分类号： O157.2 单位代码： 10335

学 号： 11335033

浙江大学

博士学位论文

中文论文题目： 信息安全与大数据存储中的几个关键问题

英文论文题目： **Several Key Problems in Information Security and Big Data Storage**

申请人姓名： 马景学

指导教师： 葛根年 教授

专业名称： 应用数学

研究方向： 组合数学与编码理论

所在学院： 数学科学学院

论文提交日期 2018 年3月20日

信息安全与大数据存储中的几个关键问题

论文作者签名： _____

指导教师签名： _____

论文评阅人1：_____

评阅人2：_____

评阅人3：_____

评阅人4：_____

评阅人5：_____

答辩委员会主席：曹海涛　教授　南京师范大学

委员1：曹海涛　教授　南京师范大学

委员2：吴佃华　教授　广西师范大学

委员3：吴志祥　教授　浙江大学

委员4：冯涛　研究员　浙江大学

委员5：葛根年　教授　浙江大学

答辩日期：2018 年4月29日

Several Key Problems in Information Security and Big Data Storage

Author's signature: _____

Supervisor's signature: _____

External Reviewers: _____

_____

_____

_____

_____

Examining Committee Chairperson:

Prof. Haitao Cao, Nanjing Normal University

Examining Committee Members:

Prof. Haitao Cao, Nanjing Normal University

Prof. Dianhua Wu, Guangxi Normal University

Prof. Zhixiang Wu, Zhejiang University

Prof. Tao Feng, Zhejiang University

Prof. Gennian Ge, Zhejiang University

Date of oral defence: April 29, 2018

浙江大学研究生学位论文独创性声明

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

学位论文作者签名：　　签字日期：　　年　　月　　日

学位论文版权使用授权书

本学位论文作者完全了解**浙江大学**有权保留并向国家有关部门或机构送交本论文的复印件和磁盘，允许论文被查阅和借阅。本人授权浙江大学可以将学位论文的全部或部分内容编入有关数据库进行检索和传播，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：　　导师签名：

签字日期：　　年　　月　　日　　签字日期：　　年　　月　　日

致　　谢

转眼间，在浙江大学的学习与生活即将接近尾声。回首这五年的博士生生涯，感慨颇多。在这篇博士论文完成之际，我要向所有指导过我的老师，帮助过我的同学，一直关心支持我的家人，致以最深的谢意！

首先，感谢我最敬爱的导师葛根年教授。衷心感谢您在学习、科研、生活与为人处世等诸多方面给予我的无私关怀和悉心指导。您优秀的做人品质，严谨的治学态度，精确的科研敏锐度深深地影响了我。您高瞻远瞩的学术视野和严谨认真的学术作风将使我终身受益！

感谢黄民强院士对我的关照与勉励。感谢冯涛研究员对我的培养与鼓励。在与他们的交流中，我得以开拓研究视野，体会到科研的乐趣！

感谢和我一起学习的各位同门：胡思煌、魏恒嘉、李抒行、张一炜、张韬、上官冲、汪馨、顾玉杰、Jerod Michel、丁报昆、李林林、孔祥梁、钱昺辰、戚立波、奚元霄、韩雪姣、徐子翔、谢城飞、兰昭君、余文俊、叶左、李伟聪、何智文、陶然等，在这段学习与生活的时光里，我们留下了很多美好的回忆，感谢诸位师兄弟姐妹对于我的悉心指导和照顾。尤其是同门中上官冲师兄和张韬师兄对我的关心指导与督促！

感谢我亲爱的朋友们：王海、魏龙、金侃、郭伟、小白、周董等，谢谢你们给我带来的快乐与宽慰！

我还要感谢母校浙江大学给我提供了优良的学习环境，让我可以自由自在地在学术的海洋里探索！

最后，我还要感谢婷婷的理解、支持与陪伴，感谢我的父母与家人，你们对我的支持与关怀是我最强大的后盾，激励着我不畏风雨、勇敢前行。在此祝愿你们永远开心、快乐、健康！我将用我的余生去回馈你们对我的付出与爱！

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

摘　　要

本学位论文主要考虑了两方面的问题：一类着重于研究有限域上的置换多项式，其在密码学、编码理论和组合设计理论中有广泛应用；另一类着重于考虑数据存储中的局部可修复码，其在当前大数据环境下的分布式存储中有重要应用。本学位论文从组合数学的观点出发，融汇应用了有限域、代数数论等相关工具，对这些问题进行了一定的思考与推进。

在第 1 章绪论部分，我们将简要介绍本文所涉及问题的背景来源，并概述本文对此问题所做的主要贡献。

在第 2 章中，我们的研究对象为有限域上的置换多项式。通过区分平方元和非平方元的方法解决了Wu等人提出的两类具有Niho指数的三项置换多项式的猜想；通过多变元方法研究特殊方程解的数目，进而构造了两类三项置换多项式，并将Kyureghyan等人给出的两个例子推广成无穷类。

在第 3 章中，我们主要考虑了完全置换多项式和低差分度的置换多项式。我们的工作是构造了四类单项完全置换多项式和一类三项完全置换多项式，其中第一类完全置换多项式解决了由Wu等人提出的一个猜想；研究了一类幂函数（置换单项式）的差分性质，对Blondeau等人提出的 8 -差分函数的猜想做出了一定的推进工作。

在第 4 章中，我们的研究对象是分布式存储中的局部可修复码。我们主要关注二元局部可修复码的维数上界以及具体的构造。首先，我们基于经典编码理论中的Johnson界得到了这类二元局部可修复码的一个维数上界，然后借助一类特殊的组合结构partial spread和弱无关集，得到了若干最优二元局部可修复码。

在第 5 章中对本人博士期间其它研究问题：追踪码、再生码、极大可修复码，做了简要概述。

关键词： 置换多项式，完全置换多项式，局部可修复码，partial spreads，弱无关集，追踪码，再生码，极大可修复码

Abstract

This thesis mainly considers two problems. The first one focuses on the study of permutation polynomials over finite fields, which have wide applications in cryptography, coding theory and combinatorial design theory. The second one mainly investigates the locally repairable code in data storage, which plays an important role in distributed storage systems. This thesis makes a further research on the problems from the perspective of combinatorics, and uses the related tools such as finite field theory, algebraic number theory and so on.

In Chapter 1, we briefly introduce the backgrounds of the problems concerned with this thesis and summarize our contributions towards these topics.

In Chapter 2, we investigate the permutation polynomials over finite fields. We prove two conjectures about the permutation trinomials with Niho exponents, which were proposed by Wu et al., by using the method of treating squares and non-squares separately. Further, we construct two new classes of permutation trinomials by studying the number of solutions to special equations. And we generalize two examples proposed by Kyureghyan et al. to an infinite class.

In Chapter 3, we mainly consider complete permutation polynomials and permutation polynomials with low differential uniformity. Four classes of monomial complete permutation polynomials and one class of trinomial complete permutation polynomials are presented, one of which confirms a conjecture proposed by Wu et al.. Further, we make some progress on a conjecture about the differential uniformity of power permutation polynomials proposed by Blondeau et al..

In Chapter 4, we investigate the locally repairable code in distributed storage systems. We mainly focus on the upper bound for the dimension k and constructions of binary linear locally repairable codes. First, we derive an explicit upper bound for the dimension of such codes. Further, based on partial spreads and weakly independent sets, we get some new optimal binary locally repairable codes.

In Chapter 5, we briefly introduce other problems considered in the PhD learning phase, such as traceability codes, regenerating codes, maximally recoverable codes.

Keywords: permutation polynomials, complete permutation polynomials, locally repairable codes, partial spreads, weakly independent sets, traceability codes, regenerating codes, maximally recoverable codes

插　　图

目　　次

1 绪论

1.1 有限域上的置换多项式

令 $\mathbb{F}_{p^n}$ 是含有 p^n 个元素的有限域，其中 p 是一个素数且 n 是一个正整数。如果多项式 $f(x) \in \mathbb{F}_{p^n}[x]$ 能够诱导出一个从 $\mathbb{F}_{p^n}$ 到其自身的双射，则称是 $f(x)$ 是 $\mathbb{F}_{p^n}$ 上的一个置换多项式。置换多项式的研究已有上百年的历史，早在1863年，Hermite就对模 p 的置换多项式进行了研究，并提出了置换多项式的判别准则。之后在1896年，Dickson研究了一般有限域上的置换多项式，被人们称为Dickson多项式。自上世纪中叶，数论、代数几何等一些深刻的数学工具应用到置换多项式上，得到了许多好的结果。在Lidl和Niederreiter[40]的著作《有限域》一书中对置换多项式有较全面的综述。近年来，由于在密码学、编码理论、组合设计理论[15–17,35,51,58] 等领域的应用，置换多项式得到了广泛关注与深入研究。例如，Ding等人[15]通过阶为 5 的Dickson置换多项式构造了一类斜Hadamard差集，推翻了长久以来的关于斜Hadamard差集的一个猜想。

目前对置换多项式的研究比较公认的两个重要方面为：有简单的或者漂亮的代数表达式（如稀疏项数的置换多项式的构造）和有额外特殊性质的多项式（如低差分均匀度）。这也是我们在第二章、第三章的主要研究对象。通常来说，寻找满足很多标准的置换多项式是困难的。如著名的“Big APN”问题！自然地，需要一些判别法则来说明某个构造的多项式是置换多项式。

我们的工作主要是构造了若干类三项置换多项式，证明了由Wu等人[69] 提出的两类具有Niho指数的三项置换多项式的猜想，另外将Kyureghyan和Zieve[34]计算机搜索遗留的两个例子推广成无穷类。这部分内容对应于第二章。研究完全置换多项式和低差分均匀度的置换多项式在密码学上具有重要意义。我们的工作是构造了四类单项完全置换多项式和一类三项完全置换多项式，其中第一类完全置换多项式解决了由Wu等人[71]提出的一个猜想；研究了一类幂函数（单项置换多项式）的差分性质，对Blondeau等人[9]提出的 8-差分函数的猜想做出了一定的推进工作。这部分内容对应于第三章。

本工作对应的两篇论文，分别发表于《Designs, Codes and Cryptography》和《Finite

Fields and Their Applications》。

1.2 二元局部可修复码

随着计算机技术的迅猛发展，网络带宽的飞速增长，智能设备的应用普及，P2P、社交网络、多媒体共享等网络技术的发展，网络通信已成为数据通信系统的主体，也逐步成为我们日常生活中不可或缺的组成部分。同时，网络中的数据总量也达到了一个惊人的程度，这一方面来自于电子商务、电子政务等日常生活领域的数据，另一方面来自于天文观测、高能物理、能源研究、基因分析等科研领域产生的数据。海量数据的日益累积，使我们迎来了大数据时代。面向大数据与网络环境的信息产业已成为21世纪的朝阳产业和支柱产业。中共中央“十三五规划”中已明确指出，“我国要大力发展数据科学的理论研究、技术发展和工业实现，要构建一个高效、安全的网络环境和社会环境，为信息时代的到来做好充分准备”。十九大报告中也多次提及了和大数据与网络相关的关键词——“推动互联网、大数据、人工智能和实体经济深度融合；网络强国；提高基于网络信息体系的联合作战能力；网络安全；运用互联网技术和信息化手段”等。

大数据时代决定了数据存储方式的改变，谷歌等商业公司的运行经验表明，现实中最常见的数据损坏情况是单个存储节点（磁盘）因为设备损坏、自然灾害等因素而失效。在节点失效后，需要即刻加入新的节点来代替失效的节点，以维持整个系统的可靠性。基于复制或纠删码的两种传统策略下，重建丢失节点的数据需要消耗较大的系统资源，亟需设计一种更好的存储编码方案以提高单个存储节点的修复效率。单个存储节点的修复效率的衡量指标主要有：节点存储容量、计算负荷、磁盘I/O、修复带宽和每次修复所访问的节点数目等。

2012年，微软研究院提出了局部可修复码（Locally Repairable Codes）的模型[23]，即在节点修复过程中每个损坏的节点可由某一组至多 r 个节点所修复，这里的 r 称为局部性参数。这一模型不仅实现了存储效率和修复效率的均衡，而且修复过程中所涉及的节点数较少，从而也优化了磁盘I/O。2014 年，本领域的专家Yekhanin受邀在国际数学家大会上作了 45 分钟报告，使得局部可修复码成为一大研究热点。

近年来，关于局部可修复码的工作已经得到很深入的研究，如Gopalan等人的开创性论文中[23]仿照经典编码理论的Singleton界，给出了局部可修复码的Singleton型界：

$$d \leq n - k - \lceil \frac{k}{r} \rceil + 2, \tag{1-1}$$

并构造了在特定参数下可达到此界的最优码类。2014年，Song等人[57] 利用矩阵秩的关系，证明了在很多参数下Singleton型界是不紧的，同时也证明了部分参数下最优线性局部可

修复码的存在性。同年，Tamo和Barg[60]利用多项式插值的想法，系统地给出了构造局部可修复码的方法。之后的拓展研究考虑多个节点失效的情况，对多个节点的修复又细分为并行修复和串行修复两种模式。所谓并行修复，即同时修复各个损坏的节点，Wang等人[65]和Prakash等人[49]分别提出了两种不同的修复方式；所谓串行修复，即各个损坏的节点的修复过程有先后顺序，允许先一步修好的节点被利用到后续节点修复的过程中[50]。为了方便计算机硬件的实现，人们也越来越多关注二元最优局部可修复码的构造问题。在文献[10]中，首次将域的大小考虑进去导出一个新的界，我们称其为Cadambe-Mazumdar (C-M)界。

$$k \leq \min_{t \in \mathbb{Z}^+} \left[tr + k_{\text{opt}}^{(q)}(n-(r+1)t, d) \right], \tag{1-2}$$

其中 $k_{\text{opt}}^{(q)}(n,d)$ 是固定域的大小 q 、码长 n 和极小距离 d 时，码所能达到的最大可能维数。Huang等人[33] 从一些不同的基码构造了若干极小距离为 3、4、5 的二元局部可修复码。Shahabinejad等人[53]构造了极小距离为 4 的二元最优局部可修复码。当前，构造拥有高码率、大的极小Hamming距离、小的局部性参数的二元局部可修复码仍是人们所关心的热点问题。

我们主要关注含有不交修复组的二元局部可修复码的维数上界以及具体的构造。首先，我们导出关于这类码的维数 k 的一个上界(定理 4.3.1)，然后对一般参数的 r ，我们给出了两类 k-最优的二元局部可修复码的构造。进一步，对于 $r \in \{2,3\}$ ，极小距离 $d=6$ 的情形，我们得到了几乎所有参数的 k-最优的具有不交修复组的二元局部可修复码的构造。这部分内容对应于第四章。

本工作已投稿至《IEEE Transactions on Information Theory》。

2 有限域上的置换多项式（一）

2.1 介绍

本章的研究主题是有限域上的置换多项式。令 $\mathbb{F}_{p^n}$ 是含有 p^n 个元素的有限域，其中 p 是一个素数， n 是一个正整数。如果多项式 $f(x) \in \mathbb{F}_{p^n}[x]$ 能够诱导出一个从 $\mathbb{F}_{p^n}$ 到其自身的双射，则称 $f(x)$ 是 $\mathbb{F}_{p^n}$ 上的一个置换多项式。特别地，若 $f(x)$ 限制在子集 $A \subseteq \mathbb{F}_{p^n}$ 上也是 A 的一个双射，则称 $f(x)$ 是 A 上的一个置换多项式。由于在密码学、编码理论、组合设计理论[15–17,35,51,58] 等领域的应用，置换多项式受到了国内外学者的深入研究，并且取得了颇为丰硕的成果。例如，Ding等人[15]通过阶为 5 的Dickson置换多项式构造了一类斜Hadamard差集，推翻了长久以来的关于斜Hadamard差集的一个猜想。近年来，研究具有稀疏项数（特别是二项、三项）的置换多项式引起人们的广泛关注，最新进展可参见[14,26,29–31,34,36–39,41,73] 。

本章，我们构造了几类三项置换多项式，主要结果总结如下：

(A) 基于特殊方程的解的数目问题[14,16]，我们构造了如下两类三项置换多项式。

1. 令 $m > 1$ 是一个奇数，记 $k = \frac{m+1}{2}$ 。则对每个 $u \in \mathbb{F}_{2^m}^*$ ，有 $f(x) = x + u^{2^{k-1}-1}x^{2^k-1} + u^{2^{k-1}}x^{2^k+1}$ 是 $\mathbb{F}_{2^m}$ 上的一个置换多项式。

2. 令 $m > 1$ 是一个奇数，记 $k = \frac{m+1}{2}$ 。则对每个 $u \in \mathbb{F}_{2^m}^*$ ，有 $f(x) = x + ux^{2^k-1} + u^{2^k}x^{2^m-2^{k+1}+2}$ 是 $\mathbb{F}_{2^m}$ 上的一个置换多项式。

(B) 具有Niho指数的置换多项式的构造。

在文献[69] 中，Wu等人在 $\mathbb{F}_{5^n}$ 上构造了几类如下形式的具有Niho指数的三项置换多项式

$$f(x) = x + \lambda_1 x^{s(5^k-1)+1} + \lambda_2 x^{t(5^k-1)+1}, \tag{2-1}$$

其中 $n = 2k, 1 \le s, t \le 5^k$, 且 $\lambda_1, \lambda_2 \in \{1, -1\}$ 。与此同时，他们提出了下述两个猜想，并且可以轻松地从这两个猜想构造出两类新的具有形式 (2-1) 的三项置换多项式。我们的工作就是完全证明了这两个猜想。

猜想2.1.1 设 k 是一个奇数，则 $f(x)=x\left(\frac{x^2-x+2}{x^2+x+2}\right)^2$ 是 $\mathbb{F}_{5^k}$ 上的一个置换多项式。

猜想2.1.2 设 $q=5^k$ 且 k 是一个偶数，则 $g(x)=-x\left(\frac{x^2-2}{x^2+2}\right)^2$ 是 μ_{q+1} 的一个置换多项式，其中 $\mu_{q+1}=\{x\in\mathbb{F}_{q^2}:x^{q+1}=1\}$。

(C) 形如 $x+\gamma\mathrm{Tr}_n(x^k)$ 的置换多项式的构造。

2016年，Kyureghyan和Zieve[34]在计算机的辅助下，构造了若干类形如 $x+\gamma\mathrm{Tr}_n(x^k)$ 的置换多项式。这些无穷类几乎覆盖了计算机搜索到的所有例子，除了几个零星的例子。我们将其中的两个例子推广成了一类新的置换多项式。结果如下：

定理2.1.3 令 $q=3^r$，$r\geq 2$，且 $n=2$，$k=3^{2r-1}+3^r-3^{r-1}$。则 $f(x)=x+\gamma\mathrm{Tr}_2(x^k)$ 是 $\mathbb{F}_{q^2}$ 上的置换多项式，其中 $\gamma\in\mathbb{F}_{q^2}$ 满足 $(\gamma-1)^{\frac{q-1}{2}}=\gamma^{\frac{q-1}{2}}$。

本章的结构如下。第 2.2 节将详细介绍本章所涉及的定义符号，以及相关研究结果；第 2.3 节基于特殊方程的解的数目问题，我们构造了两类新的三项置换多项式；第 2.4 节将通过一些不同的技巧，如区分平方元和非平方元，证明上述两个猜想；第 2.5 节将构造一类形如$x+\gamma\mathrm{Tr}_{q^n/q}(x^k)$的置换多项式；最后，第 2.6 节对本章进行总结。

2.2 预备工作

本节中我们给出所涉及的定义符号，以及后续用到的引理。下面的符号仅适用本章。

- 令 q 是一个素数幂，n 是一个正整数，且 $\mathbb{F}_{q^n}$ 是含有 q^n 个元素的有限域。
- 令 $\mathrm{Tr}_r^n:\mathbb{F}_{q^n}\mapsto\mathbb{F}_{q^r}$ 是迹映射，定义为

$$\mathrm{Tr}_r^n(x)=x+x^{q^r}+x^{q^{2r}}+\cdots+x^{q^{n-r}},$$

  其中：$r|n$。当 $r=1$ 时，退化为绝对迹函数，记为Tr_n。
- 当 $x\in\mathbb{F}_{q^2}$，定义 $\overline{x}=x^q$。

现在，我们给出在后续文中用到的两个著名的引理。

引理2.2.1 [12] 设 $p>2$，则 x^2+ax+b 在 $\mathbb{F}_{p^n}$ 中不可约当且仅当它的判别式 $\Delta=a^2-4b$ 在 $\mathbb{F}_{p^n}$ 中是非平方元。

引理2.2.2 [40] 有限域 $\mathbb{F}_q$ 上的 n 次不可约多项式在 $\mathbb{F}_{q^k}$ 上仍不可约当且仅当 $\gcd(k,n)=1$。

2.3　两类三项置换多项式

通常来说，对有限域上的三项置换多项式给出一个简单的刻画条件是困难的。2015年，Ding等人[14]运用一些不同的技巧（包括由Dobbertin[16,17]提出的多变元方法）构造了若干类三项置换多项式。在本节中，我们运用类似的技巧构造了两类新的三项置换多项式。

定理2.3.1 令 $m>1$ 是一个奇数，记 $k=\frac{m+1}{2}$。则对每个 $u\in\mathbb{F}_{2^m}^*$，有 $f(x)=x+u^{2^{k-1}-1}x^{2^k-1}+u^{2^{k-1}}x^{2^k+1}$ 是 $\mathbb{F}_{2^m}$ 上的一个置换多项式。

证明 因为 $\gcd(2,2^m-1)=1$，所以我们只需要证明 $h(x)=(f(x))^2=x^2+u^{2^k-2}x^{2^{k+1}-2}+u^{2^k}x^{2^{k+1}+2}$ 是 $\mathbb{F}_{2^m}$ 上的一个置换多项式。令 $\overline{u}=u^{2^k}$，$y=x^{2^k}$。

首先，我们证明 $h(x)=0$ 当且仅当 $x=0$。显然，若 $x=0$，有 $h(x)=0$。反过来，如果存在 $x\in\mathbb{F}_{2^m}^*$ 满足

$$u^2x^4+\overline{u}y^2+\overline{u}u^2x^4y^2=0, \tag{2-2}$$

将方程 (2-2)两边同时取其 2^k 次幂，得到

$$\overline{u}^2y^4+u^2x^4+\overline{u}^2u^2x^4y^4=0.$$

由于 $\gcd(2,2^m-1)=1$，我们有

$$\overline{u}y^2+ux^2+\overline{u}ux^2y^2=0. \tag{2-3}$$

将方程 (2-2)和 (2-3)相加得

$$u^2x^4+ux^2+\overline{u}u^2x^4y^2+\overline{u}ux^2y^2=0, \tag{2-4}$$

上式可被分解为 $ux^2(1+ux^2)^{1+2^k}=0$。即 $x^2=\frac{1}{u}$，也就是，$x=\frac{1}{u^{2^{m-1}}}$。但是 $h(\frac{1}{u^{2^{m-1}}})=\frac{1}{u}\neq 0$，矛盾！所以 $h(x)=0$ 当且仅当 $x=0$。

下面，假设 $h(x)$ 不是一个置换多项式，则存在 $x\in\mathbb{F}_{2^m}^*$ 和 $a\in\mathbb{F}_{2^m}^*$ 使得 $h(x)=h(x+ax)$。令 $b=a^{2^k}$，显然有 $a,b\neq 0,1$。因为 $h(x)=h(x+ax)$，我们有

$$\frac{u^2x^4+\overline{u}y^2+\overline{u}u^2y^2x^4}{u^2x^2}=\frac{u^2(a^4+1)x^4+\overline{u}(b+1)^2y^2+\overline{u}u^2(b+1)^2y^2(a+1)^4x^4}{u^2(a+1)^2x^2},$$

化简得

$$A_1x^2y^2 + A_2y^2 + A_3x^2 = 0, \tag{2-5}$$

其中 $A_1 = (a^2b^2 + a^2 + b^2 + b)u\overline{u}, A_2 = (b^2 + b)\overline{u}$ 以及 $A_3 = (b + a^2)u$。

现在我们论断 $A_1A_2A_3 \neq 0$。事实上，若 $A_1 = 0$，则 $(b + 1)^2a^2 = b(b + 1)$。因此 $a^2 = \frac{b}{b+1}$，同时取其 2^k 次幂，则有 $b^2 = \frac{a^2}{a^2+1}$。所以 $b^2 = b$，即可得出 $b = 0$ 或者 1，矛盾！所以 $A_1 \neq 0$。同理可得 $A_2, A_3 \neq 0$。

对方程 (2-5)两边作用 2^k 次幂，我们可得出

$$A_1^{2^k}x^4y^2 + A_3^{2^k}y^2 + A_2^{2^k}x^4 = 0. \tag{2-6}$$

联立方程 (2-5) 和 (2-6)，消去 y^2，得到

$$B_1x^4 + B_2x^2 + B_3 = 0, \tag{2-7}$$

其中 $B_1 = A_3A_1^{2^k} + A_1A_2^{2^k} = (b^3(a + 1)^4)\overline{u}u^3 \neq 0$，$B_2 = A_2^{2^k+1} \neq 0$ 以及 $B_3 = A_3^{2^k+1} \neq 0$。

将 $x^2 = \frac{B_2}{B_1}\gamma$代入方程 (2-7)得

$$\gamma^2 + \gamma + D = 0, \tag{2-8}$$

其中 $D = \frac{B_1B_3}{B_2^2} = D_1 + D_1^{2^k}$ 且 $D_1 = \frac{A_1A_3^{2^k+1}}{A_2^{2^k+2}} = \frac{A_1B_3}{A_2B_2}$。并且我们有

$$\begin{aligned}
\mathrm{Tr}_m(D_1) &= \mathrm{Tr}_m\left(\frac{A_1}{A_2}(\frac{A_3}{A_2})^{2^k+1}\right) \\
&= \mathrm{Tr}_m\left((1 + a^2 + \frac{a^2}{b})\frac{(a^2 + b)(a + b)^2}{a^2(a + 1)^2b(b + 1)}\right) \\
&= \mathrm{Tr}_m\left(\frac{(a^2 + b)(a + b)^2}{a^2(a + 1)^2b(b + 1)} + \frac{(a^2 + b)(a + b)^2}{(a + 1)^2b(b + 1)} + \frac{(a^2 + b)(a + b)^2}{(a + 1)^2b^2(b + 1)}\right) \\
&= \mathrm{Tr}_m\left(\frac{a^2}{(a + 1)^2b(b + 1)} + \frac{1}{(a + 1)^2} + \frac{b^2}{a^2(a + 1)^2(b + 1)} + \frac{a^4}{(a + 1)^2b(b + 1)} + \frac{a^2}{(a + 1)^2} + \right. \\
&\left. \frac{b^2}{(a + 1)^2(b + 1)} + \frac{a^4}{(a + 1)^2b^2(b + 1)} + \frac{a^2}{b(a + 1)^2} + \frac{b}{(a + 1)^2(b + 1)}\right) \\
&= \mathrm{Tr}_m\left(\frac{a^2}{(a + 1)^2b(b + 1)} + \frac{a^2}{b(a + 1)^2} + \frac{b}{(a + 1)^2(b + 1)}\right) + \mathrm{Tr}_m\left(\frac{1}{(a + 1)^2} + \frac{a^2}{(a + 1)^2}\right) \\
&+ \mathrm{Tr}_m\left(\frac{b^2}{a^2(a + 1)^2(b + 1)} + \frac{a^4}{(a + 1)^2b(b + 1)} + \frac{b^2}{(a + 1)^2(b + 1)} + \frac{a^4}{(a + 1)^2b^2(b + 1)}\right) \\
&= 1.
\end{aligned}$$

对方程 (2-8)两边作用 2^i 次幂，$0 \leq i \leq d - 1$，然后将这些方程相加得

$$\gamma^{2^k} = \gamma + \sum_{i=0}^{k-1}(D_1 + D_1^{2^k})^{2^i} = \gamma + D_1 + \mathrm{Tr}_m(D_1) = \gamma + D_1 + 1. \tag{2-9}$$

上式两边同时乘以 γ，并且考虑到 $\gamma^2+\gamma+D=0$，则有

$$\gamma^{2^k+1}=D_1\gamma+D. \tag{2-10}$$

联立方程 (2-5)、(2-9)和 (2-10)，我们有

$$C_1\gamma+C_2=0, \tag{2-11}$$

其中 $C_1=A_1A_2^{2^k+2}\neq 0$ 以及 $C_2=A_2^2B_1\neq 0$。因此 $\gamma=\frac{C_2}{C_1}$。所以由方程 (2-8)可得

$$B_1A_2^2+A_1A_2B_2=A_1^2B_3,$$

这就导出

$$b^2(b^2+a^4)=a^4(b^4+a^2).$$

注意到 $\gcd(2,2^m-1)=1$，则

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

对上面的方程同时取其 2^k 次幂，可以得到

$$a^4b^2+a^4+a^2b^2+b^3=0.$$

则可推出

$$b^2(a^4+b)=a^2(a^2+b^2)=(a^3+a^2b)(a+b)=b^2(1+a^2)(a+b).$$

所以

$$b=\frac{a^3+a^2+1}{a},$$

并且对其作用 2^k 次幂，我们可以导出

$$a^8+a^7+a^6+a^5+a^4+a^2+1=0.$$

由于 $x^8+x^7+x^6+x^5+x^4+x^2+1$ 是 $\mathbb{F}_2$ 上的不可约多项式，则由引理 2.2.2知，$x^8+x^7+x^6+x^5+x^4+x^2+1$在 $\mathbb{F}_{2^m}$ 上也不可约。因此 $a\notin\mathbb{F}_{2^m}^*$，矛盾! □

定理2.3.2 令 $m>1$ 是一个奇数，记 $k=\frac{m+1}{2}$。则对每个 $u\in\mathbb{F}_{2^m}^*$，有 $f(x)=x+ux^{2^k-1}+u^{2^k}x^{2^m-2^{k+1}+2}$ 是 $\mathbb{F}_{2^m}$ 上的一个置换多项式。

证明 我们首先证明 $f(x)=0$ 当且仅当 $x=0$。令 $\overline{u}=u^{2^k}$， $y=x^{2^k}$。显然，如果 $x=0$，那么 $f(x)=0$。反过来，假设存在某个 $x\in\mathbb{F}_{2^m}^*$ 使得

$$x^2y^2+uy^3+\overline{u}x^4=0. \tag{2-12}$$

将其两边同时作用 2^k 次幂，我们有

$$x^4y^2+u^2y^4+\overline{u}x^6=0. \tag{2-13}$$

对方程 (2-12)的两边都乘以 x^2，我们得到

$$x^4y^2+ux^2y^3+\overline{u}x^6=0. \tag{2-14}$$

将方程 (2-13)和 (2-14)相加可得

$$ux^2y^3+u^2y^4=0.$$

则有 $x^2=uy$。所以 $x=u^{2^{k-1}+1}$。然而，经计算 $f(u^{2^{k-1}+1})=u^{2^{k-1}+1}\neq 0$，矛盾！因此 $f(x)=0$ 当且仅当 $x=0$。

接下来，令 $\overline{a}=a^{2^k}$。我们将证明对每个非零元 $a\in\mathbb{F}_{2^m}$，方程 $f(x)=a$ 有唯一的非零解。即，对于方程

$$x^2y^2+uy^3+\overline{u}x^4+axy^2=0, \tag{2-15}$$

存在唯一解 $x\in\mathbb{F}_{2^m}^*$。将方程 (2-15)的两边同时取其 2^k 次幂，得到

$$x^4y^2+\overline{u}x^6+u^2y^4+\overline{a}x^4y=0, \tag{2-16}$$

对方程 (2-15)的两边乘以 x^2，则有

$$x^4y^2+ux^2y^3+\overline{u}x^6+ax^3y^2=0. \tag{2-17}$$

将方程 (2-16)和 (2-17)相加之后再除以 y，我们有

$$u^2y^3+ux^2y^2+\overline{a}x^4+ax^3y=0. \tag{2-18}$$

计算 (2-15)$\times u+$ (2-18)，然后除以 x，则可得到

$$(\overline{a}+u\overline{u})x^3+ax^2y+auy^2=0. \tag{2-19}$$

对方程 (2-19)的两边作用 2^k 次幂，然后与 $\overline{a}\times$ (2-15) 相加，我们有

$$(\overline{a}+\overline{u}u^2+\overline{a}u)y+a\overline{a}x=0. \tag{2-20}$$

联立方程 (2-19)和 (2-20)，求解得

$$x = \frac{a^3\overline{a}^2}{b\overline{b}}, \tag{2-21}$$

其中，$b = a^2 + \overline{u}u^2 + \overline{a}u$ ，$\overline{b} = b^{2^k}$，并且可以直接验证知 b 为非零元。因此 (2-21) 就是方程 $f(x) = a$ 的唯一非零解! □

2.4　猜想 2.1.1和 2.1.2的证明

2.4.1　猜想 2.1.1的证明

在本小节中，我们将证明Wu等人在文献[69] 中提出的猜想 2.1.1，叙述成如下定理。

定理2.4.1 (猜想 2.1.1[69]) 设 k 是一个奇数，则 $f(x) = x\left(\frac{x^2-x+2}{x^2+x+2}\right)^2$ 是 $\mathbb{F}_{5^k}$ 上的一个置换多项式。

在证明这个猜想之前，我们需要下面的两个引理。令 $\Omega_1 = \{x^2 : x \in \mathbb{F}_{5^k}^*\}$，$\Omega_2 = \{2x^2 : x \in \mathbb{F}_{5^k}^*\}$。

引理2.4.2 $f(x)$ 是 Ω_1 上的一个置换多项式。

证明 若不然，则存在两个不同的元素 $x, y \in \Omega_1$ 使得 $f(x) = f(y)$。 令 $x = a^2$， $y = b^2$，其中 $a, b \in \mathbb{F}_{5^k}^*$ 且 $a \neq \pm b$。 我们有 $f(a^2) = f(b^2)$。 也就是说

$$a^2\Big(\frac{a^4 - a^2 + 2}{a^4 + a^2 + 2}\Big)^2 = b^2\Big(\frac{b^4 - b^2 + 2}{b^4 + b^2 + 2}\Big)^2.$$

我们得到

$$\frac{a^5 - a^3 + 2a}{a^4 + a^2 + 2} = \pm\frac{b^5 - b^3 + 2b}{b^4 + b^2 + 2}.$$

情形 1： $\frac{a^5-a^3+2a}{a^4+a^2+2} = \frac{b^5-b^3+2b}{b^4+b^2+2}$。

经过一些简单的化简，我们有

$$(a-b)\Big(a^4b^4 + 2(a-b)^4 + (a^2b^2 - 2ab - 2)(a^2 + ab + b^2) + a^3b^3 - a^2b^2 - 2ab + 4\Big) = 0.$$

令 $c = ab$， $d = a - b$。 注意到 $a \neq b$， 则可得到

$$c^4 + 2d^4 + (c^2 - 2c - 2)(d^2 - 2c) + c^3 - c^2 - 2c + 4 = 0.$$

化简上述方程得到

$$d^4-(2c^2+c+1)d^2-2c^4+2c^3-c^2+c+2=0.$$

令 $z=d^2\in\mathbb{F}_{5^k}^*$， 则

$$z^2-(2c^2+c+1)z-2c^4+2c^3-c^2+c+2=0. \tag{2-22}$$

由引理 2.2.1，我们知道 $z^2-(2c^2+c+1)z-2c^4+2c^3-c^2+c+2$ 在$\mathbb{F}_{5^k}$上不可约当且仅当其判别式 Δ 为非平方元。简单计算知 $\Delta=2(c^2-c-2)^2$。

子情形 1.1: 若 $c^2-c-2\neq 0$，因为 2 是非平方元，所以 Δ 是 $\mathbb{F}_{5^k}$ 上的非平方元。因此方程 (2-22)在$\mathbb{F}_{5^k}$中无解。

子情形 1.2: 若 $c^2-c-2=0$， 则 $c=2$ 或者 $c=-1$。 下面分类讨论：

当 $c=2$ 时， $d^2=-2$。 那么有如下方程组

$$\begin{cases} xy=a^2b^2=c^2=-1, \\ x+y=a^2+b^2=(a-b)^2+2ab=d^2+2c=2. \end{cases} \tag{2-23}$$

所以 x,y 是方程 $u^2-2u-1=0$ 的两个根。然而，注意到 u^2-2u-1 的判别式 $\Delta=3$ 是 $\mathbb{F}_{5^k}$ 中的非平方元，由引理 2.2.1可知， u^2-2u-1 在 $\mathbb{F}_{5^k}$ 上是不可约的。故方程 $u^2-2u-1=0$ 在 $\mathbb{F}_{5^k}$ 中无解，矛盾!

当 $c=-1$ 时， $d^2=1$。 那么可得方程组

$$\begin{cases} xy=1, \\ x+y=-1. \end{cases} \tag{2-24}$$

所以 x,y 是方程 $u^2+u+1=0$ 的两个根。然而，注意到 u^2+u+1 的判别式 $\Delta=2$ 是 $\mathbb{F}_{5^k}$ 中的非平方元，由引理 2.2.1可知， u^2+u+1 在 $\mathbb{F}_{5^k}$ 上是不可约的。故方程 $u^2+u+1=0$ 在 $\mathbb{F}_{5^k}$ 中无解，矛盾!

情形 2： $\frac{a^5-a^3+2a}{a^4+a^2+2}=-\frac{b^5-b^3+2b}{b^4+b^2+2}$。

观察到 $-\frac{b^5-b^3+2b}{b^4+b^2+2}=\frac{(-b)^5-(-b)^3+2(-b)}{(-b)^4+(-b)^2+2}$， 易知这种情形的证明几乎和**情形 1**一样，主要的不同在于将**情形 1**中的 b 用 $-b$ 代替。记 $c=-ab$， $d=a+b$ 且 $z=d^2$。 剩下的论述和**情形 1**一样，故略掉。 □

引理2.4.3 $f(x)$ 是 Ω_2 上的一个置换多项式。

证明 运用证明引理 2.4.2的方法可以类似证明这个引理。由于论述过程几乎照搬，故略掉。□

定理2.4.1的证明 注意到 $\Omega_1 \cap \Omega_2 = \varnothing$ 且 $\Omega_1 \cup \Omega_2 = \mathbb{F}_{5^k}^*$。而且容易知道 $f(\Omega_1) \subseteq \Omega_1$，$f(\Omega_2) \subseteq \Omega_2$。因此我们只需证明 $f(x)$ 在Ω_1, Ω_2 上都是置换多项式即可。这可由引理2.4.2和2.4.3直接推出。□

2.4.2　猜想 2.1.2的证明

在本小节中，我们将证明Wu等人在文献[69] 中提出的猜想 2.1.2，叙述成如下定理。

定理2.4.4 (猜想 2.1.2[69]) 设 $q = 5^k$ 且 k 是一个偶数，则 $g(x) = -x\left(\frac{x^2-2}{x^2+2}\right)^2$ 是 μ_{q+1} 的一个置换多项式，其中 $\mu_{q+1} = \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}$。

在证明这个猜想之前，我们需要下面的一系列引理。

引理2.4.5 设 $q = 5^k$ 且 k 是一个偶数，则 ± 2 是 $\mathbb{F}_{q^2}$ 中的平方元；进一步有，$\sqrt{\pm 2} \in \mathbb{F}_q$。

证明 设 $\mathbb{F}_{q^2}^* = \langle \omega \rangle$。注意到 $8|(q^2-1)$ 且 $-1 = \omega^{\frac{q^2-1}{2}}$，我们有 $2 = \omega^{\frac{q^2-1}{4}}$ 或者 $2 = \omega^{\frac{3(q^2-1)}{4}}$。则在这两种情况下，2 均为 $\mathbb{F}_{q^2}$ 中的平方元。所以 -2 也是 $\mathbb{F}_{q^2}$ 中的平方元。

不失一般性，我们记 $\sqrt{2} = \omega^{\frac{q^2-1}{8}}$，$\sqrt{-2} = \omega^{\frac{3(q^2-1)}{8}}$。因为 k 是一个偶数，所以 $8|(q-1)$。因此，我们得到 $(\sqrt{2})^{q-1} = (-1)^{\frac{q-1}{4}} = 1$ 且 $(\sqrt{-2})^{q-1} = (-1)^{\frac{3(q-1)}{4}} = 1$，这就表明 $\sqrt{2} \in \mathbb{F}_q$，$\sqrt{-2} \in \mathbb{F}_q$。□

令 $\Omega_+ = \{x^2 : x \in \mu_{q+1}\}$，$\Omega_- = \{-x^2 : x \in \mu_{q+1}\}$。

引理2.4.6 $\Omega_+ \cap \Omega_- = \varnothing$，$\Omega_+ \cup \Omega_- = \mu_{q+1}$。

证明 如果 $\Omega_+ \cap \Omega_- \neq \varnothing$，即存在 $x_1, x_2 \in \mu_{q+1}$ 使得 $x_1^2 = -x_2^2$。那么我们有 $\left(\frac{x_1}{x_2}\right)^2 = -1$，这就意味着$\left(\frac{x_1}{x_2}\right)^4 = 1$。因为 $\left(\frac{x_1}{x_2}\right)^{q+1} = 1$，所以 $\left(\frac{x_1}{x_2}\right)^{\gcd(4,q+1)} = 1$。因此 $\left(\frac{x_1}{x_2}\right)^2 = 1$，这与 $x_1^2 = -x_2^2$ 矛盾。

进一步，由定义和上述证明显然有 $|\Omega_+| = |\Omega_-| = \frac{q+1}{2}$。因此 $\Omega_+ \cup \Omega_- = \mu_{q+1}$。□

引理2.4.7 $g(\Omega_+) \subseteq \Omega_+$，$g(\Omega_-) \subseteq \Omega_-$。

证明 $\forall x \in \Omega_+$， $\exists a \in \mu_{q+1}$， 使得 $x = a^2$。 我们只需证明存在某个 $b \in \mu_{q+1}$， 使得 $g(x) = b^2$。 事实上， $g(x) = g(a^2) = -a^2\big(\frac{a^4-2}{a^4+2}\big)^2 = \Big(2a\big(\frac{a^4-2}{a^4+2}\big)\Big)^2$。 令 $b = 2a\big(\frac{a^4-2}{a^4+2}\big)$。 注意到 $\overline{a} = \frac{1}{a}$， 我们有

$$\overline{b} = 2\overline{a}\Big(\frac{\overline{a}^4-2}{\overline{a}^4+2}\Big) = \frac{2}{a}\Big(\frac{(\frac{1}{a})^4-2}{(\frac{1}{a})^4+2}\Big) = \frac{1}{2a}\big(\frac{a^4+2}{a^4-2}\big) = \frac{1}{b}.$$

同理，我们有 $g(\Omega_-) \subseteq \Omega_-$。 事实上， $\forall x \in \Omega_-$，$\exists a \in \mu_{q+1}$， 使得$x = -a^2$。 因为 $g(x) = g(-a^2) = a^2\big(\frac{a^4-2}{a^4+2}\big)^2 = -\Big(2a\big(\frac{a^4-2}{a^4+2}\big)\Big)^2$。 令 $b = 2a\big(\frac{a^4-2}{a^4+2}\big)$。 易知$b \in \mu_{q+1}$，这就证明了 $g(x) \in \Omega_-$。 □

引理2.4.8 方程组

$$\begin{cases} xy = 1, \\ x + y = \pm 1, \end{cases}$$

在 Ω_+和 Ω_- 中都无解。

证明 若不然，存在 $x, y \in \Omega_+$ (或者 Ω_-) 满足方程组，那么 $x^2 \pm x + 1 = 0$。 所以由引理2.4.5知 $x = \pm 2 \pm 2\sqrt{2} \in \mathbb{F}_q$ 。因此，我们得到 $x^{q-1} = 1$。 又因为 $x^{q+1} = 1$， 则有 $x^{\gcd(q-1,q+1)} = 1$， 即 $x = \pm 1$， 这与 $x^2 \pm x + 1 = 0$矛盾。 □

引理2.4.9 $g(x)$ 是 Ω_+ 上的置换多项式。

证明 假设命题不成立，则存在两个不同的元素 $x, y \in \Omega_+$ 使得 $g(x) = g(y)$。 令 $x = a^2$，$y = b^2$ ，其中 $a, b \in \mu_{q+1}$ 且 $a \neq \pm b$。 因为 $g(x) = g(y)$， 我们有 $-a^2\big(\frac{a^4-2}{a^4+2}\big)^2 = -b^2\big(\frac{b^4-2}{b^4+2}\big)^2$，这意味着 $\frac{a^5-2a}{a^4+2} = \pm\frac{b^5-2b}{b^4+2}$ 。

下面，我们分 $\frac{a^5-2a}{a^4+2} = \frac{b^5-2b}{b^4+2}$ 和 $\frac{a^5-2a}{a^4+2} = -\frac{b^5-2b}{b^4+2}$ 这两种情况讨论。

情形 1: $\frac{a^5-2a}{a^4+2} = \frac{b^5-2b}{b^4+2}$。

我们有

$$(a-b)\Big(a^4b^4 + 2(a-b)^4 + 2ab(a-b)^2 - 4a^2b^2 - 4\Big) = 0,$$

这就推出

$$a^4b^4 + 2(a-b)^4 + 2ab(a-b)^2 - 4a^2b^2 - 4 = 0,$$

令 $c = ab$ ， $d = a - b$ 。因为 $a \neq b$ ，所以我们得到

$$c^4 + 2d^4 + 2cd^2 - 4c^2 - 4 = 0,$$

化简得

$$d^4 + cd^2 - 2(c^4 + c^2 + 1) = 0.$$

因为 $\Delta = -2(c^2-1)^2$ 在 $\mathbb{F}_{q^2}$ 中是一个平方元，因此

$$d^2 = 2c \pm 2\sqrt{-2}(c^2 - 1), \tag{2-25}$$

将方程 (2-25) 的两边同时取其 q 次幂得到

$$\overline{d}^2 = 2\overline{c} \pm 2\sqrt{-2}(\overline{c}^2 - 1).$$

因为 $\overline{c} = \frac{1}{c}$ 且$\overline{d} = \overline{a} - \overline{b} = \frac{1}{a} - \frac{1}{b} = \frac{b-a}{ab} = \frac{-d}{c}$ ，我们得到

$$\frac{d^2}{c^2} = \frac{2}{c} \pm 2\sqrt{-2}(\frac{1}{c^2} - 1),$$

则可推出

$$d^2 = 2c \pm 2\sqrt{-2}(1 - c^2). \tag{2-26}$$

联立方程 (2-25)和 (2-26)，我们得到 $c^2 = 1$ 。因此，

$$d^2 = 2c = \begin{cases} 2, \text{ 如果 } c = 1, \\ -2, \text{ 如果 } c = -1。 \end{cases}$$

1. 当 $c = 1$ 时， $d^2 = 2$， 我们有

$$\begin{cases} xy = a^2b^2 = c^2 = 1, \\ x + y = a^2 + b^2 = (a-b)^2 + 2ab = d^2 + 2c = -1. \end{cases} \tag{2-27}$$

由引理 2.4.8知，方程组 (2-27)在 Ω_+ 中无解，矛盾!

2. 当 $c = -1$ 时， $d^2 = -2$， 我们有

$$\begin{cases} xy = 1, \\ x + y = 1. \end{cases} \tag{2-28}$$

由引理 2.4.8知，方程组 (2-28)在 Ω_+ 中无解，矛盾!

情形 2: $\frac{a^5-2a}{a^4+2} = -\frac{b^5-2b}{b^4+2}$。

注意到 $-\frac{b^5-2b}{b^4+2} = \frac{(-b)^5-2(-b)}{(-b)^4+2}$， 易知这种情形的证明几乎和**情形 1**一样，主要的不同在于将**情形 1**中的 b 用 $-b$ 代替。记 $c = -ab$ 且 $d = a + b$ 。剩下的论述和**情形 1**完全一样，故略掉。 □

引理2.4.10 $g(x)$ 是 Ω_- 上的置换多项式。

证明 可以运用证明引理 2.4.9的方法来证明这个引理。事实上，如果结论不成立，则存在两个不同的元素 $x, y \in \Omega_-$ 使得 $g(x) = g(y)$。 令 $x = -a^2$， $y = -b^2$， 其中 $a, b \in \mu_{q+1}$ 且 $a \neq \pm b$。 因为 $g(x) = g(y)$ ，我们得到 $a^2\left(\frac{a^4-2}{a^4+2}\right)^2 = b^2\left(\frac{b^4-2}{b^4+2}\right)^2$， 这意味着 $\frac{a^5-2a}{a^4+2} = \pm\frac{b^5-2b}{b^4+2}$。剩下的论述和引理 2.4.9几乎完全一样，除了改变一下 $x+y$ 的符号，因为 $x+y = -(a^2+b^2)$，但是这不影响后面的论证。 □

定理2.4.4的证明 由引理 2.4.6、2.4.7、2.4.9和2.4.10可直接推出。 □

2.5 形如 $x + \gamma\mathbf{Tr}_n(x^k)$ 的置换多项式的构造

2016年，Kyureghyan和Zieve[34]在计算机的辅助下，搜索了当 $n > 1$, $q^n < 5000$ 时，有限域 $\mathbb{F}_{q^n}$ 上所有具有形式 $x + \gamma\mathrm{Tr}_n(x^k)$ 的置换多项式，其中 $\gamma \in \mathbb{F}_{q^n}^*$。 他们构造了若干无穷类的置换多项式。这些无穷类几乎覆盖了计算机搜索的所有例子，除了下面五个例子。

例2.5.1 $q = 7,\ n = 2,\ k = 10,\ \gamma^4 = 1.$

例2.5.2 $q = 9,\ n = 2,\ k = 33,\ \gamma^2 - \gamma = 1.$

例2.5.3 $q = 27,\ n = 2,\ k = 261,\ (\gamma - 1)^{13} = \gamma^{13}.$

例2.5.4 $q = 9,\ n = 3,\ k = \{11, 19, 33, 57\},\ \gamma^4 = -1.$

例2.5.5 $q = 49,\ n = 2,\ k = 385,\ \gamma^5 = -1.$

一个自然的问题就是如何将这些零星的例子推广成无穷类。本节主要的内容是：将其中的例 2.5.2和 2.5.3 推广成了一类新的置换多项式。

定理2.5.6 令 $q = 3^r$， $r \geq 2$， 且 $n = 2$， $k = 3^{2r-1} + 3^r - 3^{r-1}$。 则 $f(x) = x + \gamma\mathrm{Tr}_2(x^k)$ 是 $\mathbb{F}_{q^2}$ 上的置换多项式，其中 $\gamma \in \mathbb{F}_{q^2}$ 满足 $(\gamma - 1)^{\frac{q-1}{2}} = \gamma^{\frac{q-1}{2}}$ 。

证明 显然 $f(0)=0$，我们只需要证明对每个 $a\in\mathbb{F}_{q^2}^*$, 方程 $f(x)=a$ 都至多有一个非零解。也就是说方程

$$x+\gamma(x^k+\overline{x}^k)=a, \tag{2-29}$$

至多有一个解 $x\in\mathbb{F}_{q^2}$。 将方程(2-29)的两边同时取其 3 次幂，并且考虑到 $\overline{x}^q=x^{q^2}=x$，有

$$x^3+\gamma^3(x\overline{x}^2+\overline{x}x^2)=a^3. \tag{2-30}$$

因为 $(\gamma-1)^{\frac{q-1}{2}}=\gamma^{\frac{q-1}{2}}$， 我们可以轻松地得到 $\gamma\in\mathbb{F}_q$。对方程 (2-30)的两边同时取 q 次幂，那么有

$$\overline{x}^3+\gamma^3(\overline{x}x^2+x\overline{x}^2)=\overline{a}^3. \tag{2-31}$$

对方程 (2-30)和方程 (2-31)做差，可得到 $(x-\overline{x})^3=(a-\overline{a})^3$。 因为 $\gcd(3,q^2-1)=1$，所以

$$\overline{x}=x+\overline{a}-a. \tag{2-32}$$

将方程 (2-32)代入方程 (2-30)，经过简单的化简，可以得到

$$x^3+\left(\frac{\gamma}{1-\gamma}\right)^3(\overline{a}-a)^2x=\left(\frac{a}{1-\gamma}\right)^3. \tag{2-33}$$

因此， x 是方程(2-29)的解当且仅当它也是如下方程组的解

$$\begin{cases} x^3+\left(\frac{\gamma}{1-\gamma}\right)^3(\overline{a}-a)^2x &= \left(\frac{a}{1-\gamma}\right)^3, \\ \overline{x}-x &= \overline{a}-a. \end{cases} \tag{2-34}$$

下面，我们将证明方程组 (2-34)至多有一个解。假设它有两个不同的解，记为 x_1,x_2。由于 $\overline{x_1}-x_1=\overline{a}-a=\overline{x_2}-x_2$， 我们得到 $\overline{x_1-x_2}=x_1-x_2$， 即 $x_1-x_2\in\mathbb{F}_q$。设 $c=x_1-x_2\in\mathbb{F}_q^*$， 则 x_2+c,x_2,x_2-c 是方程组 (2-34)的第一个方程的三个解。那么有 $c^2=\left(\frac{\gamma}{\gamma-1}\right)^3(\overline{a}-a)^2$。 注意到 $Y=\{\gamma\in\mathbb{F}_{q^2}|(\gamma-1)^{\frac{q-1}{2}}=\gamma^{\frac{q-1}{2}}\}\subset\mathbb{F}_q^*$。令 $z=\frac{\gamma}{\gamma-1}$， 我们有 $Z=\{z\in\mathbb{F}_{q^2}|z^{\frac{q-1}{2}}=1\}=\langle\omega^{2(q+1)}\rangle\setminus\{1\}\subset\mathbb{F}_q^*$， 其中 w 是 $\mathbb{F}_{q^2}$ 的一个本原元。

因此，存在某个 j，使得 $c=\pm d(\overline{a}-a)$， 其中 $d=w^{3j(q+1)}\in\mathbb{F}_q$。对方程 $c=\pm d(\overline{a}-a)$ 的两边同时取 q 次幂，可以得到 $\overline{c}=\pm d(a-\overline{a})=-c$， 这与 $c\in\mathbb{F}_q^*$ 矛盾! □

注2.5.7 当 $q=9,\ n=2,\ k=33$ 时，上述定理中 γ 的条件与例子 *2.5.2*中的条件 $\gamma^2-\gamma=1$ 有稍微的不同，其实这是很好理解的。注意到 $(\gamma-1)^4=\gamma^4$，可推出 $(\gamma+1)(\gamma^2-\gamma-1)=0$。这意味着两个条件差一个 $\gamma=-1$ 的情况。事实上， $q=9,\ n=2,\ k=33,\ \gamma=-1$这种情形已经包含在在文献[34]中的一类置换多项式里了。

2.6 小结

本章的研究主题是有限域上的置换多项式。首先，我们运用一些不同的技巧（如Dobbertin[16,17]提出的多变元方法）构造了两类新的三项置换多项式。然后通过初等数论中的一些方法，我们解决了由Wu 等人[69]提出的两个猜想。最后我们构造了一类具有形式 $x+\gamma \mathrm{Tr}_n(x^k)$ 的置换多项式，解决了Kyureghyan和Zieve[34]遗留的五个例子中的两个。自然地，一个仍待解决的问题就是，怎么将例 2.5.1，2.5.4和 2.5.5推广成无穷类。如果这个问题能够解决，我们就可以对有限域 $\mathbb{F}_{q^n}$ 上具有形式 $x+\gamma \mathrm{Tr}_n(x^k)$ 的置换多项式有一个全面的理解，基于此，我们提出如下的公开问题:

问题2.6.1 *是否有可能将例 2.5.1，2.5.4和 2.5.5推广成具有形式 $x+\gamma \mathrm{Tr}_n(x^k)$ 的无穷类？*

3 有限域上的置换多项式（二）

3.1 介绍

本章内容是上一章内容的延续，我们的研究对象仍然是有限域上的置换多项式，但是，本章主要侧重的是对于一些具有特殊性质的置换多项式的研究。具体分为：完全置换多项式和低差分度的置换多项式。

如果多项式 $f(x)$ 和 $f(x)+x$ 都是有限域 $\mathbb{F}_{p^n}$ 上的置换多项式，则称 $f(x)$ 为完全置换多项式（Complete permutation polynomial）。这类多项式是由Niederreiter和Robinson[44]提出。自然地，人们从最简单的多项式开始研究，即判断哪些单项式是完全置换多项式。

设 d 是一个正整数， $\alpha \in \mathbb{F}_{p^n}^*$， 单项式 αx^d 是 $\mathbb{F}_{p^n}$ 上的一个完全置换多项式当且仅当 $\gcd(d, q-1)=1$ 且 $\alpha x^d + x$ 是一个置换多项式。我们称这样的一个整数 d 为完全置换多项式指数。近年来，对于完全置换多项式指数的研究也取得了很多有趣的结果。Charpin和Kyureghyan[11]证明了当 k 是奇数时，在 $\mathbb{F}_{2^{2k}}$ 上， 2^k+2 是一个完全置换多项式指数。Tu等人[64]给出了 $\mathbb{F}_{2^n}$ 上的一类Niho型的完全置换多项式指数。Wu等人[71]提出了两类新的单项完全置换多项式和一类多项的完全置换多项式。更多关于完全置换多项式的结果可参考文献[63,70,74]。

在本章中，我们构造了四类单项完全置换多项式和一类三项完全置换多项式，具体结果如下：

1. 令 p 是一个奇素数， $r+1=p$ 且 $d=\frac{p^{rk}-1}{p^k-1}+1$。那么 $a^{-1}x^d$ 是 $\mathbb{F}_{p^{rk}}$ 上的一个完全置换多项式，其中 $a \in \mathbb{F}_{p^{rk}}^*$ 满足 $a^{p^k-1}=-1$ 。

2. 设 $n=6k$，其中 k 是一个正整数且 $\gcd(k,3)=1$ 。那么 $d=2^{4k-1}+2^{2k-1}$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式指数。具体来讲， $a^{-1}x^d$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式，其中 $a \in \{\omega^{t(2^{2k}-1)} | 0<t\le 2^{2k}+2^{4k},\ 3 \nmid t\}$ 。

3. 设 $n=4k$ ，则 $d=(1+2^{2k-1})(1+2^{2k})+1$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式指数。具体来讲，如果 a 是 $\mathbb{F}_{2^{2k}}^*$ 上的非立方元，那么 $a^{-1}x^d$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式。

4. 令 p 是一个奇素数且 $n=4k$，则 $d=\frac{p^{4k}-1}{2}+p^{2k}$ 是 $\mathbb{F}_{p^n}$ 上的一个完全置换多项式指数。具体来讲，$a^{-1}x^d$ 是 $\mathbb{F}_{p^n}$ 上的一个完全置换多项式，其中 $a\in\{\omega^{t(p^{2k}-1)+\frac{p^{2k}-1}{2}}: 0\le t\le p^{2k}\}$。

5. 令 p 是一个奇素数，则 $f(x)=-x+x^{\frac{p^{2m}+1}{2}}+x^{\frac{p^{2m}+1}{2}p^m}$ 是 $\mathbb{F}_{p^{3m}}$ 上的一个完全置换多项式。

第 1 类完全置换多项式解决了由Wu等人[71]提出的一个猜想，我们解决这一问题的关键就是对于AGW准则[1]的灵活运用。通过运用所在有限域上的加法特征，我们给出了三类新的单项完全置换多项式。第 5 类的具体构造基于特殊方程的解的数目问题。

具有低差分均匀度的函数，由于其能较好地抵抗差分攻击，在密码学上备受关注。Blondeau等人[9]系统地研究了幂函数的差分性质，并提出下述的猜想：

猜想3.1.1 [9] 令 $n=2m$ 且 m 是奇数。设 $F_d: x\to x^d$ 是 $\mathbb{F}_{2^n}$ 上的单项置换多项式，其中 d 的定义如下：

(1) $d=2^m+2^{(m+1)/2}+1$,

(2) $d=2^{m+1}+3$。

则对这些 d，F_d 是一个 8-差分函数，且 0、2、4、6、8 都出现在它的差分谱里。

确定函数的差分均匀度是一个困难的问题，在本章中，我们对这个猜想做出了一定的推进工作，证明了这些多项式的差分均匀度至多为 10 。

本章的框架如下：第 3.2 节，我们介绍一些基本的符号定义和相关结论；第 3.3 节，给出了四类单项完全置换多项式的构造；第 3.4 节，我们构造了一类三项完全置换多项式和两类置换多项式；第 3.5 节，考察了幂函数的差分性质；第 3.6 节对本章做一个小结。

3.2 预备工作

下面的符号定义仅适用于本章。

- 令 q 是一个素数幂，n 是一个正整数，且 $\mathbb{F}_{q^n}$ 是含有 q^n 个元素的有限域。
- 令 $\mathrm{Tr}_r^n: \mathbb{F}_{q^n}\mapsto\mathbb{F}_{q^r}$ 是迹映射，定义为：

$$\mathrm{Tr}_r^n(x)=x+x^{q^r}+x^{q^{2r}}+\cdots+x^{q^{n-r}},$$

其中：$r|n$。当 $r=1$ 时，退化为绝对迹函数，记为 Tr_n。

- 令 $\mathrm{N}_r^n : \mathbb{F}_{p^n} \mapsto \mathbb{F}_{p^r}$ 是范数映射，定义为：

$$\mathrm{N}_r^n(x) = x x^{p^r} x^{p^{2r}} \cdots x^{p^{n-r}},$$

其中： $r|n$ 。当 $r = 1$ 时，退化为绝对范数函数，记为 N_n。

- 令 $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ 是 p 次单位根，且 $\chi_n(x) = \zeta_p^{\mathrm{Tr}_n(x)}$ 是有限域 $\mathbb{F}_{p^n}$ 上的典范加法特征。

- 当 $x \in \mathbb{F}_{q^2}$ ，定义 $\overline{x} = x^q$ 为 x 的共轭。

首先，我们先回忆一个利用所在域上的加法特征来判断置换多项式的准则。

引理3.2.1 [40] 映射 $f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_{p^n}$ 是置换多项式当且仅当对每个 $\alpha \in \mathbb{F}_{p^n}^*$ ，有

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_n(\alpha f(x)) = 0.$$

令 n, r, k 是满足 $n = rk$ 的一些整数。对任何 $a \in \mathbb{F}_{p^n}$ ，设 $a_i = a^{p^{ik}}$ ，其中 $0 \le i \le r-1$。我们定义：

$$h_a(x) = x \prod_{i=0}^{r-1} (x + a_i).$$

那么我们有下述的引理。

引理3.2.2 [71] 设 $n = rk$ 且 $d = \frac{p^{rk}-1}{p^k-1} + 1$ 。则 $x^d + ax \in \mathbb{F}_{p^n}[x]$ 是$\mathbb{F}_{p^n}$ 上的置换多项式当且仅当 $h_a(x) \in \mathbb{F}_{p^k}[x]$ 是 $\mathbb{F}_{p^k}$ 上的置换多项式。

下面的一系列引理将会在后面的小节中用到。

引理3.2.3 (AGW准则[1]) 设 A 、S 和 $\overline{S}$ 是有限集，满足 $\#S = \#\overline{S}$ 。令 $f : A \to A$ ，$h : S \to \overline{S}$ ，$\lambda : A \to S$ 以及 $\overline{\lambda} : A \to \overline{S}$ 是满足 $\overline{\lambda} \circ f = h \circ \lambda$ 的映射。如果 λ 和 $\overline{\lambda}$ 都是满射，那么下面的结论是等价的：

1. f 是双射;
2. h 是从 S 到 $\overline{S}$ 的双射，且对每个 $s \in S$ ，f 在其原像集 $\lambda^{-1}(s)$ 上是单射。

引理3.2.4 [40] 设 p 是奇素数。令 m, k 是使得 $\frac{m}{\gcd(m,k)}$ 为奇数的正整数。则 $x^{p^k} + x$ 是 $\mathbb{F}_{p^m}$ 上的一个置换多项式。

3.3 四类单项完全置换多项式

3.3.1 第一类单项完全置换多项式

在这个小节中，我们将证明由Wu等人[71]提出的猜想。在证明之前，我们先给出如下引理。

引理3.3.1 设 p 是奇素数，k 是一个正整数。则 $f(x)=x(x^2-c)^{\frac{p-1}{2}}$ 是域 $\mathbb{F}_{p^k}$ 上的置换多项式，其中 c 是 $\mathbb{F}_{p^k}$ 中的非平方元。

证明 我们首先证明 $x=0$ 是方程 $f(x)=0$ 的唯一解。如果 $f(x)=0$，那么 $x=0$ 或者 $(x^2-c)^{\frac{p-1}{2}}=0$。如果 $(x^2-c)^{\frac{p-1}{2}}=0$，则 $c=x^2$，这与题设 c 是一个非平方元矛盾！因此 $f(x)=0$ 当且仅当 $x=0$。

其次，我们要证明对每个非零 $a\in\mathbb{F}_{p^k}$，方程 $f(x)=a$ 有唯一的非零解。令 $\lambda(x)=x^2-c$，$\overline{\lambda}(x)=x^2$ 以及 $h(x)=(x+c)x^{p-1}$。则容易验证**图 3-1**交换：

$$\begin{array}{ccc}\mathbb{F}_{p^k}^* & \xrightarrow{\lambda} & \lambda(\mathbb{F}_{p^k}^*)\\ \downarrow f & & \downarrow h\\ \mathbb{F}_{p^k}^* & \xrightarrow{\overline{\lambda}} & \overline{\lambda}(\mathbb{F}_{p^k}^*).\end{array}$$

图 3-1

由引理 3.2.3知，我们只需要证明 h 是双射，而且对每个 $s\in\lambda(\mathbb{F}_{p^k}^*)$，$f$ 在$\lambda^{-1}(s)$上是单射。因为对每个 $s\in\lambda(\mathbb{F}_{p^k}^*)$，有 $\lambda^{-1}(s)=\{\pm(c+s)^{\frac{1}{2}}\}$。由于$f((c+s)^{\frac{1}{2}})\neq f(-(c+s)^{\frac{1}{2}})$，我们知道对每个 $s\in\lambda(\mathbb{F}_{p^k}^*)$，$f$ 在$\lambda^{-1}(s)$上是单射。

接下来，我们验证 h 是一个双射。注意到 $\#\lambda(\mathbb{F}_{p^k}^*)=\#\overline{\lambda}(\mathbb{F}_{p^k}^*)$，我们只需要去验证 h 是单射即可。对任意 $b\in\overline{\lambda}(\mathbb{F}_{p^k}^*)$，我们知道 b 是$\mathbb{F}_{p^k}^*$中的平方元。假设方程

$$x^p+cx^{p-1}=b \tag{3-1}$$

至少有两个不同的解。令 $y=\frac{1}{x}$，则方程

$$y^p-\frac{c}{b}y-\frac{1}{b}=0 \tag{3-2}$$

至少有两个不同的解。不妨设 y_1、 y_2就是方程(3-2)的两个不同解。则 y_1-y_2 就是方程 $y^p-\frac{c}{b}y=0$ 的一个根，也就是方程$y^{p-1}-\frac{c}{b}=0$的一个根。这就得出等式 $\frac{c}{b}=y_0^{p-1}$ 对某个 $y_0\in\mathbb{F}_{p^k}$ 成立，这与 $\frac{c}{b}$ 是 $\mathbb{F}_{p^k}$ 中的非平方元矛盾！因此，方程(3-1) 在 $\lambda(\mathbb{F}_{p^k}^*)$ 中至多有一个解。故 $h(x)$ 是双射。 □

现在我们可以对Wu等人[71]提出的猜想给出完整的证明。叙述如下：

定理3.3.2 (猜想 4.20[71]) 令 p 是一个奇素数， $r+1=p$ 且 $d=\frac{p^{rk}-1}{p^k-1}+1$。那么 $a^{-1}x^d$ 是 $\mathbb{F}_{p^{rk}}$ 上的一个完全置换多项式，其中 $a\in\mathbb{F}_{p^{rk}}^*$ 满足 $a^{p^k-1}=-1$。

证明 因为 $\gcd(p^{rk}-1,d)=1$，单项式 x^d 是 $\mathbb{F}_{p^{rk}}$ 上的置换多项式。

注意到 $a^{p^k-1}=-1$。则 $a^{p^k}=-a$ 且 $(a^2)^{p^k-1}=1$。由引理 3.2.2知，要证明这个猜想我们只需证明对任何 k , 多项式 $h_a(x)=x(x^2-a^2)^{\frac{p-1}{2}}$ 是$\mathbb{F}_{p^k}$ 上的置换多项式。事实上，令 $c=a^2\in\mathbb{F}_{p^k}$。由于 $a\notin\mathbb{F}_{p^k}$，知 c 是 $\mathbb{F}_{p^k}$ 中的非平方元。由引理 3.3.1可得所需结论。　□

3.3.2　第二类单项完全置换多项式

在本小节中，令 $p=2$，$n=6k$，其中 k 为满足 $\gcd(k,3)=1$ 的整数，并且 ω 是有限域 $\mathbb{F}_{2^{6k}}$ 的一个给定的本原元。我们将证明 $d=2^{4k-1}+2^{2k-1}$ 是 $\mathbb{F}_{2^{6k}}$ 上的一个完全置换多项式指数。定义如下集合：

$$S:=\{\omega^{t(2^{2k}-1)}|0<t\leq 2^{2k}+2^{4k},\ 3\nmid t\}. \tag{3-3}$$

引理3.3.3 对每个 $a\in S$，有 $\mathrm{Tr}_{2k}^{6k}(a)\neq 1$。

证明 如果 $a\in S\bigcap\mathbb{F}_{2^{2k}}$，那么 $\mathrm{Tr}_{2k}^{6k}(a)=a\neq 1$。因此我们可以设 $a\in S\backslash\mathbb{F}_{2^{2k}}$。

因为 $3|(2^{2k}-1)$，所以存在 $b\in\mathbb{F}_{2^{6k}}\backslash\mathbb{F}_{2^{2k}}$ 使得 $b^3=a$。由 S 的定义可知 $\mathrm{N}_{2k}^{6k}(a)=1$。令 $\eta:=\mathrm{N}_{2k}^{6k}(b)\in\mathbb{F}_4^*$。同样地， S 的定义可知 $\eta\neq 1$。

令 $B(x)=x^3+B_1x^2+B_2x+B_3\in\mathbb{F}_{2^{2k}}[x]$ 为 b 在域 $\mathbb{F}_{2^{2k}}$ 上的极小多项式。则 $B(x)$ 在 $\mathbb{F}_{2^{2k}}$ 上不可约，而且 $B_1=\mathrm{Tr}_{2k}^{6k}(b)$ 以及 $B_3=\eta$。我们可以直接验证得到

$$\mathrm{Tr}_{2k}^{6k}(a)=\mathrm{Tr}_{2k}^{6k}(b^3)=B_1^3+B_1B_2+B_3. \tag{3-4}$$

如果 $B_1=0$，那么 $\mathrm{Tr}_{2k}^{6k}(a)=B_3=\eta\neq 1$，在这种情形下，引理成立。

下面我们令 $B_1\neq 0$。假设有 $\mathrm{Tr}_{2k}^{6k}(a)=1$。则由方程 (3-4)得到 $B_2=\frac{B_1^3+\eta^2}{B_1}$，并且我们有

$$\begin{aligned}B(x)&=x^3+B_1x^2+B_2x+B_3\\&=x^3+B_1x^2+\frac{B_1^3+\eta^2}{B_1}x+B_3\\&=(\eta x+B_1)(\eta^2x^2+B_1x+\frac{\eta}{B_1}),\end{aligned}$$

这与 $B(x)$ 在 $\mathbb{F}_{2^{2k}}$ 上不可约矛盾! □

引理3.3.4 给定一个满足 $\gcd(k,3)=1$ 的整数 k。设 $n=6k$ 且 $d=2^{4k-1}+2^{2k-1}$。如果 $v\in S$，那么

$$\sum_{x\in\mathbb{F}_{2^{6k}}}\chi_{6k}(x^d+vx)=0.$$

证明 令 a 为 $\mathbb{F}_8$ 上的一个本原元满足 $a^3+a+1=0$。因为 $\gcd(k,3)=1$，我们有 $\mathbb{F}_{2^{6k}}=\mathbb{F}_{2^{2k}}(a)$。对任何 $x\in\mathbb{F}_{2^{6k}}$，它可以表示为

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

其中 x_0、x_1、$x_2\in\mathbb{F}_{2^{2k}}$。

因为 $\gcd(k,3)=1$，我们首先考虑 $k\equiv 1 \pmod 3$ 的情形，则有 $a^{2^{2k}}=a^4$。第一步就是计算 $\mathrm{Tr}_n(x^d)$，将其表示为关于 x_0、x_1 和 x_2 的函数。注意到 $\mathrm{Tr}_{2k}^{6k}(a)=\mathrm{Tr}_{2k}^{6k}(a^2)=0$ 以及 $\mathrm{Tr}_{2k}^{6k}(1)=1$，经过常规的计算得到

$$\mathrm{Tr}_{6k}(x^d)=\mathrm{Tr}_{2k}(x_0+x_1+x_2+x_1x_2).$$

接下来，令

$$v=v_0+v_1a+v_2a^2$$

其中 v_0、v_1、$v_2\in\mathbb{F}_{2^{2k}}$，我们得到

$$\mathrm{Tr}_{6k}(vx)=\mathrm{Tr}_{2k}(v_0x_0+v_1x_2+v_2x_1).$$

因此，

$$\sum_{x\in\mathbb{F}_{2^{6k}}}\chi_{6k}(x^d+vx)=\sum_{x_1,x_2\in\mathbb{F}_{2^{2k}}}\chi_{2k}(x_1+x_2+x_1x_2+v_1x_2+v_2x_1)\sum_{x_0\in\mathbb{F}_{2^{2k}}}\chi_{2k}(x_0+v_0x_0).$$

由引理 3.3.3知道 $v_0\neq 1$。所以 $\sum_{x\in\mathbb{F}_{2^{6k}}}\chi_{6k}(x^d+vx)=0$。

对于 $k\equiv 2 \pmod 3$ 的情形，通过类似的讨论可以得到 $\sum_{x\in\mathbb{F}_{2^{6k}}}\chi_{6k}(x^d+vx)=0$。

□

定理3.3.5 设$n=6k$，其中 k 是一个正整数且 $\gcd(k,3)=1$。那么 $d=2^{4k-1}+2^{2k-1}$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式指数。具体来讲，如果 $a\in S$，其中 S 由上面的 (3-3)所定义，则 $a^{-1}x^d$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式。

证明 因为 $\gcd(d, 2^{6k}-1)=1$，所以 x^d 是 $\mathbb{F}_{2^{6k}}$ 上的一个置换多项式。下面我们需证明 x^d+ax 也是 $\mathbb{F}_{2^{6k}}$ 上的一个置换多项式。由引理 3.2.1可知，我们需要证明对每个 $\alpha \in \mathbb{F}_{2^{6k}}^*$，都有

$$\sum_{x\in\mathbb{F}_{2^{6k}}} \chi_{6k}(\alpha(x^d+ax))=0,$$

其中 $a \in S$。因为 $\gcd(d, 2^{6k}-1)=1$，所以对每个非零 $\alpha \in \mathbb{F}_{p^{6k}}$，存在唯一的 $\beta \in \mathbb{F}_{2^{6k}}^*$ 使得 $\alpha=\beta^d$，并且我们有

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^{6k}}} \chi_{6k}(\alpha(x^d+ax)) &= \sum_{x\in\mathbb{F}_{2^{6k}}} \chi_{6k}((\beta x)^d+\beta^{d-1}a\beta x)\\ &= \sum_{x\in\mathbb{F}_{2^{6k}}} \chi_{6k}(x^d+\beta^{d-1}ax)\\ &= \sum_{x\in\mathbb{F}_{2^{6k}}} \chi_{6k}(x^d+\beta^{2^{4k-1}+2^{2k-1}-1}ax).\end{aligned}$$

因为 $\beta^{2^{4k-1}+2^{2k-1}-1}a \in S$，由引理 3.3.4知，对每个 $\alpha \in \mathbb{F}_{2^{6k}}^*$，都有

$$\sum_{x\in\mathbb{F}_{2^{6k}}} \chi_{6k}(\alpha(x^d+ax))=0.$$

这就完成了定理的证明。 □

3.3.3　第三类单项完全置换多项式

在本小节中，令 $p=2$，$n=4k$。我们通过运用与上一小节类似的分析方法来说明 $d=(1+2^{2k-1})(1+2^{2k})+1$ 是 $\mathbb{F}_{2^{4k}}$ 的一个完全置换多项式指数。

引理3.3.6 如果 v 是 $\mathbb{F}_{2^{2k}}^*$ 中的一个非立方元，那么

$$\sum_{x\in\mathbb{F}_{2^{4k}}} \chi_{4k}(x^{(1+2^{2k-1})(1+2^{2k})+1}+vx)=0.$$

证明 令$U=\{\lambda\in\mathbb{F}_{2^{4k}}|\lambda^{2^{2k}+1}=1\}$。则域 $\mathbb{F}_{2^{4k}}$ 中的每一个非零元素 x 通过极坐标唯一地表示为 $x=yz$，其中 $y\in U$，$z\in\mathbb{F}_{2^{2k}}^*$。那么

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^{4k}}}\chi_{4k}(x^{(1+2^{2k-1})(1+2^{2k})+1}+vx) &= 1+\sum_{x\in\mathbb{F}_{2^{4k}}^*}\chi_{4k}(x^{(1+2^{2k-1})(1+2^{2k})+1}+vx)\\ &= 1+\sum_{y\in U}\sum_{z\in\mathbb{F}_{2^{2k}}^*}\chi_{4k}((yz)^{(1+2^{2k-1})(1+2^{2k})+1}+vyz)\\ &= -2^{2k}+\sum_{y\in U}\sum_{z\in\mathbb{F}_{2^{2k}}}\chi_{4k}(yz^4+vyz)\\ &= -2^{2k}+\sum_{y\in U}\sum_{z\in\mathbb{F}_{2^{2k}}}\chi_{2k}(\mathrm{Tr}_{2k}^{4k}(yz^4+vyz))\\ &= -2^{2k}+\sum_{y\in U}\sum_{z\in\mathbb{F}_{2^{2k}}}\chi_{2k}((y+y^{2^{2k}})z^4+(y+y^{2^{2k}})vz)\\ &= -2^{2k}+\sum_{y\in U}\sum_{z\in\mathbb{F}_{2^{2k}}}\chi_{2k}(z^4(y+y^{2^{2k}}+y^4v^4+y^{2^{2k+2}}v^4))\\ &= (N(v)-1)2^{2k},\end{aligned}$$

此处，记 $N(v)=\#\{y\in U|y+y^{2^{2k}}+y^4v^4+y^{2^{2k+2}}v^4=0\}$，即在 U 中使得 $y+y^{-1}+y^4v^4+y^{-4}v^4=0$ 成立的 y 的数目，即下述方程解的数目：

$$(y+y^{-1})[1+v^4(y+y^{-1})^3]=0.$$

因为 v 是 $\mathbb{F}_{2^{2k}}^*$ 中的一个非立方元，我们得到 $1+v^4(y+y^{-1})^3\neq 0$。所以 $y=1$ 是其唯一解。因此，$N(v)=1$，这就完成了证明。 □

定理3.3.7 设 $n=4k$，则 $d=(1+2^{2k-1})(1+2^{2k})+1$ 是$\mathbb{F}_{2^n}$上的一个完全置换多项式指数。具体来讲，如果 a 是 $\mathbb{F}_{2^{2k}}^*$ 上的非立方元，那么 $a^{-1}x^d$ 是 $\mathbb{F}_{2^n}$ 上的一个完全置换多项式。

证明 首先，容易验证 $\gcd(d,2^{4k}-1)=1$。所以只需要证明对每一个非立方元 $a\in\mathbb{F}_{2^{2k}}^*$，$x^d+ax$ 是 $\mathbb{F}_{2^n}$ 上的一个置换多项式。因为对每一个非零 $\alpha\in\mathbb{F}_{2^{4k}}$，存在唯一的 $\beta\in\mathbb{F}_{2^{4k}}^*$ 使得 $\alpha=\beta^d$。则有

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^{4k}}}\chi_{4k}(\alpha(x^d+ax)) &= \sum_{x\in\mathbb{F}_{2^{4k}}}\chi_{4k}((\beta x)^d+\beta^{d-1}a\beta x)\\ &= \sum_{x\in\mathbb{F}_{2^{4k}}}\chi_{4k}(x^d+\beta^{d-1}ax)\\ &= \sum_{x\in\mathbb{F}_{2^{4k}}}\chi_{4k}(x^d+\beta^{(1+2^{2k-1})(1+2^{2k})}ax).\end{aligned}$$

注意到 $\beta^{(1+2^{2k-1})(1+2^{2k})}a$ 也是 $\mathbb{F}_{2^{2k}}^*$ 上的一个非立方元。则对每一个 $\alpha \in \mathbb{F}_{2^{4k}}^*$，由引理3.3.6知

$$\sum_{x\in\mathbb{F}_{2^{4k}}} \chi_{4k}(\alpha(x^d+ax))=0.$$

因此，由引理3.2.1可得 x^d+ax 是 $\mathbb{F}_{2^n}$ 上的一个置换多项式。 □

3.3.4　第四类单项完全置换多项式

在本小节中，我们将研究第四类单项完全置换多项式。令 p 是一个奇素数，$n=4k$ 以及 $d=\frac{p^{4k}-1}{2}+p^{2k}$。设 ω 是有限域 $\mathbb{F}_{p^n}$ 的一个给定的本原元。我们定义如下集合：

$$S:=\{\omega^{t(p^{2k}-1)+\frac{p^{2k}-1}{2}}:0\le t\le p^{2k}\}. \tag{3-5}$$

首先我们回忆两个引理。

引理3.3.8 [28] 令 p 是一个奇素数且 $d|(p^n-1)$。设 s 是满足 $d|(p^s+1)$ 的最小正整数。对每个 $0\le j<d$，定义集合：

$$C_j:=\{\omega^{di+j}\in\mathbb{F}_{p^n}^*|0\le i<\frac{p^n-1}{d}\}.$$

1. 当 d 是一个偶数，且 $(p^s+1)/d$ 和 $\frac{d}{2s}$ 都是奇数时，我们有

$$\sum_{x\in\mathbb{F}_{p^n}}\chi_n(ax^d)=\begin{cases}p^n, & \text{如果 } a=0;\\ (-1)^{\frac{n}{2s}+1}(d-1)p^{\frac{n}{2}}, & \text{如果 } a\in C_{\frac{d}{2}};\\ (-1)^{\frac{n}{2s}}p^{\frac{n}{2}}, & \text{如果 } a\notin C_{\frac{d}{2}}.\end{cases}$$

2. 对于其它所有的情形，都有

$$\sum_{x\in\mathbb{F}_{p^n}}\chi_n(ax^d)=\begin{cases}p^n, & \text{如果 } a=0;\\ (-1)^{\frac{n}{2s}+1}(d-1)p^{\frac{n}{2}}, & \text{如果 } a\in C_0;\\ (-1)^{\frac{n}{2s}}p^{\frac{n}{2}}, & \text{如果 } a\notin C_0.\end{cases}$$

引理3.3.9 [28] 令 d 是满足 $\gcd(d,p^n-1)=1$ 的一个整数。设存在整数 i，使得 $0\le i<n$ 且 $(d-p^i)|(p^n-1)$。选取整数 N 满足 $(d-p^i)N\equiv 0 \pmod{p^n-1}$，则有

$$\sum_{x\in\mathbb{F}_{p^n}}\chi_n(x^d+ax)=\frac{1}{N}\sum_{j=0}^{N-1}\sum_{y\in\mathbb{F}_{p^n}}\chi_n(y^N(a\omega^j+\omega^{djp^{-i}})).$$

我们先给出下面的一系列引理作为准备工作。

引理3.3.10 设 S 为 (3-5)所定义的集合，如果 $a \in S$，那么存在某个整数 s，使得 $\frac{a+1}{a-1} = \omega^{2s}$。

证明 若不然，假设 $\frac{a+1}{a-1} = \omega^{2s+1}$ 对某个整数 s 成立。因为 $a\overline{a} = -1$，其中 $\overline{a} = a^{p^{2k}}$，我们有

$$\frac{a+1}{a-1} = \frac{a-a\overline{a}}{a+a\overline{a}} = \frac{1-\overline{a}}{1+\overline{a}} = (\frac{1-a}{1+a})^{p^{2k}} = -\omega^{-(2s+1)p^{2k}}.$$

这可推出

$$\omega^{(2s+1)(p^{2k}+1)} = -1 = \omega^{(p^{2k}+1)\frac{p^{2k}-1}{2}},$$

这是不可能的! 所以 $\frac{a+1}{a-1} = \omega^{2s}$ 对某个整数 s 成立。 □

引理3.3.11 令 p 是奇素数，$n = 4k$ 且 $d = \frac{p^{4k}-1}{2} + p^{2k}$。如果$a \in S$，其中 S 由 (3-5)给出。则 $\sum_{x\in\mathbb{F}_{p^n}} \chi_n(x^d + ax) = 0$。

证明 由引理 3.3.9可知

$$\begin{aligned} 2\sum_{x\in\mathbb{F}_{p^n}} \chi_n(x^d + ax) &= \sum_{y\in\mathbb{F}_{p^n}} \chi_n(y^2(a+1)) + \sum_{y\in\mathbb{F}_{p^n}} \chi_n(y^2(a\omega + \omega^{dp^{2k}})) \\ &= \sum_{y\in\mathbb{F}_{p^n}} \chi_n(y^2(a+1)) + \sum_{y\in\mathbb{F}_{p^n}} \chi_n(y^2((a-1)\omega)). \end{aligned}$$

再由引理 3.3.10可得到 $a-1$、$a+1 \in C_0$ 或者 $a-1$、$a+1 \in C_1$。直接应用引理 3.3.8可推出 $\sum_{x\in\mathbb{F}_{p^n}} \chi_n(x^d + ax) = 0$。 □

现在我们给出下面的定理。

定理3.3.12 令 p 是一个奇素数且 $n = 4k$，则 $d = \frac{p^{4k}-1}{2} + p^{2k}$ 是 $\mathbb{F}_{p^n}$ 上的一个完全置换多项式指数。如果 $a \in S$，其中 S 由上面的 (3-5)所定义，则 $a^{-1}x^d$ 是 $\mathbb{F}_{p^n}$ 上的一个完全置换多项式。

证明 因为 $\gcd(d, p^n - 1) = 1$，则对每个 $a \in S$，单项式 $a^{-1}x^d$ 都是 $\mathbb{F}_{p^n}$ 上的置换多项式。接下来，我们只需去证明 $x^d + ax$ 是 $\mathbb{F}_{p^n}$ 上的置换多项式。

由 $\gcd(d, p^n-1)=1$ 可知，对每个非零 $\alpha \in \mathbb{F}_{p^n}$，存在唯一的 $\beta \in \mathbb{F}_{p^n}^*$ 使得 $\alpha=\beta^d$，则

$$\begin{aligned}\sum_{x\in\mathbb{F}_{p^n}} \chi_n(\alpha(x^d+ax)) &= \sum_{x\in\mathbb{F}_{p^n}} \chi_n((\beta x)^d+\beta^{d-1}a\beta x)\\ &= \sum_{x\in\mathbb{F}_{p^n}} \chi_n(x^d+\beta^{d-1}ax)\\ &= \sum_{x\in\mathbb{F}_{p^n}} \chi_n(x^d+\beta^{(\frac{p^{2k}+1}{2}+1)(p^{2k}-1)}ax).\end{aligned}$$

因为$\beta^{(\frac{p^{2k}+1}{2}+1)(p^{2k}-1)}a \in S$，所以由引理 3.3.11知，对每个 $\alpha \in \mathbb{F}_{p^n}^*$，我们有

$$\sum_{x\in\mathbb{F}_{p^n}} \chi_n(\alpha(x^d+ax))=0.$$

因此，由引理 3.2.1可得 x^d+ax 是 $\mathbb{F}_{p^n}$ 上的置换多项式，这就完成了证明。 □

3.4　一类三项完全置换多项式

在本节中，我们构造了一类三项完全置换多项式。

定理3.4.1 令 p 是一个奇素数，则 $f(x)=-x+x^{\frac{p^{2m}+1}{2}}+x^{\frac{p^{2m}+1}{2}p^m}$ 是 $\mathbb{F}_{p^{3m}}$ 上的一个完全置换多项式。

证明 令 $g(x)=x+x^{p^m}$，则有

$$f(x)+x=x^{\frac{p^{2m}+1}{2}}+x^{\frac{p^{3m}+p^m}{2}}=g(x^{\frac{p^{2m}+1}{2}}).$$

因为 $\gcd(\frac{p^{2m}+1}{2}, p^{3m}-1)=1$，所以我们知道 $f(x)+x$ 是 $\mathbb{F}_{p^{3m}}$ 上的置换多项式当且就当 $g(x)$ 也是其上的置换多项式。由引理 3.2.4可得 $g(x)$ 是 $\mathbb{F}_{p^{3m}}$ 上的置换多项式。故 $f(x)+x$ 是 $\mathbb{F}_{p^{3m}}$ 上的置换多项式。

接下来，我们需要去证明 $f(x)$ 是 $\mathbb{F}_{p^{3m}}$ 上的置换多项式。设 $h(x):=x+x^{p^m}-x^{1+p^m-p^{2m}}$，则有 $f(x)=h(x^{\frac{p^{2m}+1}{2}})$。因为 $\gcd(\frac{p^{2m}+1}{2}, p^{3m}-1)=1$，所以 $f(x)$ 是 $\mathbb{F}_{p^{3m}}$ 上的置换多项式当且就当 $h(x)$ 也是其上的置换多项式。注意到 $h(0)=0$，且对任何 $x\neq 0$，有

$$h(x)=\frac{x^{1+p^{2m}}+x^{p^m+p^{2m}}-x^{1+p^m}}{x^{p^{2m}}}.$$

首先我们需证明 $h(x)=0$ 只有解 $x=0$。若不然，存在某个 $x\neq 0$ 使得 $h(x)=0$，即，

$$x^{1+p^{2m}}+x^{p^m+p^{2m}}-x^{1+p^m}=0.$$

对上面的方程两边同时取其 p^m 次幂、p^{2m} 次幂，可得到

$$x^{1+p^m}+x^{1+p^{2m}}-x^{p^m+p^{2m}}=0,$$
$$x^{p^m+p^{2m}}+x^{1+p^m}-x^{1+p^{2m}}=0.$$

对上述两个方程相加可导出 $2x^{1+p^m}=0$，所以 $x=0$，这与假设矛盾。因此 $h(x)=0$ 当且仅当 $x=0$。

下面，我们证明对每一个 $a\in\mathbb{F}_{p^{3m}}^*$，方程 $h(x)=a$ 至多有一个解，即方程

$$x^{1+p^{2m}}+x^{p^m+p^{2m}}-x^{1+p^m}=ax^{p^{2m}} \tag{3-6}$$

至多有一个解。对方程 (3-6)的两边同时作用 p^m 次幂和 p^{2m} 次幂，可得到

$$x^{1+p^m}+x^{1+p^{2m}}-x^{p^m+p^{2m}}=a^{p^m}x,$$
$$x^{p^m+p^{2m}}+x^{1+p^m}-x^{1+p^{2m}}=a^{p^{2m}}x^{p^m}.$$

上面两个方程相加可导出

$$2x^{1+p^m}=a^{p^m}x+a^{p^{2m}}x^{p^m}. \tag{3-7}$$

因为 $x\neq 0$，我们有 $2x^{p^m}=a^{p^m}+a^{p^{2m}}x^{p^m-1}$。令 $y=\frac{1}{x}$，则

$$y^{p^m}+a^{p^{2m}-p^m}y-2a^{-p^m}=0. \tag{3-8}$$

假设方程 (3-8)在 $\mathbb{F}_{p^{3m}}$ 中至少有两个不同的非零解。记为 y_1、y_2。我们可以得到 $y_1-y_2\in\mathbb{F}_{p^{3m}}$ 是方程 $y^{p^m}+a^{p^{2m}-p^m}y=0$ 的一个根，即是方程 $y^{p^m-1}+a^{p^{2m}-p^m}=0$ 的一个根，这与方程 $y^{p^m-1}+a^{p^{2m}-p^m}=0$ 在 $\mathbb{F}_{p^{3m}}^*$ 中无解这个事实矛盾！因此，方程 (3-8)在 $\mathbb{F}_{p^{3m}}$ 中至多有一个解。

综上所述，我们已经证明了 $h(x)$ 是一个置换多项式。所以 $f(x)$ 是一个完全置换多项式! □

3.5 幂函数的差分性质

在本节，我们将考虑单项置换多项式的差分均匀度。首先，我们回忆一些基本的定义。

定义 3.5.1 令 F 是从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_{2^m}$的函数。对任何 $a \in \mathbb{F}_{2^n}$，F 关于a的导数就是从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_{2^m}$ 的函数 $D_a(F)$，定义为

$$D_a(F(x)) = F(x+a) + F(x),\ x \in \mathbb{F}_{2^n}.$$

用来刻画抵抗密码学中差分攻击的度量单位定义如下：

定义 3.5.2 设 F 是从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_{2^n}$的函数。对任何 $\mathbb{F}_{2^n}$ 中的元素 a 和 b，记

$$\delta(a,b) = \#\{x \in \mathbb{F}_{2^n} | D_a(F(x)) = b\}.$$

那么我们称

$$\delta(F) = \max_{a \neq 0, b \in \mathbb{F}_{2^n}} \delta(a,b)$$

为 F 的差分均匀度。

注3.5.3 当 $F(x) = x^d$ 为单项式时，对任何非零 $a \in \mathbb{F}_{2^n}$，方程 $(x+a)^d + x^d = b$ 可以变为 $a^d\left((\frac{x}{a}+1)^d + (\frac{x}{a})^d\right) = b$。这就意味着 $\delta(a,b) = \delta(1, b/a^d)$。因此，对于单项式函数，它的差分性质可由 $\delta(1,b), b \in \mathbb{F}_{2^n}$ 决定。从现在开始，对于单项式函数，我们用 $\delta(b)$ 表示 $\delta(1,b)$。

下面，我们先给出后文用到的两个引理。

引理3.5.4 [5] 对于正整数 m 以及 $a, b \in \mathbb{F}_{2^m}, a \neq 0$，二次方程 $x^2 + ax + b = 0$ 在 $\mathbb{F}_{2^m}$ 中有解当且仅当 $\mathrm{Tr}_m(\frac{b}{a^2}) = 0$。

引理3.5.5 [5] 对于正整数 m 以及 $a \in \mathbb{F}_{2^m}^*$，三次方程 $x^3 + x + a = 0$ 的解有如下三种情况：

(1) 在 $\mathbb{F}_{2^m}$ 中有唯一解当且仅当 $\mathrm{Tr}_m(a^{-1}+1) = 1$；

(2) 在 $\mathbb{F}_{2^m}$ 中有三个不同的解当且仅当 $p_m(a) = 0$，其中多项式 $p_m(x)$ 可由下面的方程递归定义：$p_1(x) = p_2(x) = x$，当 $k \geq 3$ 时，$p_k(x) = p_{k-1}(x) + x^{2^{k-3}} p_{k-2}(x)$；

(3) 对于其它情况，无解。

我们首先给出下面的引理作为预备工作。

引理3.5.6 设 $n=2m$ 且 m 为奇数，$b\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$ 以及 $y\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2$。则方程 $x^4+y^2(x^2+x+1)+x+1+b=0$ 解的数目为 0 或者 4。进一步，若 x_0 是其中的一个解，那么方程的其它三个解为 x_0+1、x_1 和 x_1+1，其中 x_1 满足 $x_1^2+x_1=x_0^2+x_0+1+y^2$。

证明 如果 x_0 是方程 $x^4+y^2(x^2+x+1)+x+1+b=0$ 的一个解，那么 x_0+1 也是其一个解。所以我们有

$$x^4+y^2(x^2+x+1)+x+1+b=(x^2+x+x_0^2+x_0)(x^2+x+x_0^2+x_0+1+y^2).$$

因为 $\mathrm{Tr}_n(x_0^2+x_0+1+y^2)=0$，由引理 3.5.4可知，方程 $x^2+x+x_0^2+x_0+1+y^2=0$ 也有两个不同于 x_0 和 x_0+1 的解。因此方程 $x^4+y^2(x^2+x+1)+x+1+b=0$ 解的数目为 0 或者 4。第二部分的结论是显然的。 □

现在我们给出本节的主要定理。

定理3.5.7 令 $n=2m$ 且 m 为奇数以及 $d=2^{m+1}+3$。那么 $F_d:x\to x^d$ 是 $\mathbb{F}_{2^n}$ 的一个置换，并且 $\delta(F_d)\le 10$。进一步，对每个 $b\in\mathbb{F}_{2^m}$，我们有 $\delta(b)\in\{0,4\}$。

证明 注意到 $\gcd(d,2^n-1)=1$，所以 F_d 是一个置换多项式。对每个 $x\in\mathbb{F}_{2^n}$，令 $\overline{x}:=x^{2^m}$。显然有 $x+\overline{x}\in\mathbb{F}_{2^m}$、$x\overline{x}\in\mathbb{F}_{2^m}$。首先，我们计算 $D_1(F_d(x))$，有

$$D_1(F_d(x))=(x+1)^d+x^d=(\overline{x}^2+x)(x^2+x+1)+1=(\overline{x}x)^2+((\overline{x}+x)^2+1)(x+1).$$

则只需去说明对任何 $b\in\mathbb{F}_{2^n}$，方程 $D_1(F_d(x))=b$ 至多有 10 个解。

假定

$$(\overline{x}x)^2+((\overline{x}+x)^2+1)(x+1)=b. \tag{3-9}$$

对方程 (3-9)两边同时取其 2^m 次幂，则有

$$(\overline{x}x)^2+((\overline{x}+x)^2+1)(\overline{x}+1)=\overline{b}. \tag{3-10}$$

将方程 (3-9)和 (3-10)相加可得到

$$((\overline{x}+x)^2+1)(\overline{x}+x)=b+\overline{b}. \tag{3-11}$$

令 $y:=\overline{x}+x\in\mathbb{F}_{2^m}$ 且 $a:=b+\overline{b}\in\mathbb{F}_{2^m}$，我们有

$$y^3+y+a=0. \tag{3-12}$$

将 $\overline{x}=y+x$ 代入方程 (3-9)，则有

$$x^4+y^2(x^2+x+1)+x+1+b=0. \tag{3-13}$$

因此 x 是方程 (3-9)的解当且仅当 (x,y) 是下列方程组的解

$$\begin{cases} x^4+y^2(x^2+x+1)+x+1+b=0, \\ y^3+y+a=0, \\ \overline{x}+x=y. \end{cases} \tag{3-14}$$

故 $\delta(F_d)\leq 12$。下面我们分 $a=0$ 和 $a\neq 0$ 两种情形讨论。

情形1: $a=0$。

显然有 $b\in\mathbb{F}_{2^m}$，并且 0、1 是方程 (3-12)的两个根。我们分情况讨论如下。

(1) 如果 $y=0$，那么 $x\in\mathbb{F}_{2^m}$，则方程 (3-14)变为 $x^4+x+1=b$，且它有 0 个解或者 2 个解；而且它有 2 个解当且仅当 $\mathrm{Tr}_m(b)=1$。

(2) 如果 $y=1$，那么方程组 (3-14)变为

$$\begin{cases} x^4+x^2+b=0, \\ \overline{x}+x=1. \end{cases} \tag{3-15}$$

因为 $\gcd(2,2^n-1)=1$，所以方程 $x^4+x^2+b=0$ 等价于 $x^2+x+b^{2^{m-1}}=0$。由引理 3.5.4知道，它有 2 个解。因为 $1=\overline{x}+x=\sum_{i=0}^{m-1}(x^2+x)^{2^i}=\mathrm{Tr}_m(b^{2^{m-1}})$，所以方程 (3-15)有 2 个解当且仅当 $\mathrm{Tr}_m(b)=1$。

综上，对于上述两种情况，方程 (3-14)有 2 个解当且仅当 $\mathrm{Tr}_m(b)=1$。因此 $\delta(b)\in\{0,4\}$。

情形2: $a\neq 0$。

在这种情形下显然有 $b\notin\mathbb{F}_{2^m}$ 且 $y\notin\mathbb{F}_2$。

由引理 3.5.5知，方程 (3-12)有 0、1 或者 3 个解。我们对这三种情形分开讨论。

(1) 若方程 (3-12)无解，则 $\delta(b)=0$。

(2) 若方程 (3-12)有一个解，不妨设为 y_0。则由引理 3.5.6知，方程 (3-13)有 0 个解或者 4 个解，且这 4 个解可记为 x_{11}、$x_{11}+1$、x_{21} 以及 $x_{21}+1$。然而，我们仍需要对 $i=1$、2 时，等式 $x_{i1}+\overline{x_{i1}}=y_0$ 成立。故 $\delta(b)\in\{0,2,4\}$。

(3) 若方程(3-12)有三个解，记为 y_1、y_2 和 y_3。则有 $y_1+y_2+y_3=0$。对每个 $y_i,\ 1\le i\le 3$，由引理 3.5.6知，方程 (3-13)有 0 个解或者 4 个解。故总共解的数目为 0、4、8 或者 12。

(i) 如果解的数目为 0、4 或者 8，则方程 (3-14)的数目至多为 8。所以 $\delta(b)\in\{0,2,4,6,8\}$。

(ii) 如果解的数目为 12，即对每个 $y_i,\ 1\le i\le 3$，方程 (3-13)都有 4 个解。设这 12 解为 $\{x_{ij},x_{ij}+1|i=1,2,3;\ j=1,2\}$，其中由 y_i 对应的解为 x_{i1}、$x_{i1}+1$、x_{i2} 和 $x_{i2}+1$。如果 x_{i1}、$x_{i1}+1$、x_{i2} 和 $x_{i2}+1$就是方程 (3-14)的解，那么我们容易得到

$$\begin{cases} x_{i1}+x_{i2}+(x_{i1}+x_{i2})^2=1+y_i^2, \\ x_{i1}+x_{i2}\in\mathbb{F}_{2^m}, \end{cases} \tag{3-16}$$

这就意味着 $t^2+t+1+y_i^2=0$ 在 $\mathbb{F}_{2^m}$ 上有两个解。由引理 3.5.4知 $\mathrm{Tr}_m(1+y_i^2)=0$，即 $\mathrm{Tr}_m(y_i)=1$。因此，若 $\delta(b)=12$，则 $\mathrm{Tr}_m(y_1)=\mathrm{Tr}_m(y_2)=\mathrm{Tr}_m(y_3)=1$。然而，$1=\mathrm{Tr}_m(y_1)+\mathrm{Tr}_m(y_2)+\mathrm{Tr}_m(y_3)=\mathrm{Tr}_m(y_1+y_2+y_3)=0$，矛盾！所以 $\delta(b)\le 10$。

综上，我们可得到 $\delta(F_d)\le 10$。 □

注3.5.8 当 $d=2^m+2^{(m+1)/2}+1$ 时，通过同样的方法我们也可以得到 $\delta(F_d)\le 10$。事实上，设 $m=2r-1$ 且 $a:=b+\overline{b}$，则上述证明中的方程 (3-14)替换为下面的方程

$$\begin{cases} x^4+(ay+1)x^2+ayx+(y^2+1)\overline{b}^{2^r}+b\overline{b}=0, \\ (y+1)x^{2^r}+x^2+yx+y+1+b=0, \\ y^3+(a+1)y^2+a^{2^r}y+a^{2^r}=0, \\ \overline{x}+x=y. \end{cases} \tag{3-17}$$

故 $\delta(F_d)\le 12$。如果 $b\in\mathbb{F}_{2^m}$，易知 $\delta(b)\in\{0,4\}$。若对某个 $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$，有 $\delta(b)=12$。则 $\mathrm{Tr}_m(ay_i)=1$ 且 $1=\mathrm{Tr}_m(ay_1)+\mathrm{Tr}_m(ay_2)+\mathrm{Tr}_m(ay_3)=\mathrm{Tr}_m(a(a+1))=0$，矛盾!

因此我们有下面的结论。

定理3.5.9 令 $n=2m$ 且 m 为奇数以及 $d=2^m+2^{(m+1)/2}+1$。那么 $F_d:x\to x^d$是 $\mathbb{F}_{2^n}$ 的一个置换，并且 $\delta(F_d)\le 10$。进一步，对每个 $b\in\mathbb{F}_{2^m}$，我们有 $\delta(b)\in\{0,4\}$。

注3.5.10 我们用一个具体的例子来阐述上面证明的想法。令 w 为 $\mathbb{F}_{2^n}$ 的一个本原元，$n=10$、$d=67$、$b=w^{27}$ 以及 $a=b+\overline{b}$。则方程 (3-12)和 (3-13)分别变为 $y^3+y+a=0$ 和 $x^4+y^2(x^2+x+1)+x+1+b=0$。

$y^3+y+a=0$ 的解	$\mathrm{Tr}_m(y_i)$	$x^4+y^2(x^2+x+1)+x+1+b=0$ 的解	$D_1(F_d(x))=b$ 的解
$y_1=w^{330}$	1	$\{w^{672},w^{1019};w^{619},w^{975}\}$	$w^{226},w^{633},$
$y_2=w^{363}$	1	$\{w^{226},w^{633};w^{586},w^{903}\}$	$w^{586},w^{903},$
$y_3=w^{924}$	0	$\{w^{129},w^{340};w^{774},w^{883}\}$	w^{129},w^{340}

图 3-2

在**图** 3-2里，对于一个固定的元素 b，方程 (3-12)有 3 个解，记为 y_1、y_2 和 y_3。对每个 y_i，由方程 (3-13)，我们得到 4 个解。我们需要去检验等式 $x+\overline{x}=y_i$ 是否成立。注意到 $\mathrm{Tr}_m(y_3)=0$，知至少有 2 个解不满足 $x+\overline{x}=y_3$ *(*在上面的例子中，w^{774} 和 w^{883} 不满足*)*。然而对每个 $y_i,\ i=1,2$，我们无法确定它的 4 个解是否满足 $x+\overline{x}=y_i$，这是由于 $\mathrm{Tr}_m(y_1)=\mathrm{Tr}_m(y_2)=1$ *(*在上面的例子中，y_1 对应的 4 个解不满足。而 y_2 对应的 4 个解满足*)*。因此，在证明中，我们只能得到 $\delta(b)\le 10$，但是事实上，在这个例子中，$\delta(b)=6$。所以，我们需要更详细的条件来描述方程的解。

3.6　小结

完全置换多项式和低差分的置换多项式在密码学中有重要的应用，如在分组密码中 S 盒的设计中就用到的是 4 差分置换多项式。本章呈现了若干新的完全置换多项式的结果。首先，通过AGW准则，我们证明了由Wu等人[71] 提出的一个猜想，得到了第一类单项完全置换多项式；然后基于所在域上的加法特征，我们构造了三类新的单项完全置换多项式；并且通过研究域上的方程解的数目，我们也构造了一类三项完全置换多项式。最后，对于 $d=2^{m+1}+3$ 和 $2^m+2^{\frac{m+1}{2}}+1$，Blondeau等人[9]猜想 x^d 是 $\mathbb{F}_{2^n}$ 上的 8-差分函数。我们证明了它的差分均匀度至多为 10。但是如何排除掉 $\delta(b)=10$ 这种情况，是一个困难的工作。

4 二元局部可修复码

在这个信息数据时代，我们所面临的首要问题是对海量的数据进行有效存储。传统的存储方案利用性能强劲的专用服务器和磁盘阵列进行数据存储，这虽然拥有很高的可靠性，但成本太高。同时，服务器的集中性成为系统存储的瓶颈，也大大降低了可靠性和安全性。对于存储海量数据而言，这种传统的存储方案已越来越不能满足当前需求。近年来，分布式存储成为海量存储的主要解决方案，它采用可扩展的系统结构，利用多台存储服务器分担存储负荷，利用位置服务器定位存储信息，不仅提高了系统的可靠性、可用性和存储效率，而且易于扩展。同时，分布式存储网络提供了地理位置上分散的存储节点，以及对其共享存储访问，因此降低了数据访问的时延。分布式存储系统已被广泛应用于商业实践中，例如，加州大学伯克利分校构建的Oceanstore、Unix高性能计算系统协会开发的Total Recall，微软的云存储项目Azure Storage和谷歌的存储系统Colossus 等。

作为分布式存储系统（Distributed Storage System）中有重要应用的一类码：局部可修复码，已成为本领域里的研究热点。目前很多已知的构造都是基于相对比较大的有限域。这会导致修复时，计算比较复杂，而且由于实际中计算机硬件的要求，人们更关心二元局部可修复码的构造。在本章，我们主要关注含有不交修复组的二元局部可修复码的维数上界以及具体的构造。

4.1 介绍

大规模的分布式存储系统（如数据中心）在存储数据时，为了保证系统的稳定性，常常加入一些冗余来抵抗节点发生错误。最简单而且最常见的方法就是 3-复制。它的明显优势就是错误发生时，修复既简单又快速。然而，这个策略带来大的存储负荷，这不适应用于当前大数据时代！为了能获得较好的存储效率，纠删码应运而生，如Windows Azure[32]、Facebook's Hadoop cluster[52]，它将原始数据划分成 k 份相等大小的块，然后将其编码为 n 块 $(n \geq k)$，存储在 n 个不同的节点。它能容忍 $d-1$ 个节点发生擦除，其中 d 为纠删码的极小距离。特别地，极大距离可分码(MDS)是一类达到Singleton 界的一类纠删码。因此对于给定存储负荷，它可以提供最高级别的容错能力。但是，它有一个弱势。因为在现实中

最常见的数据损坏情况是单个存储节点（磁盘）因为设备损坏、自然灾害等因素而失效。所以当一个节点发生错误时，我们需要通过其它任何 k 个正常的节点上的信息来恢复该错误节点的信息。这是一个极其耗时的修复过程。通常我们有两种熟知的度量来刻画修复效率，即修复带宽和局部修复性。在本章中，我们研究具有小的局部修复性的码。

局部修复性的概念是由Gopalan等人[23]、Oggier和Datta[45]、以及Papailiopoulos等人[48]提出。如果码字第 i 坐标分量可由不超过 r 个其它坐标分量来修复，那么我们称码字坐标分量 i 具有局部修复性。在本章中，若一个 $[n,k,d]$ 线性码的所有坐标分量（也称为码字符号）都具有局部修复性 r ，我们记为 $[n,k,d;r]$ 局部可修复码（LRC）。由于 $r \ll k$ ，则它在修复时可以极大地减少硬盘I/O耗时。

当考虑到码的容错能力，自然地，极小距离 d 就是局部可修复码的一个主要的度量变量。当只考虑信息位的局部修复性时，首先由Gopalan 等人[23]给出了码的极小距离的上界:

$$d \leq n-k-\lceil \frac{k}{r} \rceil + 2, \tag{4-1}$$

这个界也称为Singleton型界，因为当 $r=k$ 时，这个界退化为经典的Singleton界。然后在文献[20,47]，这个界(4-1)被推广到向量码和非线性码。尽管这个界对所有的局部可修复码都成立，但是，它在很多情形下都不是紧的。如文献[57,66]就系统地研究了这个界(4-1)的紧性。

如果一个局部可修复码达到界(4-1)，我们称其为 d-最优的。对于 $(r+1)|n$ 的情形，在文献[62]和[54]中，分别通过Reed-Solomon码和Gabidulin码构造了 d-最优的局部可修复码。然而，这两个构造都是在很大的域上实现的，域的大小是关于码长 n 的指数函数。在文献[60]中，作者通过一些“好”的多项式在一个比码长 n 大一点的域上，对 $(r+1)|n$ 的情形构造了 d-最优的局部可修复码。并且他们的构造可以推广到 $(r+1) \nmid n$ 的情形，只是极小距离比界(4-1)至多少 1 。在其后续的文章[4,61]，进一步将构造的思想推广到了循环码和代数几何码。

之后的拓展研究考虑多个节点失效的情况，对多个节点的修复又细分为并行修复和串行修复两种模式。所谓并行修复，即同时修复各个损坏的节点，Wang等人[65]和Prakash等人[49]分别提出了两种不同的修复方式；所谓串行修复，即各个损坏的节点的修复过程有先后顺序，允许先一步修好的节点被利用到后续节点修复的过程中，在文献[50]中首先提出。对于处理多个节点失效的进一步工作可参见[3,46,56,59,60,67]。

考虑到在计算机上实施的便捷性，在小域（特别是二元域）上的码备受关注。对于二元的情形，界(4-1) 几乎对所有情形都不是紧的。事实上，Hao等人[27]证明了只存在 4 类

d-最优的局部可修复码达到Singleton型界。在文献[10] 中，将域的大小考虑进去导出一个新的界，我们称其为Cadambe-Mazumdar (C-M) 界。

$$k \leq \min_{t \in \mathbb{Z}^+} \left[tr + k_{\text{opt}}^{(q)}(n-(r+1)t, d) \right], \tag{4-2}$$

其中 $k_{\text{opt}}^{(q)}(n,d)$ 是固定域的大小 q 、码长 n 和极小距离 d 时，码所能达到的最大可能维数。

首先，文献[10]指出二元极长码可以达到C-M界。后来在文献[55]中，通过反码构造了局部修复性 $r=2$ 和 3 且达到界(4-2)的二元局部可修复码。基于不同的二元系统码作为基码，Huang等人[33]提出了 $d=3$、4 和 5 的二元局部可修复码的构造，其中一些被证明是 d-最优的。在文献[24]中，当极小距离为 2、6 和 10，局部修复性 $r=2$ 时，构造了维数最优的二元局部可修复循环码。后来，在文献[72]中，对于 $r=2$ 和 $d=10$ 的情形，也构造了一类新的维数最优的二元局部可修复循环码。另外，Shahabinejad等人[53]构造了一类极小距离为 4 的二元局部可修复码。同样地，在文献[68]中，作者构造了一类维数最优的二元局部可修复码，它的极小距离至少为 6 。另外在文献[43]中，也构造了极小距离至少为 6 的二元局部可修复码，但是它只是部分例子是达到界(4-2)。在文献[21]，作者考察了MacDonald码和广义MacDonald码的局部修复性，并且提出了一些二元局部可修复码的构造。

注意到上述关于局部可修复码的最优构造，大部分都采用了一个特殊的结构，称之为不交修复组(定义 4.2.9)。在本章中，我们主要研究具有不交修复组这样结构的二元局部可修复码的界以及最优构造。首先，我们导出关于这类码的维数 k 的一个上界(定理 4.3.1)，这个界可以看作是文献[68]中的界的一个推广。并且，如果一个二元局部可修复码达到了定理 4.3.1中的界，我们就称它是 k-最优的。同样地，对一般的参数 r ，我们给出了两类 k- 最优的二元局部可修复码的构造，并且我们的第一类构造结果涵盖了文献[68] 中的构造。进一步，对于 $r \in \{2,3\}$ ，极小距离 $d=6$ 的情形，我们得到了几乎所有参数的 k-最优的具有不交修复组的二元局部可修复码。

本章的框架如下：在下一节，我们给出一些记号、定义以及关于partial spread的结果；第 4.3 节，给出具有不交修复组的 $[n,k,d;r]_2$ LRCs的维数上界；第 4.4 节，给出 $d=6$ 时的最优二元局部可修复码的构造；在最后一节，我们对 $d \geq 8$ 时，具有不交修复组的 k-最优的二元局部可修复码的构造进行了讨论并对本章进行总结。

4.2　准备工作

下面的符号仅适用于本章。

- 设 $[n]=\{1,2,\cdots,n\}$ 。若 $a \leq b$ 为两个整数，定义 $[a,b]=\{a,a+1,\cdots,b\}$ 。

- 设 q 是一个素数幂，$\mathbb{F}_q$ 是含有 q 个元素的有限域。
- 设 $\mathbb{F}_q^n$ 为 $\mathbb{F}_q$ 上的 n 维向量空间。
- 对任何向量 $\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{F}_q^n$，令 $\mathrm{supp}(\mathbf{v}) = \{i \in [n] | v_i \neq 0\}$ 以及 $\mathrm{wt}(\mathbf{v}) = |\mathrm{supp}(v)|$。对于集合 $S = \{i_1, \cdots, i_{|S|}\} \subseteq [n]$，定义 $\mathbf{v}|_S = (v_{i_1}, \ldots, v_{i_{|S|}})$。
- 令 $d(\mathbf{u}, \mathbf{v})$ 为任何两个向量 $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ 的Hamming距离。
- 设 $U \subseteq \mathbb{F}_q^n$ 为一个集合，$\mathbf{v}$ 是一个向量。定义$d(U, \mathbf{v}) = \min\{d(\mathbf{u}, \mathbf{v}) | \mathbf{u} \in U\}$。
- 令 I_n 为 $n \times n$ 的单位阵，以及 $\mathbf{1}_n$ 和 $\mathbf{0}_n$ 分别为全 1 和全 0 向量。

首先，我们给出弱无关集（Weakly Independent Set）[22]的概念。

定义 4.2.1 设 $\mathbb{F}$ 为特征为 2 的域，$T \subseteq \mathbb{F}$ 是一个集合，τ 为一个正整数。如果对 T 的任何子集 T'，$2 \leq |T'| \leq \tau$，它里面的所有的元素的和不为零，则称集合 T 为 $\mathbb{F}_2$ 上的 τ-弱无关集。

下面，我们给出partial spread的一些相关结论。

定义 4.2.2 设 $S = \{W_1, \cdots, W_l\}$ 是向量空间$\mathbb{F}_q^m$上的一些 t-维子空间的集合。如果满足对任何 $1 \leq i < j \leq l$，都有 $W_i \cap W_j = \{0\}$，则称 S 为*partial t-spread*。并且称集合 S 的大小为 l。进一步，如果 S 的大小达到它的最大可能，则称 S 为极大的。特别地，如果 $\cup_{i=1}^{l} W_i = \mathbb{F}_q^m$，我们简称 S 为 *t-spread*。

众所周知，$\mathbb{F}_q^m$上的一个 t-spread存在当且仅当 $t|m$。近几年在网络编码领域，由于 t-spread对应于一类特殊的子空间码，以及其自身的一些性质，关于极大partial t-spread 的大小已有深入的研究。在子空间码中，熟知的距离不再是Hamming 距离，而是所谓的子空间距离，即对任何 $\mathbb{F}_q^m$ 中的子空间 U、V，定义 $d_S(U, V) := \dim(U + V) - \dim(U \cap V)$。令 $k \in [m]$，由 $\mathbb{F}_q^m$ 上的 k 维子空间生成的极小子空间距离为 d 的子空间码所含有的极大码字个数，记为 $A_q(m, k, d)$。则 $\mathbb{F}_q^m$ 上的极大partial k-spread的大小用这个记号表示就是 $A_q(m, k, 2k)$。

到目前为止，关于 $A_q(m, k, 2k)$ 的确切值的结果比较少。我们列举后文要用到的一些结果如下。

引理4.2.3 [19] 对于正整数 $1 \leq k \leq m$ 且 $m \equiv r \pmod{k}$，我们有

$$A_q(m,k,2k) \geq \frac{q^m - q^k(q^r-1)-1}{q^k-1}.$$

引理4.2.4 [6] 对于正整数 $1 \leq k \leq m$ 且 $m \equiv r \pmod{k}$，我们有

$$A_q(m,k,2k) = \begin{cases} \frac{q^m-1}{q^k-1}, & \text{如果 } r=0; \\ \frac{q^m-q^{k+1}+q^k-1}{q^k-1}, & \text{如果 } r=1. \end{cases}$$

推论4.2.5

$$A_2(m,2,4) = \begin{cases} \frac{2^m-1}{3}, & \text{如果 } m \equiv 0 \pmod{2}; \\ \frac{2^m-5}{3}, & \text{如果 } m \equiv 1 \pmod{2}. \end{cases}$$

引理4.2.6 [18]

$$A_2(m,3,6) = \begin{cases} \frac{2^m-1}{7}, & \text{如果 } m \equiv 0 \pmod{3}; \\ \frac{2^m-9}{7}, & \text{如果 } m \equiv 1 \pmod{3}; \\ \frac{2^m-18}{7}, & \text{如果 } m \equiv 2 \pmod{3}. \end{cases}$$

现在，我们给出本章所讨论的线性局部可修复码的定义。

定义 4.2.7 令 $1 \leq i \leq n$，如果线性码 $[n,k,d]_q$ 中的码字的第 i 坐标分量可由该码字的其它不超过 r 个分量（也称为码字符号）来修复，则称第 i 坐标分量具有局部修复性 r。等价地说，存在对偶码 $\mathcal{C}^{\perp}$ 中的一个码字 $\boldsymbol{h}_i$ 使得 $i \in \mathrm{supp}(\boldsymbol{h}_i)$，并且 $|\mathrm{supp}(\boldsymbol{h}_i)| \leq r+1$。

定义 4.2.8 如果线性码 $[n,k,d]_q$ 中的码字的所有坐标分量都具有局部修复性 r，则称 $[n,k,d]_q$ 线性码 $\mathcal{C}$ 具有局部修复性 r，也称 $\mathcal{C}$ 为局部可修复码（*Locally Repairable Code*，简称为*LRC*），记为 $[n,k,d;r]_q$ *LRC*。

定义 4.2.9 对于一个 $[n,k,d;r]_2$ *LRC*，如果存在一组局部校验向量 $\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_l \in \mathcal{C}^{\perp}$ 使得 $\cup_{i=1}^{l} \mathrm{supp}(\boldsymbol{h}_i) = [n]$，$\mathrm{wt}(\boldsymbol{h}_i) = r+1$，而且 $\mathrm{supp}(\boldsymbol{h}_i) \cap \mathrm{supp}(\boldsymbol{h}_j) = \varnothing$ 对任意 $1 \leq i \neq j \leq l$ 成立，那么我们称 $[n,k,d;r]_2$ *LRC*具有不交修复组（*Disjoint Repair Groups*）。

4.3　具有不交修复组的二元LRCs的上界

在本节，我们基于经典编码理论中的Johnson界的思想给出具有不交修复组的二元LRCs的维数上界。令 $\mathcal{C}$ 为一个具有不交修复组的 $[n,k,d;r]_2$ LRC。不妨假设码 $\mathcal{C}$ 的校验

矩阵 $\mathbf{H}$ 由两部分组成。

$$\mathbf{H}=\begin{pmatrix}\mathbf{H}_L\\ \mathbf{H}_G\end{pmatrix}. \tag{4-3}$$

其中，矩阵 $\mathbf{H}_L$ 用来保证码 $\mathcal{C}$ 的局部修复性；矩阵 $\mathbf{H}_G$ 用来决定码 $\mathcal{C}$ 的极小距离。由于本章我们只考虑具有不交修复组的码，故可假设 $r+1$ 整除 n 。不失一般性，不妨设

$$\mathbf{H}_L=I_{\frac{n}{r+1}}\bigotimes\mathbf{1}_{r+1}.$$

注意到矩阵 $\mathbf{H}_L$ 的所有行向量的和是一个全 1 向量，则码 $\mathcal{C}$ 的极小距离必然为偶数。

定理4.3.1 设 $\mathcal{C}$ 为一个具有不交修复组的 $[n,k,d;r]_2$ *LRC*，其中 $d=2t+2$ ，$n=(r+1)l$ 。

1. 如果 $t+1$ 是一个奇数，我们有

$$k\le\frac{rn}{r+1}-\left\lceil\log_2(\sum_{0\le i_1+\cdots+i_l\le\lfloor\frac{d-1}{4}\rfloor}\prod_{j=1}^{l}\binom{r+1}{2i_j})\right\rceil. \tag{4-4}$$

2. 如果 $t+1$ 是一个偶数，则有

$$k\le\frac{rn}{r+1}-\left\lceil\log_2(\sum_{0\le i_1+\cdots+i_l\le\lfloor\frac{d-1}{4}\rfloor}\prod_{j=1}^{l}\binom{r+1}{2i_j}+\frac{\sum_{i_1+\cdots+i_l=\frac{d}{4}}\prod_{j=1}^{l}\binom{r+1}{2i_j}}{\lfloor\frac{n}{t+1}\rfloor})\right\rceil. \tag{4-5}$$

证明 设 $\{\mathbf{h}_1,\mathbf{h}_2,\cdots,\mathbf{h}_l\}$ 为具有不交修复组的局部可修复码 $\mathcal{C}$ 的一组局部校验向量。令 $L=\mathrm{span}_{\mathbb{F}_2}\{\mathbf{h}_1,\mathbf{h}_2,\cdots,\mathbf{h}_l\}$ ，$V=L^{\perp}$ 。显然有，$L\subseteq\mathcal{C}^{\perp}$ ，$\dim(L)=l$ 。则有 $\mathcal{C}\subseteq V$ ，$\dim(V)=n-l=\frac{rn}{r+1}$。

注意到 t 是码 $\mathcal{C}$ 的填充半径，并且以码字为球心，半径为 t 的球都不相交。令 $B_V(\mathbf{c},t)=\{\mathbf{v}\in V|d(\mathbf{c},\mathbf{v})\le t\}$，并将 $B_V(\mathbf{0},t)$ 简记为 $B_V(t)$ 。因为 $\mathcal{C}\subseteq V$ ，我们有 $|B_V(\mathbf{c},t)|=|B_V(t)|$ 。令 $\mathcal{N}$ 是与码 $\mathcal{C}$ 距离为 $t+1$ 的向量的集合，即，$\mathcal{N}=\{\mathbf{x}\in V|d(\mathcal{C},\mathbf{x})=t+1\}$ 。显然，我们有

$$|\mathcal{C}|\times|B_V(t)|+|\mathcal{N}|\le 2^{\dim(V)}. \tag{4-6}$$

我们首先计算球 $B_V(t)$ 的大小。注意到线性空间 L 的重量分布多项式为 $W_L(x,y)=(x^{r+1}+y^{r+1})^l$ 。由MacWilliams恒等式知，对偶空间 V 的重量分布多项式为

$$W_V(x,y)=\frac{1}{|L|}W_L(x+y,x-y)=\sum_{0\le u\le\frac{n}{2}}A_u x^{n-2u}y^{2u},$$

其中 $A_u = \sum_{i_1+\cdots+i_l=u} \prod_{j=1}^{l} \binom{r+1}{2i_j}$。则可导出

$$|B_V(t)| = A_0 + \cdots + A_{\lfloor \frac{d-1}{4} \rfloor} = \sum_{0 \le i_1+\cdots+i_l \le \lfloor \frac{d-1}{4} \rfloor} \prod_{j=1}^{l} \binom{r+1}{2i_j}. \tag{4-7}$$

然后，我们证明 $|\mathcal{N}|$ 的一个下界。

当 $t+1$ 为奇数时，容易得到 $|\mathcal{N}| = 0$。事实上，如果存在 $\mathbf{x} \in \mathcal{N} \subseteq V$ 使得 $d(\mathbf{c}, \mathbf{x}) = t+1$ 对某个 $\mathbf{c} \in \mathcal{C} \subseteq V$ 成立，则我们有 $\mathrm{wt}(\mathbf{c}-\mathbf{x}) = d(\mathbf{c}, \mathbf{x}) = t+1$，这是一个奇数。另一方面，由重量分布多项式 $W_V(x, y)$ 知，对任何 $\mathbf{v} \in V$，$\mathrm{wt}(\mathbf{v})$ 是一个偶数。这就得出矛盾！因此，界(4-4)可以由方程(4-6)和(4-7)直接推出。

当 $t+1$ 为偶数时，令 $\Omega = \{(\mathbf{c}, \mathbf{x}) \in \mathcal{C} \times \mathcal{N} | d(\mathbf{c}, \mathbf{x}) = t+1\}$，$\Omega_c = \{\mathbf{x} \in \mathcal{N} | (\mathbf{c}, \mathbf{x}) \in \Omega\}$。则有 $|\Omega| = \sum_{\mathbf{c} \in \mathcal{C}} |\Omega_{\mathbf{c}}|$。固定 $\mathbf{c} \in \mathcal{C}$，设 $\mathbf{x} \in V$ 是一个与码字 $\mathbf{c}$ 距离为 $t+1$ 的向量，即，$\mathrm{wt}(\mathbf{c}-\mathbf{x}) = t+1$。显然，这样的向量 $\mathbf{x}$ 共有 $A_{d/4}$ 个。

我们断言：这样的向量 $\mathbf{x}$ 都属于 $\Omega_{\mathbf{c}}$。因为 $\mathrm{wt}(\mathbf{c}-\mathbf{x}) = t+1$，我们知道 $d(\mathcal{C}, \mathbf{x}) \le t+1$。令 $\mathbf{c}' \in \mathcal{C}$ 且 $\mathbf{c}' \neq \mathbf{c}$。则由三角不等式，我们有 $d \le \mathrm{wt}(\mathbf{c}'-\mathbf{c}) = \mathrm{wt}(\mathbf{c}'-\mathbf{x}-(\mathbf{c}-\mathbf{x})) \le \mathrm{wt}(\mathbf{c}'-\mathbf{x}) + \mathrm{wt}(\mathbf{c}-\mathbf{x}) = \mathrm{wt}(\mathbf{c}'-\mathbf{x}) + t + 1$，这就导出 $\mathrm{wt}(\mathbf{c}'-\mathbf{x}) \ge t+1$。又因为 $\mathbf{c}' \in \mathcal{C}$ 选取的任意性以及之前的结论 $d(\mathcal{C}, \mathbf{x}) \le t+1$，我们得到 $d(\mathcal{C}, \mathbf{x}) = t+1$。因此，这样的向量 $\mathbf{x}$ 都落在 $\Omega_{\mathbf{c}}$ 中，则可知 $|\Omega_{\mathbf{c}}| = A_{d/4}$。所以

$$|\Omega| = |\mathcal{C}| \times A_{d/4}. \tag{4-8}$$

另一方面，固定 $\mathbf{x} \in \mathcal{N}$。我们将对码 $\mathcal{C}$ 中满足 $d(\mathbf{c}, \mathbf{x}) = t+1$ 的码字的个数给一个上界。显然，集合 $\{\mathbf{c}-\mathbf{x} | \mathbf{c} \in \mathcal{C}$ 且 $d(\mathbf{c}, \mathbf{x}) = t+1\}$ 是一个长为 n，重量为 $t+1$，极小距离为 $d = 2t+2$ 的二元常重码。因此，对每个 $\mathbf{x} \in \mathcal{N}$，满足 $d(\mathbf{c}, \mathbf{x}) = t+1$ 的码字的个数至多为 $\lfloor \frac{n}{t+1} \rfloor$。因此，

$$|\Omega| \le |\mathcal{N}| \times \left\lfloor \frac{n}{t+1} \right\rfloor. \tag{4-9}$$

所以，界(4-5)可由方程(4-6)、(4-7)、(4-8)和(4-9)直接导出。 □

注4.3.2 最近，在文献[68]中证明了界(4-4)对$d \ge 6$成立，我们的结果可以看做对它的一个推广。

注4.3.3 当 $d = 4$ 时，上界(4-5)退化为 $k \le \frac{rn}{r+1} - \lceil \log_2(1+r) \rceil$。注意到*Shahabinejad*等人[53]构造了参数为 $[n, k = \frac{rn}{r+1} - \lceil \log_2(1+r) \rceil, d = 4; r]_2$ 的具有不交修复组的局部可修复码，这说明我们的界是紧的。

注4.3.4 在文献[24]中，从本原循环码出发构造了码长为 $n=2^m-1$、局部修复性 $r=2$ 以及极小距离为 2、6 或 10的二元局部可修复码。后来，在文献[72]中，运用类似的方法对于参数 $n=2^m+1$、$r=2$ 以及 $d=10$ 的情形，也构造了一类新的二元局部可修复码。另外，在文献[68] 中，作者构造了 $[n=\frac{2^s-1}{2^t-1}, k\geq \frac{rn}{r+1}-s, d\geq 6; r=2^t]_2$ *LRC*。这些*LRCs*都具有不交修复组的结构且达到了我们的上界(4-4)。

在本节的最后，对于具有不交修复组的二元局部可修复码，我们给出在渐进意义下最优的一般性构造，这里的渐进最优是指当 n 趋于无穷时，码率达到上界。令 $S'=\{\beta_1,\beta_2,\cdots,\beta_n\}\subseteq \mathbb{F}_{2^{\lceil\log_2 n\rceil}}$，其中 $\beta_1,\beta_2,\cdots,\beta_n$ 是域中的不同的元素。定义 $S=\{\mathbf{a}_1,\mathbf{a}_2,\cdots,\mathbf{a}_n\}\subseteq \mathbb{F}^t_{2^{\lceil\log_2 n\rceil}}$，其中 $\mathbf{a}_i=(\beta_i,\beta_i^3,\cdots,\beta_i^{2t-1})^\top, i\in[n]$。

构造4.3.5 设 $\mathbf{H}_L=I_{\frac{n}{r+1}}\bigotimes \boldsymbol{1}_{r+1}$。令 $\mathbf{H}_G$ 是一个 $t\lceil\log_2 n\rceil\times n$ 的矩阵，对任意 $1\leq j\leq n$，它的第 j 列由向量$\mathbf{a}_j$作二元展开得到。则可定义一个型为(4-3)的矩阵 $\mathbf{H}$。进而由 $\mathbf{H}$ 作为校验矩阵定义了一个二元局部可修复码 $\mathcal{C}$。

定理4.3.6 由构造 4.3.5得到的码 $\mathcal{C}$ 是一个具有不交修复组的 $[n,k\geq \frac{rn}{r+1}-t\lceil\log_2 n\rceil, d\geq 2t+2; r]_2$ *LRC*。

证明 由于矩阵 $\mathbf{H}$ 的行数为$\frac{n}{r+1}+t\lceil\log_2 n\rceil$，我们知道 $k\geq \frac{rn}{r+1}-t\lceil\log_2 n\rceil$。又由矩阵 $\mathbf{H}_L$ 知，码 $\mathcal{C}$ 的局部修复性为 r。

现在我们证明极小距离 d 的下界。注意到矩阵 $\mathbf{H}_L$ 的所有行向量的和为 $\mathbf{1}_n$，则码 $\mathcal{C}$ 的极小距离必然为偶数。因此，只需要证明 $d\geq 2t+1$。假设存在码字 $\mathbf{c}\in\mathcal{C}$ 且 $2\leq \mathrm{wt}(\mathbf{c})\leq 2t$ 使得 $\mathbf{Hc}^\top=\mathbf{0}$。不失一般性，我们可以令 $\mathbf{c}=(c_1,\cdots,c_{2t},0,\cdots,0)$，这就导出 $\sum_{i=1}^{2t}c_i\mathbf{a}_i=\mathbf{0}$。因此，对任意 $s\in[t]$，有 $\sum_{i=1}^{2t}c_i\beta_i^{2s-1}=0$。对其两边同时取 2^b 次幂，我们得到 $\sum_{i=1}^{2t}c_i\beta_i^{2^b(2s-1)}=0$，其中 b 是一个非负整数。注意到，对每个非负整数 m，它都可以唯一地表示为 $m=2^se$，其中 e 为奇数。则我们就有 $\sum_{i=1}^{2t}c_i\beta_i^m=0,$其中 $m\geq 1$ 是一个整数。换句话说，我们得到下述齐次线性方程组 $\mathbf{M}x=0$ 的一个非零解 $x=(c_1\beta_1,c_2\beta_2,\cdots,c_{2t}\beta_{2t})^\top$，其中

$$\mathbf{M}=\begin{pmatrix}1 & 1 & \cdots & 1\\ \beta_1 & \beta_2 & \cdots & \beta_{2t}\\ \vdots & \vdots & \ddots & \vdots\\ \beta_1^{2t-1} & \beta_2^{2t-1} & \cdots & \beta_{2t}^{2t-1}\end{pmatrix}.$$

又因为 $\mathbf{M}$ 是Vandermonde矩阵，知它是满秩矩阵，即齐次线性方程组 $\mathbf{M}x=0$ 只有零解。矛盾! □

4.4 k-最优的二元LRCs的构造

在本节，我们将给出一些具有不交修复组的 k-最优的 $[n,k,d;r]_2$ LRCs的构造。校验矩阵 $\mathbf{H}$ 可以表示为如下形式:

$$\mathbf{H}=\begin{pmatrix}\mathbf{H}_L\\ \mathbf{H}_G\end{pmatrix}=\begin{pmatrix}\mathbf{H}_L^1 & \mathbf{H}_L^2 & \dots & \mathbf{H}_L^l\\ \mathbf{H}_G^1 & \mathbf{H}_G^2 & \dots & \mathbf{H}_G^l\end{pmatrix}, \tag{4-10}$$

其中 $l=\frac{n}{r+1}$ 。对于任何 $i\in[l]$ ，$\mathbf{H}_L^i$ 是一个 $l\times(r+1)$ 的矩阵，其第 i 行是 $\mathbf{1}_{r+1}$ ，而其它行的元素都是零；$\mathbf{H}_G^i$ 为 $\mathbf{H}_G$ 的第 i 块 $(n-k-l)\times(r+1)$ 子矩阵。

子矩阵 $\mathbf{H}_G=(\mathbf{H}_G^1\,\mathbf{H}_G^2\,\dots\,\mathbf{H}_G^l)$ 将用来决定码 $\mathcal{C}$ 的极小距离。众所周知：一个线性码的极小距离至少为 d 当且仅当它的校验矩阵中的任何 $d-1$ 列线性无关。

引理4.4.1 *令 $\mathcal{C}$ 是由型为(4-10)的校验矩阵 $\mathbf{H}$ 定义的码，其中 $l=\frac{n}{r+1}$ 。设 $t\geq 0$ 为一个整数。则 $d\geq 2t+2$ 当且仅当*

$$\sum_{i=1}^{l}\sum_{j=1}^{a_i}\boldsymbol{c}_j^i\neq\boldsymbol{0},$$

其中 $a_1,a_2,\cdots,a_l$ 满足以下两个条件：(1) 对任何 $1\leq i\leq l$ ，a_i 是一个偶数且 $0\leq a_i\leq\min\{2t,r+1\}$ ，(2) $2\leq\sum_{i=1}^{l}a_i\leq 2t$ ；并且 $\{\boldsymbol{c}_1^i,\boldsymbol{c}_2^i,\cdots,\boldsymbol{c}_{a_i}^i\}$ 是矩阵 $\mathbf{H}_G^i$ 中的任何 a_i 列的集合。

证明 令 $\mathbf{H}^{(i)}=\begin{pmatrix}\mathbf{H}_L^i\\ \mathbf{H}_G^i\end{pmatrix}$ 为 $\mathbf{H}$ 的第 i 块。且设 $\mathbf{h}_j^i$ 为矩阵 $\mathbf{H}^{(i)}$ 中满足 $\mathbf{h}_j^i|_S=\mathbf{c}_j^i$ 的列，其中 $S=[l+1,n-k]$ 。

我们首先证明必要性。因为 $d\geq 2t+2$ ，我们知道 $\mathbf{H}$ 中的任何 $\leq d-1$ 列都是线性无关。那么对任何 $a_1,a_2,\cdots,a_l$ 满足条件(1)和(2)，都有 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{h}_j^i\neq\mathbf{0}$ 。注意到 $\mathbf{H}_L^i$ 中任何偶数列的和为 $\mathbf{0}$ ，则有 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{c}_j^i\neq\mathbf{0}$ 。

对于充分性，我们只需要去证明 $\mathbf{H}$ 的任何 $2t+1$ 列线性无关。即，我们需要证明对任何 $m\in[2t+1]$ ，不存在 $\mathbf{H}$ 的 m 列求和为 $\mathbf{0}$ 。令 $m=\sum_{i=1}^{l}a_i$ ，且设 $\{\mathbf{h}_1^i,\mathbf{h}_2^i,\cdots,\mathbf{h}_{a_i}^i\}$ 是矩阵 $\mathbf{H}^{(i)}$ 中的任何 a_i 列的集合，其中 $1\leq i\leq l$ ，a_i 是一个整数且 $0\leq a_i\leq\min\{2t+1,r+1\}$。则我们需要证明 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{h}_j^i\neq\mathbf{0}$ 。

如果存在某个 $j \in [l]$，有 a_j 为奇数，那么 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{h}_j^i$ 的第 j 个坐标为 1，也就是 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{h}_j^i \neq \mathbf{0}$。所以我们可以假定：对任何 $j \in [l]$，a_j 都是偶数。注意到 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{h}_j^i|_S = \sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{c}_j^i \neq \mathbf{0}$，则有 $\sum_{i=1}^{l}\sum_{j=1}^{a_i}\mathbf{h}_j^i \neq \mathbf{0}$。这就完成了证明。 □

4.4.1 $d = 6$ 的 k-最优二元LRCs构造：一般的参数 r

首先，我们给出极小距离 $d \geq 6$ 的二元LRCs的充要条件，由引理 4.4.1，显然有下述的推论。

推论4.4.2 令 $\mathcal{C}$ 是由型为(4-10)的校验矩阵 $\mathbf{H}$ 定义的码，其中 $l = \frac{n}{r+1}$。则 $d \geq 6$ 当且仅当 $\mathbf{H}_G$ 中的列满足下列的条件：

(1) 对每个 $i \in [l]$，有 $\boldsymbol{c}_1^i + \boldsymbol{c}_2^i \neq \boldsymbol{0}$；

(2) 对每个 $i \in [l]$，有 $\boldsymbol{c}_1^i + \boldsymbol{c}_2^i + \boldsymbol{c}_3^i + \boldsymbol{c}_4^i \neq \boldsymbol{0}$;

(3) 对任何 $i \neq j \in [l]$，有$\boldsymbol{c}_1^i + \boldsymbol{c}_2^i + \boldsymbol{c}_1^j + \boldsymbol{c}_2^j \neq \boldsymbol{0}$。

为了更好地理解接下来的构造，我们先给出如下解释。首先，给定一个空间 W，可由弱无关集来构造一个由 W 中的向量组成的集合满足条件 (1) 和 (2)。然后令 W_i 是由矩阵 $\mathbf{H}_G^i$ 中的列向量生成的向量空间，则有 $\dim(W_i) \leq n-k-l$。为了保证条件 (3) 成立，一种简单的方法就是假定这些空间满足 $W_i \cap W_j = \{\mathbf{0}\}$，显然这样的空间可以从partial spread中选取。

注4.4.3 在最近的文献[43]同样得到了上述推论中的充分条件，也想到了运用*spread*作为工具，构造了一些 $d \geq 6$ 的一些二元局部可修复码，但是只有部分例子是最优的。在下文，我们会给出大量最优的码类！一个核心区别在于我们多了一个想法：弱无关集！

引理4.4.4 令 V 为 $\mathbb{F}_2^m$ 中的 t 维子空间，设 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_t\}$ 为 V 的一组基。若存在参数为 $[n, n-t, d \geq 5]$ 的二元线性码，设其校验矩阵为 $\mathbf{H} = (\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_n)$。那么集合 $T = \{\boldsymbol{0}\} \cup \{\boldsymbol{f}_i | i \in [n]\}$是 $\mathbb{F}_2$上的 4-弱无关集，其中 $\boldsymbol{f}_i = \sum_{j \in \mathrm{supp}(\boldsymbol{h}_i)} \boldsymbol{e}_j$。

证明 我们只需证明：对任何 $\{i_1, \ldots, i_r\} \subseteq [n]$ 且 $1 \leq r \leq 4$，有 $\sum_{j=1}^{r}\mathbf{f}_{i_j} \neq \mathbf{0}$。不失一般性，我们可以假设对任何 $1 \leq r \leq 4$，有 $\sum_{i=1}^{r}\mathbf{f}_i = 0$。那么有 $\sum_{j=1}^{r}\mathbf{h}_j = \mathbf{0}$，这就表明

$\{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_r\}$ 是线性相关的。由于 $\mathbf{H}$ 是极小距离 $d \geq 5$ 的二元线性码的校验矩阵，我们知道 $\mathbf{H}$ 中任何 ≤ 4 列都是线性无关的，这就得出矛盾! □

下面，对于一般的参数 r，我们给出两类 k-最优的二元局部可修复码。

4.4.1.1　第一类最优的二元LRCs

引理4.4.5 [42,68] 对任何整数 $m \geq 3$，都存在参数为 $[2^m, 2^m - 2m, \geq 5]$ 的二元线性码。

构造4.4.6 令 $r = 2^t$，$\{W_1, W_2, \cdots, W_a\}$ 为 $\mathbb{F}_2^s$ 上的一个极大*Partial* $2t$*-spread*。记 W_i 的一组基为 $\{\boldsymbol{e}_1^{(i)}, \boldsymbol{e}_2^{(i)}, \cdots, \boldsymbol{e}_{2t}^{(i)}\}$。当 $t \geq 3$ 时，由引理 4.4.5知，存在参数为 $[2^t, 2^t - 2t, \geq 5]_2$ 的线性码。则对每个 $i \in [a]$，定义 $T^{(i)}$ 为引理 4.4.4所给出的集合；当 $t = 1$、2时，我们定义 $T^{(i)} = \{\boldsymbol{0}, \boldsymbol{e}_1^{(i)}, \boldsymbol{e}_2^{(i)}, \cdots, \boldsymbol{e}_{2t}^{(i)}\}$。将集合 $T^{(i)}$ 中的向量作为列向量形成的 $s \times (r+1)$ 矩阵记为 $\mathbf{H}_G^i$。这样我们定义了一个型为(4-10)的矩阵 $\mathbf{H}$，其中 $\frac{s}{r} < l \leq a$。进而由 $\mathbf{H}$ 作为校验矩阵定义了一个二元局部可修复码，记为 $\mathcal{C}$。

定理4.4.7 由构造 4.4.6得到的码 $\mathcal{C}$ 是一个具有不交修复组的 $[n = (2^t+1)l, k \geq \frac{rn}{r+1} - s, d \geq 6; r = 2^t]_2$ *LRC*。进一步，当

$$\frac{2^{s-1}-1}{2^{t-1}(2^t+1)} < l \leq A_2(s, 2t, 4t),$$

我们有 $k = \frac{rn}{r+1} - s$ 以及 $d = 6$，即，码 $\mathcal{C}$ 达到界(4-4)，是 k-最优的局部可修复码。

证明 首先，由校验矩阵 $\mathbf{H}$ 的构造，显然有 $n = (2^t+1)l, k \geq \frac{rn}{r+1} - s$ 以及局部修复性 $r = 2^t$。然后，我们需要去证明 $d \geq 6$。则只需要证明矩阵 $\mathbf{H}_G$ 满足推论 4.4.2中的条件。由引理 4.4.4易知 $\mathbf{H}_G$ 满足条件 (1) 和 (2)。注意到对 $\mathbf{H}_G^i$ 中的任何两个向量 $\mathbf{c}_1^i, \mathbf{c}_2^i$，有$\mathbf{c}_1^i + \mathbf{c}_2^i$ 是子空间 W_i 中的一个非零向量。因为对任何 $i \neq j$，都有 $W_i \cap W_j = \{\mathbf{0}\}$。所以 $\mathbf{c}_1^i + \mathbf{c}_2^i$ 和 $\mathbf{c}_1^j + \mathbf{c}_2^j$ 为两个不同的向量。则条件 (3) 也成立。

现在我们说明，当 $\frac{2^{s-1}-1}{2^{t-1}(2^t+1)} < l \leq A_2(s, 2t, 4t)$ 时，$\mathcal{C}$ 是最优的。事实上，对于一个具有不交修复组的 $[n, k, d \geq 6; r]_2$ LRC，由上界(4-4) 知 $k \leq \frac{rn}{r+1} - \lceil \log_2(1 + \frac{r}{2}n) \rceil$。因为 $\frac{2^{s-1}-1}{2^{t-1}(2^t+1)} < l \leq A_2(s, 2t, 4t)$，所以 $2^{s-1} < 1 + \frac{rn}{2} \leq 2^s$。则有 $\lceil \log_2(1 + \frac{r}{2}n) \rceil = s$，这就意味着，在这种情形下，上界为 $k \leq \frac{rn}{r+1} - s$。结合之前的结论 $k \geq \frac{rn}{r+1} - s$，我们得到$k = \frac{rn}{r+1} - s$。最后，我们证明在这种情形下的极小距离 $d = 6$。事实上，如果 $d > 6$，由于码 $\mathcal{C}$ 的极小距离必然为偶数，我们有 $d \geq 8$。注意到 $1 + \frac{rn}{2} + \frac{\binom{l}{2}\binom{r+1}{2}\binom{r+1}{2}}{n/4} > 2^s$，则由方程(4-5)，我们得到 $k < \frac{rn}{r+1} - s$，这与之前的结论 $k = \frac{rn}{r+1} - s$ 矛盾! □

注4.4.8 如果在构造 4.4.6中取 $2t|s$ 、$s \geq 4t$ 以及 $l = A_2(s, 2t, 4t) = \frac{2^s-1}{2^{2t}-1}$ ，那么我们就得到了文献[68]中给出 k-最优的二元线性局部可修复码。

例4.4.9 令 $s \equiv u \pmod{2t}$ ，由引理 4.2.3知道 $A_2(s, 2t, 4t) \geq \frac{2^s-2^{2t}(2^u-1)-1}{2^{2t}-1}$ 。那么只要 $\frac{2^{s-1}-1}{2^{t-1}(2^t+1)} < l \leq \frac{2^s-2^{2t}(2^u-1)-1}{2^{2t}-1}$ （简单计算可知：当 $s \geq 5t-1$ 时，这样的 l 总是存在的），通过构造 4.4.6，我们总是可以得出参数为 $[n = (2^t+1)l, k = \frac{rn}{r+1} - s, d = 6; r = 2^t]_2$ 的局部可修复码，并且这类码达到了界(4-4)。另外，给定一对 r 和 s 的数值，上述的构造包含了大量的 k-最优的二元局部可修复码的例子（**图 4-1**可作为一个简单说明）。

s	l	n	k
4	$[3, 5]$	$3l$	$2l-4$
5	$[6, 9]$	$3l$	$2l-5$
6	$[11, 21]$	$3l$	$2l-6$
7	$[22, 41]$	$3l$	$2l-7$

图 4-1 $r = 2$、$s \in \{4, 5, 6, 7\}$ **时，具有不交修复组的最优二元LRCs的一些例子**

4.4.1.2 第二类最优的二元LRCs

引理4.4.10 [42] 对任何整数 $t \geq 3$ ，都存在参数为 $[2^t + 2^{\lfloor (t+1)/2 \rfloor} - 1, 2^t + 2^{\lfloor (t+1)/2 \rfloor} - 2t - 2, 5]$ 的二元线性码。

构造4.4.11 令 $r = 2^t + 2^{\lfloor (t+1)/2 \rfloor} - 1$，$\{W_1, W_2, \cdots, W_a\}$ 为 $\mathbb{F}_2^s$ 上的一个极大*partial* $(2t+1)$-*spread*。记 W_i 的一组基为 $\{\boldsymbol{e}_1^{(i)}, \boldsymbol{e}_2^{(i)}, \cdots, \boldsymbol{e}_{2t+1}^{(i)}\}$ 。当 $t \geq 3$ 时，由引理 4.4.10知，存在参数为 $[2^t + 2^{\lfloor (t+1)/2 \rfloor} - 1, 2^t + 2^{\lfloor (t+1)/2 \rfloor} - 2t - 2, 5]$ 的二元线性码。则对每个 $i \in [a]$ ，定义 $T^{(i)}$ 为引理 4.4.4所给出的集合；当 $t = 1$、2时，我们定义 $T^{(i)} = \{\boldsymbol{0}, \boldsymbol{e}_1^{(i)}, \boldsymbol{e}_2^{(i)}, \cdots, \boldsymbol{e}_{2t+1}^{(i)}\}$ 。将集合 $T^{(i)}$ 中的向量作为列向量形成的 $s \times (r+1)$ 矩阵记为 $\mathbf{H}_G^i$ 。这样我们定义了一个型为(4-10)的矩阵 $\mathbf{H}$ ，其中 $\frac{s}{r} < l \leq a$ 。进而由 $\mathbf{H}$ 作为校验矩阵定义了一个二元局部可修复码，记为 $\mathcal{C}$ 。

定理4.4.12 由构造 4.4.11得到的码 $\mathcal{C}$ 是一个具有不交修复组的 $[n = (r+1)l, k \geq \frac{rn}{r+1} - s, d \geq 6; r = 2^t + 2^{\lfloor (t+1)/2 \rfloor} - 1]_2$ ***LRC***。进一步，当

$$\frac{2^s - 2}{(2^t + 2^{\lfloor (t+1)/2 \rfloor} - 1)(2^t + 2^{\lfloor (t+1)/2 \rfloor})} < l \leq A_2(s, 2t+1, 4t+2),$$

我们有 $k=\frac{rn}{r+1}-s$ 以及 $d=6$，即，码 $\mathcal{C}$ 达到界(4-4)，是 k-最优的局部可修复码。

证明 类似于定理 4.4.7的证明，故略。 □

例4.4.13 设 $t=3$，我们有参数为 $[11,4,5]$ 的二元线性码。令 $\{W_1,W_2,\cdots,W_{129}\}$ 为线性空间 $\mathbb{F}_2^{14}$ 上的一个 7-*spread*。则当取 $125\leq l\leq 129$ 时，由定理 4.4.12，我们得到参数为 $[n=12l,k=11l-14,d=6;r=11]_2$ *LRCs*，这些码达到了界(4-4)。

例4.4.14 令$t=1$，我们有 $r=3$，则由定理 4.4.12知，当 $\frac{2^s-2}{12}<l\leq A_2(s,3,6)$ 时，我们都可以得到 $[n=4l,k=3l-s,d=6;r=3]_2$ 的 k-最优局部可修复码（**图 4-2**可作为一个简单说明）。

s	l	n	k
6	$[6,9]$	$4l$	$3l-6$
7	$[11,17]$	$4l$	$3l-7$
8	$[22,34]$	$4l$	$3l-8$

图 4-2　$r=3$、$s\in\{6,7,8\}$ **时，具有不交修复组的最优二元LRCs的一些例子**

4.4.2　几乎所有参数的 k-最优二元LRCs的构造：$r\in\{2,3\}$ 的情形

当在构造 4.4.6（或者构造 4.4.11）中取 $t=1$，我们可得到大量局部修复性 $r=2$（或者 $r=3$）的 k-最优二元LRCs。通过观察例 4.4.9可知，当 $l\in[3,41]\setminus\{10\}$，我们都可以构造出参数为 $[3l,2l-s,6;2]$ 的最优二元LRCs。我们将在引理 4.4.15和定理 4.4.16中证明这种现象的一般情况。然而，对于 $r=3$ 的情形，通过观察例 4.4.14可知，当 $l\in[6,34]\setminus\{10,18,19,20,21\}$，通过构造 4.4.11，我们也可以构造出参数为 $[4l,3l-s,6;3]$ 的最优二元LRCs。但看上去没有 $r=2$ 的情形好。在本小节，我们通过对构造 4.4.6进行稍微的调整，对 $r=3$ 给出一个不同的构造，这个构造几乎涵盖了所有的正整数 l，得到了类似 $r=2$ 优美的结果。

首先，我们先对参数为 $[n,k,6;2]_2$ 的最优二元局部可修复码做一个全面的分析。为了记号方便，我们设 $A_2(3,2,4):=1$。定义

$$N_m:=[A_2(2m-1,2,4)+2,A_2(2m+1,2,4)].$$

则我们有下面的引理。

引理4.4.15 集合 $\cup_{m=2}^{\infty} N_m$ 涵盖了除了形为 $\frac{2^{2m+1}-2}{3}$ 之外所有大于 2 的正整数。

证明 注意到 $N_m = [A_2(2m-1,2,4)+2, A_2(2m+1,2,4)] = [\frac{2^{2(m-1)+1}-2}{3}+1, \frac{2^{2m+1}-2}{3}-1]$，结论是显然的。 □

定理4.4.16 设 $n = 3l$ 且 $l \neq \frac{2^{2m+1}-2}{3}$，其中 $m \geq 2$ 是一个整数。则存在达到上界(4-4)的 $[n,k,6;2]_2$ ***LRC***，其中

$$k = \begin{cases} 2l-2m & \text{如果 } l \in [A_2(2m-1,2,4)+2, A_2(2m,2,4)], \\ 2l-2m-1 & \text{如果 } l \in [A_2(2m,2,4)+1, A_2(2m+1,2,4)]. \end{cases}$$

证明 在定理 4.4.7中取 $t=1$，$s=2m$ 或者 $2m+1$，可直接得出结论。 □

例4.4.17 令 $l = 4 \in [A_2(3,2,4)+2, A_2(4,2,4)] \subseteq N_2$。则有 $2m=4$。我们首先构造空间 $\mathbb{F}_2^4$ 中的一个 2-*spread*。设 α 是有限域 $\mathbb{F}_{2^4}$ 的一个本原元，则 $\{1,\alpha,\alpha^2,\alpha^3\}$ 是 $\mathbb{F}_{2^4}$ 在 $\mathbb{F}_2$ 上的一组基。取 $\beta = \alpha^5$，则我们得到一个 2-*spread*：$S = \left\{W_i = \mathrm{span}_{\mathbb{F}_2}\{\alpha^i, \alpha^i\beta\} | 0 \leq i \leq 4\right\}$。不失一般性，在构造 4.4.6中，我们可以选取 S 中的前四个子空间。则我们得到参数为 $[12,4,6;2]_2$ 的最优局部可修复码，其校验矩阵构造如下：

$$\mathbf{H} = \begin{pmatrix} 1&1&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&1&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&1&0&0&0&1 \\ 0&0&1&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&0&1&0&0&1 \end{pmatrix}.$$

注4.4.18 当 $l = \frac{2^{2m+1}-2}{3}$ 时，注意到 $A_2(2m+1,2,4) < l < A_2(2m+2,2,4)$，在构造 4.4.6中取 $s=2m+2$、$t=1$，我们得到参数为 $[n = 2^{2m+1}-2, k \geq \frac{2^{2m+2}-4}{3} - 2m - 2, d \geq 6; r=2]_2$ 局部可修复码。由上界(4-4)知 $k \leq \frac{2^{2m+2}-4}{3} - 2m - 1$，所以我们构造的这个码的维数至多比上界少 1。因此它是几乎最优的。

现在，我们对 $r=2$ 的校验矩阵 $\mathbf{H}$ 中的每一个子块 $\mathbf{H}^{(i)}$ 增加一行一列得到 $r=3$ 的情形，给出一个几乎对所有参数 l 都成立的 k-最优二元LRCs的构造。

构造4.4.19 令空间 $\mathbb{F}_2^s$ 上的一个极大*partial 2-spread*为 $\{W_1, W_2, \cdots, W_a\}$。记 W_i 的一组基为 $\{\boldsymbol{e}_1^{(i)}, \boldsymbol{e}_2^{(i)}\}$。令 $\frac{s+1}{3} < l \leq a$，则我们定义一个型为 (4-10)的矩阵 $\mathbf{H}$ 作为一个二元局部可修复码 $\mathcal{C}$ 的校验矩阵，其中它的子矩阵 $\mathbf{H}_G^i, i \in [l]$ 定义如下：

$$\mathbf{H}_G^i = \begin{pmatrix} \boldsymbol{0} & \boldsymbol{e}_1^{(i)} & \boldsymbol{e}_2^{(i)} & \boldsymbol{e}_1^{(i)} + \boldsymbol{e}_2^{(i)} \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

注4.4.20 类似于定理 4.4.7可以证明由构造 4.4.19得到的码 $\mathcal{C}$ 是一个参数为 $[n=4l, k \geq 3l-s-1, d \geq 6; r=3]_2$ 的局部可修复码。

下面的定理说明对几乎所有的被 4 整除的 n，我们都有一个 k-最优局部可修复码。

定理4.4.21 设 $n=4l$ 且 $l \neq \frac{2^{2m+1}-2}{3}$，其中 $m \geq 2$ 是一个整数，则存在达到上界(4-4)的 $[n, k, 6; 3]_2$ *LRC*，其中

$$k = \begin{cases} 3l-2m & \text{如果 } l \in [A_2(2m-1,2,4)+2, A_2(2m,2,4)], \\ 3l-2m-1 & \text{如果 } l \in [A_2(2m,2,4)+1, A_2(2m+1,2,4)]. \end{cases}$$

证明 情形 1: $l \in [A_2(2m-1,2,4)+2, A_2(2m,2,4)]$。

在构造 4.4.19中取 $s=2m$，由注 4.4.20知，码 $\mathcal{C}$ 是一个 $[n=4l, k \geq 3l-2m-1, d \geq 6; r=3]_2$ LRC。另一方面，由上界(4-4)知 $k \leq 3l - \lceil \log_2(1+6l) \rceil = 3l-2m-1$。因此 $k=3l-2m-1$。

然后，我们证明 $d=6$。事实上，如果 $d>6$，由于码 $\mathcal{C}$ 的极小距离必然为偶数，我们有 $d \geq 8$。对上界(4-5)进行简单的计算，我们知道 $k < 3l-2m-1$，这就与之前的结论 $k=3l-2m-1$ 矛盾!

情形 2: $l \in [A_2(2m,2,4)+1, A_2(2m+1,2,4)]$。

在构造 4.4.19中取 $s=2m+1$。剩下的证明和**情形 1**类似，故略。 □

例4.4.22 由例 4.4.17和构造 4.4.19，我们得到参数为 $[16,7,6;3]_2$ 最优局部可修复码，其校验矩阵为

$$\mathbf{H}=\begin{pmatrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1\\
0&0&1&1&0&1&0&1&0&0&1&1&0&0&0&0\\
0&1&0&1&0&0&0&0&0&0&1&1&0&0&1&1\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0
\end{pmatrix}.$$

注4.4.23 上面的例子也达到了*C-M*界(4-2)。此外，如果我们从空间 $\mathbb{F}_2^4$ 上一个 2-*spread*中取其所有的 5 个子空间，那么我们就得到了一个 $[20,10,6;3]_2$ *LRC*，同样地，这个例子也达到了*C-M*界(4-2)。

注4.4.24 当 $l=\frac{2^{2m+1}-2}{3}$ 时，注意到 $A_2(2m+1,2,4)<l<A_2(2m+2,2,4)$，在构造 4.4.19中取 $s=2m+2$，我们得到参数为 $[n=\frac{4(2^{2m+1}-2)}{3},k\geq 2^{2m+1}-2m-5,d\geq 6;r=3]_2$ 局部可修复码。由上界(4-4)知 $k\leq 2^{2m+1}-2m-4$，所以我们构造的这个码的维数至多比上界少 1。因此它是几乎最优的。

4.5 讨论与总结

在本节，我们先对极小距离 $d\geq 8$ 的情形进行讨论，即如何去构造具有不交修复组的 k-最优的二元局部可修复码。为了方便起见，讨论 $r=2$ 的情形。由引理 4.4.1可直接导出下面的推论。

推论4.5.1 令 $\mathcal{C}$ 是由型为(4-10)的校验矩阵 $\mathbf{H}$ 定义的码，其中 $n=3l$。则 $d\geq 8$ 当且仅当 $\mathbf{H}_G$ 中的列满足下列的条件：

(1) 对每个 $u\in[l]$，有 $\boldsymbol{c}_1^u+\boldsymbol{c}_2^u\neq\boldsymbol{0}$；

(2) 对任何 $1 \le u < v \le l$，有 $\boldsymbol{c}_1^u + \boldsymbol{c}_2^u + \boldsymbol{c}_1^v + \boldsymbol{c}_2^v \neq \boldsymbol{0}$；

(3) 对任何 $1 \le u < v < w \le l$，有 $\boldsymbol{c}_1^u + \boldsymbol{c}_2^u + \boldsymbol{c}_1^v + \boldsymbol{c}_2^v + \boldsymbol{c}_1^w + \boldsymbol{c}_2^w \neq \boldsymbol{0}$。

显然，从一个极大partial 2-spread S中选取的子空间可以保证条件（1）和（2）成立。为了使得条件（3）成立，我们需要从 S 中选取满足某种性质**P**的子集 Y，也就是定义性质**P**为：对 Y 中的任何三个子空间，不妨记为 W_i, W_j, W_k，满足 $\dim(W_i + W_j + W_k) = 6$。则这样的子集 Y 就可以用来构造 $d \ge 8$ 的局部可修复码。

构造4.5.2 令 $S = \{W_1, W_2, \cdots, W_a\}$ 为空间 $\mathbb{F}_2^s$ 中的一个极大*partial 2-spread*。设集合 Y 是 S 中满足性质***P***的最大子集，并且设其大小为 b。则可设 $Y = \{W_{y_1}, W_{y_2}, \cdots, W_{y_b}\}$。令 $\{\boldsymbol{e}_1^{(i)}, \boldsymbol{e}_2^{(i)}\}$ 为子空间 W_{y_i} 的一组基。当 $\frac{s}{2} < l \le b$ 时，我们可以定义一个型为 (4-10)的矩阵 $\mathbf{H}$ 作为一个参数为 $[n = 3l, k \ge 2l - s, d \ge 8; r = 2]_2$ 的局部可修复码 $\mathcal{C}$ 的校验矩阵，其中它的子矩阵 $\mathbf{H}_G^i, i \in [l]$ 定义如下：

$$\mathbf{H}_G^i = \begin{pmatrix} \boldsymbol{0} & \boldsymbol{e}_1^{(i)} & \boldsymbol{e}_2^{(i)} \end{pmatrix}.$$

例4.5.3 设 α 是有限域 $\mathbb{F}_{2^6}$ 的本原元，且其极小多项式为 $x^6 + x^4 + x^3 + x + 1$。令 S 为空间 $\mathbb{F}_2^6$ 中的一个 2-*spread*。我们知道 $|S| = A_2(6, 2, 4) = 21$。事实上，$S = \{W_i = \mathrm{span}_{\mathbb{F}_2}\{\alpha^i, \beta\alpha^i\} | 0 \le i \le 20\}$，其中 $\beta = \alpha^{21}$。通过计算机搜索，我们可以得到一个合适的子集 $Y = \{W_0, W_1, W_2, W_3, W_{10}, W_{19}\}$。取 $l = 6$，我们得到一个达到上界(4-5)的 $[18, 6, 8; 2]_2$ *LRC*，其校验矩阵见**图 4-3**。

注4.5.4 如果我们在上面的例子中取 $l = 5$，那么我们就得到一个 $[15, 4, 8; 2]_2$ *LRC*。此外，通过构造 4.4.19中的技巧，我们也可以得到参数为 $[20, 8, 8; 3]_2$ 和 $[24, 11, 8; 3]_2$ 的局部可修复码。这几个例子都达到了上界(4-5)。

在本章，我们通过 4-弱无关集和(partial) spreads构造了极小距离为 6 的若干类 k-最优二元局部可修复码；特别地，对于 $r \in \{2, 3\}$ 的情形，我们得到了几乎所有参数的 k-最优二元局部可修复码。然而当极小距离 $d \ge 8$ 时，构造变得更加困难。对于 $d = 8$ 的情形，当考虑 $r = \{2, 3\}$ 时，我们提出了一种可能得到最优二元局部可修复码的方法。即，我们首先需要构造满足性质**P** 的某个partial spread 的子集；而对于比较大的 r，自然地，可能需要去考虑 6-弱无关集的构造。另外，如果能对一般的参数 d，给出达到定理 4.3.1中的界

$$\mathbf{H}=\begin{pmatrix}
1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
1&0&1&0&0&0&0&0&0&0&1&1&1&1&0&0&1&1\\
0&1&1&1&0&1&0&0&0&0&1&1&0&0&0&1&0&1\\
0&1&1&0&1&1&1&0&1&0&0&0&0&0&0&1&1&0\\
0&1&1&0&1&1&0&1&1&1&1&0&0&1&1&1&0&1\\
0&0&0&0&1&1&0&1&1&0&0&0&1&1&0&0&1&1\\
0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&1&0&1
\end{pmatrix}.$$

图 4-3 $[18,6,8;2]_2$ **LRC的校验矩阵**

的局部可修复码，这是一件非常有意义的工作，我们今后会考虑这方面的工作。

5 其它在研问题

本章补充了在攻读博士学位期间的其它研究工作，只对这些课题的进展做简要介绍而不再展开论述。

5.1 数字指纹码

在数字指纹与多媒体广播加密中，经常会考虑如何有效地防止盗版剽窃行为。在美密会(1994)上，Chor等人提出了“Tracing traitors”，即追踪盗版。其实就是如何去设计那些具有追踪性能的码，如父代识别码（Identifying Parent Property Codes，简称IPP Codes）、追踪码（Traceability Codes，简称TA codes）。特别地，该领域内一个核心问题就是：给定码长 N 、字母集大小 q 和码的强度 t ，确定这些追踪性能的码类的极大码字数量。

令 $M_{IPPC}(N,q,t)$ 和 $M_{TA}(N,q,t)$ 分别为 t-IPP码和 t-TA码的极大码字数量。我们对此问题的贡献主要为：

1. 我们证明了 $M_{IPPC}(N,q,t) \leq rq^{\lceil N/(v-1)\rceil} + (v-1-r)q^{\lfloor N/(v-1)\rfloor}$ ，其中 $v = \lfloor (t/2+1)^2 \rfloor, 0 \leq r \leq v-2$ 以及 $N \equiv r \mod (v-1)$ 。这一结果改进了Blackburn[7]、Alon和Stav[2]给出的两个著名上界。

2. Blackburn、Etzion和Ng[8]在 2010 年提出：对任何的 t ，是否都存在只与码长 N 有关的常数 c ，使得 $M_{TA}(N,q,t) \leq cq^{\lceil N/t^2 \rceil}$ ？我们证明了 $t=3$ 的情形，回答是肯定的。这是研究 3-TA码的历史上第一个非平凡的上界。

本工作已发表在《Designs, Codes and Cryptography》。

5.2 再生码

大数据时代决定了数据存储方式的改变，谷歌等商业公司的运行经验表明，现实中最常见的数据损坏情况是单个存储节点（磁盘）因为设备损坏、自然灾害等因素而失效。在

节点失效后，需要即刻加入新的节点来代替失效的节点，以维持整个系统的可靠性。基于复制或纠删码的两种传统策略，重建丢失节点的数据需要消耗较大的系统资源，亟需设计一种更好的存储编码方案以提高单个存储节点的修复效率。单个存储节点的修复效率的两个重要的度量指标是修复带宽和修复度（也就是每次修复所访问的节点数目）。考虑修复度这个指标就是本文第 4 章所考虑的局部可修复码。本部分将对修复带宽这个指标进行概述。

修复带宽，即修复单个节点需要从系统中传递的数据总量。刻画修复带宽与各节点存储容量之间的关联，是分布式存储问题中最先受到关注的优化目标，其奠基性的工作源于Dimakis等人在2010年的工作[13]，他们率先在分布式存储系统中引入网络编码的思想，提出了再生码（Regenerating Codes）这一概念。再生码模型中的基本设定是：信息被编码存储于 n 个节点之中，其中读取任意 k 个节点可以完全恢复所有信息，每一个损坏的节点可被之外的任意 d 个节点所修复。通过对网络信息流图模型的分析，利用网络编码中的“最大流最小割原理”得到了分布式存储系统中各节点存储容量与修复带宽之间的理论下界（Cut-set Bound）。之后的工作致力于达到或接近此下界的再生码的设计与构造，尤其是特殊的两种码：最小带宽再生码（Minimum Bandwidth Regenerating Codes, MBR）和最小存储再生码（Minimum Storage Regenerating Codes, MSR）。

最近，Goparaju等人[25]介绍了一种只考虑系统节点修复时，对所有的 $d\,(k \le d \le n-1)$ 同时达到最优修复带宽的最小存储再生码的构造方法。但是它的一个劣势就是子包(sub-packetization) α 的急剧增大。当考虑如何减小子包 α 时，他们提出了一个有趣的组合问题：如何去优化 (r,θ)-张量矩阵使得其列数最小。

设 $\theta(r)$ 是存在 (r,θ)-张量矩阵的最小整数 θ。Goparaju、Fazeli和Vardy (2017)给出了这样的张量矩阵的一个平凡构造，其中$\theta = \mathcal{O}(2^r)$ 。我们的工作就是证明了 $\theta(r)$ 的下界，并且基于完美哈希族给出了 (r,θ)-张量矩阵的一种构造，进而得到 $\theta(r)$ 的一个非平方上界，并且考虑其渐进结果，得到了 $\Omega(2^{0.5307r}) \lesssim \theta(r) \lesssim \mathcal{O}(2^{0.9355r})$ 。

本工作已整理成初稿。

5.3 极大可修复码

近年来，人们在研究局部修复码的同时，也希望存储系统具有极大的容错能力，即拥有MDS码的性质（任何 k 个节点存储的信息可译得完整数据）。微软研究院首先在 2007 年提出了极大可修复码（Maximally Recoverable Codes）的模型，这一模型涵盖了部分先前的码类，考虑了存储系统特定的拓扑结构。他们考虑了存储系统的一类最简单拓扑结构：

即任何校验位都是只由若干部分信息位生成，不涉及其它校验位，我们把这些校验位称之为局部校验位。2013 年，IBM公司Blaum等人考虑磁盘阵列下的修复问题时，引入了全局校验位（这些校验位是由全部信息位生成的），我们用符号 h 表示全局校验位的数目，并对 $h=1$ 、2 的情形，给出了极大可修复码的构造。微软研究院的Gopalan等人在2014年不仅考虑了 h 为常数阶，局部性参数 r 为常数阶，信息节点数 k 趋于无穷的渐进情形下的极大可修复码的构造，而且对 $h=3$ 、4 也有进一步的结果，并且将极大可修复码的概念推广到任意拓扑结构，并证明了其存在性。

在 2017 年的SODA会议上，Gopalan等人从实际应用出发，提出了网格形的拓扑结构，统一了之前研究的拓扑结构。具体模型可以表示如下：网格拓扑用 $T_{m\times n}(a,b,h)$ 表示，码字存储形式为 $m\times n$ 的矩阵，每一列上的信息之间满足 a 个校验方程，每一行上的信息之间满足 b 个校验方程，整个矩阵最终还需满足 h 个全局校验方程。也可以等价地考虑一个由 $(m-a)(n-b)-h$ 个信息位和由这些信息位所满足的 h 个校验位形成的的矩阵，进而在每列增加 a 个校验，每行增加 b 个校验以实现这个拓扑。$T_{m\times n}(a,b,h)$ 极大可修复码的一些特殊情形对应于若干先前的码类，如：$T_{m\times n}(0,0,h)$ 是经典的MDS码；$T_{m\times n}(0,b,h)$ 即为局部可修复码；$T_{m\times n}(a,b,0)$ 就是经典的张量积码。当 $a>0$、$b>0$ 以及 $h>0$ 时，Gopalan等人对 $T_{m\times n}(a,b,h)$ 极大可修复码所需的字母集的大小给出了第一个指数型下界；指出对于 $m=n$ 、$a=b=h=1$ 这一情形，所需的字母集大小等价于对完全二部图上的边的赋值问题；对 $T_{m\times n}(1,b,0)$ 的情形，给出了它的极大可修复的擦除类型的充分必要条件。之后的FOCS会议上，由Kane等人，对 $T_{n\times n}(1,1,1)$ 给出了所需要的字母集 2^d 的上下界，其中下界 $d=n/2-2$ 依赖于运用对称群表示论的方法对Birkhoff polytope graph 的独立数的估计，上界 $d=3n$ 来自递归构造完全二部图上的边的赋值。以上这些结果都只是说明了极大可修复码的存在性。然而在具体的构造方面，目前所知甚少。甚至对于 $a>1$ 时的极大可修复张量积码的可修复的擦除类型还没刻画清楚，更何谈构造。

我们对此问题的贡献是：对于极大可修复张量积码，给出了 $T_{m\times n}(1,b,0)$ 的所需字母集的大小的一个上界，以及 $T_{3\times n}(1,3,0)$ 的具体构造结果。对其它参数的构造还在研究中。

参考文献

[1] A. Akbary, D. Ghioca, and Q. Wang. On constructing permutations of finite fields. *Finite Fields Appl.*, 17:51–67, 2011.

[2] N. Alon and U. Stav. New bounds on parent-identifying codes: the case of multiple parents. *Combin. Probab. Comput.*, 13(6):795–807, 2004.

[3] S. B. Balaji, K. P. Prasanth, and P. V. Kumar. Binary codes with locality for multiple erasures having short block length. In *IEEE International Symposium on Information Theory*, pages 655–659, 2016.

[4] A. Barg, I. Tamo, and S. Vlăduţ. Locally recoverable codes on algebraic curves. *IEEE Trans. Inform. Theory*, 63(8):4928–4939, 2017.

[5] E. R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Inform. Control*, 10:553–564, 1967.

[6] A. Beutelspacher. Partial spreads in finite projective spaces and partial designs. *Math. Z.*, 145(3):211–229, 1975.

[7] S. R. Blackburn. An upper bound on the size of a code with the k-identifiable parent property. *J. Combin. Theory Ser. A*, 102(1):179–185, 2003.

[8] S. R. Blackburn, T. Etzion, and S. Ng. Traceability codes. *J. Combin. Theory Ser. A*, 117(8):1049–1057, 2010.

[9] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions. *Int. J. Inf. Coding Theory*, 1(2):149–170, 2010.

[10] V. Cadambe and A. Mazumdar. Bounds on the size of locally recoverable codes. *IEEE Trans. Inform. Theory*, 61(11):5787–5794, 2015.

[11] P. Charpin and G. M. Kyureghyan. Cubic monomial bent functions: a subclass of $\mathcal{M}$. *SIAM J. Discrete Math.*, 22(2):650–665, 2008.

[12] L. E. Dickson. Criteria for the irreducibility of functions in a finite field. *Bull. Amer. Math. Soc.*, 13(1):1–8, 1906.

[13] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran. Network coding for distributed storage systems. *IEEE Trans. Inform. Theory*, 56(9):4539–4551, 2010.

[14] C. Ding, L. Qu, Q. Wang, J. Yuan, and P. Yuan. Permutation trinomials over finite fields with even characteristic. *SIAM J. Discrete Math.*, 29(1):79–92, 2015.

[15] C. Ding and J. Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.

[16] H. Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, 45(4):1271–1275, 1999.

[17] H. Dobbertin. Kasami power functions, permutation polynomials and cyclic difference sets. In *Difference sets, sequences and their correlation properties (Bad Windsheim, 1998)*, volume 542 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 133–158. Kluwer Acad. Publ., Dordrecht, 1999.

[18] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence. The maximum size of a partial 3-spread in a finite vector space over $\mathrm{GF}(2)$. *Des. Codes Cryptogr.*, 54(2):101–107, 2010.

[19] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Trans. Inform. Theory*, 57(2):1165–1173, 2011.

[20] M. Forbes and S. Yekhanin. On the locality of codeword symbols in non-linear codes. *Discrete Math.*, 324:78–84, 2014.

[21] Q. Fu, R. Li, L. Guo, and L. Lv. Locality of optimal binary codes. *Finite Fields Appl.*, 48:371–394, 2017.

[22] P. Gopalan, C. Huang, B. Jenkins, and S. Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Trans. Inform. Theory*, 60(9):5245–5256, 2014.

[23] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin. On the locality of codeword symbols. *IEEE Trans. Inform. Theory*, 58(11):6925–6934, 2012.

[24] S. Goparaju and R. Calderbank. Binary cyclic codes that are locally repairable. In *IEEE International Symposium on Information Theory*, pages 676–680, 2014.

[25] S. Goparaju, A. Fazeli, and A. Vardy. Minimum storage regenerating codes for all parameters. *IEEE Trans. Inform. Theory*, 63(10):6318–6328, 2017.

[26] R. Gupta and R. K. Sharma. Some new classes of permutation trinomials over finite fields with even characteristic. *Finite Fields Appl.*, 41:89–96, 2016.

[27] J. Hao, S. Xia, and B. Chen. Some results on optimal locally repairable codes. In *IEEE International Symposium on Information Theory*, pages 440–444, 2016.

[28] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.

[29] X. Hou. Determination of a type of permutation trinomials over finite fields. *Acta Arith.*, 166(3):253–278, 2014.

[30] X. Hou. Determination of a type of permutation trinomials over finite fields, II. *Finite Fields Appl.*, 35:16–35, 2015.

[31] X. Hou. Permutation polynomials over finite fields—a survey of recent advances. *Finite Fields Appl.*, 32:82–119, 2015.

[32] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, S. Yekhanin, et al. Erasure coding in windows azure storage. In *USENIX Annual Technical Conference*, pages 15–26, 2012.

[33] P. Huang, E. Yaakobi, H. Uchikawa, and P. H. Siegel. Binary linear locally repairable codes. *IEEE Trans. Inform. Theory*, 62(11):6268–6283, 2016.

[34] G. Kyureghyan and M. Zieve. Permutation polynomials of the form $x + \gamma tr(x^k)$. In *Contemporary Developments in Finite Fields and Applications*, pages 178–194. World Scientific, 2016.

[35] Y. Laigle-Chapuy. Permutation polynomials and applications to coding theory. *Finite Fields Appl.*, 13:58–70, 2007.

[36] K. Li, L. Qu, and X. Chen. New classes of permutation binomials and permutation trinomials over finite fields. *Finite Fields Appl.*, 43:69–85, 2017.

[37] K. Li, L. Qu, C. Li, and S. Fu. New permutation trinomials constructed from fractional polynomials. 2016. arXiv:1605.06216.

[38] N. Li and T. Helleseth. New permutation trinomials from Niho exponents over finite fields with even characteristic. 2016. arXiv:1606.03768.

[39] N. Li and T. Helleseth. Several classes of permutation trinomials from Niho exponents. *Cryptography and Communications*, 9(6):693–705, Nov 2017.

[40] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983.

[41] J. Ma, T. Zhang, T. Feng, and G. Ge. Some new results on permutation polynomials over finite fields. *Des. Codes Cryptogr.*, 83(2):425–443, 2017.

[42] F. J. Macwilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland, 1977.

[43] M. Y. Nam and H. Y. Song. Binary locally repairable codes with minimum distance at least six based on partial t-spreads. *IEEE Communications Letters*, 21(8):1683–1686, 2017.

[44] H. Niederreiter and K. H. Robinson. Complete mappings of finite fields. *J. Austral. Math. Soc. Ser. A*, 33(2):197–212, 1982.

[45] F. Oggier and A. Datta. Self-repairing homomorphic codes for distributed storage systems. In *INFOCOM, 2011 Proceedings IEEE*, pages 1215–1223, 2011.

[46] L. Pamies-Juarez, H. D. L. Hollmann, and F. Oggier. Locally repairable codes with multiple repair alternatives. In *IEEE International Symposium on Information Theory*, pages 892–896, 2013.

[47] D. S. Papailiopoulos and A. G. Dimakis. Locally repairable codes. In *IEEE International Symposium on Information Theory*, pages 2771–2775, 2012.

[48] D. S. Papailiopoulos, J. Luo, A. G. Dimakis, C. Huang, and J. Li. Simple regenerating codes: Network coding for cloud storage. In *INFOCOM, 2012 Proceedings IEEE*, pages 2801–2805, 2012.

[49] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar. Optimal linear codes with a local-error-correction property. In *IEEE International Symposium on Information Theory*, pages 2776–2780, 2012.

[50] N. Prakash, V. Lalitha, and P. V. Kumar. Codes with locality for two erasures. In *IEEE International Symposium on Information Theory*, pages 1962–1966, 2014.

[51] L. Qu, Y. Tan, C. H. Tan, and C. Li. Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. *IEEE Trans. Inform. Theory*, 59(7):4675–4686, 2013.

[52] M. Sathiamoorthy, M. Asteris, D. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur. XORing elephants: Novel erasure codes for big data. In *Proceedings of the VLDB Endowment*, volume 6, pages 325–336. VLDB Endowment, 2013.

[53] M. Shahabinejad, M. Khabbazian, and M. Ardakani. A class of binary locally repairable codes. *IEEE Transactions on Communications*, 64(8):3182–3193, 2016.

[54] N. Silberstein, A. S. Rawat, O. Koyluoglu, and S. Vishwanath. Optimal locally repairable codes via rank-metric codes. In *IEEE International Symposium on Information Theory*, pages 1819–1823, 2013.

[55] N. Silberstein and A. Zeh. Optimal binary locally repairable codes via anticodes. In *IEEE International Symposium on Information Theory*, pages 1247–1251, 2015.

[56] W. Song, K. Cai, C. Yuen, K. Cai, and G. Han. On sequential locally repairable codes. *IEEE Transactions on Information Theory*, 64(5):3513–3527, 2018.

[57] W. Song, S. H. Dau, C. Yuen, and T. J. Li. Optimal locally repairable linear codes. *IEEE Journal on Selected Areas in Communications*, 32(5):1019–1036, 2014.

[58] J. Sun and O. Y. Takeshita. Interleavers for turbo codes using permutation polynomials over integer rings. *IEEE Trans. Inform. Theory*, 51(1):101–119, 2005.

[59] I. Tamo and A. Barg. Bounds on locally recoverable codes with multiple recovering sets. In *IEEE International Symposium on Information Theory*, pages 691–695, 2014.

[60] I. Tamo and A. Barg. A family of optimal locally recoverable codes. *IEEE Trans. Inform. Theory*, 60(8):4661–4676, 2014.

[61] I. Tamo, A. Barg, S. Goparaju, and R. Calderbank. Cyclic LRC codes, binary LRC codes, and upper bounds on the distance of cyclic codes. *Int. J. Inf. Coding Theory*, 3(4):345–364, 2016.

[62] I. Tamo, D. S. Papailiopoulos, and A. G. Dimakis. Optimal locally repairable codes and connections to matroid theory. In *IEEE International Symposium on Information Theory*, pages 1814–1818, 2013.

[63] Z. Tu, X. Zeng, and L. Hu. Several classes of complete permutation polynomials. *Finite Fields Appl.*, 25:182–193, 2014.

[64] Z. Tu, X. Zeng, L. Hu, and C. Li. A class of binomial permutation polynomials. 2013. arXiv:1310.0337.

[65] A. Wang and Z. Zhang. Repair locality with multiple erasure tolerance. *IEEE Trans. Inform. Theory*, 60(11):6979–6987, 2014.

[66] A. Wang and Z. Zhang. An integer programming-based bound for locally repairable codes. *IEEE Trans. Inform. Theory*, 61(10):5280–5294, 2015.

[67] A. Wang, Z. Zhang, and D. Lin. Two classes of (r, t)-locally repairable codes. In *IEEE International Symposium on Information Theory*, pages 445–449, 2016.

[68] A. Wang, Z. Zhang, and D. Lin. Bounds and constructions for linear locally repairable codes over binary fields. In *IEEE International Symposium on Information Theory*, pages 2033–2037, 2017.

[69] G. Wu and N. Li. Several classes of permutation trinomials over $\mathbb{F}_{5^n}$ from Niho exponents. 2017. arXiv:1702.06446.

[70] G. Wu, N. Li, T. Helleseth, and Y. Zhang. Some classes of monomial complete permutation polynomials over finite fields of characteristic two. *Finite Fields Appl.*, 28:148–165, 2014.

[71] G. Wu, N. Li, T. Helleseth, and Y. Zhang. Some classes of complete permutation polynomials over $\mathbb{F}_q$. *Sci. China Math.*, 58(10):2081–2094, 2015.

[72] A. Zeh and E. Yaakobi. Optimal linear and cyclic locally repairable codes over small fields. In *Information Theory Workshop*, pages 1–5, 2015.

[73] Z. Zha, L. Hu, and S. Fan. Further results on permutation trinomials over finite fields with even characteristic. *Finite Fields Appl.*, 45:43–52, 2017.

[74] M. E. Zieve. Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares. 2013. arXiv:1312.1325.

攻读博士学位期间主要研究成果

1. Jingxue Ma, Tao Zhang, Tao Feng, Gennian Ge, Some new results on permutation polynomials over finite fields, Des. Codes Cryptogr., 83 (2017), pp. 425-443.

2. Jingxue Ma, Gennian Ge, A note on permutation polynomials over finite fields, Finite Fields Appl., 48 (2017), pp. 261-270.

3. Chong Shangguan, Jingxue Ma, Gennian Ge, New upper bounds for parent-identifying codes and traceability codes, Des. Codes Cryptogr., 86 (2018), pp. 1727-1737.

4. Jingxue Ma, Gennian Ge, Optimal binary linear locally repairable codes with disjoint repair groups, (2017), submitted.

5. Jingxue Ma, Gennian Ge, Bound and construction on (r, θ)-product matrix with application to MSR codes, in preparation.