209] O. Moreno, J. P. Pedersen, and D. Polemi, "An improved Serre bound for elementary abelian extensions of $F_q(x)$ and the generalized Hamming weights of duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1291–1293, 1998.

[210] R. C. Mullin, P. J. Schellenberg, S. A. Vanstone, and W. D. Wallis. "On the existence of frames," *Discrete Math.*, vol. 37, no. 1, pp. 79–104, 1981.

[211] R. C. Mullin and J. Yin. "On packings of pairs by quintuples: $v \equiv 3, 9$ or $17 \pmod{20}$," *Ars Combin.*, vol. 35, no. 1, pp. 161–171, 1993.

[212] C. Munuera, "On the generalized Hamming weights of geometric Goppa codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 2092–2099, 1994.

[213] C. Munuera and D. Ramirez, "The second and third generalized Hamming weights of Hermitian codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 709–712, 1999.

[214] B. K. Natarajan, "Sparse approximate solutions to linear systems," *SIAM J. Comput.*, vol. 24, no. 2, pp. 227–234, 1995.

[215] D. Needell and J. Tropp, "CoSaMP: iterative signal recovery from incomplete and inaccurate samples," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 301–321, 2009.

[216] D. Needell and R. Vershynin, "Uniform uncertainty principle and signal recovery via regularized orthogonal matching pursuit," *Found. Comput. Math.*, vol. 9, no. 3, pp. 317–334, 2009.

[217] G. J. Ness and T. Helleseth, "Cross correlation of m-sequences of different lengths," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1637–1648, 2006.

[218] G. J. Ness and T. Helleseth, "A new three-valued cross correlation between m-sequences of different lengths," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4695–4701, 2006.

[219] G. J. Ness and T. Helleseth, "A new family of four-valued cross correlation between m-sequences of different lengths," *IEEE Trans. Inform. Theory*, vol. 53, no. 11, pp. 4308–4313, 2007.

[220] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*, ser. London Mathematical Society Lecture Note Series. Cambridge: Cambridge University Press, 2001, vol. 285.

[221] Y. Niho, "Multivalued cross-correlation functions between two maximal linear recursive sequence," Ph.D. dissertation, Univ. Southern Calif., Los Angeles, 1970.

[222] C. Ngai, R. W. Yeung, and Z. Zhang, "Network generalized Hamming weight," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1136–1143, 2011.

[223] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 1994, vol. 765, pp. 55–64.

[224] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in cryptology (Paris, 1984)*, ser. Lecture Notes in Comput. Sci. Springer, Berlin, 1985, vol. 209, pp. 33–50.

[225] J. Y. Park, "The weight hierarchies of some product codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 2228–2235, 2000.

[226] N. Pavlidou, A. J. H. Vinck, J. Yazdani, and B. Honary. "Power line communications: state of the art and future trends," *IEEE Comm. Magazine*, vol. 41, no. 4, pp. 34–40, 2003.

[227] W. W. Peterson, "Some new results on finite fields with applications to BCH codes," in: R. C. Bose and T. A. Dowling, Eds., *Combinatorial Mathematics and Its Applications,* Univ. North Carolina Press, Chapel Hill, NC, 1969.

[228] W. W. Peterson and E. J. Weldon, *Error-correcting codes*, 2nd ed. The M.I.T. Press, Cambridge, Mass.-London, 1972.

[229] V. Pless, "Power moment identities on weight distributions in error correcting codes," *Inf. Control*, vol. 6, pp. 147–152, 1963.

[230] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.

[231] A. Pott and Y. Zhou, "Switching construction of planar functions on finite fields," in *Arithmetic of finite fields*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2010, vol. 6087, pp. 135–150.

[232] E. Rains, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.

[233] R. S. Rees. "Two new direct product-type constructions for resolvable group-divisible designs," *J. Combin. Des.*, vol. 1, no. 1, pp. 15–26, 1993.

[234] R. S. Rees. "Group-divisible designs with block size k having $k + 1$ groups, for $k = 4, 5$," *J. Combin. Des.*, vol. 8, no. 5, pp. 363–386, 2000.

[235] R. S. Rees. "Truncated transversal designs: a new lower bound on the number of idempotent MOLS of side n," *J. Combin. Theory Ser. A*, vol. 90, no. 2, pp. 257–266, 2000.

[236] R. S. Rees and D. R. Stinson. "On combinatorial designs with subdesigns," *Discrete Math.*, vol. 77, no. 1-3, pp. 259–279, 1989.

[237] S. E. Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Trans. Inform. Theory*, vol. 58, no. 3, pp. 1361–1371, 2012.

[238] P. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2005, pp. 1023–1027.

[239] D. Sarwate, "Meeting the Welch bound with equality," in *Sequences and their applications (Singapore, 1998)*, ser. Springer Ser. Discrete Math. Theor. Comput. Sci. London: Springer, 1999, pp. 79–102.

[240] D. Sarwate and M. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proceedings of the IEEE*, vol. 68, no. 5, pp. 593–619, 1980.

[241] H. G. Schaathun, "The weight hierarchy of product codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2648–2651, 2000.

[242] H. G. Schaathun and W. Willems, "A lower bound on the weight hierarchies of product codes," *Discrete Appl. Math.*, vol. 128, no. 1, pp. 251–261, 2003.

[243] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Math. Comp.*, vol. 44, no. 170, pp. 483–494, 1985.

[244] J. Schwinger, "Unitary operator bases," *Proc. Nat. Acad. Sci. U.S.A.*, vol. 46, pp. 570–579, 1960.

[245] E. Y. Seo, Y. S. Kim, J. S. No, and D. J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $(\frac{p^{2k}+1}{2})^2$," *IEEE Trans. Inform. Theory*, vol. 54, no. 7, pp. 3140–3149, 2008.

[246] C. Shim and H. Chung, "On the second generalized Hamming weight of the dual code of a double-error-correcting binary BCH code," *IEEE Trans. Inform. Theory*, vol. 41, no. 3, pp. 805–808, 1995.

[247] P. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. R2493–R2496, 1995.

[248] I. E. Shparlinski and A. Winterhof, "Constructions of approximately mutually unbiased bases," in *LATIN 2006: Theoretical informatics*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2006, vol. 3887, pp. 793–799.

[249] D. A. Sprott. "A series of symmetrical group divisible incomplete block designs," *Ann. Math. Statist.*, vol. 30, no. 1, pp. 249–251, 1959.

[250] A. Steane, "Multiple particle interference and quantum error correction," *Proc. R. Soc. Lond. A*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[251] A. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.

[252] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., ser. Grad. Texts in Math. Berlin: Springer, 2009, vol. 254.

[253] H. Stichtenoth and C. Voß, "Generalized Hamming weights of trace codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 554–558, 1994.

[254] D. R. Stinson. "A general construction for group-divisible designs," *Discrete Math.*, vol. 33, no. 1, pp. 89–94, 1981.

[255] D. R. Stinson. "Frames for Kirkman triple systems," *Discrete Math.*, vol. 65, no. 3, pp. 289–300, 1987.

[256] L. Storme, "Finite geometry," in *The CRC Handbook of Combinatorial Designs*, 2nd ed. Boca Raton: CRC Press, 2007, pp. 702–729.

[257] T. Strohmer and R. W. Heath, "Grassmannian frames with applications to coding and communication," *Appl. Comput. Harmon. Anal.*, vol. 14, no. 3, pp. 257–275, 2003.

[258] M. A. Sustik, J. A. Tropp, I. S. Dhillon, and R. W. Heath, "On the existence of equiangular tight frames," *Linear Algebra Appl.*, vol. 426, no. 2-3, pp. 619–635, 2007.

[259] A. Thangaraj and S. McLaughlin, "Quantum codes from cyclic codes over $\mathrm{GF}(4^m)$," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1176–1178, 2001.

[260] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inform. Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[261] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, ser. Mathematics and its Applications (Soviet Series). Dordrecht: Kluwer, 1991, vol. 58.

[262] M. A. Tsfasman and S. G. Vlăduţ, "Geometric approach to higher weights," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1564–1588, 1995.

[263] G. van der Geer and M. van der Vlugt, "Generalized Hamming weights of Melas codes and dual Melas codes," *SIAM J. Discrete Math.*, vol. 7, no. 4, pp. 554–559, 1994.

[264] G. van der Geer and M. van der Vlugt, "On generalized Hamming weights of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 543–546, 1994.

[265] G. van der Geer and M. van der Vlugt, "Fibre products of Artin-Schreier curves and generalized Hamming weights of codes," *J. Combin. Theory Ser. A*, vol. 70, no. 2, pp. 337–348, 1995.

[266] G. van der Geer and M. van der Vlugt, "Generalized hamming weights of BCH(3) revisited," *IEEE Trans. Inform. Theory*, vol. 41, no. 1, pp. 300–301, 1995.

[267] G. van der Geer and M. van der Vlugt, "The second generalized Hamming weight of the dual codes of double-error correcting binary BCH-codes," *Bull. London Math. Soc.*, vol. 27, no. 1, pp. 82–86, 1995.

[268] G. van der Geer and M. van der Vlugt, "Quadratic forms, generalized Hamming weights of codes and curves with many points," *J. Number Theory*, vol. 59, no. 1, pp. 20–36, 1996.

[269] M. van der Vlugt, "On the weight hierarchy of irreducible cyclic codes," *J. Combin. Theory Ser. A*, vol. 71, no. 1, pp. 159–167, 1995.

[270] M. van der Vlugt, "A note on generalized Hamming weights of BCH(2)," *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 254–256, 1996.

[271] G. Vega, "The weight distribution of an extended class of reducible cyclic codes," *IEEE Trans. Inform. Theory*, vol. 58, no. 7, pp. 4862–4869, 2012.

[272] G. Vega and L. B. Morales, "A general description for the weight distribution of some reducible cyclic codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 9, pp. 5994–6001, 2013.

[273] Z. Wan, *Geometry of classical groups over finite fields*, 2nd ed. Beijing: Science Press, 2006.

[274] Z. Wan, *Lectures on finite fields and Galois rings*. River Edge, NJ: World Scientific Publishing Co. Inc., 2003.

[275] B. Wang, C. Tang, Y. Qi, Y. Yang, and M. Xu, "The weight distributions of cyclic codes and elliptic curves," *IEEE Trans. Inform. Theory*, vol. 58, no. 12, pp. 7253–7259, 2012.

[276] J. Wang and J. Yin. "Two-dimensional optical orthogonal codes and semicyclic group divisible designs," *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2177–2187, 2010.

[277] L. Wang and S. Zhu, "New quantum MDS codes derived from constacyclic codes," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 881–889, 2015.

[278] Q. Wang and Y. Zhou. "Sets of zero-difference balanced functions and their applications," *Adv. Math. Commun.*, vol. 8, no. 1, pp. 83–101, 2014.

[279] X. Wang and J. Wang. "Partitioned difference families and almost difference sets," *J. Statist. Plann. Inference*, vol. 141, no. 5, pp. 1899–1909, 2011.

[280] L. C. Washington, *Elliptic curves: Number theory and cryptography*, 2nd ed., ser. Discrete Math. Appl. (Boca Raton). Boca Raton, FL: Chapman & Hall/CRC, 2008.

[281] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

[282] V. K. Wei and K. Yang, "On the generalized Hamming weights of product codes," *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1709–1713, 1993.

[283] L. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, no. 3, pp. 397–399, 1974.

[284] R. M. Wilson. "An existence theory for pairwise balanced designs. I. Composition theorems and morphisms," *J. Combin. Theory Ser. A*, vol. 13, no. 2, pp. 220–245, 1972.

[285] R. M. Wilson. "An existence theory for pairwise balanced designs. II. The structure of PBD-closed sets and the existence conjectures," *J. Combin. Theory Ser. A*, vol. 13, no. 2, pp. 246–273, 1972.

[286] R. M. Wilson. "An existence theory for pairwise balanced designs. III. Proof of the existence conjectures," *J. Combin. Theory Ser. A*, vol. 18, no. 1, pp. 71–79, 1975.

[287] R. M. Wilson. "Cyclotomy and difference families in elementary abelian groups," *J. Number Theory*, vol. 4, no. 1, pp. 17–47, 1972.

[288] J. Wolfmann, "Weight distributions of some binary primitive cyclic codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 2068–2071, 1994.

[289] W. K. Wootters and B. D. Fields, "Optimal state determination by mutually unbiased measurements," *Ann. Phys.*, vol. 191, no. 2, pp. 363–381, 1989.

[290] P. Xia, S. Zhou, and G. B. Giannakis, "Achieving the Welch bound with difference sets," *IEEE Trans. Inform. Theory*, vol. 51, no. 5, pp. 1900–1907, 2005.

[291] Y. Xia, X. Zeng, and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Engrg. Comm. Comput.*, vol. 21, no. 5, pp. 329–342, 2010.

[292] M. Xiong, "The weight distributions of a class of cyclic codes," *Finite Fields Appl.*, vol. 18, no. 5, pp. 933–945, 2012.

[293] C. P. Xing, H. Niederreiter, and K. Y. Lam, "Constructions of algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 4, pp. 1186–1193, 1999.

[294] E. Yaakobi, J. Bruck, and P. H. Siegel. "Decoding of cyclic codes over symbol-pair read channels," In *Proc. Int. Symp. Inf. Theory*, pages 2891–2895, 2012.

[295] J. Yang, M. Xiong, C. Ding, and J. Luo, "Weight distribution of a class of cyclic codes with arbitrary number of zeros," *IEEE Trans. Inform. Theory*, vol. 59, no. 9, pp. 5985–5993, 2013.

[296] K. Yang, P. V. Kumar, and H. Stichtenoth, "On the weight hierarchy of geometric Goppa codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp. 913–920, 1994.

[297] M. Yang, J. Li, K. Feng, and D. Lin, "Generalized Hamming weights of irreducible cyclic codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 9, pp. 4905–4913, 2015.

[298] J. Yin, X. Shan, and Z. Tian. "Constructions of partitioned difference families," *European J. Combin.*, vol. 29, no. 6, pp. 1507–1519, 2008.

[299] D. Yue and G. Feng, "Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2625–2628, 2000.

[300] D. Yue and H. Zhu, "On the minimum distance of composite-length BCH codes," *IEEE Communications Letters*, vol. 3, no. 9, pp. 269–271, 1999.

[301] X. Zeng, L. Hu, W. Jiang, Q. Yue, and X. Cao, "The weight distribution of a class of p-ary cyclic codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 56–73, 2010.

[302] X. Zeng, N. Li, and L. Hu, "A class of nonbinary codes and sequence families," in *Sequences and their applications—SETA 2008*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2008, vol. 5203, pp. 81–94.

[303] Z. Zha and L. Hu. "Cyclotomic constructions of zero-difference balanced functions with applications," *IEEE Trans. Inform. Theory*, vol. 61, no. 3, pp. 1491–1495, 2015.

[304] G. Zhang and B. Chen, "New quantum MDS codes," *Int. J. Quantum Inf.*, vol. 12, no. 4, p. 1450019, 2014.

[305] T. Zhang and G. Ge, "Some new classes of quantum MDS codes from constacyclic codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 9, pp. 5224–5228, 2015.

[306] Y. Zhou, "$(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations," *J. Combin. Des.*, vol. 21, no. 12, pp. 563–584, 2013.

[307] Y. Zhou. *Difference Sets From Projective Planes*. PhD thesis, University of Magdeburg, 2013.

[308] Z. Zhou, C. Ding, J. Luo, and A. Zhang, "A family of five-weight cyclic codes and their weight enumerators," *IEEE Trans. Inform. Theory*, vol. 59, no. 10, pp. 6674–6682, 2013.

[309] Z. Zhou, X. Tang, D. Wu, and Y. Yang. "Some new classes of zero-difference balanced functions," *IEEE Trans. Inform. Theory*, vol. 58, no. 1, pp. 139–145, 2012.

[310] L. Zhu. "Some recent developments on BIBDs and related designs," *Discrete Math.*, vol. 123, no. 1-3, pp. 189–214, 1993.

个人简介

- 李抒行，男，浙江大学数学科学学院，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：sxli@zju.edu.cn

- 教育经历：

  2006.9–2010.6，浙江大学数学科学学院，数学与应用数学专业，理学学士.

  2010.9– 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：代数编码、组合设计和代数组合.

- 研究兴趣：代数编码、组合设计理论，代数组合学.

攻读博士学位期间主要研究成果

[1] S. Li, F. Gao, G. Ge, and S. Zhang. Deterministic construction of compressed sensing matrices via algebraic curves. *IEEE Transactions on Information Theory*, 58(8):5035–5041, 2012. **(ZJU Top 100)**

[2] S. Li and G. Ge. Deterministic construction of sparse sensing matrices via finite geometry. *IEEE Transactions on Signal Processing*, 62(11):2850–2859, 2014. **(ZJU Top)**

[3] S. Li and G. Ge. Deterministic sensing matrices arising from near orthogonal systems. *IEEE Transactions on Information Theory*, 60(4):2291–2302, 2014. **(ZJU Top 100)**

[4] S. Li, S. Hu, T. Feng, and G. Ge. The weight distribution of a class of cyclic codes related to Hermitian forms graphs. *IEEE Transactions on Information Theory*, 59(5):3064–3067, 2013. **(ZJU Top 100)**

[5] S. Li, T. Feng, and G. Ge. On the weight distribution of cyclic codes with Niho exponents. *IEEE Transactions on Information Theory*, 60(7):3903–3912, 2014. **(ZJU Top 100)**

[6] T. Zhang, S. Li, T. Feng, and G. Ge. Some new results on the cross correlation of m-sequences. *IEEE Transactions on Information Theory*, 60(5):3062–3068, 2014. **(ZJU Top 100)**

[7] M. Xiong, S. Li, and G. Ge. The weight hierarchy of some reducible cyclic codes. *IEEE Transactions on Information Theory* Accepted. **(ZJU Top 100)**

[8] T. Feng, S. Hu, S. Li, and G. Ge. Difference sets with few character values. *Designs, Codes and Cryptography*, 73(3):825–839, 2014. **(SCI)**

[9] S. Hu, S. Li, T. Zhang, T. Feng, and G. Ge. New pseudo-planar binomials in characteristic two and related schemes. *Designs, Codes and Cryptography*, 76(2):345–360, 2015. **(SCI)**

[10] S. Li, H. Wei, and G. Ge. Generic constructions for partitioned difference families with applications: A unified combinatorial approach. *Designs, Codes and Cryptography* Accepted. **(SCI)**

[11] G. Ge, S. Li, and H. Wei. A new construction of group divisible designs with non-uniform group type. *Journal of Combinatorial Designs* Accepted. **(SCI)**

[12] S. Li, M. Xiong, and G. Ge. Pseudo-cyclic codes and the construction of quantum MDS codes. *IEEE Transactions on Information Theory*, 62(4):1703–1710, 2016. **(ZJU Top 100)**

[13] S. Li, C. Ding, M. Xiong, and G. Ge. Narrow-sense BCH codes over GF(q) with length $n = \frac{q^m-1}{q-1}$. Submitted.

[14] S. Li and G. Ge. Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes. Submitted.