密级:_____

中国科学院大学
University of Chinese Academy of Sciences

博士学位论文

布尔函数在密码学中的应用

作者姓名: 张 寅

指导教师: 林东岱 研究员

中国科学院信息工程研究所

学位类别: 工学博士

学科专业: 信息安全

培养单位: 中国科学院信息工程研究所

2013 年 5 月

Applications of Boolean Functions in Cryptography

By

Yin Zhang

A Dissertation Submitted to

University of Chinese Academy of Sciences

In partial fulfillment of the requirement

For the degree of

Doctor of Information Security

Institute of Information Engineering

Chinese Academy of Sciences

May, 2013

中国科学院信息工程研究所
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林东岱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内容外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得中国科学院信息工程研究所或其他教育机构的学位或证书而使用过的材料。与我共同工作的同志对本研究所做的任何贡献均已在论文中做了明确的说明并表示谢意。

论文与资料若有不实之处，本人承担一切相关责任。

学位论文作者签名：张寅　　签字日期：2013年5月13日

学位论文版权使用授权说明

本学位论文作者完全了解中国科学院信息工程研究所有关保留、使用学位论文的规定。特授权中国科学院信息工程研究所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，并采用影印、缩印或扫描等复制手段保存、汇编，以供查阅和借阅。同意研究所向国家有关部门或机构送交论文的复印件和磁盘。

（保密的论文在解密后应遵循此规定）

学位论文作者签名：张寅　　导师签名：林东岱

签字日期：2013年5月13日　　签字日期：2013年5月13日

摘　要

布尔函数在流密码，分组密码和散列函数的设计中都有着广泛的应用。很多布尔函数所需要遵循的密码学准则都是在对基于线性反馈移位寄存器和过滤函数的流密码系统的研究中产生的，如平衡性，高代数次数，高非线性度，高相关免疫度等等。而寻找满足一定密码学性质的布尔函数是密码学理论中最基本的问题之一。在这篇论文里，我们针对一些特殊的布尔函数类，在已有的研究基础上，进一步的探究了它们的密码学性质，如*Bent*函数的存在性研究，布尔函数对快速代数攻击的抵抗程度研究，布尔函数的谱免疫度研究等等。

本文的主要成果和贡献如下：

首先，研究了*Bent*函数在代数标准型不包含 d 次以下单项式的布尔函数类中的存在性。证明了，如果对于这个函数类中的布尔函数，其代数标准型中单项式的个数小于 $n+d-3$，那么它不是*Bent*函数。同时，这个函数类中*Bent*函数的 d 值是小于 $\lceil 3n/8+3/4 \rceil$ 的。

第二，提出了一个有效的算法来计算循环对称布尔函数对快速代数攻击的免疫程度。该算法是偏真的，并且判定的正确率几乎接近于 1。此外，证明了当 n 为偶数且 n 不是 2 的幂次时，对于 n 元循环对称布尔函数 f，存在次数不超过 $e \leq n/3$ 的布尔函数 g，使得 gf 的次数不超过 $n-e-1$。

第三，证明了一个平衡的完全代数免疫函数的变元数一定是 2^m+1；一个不平衡的完全代数免疫函数的变元数一定是 2^m。同时，给出了一个判定单变元表示布尔函数快速代数免疫性的有效算法，并且由此证明了一些Carlet-Feng函数是完全代数免疫函数。

最后，运用离散傅里叶变换理论研究了由 m 序列生成的非线性滤波序列。针对等距过滤函数类，给出了滤波生成序列线性复杂度的一个改进的下界。同时，还给出了布尔函数谱免疫度的概念来衡量布尔函数抵抗离散傅里叶谱攻击的能力。

关键词： 布尔函数，Bent函数，代数攻击，循环对称布尔函数，离散傅里叶变换

Abstract

Boolean functions are frequently used in the design of stream ciphers, block ciphers and hash functions. Especially, the study of the cryptanalysis of the filter and combination generators of stream ciphers based on Linear Feedback Shift Registers (LFSR) has resulted in a wealth of cryptographic criteria for Boolean functions, such as balancedness, high algebraic degree, high nonlinearity, high correlation immunity and so on. A fundamental objective of cryptography is to attain Boolean functions satisfying some desired conditions. This thesis focus on some special classes of Boolean functions, and tries to make a further study on their cryptographic properties, Such as the existence of Bent functions, the immunity of Boolean functions against fast algebraic attacks, spectral immunity of Boolean functions and so on.

The main results and contributions of this thesis are as follows:

Firstly, we study the existence of Bent functions in the subclass of Boolean functions which have no monomials with degree less than d in the algebraic normal form. We prove that if a function of this class has less than $n+d-3$ monomials, then the function is not Bent. We also show that the parameter d is less than $\lceil 3n/8+3/4 \rceil$ for Bent functions.

Secondly, we propose an efficient algorithm to estimate the immunity of rotation symmetric Boolean functions against fast algebraic attacks. The algorithm is true-biased and almost always outputs the correct answer. Besides, it is shown that an n-variable rotation symmetric Boolean function f with n even but not a power of 2 admits a rotation symmetric function g of degree at most $e \leq n/3$ such that the product gf has degree at most $n-e-1$.

Thirdly, we prove that for a perfect algebraic immune balanced function the number of input variables is one more than a power of two; for a perfect algebraic immune unbalanced function the number of input variables is a power of two. We propose an efficient theorem to estimate the immunity of Boolean functions using univariate polynomial representation against fast algebraic attacks. Also some Carlet-Feng functions are shown to be perfect algebraic immune functions.

Finally, we study binary sequences generated by nonlinear filters on m-sequences with the method of Discrete Fourier Transform (DFT). We focus on the certain class of equidistant filters and give an improved lower bound on the linear complexity of the filtered sequences. We also give the definition of spectral immunity of Boolean functions to measure the ability of Boolean functions to resist Discrete Fourier Spectra Attacks.

Keywords: Boolean function, Bent function, Algebraic attack, Rotation symmetric Boolean function, Discrete Fourier Transform

目　录

摘要 i

Abstract iii

目录 v

第一章　引言 1

1.1　研究背景和意义 1

1.2　布尔函数的相关研究进展 2

1.3　内容安排和主要结果 4

第二章　预备知识 7

2.1　有限域基础知识 7

2.1.1　群、环、域的基本知识 7

2.1.2　环上的多项式理论 8

2.2　离散傅利叶变换 9

2.3　布尔函数理论 11

2.3.1　布尔函数的表示 12

2.3.2　布尔函数的密码学性质 15

2.4　本章小结 17

第三章　*Bent*函数的存在性研究 19

3.1　*Bent*函数的定义和基本性质 19

3.1.1　*Bent*函数的$Walsh$谱定义 19

3.1.2　*Bent*函数的等价定义及性质 20

3.2　齐次*Bent*函数的存在性 21

3.3　一类*Bent*函数的存在性研究 22

3.3.1　*Bent*函数的谱表示性质 22

3.3.2　*d-upper*布尔函数的定义 23

3.3.3　*d-upper Bent*函数与其代数标准型的关系 24

3.3.4 *d-upper Bent*函数的次数 25
3.4 本章小结 28

第四章 循环对称布尔函数的代数免疫性研究 29
4.1 代数攻击与快速代数攻击 29
4.1.1 代数攻击与代数免疫度 29
4.1.2 快速代数攻击及布尔函数的快速代数免疫性 31
4.2 循环对称布尔函数简介 32
4.3 循环对称布尔函数的快速代数免疫性 33
4.3.1 计算循环对称布尔函数的快速代数免疫度的快速算法 34
4.3.2 算法实例 37
4.3.3 矩阵 $S(f;e,d)$ 的性质 40
4.3.4 循环对称布尔函数对快速代数攻击的免疫程度 45
4.4 本章小结 47

第五章 完全代数免疫函数 49
5.1 完全代数免疫度 49
5.2 一般布尔多项式的完全代数免疫性 50
5.2.1 $M(f;e,d)$ 的性质 50
5.2.2 布尔函数具有完全代数免疫度的必要条件 52
5.3 单变元表示布尔函数的完全代数免疫度 54
5.3.1 具有完全代数免疫度的单变元表示布尔函数的判定 54
5.3.2 Carlet-Feng函数的完全代数免疫度 57
5.3.3 移位Carlet-Feng函数的完全代数免疫度 59
5.4 本章小结 61

第六章 离散傅里叶谱攻击相关研究 63
6.1 离散傅里叶谱攻击简介 63
6.1.1 离散傅里叶谱攻击原理 63
6.1.2 离散傅里叶谱攻击算法与实例 65
6.2 快速离散傅里叶谱攻击 67
6.2.1 攻击算法简介 68
6.2.2 算法原理及简化 69

6.3 滤波生成器序列的线性复杂度 70
6.3.1 序列的谱免疫度 70
6.3.2 滤波生成器序列的线性复杂度 71
6.3.3 等距过滤函数已有的研究结果 73
6.3.4 等距序列线性复杂度的一些新的下界 75
6.4 布尔函数的谱免疫度 77
6.5 本章小结 78

第七章 结论与展望 **79**

参考文献 **81**

发表文章目录 **89**

致谢 **91**

表　格

2.1　$f(x)$的真值表 …… 12

3.1　齐次*Bent*函数的次数上界[62] …… 21
3.2　*d-upper Bent*函数中 d 的上界 …… 28

4.1　计算当 $n=2^m$ 时循环对称布尔函数的快速代数免疫程度 …… 38
4.2　当 $n\neq 2^m$ 且 $e+d=n-1$ 时算法2的成功率 …… 38
4.3　当 $n\neq 2^m$ 且 $e+d=n-2$ 时算法2的成功率 …… 39

插　图

6.1　基于线性移位寄存器的流密码体制 63

第一章　引言

布尔函数和向量布尔函数在密码学中有着广泛的应用，特别是在分组密码和流密码的算法设计与分析中作为密码算法中的重要组件占有极其重要的地位。对于密码算法的各类攻击对其使用的布尔函数包括向量布尔函数提出了不同的密码学性质要求，对于这些性质的分析也是研究基于密码函数的各种密码体制的热点问题。本篇论文的研究内容主要是通过分析布尔函数的各种密码学性质，探究其在密码学，尤其是对称密码设计与分析方面的应用。

1.1　研究背景和意义

密码作为一种技术或通讯保密的软件工具, 其发展历史可谓源远流长; 但是直到1949年Shannon发表了“Communication Theory of Secret System”[83]一文后, 密码学才真正成为一门科学。随着计算机和网络在社会政治、经济、文化、生产等领域的普及，社会信息化建设已初具规模。越来越多的商业行为和交易及政府的服务都在公开的计算机和通讯网络进行，这也产生了信息安全问题，它不仅和国家的政治，军事和外交等有关，而且与各个团体和个人密切相关, 因此，信息系统的安全和保密至关重要。而信息安全的核心是密码理论与技术。1976年W. Diffie和L.E. Hellman论文“密码学的新方向”[28]的发表及1977年美国数据加密标准DES的公开标志着现代密码学的开始，而此后密码体制的研究基本上就沿着这两个方向——非对称密码体制和对称密码体制进行。

非对称密码体制又叫做公钥密码体制，典型代表如RSA[72]等。其对于通信环境的安全性要求相对比较弱，因此应用领域越来越广。但它最大的缺点是加密和解密的时间长且结构复杂，严重影响了这类方案的效率。而对称密码体制的结构及实现都比较简单，并且加密速度是非对称密码体制的上百倍甚至上千倍。但它的私钥必须是保密的，这就对通信环境的安全性要求比较高。现实中使用的密码方案一般要同时使用这两种密码体制: 使用公钥密码体制来生成和交换密钥，而使用对称密码体制来传输大部分的数据。

1997年，美国启动了AES(Advanced Encryption Standard)计划，在全世界范围内征集高级加密标准，用于取代DES。2000 年10月，NIST最终推荐Rijindael作为高级加密标准AES。欧洲于2000年1月启动了新欧洲签名、完整性和加密计划 - NESSIE(New European Schemes for Signatures, Integrity, and Encryption)计划，以满足21世纪信息安全发展的全面需求。NESSIE涉及的不但有分组密码，还包括序列密码、公钥密码、认证码、杂凑函数和数字签名等标准。2004年2月，欧洲又启动了ECRYPT(European

Network of Excellence for Cryptology)，该计划是欧洲在NESSIE计划结束后启动的一个更大的信息安全研究项目。并且在2008年公布了最终的结果, 选定了Grain、Mickey-128、Trivium三个算法作为面向硬件序列算法的胜出者，选定了HC-128、Rabbit、Salsa20/12、SOSEMANUK作为面向软件序列算法的胜出者.

可见，随着社会的进步, 各国都认识到信息安全的重要性, 从而加大了对各种密码算法的研究投入，其中，序列密码、分组密码和Hash函数的设计与分析是目前信息安全领域中的热点问题。我国也在抓紧制定序列密码、分组密码、公钥密码和Hash函数等方面的国家标准。

对称密码体制按照对明文加密方式的区别可分为流密码和分组密码。流密码又称序列密码，序列密码的加密是用一个序列与明文序列进行叠加来产生密文，解密用同一个序列与密文叠加来恢复明文。这个序列一般称为密钥流序列，它决定着流密码的安全。如果产生的密钥流序列有某种规律性或者能暴露某种特性，这对攻击者来说有很大的好处，所以怎样产生安全性高的密钥流序列是流密码安全的关键。Rueppel[78]将生成流密码的密钥流生成器分解成驱动部分和非线性组合部分。驱动部分控制存储器的状态转移，负责提供若干周期大,统计特性好的序列供组合部分使用（一般使用线性移位寄存器），而非线性部分则将由驱动部分提供的序列组进行混淆和扩散，从而合成满足要求的,性质良好的密钥流序列。由于线性移位寄存器的技术已经很成熟，所以驱动部分的设计比较容易，而非线性组合部分的设计则成为了提高密钥流安全强度的重点和难点。而非线性组合部分也可以由布尔函数来描述，例如LILI-128[27]，因此对非线性组合部分的研究等价于对布尔函数的研究。布尔函数不仅在序列密码体制的设计和分析中扮演着重要的角色，它也被用于分组密码的设计中。DES是分组密码的一个最经典的例子，它的安全性取决于S盒密码学性质的好坏，而S盒可以用向量布尔函数来描述。分组密码中用到的各种置换也可以看作多输出密码函数。可以看出，构造密码学性质优良的向量布尔函数是设计较高安全性的分组密码体制的关键。

综上所述，布尔函数和向量布尔函数作为密码算法中的重要组件，其好坏直接影响到算法本身的安全性。对密码算法的各类攻击使得对其使用的布尔函数和向量布尔函数提出了不同的密码学性质要求，如非线性度以抵抗线性攻击，差分均匀度以抵抗差分攻击等。而布尔函数的各类密码学性质研究也成为了一个热门的课题.

1.2 布尔函数的相关研究进展

为了抵抗各种攻击，对称密码使用的布尔函数必须满足若干密码学准则，例如：平衡性，非线性性，相关免疫性，代数次数，代数免疫度等；因此研究具有良好密码学性质的布尔函数是非常有意义的。随着密码学的发展，人们对密码系统中的布尔函数的研究逐步深入,出现了许多衡量布尔函数密码学性质的指标，主要有以下一些：

（1）非线性度:

布尔函数的非线性度是指其与所有仿射函数之间的最短距离。在密码学中，仿射函数是最容易被攻击的函数，所以一个函数越接近仿射函数，非线性度越低，也就越容易被攻击。所以在密码学系统中要求布尔函数具有较高的非线性度。1976年，Rothaus[75]证明了n 元布尔函数的非线性度上界是$2^{n-1}-2^{\frac{n}{2}-1}$，并且提出了具有最高非线性度的函数，即*Bent*函数的定义。*Bent*函数不仅本身是很重要的组合结构，而且还在编码、密码及序列设计中有重要的应用[7, 11]。尽管这类函数可以有效的抵抗线性攻击[31], 但它不是平衡的，这限制了它在密码学中的广泛应用。但是构造具有高的非线性度的函数[7, 79, 82] 以及探索非线性度与其他密码学性质的关系[57]依然具有研究意义。bent 函数都是偶变元的，当n为奇数变元时，T. Helleseth, T. Klove 和J. Mykkelveit等在[45, 64]证明了当$n=357$时，n 元布尔函数的非线性度上界为$2^{n-1}-2^{\frac{n-1}{2}}$；N.J. Patterson 和D.H. Wiedemann则在[68, 69]证明当$n>14$时，n 元布尔函数的非线性度上界严格大于$2^{n-1}-2^{\frac{n-1}{2}}$。2006年，S. Kavut 等人找到了非线性度大于240 的9 元旋转对称布尔多项式[46]使得构造具有高非线性度的奇变元布尔函数成为可能。

（2）代数免疫度：

通过求解多变元高次超定方程组来获得密钥信息的思想最早是在[83]中提出的。2003 年，N.Courtois等[17]发展了代数攻击的思想：通过建立初始密钥和输出密钥流比特之间的代数方程,运用线性化方法来求解超定的多元高次方程组以获得初始密钥。为了衡量布尔函数对于代数攻击的抵抗程度，Meier等[60] 提出了代数免疫度的概念。之后人们研究了代数免疫度与其它密码学指标的关系：D.K.Dalai给出了布尔函数代数免疫度与非线性度之间的关系[24]；C.Carlet研究了代数免疫度与高阶非线性度之间的关系[10]。构造具有最大代数免疫度的布尔函数也引起了广泛的关注：D.K.Dalai等[23]从零化子的基本思想出发,首次提出了构造具有最大代数免疫度布尔函数的一般方法,并研究了所构造布尔函数的其它密码学性质；李娜等[52] 提出了一种构造全部的具有最大代数免疫度的奇变元布尔函数的方法；C. Carlet 等[12] 构造出了一类布尔函数：不仅具有最优代数免疫度和代数次数，同时还具有很高的非线性度。Didier[30]从理论上证明了当n趋近于无穷时,一个n元随机平衡布尔函数的代数免疫度以接近于1的概率为$\frac{n}{2}(1-o(1))$。同时，求解代数免疫度的算法也受到了广泛的关注[2, 26, 54]。Armderik[2] 等在2006 年的欧密会提出了一种基于多变元多项式差值求解布尔函数代数免疫度的算法,降低了其计算复杂度。尽管代数免疫度理论已有了丰富的结果，但诸如能否找到兼顾各个密码学性质好的衡量指标或找到更好的衡量指标来代替代数免疫度等也都是值得研究的问题。

一般的代数攻击中，密钥流可以是不连续的，并没有利用到由LFSR产生的相邻连续状态的迭代结构。而对于连续的密钥流,因为LFSR的反馈逻辑具有迭代性，即前后相邻的时刻，f函数的输入是满足一定的线性迭代关系的。2003年Courtois[19]提出的快速

代数攻击注意并利用了这个迭代性，从而得到了次数更低的关于初始密钥与密钥流的方程。随后，Armknecht 等[1]指出：具有好的代数免疫度的布尔函数不一定能抵抗快速代数攻击；并在之后[2]给出了一种计算布尔函数抵抗快速代数攻击能力的算法。C. Carlet 等[12]构造出的一类布尔函数：不仅具有最优代数免疫度和代数次数，同时还具有很高的非线性度和对快速代数攻击的免疫性。龚光[40]提出了一种度量布尔函数对快速代数攻击抵抗程度的标准：(e,d)-抵抗；P.Rizomiliotion[73]将布尔函数对快速代数攻击的抵抗性归纳为$(d1,d2)$- 对的存在性问题并且给出了一种计算单变元表示布尔函数抵抗性的算法。尽管布尔函数对快速代数攻击抵抗性的研究已经有了一些结果，但寻找一个好的衡量指标和构造能够抵抗快速代数攻击的布尔函数等也是值得研究的问题。

（3）相关免疫度：

布尔函数相关免疫度的概念最早是由T. Siegenthaler[85]针对密码系统的相关攻击[84]提出的，其本质上是一种更强的平衡性的要求。T. Siegenthaler 紧接着证明了布尔函数的相关免疫阶数,变元数和代数次数的制约关系，同时提出了几种构造办法。1988 年Xiao-Massey定理[91]给出了相关免疫度与Walsh 谱的关系，给人们提供了通过Walsh谱研究相关免疫函数的新途径。1985年Chor 等人[15]推广了相关免疫函数的概念并提出了弹性函数的概念。2000年Tarannikov[88]得到了m- 弹性函数的Walsh谱特征；2001年Cheon [14]改进了上述结果并且得到了m 阶弹性函数Walsh谱的特点：

$$F(f\oplus\varphi)\equiv 0 \mod 2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor},$$

其中d 为n元布尔函数$f(x)$的代数次数。此外，弹性函数在S 盒的设计中也有应用[14, 42]。

布尔函数的密码学性质还包括平衡性和代数次数的要求，由于这些要求比较基础，一般都会在研究其他密码学性质时一并讨论。事实上，确定布尔函数的密码学性质之间的关系以及寻找满足一定密码学性质的布尔函数是密码学理论的重要内容。但是由于人们对非线性理论知之甚少，加之密码体制本身的缺陷，研究和构造具有优良密码学性质的密码函数不是一件容易的事。针对相应的密码学性质或根据布尔函数的性质对现有的密码体系进行攻击也是一件非常有意义的工作。

1.3 内容安排和主要结果

本文共分为七章，其中第三章到第六章是论文的核心，各章的安排及内容简介如下：

第一章是引言部分，给出了文章研究工作的大背景，确定了论文的研究内容，给出了相关研究进展基础以及文章的组织结构。

第二章介绍了文章所要用到的一些基本概念和性质。首先，我们介绍了有限域以及域上布尔函数的相关背景知识；然后，我们介绍了离散傅利叶变换的相关知识；最后我们总结了布尔函数的表示方法以及一些密码学性质，这也是我们之后的研究工作的重点。

第三章我们主要研究了*Bent*函数的存在性问题。在介绍了*Bent*函数的定义、性质以及相关研究进展之后，我们定义了一类新的布尔函数—*d-upper*布尔函数，并且在齐次*Bent*函数相关研究成果的基础上，给出了*d-upper Bent*函数存在的一些必要条件，并且深入分析了*d-upper Bent*函数与其次数和代数标准型的关系。

第四章基于针对流密码的代数攻击以及快速代数攻击，我们研究了循环对称布尔函数对于快速代数攻击的抵抗程度。我们给出了一个计算其快速代数免疫性的优化算法并分析了其计算复杂度与可行性；之后，我们又研究了算法系数矩阵的各种性质，给出了循环对称布尔函数具有最优快速代数免疫性的一些必要条件。

第五章我们基于上一章的工作，将矩阵推广到了更一般的布尔多项式上，得到了布尔函数具有最优快速代数免疫性的一些必要条件。我们定义了完全代数免疫函数，并且证明了单变元表示的$Carlet-Feng$函数及其衍生函数都是完全代数免疫函数。

第六章首先介绍了离散傅里叶谱攻击的相关研究进展，并给出了其算法的复杂度分析；然后我们基于该攻击的应用环境，研究了等距滤波生成序列的线性复杂度问题；最后，我们基于快速离散傅里叶谱攻击，给出了布尔函数谱免疫度的概念，并对其上界给出了估计。

第七章对本文进行了总结，在总结全文的基础上，指出了有待于进一步开展的工作。

第二章　预备知识

本文的相关研究结果很多都建立在基础数学理论的基础上。本章将介绍论文所应用的主要数学理论基础：第一部分将介绍有限域的基础知识；第二部分将介绍布尔函数的基本概念和理论以及其的密码学性质；第三部分将介绍离散傅利叶变换的相关知识及其在布尔函数中的应用。

2.1　有限域基础知识

2.1.1　群、环、域的基本知识

在这一章，我们主要介绍群、环、域的一些基本概念与性质。

定义 2.1. 我们说一个非空集合 G 对于 G 上一个二元运算 $\circ$ 来说作成一个群，若：

1. $\circ$ 在 G 中是封闭的，即对任何 $a, b \in G$, $a \circ b \in G$;
2. $\circ$ 满足结合律，即对任何 $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$;
3. G 中存在单位元 e, 即对$\forall a \in G$, $a \circ e = e \circ a = a$;
4. G 中任意元素均存在逆元，即对 $\forall a \in G$, 都存在 $a^{-1} \in G$, 使得 $a \circ a^{-1} = a^{-1} \circ a = e$。

在上述定义中，若运算 $\circ$ 满足交换律，即对 $\forall a, b \in G$, 都有 $a \circ b = b \circ a$，那么群 G 称为交换群或者 *Abel* 群。这时我们也将 $\circ$ 表示成 $+$, 同时把单位元 e 写成 0，a 的逆元记作 $-a$, 因此交换群也称为加法群。群 G 中所含元素的个数称为群 G 的阶, 记作 $|G|$。若群中元素个数有限, 称 G 为有限群; 否则, 称 G 为无限群. 如果群 G 的所有元素都可由其中的一个元素来生成, 则称它是循环群。循环群必然是 *Abel* 群。

下面我们给出环和域的概念和性质。

定义 2.2. 我们说一个非空集合 R 是一个环，若 R 上有一个加法 $+$ 和乘法 $\circ$，满足：

1. $(R, +)$是一个交换群；
2. 关于 $\circ$ 是封闭的且满足结合律，即对任何 $a, b, c \in R$, $a \circ (b \circ c) = (a \circ b) \circ c$;
3. 加法和乘法满足分配率，即对任何 $a, b, c \in R$, $a \circ (b + c) = a \circ b + a \circ c$。

其中如果 R 中的乘法运算 $\circ$ 是交换的，那么 R 叫做交换环。

定义 2.3. 我们说一个非空集合 F 是一个域，若 R 上有一个加法 $+$ 和乘法 $\circ$，满足：

1. F 关于 $+$ 是一个交换群，加法单位元记为 0；
2. F 中的非零元关于 $\circ$ 是一个交换群，乘法单位元记为 1；
3. 加法和乘法满足分配率，即对任何 $a, b, c \in F$, $a \circ (b + c) = a \circ b + a \circ c$。

可以看出域是非零元构成一个乘法交换群的环，是环的一个特例。

由有限个元素所构成的域称为有限域, 或称为伽罗瓦(Galois) 域。域中的元素个数称为该有限域的阶. 我们用 F_q 表示 q 阶有限域。

设 F 是任意一个域, 而 e 是它的乘法单位元。如果对于任意正整数 m, 都有 $me = 0$, 我们就说 F 的特征是 0, F 是特征 0 的域。如果存在正整数 m 使 $me = 0$, 那么就说F 的特征不等于 0 , 而适合条件 $pe = 0$ 的最小正整数 p 就叫做 F 的特征, 或者说 F 是特征为 p 的域。所以我们就知道任意一个域 F 的特征或者是 0, 或者是一个素数 p。

设 F 是域，K 是 F 的子集。如果 K 在 F 的运算下也构成一个域，则称 K 是 F 的子域，而 F 则称为 K 的扩域。特别的，如果 $K \neq F$，则称K 是 F 的真子域。

定义 2.4. 一个域如果不包含任何真子域，则称为素域。如果一个域 F 的子域作为域是素域，则称该子域为 F 的素子域。

注意到任意多个子域的交仍然是子域，我们可以知道一个域的素子域实际上就是该域的所有子域的交。显然，有理数域 Q 和阶为素数 p 的有限域 F_q 都是素域。

有限域作为一种只含有有限个元素的特殊的域，有着许多其他域所没有的特殊性质。

定理 2.1. 假设 F 是一个特征为p的有限域，则 F 有 p^n 个元素，其中 n 是 F 关于其素域的扩张次数。

定理 2.2. 假设 F 是一个具有q个元素的有限域，则对任意 $a \in F$，有 $a^q = a$。

2.1.2 环上的多项式理论

假设 R 是环，$R[x]$ 是由系数在 R 中，未定元为 x 的多项式全体组成的集合。那么任给 $R[x]$ 中的一个非零元素 $f(x) \in R[x]$，一定可以写成

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, a_n \neq 0$$

的形式，其中 $a_0, a_1, \ldots, a_n \in R$ 且 $a_n \neq 0$。其中 n 称为多项式 $f(x)$ 的次数，记作 $deg(f(x))$。

首先我们在 $R[x]$ 中引入加法运算，设

$$f(x)=a_nx^n+\cdots+a_1x+a_0, g(x)=b_nx^n+\cdots+b_1x+b_0$$

是 $R[x]$ 中的两个多项式，定义 $f(x)$ 和 $g(x)$ 的加法为

$$f(x)+g(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0)$$

其次，我们再定义 $R[x]$ 中多项式的乘法运算。设

$$f(x)=a_nx^n+\cdots+a_1x+a_0, g(x)=b_mx^m+\cdots+b_1x+b_0, a_n, b_m\neq 0$$

是 $R[x]$ 中的两个次数分别为 n 和为 m 的多项式。定义 $f(x)$ 和 $g(x)$ 的乘法为

$$f(x)\cdot g(x)=c_{m+n}x^{m+n}+\cdots+c_1x+c_0,$$

其中

$$c_k=\sum_{0\leq i\leq n, 0\leq j\leq m, i+j=k} a_jb_j, k=0,1,\ldots,m+n.$$

显然，$R[x]$ 在上面定义的运算下构成了一个环，我们称这个环为 R 上的多项式环。

有了上面的定义我们可以给出多个变量的多项式。设 $x_1,x_2,\ldots,x_n$ 是域 F_q 上的 n 个变元，设 $k_1,k_2,\ldots,k_n$ 是非负数，$a_{k_1,k_2,\ldots,}\in F_q$，则称

$$f(x_1,x_2,x_3,\ldots,x_n)=\sum_{k_1,k_2,\ldots,k_n} a_{k_1,k_2,\ldots,k_n}x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$$

为域 F_q 上的 n 元多项式。

这两节只是对有限域和多项式理论做一些简单的介绍，对其更为详尽的介绍参见文献[92]。

2.2　离散傅利叶变换

对于序列 $\boldsymbol{s}=s_0,s_1,s_2,\ldots$，$s_i\in\mathbb{F}_q$，$q=p^n$ 且 p 为素数。如果 $s_i=s_{i+t}$ 对所有的 i 都成立，那么我们说 $\boldsymbol{s}$ 是一个周期为 t 的序列。$\boldsymbol{s}$ 被称为 L 阶的线性递归序列当且仅当存在 $c_0,c_1,c_2,\ldots,c_{L-1}\in\mathbb{F}_q$ 满足 $s_j+s_{j-1}c_0+\cdots+s_{j-L}c_{L-1}$，$f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$ 称作 $\boldsymbol{s}$ 的特征多项式。我们通常用 $G(f)$ 来表示 $f(x)$ 产生的所有序列的全体组成的集合。

定义 2.5. 设 $\boldsymbol{s}$ 是 $\mathbb{F}_q$ 上的一个周期序列，那么存在 $\mathbb{F}_q$ 上唯一的首一多项式 $f(x)$ 使得 $\boldsymbol{s}\in G(h)$ 当且仅当 $f(x)|h(x)$。f 便称为 $\boldsymbol{s}$ 的极小多项式。f 的次数就称为 $\boldsymbol{s}$ 的线性复杂度，记作 $LS(\boldsymbol{s})$。

定义 2.6. 对于 $x \in \mathbb{F}_{q^n}$，其迹方程为：

$$Tr_1^n(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}.$$

定理 2.3. 令 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ 是 $\mathbb{F}_q$ 上的一个 n 次不可约多项式且 α是$f(x)$ 的一个根。考虑序列 $\boldsymbol{s}$:

$$s_i = Tr_1^n(\beta\alpha^i), \quad i \geq 0,$$

其中 $\beta \in \mathbb{F}_{q^n}$。那么 $\boldsymbol{s} \in G(f)$。

此定理反之依然成立。注意到 β 不必要是 $\mathbb{F}_{q^n}$ 的本原元，而且当 $\beta \neq 0$ 时 $\boldsymbol{s} \in G(f)$ 是一个周期为 $q^n - 1$ 的序列。

包含 s 的模 N 分圆陪集定义为：

$$C = \{sq^i(mod\ N) | i = 0, 1, \ldots, n_s - 1\}$$

其中 n_s 是使得 $s \equiv sq^t(mod\ N)$ 成立的最小整数$(n_s|n)$。而 C 中最小的整数 s 就是集合的代表元，记 $C = C_s$。而包含所有模 N 代表元的集合定义为 $\Gamma(N)$。

容易得到 n_s 与 α^s 在 F_q 上最小多项式的次数相同。

令 N 是一个整数且存在 $n \geq 0$ 使得 $N|q^n - 1$。令

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{N-1})$$

是 $\mathbb{F}_q^n$ 上的一个元素，且 α 是在 $\mathbb{F}_{q^n}$ 上的阶为 N 的元素。序列 $\boldsymbol{a}$ 的离散傅里叶变换(DFT)定义为：

$$A_k = \sum_{i=0}^{N-1} a_i\alpha^{-ik}, k = 0, 1, 2, \ldots, N-1. \tag{2.1}$$

反解的关系是:

$$a_k = \frac{1}{N^*}\sum_{i=0}^{N-1} A_i\alpha^{ik}, k = 0, 1, 2, \ldots, N-1 \tag{2.2}$$

其中 $N^* \equiv N(mod\ p)$。

当 $q = 2$ 时，上述表达式可以写成:

$$a_k = \sum_{i=0}^{N-1} A_i\alpha^{ik}, k = 0, 1, 2, \ldots, N-1. \tag{2.3}$$

引理 2.4. 对于任意的 $1 \leq k \leq n-1$，有 $A_{kq^j} = A_k^{q^j}$。

也就是说离散傅里叶变换可以表示成如下形式：

$$a_k = \frac{1}{N^*} \sum_{i \in \Gamma(N)} Tr_1^{n_i}(A_i \alpha^{ik}). \tag{2.4}$$

离散傅里叶变换具有如下性质：

命题 2.5. 如果 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 是 $\mathbb{F}_q^N$ 上的向量，x、$y \in \mathbb{F}_q$；而且 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 分别是 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的 DFT；那么有 $x\boldsymbol{a} + y\boldsymbol{b}$ 的 DFT 是 $x\boldsymbol{A} + y\boldsymbol{B}$。

命题 2.6. 如果 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 是 $\mathbb{F}_q^N$ 上的向量，$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 分别是 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的 DFT，且有：

$$b_i = a_{i+k}, \quad 0 \le i < N$$

那么有

$$B_i = A_i \alpha^{-ki}, \quad 0 \le i < N.$$

命题 2.7. 如果 $\boldsymbol{a}$、$\boldsymbol{b}$ 和 $\boldsymbol{c}$ 是 $\mathbb{F}_q^N$ 上的向量，$\boldsymbol{A}$、$\boldsymbol{B}$ 和 $\boldsymbol{C}$ 分别是 $\boldsymbol{a}$、$\boldsymbol{b}$ 和 $\boldsymbol{c}$ 的 DFT，而且 $c_i = a_i b_i$，那么有：

$$C_i = \frac{1}{N^*} \sum_{j=0}^{N-1} A_{i-j} B_j, \quad 0 \le i < N.$$

序列的离散傅里叶谱序列与其线性复杂度密切相关。

定理 2.8 (Blahut Theorem). 令 $\boldsymbol{A} = \{A_0, A_1, \ldots, A_{N-1}\}$，则 $LS(\boldsymbol{a}) = wt(\boldsymbol{A})$。

证明. 令

$$a_k = a_{1k} + \cdots + a_{sk}, \quad a_{ik} = Tr_1^{n_i}(A_i \alpha^{ik}), i \in \Gamma(N)。$$

则

$$LS(\boldsymbol{a}) = LS(\boldsymbol{a_1}) + \cdots + LS(\boldsymbol{a_s}) = n_1 + \cdots + n_s, \quad A_i \neq 0。$$

易知结论。 □

离散傅利叶变换的理论结果非常丰富，这里只是简单介绍一些基础知识，更多的内容参见文献[39]。

2.3　布尔函数理论

在许许多多复杂的现代化设备中都少不了一个基本的元器件, 即逻辑电路。 这是一种在其输入和输出之间有一定逻辑关系的电路。 这种电路的输入和输出间通常都是用脉冲的有无或电位的高底来表示的。 然后运用数学中的一些基本的公理及定理对其进行数学运算, 便可得到合乎逻辑的结果。 在此基础上发展出了一门重要学科, 称为布尔代数学。

作为表示逻辑运算的函数, 布尔函数是研究数字逻辑电路的重要数学工具, 也是研究以此为基础的一切科学技术的重要工具, 从而也是研究密码学和密码技术的重要工具。 无论在流密码还是分组密码中, 无论在私钥还是公钥密码中, 布尔函数都有很重要的应用。 尤其在流密码中, 所使用的主要数学工具之一就是布尔函数。 本节我们介绍布尔函数的基本概念和研究方法。

2.3.1 布尔函数的表示

令 F_2 表示二元有限域，F_2^n 表示 F_2 上的 n 元向量空间，那么 F_2 上的 n 元布尔函数 $f(x)$ 就定义为

$$f(x) : F_2^n \to F_2,$$

其中 $x = (x_1, x_2, \ldots, x_n) \in F_2^n$。为了方便我们用 B_n 表示 F_2^n 上的 n 元布尔函数全体。用 $\oplus$ 表示 F_2, F_2^n, B_n 上的加法。

布尔函数的表示方法有很多种，这里我们主要介绍，真值表表示，多项式表示，单变元表示以及$Walsh$谱表示。

1. 真值表表示

布尔函数由于其定义域和值域都是有限集, 自然可以用列表法表示。

x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

表 2.1: $f(x)$的真值表

例如, 表2.3.1定义一个布尔函数 $f(x) = f(x1, x2, x3)$：表中左列是 x 的值, 右列是相应的函数值 $f(x)$。我们把这样的一个表称为 $f(x)$ 的真值表，把右列函数值构成的矢量称为 $f(x)$ 的函数值向量。该向量中 1 的个数称为 $f(x)$ 的汉明(Hamming)重量, 记为 $wt(f)$。若 n 元布尔函数 $f(x)$ 满足 $wt(f) = 2^n - 1$, 则称 $f(x)$ 是平衡函数。 同时称支撑集 $Supp(f)$ 为使得 $f(x) = 1$ 的 x 取值的集合，即

$$Supp(f) = x \in F_2^n | f(x) = 1。$$

容易得到，$wt(f) = |Supp(f)|$。但是列表法表示的实函数不一定有解析表达式，而任何布尔函数都有解析表达式。

2. 代数标准型表示

在所有布尔函数的表示方法中，最为常用的表示是代数标准型(Algebraic Normal Form, 简称ANF)，一个 n 元布尔函数在 F_2 上的表示形如：

$$f(x) = \bigoplus_{I \in P(N)} a_I (\prod_{i \in I} x_i) = \bigoplus_{I \in P(N)} a_I x^I, \tag{2.5}$$

其中 $P(N)$ 是集合 $N = 1, 2, \ldots, n$ 的幂集，这一表示属于 $F_2[x_1, \ldots, x_n]/(x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n)$。

我们还可以用向量空间 F_2^n 替代集合 N 的幂集来表示函数的代数标准型：对任意的向量 u，定义 $a_u \in F_2$，我们就有

$$f(x) = \bigoplus_{u \in F_2^n} a_u (\prod_{j=1}^{n} x_j^{u_j}) = \bigoplus_{u \in F_2^n} a_u x^u, \tag{2.6}$$

其中 $x^u = \prod_{j=1}^{n} x_j^{u_j}$。

n 元布尔函数 $f(x)$ 的代数次数 $deg(f)$ 是变量最多的非零单项式的变元个数。代数次数最多为 1 的布尔函数称为仿射函数，记为 A_n ，若其常数项为零，则称为线性函数, 记为 L_n。

由于 $x^I = \prod_{i \in I} x_i$ 不为 0 当且仅当 $x_i \neq 0$ 对任意的 $i \in I$。所以，布尔函数 $f(x) = \bigoplus_{I \in P(N)}$ 的值是

$$f(x) = \bigoplus_{I \subseteq supp(x)} a_I$$

其中 $supp(x)$ 是 x 的支撑集。

定理 2.9. 假设 $f(x) = \bigoplus_{I \in P(N)} a_I x^I$ 是 F_2^n 上的布尔多项式，我们有：

$$\forall I \in P(N), a_I = \bigoplus_{x \in F_2^n / supp(x) \subseteq I} f(x) \tag{2.7}$$

由上面的定理我们可以得到代数标准型与真值表的换算方法。例如表2.3.1所定义布尔函数的ANF就是

$$f(x) = x_1 x_2 x_3 \oplus x_2 x_3 \oplus x_3。$$

3. 单变元多项式表示

令 F_{2^n} 为 2^n 元有限域，任意一个非零多项式 $f : F_{2^n} \to F_2$都可以表示成如下形式：

$$f(x) = \bigoplus_{i=0}^{2^n - 1} f_i x^i,$$

其中 $f_0, f_{2^n-1} \in F_2$，且 $f_{2i} = (f_i)^2 \in F_{2^n}, 1 \le i \le 2^n - 2$。函数 f 的代数次数 $deg(x)$ 定义为满足 $s = wt_2(k)$ 且 $f_k \neq 0$ 的最大的整数 s，其中 $wt_2(k)$ 是 k 二进制表示中非零项的个数。

函数 f 的系数 f_i 为

$$f_i = \begin{cases} f(0), & \text{for } i = 0, \\ F(\alpha^{-i}), & \text{for } 1 \le i \le 2^n - 2 \\ F(1) \oplus f_0, & \text{for } i = 2^n - 1 \end{cases}$$

其中

$$F(x) = \bigoplus_{j=0}^{2^n-2} f(\alpha^j) x^j,$$

且 α 是 F_{2^n} 中的一个本原元。

令 $\{\beta_1, \beta_2, \ldots, \beta_n\}$ 是 F_{2^n} 上的一组基。如果我们将 F_{2^n} 中的元素 $x = \sum_{i=1}^{n} x_i \beta_i$ 用向量 $(x_1, x_2, \ldots, x_n)$ 来表示，那么在布尔多项式与 $F_{2^n} \to F_2$ 的多项式之间有着很明显的一一对应关系。我们将任意布尔多项式所对应的 $F_{2^n} \to F_2$ 的多项式表示称为其单变元表示。我们在之后所要讨论的Carlet-Feng函数类[12]就是运用了这种表示方法。

设 α 是在 $\mathbb{F}_{2^n}$ 上的本原元，则多项式

$$A(x) = \bigoplus_{j=1}^{2^n-1} A_j x^{2^n-1-j} = \bigoplus_{j=0}^{2^n-2} A_{-j} x^j$$

其中

$$A_j = \bigoplus_{k=0}^{2^n-2} f(\alpha^k) \alpha^{kj}$$

满足

$$A(\alpha^i) = \bigoplus_{j=1}^{2^n-1} A_j \alpha^{-ij} = \bigoplus_{j=1}^{2^n-1} \bigoplus_{k=0}^{2^n-2} f(\alpha^k) \alpha^{(k-i)j} = f(\alpha^i)$$

。由此，我们可以得到当$x \neq 0$时，$f(x) = A(x)$。运用离散傅利叶变换的相关知识，我们可以得到

$$f(x) = \bigoplus_{j \in \Gamma(n)} Tr_1^{n_j}(A_j x^j) \oplus e(1 \oplus x^{2^n-1}),$$

其中 $e = wt(f)[mod\ 2]$。我们把写成这种形式的单变元表示称为布尔函数的$Trace$-表示，其与布尔函数代数标准型的关系更容易得到。

4. $Walsh$谱表示

定义 2.7. 设 $x = (x_1, x_2, \ldots, x_n)$，$a = (a_1, a_2, \ldots, a_n) \in F_2^n$，定义 x 和 a 的点积运算为

$$x \cdot a = x_1 a_1 \oplus x_2 a_2 \oplus \cdots \oplus x_n a_n,$$

则 n 元布尔函数 $f(x)$ 的 $Walsh$ 变换定义为

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x \cdot a}, \tag{2.8}$$

其逆变换为

$$(-1)^{f(x)} = 2^{-n} \sum_{a \in F_2^n} (-1)^{W_f(a) + x \cdot a}。 \tag{2.9}$$

容易得到

$$(-1)^{f(x)} = 1 - 2f(x),$$

所以我们可以把式2.9称为布尔函数 $f(x)$ 的$Walsh$谱表示。

可以证明，任意布尔函数 $f(x)$ 和其$Walsh$谱是一一对应的。令 $a = 0$，我们有

$$W_f(0) = \sum_{x \in F_2^n} (-1)^{f(x)} = 2^n - 2wt(f),$$

所以我们可以从 $f(x)$ 的$Walsh$谱中得到 $f(x)$ 的重量

$$wt(f) = 2^{n-1} - 2^{-1} wt(f)。$$

布尔函数表示的更详细内容及其他表示请参见文献[9]，这里不再详述。在下一节中，我们将看到这些表示在布尔函数理论中的重要用途。

2.3.2　布尔函数的密码学性质

为了抵抗各种攻击,流密码和分组密码算法中所应用的布尔函数必须满足一定的密码学准则。例如,为了抵抗代数攻击,它们必须具有代数免疫度；为了抵抗线性攻击,它们必须有高的非线性度等等。这些密码学性质主要包括：

- 平衡性
- 代数次数
- 非线性度
- 相关免疫度
- 代数免疫度

这其中，平衡性与代数次数的概念在上一节已经有所介绍。一般来说，密码系统要求其中的布尔函数是平衡的，并且具有较高的代数次数。下面我们对其他的一些密码学性质进行简单的介绍。

1. 非线性度

对任意两个布尔函数 f 和 g，定义 f 和 g 的汉明距离

$$d(f, g) = wt(f \oplus g)。$$

定义 2.8. 布尔函数 f 的非线性度，定义为 f 与所有放射函数之间的最短汉明距离，记作 $nl(f)$。若计 $L_n[x]$ 为所有的 n 元仿射函数，则 f 的非线性度为

$$nl(f) = \min_{l \in L_n[x]} d(f,l) = \min_{l \in L_n[x]} wt(f \oplus l)。$$

容易得到，仿射函数的非线性度为 0。在密码学系统中，仿射函数是最容易进行线性攻击的布尔函数。一个函数的非线性度越低，也就越接近仿射函数，也就越容易为线性攻击所攻击，所以密码学系统中的布尔函数要有较高的非线性度。

利用$Walsh$谱的概念，我们可以得到布尔函数 f 非线性度的$Walsh$谱：

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} |W_f(a)|。$$

2. 代数免疫度

布尔函数的代数免疫度是在 2004 年基于针对流密码系统的代数攻击而提出的。代数攻击的基本思想是：首先建立起初始密钥、输入比特和输出比特之间的代数方程，再解方程以恢复密钥或者将密钥限制在一个小的区域内。因此，尽量降低方程的次数就可以使代数攻击的效率上升。

定义 2.9. 设 $f \in B_n$，若存在 $g \in B_n$，使得 $f*g = 0$，则称 g 是 f 的零化子(Annihilator)，记作

$$AN(f) = \{g \in B_n | f * g = 0\}。$$

对于高代数次数的布尔函数 f，有三种降低次数的情形[60]:

S3a 存在低次布尔函数 g，使得其乘积函数 $f*g$ 是低次的。即 $f*g = h$，其中 h 是非零的低次布尔函数。

S3b 存在低次布尔函数 g，满足 $f*g = 0$。

S3c 存在高次布尔函数 g，满足 $f*g = h$，其中 h 是非零的低次布尔函数。

考虑 *S3c*，因为 $f*g = h \neq 0$，将等式两边同时乘上 f，由于在 F_2 上 $f^2 = f$，故 $f^2*g = f*h = f*g = h$，即 $f*h = h$。因为 h 是一个低次函数，所以 *S3c* 转化为 *S3a*。进一步考虑 $f = g*h$ 的因式分解形式，将等式两边同时乘上 $1 \oplus g$，由于在 F_2 上 $g*(1 \oplus g) = 0$，故 $f*(1 \oplus g) = g*h*(1 \oplus g) = 0$，得 $f*(1 \oplus g) = 0$，这样就转化为 *S3b* 的形式。因此降低代数方程次数的情形最终可以归结为 *S3a* 和 *S3b* 两种形式。

在文献[25]中降低代数方程次数的两种情形等价于寻找布尔函数 f 或 $1 \oplus f$ 的零化子，因而产生了关于布尔函数的代数免疫度AI(Algebraic Immunity)的概念。

定义 2.10. [60] 设 $f \in B_n$，则 f 的代数免疫度 $AI(f)$ 为在 $AN(f) \cup AN(1 \oplus f)$ 中非零布尔函数的代数次数的最小值，即

$$AI(f) = \min\{deg(g) \geq 1 | g \in AN(f) \cup AN(1 \oplus f)\}。$$

考虑 $f(x)$ 和 $f(x)\oplus 1$ 两种类型的代数方程。对于代数方程 $f(x)=0$，若 $1\oplus f$ 存在低次零化子 g，即 $(1\oplus f)*g=0$，则得到低次方程 $g(x)=0$。对于代数方程 $f(x)=1$，若 f 存在低次零化子 h，即 $f*h=O$，则得到低次方程 $h(x)=0$。由此可见,在代数攻击中,建立的关于初始密钥的高次布尔函数 f 可以被 $f(x)$ 或 $f(x)\oplus 1$ 的零化子替代来得到低次的代数方程从而恢复密钥。因此，代数免疫度量化了布尔函数 f 的抗代数攻击性。

3. 相关免疫度

布尔函数相关免疫度本质上是一种更强的平衡性的要求。其概念最早是由T. Siegenthaler[85]针对密码系统的相关攻击[84]提出来的：

定义 2.11. 设 $n\in Z_+$，$f\in B_n$，若对于整数 $1\le m<n$ 满足：对所有的 $1\le r\le m$，限制 f 的任意 r 个分量以后，得到的函数均为平衡函数，则称 f 是 m 阶相关免疫的。更进一步，若 f 本身是平衡的，则称 f 是 m 阶弹性的。

利用布尔函数的$Walsh$变换，容易得到 m 阶相关免疫函数的一个简单刻画[91]：

定理 2.10. 设 $f\in B_n$，$m\le n$，则 f 是 m 阶相关免疫的，当且仅当对任意的 $\alpha\in F_2^n$，$1\le wt\alpha\le m$，都满足$W_f\alpha=0$。

布尔函数还有很多值得研究的密码学性质，更为详细的介绍参见文献[9]。

2.4　本章小结

本章主要介绍了有限域和布尔函数的一些基本知识。在介绍中所提及只是布尔函数几条常见的密码学性质，而针对不同的攻击，还有其它很多的密码学准则，如：高阶非线性度，高阶相关免疫度等等，在这里不再一一详述。相信随着新的攻击方法的出现，新的布尔函数的设计准则也会不断地被人们提出来。

因为布尔函数的这些密码学准则都是在不同的背景下提出来的，它们之间经常存在一种折衷的关系。某个准则达到最优的同时往往也削弱了其它的密码学性质。因此，针对不同的应用场合，研究密码函数的各种性质并且构造具有较好的综合的密码学性能的布尔函数也是非常有意义的研究课题。

第三章　*Bent*函数的存在性研究

*Bent*函数是具有最大非线性度的函数，这个概念首次由Rothaus[75]于1976 年提出。*Bent*函数不仅本身是很重要的组合结构，而且还在编码、密码及序列设计中有重要的应用；由此,很多学者对它进行了研究,特别是近十年,得到很多的研究成果[7, 11, 31, 79, 82]。

虽然*Bent*函数的定义很简单，但是*Bent*函数的结构是很复杂的。尽管迄今为止已经得到了很多的*Bent*函数的构造方法,包括一些直接构造和二次构造。但是就目前而言,对*Bent*函数的完全分类也是十分困难的。因此，对于*Bent*函数存在性的研究也是十分有意义的。

本章对*Bent*函数做了进一步的研究, 总结了*Bent*函数的定义与性质，以及齐次*Bent*函数的研究成果，并且给出了一类布尔函数不是*Bent*函数的充分条件。

3.1　*Bent*函数的定义和基本性质

3.1.1　*Bent*函数的*Walsh*谱定义

我们先以定义的方式重新回顾一下*Walsh*谱的概念。

定义 3.1. [75] 令$w=(w_1,w_2,\ldots,w_n)\in F_2^n$。 $f(x)$ 的傅里叶谱就被定义为

$$S_f(w)=\sum_{x\in F_2^n} f(x)(-1)^{w\cdot x}; \tag{3.1}$$

$f(x)$ 的*Walse*谱就被定义为

$$W_f(w)=\sum_{x\in F_2^n}(-1)^{w\cdot x\oplus f(x)} \tag{3.2}$$

其中$w\cdot x=w_1x_1+w_2x_2+\cdots+w_nx_n$。

引理 3.1. *[63]* 这两种变换的关系是:

$$S_f(w)=\begin{cases} 2^{n-1}-W_f(w)/2 & 若w=(0,0,\ldots,0),\\ -W_f(w)/2 & 其他。\end{cases}$$

利用布尔函数*Walsh*谱的概念，可以得到 $f(x)$ 的非线性度可以用其*Walsh*谱表示为

$$nl(f)=2^{n-1}-\frac{1}{2}\max_{w\in F_2^n}|W_f(w)|。 \tag{3.3}$$

容易验证，任意布尔函数的$Walsh$谱序列都满足 $Parseval$ 等式，即对任意的 $f \in B_n$，都有

$$\sum_{w \in F_2^n} W_f^2(w) = 2^{2n},$$

于是有

$$\max_{w \in F_2^n} |W_f(w)| \geq 2^{\frac{n}{2}}$$

所以对任意的布尔函数 f，都有

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1},$$

即 $nl(f)$ 有最大值 $2^{n-1} - 2^{\frac{n}{2}-1}$，此时 n 为偶数且 $\max_{w \in F_2^n} |W_f(w)|$，而达到此界的函数称为$Bent$函数。

定义 3.2. [75] 令$f(x)$ 是$F_2^n \to F_2$上的布尔函数。如果$|W_f(w)| = 2^{\frac{n}{2}}$对任意$w \in F_2^n$都成立，那么$f(x)$就被称为$Bent$函数。

因为非线性度是与所有的仿射函数之间的最小距离，因此$Bent$函数的非线性度也是 n 为偶数时1阶$Reed-Muller$码的覆盖半径。

3.1.2 $Bent$函数的等价定义及性质

下面的定理给出了$Bent$函数的一些等价定义。

定理 3.2. *[29]* 设 n 为正的偶数，$f \in B_n$，则下列说法等价:

- f 为$Bent$函数。
- 对任意的 $\alpha \in F_2^n$，$|W_f(\alpha)| = 2^{\frac{n}{2}}$。
- 定义 $2^n \times 2^n$ 阶矩阵 $A = ((-1)^{f(x \oplus y)})_{x,y \in F_2^n}$，$A$ 为 $Hadamard$ 矩阵。
- 对任意的 $a \in F_2^n$，$a \neq 0$，函数 $\triangle_f(a) = f(x) \oplus f(x \oplus a)$ 是平衡函数。
- 设 $g \in B_n$ 为任意仿射函数，$f + g$是$Bent$函数。

$Bent$函数还具有以下的性质:

定理 3.3. *[75]* 设 f 是 n 元$Bent$函数，n 是大于等于 4 的偶数，则必有

$$deg(f) \leq \frac{n}{2}。$$

定理 3.4. *[75]* 设 $f \in B_n$，$g(y) \in B_m$，则 $h(x,y) = f(x) \oplus g(y)$ 是 F_2^{n+m} 上的$Bent$函数，当且仅当 f, g 分别是 F_2^n 和 F_2^m 上的$Bent$函数。

3.2　齐次Bent函数的存在性

由于我们将一直研究Bent函数，在本章的剩余部分，我们将总是假设 n 为偶数。

关于二次Bent函数，它的计数及结构已经被研究清楚了[58]，一般地，二次函数的代数范式为：

$$f(x)=\sum_{1\le i<j\le n} a_{ij}x_ix_j \oplus l(x)\ \ l(x)\in A(n)a_{ij}\in F_2。$$

则其为Bent函数当且仅当它满足下面条件之一:

- 它的汉明重量为 $2^{n-1}\pm 2^{\frac{n}{2}-1}$;
- 定义 F_2 上的非奇异矩阵(m_{ij})：如果 $i<j$，$m_{ij}=a_{ij}$；如果 $i=j$，$m_{ij}=0$；如果 $i>j$，$m_{ij}=a_{ji}$，则该矩阵不是奇异的;
- 如果经过一个仿射非奇异变换，$f(x)$等价于函数

$$x_1x_2\oplus x_3x_4\oplus\cdots\oplus x_{n-1}x_n\oplus e,$$

其中 $e\in F_2$。

而对于 3 次以上的齐次Bent函数是否存在一直以来都是公开问题，直到文献[71]中发现了 3 次 6 元的齐次Bent函数后，关于齐次Bent函数的研究也有了很大的进展[13, 61, 62, 86, 90]。

定理 3.5. *[90] 设 f 是 $2n+2$ 元的 $n+1$ 次齐次布尔函数(其中 $n\ge 3$)，那么 f 不是一个Bent函数。*

该定理证明了 $2n$ 元的 n 次齐次Bent函数在 $n\ge 4$ 时是不存在的。文献[62]扩展了这个结论，给出了齐次Bent函数与变元数的进一步的关系：

定理 3.6. *[62] 对任意的非零整数 k，都存在整数 N 使得对任意的 $n\ge N$，$2n$ 变元的 $n-k$ 次或更高次的齐次Bent函数都不存在，其中 N 是满足*

$$2^{N-1}>\binom{N+1}{0}+\binom{N+1}{1}+\cdots+\binom{N+1}{k+1}$$

的最小的整数。

表 3.1: 齐次Bent函数的次数上界[62]

n	4	6	9	11	13	15	17
$d_{\max}$	0	1	2	3	4	5	6
$d_{\max}/n$	0	0.167	0.222	0.272	0.307	0.333	0.353

从图表3.1中我们可以发现，随着变元数 n 的增加，齐次Bent函数的最高次数与 n 的比例在逐渐提升，但始终低于 0.5。是否可以将这个性质推广到更一般的布尔函数上就成为了我们思考的问题，在下一节，我们将具体研究这个问题。

3.3 一类*Bent*函数的存在性研究

在这一节中，我们将构造一类特殊的布尔函数，并且研究其非线性度与代数标准型的关系。

3.3.1 *Bent*函数的谱表示性质

从引理3.1和定义3.2，我们可以得到 f 是*Bent*函数当且仅当

$$S_f(w)=\begin{cases}2^{n-1}\pm 2^{\frac{n}{2}-1} & 若w=(0,0,\ldots,0),\\ \pm 2^{\frac{n}{2}-1} & 其他。\end{cases}$$

首先我们给出*Bent*函数的傅里叶谱表示的一个应用。

引理 3.7. *[63]* 假设 $\alpha\in\mathbb{F}_2^k$ 且 $\beta\in\mathbb{F}_2^{n-k}$，其中 k,n 是满足 $k<n$ 的正整数。若 $f\in B_n$，则

$$f(\alpha,\beta)=\sum_{i=0}^{2^k-1}\delta_{a_i}(\alpha)f_i(\beta),$$

其中 $f_i\in B_{n-k}$，$0\le i\le 2^n-1$, $a_i\in\mathbb{F}_2^k$ 是i的二进制表示且满足

$$\delta_{a_i}(\alpha)=\begin{cases}1 & 若\alpha=a_i,\\ 0 & 其它。\end{cases}$$

根据上面的条件，我们有

$$[S_{f_0}(\beta),S_{f_1}(\beta),\ldots,S_{f_{2^k-1}}(\beta)]=[S_f(a_0,\beta),S_f(a_1,\beta),\ldots,S_f(a_{2^k-1},\beta)]H_k/2^k,$$

其中 H_k 是阶为 k 的*Hadamard*矩阵。

注 1. 由于*Hadamard*矩阵的第一行 H_k 是 $[1,1,\ldots,1]$，容易得到

$$S_{f_0}(\beta)=[S_f(a_0,\beta)+S_f(a_1,\beta)+\cdots+S_f(a_{2^k-1},\beta)]/2^k。$$

该引理揭示了布尔函数在部分点的*Walse*谱和其子函数汉明重量的关系。

从这条引理得到启发，对任意的非零布尔函数 $f\in B_n$，我们都可以将其表示成如下形式：

$$f(\boldsymbol{x})=\bigoplus_{i=1}^{k}x_{\delta_i}g_i(x_{\delta_{i+1}},x_{\delta_{i+2}},\ldots,x_{\delta_n})\oplus g(x_{\delta_{k+1}},x_{\delta_{k+2}},\ldots,x_{\delta_n}),\tag{3.4}$$

其中$g_i\in B_{n-i}$且 $(k\ge 0,1\le i\le k)$，$g\in B_{n-k}$且$(\delta_1,\delta_2,\ldots,\delta_n)$ 是$(1,2,\ldots,n)$的任意一个置换。

引理 3.8. 令 $f \in B_n$ 都有类似*(3.4)*的表示，那么有

$$\max_{w' \in \mathbb{F}_2^{n-k}} |W_g(w')| \leq \max_{w \in \mathbb{F}_2^n} |W_f(w)|。$$

证明. 令$\alpha = (x_{\delta_1}, x_{\delta_2}, \ldots, x_{\delta_k})$，$\beta = (x_{\delta_{k+1}}, x_{\delta_{k+2}}, \ldots, x_{\delta_n})$ 与引理3.7相同。若 $\alpha = (0, 0, \ldots, 0)$，那么我们可以的得到 $f_0 = g$。运用引理3.1及注1，可以得到

$$\begin{aligned} |W_{f_0}(\beta)| &= |[W_f(a_0, \beta) + W_f(a_1, \beta) + \cdots + W_f(a_{2^k-1}, \beta)]/2^k| \\ &\leq \max(|W_f(a_0, \beta)|, |W_f(a_1, \beta)|, \ldots, |W_f(a_{2^k-1}, \beta)|) \\ &\leq \max_{w \in \mathbb{F}_2^n} |W_f(w)| \end{aligned}$$

对任意的 $\beta \in \mathbb{F}_2^{n-k}$ 都成立。从而有

$$\max_{w' \in \mathbb{F}_2^{n-k}} |W_g(w')| = \max_{w' \in \mathbb{F}_2^{n-k}} |W_{f_0}(w')| \leq \max_{w \in \mathbb{F}_2^n} |W_f(w)|。$$

□

定理 3.9. 令 $f \in B_n$ 具有形式*(3.4)*。那么如果 $|W_g(w')| > 2^{\frac{n}{2}}$ 对任意一个 $w' \in \mathbb{F}_2^{n-k}$ 成立，则 f 不是*Bent*函数。

证明. 运用反证法。

如果 f 是 *Bent* 函数，那么有 $|W_f(w)| = 2^{\frac{n}{2}}$ 对任意 $w \in \mathbb{F}_2^n$。根据引理3.8，我们有

$$\max_{w' \in \mathbb{F}_2^{n-k}} |W_g(w')| \leq \max_{w \in \mathbb{F}_2^n} |W_f(w)| = 2^{\frac{n}{2}}。$$

易知结论。 □

为了得到最后的证明，我们还要介绍下面的一条引理。

引理 3.10. *[9]* 令 $f(x) \in B_m$, $g(y) \in B_n$ 且 $h(x, y) \in B_{m+n}$。如果

$$h(x, y) = f(x) \oplus g(y),$$

那么有

$$W_h(a, b) = W_f(a) \cdot W_g(b)$$

对任意 $a \in F_2^m$，$b \in F_2^n$ 都成立。

3.3.2 *d-upper*布尔函数的定义

从前一部分我们已经有了一些关于齐次*Bent*函数的研究进展，现在我们将介绍一类新的布尔函数，并以此研究*Bent*函数和其代数标准型的进一步关系。

定义 3.3. 如果在一个 n 元布尔函数 f 的代数标准型中，每个单项式的次数都大于等于 d，其中 $n \geq d$，那么 f 就叫做 *d-upper*布尔函数。特别的，我们将所有 n 元 *d-upper*布尔函数所构成的集合定义为$B_{n,d}$。

显然$B_{n,d}$包含了所有的 n 元 d 次齐次布尔多项式。

3.3.3 *d-upper Bent*函数与其代数标准型的关系

下面的定理揭示了*d-upper Bent*函数与其代数标准型中单项式数量的关系。

定理 3.11. *若 $d \geq 3$，$f \in B_{n,d}$且 f 的代数标准型中的单项式数量小于等于 $n+d-3$，那么 f 不是Bent函数。*

证明. 我们运用以下的策略来选择 f 的代数标准型中的 $\{x_{\delta_i}\}$：

1. 选择在 f 的代数标准型中单项式里出现次数最多的变元(至少为2，如果有多个，任选其一)作为 x_{δ_1}；

2. 选择在 f 的代数标准型中除了包含 x_{δ_1} 的单项式以外出现次数最多的变元(至少为2，如果有多个，任选其一)作为 x_{δ_2}；

3. 选择在 f 的代数标准型中除了包含 x_{δ_1} 和 x_{δ_2} 的单项式以外出现次数最多的变元(至少为2，如果有多个，任选其一)作为 x_{δ_3}；

4. 一直这样挑选直到所有的变元在 f 的代数标准型中至多出现一次。

假设我们挑选出了 k 个这样的变元，那么我们可以按照3.4的形式表示 f：

$$f(\boldsymbol{x}) = \bigoplus_{i=1}^{k} x_{\delta_i} g_i(x_{\delta_{i+1}}, x_{\delta_{i+2}}, \ldots, x_{\delta_n}) \oplus g(x_{\delta_{k+1}}, x_{\delta_{k+2}}, \ldots, x_{\delta_n})。$$

设 k_0 是 g 的代数标准型中单项式的数量，n_0 是 f 的代数标准型中单项式的数量。因为任意 x_{δ_i} 满足 $1 \leq i \leq k$ 都至少出现在两个单项式中，那么我们可以得到

$$2k + k_0 \leq n_0 \leq n + d - 3。$$

现在我们考虑下述两种情形：

1. 若 $n_0 < n$，则 $2k + k_0 \leq n_0 < n$。

2. 若 $n + d - 3 \geq n_0 \geq n$，则 x_{δ_1} 出现在至少d个单项式中(因为 f 的每个单项式至少包含 d 个变元)。因此，我们可以得到

$$2(k-1) + d + k_0 \leq n + d - 3$$

且 $2k + k_0 \leq n - 1$。

结合这两种情况，我们可以得到若 $n_0 \leq n + d - 3$，则 $2k + k_0 \leq n - 1$。

考虑 g 的代数标准型中单项式为

$$p_1, p_2, \ldots, p_{k_0}$$

并且它们的代数次数分别为

$$d_1, d_2, \ldots, d_{k_0}。$$

由于每个变元至多在 g 的代数标准型中出现一次，因此有 $n-k-(\sum_{i=1}^{k_0} d_i)$ (若$k_0=0$, $\sum_{i=1}^{k_0} d_i = 0$) 个变元不会出现在 g 的代数标准型中，除了$\{x_{\delta_j}\}$, $1 \le j \le k$之外。

考虑 g 的$Walsh$谱，通过引理3.10我们可以得到以下的方程：

$$\begin{aligned}
\max_{w' \in \mathbb{F}_2^{n-k}} |W_g(w')| &= 2^{n-k-(\sum_{i=1}^{k_0} d_i)} \prod_{j=1}^{k_0} \max_{a \in \mathbb{F}_2^{d_j}} |W_{p_j}(\boldsymbol{a})| \\
&= 2^{n-k-(\sum_{i=1}^{k_0} d_i)} \prod_{j=1}^{k_0} (2^{d_j} - 2) \\
&= 2^{n-k} \prod_{j=1}^{k_0} (1 - 2^{1-d_j})
\end{aligned}$$

注意到

$$当1 \le j \le k_0时，\ d_j \ge d \ge 3,$$

我们可以得到如下的不等式：

$$\begin{aligned}
\max_{w' \in \mathbb{F}_2^{n-k}} |W_g(w')| &\ge 2^{n-k} (\frac{3}{4})^{k_0} \\
&> 2^{n-k-\frac{k_0}{2}}。
\end{aligned}$$

由于 $2k + k_0 \le n-1 < n$，我们有 $k + \frac{k_0}{2} < \frac{n}{2}$。所以

$$\max_{w' \in \mathbb{F}_2^{n-k}} |W_g(w')| > 2^{n-k-\frac{k_0}{2}} = 2^{n-(k+\frac{k_0}{2})} > 2^{\frac{n}{2}}。$$

根据定理3.9，我们可以知道 f 不是一个$Bent$函数。 □

由于d 次齐次布尔函数也显然是一个d-$upper$布尔函数。根据定理3.11可以很容易得到下面的推论。

推论 3.12. *如果 f 是一个 n 元 d 次齐次布尔函数$(d \ge 3)$且 f 的代数标准型中的单项式数量小于等于 $n+d-3$，那么 f 不是$Bent$函数。*

3.3.4　d-$upper$ $Bent$函数的次数

与齐次布尔函数的结果类似，我们还可以得到d-$upper$ $Bent$函数中 d 的一个上界。

定理 3.13. 如果$f \in \mathbf{B}_{n,d}$并且

$$\sum_{i=0}^{\frac{n}{2}+1-d} \binom{\frac{n}{2}+1}{i} < 2^{\frac{n}{2}-1},$$

那么 f 不是$Bent$函数。

证明. 在 f 的表示(3.4)中令$k = \frac{n}{2} - 1$，则：

$$f(x) = \bigoplus_{i=1}^{\frac{n}{2}-1} x_{\delta_i} g_i(x_{\delta_{i+1}}, x_{\delta_{i+2}}, \ldots, x_{\delta_n}) \oplus g(x_{\delta_{\frac{n}{2}}}, x_{\delta_{\frac{n}{2}+1}}, \ldots, x_{\delta_n})。$$

显然 g 也是一个 $(\frac{n}{2}+1)$元的 d-$upper$布尔函数。所以 $g(x) = 0$ 若

$$wt(x) \leq d-1, \ x \in \mathbb{F}_2^{\frac{n}{2}+1},$$

那么我们有

$$S_g(0,0,\ldots,0) = wt(g) \leq \sum_{i=d}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{i}。$$

根据引理3.1，我们有

$$\begin{aligned} W_g(0,0,\ldots,0) &= 2^{\frac{n}{2}+1} - 2S_g(0,0,\ldots,0) \\ &\geq 2^{\frac{n}{2}+1} - 2\sum_{i=d}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{i} \\ &= 2^{\frac{n}{2}+1} - 2\sum_{i=d}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{\frac{n}{2}+1-i} \\ &= 2^{\frac{n}{2}+1} - 2\sum_{i=0}^{\frac{n}{2}+1-d} \binom{\frac{n}{2}+1}{i}。 \end{aligned}$$

因为

$$\sum_{i=0}^{\frac{n}{2}+1-d} \binom{\frac{n}{2}+1}{i} < 2^{\frac{n}{2}-1},$$

可以得到

$$\begin{aligned} W_g(0,0,\ldots,0) &\geq 2^{\frac{n}{2}+1} - 2\sum_{i=0}^{\frac{n}{2}+1-d} \binom{\frac{n}{2}+1}{i} \\ &> 2^{\frac{n}{2}+1} - 2 \cdot 2^{\frac{n}{2}-1} \\ &= 2^{\frac{n}{2}}。 \end{aligned}$$

由定理3.9可得 f 不是*Bent*函数。 □

由于d 次齐次布尔函数也显然是一个*d-upper*布尔函数，我们可以将之前介绍的齐次定理3.6作为本定理的一个显然的推论。

推论 3.14. *若* $f \in \mathbf{B}_{n,d}$ *且*

$$d \geq \lceil \frac{3n}{8} + \frac{3}{4} \rceil,$$

那么 f *不是Bent函数。*

证明. 由于

$$d \geq \lceil \frac{3n}{8} + \frac{3}{4} \rceil,$$

我们有

$$\begin{aligned} \sum_{i=0}^{\frac{n}{2}-d+1} \binom{\frac{n}{2}+1}{i} &\leq \sum_{i=0}^{\lfloor (\frac{n}{2}+1)/4 \rfloor} \binom{\frac{n}{2}+1}{i} \\ &< \frac{1}{4} \sum_{i=0}^{\frac{n}{2}+1} \binom{\frac{n}{2}+1}{i} \\ &= 2^{\frac{n}{2}+1}/4 \\ &= 2^{\frac{n}{2}-1}。 \end{aligned}$$

根据推论3.13，f 不是*Bent*函数。 □

上述推论暗示了对于*d-upper Bent*函数来说

$$d < \lceil \frac{3n}{8} + \frac{3}{4} \rceil。$$

事实上，根据定理3.13，我们可以得到*d-upper Bent*函数中 d 的上界。根据文献[58]，可以得到

$$\sum_{i=0}^{\lambda n} \binom{n}{i} < 2^{nH_2(\lambda)} \text{ for } 0 < \lambda < 1/2,$$

其中

$$H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)。$$

由此可以推出当 d 满足

$$\sum_{i=0}^{\frac{n}{2}+1-d} \binom{\frac{n}{2}+1}{i} < 2^{\frac{n}{2}-1}$$

时有

$$H_2(\frac{\frac{n}{2}+1-d}{\frac{n}{2}+1}) < \frac{\frac{n}{2}-1}{\frac{n}{2}+1} \text{ and } \frac{\frac{n}{2}+1-d}{\frac{n}{2}+1} < 1/2。$$

在 d 满足上述条件的时候，根据定理3.13，我们知道所有 $f \in B_{n,d}$ 都不是*Bent*函数。可以看到 $H_2(x) < 1$ 当 $x \neq 1/2$ 时，这意味着当 $n \to \infty$ 时，*d-upper Bent*函数中 d 的上界趋向于 $\frac{n}{4}$。

表3.2给出了一些 n 为具体值时 d 的上界。

表 3.2: *d-upper Bent*函数中 d 的上界

n	16	32	64	128	256	512	1024
$d_{\max}$	6	10	18	35	68	134	264
$d_{\max}/n$	0.375	0.312	0.281	0.273	0.266	0.262	0.258

3.4 本章小结

本章中我们阐述了*Bent*函数的定义并介绍了齐次*Bent*函数研究的相关成果和进展。进一步的，我们提出了一类新的布尔函数：*d-upper* 布尔函数，使得 d 次齐次布尔函数作为了其中的一个子集来进行研究。通过对*d-upper* 布尔函数代数标准型的分析，我们得到了*d-upper Bent*函数存在的一些必要条件，这也为寻找性质更好的*Bent*函数提供了参考。同时，分析*d-upper* 布尔函数的其他密码学性质也是值得研究的问题之一。

第四章　循环对称布尔函数的代数免疫性研究

代数攻击是近年来兴起的一种对多种类型的密码体制都有效的密码攻击方法，而构造高性能的布尔函数能够提高密码系统对代数攻击的抵抗程度。然而，由于布尔函数的数量极其巨大，通过穷举的方法获得具有高代数免疫性的布尔函数是十分困难的，大部分的研究都针对于某一类或者某几类布尔函数来进行。在这一章，我们将针对循环对称布尔函数，利用其特殊的性质，研究其对于快速代数攻击的抵抗程度。

4.1　代数攻击与快速代数攻击

早在1949年, *Shannon*便提出：我们可以将密码系统视作多变元的方程系统，密码破译的难点转化为通过寻找和求解某类特定的方程组，得到原始密钥。这是最早出现的代数攻击的思想，而在随后的几十年来并没有这方面的学术成果发表。近年来最初的代数攻击是在分析公钥密码系统$HFE(Hidden\ Field\ Equation)$等的基础上发展而来的。$HFE$公钥密码是建立在求解超定的二次多变元方程组的困难性基础上的，*Courtois*通过分析发现HFE中存在多余的多元等式[18]，引入了代数攻击。流密码的代数攻击的基本思想是建立密钥比特和输出比特之间的方程，通过解超定的低次方程组来恢复密钥。代数攻击在分析流密码的安全性方面起到了显著的效果，这一节我们将对针对流密码的代数攻击与快速代数攻击做一个简要的介绍。

4.1.1　代数攻击与代数免疫度

2003年,Courtois和Meier提出了代数攻击的概念[17]，对基于线性移位寄存器和高度非线性的布尔函数的无记忆的流密码体制进行了分析。其基本思想是通过将过滤布尔函数乘以另外一个多项式得到更低次的方程直接降低要求解的方程组的次数。从而求解次数更低的方程组来获得密钥。

对于仅有一个线性反馈移位寄存器 $LFSR$ 和一个布尔函数 f 构成的流密码算法，假设 $LFSR$ 的反馈函数为 L，初始密钥为 $K=(k_0,k_1,\ldots,k_{n-1})$，则对于任意时刻 t，$LFSR$ 的状态为 $L_t(K)=(k_t,k_{t+1},\ldots,k_{n+t-1})$。此时密钥流为 $f(L_t(K))=z_t$。假设 t 时候的密钥流已知，可以建立关于初始密钥和密钥流的代数方程。由于 L 是线性变换，代数方程的次数恒为 f 的代数次数，而不会随着迭代次数的增多而增高。假设我们得到很多时刻和其对应的密钥流，我们可以建立方程组：

$$\begin{cases} z_{t_1} = f(L_{t_1}(K)) \\ z_{t_2} = f(L_{t_2}(K)) \\ \vdots \\ z_{t_m} = f(L_{t_m}(K))。 \end{cases} \tag{4.1}$$

假设已知某些时刻和这些时刻的密钥流，这些时刻不一定是连续的。若存在多变元多项式g，使得fg有较低的代数次数或者能被较低代数次数的多项式逼近，便可将求解方程组(4.1)转化为求解一个较低次数的方程组

$$\begin{cases} z_{t_1} g(L_{t_1}(K) = f(L_{t_1}(K))g(L_{t_1}(K)) \\ z_{t_2} g(L_{t_2}(K) = f(L_{t_2}(K))g(L_{t_2}(K)) \\ \vdots \\ z_{t_m} g(L_{t_m}(K) = f(L_{t_m}(K))g(L_{t_m}(K))。 \end{cases} \tag{4.2}$$

的问题。

具体到针对流密码的代数攻击，我们可以可以通过两种方式获得包含密钥比特和输出比特的低次方程：一种是选择某一低次布尔函数 g，使得 fg 具有较低的代数次数，即 f 具有低次倍式，从而通过 f 的低次倍式来建立低次方程组；另一种是通过寻找 f 或 $f \oplus 1$ 的低次零化子建立低次方程。同时，如果 f 具有低次倍式，f 或 $f \oplus 1$ 的低次零化子。也就是说，在基于流密码的代数攻击中，如果 f 存在低次零化子 g，即 $fg = 0$，那么可以得到低次方程 $g(x) = 0$；若 $f \oplus 1$ 存在低次零化子 h，即 $(f \oplus 1)h = 0$，则可以得到低次方程 $h(x) = 0$。由此可见，布尔函数零化子的构造是代数攻击中的首要问题。

为了衡量布尔函数对代数攻击的抵抗程度，W.Meier 在2004年首先提出了代数免疫度(定义2.10)的概念。

定理 4.1. *[60] 令 f 为 n 元布尔函数。那么存在次数不超过 $\lceil \frac{n}{2} \rceil$ 布尔函数 g 使得 fg 的次数不超过 $\lceil \frac{n}{2} \rceil$。*

假设 $fg = h$，$deg(g) \leq \lceil \frac{n}{2} \rceil$，$deg(h) \leq \lceil \frac{n}{2} \rceil$，那么

$$f(g+h) = fg + f(fg) = 2fg = 0$$

且$deg(g+h) \leq \lceil \frac{n}{2} \rceil$。容易得到，对任意的布尔函数 f 都有

$$AI(f) \leq \lceil \frac{n}{2} \rceil。$$

4.1.2　快速代数攻击及布尔函数的快速代数免疫性

一般的代数攻击中，密钥流可以是不连续的，并没有利用到由 $LFSR$ 产生的相邻连续状态的迭代性。而对于连续的密钥流，因为 $LFSR$ 的反馈逻辑具有迭代性，即前后相邻的时刻，f函数的输入是满足一定的线性迭代关系的。Courtois在2003年CRYPTO上提出的快速代数攻击注意并利用了这个迭代性[19]。

假设在t时刻，我们可以得到方程

$$f(L_t(K)) = z_t,$$

并且存在布尔函数g $(degree(g) < AI(f))$，使得$fg = h$，其中h的次数不太大$(degree(h) \geq AI(f))$。则有

$$z_t g(L_t(K)) = h(L_t(K)),$$

可以用BM 算法求出线性关系α，使得

$$\bigoplus_{\alpha} z_t g(L_t(K)) = \bigoplus_{\alpha} h(L_t(K)) = 0,$$

从而得到次数更低关于初始密钥与密钥流的方程组。

文献[2, 55]都指出，布尔函数对于快速代数攻击的免疫程度，不能被代数免疫度所包含。因此，研究布尔函数对于快速代数攻击的免疫程度是一个非常有意义的问题。

对于流密码系统中的布尔函数而言，快速代数攻击的理念其实是找到一个次数比较低的多项式 g，使得 $gf = h$ 的次数不是太高，从而得到次数不超过 $deg(g)$ 的布尔函数方程组。而对于 $deg(g)$ 与 $deg(h)$ 的关系，有如下定理：

定理 4.2. *[60] 令 f 为 n 元布尔函数。那么对任意的整数 $e + d \geq n$，都存在 e 次多项式 g 和 d 次多项式 h，使得 $gf = h$。*

即有

$$deg(g) + deg(f) \leq n。$$

由此，布尔函数对于快速代数攻击的抵抗程度可以用以下指标来衡量：

定义 4.1. [40] 对于一个给定的多项式 f 和整数对 (e, d)，设存在某多项式 g 满足 $deg(g) \leq e$ 使得 $h = fg \neq 0$ 满足 $deg(h) \leq d$，那么我们称整数对 (e, d) 为 f 的可行对。

也就是说，如果我们想要寻找具有最优快速代数免疫度的函数，就要找到这样的布尔函数 f，其所有可行对 (d, e) 都满足 $d + e \geq n$。

4.2 循环对称布尔函数简介

循环对称布尔函数的概念最早由J. Pieprzyk和C.X. Qu在文献[70]中提出，他们对循环对称布尔函数的密码学性质进行了初步的分析，他们给出了所有单轨道2次齐次布尔函数的重量分布和非线性度的取值范围，并且估计了其求值运算的计算复杂度。由于循环对称布尔函数具有良好的密码学性质以及高效的求值算法，它很快受到了人们的广泛关注，多篇文章针对其不同的性质进行了不同角度的研究[22, 61, 80, 81, 86, 87]。

接下来我们先来介绍其基本定义。

设$x=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_2^n$，令

$$\rho(x)=(x_2,\ldots,x_n,x_1),$$

且

$$\rho^k(x)=\rho(\rho^{k-1}(x))。$$

定义 4.2. 设n元布尔函数f如果对任意的

$$x=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_2^n,$$

都有$f(\rho(x))=f(x)$，那么我们定义它为循环对称布尔函数。

定义$\mathbf{RSB}_n$为所有n元循环对称布尔函数f (RSBF)的集合。容易得到，循环对称布尔函数的代数标准型不会因为其变元$x_1,x_2,\cdots,x_n$做了循环置换ρ^k而随之改变。

设$c\in\mathbb{F}_2^n$，我们定义

$$G_n(c)=\{\rho^k(c):0\le k\le n-1\}。$$

定义$G_n(c)$中不同元素的数量为$order(c)$，即$order(c)=|G_n(c)|$。我们将$G_n(c)$中元素按字典序排第一的元素作为其代表元，那么定义$G_n(c)$ $(c\in\mathbb{F}_2^n)$中所有不同的代表元集合为$\Gamma(n)$。如果单项式x^c在循环对称布尔多项式f的代数标准型中系数为1，那么所有满足$u\in G_n(c))$的x^u都在f的代数标准型中系数为1，即$f\in\mathbf{RSB}_n$的代数标准型可以写成

$$f(x)=\bigoplus_{c\in\Gamma(n)} f_c \bigoplus_{u\in G_n(c)} x^u,\ x^u=x_1^{u_1}x_2^{u_2}\cdots x_n^{u_n},\ f_c\in\mathbb{F}_2。$$

对一个给定的整数c，我们记所有满足$u\in G_n(c))$的x^u为一个轨道。

例 4.1. 以$n=4$为例，我们来计算F_2^4上的所有轨道。

$$\{G_n(0,0,0,0)=(0,0,0,0)\},$$

$$\{G_n(0,0,0,1)=(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0)\},$$

$$\{G_n(0,0,1,1)=(0,0,1,1),(0,1,1,0),(1,0,0,1),(1,1,0,0)\},$$

$$\{G_n(0,1,0,1)=(0,1,0,1),(1,0,1,0)\},$$

$$\{G_n(0,1,1,1)=(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\},$$

$$\{G_n(1,1,1,1)=(1,1,1,1)\}。$$

可以看到，上面的每一行就代表着一个轨道，那么 F_2^4 上的循环对称布尔函数就是在每个轨道上取值都相同的布尔函数。

4.3　循环对称布尔函数的快速代数免疫性

为了计算布尔多项式的快速代数免疫性，文献[2]提出了运用矩阵来计算相应的 g 和 h 的算法。定义集合

$$\{x\in\mathbb{F}_2^n|wt(x)\leq e\}$$

为 $\mathcal{W}_e$，集合

$$\{x\in\mathbb{F}_2^n|wt(x)\geq e+1\}$$

为$\overline{\mathcal{W}_e}$。设 $y,z\in\mathbb{F}_2^n$，定义 $supp(z)\subset supp(y)$ 为 $z\subset y$，其中

$$supp(x)=\{i|x_i=1\};$$

并且定义

$$y\cup z=(y_1\vee z_1,\ldots,y_n\vee z_n),$$

其中∨是或计算符。

设代数次数不超过 e 的布尔函数 g 满足 $h=gf$的次数至多不超过 d。记

$$f(x)=\bigoplus_{c\in\mathbb{F}_2^n}f_cx^c,\ f_c\in\mathbb{F}_2,$$

$$g(x)=\bigoplus_{z\in\mathcal{W}_e}g_zx^z,\ g_z\in\mathbb{F}_2,$$

和

$$h(x)=\bigoplus_{y\in\mathcal{W}_d}h_yx^y,\ h_y\in\mathbb{F}_2。$$

我们有 $h_y=0$ 对任意的 $y\in\overline{\mathcal{W}_d}$ 都成立。那么我们可以得到

$$0=h_y=\bigoplus_{z\in\mathcal{W}_e}\bigoplus_{c\cup z=y}f_cg_z=\bigoplus_{z\in\mathcal{W}_e}g_z\bigoplus_{c\cup z=y}f_c,\ \text{for } y\in\overline{\mathcal{W}_d}。\tag{4.3}$$

上面的方程组如果看做关于变元 g_z 的方程组将是齐次线性的，将这个方程组的系数矩阵记作

$$\sum_{i=0}^{n-d-1}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$$

阶的矩阵 $M(f;e,d)$。运用以上的定义，对于布尔函数 f，不存在次数不大于 e 的 g 使得 $h=gf$ 的次数不大于 d 当且仅当矩阵 $M(f;e,d)$ 的秩与变元 g_z 的数量相同($\sum_{i=0}^{e}\binom{n}{i}$)，即 $M(f;e,d)$ 是列满秩的(证明参见[2, 32])。

定理 4.3. *[2, 32]* 设 $f\in\mathbf{B}_n$。那么不存在次数不大于 e 的 g 使得 gf 的次数不大于 d 当且仅当矩阵 $M(f;e,d)$ 是列满秩的。

假设 $D=\sum_{i=0}^{n-d-1}\binom{n}{i}$ 且 $E=\sum_{i=0}^{e}\binom{n}{i}$，由定理4.3可以得到计算布尔函数快速代数免疫性的一个判定算法：

Algorithm 1 [2] 是否对布尔函数 f 存在满足条件的 g and h

输入: n 元布尔函数 f 以及整数 e 和 d 满足 $1\le e\le d\le n-1$。

输出: 判定是否存在次数不大于 e 的 g 使得 $\deg(gf)\le d$。

1: 初始化$E\times E$ matrix G，且让其每一列都是 0。
2: 计算有序集合 $I\leftarrow\{\beta:|\beta|\le e\}$。
3: **for all** i 从 1 到 E **do**
4: 选择一个随机的 γ 满足 $|\gamma|=d+1$。
5: 决定集合 $B\leftarrow\{\beta:|\beta|\subseteq\gamma,|\beta|\le e\}$。
6: **for all** $\beta\in B$ **do**
7: 决定集合 $A\leftarrow\{\alpha\leftarrow\beta\subseteq\alpha\subseteq\gamma\}$。
8: 计算 $A\leftarrow\bigoplus_A f(\alpha)$。
9: 令 G 中第 i 行和第 β 列为 1 如果 $A=1$。
10: **end for**
11: **end for**
12: 求解线性方程组且输出不存在这样次数的 g 满足条件如果该方程组只有零解。

在这一章，我们将基于该定理和算法对循环代数布尔函数的快速代数免疫性进行研究。

4.3.1 计算循环对称布尔函数的快速代数免疫度的快速算法

在这一节中我们将运用循环对称布尔函数的性质减少在定理5.3中所应用的矩阵规模来有效的求解相应的方程组。运用循环对称布尔函数的代数标准型不会随着 ρ^k 而变化的性质，我们可以减少定理5.3中的变元数和方程数。这一节我们将介绍算法的实践过程并且在下一节对其进行分析和比较。

定义集合

$$\{y \in \Gamma(n) | wt(y) \leq e\}$$

为 $\Gamma_e(n)$，集合

$$\{y \in \Gamma(n) | wt(y) \geq d+1\}$$

为 $\bar{\Gamma}_d(n)$。那么可以得到 $|\bar{\Gamma}_d(n)| \approx D/n$ 和 $|\Gamma_e(n)| \approx E/n$。文献[87]给出了 $|\bar{\Gamma}_d(n)|$ 和 $|\Gamma_e(n)|$ 的具体值。设 $f \in \mathbf{RSB}_n$，假设次数不大于 e 的 $g \in \mathbf{RSB}_n$ 满足 $h = gf$ 的次数不大于 d。那么 h 也是一个循环对称布尔函数。设 g 的代数标准型为：

$$g(x) = \bigoplus_{z \in \Gamma_e(n)} g_z \bigoplus_{u \in G_n(z)} x^u,\ g_z \in \mathbb{F}_2。 \tag{4.4}$$

那么对于 $y \in \bar{\Gamma}_d(n)$ 我们可以得到：

$$0 = h_y = \bigoplus_{z \in \Gamma_e(n)} g_z \bigoplus_{u \in G_n(z)} \bigoplus_{c \cup u = y} f_c。 \tag{4.5}$$

上述关于 g_z 的方程是齐次线性的。记这些方程的系数矩阵为 $S(f;e,d)$，则其是一个 $|\bar{\Gamma}_d(n)| \times |\Gamma_e(n)|$ 阶的矩阵且它的第 y 行和第 z 列的元素是：

$$s_{y,z} = \bigoplus_{u \in G_n(z)} \bigoplus_{c \cup u = y} f_c, \tag{4.6}$$

其中 $y \in \bar{\Gamma}_d(n)$ 且 $z \in \Gamma_e(n)$。上述方程组具有非零解当且仅当矩阵 $S(f;e,d)$ 不是列满秩的。因此我们可以得到以下结论：

定理 4.4. *设 $f \in \mathbf{RSB}_n$。那么存在非零且次数不大于 e 的循环对称布尔函数 g 使得 gf 的次数不高于 d 当且仅当矩阵 $S(f;e,d)$ 是列满秩的。*

对于循环对称布尔函数，我们给出了一个更有效率的算法2。该算法是基于定理4.4而作出的。其中的矩阵 S 是定理4.4中的 $S(f;e,d)$。如果算法返回"*yes*"，那么说明矩阵 $S(f;e,d)$ 不是列满秩的，即根据定理4.4存在循环对称布尔函数 g 使得 $\deg(g) \leq e$ 且 $\deg(gf) \leq d$，也就是说 f 有 (e,d) 可行对(循环对称布尔函数 g 仍然是布尔函数)。如果 $S(f;e,d)$ 和 $V(f;e,d)$ 都是列满秩的，也就是根据定理4.3)不存在这样的 g满足条件，那么这个算法将返回"*no*"且这个回答是正确的；如果 $S(f;e,d)$ 是列满秩而矩阵 $V(f;e,d)$ 不是列满秩的，也就是根据定理4.3)存在这样的 g满足条件，那么这个算法将返回"*no*"，但是这个回答是错误的，如果我们要得到正确的结果，那么在执行了算法2后，还要执行算法1来确定其准确性。因此算法2是一个偏真算法。但是在下一节我们将通过实例来说明该算法的正确率是非常高的。

接下来我们来讨论算法2的计算复杂度。

Algorithm 2 对任意的循环对称布尔函数 f 判定满足条件的 g 和 h 是否存在

输入: 一个 n 元循环对称布尔函数 f 以及整数 e 和 d 满足 $1 \le e \le d \le n-1$。

输出: 判定是否存在次数不高于 e 的 g 使得 $\deg(gf) \le d$。

1: 初始化 $|\bar{\Gamma}_d(n)| \times |\Gamma_e(n)|$ 阶矩阵 S，并且令其每一列都是 0。
2: 计算有序集合 $\Gamma_e(n)$ 和 $\bar{\Gamma}_d(n)$。
3: **for all** $y \in \bar{\Gamma}_d(n)$ **do**
4: **for all** $z \in \Gamma_e(n)$ **do**
5: 构造集合 $\mathcal{A} \leftarrow \{c|c \cup u = y, u \in G_n(z)\}$。
6: 计算 $s \leftarrow \bigoplus_{c \in \mathcal{A}} f_c$。
7: 如果 $s = 1$，那么令矩阵 S 第 y 行和第 z 列的元素为 1。
8: **end for**
9: **end for**
10: **if** S 不是满秩的 **then**
11: 输出*yes*。
12: **else**
13: 输出*no*。
14: **end if**

在算法2中矩阵 S 的阶是

$$|\bar{\Gamma}_d(n)| \times |\Gamma_e(n)| \approx D/n \times E/n。$$

所以矩阵 S 的初始化需要至多

$$\mathcal{O}(|\bar{\Gamma}_d(n)| \cdot |\Gamma_e(n)|) \approx \mathcal{O}(DE/n^2)$$

的时间和空间。集合 $\Gamma_e(n)$ 和 $\bar{\Gamma}_d(n)$ 可以在 $\mathcal{O}(E+D)$ 的时间内构造完成。之后我们从集合 $\bar{\Gamma}_d(n)$ 选择一个给定的 y，并且从 $\Gamma_e(n)$ 中选择一个给定的 z。这一步将重复 $|\Gamma_e(n)| \cdot |\bar{\Gamma}_d(n)|$ 次。对于给定的 y 和 z，计算 $\mathcal{A}$ 的时间复杂度至多是

$$|G_n| \cdot |\{c|c \cup u = y\}| \ \le \ n2^{wt(u)} \ \le \ n2^e < nE$$

(因为对任意的 $e < n/2$ 有 $2^e < \binom{n}{e} < E$)。我们可以知道 $|\mathcal{A}| < nE$。综上所述

$$|\Gamma_e(n)| \cdot |\bar{\Gamma}_d(n)| \cdot 2nE \approx 2DE^2/n。$$

最后一步求解多项式组的时候需要

$$\mathcal{O}(|\bar{\Gamma}_d(n)| \cdot |\Gamma_e(n)|^2) \approx \mathcal{O}(DE^2/n^3)$$

的时间复杂度。因此算法2的时间复杂度是 $\mathcal{O}(DE^2/n)$，空间复杂度是 $\mathcal{O}(DE/n^2)$ 。

4.3.2　算法实例

我们的算法是基于 *Armknecht* 的算法[2]的改进。在 *Armknecht* 的算法中所需要的矩阵[1]大小为$D \times E$。其算法需要 $\mathcal{O}(DE^2)$ 的步骤并且需要 $\mathcal{O}(DE)$ 的复杂度。与 *Armknecht* 的算法相比，算法2 在循环对称布尔函数的计算中无疑具有更高的效率。如果是求解相关的多项式组(而不是判定这个矩阵是不是列满秩的)，那么算法2 的时间复杂度是 $\mathcal{O}(DE^2/n + D^2E/n^3)$，空间复杂度是 $\mathcal{O}(DE/n^2)$；而 *Armknecht* 的算法的时间复杂度是 $\mathcal{O}(D^2E)$，空间复杂度是 $\mathcal{O}(DE)$ 。

注意到当 $wt(c) \leq d - e$ 时，f 的代数标准型中的系数 f_c 对是否存在次数不超过 e 的 g 使得 $\deg(gf) \leq d$ 没有影响。所以，在实际的算法运用中，对于给定的整数对 (d, e)，满足 $wt(c) \leq d - e$ 的系数 f_c 都可以设置为零以简化计算。运用这种技巧，我们提高算法的效率。

下面的图表4.1、4.2和4.3是该算法的实例结果。对于那些我们没有办法穷举全部的循环对称布尔函数的数字 (n, e, d)，我们都选择了尽量多的随机布尔函数来运行该算法。我们用 $num(f)$、$num(f_S)$ 和 $num(f_V)$ 分别表示我们计算的循环对称布尔函数的数量，满足矩阵 $S(f; e, d)$ 是列满秩的布尔函数的数量，以及满足矩阵 $V(f; e, d)$ 是列满秩的布尔函数的数量。而符号 $\Pr(f_V|f_S)$ 和 $\Pr(\text{Alg.2})$ 分别表示概率

$$\Pr(f_V|f_S) = \Pr[V(f; e, d)\text{列满秩}|S(f; e, d)\text{ 列满秩}] = \frac{num(f_V)}{num(f_S)}$$

以及概率

$$\Pr(\text{Alg.2}) = \Pr[\text{算法2结果正确}] = 1 - \frac{num(f_S) - num(f_V)}{num(f)}。$$

在实验中我们发现当 $n = 2^m$ 时，算法2的结果总是正确的，见表格4.1。在这个表格中我们穷举了所有满足 $(2^m, e, d)$ 的循环对称布尔函数。我们还对于大量的 8 元和 16 元循环对称布尔函数运用该算法进行了检验，发现该规律依然成立。基于上述观察我们提出以下猜想：

猜想 4.1. 设 $m \geq 2$ 且 $f \in \mathbf{RSB}_{2^m}$。那么存在次数不超过 e 的非零布尔函数 g 使得 $\deg(gf) \leq d$ 成立当且仅当存在次数不超过 e 的非零循环对称布尔函数 g 使得 $\deg(gf) \leq d$。也就是说，矩阵 $V(f; e, d)$ 是列满秩的当且仅当矩阵 $S(f; e, d)$ 是列满秩的。

根据上述实验结果，算法2的结果是正确的概率依然很大当 $n \neq 2^m$时，参见图表4.2、4.3。在图表4.2和4.3中，除了 $num(f)$，$num(f_S)$ 和 $num(f_V)$ 以外，我们还计

[1]在这里我们指的是在定理4.3中的矩阵 $V(f; e, d)$，而不是算法1中的 $E \times E$ 阶的矩阵 G，因为这个算法只是一个偏错算法，而不是确定算法

表 4.1: 计算当 $n = 2^m$ 时循环对称布尔函数的快速代数免疫程度

(n, e, d)	$num(f)$	$num(f_S)$	$num(f_V)$
(4,1,2)	16	4	4
(4,1,1)	32	14	14
(8,1,6)	64	16	16
(8,1,5)	8192	6848	6848
(8,2,5)	8388608	720896	720896
(16,1,14)	1024	256	256

表 4.2: 当 $n \neq 2^m$ 且 $e + d = n - 1$ 时算法2的成功率

(n, e, d)	$num(f)$	$num(f_S)$	$num(f_V)$	$\Pr(f_V \mid f_S)$	Pr(Alg.2)
(5,1,3)	16	4	3	0.750	0.938
(5,2,2)	128	28	15	0.536	0.898
(6,1,4)	32	8	4	0.500	0.875
(6,2,3)	4096	384	112	0.292	0.934
(7,1,5)	32	8	7	0.875	0.969
(7,2,4)	32768	7168	5530	0.771	0.950
(7,3,3)	524288	21952	10416	0.474	0.978
(9,1,7)	64	16	7	0.438	0.859
(9,2,6)	471194	100000	50004	0.500	0.894
(9,3,5)	571059	100000	49436	0.494	0.911
(9,4,4)	4273707	100000	16390	0.164	0.980
(10,1,8)	128	32	24	0.750	0.938
(10,2,7)	941650	100000	59049	0.590	0.957
(10,3,6)	983716	100000	59131	0.591	0.958
(10,4,5)	1289362	100000	41734	0.417	0.955
(11,1,9)	128	32	31	0.969	0.992
(11,2,8)	470759	100000	96823	0.968	0.993
(11,3,7)	258831	53573	52163	0.974	0.995
(11,4,6)	54786	11593	11251	0.970	0.994
(11,5,5)	127921	2061	1043	0.506	0.992

算了 $\Pr(f_V|f_S)$ 和 Pr(Alg.2)对任意的 n 满足 $5 \leq n \leq 11$ 且 $n \neq 8$ 和每一对 (e, d) 满足 $e + d = n - 1$ 及 $e + d = n - 2$。

表 4.3: 当 $n \neq 2^m$ 且 $e+d=n-2$ 时算法2的成功率

(n,e,d)	$num(f)$	$num(f_S)$	$num(f_V)$	$\Pr(f_V\|f_S)$	$\Pr(\text{Alg.2})$
(5,1,2)	64	46	45	0.978	0.984
(6,1,3)	512	408	394	0.966	0.973
(6,2,2)	8192	3676	2914	0.793	0.907
(7,1,4)	1024	872	869	0.997	0.997
(7,2,3)	262144	216048	213654	0.989	0.991
(9,1,6)	65536	60544	60319	0.996	0.997
(9,2,5)	100875	100000	99915	0.999	0.999
(9,3,4)	102651	100000	99875	0.999	0.999
(10,1,7)	524288	496128	496068	0.9999	0.9999
(10,2,6)	100498	100000	100000	1	1
(10,3,5)	100033	100000	100000	1	1
(10,4,4)	107218	100000	99873	0.999	0.999
(11,1,8)	4194304	4032512	4032511	$1-2^{-21.9}$	$1-2^{-22}$
(11,2,7)	100010	100000	100000	1	1
(11,3,6)	28120	28120	28120	1	1
(11,4,5)	9319	9319	9319	1	1

当 $e+d=n-1$ 时，如表4.2所示，$\Pr(\text{Alg.2})$总是接近于 1，同时 $\Pr(f_V|f_S)$ 基本是由 n 和 e 所决定的。

当 $e+d=n-2$ 是，如表4.3所示，$\Pr(\text{Alg.2})$和 $\Pr(f_V|f_S)$ 都与 1 很接近。在这种情形中，我们可以发现 $num(f_V)$ 与 $num(f)$ 非常接近，也就是说

$$num(f_V) \approx num(f_S) \approx num(f)$$

且

$$num(f_V) \leq num(f_S) \leq num(f)。$$

因此

$$\Pr(\text{Alg.2}) \approx \Pr(f_V|f_S) \approx 1。$$

注意到如果 f 不存在可行对 (e,d) 满足 $e+d=n-2$，那么也就不存在可行对 (e,d) 满足 $e+d<n-2$ 所以，对于 $e+d<n-2$ 的情形，我们有 $num(f_V)$ 与 $num(f)$ 的数量非常接近，因此也会有

$$\Pr(\text{Alg.2}) \approx \Pr(f_V|f_S) \approx 1。$$

综上所诉，实验结果表明，我们的算法以一个非常接近 1 的概率输出正确的结果，并且在 n 取某些值时，总是输出正确的结果。

4.3.3 矩阵 $S(f;e,d)$ 的性质

如果 $d=n-e-1$，那么 $|\bar{\Gamma}_d(n)|=|\Gamma_e(n)|$，即 $S(f;e,d)$ 是一个方阵。那么决定是否存在次数不超过 e 的非零循环对称布尔函数 g 使得 $\deg(gf)\leq n-e-1$ 的问题就转化为判定矩阵 $S(f;e,n-e-1)$ 是否可逆的问题。在这一节，我们将对于非零整数 m,t，具体研究矩阵 $S(f;e,d)$ 在 $n=2^m t$ 时的性质。

命题 4.5. 设 $y\in\Gamma(n)$，则 $s_{y,\mathbf{0}_n}=f_y$。

证明. 根据 (4.6)，我们有

$$s_{y,\mathbf{0}_n}=\bigoplus_{u\in G_n(\mathbf{0}_n)}\bigoplus_{c\cup u=y} f_c=\bigoplus_{c\cup \mathbf{0}_n=y} f_c=f_y。$$

□

在考虑矩阵 $S(f;e,d)$ 的其他性质之前，我们先介绍一些有用的引理。引理4.6将用于证明4.7；引理4.8及引理4.9将用于证明命题4.10和命题4.11。

引理4.6在文献[80]中有描述性的证明，在这里我们给出一个完整的证明。

引理 4.6. 设 $c\in\mathbb{F}_2^n$，那么

1) $order(c)|n$;

2) $\frac{n}{\gcd(n,\,wt(c))}|\,order(c)$。

证明. 1) 考虑 $order(c)$ 是 $G_n(c)$ 的阶，即 $order(c)$与满足 $\rho^t(c)=c$ 的最小整数 t相等。所以从 $\rho^n(c)=c$ 可以得到 $order(c)|n$。

2) 设 $k=n/\,order(c)$。则 c 可以表示成

$$c=(\underbrace{b,b,\ldots,b}_{k}),\ b\in\mathbb{F}_2^{order(c)}。$$

所以 $wt(b)=wt(c)/k$，也就是说 $k|\,wt(c)$ 且 $n|\,order(c)\cdot wt(c)$。易得此引理。 □

设 $t|n$，我们定义

$$\eta_t=(\underbrace{1,1,\ldots,1,0}_{t},\underbrace{1,1,\ldots,1,0}_{t},\ldots,\underbrace{1,1,\ldots,1,0}_{t}),$$

和

$$\tilde{\eta}_t=(\underbrace{1,0,0,\ldots,0}_{t},\underbrace{1,0,0,\ldots,0}_{t},\ldots,\underbrace{1,0,0,\ldots,0}_{t})。$$

容易得到

$$wt(\eta_t) = n - n/t,\ wt(\tilde{\eta}_t) = n/t$$

和

$$order(\eta_t) = order(\tilde{\eta}_t) = t。$$

设 $c \in \mathbb{F}_2^n$ 且 $t|n$，设

$$G_n^t(c) = \{c, \rho^t(c), \ldots, \rho^{(\nu_t(c)-1)t}(c)\},$$

其中 $\nu_t(c)$ 是满足 $\rho^{\nu_t(c)t}(c) = c$ 的最小整数。根据 $\nu(c)$ 和 $\nu_t(c)$ 我们可以得到

$$\nu_t(c) = \frac{order(c)}{\gcd(order(c), t)}。 \tag{4.7}$$

引理 4.7. 设 $n = 2^m t$ 且 $n - 2^m \leq wt(c) \leq n - 1$。如果 $c \in G_n(\eta_t)$，那么 $\nu(c) = t$ 且 $\nu_t(c) = 1$；否则，$\nu(c)$ 和 $\nu_t(c)$ 都是偶数。

证明. 设 $c \in G_n(\eta_t)$ 我们有 $\nu(c) = t$，而且根据(4.7)我们有 $order_t(c) = 1$。

接下来我们来证明引理的后半部分。

设 $c \notin G_n(\eta_t)$ 且 $wt(c) = n - 2^m$，那么我们有 $\rho^t(c) \neq c$ 且 $\nu(c) \neq t$。根据引理4.6(1)我们可以得到 $order(c)|n = 2^m t$，且根据4.6(2)我们有$t|\ order(c)$。由此可得 $2t|\nu(c)$。那么 $order(c)$ 和

$$\nu_t(c) = order(c)/\gcd(order(c), t) = order(c)/t$$

都是偶数。

设 $n - 2^m < wt(c) \leq n - 1$，那么可以得到 $1 \leq n - wt(c) < 2^m$ 且

$$\gcd(n, wt(c)) = \gcd(n, n - wt(c)) < 2^m。$$

根据(4.7)我们可以知道

$$order(c)|\ order_t(c) \cdot t,$$

由此根据4.6(2)我们可以得到

$$\frac{2^m t}{\gcd(2^m t, wt(c))}|\ order_t(c) \cdot t,$$

和 $\nu_t(c)$ 都是偶数，即当 $\nu_t(c)|\nu(c)$时，$\nu(c)$ 是偶数。 □

引理4.8可以用类似的方法证明。

引理 4.8. 设 $n = 2^m t$ 且 $1 \leq wt(c) \leq 2^m$。如果 $c \in G_n(\tilde{\eta}_t)$，那么 $\nu(c) = t$ 且 $\nu_t(c) = 1$；否则，$\nu(c)$ 和 $\nu_t(c)$ 都是偶数。

引理 4.9. 设 $n = 2^m t$ 且 $n - 2^{m+1} \leq wt(c) \leq n - 2^m$。如果 $c \in G_n(\eta_t)$ 或者 $c \in G_n(\eta_t \oplus \rho^k(\tilde{\eta}_t))$ 当 $2 \leq k \leq n$ 时，则 $\nu_t(c) = 1$；否则，$\nu_t(c)$ 是偶数。

证明. 当 $wt(c) = n - 2^m$ 时，引理4.7已经证明了该结果。

当 $c \in G_n(\eta_t \oplus \rho^k(\tilde{\eta}_t))$ 且满足 $2 \leq k \leq n$ 时，我们可以得到 $\rho^t(c) = c$，由此可得 $\nu_t(c) = 1$。

当 $c \notin G_n(\eta_t \oplus \rho^k(\tilde{\eta}_t))$ 且满足 $wt(c) = n - 2^{m+1}$ 时，可以得到 $\rho^t(c) \neq c$，由此可得 $\nu(c) \nmid t$。根据引理4.6(1)，我们可以得到 $order(c) | n = 2^m t$；根据引理4.6(2)，我们了以得到

$$\frac{2^m t}{\gcd(2^m t,\ wt(c))} = \frac{t}{\gcd(t, 2)} | \ order(c)。$$

因此 $2t | \nu(c)$。那么根据(4.7)可以得到 $\nu_t(c) = \ order(c)/t$。

当 $n - 2^{m+1} < \ wt(c) < n - 2^m$时，可以得到 $2^m < n - \ wt(c) < 2^{m+1}$，由此可得

$$2^m \nmid \gcd(n, n - \ wt(c)) = \gcd(n,\ wt(c))。$$

根据(4.7)我们知道 $order(c) |\ order_t(c) \cdot t$，再根据引理4.6(2)我们有

$$\frac{2^m t}{\gcd(2^m t,\ wt(c))} | \ order_t(c) \cdot t,$$

因此 $\nu_t(c)$ 是偶数。 □

命题 4.10. 设 $n = 2^m t$。那么

$$s_{\mathbf{1}_n, z} = \begin{cases} f_{\mathbf{1}_n} & \text{当 } z = \mathbf{0}_n \text{ 时;} \\ t(f_{\mathbf{1}_n} \oplus f_{\eta_t}) & \text{当 } z = \tilde{\eta}_t \text{ 时;} \\ 0 & \text{当 } z \in \Gamma_{2^m}(n) \setminus \{\mathbf{0}_n, \tilde{\eta}_t\} \text{ 时。} \end{cases}$$

证明. 根据命题4.5，可以得到$s_{\mathbf{1}_n, \mathbf{0}_n} = f_{\mathbf{1}_n}$。根据(4.6)，我们有

$$\begin{aligned} s_{\mathbf{1}_n, z} &= \bigoplus_{u \in G_n(z)} \bigoplus_{c \cup u = \mathbf{1}_n} f_c \\ &= \bigoplus_{k=0}^{\nu(z)-1} \bigoplus_{c \cup \rho^k(z) = \mathbf{1}_n} f_c \\ &= \bigoplus_{k=0}^{\nu(z)-1} \bigoplus_{\rho^k(c) \cup \rho^k(z) = \mathbf{1}_n} f_{\rho^k(c)}。 \end{aligned}$$

由于 $\rho^k(c) \cup \rho^k(u) = \mathbf{1}_n$ 当且仅当 $c \cup u = \mathbf{1}_n$。而且又因为 $f_{\rho^k(c)} = f_c$ 当 $f \in \mathbf{RSB}_n$时，我们知道

$$s_{\mathbf{1}_n, z} = \nu(z) \bigoplus_{c \cup z = \mathbf{1}_n} f_c。$$

根据引理4.8，可以得到

$$s_{\mathbf{1}_n,z}=0,\ \text{for}\ z\in\Gamma_{2^m}(n)\setminus\{\mathbf{0}_n,\tilde{\eta}_t\},$$

而且当 $z=\tilde{\eta}_t$ 时，

$$s_{1^n,\tilde{\eta}_t}=t\bigoplus_{c\cup\tilde{\eta}_t=\mathbf{1}_n}f_c。$$

定义所有集合 $G_n^t(c)$ 中的字典序首元素集合记为 C，其中

$$wt(c)\geq n-\ wt(\tilde{\eta}_t)=n-2^m,$$

那么

$$s_{1^n,\tilde{\eta}_t}=t\bigoplus_{c\in C}\ \bigoplus_{\substack{0\leq k\leq\nu_t(c)-1\\ \rho^{kt}(c)\cup\tilde{\eta}_t=\mathbf{1}_n}}f_{\rho^{kt}(c)}。$$

由于$\rho^t(\tilde{\eta}_t)=\tilde{\eta}_t$，可以推出 $\rho^t(c)\cup\tilde{\eta}_t=\mathbf{1}_n$ 当且仅当 $c\cup\tilde{\eta}_t=\mathbf{1}_n$。那么有

$$\begin{aligned}s_{1^n,\tilde{\eta}_t}&=t\bigoplus_{\substack{c\in C\\ c\cup\tilde{\eta}_t=\mathbf{1}_n}}\nu_t(c)f_c\\&=t(f_{1_n}\oplus f_{\eta_t})\oplus t\bigoplus_{\substack{c\in C\setminus\{1_n,\eta_t\}\\ c\cup\tilde{\eta}_t=\mathbf{1}_n}}\nu_t(c)f_c\\&=t(f_{1_n}\oplus f_{\eta_t})\ (\text{根据引理4.7})。\end{aligned}$$

□

命题 4.11. 设 $n=2^mt$。那么有

$$s_{\eta_t,z}=\begin{cases}f_{\eta_t} & \text{当 } z=\mathbf{0}_n \text{ 时;}\\ 0 & \text{当 } z\in\Gamma_{2^m}(n)\setminus\{\mathbf{0}_n,\tilde{\eta}_t\} \text{ 时。}\end{cases}$$

且

$$s_{\eta_t,\tilde{\eta}_t}=\begin{cases}0 & \text{当 } t \text{ 为偶数;}\\ f_{\eta_t}\oplus f_{\eta_{\frac{t}{2}}} & \text{当 } t \text{ 为奇数。}\end{cases}$$

证明. 应用命题4.5，可以得到

$$s_{\eta_t,\mathbf{0}_n}=f_{\eta_t}。$$

根据(4.6)，可以得到

$$s_{\eta_t,z}=\bigoplus_{u\in G_n(z)}\ \bigoplus_{c\cup u=\eta_t}f_c。$$

定义所有集合 $G_n^t(u)$ 中的字典序首元素集合记为 U，其中 $u \in G_n(z)$。由 $\rho^{kt}(c) \cup \rho^{kt}(u) = \eta_t$ 当且仅当 $c \cup u = \eta_t$ 可以得到

$$\begin{aligned} s_{\eta_t,z} &= \bigoplus_{u\in U} \bigoplus_{k=0}^{\nu_t(u)-1} \bigoplus_{c\cup\rho^{kt}(u)=\eta_t} f_c \\ &= \bigoplus_{u\in U} \bigoplus_{k=0}^{\nu_t(u)-1} \bigoplus_{\rho^{kt}(c)\cup\rho^{kt}(u)=\eta_t} f_{\rho^{kt}(c)} \\ &= \bigoplus_{u\in U} \bigoplus_{k=0}^{\nu_t(u)-1} \bigoplus_{c\cup u=\eta_t} f_c \\ &= \bigoplus_{u\in U} \nu_t(u) \bigoplus_{c\cup u=\eta_t} f_c。 \end{aligned}$$

当 $z \in \Gamma_{2^m}(n) \setminus \{0_n, \tilde{\eta}_t\}$ 时，根据引理4.8，我们可以得到$\nu_t(u)$ with $u \in G_n(z)$ 是偶数，因此 $s_{r,z} = 0$。

当 $z = \tilde{\eta}_t$, we have $\rho(\tilde{\eta}_t) \not\subset \eta_t$ 时，因此当 $u = \rho(\tilde{\eta}_t)$ 时，$c \cup u \neq \eta_t$，所以有

$$s_{\eta_t,\tilde{\eta}_t} = \bigoplus_{\substack{u\in G_n(\tilde{\eta}_t)\\ u\neq\rho(\tilde{\eta}_t)}} \bigoplus_{c\cup u=\eta_t} f_c = \bigoplus_{k=2}^{t} \bigoplus_{c\cup\rho^k(\tilde{\eta}_t)=\eta_t} f_c。$$

定义所有集合 $G_n^t(c)$ 中的字典序首元素集合记为 C，其中 $n-2^{m+1} \leq wt(c) \leq n-2^m$。由于 $\rho^t(\eta_t) = \eta_t$ 和 $\rho^t(\rho^k(\tilde{\eta}_t)) = \rho^k(\tilde{\eta}_t)$，因此有 $\rho^{it}(c) \cup \rho^k(\tilde{\eta}_t) = \eta_t$ 当且仅当 $c \cup \rho^k(\tilde{\eta}_t) = \eta_t$。因此

$$\begin{aligned} s_{\eta_t,\tilde{\eta}_t} &= \bigoplus_{k=2}^{t} \bigoplus_{c\in C} \bigoplus_{\substack{u\in G_n^t(c)\\ u\cup\rho^k(\tilde{\eta}_t)=\eta_t}} f_u \\ &= \bigoplus_{k=2}^{t} \bigoplus_{c\in C} \bigoplus_{\substack{0\leq i\leq \nu_t(c)-1\\ \rho^{it}(c)\cup\rho^k(\tilde{\eta}_t)=\eta_t}} f_{\rho^{it}(c)} \\ &= \bigoplus_{k=2}^{t} \bigoplus_{\substack{c\in C\\ c\cup\rho^k(\tilde{\eta}_t)=\eta_t}} \nu_t(c) f_c \\ &= \bigoplus_{k=2}^{t} (f_{\eta_t} \oplus f_{\eta_t\oplus\rho^k(\tilde{\eta}_t)}) \text{ (根据引理4.9)。} \end{aligned}$$

注意到当 $2 \leq k \leq t$时，

$$\eta_t \oplus \rho^k(\tilde{\eta}_t) = \rho^{k-1}(\eta_t) \oplus \rho(\tilde{\eta}_t) = \rho^{k-1}(\eta_t \oplus \rho^{t+2-k}(\tilde{\eta}_t))。$$

那么 $f_{\eta_t\oplus\rho^k(\tilde{\eta}_t)}=f_{\eta_t\oplus\rho^{t+2-k}(\tilde{\eta}_t)}$ 并且对于奇数 t，

$$s_{\eta_t,\tilde{\eta}_t}=2\bigoplus_{k=2}^{\frac{t+1}{2}}(f_{\eta_t}\oplus f_{\eta_t\oplus\rho^k(\tilde{\eta}_t)})=0。$$

而对于偶数 t，

$$\begin{aligned}s_{\eta_t,\tilde{\eta}_t}&=f_{\eta_t}\oplus f_{\eta_t\oplus\rho^{\frac{t}{2}+1}(\tilde{\eta}_t)}\oplus 2\bigoplus_{k=2}^{\frac{t}{2}}(f_{\eta_t}\oplus f_{\eta_t\oplus\rho^k(\tilde{\eta}_t)})\\&=f_{\eta_t}\oplus f_{\eta_{\frac{t}{2}}}。\end{aligned}$$

□

在这里我们给出矩阵 $S(f;e,d)$ 的一个例子。

例 4.2. 当 $e=1$ 且 $d=n-2$ 时，矩阵 $S(f;e,d)$ 是

$$S(f;1,n-2)=\begin{pmatrix}s_{\mathbf{1}_n,\mathbf{0}_n} & s_{\mathbf{1}_n,\tilde{\eta}_n}\\ s_{\eta_n,\mathbf{0}_n} & s_{\eta_n,\tilde{\eta}_n}\end{pmatrix}。$$

设 $m=0$ 且 $t=n$，在命题4.10和4.11里，我们可以得到

$$S(f;1,n-2)=\begin{pmatrix}f_{\mathbf{1}_n} & 0\\ f_{\eta_n} & f_{\eta_n}\oplus f_{\eta_{\frac{n}{2}}}\end{pmatrix}，\text{当 } n \text{ 为偶数时，}$$

且

$$S(f;1,n-2)=\begin{pmatrix}f_{\mathbf{1}_n} & f_{\mathbf{1}_n}\oplus f_{\eta_n}\\ f_{\eta_n} & 0\end{pmatrix}，\text{当 } n \text{ 为奇数时。}$$

4.3.4　循环对称布尔函数对快速代数攻击的免疫程度

在这一小节，我们将考察当 $n=2^m t$ 且 $e=2^m$ 时矩阵 $S(f;e,n-e-1)$ 的性质。我们将说明这一类矩阵在很多情形下是奇异的，证明了当 n 为偶数且$n\neq 2^m$时，n元循环对称布尔函数都不具有最优的快速代数攻击性。

定理 4.12. *设 $n=2^m t$，t 是奇数，且 $f\in\mathbf{RSB}_n$。如果 $f_{\mathbf{1}_n}=1$ 或 $f_{\eta_t}=0$，那么存在次数不超过 2^m 的非零的循环对称布尔函数 g 使得 gf 的次数至多不超过 $n-2^m-1$。*

证明. 考虑 $|\Gamma_{2^m}(n)|\times|\Gamma_{2^m}(n)|$ 阶矩阵 $S(f;2^m,n-2^m-1)$。应用命题4.10，矩阵 $S(f;2^m,n-2^m-1)$ 的第 $\mathbf{1}_n$ 行是

$$(f_{\mathbf{1}_n},0,\ldots,0,f_{\mathbf{1}_n}\oplus f_{\eta_t},0,\ldots,0),$$

且根据命题4.11，矩阵 $S(f;2^m,n-2^m-1)$ 的第 η_t 行是

$$(f_{\eta_t},0,\ldots,0)。$$

当 $f_{\mathbf{1}_n}=1$ 或者 $f_{\eta_t}=0$ 时，这两行是线性相关的。因此，根据定理4.4，易得结论。 □

定理4.12说明，当 $n \neq 2^m$ 时，满足 $f_{\mathbf{1}_n} = 1$ 的 n 元循环对称布尔函数 f 不具有最优快速代数免疫性(因为$e = 2^m = n/t \leq n/3 < n/2$)。特别的，当 n为奇数，$f \in \mathbf{RSB}_n$ 且 $\deg(f) = n$时，令定理4.12中的 $m = 0$，则存在非零仿射循环对称布尔函数 g 使得 gf 的次数不超过 $n-2$。进一步的，根据例4.2，我们可以得到

$$S(f;1,n-2) = \begin{pmatrix} 1 & 1 \oplus f_{\eta_n} \\ f_{\eta_n} & 0 \end{pmatrix},$$

且由此可以得到 $g(x) = 1 + f_{\eta_n} + x_1 + x_2 + \cdots + x_n$。

定理 4.13. *设 $n = 2^m t$，t 为偶数，且 $f \in \mathbf{RSB}_n$。如果 $f_{\mathbf{1}_n} = 0$ 或 $f_{\eta_t} = f_{\eta_{\frac{t}{2}}}$，那么存在次数不超过 2^m 的非零的循环对称布尔函数 g 使得 gf 的次数至多不超过 $n - 2^m - 1$。*

证明. 考虑矩阵 $S(f;2^m, n-2^m-1)$。根据命题4.10，$S(f;2^m, n-2^m-1)$ 的第 $\mathbf{1}_n$ 行是

$$(f_{\mathbf{1}_n}, 0, \ldots, 0),$$

根据命题4.11，$S(f;2^m, n-2^m-1)$ 的第 η_t 行是

$$(f_{\eta_t}, 0, \ldots, 0, f_{\eta_t} \oplus f_{\eta_{\frac{t}{2}}}, 0, \ldots, 0)。$$

如果 $f_{\mathbf{1}_n} = 0$ 或者 $f_{\eta_t} = f_{\eta_{\frac{t}{2}}}$，那么这两行是线性相关的。因此，根据定理4.4，可以得到该定理。 □

定理4.13说明当 $f_{\mathbf{1}_n} = 0$ 且 n 为偶数时时，n 元循环对称布尔函数 f 不具有最优快速代数免疫性。特别的，当 $f \in \mathbf{RSB}_n$，n 为偶数且 $\deg(f) < n$，令定理4.13中的$m = 0$，则存在非零仿射循环对称布尔函数 g 使得 gf 的次数不超过 $n-2$。进一步的，根据例4.2，我们可以得到

$$S(f;1,n-2) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \oplus f_{\eta_{\frac{n}{2}}} \end{pmatrix},$$

且由此可以得到 $g(x) = 1 + f_{\eta_{\frac{n}{2}}} + x_1 + x_2 + \cdots + x_n$。

对于 $f \in \mathbf{RSB}_n$，我们可以轻易地根据定理获得 g 的代数标准型。运用这些 $(e,d) = (1, n-2)$ 我们关于循环对称布尔函数的算法比文献[2, 32]的算法效率更高。

定理 4.14. *设 $n = 2^m t$，$m \geq 1$，t 是偶数，且 $f \in \mathbf{RSB}_n$。那么存在整数 $e \leq 2^m$ 和次数不超过 e 的非零循环对称布尔函数 g 使得 gf 的次数不超过 $n - e - 1$。*

证明. 如果 $f_{\mathbf{1}_n} = 1$，那么结论可以通过定理 4.12所得到；否则，结论可以通过定理4.13所得到。 □

4.4　本章小结

在这一节，我们运用了矩阵的手段，给出了一个计算循环对称布尔函数快速代数免疫性的优化概率算法，而且说明其正确率接近于 1；并且我们通过分析算法系数矩阵的特殊性质，发现好几类循环对称布尔函数是不具有最优的快速代数免疫性。

在下一节，我们将基于这些结果和方法，进一步对更一般布尔函数的快速代数免疫性进行研究。

第五章　完全代数免疫函数

在上一章，我们提到了，具有最优代数免疫度的布尔函数未必具有最优的快速代数免疫[2]，很多研究结果也发现，许多具有最优代数免疫度的的布尔函数可能对快速代数攻击的抵抗能力很低，例如文献[2, 8]就给出了一些实例，而对于布尔函数的最优快速代数免疫性一直没有定论。

上一章，我们具体研究了循环对称布尔函数的快速代数免疫性，发现许多循环对称布尔函数都不具有最优的快速代数免疫性。而在这一章，我们将尝试研究一般布尔函数的快速代数免疫度，并探寻具有最优快速代数免疫性的布尔函数的存在性。

5.1　完全代数免疫度

假设对于布尔函数 f，如果存在一个低次布尔函数 g，满足 $h = gf$ 不是特别高，那么快速代数攻击对于该函数就是有效的。那么布尔函数 f 对快速代数攻击的免疫性就与 g 的次数 e 和 h 的次数 d 相关且满足 $e < d$。如定理4.2，则对于任意的 n 元布尔函数 f 和整数 e 满足 $e < \frac{n}{2}$，存在次数不超过 e 的 g 使得 gf 的次数不超过 $n - e$。在这一节，我们将引入完全代数免疫度的概念，满足这种性质的布尔函数将对所有代数攻击均有良好的免疫性质，并且代数次数至少为 $n - 1$，因为对于一个次数小于等于 $n - 1$ 的布尔函数，总是有可行对 (e, d) 满足 $e = 1$ 且 $d = \deg(f) \leq n - 2$，即 $e + d < n$。

定义 5.1. 设 f 是一个 n 元布尔函数。如果对任意的正整数 $e < n/2$ 和代数次数不超过 e 的布尔函数 g，都有gf 的代数次数不小于 $n - e$，那么布尔函数 f 被称为完全代数免疫的($\mathcal{PAI}$)。

命题 5.1. *设 f 是一个 n 元 $\mathcal{PAI}$ 布尔函数，那么 f 具有最优的代数免疫度，即 $AI(f) = \lceil n/2 \rceil$。*

证明. 运用反证法。

假设存在布尔函数 g，$deg(g) < \lceil n/2 \rceil$ 使得 $fg = 0$，那么

$$f(g \oplus 1) = fg \oplus g = g,$$

其中

$$deg(g) + deg(g \oplus 1) = 2deg(g) \leq 2\lceil n/2 \rceil < n。$$

假设存在布尔函数 h，$deg(h) < \lceil n/2 \rceil$ 使得 $(f \oplus 1)h = 0$，那么$fh = h$, 其中

$$deg(h) + deg(h) \leq 2\lceil n/2 \rceil < n。$$

即 f 不是一个 $\mathcal{PAI}$ 布尔函数。 □

因此，$\mathcal{PAI}$ 布尔函数即可以抵抗快速代数攻击，有具有最优代数免疫度。

5.2 一般布尔多项式的完全代数免疫性

寻找 $\mathcal{PAI}$ 布尔函数，关键是对于布尔函数 f 研究符合条件的 g 是否存在。

首先，我们设有序集合

$$\mathcal{W}_e = \{x \in \mathbb{F}_2^n | wt(x) \leq e\}$$

遵循字典序；集合

$$\overline{\mathcal{W}}_e = \{x \in \mathbb{F}_2^n | wt(x) \geq e+1\}$$

遵循反字典序。

重新回顾一下定理4.3

定理 5.2. *[2, 32]* 设 $f \in \mathbf{B}_n$ 且代数标准型为 $\bigoplus_{c \in F_2^n} f_c x^c$。定义矩阵 $M(f;e,d)$ 的 (i,j) 元素为 $\bigoplus_{c \cup z = y} f_c$，其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素。那么不存在次数不大于 e 的 g 使得 gf 的次数不大于 d 当且仅当矩阵 $M(f;e,d)$ 是列满秩的。

接下来我们将研究矩阵 $M(f;e,d)$ 的特殊性质，探寻一般函数对于快速代数攻击的免疫性。

5.2.1 $M(f;e,d)$ 的性质

容易得到，$M(f;e,d)$ 是一个

$$\sum_{i=d+1}^{n} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$$

阶的矩阵，其 (i,j) 元素为

$$m_{yz} = \bigoplus_{c \cup z = y} f_c = \bigoplus_{\substack{y \cap \bar{z} \subset c \subset y \\ z \subset y}} f_c = y^z \bigoplus_{y \cap \bar{z} \subset c \subset y} f_c \tag{5.1}$$

其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素。

考虑矩阵的列变换 $\bigoplus_{z^* \subset z} m_{yz^*}$，我们有如下定理：

引理 5.3. $\bigoplus_{z^* \subset z} m_{yz^*} = f_{y \cap \bar{z}}$。

证明. 由于 $c\cup z=y$ 当且仅当 $c\subset y, z\subset y$ 以及 $y\subset c\cup z$，也就是说，$y^c=1, y^z=1$ 且 $(c\cup z)^y=1$，我们有

$$\begin{aligned}\bigoplus_{z^*\subset z} m_{yz^*} &= \bigoplus_{z^*\subset z}\bigoplus_{c\cup z^*=y} f_c\\ &= \bigoplus_{z^*\subset z}\bigoplus_{c} y^c y^{z^*}(c\cup z^*)^y f_c\\ &= \bigoplus_{c} y^c f_c \bigoplus_{z^*\subset z} y^{z^*}(c\cup z^*)^y\\ &= \bigoplus_{c\subset y} f_c \bigoplus_{\substack{z^*\subset z\cap y\\ y\subset c\cup z^*}} 1\\ &= \bigoplus_{c\subset y} f_c \bigoplus_{y\cap\bar{c}\subset z^*\subset z\cap y} 1\\ &= \bigoplus_{c\subset y, c=y\cap\bar{z}} f_c\\ &= f_{y\cap\bar{z}}。\end{aligned}$$

□

根据引理5.3，我们可以对 $M(f;e,d)$ 进行相应的列变换从而使得其变为一个 (i,j) 元素为

$$w_{yz}=f_{y\cap\bar{z}}$$

的新矩阵，其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素。记这个新矩阵为 $W(f;e,d)$。

矩阵 $W(f;e,d)$ 的 (j,i) 元素就满足

$$w_{\bar{z}\bar{y}}=f_{\bar{z}\cap\bar{\bar{y}}}=f_{y\cap\bar{z}},$$

其中 $\bar{z}$ 是 $\overline{\mathcal{W}}_d$ 的第 j 个元素，$\bar{y}$ 是 $\mathcal{W}_e$ 的第 i 个元素，即矩阵 $W(f;e,d)$ 是一个对称矩阵。而且

$$w_{z\bar{z}}=f_{z\cap\bar{\bar{z}}}=f_z=w_{z0_n}=w^2_{z0_n}。$$

特别的，当

$$\sum_{i=d+1}^{n}\binom{n}{i}=\sum_{i=0}^{e}\binom{n}{i}$$

时，矩阵 $W(f;e,d)$ 是一个对称矩阵，记作 $W(f;e)$。由于矩阵 $W(f;e,d)$ 是由矩阵 $M(f;e,d)$ 进行相应的列变换得到的，因此其秩不变；因此，根据定理4.3我们可以得到如下定理：

定理 5.4. 设 $f \in \mathbf{B}_n$ 且代数标准型为 $\bigoplus_{c\in F_2^n} f_c x^c$。定义矩阵 $W(f;e,d)$ 的 (i,j) 元素为 $f_{y\cap z}$，其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素。那么不存在次数不大于 e 的 g 使得 gf 的次数不大于 d 当且仅当矩阵 $W(f;e,d)$ 是列满秩的。

下面的一个引理给出了形如矩阵 $W(f;e)$ 的对称矩阵的性质：

引理 5.5. *[*]* 设 A 是一个在特征为 2 的域 K 上生成的 $m\times m$ 阶对称矩阵，即 A 具有形式

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\ a_{12} & a_{12}^2 & a_{23} & \cdots & a_{2m} \\ a_{13} & a_{23} & a_{13}^2 & \cdots & a_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & a_{3m} & \cdots & a_{1m}^2 \end{pmatrix}。 \tag{5.2}$$

那么如果

$$a_{11} = (m+1) \mod 2,$$

那么我们有$\det(A)=0$。

注 2. 证明详见刘美成博士的毕业论文。

设 $A^{(i,j)}$ 是由矩阵 A 移除第 i 行和第 j 列所生成的一个 $(m-1)\times(m-1)$ 阶的矩阵。根据上述引理，我们可以得到当 $a_{11}=m \mod 2$ 时，$\det(A)=\det(A^{(1,1)})$。

5.2.2 布尔函数具有完全代数免疫度的必要条件

这一小节我们来考虑具有完全代数免疫度的布尔函数的性质。如果布尔函数 f 具有了完全代数免疫度，也就是说，对于任意的正整数对 (e,d) 满足 $e+d\le n-1$ 且 $e<\lceil\frac{n}{2}\rceil<d$，不存在次数不超过 e 的非零布尔函数 g 使得 $deg(gf)\le d$。具体到矩阵，就是说对于任意的 $e<\lceil\frac{n}{2}\rceil$，都有矩阵 $W(f;e)$ 是可逆的。所以布尔函数是否是完全代数免疫的，与矩阵 $W(f;e)$ 的奇异性具有着直接的联系。

我们先来考虑具有快速代数免疫性布尔函数的存在性问题。

引理 5.6. *[53]* 设 $f\in\mathbf{B}_n$，$\mathrm{wt}(f)=\sum_{i=0}^{e}\binom{n}{i}$ 且 $1\le e<n/2$。那么布尔多项式 f 没有次数小于等于 e 的零化子当且仅当 $f+1$ 没有次数小于等于 $n-e-1$ 的零化子。

命题 5.7. *[53]* 设整数 n 和 e 满足 $1\le e<n/2$，那么存在一个 n 元布尔函数 f 使得 $W(f;e)$ 是可逆的。

定理 5.8. 设 $f \in \mathbf{B}_n$ 且 f_{2^n-1} 是 f 代数标准型中单项式 $x_1x_2\cdots x_n$ 的系数。设 e 是不超过 $\frac{n}{2}$ 的一个整数。如果

$$f_{2^n-1} = \binom{n-1}{e} + 1 \mod 2,$$

那么存在次数不超过 e 的非零布尔函数 g 使得 gf 的次数不超过 $n-e-1$。

证明. 为证明该定理，我们只需要证明当

$$f_{2^n-1} = \binom{n-1}{e} + 1 \mod 2$$

时，方阵 $W(f;e)$ 是奇异的。设 $W = W(f;e)$。因为 $\mathbf{1} = (1,1,\cdots,1)$ 和 $\mathbf{0} = (0,0,\cdots,0)$ 分别是矩阵 $\overline{\mathcal{W}}_{n-e-1}$ 和 $\mathcal{W}_e$ 按既有顺序的第一个元素，根据 $W(f;e)$ 的定义，我们可以得到

$$W_{11} = w_{\mathbf{1},\mathbf{0}} = f_{2^n-1}。$$

因为

$$\sum_{i=0}^{e}\binom{n}{i} = \sum_{i=1}^{e}\binom{n-1}{i} + \sum_{i=1}^{e}\binom{n-1}{i-1} + 1 \equiv \binom{n-1}{e} (\mod 2),$$

我们可以得到当

$$f_{2^n-1} = \binom{n-1}{e} + 1 \mod 2$$

时，有

$$W_{11} = \sum_{i=0}^{e}\binom{n}{i} + 1 \mod 2。$$

如前所述，$W(f;e)$ 是一个

$$\sum_{i=0}^{e}\binom{n}{i} \times \sum_{i=0}^{e}\binom{n}{i}$$

阶的对称矩阵。根据 $W(f;e)$ 的定义，我们可以得到

$$W_{1i}^2 = W_{1i} = w_{\mathbf{1}z} = f_{\mathbf{1}\cap\bar{z}} = f_{\bar{z}} = f_{\bar{z}\cap\bar{z}} = w_{\bar{z}z} = W_{ii}$$

，其中 $\bar{z}$ 是 $\overline{\mathcal{W}}_d$ 的第 j 个元素，$\bar{y}$ 是 $\mathcal{W}_e$ 的第 i 个元素。根据引理5.5，有$\det(M) = 0$。

□

推论 5.9. 设 n 为偶数且 $f \in \mathbf{B}_n$。如果 f 是平衡的，那么存在一个次数小于等于 1 的非零布尔函数 g 使得 gf 不超过 $n-2$。

证明. 如果 f 是平衡的，那么我们有 $f_{2^n-1} = 0$。当 n 为偶数时，我们有

$$\binom{n-1}{1} + 1 \equiv 0 (\mod 2)。$$

因此根据定理5.8，命题得证。 □

Lucas定理证明了对于整数 m 和 i，总是满足如下的关系：

$$\binom{m}{i} \equiv \prod_{k=0}^{s} \binom{m_k}{i_k} (\mod 2),$$

其中

$$m = \sum_{k=0}^{s} m_k 2^k \text{ 和 } i = \sum_{k=0}^{s} i_k 2^k$$

反别是 m 和 i 的二进制表示。该定理说明了 $\binom{n-1}{e} \mod 2 = 1$ 当且仅当 $e \subset n-1$。

注意到 $f_{2^n-1} = 1$ 当且仅当 $\deg(f) = n$。定理5.8说明对于一个 n 元布尔函数 f 来说，如果 $deg(f) = n$ 且 $e \subset n-1$，那么存在次数不超过 e 的非零布尔函数 g 使得 gf 的次数不超过 $n-e-1$；如果 $deg(f) < n$ 且 $e \not\subset n-1$，那么存在次数不超过 e 的非零布尔函数 g 使得 gf 的次数不超过 $n-e-1$。

当 $n-1 \notin \{2^m, 2^m-1\}$ 时，存在整数 e, e^* 且 $0 < e, e^* < n/2$ 使得 $e \subset n-1$ $e^* \not\subset n-1$，因此 n 元布尔函数 f 不是 PAI 的；也就是说只有当变元数 n 满足 $n = 2^m$ 或者 $n = 2^m+1$时，f 才是 PAI 的。当 $n-1 = 2^m$ (或者 2^m-1)时，对整数 $e < n/2$ 可以得到 $e \not\subset n-1$ (或者 $e \subset n-1$)，因此一个 n 元布尔函数如果代数次数等于 n (或者小于等于 n)，那么 f 不是PAI的。

考虑到具有最优代数免疫度的奇变元布尔函数总是平衡的[52]，则如果 $n = 2^m+1$，那么一个完全代数免疫函数的次数为 $n-1$ 且总是平衡的；则如果 $n = 2^m$，那么一个完全代数免疫函数的次数为 n 且总是不平衡的。

综上所述，我们可以得到如下的定理：

定理 5.10. 设 $f \in \mathbf{B}_n$ 且 m 是一个大于等于 2 的正整数。如果 f 是一个完全代数免疫函数，那么 $n = 2^m$ 或者 $n = 2^m+1$。进一步的，如果 f 是一个平衡的完全代数免疫函数，那么 $n = 2^m+1$；如果 f 是一个不平衡的完全代数免疫函数，那么 $n = 2^m$。

5.3 单变元表示布尔函数的完全代数免疫度

在这一节，我们将主要研究单变元表示布尔函数的完全代数免疫性，并且给出了Carlet-Feng函数所能达到的快速代数免疫性的界限。

5.3.1 具有完全代数免疫度的单变元表示布尔函数的判定

我们继续设有序集合

$$\mathcal{W}_e = \{x \in \mathbb{F}_2^n | wt(x) \leq e\}$$

遵循字典序；集合

$$\overline{\mathcal{W}}_e = \{x \in \mathbb{F}_2^n | wt(x) \geq e+1\}$$

遵循反字典序。元素

$$z=(z_1,z_2,\cdots,z_n)\in \mathcal{W}_e或者\overline{\mathcal{W}}_d$$

就要看成是整数

$$z_1+z_2 2+\cdots+z_n 2^{n-1}\in[0,2^n-1]。$$

设代数次数不超过 e $(e<\frac{n}{2})$的布尔函数 g 满足 $h=gf$的次数至多不超过 $d(d>\frac{n}{2})$。记

$$f(x)=\sum_{k=0}^{2^n-1} f_k x^k,\ f_k\in\mathbb{F}_{2^n},$$

$$g(x)=\sum_{z\in\mathcal{W}_e} g_z x^z,\ g_z\in\mathbb{F}_{2^n},$$

和

$$h(x)=\sum_{y\in\mathcal{W}_d} h_y x^y,\ h_y\in\mathbb{F}_{2^n}$$

分别是布尔函数 f，g 和 h 的单变元表示形式。设 $y\in\overline{\mathcal{W}}_d$，我们有 $h_y=0$ 且

$$0=h_y=\sum_{\substack{k+z=y\\ z\in\mathcal{W}_e}} f_k g_z=\sum_{z\in\mathcal{W}_e} f_{y-z}g_z。\tag{5.3}$$

上面的方程组如果看做关于变元 g_z 的方程组将是齐次线性的，将这个方程组的系数矩阵记作

$$\sum_{i=0}^{n-d-1}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$$

阶的矩阵 $U(f;e,d)$。其(i,j)元为

$$u_{yz}=f_{y-z}。\tag{5.4}$$

其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素。那么我们可以得到如下定理：

定理 5.11. *设 $f\in\mathbf{B}_n$ 且代数标准型为 $\sum_{i=0}^{2^n-1} f_i x^i$。定义矩阵 $U(f;e,d)$ 的 (i,j) 元素为 f_{y-z}，其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素。那么不存在次数不大于 e 的非零布尔多项式 g 使得 gf 的次数不大于 d 当且仅当矩阵 $U(f;e,d)$ 是列满秩的。*

证明. $\Longleftarrow$:

如果矩阵 $U(f;e,d)$ 是列满秩的，那么可以得到方程组5.3只有零解，即不存在次数不大于 e 的非零布尔多项式 g 使得 gf 的次数不大于 d。

$\Longrightarrow$: $(*)$ 如果矩阵 $U(f;e,d)$ 不是是列满秩的，那么总可以得到方程组5.3的一个非零解。不失一般性，设非零多项式

$$g(x)=\sum_{\mathcal{W}_e} g_z x^z,\ g_z\in F_{2^n}$$

满足方程组5.3，则我们可以得到

$$0 = h_y^2 = \sum_{\mathcal{W}_e} g_z^2 f_{y-z}^2 = \sum_{\mathcal{W}_e} g_z^2 f_{2y-2z}, y \in \overline{\mathcal{W}_d}, \tag{5.5}$$

其中 $f_{2(2^n-1)} = f_{2^n-1}$ 且

$$f_{2i} = f_{2i \mod (2^n-1)}, \ i \neq 2^n - 1,$$

由此我们可以得到

$$g^2(x) = \sum_{z \in \mathcal{W}_e} g_z^2 x^{2z} \mod (x^{2^n} - x)$$

满足方程5.5。注意到多项式组5.3和5.5其实是一样的，即如果 $g(x)$ 满足方程组5.3，那么 $Tr(g(x))$ 也满足方程组5.3，其中

$$Tr(x) = x + x^2 + \cdots + x^{2^{n-1}}。$$

也就是说，对任意的 $\beta \in F_{2^n}$，如果 $g(x)$ 满足方程组5.3，那么 $\beta g(x)$ 和 $Tr(\beta g(x))$ 也满足方程组5.3。因为 $g(x)$ 非零，那么存在 $c \in F_{2^n}$ 使得 $g(c) \neq 0$，即 $Tr(\beta g(c)) \neq 0$。也就是说 $Tr(\beta g(x))$ 是一个非零多项式。因此如果存在方程组5.3的一个非零解，那么一定存在一个非零布尔多项式 $g(x)$ 满足该方程组。

命题得证。 □

注 3. 该定理必要性的证明是由刘美成博士完成的，但是为了保证文章的完整性，这里引用了这一证明。

注 4. 矩阵 $U(f; e, n-e-1)$，记作 $U(f; e)$，是一个对称矩阵。因为

$$u_{\bar{z}\bar{y}} = f_{\bar{z}-\bar{y}} = f_{(2^n-1-z)-(2^n-1-y)} = f_{y-z} = u_{yz}。$$

进一步的，我们有

$$u_{y\bar{y}} = f_{y-\bar{y}} = f_{y-(2^n-1-y)} = f_{2y} = f_y^2 = u_{y1}^2,$$

因此 $U(f; e)$ 具有形式5.2。

这个定理利用一个矩阵就给出了计算单变元表示布尔函数对快速代数攻击免疫性的充要条件，相比之下，文献[73]用了三个矩阵来完成类似的工作，显然要复杂得多。而且，根据该矩阵的特殊结构，我们将在下一小节基于该算法研究Carlet-Feng函数的快速代数免疫性。

5.3.2 Carlet-Feng函数的完全代数免疫度

首先我们来介绍一下C. Carlet和冯克勤老师在文献[12]所构造的具有最优代数免疫度的一类单变元表示的布尔函数————Carlet-Feng函数。这类函数具有最优代数免疫度和较高的非线性度，并且根据计算机验证，其对于快速代数攻击也具有良好的抵抗程度。

定义 5.2. [12] 设 n 是一个整数且 α 是 $\mathbb{F}_{2^n}$ 上的一个本原元。定义函数 $f \in \mathbf{B}_n$ 且满足

$$supp(f) = \{\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+2^{n-1}-1}\}, 0 \le l \le 2^n - 2, \tag{5.6}$$

的函数为Carlet-Feng函数。

对于一个Carlet-Feng函数 f，根据文献[12]可以得到 $AI(f) = \lceil \frac{n}{2} \rceil$ 且

$$nlf \ge 2^{n-1} - \frac{2^{\frac{n}{2}+m}}{\pi} ln(\frac{4(2^n-1)}{\pi}) - 1 \sim 2^{n-1} - \frac{ln2}{\pi} 2^{\frac{n}{2}+m} \cdot n。$$

对于Carlet-Feng函数的代数标准型有以下定理，这里我们给出证明从而方便之后进一步的研究。

命题 5.12. *[12]* 设

$$f(x) = \sum_{i=0}^{2^n-1} f_i x^i (f_i \in \mathbb{F}_{2^n})$$

是一个单变元表示的*Carlet-Feng*函数。那么 $f_0 = 0$，$f_{2^n-1} = 0$，并且当 $1 \le i \le 2^n - 2$ 时，

$$f_i = \frac{\alpha^{-il}}{1 + \alpha^{-i/2}}。$$

因此 f 的代数次数为 $n-1$。

注 5. 设 f 为一个Carlet-Feng函数，那么矩阵 $U(f; e, d)$ $(e \le d)$的 (i, j) 元为：

$$u_{yz} = f_{y-z} = \frac{\alpha^{-yl}\alpha^{zl}}{1 + \alpha^{-y/2}\alpha^{z/2}}, (i, j) \ne (1, 1),$$

其中 y 是 $\overline{\mathcal{W}}_d$ 的第 i 个元素，z 是 $\mathcal{W}_e$ 的第 j 个元素，容易得到当 $(i, j) \ne (1, 1)$ 且 $e \le d$ 时，$y - z \notin \{0, 2^n - 1\}$。

考虑当 $d = n - e - 1$ 时，f 的矩阵 $U(f; e, d)$ 所具有的特殊性质：

引理 5.13. *[*]* 设 A 是一个 $m \times m$ 阶的矩阵且其 (i, j) 元是特征为 2 的域 K 上的元素

$$a_{ij} = (1 + \beta_i \gamma_j)^{-1},$$

其中 $\beta_i, \gamma_j \in K$ 且 $\beta_i\gamma_j \neq 1$，其中 $1 \leq i, j \leq m$。那么 A 的行列式值为

$$\prod_{1\leq i<j\leq m}(\beta_i+\beta_j)(\gamma_i+\gamma_j)\prod_{1\leq i,j\leq m}a_{ij}。$$

进一步的，如果当 $i \neq j$ 时，$\beta_i \neq \beta_j$ 且 $\gamma_i \neq \gamma_j$，那么 A 所有的主子矩阵行列式值都不为 0。

引理 5.14. *[*]* 设 $A = (a_{ij})_{m\times m}$ 和 $B = (b_{ij})_{m\times m}$ 是 $m \times m$ 阶的矩阵，其中 $a_{ij} = \beta_i\gamma_j b_{ij}$ 且 $\beta_i\gamma_j \neq 0$ 当 $1 \leq i, j \leq m$。那么 $\det(A) \neq 0$ 当且仅当 $\det(B) \neq 0$。

注 6. 上述引理的证明详见刘美成博士的毕业论文。

运用上述引理，我们就可以证明 $2^m + 1$ 元的 Carlet-Feng函数是一个完全代数免疫函数。

命题 5.15. 设 $e < \frac{n}{2}$ 且 f 是*Carlet-Feng*函数。当 $e \not\subset n-1$ 时，$U(f;e)$ 是可逆的；当 $e \subset n-1$ 时，$U(f;e,n-e-2)$ 是列满秩的。

证明. 记 $U = U(f;e)$，可以得到 $U_{11} = f_{2^n-1} = 0$。注意到 U 是一个阶为 $\sum_{i=0}^{e}\binom{n}{i}$ 的对称矩阵。

当 $e \not\subset n-1$ 时，根据Lucas定理我们可以得到 $\binom{n-1}{e} \mod 2 = 0$ 并且因此

$$\sum_{i=0}^{e}\binom{n}{i} \mod 2 = U_{11}。$$

根据引理 5.5，有 $\det(U) = \det(U^{(1,1)})$。注5说明矩阵 $U^{(1,1)}$ 的 (i,j) 元是

$$U_{ij}^{(1,1)} = \frac{\alpha^{-yl}\alpha^{zl}}{1+\alpha^{-y/2}\alpha^{z/2}},$$

其中 y 是 $\overline{W}_d$ 的第 $i+1$ 个元素，z 是 $\mathcal{W}_e$ 的第 $j+1$ 个元素。设 U^* 是一个

$$(\sum_{i=0}^{e}\binom{n}{i}-1)\times(\sum_{i=0}^{e}\binom{n}{i}-1)$$

阶的矩阵满足其 (i,j) 元是

$$U_{ij}^{*} = \frac{1}{1+\alpha^{-y/2}\alpha^{z/2}}。$$

根据引理5.14，我们可以得到，如果 $\det(U^*) \neq 0$，那么 $\det(U^{(1,1)}) \neq 0$。根据引理L5.13，我们可以得到 $\det(U^*) \neq 0$，因此 $U(f;e)$ 是可逆的。

当 $e \subset n-1$ 时，矩阵 $U(f;e,n-e-2)$ 是一个

$$\sum_{i=0}^{e+1}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$$

阶的矩阵。设 U^{**} 是一个

$$\sum_{i=0}^{e}\binom{n}{i}\times\sum_{i=0}^{e}\binom{n}{i}$$

阶的矩阵，是由矩阵 $U(f;e,n-e-2)$ 去掉了前 $\binom{n}{e+1}$ 行后生成的。根据引理5.14，我们可以得到，如果 $\det(U^{**})\neq 0$，那么 $\det(U^{(1,1)})\neq 0$。所以在这种情况下，矩阵$U(f;e,n-e-2)$ 是列满秩的。

综上，命题得证。 □

从上面的引理我们可以得到：

定理 5.16. *设 e 是小于 $\frac{n}{2}$ 的正整数，f 是Carlet-Feng函数。如果*

$$\binom{n-1}{e}\equiv 0(\mod 2),$$

那么不存在次数不大于 e 的非零布尔多项式 g 使得 gf 的次数不大于 $n-e-1$；如果

$$\binom{n-1}{e}\equiv 1(\mod 2),$$

那么不存在次数不大于 e 的非零布尔多项式 g 使得 gf 的次数不大于 $n-e-2$。

推论 5.17. *设 $n=2^m+1$ 且 f 是 n 元Carlet-Feng函数。那么 f 是完全代数免疫函数。*

证明. 因为当 $1\leq e<\frac{n}{2}$ 时，

$$\binom{n-1}{e}=\binom{2^m}{e}\equiv 0(\mod 2)。$$

所以根据定理5.16，我们可以知道 f 是 PAI 的。 □

定理5.16说明Carlet-Feng函数具有最优的抵抗快速代数免疫度的能力，同时也说明了我们在之前所给定的关于布尔函数对于快速代数攻击抵抗程度的界是紧的；同时，推论5.17说明 2^m+1 元的Carlet-Feng函数是完全代数免疫的布尔函数。这些结果证明了文献[12]中所提出的猜想，并且与文献[12, 32]中的实验结果相一致。

5.3.3　移位Carlet-Feng函数的完全代数免疫度

下面我们将讨论一类代数次数为 n 的布尔函数的快速代数免疫性。

定义 5.3. *设 n 是一个整数且 α 是 $\mathbb{F}_{2^n}$ 上的一个本原元。定义函数 $f\in\mathbf{B}_n$ 且满足*

$$supp(f)=\{0,\alpha^l,\alpha^{l+1},\cdots,\alpha^{l+2^{n-1}-1}\},0\leq l\leq 2^n-2, \tag{5.7}$$

的函数为移位Carlet-Feng函数。

运用和命题5.12类似的证明方法，我们可以得到该函数的代数标准型的具体形式：

命题 5.18. 设

$$f(x)=\sum_{i=0}^{2^n-1} f_i x^i (f_i \in \mathbb{F}_{2^n})$$

是一个单变元表示的移位*Carlet-Feng*函数。那么 $f_0=1$，$f_{2^n-1}=1$，并且当 $1\leq i\leq 2^n-2$ 时，

$$f_i=\frac{\alpha^{-il}}{1+\alpha^{-i/2}}。$$

因此 f 的代数次数为 $n-1$。

同样的，我们可以得到移位Carlet-Feng函数快速代数免疫性的一般性质。

命题 5.19. 设 $e<\frac{n}{2}$ 且 f 是移位*Carlet-Feng*函数。当

$$\binom{n-1}{e}\equiv 1(\mod 2)$$

时，$U(f;e)$ 是可逆的；当

$$\binom{n-1}{e}\equiv 0(\mod 2)$$

时，$U(f;e,n-e-2)$ 是列满秩的。

定理 5.20. 设 e 是小于 $\frac{n}{2}$ 的正整数，f 是移位*Carlet-Feng*函数。如果

$$\binom{n-1}{e}\equiv 1(\mod 2)$$

，那么不存在次数不大于 e 的非零布尔多项式 g 使得 gf 的次数不大于 $n-e-1$；如果

$$\binom{n-1}{e}\equiv 0(\mod 2)$$

，那么不存在次数不大于 e 的非零布尔多项式 g 使得 gf 的次数不大于 $n-e-2$。

推论 5.21. 设 $n=2^m$ 且 f 是 n 元移位*Carlet-Feng*函数。那么 f 是完全代数免疫函数。

证明. 因为当 $1\leq e<\frac{n}{2}$ 时，

$$\binom{n-1}{e}=\binom{2^m-1}{e}\equiv 1(\mod 2)。$$

所以根据定理5.16，我们可以知道 f 是 PAI 的。 □

定理5.20说明移位Carlet-Feng函数也具有最优的抵抗快速代数免疫度的能力，同时也说明了我们在之前所给定的关于布尔函数对于快速代数攻击抵抗程度的界是紧的；同时，推论5.17说明 2^m 元的移位Carlet-Feng函数是完全代数免疫的布尔函数。

5.4　本章小结

在这一节，我们解决了关于布尔函数快速代数免疫性的一些公开问题。我们证明了最优快速代数免疫性的上界，并且证明了Carlet-Feng函数达到了这个上界，具有最优的快速代数免疫性。我们还发现，如果要寻找具有好的密码学性质的函数，$n=2^m+1$ 元的 $n-1$ 次布尔函数可能是一个很好的选择。其中，$n=2^m+1$ 元的 $n-1$ 次Carlet-Feng函数具有最优的代数免疫度，较高的非线性度，是平衡函数且具有最优的快速代数免疫性，是一个完全代数免疫函数。这也是第一次有一类布尔函数被证明具有最优的快速代数免疫度。

第六章　离散傅里叶谱攻击相关研究

离散傅里叶谱攻击是一类对基于线性移位寄存器和非线性过滤函数的密码系统的特殊的代数攻击。这种攻击在进行预计算后只需求解一组线性方程组就可以恢复初始密钥。其攻击复杂度则与相应的滤波生成器序列的线性复杂度相关。本章我们将介绍离散傅里叶谱攻击及其扩展算法并对其进行简单的分析，同时我们也介绍滤波生成器序列线性复杂度的相关研究进展并提出了布尔函数的谱免疫度概念。

6.1　离散傅里叶谱攻击简介

6.1.1　离散傅里叶谱攻击原理

考虑如下图所示的基于线性移位寄存器和高度非线性的布尔函数的无记忆的流密码体制。

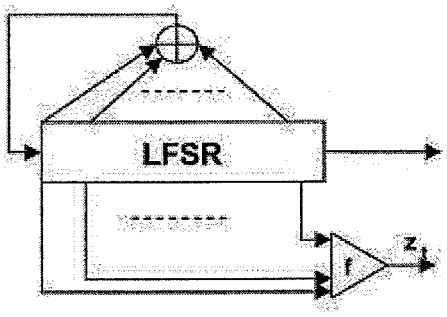

图 6.1: 基于线性移位寄存器的流密码体制

为了简单起见，下面只考虑$q=2$的情形。

如上所述，

$$z_t = f(s_t, s_{t+n}, \ldots, s_{t+n-1}) = f_t(s_0, s_1, \ldots, s_{n-1})。$$

以f是个单项式为例，由于$\{s_t\}$是m-序列，则

$$s_t = Tr_1^n(\beta\alpha^t) \quad t = 0, 1, 2, \ldots, \beta \in \mathbb{F}_{q^n}$$

将$\{s_t\}$带入上式，则：

$$\begin{aligned} z_t &= s_{t+\delta_1}s_{t+\delta_2}\cdots s_{t+\delta_k} \\ &= [\sum_{v_1=0}^{n-1}(\beta\alpha^{\delta_1+t})^{2^{v_1}}][\sum_{v_2=0}^{n-1}(\beta\alpha^{\delta_2+t})^{2^{v_2}}]\ldots[\sum_{v_k=0}^{n-1}(\beta\alpha^{\delta_k+t})^{2^{v_k}}] \\ &= \sum_{v_1,v_2,\ldots,v_k}\alpha^{\delta_1 2^{v_1}+\delta_2 2^{v_2}+\ldots+\delta_k 2^{v_k}}(\beta\alpha^t)^{2^{v_1}+2^{v_2}+\ldots+2^{v_k}} \\ &= \sum_{wt(v)\le k}A_{|v|}(\beta\alpha^t)^{|v|} \end{aligned}$$

其中$|\boldsymbol{v}|$是$\boldsymbol{v}$的整数表示。所以$\{z_t\}$的谱序列$\{Z_t\}$满足$Z_t = A_t\beta^t$。

设α^k的极小多项式为$p_k(x)$，那么$p_k(\alpha^{2^i k}) = 0, (0 \le i \le n_k)$。设

$$p(x) = \prod_{j\in\Gamma(2^n-1)} p_j(x),$$

那么$p(\alpha^{2^i j}) = 0, (0 \le i \le n_j, j \in \Gamma(2^n-1))$。令

$$q_k(x) = p(x)/p_k(x) = \sum_{i=0}^{r} c_i a_{i+t},$$

则$q_k(\alpha^{2^i j}) = 0, (0 \le i \le n_j, j \in \Gamma(2^n-1), j \ne k)$。

由$z_t = \sum_{j=0}^{2^n-1} Z_j\alpha^{tj}$，令

$$\begin{aligned} v_t &= \sum_{i=0}^{r} c_i z_{i+t} \\ &= \sum_{i=0}^{r} c_i \sum_{j=0}^{2^n-1} Z_j\alpha^{(i+t)j} \\ &= \sum_{j=0}^{2^n-1} Z_j\alpha^{tj}\sum_{i=0}^{r} c_i\alpha^{ij} \\ &= \sum_{j=0}^{2^n-1} Z_j\alpha^{tj}q_k(\alpha^j) \\ &= \sum_{j=1}^{n_k} Z_{k2^{j-1}}\alpha^{tk2^{j-1}}q_k(\alpha^{k2^{j-1}}) \end{aligned}$$

将$Z_t = A_t\beta^t$带入，有

$$v_t = \sum_{j=1}^{n_k} A_{k2^{j-1}}\beta^{k2^{j-1}}\alpha^{tk2^{j-1}}q_k(\alpha^{k2^{j-1}})$$

取$t = 0, 1, \ldots, n_k - 1$就可以得到一组关于$\beta^{k2^{j-1}}, (1 \le j \le n_k)$的线性方程组。如果可以求解出$\beta$，那么就可以恢复出初始密钥$s_t$。

6.1.2　离散傅里叶谱攻击算法与实例

离散傅里叶谱攻击的的具体算法如下：

算法 6.1. *[77]*

基于线性移位寄存器和非线性布尔函数的无记忆的流密码体制，其中$\{s_t\}$是m-序列。

输入：反馈序列$(z_0, z_1, \ldots, z_{D-1})$，$D = LS(\boldsymbol{b})$

输出：初始密钥$(s_0, s_1, \ldots, s_{n-1})$

预计算部分:

1. 计算A_k，其中$k \in \Gamma(2^n - 1)$且$A_k \neq 0$。

2. 计算α^k的极小多项式$p_k(x)$和$p(x) = \prod_{k \in \Gamma(2^n-1), A_k \neq 0} p_k(x)$。

3. 计算$q(\alpha^k)$，其中

$$q(x) = p(x)/p_k(x) = \sum_{i=0}^{r} c_i x^i。$$

计算部分:

1. 计算$\{v_t\}$，$v_t = \sum_{i=0}^{r} c_i z_{i+t}$。

2. 解关于θ的方程

$$v_t = Tr_1^{n_k}(\theta \alpha^{tk}),\ t = 0, 1, \ldots, n_k - 1,\ \theta = A_k q(\alpha^k) \beta^k。$$

以上方程可以看作是关于n_k个变量

$$\{\theta^{2^i} | i = 0, 1, \ldots, n_k - 1\}$$

的$\mathbb{F}_{2^{n_k}}$上的线性方程组。

3. 反解出β或给出β^k的值并且换一个k继续求解。

4. 返回初始密钥$s_t = Tr_1^n(\beta \alpha^t)$。

容易看出这个方法需要$LS(z)$个连续的密文序列。

该算法可以求出初始密钥当且仅当下述条件之一成立：

(a) 存在这样的k，使得$gcd(k, 2^n - 1) = 1$且$A_k \neq 0$。

(b) 存在一组$k_1, k_2, \ldots, k_t$，使得$\sum_{i=0}^{t} a_i k_i (mod\ 2^n - 1)$与$2^n - 1$互素。

下面我们给出一个计算的简单例子。

例 6.1. 考虑m-序列$\{s_t\}$的生成多项式为$f(x)=x^4+x+1$，所以

$$s_t = Tr_1^n(\beta\alpha^t) \quad t=0,1,2,\ldots,\beta\in\mathbb{F}_{2^4}。$$

假设过滤多项式只是一个简单的单项式：

$$f(x_0,x_1,x_3)=x_0x_1x_3,$$

则生成反馈序列为

$$b_t = f_t(s_0,s_1,s_2,s_3)=s_ts_{t+1}s_{t+3}$$

这里假设$b_t=0001000010\ldots$。

模$2^4-1=15$的分圆陪集为:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1,2,4,8\} \\ C_3 &= \{3,6,9,12\} \\ C_5 &= \{5,10\} \\ C_7 &= \{7,11,13,14\} \end{aligned}$$

所以相关的$p_k(x)$如下：

$$\begin{aligned} p_1(x) &= \prod_{i\in C_1}(x+\alpha^i)=x^4+x+1 \\ p_3(x) &= \prod_{i\in C_3}(x+\alpha^i)=x^4+x^3+x^2+x+1 \\ p_5(x) &= \prod_{i\in C_5}(x+\alpha^i)=x^2+x+1 \\ p_7(x) &= \prod_{i\in C_7}(x+\alpha^i)=x^4+x^3+1 \end{aligned}$$

$$p(x)=p_1(x)p_3(x)p_4(x)p_7(x)=\frac{x^{15}+1}{x+1}$$

下面计算A_k，当$k=1$时，寻找所有的$\{v_0,v_1,v_2,v_3\}$使得

$$\sum_{i=0}^{3}2^{v_i}=1(mod15)。$$

所以$u=\{v_0,v_1,v_2,v_3\}$是$\{2,2,2,2\}$和$\{1,1,2,3\}$的任意排列，所以

$$A_1=\sum_{v}\alpha^{(2^{v_1}+3\cdot 2^{v_3})}=\alpha^{14}。$$

同理可得$A_3 = 0, A_5 = \alpha^{10}$和$A_7 = \alpha^8$。

由于A_1，A_5和A_7均不为零，所以

$$q_7(x) = p(x)/(p_3(x)p_7(x)) = x^6 + x^5 + x^4 + x^3 + 1。$$

由于$b_t = 0001000010\ldots$，

$$u_t = b_{t+6} + b_{t+5} + b_{t+4} + b_{t+3} + b_t$$

可以得到

$$\{u_0, u_1, u_2, u_3\} = \{1, 0, 1, 0\}。$$

求解方程组

$$\begin{cases} v_0 = 1 = Tr_1^4(\theta) \\ v_1 = 0 = Tr_1^4(\theta\alpha^7) \\ v_2 = 1 = Tr_1^4(\theta\alpha^{14}) \\ v_3 = 0 = Tr_1^4(\theta\alpha^6) \end{cases}$$

从而解出$\theta = \alpha^{13}$。又因为

$$\theta = A_k q(\alpha^k)\beta^k,$$

所以求出$\beta = \alpha^3$。所以初始密钥

$$\begin{aligned} (s_0, s_1, s_2, s_3) &= (Tr(\beta), Tr(\beta\alpha), Tr(\beta\alpha^2), Tr(\beta\alpha^3)) \\ &= (1, 0, 0, 1)。 \end{aligned}$$

可以看到在文献[41]中，其计算复杂度并没有考虑计算A_k的复杂度。如果不考虑计算A_k的复杂度，那么这个方法主要的复杂度就集中在计算$q(\alpha^k)$上了。其复杂度为$o(LS(s)(log(LS(s)))^3)$。如果只计算一个或数个A_k，那么其计算复杂度就会为$o(D(logD)^3)$，其中$D = \sum_{i=0}^{deg(f)}\binom{n}{i}$。如果不考虑预计算，那么其计算复杂度仅为$o(nlog(n)\eta(n))$，其中$\eta(n) = nlog(n)loglog(n)$。

注意到如果f不是不可约多项式，那么是不能通过求出β来恢复初始密钥的，离散傅里叶谱攻击也就无法实现。但是如果序列$\{z_t\}$的线性复杂度足够的低，可以恢复出z_t的谱序列Z_t从而得到新的线性移位寄存器来求出全部的z_t。

6.2　快速离散傅里叶谱攻击

当反馈序列的线性复杂度比较高的时候，离散傅里叶谱攻击需要的密文序列过长从而不是很有效。文献[41]运用了类似代数攻击寻找零化子的手段推广了离散傅里叶谱攻击。

6.2.1 攻击算法简介

快速离散傅里叶谱攻击的实质是找到一个与原先的序列由相同的结构和不同的过滤函数生成的新的序列，使得这两个序列逐项相乘后生成的新序列线性复杂度尽量的低，从而使得所需要的密文序列尽可能的短来达到优化算法的目的。

具体算法如下：

算法 6.2. *[41]* 对基于线性移位寄存器和非线性布尔函数的无记忆的流密码体制，其中$\{s_t\}$是m-序列。

输入：反馈序列$(z_0, z_1, \ldots, z_{D-1})$，$D < LS(\boldsymbol{h})$

输出：初始密钥$(s_0, s_1, \ldots, s_{n-1})$

预计算部分：

1. 选择序列$\{h_t\}$并计算$\{u_t = h_t z_t\}$，满足

$$|\overline{N_h} \bigcup \overline{N_u}| < LS(\boldsymbol{b})。$$

2. 计算α^k的极小多项式$p_k(x)$和$q(x) = \prod_{k\in T} p_k(x)$，其中

$$T = \begin{cases} N_u^*/N_h & 若N_u^* \not\subset N_h, \\ \{k_0\} \subset N_u^* & 否则, \end{cases}$$

$(\overline{N_u} = \{k_0, k_1, \ldots, k_{LS(u)-1}\}$，其中$U_{k_i} \neq 0$；$N_u$是$\overline{N_u}$中所有陪集头的集合$)$

3. 对于$q(x) = \sum_{i=0}^{r} c_i x^i$，计算$q(\alpha^k)$和

$$\gamma_{t,k} = U_k q(\alpha^k)\alpha^{tk},\ k \in \mathcal{J}$$

其中$\mathcal{J} =$

$$\begin{cases} (N_u \bigcap N_h) \bigcup \{0\}\ N_u^* \not\subset N_h, 0 \in N_u \\ (N_u \bigcap N_h) \bigcup \{0\}\ N_u^* \not\subset N_h, 0 \notin N_u \\ N_u/k_0 \end{cases}$$

计算部分：

1. 计算

$$\zeta_{t,k} = H_k f_t(\alpha^k)\alpha^(tk),\ t = 0, 1, \ldots, LS(\boldsymbol{h}) - 1。$$

其中

$$f_t(x) = \sum_{i=0}^{r} c_i s_{i+t} x^i。$$

2. 求解关于β^k的线性方程组：

$$\sum_{k\in\overline{\mathcal{J}}} \gamma_{t,k}\beta^k = \sum_{k\in\overline{N_h}} \zeta_{t,k}\beta^k,\ t = 0, 1, \ldots, LS(\boldsymbol{h}) - 1)。$$

3. 反解出β或给出β^k的值并且换一个k继续求解。

4. 返回初始密钥$s_t = Tr_1^n(\beta\alpha^t)$。

6.2.2　算法原理及简化

考虑$u_t = \sum_{j=0}^{2^n-1} U_j \beta^j \alpha^{tj}$，令

$$\begin{aligned} v_t &= \sum_{i=0}^{r} c_i u_{i+t} \\ &= \sum_{i=0}^{r} c_i \sum_{j=0}^{2^n-1} U_j \beta^j \alpha^{(i+t)j} \\ &= \sum_{j=0}^{2^n-1} U_j \beta^j \alpha^{tj} \sum_{i=0}^{r} c_i \alpha^{ij} \\ &= \sum_{j=0}^{2^n-1} U_j \beta^j \alpha^{tj} q(\alpha^j) \\ &= \sum_{j \in \overline{J}} U_j \beta^j \alpha^{tj} q(\alpha^j) \end{aligned}$$

由$u_t = s_t h_t$，令

$$\begin{aligned} v_t &= \sum_{i=0}^{r} c_i s_{i+t} h_{i+t} \\ &= \sum_{i=0}^{r} c_i s_{i+t} \sum_{j=0}^{2^n-1} H_j \beta^j \alpha^{(i+t)j} \\ &= \sum_{j \in \overline{N_h}} H_j \beta^j \alpha^{tj} f_t(\alpha^j) \end{aligned}$$

这样取不同的t就可以得到一组关于β的方程。

在[41]中，其计算复杂度并没有考虑计算H_k, U_k的复杂度。考虑最好的情况，也就是$U_k \equiv 0$时，这时只需要计算$H_k, q(x)$和最终关于β^k的线性方程组的复杂度了，而对于这种情况，可以有下述简化方法来计算。

算法 6.3. 对基于线性移位寄存器和非线性布尔函数的无记忆的流密码体制，其中$\{s_t\}$是m-序列

输入：反馈序列$(z_0, z_1, \ldots, z_{D-1})$，$D < LS(\boldsymbol{h})$

输出：初始密钥$(s_0, s_1, \ldots, s_{n-1})$ 计算部分：

1. 选择序列$\{h_t\}$使得$u_t = h_t z_t \equiv 0$，并计算$\{H_t\}$。

2. 计算α^k的极小多项式$p_k(x)(H_k \neq 0)$和

$$p(x) = \prod_{j \in \Gamma(2^n-1), H_j \neq 0} p_k(x)。$$

3. 计算$q(\alpha^k)$，其中

$$q(x) = p(x)/p_k(x) = \sum_{i=0}^{r} c_i x^i。$$

计算部分:

1. 计算$\{v_t\}$，$0 = \sum_{i=0}^{r} c_i s_{i+t} h_{i+t}$。

2. 解关于θ的方程

$$\begin{aligned} v_t &= \sum_{i=0}^{r} c_i s_{i+t} h_{i+t} \\ &= \sum_{i=0}^{r} c_i s_{i+t} \sum_{j=0}^{2^n-1} H_j \beta^j \alpha^{(i+t)j} \\ &= \sum_{j=0}^{2^n-1} H_j \beta^j \alpha^{tj} \sum_{i=0}^{r} c_i s_{i+t} \alpha^{ij} \end{aligned}$$

以上方程可以看作是关于$LS(\boldsymbol{h})$个变量$\{\beta^i | i = 0, 1, \ldots, LS(\boldsymbol{h}) - 1\}$的$\mathbb{F}_{2^{n_k}}$上的线性方程组。

3. 反解出β或给出β^k的值并且换一个k继续求解。

4. 返回初始密钥$s_t = Tr_1^n(\beta\alpha^t)$。

在这个简化特例中，即使不考虑预计算的复杂度，实际计算的复杂度也相当于求解一个有$LS(\boldsymbol{h})$个变量的$\mathbb{F}_{2^n}$上的线性方程组。这个复杂度大致上为$o(LS(\boldsymbol{h})^{2.37}\eta(n))$，与快速代数攻击的结果类似。

6.3 滤波生成器序列的线性复杂度

根据快速离散傅里叶谱攻击算法可以知道，在实现攻击的时候我们需要得到一个新的多项式h，使得由与f相同的一个LFSR生成的反馈序列的线性复杂度比较小，并且hf最好为0或者次数尽量低。然后用h和fh求出H_k和U_k。

6.3.1 序列的谱免疫度

根据快速离散傅里叶谱攻击，G.Gong等提出了谱免疫度的概念:

定义 6.1. [41] 序列$\boldsymbol{s} = \{s_t\}$的谱免疫度:

$$P_s = \min_{\boldsymbol{h} \in \mathbb{Z}_0^N} \{LS(\boldsymbol{h}) | \boldsymbol{s} \cdot \boldsymbol{h} = 0 \text{ 或 } (\boldsymbol{s} \oplus 1) \cdot \boldsymbol{h} = 0\}$$

注意到

$$LS(g[\boldsymbol{s}]) \leq \sum_{i=1}^{deg(g)} \binom{n}{i}$$

$$P_s \leq \sum_{i=1}^{AI(g)} \binom{n}{i}。$$

假设密码系统LFSR的生成序列是x^4+x+1。

例 6.2. 假设过滤多项式是

$$f(x_1,x_2,x_3,x_4,x_5) = x_1x_2x_3x_4 + x_1x_2x_3 + x_2x_3x_4 + x_2x_3x_5 + x_5,$$

我们可以得到$AI(f)=2$，且

$$P_s = 15 = \sum_{i=1}^{AI(f)} \binom{4}{i}。$$

例 6.3. 假设过滤多项式是

$$f(x_1,x_2,x_3,x_4) = x_2 + x_1x_3 + x_1x_4 + x_1x_2x_3。$$

我们可以得到$AI(f)=2$，且

$$P_s = 4 < \sum_{i=1}^{AI(f)} \binom{4}{i} = 10。$$

以上的例子告诉我们，具有最优代数免疫度的布尔函数，其反馈序列不一定拥有最优的谱免疫度。这样如何构造具有最优谱免疫度的序列也是值得我们研究的问题。

6.3.2　滤波生成器序列的线性复杂度

同样考虑基于线性移位寄存器和高度非线性的布尔函数的无记忆的流密码体制。

$f(\boldsymbol{x})$是从F_2^n到F_2的一个非线性函数，其代数标准形为

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{d}\in\mathbb{F}_2^n} a_{\boldsymbol{d}}\boldsymbol{x}^{\boldsymbol{d}},$$

其中$\boldsymbol{d}=(d_1,d_2,\ldots,d_n)\in\mathbb{F}_2^n$，$a_{\boldsymbol{d}}\in\mathbb{F}_2$且$\boldsymbol{x}^{\boldsymbol{d}} = x_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$。设$\boldsymbol{s}$是由$LFSR$生成的序列，那么

$$z_t = f(s_t, s_{t+n}, \ldots, s_{t+n-1}) = f_t(s_0, s_1, \ldots, s_{n-1}),$$

其中$\{z_t\}$叫做滤波生成器序列。

如上所述，

$$z_t = f(s_t, s_{t+n}, \ldots, s_{t+n-1}) = f_t(s_0, s_1, \ldots, s_{n-1})。$$

以f是个单项式为例：

$$f(x_1, x_2, \ldots, x_n) = x_{\delta_1} x_{\delta_2} \ldots x_{\delta_k}。$$

设$\{s_t\}$是m-序列，即

$$s_t = Tr_1^n(\beta\alpha^t) \quad t = 0, 1, 2, \ldots, \beta \in \mathbb{F}_{q^n}^*$$

将$\{s_t\}$带入上式，则：

$$\begin{aligned} z_t &= s_{t+\delta_1} s_{t+\delta_2} \cdots s_{t+\delta_k} \\ &= [\sum_{v_1=0}^{n-1} (\beta\alpha^{\delta_1+t})^{2^{v_1}}][\sum_{v_2=0}^{n-1} (\beta\alpha^{\delta_2+t})^{2^{v_2}}] \ldots [\sum_{v_k=0}^{n-1} (\beta\alpha^{\delta_k+t})^{2^{v_k}}] \\ &= \sum_{v_1, v_2, \ldots, v_k} \alpha^{\delta_1 2^{v_1} + \delta_2 2^{v_2} + \ldots + \delta_k 2^{v_k}} (\beta\alpha^t)^{2^{v_1} + 2^{v_2} + \ldots + 2^{v_k}} \\ &= \sum_{wt(v) \le k} A_{|v|} (\beta\alpha^t)^{|v|} \end{aligned}$$

其中

$$|\boldsymbol{v}| = 2^{v_1} + 2^{v_2} + \ldots + 2^{v_k}$$

是$\boldsymbol{v}$的整数表示。所以$\{z_t\}$的谱序列$\{Z_t\}$满足$Z_t = A_t\beta^t$。f为多项式的情况求和即可。

由于$\beta \neq 0$，那么$Z_t \neq 0$当且仅当$A_t \neq 0$。容易得到以下定理

定理 6.1. *[47]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f的次数为k，那么滤波生成器序列$\{z_t\}$的线性复杂度满足：

$$LS(\boldsymbol{z}) \le \sum_{i=1}^{k} \binom{n}{i}。$$

推论 6.2. 如上所述，令$wt(v) = k$, $v = 2^{v_1} + 2^{v_2} + \ldots + 2^{v_k}, v_1 \neq v_2 \neq \ldots \neq v_k$。则$\alpha^v$是$z$最小多项式的一个根当且仅当矩阵

$$D_v = (\alpha^{\delta_i 2^{v_i}}), 0 \le i, j < k$$

的行列式非零。

证明. 注意到当$wt(v) = k$时，$\hat{A}_v = det(\alpha^{\delta_i 2^{v_i}}), 0 \le i, j < k$。 □

6.3.3　等距过滤函数已有的研究结果

考虑k次的等距过滤单项式：

$$f(x) = x_0 x_d \dots x_{(k-1)d}, \quad (k-1)d \le n,$$

则生成序列$\{z_t\}$为

$$z_t = s_t s_{t+d} \dots s_{t+(k-1)d}。$$

很多文章都研究过研究等距过滤函数所生成的滤波序列的线性复杂度[47–49, 67, 78]，也有了不少结果和进展。

最早在1976年，E.L. Key就证明了2次等距过滤函数所生成的滤波序列的线性复杂度达到了最大值。

定理 6.3. *[47]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为2次单项式，即

$$z_t = s_t s_{t+d}$$

那么滤波生成器序列$\{z_t\}$的线性复杂度满足：

$$LS(z) = \binom{n}{2} + n,$$

即达到了最大值。

之后，运用查根法，R.A. Rueppel给出了等距滤波序列的线性复杂度的一个下界。

定理 6.4. *[78]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为k次等距过滤单项式，即

$$z_t = s_t s_{t+d} \dots s_{t+(k-1)d}$$

若$gcd(d, 2^n - 1) = 1$，那么滤波生成器序列$\{z_t\}$的线性复杂度满足：

$$LS(z) \ge \binom{n}{k}。$$

对于多项式的情形，他也给出了如下定理：

定理 6.5. *[78]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为由k次等距过滤单项式所组成的多项式，即

$$z_t = \sum_{i=0}^{M-1} c_i s_{t+i} s_{t+i+d} \dots s_{t+i+(k-1)d}$$

若$gcd(d, 2^n - 1) = 1$，那么滤波生成器序列$\{z_t\}$的线性复杂度满足：

$$LS(z) \ge \binom{n}{k} - M + 1。$$

1998年，K.J. Paterson细化了查根法，给出了稍好的下界。

定理 6.6. *[67]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为k次等距过滤单项式，即

$$z_t = s_t s_{t+d} \cdots s_{t+(k-1)d}$$

若t是使得$2^n - 1 | d(2^t - 1)$的最小整数，那么滤波生成器序列$\{z_t\}$的线性复杂度满足:

$$LS(z) \geq \binom{t}{k} (\frac{n}{t})^k。$$

对于多项式的情形，也给出了类似的结果。

定理 6.7. *[67]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为k次等距过滤多项式，即

$$z_t = \sum_{i=0}^{M-1} s_{t+i} s_{t+i+d} \cdots s_{t+i+(k-1)d}$$

若t是使得$2^n - 1 | d(2^t - 1)$的最小整数，那么滤波生成器序列$\{z_t\}$的线性复杂度满足:

$$LS(z) \geq \binom{t}{k} (\frac{n}{t})^k - M + 1。$$

2006年，N. Kolokotronis等又进一步给出了一个更好的下界。

定理 6.8. *[48]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为k次等距过滤单项式，$k = 2, 3, n, n-1$，即

$$z_t = s_t s_{t+d} \cdots s_{t+(k-1)d}$$

若$gcd(d, 2^n - 1) = 1$，那么滤波生成器序列$\{z_t\}$的线性复杂度满足:

$$LS(z) \geq \binom{n}{k} + \binom{n}{k-1}。$$

定理 6.9. *[48]* 设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为k次等距过滤单项式，$4 \leq k \leq n-2$，即

$$z_t = s_t s_{t+d} \cdots s_{t+(k-1)d}$$

若$gcd(d, 2^n - 1) = 1$，那么滤波生成器序列$\{z_t\}$的线性复杂度满足:

$$LS(z) \geq \binom{n}{k} + n。$$

6.3.4　等距序列线性复杂度的一些新的下界

基于上述结果，我们进一步推广了已有的方法，并给出了一些新的上界。首先从3次等距多项式入手，我们有如下定理：

定理 6.10. *设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为3次等距过滤单项式，即*

$$z_t = s_t s_{t+d} s_{t+2d}$$

若$gcd(d, 2^n - 1) = 1$，那么滤波生成器序列$\{z_t\}$的线性复杂度满足:

$$LS(z) = \binom{n}{3} + \binom{n}{2} + n。$$

即达到了最大值。

证明. 由以上定理可知

$$L(z) \geq \tbinom{n}{3} + \tbinom{n}{2},$$

所以我们只考虑$wt(v) = 1$的情形。当$wt(v) = 1$时，不失一般性，考虑$v = 2^{3-1} = 4$我们可以得到$v_1 = v_2 = 0, v_3 = 1$ 或$v_1 = v_3 = 0, v_2 = 1$ 或$v_2 = v_3 = 0, v_1 = 1$。那么有

$$\begin{aligned} Z_4 &= \sum_{2^{v_1}+2^{v_2}+2^{v_3}=4} \alpha^{d2^{v_2}+2d2^{v_3}} \\ &= \alpha^{5d} + \alpha^{4d} + \alpha^{3d} \\ &= \alpha^{3d}(1 + \alpha^d + \alpha^{2d}) \\ &= \frac{\alpha^{3d}(1 + \alpha^{3d})}{(1 + \alpha^d)}。 \end{aligned}$$

因为$n \geq 3$且$\gcd(d, 2^n - 1) = 1$，我们有$(2^n - 1) \nmid 3d$。所以$Z_v \neq 0$ 当$wt(v) = 1$时。　□

考虑当 $k = 4, wt(v) = 1$ 且令 $v = 2^{4-1} = 8$时，可以得到

$$\{v_1, v_2, v_3, v_4\} = \{1, 1, 1, 1\}$$

或者

$$\{v_1, v_2, v_3, v_4\} = \{2, 1, 0, 0\}。$$

运用和上一定理类似的方法，我们可以得到：

$$Z_8 = \alpha^{7\delta}(\alpha^{2\delta} + \alpha^{\delta} + 1)^2(\alpha^{3\delta} + \alpha^{\delta} + 1)(\alpha^{3\delta} + \alpha^{2\delta} + 1)。$$

如果 $n \geq 4$，那么 $Z_8 \neq 0$。因此我们可以得到以下结论：

定理 6.11. 当 $k=4$ 且 $gcd(\delta, 2^n-1)=1$ 时，

$$L(\boldsymbol{z}) \geq \binom{n}{4} + 2n。$$

从之前的计算总结经验，我们可以很明显的看到当 $wt(v)=1$ 时，$Z_v = \alpha^{m\delta} g(\alpha^{\delta})$，其中 $g(x)$ 是一个包含1的函数。如果 $n > deg(g)$，由于 α^{δ} 是 $GF(2^n)$ 中的一个变元，可以得到 $g(\alpha^{\delta}) \neq 0$，即 $Z_v \neq 0$。

引理 6.12. *(Rearrangement inequality)*

$$\begin{aligned} & x_1y_1 + x_2y_2 + \ldots + x_ny_n \\ \geq\ & x_{\sigma(1)}y_1 + x_{\sigma(2)}y_2 + \ldots + x_{\sigma(n)}y_n \\ \geq\ & x_ny_1 + x_{n-1}y_2 + \ldots + x_1y_n \end{aligned}$$

对任意满足

$$x_1 \geq x_2 \geq \ldots \geq x_n, y_1 \geq y_2 \geq \cdots \geq y_n$$

的实数和所有 $x_1, \ldots, x_n$ 的置换 $x_{\sigma(1)}, \ldots, x_{\sigma(n)}$。

运用以上引理，我们可以得到一个一般性的上界：

定理 6.13. 和之前所提及的一样，如果 $k>4$，$n > (k-3)2^{k-1}+2$ 且 $\gcd(\delta, 2^n-1)=1$，那么 $L(\boldsymbol{z}) \geq \binom{n}{k} + 2n$。

证明. 考虑分解 $2^{k-1} = 2^{k-2} + 2^{k-3} + \ldots + 2^0 + 2^0$。

根据上面的引理，可以得到：

$$\begin{aligned} & 2^{k-2}\cdot 0 + 2^{k-3}\cdot 1 + \ldots + 2^0\cdot(k-1) && (6.1) \\ \leq\ & \sigma_1\cdot 0 + \sigma_2\cdot 1 + \ldots + \sigma_{k-1}\cdot(k-1) \\ \leq\ & 2^{k-2}\cdot(k-1) + 2^{k-3}\cdot(k-2) + \ldots + 2^0\cdot 0 && (6.2) \end{aligned}$$

其中 $\boldsymbol{\sigma} = \sigma_i$ 是

$$2^{k-2}, 2^{k-3}, \ldots, 2^0, 2^0$$

的一个置换。

注意到其他 2^{k-1} 的分解都会有比这种分解更多的相同项，所以上述分解可以得到该表达式的最大和最小值，从而我们可以得到：

$$\deg(g) \leq (10) - (9) = (k-3)2^{k-1} + 2,$$

易得此定理。 □

同样的，我们可以得到在多项式情形下的类似定理

定理 6.14. *设$LFSR$的生成多项式为n次不可约多项式，过滤函数f为k次等距过滤多项式，即*

$$z_t = \sum_{i=0}^{M-1} s_{t+i}s_{t+i+d}\cdots s_{t+i+(k-1)d}$$

如果 $k>4$，$n>(k-3)2^{k-1}+2$ 且 $\gcd(\delta, 2^n-1)=1$，那么滤波生成器序列$\{z_t\}$的线性复杂度满足:

$$LS(\boldsymbol{z}) \geq \binom{n}{k} + 2n - M + 1。$$

证明. 注意到当$wt(v)=k$时，

$$A_v = \sum_{i=0}^{M-1} c_i\alpha^{iv} det(\alpha^{(i-1)d2^{v_i}}), 0 \leq i,j < k。$$

则$A_v \neq 0$当且仅当$det(\alpha^{(i-1)d2^{v_i}}) \neq 0$且$\alpha^v$不是方程$\sum_{i=0}^{M-1} c_i x^i = 0$的根。由于$\sum_{i=0}^{M-1} c_i x^i = 0$至多有$M-1$个根，命题易得。 □

6.4　布尔函数的谱免疫度

为了抵抗快速离散傅里叶谱攻击，G.Gong等在定义6.2提出了序列的谱免疫度的概念。

当输入序列是m-序列(即周期达到最大的伪随机序列)时，滤波生成序列的线性复杂度只与作为反馈多项式的布尔函数有关，由此我们可以给出布尔函数谱免疫度的概念。

定义 6.2. *令 f 是 n 元布尔函数且 s 是 F_2 上任意的(2^n-1)-周期序列(即m-序列)。*

$$P_f = min\{L(g[s]) | fg = 0 \quad or \quad (f+1)g = 0\}。$$

P_f 就定义为 f 的谱免疫度。

注意到

$$L(g[s]) \leq \sum_{i=1}^{deg(g)} \binom{n}{i},$$

容易得到P_f的上界：

定理 6.15. *令 f 是 n 元布尔函数，那么我们有*

$$P_f \leq \sum_{i=1}^{AI(f)} \binom{n}{i}。$$

例 6.4. [41] 对于布尔函数

$$f(x_1, x_2, x_3, x_4) = x_2 + x_1x_3 + x_1x_4 + x_1x_2x_3,$$

我们可以得到 $AI(f) = 2$ 且

$$P_f \leq 4 < \sum_{i=1}^{AI(f)} \binom{4}{i} = 10。$$

这个例子也告诉我们具有最有代数免疫的布尔函数未必具有最优的谱免疫度。

6.5 本章小结

众所周知，常用的基于线性移位寄存器和非线性布尔函数的流密码体制对于代数攻击的抵抗能力不高。这一章我们首先介绍了离散傅里叶谱攻击的原理和算法，说明了它其实是一种特殊的代数攻击，并且针对快速离散傅里叶谱攻击的特殊情形给出了简化算法。之后，由于离散傅里叶谱攻击的算法主要与生成序列的线性复杂度有关，我们从滤波生成序列的角度出发，给出了等距滤波生成序列线性复杂度的一些新的下界。最后我们结合序列的谱免疫度，提出了布尔函数谱免疫度的概念。结合谱免疫度和序列的线性复杂度来分析和构造布尔函数也是我们以后工作的目标之一。

第七章　结论与展望

本文意在研究布尔函数的各项密码学性质以及其与给类密码攻击的联系。我们针对一些特殊的布尔函数类和攻击方法，在已有的研究基础上，进一步的探究了函数的密码学性质，其主要结果如下：

1. 研究了*Bent*函数在 *d-upper* 布尔函数类中的存在性。证明了，如果在属于这个函数类的布尔函数代数标准型中单项式的个数小于 $n+d-3$，那么它不是*Bent*函数。同时，这个函数类中*Bent*函数的 d 值是小于 $\lceil 3n/8+3/4 \rceil$ 的。

2. 提出了一个正确率极高的偏真算法来计算循环对称布尔函数对快速代数攻击的免疫程度。还证明了当 n 为偶数且 n 不是 2 的幂次时，对于 n 元循环对称布尔函数 f，存在次数不超过 $e \leq n/3$ 的布尔函数 g，使得 gf 的次数不超过 $n-e-1$。

3. 提出了完全代数免疫的概念，并且证明了一个平衡的完全代数免疫函数的变元数一定是 2^m+1；一个不平衡的完全代数免疫函数的变元数一定是 2^m。同时，给出了一个判定单变元表示布尔函数快速代数免疫性的有效算法，并且由此证明了变元数为 2^m+1 的Carlet-Feng函数和变元数为 2^m 的移位Carlet-Feng函数是完全代数免疫函数。

4. 运用离散傅里叶变换理论(DFT)，针对等距过滤函数类，给出了由 m 序列生成的滤波序列线性复杂度的一个改进的下界。同时，还给出了布尔函数谱免疫度的概念来衡量布尔函数抵抗离散傅里叶谱攻击的能力，并给出了其一个上界。

虽然这篇论文研究了布尔函数的一些密码学性质，特别对于布尔函数的快速代数免疫性有着深入的研究，但是遗留下来的问题也很多：

1. *d-upper* 布尔函数类除了非线性度以外，其他相关的密码学性质还没有得到进一步的研究，这也是我们之后的工作方向之一。

2. 除了Carlet-Feng函数以外，我们还没有找到其他的完全代数免疫函数。构造具有最优快速代数免疫度函数的问题依然没有得到解决。具体到循环对称布尔函数类，是否可以在其中找到完全代数免疫函数也是今后我们需要重点关注的问题之一。考虑一些已经证明具有最优代数免疫度的布尔函数类，是否能够抵抗快速代数攻击，也是值得研究的问题。

3. 对于滤波序列线性复杂度的下界问题，我们的研究也依然不够完善；是否可以运用其他的数学工具来研究这个问题尚待进一步的考察。

4. 对于布尔函数的谱免疫度的研究，我们这里只是浅尝辄止，进一步的研究将在未来进行。

总之，布尔函数的密码学性质研究是密码学理论中的一个重要课题，而探究其各种密码学性质之间的联系并尝试构造具有好的密码学性质的布尔函数是我们接下来工

作的重点。

由于作者的水平有限，论文中的不足之处在所难免，敬请各位评审专家和读者批评指正！