博士后文库
中国博士后科学基金资助出版

布尔函数间接构造的研究

张凤荣　编著

科学出版社

博士后文库

中国博士后科学基金资助出版

布尔函数间接构造的研究

张凤荣　编著

科学出版社

北京

内 容 简 介

Bent 函数和 plateaued 函数是密码学和编码与设计中两类重要的布尔函数。本书较为系统地介绍了 Bent 函数的间接构造方法。给出了两种构造“谱不相交函数集”的方法，并给出了许多目前非线性度最优的奇变元弹性函数和平衡函数。同时利用间接构造方法构造出不属于“完全 Maiorana-McFarland(M-M)类”的 Bent 函数和 Bent-negabent 函数。

本书可以作为信息安全和密码学研究生的选修教材，也可以作为从事密码理论研究的科技人员的参考书。

图书在版编目(CIP)数据

布尔函数间接构造的研究/张凤荣编著. —北京：科学出版社，2019.6
(博士后文库)
ISBN 978-7-03-061542-8

I. ①布… II. ①张… III. ①布尔函数-函数构造论 IV. ①O153.2

中国版本图书馆 CIP 数据核字(2019)第 111646 号

责任编辑：陈 静 金 蓉/责任校对：郑金红

责任印制：师艳茹/封面设计：陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销
*
2019 年 6 月第 一 版 开本：720×1000 1/16
2019 年 6 月第一次印刷 印张：10
字数：202 000

定价：68.00 元

(如有印装质量问题，我社负责调换)

《博士后文库》编委会名单

《博士后文库》序言

1985 年，在李政道先生的倡议和邓小平同志的亲自关怀下，我国建立了博士后制度，同时设立了博士后科学基金。30 多年来，在党和国家的高度重视下，在社会各方面的关心和支持下，博士后制度为我国培养了一大批青年高层次创新人才。在这一过程中，博士后科学基金发挥了不可替代的独特作用。

博士后科学基金是中国特色博士后制度的重要组成部分，专门用于资助博士后研究人员开展创新探索。博士后科学基金的资助，对正处于独立科研生涯起步阶段的博士后研究人员来说，适逢其时，有利于培养他们独立的科研人格、在选题方面的竞争意识以及负责的精神，是他们独立从事科研工作的“第一桶金”。尽管博士后科学基金资助金额不大，但对博士后青年创新人才的培养和激励作用不可估量。四两拨千斤，博士后科学基金有效地推动了博士后研究人员迅速成长为高水平的研究人才，“小基金发挥了大作用”。

在博士后科学基金的资助下，博士后研究人员的优秀学术成果不断涌现。2013 年，为提高博士后科学基金的资助效益，中国博士后科学基金会联合科学出版社开展了博士后优秀学术专著出版资助工作，通过专家评审遴选出优秀的博士后学术著作，收入《博士后文库》，由博士后科学基金资助、科学出版社出版。我们希望，借此打造专属于博士后学术创新的旗舰图书品牌，激励博士后研究人员潜心科研，扎实治学，提升博士后优秀学术成果的社会影响力。

2015 年，国务院办公厅印发了《关于改革完善博士后制度的意见》（国办发〔2015〕87 号），将“实施自然科学、人文社会科学优秀博士后论著出版支持计划”作为“十三五”期间博士后工作的重要内容和提升博士后研究人员培养质量的重要手段，这更加凸显了出版资助工作的意义。我相信，我们提供的这个出版资助平台将对博士后研究人员激发创新智慧、凝聚创新力量发挥独特的作用，促使博士后研究人员的创新成果更好地服务于创新驱动发展战略和创新型国家的建设。

祝愿广大博士后研究人员在博士后科学基金的资助下早日成长为栋梁之才，为实现中华民族伟大复兴的中国梦做出更大的贡献。

中国博士后科学基金会理事长

前　言

密码函数是构成密码算法的重要组件。Bent 函数、plateaued 函数和弹性函数等密码函数是密码学者研究的热点问题。这些密码函数主要应用于对称密码(流密码和分组密码)非线性部件，如反馈移位寄存器中的反馈函数、非线性组合序列中的组合函数、分组密码中的 S 盒等。此外，Bent 函数在编码、组合和设计中也有重要的作用。

40 多年来，Bent 函数一直是人们关注的热点和难点问题，几乎每年都有许多新方法、新结果在学术期刊上发表。但目前知道的 Bent 函数最主要的只有两类：Maiorana-McFarland(M-M)类 Bent 函数和 Partial Spread(PS)类 Bent 函数。作者对 Bent 函数的间接构造给出了详细的论述，并利用“间接构造”构造出不属于“完全 M-M 类”的 Bent 函数。此外，对“谱不相交函数集”进行了研究。书中的内容包含了作者近年来在密码函数方面的部分成果，如 Bent 函数的新间接构造和没有非零线性结构的“谱不相交函数集”的构造等。

全书共 8 章。第 1 章主要介绍了密码函数研究中所需要的基本知识。第 2 章主要介绍了 9 种 Bent 函数的间接构造方法。第 3 章对 Rothaus 构造做了进一步的研究，利用该方法构造出不属于“完全 M-M 类”的 Bent 函数。第 4 章给出了一个 Bent-negabent 函数的新构造，首次构造出不属于“完全 M-M 类”的 Bent-negabent 函数。第 5 章介绍了一种广义 Bent 函数的间接构造。第 6 章给出了一个构造高非线性度布尔函数方法和一个构造谱不相交 plateaued 函数集的方法，研究了谱不相交 plateaued 函数为平衡函数的条件。第 7 章给出了一个构造势更大的谱不相交函数集的方法，给出了许多目前非线性度最优的奇变元弹性函数，特别是，当函数变元大于 33 时，给出了目前非线性度最优的奇变元平衡函数。第 8 章给出了 Rothaus 构造的一般化形式。

中国矿业大学计算机科学与技术学院夏士雄教授、周勇教授、曹天杰教授，西安电子科技大学胡予濮教授和桂林电子科技大学韦永壮教授对本书的出版给予

了极大的鼓励和支持，在此表示深深的谢意！全书的编写工作得到了中国矿业大学计算机科学与技术学院刘师师硕士生、郝学轩硕士生、黄晨帆硕士生和季霄鹏硕士的全力协作和密切配合，在此一并对他们表示衷心的感谢！

本书的出版得到了《博士后文库》出版资助和中国矿业大学优秀青年骨干教师项目资助，在此表示感谢！

由于作者水平和时间有限，书中疏漏与不妥之处在所难免，恳请读者批评指正。

作　者

2019 年 2 月 6 日

目　录

第1章 绪 论

密码函数在分组密码和流密码的设计和分析中起着重要的作用。布尔函数和多输出布尔函数是两类重要的密码函数。布尔函数主要用于流密码的分析与设计，如基于线性反馈移位寄存器(linear feedback shift register，LFSR)的密钥流生成器。多输出布尔函数主要用于分组密码的分析和设计，比如分组密码的S盒由非线性多输出布尔函数构成。数据加密标准(data encryption standard，DES)就是分组密码的一个经典的例子，它的安全性取决于S盒密码学性质的好坏，而S盒可以用多输出布尔函数来描述。构造密码学性质优良的密码函数是设计较高安全性的分组密码体制的关键。

本章先介绍高非线性度弹性函数和Bent函数的研究现状，然后介绍布尔函数一些基本概念。

1.1 布尔函数研究现状

为了抵抗各种攻击，密码系统中的函数应具有非常好的密码学性质。因此，具有良好密码学性质的函数的构造目前仍是密码学界关注的焦点问题，特别是代数攻击[1]在流密码上取得的成功，使得最优代数免疫函数的构造与分析成为密码学界关注的重要问题。起初，研究最优代数免疫函数的通常做法是：先构造具有最优代数免疫度的函数，然后分析该函数的其他密码学性质。然而，这些函数的非线性度要么比较低，要么不能给出下界。2008年，Carlet和我国数学家冯克勤[2]在亚洲密码学年会上给出了一类具有最优代数免疫的平衡函数，并确定了其非线性度的一个较高理论下界。实际上，这类函数的一些低变元例子被验证具有很高的非线性度和很好的抗快速代数攻击的能力。在这之后，很多高非线性度最优代数免疫函数[3-15]也相继被给出。Liu等[12]引入了“完全代数免疫”的概念，证明了完全代数免疫函数只有当变元为2^m和2^m+1时才存在，其中m为整数。文献[12]为研究密码函数提供了一个新的思路，如构造更多的完全代数免疫函数等。

由于边信道攻击(特别是硬差错攻击，其攻击的核心思想是利用一种物理技术使密码系统嵌入一些错误，即保证密码系统中某些值始终为一个常数，然后利用数学方法对破坏后的密码系统进行分析，进而得到密钥)在对称密码上取得的成功[16,17]，非线性密码函数的研究面临着新的挑战和机遇。因此，对非线性密码函数的研究，不仅要考虑非线性度、代数次数、弹性阶、代数免疫度以及抵抗快速代数攻击的能力，还要考虑它抗“硬差错攻击”的能力(即在确定某几个输入变量后所得函数的密码学性质)。函数固定变元后所得函数密码学性质早在2002年就已开始被研究，例如，Carlet 指出 Maiorana-McFarland(M-M)技术所构造的函数存在缺陷(即当固定一些输入变量时，所构造的函数以很大的概率退化为仿射函数)，并利用级联二次函数的方法构造出了一些 M-M 超类函数[15]。其后 Zeng 等[18]以及文献[19]也给出了一些高非线性度高代数次数的 M-M 超类函数。最近，大量的高非线性度布尔函数被给出[20-24]，特别是文献[23]通过级联非线性函数得到了许多高非线性度函数。

Bent 函数[25,26]是一类非线性度最高的特殊非线性布尔函数，几乎每年都有许多新方法、新结果在国际高端学术期刊上发表。但目前知道的 Bent 函数最主要有：M-M 类 Bent 函数、Partial Spread(PS)类 Bent 函数和 Dobbertin 给出的 Bent 函数。

Bent 函数是一类具有最高非线性度和最好扩散性的函数。虽然 Bent 函数不具有平衡性，即不能被直接用于密码系统的设计中，但其修改或变种常用于对称密码的设计中；再者，这类函数在纠错码理论和组合学上也有着独立的研究价值。自 Bent 函数的概念提出以来，Bent 函数一直是密码学者关注的热点问题。目前，对 Bent 函数的研究主要包括：Bent 函数的构造[27-38]、Bent 函数的高阶非线性度[39]、齐次 Bent 函数[40]、Bent 函数和弹性函数的距离[41]、Bent 函数的分解[42]以及 Bent 函数的计数等[43,44]。Bent 函数的构造是 Bent 函数研究中的热点问题，这类函数的构造可归结为两种形式：直接构造法(按照某种特定的方式构造 Bent 函数)和间接构造法(利用已知的 Bent 函数来构造 Bent 函数)。

Bent函数的间接构造可以追溯到1974年，Dillon给出了一个简单的构造方法，即直和构造法[26]。此后，Rothaus 给出了一个构造 Bent 函数的间接方法——Rothaus 构造[25]。1994 年，Carlet 从 M-M 类 Bent 函数中导出两类新的 Bent 函数[27]。紧接着，他给出了一个构造 Bent 函数的抽象间接构造方法[28]，并发现“直和构造

法”和“Rothaus 构造”均可以看成该构造的特例。近年来，基于文献[28]的抽象间接构造，人们又给出了非直和构造[29]和广义非直和构造[31]等。最近，文献[45]发现了一个由 n 元和 m 元 Bent 函数构造 $(n+m-2)$ 元 Bent 函数的方法，并分析了选择不同初始函数时的部分情况，但该方法是否能构造出新函数以及所构造的函数与已知函数的关系还不清楚。Budaghyan 等[44]证明了两类 Niho Bent 函数不属于完全 M-M 类 Bent 函数。

Bent 函数可以通过迹函数来描述，这类函数通常被认为是通过直接构造得到的。近年来，人们十分关注迹函数表示的 Bent 函数的构造，如单个幂函数的绝对迹函数(也称单项式函数)的构造、多项式二次 Bent 函数的构造[32]和多个迹函数项的 Bent 函数[33-38](即多项式 Bent 函数)的构造等。目前，人们对多项式 Bent 函数尤为感兴趣。早在 2006 年，Leander 等[34]就通过对 Niho 幂函数构造的推广，给出了一类多项式 Bent 函数；之后，Charpin 等[33]引入了分析多项式函数“Bent 性”(即是否为 Bent 函数)的新工具，并对几类多项式函数的 Bent 性进行了刻画；又后来，Mesnager[37,38]推广了文献[33]的结果，指出了一类新多项式函数的 Bent 性与指数和(包括 Dickson 多项式)之间的联系。

1.2 密码函数的密码学指标

密码函数作为设计序列密码、分组密码和 Hash 函数的重要组件，其密码学性质的好坏直接影响密码系统的安全性[1]。密码函数的密码学指标是衡量一个函数密码学性质好坏的重要参数。密码函数的发展与密码体制的各种攻击的提出是分不开的(如非线性度是针对线性攻击提出的，代数免疫度是针对代数攻击提出的，差分均匀度是针对差分攻击提出的，相关免疫阶是针对相关攻击提出的)。为了使构造的密码体制能够抵抗不同的攻击和适应不同的需求，密码学界一直致力于寻找和构造具有优良性质的密码函数。

目前，密码函数的密码学指标主要有：平衡性、高非线性度、高代数免疫度、低差分均匀度、高代数次数和相关免疫阶等。

下面介绍一下布尔函数的一些相关定义。

设整数集、实数集和复数集分别用符号 $\mathbb{Z}$,$\mathbb{R}$ 和 $\mathbb{C}$ 表示，$\mathbb{Z}_r$ 表示模 r 的整数环。

在不影响理解情况下，用“+”表示$\mathbb{Z},\mathbb{R},\mathbb{C}$和模$q$（$q\neq 2$）的加法。用$\mathbb{F}_2^n$表示基于素域$\mathbb{F}_2$的$n$维向量空间。用$\oplus$表示$\mathbb{F}_2^n$和$\mathbb{F}_2$上的加法。设$\omega=(\omega_1,\cdots,\omega_n)\in\mathbb{F}_2^n$和$x=(x_1,\cdots,x_n)\in\mathbb{F}_2^n$为两个$n$维向量，定义两个向量的内积为$\omega\cdot x=\omega_1x_1\oplus\cdots\oplus\omega_nx_n$。若$z=a+b\mathrm{i}\in\mathbb{C}$，$a,b\in\mathbb{R}$，则$|z|=\sqrt{a^2+b^2}$表示$z$的绝对值，其中$\mathrm{i}^2=-1$。一个$n$元布尔函数是指一个从$\mathbb{F}_2^n$映射到$\mathbb{F}_2$的函数。定义$\mathcal{B}_n$是所有$n$元布尔函数的集合。

布尔函数$f\in\mathcal{B}_n$，其定义域$x\in\mathbb{F}_2^n$，值域$f(x)\in\{0,1\}$。将函数的真值依字典序排列可以得到一个二元序列，即

$$\left[f(0,0,\cdots,0,0),f(0,0,\cdots,0,1),\cdots,f(1,1,\cdots,1,1)\right]$$

该序列唯一地表示了布尔函数，称为函数的真值表。

设向量$x\in\mathbb{F}_2^n$的汉明重量为$\mathrm{wt}(x)$，表示向量x中1的个数。布尔函数的汉明重量$\mathrm{wt}(f)$是指函数真值表中1的个数。若函数真值表中0和1的个数相等则称该布尔函数是均衡的或平衡的。支撑集$\mathrm{sup}(f)$是指满足$f(x)=1$的x构成的集合，记为$\mathrm{sup}(f)=\{x\mid f(x)=1\}$。本书中$0_n$表示长度为$n$的0向量，$1_n$表示长度为$n$的1向量。

例1.1　设f是一个4元布尔函数，其真值表为$[1,0,1,0,1,0,1,0,1,0,1,0,1,0,0,1]$，从真值表可知，$\mathrm{wt}(f)=8$，$\mathrm{sup}(f)=\{0000,0010,0100,0110,1000,1010,1100,1111\}$。

任何一个布尔函数$f(x)$都具有唯一的代数正规型（algebraic normal form，ANF）：

$$f(x_1,\cdots,x_n)=\bigoplus_{I\subseteq\{1,\cdots,n\}}a_I\prod_{i\in I}x_i$$

其中，a_I属于$\mathbb{F}_2$，$\prod_{i\in I}x_i$表示单项式。函数f的代数次数$\deg(f)$等于在其代数正规型中系数不为零的单项式的最大次数。函数f有不同的表示形式：

$$f(x)=\bigoplus_{u\in\mathbb{F}_2^n}a_ux^u$$

其中，$a_u\in\mathbb{F}_2,x^u=\prod_{i=1}^n x_i^{u_i}$。那么

$$\deg(f)=\max_{a_u\neq 0}\mathrm{wt}(u)$$

其中，$\mathrm{wt}(u)$ 表示 u 的汉明重量。

定义 $\mathrm{wt}(f)=\left|\{x\in\mathbb{F}_2^n \mid f(x)=1\}\right|$ 为函数的汉明重量，其中 $|\cdot|$ 表示一个集合的势。

除了上述两种表示方法，函数还有其他的表示方法，如小项表示和矩阵表示等。

首先介绍一下小项表示。

对于 $x_i,c_i\in\mathbb{F}_2$，规定 $x_i^1=x_i,x_i^0=\overline{x}_i(\overline{x}_i$为 x_i 的补)，于是

$$x_i^{c_i}=\begin{cases}1, & x_i=c_i\\ 0, & x_i\neq c_i\end{cases}$$

设 $c=(c_1,\cdots,c_n),x=(x_1,\cdots,x_n)$，则有

$$x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}=\begin{cases}1, & (x_1,\cdots,x_n)=(c_1,\cdots,c_n)\\ 0, & (x_1,\cdots,x_n)\neq(c_1,\cdots,c_n)\end{cases}$$

为了方便，记 $x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}=x^c$，于是

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

其中，$f(c)$ 是真值表中 c 对应的函数值，该表示方法被称为小项表示，常用于布尔函数的设计实现。

例 1.2　例 1.1 中布尔函数小项表示为

$$\begin{aligned}f(x)=&x_1^0x_2^0x_3^0x_4^0\oplus x_1^0x_2^0x_3^1x_4^0\oplus x_1^0x_2^1x_3^0x_4^0\oplus x_1^0x_2^1x_3^1x_4^0\\&\oplus x_1^1x_2^0x_3^0x_4^0\oplus x_1^1x_2^0x_3^1x_4^0\oplus x_1^1x_2^1x_3^0x_4^0\oplus x_1^1x_2^1x_3^1x_4^1\end{aligned}$$

接下来介绍一下矩阵表示。

设 $f(x)$ 是 $\mathbb{F}_2^n$ 上的 n 元布尔函数，若 $f(x)=1$，则称 x 为 $f(x)$ 的一个特征向量。记 $f(x)$ 的全体特征向量的集合为 S，即

$$S=\{\alpha \mid f(\alpha)=1,\alpha\in\mathbb{F}_2^n\}$$

记 $|S|=w$，其中 w 表示 $f(x)$ 的汉明重量。将 S 中 w 个向量按字典序从大到小排列，记第 i 个向量 $w_i=(c_{i1},\cdots,c_{in}),1\leqslant i\leqslant w$，称 0, 1 矩阵：

$$\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{w1} & c_{w2} & \cdots & c_{wn} \end{bmatrix}$$

为 $f(x)$ 的特征矩阵。

布尔函数与其特征矩阵是一一对应的，于是可将布尔函数某些问题的研究转化为矩阵问题的研究。

此外，布尔函数还有状态图等其他表示方法，这里不再一一列举。

设 f 是 n 元布尔函数，定义函数 f 在点 ω 的 Walsh 谱为

$$W_f(\omega)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+x\cdot\omega} \tag{1.1}$$

其中，$x\cdot\omega=x_1\omega_1\oplus x_2\omega_2\oplus\cdots\oplus x_n\omega_n$。

容易证明，Walsh 谱的逆变换为

$$(-1)^{f(x)}=\frac{1}{2^n}\sum_{\omega\in\mathbb{F}_2^n}W_f(\omega)(-1)^{x\cdot\omega} \tag{1.2}$$

从式(1.1)和式(1.2)可以看出，函数 f 的 Walsh 变换可以看成函数 $(-1)^{f(x)}$ 的离散傅里叶(Fourier)变换。如果考虑函数 f 的离散傅里叶变换，那么

$$S_f(\omega)=\sum_{x\in\mathbb{F}_2^n}f(x)(-1)^{x\cdot\omega} \tag{1.3}$$

相应的逆变换为

$$f(x)=\frac{1}{2^n}\sum_{\omega\in\mathbb{F}_2^n}S_f(\omega)(-1)^{x\cdot\omega} \tag{1.4}$$

为区分上面两种变换，式(1.1)通常被称为循环 Walsh 谱，式(1.3)被称为线性 Walsh 谱，两个变换之间具有如下的转换关系：

$$W_f(\omega)=\begin{cases}-2S_f(\omega), & \omega\neq 0_n\\ 2^n-2S_f(\omega), & \omega=0_n\end{cases}$$

由此可知，这两种变换可以相互确定，因此，只用一种变换来刻画函数即可。

定义 1.1　设 f 是一个 n 元布尔函数，A_n 表示所有 n 元仿射函数构成的集合。

令

$$N_f = \min_{l \in A_n} d(f,l) = \min_{l \in A_n} \mathrm{wt}(f \oplus l) \tag{1.5}$$

则称 N_f 为函数 f 的非线性度。

设 $l(x) = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n \oplus b = \omega \cdot x \oplus b$ 是一个仿射函数，其中 $b \in \mathbb{F}_2$，那么

$$d(f,l) = 2^{n-1} - \frac{1}{2}(-1)^b W_f(\omega) \tag{1.6}$$

进一步，结合式(1.4)和式(1.5)，函数 $f(x)$ 的非线性度用 Walsh 谱来描述为

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega \in \mathbb{F}_2^n} \left| W_f(\omega) \right| \tag{1.7}$$

众所周知，函数的 Walsh 谱满足帕塞瓦尔(Parseval)恒等式

$$\sum_{\omega \in \mathbb{F}_2^n} W_f^2(\omega) = 2^{2n}$$

从 Parseval 恒等式容易知道 $W_f^2(\omega)$ 的平均值为 2^n，也就是说：

$$\max_{\omega \in \mathbb{F}_2^n} \left| W_f(\omega) \right| \geqslant 2^{n/2}$$

这样可以得到布尔函数的一个非线性度上限：

$$N_f \leqslant 2^{n-1} - 2^{n/2-1} \tag{1.8}$$

这样，根据式(1.8)可知，对每一个 $\omega \in \mathbb{F}_2^n$，当且仅当 $\left| W_f(\omega) \right| = 2^{n/2}$ 时等号成立。该类函数只有当 n 为偶数时才存在，因此被称为 Bent 函数[25,26]。

当 n 为奇数时，n 元布尔函数的非线性度在 $2^{n-1} - 2^{(n-1)/2}$ 和 $2^{n-1} - 2^{n/2-1}$ 之间。更准确地说，当 $n = 1,3,5,7$ 时，已经证明非线性度的上限为 $2^{n-1} - 2^{(n-1)/2}$；当 $n > 7$ 时，文献[46]证明奇变元函数的非线性度上限严格大于 $2^{n-1} - 2^{(n-1)/2}$。值 $2^{n-1} - 2^{(n-1)/2}$ 通常被称为 Bent 级联限，这是因为它能够通过级联两个 $(n-1)$ 元的 Bent 函数得到。

对任意的 $0 \leqslant r \leqslant n$，$r$ 阶的里德-缪勒 (Reed-Muller)码 $\mathrm{RM}(r,n)$ 是一个长度为 2^n 的线性码，该码也可以用布尔函数来表述。$\mathrm{RM}(r,n)$ 表示所有代数次数不大于 r 的 n 元布尔函数组成的集合。函数的非线性度也可以通过线性码的最小距离