源于秘密共享应用的若干编码与组合设计问题

（申请清华大学理学博士学位论文）

培 养 单 位：数学科学系

学　　科：数学

研　究　生：吴 华 伟

指 导 教 师：杨　　晶　副教授

二〇二四年五月

Several Problems on Codes and Combinatorial Designs Arising from Secret Sharing Applications

Dissertation submitted to

Tsinghua University

in partial fulfillment of the requirement

for the degree of

Doctor of Philosophy

in

Mathematics

by

Wu Huawei

Dissertation Supervisor: Associate Professor Yang Jing

May, 2024

学位论文公开评阅人和答辩委员会名单

公开评阅人名单

曹喜望	教授	南京航空航天大学
冯荣权	教授	北京大学
陆玫	教授	清华大学
王丽萍	研究员	中国科学院信息工程研究所

答辩委员会名单

主席	冯荣权	教授	北京大学
委员	冯克勤	教授	清华大学
	陆玫	教授	清华大学
	王丽萍	研究员	中国科学院信息工程研究所
	杨晶	副教授	清华大学
秘书	李培根	博士后研究员	北京雁栖湖应用数学研究院

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容；（3）根据《中华人民共和国学位条例暂行实施办法》及上级教育主管部门具体要求，向国家图书馆报送相应的学位论文。

本人保证遵守上述规定。

（保密的论文在解密后遵守此规定）

作者签名：_____ 导师签名：_____

日　　期：_____ 日　　期：_____

摘 要

秘密共享与编码理论及组合设计理论之间存在着密切的联系。从线性纠错码和组合设计出发构造秘密共享方案，是现有的构造秘密共享方案的常用方法。本文研究源自秘密共享应用的若干编码与组合设计的问题，主要分为以下两个部分：

(1) 本文研究了两类由 Carlet、丁存生等人提出的基于有限域 $\mathbb{F}_{p^m}$ 上完全非线性函数 Π 的线性码：C_Π 与 $\overline{C_\Pi}$，其中 p 为一个奇素数。这两类线性码不仅本身具有良好的参数，并且由它们的对偶码构造的秘密共享方案具有非常有应用价值的存取结构。在本文中，对于 m 为奇数的情形，我们采用了一个统一的方法，对任意的奇素数 p，不依赖于 Π 的具体形式，只利用它是完全非线性函数这一条件，即可确定 C_Π 和 $\overline{C_\Pi}$ 的重量分布（定理3.6及定理3.7）。对于 m 为偶数的情形，我们给出了一些宽松的条件（目前已知的 $\mathbb{F}_{p^m}$ 上的完全非线性函数均满足这些条件中的至少一个），使得类似的结论依然成立（定理3.6及定理3.7）。此外，基于我们得到的重量分布的结果，我们探讨了 C_Π 与 $\overline{C_\Pi}$ 的覆盖问题，使得绝大部分的情形得到了解决（定理3.9及定理3.10）。

(2) 本文研究了两类由 Veitch 和 Stinson 为了构造无条件安全的不可延展秘密共享方案而提出的新组合对象：循环外差族与强循环外差族。它们作为外差族与强外差族的变形，无论是单纯作为组合设计理论中的新概念，还是出于构造秘密共享方案等现实应用的目的，都是非常值得研究的对象。在本文中，我们利用有限域中的分圆类构造出循环外差族的无穷族（推论4.1）、证明了所有的强循环外差族都是平凡的（推论4.2），并且给出一个新的强外差族的不存在性结果（定理4.9），从而回答了 Veitch 和 Stinson 提出的若干开放问题。

本文中使用的方法与技术兼具典型性与创新性，不仅使我们得到了新的重要结果，同时对于相关主题的研究也具有启发意义。

关键词：秘密共享；完全非线性函数；线性码；差集；循环外差族

Abstract

Secret sharing has a close connection with coding theory and combinatorial design theory. Constructing secret sharing schemes from linear error-correcting codes and combinatorial designs is a common method in existing constructions. This thesis investigates several problems on codes and combinatorial designs arising from secret sharing applications, primarily divided into the following two parts:

(1) The thesis studies two classes of linear codes C_{Π} and $\overline{C_{\Pi}}$ constructed from perfect nonlinear functions Π over the finite field $\mathbb{F}_{p^m}$, which were proposed by Carlet, Ding Cunsheng, et al., where p is an odd prime. These linear codes possess nice parameters, whose dual codes lead to secret sharing schemes with highly valuable access structures. In this thesis, when m is odd, we employ a unified approach to determining the weight distributions of C_{Π} and $\overline{C_{\Pi}}$ only using the assumption that Π has perfect nonlinearity for any odd prime p (see Theorem 3.6 and Theorem 3.7). When m is even, we provide some mild conditions (all the known perfect nonlinear functions over $\mathbb{F}_{p^m}$ satisfy at least one of these conditions) under which similar conclusions still hold (see Theorem 3.6 and Theorem 3.7). Furthermore, based on the obtained weight distribution results, we explore the covering problem of C_{Π} and $\overline{C_{\Pi}}$, resolving a majority of cases (see Theorem 3.9 and Theorem 3.10).

(2) The thesis investigates two new combinatorial objects proposed by Veitch and Stinson for constructing unconditionally secure non-malleable secret sharing schemes: circular external difference families and strong circular external difference families. These two objects, as variations of external difference families and strong external difference families, respectively, are significant both conceptually and practically. In this thesis, we construct an infinite family of circular external difference families using cyclotomic classes in finite fields (see Corollary 4.1), prove that all strong circular external difference families are trivial (see Corollary 4.2), and provide a new non-existence result for strong external difference families (see Theorem 4.9), thereby solving several open problems posed by Veitch and Stinson.

The methods and techniques employed in this thesis are characterized by both typicality and innovation, which not only lead to novel results but also inspire further exploration of related topics.

Keywords: Secret sharing; perfect nonlinear functions; linear codes; difference sets; circular external difference families

目 录

插图和附表清单

符号和缩略语说明

$\mathbb{N}$	自然数集 $\{0,1,2,\cdots\}$
$\mathbb{Z}$	整数环
$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$	有理数域，实数域，复数域
$\mathbb{F}_q$	含 q 个元素的有限域
$\mathbb{Z}_m$	整数环 $\mathbb{Z}$ 的模 m 剩余类环
R^*	含幺环 R 中的可逆元群
$\gcd(m,n)$	正整数 m 和 n 的最大公因数
$C^{\perp}$	线性码 C 的对偶码
$\lvert A\rvert$	集合 A 的元素个数
$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$	从有限域 $\mathbb{F}_q$ 到其子域 $\mathbb{F}_p$ 的迹映射
PN 函数	完全非线性函数 (Perfect Nonlinear Function)

第 1 章　引言

1.1　选题背景及其意义

秘密共享（secret sharing）是一种秘密分割存储技术，由 Blakley[1] 和 Shamir[2] 于 1979 年分别独立地提出。其核心思想是将完整的秘密拆分为 n 份，分别交给 n 名保管者保管，使得只有满足特定条件的部分保管者所保管的秘密份额“拼凑”起来，才能还原出完整的秘密。在一个秘密共享方案中，所有可以还原出完整秘密的保管者子集所构成的集合，称为该秘密共享方案的存取结构（access structure）。

阈值秘密共享（threshold secret sharing）是最常见、同时也是最被广泛研究的秘密共享类型。在一个 (k,n)-阈值秘密共享方案中，完整的秘密被分为 n 份，分别交给 n 名保管者保管，使得只有至少 k 名保管者所拥有的秘密份额“拼凑”起来，才可以还原出完整的秘密。上面提到的 Blakey 和 Shamir 的构造，就属于阈值秘密共享方案。Blakley 的构造依赖于有限几何，而 Shamir 的构造则使用多项式插值来还原出完整秘密。

在秘密共享的概念被提出后不久，其与编码理论的联系就被学者们所发现。1981 年，McEliece 和 Sarwate 发现 Shamir 的秘密共享方案与编码理论中的 Reed-Solomon 码之间存在联系[3]。1993 年，Massey 又给出一种基于纠错码的秘密共享方案的构造[4-5]。此后，许多学者沿着这个方向进行了深入的研究，从纠错码出发构造了许多的秘密共享方案[6-9]。

从原则上来说，每一个线性纠错码都可以给出一个秘密共享方案。然而，如何确定一个线性纠错码给出的的秘密共享方案的存取结构，可能是很困难的。实际上，这个问题等价于线性纠错码的覆盖问题（covering problem，参见3.7节），即如何确定一个线性纠错码中的极小码字，而只有一些特殊线性纠错码的覆盖问题得到了解决。因此，如果能解决一类新的线性纠错码的覆盖问题，那么不管是对编码理论本身，还是对秘密共享方案的构造，都具有重要的意义。

秘密共享与组合设计理论之间也存在着密不可分的联系。在许多的研究中，学者们发现，具有某种设计目标的秘密共享方案的构造，往往会归结为某类组合设计的存在性。事实上，秘密共享的问题叙述本身就具有很强的组合意味，因此与组合设计理论之间产生联系也并不奇怪。从组合设计出发构造秘密共享方案，也是现有的构造秘密共享方案的常用方法之一。反之，很多组合设计理论中的新概念，都是源自于秘密共享或其他通信应用中的需要。

在接下来的两小节中，我们将分别介绍源自秘密共享应用的一个编码问题和

一个组合设计问题，包括它们的问题背景、研究进展，以及其中尚未被解决的部分。

1.2　由完全非线性函数构造的线性码及其秘密共享方案

设 $(A,+)$ 和 $(B,+)$ 为两个有限交换加法群。称函数 $f:A\to B$ 为完全非线性函数（perfect nonlinear function），如果对任意的 $a\in A\setminus\{0\}$，差分函数 $D_af:A\to B$，$x\mapsto f(x+a)-f(x)$ 均为平衡函数，即对任意的 $b\in B$，都有 $|D_af^{-1}(b)|=|A|/|B|$。

完全非线性性是为了抵御差分密码分析而提出的，它是一种度量密码函数非线性程度的稳健指标。构造新的完全非线性函数，是一件很困难的事情。直到目前为止，所有已知的有限域 $\mathbb{F}_q$（$q=p^m$，p 为奇素数）到自身的完全非线性函数，在仿射等价的意义下，只有两大类：Dembowski-Ostrom 类和 Coulter-Matthews 类（参见3.1节）。

完全非线性函数还可以用于构造具有良好参数的线性纠错码。设 $\Pi:\mathbb{F}_q\to\mathbb{F}_q$ 为一个完全非线性函数。Carlet、丁存生等人在 2005 年考虑了下面两类 $\mathbb{F}_p$ 上的线性码[10]：

$$C_\Pi=\{c_{a,b}=\big(f_{a,b}(x)\big)_{x\in\mathbb{F}_q^*}:\ a,\ b\in\mathbb{F}_q\},\tag{1-1}$$

其中

$$f_{a,b}(x)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big(a\Pi(x)+bx\big),\tag{1-2}$$

及

$$\overline{C_\Pi}=\{c_{a,b,c}=\big(f_{a,b,c}(x)\big)_{x\in\mathbb{F}_q}:\ a,\ b,\ c\in\mathbb{F}_q\},\tag{1-3}$$

其中

$$f_{a,b,c}(x)=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big(a\Pi(x)+bx+c\big).\tag{1-4}$$

在式（1-2）和式（1-4）中，$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ 表示从有限域 $\mathbb{F}_q$ 到其子域 $\mathbb{F}_p$ 的迹映射（trace map）。他们证明了 C_Π 是一个 $[q-1,2m]_p$ 线性码（若 $\Pi(0)=0$），$\overline{C_\Pi}$ 是一个 $[q,1+2m]_p$ 线性码，并给出了 C_Π 和 $\overline{C_\Pi}$ 的最小非零汉明重量（Hamming weight）所满足的界。此外，他们还研究了这两类线性码的对偶码，考察了对偶码的最小距离并分析了其对应的秘密共享方案的存取结构，证明了这样构造出的秘密共享方案的存取结构根据对偶码的最小距离分为两类：一类是“民主”的，而另一类中包含“独裁者”（参见定理3.8）。这两类存取结构在现实世界中都普遍存在，具有不菲的应用价值。

一般而言，确定线性码的重量分布，对解决其覆盖问题而言是有很大帮助的

（参见3.7节）。因此，为了确定由 C_Π 和 $\overline{C_\Pi}$ 的对偶码构造出的秘密共享方案的存取结构，自然希望能够确定 C_Π 和 $\overline{C_\Pi}$ 的重量分布（当然，这本身也有重要意义），而这并未在 [10] 中完成。

2006 年，Carlet、丁存生等人对下面三类完全非线性函数 Π，确定了 C_Π 的重量分布[11]：

(1) $\Pi(x) = x^{p^k+1}$，其中 $k \in \mathbb{N}$ 且 $m/\gcd(m,k)$ 为奇数；

(2) $\Pi(x) = x^{\frac{3^k+1}{2}}$，其中 $p=3$，k、m 为奇数，且 $\gcd(m,k)=1$；

(3) $\Pi(x) = x^{10} - ux^6 - u^2x^2$，其中 $p=3$，m 为奇数且 $u \in \mathbb{F}_q^*$。

对于第二类中 m 为偶数的情形，他们未能解决。值得注意的是，他们对每一类完全非线性函数，都采用了不用的处理方法。此外，他们还发现，从上面三类完全非线性函数 Π 构造的 C_Π 中的许多，要么是最优的，要么是已知最优的。在这里，一个 $[n,k,d]_p$ 线性码被称为最优的，如果不存在 $[n,k,d']_p$ 线性码使得 $d' > d$。

2007 年，冯克勤与罗金权计算了由完全非线性函数构造的指数和的值分布，并将其结果用于确定 C_Π 的重量分布[12]。他们的方法，统一处理了 Dembowski-Ostrom 类型和 Coulter-Matthews 类型的完全非线性函数。至此，对所有已知的完全非线性函数 Π，C_Π 的重量分布都被确定了。

2008 年，李超、屈龙江及林杉用统一的方法，对上面给出的三类完全非线性函数 Π，确定了 C_Π 和 $\overline{C_\Pi}$ 的重量分布[13]。他们是第一次给出了 $\overline{C_\Pi}$ 的重量分布，并且他们确定 C_Π 重量分布的方法是新的。

前面提到的这些工作，用到的主要工具是指数和以及有限域上的二次型理论。这些工作有一个主要缺陷，即它们都依赖于完全非线性函数 Π 的具体形式，所以它们当中的结论只对已知的完全非线性函数 Π 成立。然而，从他们证明的结果来看，C_Π 和 $\overline{C_\Pi}$ 的重量分布并不依赖于 Π 的具体形式。因此，一个很自然的问题就是，能否找到一个统一的方法，不依赖于 Π 的具体形式，只利用它是完全非线性函数这一条件，即可确定 C_Π 和 $\overline{C_\Pi}$ 的重量分布。

2008 年，李超、李强及林杉对于 $p=3$ 的情形，通过研究某个整系数二次型表示整数的问题，确定了所有从 F_{3^m} 到 F_3 的完全非线性函数（此时也称为 Bent 函数，参见3.2节）的值分布，从而在仅仅利用 Π 是完全非线性函数这一条件的前提下，确定了 C_Π 的重量分布[14]。他们的出发点是下面这个引理：

引理 1.1 ([15]，定理 9)： 设 $(A,+)$ 和 $(B,+)$ 为两个有限交换加法群，其阶分别为 m 和 n，其中 $m \mid n$，并设 $f : A \to B$ 为一个完全非线性函数。对任意的 $b \in B$，令

$k_b = |f^{-1}(b)|$，则有

$$\begin{cases} \sum\limits_{z\in B} k_z^2 = \frac{n^2+(m-1)n}{m}, \\ \sum\limits_{z\in B} k_z k_{z+b} = \frac{n(n-1)}{m}, \ \forall\, b \in B \setminus \{0\}, \\ \sum\limits_{z\in B} k_z = n. \end{cases} \tag{1-5}$$

在一般情况下，式（1-5）第二行中的那些方程是非对称的，因此想要解它们是极为困难的。然而，若 $A = \mathbb{F}_{3^m}$ 且 $B = \mathbb{F}_3$，则式（1-5）中的方程组就变得极为简单（特别地，它是对称的）。实际上，此时解方程组（1-5）等价于确定下列整系数二次型表出 3^{m-1} 的所有方式：

$$X^2 + XY + Y^2. \tag{1-6}$$

这个策略并不能推广到一般的奇素数 p 的情形，因为此时式（1-5）中的方程组十分难解。因此，对于一般的奇素数 p，能否仅仅利用 Π 是完全非线性函数这一条件，来确定 C_Π 和 $\overline{C_\Pi}$ 的重量分布，依然是一个公开问题。

在第3章中，对于 m 为奇数的情形，我们将采用一个统一的方法，对任意的奇素数 p，不依赖于 Π 的具体形式，只利用它是完全非线性函数这一条件，来确定 C_Π 和 $\overline{C_\Pi}$ 的重量分布。对于 m 为偶数的情形，我们将给出一些宽松的条件（目前已知的 $\mathbb{F}_q$ 上的完全非线性函数均满足这些条件中的至少一个），使得类似的结论依然成立。确定了 C_Π 和 $\overline{C_\Pi}$ 的重量分布后，我们将进一步探讨它们的对偶码所确定的秘密共享方案的存取结构。

1.3　无条件安全的不可延展秘密共享与循环外差族

通常来说，我们考虑的都是无条件安全（unconditionally secure）的秘密共享。也就是说，方案的安全性不受攻击者的算力影响。在本节中，我们只考虑无条件安全的秘密共享。

Tompa 和 Woll 在 1989 年提出了稳健（robust）秘密共享的概念[16]，第一次挑战了经典的秘密共享对抗模型。在他们的模型中，一部分秘密共享的参与者可能不怀好意地篡改他们所保管的秘密份额，从而使得还原出来的完整秘密是错误但有意义的。可以证明，Shamir 基于多项式插值的构造[2] 并不是稳健的。下面这个基于游戏的定义，与 Tompa 和 Woll 在 [16] 中给出的描述是等价的：

定义 1.1 (稳健性游戏)： 设有一个 (k, n)-阈值秘密共享方案，其中秘密 s 等概率地取自所有可能秘密构成的集合 S。

- 步骤 1. 分发者选取秘密 $s \in S$ 并生成 n 个秘密份额；

- 步骤 2. 将 n 份中的 $k-1$ 份交给攻击者，且攻击者篡改了这 $k-1$ 个秘密份额；
- 步骤 3. 由攻击者选取 k 个秘密份额（包含 $k-1$ 个被篡改的），用它们还原出完整秘密 s'。在这个过程中，攻击者可以选择使用哪一个未被篡改的秘密份额，但是无法知道它的具体值。

称攻击者赢得这个稳健性游戏，如果还原出的完整秘密 s' 满足 $s' \in \mathcal{S}$ 且 $s' \neq s$。如果攻击者赢得这个稳健性游戏的概率不超过 ϵ，那么我们称这个秘密共享方案是一个 ϵ-稳健的秘密共享方案。

有许多方法可以实现稳健秘密共享，其中最普遍的是使用代数操作检测码（algebraic manipulation detection code，简称 AMD 码）。AMD 码由 Cramer、Dodis 及 Fehr 等人于 2008 年提出[17]，分为强弱两种版本。与弱版本相比，强版本的 AMD 码可以应对攻击者事先知道完整秘密源集合的情形。弱 AMD 码与强 AMD 码的定义如下：

定义 1.2 (弱 AMD 码)： 设 G 为一个有 n 个元素的有限交换群，$\mathcal{A} = \{A_0, \cdots, A_{m-1}\}$ 为一个由 G 中 m 个两两不相交的 l-子集构成的子集族（即每个 A_i 的元素个数均为 l）。对于 $0 < \epsilon < 1$，称 $(G, \mathcal{A})$ 为一个 ϵ-安全的弱 (n, m, l)-AMD 码，如果攻击者赢得下述 AMD 游戏的概率不超过 ϵ：

- 步骤 1. 攻击者选取一个 $\Delta \in G \setminus \{0\}$；
- 步骤 2. 从 $\{0, 1, \cdots, m-1\}$ 中（均匀）随机地选取一个源下标 i；
- 步骤 3. 从 A_i 中（均匀）随机地选取一个元素 g；
- 步骤 4. 如果对于某个 $j \neq i$，有 $g + \Delta \in A_j$，则攻击者赢得游戏。

定义 1.3 (强 AMD 码)： 设 G 为一个有 n 个元素的有限交换群，$\mathcal{A} = \{A_0, \cdots, A_{m-1}\}$ 为一个由 G 中 m 个两两不相交的 l-子集构成的子集族。对于 $0 < \epsilon < 1$，称 $(G, \mathcal{A})$ 为一个 ϵ-安全的强 (n, m, l)-AMD 码，如果攻击者赢得下述强 AMD 游戏的概率不超过 ϵ：

- 步骤 1. 指定一个源下标 $i \in \{0, 1, \cdots, m-1\}$ 给攻击者；
- 步骤 2. 攻击者选取一个 $\Delta \in G \setminus \{0\}$；
- 步骤 3. 从 A_i 中（均匀）随机地选取一个元素 g；
- 步骤 4. 如果对于某个 $j \neq i$，有 $g + \Delta \in A_j$，则攻击者赢得游戏。

不可延展性（non-malleability）是一个比稳健性更弱的概念。在一个 (k, n)-阈值秘密共享方案中，稳健性意味着可以抵御最多 $k-1$ 个秘密份额的篡改，而不可延展性仅仅要求可以抵御某些特定类型的篡改。密码学中的不可延展性概念，是由 Dolev、Dwork 及 Naor 于 2000 年在公钥加密方案的背景下引入的[18]，它的含

义是使得攻击者无法对密文进行可预测的修改。之后，这一概念被引申到了其他的密码学领域中[19-21]，包括秘密共享。

文献中首次提到不可延展的秘密共享，是在 2006 年 Kenthapadi 的一篇博士毕业论文[22] 及其与 Dwork 等人的一篇关于分布式噪声生成的论文[23] 中。他们提出的不可延展可验证秘密共享，是可验证秘密共享（VSS）的一种拓展。虽然他们并没有给出不可延展 VSS 的形式定义，但是主要的想法已然形成。

2008 年，Ishai、Prabhakaran 及 Sahai 在一篇关于多方计算的论文[24] 的扩展版本中，提出了不可延展秘密共享的另一种定义。在他们的文章中，他们称一个 $(2,2)$-阈值秘密共享方案是不可延展的，如果攻击者无法赢得下面的游戏：

- 步骤 1. 由完整秘密 s 产生两个秘密份额 a 和 b；
- 步骤 2. 攻击者修改其中一个秘密份额，比如说 a，得到 $\tilde{a}$；
- 步骤 3. 将秘密份额 $\tilde{a}$ 和 b“拼凑”起来，还原出完整的秘密 s'。如果 $\tilde{a} \neq a$ 且 s' 是有意义的秘密，则攻击者赢得游戏。

如果攻击者赢得上述游戏的概率不超过 ϵ，则称该秘密共享方案是 ϵ-不可延展的。此后，在一些研究安全计算公平性的工作中，学者们使用了相同的不可延展秘密共享的定义[25-27]。此外，学者们已经渐渐注意到，与实现稳健秘密共享类似，这种不可延展秘密共享也可以通过 AMD 码来实现[17,26]。

在 2010 年被引入的不可延展码[20,28]，是这方面工作进展的另一路线。在编码理论中，不可延展码可以看作是对纠错码与检错码的放宽。在这里，“不可延展”的定义涉及篡改函数（tampering function）族，其目标是使得篡改后的信息解码出来要么是正确的，要么是与原始信息“独立且无关”的。

对不可延展秘密共享的正式研究，始于 Goyal 和 Kumar 在 2018 年的一项工作[29]。在该研究中，他们提出了基于不可延展码的不可延展阈值秘密共享方案。他们给出了不可延展秘密共享的形式定义，该定义为不可延展码在所谓“分割状态模型”（split-state model）中的推广版本。近期关于不可延展秘密共享的研究，大多都是基于这个定义的。这些研究前期主要集中在阈值秘密共享上，后来的一些则考虑了一般的存取结构[30-32]——它们当中给出的构造均满足统计隐私性与统计不可延展性。

Albab，Issa 及 Varia 等人在 2022 年基于 Goyal 和 Kumar 的想法，提出了一个在无条件安全框架下的不可延展秘密共享的定义[33]。然而，他们的定义只针对增量式（incremental）秘密共享。在一个增量式秘密共享方案中，随着秘密份额的提交，一个累积器被维护，并且最终的累积器就对应于原始的完整秘密。他们的定义无法推广到一般的情形，因为他们基于游戏的定义排除了最后一个份额由对手

控制的可能性。

为了解决上述不足，Veitch 和 Stinson 提出了如下的基于游戏的无条件安全的不可延展秘密共享的定义[34]。这一定义的基本思想是，攻击者不应该能够以某种预先指定的方式修改秘密份额，使得还原后得到的完整秘密与真实秘密通过在可能秘密集上的某种特定关系相关联。他们给出的定义具体如下：

定义 1.4 (∼-延展性游戏，[34]，定义 3.1)： 设有一个 (k,n)-阈值秘密共享方案，其中秘密 s 等概率地取自所有可能秘密构成的集合 $\mathcal{S}$，而 $\sim$ 是 $\mathcal{S}$ 上的一个非自反二元关系（即对任意的 $s\in\mathcal{S}$，有 $s\nsim s$）。令 t 为满足 $1\leqslant t<k$ 的一个整数。

- 步骤 1. 分发者选取秘密 $s\in\mathcal{S}$ 并生成 n 个秘密份额；
- 步骤 2. 将 n 份中的 t 份交给攻击者，且攻击者篡改了这 t 个秘密份额；
- 步骤 3. 由攻击者选取 k 个秘密份额（包含 t 个被篡改的），用它们还原出完整秘密 s'。在这个过程中，攻击者可以选择使用哪 $k-t$ 个未被篡改的秘密份额，但是无法知道它们的具体值。

称攻击者赢得这个 $\sim$-延展性游戏，如果还原出的完整秘密 s' 满足 $s'\in\mathcal{S}$ 且 $s'\sim s$。如果攻击者赢得这个 $\sim$-延展性游戏的概率不超过 ϵ，那么我们称这个秘密共享方案为 ϵ-安全的 t-不可延展秘密共享方案（相对于关系 $\sim$）。

注释 1.1： 如果我们考虑不等于关系 $\neq$，则攻击者赢得 $\neq$-延展性游戏的条件即为 $s\in\mathcal{S}$ 且 $s'\neq s$。对照定义1.1，可以看出 $\neq$-不可延展性的定义与稳健性的定义是等价的（如果 $t=k-1$）。

提出上述定义后，Veitch 和 Stinson 聚焦于如下的加性关系：

定义 1.5 (加性关系，[34]，定义 3.2)： 设 m 为一个正整数，整数 c 满足 $1\leqslant c\leqslant m-1$。定义关系 $\sim_c$ 如下：对于 s，$s'\in\mathbb{Z}_m$，$s'\sim_c s$ 当且仅当 $s'-s\equiv c\pmod m$。

可以证明，Shamir 基于多项式插值的构造[2] 相对于上述加性关系，并不是不可延展的，即我们有：

命题 1.1 ([34]，定理 3.1)： 设 p 为一个素数，整数 c 满足 $1\leqslant c\leqslant p-1$，则秘密取自 $\mathbb{Z}_p$ 的 (k,n)-Shamir 阈值秘密共享方案不是 $\sim_c$-不可延展的。

为了构造 $\sim_c$-不可延展秘密共享方案，Veitch 和 Stinson 引入了一种新的 AMD 码：弱循环 AMD 码，其定义如下：

定义 1.6 (弱循环 AMD 码，[34]，定义 4.1)： 设 G 为一个有 n 个元素的有限交换群，$\mathcal{A}=\{A_0,\cdots,A_{m-1}\}$ 为一个由 G 中 m 个两两不相交的 l-子集构成的子集族。对于 $0<\epsilon<1$ 以及整数 c 满足 $1\leqslant c\leqslant m-1$，称 $(G,\mathcal{A})$ 为一个 ϵ-安全的弱 c-循环 (n,m,l)-AMD 码，如果攻击者赢得下述循环 AMD 游戏的概率不超过 ϵ：

- 步骤 1. 攻击者选取一个 $\Delta\in G\setminus\{0\}$；

- 步骤 2. 从 $\{0,1,\cdots,m-1\}$ 中（均匀）随机地选取一个源下标 i；
- 步骤 3. 从 A_i 中（均匀）随机地选取一个元素 g；
- 步骤 4. 如果 $g+\Delta\in A_j$，其中 $j\equiv i+c \pmod m$，则攻击者赢得游戏。

与稳健性的情形相似，如果可以构造出一个弱循环 AMD 码，那么就可以基于它构造出一个 $\sim_c$-不可延展秘密共享方案。

AMD 码与组合设计理论中的外差族之间存在密切关系。外差族是组合设计理论中经典概念——差族的变形，由 Levenshtein 于 1971 年提出[35]，可以用于构造安全同步通信中的最优无逗点码。后来，Ogata 等人又发现外差族及强外差族（参见4.1节）可以用于构造安全校验码以及秘密共享方案[36]。在 [37] 中，Paterson 和 Stinson 定义了 R-最优弱 AMD 码，并证明了其与外差族的等价性。一个弱 AMD 码被称为 R-最优的，如果攻击者赢得定义1.2中 AMD 游戏的概率取到最小可能值。更准确的定义如下：

定义 1.7 (R-最优弱 AMD 码)： 一个弱 (n,m,l)-AMD 码被称为 R-最优的，如果它是 ϵ-安全的，其中

$$\epsilon=\frac{l(m-1)}{n-1}. \tag{1-7}$$

类比于弱 AMD 码与外差族的关系，Veitch 和 Stinson 提出了一种新的外差族：循环外差族（参见4.2节），并证明了一个 R-最优弱 c-循环 (n,m,l)-AMD 码等价于一个 $(n,m,l;\lambda)$-c-循环外差族，其中 $\lambda=ml^2/(n-1)$[34]。对于弱循环 AMD 码，R-最优的定义如下：

定义 1.8 (R-最优弱循环 AMD 码，[34]，定义 4.4)： 一个弱 c-循环 (n,m,l)-AMD 码被称为 R-最优的，如果它是 ϵ-安全的，其中

$$\epsilon=\frac{l}{n-1}. \tag{1-8}$$

AMD 码根据是否可以应对攻击者事先知道完整秘密源集合的情形，分为强弱两种版本。类似地，也可以考虑强循环 AMD 码，其定义如下：

定义 1.9 (强循环 AMD 码，[34]，定义 4.6)： 设 G 为一个有 n 个元素的有限交换群，$\mathcal{A}=\{A_0,\cdots,A_{m-1}\}$ 为一个由 G 中 m 个两两不相交的 l-子集构成的子集族。对于 $0<\epsilon<1$ 以及整数 c 满足 $1\leqslant c\leqslant m-1$，称 $(G,\mathcal{A})$ 为一个 ϵ-安全的强 c-循环 (n,m,l)-AMD 码，如果攻击者赢得下述强循环 AMD 游戏的概率不超过 ϵ：

- 步骤 1. 指定一个源下标 $i\in\{0,1,\cdots,m-1\}$ 给攻击者；
- 步骤 2. 攻击者选取一个 $\Delta\in G\setminus\{0\}$；
- 步骤 3. 从 A_i 中（均匀）随机地选取一个元素 g；
- 步骤 4. 如果 $g+\Delta\in A_j$，其中 $j\equiv i+c \pmod m$，则攻击者赢得游戏。

同样地，可以证明，一个 R-最优强 c-循环 (n,m,l)-AMD 码等价于一个 $(n,m,l;\lambda)$-强 c-循环外差族（参见4.3节），其中 $\lambda=l^2/(n-1)$。

另一方面，可以将定义1.5中的加性关系 $\sim_c$ 推广到一般的非空子集 $S\subseteq\mathbb{Z}_m\setminus\{0\}$ 上。相应地，可以考虑弱 S-循环 AMD 码与 S-循环外差族（参见定义4.4）。S-加性关系 $\sim_S$ 的定义如下：

定义 1.10 (S-加性关系)： 设 m 为一个正整数，S 为 $\mathbb{Z}_m\setminus\{0\}$ 的一个非空子集。定义关系 $\sim_S$ 如下：对于 s，$s'\in\mathbb{Z}_m$，$s'\sim_S s$ 当且仅当 $s'-s\in S$。

综上所述，弱循环 AMD 码与强循环 AMD 码的研究，分别可以转换为循环外差族与强循环外差族的研究。与外差族和强外差族一样，循环外差族和强循环外差族，无论是单纯作为组合设计理论中的新概念，还是出于构造秘密共享方案等现实应用的目的，都是非常值得研究的对象。

在 [34] 中，Veitch 和 Stinson 给出了一些循环外差族的构造。之后，基于词典积（lexicographic product）的优雅标号（labelling）与有限域中的分圆理论，Paterson 和 Stinson 给出了更多的系统性构造方法[38]。同时，他们也遗留下一些开放问题，主要包括以下几个：

(1) 是否存在非平凡的强循环外差族？

(2) 如何构造循环外差族的无穷族，特别是参数 $\lambda=1$ 的？

(3) 对于一般的子集 $S\subseteq Z_m\setminus\{0\}$，如何构造 S-循环外差族？

在第4章中，我们将深入地研究循环外差族与强循环外差族，从而在某种程度上解决上述的开放问题。具体的结果包括：

(1) 对于循环外差族，我们将从多个角度推广 [34] 中的分圆构造。特别地，我们将会证明：只要素数方幂 $q=4m+1\geqslant 13$，那么 $(\mathbb{F}_q,+)$ 中必然存在某个 $(q,m,2;1)$-c-循环外差族，其中 $c\in\{1,\cdots,m\}$。此外，我们将会证明一个循环外差族的提升定理。

(2) 对于强循环外差族，我们将证明所有的强循环外差族都是平凡的，即它们都是通过拼凑若干 $(n,2,l;\lambda)$-强外差族所得。我们也将证明一个新的关于这种类型的强外差族的不存在性结果。

1.4　论文结构安排

本文后续的章节安排如下：

(1) 在第2章中，我们将介绍本文后续章节所需的一些预备知识，包括分圆域、有限交换群的特征理论、高斯和与雅可比和、有限域上的分圆数以及线性码的 MacWilliams 恒等式与 Pless 幂矩。

(2) 在第3章中，我们将利用 Bent 函数值分布的一般性结果，来探究两类由完全非线性函数 $\Pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ 构造的 $\mathbb{F}_p$ 上的线性码 C_Π 与 $\overline{C_\Pi}$ 的重量分布。对于 m 为奇数的情形，我们在仅利用 Π 是完全非线性函数这一条件的前提下，完全确定了 C_Π 和 $\overline{C_\Pi}$ 的重量分布（定理3.6及定理3.7）。对于 m 为偶数的情形，我们给了一些宽松的条件，使得类似的结果依然成立。此外，在确定了 C_Π 和 $\overline{C_\Pi}$ 的重量分布后，我们还将进一步探讨它们的覆盖问题（定理3.9及定理3.10）。

(3) 在第4章中，我们将深入研究循环外差族与强循环外差族，主要结果包括利用有限域中的分圆类构造出循环外差族的无穷族（推论4.1）、证明所有强循环外差族都是平凡的（推论4.2），以及给出一个新的强外差族的不存在性结果（定理4.9）。

(4) 在第5章中，我们将总结本文的主要工作，并对未来的研究方向进行展望。

第 2 章　预备知识

2.1　分圆域

分圆域是一类非常重要的代数数域，在代数数论中起到非常重要的作用。在这一节中，我们将介绍分圆域的概念与基本性质。更详细的内容可以参见 [39]。

定义 2.1 (分圆域)： 对于正整数 n，令 $\xi_n = \exp(2\pi \mathrm{i}/n)$，称 $K = \mathbb{Q}(\xi_n)$ 为 $\mathbb{Q}$ 上的 n 阶分圆域。

注释 2.1： ξ_n 是 $\mathbb{C}$ 中的一个 n 次本原单位根，即 ξ_n 的乘法阶为 n。由初等数论的知识可知，对任意的 $d \in \mathbb{Z}$，ξ_n^d 的阶为 $n/\gcd(n,d)$。特别地，ξ_n^d 为 n 次本原单位根当且仅当 $\gcd(n,d) = 1$。因此 $\mathbb{C}$ 中的 n 次本原单位根共有 $\varphi(n)$ 个，其中 $\varphi(n)$ 是欧拉函数。

注释 2.2： 因为 $\mathbb{Q}(\xi_n)$ 是多项式 $X^n - 1$ 在 $\mathbb{Q}$ 上的分裂域，所以 $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是一个伽罗瓦扩张。因为 $\overline{\xi_n} = \xi_n^{-1} = \xi_n^{n-1} \in \mathbb{Q}(\xi_n)$，所以 $\mathbb{C}$ 上的共轭置换可以看作 $\mathrm{Gal}\big(\mathbb{Q}(\xi_n)/\mathbb{Q}\big)$ 中的元素。

下面的命题刻画了伽罗瓦群 $\mathrm{Gal}\big(\mathbb{Q}(\xi_n)/\mathbb{Q}\big)$ 的结构。

命题 2.1 ([40]，定理 4.9)： 设 $n \in \mathbb{N}_+$，用 μ_n 表示 $\mathbb{C}$ 中的全体 n 次单位根构成的乘法群。我们有自然的群同构

$$\begin{aligned} \tau_n : \mathrm{Gal}\big(\mathbb{Q}(\xi_n)/\mathbb{Q}\big) &\to \mathrm{Aut}(\mu_n), \\ \sigma &\mapsto \sigma|_{\mu_n}, \end{aligned} \tag{2-1}$$

其中 $\mathrm{Aut}(\mu_n)$ 表示群 μ_n 的自同构群。

注释 2.3： 我们有群同构

$$\begin{aligned} \mathrm{Aut}(\mu_n) &\to (\mathbb{Z}/n\mathbb{Z})^*, \\ \sigma &\mapsto \sigma_k. \end{aligned} \tag{2-2}$$

其中 σ_k 由关系式 $\sigma(\xi_n) = \xi_n^{\sigma_k}$ 定义。因此，$\mathrm{Gal}\big(\mathbb{Q}(\xi_n)/\mathbb{Q}\big)$ 是一个阶为 $\varphi(n)$ 的交换群。

定义 2.2 (分圆多项式)： 设 $n \in \mathbb{N}_+$，定义 $\mathbb{Q}$ 上的 n 阶分圆多项式为

$$\Phi_n(X) = \prod_{\substack{1 \leqslant k \leqslant n \\ (k,n)=1}} (X - \xi_n^k). \tag{2-3}$$

注释 2.4： 由命题2.1，我们知道

$$\Phi_n(X)=\prod_{\sigma\in \mathrm{Gal}\left(\mathbb{Q}(\xi_n)/\mathbb{Q}\right)}\left(X-\sigma(\xi_n)\right), \tag{2-4}$$

所以 $\Phi_n(X)$ 是 ξ_n 在 $\mathbb{Q}$ 上的极小多项式。特别地，$\Phi_n(X)$ 的系数都属于 $\mathbb{Q}$。

注释 2.5： 如果 p 为素数，则 $\Phi_p(X)=X^{p-1}+X^{p-2}+\cdots+X+1$。

一个重要的事实是，分圆多项式实际上是整系数多项式。

命题 2.2 ([41]，定理 2.45)： 设 $n\in\mathbb{N}_+$，则

(1) $X^n-1=\prod_{d|n}\Phi_d(X)$；

(2) $\Phi_n(X)\in\mathbb{Z}[X]$ 且 $\Phi_n(X)$ 的常数项为 ±1。

因为分圆多项式是整系数多项式，所以一个自然的问题就是其模 p（p 为素数）后是否依然不可约。下面的定理完整地回答了这个问题。

定理 2.1 ([41]，定理 2.47)： 设 $n\in\mathbb{N}_+$，p 为素数，则 $\Phi_n(X)$ 在 $\mathbb{F}_p$ 上不可约当且仅当 p 模 n 本原，即 p（在 $\mathbb{Z}_n$ 中的像）是 $\mathbb{Z}_n^*$ 的一个生成元。

下面的定理刻画了分圆域的整数环。

定理 2.2 ([42]，命题 10.2)： 设整数 $n\geqslant 3$，则分圆域 $K=\mathbb{Q}(\xi_n)$ 的整数环为 $\mathcal{O}_K=\mathbb{Z}[\xi_n]$。特别地，$\{\xi_n^l:\ 0\leqslant l\leqslant \varphi(n)-1\}$ 是 $\mathcal{O}_K$ 的一组整基。

素数在 $\mathcal{O}_K$ 中的分解也有很好的结果。

定理 2.3 ([40]，定理 4.12)： 设 $K=\mathbb{Q}(\xi_n)$，其中 $n\geqslant 3$。对于素数 p，令 $n=p^ln'$，其中 $l\in\mathbb{N}$，$p\nmid n'$，则 p 在 $\mathcal{O}_K=\mathbb{Z}[\xi_n]$ 中的素理想分解式为

$$p\mathcal{O}_K=\mathfrak{p}_1^e\cdots\mathfrak{p}_g^e,\qquad f(\mathfrak{p}_i/p)=f\quad(1\leqslant i\leqslant g), \tag{2-5}$$

其中 $\mathfrak{p}_1$，…，$\mathfrak{p}_g$ 是 $\mathcal{O}_K$ 中的不同素理想，f 为 p 模 n' 的阶，而 $g=\varphi(n')/f$。

推论 2.1： 设 $K=\mathbb{Q}(\xi_n)$，其中 $n\geqslant 3$。若素数 p 模 n 本原，则 $p\mathcal{O}_K$ 为 $\mathcal{O}_K=\mathbb{Z}[\xi_n]$ 中的素理想。

证明： 因为 p 模 n 本原，所以 p 模 n 的阶为 $\varphi(n)$，从而 $g=\varphi(n)/\varphi(n)=1$。由定理2.3，$p\mathcal{O}_K$ 为 $\mathcal{O}_K=\mathbb{Z}[\xi_n]$ 中的素理想。 ∎

2.2　有限交换群的特征理论

定义 2.3 (特征)： 有限交换群 G 到非零复数乘法群 $\mathbb{C}^*$ 的群同态称为群 G 的特征。群 G 的所有特征构成的集合记为 $\widehat{G}$，它们在逐点乘法运算下构成一个有限交换群。群 G 的特征 χ 的阶是指它作为群 $\widehat{G}$ 的元素的阶。

注释 2.6： 对任意的 $\chi\in\widehat{G}$ 以及 $g\in G$，由拉格朗日定理，我们有

$$\chi(g)^{|G|}=\chi(g^{|G|})=\chi(1_G)=1, \tag{2-6}$$

从而 $|\chi(g)|=1$，且

$$\chi(g^{-1})=\chi(g)^{-1}=\overline{\chi(g)}, \tag{2-7}$$

也就是说，共轭特征 $\overline{\chi}$ 为 χ 在 $\widehat{G}$ 中的逆元。

注释 2.7： 将 G 中所有元素映射为 $1\in\mathbb{C}^*$ 的特征称为 G 的平凡特征，记为 $1_{\widehat{G}}$。

有限交换群 G 与其特征群 $\widehat{G}$ 之间存在如下的关系：

定理 2.4 ([40]，定理 7.1)： 对于任意有限交换群 G，$\widehat{G}$ 和 G 是群同构的。

注释 2.8： 要注意的是，对于一般的有限交换群 G，并不存在 G 到 $\widehat{G}$ 的典范同构。不过，G 与 $\widehat{\widehat{G}}$ 是典范同构的。

特征最重要的性质是下面的正交性。

定理 2.5 ([40]，推论 7.1)： 设 G 为有限交换群。

(1) 对任意的 χ_1，$\chi_2\in\widehat{G}$，我们有

$$\sum_{g\in G}\chi_1(g)\overline{\chi_2(g)}=\begin{cases}|G|, & \text{若 } \chi_1=\chi_2,\\ 0, & \text{若 } \chi_1\neq\chi_2.\end{cases} \tag{2-8}$$

(2) 对任意的 g_1，$g_2\in G$，我们有

$$\sum_{\chi\in\widehat{G}}\chi(g_1)\overline{\chi(g_2)}=\begin{cases}|\widehat{G}|=|G|, & \text{若 } g_1=g_2,\\ 0, & \text{若 } g_1\neq g_2.\end{cases} \tag{2-9}$$

在调和分析理论中，傅里叶变换是一个非常重要的工具。对于有限交换群 G，我们可以定义类似的傅里叶变换：

定义 2.4 (傅里叶变换)： 设 G 为有限交换群，$f:G\to\mathbb{C}$ 为 G 上的复值函数。我们定义 f 的傅里叶变换 $\widehat{f}:\widehat{G}\to\mathbb{C}$ 为

$$\widehat{f}(\chi)=\sum_{g\in G}f(g)\chi(g),\quad \chi\in\widehat{G}. \tag{2-10}$$

由正交性，我们可以得到傅里叶反转公式。它告诉我们，有限交换群上的复值函数与其傅里叶变换是相互决定的。

定理 2.6 ([40]，定理 7.4)： 设 G 为有限交换群，$f:G\to\mathbb{C}$ 为 G 上的复值函数。那么对于任意的 $g\in G$，我们有

$$f(g)=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\widehat{f}(\chi)\overline{\chi(g)}. \tag{2-11}$$

从有限交换群出发，我们可以构造一个新的代数结构：群环，其在理论和应用中都是非常重要的工具。

定义 2.5 (群环)： 设 $(G,\cdot)$ 为有限乘法群，R 为一个含幺交换环。考虑集合

$$R[G]=\{\sum_{g\in G} r_g g:\ r_g\in R\}. \tag{2-12}$$

可以在这个集合中引入加（减）法和乘法：对于 $R[G]$ 中的元素

$$\alpha=\sum_{g\in G} r_g g,\qquad \beta=\sum_{g\in G} s_g g,\quad (r_g,\ s_g\in R), \tag{2-13}$$

定义

$$\alpha\pm\beta=\sum_{g\in G}(r_g\pm s_g)g, \tag{2-14}$$

以及

$$\alpha\cdot\beta=\sum_{g\in G}\Big(\sum_{h\in G} r_h s_{h^{-1}g}\Big)g. \tag{2-15}$$

不难证明，对于上述的运算，$R[G]$ 构成一个含幺环，其幺元就是 G 中的幺元。如果 G 是交换群，那么 $R[G]$ 是交换环。

下面我们考虑 R 为复数域 $\mathbb{C}$。我们可以将有限交换群 G 的特征延拓到它的群环 $\mathbb{C}[G]$ 上。

定义 2.6 (特征的延拓)： 设 G 为有限交换群。对任意的 $\chi\in\widehat{G}$ 以及 $\alpha=\sum_{g\in G} c_g g\in\mathbb{C}[G]$（$c_g\in\mathbb{C}$），我们定义

$$\chi(\alpha)=\sum_{g\in G} c_g\chi(g)\in\mathbb{C}. \tag{2-16}$$

不难证明，χ 为 $\mathbb{C}[G]$ 到 $\mathbb{C}$ 的环同态。

下面的定理告诉我们，可以用特征区分群环 $\mathbb{C}[G]$ 中的元素。

定理 2.7 ([40]，定理 7.5)： 设 G 为有限交换群，α 和 β 为群环 $\mathbb{C}[G]$ 中的元素，则 $\alpha=\beta$ 当且仅当对任意群 G 的特征 χ，都有 $\chi(\alpha)=\chi(\beta)$。

证明： 设 $\alpha=\sum_{g\in G} c_g g$（$c_g\in\mathbb{C}$），考虑函数 $f:G\to\mathbb{C}$，$g\mapsto c_g$。那么对于任意的 $\chi\in\widehat{G}$，我们有

$$\widehat{f}(\chi)=\sum_{g\in G} f(g)\chi(g)=\sum_{g\in G} c_g\chi(g)=\chi(\alpha). \tag{2-17}$$

由傅里叶反转公式，f 由其傅里叶变换 $\widehat{f}$ 所唯一决定，因此 α 也由 $\chi(\alpha)$ $(\chi\in\widehat{G})$ 所唯一决定。 ∎

考虑完一般性的理论，我们现在聚焦于有限域的情形。设 p 为一个素数，a 为正整数，$q=p^a$。在有限域 $\mathbb{F}_q$ 中，有两个有限交换群：加法群 $(\mathbb{F}_q,+)$ 与乘法群 $(\mathbb{F}_q^*,\cdot)$。

定义 2.7 (加性特征，乘性特征)： 加法群 $(\mathbb{F}_q,+)$ 的特征称为 $\mathbb{F}_q$ 的加性特征，乘法

群 $(\mathbb{F}_q^*,\cdot)$ 的特征称为 $\mathbb{F}_q$ 的乘性特征。

注释 2.9： 由有限域的理论，$\mathbb{F}_q^*$ 是一个循环群。设 θ 为 $\mathbb{F}_q^*$ 的一个生成元，固定一个 $\mathbb{C}$ 中的 $q-1$ 次本原单位根 ξ_{q-1}，定义

$$\begin{aligned}\chi_1 : \mathbb{F}_q^* &\to \mathbb{C}^*,\\ \theta^i &\mapsto \xi_{q-1}^i,\end{aligned} \tag{2-18}$$

则 χ_1 为 $\mathbb{F}_q$ 的一个乘性特征且为 $\widehat{\mathbb{F}_q^*}$ 的生成元。

前面我们说到，对于一般的有限交换群 G，并不存在 G 到 $\widehat{G}$ 的典范同构。但是，对于加法群 $(\mathbb{F}_q,+)$，如果我们固定一个 $\mathbb{C}$ 中的 p 次本原单元根 ξ_p，那么 $\mathbb{F}_q$ 与 $\widehat{\mathbb{F}_q}$ 之间就存在一个自然的同构。

定理 2.8 ([40]，定理 7.7)： 对任意的 $a\in\mathbb{F}_q$，定义

$$\begin{aligned}\psi_a : \mathbb{F}_q &\to \mathbb{C}^*,\\ x &\mapsto \xi_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)},\end{aligned} \tag{2-19}$$

则 $\widehat{\mathbb{F}_q}=\{\psi_a:\ a\in\mathbb{F}_q\}$，且映射 $\mathbb{F}_q\to\widehat{\mathbb{F}_q}, a\mapsto\psi_a$ 定义了一个从 $\mathbb{F}_q$ 到 $\widehat{\mathbb{F}_q}$ 的自然同构。

虽然有限域 $\mathbb{F}_q$ 中有两个有限交换群，但是一般我们提到 $\mathbb{F}_q$ 上的傅里叶变换，均是指加法群 $(\mathbb{F}_q,+)$ 上的傅里叶变换。由定理2.8，如果固定一个 $\mathbb{C}$ 中的 p 次本原单元根 ξ_p，那么 $\mathbb{F}_q$ 与 $\widehat{\mathbb{F}_q}$ 就自然地同构，因此我们通常是将 $\mathbb{F}_q$ 上复值函数的傅里叶变换定义为 $\mathbb{F}_q$ 上的复值函数，而非 $\widehat{\mathbb{F}_q}$ 上的。更具体地说，对于复值函数 $f:\mathbb{F}_q\to\mathbb{C}$，我们定义其傅里叶变换为

$$\begin{aligned}\widehat{f} : \mathbb{F}_q &\to \mathbb{C},\\ a &\mapsto \sum_{x\in\mathbb{F}_q} f(x)\xi_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}.\end{aligned} \tag{2-20}$$

2.3　高斯和，雅可比和与分圆数

特征和是一个非常重要的概念，它在数论中有着广泛的应用。在这一节中，我们将介绍两种最基本的特征和：高斯和与雅可比和。在本节中，令 p 为一个素数，m 为正整数，$q=p^m$，固定一个 $\mathbb{C}$ 中的 p 次本原单元根 ξ_p 和一个 $q-1$ 次本原单位根 ξ_{q-1}。

定义 2.8 (高斯和)： 设 ψ 为 $\mathbb{F}_q$ 的一个加法特征，χ 为 $\mathbb{F}_q$ 的一个乘法特征，定义它们对应的高斯和为

$$G(\chi,\psi)=\sum_{x\in\mathbb{F}_q^*}\chi(x)\psi(x). \tag{2-21}$$

注释 2.10： 由定理2.8，我们有 $\widehat{\mathbb{F}_q}=\{\psi_a:\ a\in\mathbb{F}_q\}$。我们将 $G(\chi,\psi_1)$ 简写为 $G(\chi)$。简单的计算可以得到：对任意的 $a\in\mathbb{F}_q^*$，有 $G(\chi,\psi_a)=\overline{\chi}(a)G(\chi)$。

定义 2.9 (雅可比和)： 对于 $\mathbb{F}_q$ 上的两个乘法特征 χ_1 与 χ_2，定义它们对应的雅可比和为

$$J(\chi_1,\chi_2)=\sum_{\substack{x\in\mathbb{F}_q\\ x\neq 0,1}}\chi_1(x)\chi_2(1-x). \tag{2-22}$$

注释 2.11： 显然有

$$J(\chi_1,\chi_2)=\sum_{\substack{x,y\in\mathbb{F}_q^*\\ x+y=1}}\chi_1(x)\chi_2(y)=J(\chi_2,\chi_1). \tag{2-23}$$

关于一些平凡的情形，我们有如下的结论：

命题 2.3 ([40]，定理 7.8)：

(1) 任取 $\mathbb{F}_q$ 的加法特征 ψ 与乘法特征 χ，有

$$G(\chi,\psi)=\begin{cases}0, & \text{若 } \psi=1,\ \chi\neq 1,\\ -1, & \text{若 } \psi\neq 1,\ \chi=1,\\ q-1, & \text{若 } \psi=1,\ \chi=1,\end{cases} \tag{2-24}$$

其中，$\psi=1$ 表示 ψ 为 $\mathbb{F}_q$ 的平凡加法特征，而 $\chi=1$ 表示 χ 为 $\mathbb{F}_q$ 的平凡乘法特征。

(2) 任取 $\mathbb{F}_q$ 的乘法特征 χ_1 与 χ_2，有

$$J(\chi_1,\chi_2)=\begin{cases}q-2, & \text{若 } \chi_1=\chi_2=1,\\ -1, & \text{若 } \chi_1,\ \chi_2 \text{ 中恰有一个为1},\\ -\chi_1(-1), & \text{若 } \chi_1\neq 1,\ \chi_1\chi_2=1.\end{cases} \tag{2-25}$$

若 p 为奇素数，则 $2\mid(q-1)$，从而 $\mathbb{F}_q$ 拥有唯一的一个二阶乘法特征 η，它满足

$$\eta(x)=\begin{cases}1, & \text{若 } x \text{ 为 } \mathbb{F}_q^* \text{ 中的平方元},\\ -1, & \text{若 } x \text{ 为 } \mathbb{F}_q^* \text{ 中的非平方元}.\end{cases} \tag{2-26}$$

如果 $q=p$，那么 η 实际上就是模 p 的勒让德符号。二次高斯和的值可以被完全确定。

定理 2.9 ([40]，定理 7.14)： 我们有

$$G(\eta)=\begin{cases}(-1)^{m-1}\sqrt{q}, & \text{若 } q\equiv 1 \pmod 4,\\ (-1)^{m-1}\mathrm{i}^{m}\sqrt{q}, & \text{若 } q\equiv 3 \pmod 4.\end{cases} \tag{2-27}$$

许多有限域上的计数问题，都可以转化为分圆数的计算。我们在此介绍分圆类以及分圆数的概念。

定义 2.10 (分圆类，分圆数)： 设 $q-1=ef$，其中 e，f 为 $\geqslant 2$ 的整数，固定 $\mathbb{F}_q$ 的一个本原元素 θ。对任意的 $i\in\mathbb{Z}$，定义集合 $C_i=\theta^i C$，其中 $C=\langle\theta^e\rangle$ 为 θ^e 在 $\mathbb{F}_q^*$ 中生成的子群。不难看出 $C_{i_1}=C_{i_2}$ 当且仅当 $i_1\equiv i_2 \pmod e$，且集合 C_i（$0\leqslant i\leqslant e-1$）就是 C 在 $\mathbb{F}_q^*$ 中的所有陪集。对于 $0\leqslant i\leqslant e-1$，我们称 C_i 为 $\mathbb{F}_q$ 中的第 i 个分圆类（cyclotomic class）。对于 i，$j\in\mathbb{Z}$，我们定义 $\mathbb{F}_q$ 的 e 阶分圆数（cyclotomic number）为

$$(i,j)_e^{(q)}=|\{x\in C_i:\ x+1\in C_j\}|. \tag{2-28}$$

注释 2.12： 显然，分圆类的编号与本原元素 θ 的选取有关。

分圆数的计算本质上就是雅可比和的计算。

命题 2.4 ([40]，定理 7.19)： 设 $q-1=ef$，其中 e，f 为 $\geqslant 2$ 的整数，固定 $\mathbb{F}_q$ 的一个本原元素 θ。取一个 $\mathbb{C}$ 中的 e 次本原单位根 ξ_e，设 $\chi:\mathbb{F}_q^*\to\mathbb{C}^*$ 为将 θ 映射到 ξ_e 的 e 阶乘法特征。于是对任意的 i，$j\in\mathbb{Z}$，有

$$(i,j)_e^{(q)}=\frac{1}{e^2}\sum_{\lambda,\mu=0}^{e-1}\xi_e^{-(i\lambda+j\mu)}\chi^{\lambda}(-1)J(\chi^{\lambda},\chi^{\mu}). \tag{2-29}$$

下面这个四阶分圆数的结果我们之后将会用到。

定理 2.10 ([40]，定理 7.22)： 设 p 为奇素数，m 为正整数，$q=p^m$ 满足 $q\equiv 1 \pmod 4$，并设 $q-1=ef$，其中 e，f 为 $\geqslant 2$ 的整数。

若 $p\equiv 1 \pmod 4$，则存在整数 s，t 使得 $q=s^2+4t^2$，$p\nmid st$ 且 $s\equiv 1 \pmod 4$。其中 s 是唯一确定的，而 t 确定到相差一个符号。若 $p\equiv 3 \pmod 4$（从而 m 为偶数），则取 $t=0$，并取 s 为 $\{\pm p^{\frac{m}{2}}\}$ 中模 4 余 1 的那一个。在本定理的剩余部分中，s 和 t 均保持在本段中的意义。

(1) 若 $q\equiv 1 \pmod 8$，则

$$(1,0)_4^{(q)}=\frac{1}{16}(q-3+2s+8t),\qquad (3,0)_4^{(q)}=\frac{1}{16}(q-3+2s-8t); \tag{2-30}$$

(2) 若 $q\equiv 5 \pmod 8$，则

$$(1,0)_4^{(q)}=(3,0)_4^{(q)}=\frac{1}{16}(q-3-2s). \tag{2-31}$$

2.4　MacWilliams 恒等式与 Pless 幂矩

定义 2.11 (重量分布)： 设 C 为一个 $[n,k,d]_q$ 线性码。对于 $0 \leqslant i \leqslant n$，令 A_i 表示 C 中汉明重量为 i 的码字个数。我们称 $(A_0, A_1, \cdots, A_n)$ 为 C 的重量分布。

定义 2.12 (对偶码)： 设 C 为一个 $[n,k,d]_q$ 线性码，定义其对偶码 $C^\perp$ 为线性空间

$$C^\perp = \{v \in \mathbb{F}_q^n : \forall\, c \in C,\ c \cdot v = 0\}, \tag{2-32}$$

其中点乘表示欧式内积。

编码理论中的一个优美结果告诉我们，线性码与其对偶码的重量分布是可以相互决定的。

定理 2.11 (MacWilliams 恒等式，[40]，定理 9.2)： 设 C 为一个 $[n,k,d]_q$ 线性码，其重量分布为 $(A_0, A_1, \cdots, A_n)$，其对偶码 $C^\perp$ 的重量分布为 $(A_0^\perp, A_1^\perp, \cdots, A_n^\perp)$。考虑多项式

$$f_C(X,Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i, \tag{2-33}$$

$$f_{C^\perp}(X,Y) = \sum_{i=0}^{n} A_i^\perp X^{n-i} Y^i. \tag{2-34}$$

我们有

$$f_{C^\perp}(X,Y) = q^{-k} f_C\big(X + (q-1)Y, X - Y\big). \tag{2-35}$$

MacWilliams 恒等式可以表达为下面这个在实际中更方便使用的等价形式：

定理 2.12 ([43])： 设 C 为一个 $[n,k,d]_q$ 线性码，其重量分布为 $(A_0, A_1, \cdots, A_n)$，其对偶码 $C^\perp$ 的重量分布为 $(A_0^\perp, A_1^\perp, \cdots, A_n^\perp)$。对任意的 $r \geqslant 0$，我们有

$$\sum_{j=0}^{n} j^r A_j = \sum_{j=0}^{\min(n,r)} (-1)^j A_j^\perp \cdot \Big(\sum_{l=j}^{r} l! S(r,l) q^{k-l} (q-1)^{l-j} \binom{n-j}{n-l} \Big), \tag{2-36}$$

其中 $S(r,l)$ 是第二类斯特林数（Stirling number），即

$$S(r,l) = \frac{1}{l!} \sum_{i=0}^{l} (-1)^{l-i} \binom{l}{i} i^r = \sum_{i=0}^{l} \frac{(-1)^{l-i} i^r}{(l-i)!\, i!}. \tag{2-37}$$

注释 2.13： 我们称和式 $\sum_{j=0}^{n} j^r A_j$ 为 C 的 r 阶 Pless 幂矩（Pless power moment）。

第 3 章　由完全非线性函数构造的线性码及其秘密共享方案

3.1　完全非线性函数

本节我们介绍完全非线性函数的概念及其基本性质。我们只列出部分结果的证明，其余的读者可以参考 [15,44-45]。

完全非线性函数与密码学中的差分密码分析紧密相关。差分密码分析的实施，取决于能够找到一条高概率的差分或者差分特征。而高概率的差分或者差分特征的寻找，则取决于轮函数中非线性组件的差分均匀度。

差分均匀度的概念最早由 Nyberg 在 1993 年的欧洲密码年会上提出[46]。由于密码算法的设计与分析大多基于 $\mathbb{F}_2^n$，所以 Nyberg 提出的差分均匀度也是定义在 $\mathbb{F}_2^n$ 上的。然而，事实上，差分均匀度的概念可以自然地推广到一般的交换群上。

定义 3.1 (差分均匀度)： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数，令

$$\delta_f = \max_{a\in A\setminus\{0\}} \max_{b\in B} |\{x \in A : f(x+a) - f(x) = b\}|, \tag{3-1}$$

称之为函数 f 的差分均匀度（differential uniformity）。

不难看出，差分均匀度被下面的界所控制：

命题 3.1 ([15]，引理 2)： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数，则

$$\frac{|A|}{|B|} \leqslant \delta_f \leqslant |A|. \tag{3-2}$$

如前文所述，差分均匀度的值与差分密码分析密切相关。具体来说，函数 f 的差分均匀度 δ_f 越小，则利用其设计的密码系统抵抗差分密码攻击的能力就越强。因此，我们自然希望函数的差分均匀度可以取到命题3.1中的下界，而这就引出了完全非线性函数的概念。

定义 3.2 (完全非线性函数)： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数，其中 $|A| \geqslant |B|$。如果 $\delta_f = |A|/|B|$，则称 f 为完全非线性函数，简称为 PN 函数。

定义 3.3 (线性函数，仿射函数)： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数。若 f 为群同态，则称 f 为线性函数；若存在线性函数 $l : A \to B$ 和 $b \in B$，使得 $f(x) = l(x) + b$ 对任意的 $x \in A$ 成立，则称 f 为仿射函数。

注释 3.1： 如果仿射函数 $f : A \to A$ 为双射，那么我们称之为仿射置换。

由定义不难算出，当 $f:A\to B$ 为仿射函数时，f 的差分均匀度 δ_f 取到了命题3.1中的上界。这表示完全非线性函数与仿射函数在差分均匀度上是两个极端，而这也是“完全非线性”一词的由来。

定义 3.4 (平衡函数)： 设 f 为从有限集合 A 到有限集合 B 的函数。如果对任意的 $b\in B$，都有

$$|\{x\in A:f(x)=b\}|=\frac{|A|}{|B|}, \tag{3-3}$$

则称 f 为平衡函数（balanced function）。

很容易可以证明下面这个对 PN 函数的刻画：

命题 3.2 ([15]，定理 5)： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数，其中 $|A|\geqslant|B|$，则 f 为 PN 函数当且仅当对任意的 $a\in A\setminus\{0\}$，差分函数 $D_af:A\to B,x\mapsto f(x+a)-f(x)$ 为平衡函数。

注释 3.2： 这正是我们在1.2节中使用的 PN 函数的定义。

我们可以从已有的 PN 函数出发，构造新的 PN 函数。

命题 3.3： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的 PN 函数，l 为从 $(A,+)$ 到 $(B,+)$ 的仿射函数，则 $f+l$ 为从 $(A,+)$ 到 $(B,+)$ 的 PN 函数。

证明： 设 $l(x)=g(x)+b$，其中 g 为从 $(A,+)$ 到 $(B,+)$ 的线性函数，b 为 B 中的固定元素。于是对任意的 $a\in A\setminus\{0\}$ 以及 $x\in A$，我们有

$$\begin{aligned}D_a(f+l)(x)&=(f+l)(x+a)-(f+l)(x)\\&=f(x+a)-f(x)+g(a)\\&=D_af(x)+g(a).\end{aligned} \tag{3-4}$$

由于 f 为 PN 函数，所以 D_af 为平衡函数，从而 $D_a(f+l)$ 也为平衡函数。由命题3.2，$f+l$ 为 PN 函数。 ∎

命题 3.4 ([15]，定理 6)： 设 f 为从有限交换群 $(B,+)$ 到有限交换群 $(C,+)$ 的 PN 函数，l 为从有限交换群 $(A,+)$ 到 $(B,+)$ 的可逆仿射函数，则 $f\circ l$ 为 $(A,+)$ 到 $(C,+)$ 的 PN 函数。

证明： 设 $l(x)=g(x)+b$，其中 g 为从 $(A,+)$ 到 $(B,+)$ 的线性函数，b 为 B 中的固定元素。于是对任意的 $a\in A\setminus\{0\}$ 以及 $x\in A$，我们有

$$\begin{aligned}D_a(f\circ l)(x)&=f\big(l(x+a)\big)-f\big(l(x)\big)\\&=f\big(l(x)+g(a)\big)-f\big(l(x)\big)=(D_{g(a)}f\circ l)(x).\end{aligned} \tag{3-5}$$

由于 l 为可逆仿射函数，所以 g 为可逆线性函数，从而 $g(a)\neq0$。由于 f 为 PN 函数，所以 $D_{g(a)}f$ 为平衡函数，从而 $D_a(f\circ l)=D_{g(a)}f\circ l$ 也为平衡函数。由命题3.2，

$f \circ l$ 为 PN 函数。 ∎

命题 3.5 ([15]，定理 7)： 设 f 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的 PN 函数，l 为 $(B,+)$ 到有限交换群 $(C,+)$ 的满仿射函数，则 $l \circ f$ 为 $(A,+)$ 到 $(C,+)$ 的 PN 函数。

证明： 设 $l(x) = g(x) + c$，其中 g 为 $(B,+)$ 到 $(C,+)$ 的线性函数，c 为 C 中的固定元素。于是任取 $a \in A \setminus \{0\}$ 以及 $x \in A$，我们有

$$\begin{aligned} D_a(l \circ f)(x) &= l\big(f(x+a)\big) - l\big(f(x)\big) \\ &= g\big(f(x+a)\big) - g\big(f(x)\big) \\ &= g\big(f(x+a) - f(x)\big) = (g \circ D_a f)(x). \end{aligned} \tag{3-6}$$

由于 f 为 PN 函数，所以 $D_{g(a)}f$ 为平衡函数。由于 l 为满射，所以 g 为平衡函数（注意 g 为线性函数），从而 $g \circ D_a f$ 也为平衡函数。由命题3.2，$l \circ f$ 为 PN 函数。 ∎

由上面命题3.4与命题3.5，我们可以定义 PN 函数的仿射等价关系。

定义 3.5 (仿射等价)： 设 f，g 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的两个 PN 函数。若存在 $(A,+)$ 上的仿射置换 l_1，以及 $(B,+)$ 上的仿射置换 l_2，使得 $f = l_2 \circ g \circ l_1$，则称 f 与 g 为仿射等价的。

我们主要关心有限域 $\mathbb{F}_q$ 到自身的 PN 函数，其中 $q = p^m$，p 为奇素数，m 为整数。根据命题3.2，函数 $\Pi : (\mathbb{F}_q,+) \to (\mathbb{F}_q,+)$ 为 PN 函数，当且仅当对任意的 $a \in \mathbb{F}_q^*$，差分函数 $D_a\Pi$ 为 $\mathbb{F}_q$ 上的双射。

构造 PN 函数是一件很困难的事。直到目前为止，所有已知的 $\mathbb{F}_q$ 上的 PN 函数在仿射等价的意义下，都属于下面六类中的一类：

(1) Dembowski-Ostrom 幂函数[47]：

$$\Pi_1(x) = x^{p^t+1}, \quad \text{其中整数 } t \geqslant 0, \ \frac{n}{\gcd(n,t)} \text{为奇数;} \tag{3-7}$$

(2) Coulter-Matthews 幂函数[48]：

$$\Pi_2(x) = x^{\frac{3^k+1}{2}}, \quad \text{其中 } p = 3, \ k \text{ 为奇数且 } (n,k) = 1; \tag{3-8}$$

(3) Ding-Yuan 多项式[49]：

$$\Pi_3(x) = x^{10} - ux^6 - u^2x^2, \quad \text{其中 } p = 3, \ k \text{ 为奇数且 } u \in \mathbb{F}_q^*; \tag{3-9}$$

(4) Budaghyan-Helleseth 第一类多项式[50]：

$$\Pi_4(x) = (bx)^{p^s+1} - \big((bx)^{p^s+1}\big)^{p^k} + \sum_{i=0}^{k-1} c_i x^{p^i(p^k+1)}, \tag{3-10}$$

其中 $n=2k$，s 和 k 为正整数，满足

$$\begin{cases}\gcd(k+s,2k)=\gcd(k+s,k),\\ \gcd(p^s+1,p^k+1)\neq\gcd(p^s+1,\frac{p^k+1}{2}),\end{cases} \tag{3-11}$$

$b\in\mathbb{F}_q^*$，$\sum_{i=0}^{k-1}c_i x^{p^i}$ 为 $\mathbb{F}_q$ 上的置换多项式，并且系数 $c_i\in\mathbb{F}_{p^k}$（$0\leqslant i\leqslant k-1$）；

(5) Budaghyan-Helleseth 第二类多项式[50]：

$$\Pi_5(x)=ux^{p^k+1}+vx^{p^s+p^t}+v^{p^k}x^{p^{k+s}+p^{k+t}}+\sum_{i=0}^{k-1}w_i x^{p^{k+i}+p^i}, \tag{3-12}$$

其中 $n=2k$，s 和 t 为正整数，满足

$$2\nmid\frac{n}{gcd(n,t-s)}, \tag{3-13}$$

$u\notin\mathbb{F}_{p^k}$，α 为 $\mathbb{F}_q$ 中本原元，$v=\alpha^r$，$\gcd(p^{s-t}+1,p^k+1)\nmid r$，并且对任意的 $0\leqslant i\leqslant k-1$，$w_i\in\mathbb{F}_{p^k}$；

(6) Zha-Kyureghyan-Wang 多项式[51]：

$$\Pi_6(x)=ux^{p^s+1}-u^{p^k}x^{p^{lk}+p^{-lk+s}}, \tag{3-14}$$

其中 u 为 $\mathbb{F}_q$ 中的本原元，$n=3k$，$\gcd(3,k)=1$，$k/\gcd(k,s)$ 为奇数，$s\equiv\pm k\pmod 3$，且

$$l=\begin{cases}1, & \text{若 } s\equiv k\pmod 3,\\ -1, & \text{若 } s\equiv -k\pmod 3.\end{cases} \tag{3-15}$$

需要注意的是，上面的六类中，除了第二类，其余的五类均为 Dembowski-Ostrom 型的 PN 函数，也就是说，它们都具有如下的形式：

$$\Pi(x)=\sum_{0\leqslant i\leqslant j\leqslant m-1}a_{ij}x^{p^i+p^j}, \tag{3-16}$$

其中 $a_{ij}\in\mathbb{F}_q$。

3.2　Walsh 谱与 Bent 函数

除了命题3.2中的刻画，PN 函数还可以使用 Walsh 谱来刻画。为此，我们先介绍 Walsh 变换以及 Walsh 谱的概念。

定义 3.6 (Walsh 变换，Walsh 谱)： 设 F 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数。任取特征 $\chi\in\widehat{B}$，我们有复值函数 $F_\chi=\chi\circ F:A\to\mathbb{C}$。定义映射

$$W_F:\widehat{A}\times\widehat{B}\to\mathbb{C} \tag{3-17}$$

$$(\phi,\chi)\mapsto \widehat{F_\chi}(\phi),$$

称之为 F 的 Walsh 变换（Walsh transform），其中 $\widehat{F_\chi}$ 为复值函数 F_χ 的傅里叶变换。称集合

$$\left\{W_F(\phi,\chi):\ \phi\in\widehat{A},\ \chi\in\widehat{B}\setminus\{1_{\widehat{B}}\}\right\} \tag{3-18}$$

为 F 的 Walsh 谱（Walsh spectrum），其中 $1_{\widehat{B}}$ 为 B 的平凡特征。

下面的定理使用 Walsh 谱来刻画 PN 函数。

定理 3.1 ([15]，定理 16)： 设 F 为从有限交换群 $(A,+)$ 到有限交换群 $(B,+)$ 的函数，则 F 为 PN 函数，当且仅当对任意的 $\phi\in\widehat{A}$ 及 $\chi\in\widehat{B}\setminus\{1_{\widehat{B}}\}$，都有

$$|W_F(\phi,\chi)|=\sqrt{|A|}. \tag{3-19}$$

考虑完一般的情形，我们现在关注有限域的特殊情形。设 p 为一个素数，m 为整数，$q=p^m$。如2.2节中所述，对于 $\mathbb{F}_q$ 上的复值函数 f，我们通常通过自然同构 $(\mathbb{F}_q,+)\xrightarrow{\cong}(\widehat{\mathbb{F}_q},+)$，$a\mapsto\psi_a$，将其傅里叶变换定义为 $\mathbb{F}_q$ 上的复值函数

$$\begin{aligned}\widehat{f}:\mathbb{F}_q&\to\mathbb{C}\\ a&\mapsto\sum_{x\in\mathbb{F}_q}f(x)\xi_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}.\end{aligned} \tag{3-20}$$

类似地，任取 m 的正因子 h 以及函数 $F:\mathbb{F}_q\to\mathbb{F}_{p^h}$，我们更习惯于定义 F 的 Walsh 变换为

$$\begin{aligned}W_F(a,b)&=\sum_{x\in\mathbb{F}_q}\psi_a(x)\psi_b\big(F(x)\big)\\ &=\sum_{x\in\mathbb{F}_q}\xi_p^{\mathrm{Tr}_{\mathbb{F}_{p^h}/\mathbb{F}_p}\left(bF(x)\right)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)},\end{aligned} \tag{3-21}$$

其中 $a\in\mathbb{F}_q$，$b\in\mathbb{F}_{p^h}$。

注释 3.3： 注意，在文献中，$W_F(a,b)$ 更经常被定义为

$$W_F(a,b)=\sum_{x\in\mathbb{F}_q}\xi_p^{\mathrm{Tr}_{\mathbb{F}_{p^h}/\mathbb{F}_p}\left(bF(x)\right)-\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}. \tag{3-22}$$

然而，无论采取哪种定义，对应的 Walsh 谱是一样的，所以不会造成实质性影响。

由定理3.1，函数 $F:\mathbb{F}_q\to\mathbb{F}_{p^h}$ 为 PN 函数，当且仅当对任意的 $a\in\mathbb{F}_q$ 以及 $b\in\mathbb{F}_{p^h}^*$，有

$$|W_F(a,b)|=\sqrt{q}. \tag{3-23}$$

1993 年，Matsui 在欧洲密码年会上提出了针对加密算法 DES 的线性密码分

析[52]。线性密码分析的基本思想，是寻找密码算法有效的线性近似表达式来破译密码系统。非线性度是一个密码函数抵御线性密码攻击能力的度量。非线性度越大，函数与仿射函数的距离越远，从而抵御线性密码攻击的能力也就越强。

非线性度最优的布尔函数被称为 Bent 函数。除了使用非线性度，还可以使用 Walsh 谱来刻画 Bent 函数。并且，使用 Walsh 谱的刻画还可以自然地推广到奇特征的情形。因此，我们这里直接用 Walsh 谱来定义 Bent 函数。

定义 3.7 (Bent 函数)： 设 p 为素数，q 为 p 的一个方幂。称函数 $f:\mathbb{F}_q\to\mathbb{F}_p$ 为 Bent 函数，如果对任意的 $a\in\mathbb{F}_q$，$W_f(a):=W_f(a,1)$ 的绝对值均为 $\sqrt{q}$。

注释 3.4： 从定义上看，Bent 函数的定义似乎与 p 次本原单位根 ξ_p 的选取有关。然而，我们将在定理3.2中看到，实际上是无关的。

由定义及式（3-23），我们不难看出从 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的 PN 函数一定为 Bent 函数。实际上，反之也是成立的。

定理 3.2 ([53], 命题 2)： 设 p 为素数，q 为 p 的一个方幂。函数 $f:\mathbb{F}_q\to\mathbb{F}_p$ 为 Bent 函数当且仅当它为 PN 函数。

证明： 由式（3-23），只需证明对任意的 $a\in\mathbb{F}_q$ 以及 $b\in\mathbb{F}_p^*$，都有

$$|W_f(a,b)|=\sqrt{q}. \tag{3-24}$$

令 $K=\mathbb{Q}(\xi_p)$。由于 $b\in\mathbb{F}_p^*$，所以 ξ_p^b 也是 $\mathbb{C}$ 中 p 次本原单位根，因此存在 $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$，使得 $\sigma(\xi_p)=\xi_p^b$。因为 $\overline{\xi_p}=\xi_p^{p-1}$，我们知道复数域 $\mathbb{C}$ 的共轭置换 τ 可以限制到 K 上成为 $\mathrm{Gal}(K/\mathbb{Q})$ 中的元素。由于 $\mathrm{Gal}(K/\mathbb{Q})$ 为交换群，所以 $\sigma\circ\tau=\tau\circ\sigma$。因为

$$\begin{aligned}
W_f(a,b)&=\sum_{x\in\mathbb{F}_q}\xi_p^{bf(x)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}\\
&=\sum_{x\in\mathbb{F}_q}(\xi_p^b)^{f(x)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{a}{b}x)}\\
&=\sum_{x\in\mathbb{F}_q}\sigma(\xi_p)^{f(x)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{a}{b}x)}\\
&=\sigma\Big(\sum_{x\in\mathbb{F}_q}\xi_p^{f(x)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\frac{a}{b}x)}\Big)=\sigma\big(W_f(\frac{a}{b})\big),
\end{aligned} \tag{3-25}$$

所以

$$\begin{aligned}
|W_f(a,b)|^2&=W_f(a,b)\cdot\tau\big(W_f(a,b)\big)\\
&=\sigma\big(W_f(\frac{a}{b})\big)\cdot\tau\sigma\big(W_f(\frac{a}{b})\big)\\
&=\sigma\big(W_f(\frac{a}{b})\big)\cdot\sigma\tau\big(W_f(\frac{a}{b})\big)
\end{aligned} \tag{3-26}$$

$$= \sigma\Big(W_f(\frac{a}{b}) \cdot \tau\big(W_f(\frac{a}{b})\big)\Big)$$
$$= \sigma\big(|W_f(\frac{a}{b})|^2\big) = \sigma(q) = q,$$

从而 $|W_f(a,b)| = \sqrt{q}$。 ∎

注释 3.5： 这里给出的证明与 [53] 中的不同。

关于 Bent 函数 Walsh 谱的具体值，我们有如下的深刻结果：

定理 3.3 ([54]，性质 7-8)： 设 p 为奇素数，$q = p^m$ 为 p 的一个方幂。对任意的 Bent 函数 $f : \mathbb{F}_q \to \mathbb{F}_p$，都存在函数 $f^* : \mathbb{F}_q \to \mathbb{F}_p$，称为 f 的对偶，使得对任意的 $a \in \mathbb{F}_q$，若 m 为奇数时有

$$W_f(a) = \begin{cases} \pm\xi_p^{f^*(a)}\sqrt{q}, & \text{若 } q \equiv 1 \pmod 4, \\ \pm \mathrm{i}\xi_p^{f^*(a)}\sqrt{q}, & \text{若 } q \equiv 3 \pmod 4, \end{cases} \tag{3-27}$$

若 m 为偶数时有

$$W_f(a) = \pm\xi_p^{f(a)}\sqrt{q}. \tag{3-28}$$

式（3-27）或式（3-28）中的 ± 1 称为 f 在 a 处的符号。

有了定理3.3，我们可以对 Bent 函数再做进一步的细分。

定义 3.8 (（弱）正则 Bent 函数)： 设 p 为奇素数，q 为 p 的一个方幂，$f : \mathbb{F}_q \to \mathbb{F}_p$ 为一个 Bent 函数。如果 f 在所有 $a \in \mathbb{F}_q$ 处的符号都相同，则称 f 为弱正则 Bent 函数，称这个统一的符号为 f 的符号。如果对任意的 $a \in \mathbb{F}_q$，都有

$$W_f(a) = \xi_p^{f^*(a)}\sqrt{q}, \tag{3-29}$$

其中 f^* 为 f 的对偶，则称 f 为正则 Bent 函数。

下面的定义并不是标准的，主要是为了后面叙述的方便。

定义 3.9 (弱正则 PN 函数)： 设 p 为奇素数，q 为 p 的一个方幂，$\Pi : \mathbb{F}_q \to \mathbb{F}_q$ 为一个 PN 函数。我们称 Π 为弱正则 PN 函数，如果对任意的 $a \in \mathbb{F}_q^*$，函数

$$\begin{aligned} \Pi_a : \mathbb{F}_q &\to \mathbb{F}_p \\ x &\mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big(a\Pi(x)\big) \end{aligned} \tag{3-30}$$

都是弱正则 Bent 的。

注释 3.6： 注意到 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ 是一个满线性函数，由命题3.5，Π_a（$a \in \mathbb{F}_q^*$）均为 PN 函数。由定理3.2，它们都是 Bent 函数，因此上面的定义是合理的。

3.3　Bent 函数的值分布

在这一节中，设 p 为奇素数，$q=p^m$ 为 p 的一个方幂。对于函数 $f:\mathbb{F}_q\to\mathbb{F}_p$，我们称它的值分布为 $(n_0,\cdots,n_{p-1})$，如果对任意的 $0\leqslant i\leqslant p-1$，有 $n_i=|f^{-1}(i)|$。在这里，我们将 $\mathbb{F}_p$ 等同于集合 $\{0,1,\cdots,p-1\}$。

下面的两个定理完全地刻画了 Bent 函数的值分布。虽然它们的证明在文献中已存在，但是我们后面不仅需要这两个定理本身，也需要它们的证明，所以我们在这里给出证明。

定理 3.4 ([55]，定理 3.2)： 若 m 为偶数，则对任意的 Bent 函数 $f:\mathbb{F}_q\to\mathbb{F}_p$，都存在 $s\in\{0,1,\cdots,p-1\}$，使得 f 的值分布为 $(n_0,\cdots,n_{p-1})$，其中

$$\begin{aligned} n_s&=p^{m-1}+(p-1)p^{\frac{m}{2}-1},\\ n_i&=p^{m-1}-p^{\frac{m}{2}-1},\quad i\neq s, \end{aligned}\tag{3-31}$$

或

$$\begin{aligned} n_s&=p^{m-1}-(p-1)p^{\frac{m}{2}-1},\\ n_i&=p^{m-1}+p^{\frac{m}{2}-1},\quad i\neq s. \end{aligned}\tag{3-32}$$

证明： 由定义，我们有

$$W_f(0)=\sum_{x\in\mathbb{F}_q}\xi_p^{f(x)}=\sum_{i=0}^{p-1}n_i\xi_p^i,\tag{3-33}$$

其中 $n_i=|f^{-1}(i)|$（$0\leqslant i\leqslant p-1$）。由定理3.3，我们有

$$W_f(0)=\epsilon\xi_p^s\sqrt{q},\tag{3-34}$$

其中 $0\leqslant s\leqslant p-1$，且 $\epsilon\in\{\pm1\}$ 为 f 在 0 处的符号。由式（3-33）和式（3-34），我们有

$$\sum_{i=1}^{p-1}n_{i+s}\xi_p^i+(n_s-\epsilon\sqrt{q})=\sum_{i=1}^{p-1}(n_{i+s}-n_s+\epsilon\sqrt{q})\xi_p^i=0,\tag{3-35}$$

其中用到了事实

$$1+\xi_p+\cdots+\xi_p^{p-1}=0.\tag{3-36}$$

因为 m 为偶数，所以 $\sqrt{q}\in\mathbb{Q}$。由于 ξ_p^i（$1\leqslant i\leqslant p-1$）构成分圆域 $K=\mathbb{Q}(\xi_p)$ 在 $\mathbb{Q}$ 上的一组基，所以由式（3-35），我们有

$$n_{i+s}=n_s-\epsilon\sqrt{q},\quad 1\leqslant i\leqslant p-1.\tag{3-37}$$

由于

$$\sum_{i=0}^{p-1} n_i = |\mathbb{F}_q| = q = p^m, \tag{3-38}$$

结合式（3-37）我们解得

$$\begin{aligned} n_s &= p^{m-1} + \epsilon(p-1)p^{\frac{m}{2}-1}, \\ n_i &= p^{m-1} - \epsilon p^{\frac{m}{2}-1}, \quad i \neq s. \end{aligned} \tag{3-39}$$

定理得证。 ∎

注释 3.7： 从定理3.4的证明中，我们可以看出，f 的值分布是类型（3-31）还是类型（3-32），取决于 f 在 0 处的符号。

定理 3.5 ([55]，定理 3.4)： 若 m 为奇数，则对任意的 Bent 函数 $f : \mathbb{F}_q \to \mathbb{F}_p$，都存在 $s \in \{0, 1, \cdots, p-1\}$，使得 f 的值分布为 $(n_0, \cdots, n_{p-1})$，其中

$$n_i = p^{m-1} + (\frac{i+s}{p})p^{\frac{m-1}{2}}, \quad i = 0, \cdots, p-1, \tag{3-40}$$

或

$$n_i = p^{m-1} - (\frac{i+s}{p})p^{\frac{m-1}{2}}, \quad i = 0, \cdots, p-1, \tag{3-41}$$

其中，$(\frac{\cdot}{p})$ 是模 p 的勒让德符号，并且我们约定 $(\frac{0}{p}) = 0$。

为证明定理3.5，我们需要下面的引理，它实际上是定理2.9的一个简单推论。

引理 3.1 ([55]，定理 3.4 前的引理)： 设 p 为一个奇素数。若存在有理数 a_1，…，a_{p-1}，使得

$$a_1\xi_p + a_2\xi_p^2 + \cdots + a_{p-1}\xi_p^{p-1} = \begin{cases} \sqrt{p}, & \text{若 } p \equiv 1 \pmod 4, \\ \sqrt{-p}, & \text{若 } p \equiv 3 \pmod 4, \end{cases} \tag{3-42}$$

则对任意的 $1 \leqslant i \leqslant p-1$，有 $a_i = (\frac{i}{p})$。

定理3.5的证明： 类似定理3.4的证明，我们可以得到

$$\sum_{i=1}^{p-1} \epsilon p^{\frac{1-m}{2}}(n_{i+s} - n_s)\xi_p^i = \alpha\sqrt{p}, \tag{3-43}$$

其中 $0 \leqslant s \leqslant p-1$，$\epsilon \in \{\pm 1\}$ 为 f 在 0 处的符号，且

$$\alpha = \begin{cases} 1, & \text{若 } q \equiv 1 \pmod 4, \\ \sqrt{-1}, & \text{若 } q \equiv 3 \pmod 4. \end{cases} \tag{3-44}$$

由于 m 为奇数，所以 $p^{\frac{1-m}{2}}$ 为有理数且

$$\alpha=\begin{cases}1, & \text{若 } p\equiv 1 \pmod 4,\\ \sqrt{-1}, & \text{若 } p\equiv 3 \pmod 4.\end{cases} \tag{3-45}$$

由引理3.1，我们有

$$\epsilon p^{\frac{1-m}{2}}(n_{i+s}-n_s)=(\frac{i}{p}),\quad 1\leqslant i\leqslant p-1, \tag{3-46}$$

即

$$n_{i+s}=n_s+\epsilon(\frac{i}{p})p^{\frac{m-1}{2}},\quad 1\leqslant i\leqslant p-1. \tag{3-47}$$

结合式（3-38），定理得证。 ∎

注释 3.8： 从定理3.5的证明中，我们可以看出，f 的值分布是类型（3-40）还是类型（3-41），取决于 f 在 0 处的符号。

推论 3.1： 设 m 为偶数，$f:\mathbb{F}_q\to\mathbb{F}_p$ 为弱正则 Bent 函数，则对任意的 $b\in\mathbb{F}_q$，f_b 与 f 的值分布类型一致（类型（3-31）或类型（3-32）），其中

$$f_b(x)=f(x)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx),\quad x\in\mathbb{F}_q. \tag{3-48}$$

证明： 上面提到，一个 Bent 函数值分布的类型取决于它在 0 处的符号。由于 f 为弱正则 Bent 函数，其在任意点处的符号都相同。注意到对任意的 $b\in\mathbb{F}_q$，有

$$W_f(b)=\sum_{x\in\mathbb{F}_q}\xi_p^{f(x)+\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx)}=W_{f_b}(0), \tag{3-49}$$

即 f_b 在 0 处的符号与 f 在 b 处的符号相同。因此，f_b 在 0 处的符号与 f 在 0 处的符号相同。 ∎

3.4　C_Π 与 $\overline{C_\Pi}$ 的基本性质

在本章的剩余部分，我们设 p 为一个奇素数，m 为一个正整数，$q=p^m$，以及 $\Pi:\mathbb{F}_q\to\mathbb{F}_q$ 为一个 PN 函数。在1.2节中，我们定义了两类 $\mathbb{F}_p$ 上的线性码：C_Π（参见式（1-1））和 $\overline{C_\Pi}$（参见式（1-3））。在 [10] 中，Carlet、丁存生等人已经证明了 C_Π 与 $\overline{C_\Pi}$ 的一些基本性质。在这一节中，我们只列出之后我们将会用到的。

命题 3.6 ([10]，定理 4)： 设 $\Pi(0)=0$，则 C_Π 为一个 $[q-1,2m,d]_p$ 线性码，其中

$$d\geqslant\frac{p-1}{p}(p^m-p^{\frac{m}{2}}). \tag{3-50}$$

实际上，对 C_Π 中的任意非零码字 $\boldsymbol{c}$，都有

$$\frac{p-1}{p}(p^m-p^{\frac{m}{2}})\leqslant w_H(\boldsymbol{c})\leqslant\frac{p-1}{p}(p^m+p^{\frac{m}{2}}). \tag{3-51}$$

命题 3.7 ([10]，定理 5)： $\overline{C_\Pi}$ 为一个 $[q, 2m+1, d]_p$ 线性码，其中

$$d \geqslant \frac{p-1}{p}(p^m - p^{\frac{m}{2}}). \tag{3-52}$$

实际上，对 $\overline{C_\Pi}$ 中的任意非零码字 $\boldsymbol{c}$，都有

$$\frac{p-1}{p}(p^m - p^{\frac{m}{2}}) \leqslant w_H(\boldsymbol{c}) \leqslant \frac{p-1}{p}(p^m + p^{\frac{m}{2}}). \tag{3-53}$$

命题 3.8 ([10]，定理 6)： 设 $\Pi(0) = 0$，$d^\perp$ 为 C_Π 的对偶码 $C_\Pi^\perp$ 的最小距离，则 $2 \leqslant d^\perp \leqslant 4$，且 $d^\perp = 2$ 当且仅当存在 $x \in \mathbb{F}_q^*$ 及 $c \in \mathbb{F}_p \setminus \{0, 1\}$，使得 $\Pi(cx) = c\Pi$。

此外，若 $p = 3$，并且 Π 为偶函数，即对任意的 $x \in \mathbb{F}_q$，有 $\Pi(x) = \Pi(-x)$，则 $d^\perp = 4$。

命题 3.9 ([10]，定理 7)： 设 $\overline{d}^\perp$ 为 $\overline{C_\Pi}$ 的对偶码 $\overline{C_\Pi}^\perp$ 的最小距离，则

(1) 若 $p = 3$，则 $\overline{d}^\perp = 5$；

(2) 对于其余情形，$3 \leqslant \overline{d}^\perp \leqslant 4$。

3.5　$\overline{C_\Pi}$ 的重量分布

在这一节中，我们先确定 $\overline{C_\Pi}$ 的重量分布。实际上，我们甚至可以完全确定其码字的类型以及每种类型的个数。

对于 $\overline{C_\Pi}$ 中的码字 $c_{a,b,c}$（a，b，$c \in \mathbb{F}_q$），我们称它为一个 $(n_0, \cdots, n_{p-1})$-码字，如果函数 $f_{a,b,c} : \mathbb{F}_q \to \mathbb{F}_p$（参见式（1-2））的值分布为 $(n_0, \cdots, n_{p-1})$，即对任意的 $0 \leqslant i \leqslant p-1$，有 $|f_{a,b,c}^{-1}(i)| = n_i$。

$\overline{C_\Pi}$ 中有一些码字的类型是容易确定的，我们先来考察它们。实际上，当 $a = 0$ 且 $b = 0$ 时，对任意的 $x \in \mathbb{F}_q$，有 $f_{0,0,c}(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c)$。对任意的 $0 \leqslant i \leqslant p-1$，若 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c) = i$，则 $c_{0,0,c} = (i, \cdots, i)$，即 $c_{0,0,c}$ 为一个 $(0, \cdots, 0, p^m, 0, \cdots, 0)$-码字，其中 p^m 位于第 i 位。在 $\overline{C_\Pi}$ 中，这 p 种类型的码字每种都只有一个。当 $a = 0$ 但 $b \neq 0$ 时，任取 $c \in \mathbb{F}_q$，$x \mapsto bx + c$ 为 $\mathbb{F}_q$ 的一个置换，因此 $c_{0,b,c}$ 是一个 $(p^{m-1}, \cdots, p^{m-1})$-码字。在 $\overline{C_\Pi}$ 中，一共有 $p(q-1) = p^{m+1} - p$ 个这种类型的码字。

剩下的就是 $a \neq 0$ 的情形。由命题3.3，命题3.5及定理3.2，此时对任意的 b，$c \in \mathbb{F}_q$，$f_{a,b,c} : \mathbb{F}_q \to \mathbb{F}_p$ 均为 Bent 函数。令

$$\overline{\Omega} = \{c_{a,b,c} \in \overline{C_\Pi} : \ a \neq 0\}. \tag{3-54}$$

不难算出 $\overline{\Omega}$ 中一共有 $pq(q-1) = p^{m+1}(p^m - 1)$ 个码字。

对 $\overline{\Omega}$ 中码字类型的分析，关键是在其上引入一个群作用。考虑群 $G = \mathbb{F}_p^* \times \mathbb{F}_p$，其乘法运算定义如下：

$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1\alpha_2, \alpha_1\beta_2 + \beta_1). \tag{3-55}$$

不难看出 G 中的单位元为 $(1,0)$。对任意的 $\alpha \in \mathbb{F}_p^*$，$\beta \in \mathbb{F}_p$ 以及 a，b，$c \in \mathbb{F}_q$，我们有

$$\begin{aligned} \alpha f_{a,b,c}(x) + \beta &= \alpha \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big(a\Pi(x) + bx + c\big) + \beta \\ &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big(\alpha a\Pi(x) + \alpha bx + \alpha c + \beta'\big), \end{aligned} \tag{3-56}$$

即 $\alpha f_{a,b,c} + \beta = f_{\alpha a,\alpha b,\alpha c+\beta'}$，其中 $\beta' \in \mathbb{F}_q$ 是任意使得 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta') = \beta$ 的元素。因此，我们可以如下定义一个群 G 在 $\overline{\Omega}$ 上的作用：

$$(\alpha,\beta)\cdot c_{a,b,c} = c_{\alpha a,\alpha b,\alpha c+\beta'}. \tag{3-57}$$

显然，这个定义与 β' 的选取无关。

引理 3.2： 群 G 在 $\overline{\Omega}$ 上的作用是自由的，也就是说，如果 $(\alpha,\beta) \in G$ 固定了某个码字 $c_{a,b,c} \in \overline{\Omega}$，那么一定有 $(\alpha,\beta) = (1,0)$。

证明： 由定义，我们有

$$\alpha a = a, \quad \alpha b = b, \quad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha c + \beta' - c) = 0. \tag{3-58}$$

因为 $a \neq 0$，所以 $\alpha = 1$，从而

$$\beta = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta') = 0. \tag{3-59}$$

因此，群 G 在 $\overline{\Omega}$ 上的作用是自由的。 ∎

由引理3.2，我们立马知道：$\overline{\Omega}$ 中有 $p^m(p^m-1)/(p-1)$ 个 G-轨道，且每个 G-轨道中均包含 $(p-1)p$ 个码字。证明定理3.6的核心，在于仔细地考察 $\overline{\Omega}$ 中码字的类型在群 G 作用下是如何变化的。经过简单的计算，不难看出若 $c_{a,b,c} \in \overline{\Omega}$ 是一个 $(n_0,\cdots,n_{p-1})$-码字，则对任意的 $(\alpha,\beta) \in G$，$(\alpha,\beta)\cdot c_{a,b,c}$ 是一个 $(n'_0,\cdots,n'_{p-1})$-码字，其中 $n'_i = n_{\alpha^{-1}(i-\beta)}$（$0 \leqslant i \leqslant p-1$）。

为了叙述的方便，我们引入下面的定义：

定义 3.10： 当 m 为奇数时，称 $\overline{\Omega}$ 中的码字 $c_{a,b,c}$ 为 s^+-码字（相应地，s^--码字），其中 $0 \leqslant s \leqslant p-1$，如果它是一个 $(n_0,\cdots,n_{p-1})$-码字，其中

$$n_i = p^{m-1} + (\frac{i+s}{p})p^{\frac{m-1}{2}}, \quad \forall\, 0 \leqslant i \leqslant p-1, \tag{3-60}$$

（相应地，$n_i = p^{m-1} - (\frac{i+s}{p})p^{\frac{m-1}{2}}$，$\forall\, 0 \leqslant i \leqslant p-1$）. (3-61)

当 m 为偶数时，称 $\overline{\Omega}$ 中的码字 $c_{a,b,c}$ 为 s^+-码字（相应地，s^--码字），其中 $0 \leqslant s \leqslant p-1$，如果它是一个 $(n_0,\cdots,n_{p-1})$-码字，其中

$$n_i = \begin{cases} p^{m-1} + (p-1)p^{\frac{m}{2}-1}, & \text{若 } i = s, \\ p^{m-1} - p^{\frac{m}{2}-1}, & \text{若 } i \neq s, \end{cases} \tag{3-62}$$

$$（相应地，n_i=\begin{cases}p^{m-1}-(p-1)p^{\frac{m}{2}-1}, & 若\ i=s,\\ p^{m-1}+p^{\frac{m}{2}-1}, & 若\ i\neq s,\end{cases}）. \tag{3-63}$$

如果存在 $0\leqslant s\leqslant p-1$，使得 $c_{a,b,c}\in\overline{\Omega}$ 是一个 s^+-码字（相应地，s^--码字），则称 $c_{a,b,c}$ 为一个正（相应地，负）码字。如果 s 还不为 0，则称 $c_{a,b,c}$ 为一个严格正（相应地，负）码字。

注释 3.9： 由定理3.4及定理3.5，对 $\overline{C_\Pi}$ 中的任意码字 $c_{a,b,c}$，都存在 $0\leqslant s\leqslant p-1$，使得 $c_{a,b,c}$ 是一个 s^+-码字或 s^--码字。

有了前面的准备，我们终于可以叙述关于 $\overline{C_\Pi}$ 的重量分布的主要定理。对任意的 $0\leqslant i\leqslant q$，用 $\overline{A}_i$ 表示 $\overline{C_\Pi}$ 中汉明重量为 i 的码字的个数。

定理 3.6： 设 $\Pi:\mathbb{F}_q\to\mathbb{F}_q$ 为一个 PN 函数。

(1) 若 m 为奇数，则 $\overline{C_\Pi}$ 中码字的类型以及每种类型的码字个数如表3.1所示。因此，除了下面几个值以外，$\overline{A}_i$ 均为 0：

$$\begin{aligned}&\overline{A}_0=1,\\ &\overline{A}_{(p-1)p^{m-1}-p^{\frac{m-1}{2}}}=\frac{(p-1)p^m(p^m-1)}{2},\\ &\overline{A}_{(p-1)p^{m-1}}=(p^m-1)(p^m+p),\\ &\overline{A}_{(p-1)p^{m-1}+p^{\frac{m-1}{2}}}=\frac{(p-1)p^m(p^m-1)}{2},\\ &\overline{A}_{p^m}=p-1.\end{aligned} \tag{3-64}$$

特别地，$\overline{C_\Pi}$ 是一个 4 重码，最小距离为 $(p-1)p^{m-1}-p^{\frac{m-1}{2}}$。

(2) 若 m 为偶数，且 Π 满足下面两个条件中的一个：

(a) $p=3$；

(b) $|\Pi^{-1}(0)|=1$，Π 是一个弱正则 PN 函数，且函数 $\mathbb{F}_q^*\to\mathbb{F}_p,\ a\mapsto\Pi_a^*(0)$ 不为满射，其中 $\Pi_a=f_{a,0,0}$，Π_a^* 为 Π_a 的对偶，

则 $\overline{C_\Pi}$ 中码字的类型以及每种类型的码字个数如表3.1所示。因此，除了下面几个值以外，$\overline{A}_i$ 均为 0：

$$\begin{aligned}&\overline{A}_0=1,\\ &\overline{A}_{(p-1)(p^{m-1}-p^{\frac{m}{2}-1})}=\frac{p^m(p^m-1)}{2},\\ &\overline{A}_{(p-1)p^{m-1}-p^{\frac{m}{2}-1}}=\frac{(p-1)p^m(p^m-1)}{2},\\ &\overline{A}_{(p-1)p^{m-1}}=p^{m+1}-p,\\ &\overline{A}_{(p-1)p^{m-1}+p^{\frac{m}{2}-1}}=\frac{(p-1)p^m(p^m-1)}{2},\end{aligned} \tag{3-65}$$

$$\overline{A}_{(p-1)(p^{m-1}+p^{\frac{m}{2}-1})} = \frac{p^m(p^m-1)}{2},$$
$$\overline{A}_{p^m} = p-1.$$

特别地，$\overline{C_{\Pi}}$ 是一个 6 重码，最小距离为 $(p-1)(p^{m-1}-p^{\frac{m}{2}-1})$。

表 3.1　$\overline{C_{\Pi}}$ 中码字的类型及其数量

类型	数量
$\substack{(0,\cdots,0,p^m,0,\cdots,0)\\(\forall\ 0\leqslant i\leqslant p-1)}$	1
$(p^{m-1},\cdots,p^{m-1})$	$p^{m+1}-p$
$s^+\ (\forall\ 0\leqslant s\leqslant p-1)$	$\frac{p^m}{2}(p^m-1)$
$s^-\ (\forall\ 0\leqslant s\leqslant p-1)$	$\frac{p^m}{2}(p^m-1)$

证明： 先考虑 m 为奇数的情形。设 $(\alpha,\beta)\in G$ 及 $c_{a,b,c}\in\overline{\Omega}$。若 $c_{a,b,c}$ 是一个 s^+-码字，通过简单计算可知：当 $(\frac{\alpha}{p})=1$ 时，$c_{a,b,c}$ 为 $(\alpha s-\beta)^+$-码字；当 $(\frac{\alpha}{p})=-1$ 时，$c_{a,b,c}$ 为 $(\alpha s-\beta)^-$-码字。类似地，若 $c_{a,b,c}$ 是一个 s^--码字，则当 $(\frac{\alpha}{p})=1$ 时，$c_{a,b,c}$ 为 $(\alpha s-\beta)^-$-码字；当 $(\frac{\alpha}{p})=-1$ 时，$c_{a,b,c}$ 为 $(\alpha s-\beta)^+$-码字。特别地，每个 $\overline{\Omega}$ 的 G-轨道中都包含一个 0^+-码字。

设 O 为 $\overline{\Omega}$ 的一个 G-轨道，且 $c_{a,b,c}$ 为 O 中的一个 0^+-码字。于是对任意的 $(\alpha,\beta)\in G$，当 $(\frac{\alpha}{p})=1$ 时，$(\alpha,\beta)\cdot c_{a,b,c}$ 是一个 $(-\beta)^+$-码字；当 $(\frac{\alpha}{p})=-1$ 时，$(\alpha,\beta)\cdot c_{a,b,c}$ 是一个 $(-\beta)^-$-码字。在 $\mathbb{F}_p^*$ 中，共有 $(p-1)/2$ 个元素 α 使得 $(\frac{\alpha}{p})=1$，以及 $(p-1)/2$ 个元素 α 使得 $(\frac{\alpha}{p})=-1$。因此，对任意的 $0\leqslant s\leqslant p-1$，在 O 中有 $(p-1)/2$ 个 s^+-码字以及 $(p-1)/2$ 个 s^--码字。这就证明了关于 $\overline{C_{\Pi}}$ 中码字的类型及其数量的断言。

为了确定 $\overline{C_{\Pi}}$ 的重量分布，只需考虑 $\overline{\Omega}$ 中码字的汉明重量，因为其余码字的汉明重量是显然的。由定义不难看出，一个 $\overline{\Omega}$ 中码字的汉明重量为 $(p-1)p^{m-1}$，当且仅当它是一个 0^+-码字或 0^--码字。设 $1\leqslant s\leqslant p-1$。若 $(\frac{s}{p})=1$，则任意的 s^+-码字具有汉明重量 $(p-1)p^{m-1}-p^{\frac{m-1}{2}}$，以及任意的 s^--码字具有汉明重量 $(p-1)p^{m-1}+p^{\frac{m-1}{2}}$。若 $(\frac{s}{p})=-1$，则情况刚好相反。因此，在 $\overline{\Omega}$ 中，汉明重量为 $(p-1)p^{m-1}-p^{\frac{m-1}{2}}$ 的码字与汉明重量为 $(p-1)p^{m-1}+p^{\frac{m-1}{2}}$ 的码字的个数相等。这就证明了关于 $\overline{C_{\Pi}}$ 的重量分布的断言。

下面假设 m 为偶数。设 $(\alpha,\beta)\in G$ 及 $c_{a,b,c}\in\overline{\Omega}$。若 $c_{a,b,c}$ 是一个 s^+-码字，则

$(\alpha,\beta)\cdot c_{a,b,c}$ 是一个 $(\alpha s+\beta)^+$-码字。特别地，$c_{a,b,c}$ 所在的 G-轨道中存在 0^+-码字。若 $c_{a,b,c}$ 是一个 s^--码字，则 $(\alpha,\beta)\cdot c_{a,b,c}$ 是一个 $(\alpha s+\beta)^-$-码字。特别地，$c_{a,b,c}$ 所在的 G-轨道中存在 0^--码字。设 O 为 $\overline{\Omega}$ 的一个 G-轨道。由前面的分析知道，O 中要么全部都是正码字，要么全部都是负码字。我们将前者称为正轨道，将后者称为负轨道。

若 O 为 $\overline{\Omega}$ 的一个正轨道，且 $c_{a,b,c}$ 为 O 中的一个 0^+-码字，则对任意的 $(\alpha,\beta)\in G$，$(\alpha,\beta)\cdot c_{a,b,c}$ 是一个 β^+-码字。特别地，对任意的 $0\leqslant s\leqslant p-1$，在 O 中有 $p-1$ 个 s^+-码字。如果 $c_{a,b,c}$ 是 s^+-码字，则

$$w_H(c_{a,b,c})=\begin{cases}(p-1)(p^{m-1}-p^{\frac{m}{2}-1}), & \text{若 } s=0,\\ (p-1)p^{m-1}+p^{\frac{m}{2}-1}, & \text{若 } s\neq 0.\end{cases} \tag{3-66}$$

因此，在 O 中有 $p-1$ 个汉明重量为 $(p-1)(p^{m-1}-p^{\frac{m}{2}-1})$ 的码字，有 $(p-1)^2$ 个汉明重量为 $(p-1)p^{m-1}+p^{\frac{m}{2}-1}$ 的码字。类似地，若 O 为 $\overline{\Omega}$ 的一个负轨道，且 $c_{a,b,c}$ 为 O 中的一个 0^--码字，则对任意的 $0\leqslant s\leqslant p-1$，在 O 中有 $p-1$ 个 s^--码字。此外，O 中有 $p-1$ 个汉明重量为 $(p-1)(p^{m-1}+p^{\frac{m}{2}-1})$ 的码字，有 $(p-1)^2$ 个汉明重量为 $(p-1)p^{m-1}-p^{\frac{m}{2}-1}$ 的码字。

设 $\overline{\Omega}$ 有 k_+ 个正轨道，有 k_- 个负轨道。为了证明 $k_+=k_-$，我们需要先考虑 $\overline{C_\Pi}$ 的重量分布。由前面的讨论，我们知道对于 $i\neq 0$，$(p-1)p^{m-1}$，p^m，$(p-1)p^{m-1}\pm p^{\frac{m}{2}-1}$，$(p-1)(p^{m-1}\pm p^{\frac{m}{2}-1})$，$\overline{A}_i$ 均为 0。此外，我们有

$$\begin{aligned}
&\overline{A}_0=1,\\
&\overline{A}_{(p-1)(p^{m-1}-p^{\frac{m}{2}-1})}=(p-1)k_+,\\
&\overline{A}_{(p-1)p^{m-1}-p^{\frac{m}{2}-1}}=(p-1)^2k_-,\\
&\overline{A}_{(p-1)p^{m-1}}=p^{m+1}-p,\\
&\overline{A}_{(p-1)p^{m-1}+p^{\frac{m}{2}-1}}=(p-1)^2k_+,\\
&\overline{A}_{(p-1)(p^{m-1}+p^{\frac{m}{2}-1})}=(p-1)k_-,\\
&\overline{A}_{p^m}=p-1.
\end{aligned} \tag{3-67}$$

若 $p=3$，由命题3.9可知，$\overline{C_\Pi}$ 的对偶码 $\overline{C_\Pi}^\perp$ 的最小距离是 5。计算 $\overline{C_\Pi}$ 的前

4 阶 Pless 幂矩，我们得到

$$\begin{cases} \sum\limits_{j=0}^{3^m} \overline{A}_j = 3^{2m+1}, \\ \sum\limits_{j=0}^{3^m} j\overline{A}_j = 2\cdot 3^{3m}, \\ \sum\limits_{j=0}^{3^m} j^2\overline{A}_j = 2\cdot 3^{3m-1}(2\cdot 3^m+1), \\ \sum\limits_{j=0}^{3^m} j^3\overline{A}_j = 2\cdot 3^{3m-2}(4\cdot 3^{2m}+2\cdot 3^{m+1}-1). \end{cases} \tag{3-68}$$

上面的式子可以看作关于

$$\overline{A}_{2\cdot(3^{m-1}\pm 3^{\frac{m}{2}-1})}, \qquad \overline{A}_{2\cdot 3^{m-1}\pm 3^{\frac{m}{2}-1}} \tag{3-69}$$

的线性方程组。由于其系数矩阵为一个范德蒙德矩阵，因此它有唯一解。经计算，可得

$$\begin{cases} \overline{A}_{2\cdot(3^{m-1}\pm 3^{\frac{m}{2}-1})} = \frac{3^m(3^m-1)}{2}, \\ \overline{A}_{2\cdot 3^{m-1}\pm 3^{\frac{m}{2}-1}} = 3^m(3^m-1), \end{cases} \tag{3-70}$$

从而

$$k_+ = k_- = \frac{3^m(3^m-1)}{4}. \tag{3-71}$$

现假设 Π 满足条件 (b)。于是对任意的 $a\in\mathbb{F}_q^*$，函数 $\Pi_a : \mathbb{F}_q \to \mathbb{F}_p$，$x \mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big(a\Pi(x)\big)$ 是一个弱正则 Bent 函数。由推论3.1，若 $c_{a,0,0}\in\overline{\Omega}$ 为正（相应地，负）码字，则对任意的 b，$c\in\mathbb{F}_q$，$c_{a,b,c}$ 也是正（相应地，负）码字。因此，为了证明 $k_+ = k_-$，我们只需证明在 $c_{a,0,0}$（$a\in\mathbb{F}_q^*$）中，有一半为正码字，另一半为负码字即可。由定理3.4的证明，只需证明在弱正则 Bent 函数 Π_a（$a\in\mathbb{F}_q^*$）中，有一半符号为 1，而另一半符号为 -1 即可。

由定理3.3，对任意的 $a\in\mathbb{F}_q^*$，我们有

$$W_{\Pi_a}(0) = \epsilon_a \xi_p^{\Pi_a^*(0)}\sqrt{q}, \tag{3-72}$$

其中 $\epsilon_a\in\{\pm 1\}$ 为 Π_a 的符号。注意到

$$\begin{aligned} \sum_{a\in\mathbb{F}_q^*} W_{\Pi_a}(0) &= \sum_{a\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q} \xi_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(a\Pi(x)\right)} \\ &= \sum_{x\in\mathbb{F}_q}\sum_{a\in\mathbb{F}_q^*} \xi_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\left(a\Pi(x)\right)} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{x\in\mathbb{F}_q \\ \Pi(x)=0}} (q-1) + \sum_{\substack{x\in\mathbb{F}_q \\ \Pi(x)\neq 0}} (-1) \\
&= |\Pi^{-1}(0)|(q-1) - (q - |\Pi^{-1}(0)|) \\
&= q|\Pi^{-1}(0)| - q = 0,
\end{aligned} \tag{3-73}
$$

因此

$$
\sum_{a\in\mathbb{F}_q^*} \epsilon_a \xi_p^{\Pi_a^*(0)} = 0. \tag{3-74}
$$

上式可改写为

$$
\sum_{r=0}^{p-1} \Big(\sum_{\substack{a\in\mathbb{F}_q^* \\ \Pi_a^*(0)=r}} \epsilon_a \Big) \xi_p^r = 0, \tag{3-75}
$$

这表明 ξ_p 是下列多项式的根：

$$
\sum_{r=0}^{p-1} \Big(\sum_{\substack{a\in\mathbb{F}_q^* \\ \Pi_a^*(0)=r}} \epsilon_a \Big) X^r \in \mathbb{Z}[X]. \tag{3-76}
$$

由于 ξ_p 在 $\mathbb{Q}$ 上的极小多项式为 $X^{p-1} + X^{p-2} + \cdots + 1$，我们知道和式

$$
S_r = \sum_{\substack{a\in\mathbb{F}_q^* \\ \Pi_a^*(0)=r}} \epsilon_a, \quad 0 \leqslant r \leqslant p-1 \tag{3-77}
$$

全部都相等。由于函数 $\mathbb{F}_q^* \to \mathbb{F}_p$，$a \mapsto \Pi_a^*(0)$ 不为满射，所以对于某个 $0 \leqslant i \leqslant p-1$，有 $S_i = 0$，从而所有的 S_r（$0 \leqslant r \leqslant p-1$）都为 0。又因为

$$
\sum_{r=0}^{p-1} S_r = \sum_{a\in\mathbb{F}_q^*} \epsilon_a = |\{a \in \mathbb{F}_q^* : \epsilon_a = 1\}| - |\{a \in \mathbb{F}_q^* : \epsilon_a = -1\}|, \tag{3-78}
$$

我们得到：在弱正则 Bent 函数 Π_a（$a \in \mathbb{F}_q^*$）中，有一半符号为 1，而另一半符号为 -1。这就证明了 $k_+ = k_-$。剩余的部分与 m 为奇数的情形基本相同，我们就不再赘述了。 ∎

注释 3.10： 从定理3.6的证明过程中，我们可以看出：当 m 为奇数时，正码字与负码字之间可以通过群 G 的作用互相转换；而当 m 为偶数时，正码字全体和负码字全体分别是 G-稳定的——这正是偶数情形我们需要添加额外条件的原因。

注释 3.11： 假设 Π 是 Dembowski-Ostrom 类型或 Coulter-Matthews 类型的 PN 函数。由 [12] 中的引理 2，$\Pi^{-1}(0) = \{0\}$。由 [12] 中的引理 3 ii)，Π 是一个弱正则 PN 函数，并且函数 $\mathbb{F}_q^* \to \mathbb{F}_p$，$a \mapsto \Pi_a^*(0)$ 是恒零映射。因此，所有已知的 $\mathbb{F}_q$ 上的

PN 函数都满足定理3.6中的条件 (b)。

3.6　C_Π 的重量分布

本节确定 C_Π 的重量分布。对任意的 $0 \leqslant i \leqslant q-1$，用 A_i 表示 C_Π 中汉明重量为 i 的码字的个数。我们有如下的主要定理：

定理 3.7：设 $\Pi : \mathbb{F}_q \to \mathbb{F}_q$ 为一个 PN 函数，使得 $\Pi(0)=0$，且对任意的 $c \in \mathbb{F}_p \setminus \{0,1\}$ 及 $x \in \mathbb{F}_q^*$，有 $\Pi(cx) \neq c\Pi(x)$。

(1) 若 m 为奇数，则除了下面几个值以外，A_i 均为 0：

$$\begin{aligned} &A_0 = 1, \\ &A_{(p-1)p^{m-1}-p^{\frac{m-1}{2}}} = (p-1)(p^m-1)\frac{p^{m-1}+p^{\frac{m-1}{2}}}{2}, \\ &A_{(p-1)p^{m-1}} = (p^{m-1}+1)(p^m-1), \\ &A_{(p-1)p^{m-1}+p^{\frac{m-1}{2}}} = (p-1)(p^m-1)\frac{p^{m-1}-p^{\frac{m-1}{2}}}{2}. \end{aligned} \tag{3-79}$$

特别地，C_Π 是一个 3 重码，最小距离为 $(p-1)p^{m-1}-p^{\frac{m-1}{2}}$。

(2) 若 m 为偶数，且 Π 满足下面两个条件中的一个：

(a) $p=3$；

(b) $|\Pi^{-1}(0)|=1$，Π 是一个弱正则 PN 函数，且函数 $\mathbb{F}_q^* \to \mathbb{F}_p,\ a \mapsto \Pi_a^*(0)$ 不为满射，其中 $\Pi_a = f_{a,0,0}$，Π_a^* 为 Π_a 的对偶，

则除了下面几个值以外，A_i 均为 0：

$$\begin{aligned} &A_0 = 1, \\ &A_{(p-1)(p^{m-1}-p^{\frac{m}{2}-1})} = \frac{p^m-1}{2}(p^{m-1}+p^{\frac{m}{2}}-p^{\frac{m}{2}-1}), \\ &A_{(p-1)p^{m-1}-p^{\frac{m}{2}-1}} = \frac{p^m-1}{2}(p-1)(p^{m-1}+p^{\frac{m}{2}-1}), \\ &A_{(p-1)p^{m-1}} = p^m-1, \\ &A_{(p-1)p^{m-1}+p^{\frac{m}{2}-1}} = \frac{p^m-1}{2}(p-1)(p^{m-1}-p^{\frac{m}{2}-1}), \\ &A_{(p-1)(p^{m-1}+p^{\frac{m}{2}-1})} = \frac{p^m-1}{2}(p^{m-1}-p^{\frac{m}{2}}+p^{\frac{m}{2}-1}). \end{aligned} \tag{3-80}$$

特别地，C_Π 是一个 5 重码，最小距离为 $(p-1)(p^{m-1}-p^{\frac{m}{2}-1})$。

证明：　注意到对任意的 a，$b \in \mathbb{F}_q$，有 $w_H(c_{a,b}) = w_H(c_{a,b,0})$。此外，由命题3.8，$C_\Pi$ 的对偶码 $C_\Pi^\perp$ 的最小距离至少为 3。

m 为奇数的情形是容易处理的。由定理3.5，C_Π 中非零码字的汉明重量只可能

是 $(p-1)p^{m-1}$，$(p-1)p^{m-1}+p^{\frac{m-1}{2}}$，$(p-1)p^{m-1}-p^{\frac{m-1}{2}}$ 中的一个。只需计算 C_{Π} 的前 3 阶 Pless 幂矩（可以参见 [11] 中的定理 2），我们即可证明定理3.7中的断言。

下面考虑 m 为偶数的情形。若 $a=0$ 且 $b\neq 0$，则 $w_H(c_{a,b,0})=(p-1)p^{m-1}$。一共有 p^m-1 个这样的码字。接着，令

$$\Omega=\{c_{a,b,0}\in\overline{\Omega}\}. \tag{3-81}$$

由定理3.4，对任意的码字 $c_{a,b,0}\in\Omega$，都存在 $0\leqslant s\leqslant p-1$，使得 $c_{a,b,0}$ 是一个 s^+-码字或 s^--码字。不难看出，在 Ω 中，一共有 $A_{(p-1)(p^{m-1}-p^{\frac{m}{2}-1})}$ 个 0^+-码字，$A_{(p-1)(p^{m-1}+p^{\frac{m}{2}-1})}$ 个 0^- 码字，$A_{(p-1)p^{m-1}+p^{\frac{m}{2}-1}}$ 个严格正码字，以及 $A_{(p-1)p^{m-1}-p^{\frac{m}{2}-1}}$ 个严格负码字。若 $c_{a,b,0}\in\Omega$ 是一个正码字，则对任意的 $0\leqslant s\leqslant p-1$，在 $(\{1\}\times\mathbb{F}_p)\cdot c_{a,b,0}$ 中恰有 1 个 s^+-码字。若 $c_{a,b,0}\in\Omega$ 是一个负码字，也有类似的结论成立。因为

$$\overline{\Omega}=(\{1\}\times\mathbb{F}_p)\cdot\Omega, \tag{3-82}$$

由表3.1，我们得到

$$\begin{cases} A_{(p-1)(p^{m-1}-p^{\frac{m}{2}-1})}+A_{(p-1)p^{m-1}+p^{\frac{m}{2}-1}}=\dfrac{p^m(p^m-1)}{2},\\ A_{(p-1)(p^{m-1}+p^{\frac{m}{2}-1})}+A_{(p-1)p^{m-1}-p^{\frac{m}{2}-1}}=\dfrac{p^m(p^m-1)}{2}. \end{cases} \tag{3-83}$$

计算 C_{Π} 的 1 阶与 2 阶 Pless 幂矩，我们得到

$$\begin{cases} \sum\limits_{j=0}^{p^m-1} jA_j=p^{2m-1}(p-1)(p^m-1),\\ \sum\limits_{j=0}^{p^m-1} j^2A_j=p^{2m-2}(p-1)(p^m-1)\big(p+(p-1)(p^m-2)\big). \end{cases} \tag{3-84}$$

上面的式子可以看作关于

$$A_{(p-1)p^{m-1}\pm p^{\frac{m}{2}-1}},\qquad A_{(p-1)(p^{m-1}\pm p^{\frac{m}{2}-1})} \tag{3-85}$$

的线性方程组。经计算，可以发现该线性方程组只有唯一解，即定理叙述中给出的那个解。于是定理得证。 ∎

注释 3.12：假设 Π 是 Coulter-Matthews 类型的 PN 函数，则 $\Pi(0)=0$ 且 Π 为偶函数，即对任意的 $x\in\mathbb{F}_{3^m}$，有 $\Pi(x)=\Pi(-x)$。假设存在 $x\in\mathbb{F}_q^*$，使得 $\Pi(2x)=2\Pi(x)$，则

$$\Pi(x)=\Pi(-x)=\Pi(2x)=2\Pi(x), \tag{3-86}$$

从而 $\Pi(x)=0$。然而，由 [12] 中的引理 2，有 $\Pi^{-1}(0)=\{0\}$，矛盾。因此，Π 满足定理3.7中的条件。

注释 3.13： 假设 Π 为 Dembowski-Ostrom 类型的 PN 函数，即

$$\Pi(x)=\sum_{0\leqslant i\leqslant j\leqslant m-1} a_{ij}x^{p^i+p^j}, \tag{3-87}$$

其中 $a_{ij}\in\mathbb{F}_q$。若存在 $y\in\mathbb{F}_q^*$ 以及 $c\in\mathbb{F}_p^*\setminus\{0,1\}$，使得 $\Pi(cy)=c\Pi(y)$，则

$$\begin{aligned} c\Pi(y)=\Pi(cy)&=\sum_{0\leqslant i\leqslant j\leqslant m-1} a_{ij}(cy)^{p^i+p^j}\\ &=\sum_{0\leqslant i\leqslant j\leqslant m-1} a_{ij}c^{p^i+p^j}y^{p^i+p^j}\\ &=\sum_{0\leqslant i\leqslant j\leqslant m-1} a_{ij}c^{p^i}c^{p^j}y^{p^i+p^j}\\ &=\sum_{0\leqslant i\leqslant j\leqslant m-1} a_{ij}c^{2}y^{p^i+p^j}\\ &=c^2\sum_{0\leqslant i\leqslant j\leqslant m-1} a_{ij}y^{p^i+p^j}=c^2\Pi(y). \end{aligned} \tag{3-88}$$

因为 Π 是偶函数且 $\Pi(0)=0$，由 [12] 中的引理 2，有 $\Pi^{-1}(0)=\{0\}$。于是 $\Pi(y)\neq 0$，从而 $c=c^2$，即 $c=0$ 或 $c=1$，矛盾。因此，Π 满足定理3.7中的条件。

从上面的两个注释中，我们可以看出，所有已知的 $\mathbb{F}_q$ 上的 PN 函数都满足定理3.7中的条件。

3.7　由线性码构造秘密共享方案的 Massey 框架

设 q 为一个素数方幂，C 为一个 $[n,k,d]_q$ 线性码，$G=[\boldsymbol{g}_0,\boldsymbol{g}_1,\cdots,\boldsymbol{g}_{n-1}]$ 为 C 的一个生成矩阵，也就是说，G 的行向量张成了 $\mathbb{F}_q$ 上的线性空间 C。我们假设矩阵 G 的任一列向量都不为零向量。有许多从线性码构造秘密共享方案的方法[3-4,56]，在这里我们介绍 Massey 的框架[4]。

在由 C 构造的秘密共享方案中，每个秘密用 $\mathbb{F}_q$ 中的一个元素表示，有一名分发者以及 $n-1$ 名秘密保管者，分别为 P_1，P_2，…，P_{n-1}。为了将秘密 s 分为 $n-1$ 份额，分发者首先要随机选取一个 $\mathbb{F}_q^k$ 中的向量 $\boldsymbol{u}=(u_0,\cdots,u_{k-1})$，使得 $s=\boldsymbol{u}\boldsymbol{g}_0$。在 $\mathbb{F}_q^k$ 中，满足这个条件的 $\boldsymbol{u}$ 一共有 q^{k-1} 个。接着，分发者将 $\boldsymbol{u}$ 当作信息向量，计算

$$\boldsymbol{t}=(t_0,t_1,\cdots,t_{n-1})=\boldsymbol{u}G, \tag{3-89}$$

并将 t_i 分发给保管者 P_i（$1\leqslant i\leqslant n-1$）。

秘密 s 的恢复过程也很简单。由于 $t_0=\boldsymbol{u}\boldsymbol{g}_0=s$，因此秘密份额集 $\{t_{i_1},t_{i_2},\cdots,t_{i_m}\}$

可以唯一地确定 s，当且仅当 $\boldsymbol{g}_0$ 为 $\boldsymbol{g}_1$，…，$\boldsymbol{g}_{i_m}$ 的线性组合。实际上，若

$$\boldsymbol{g}_0 = \sum_{j=1}^{m} x_j \boldsymbol{g}_{i_j}, \quad x_j \in \mathbb{F}_q, \tag{3-90}$$

则

$$s = \sum_{j=1}^{m} x_j t_{i_j}. \tag{3-91}$$

于是我们有如下的引理：

引理 3.3 ([4])： 设 G 为 $[n,k,d]_q$ 线性码 C 的一个生成矩阵，则秘密份额集 $\{t_{i_1}, t_{i_2}, \cdots, t_{i_m}\}$（$1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n-1$，$1 \leqslant m \leqslant n-1$）可以唯一地确定秘密 s，当且仅当在 C 的对偶码 $C^{\perp}$ 中存在形如

$$(1, 0, \cdots, 0, c_{i_1}, 0, \cdots, 0, c_{i_m}, 0, \cdots, 0) \tag{3-92}$$

的码字，其中至少有一个 c_{i_j} 不为 0。

注释 3.14： 要注意的是，生成矩阵 G 的选取会影响秘密共享方案中秘密份额的构造与分配，但不会影响秘密共享方案的存取结构。

显然，在一个秘密共享方案中，如果一个保管者的子集可以合谋“拼凑”出完整秘密，那么任何一个包含该子集的保管者子集也可以合谋“拼凑”出完整秘密。我们称一个保管者的子集为秘密共享方案的极小访问集，如果该子集所含保管者的秘密份额“拼凑”起来可以还原出完整秘密，且该子集的任意一个真子集都不满足这个性质。

我们自然地对确定秘密共享方案的极小访问集十分感兴趣。在 Massey 的框架中，与极小访问集对应的是极小码字的概念：

定义 3.11 (极小码字)： 定义 $\mathbb{F}_q^n$ 中向量 $\boldsymbol{c} = (c_0, \cdots, c_{n-1})$ 的支撑集为

$$\{0 \leqslant i \leqslant n-1 : \ c_i \neq 0\}. \tag{3-93}$$

称向量 $\boldsymbol{c}_2$ 覆盖向量 $\boldsymbol{c}_1$，如果 $\boldsymbol{c}_2$ 的支撑集包含 $\boldsymbol{c}_1$ 的支撑集。

设 $\boldsymbol{c}$ 为线性码 C 中的一个非零码字。如果 C 中所有被 $\boldsymbol{c}$ 覆盖的码字均为 $\boldsymbol{c}$ 的倍数，则称 $\boldsymbol{c}$ 为 C 的一个极小码字。

由引理3.3，我们不难看出，由线性码 C 构造的秘密共享方案的极小访问集，与 C 的对偶码 $C^{\perp}$ 中第一个分量为 1 的极小码字之间有一个一一对应。为此，在 Massey 的框架中，确定秘密共享方案的极小访问集的问题就转换为确定相应对偶码的极小码字的问题，即所谓覆盖问题。

码字是否为极小码字，与码字的汉明重量有如下的关系：

引理 3.4 ([57], 引理 2.1)： 设 C 为一个 $[n,k,d]_q$ 线性码。C 中汉明重量大于 $n-k+1$

的码字必不为极小码字，而汉明重量小等于 $(qd-q+1)/(q-1)$ 的码字必为极小码字。

下面的定理告诉我们，如果线性码 C 的所有非零码字都是极小码字，则由其对偶码 $C^{\perp}$ 构造的秘密共享方案具有有趣的存取结构。

定理 3.8 ([10]，定理 17)： 设 C 为一个 $[n,k,d]_q$ 线性码，$G=[\boldsymbol{g}_0,\boldsymbol{g}_1,\cdots,\boldsymbol{g}_{n-1}]$ 为 C 的一个生成矩阵，$d^{\perp}$ 为 C 的对偶码 $C^{\perp}$ 的最小距离。若 C 的所有非零码字都是极小码字，则在由线性码 $C^{\perp}$ 构造的秘密共享方案中，一共有 q^{k-1} 个极小访问集。

(1) 若 $d^{\perp}=2$，则由 $C^{\perp}$ 构造的秘密共享方案的极小访问集可以描述如下：若 $\boldsymbol{g}_i$ 是 $\boldsymbol{g}_0$ 的一个倍数（$1\leqslant i\leqslant n-1$），则保管者 P_i 在任何一个极小访问集中（这样的保管者被称为“独裁者”）；若 $\boldsymbol{g}_i$ 不是 $\boldsymbol{g}_0$ 的一个倍数（$1\leqslant i\leqslant n-1$），则保管者 P_i 恰好在 $(q-1)q^{k-2}$ 个极小访问集中。

(2) 若 $d^{\perp}\geqslant 3$，则对任意的

$$1\leqslant t\leqslant \min\{k-1,d^{\perp}-2\}, \tag{3-94}$$

任何 t 名保管者都恰好同在 $(q-1)^t q^{k-t-1}$ 个极小访问集中。特别地，所有的保管者都在相同个数的极小访问集中（这样的秘密共享方案被称为“民主”的）。

3.8　C_{Π} 与 $\overline{C_{\Pi}}$ 的覆盖问题

有了 C_{Π} 和 $\overline{C_{\Pi}}$ 的重量分布，我们可以在一定程度上解决它们的覆盖问题。

定理 3.9： 设 $\Pi:\mathbb{F}_q\to\mathbb{F}_q$ 为一个 PN 函数，使得 $\Pi(0)=0$，且对任意的 $c\in\mathbb{F}_p\setminus\{0,1\}$ 及 $x\in\mathbb{F}_q^*$，有 $\Pi(cx)\neq c\Pi(x)$。假设 m 为奇数，或 m 为偶数且下面两个条件之一成立：

(a) $p=3$；

(b) $|\Pi^{-1}(0)|=1$，Π 是一个弱正则 PN 函数，且函数 $\mathbb{F}_q^*\to\mathbb{F}_p,\ a\mapsto \Pi_a^*(0)$ 不为满射，其中 $\Pi_a=f_{a,0,0}$，Π_a^* 为 Π_a 的对偶，

则 C_{Π} 中极小码字的情况如下：

(1) 若 $m\geqslant 3$，则 C_{Π} 中的所有非零码字均为极小码字；

(2) 若 $m=2$ 且 $p=3$，则 C_{Π} 中汉明重量为 4 或 5 的码字为极小码字，而其余码字均不为极小码字；

(3) 若 $m=2$ 且 $p>3$，则 C_{Π} 中汉明重量为 p^2-2p+1 或 p^2-p-1 的码字为极小码字，而汉明重量为 p^2-1 的码字不为极小码字。（汉明重量为 p^2-p 或 p^2-p+1 的码字是否为极小码字无法确定）

证明： 当 m 为奇数时，由定理3.7，C_{Π} 中非零码字的汉明重量只可能是 $(p-1)p^{m-1}$，$(p-1)p^{m-1}+p^{\frac{m-1}{2}}$，$(p-1)p^{m-1}-p^{\frac{m-1}{2}}$ 中的一个。特别地，C_{Π} 的最小距离为 $d=(p-1)p^{m-1}-p^{\frac{m-1}{2}}$。此时，我们有

$$\frac{pd-p+1}{p-1}=\frac{p^{m+1}-p^m-p^{\frac{m+1}{2}}-p+1}{p-1}. \tag{3-95}$$

不难证明当 $m\geqslant 3$ 时，有

$$(p-1)p^{m-1}+p^{\frac{m-1}{2}}\leqslant\frac{pd-p+1}{p-1}. \tag{3-96}$$

由引理3.4，C_{Π} 中的所有非零码字均为极小码字。

当 m 为偶数时，由定理3.7，C_{Π} 中非零码字的汉明重量只可能是 $(p-1)(p^{m-1}-p^{\frac{m}{2}-1})$，$(p-1)p^{m-1}-p^{\frac{m}{2}-1}$，$(p-1)p^{m-1}$，$(p-1)p^{m-1}+p^{\frac{m}{2}-1}$，$(p-1)(p^{m-1}+p^{\frac{m}{2}-1})$ 中的一个。特别地，C_{Π} 的最小距离为 $d=(p-1)(p^{m-1}-p^{\frac{m}{2}-1})$。此时，我们有

$$\frac{pd-p+1}{p-1}=p^m-p^{\frac{m}{2}}-1. \tag{3-97}$$

不难证明当 $m\geqslant 4$ 时，有

$$(p-1)(p^{m-1}+p^{\frac{m}{2}-1})\leqslant\frac{pd-p+1}{p-1}. \tag{3-98}$$

由引理3.4，C_{Π} 中的所有非零码字均为极小码字。

当 $m=2$ 且 $p=3$ 时，则 C_{Π} 中非零码字的汉明重量只可能是 4，5，6，7，8 中的一个。特别地，C_{Π} 的最小距离为 $d=4$。由命题3.6，C_{Π} 为一个 $[n,k,d]_p=[8,4,4]_3$ 线性码，因此我们有

$$\frac{pd-p+1}{p-1}=5,\qquad n-k+1=5. \tag{3-99}$$

由引理3.4，C_{Π} 中汉明重量为 4 或 5 的码字为极小码字，而其余码字均不为极小码字。

若 $m=2$ 且 $p>3$ 时，则 C_{Π} 中非零码字的汉明重量只可能是 p^2-2p+1，p^2-p-1，p^2-p，p^2-p+1，p^2-1 中的一个。特别地，C_{Π} 的最小距离为 $d=p^2-2p+1$。此时，由命题3.6，我们有

$$\frac{pd-p+1}{p-1}=p^2-p-1,\qquad n-k+1=p^2-4. \tag{3-100}$$

由引理3.4，C_{Π} 中汉明重量为 p^2-2p+1 或 p^2-p-1 的码字为极小码字，而汉明重量为 p^2-1 的码字不为极小码字。 ∎

下面这个定理的证明与定理3.9的几乎相同，故略去。

定理 3.10： 设 $\Pi:\mathbb{F}_q\to\mathbb{F}_q$ 为一个 PN 函数。假设 m 为奇数，或 m 为偶数且下面两个条件之一成立：

(a) $p=3$；

(b) $|\Pi^{-1}(0)|=1$，Π 是一个弱正则 PN 函数，且函数 $\mathbb{F}_q^* \to \mathbb{F}_p, a \mapsto \Pi_a^*(0)$ 不为满射，其中 $\Pi_a = f_{a,0,0}$，Π_a^* 为 Π_a 的对偶，

则 $\overline{C_\Pi}$ 中极小码字的情况如下：

(1) 若 $m \geqslant 3$，则 $\overline{C_\Pi}$ 中的所有非零码字除了汉明重量为 p^m 的，均为极小码字；

(2) 若 $m=2$ 且 $p=3$，则 $\overline{C_\Pi}$ 中汉明重量为 4 或 5 的码字为极小码字，而其余码字均不为极小码字；

(3) 若 $m=2$ 且 $p>3$，则 $\overline{C_\Pi}$ 中汉明重量为 p^2-2p+1 或 p^2-p-1 的码字为极小码字，而汉明重量为 p^2-1 的码字不为极小码字。（汉明重量为 p^2-p 或 p^2-p+1 的码字是否为极小码字无法确定）

第 4 章　循环外差族与强循环外差族

4.1　差集、差族与外差族

差集是组合设计理论中的一个基本概念，本节我们介绍差集及其两个变形：差族和外差族。

定义 4.1 (差集)： 设 $(G,\cdot)$ 为一个含有 n 个元素的有限群。对于 G 的子集 A，B，定义 $\Delta(A,B)$ 为下列多重集：

$$\{\{ab^{-1}\ :\ a\in A,\ b\in B\}\}. \tag{4-1}$$

称 G 中的非空子集 D 为 G 中的一个 $(n,l;\lambda)$-差集（difference set，简称 DS），如果 $|D|=l$，且任意元素 $g\in G\setminus\{1_G\}$ 在 $\Delta(D,D)$ 中出现 λ 次。

注释 4.1： 多重集与集合的差别在于多重集中的元素要考虑重数。

注释 4.2： 显然，$(n,l;\lambda)$-差集存在的一个必要条件就是 $l(l-1)=\lambda(n-1)$。

设 G 为一个有限群，我们可以将任意元素取于 G 的多重集看作群环 $\mathbb{Z}[G]$ 中的一个元素。实际上，若 A 是一个元素取于 G 的多重集，那么我们可以将其等同于 $\mathbb{Z}[G]$ 中的元素 $\sum_{g\in G}n_g g$，其中对任意的 $g\in G$，n_g 是 g 在 A 中的重数。反之，一个系数均为非负整数的 $\mathbb{Z}[G]$ 中的元素对应一个元素取于 G 的多重集。之后，我们不再对这二者进行区分。

利用群环的语言，G 中的非空子集 D 为 G 中的一个 $(n,l;\lambda)$-差集当且仅当

$$DD^{(-1)}=l\cdot 1_G+\lambda(G-1_G)\in\mathbb{Z}[G], \tag{4-2}$$

其中 $D^{(-1)}=\{d^{-1}\ :\ d\in D\}$。

如果 G 是一个交换群，那么我们还可以用 G 的特征来刻画差集。在2.2节中我们看到，任意 G 的特征都可以延拓到 $\mathbb{Z}[G]$ 上，并且 $\mathbb{Z}[G]$ 中的元素可以用 G 的特征来区分。利用特征的语言，式（4-2）等价于

$$|\chi(D)|^2=\chi(D)\overline{\chi}(D)=\begin{cases}l^2, & \text{若 } \chi=1_{\widehat{G}},\\ l-\lambda, & \text{若 } \chi\in\widehat{G}\setminus\{1_{\widehat{G}}\}.\end{cases} \tag{4-3}$$

关于差集的基本性质，可以参见 [58]。

在过去的几十年中，有许多差集的变形和推广被提出。一个自然的将差集从单子集的情形推广到子集族情形的概念是差族。

定义 4.2 (差族)： 设 $(G,\cdot)$ 为一个含有 n 个元素的有限群。称 G 的一个子集族 $\{A_1,\cdots,A_m\}$ 为 G 中的一个 $(n,m,l;\lambda)$-差族（difference family，简称 DF），如果

(1) 对任意的 $1 \leqslant i \leqslant m$，$|A_i| = l$；

(2) 任意元素 $g \in G \setminus \{1_G\}$ 在 $\bigcup_{i=1}^{m} \Delta(A_i, A_i)$ 中出现 λ 次。

与差集的情形类似，利用群环的语言，一个两两不相交的子集族 $\{A_1, \cdots, A_m\}$ 为 G 中的一个 $(n, m, l; \lambda)$-差族，当且仅当对任意的 $1 \leqslant i \leqslant m$，有 $|A_i| = l$，且

$$\sum_{j=1}^{m} A_j A_j^{(-1)} = ml \cdot 1_G + \lambda(G - 1_G) \in \mathbb{Z}[G]. \tag{4-4}$$

一些差族的变形与推广是为了满足密码学和信息安全领域的需求而提出的。1971 年，Levenshtein 提出外差族的概念[35]，它可以用于构造安全同步通信中的最优无逗点码。后来，Ogata 等人又发现外差族与强外差族可以用于构造安全校验码以及秘密共享方案[36]。外差族与强外差族的定义如下：

定义 4.3 (外差族，强外差族)： 设 $(G, \cdot)$ 为一个含有 n 个元素的有限群。称 G 的一个两两不相交的子集族 $\{A_1, \cdots, A_m\}$ 为 G 中的一个 $(n, m, l; \lambda)$-外差族（external difference family，简称 EDF），如果

(1) 对任意的 $1 \leqslant i \leqslant m$，$|A_i| = l$；

(2) 任意元素 $g \in G \setminus \{1_G\}$ 在 $\bigcup_{1 \leqslant i \neq j \leqslant m} \Delta(A_i, A_j)$ 中出现 λ 次，或者等价地，

$$\sum_{1 \leqslant i \neq j \leqslant m} A_i A_j^{(-1)} = \lambda(G - 1_G) \in \mathbb{Z}[G]. \tag{4-5}$$

称 G 的一个两两不相交的子集族 $\{A_1, \cdots, A_m\}$ 为 G 中的一个 $(n, m, l; \lambda)$-强外差族（strong external difference family，简称 SEDF），如果

(1) 对任意的 $1 \leqslant i \leqslant m$，$|A_i| = l$；

(2) 任取 $1 \leqslant i \leqslant m$，任意元素 $g \in G \setminus \{1_G\}$ 在 $\bigcup_{1 \leqslant j \leqslant m, j \neq i} \Delta(A_i, A_j)$ 中出现 λ 次，或者等价地，

$$\sum_{\substack{1 \leqslant j \leqslant m \\ j \neq i}} A_i A_j^{(-1)} = \lambda(G - 1_G) \in \mathbb{Z}[G]. \tag{4-6}$$

注释 4.3： 与外差族相比，定义4.2中的差族可以被称为“内”差族。

关于外差族与强外差族的构造与不存在性，已经有很多研究，可以参见 [59]。

4.2　循环外差族的构造

在1.3节中，我们提到，为了构造弱循环 AMD 码，Veitch 和 Stinson 提出了循环外差族的概念。在这里我们正式给出循环外差族的定义。

定义 4.4 (循环外差族，[34]，定义 4.2，定义 4.5)： 设 $(G, \cdot)$ 为一个含有 n 个元素的有限群，l 和 m 为 $\geqslant 2$ 的整数，S 为 $\{1, \cdots, m-1\}$ 的一个非空子集。称 G 的一个两

两不相交的子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 G 中的一个 $(n,m,l;\lambda)$-S-循环外差族（circular external difference family，简称 CEDF），如果

(1) 对任意的 $0\leqslant i\leqslant m-1$，$|A_i|=l$；

(2) 任意元素 $g\in G\setminus\{1_G\}$ 在 $\bigcup_{c\in S}\bigcup_{i=0}^{m-1}\Delta(A_{i+c},A_i)$ 中出现 λ 次，或者等价地，

$$\sum_{c\in S}\sum_{i=0}^{m-1}A_{i+c}A_i^{(-1)}=\lambda(G-1_G)\in\mathbb{Z}[G],\tag{4-7}$$

其中子集族下标的加法是模 m 的。

显然，$(n,m,l;\lambda)$-S-循环外差族存在的一个必要条件就是 $|S|\cdot ml^2=\lambda(n-1)$。如果 $S=\{c\}$，其中 $c\in\{1,\cdots,m-1\}$，那么 $(n,m,l;\lambda)$-S-循环外差族也称为 $(n,m,l;\lambda)$-c-循环外差族。

构造（内）差族与外差族最基本的方法，就是利用有限域中的分圆类。因此，我们自然地会考虑循环外差族的分圆构造。实际上，在 [34] 中，Veitch 和 Stinson 就给出了如下的分圆构造：

定理 4.1 ([34]，定理 4.3)： 设 q 为一个素数方幂，$q-1=ml^2$，其中 m 和 l 为 $\geqslant 2$ 的整数。令 θ 为一个 $\mathbb{F}_q$ 中的本原元，$\beta=\theta^l$，$C=\langle\beta^m\rangle=\left\langle\theta^{ml}\right\rangle$，以及 $C_i=\theta^iC$（$0\leqslant i\leqslant ml-1$）为 $\mathbb{F}_q$ 中所有的 ml 阶分圆类（相对于 θ）。

对任意的 $0\leqslant j\leqslant m-1$，令 $A_j=\beta^jC(=C_{jl})$，则子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,l;1)$-1-循环外差族，当且仅当

$$\{\beta^{1+km}-1:\ 0\leqslant k\leqslant l-1\}\tag{4-8}$$

为子群 $H=\langle\beta\rangle$ 在 $\mathbb{F}_q^*$ 中的一个完备陪集代表元集。若 $l=2$（从而 $q=4m+1$，$\beta=\theta^2$），则子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,2;1)$-1-循环外差族，当且仅当 θ^4-1 是 $\mathbb{F}_q^*$ 中的非平方元。

注释 4.4： 在 [34] 的注记 4.1 中，作者提到对于 $q>7.867\times10^8$，$\mathbb{F}_q$ 中存在一个本原元 θ，使得 θ^4-1 是 $\mathbb{F}_q^*$ 中的非平方元。之后，在 [38] 的定理 2.28 中，作者提到他们用计算机检验了所有满足 $13\leqslant q<10^9$ 且模 4 余 1 的素数 q，发现 $\mathbb{F}_q$ 中总存在一个本原元 θ，使得 θ^4-1 是 $\mathbb{F}_q^*$ 中的非平方元。我们使用著名的程序包 SageMath 对这个范围内模 4 余 1 的素数方幂进行了检验，发现只有 $q=25$ 是一个反例。

如果我们允许 c 变动，而不是固定为 1，那么很容易可以证明对任意的素数方幂 $q=4m+1\geqslant 13$，$(\mathbb{F}_q,+)$ 中存在一个 $(q,m,2;1)$-c-循环外差族，其中 $c\in\{1,\cdots,m-1\}$。

定理 4.2： 保持定理4.1中的记号。对任意的 $c\in\{1,\cdots,m-1\}$，子集族 $\{A_0,\cdots,A_{m-1}\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,l;1)$-c-循环外差族，当且仅当

$$\{x-1:\ x\in A_c\}=\{\beta^{c+km}-1:\ 0\leqslant k\leqslant l-1\}\tag{4-9}$$

为子群 $H=\langle\beta\rangle$ 在 $\mathbb{F}_q^*$ 中的一个完备陪集代表元集。

若 $l=2$（从而 $q=4m+1$，$\beta=\theta^2$），则对任意的 $c\in\{1,\cdots,m-1\}$，子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,2;1)$-c-循环外差族，当且仅当 $\theta^{4c}-1$ 是 $\mathbb{F}_q^*$ 中的非平方元。

证明： 该定理的证明与定理4.1的类似。注意到 β（相应地，β^m）在 $\mathbb{F}_q^*$ 中的阶为 ml（相应地，l），且任意 $\{0,1,\cdots,ml-1\}$ 中的整数 s 都可以唯一地表示为 $s=j+mt$，其中 t 和 j 为整数，满足 $0\leqslant t\leqslant l-1$，$0\leqslant j\leqslant m-1$。因此

$$\begin{aligned}
\bigcup_{j=0}^{m-1}\Delta(A_{j+c},A_j)&=\bigcup_{j=0}^{m-1}\Delta(\beta^{j+c}C,\beta^jC)\\
&=\bigcup_{j=0}^{m-1}\{\{\beta^{j+c}\cdot\beta^{mn_1}-\beta^j\cdot\beta^{mn_2}:\ 0\leqslant n_1,n_2\leqslant l-1\}\}\\
&=\bigcup_{j=0}^{m-1}\{\{\beta^j\cdot(\beta^m)^{n_2}\cdot\left(\beta^c\cdot(\beta^m)^{n_1-n_2}-1\right):\ 0\leqslant n_1,n_2\leqslant l-1\}\}\\
&=\bigcup_{j=0}^{m-1}\{\{\beta^j\cdot(\beta^m)^t\cdot\left(\beta^c\cdot(\beta^m)^k-1\right):\ 0\leqslant k,t\leqslant l-1\}\}\qquad(4\text{-}10)\\
&=\{\{\beta^{j+mt}(\beta^{c+mk}-1):\ 0\leqslant k,t\leqslant l-1,\ 0\leqslant j\leqslant m-1\}\}\\
&=\bigcup_{k=0}^{l-1}(\beta^{c+mk}-1)\cdot\{\beta^s:\ 0\leqslant s\leqslant ml-1\}\\
&=\bigcup_{k=0}^{l-1}(\beta^{c+mk}-1)H.
\end{aligned}$$

所以，子集族 $\{A_0,\cdots,A_{m-1}\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,l;1)$-c-循环外差族，即

$$\sum_{j=0}^{m-1}A_{j+c}A_j^{(-1)}=\mathbb{F}_q^*,\qquad(4\text{-}11)$$

当且仅当

$$\{\beta^{c+km}-1:\ 0\leqslant k\leqslant l-1\}\qquad(4\text{-}12)$$

为子群 $H=\langle\beta\rangle$ 在 $\mathbb{F}_q^*$ 中的一个完备陪集代表元集。

特别地，当 $l=2$ 时，子集族 $\{A_0,\cdots,A_{m-1}\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,2;1)$-c-循环外差族，当且仅当

$$\{\beta^{c+km}-1:\ 0\leqslant k\leqslant 1\}=\{\beta^c-1,\beta^{c+m}-1\}\qquad(4\text{-}13)$$

为子群 $H=\langle\beta\rangle=\left\langle\theta^2\right\rangle$ 在 $\mathbb{F}_q^*$ 中的一个完备陪集代表元集。后者等价于在 β^c-1

和 $\beta^{c+m}-1$ 中，有一个为 $\mathbb{F}_q^*$ 中的非平方元，而另一个不是，而这又进一步等价于 β^c-1 和 $\beta^{c+m}-1$ 的乘积为 $\mathbb{F}_q^*$ 中的非平方元。由于 β 在 $\mathbb{F}_q^*$ 中的阶为 $2m$，我们有 $\beta^m=-1$，从而

$$(\beta^c-1)(\beta^{c+m}-1)=(\beta^c-1)(-\beta^c-1)=1-\beta^{2c}=1-\theta^{4c}. \tag{4-14}$$

由于 $q\equiv 1 \pmod 4$，所以 -1 为 $\mathbb{F}_q^*$ 中的平方元，因此 $1-\theta^{4c}$ 是 $\mathbb{F}_q^*$ 中的非平方元，当且仅当 $\theta^{4c}-1$ 是 $\mathbb{F}_q^*$ 中的非平方元。这就完成了定理中第二个断言的证明。 ∎

推论 4.1： 设 q 为一个素数方幂，使得 $q=4m+1\geqslant 13$，其中 m 为整数。令 θ，β，C_i（$0\leqslant i\leqslant 2m-1$）和 A_j（$0\leqslant j\leqslant m-1$）保持它们在定理4.1中的含义。于是存在 $c\in\{1,\cdots,m-1\}$，使得 $\{A_0,\cdots,A_{m-1}\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,2;1)$-c-循环外差族。

证明： 由定理4.2，只需证明存在 $c\in\{1,\cdots,m-1\}$，使得 $\theta^{4c}-1$ 是 $\mathbb{F}_q^*$ 中的非平方元。令 $\alpha=\theta^4$，以及 $E_i=\theta^i\langle\alpha\rangle$（$0\leqslant i\leqslant 3$）为 $\mathbb{F}_q$ 中的 4 阶分圆类（相对于 θ）。于是

$$\begin{aligned}
&\#\{c\in[m-1]:\ \theta^{4c}-1\text{ 为非平方元}\}\\
=&\#\{c\in[m-1]:\ \alpha^c-1\in E_1\cup E_3\}\\
=&\#\{x\in E_0:\ x-1\in E_1\cup E_3\}\\
=&(1,0)_4^{(q)}+(3,0)_4^{(q)}.
\end{aligned} \tag{4-15}$$

设 $q=p^n$，其中 p 为一个奇素数。若 $q\equiv 1 \pmod 8$，由定理2.10，存在整数 s，t 使得

$$\begin{aligned}
(1,0)_4^{(q)}+(3,0)_4^{(q)}&=\frac{1}{16}(q-3+2s+8t)+\frac{1}{16}(q-3+2s-8t)\\
&=\frac{1}{8}(q-3+2s).
\end{aligned} \tag{4-16}$$

如果 $q\equiv 5 \pmod 8$，则存在整数 s，使得

$$\begin{aligned}
(1,0)_4^{(q)}+(3,0)_4^{(q)}&=\frac{1}{16}(q-3-2s)+\frac{1}{16}(q-3-2s)\\
&=\frac{1}{8}(q-3-2s).
\end{aligned} \tag{4-17}$$

不论是哪种情形，我们都有

$$(1,0)_4^{(q)}+(3,0)_4^{(q)}=\frac{1}{8}(q-3\pm 2s). \tag{4-18}$$

(1) 如果 $p\equiv 1 \pmod 4$，则上述的整数 s 和 t 满足 $q=s^2+4t^2$，$p\nmid st$（特别地，$t\neq 0$），以及 $s\equiv 1 \pmod 4$。于是

$$(1,0)_4^{(q)}+(3,0)_4^{(0)}=0\iff q-3\pm 2s=0$$

$$\begin{aligned}
&\iff (s\pm 1)^2+4t^4=4 && (4\text{-}19)\\
&\iff s\pm 1=0,\ t\in\{\pm 1\}\quad (\text{因为 } t\neq 0)\\
&\iff s=1,\ t\in\{\pm 1\}\quad (\text{因为 } s\equiv 1\ (\mathrm{mod}\ 4))\\
&\iff q=5,
\end{aligned}$$

这与 $q\geqslant 13$ 的假设矛盾。

(2) 如果 $p\equiv 3\ (\mathrm{mod}\ 4)$，则 $s\in\{\pm p^{n/2}\}$。于是

$$\begin{aligned}
(1,0)_4^{(q)}+(3,0)_4^{(0)}=0 &\iff q-3\pm 2s=0\\
&\iff (\sqrt{q}\pm 1)^2=4 && (4\text{-}20)\\
&\iff q=9,
\end{aligned}$$

这与 $q\geqslant 13$ 的假设矛盾。

因此，在所有的情形中，我们始终有 $(1,0)_4^{(q)}+(3,0)_4^{(q)}\geqslant 1$。定理得证。 ∎

定理4.2可以推广到一般非空子集 $S\subset\{1,\cdots,m-1\}$ 的情形。证明是类似的，因此我们在此略去。

定理 4.3： 保持定理4.1中的记号。对任意的非空子集 $S\subset\{1,\cdots,m-1\}$，子集族 $\{A_0,\cdots,A_{m-1}\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,l;|S|)$-S-循环外差族，当且仅当对任意 $H=\langle\beta\rangle$ 在 $\mathbb{F}_q^*$ 中的陪集，在

$$\bigcup_{c\in S}\{x-1:\ x\in A_c\}=\{\beta^{c+km}-1:\ 0\leqslant k\leqslant l-1,\ c\in S\} \qquad (4\text{-}21)$$

中恰有 $|S|$ 个元素属于该陪集。

表 4.1　余数 $2^i \bmod 37$（$0\leqslant i\leqslant 18$）

i	0	1	2	3	4	5	6	7	8	
$2^i \bmod 37$	1	2	4	8	16	32	27	17	34	
i	9	10	11	12	13	14	15	16	17	18
$2^i \bmod 37$	31	25	13	26	15	30	23	9	18	36 (= −1)

例 4.1： 取 $q=37$，$m=4$ 以及 $l=3$，则 $q=ml^2+1$。余数 $2^i \bmod 37$（$0\leqslant i\leqslant 18$）如表4.1所示，显然 $\theta=2$ 是 $\mathbb{F}_q$ 中的一个本原元。令 $\beta=\theta^3=8$，$H=\langle\beta\rangle=\langle 8\rangle$，$C=\langle\beta^m\rangle=\left\langle 2^{12}\right\rangle=\{1,2^{12},2^{24}\}=\{1,26,10\}$，以及 $A_j=\beta^j C$（$0\leqslant j\leqslant 3$）。于是

$$\begin{aligned}
A_0=\{1,26,10\},\quad A_1=\{8,23,6\},\\
A_2=\{27,36,11\},\quad A_3=\{31,29,14\}.
\end{aligned} \qquad (4\text{-}22)$$

令 $\chi:\mathbb{F}_q^*\to\mathbb{C}$ 为 $\mathbb{F}_q$ 上将 2 映射为 $\omega=\exp(2\pi\mathrm{i}/3)$ 的 3 阶乘法特征。任取 $x\in\mathbb{F}_q^*$，我们有

$$\chi(x)=\begin{cases}1, & x\in H=\{\pm1,\pm6,\pm8,\pm10,\pm11,\pm14\},\\ \omega, & x\in 2H=\{\pm2,\pm9,\pm12,\pm15,\pm16,\pm17\},\\ \omega^2, & x\in 4H=\{\pm3,\pm4,\pm5,\pm7,\pm13,\pm18\}.\end{cases}\tag{4-23}$$

由定理4.3，对任意的非空子集 $S\subset\{1,2,3\}$，子集族 $\{A_0,A_1,A_2,A_3\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(37,4,3;|S|)$-S-循环外差族，当且仅当对任意 $H=\langle\beta\rangle$ 在 $\mathbb{F}_q^*$ 中的陪集，在

$$\bigcup_{c\in S}\{x-1:\ x\in A_c\}=\{8^{c+km}-1:\ 0\leqslant k\leqslant 2,\ c\in S\}\tag{4-24}$$

恰有 $|S|$ 个元素属于该陪集。后者等价于多重集

$$\{\{\chi(x-1):\ x\in A_c,\ c\in S\}\}\tag{4-25}$$

是集合 $\{1,\omega,\omega^2\}$ 重复 $|S|$ 份所得。因为

$$\begin{aligned}\mathcal{A}_1&=\{\{\chi(x-1)|\ x\in A_1\}\}=\{\{\chi(7),\chi(22),\chi(5)\}\}=\{\{\omega^2,\omega,\omega^2\}\},\\ \mathcal{A}_2&=\{\{\chi(x-1)|\ x\in A_2\}\}=\{\{\chi(26),\chi(35),\chi(10)\}\}=\{\{1,\omega,1\}\},\\ \mathcal{A}_3&=\{\{\chi(x-1)|\ x\in A_3\}\}=\{\{\chi(30),\chi(28),\chi(13)\}\}=\{\{\omega^2,\omega,\omega^2\}\},\end{aligned}\tag{4-26}$$

所以对任意的 $c\in\{1,2,3\}$，子集族 $\{A_0,A_1,A_2,A_3\}$ 不为 $(\mathbb{F}_q,+)$ 中的一个 $(37,4,3;1)$-1-循环外差族。另一方面，因为

$$\mathcal{A}_1\cup\mathcal{A}_2=\mathcal{A}_2\cup\mathcal{A}_3=\{\{1,1,\omega,\omega,\omega^2,\omega^2\}\},\tag{4-27}$$

所以对于 $S=\{1,2\}$ 或 $\{2,3\}$，子集族 $\{A_0,A_1,A_2,A_3\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(37,4,3;2)$-S-循环外差族。[34] 中的例 4.7 正是 $S=\{1,2\}$ 的情形。

在上面的分圆构造中，$A_j=C_{jl}$（$0\leqslant j\leqslant m-1$）正是 $\mathbb{F}_q$ 的编号位于算术序列 0，l，$2l$，…，$(m-1)l$ 中的那 m 个 ml 阶分圆类。下面的定理告诉我们，当我们选取任意 m 个 $\mathbb{F}_q$ 的 ml 阶分圆类构成子集族时，该子集族何时为循环外差族。

定理 4.4： 设 q 为一个素数方幂，$q-1=ml^2$，其中 m 和 l 为 $\geqslant 2$ 的整数。令 θ 为一个 $\mathbb{F}_q$ 中的本原元，$\beta=\theta^l$，$C=\langle\beta^m\rangle=\left\langle\theta^{ml}\right\rangle$，以及 $C_i=\theta^iC$（$0\leqslant i\leqslant ml-1$）为 $\mathbb{F}_q$ 中所有的 ml 阶分圆类（相对于 θ）。

设 $\sigma:\mathbb{Z}_m\to\mathbb{Z}_{ml}$ 为一个单射。对任意的 $0\leqslant j\leqslant m-1$，令 $D_j=\theta^{\sigma(j)}C=C_{\sigma(j)}$。于是对任意非空子集 $S\subset\{1,\cdots,m-1\}$，子集族 $\{D_0,\cdots,D_{m-1}\}$ 是 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,l;|S|)$-S-循环外差族，当且仅当对任意 C 在 $\mathbb{F}_q^*$ 中的陪集，在多重集

$$\{\{\theta^{\sigma(j+c)}-\theta^{\sigma(j)}\beta^{mr}:\ 0\leqslant j\leqslant l-1,\ 0\leqslant r\leqslant m-1,\ c\in S\}\}\tag{4-28}$$

中恰有 $|S|$ 个元素属于该陪集。

证明： 因为 $\sigma : \mathbb{Z}_m \to \mathbb{Z}_{ml}$ 为单射, 所以 $D_j = \theta^{\sigma(j)}C$ $(0 \leqslant j \leqslant m-1)$ 两两不同。我们有

$$\begin{aligned}
\bigcup_{c\in S}\bigcup_{j=0}^{m-1}\Delta(D_{j+c}, D_j) &= \bigcup_{c\in S}\bigcup_{j=0}^{m-1}\Delta(C_{\sigma(j+c)}, D_{\sigma(j)}) \\
&= \bigcup_{c\in S}\bigcup_{j=0}^{m-1}\{\{\theta^{\sigma(j+c)}x - \theta^{\sigma(j)}y : x, y \in C\}\} \\
&= \bigcup_{c\in S}\bigcup_{j=0}^{m-1}\{\{(\theta^{\sigma(j+c)} - \theta^{\sigma(j)}yx^{-1})x : x, y \in C\}\} \qquad (4\text{-}29) \\
&= \bigcup_{c\in S}\bigcup_{j=0}^{m-1}\{\{(\theta^{\sigma(j+c)} - \theta^{\sigma(j)}z)x : x, z \in C\}\} \\
&= \bigcup_{c\in S}\bigcup_{j=0}^{m-1}\{\{\theta^{\sigma(j+c)} - \theta^{\sigma(j)}z : z \in C\}\} \cdot C \\
&= \bigcup_{c\in S}\bigcup_{j=0}^{m-1}\{\{\theta^{\sigma(j+c)} - \theta^{\sigma(j)}\beta^{mr} : 0 \leqslant r \leqslant l-1\}\} \cdot C.
\end{aligned}$$

所以子集族 $\{D_0, \cdots, D_{m-1}\}$ 为 $(\mathbb{F}_q, +)$ 中的一个 $(q, m, l; |S|)$-S-循环外差族，即

$$\sum_{c\in S}\sum_{j=0}^{m-1} D_{j+c}D_j^{(-1)} = |S| \cdot \mathbb{F}_q^*, \qquad (4\text{-}30)$$

当且仅当对任意 C 在 $\mathbb{F}_q^*$ 中的陪集，在多重集

$$\{\{\theta^{\sigma(j+c)} - \theta^{\sigma(j)}\beta^{mr} : 0 \leqslant j \leqslant l-1,\ 0 \leqslant r \leqslant m-1,\ c \in S\}\} \qquad (4\text{-}31)$$

中恰有 $|S|$ 个元素属于该陪集。 ∎

表 4.2　余数 $2^i \bmod 19$（$0 \leqslant i \leqslant 9$）

i	0	1	2	3	4	5	6	7	8	9
$2^i \bmod 19$	1	2	4	8	16	13	7	14	9	18 (= −1)

例 4.2： 取 $q = 19$，$m = 2$ 以及 $l = 3$，则 $q = ml^2 + 1$。余数 $2^i \bmod 19$（$0 \leqslant i \leqslant 9$）如表4.2所示，显然 $\theta = 2$ 是 $\mathbb{F}_q$ 中的一个本原元。令 $\beta = \theta^3 = 8$，$H = \langle\beta\rangle = \langle 8\rangle$，$C = \langle\beta^m\rangle = \langle 2^6\rangle = \{1, 2^6, 2^{12}\} = \{1, 7, 11\}$，$C_i = \theta^i C$（$0 \leqslant i \leqslant 5$），以及 $A_j = \beta^j C$（$0 \leqslant j \leqslant 1$）。于是

$$A_0 = \{1, 7, 11\}, \quad C_1 = \{2, 14, 3\}, \quad A_1 = \{8, 18, 12\}, \qquad (4\text{-}32)$$

且

$$\begin{aligned}\Delta(A_0,A_1)&=\{x-y:\ x\in\{1,7,11\},\ y\in\{8,18,12\}\}\\&=\{2,3,8,8,12,12,14,18,18\},\\\Delta(A_1,A_0)&=-\Delta(A_0,A_1)=\{17,16,11,11,7,7,5,1,1\}.\end{aligned}\tag{4-33}$$

因为 $\Delta(A_0,A_1)\cup\Delta(A_1,A_0)\neq\mathbb{F}_{19}^*$，所以子集族 $\{A_0,A_1\}$ 不为 $(\mathbb{F}_{19},+)$ 中的一个 $(19,2,3;1)$-1-循环外差族。

另一方面，如果我们取 $D_0=C=\{1,7,11\}$，$D_1=C_1=\{2,14,3\}$，则

$$\begin{aligned}\Delta(D_0,D_1)&=\{x-y:\ x\in\{1,7,11\},\ y\in\{2,14,3\}\}\\&=\{4,5,6,8,9,12,16,17,18\},\\\Delta(D_1,D_0)&=-\Delta(D_0,D_1)=\{15,14,13,11,10,7,3,2,1\}.\end{aligned}\tag{4-34}$$

因为 $\Delta(D_0,D_1)\cup\Delta(D_1,D_0)=\mathbb{F}_{19}^*$，所以子集族 $\{D_0,D_1\}$ 是 $(\mathbb{F}_{19},+)$ 中的一个 $(19,2,3;1)$-1-循环外差族。

我们以一个循环外差族的提升定理结束本节。

定理 4.5： 设 q 为一个素数方幂，$q-1=ml^2$，其中 m 和 l 为 $\geqslant 2$ 的整数。令 θ 为一个 $\mathbb{F}_q$ 中的本原元，$\beta=\theta^l$，$H=\langle\beta\rangle$，$C=\langle\beta^m\rangle=\left\langle\theta^{ml}\right\rangle$，以及 $A_j=\beta^jC$（$0\leqslant j\leqslant m-1$）。

设 $Q=q^t$，其中 t 为正整数，$M=(Q-1)/l^2$。令 $\tilde{\theta}$ 为 $\mathbb{F}_Q$ 中的一个本原元，满足 $\theta=\tilde{\theta}^{(Q-1)/(q-1)}=\tilde{\theta}^{M/m}$，$\tilde{\beta}=\tilde{\theta}^l$，$\widetilde{H}=\left\langle\tilde{\beta}\right\rangle$，$\widetilde{C}=\left\langle\tilde{\beta}^M\right\rangle$，以及 $\widetilde{A}_k=\tilde{\beta}^k\widetilde{C}$（$0\leqslant k\leqslant M-1$）。

假设 $\gcd(l,t)=1$，则对任意的非空子集 $S\subset\{1,\cdots,m-1\}$，子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 $(\mathbb{F}_q,+)$ 中的一个 $(q,m,l;|S|)$-S-循环外差族，当且仅当子集族 $\{\widetilde{A}_0,\cdots,\widetilde{A}_{M-1}\}$ 为 $(\mathbb{F}_Q,+)$ 中的一个 $(Q,M,l;|\widetilde{S}|=|S|)$-$\widetilde{S}$-循环外差族，其中

$$\widetilde{S}=\frac{M}{m}S=\{\frac{M}{m}c:\ c\in S\}\subset\{1,\cdots,M-1\}.\tag{4-35}$$

证明： 令

$$B=\{\beta^{c+km}-1:\ 0\leqslant k\leqslant l-1,\ c\in S\}\tag{4-36}$$

以及

$$\widetilde{B}=\{\tilde{\beta}^{c+kM}-1:\ 0\leqslant k\leqslant l-1,\ \tilde{c}\in\widetilde{S}\}.\tag{4-37}$$

由定理4.3, 子集族 $\{A_0,\cdots,A_{m-1}\}$（相应地，$\{\widetilde{A}_0,\cdots,\widetilde{A}_{m-1}\}$）是 $(\mathbb{F}_q,+)$（相应地，$(\mathbb{F}_Q,+)$）中的一个 $(q,m,l;|S|)$-S-循环外差族（相应地，$(Q,M,l;|\widetilde{S}|)$-$\widetilde{S}$-循环外差族），当且仅当对任意 H（相应地，$\widetilde{H}$）在 $\mathbb{F}_q^*$（相应地，$\mathbb{F}_Q^*$）中的陪集，在 B（相

应地，$\widetilde{B}$）中恰有 $|S| = |\widetilde{S}|$ 个元素属于该陪集。因为

$$\begin{aligned} B &= \{\beta^{c+km} - 1 : \ 0 \leqslant k \leqslant l-1, \ c \in S\} \\ &= \{\tilde{\beta}^{\frac{M}{m}(c+km)} - 1 : \ 0 \leqslant k \leqslant l-1, \ c \in S\} \\ &= \{\tilde{\beta}^{\frac{M}{m}c+kM} - 1 : \ 0 \leqslant k \leqslant l-1, \ c \in S\} \\ &= \{\tilde{\beta}^{\tilde{c}+kM} - 1 : \ 0 \leqslant k \leqslant l-1, \ \tilde{c} \in \widetilde{S}\} = \widetilde{B}, \end{aligned} \tag{4-38}$$

我们只需证明自然嵌入 $\mathbb{F}_q^* \to \mathbb{F}_Q^*$ 诱导一个群同构 $\mathbb{F}_q^*/H \xrightarrow{\cong} \mathbb{F}_Q^*/\widetilde{H}$。因为 $\mathbb{F}_q^*/H$ 和 $\mathbb{F}_Q^*/\widetilde{H}$ 均是阶为 l 的循环群，且 θ 在 $\mathbb{F}_q^*/H$ 中的像是 $\mathbb{F}_q^*/H$ 的一个生成元，我们只需证明 θ（的像）在 $\mathbb{F}_Q^*/\widetilde{H}$ 中的阶为 l。因为 $\theta = \tilde{\theta}^{M/m}$ 且 $\tilde{\theta}$ 在 $\mathbb{F}_Q^*/\widetilde{H}$ 中的阶为 l，所以 θ 在 $\mathbb{F}_Q^*/\widetilde{H}$ 中的阶为 $l/\gcd(l, M/m)$，从而只需证明 $\gcd(l, M/m) = 1$。实际上，因为 $l \mid (q-1)$，即 $q \equiv 1 \pmod{l}$，我们有

$$\begin{aligned} \gcd(l, \frac{M}{m}) &= \gcd(l, \frac{Q-1}{q-1}) \\ &= \gcd(l, q^{t-1} + q^{t-2} + \cdots + q + 1) = \gcd(l, t) = 1. \end{aligned} \tag{4-39}$$

这就完成了定理的证明。 ∎

4.3　强循环外差族的构造与不存在性

R-最优弱循环 AMD 码与循环外差族等价，而 R-最优强循环 AMD 码与强循环外差族等价。下面是强循环外差族的定义。

定义 4.5 (强循环外差族，[34]，定义 4.7)： 设 $(G, \cdot)$ 为一个含有 n 个元素的有限群，l 和 m 为 $\geqslant 2$ 的整数，$c \in \{1, \cdots, m-1\}$。称 G 的一个两两不相交的子集族 $\{A_0, \cdots, A_{m-1}\}$ 为 G 中一个的 $(n, m, l; \lambda)$-强 c-循环外差族（strong circular external difference family，简称 SCEDF），如果

(1) 对任意的 $0 \leqslant i \leqslant m-1$，$|A_i| = l$；

(2) 任取 $0 \leqslant i \leqslant m-1$，任意元素 $g \in G \setminus \{1_G\}$ 在 $\Delta(A_{i+c}, A_i)$ 中出现 λ 次，或者等价地，

$$A_{i+c} A_i^{(-1)} = \lambda(G - 1_G) \in \mathbb{Z}[G], \tag{4-40}$$

其中子集族下标的加法是模 m 的。

显然，$(n, m, l; \lambda)$-强 c-循环外差族存在的一个必要条件就是 $l^2 = \lambda(n-1)$。

在 [34] 中，Veitch 和 Stinson 提到强循环外差族似乎是很难构造的，因此他们在文章末提的问题中的第一个就是是否存在非平凡的强循环外差族。在本节中，我们将证明不存在非平凡的强循环外差族。为此，我们首先定义何为“平凡”的强循

环外差族。简单来说，平凡的强循环外差族就是那些用若干 $(n,2,l;\lambda)$-强外差族拼起来得到的强循环外差族。

由定义4.3和定义4.5，$(n,2,l;\lambda)$-强 1-循环外差族就是 $(n,2,l;\lambda)$-强外差族。下面的两个引理告诉我们如何利用强外差族构造强循环外差族。

引理 4.1： 设 $(G,\cdot)$ 为一个含有 n 个元素的有限群，l 和 m 为 $\geqslant 2$ 的整数，$c\in\{1,\cdots,m-1\}$，$\{A_0,\cdots,A_{m-1}\}$ 为 G 的一个两两不相交的子集族，满足对任意的 $0\leqslant i\leqslant m-1$，$|A_i|=l$。

令 $t=\gcd(c,m)$，$c'=c/t$，$m'=m/t$，以及对任意的 $0\leqslant i\leqslant t-1$，令

$$\mathcal{D}^{(i)}=\{D_0^{(i)}=A_i,\ D_1^{(i)}=A_{i+t},\ \cdots,\ D_{m'-1}^{(i)}=A_{i+(m'-1)t}\},\tag{4-41}$$

则子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 G 中的一个 $(n,m,l;\lambda)$-强 c-循环外差族，当且仅当对任意的 $0\leqslant i\leqslant t-1$，子集族 $\mathcal{D}^{(i)}$ 为 G 中的一个 $(n,m',l;\lambda)$-强 c'-循环外差族。

证明： 因为任意的整数 $r\in\{0,\cdots,m-1\}$ 都可以唯一地表示为 $r=i+jt$，其中 i 和 j 为整数，满足 $0\leqslant i\leqslant t-1$，$0\leqslant j\leqslant m'-1$，所以子集族 $\{A_0,\cdots,A_{m-1}\}$ 是子集族 $\mathcal{D}^{(0)}$，$\cdots$，$\mathcal{D}^{(t)}$ 的无交并。此外，对任意的 $0\leqslant i\leqslant t-1$ 以及 $0\leqslant j\leqslant m'-1$，我们有

$$D_{j+m'}^{(i)}=A_{i+(j+m')t}=A_{i+jt+m}=A_{i+jt}=D_j^{(i)}\tag{4-42}$$

以及

$$\Delta(D_{j+c'}^{(i)},D_j^{(i)})=\Delta(A_{i+(j+c')t},A_{i+jt})=\Delta(A_{(i+jt)+c},A_{i+jt}).\tag{4-43}$$

由定义，引理得证。∎

引理 4.2： 设 $(G,\cdot)$ 为一个含有 n 个元素的有限群，l 和 m 为 $\geqslant 2$ 的整数，$c\in\{1,\cdots,m-1\}$ 满足 $\gcd(c,m)=1$，$\{A_0,\cdots,A_{m-1}\}$ 为 G 的一个两两不相交的子集族，满足对任意的 $0\leqslant i\leqslant m-1$，$|A_i|=l$。

对任意的 $0\leqslant i\leqslant m-1$，令 $D_i=A_{ic}$，则子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 G 中的一个 $(n,m,l;\lambda)$-强 c-循环外差族，当且仅当子集族 $\{D_0,\cdots,D_{m-1}\}$ 为 G 中的一个 $(n,m,l;\lambda)$-强 1-循环外差族。

证明： 因为 $\gcd(c,m)=1$，所以子集族 $\{D_0,\cdots,D_{m-1}\}$ 是子集族 $\{A_0,\cdots,A_{m-1}\}$ 的一个置换。此外，对任意的 $0\leqslant i\leqslant m-1$，我们有

$$D_{i+m}=A_{(i+m)c}=A_{ic+mc}=A_{ic}=D_i\tag{4-44}$$

以及

$$\Delta(D_{i+1},D_i)=\Delta(A_{(i+1)c},A_{ic})=\Delta(A_{ic+c},A_{ic}).\tag{4-45}$$

由定义，引理得证。 ∎

现令 $\mathcal{D}^{(i)}=\{D_0^{(i)},D_1^{(i)}\}$（$0\leqslant i\leqslant c-1$）为有限交换群 $(G,\cdot)$ 中 c 个两两不相交的 $(n,2,l;\lambda)$-强外差族。对任意的 $r\in\{0,\cdots,2c-1\}$，令 $A_r=D_j^{(i)}$，其中 i，j 为使得 $0\leqslant i\leqslant c-1$，$0\leqslant j\leqslant 1$ 且 $r=i+jc$ 的唯一确定的一对整数。由引理4.1，子集族 $\{A_0,\cdots,A_{2c-1}\}$ 是 G 中的一个 $(n,2c,l;\lambda)$-强 c-循环外差族。我们称通过这种方式构造的强循环外差族为平凡的强循环外差族。将上面的过程反过来，我们可以看到任何满足 $m=2c$ 的 (n,m,l,λ)-强 c-循环外差族都是平凡的。

定理 4.6： 设 $(G,\cdot)$ 为一个含有 n 个元素的有限群，l 和 m 为 $\geqslant 2$ 的整数。若子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 G 中的一个 $(n,m,l;\lambda)$-强 1-循环外差族，则必然有 $m=2$。

证明： 由定义，子集族 $\{A_0,\cdots,A_{m-1}\}$ 为 G 中的一个 $(n,m,l;\lambda)$-强 1-循环外差族，当且仅当对任意的 $0\leqslant i\leqslant m-1$，有

$$A_{i+1}A_1^{(-1)}=\lambda(G-1_G)\in\mathbb{Z}[G]. \tag{4-46}$$

于是，对任意的非平凡特征 $\chi\in\widehat{G}$ 以及任意的 $0\leqslant i\leqslant m-1$，我们有

$$\chi(A_{i+1})\overline{\chi(A_i)}=\chi(A_{i+1})\chi(A_i^{(-1)})=\lambda\cdot\chi(G)-\lambda\cdot\chi(1_G)=-\lambda\quad\in\mathbb{C}. \tag{4-47}$$

特别地，我们有

$$\chi(A_1)\overline{\chi(A_0)}=-\lambda=\chi(A_2)\overline{\chi(A_1)}. \tag{4-48}$$

因为 $\lambda\neq 0$，所以 $\chi(A_1)\neq 0$。因为 $\lambda\in\mathbb{R}$，所以有

$$\chi(A_0)\overline{\chi(A_1)}=\overline{\chi(A_1)\overline{\chi(A_0)}}=\overline{-\lambda}=-\lambda=\chi(A_2)\overline{\chi(A_1)}. \tag{4-49}$$

由于 $\chi(A_1)\neq 0$，所以 $\chi(A_0)=\chi(A_2)$。此外，我们有

$$1_{\widehat{G}}(A_0)=|A_0|=l=|A_2|=1_{\widehat{G}}(A_2). \tag{4-50}$$

由上面的论证可知，对任意的 $\chi\in\widehat{G}$，我们都有 $\chi(A_0)=\chi(A_2)$。由定理2.7，我们有 $A_0=A_2$，从而 $m=2$。 ∎

将上面的结果综合在一起，我们就可以证明不存在非平凡的强循环外差族。

推论 4.2： 不存在非平凡的强循环外差族。

证明： 假设子集族 $\{A_0,\cdots,A_{m-1}\}$ 是有限交换群 G 中的一个 $(n,m,l;\lambda)$-强 c-循环外差族，其中 $m\neq 2c$。由引理4.1，存在一个 G 中的 $(n,m',l;\lambda)$-强 c'-循环外差族，其中 $m'=m/t$，$c'=c/t$，且 $t=\gcd(c,m)$。由引理4.2，我们不妨假设 $c'=1$。因为 $c\in\{1,\cdots,m-1\}$ 且 $m\neq 2c$，我们必有 $t=\gcd(c,m)<m/2$，从而 $m'=m/t>2$。由定理4.6，这是不可能的。因此所有的强循环外差族都是平凡的。 ∎

所以，强循环外差族的研究，本质上就是 $(n,2,l;\lambda)$-强外差族的研究。在下一

节中，我们将证明一个新的关于此类强外差族的不存在性结果。

4.4　$m=2$ 的强外差族的构造与不存在性

下面的定理总结了目前已经构造出的参数 $m=2$ 的强外差族：

定理 4.7 ([60]，命题 1.1)： 下面这些参数的强外差族存在：

1. $(n,m,l;\lambda)=(k^2+1,2,k;1)$，构造于 $G=\mathbb{Z}_{k^2+1}$；
2. $(n,m,l;\lambda)=(v,2,\frac{v-1}{2};\frac{v-1}{4})$，其中 $v\equiv 1 \pmod 4$，假设有限交换群 G 中存在 $(v,\frac{v-1}{2},\frac{v-5}{4};\frac{v-1}{4})$-偏差集（partial difference set）；
3. $(n,m,l;\lambda)=(p,2,\frac{p-1}{4};\frac{p-1}{16})$，其中 $p=16t^2+1$ 为素数，t 为整数，构造于 $G=\mathbb{Z}_p$；
4. $(n,m,l;\lambda)=(p,2,\frac{p-1}{6};\frac{p-1}{36})$，其中 $p=108t^2+1$ 为素数，t 为整数，构造于 $G=\mathbb{Z}_p$。

注释 4.5： 由于偏差集与本文的核心内容无关，所以我们在此并不给出其定义，可以参见 [61-62]。

此外，还有下面这个关于参数 $m=2$ 的强外差族的不存在性的一般性结果：

定理 4.8 ([60]，定理 4.2)： 设 $(G,\cdot)$ 为一个含有 n 个元素的有限交换群，l 和 λ 为正整数，满足 $l\geqslant 2$，且 $l^2=\lambda(n-1)$。假设

(1) p 是 n 的一个素因子，q 是 λ 的一个素因子，使得 $d=\max\{i\in\mathbb{N}_+:\ p^i\mid n\}$ 以及 $f=\max\{j\in\mathbb{N}_+:\ q^j\mid\lambda\}$；

(2) q 模 p^d 本原，即 q（在 $\mathbb{Z}_{p^d}$ 中的像）是 $\mathbb{Z}_{p^d}^*$ 的一个生成元；

(3) $|G_p|>n/q^{\lceil f/2\rceil}$，其中 G_p 为 G 的 Sylow p-子群，即 G 中阶为 p 的方幂的最大循环群，

则 G 中不存在 $(n,2,l;\lambda)$-强外差族。

如果在定理4.8中有 $n=p$，则 $G=G_p$，从而 $|G_p|=p>n/q\geqslant n/q^{\lceil f/2\rceil}$，也就是说，定理4.8中的条件（3）满足。因此我们有如下的推论：

推论 4.3： 设 p 为一个素数，λ，l 为正整数，满足 $2\leqslant l\leqslant p/2$ 且 $\lambda(p-1)=l^2$。如果 λ 有一个素因子 q 是模 p 本原的，则不存在任何的 $(p,2,l;\lambda)$-强外差族。

注释 4.6： 设 p 和 q 为两个素数，满足 $p\geqslant 3$ 且 q 模 p 本原。我们希望确定所有正整数 λ，l，满足 $2\leqslant l\leqslant (p-1)/2$，$q\mid\lambda$ 且 $\lambda(p-1)=l^2$。首先，将 $p-1$ 分解为

$$p-1=q^c p_1^{2a_1}\cdots p_s^{2a_s}q_1^{2b_1-1}\cdots q_r^{2b_r-1},\tag{4-51}$$

其中 p_1，…，p_s，q_1，…，q_r 为两两不同且不同于 q 的素数，$c\in\mathbb{N}$，且 a_1，…，a_s，b_1，…，$b_r\in\mathbb{N}_+$。因为 $p\geqslant 3$，所以 $c+s+r\geqslant 1$。令

$$l_{\min}=q^{\lceil\frac{c+1}{2}\rceil}p_1^{a_1}\cdots p_s^{a_s}q_1^{b_1}\cdots q_r^{b_r}\ (\geqslant 2).\tag{4-52}$$

表 4.3　不存在的 $(p, 2, l; \lambda)$-强外差族

p	q	$p-1$	$l_{\min}$	$\lambda_{\min}$	$d = \lfloor \frac{p-1}{2l_{\min}} \rfloor$
19	2	$2 \cdot 3^2$	$2 \cdot 3$	2	1
37	2	$2^2 \cdot 3^2$	$2^2 \cdot 3$	2^1	1
101	2	$2^2 \cdot 5^2$	$2^2 \cdot 5$	2^2	2
101	3	$2^2 \cdot 5^2$	$2 \cdot 5 \cdot 3$	3^2	1
163	2	$2 \cdot 3^4$	$2 \cdot 3^2$	2	4
163	3	$2 \cdot 3^4$	$2 \cdot 3^3$	$2 \cdot 3^2$	1
181	2	$2^2 \cdot 3^2 \cdot 5$	$2^2 \cdot 3 \cdot 5$	$2^2 \cdot 5$	1
197	2	$2^2 \cdot 7^2$	$2^2 \cdot 7$	2^2	3
197	3	$2^2 \cdot 7^2$	$2 \cdot 7 \cdot 3$	3^2	2
197	5	$2^2 \cdot 7^2$	$2 \cdot 7 \cdot 5$	5^2	1
257	3	2^8	$2^4 \cdot 3$	3^2	2
257	5	2^8	$2^4 \cdot 5$	5^2	1
257	7	2^8	$2^4 \cdot 7$	7^2	1
401	3	$2^4 \cdot 5^2$	$2^2 \cdot 3 \cdot 5$	3^2	3
433	5	$2^4 \cdot 3^3$	$2^2 \cdot 3^2 \cdot 5$	$3 \cdot 5^2$	1
449	3	$2^6 \cdot 7$	$2^3 \cdot 3 \cdot 7$	$3^2 \cdot 7$	1
487	3	$2 \cdot 3^5$	$2 \cdot 3^3$	$2 \cdot 3$	4
491	2	$2 \cdot 5 \cdot 7^2$	$2 \cdot 5 \cdot 7$	$2 \cdot 5$	3
541	2	$2^2 \cdot 3^3 \cdot 5$	$2^2 \cdot 3^2 \cdot 5$	$2^2 \cdot 3 \cdot 5$	1
577	5	$2^6 \cdot 3^2$	$2^3 \cdot 3 \cdot 5$	5^2	2
577	7	$2^6 \cdot 3^2$	$2^3 \cdot 3 \cdot 7$	7^2	1
641	3	$2^7 \cdot 5$	$2^4 \cdot 3 \cdot 5$	$2 \cdot 5 \cdot 3^2$	1
677	2	$2^2 \cdot 13^2$	$2^2 \cdot 13$	2^2	6
701	2	$2^2 \cdot 5^2 \cdot 7$	$2^2 \cdot 5 \cdot 7$	$2^2 \cdot 7$	2
727	5	$2 \cdot 3 \cdot 11^2$	$2 \cdot 3 \cdot 5 \cdot 11$	$2 \cdot 3 \cdot 5^2$	1
757	2	$2^2 \cdot 3^2 \cdot 7$	$2^2 \cdot 3^2 \cdot 7$	$2^2 \cdot 3 \cdot 7$	1
811	3	$2 \cdot 3^4 \cdot 5$	$2 \cdot 3^3 \cdot 5$	$2 \cdot 3^2 \cdot 5$	1
829	2	$2^2 \cdot 3^2 \cdot 23$	$2^2 \cdot 3 \cdot 23$	$2^2 \cdot 23$	1
883	2	$2 \cdot 3^2 \cdot 7^2$	$2 \cdot 3 \cdot 7$	2	10

若 $\lambda(p-1)=l^2$ 且 $q\mid\lambda$，则 $q(p-1)\mid l^2$，从而 $l_{\min}\mid l$。若 $l_{\min}>(p-1)/2$，则没有整数 λ, l 满足所需的条件；若 $l_{\min}\leqslant(p-1)/2$，取 $\lambda_{\min}=l_{\min}^2/(p-1)$，则 $\lambda=\lambda_{\min}$，$l=l_{\min}$ 满足所需的条件。更一般地，对任意的 $1\leqslant t\leqslant d:=\lfloor(p-1)/2l_{\min}\rfloor$，$\lambda=t^2\lambda_{\min}$，$l=tl_{\min}$ 满足所需的条件。由推论4.3，对于这样的 λ 和 l，不存在 $(p,2,l;\lambda)$-强外差族。在表4.3中，我们列出了所有 $p<1000$ 时的情形。

例 4.3： 如果 $p=4357$，则 $q=2$ 为模 p 本原的素数。因为 $p-1=2^2\cdot3^2\cdot11^2$，我们有 $l_{\min}=2^2\cdot3\cdot11=132$，$\lambda_{\min}=l_{\min}^2/(p-1)=4$，以及 $d=\lfloor(p-1)/2l_{\min}\rfloor=16$。所以对任意的整数 t 满足 $1\leqslant t\leqslant16$，不存在任何的 $(4357,2,132t,4t^2)$-强外差族。

推论4.3也可以不从定理4.8推出，在这里我们给一个初等的直接证明。

推论4.3的证明： 假设子集族 $\{A_0,A_1\}$ 是有限交换群 G 中的一个 $(p,2,l;\lambda)$-强外差族。因为 $|G|=p$ 为素数，所以 G 为循环群。设 g_0 为 G 的一个生成元，χ 为 G 的将 g_0 映射到 $\xi_p=\exp(2\pi\mathrm{i}/p)$ 的 p 阶特征，于是 $\widehat{G}=\{\chi^j:0\leqslant j\leqslant p-1\}$。由强外差族的定义，我们有

$$A_0A_1^{(-1)}=\lambda(G-1_G)\in\mathbb{Z}[G], \tag{4-53}$$

从而对任意的 $1\leqslant j\leqslant p-1$，有

$$\chi^j(A_0)\chi^{p-j}(A_1)=\chi^j(A_0)\chi^j(A_1^{-1})=\lambda\big(\chi^j(G)-\chi^j(1_G)\big)=-\lambda. \tag{4-54}$$

如果我们令

$$f(X)=\sum_{\substack{0\leqslant i\leqslant p-1\\ g_0^i\in A_0}}X^i,\quad g(X)=\sum_{\substack{0\leqslant i\leqslant p-1\\ g_0^i\in A_1}}X^{p-i}\in\mathbb{Z}[X], \tag{4-55}$$

则式（4-54）可改写为

$$f(\xi_p^j)g(\xi_p^j)+\lambda=0,\qquad\forall\,1\leqslant j\leqslant p-1. \tag{4-56}$$

也就是说，对任意的 $1\leqslant j\leqslant p-1$，$\xi_p^j$ 均为首一整系数多项式 $f(X)g(X)+\lambda$ 的根。因为

$$\prod_{j=1}^{p-1}(X-\xi_p^j)=\boldsymbol{\Phi}_p(X)=X^{p-1}+X^{p-2}+\cdots+X+1, \tag{4-57}$$

所以 $\boldsymbol{\Phi}_p(X)\mid\big(f(X)g(X)+\lambda\big)$ 于 $\mathbb{Q}[X]$。

由于 $\boldsymbol{\Phi}_p(X)$ 和 $f(X)g(X)+\lambda$ 均为首一整系数多项式，所以 $\boldsymbol{\Phi}_p(X)$ 在 $\mathbb{Z}[X]$ 中整除 $f(X)g(X)+\lambda$。模 q 后，就有 $\boldsymbol{\Phi}_p(X)$ 在 $\mathbb{F}_q$ 上整除 $f(X)g(X)$。因为 $\gcd(\boldsymbol{\Phi}_p(X),X)=1$，所以 $\boldsymbol{\Phi}_p(X)$ 在 $\mathbb{F}_q$ 上整除 $f(X)g(X)/X$。因为 q 模 p 本原，所以由定理2.1，$\boldsymbol{\Phi}_p(X)$ 在 $\mathbb{F}_q$ 上不可约，从而 $\boldsymbol{\Phi}_p(X)$ 在 $\mathbb{F}_q$ 上整除 $f(X)$ 或 $g(X)/X$。注意到 $f(X)$ 和 $g(X)/X$ 的次数均小等于 $\boldsymbol{\Phi}_p(X)$ 的次数 $p-1$，所以必有 $f(X)=\boldsymbol{\Phi}_p(X)$ 或 $g(X)/X=\boldsymbol{\Phi}_p(X)$。

又因为 A_0 和 A_1 为不交的 l-子集（$l \geqslant 2$），所以 $f(X)$ 和 $g(X)/X$ 均不等于 $\boldsymbol{\Phi}_p(X)$，矛盾。因此，不存在任何的 $(p,2,l;\lambda)$-强外差族。 ∎

最后，我们证明一个新的关于 $m=2$ 的强外差族的不存在性结果。

定理 4.9： 设 p 为一个奇素数，λ，l 为正整数，满足 $2 \leqslant l \leqslant p/2$ 且 $\lambda(2p-1)=l^2$。如果 λ 有一个素因子 q 是模 p 本原的，则不存在任何的 $(2p,2,l;\lambda)$-强外差族。

证明： 假设子集族 $\{A_0,A_1\}$ 是有限交换群 G 中的一个 $(2p,2,l;\lambda)$-强外差族。因为 $|G|=2p$ 且 $\gcd(2,p)=1$，我们知道 G 必定是一个循环群。设 g_0 为 G 的一个生成元，χ 为 G 的将 g_0 映射到 $\xi_{2p}=\exp(\pi \mathrm{i}/p)$ 的 $2p$ 阶特征。令

$$\alpha=\chi(A_0)=\sum_{g\in A_0}\chi(g),\quad \beta=\chi(A_1^{(-1)})=\sum_{g\in A_1}\overline{\chi(g)}=\overline{\chi(A_1)}. \tag{4-58}$$

因为 $\{A_0,A_1\}$ 是一个 $(2p,2,l;\lambda)$-强外差族，我们有 $A_0A_1^{(-1)}=\lambda(G-1_G)\in\mathbb{Z}[G]$，从而

$$\alpha\beta=\lambda\big(\chi(G)-\chi(1_G)\big)=-\lambda\in\mathbb{C}. \tag{4-59}$$

因为 $\lambda\neq 0$，我们有 α，$\beta\neq 0$。注意到 α，β 在 $\mathcal{O}_K=\mathbb{Z}[\xi_{2p}]=\mathbb{Z}[\xi_p]$（因为 $\xi_{2p}=\xi_{2p}^{2p+1}=-\xi_{2p}^{p+1}=-\xi_p^{(p+1)/2}$），即分圆域 $K=\mathbb{Q}(\xi_{2p})=\mathbb{Q}(\xi_p)$ 的整数环中，其中 $\xi_p=\exp(2\pi \mathrm{i}/p)$。

由假设，q 在 $\mathbb{Z}$ 中整除 λ，所以 q 在 $\mathcal{O}_K$ 中整除 $\alpha\beta$。因为 q 模 p 本原，由推论2.1，$q\mathcal{O}_K$ 是 $\mathcal{O}_K$ 中的素理想，从而 q 在 $\mathcal{O}_K$ 中整除 α 或 β。不失一般性，我们假设 q 在 $\mathcal{O}_K$ 中整除 α。

对任意的 $0\leqslant i\leqslant 2p-1$，令

$$n_i=\begin{cases}1, & \text{若 } g_0^i\in A_0,\\ 0, & \text{若 } g_0^i\notin A_0,\end{cases} \tag{4-60}$$

则 $\sum\limits_{i=0}^{2p-1}n_i=|A_0|=l$。此外，我们有

$$\begin{aligned}\alpha&=\sum_{g\in A_0}\chi(g)=\sum_{i=0}^{2p-1}n_i\chi(g_0^i)=\sum_{i=0}^{2p-1}n_i\xi_{2p}^i\\&=\sum_{i=0}^{p-1}(n_i\xi_{2p}^i+n_{i+p}\xi_{2p}^{i+p})\\&=\sum_{i=0}^{p-1}(n_i-n_{i+p})\xi_{2p}^i=\sum_{i=0}^{p-1}a_i\xi_{2p}^i,\end{aligned} \tag{4-61}$$

其中对任意的 $0\leqslant i\leqslant p-1$，$a_i:=n_i-n_{i+p}\in\{0,\pm 1\}$。因为 $\alpha\neq 0$，所以至少有一

个 a_i（$0 \leqslant i \leqslant p-1$）不为 0。如果对任意的 $0 \leqslant i \leqslant p-1$，都有 $a_i = n_i - n_{i+p} \neq 0$，则对任意的 $0 \leqslant i \leqslant p-1$，必有 $n_i + n_{i+p} = 1$，从而

$$l = \sum_{i=0}^{2p-1} n_i = \sum_{i=0}^{p-1} (n_i + n_{i+p}) = p. \tag{4-62}$$

如果 $l = p$，则假设 $\lambda(n-1) = l^2$ 就变为 $\lambda(2p-1) = p^2$。因为 $(2p-1, p) = 1$ 且 $2p-1 > 1$，这是不可能的。所以存在 $0 \leqslant i_0 \leqslant p-1$，使得 $a_{i_0} = 0$。因为 $[K : \mathbb{Q}] = [\mathbb{Q}(\xi_p) : \mathbb{Q}] = p-1$，所以

$$\{\xi_{2p}^i : 0 \leqslant i \leqslant p-1,\ i \neq i_0\} \tag{4-63}$$

构成 K 在 $\mathbb{Q}$ 的一组基。因为 q 在 $\mathcal{O}_K$ 中整除 α，且

$$\alpha = \sum_{g \in A_0} \chi(g) = \sum_{\substack{0 \leqslant i \leqslant p-1 \\ i \neq i_0}} a_i \xi_{2p}^i, \tag{4-64}$$

所以对任意的 $0 \leqslant i \leqslant p-1$，$q$ 在 $\mathbb{Z}$ 中整除 a_i。因为 $a_i \in \{0, \pm 1\}$ 且至少有一个 a_i 不为 0，我们必有 $q = 1$，而这与 q 是素数的假设矛盾。因此 q 在 $\mathcal{O}_K$ 中不整除 α，从而一开始的假设是不成立的，即不存在任何的 $(2p, 2, l; \lambda)$-强外差族。 ∎

注释 4.7： 如果定理4.9中的条件成立，且 $q = 2$，$2^3 \nmid \lambda$，则定理4.8中的条件 $|G_p| > n/q^{\lceil f/2 \rceil}$ 不满足。事实上，此时我们有 $|G_p| = p$，$1 \leqslant f \leqslant 2$，从而 $n/q^{\lceil f/2 \rceil} = 2p/2 = p = |G_p|$。因此，定理4.9并不包含在定理4.8中。由定理4.9，表4.4中那些参数的 $(2p, 2, l; \lambda)$-强外差族不存在，而这不能由定理4.8导出。

表 4.4　不存在的 $(2p, 2, l; \lambda)$-强外差族

$n = 2p$	p	q	$n-1$	l	λ	$(2l \leqslant n)$
1226	613	2	35^2	$70(2t+1)$	$4(2t+1)^2$	$(0 \leqslant t \leqslant 3)$
2602	1301	2	51^2	$102(2t+1)$	$4(2t+1)^2$	$(0 \leqslant t \leqslant 5)$
7226	3613	2	85^2	$170(2t+1)$	$4(2t+1)^2$	$(0 \leqslant t \leqslant 10)$

第 5 章　总结与展望

5.1　主要结果

本文研究了源自秘密共享应用的若干编码与组合设计的问题。

首先，本文研究了两类由有限域 $\mathbb{F}_{p^m}$ 上的完全非线性函数 Π 构造的线性码：C_Π 与 $\overline{C_\Pi}$。这两类线性码不仅本身具有良好的参数，并且由它们的对偶码构造的秘密共享方案具有十分有应用价值的存取结构。当 m 为奇数时，我们在仅利用 Π 是完全非线性函数这一条件的前提下，用统一的方法完全确定了 C_Π 与 $\overline{C_\Pi}$ 的重量分布。当 m 为偶数时，我们也给了比较宽松的条件，使得类似的结果依然成立。此外，基于我们得到的重量分布的结果，我们探讨了 C_Π 与 $\overline{C_\Pi}$ 的覆盖问题，使得绝大部分的情形得到了解决。

然后，本文研究了两类组合设计理论中的对象：循环外差族与强循环外差族。它们是外差族与强外差族的变形，可以用于构造无条件安全的不可延展秘密共享方案。我们利用有限域中的分圆类构造出循环外差族的无穷族、证明了所有强循环外差族都是平凡的，并且给出了一个新的强外差族的不存在性结果。

5.2　可进一步开展的工作

下面是一些与本文相关的可进一步开展的工作：

(1) 为了在 m 为偶数时确定 C_Π 和 $\overline{C_\Pi}$ 的重量分布，我们添加了额外的条件。虽然我们添加的条件比较宽松，并且被所有已知的完全非线性函数所满足，但是如果去掉这些条件，结论是否依然成立，或者这些条件是否是多余的，这都是值得进一步探讨的问题。

(2) 在定理3.9和定理3.10中，当 $m=2$ 且 $p>3$ 时，C_Π 和 $\overline{C_\Pi}$ 中均有部分码字是否为极小码字无法确定。因此，能否对一般的 Π，来确定这部分码字是否为极小码字，还有待进一步研究。

(3) 本文构造的循环外差族，均是基于有限域中的分圆类。然而，亦可考虑有限域中不基于分圆类的构造，或者是其他有限交换群中的构造。

参考文献

[1] Blakley G R. Safeguarding cryptographic keys[C]// Managing Requirements Knowledge, International Workshop on. IEEE Computer Society, 1979: 313-313.

[2] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[3] McEliece R J, Sarwate D V. On sharing secrets and Reed-Solomon codes[J]. Communications of the ACM, 1981, 24(9): 583-584.

[4] Massey J L. Minimal codewords and secret sharing[C]// Proceedings of the 6th joint Swedish-Russian international workshop on information theory. 1993: 276-279.

[5] Massey J L. Some applications of coding theory in cryptography[J]. Codes and Ciphers: Cryptography and Coding IV, 1995: 33-47.

[6] Anderson R, Ding C, Helleseth T, et al. How to build robust shared control systems[J]. Designs, Codes and Cryptography, 1998, 15: 111-124.

[7] Ding C, Kohel D R, Ling S. Secret-sharing with a class of ternary codes[J]. Theoretical Computer Science, 2000, 246(1-2): 285-298.

[8] Ding C, Yuan J. Covering and secret sharing with linear codes[C]// International Conference on Discrete Mathematics and Theoretical Computer Science. Springer, 2003: 11-25.

[9] Pieprzyk J, Zhang X. Ideal secret sharing schemes from MDS codes[C]// Proc. 5th Int. Conf. Information Security and Cryptology (ICISC 2002). 2002: 269-279.

[10] Carlet C, Ding C, Yuan J. Linear codes from perfect nonlinear mappings and their secret sharing schemes[J]. IEEE Transactions on Information Theory, 2005, 51(6): 2089-2102.

[11] Yuan J, Carlet C, Ding C. The weight distribution of a class of linear codes from perfect nonlinear functions[J]. IEEE transactions on information theory, 2006, 52(2): 712-717.

[12] Feng K, Luo J. Value distributions of exponential sums from perfect nonlinear functions and their applications[J]. IEEE transactions on information theory, 2007, 53(9): 3035-3041.

[13] Li C, Qu L, Ling S. On the covering structures of two classes of linear codes from perfect nonlinear functions[J]. IEEE transactions on information theory, 2008, 55(1): 70-82.

[14] Li C, Li Q, Ling S. Properties and applications of preimage distributions of perfect nonlinear functions[J]. IEEE transactions on information theory, 2008, 55(1): 64-69.

[15] Carlet C, Ding C. Highly nonlinear mappings[J]. Journal of complexity, 2004, 20(2-3): 205-244.

[16] Tompa M, Woll H. How to share a secret with cheaters[J]. journal of Cryptology, 1989, 1(3): 133-138.

[17] Cramer R, Dodis Y, Fehr S, et al. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2008: 471-488.

[18] Dolev D, Dwork C, Naor M. Non-malleable cryptography[C]// Proceedings of the twenty-third annual ACM symposium on Theory of computing. 1991: 542-552.

[19] Damgard I, Groth J. Non-interactive and reusable non-malleable commitment schemes[C]// Proceedings of the thirty-fifth annual ACM symposium on Theory of computing. 2003: 426-437.

[20] Dziembowski S, Pietrzak K, Wichs D. Non-malleable codes[J]. Journal of the ACM (JACM), 2018, 65(4): 1-32.

[21] Fischlin M, Fischlin R. Efficient non-malleable commitment schemes[C]// Annual International Cryptology Conference. Springer, 2000: 413-431.

[22] Kenthapadi K. Models and algorithms for data privacy[D]. Stanford University Stanford, CA, USA, 2006.

[23] Dwork C, Kenthapadi K, McSherry F, et al. Our data, ourselves: Privacy via distributed noise generation[C]// Advances in Cryptology-EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28-June 1, 2006. Proceedings 25. Springer, 2006: 486-503.

[24] Ishai Y, Prabhakaran M, Sahai A. Founding cryptography on oblivious transfer–efficiently[C]// Advances in Cryptology–CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings 28. Springer, 2008: 572-591.

[25] Bentov I, Kumaresan R. How to use bitcoin to design fair protocols[C]// Annual Cryptology Conference. Springer, 2014: 421-439.

[26] Gordon S D. On fairness in secure computation[D]. University of Maryland, College Park, 2010.

[27] Gordon D, Ishai Y, Moran T, et al. On complete primitives for fairness[C]// Theory of Cryptography: 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings 7. Springer, 2010: 91-108.

[28] Dziembowski S, Pietrzak K, Wichs D. Non-malleable codes[J]. Innovations in Computer Science, 2010: 434-452.

[29] Goyal V, Kumar A. Non-malleable secret sharing[C]// Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing. 2018: 685-698.

[30] Aggarwal D, Damgård I, Nielsen J B, et al. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures[C]// Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39. Springer, 2019: 510-539.

[31] Badrinarayanan S, Srinivasan A. Revisiting non-malleable secret sharing[C]// Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part I 38. Springer, 2019: 593-622.

[32] Goyal V, Kumar A. Non-malleable secret sharing for general access structures[C]// Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38. Springer, 2018: 501-530.

[33] Albab K D, Issa R, Varia M, et al. Batched differentially private information retrieval[C]// 31st USENIX Security Symposium (USENIX Security 22). 2022: 3327-3344.

[34] Veitch S, Stinson D R. Unconditionally secure non-malleable secret sharing and circular external difference families[J]. Designs, Codes and Cryptography, 2023.

[35] Levenshtein V I. One method of constructing quasilinear codes providing synchronization in the presence of errors[J]. Problemy Peredachi Informatsii, 1971, 7(3): 30-40.

[36] Ogata W, Kurosawa K, Stinson D R, et al. New combinatorial designs and their applications to authentication codes and secret sharing schemes[J]. Discrete Mathematics, 2004, 279(1-3): 383-405.

[37] Paterson M B, Stinson D R. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families[J]. Discrete Mathematics, 2016, 339(12): 2891-2906.

[38] Paterson M B, Stinson D R. Circular external difference families, graceful labellings and cyclotomy[J]. arXiv preprint arXiv:2310.02810, 2023.

[39] Washington L C. Introduction to cyclotomic fields: volume 83[M]. New York: Springer Science & Business Media, 1997.

[40] 冯克勤, 刘凤梅, 杨晶. 代数数论及其通信应用 [M]. 北京: 科学出版社, 2023.

[41] Lidl R, Niederreiter H. Finite fields: number 20[M]. Cambridge University Press, 1997.

[42] Neukirch J. Algebraic number theory: volume 322[M]. Springer Science & Business Media, 2013.

[43] Pless V, Brualdi R A, Huffman W C. Handbook of coding theory[M]. Elsevier Science Inc., 1998.

[44] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析 [M]. 北京: 科学出版社, 2011.

[45] Mesnager S. Bent functions: volume 1[M]. Springer, 2016.

[46] Nyberg K. Differentially uniform mappings for cryptography[C]// Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 1993: 55-64.

[47] Dembowski P, Ostrom T G. Planes of order n with collineation groups of order n^2[J]. Mathematische Zeitschrift, 1968, 103(3): 239-258.

[48] Coulter R S, Matthews R W. Planar functions and planes of Lenz-Barlotti class II[J]. Designs, Codes and Cryptography, 1997, 10(2): 167-184.

[49] Ding C, Yuan J. A family of skew Hadamard difference sets[J]. Journal of Combinatorial Theory, Series A, 2006, 113(7): 1526-1535.

[50] Budaghyan L, Helleseth T. New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p[C]// International Conference on Sequences and Their Applications. Springer, 2008: 403-414.

[51] Zha Z, Kyureghyan G M, Wang X. Perfect nonlinear binomials and their semifields[J]. Finite Fields and Their Applications, 2009, 15(2): 125-133.

[52] Matsui M. Linear cryptanalysis method for des cipher[C]// Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 1993: 386-397.

[53] Carlet C, Dubuc S. On generalized bent and q-ary perfect nonlinear functions[C]// Finite Fields and Applications: Proceedings of The Fifth International Conference on Finite Fields and Applications F q 5, held at the University of Augsburg, Germany, August 2–6, 1999. Springer, 2001: 81-94.

[54] Kumar P V, Scholtz R A, Welch L R. Generalized bent functions and their properties[J]. Journal of Combinatorial Theory, Series A, 1985, 40(1): 90-107.

[55] Nyberg K. Constructions of bent functions and difference sets[C]// Advances in Cryptology—EUROCRYPT'90: Workshop on the Theory and Application of Cryptographic Techniques Aarhus, Denmark, May 21–24, 1990 Proceedings 9. Springer, 1991: 151-160.

[56] Renvall A, Ding C. The access structure of some secret-sharing schemes[C]// Information Security and Privacy: First Australasian Conference, ACISP'96 Wollongong, NSW, Australia, June 24–26, 1996 Proceedings 1. Springer, 1996: 67-78.

[57] Ashikhmin A, Barg A. Minimal vectors in linear codes[J]. IEEE Transactions on Information Theory, 1998, 44(5): 2010-2017.

[58] Storer T. Cyclotomy and difference sets[J]. Lectures in Advanced Mathematics, 1967.

[59] Huczynska S, Johnson L M. Internal and external partial difference families and cyclotomy[J]. Discrete Mathematics, 2023, 346(3): 113295.

[60] Jedwab J, Li S. Construction and nonexistence of strong external difference families[J]. Journal of Algebraic Combinatorics, 2019, 49: 21-48.

[61] Ma S L. A survey of partial difference sets[J]. Designs, Codes and Cryptography, 1994, 4(4): 221-261.

[62] Arasu K, Jungnickel D, Ma S L, et al. Strongly regular Cayley graphs with $\lambda - \mu = -1$[J]. Journal of Combinatorial Theory, Series A, 1994, 67(1): 116-125.

致　谢

首先，我要感谢我的家人，是你们一直以来的支持和鼓励，让我能够顺利完成博士学业。你们的支持是我最大的动力。

其次，我要感谢我的女朋友黄敏，感谢你在我最沮丧、最没有信心的时候激励我坚持下去，感谢你对我的不离不弃，感谢你对我的鞭策与陪伴。同时，也要感谢黄敏的家人，感谢你们对我学业的支持与鼓励。

接着，我要感谢我的前导师扶磊教授，感谢您的言传身教，让我无论是在专业知识还是在治学态度上，都收获良多。您对严谨与真实的坚持，也将成为我一生的信条。

然后，我还要感谢我的导师杨晶副教授，感谢您在我十分困窘之际给了我一个机会，感谢您给我提供的专业指导与丰富的学术资源，让我得以迅速进入到新的研究方向。您的鼓励与帮助，我终生难忘。

我要特别感谢的是冯克勤教授。冯老师虽已年过八旬，但依然精力充沛，对学术研究充满了热情，而且经常出席大大小小的学术会议，给后辈们精神上的鼓励与学术上的指导。从冯老师身上，我看到了老一辈学者孜孜不倦的治学精神与谦和从容的处事之道，也让我对自己的未来有了更多的期待。

对于我的师兄张浩、李培根与王浩旭，我也要表达我诚挚的感谢。感谢你们经常解答我的问题，感谢你们在我遇到困难时给予的帮助，感谢你们给我的学术研究提供的宝贵意见。

最后，我要感谢所有我在读博期间遇到的师长和朋友，特别是杨雪梅老师、谌昭学长、刘思汉学长、冯立同学、司徒泉学弟、杨芳学妹、张港回学弟、邵钰菓学弟、郑钦城学弟、段哲凡学弟以及黄起涛学弟，感谢你们在学习以及生活上给予我的帮助，感谢你们在我枯燥的博士生活里给我增添的乐趣。

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：_____ 日　期：_____

个人简历、在学期间完成的相关学术成果

个人简历

1996 年 9 月 3 日出生于福建省莆田市。

2014 年 9 月考入华中科技大学数学与统计学院信息与计算科学专业，2018 年 6 月本科毕业并获得理学学士学位。

2018 年 9 月免试进入清华大学数学系攻读博士学位至今。

在学期间完成的相关学术成果

学术论文：

[1] Wu H, Yang J, Feng K. The weight distributions of two classes of linear codes from perfect nonlinear functions[J/OL]. IEEE Transactions on Information Theory, 2023: 1-1.（已录用并在线发表）

[2] Wu H, Yang J, Feng K. Circular external difference families: Construction and non-existence[J]. arXiv preprint arXiv:2310.10200, 2023.

[3] Wu H, DNA-Correcting Codes in DNA Storage Systems[J]. arXiv preprint arXiv:2311.09910, 2023.

指导教师评语

吴华伟博士论文使用代数数论、代数和组合的数学工具，研究了通信中代数编码理论和密码学中两个重要问题，取得新的进展。

其一，2005 年，Carlet 和丁存生提出用有限域 $\mathbb{F}_{p^m}$ 上完全非线性函数构作线性纠错码的方案，这种码和它的对偶码有好的纠错性能，并可用来构作好的秘密共享方案。决定这种纠错码的重量分布是一个重要的研究课题。近二十年来，许多学者对于某些特殊情形决定了重量分布。本论文采用统一的方法，对几乎全部情形（只对 m 为偶数时加上了一个宽松条件）完全决定了重量分布。特别在论证方法方面，创新性地研究了在某种群作用之下对于码字追行分类和计数。

其二，2023 年, Veitch 和 Stinson 为构作无条件安全的不可扩展秘密共享方案，提出了两种新型组合设计：循环外差族和强循环外差族，给出循环外差族的一些构作方式，并提出一些待研究的问题，其中特别提出如何构作非平凡的强循环外差族，被认为是困难的。本论文利用代数数论（分圆域理论）和代数学（有限交换群特征理论），给出构作循环外差族的更多方式（包括对前人构作方式的推广，以及由已知结果构作新循环外差族的提升方法），并且证明了非平凡的强循环外差族是不存在的。

本论文这两项结果结果都很重要，第一项工作已发表于 IEEE Trans. Information Theory（2023 年），第二项工作是很新的课题，本论文相关的部分结果已登在 arxiv 上（2023 年，待正式发表），并且已被 Huczynska 和 Hume 于 2024 年 3 月的文章（arxiv:2403.16284 v1）所引用。

该论文表明吴华伟在组合学、数论和代数方面有坚实的数学基础，同时也具有提取捕捉信息领域重要问题的研究能力。论文逻辑清晰，论证严谨，语言通畅，是一篇优秀的博士论文。

答辩委员会决议书

秘密共享方案是重要的密码学原语，有很多重要的应用。本论文针对应用在秘密共享方案中的编码与组合设计问题展开研究，选题具有重要的理论意义和应用价值。论文的主要创新点如下：

(1) 用统一的方法，对于由完全非线性函数构造的两类线性码，通过某种群作用，对码字进行分类和计数，完全确定了这两类码的重量分布，包括了前人对各种特定形式做出的结果。

(2) 利用分圆类给出了循环外差族的一些新的构造方式，得到了一系列新参数的循环外差族。

(3) 证明了所有强循环外差族都归结于两个集合的强外差族，回答了前人提出的关于强循环外差族的公开问题。同时利用分圆域的知识，证明了一个关于强外差族的不存在性的新结果。

论文结论正确，论证严谨，成果丰富，创新性强，写作规范，是一篇优秀的博士学位论文。论文工作表明作者具有扎实的数学基础和深入的专业知识，对相关研究领域的发展现状有全面的了解，具备很强的独立科研能力。

答辩过程中，吴华伟叙述清晰，回答问题准确。答辩委员会经投票一致同意通过论文答辩，并建议授予吴华伟同学理学博士学位。