doi:10.3969/j.issn.1000-436x.2013.03.022

旋转对称布尔函数线性结构的 2 个公开问题

赵亚群[1,2]，李旭[1]
（1. 信息工程大学 四院，河南 郑州 450002；2. 信息工程大学 数学工程与先进计算国家重点实验室，河南 郑州 450002）

摘 要：证明了代数次数为 $n-1$ 的偶变元平衡旋转对称布尔函数不存在非零线性结构这个公开问题，给出了代数次数为 $n-2$ 的奇变元旋转对称布尔函数不存在非零线性结构这个公开问题成立的充分条件和不成立的必要条件。

关键词：布尔函数；旋转对称；线性结构；代数次数
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2013)03-0171-04

Two open problems about the liner structure of rotation symmetric Boolean functions

ZHAO Ya-qun[1,2], LI Xu[1]
(1. The Fourth Institute, Information Engineering University, Zhengzhou 450002, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450002, China)

Abstract: One open problem that the balanced rotation symmetric Boolean functions with degree $n-1$ on even number of variables have no non-zero linear structure was proved. A sufficient and a necessary condition were respectively given when another open problem that the rotation symmetric ean functions with degree $n-2$ on odd number of variables have no non-zero linear structure succeed or not.

Key words: Boolean functions; rotation symmetric; linear structure; algebraic degree

1 引言

旋转对称布尔函数(RSBF, rotation symmetric boolean function)是一类具有特殊代数结构的布尔函数，由 Pieprzyk 和 Qu[1]最先提出并应用于散列算法中。由于其良好的结构特性和在散列算法中广泛的应用，RSBF 受到了极大的关注，RSBF 的密码学性质一直是研究的热点问题[2~6]。其中，线性结构是度量布尔函数安全性的一个重要指标，具有非零线性结构的布尔函数是密码学中的一类“弱函数”。因此，研究 RSBF 的线性结构对于密码算法的安全性设计是很有意义的。

Elsheh 在文献[7]中系统地研究了 RSBF 的线性结构，证明了 $n-1$ 次 RSBF 不存在除全 0 和全 1 的线性结构，并提出了 2 个公开问题：对任意的 $n>3$，$n-1$ 次偶变元平衡 RSBF 和 $n-2$ 次奇变元 RSBF 均不存在非零线性结构。当 $n\leq 10$ 时，Elsheh 通过计算机验证了这 2 个公开问题的正确性。在此基础上，本文进一步研究了 RSBF 的线性结构，完全证明了公开问题 1，给出了公开问题 2 成立的充分条件以及不成立的必要条件。

2 预备知识

设 n 是任一正整数，记二元域 $F_2=\{0,1\}$，以 F_2^n 表示 n 个 F_2 的笛卡尔积，$F_2^n=\{0,1\}^n$，称 $F_2^n\to F_2$ 的任一映射 $f(\cdot)$ 为 n 个变元的(F_2^n 上的)布尔函数。即若记 $x=(x_1,x_2,\mathrm{L},x_n)\in F_2^n$，则有 $f(x)=f(x_1,x_2,\mathrm{L},x_n)\in F_2$。记 B_n 为所有 n 变元布尔函数构成的集合。

任意一个 B_n 中的布尔函数 $f(x)$ 都可以唯一地

收稿日期：2011-11-20；修回日期：2013-01-08
基金项目：国家自然科学基金资助项目(61072046)
Foundation Item: The National Natural Science Foundation of China (61072046)

表示成 F_2 上的多变元多项式。

$$f(x_1,x_2,\L,x_n)=\sum_{I\subseteq\{1,2,\L,n\}}a_I\prod_{i\in I}x_i \tag{1}$$

其中，$a_I\in F_2$，式(1)称为 $f(x)$ 的代数正规型（ANF, algebraic normal form）。定义布尔函数 $f(x)$ 的代数次数 $\deg f$ 为ANF中系数非零次数最高的单项式次数。若 $\deg f\le 1$，则称 $f(x)$ 为仿射函数，A_n 表示 B_n 中的全体仿射函数。定义 $f(x)\in B_n$ 的支撑集 $Supp(f)=\{x\in F_2^n\,|\,f(x)=1\}$，那么 $f(x)$ 的汉明重量 $wt(f)=|Supp(f)|$（$|M|$ 表示集合 M 的元素个数）。若 $wt(f)=2^{n-1}$，则称 $f(x)$ 为平衡函数。对任意的 $x=(x_1,x_2,\L,x_n)\in F_2^n$，定义 x 的支撑集为 $WS(x)=\{i\,|\,x_i=1,1\le i\le n\}$，那么 x 的汉明重量 $wt(x)=|WS(x)|$。对任意的 $I\subseteq\{1,2,\L,n\}$，有

$$a_I=\bigoplus_{x\in F_2^n,WS(x)\subseteq I}f(x) \tag{2}$$

定义 1 设 w、$x\in F_2^n$，x 和 w 的点积定义为 $wx=w_1x_1\oplus w_2x_2\oplus\L\oplus w_nx_n$。设 $f(x)\in B_n$，称 $S_{(f)}(w)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus wx}$ 为 $f(x)$ 的 Walsh 变换，集合 $\{S_{(f)}(w)\,|\,w\in F_2^n\}$ 称为 $f(x)$ 的 Walsh 循环谱。

关于弹性(相关免疫)函数的谱特征有如下定义。

引理 1[8] 设 $f(x)\in B_n$，$f(x)$ 具有 m 阶弹性(相关免疫性)，当且仅当对任意的 $w\in F_2^n$ 且 $0\le wt(w)\le m$ ($1\le wt(w)\le m$)时，有 $S_{(f)}(w)=0$。

为了叙述方便，本文将 F_2^n 中全0和全1向量分别记为 ***0*** 和 ***1***。

定义 2 设 $f(x)\in B_n$，$s\in F_2^n$，记 $D_sf(x)=f(x)\oplus f(x\oplus s)$。若对所有的 $x\in F_2^n$，都有 $D_sf(x)=D_sf(\boldsymbol{0})=$常数(0或1)，则称 s 为 $f(x)$ 的一个线性结构。

记 $U_f=\{s\,|\,$对所有的$x\in F_2^n$，有$D_sf(x)=$常数$\}$，$U_f^{(0)}=\{s\,|\,$对所有的$x\in F_2^n$，有$D_sf(x)=0\}$，$U_f^{(1)}=\{s\,|\,$对所有的$x\in F_2^n$，有$D_sf(x)=1\}$。可见，$U_f=U_f^{(0)}\cup U_f^{(1)}$，$\boldsymbol{0}\in U_f^{(0)}$，$U_f$ 和 $U_f^{(0)}$ 均为 F_2^n 的线性子空间。若 $s\in U_f$ 且 $s\ne\boldsymbol{0}$，则称 s 为 $f(x)$ 的一个非零线性结构。

定义 3 设 n 为正整数，对任意的 $x=(x_1,x_2,\L,x_n)\in F_2^n$ 和 $0\le k\le n-1$，定义 $?_n^k(x)=(?_n^k(x_1),?_n^k(x_2),\L,?_n^k(x_n))$，其中，

$$?_n^k(x_i)=\begin{cases}x_{i+k}, & i+k\le n\\ x_{i+k-n}, & i+k>n\end{cases}$$

如果对任意的 $x=(x_1,x_2,\L,x_n)\in F_2^n$ 都有 $f(?_n^k(x))=f(x)$，$0\le k\le n-1$，则称 $f(x)$ 为 RSBF。令 $G_n(x)=\{?_n^k(x)\,|\,0\le k\le n-1\}$ 表示在该循环群作用下由向量 x 生成的轨道。

3 2个关于RSBF线性结构的公开问题

首先，给出文献[7]中关于RSBF的一些基本性质。

引理 2 设 $f(x)\in B_n$ 为RSBF，则有如下描述。

1) 若 $a\in F_2^n$ 为 $f(x)$ 的一个线性结构，那么对任意的 $ß\in G_n(a)$，$ß$ 仍为 $f(x)$ 的线性结构。

2) 若 $\deg f=n$，那么 $f(x)$ 不存在非零线性结构。

3) 若 $\deg f=n-1$，那么 $f(x)$ 不存在除 ***0*** 和 ***1*** 以外的线性结构。

在文献[7]的最后，Elsheh通过对 n 元RSBF的考察，提出了2个关于RSBF线性结构的公开问题：对任意的 $n>3$，1) 代数次数为 $n-1$ 的偶变元平衡RSBF不存在非零线性结构；2) 代数次数为 $n-2$ 的奇变元RSBF不存在非零线性结构。

注：由于任意向量均为线性布尔函数的线性结构，因此，在讨论布尔函数的线性结构时，所涉及的布尔函数均默认为非线性布尔函数。故文献[7]提出的2个公开问题中，有 $n>3$ 的条件。

首先，给出公开问题1的证明。

引理 3[9] 设 $f(x)\in B_n$，$s\in F_2^n$，那么 $s\in U_f^{(i)}$ ($i=0$ 或 1)的充分必要条件是对任意的 $w\in F_2^n$ 且 $ws=i\oplus 1$，都有 $S_{(f)}(w)=0$。

引理 4[9] 设 $f(x)\in B_n$ 具有 m 阶相关免疫性，$\deg f=k$，则 $k+m\le n$。若设 $f(x)$ 是平衡的，且 $1\le m\le n-2$，则 $k+m\le n-1$。

定理1 设 $f(x)\in B_n$ 为RSBF(n 为偶数且 $n>3$)，若 $\deg f=n-1$，$wt(f)=2^{n-1}$，那么 $f(x)$ 不存在非零线性结构。

证明 根据引理2中的3)，只需证明 ***1*** 不是 $f(x)$ 的线性结构。

设 $b=(1,0,1,0,\L,1,0)\in F_2^n$，由 $f(x)\in B_n$ 为RSBF，n 为偶数知：$b\oplus\boldsymbol{1}=(0,1,0,\L,1,0,1)\in G_n(b)$，$f(b)=f(b\oplus\boldsymbol{1})$，即 $f(b)\oplus f(b\oplus\boldsymbol{1})=0$。假设 ***1*** 是 $f(x)$ 的线性结构，那么 $\boldsymbol{1}\in U_f^{(0)}$。对任意的 $w\in F_2^n$ 且

$wt(w)=1$，有 $w\cdot \mathbf{1}=1$。由引理 3 可知，对任意的 $w\in F_2^n$ 且 $wt(w)=1$，$S_{(f)}(w)=0$。又 $wt(f)=2^{n-1}$，那么 $f(x)$ 为 1 阶弹性函数。根据引理 4 可知，$\deg f+1=n-1+1=n\le n-1$ 矛盾，故假设不成立。定理得证。

在讨论公开问题 2 之前，先引入 FP(fast point) 的概念及其部分性质。

定义 4[10]　设 $f(x)\in B_n$，$c\in F_2^n$，若 $\deg(D_c f)<\deg f-1$，则称 c 为 $f(x)$ 的一个 FP。

可见，非线性布尔函数 $f(x)$ 的任一线性结构均为 $f(x)$ 的一个 FP。若 $c=\mathbf{0}$，则称 c 为 $f(x)$ 的平凡 FP；否则，称 c 为 $f(x)$ 的非平凡 FP。$f(x)$ 的全体 FP 构成 F_2^n 上的一个线性子空间，也就是说，若 a、$ß\in F_2^n$ 为 $f(x)\in B_n$ 的 2 个 FP，那么 $a\oplus ß$ 仍为 $f(x)$ 的 FP。

引理 5[10]　设 $f(x)\in B_n$ $(n\ge 3)$，$f(x)$ 的 ANF 中只含有代数次数为 $n-2$ 的单项式，记其单项式 $\prod_{t=1}^{n}x_t\Big/x_ix_j$ 的系数为 $r_{i,j}$（或 $r_{j,i}$），$F=\{f(x)\mid$ 存在 $c\in F_2^n\setminus\{\mathbf{0}\}$，使 $\deg(D_c f)<\deg(f)-1$，$f(x)\in B_n$ 且只含有 $n-2$ 次项$\}$。对任意的 $f(x)\in F$，$f(x)$ 有且只有 3 个非平凡 FP，且其中任意的 2 个非平凡 FP(设为 c、$c'\in F_2^n$)满足：

$$c_ic'_j\oplus c_jc'_i=r_{i,j},\quad 1\le i<j\le n \tag{3}$$

注：下文中出现的 $r_{i,j}$ 均表示 $n-2$ 次单项式 $\prod_{t=1}^{n}x_t\Big/x_ix_j$ 的系数。

定理 2　设 $f(x)\in B_n$，$\deg f=k$ $(k>1)$，令 $f(x)=g(x)\oplus h(x)$，其中，$g(x)$ 为 $f(x)$ 中所有代数次数为 k 的单项式之和，那么 $f(x)$ 的任意非零线性结构均为 $g(x)$ 的非平凡 FP。

证明　$\deg f=\deg g=k$，$\deg h\le k-1$。易知，对任意的 $a\in F_2^n\setminus\{\mathbf{0}\}$，有

$$\begin{cases}D_af=D_ag\oplus D_ah\\ \deg(D_af)\le\deg f-1=k-1\\ \deg(D_ag)\le\deg g-1=k-1\\ \deg(D_ah)\le\deg h-1\le k-2\end{cases} \tag{4}$$

若 $a\in F_2^n\setminus\{\mathbf{0}\}$ 为 $f(x)$ 的线性结构，那么 $D_af=D_ag\oplus D_ah=$ 常数，由式(4)可知 $\deg(D_ag)=\deg(D_ah)\le k-2$，即 $a\in F_2^n\setminus\{\mathbf{0}\}$ 为 $g(x)$ 的一个非平凡 FP。证毕。

设 $f(x)\in B_n$ 为 RSBF，$\deg f=n-2$，令 $f(x)=g(x)\oplus h(x)$，其中，$g(x)$ 为 $f(x)$ 中所有代数次数为 n-2 的单项式之和，那么 $g(x)$ 和 $h(x)$ 均为 RSBF，且 $\deg g=n-2$，$\deg h\le n-3$。

注：下文中出现的 $g(x)$、$h(x)$ 和 $f(x)$ 均具有如上关系。

定理 3　设 $f(x)\in B_n$ 为 RSBF(n 为奇数且 $n>3$)，若 $\deg f=n-2$，那么：

1) 当 $3\nmid n$ 时，$f(x)$ 不存在非零线性结构；

2) 当 $3\mid n$ 时，若 $f(x)$ 存在非零线性结构 $a\in F_2^n$，必有 $a\in G_n(0,1,1,0,1,1,\cdots,0,1,1)$，且有：

$$r_{i,j}=\begin{cases}0, & (j-i)\equiv 0\bmod 3\\ 1, & \text{其他}\end{cases}\quad(1\le i<j\le n)$$

证明　首先，证明 $\mathbf{1}$ 不是 $f(x)$ 的线性结构。$g(x)$ 为只含有代数次数为 $n-2$ 的单项式的 RSBF，不妨设 $n-2$ 次项 $\prod_{t=1}^{n}x_t\Big/x_1x_i$ 出现，又 n 为奇数，$\gcd(n,n-2)=1$，那么 $n-2$ 次项 $\prod_{t=1}^{n}x_t\Big/x_{1+j}x_{i+j}$ $(0\le j\le n-1)$ 均出现，即 $r_{1+j,i+j}=1$ $(0\le j\le n-1)$。

注：在不引起混淆的情况下，若 $i+j>n$，笔者仍然用 $i+j$ 表示 $(i+j)\bmod n$。

假设 $\mathbf{1}$ 是 $f(x)$ 的线性结构，由定理 2 可知，$\mathbf{1}$ 是 $g(x)$ 的一个非平凡 FP。由引理 5 可知 $g(x)$ 存在其他 2 个非平凡 FP，设其中的一个为 $c\in F_2^n$，根据式(3)有

$$c_{1+j}\oplus c_{i+j}=1,\quad 0\le j\le n-1 \tag{5}$$

由 n 为奇数可知，$\oplus_{j=0}^{n-1}(c_{1+j}\oplus c_{i+j})=1$。又由于 $\oplus_{j=0}^{n-1}(c_{1+j}\oplus c_{i+j})=0$，矛盾。故 $\mathbf{1}$ 不是 $f(x)$ 的线性结构。

假设 $a\in F_2^n\setminus\{\mathbf{0},\mathbf{1}\}$ 是 $f(x)$ 的线性结构，由引理 1 中的 1)可知，任意的 $ß\in G_n(a)$ 均为 $f(x)$ 的线性结构，由定理 2 可知，任意的 $ß\in G_n(a)$ 均为 $g(x)$ 的非平凡 FP。根据引理 5，若 $g(x)$ 存在非平凡 FP，那么 $g(x)$ 有且只有 3 个非平凡 FP，可得 $|G_n(a)|\le 3$。又 $|G_n(a)|$ 为 n 的因子(n 为奇数)，且当 $a\in F_2^n\setminus\{\mathbf{0},\mathbf{1}\}$ 时，$|G_n(a)|>1$，那么 $|G_n(a)|\ge 3$。从而 $|G_n(a)|=3$。

当 $3\nmid n$ 时，不存在 $a\in F_2^n\setminus\{\mathbf{0},\mathbf{1}\}$ 使得 $|G_n(a)|=3$，

那么 $a \in F_2^n \setminus \{\mathbf{0},\mathbf{1}\}$ 不是 $f(x)$ 的线性结构。此时，$f(x)$ 不存在非零线性结构。

当 $3 \mid n$ 时，设 $n = 3k$ (k 为奇数)，记 $(a_1, a_2, a_3, a_1, a_2, a_3, \cdots, a_1, a_2, a_3) = (a_1, a_2, a_3)_k \in F_2^n$。若 $a \in F_2^n \setminus \{\mathbf{0},\mathbf{1}\}$ 是 $f(x)$ 的线性结构，那么必有 $a \in G_n((0,1,1)_k) = \{(0,1,1)_k, (1,0,1)_k, (1,1,0)_k\}$。事实上，笔者知道 $\left|G_n(a)\right| = 3$，那么 $a \in G_n((0,0,1)_k)$ 或 $G_n((0,1,1)_k)$。若 $a \in G_n((0,0,1)_k) = \{(0,0,1)_k, (0,1,0)_k, (1,0,0)_k\}$，有 $(0,0,1)_k \oplus (0,1,0)_k \oplus (1,0,0)_k = \mathbf{1}$ 仍为 $g(x)$ 的非平凡 FP 矛盾。可知，$a \in G_n((1,0,0)_k)$ 不是 $f(x)$ 的线性结构。

若 $a \in G_n((0,1,1)_k)$ 为 $f(x)$ 的线性结构，那么 $G_n((0,1,1)_k)$ 为 $g(x)$ 的非平凡 FP。根据式(3)可得：$f(x)$ 中代数次数为 $n-2$ 的单项式的系数满足下式

$$r_{i,j} = \begin{cases} 0, & (j-i) \equiv 0 \bmod 3 \\ 1, & \text{其他} \end{cases} \quad (1 \le i < j \le n)$$

4 结束语

本文利用了 FP 的一些性质，讨论了文献[7]提出的 2 个关于 RSBF 线性结构的 2 个公开问题。非线性布尔函数的线性结构必定为其 FP，但布尔函数的非平凡 FP 不一定是其非零线性结构。讨论线性结构和 FP 之间的关系以及对公开问题 2 的完全证明将是下一步需要进行的工作。

参考文献：

[1] PIEPRZYK J, QU C. Fast hashing and rotation-symmetric functions[J]. Journal of Universal Computer Science, 1999, 5(1):20-31.

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

[3] STANICA P, MAITRA S. Construction of rotation symmetri lean functions with optimal algebraic immunity[J]. Computer Systems, 2009, 12(3):267-284.

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

[5] STANICA P, MAITRA S. Results on rotation symmetric bent and correlation immune Boolean functions[A]. Fast Software Encryption Workshop (FSE 2004)[C]. Delhi, India, 2004. 161-177.

[6] MAXIMOV A, HELL M, MAITRA S. Plateaued rotation symmetric Boolean functions on odd number of variables[A]. Proceedings of the First Workshop on Boolean Functions: Cryptography and Applications[C]. Rouen, France, 2005.

[7] ELSHEH E. On the linear structures of cryptographic rotation symmetric Boolean functions[A]. Proceedings of the 9th International Conference for Young Computer Scientists(ICYCS '08)[C]. Zhangjiajie, China, 2008. 2085-2089.

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

[9] **李世取, 曾本胜, 廉玉忠等. 密码学中的逻辑函数**[M]. **北京: 北京中软电子出版社**, 2003.
LI S Q, ZENG B S, LIAN Y Z, *et al*. Logical Functions in Cryptography[M]. Beijing: China National Computer Software and Technology Service Corporation Press, 2003.

[10] DUAN M, LAI X, YANG M, *et al*. Distinguishing properties of higher order derivatives of Boolean functions[EB/OL]. http://eprint.iacr.org/2010/417, 2011.

作者简介：

赵亚群（1961-），女，江苏淮安人，博士，信息工程大学教授、硕士生导师，主要研究方向为密码基础理论及概率统计应用。

李旭（1986-），男，河北定州人，信息工程大学硕士生，主要研究方向为密码基础理论及概率统计应用。