Gao Feixianxingdu Buer Hanshu De Sheji Yu Fenxi

高非线性度布尔函数的设计与分析

张凤荣 著

中国矿业大学出版社

高非线性度布尔函数的设计与分析

张凤荣 著

中国矿业大学出版社

内 容 简 介

Bent 函数和弹性函数是密码函数中两类重要的布尔函数。本书较为系统地介绍了 Bent 函数和高非线性度弹性函数的直接构造和间接构造。同时，分析了 Maiorana-McFarland（M-M）类类函数的零化子，给出了三次齐次 Bent 函数和谱不相交 Plateaued 函数的构造方法。

本书可以作为研究生的选修教材，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

高非线性度布尔函数的设计与分析/张凤荣著. —
徐州：中国矿业大学出版社，2014.11

ISBN 978-7-5646-2540-5

Ⅰ.①高… Ⅱ.①张… Ⅲ.①布尔函数—研究 Ⅳ.
①O153.2

中国版本图书馆 CIP 数据核字(2014)第 260420 号

书　　名　高非线性度布尔函数的设计与分析
著　　者　张凤荣
责任编辑　张　岩　郭　玉
出版发行　中国矿业大学出版社有限责任公司
（江苏省徐州市解放南路　邮编 221008）
营销热线　(0516)83885307　83884995
出版服务　(0516)83885767　83884920
网　　址　http://www.cumtp.com　**E-mail**:cumtpvip@cumtp.com
印　　刷　徐州中矿大印发科技有限公司
开　　本　850×1168　1/32　**印张** 4.625　**字数** 118 千字
版次印次　2014年11月第1版　2014年11月第1次印刷
定　　价　18.00元
（图书出现印装质量问题，本社负责调换）

前　言

密码函数是构成密码算法的重要组件。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。近年来，不断出现的新攻击给密码函数研究带来了许多新的挑战和机遇，使得在构造密码函数时需要考虑的指标越来越多，如虑非线性度、代数免疫度、弹性阶等密码学指标等。

Bent函数、Plateaued函数、弹性函数和最优代数免疫函数等是近二十年来密码理论研究的热点问题。特别是Bent函数，几乎每年都有许多新方法、新结果层出不穷地发表在国际高端学术期刊上。但目前知道的最主要的Bent函数只有两类：Maiorana-McFarland（M-M）类Bent函数和Partial Spread(PS)类Bent函数；而且Bent函数的个数还不知道，广义结构也不清楚，对它们的完全分类更是没有希望。作者试图对Bent函数和弹性函数的构造算法，从直接构造和间接构造两个方面进行详细的论述。书中的部分内容包含了作者近年来在密码函数

方面的一部分成果，如 Bent 函数的广义间接构造、高非线性函数的直接和间接构造，谱不相交 Plateaued 函数的间接构造等。

全书共分 6 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 章主要给出一些 Bent 函数的直接构造，并给出 M-M 类 Bent 函数的零化子以及三次齐次 Plateaued 函数。第 3 章主要介绍 Bent 函数的直和构造、Rothaus 构造、非直和构造以及一个由 n 元 Bent 函数和 m 元 Bent 函数构造的 $n+m-2$ 元 Bent 函数的方法等。第 4 章介绍弹性函数的概念及其等价刻画、弹性阶与非线性度、代数次数及其他密码指标之间的关系。另外，介绍了一些代表性的弹性函数的直接构造方法。第 5 章首先给出了一类高非线性度弹性函数的构造方法，其次，基于该构造给出了一个多输出弹性函数的构造方法。第 6 章介绍了弹性函数的间接构造，给出了一个新的构造高非线性度弹性函数的方法和一个构造谱不相交 Plateaued 函数的间接构造方法。

西安电子科技大学胡予濮教授，中国矿业大学计算机科学与技术学院夏士雄教授、周勇副教授、曹天杰教授，以及桂林电子科技大学韦永壮教授等人对本书的出版给予了极大的鼓励和支持，在此表示深深的感谢！全书的编写工作得到了石家庄铁道大学计算机学院赵永斌副教授以及中国矿业大学计算机科学与技术学院陈秀清

博士生的全力协作和密切配合，在此一并对他们表示衷心的感谢！

本书的出版得到了国家自然科学基金项目（NO：61303263）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！

由于水平有限，时间有限，书中若有疏漏与不妥之处，恳请读者批评指正。

著　者

2014 年 1 月

目　录

1 绪 论

密码学包含密码编码学和密码分析学两个分支. 密码编码学的主要任务是寻找保证信息的机密性和可认证性的方法;密码分析学的主要任务是研究加密信息的破译和信息的伪造. 这两个分支既相互独立,又统一. 根据密钥的特点,密码体制分为对称和非对称密码体制. 就对称密码而言,又可分为流密码和分组密码. 密码函数(包括布尔函数和多输出布尔函数)在流密码和分组密码的分析和设计中起着非常重要的作用. 本书主要介绍具有优良密码学性质(如高非线性度、高代数次数、高代数免疫度等)布尔函数和多输出布尔函数的构造.

密码函数包括布尔函数和多输出布尔函数两大类. 布尔函数主要用于流密码的分析与设计,如基于线性移位寄存器(LFSR)的密钥流生成器非线性滤波生成器、非线性组合生成器都要用到密码函数 $f(x)$(如图 1-1 所示).

多输出布尔函数主要用于分组密码的分析和设计中,比如分组密码的 S 盒由非线性多输出布尔函数构成. 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(一个 S 盒可以用 4 个 4 元布尔置换)来描述. 分组密码中用到的各种置换也可以看成多输出密码函数. 可以看出,构造密码学性质优良的多输出密码函数是设计较高安全性的分组密码体制的关键.

密码函数作为设计序列密码、分组密码和 Hash 函数的重要

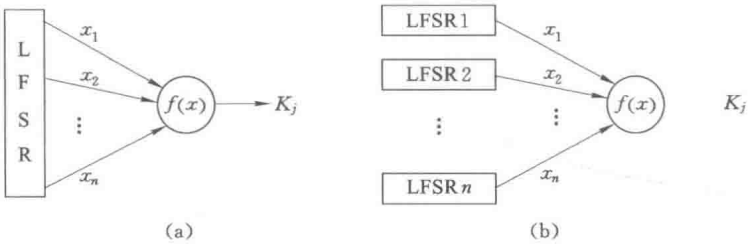

图 1-1　非线性滤波生成器和非线性组合生成器

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满足不同的需求，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.

定义 1.1　设 n 是一个正整数，F_2 为二元域，F_2^n 是一个基于 F_2 的 n 维线性空间. 定义 B_n 是 F_2^n 上所有 n 元布尔函数的集合.

布尔函数 $f\in B_n$，其定义域 $x\in F_2^n$，值域 $f(x)\in\{0,1\}$. 可以用枚举法将函数的真值依字典序排列的二元序列，即

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

该序列唯一地表示了布尔函数，该序列叫函数的真值表.

向量 $x\in F_2^n$ 的汉明重量即为 $wt(x)$，表示向量 x 中 1 的个数. 布尔函数的重量 $wt(f)$ 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 $\sup(f)$指满足 $f(x)=1$ 的 x 构成的集合，记为 $\sup(f)=\{x|f(x)=1\}$.

例 1.1 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，$wt(f)=8$，$\sup(f)=\{0000,0010,0100,0110,1000,1010,1100,1111\}$.

任何一个布尔函数 $f(x)$都具有唯一的代数正规型(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 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 $f(x)=\bigoplus_{u\in F_2^n} a_u x^u$，其中 $a_u\in F_2$，$x^u=\prod_{i=0}^{n}x_i^{u_i}$. 那么，$\deg(f)=\max_{a_u\neq 0} wt(u)$，其中 $wt(u)$表示 u 的汉明重量. 定义 $wt(f)=\|\{x\in F_2^n|f(x)=1\}\|$ 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.

1.1.1 小项表示

对于 $x_i,c_i\in F_2$，规定

$$x_i^1=x_i,x_i^0=\bar{x_i}$$

于是

$$x_i^{c_i}=\begin{cases}1,\text{当 } x_i=c_i \text{ 时}\\0,\text{当 } x_i\neq c_i \text{ 时}\end{cases}$$

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

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

为了方便，今后记

$$x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n} = x^c$$

于是

$$f(x) = \sum_{c \in F_2^n} f(c) x^c$$

其中 $f(c)$是真值表中 c 对应的函数值. 小项表示布尔函数代数表达方式. 这种表示法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:

$$f(x) = x_1^0 x_2^0 x_3^0 x_4^0 \oplus x_1^0 x_2^0 x_3^1 x_4^0 \oplus x_1^0 x_2^1 x_3^0 x_4^0 \oplus x_1^0 x_2^1 x_3^1 x_4^0 \oplus$$
$$x_1^1 x_2^0 x_3^0 x_4^0 \oplus x_1^1 x_2^0 x_3^1 x_4^0 \oplus x_1^1 x_2^1 x_3^0 x_4^0 \oplus x_1^1 x_2^1 x_3^1 x_4^1$$

1.1.2 矩阵表示

定义 1.2 设 $f(x)$是 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.

$$S = \{\alpha \mid f(\alpha) = 1, \alpha \in GF(2)^n\}$$

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 $w_i = (c_{i1}, \cdots, c_{in})$, $1 \leqslant i \leqslant w$,则称 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,于是可将布尔函数的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:

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

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

$$(-1)^{f(x)}=\frac{1}{2^n}\sum_{\omega\in F_2^n}W_f(\omega)(-1)^{x\cdot\omega}$$

从上面的两个式子可以看出,函数 f 的 Walsh 变换可以看成函数 $(-1)^{f(x)}$ 的离散 Fourier 变换. 如果考虑函数 f 的离散 Fourier 变换,那么

$$S_f(\omega)=\sum_{x\in F_2^n}f(x)(-1)^{x\cdot\omega} \tag{1-2}$$

相应的逆变换为

$$f(x)=\frac{1}{2^n}\sum_{\omega\in F_2^n}S_f(\omega)(-1)^{x\cdot\omega}.$$

为区分上面两种变换,式(1-1)通常被称为循环 Walsh 谱,式(1-2)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,只要用一种刻画函数即可.

定义 1.3 设 f 是一个 n 元布尔函数. 设 A_n 表示所有 n 元仿射函数构成的集合. 令

$$N_f=\min_{l\in A_n}d(f,l)=\min_{l\in A_n}wt(f\oplus l), \tag{1-3}$$

则称 N_f 为函数 f 的非线性度.

设 $l(x)=\omega_1x_1\oplus\omega_2x_2\oplus\cdots\oplus\omega_nx_n\oplus b=\omega\cdot x\oplus b$ 是一个仿射函数,其中 $b\in F_2$,那么

$$d(f,l)=2^{n-1}-\frac{1}{2}(-1)^bW_f(\omega).$$

进一步，结合式（1-3）和上式，函数 $f(x)$ 的非线性度用 Walsh 谱来描述为：

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega\in F_2^n}|W_f(\omega)| \tag{1-4}$$

众所周知，函数的 Walsh 谱满足“Parseval 恒等式”[2]：$\sum_{\omega\in F_2^n} W_f^2(\omega)=2^{2n}$. 从 Parseval 恒等式容易知道 $W_f^2(\omega)$ 的平均值为 2^n，也就是说，$\max_{\omega\in F_2^n}|W_f(\omega)|\geqslant 2^{n/2}$. 这样，立即可以得到布尔函数的一个非线性度上限：

$$N_f\leqslant 2^{n-1}-2^{n/2-1} \tag{1-5}$$

这样，根据式(1-4)可知，上式等号成立当且仅当，对每一个 $\omega\in F_2^n$，都有 $|W_f(\omega)|=2^{n/2}$. 该类函数只有当 n 为偶数时才存在，被称为 Bent 函数[3].

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 $2^{n-1}-2^{(n-1)/2}$[4-5]；当 $n>7$ 时，文献[6]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”由于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 Reed-Muller 码 $RM(r,n)$ 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，及 $RM(r,n)$ 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来刻画. 具体来说，一个 n 元布尔函数 f 的非线性度等于线性码 $RM(1,n)\cup(f\oplus RM(1,n))$ 的最小汉明距离. 另外，n 元布尔函数与 $RM(1,n)$ 之间汉明距离的最大值被称为 $RM(1,n)$ 的覆盖半径（covering radius），即布尔函数的非线性度上限.

定义 1.4 设 $\varphi_j(x), j=1,2,\cdots,n$ 是 n 元布尔函数，$\varphi(x)=(\varphi_1(x),\cdots,\varphi_n(x))$. 如果对任意的 $a\in F_2^n$，都有

$$\| \{x\in GF(2)^n \mid \varphi(x)=a\} \| =1,$$

则称 $\varphi(x)$是一个 n 元布尔置换.

定义 1.5 设 $\varphi(x)=(\varphi_1(x),\cdots,\varphi_m(x))$是一个 n 输入 m 输出的函数. 那么该函数的代数次数和非线性度分别定义为：

$$\mathrm{Deg}(\varphi)=\min\{\deg(c\cdot\varphi)\mid c\in F_2^m\backslash\{0_m\}\}$$

和

$$N_\varphi=\min\{N_{c\cdot\varphi}\mid c\in F_2^m\backslash\{0_m\}\}.$$

定义 1.6 设 $f(x)$是 F_2^n 上的 n 元布尔函数，$x_1,x_2,\cdots,x_n$ 是 F_2 上的独立的、均匀分布的随机变量，如果对任意的$(a_1,a_2,\cdots,a_m)\in F_2^m(m\leqslant n)$和 $b\in F_2$，都有

$$P(f=b,x_{i_1}=a_1,x_{i_2}=a_2,\cdots,x_{i_m}=a_m)=\frac{1}{2^m}P(f=b)$$

则称 $f(x)$与变元 $x_{i_1},x_{i_2},\cdots,x_{i_m}$ 统计无关. 如果 $f(x)$与 $x_1,x_2,\cdots,x_n$ 中任意 m 个变元的统计无关，则称 $f(x)$是 m 阶相关免疫的.

平衡的 m 阶相关免疫函数称为 m 阶弹性函数. 平衡的但没有相关免疫性的布尔函数可以看为 0 阶弹性函数.

相关免疫的概念是为了防止密码分析者对流密码进行相关攻击 Siegnthaler[7] 提出的，下面给出众所周知的 Xiao-Massey 定理[8]，它刻画了相关免疫函数的频谱特征.

定理 1.1 设 $f(x)$是 F_2^n 上的 n 元布尔函数，$\omega\in F_2^n$，$1\leqslant t\leqslant n$. $f(x)$是 t 阶弹性函数当且仅当对任意满足 $0\leqslant W_H(\omega)\leqslant t$ 的 ω，下式均成立：

$$W_f(\omega)=0$$

相关免疫记为 CI，m 阶相关免疫记为 $CI(m)$，相应函数称为 CI 函数和 $CI(m)$函数.

代数免疫度是由 Meier 等[9]引入的为了衡量一个函数抵抗代数攻击能力的一个密码学指标. 下面给出代数免疫度的概念.

定义 1.7 设 f 是 n 元布尔函数. 如果 n 元布尔函数 g 使得 $fg=0$,则称 g 为 f 的一个零化子. 记 $AN(f)=\{g(x)\in B_n \mid f(x)g(x)=0\}$为 f 的所有零化子的集合,称 $AI(f)=\min\limits_{g\in S,g\neq 0}\deg(g)$为 f 的代数免疫度,其中 $S=AN(f)\cup AN(f\oplus 1)$.

小项表示和矩阵表示的内容可参考文献[10],[11].

参考文献

[1] CARLET C. Boolean Functions for Cryptography and Error Correcting Codes[M\OL]. Cambridge: Cambridge University Press, 2010. http://www-roc. inria. fr/secret/Claude. Carlet/chap-fcts-Bool-corr. pdf.

[2] MACWILLIAMS F J, SLOANE N J A. The theory of error-correcting Codes[M]. Amsterdam, Netherlands: North-Holland, 1977.

[3] ROTHAUS O S. On "bent" functions[J]. Journal of Combinatorial Theory, Series A, 1976, 20:300-305.

[4] HELLESETH T, KLΦVE T, MyKKELVEIT J. On the covering radius of binary codes[J]. IEEE Transactions on Information Theory, 1978, 24(5): 627-628.

[5] MYKKELVEIT J. The covering radius of the [128,8] Reed-Muller code is 56[J]. IEEE Transactions on Information Theory, 1980, 26 (3): 359-362.

[6] KAVUT S, MAITRA S, YÜCEL M D. Search for Boolean functions with excellent profiles in the rotation symmetric class[J]. IEEE Transactions on Information

Theory, 2007, 53 (5): 1743-1751.

[7] SIEGENTHALER T. Correlation-immunity of nonlinear combining functions for cryptographic applications [J]. IEEE Transactions on Information Theory, 1984, 30 (5): 776-780.

[8] XIAO G, MASSEY J L. A spectral characterization of correlation-immune combining functions [J]. IEEE Transactions on Information Theory, 1988, 34 (3): 569-571.

[9] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[C]. In: Proceedings of Cryptology-EUROCRYPT 2004. Berlin, Herdelberg: Springer-Verlag, 2004: 474-491.

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

[11] 温巧燕,钮心忻,杨义先. 现代密码学中的布尔函数[M]. 北京:科学出版社, 2000.