关于旋转对称布尔函数线性结构的几点注记

高光普* 刘文芬
(信息工程大学信息工程学院 郑州 450002)

摘 要：该文研究了旋转对称布尔函数(RSBF)的线性结构特征，讨论了 RSBF 的代数次数与线性结构点之间的关系。证明了代数次数为 $n-1$ 且平衡的偶数元 RSBF 不存在非全 0 的线性结构点这个公开问题。给出了自共轭轨道的计数公式，并以此计算了以全 1 向量为其线性结构点的 RSBF 的个数。

关键词：密码学；旋转对称布尔函数；线性结构；自共轭轨道
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2012)09-2273-04
DOI: 10.3724/SP.J.1146.2012.00193

The Notes on the Linear Structures of Rotation Symmetric Boolean Functions

Gao Guang-pu Liu Wen-fen
(*Institute of Information Engineering*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: In this paper, the linear structure of Rotation Symmetric Boolean Functions (RSBF) is studied. The relationship between the degree and the existence of linear structures in RSBFs is investigated. The open problem that an n -variable RSBF being balanced and of degree $n-1$ has no linear structure except the all-zero vector is proved. A formula for enumerating the self-conjugate orbits is presented. By this formula, the number of RSBFs, which have no linear structure except all-one vectors, is obtained.

Key words: Cryptography; Rotation Symmetric Boolean Functions (RSBF); Linear structures; Self-conjugate orbits

1 引言

旋转对称布尔函数(RSBF)是密码学中一类重要的函数，最初由文献[1]在研究 Hash 算法的快速实现时提出。一个 n 元布尔函数称为 RSBF 当且仅当该函数的输入在 n 阶循环群作用下时输出保持不变。由于 RSBF 在 Hash 算法(如 MD4, MD5 和 HAVAL) 中的广泛应用，人们对其自身代数结构的性质产生了极大兴趣[2–6]。

文献[2]应用 Burnside 引理计算了 RSBF 的个数，并且给出了计算齐次 RSBF 的递归公式。基于实验结果，该文猜测不存在次数大于 2 的齐次 RS bent 函数。通过级联线性子空间，文献[3]构造了一类三次 RS bent 函数。利用轨道划分的方法，文献[4,5,7]构造了 2^m 元与 $2p$ (p 为素数)元代数免疫最优的 RSBF。但是由于自共轭轨道的计数问题还没有解决，这些方法无法构造变元个数一般的代数免疫最优的 RSBF。

由于具有非零线性结构点的布尔函数容易受到差分攻击[8]，用于密码体制的布尔函数应该避免具有线性结构点[8,9]。因此考察 RSBF 的线性结构特征既有理论意义又有应用价值。文献[6]证明了若 $f(\boldsymbol{x})$ 为 RSBF，则 $f(\boldsymbol{x}+\mathbf{1})$ 也是 RSBF，其中 $\mathbf{1}$ 为全 1 向量。且任意的代数次数为 $n-1$ 的 n 元 RSBF 不存在非全 0 和全 1 的线性结构点。该文还猜测代数次数为 $n-1$ 且平衡的偶数元 RSBF 不存在非全 0 的线性结构点。

本文在文献[6]的基础上进一步研究了 RSBF 的线性结构特征以及自共轭轨道的计数。首先，证明了文献[6]提出的公开问题，即证明了代数次数为 $n-1$ 且平衡的偶数元 RSBF 不存在非全 0 的线性结构点。其次，分析了 RSBF 轨道的性质，给出了自共轭轨道的计数公式。在此基础上计算了以全 1 向量为线性结构点的 RSBF 的个数。本文的结论为构造抗差分攻击和代数免疫最优函数提供了理论基础。

2 预备知识

记 $\mathrm{GF}^n(2)$ 为有限域 $\mathrm{GF}(2)$ 上的向量空间，B_n 为全体 n 元布尔函数 $f:\mathrm{GF}^n(2)\to\mathrm{GF}(2)$ 的集合。布尔

2012-02-29 收到，2012-05-07 改回
国家 973 计划项目(2012CB315905)资助课题
*通信作者：高光普 gaoguangpu@yahoo.com.cn

函数 f 可以用如下的多变元多项表示

$$f(\boldsymbol{x})=\mathop{\oplus}_{I\in P(N)}a_I\left(\prod_{i\in I}x_i\right)=\mathop{\oplus}_{I\in P(N)}a_I\boldsymbol{x}^I \tag{1}$$

其中 $N=\{1,2,\cdots,n\}$，$P(N)$ 为集合 N 的幂集，$a_I\in \mathrm{GF}(2)$。称式(1)为布尔函数的代数标准型(ANF)。所有形如 $\boldsymbol{w}\cdot\boldsymbol{x}+a$, $\boldsymbol{w}\in\mathrm{GF}^n(2)$, $a\in\mathrm{GF}(2)$ 的布尔函数称为仿射函数，记为 $A_n(\boldsymbol{x})$。定义 f 的代数次数 $\deg(f)=\max\{\#I,a_I\neq 0\}$。记 $\mathrm{GF}^n(2)$ 中全 0 与全 1 向量分别为 $\mathbf{0}$, $\mathbf{1}$。对任意的向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\mathrm{GF}^n(2)$，定义 $WS(x)=\{\,i:x_i=1,\ 1\le i\le n\}$ 为向量 $\boldsymbol{x}$ 的支撑集，则 $\boldsymbol{x}$ 的汉明重量 $w_H(\boldsymbol{x})=|WS(\boldsymbol{x})|$。对任意的 $I\in P(N)$，有

$$a_I=\mathop{\oplus}_{\boldsymbol{x}\in\mathrm{GF}^n(2)/WS(\boldsymbol{x})\subseteq I}f(\boldsymbol{x}) \tag{2}$$

令 f 的支撑集为 $\mathrm{supp}(f)=\{\boldsymbol{x}\in\mathrm{GF}^n(2)\,|\,f(\boldsymbol{x})=1\}$。称支撑集所含元素的个数为 $f(\boldsymbol{x})$ 的汉明重量，记为 $w_H(f)$。若 $w_H(f)=2^{n-1}$，称 $f(\boldsymbol{x})$ 是平衡的。

下面讨论 RSBF 的代数结构特征，首先给出其定义。

定义 1 设 n 为正整数，对任意的 $(x_1,x_2,\cdots,x_n)\in\mathrm{GF}^n(2)$ 和 $0\le k\le n-1$，定义 $\rho_n^k(\boldsymbol{x})=(\rho_n^k(x_1),\rho_n^k(x_2),\cdots,\rho_n^k(x_n))$，其中 $\rho_n^k(x_i)=x_{(i+k)\bmod n}$。

如果对任意的 $(x_1,x_2,\cdots,x_n)\in\mathrm{GF}^n(2)$ 都有 $f(\rho_n^k(\boldsymbol{x}))=f(\boldsymbol{x})$, $0\le k\le n-1$，则称 $f(\boldsymbol{x})$ 为 RSBF。

令 $G_n(\boldsymbol{x})=\{\rho_n^k(\boldsymbol{x})\,|\,0\le k\le n-1\}$ 表示由向量 $\boldsymbol{x}$ 生成的轨道，定义轨道的重量为向量 $\boldsymbol{x}$ 的汉明重量。$\mathrm{GF}^n(2)$ 的轨道个数记为 g_n，则 n 阶循环群 $\{\rho_n^k\,|\,0\le k\le n-1\}$ 将 $\mathrm{GF}^n(2)$ 分成了 g_n 个不相交的轨道 $G_n^j(1\le j\le g_n)$。显然 G_n^j 中元素的个数 $\#G_n^j$ 为 n 的因子。称 $\#G_n^j=n$ 的轨道为长圈；称 $\#G_n^j=d$ $(d<n,d\mid n)$ 的轨道为短圈。记 R_n 为全体 RSBF 的集合。由于当 $n\le 3$ 时，n 阶循环群退化为置换群，因此本文考察的 RSBF 的变元个数 $n>3$。

下面给出布尔函数线性结构点的定义。

定义 2 设 $f\in B_n$，向量 $\boldsymbol{\alpha}\in\mathrm{GF}^n(2)$ 称为布尔函数 f 的线性结构点当且仅当 $f(\boldsymbol{x}+\boldsymbol{\alpha})+f(\boldsymbol{x})$ 为常值。

若 $f(\boldsymbol{x}+\boldsymbol{\alpha})+f(\boldsymbol{x})\equiv 0$，则称 $\boldsymbol{\alpha}$ 为 f 的 0-类线性结构点；若 $f(\boldsymbol{x}+\boldsymbol{\alpha})+f(\boldsymbol{x})\equiv 1$，则称 $\boldsymbol{\alpha}$ 为 f 的 1-类线性结构点。显然对任意的布尔函数 f，向量 $\mathbf{0}$ 都是其 0-类线性结构点，称其为平凡的线性结构点。由于任意的向量 $\boldsymbol{\alpha}$ 都是仿射函数的线性结构点，因此除特别声明外，以下讨论的 RSBF 都是非线性的。

3 旋转对称函数的线性结构

文献[6]之定理 5 证明了任意的代数次数为 $n-1$ 的 n 元 RSBF f 都不存在非 $\mathbf{0},\mathbf{1}$ 的线性结构点。作者还推测代数次数为 $n-1$ 且平衡的偶数元 RSBF 只存在平凡的线性结构点。本节将证明该结论是正确的。

定理 1 设 n 是偶数，$f\in B_n$ 为代数次数为 $n-1$ 且平衡的 RSBF，则 f 不存在非平凡的线性结构点。

证明 设 n 是偶数，f 为代数次数为 $n-1$ 且平衡的偶数元 RSBF。一方面，由 RSBF 的性质可知，在 f 的代数标准型中 $n-1$ 次项全部出现。故不妨令 $I=\{2,3,\cdots,n\}$，由式(2)可知

$$a_I=\mathop{\oplus}_{WS(\boldsymbol{x})\subseteq I}f(\boldsymbol{x})=1 \tag{3}$$

令 $M=\#\{\boldsymbol{x}\in\mathrm{GF}^n(2)\,|\,WS(\boldsymbol{x})\subseteq I,f(\boldsymbol{x})=1\}$，由式(3)可知 M 为奇数。另一方面，由文献[6]定理 5 可知，f 不存在非 $\mathbf{0},\mathbf{1}$ 的线性结构点。注意到 f 的变元个数为偶数。因此，若向量 $\mathbf{1}$ 是 f 的线性结构点必有 $f(\boldsymbol{x})+f(\boldsymbol{x}+\mathbf{1})\equiv 0$。由

$$\begin{aligned}\mathrm{supp}(f)=&\{\boldsymbol{x}\in\mathrm{GF}^n(2)\,|\,WS(\boldsymbol{x})\subseteq I,f(\boldsymbol{x})=1\}\\&\cup\{\boldsymbol{x}\in\mathrm{GF}^n(2)\,|\,WS(\boldsymbol{x})\supseteq N\setminus I,f(\boldsymbol{x})=1\}\end{aligned}$$

可得 $2M=w_H(f)=2^{n-1}$，即 $M=2^{n-2}$。这与 M 为奇数矛盾。这说明 f 不存在非 $\mathbf{0}$ 的线性结构点，结论成立。 证毕

注：由于不存在非 $\mathbf{0}$ 线性结构点的布尔函数都是非退化的，因此代数次数 $n-1$ 且平衡的偶数元 RSBF 都是非退化的[10]。值得注意的是，根据 Sigenthaler 不等式可知，代数次数 $n-1$ 的且平衡的偶数元 RSBF 不具有相关免疫性。如何寻找或构造代数次数较高、非退化且具有相关免疫性的 RSBF 是一个值得研究的问题。

文献[6]指出，如果 f 为 RSBF，那么 $f(\boldsymbol{x}+\mathbf{1})$ 也是 RSBF。下面我们讨论以向量 $\mathbf{1}$ 为线性结构点的 RSBF 的个数。记 $R_n(0)=\{f\in B_n\,|\,f(\boldsymbol{x})+f(\boldsymbol{x}+\mathbf{1})=0\}$，$R_n(1)=\{f\in B_n\,|\,f(\boldsymbol{x})+f(\boldsymbol{x}+\mathbf{1})=1\}$。当 n 是奇数时，有定理 2 成立。

定理 2 若 n 是奇数，则 $\#R_n(0)=\#R_n(1)=2^{g_n/2}$。

证明 若 n 是奇数，则对任意的向量 $\boldsymbol{x}\in\mathrm{GF}^n(2)$，$G_n(\boldsymbol{x})\cap G_n(\boldsymbol{x}+\mathbf{1})=\varnothing$。因此，$f\in R_n(0)$ 当且仅当 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+\mathbf{1})$ 同时属于或同时不属于 f 的支撑集；$f\in R_n(1)$ 当且仅当 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+\mathbf{1})$ 恰有一个属于 f 的支撑集。由此可知 $\#R_n(0)=\#R_n(1)=2^{g_n/2}$。 证毕

当 n 是偶数时，必然存在某个汉明重量为 $n/2$ 的向量使得 $G_n(\boldsymbol{x})=G_n(\boldsymbol{x}+\mathbf{1})$。我们称这样的轨道为自共轭轨道。由于偶数元 RSBF 在自共轭轨道上取值相等，因此偶数元 RSBF 不存在 1-类线性结构

点，即 $\#R_n(1)=0$。同时可知，若要得到 $R_n(0)$ 的计数需要计算所有自共轭轨道的个数。令 s_n 表示所有自共轭轨道的个数，$s_n(r)$ 表示所有圈长为 r 的自共轭轨道的个数($r \mid n$)。显然有：

命题 1　设 n 为偶数，则 $\mathrm{GF}^n(2)$ 中自共轭轨道的个数 $s_n=\sum_{r\mid n} s_n(r)$。

由命题 1 可知，如果能够给出 $s_n(r)$ 的计数公式，那么 s_n 的计数公式也就确定了。下面，应用递归法给出 $s_n(r)$ 的计数公式。

定理 3　设 $r \mid n$，则 $\mathrm{GF}^n(2)$ 中圈长为 r 的所有自共轭轨道的个数为

$$s_n(r)=\frac{1}{r}\left(2^{r/2}-\sum_{t<r/2,\ t\nmid r/2} t s_n(t)\right) \tag{4}$$

证明　令 $S_n(r)=\{\boldsymbol{x}\in \mathrm{GF}^n(2) \mid G_n(\boldsymbol{x})=G_n(\boldsymbol{x}+\mathbf{1}), \#G_n(\boldsymbol{x})=r\}$ 为所有圈长为 r 的自共轭轨道的集合。对任意的 $\boldsymbol{x}\in S_n(r)$，因为 $\boldsymbol{x}$ 是以 r 为周期的向量，所以 $\boldsymbol{x}$ 能够表示成 n/r 个 $\boldsymbol{b}$ 的级联，即 $\boldsymbol{x}=(\boldsymbol{b},\boldsymbol{b},\cdots,\boldsymbol{b})$，其中 $\boldsymbol{b}=[x_1,\cdots,x_r]$。由于 $G_n(\boldsymbol{x})=G_n(\boldsymbol{x}+\mathbf{1})$，所以一定存在某个最小的整数 k，$0<k<n$，使得 $\rho_n^k(\boldsymbol{x})=\boldsymbol{x}+\mathbf{1}$，故有 $\rho_n^{2k}(\boldsymbol{x})=\boldsymbol{x}$。由 k 的最小性可知 $2k=r$。这说明 r 是偶数，于是 $\boldsymbol{b}$ 可以表示为：$\boldsymbol{b}=[x_1,\cdots,x_{r/2},x_1+1,\cdots,x_{r/2}+1]$。反之，对任意具有上述形式的向量 $\boldsymbol{x}=(x_1,\cdots,x_{r/2},x_1+1,\cdots,x_{r/2}+1,\cdots)$，必有 $\#G_n(\boldsymbol{x})\nmid r/2$。注意到这样的向量共有 $2^{r/2}$ 个，因此圈长为 r 的所有自共轭轨道的个数为

$$s_n(r)=\frac{1}{r}\left(2^{r/2}-\sum_{t<r/2,\ t\nmid r/2} t s_n(t)\right)$$

证毕

注：若 $n=2^d$，则 $\mathrm{GF}^n(2)$ 中任意轨道的长度都是 2 的方幂。由式(4)可知，对任意的 $1\le q\le d$，周期为 2^q 的共轭轨道的个数为 $s_n(2^q)=2^{2^{q-1}-q}$。此即为文献[6]命题 3 的结论。

下面以 $n=12$ 为例，计算 $\mathrm{GF}^{12}(2)$ 中自共轭轨道的个数。

例 1　令 $n=12$，$\mathrm{GF}^{12}(2)$ 中自共轭轨道可能的长度为 2, 4, 6, 12。显然 $s_{12}(2)=1$，$s_{12}(4)=1$，则 $s_{12}(6)=(1/6)(2^3-2s_{12}(2))=1$，$s_{12}(12)=(1/12)(2^6-4s_{12}(4))=5$。因此，$\mathrm{GF}^{12}(2)$ 中自共轭轨道的个数 $s_{12}=8$。当 $n=2,4,\cdots,12$ 时，通过计算机搜索，表 1 给出了 s_n 的取值。

下面利用定理 3 计算不存在 1-类线性结构点的偶数元 RSBF 的个数。

表 1　$n=2,4,\cdots,12$ 时，s_n 的取值

n	$s_n(2)$	$s_n(4)$	$s_n(6)$	$s_n(8)$	$s_n(10)$	$s_n(12)$	s_n
4	1	1	–	–	–	–	2
6	1	–	1	–	–	–	2
8	1	1	–	2	–	–	4
10	1	–	–	–	3	–	4
12	1	1	1	–	–	5	8

定理 4　若 n 是偶数，则 $\#R_n(0)=2^{(g_n+s_n)/2}$，$\#R_n(1)=0$。

证明　若 n 是偶数，则存在某个重量为 $n/2$ 的向量 $\boldsymbol{x}$ 使得 $G_n(\boldsymbol{x})=G_n(\boldsymbol{x}+\mathbf{1})$，故 $\#R_n(1)=0$。由定理 3 可知，重量为 $n/2$ 的自共轭轨道的个数为 s_n，因此非共轭的轨道的个数为 g_n-s_n。且若 $G_n(\boldsymbol{x})$ 是非共轭的，则有 $G_n(\boldsymbol{x})\bigcap G_n(\boldsymbol{x}+\underline{\mathbf{1}})=\varnothing$。再根据 $f\in R_n(0)$ 当且仅当 $G_n(\boldsymbol{x})$ 与 $G_n(\boldsymbol{x}+\mathbf{1})$ 同时属于或同时不属于 f 的支撑集可知，以向量 $\mathbf{1}$ 为 0-类线性结构点的偶数元 RSBF 的个数为

$$\#R_n(0)=2^{(g_n-s_n)/2}2^{s_n}=2^{(g_n+s_n)/2}$$

证毕

4　结束语

本文主要研究了 RSBF 的线性结构特征和自共轭轨道的性质。首先证明了文献[6]关于代数次数为 $n-1$ 且平衡的偶数元 RSBF 不存在非 0 的线性结构点这个公开问题。其次，给出了自共轭轨道的计数公式，由此得到了以全 1 向量为其线性结构点的 RSBF 的个数。需要注意的是，文献[4,5,7]通过划分自共轭轨道构造了 2^d 元与 $2p$ 元代数免疫最优且平衡的 RSBF，其中 $d>2$ 为正整数，p 为奇素数。如何利用本文关于自共轭轨道的计数公式构造变元个数更为一般的代数免疫最优且平衡的偶数元 RSBF 值得进一步研究。

参 考 文 献

[1] Pieprzyk J and Qu C X. Fast Hashing and rotation symmetric functions[J]. *Journal of Universal Computer Science*, 1999, 5(1): 20–31.

[2] Sarkar P and Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties[J]. *Discrete Applied Mathematics*, 2008, 156(10): 1567–1580.

[3] Cusick T and Padgett D. A recursive formula for weights of Boolean rotation symmetric functions[J]. *Discrete Applied Mathematics*, 2012, 160, (4/5): 391–397.

[4] Fu S J, Qu L J, Li C, *et al*.. Balanced rotation symmetric Boolean functions with maximum algebraic immunity[J]. *IET Information Security*, 2011, 5(2): 93–99.

[5] Fu S J, Li C, Matsuura K, *et al*.. Balanced 2p-variable rotation symmetric Boolean functions with maximum algebraic immunity[J]. *Applied Mathematics Letters*, 2011, 24(12): 2093–2096.

[6] Elsheh E. On the linear structures of cryptographic Rotation symmetric boolean functions[C]. The 9th International Conference for Young Computer Scientists, ICYCS 2008, Zhangjiajie, China, 2008: 2085–2089.

[7] 孟强, 陈鲁生, 符方伟. 一类代数免疫度达到最优的布尔函数的构造[J]. 软件学报, 2010, 21(7): 1758–1767.
Meng Q, Chen L S, and Fu F W. Construction of Boolean functions with maximum algebraic immunity[J]. *Journal of Software*, 2010, 21(7): 1758–1767.

[8] Biham E and Shamir A. Differential cryptanalysis of feal and N-Hash[C]. Advances in Cryptology, Proc. Eurocrypt'91, 1991, LNCS 547: 1–16.

[9] Preneel B, Leekwijck W, Linden L, *et al*.. Propagation characteristics of Boolean functions[C]. Proceedings of Eurocrypt'90, 1991, LNCS 473: 161–173.

[10] 李世取, 曾本胜, 廉玉忠, 等. 密码学中的逻辑函数[M]. 北京中软电子出版社, 2003: 74–76.
Li S Q, Zeng B S, Lian Y Z, *et al*.. The Logic Functions in Cryptography[M]. Beijing Zhongruan Electric Press, 2003: 74–76.

高光普： 男，1984 年生，博士生，研究方向为密码学中布尔函数.
刘文芬： 女，1965 年生，教授，研究方向为通信及密码学中的概率论应用.