偶变元 MAI 旋转对称布尔函数*

董德帅[1]，李 超[1]，屈龙江[1]，付绍静[2]
（1. 国防科技大学 理学院，湖南 长沙 410073；
2. 国防科技大学 计算机学院，湖南 长沙 410073）

摘 要：代数免疫度是布尔函数的一个重要密码学指标。给出了具有最大代数免疫度的偶数元旋转对称布尔函数的两种构造方法。进一步地，研究了特殊情形时所构造的旋转对称布尔函数的非线性度，当 $n \geq 18$ 时，构造 3 得到的 MAI 旋转对称布尔函数的非线性度优于已知构造的偶数元 MAI 旋转对称布尔函数的非线性度。

关键词：布尔函数；旋转对称对布尔函数；代数免疫度；非线性度
中图分类号：TN918；TP309 **文献标志码**：A **文章编号**：1011－2486(2012)04－0085－05

Rotation symmetric Boolean functions in even-variable with maximum algebraic immunity

DONG Deshuai[1], *LI Chao*[1], *QU Longjiang*[1], *FU Shaojing*[2]
(1. College of Science, National University of Defense Technology, Changsha 410073, China;
2. College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: Algebraic immunity has been considered as one of significant properties for Boolean functions. Two constructions of rotation symmetric Boolean functions (RSBFs) in even-variable with maximum algebraic immunity (MAI) were proposed. Furthermore, the nonlinearity of constructed RSBFs were investigated under special cases of Construction 2. When $n \geq 18$, the constructed MAI RSBFs by using Construction 3 have higher nonlinearity than that of all known MAI RSBFs in even-variable.

Key words: Boolean functions; rotation symmetric Boolean functions; algebraic immunity; nonlinearity

近年来，代数攻击引起了国内外密码学者的关注，代数攻击的基本思想源于 Shannon：他认为一个密码算法可以表示为一个大的多变元多项式方程组，求解这个方程组就可以解得密钥。更准确说，攻击者把一个加密变换表示为一个大的多变元多项式方程组，然后求解这个方程组来获得密钥。在 2003 年的欧密会上，Courtois 等针对流密码系统中使用的前馈函数或非线性组合函数等，提出了代数攻击的方法[1]。通过分析使得代数攻击有效的条件，可以发现，代数攻击的关键是找到布尔函数 f 或者 $1 \oplus f$ 的低次零化子。为了抵抗代数攻击，Miller 等于 2004 年首先提出了布尔函数的代数免疫度的概念[2]，并证明了对任意 n 元布尔函数 f，都有 $AI(f) \leqslant \lceil n/2 \rceil$，若上述等号成立，则称 n 元布尔函数 f 具有最大代数免疫度，即为 MAI 函数。由于布尔函数达到 MAI，则其抵抗一般代数攻击的能力也就最强。因此，具有最大代数免疫度 $\lceil n/2 \rceil$ 的布尔函数的构造就引起了人们的关注，得到了众多研究[6－12]。

旋转对称布尔函数作为一类特殊的布尔函数，在密码学中有着广泛的应用。因此，如何构造 MAI 旋转对称布尔函数就成为一个值得研究的问题。文献[3－5]相继给出了 MAI 旋转对称布尔函数的构造方法，其中文献[5]构造出的偶数元 MAI 旋转对称布尔函数在上述构造中具有最好的非线性度。本文给出了偶数元 MAI 旋转对称布尔函数的两种构造方法，并研究了特殊情形下所得到的 MAI 函数的非线性度。

1 预备知识

设 F_2^n 是 F_2 上的 n 维向量空间，一个 n 元布尔函数 $f(x)$ 是从 F_2^n 到 F_2 上的一个映射。f 可以唯一表示为：

$$f(x) = \sum_{I \subseteq \{1,\cdots,n\}} a_I \prod_{i \in I} x_i \ (a_I \in F_2)$$

* **收稿日期**：2012－01－10
基金项目：国家自然科学基金资助项目(61070215, 61103192)
作者简介：董德帅(1984—)，男，河南原阳人，博士研究生，E-mail：dds3435@163.com；
李超(通信作者)，男，博士，教授，博士生导师，E-mail：lichao_nudt@sina.com

f 的这种表示形式称之为其代数正规型。其代数次数,记为 $\deg(f)$,定义为

$$\deg(f)=\max\{|I|:I\subseteq\{1,\cdots,n\},a_I=1\},$$

代数次数不超过 1 的布尔函数称为仿射函数。记 B_n 为全体 n 元布尔函数的集合,A_n 为全体 n 元仿射布尔函数的集合。

n 元布尔函数 f 的支撑集定义为

$$\mathrm{supp}(f)=\{x\in F_2^n;f(x)=1\},$$

f 的非线性度为其与 A_n 的最小距离,即 $nl_f=\min\{d_h(f,g):g\in A_n\}$,其中

$$d_h(f,g)=|\{x\in F_2^n:f(x)\neq g(x)\}|$$

布尔函数 f 的 Walsh 变换定义为

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

$$nl_f=2^{n-1}-\frac{1}{2}\max\{|W_f(\omega)|:\omega\in F_2^n\}$$

记 f 的零化子集合为

$$Ann(f)=\{g\in B_n|f\cdot g=0\}$$

则 f 的代数免疫度 $AI(f)$ 为

$$AI(f)=\min\{\deg(g):g\neq 0,g\in Ann(f)\text{或者 }g\in Ann(f+1)\}$$

下面给出旋转对称布尔函数的定义,设 $x_i\in F_2(1\leqslant i\leqslant n)$,$0\leqslant k\leqslant n-1$,令

$$\rho_n^k(x_i)=\begin{cases}x_{i+k}, & \text{如果 } i+k\leqslant n,\\ x_{i+k-n} & \text{其他}\end{cases}$$

ρ_n^k 的定义可以推广到向量 $x=(x_1,x_2,\cdots,x_n)\in F_2^n$ 上,

$$\rho_n^k(x_1,\cdots,x_n)=(\rho_n^k(x_1),\cdots,\rho_n^k(x_n))$$

定义 1:对任意 $x=(x_1,\cdots,x_n)\in F_2^n$,$0\leqslant k\leqslant n-1$,都有

$$f(\rho_n^k(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n),$$

则称 $f(x_1,x_2,\cdots,x_n)$ 为旋转对称布尔函数。$G_n(x_1,\cdots,x_n)=\{\rho_n^k(x_1,\cdots,x_n)|0\leqslant k\leqslant n-1\}$,即 $G_n(x_1,x_2,\cdots,x_n)$ 为 $(x_1,x_2,\cdots,x_n)$ 在 $\rho_n^k(0\leqslant k\leqslant n-1)$ 作用下的轨道。显然 F_2^n 里的元素被划分为不同的轨道。设 n 为偶数,定义 n 元布尔函数 $F_n(x)$:

$$F_n(x)=\begin{cases}0, & wt(x)\leqslant\dfrac{n}{2}\\ 1, & wt(x)>\dfrac{n}{2}\end{cases}$$

文献[7]证明了 $AI(F_n)=n/2$。

引理 1[6]:设 n 是一个偶数,$a_1,\cdots,a_{\binom{n}{n/2}}$ 是 F_2^n 中所有重量等于 $n/2$ 的向量的一个排列,对于任意的 $i\in T=\{1,2,\cdots,\binom{n}{n/2}\}$,

$$A_i=\{x\in F_2^n|\mathrm{supp}(x)\subseteq\mathrm{supp}(a_i)\},$$

$$A^\circ{}_i=\{x\in F_2^n|\mathrm{supp}(a_i)\subseteq\mathrm{supp}(x)\}.$$

对于 T 的三个不相交子集 I,J,K,如果对任意 $i\in I$,存在向量 $b_i\neq a_i$,使得 $b_i\in A_i$,$[\cup_{i^*<i}A_{i^*}]$;对任意 $j\in J$,存在向量 $c_j\neq a_j$,使得 $c_j\in A^\circ{}_j$,$[\cup_{j^*<j}A^\circ{}_{j^*}]$。则满足支撑集为

$$\{x\in F_2^n|wt(x)>n/2\}\cup\{a_i|i\in J\cup K\}\cup\{b_i|i\in I\},\{c_i|i\in J\}$$

的 n 元布尔函数为 MAI 函数。

2 偶变元 MAI 旋转对称布尔函数构造

下面利用引理 1 给出一类 MAI 旋转对称布尔函数的构造,以下都假定 n 偶。设集合 $S=\{i_1,\cdots,i_s\}\subset\{1,2,\cdots,n/2-2\}$,且 S 中元素已按升序排列。对任意 $p\in S$,定义向量 $\lambda_p,v_p\in F_2^n$,满足

$$\mathrm{supp}(\lambda_p)=\{1,2,\cdots,h_p\}\cup\{n/2+u_p\}\quad(1)$$

$$\mathrm{supp}(\nu_p)=\{1,\cdots,n/2-1\}\cup\{n/2+u_p\}\quad(2)$$

其中,$2\leqslant h_p\leqslant n/2-2$,$1\leqslant u_p\leqslant h_p+1$,且若 $i_1<i_2$,则 $h_{i_1}\leqslant h_{i_2}$,$u_{i_1}<u_{i_2}<n/2-1$.

引理 2:对于任意 $p\in S$,有

1. $|G_n(\lambda_p)|=|G_n(v_p)|=n$,
   $|G_n(\bar{\lambda}_p)|=|G_n(\bar{\nu}_p)|=n$;
2. 对任意 $0\leqslant q\leqslant n-1$,
   $\mathrm{supp}(\rho^q(\lambda_p))\subseteq\mathrm{supp}(\rho^q(\nu_p))$,
   $\mathrm{supp}(\rho^q(\bar{\nu}_p))\subseteq\mathrm{supp}(\rho^q(\bar{\lambda}_p))$.

引理 3:

$(\cup_{p\in S}G_n(\nu_p))\cap(\cup_{p\in S}G_n(\bar{\nu}_p))=\varnothing$,且对任意 $p\in S$,$0\leqslant q_1,q_2<n$,$q_1\neq q_2$,有

1. $\mathrm{supp}(\rho^{q_2}(\lambda_p))\not\subseteq\mathrm{supp}(\rho^{q_1}(v_p))$;
2. $\mathrm{supp}(\rho^{q_2}(\bar{\nu}_p))\not\subseteq\mathrm{supp}(\rho^{q_1}(\bar{\lambda}_p))$。

证明:首先证明前者,不妨设 $(\cup_{p\in S}G_n(\nu_p))\cap(\cup_{p\in S}G_n(\bar{\nu}_p))\neq\varnothing$,则存在 $p_1,p_2\in S$,$G_n(\nu_{p_1})\cap G_n(\bar{\nu}_{p_2})\neq\varnothing$,由于 $\nu_{p_1},\bar{\nu}_{p_2}$ 的重量都为 $n/2$,故必有 $G_n(\nu_{p_1})=G_n(\bar{\nu}_{p_2})$。若 $1<u_{p_2}<n/2-1$,则 $G_n(\bar{\nu}_{p_2})$ 中每个元素都是由两段不相邻且重量不小于 2 的片段构造,而 $G_n(\nu_{p_1})$ 中元素都是由一个 1 与不相邻的连续 $n/2-1$ 个 1 构成,故二者所在轨道不可能相等。若 $u_{p_2}=1$,则

$$\mathrm{supp}(\bar{\nu}_{p_2})=\{n/2\}\cup\{n/2+2,\cdots,n\}$$

易知 $\bar{\nu}_{p_2}\notin G_n(\nu_{p_1})$。故假设不成立。

对于后者,只需证

$\mathrm{supp}(\rho^{q_2}(\lambda_p))\not\subseteq\mathrm{supp}(\rho^{q_1}(v_p))$ 即可,此时只需证 $q_1<q_2$(或 $q_1>q_2$)时的情形,不妨设 $q_1<q_2$,这等价证明

$$\mathrm{supp}(\rho^{q_2-q_1}(\lambda_p)) \not\subseteq \mathrm{supp}(\rho(v_p)).$$

若$(q_2-q_1)+n/2+u_p \leqslant n$,则

$$\begin{cases}(q_2-q_1)+n/2+u_p \in \mathrm{supp}(\rho^{q_2-q_1}(\lambda_p)),\\ (q_2-q_1)+n/2+u_p \notin \mathrm{supp}(\nu_p).\end{cases}$$

故此时结论成立。否则,若要证 $\mathrm{supp}(\rho^{q_2-q_1}(\lambda_p)) \not\subseteq \mathrm{supp}(\rho(v_p))$,只需证

$$\mathrm{supp}(\rho(\lambda_p)) \not\subseteq \mathrm{supp}(\rho^{n-q_2+q_1}(v_p)).$$

已知$\{1,2,\cdots,h_p,n/2+u_p\} \subseteq \mathrm{supp}(\lambda_p)$,令 $0<q=n-q_2+q_1$,若

$$\mathrm{supp}(\rho(\lambda_p)) \subseteq \mathrm{supp}(\rho^q(v_p))$$

则必存在某个 $1 \leqslant i \leqslant n/2-1$,使得 $i+q=n/2+u_p$,此时有

$$n/2-1+q=n+u_p-1-i \leqslant n+h_p-i<n+h_p,$$

故必有$\{h_p-1,h_p\} \not\subseteq \mathrm{supp}(\rho^q(\nu_p))$。即

$$\mathrm{supp}(\rho(\lambda_p)) \not\subseteq \mathrm{supp}(\rho^{n-q_2+q_1}(v_p)).$$

引理 4: 设 $p_1<p_2(p_1,p_2 \in S)$, $0 \leqslant q_1,q_2 \leqslant n-1$,则

$$\mathrm{supp}(\rho^{q_2}(\lambda_{p_2})) \not\subseteq \mathrm{supp}(\rho^{q_1}(\nu_{p_1})),$$

$$\mathrm{supp}(\rho^{q_1}(\bar{\nu}_{p_1})) \not\subseteq \mathrm{supp}(\rho^{q_2}(\bar{\lambda}_{p_2})).$$

证明:与引理 3 的证明类似。

构造 1

Step 1 选取偶数 n,$n \geqslant 10$。

Step 2 取非空集合 S,

$S=\{k_1,\cdots,k_s\} \subseteq \{1,2,\cdots,n/2-2\}$,且已按从小到大顺序排列。对所有 $p \in S$,构造形如(1)(2)的向量 $\lambda_p,v_p \in F_2^n$,且满足相应条件。

Step 3 构造布尔函数 f,f 的支撑集为

$$\{x \in F_2^n \mid wt(x)>n/2\} \cup \{G_n(\lambda_p) \mid p \in S\} \cup \{G_n(\bar{\nu}_p) \mid p \in S\} \setminus \{G_n(\bar{\lambda}_p) \mid p \in S\}.$$

定理 1:构造 1 所得的布尔函数为 MAI 旋转对称函数。

证明:旋转对称性是显然的。下面证明其 MAI 性质,已知 $S=\{k_1,\cdots,k_s\}$,将$\{G_n(\lambda_p) \mid p \in S\}$上共 $s \cdot n$ 个元素按所在轨道 $G_n(\lambda_p)$ 中 p 的大小从小到大排列,同一轨道上的 n 个元素可任意排列,得到的元素集合记为 $T=\{b_1,b_2,\cdots,b_{s\cdot n}\}$。对任意 $1 \leqslant i \leqslant s \cdot n$,设 $b_i=\rho^{q_2}(\lambda_{k_{p_2}})$,定义

$$A_i=\{x \in F_2^n \mid \mathrm{supp}(x) \subseteq \mathrm{supp}(a_i)\},$$

其中 $a_i=\rho^{q_2}(\nu_{k_{p_2}})$,显然 $b_i \neq a_i$,$b_i \in A_i$。下证当 $i^*<i$ 时,$b_i \notin \cup_{i^*<i} A_{i^*}$ 成立。假设存在 $i^*<i$,$b_i=\rho^{q_2}(\lambda_{k_{p_2}}) \in A_{i^*}$,不妨设 $a^{i^*}=\rho^{q_1}(\nu_{k_{p_1}})$。根据 A_i 的定义,有

$$\mathrm{supp}(\rho^{q_2}(\lambda_{k_{p_2}})) \subseteq \mathrm{supp}(\rho^{q_1}(\nu_{k_{p_1}})).$$

由于 $i^*<i$,故必有 $k_{p_1}<k_{p_2}$ 或者 $k_{p_1}=k_{p_2}$,$q_1 \neq q_2$,从而上述式子与引理 3,引理 4 矛盾。即当 $i^*<i$ 时,$b_i \notin \cup_{i^*<i} A_{i^*}$。

对任意 $1 \leqslant i \leqslant s \cdot n$,设

$$b_i=\rho^{q_2}(\bar{\lambda}_{k_{p_2}}),a_i=\rho^{q_2}(\bar{\nu}_{k_{p_2}}),$$

$$A^{\circ}{}_i=\{x \in F_2^n \mid \mathrm{supp}(a_i) \subseteq \mathrm{supp}(x)\}.$$

显然 $b_i \neq a_i$,$b_i \in A^{\circ}{}_i$。与上面的证明类似,可证当 $i^*<i$ 时,$b_i \notin \cup_{i^*<i} A^{\circ}{}_{i^*}$ 成立。

令 $K=\varnothing$,I 为$\{G_n(v_p) \mid p \in S\}$,对应选取的元素为$\{G_n(\lambda_p) \mid p \in S\}$,$J$ 为$\{G_n(\bar{\nu}_p) \mid p \in S\}$,对应选取的元素为$\{G_n(\lambda_p) \mid p \in S\}$,由引理 1 得支撑集为

$$\{x \in F_2^n \mid wt(x)>n/2\} \cup \{G_n(\lambda_p) \mid p \in S\} \cup \{G_n(\bar{\nu}_p) \mid p \in S\} \setminus \{G_n(\bar{\lambda}_p) \mid p \in S\}$$

的 n 元布尔函数为 MAI 函数,结论得证。

进一步,可以将 λ_p,v_p 进行修改,以得到更多的 MAI 旋转对称函数。设集合 $S=\{i_1,\cdots,i_s\} \subset \{1,2,\cdots,n/2-5\}$,且对任意 $1 \leqslant j<k \leqslant s$,都有 $i_j<i_k$。对任意 $p \in S$,定义 $\lambda_p,v_p \in F_2^n$,其支撑分别为:

$$\{1,\cdots,h_p\} \cup \{n/2+t_p,\cdots,n/2+u_p\} \quad (3)$$

$$\{1,\cdots,n/2-1+v_p-u_p\} \cup \{n/2+v_p,\cdots,n/2+u_p\} \quad (4)$$

其中 $3 \leqslant h_p \leqslant n/2-3$,$1 \leqslant t_p \leqslant u_p \leqslant h_p+1$,$u_p-t_p+1<h_p$,$u_p-t_p+1+h_p<n/2$.

若 $i_1<i_2(i_1,i_2 \in S)$,都有 $h_{i_1} \leqslant h_{i_2}$,$u_{i_1}<u_{i_2}$.

引理 5:对任意 $p,p_1,p_2 \in S(p_1<p_2)$,有

1. $|G_n(\lambda_p)|=|G_n(v_p)|=n$;
2. 对任意 $0 \leqslant q \leqslant n-1$,

$$\mathrm{supp}(\rho^q(\lambda_p)) \subseteq \mathrm{supp}(\rho^q(\nu_p));$$

3. 且对任意 $p \in S$,$0 \leqslant q_1,q_2<n$,$q_1 \neq q_2$,都有 $\mathrm{supp}(\rho^{q_2}(\lambda_p)) \not\subseteq \mathrm{supp}(\rho^{q_1}(v_p))$;
4. 设 $0 \leqslant q_1,q_2 \leqslant n-1$,则

$$\mathrm{supp}(\rho^{q_2}(\lambda_{p_2})) \not\subseteq \mathrm{supp}(\rho^{q_1}(\nu_{p_1})).$$

证明:与引理 3 的证明类似,不再详述。

构造 2

Step 1 选取偶数 n,$n \geqslant 10$;

Step 2 取非空集合 S,

$$S=\{k_1,\cdots,k_s\} \subseteq \{1,2,\cdots,n/2-5\},$$

且已按升序排列。对所有 $p \in S$,构造形如(3)(4)的向量 $\lambda_p,v_p \in F_2^n$,且满足相应条件;

Step 3 构造布尔函数 f,f 的支撑集为

$$\{x \in F_2^n \mid wt(x)>n/2\} \cup \{G_n(\lambda_p) \mid p \in S\}.$$

定理 2 :构造 2 所得的布尔函数为 MAI 旋转对称函数。

证明:与定理 1 的证明类似,不再详述。

3 高非线性度 MAI 旋转对称布尔函数

一般情形下,构造 1 与构造 2 所给出的 MAI 函数的非线性度不容易刻画,下面研究特殊构造的旋转对称布尔函数的非线性度。设 $n(n\geqslant 14)$ 为偶数,$N=n/2-5$,$S=\{1,2,\cdots,N\}$,对所有 $p(1\leqslant p\leqslant N)$,构造 $\lambda_p,v_p\in F_2^n$,使得

$$\mathrm{supp}(\lambda_p)=\{1,2,\cdots,p+2\}\cup\{n/2+p+3\}\cup T_p \quad (5)$$

$$\mathrm{supp}(\nu_p)=\{1,2,\cdots,n/2-l_p\}\cup\{n/2+p+3\}\cup T_p \quad (6)$$

其中,$l_p=|\{\{n/2+p+3\}\cup T_p\}|$,

$$T_p=\begin{cases}\varnothing & n/2,p\text{ 奇偶性不同},\\ \{n/2+p+2\} & n/2,p\text{ 奇偶性相同}.\end{cases}$$

引理 6:对于任意 $p\in S$,有

1. $|G_n(\lambda_p)|=|G_n(v_p)|=|G_n(\bar{\lambda}_p)|=|G_n(\bar{\nu}_p)|=n$;
2. 对任意 $0\leqslant q\leqslant n-1$,
   $\mathrm{supp}(\rho^q(\lambda_p))\subseteq\mathrm{supp}(\rho^q(\nu_p))$,
   $\mathrm{supp}(\rho^q(\bar{\nu}_p))\subseteq\mathrm{supp}(\rho^q(\bar{\lambda}_p))$;
3. 对任意 $p\in S,0\leqslant q_1,q_2<n,q_1\neq q_2$,
   $\mathrm{supp}(\rho^{q_2}(\lambda_p))\nsubseteq\mathrm{supp}(\rho^{q_1}(v_p))$,
   $\mathrm{supp}(\rho^{q_2}(\bar{\nu}_p))\nsubseteq\mathrm{supp}(\rho^{q_1}(\bar{\lambda}_p))$;
4. $(\cup_{p\in S}G_n(\nu_p))\cap(\cup_{p\in S}G_n(\bar{\nu}_p))=\varnothing$.

证明:前三个结论为引理 5 的直接推论,下面给出结论 4 的证明。若存在 $p_1,p_2\in S$,使得 $G_n(\nu_{p_1})\cap G_n(\bar{\nu}_{p_2})\neq\varnothing$,则同样易有 $G_n(\nu_{p_1})=G_n(\bar{\nu}_{p_2})$。若 $p_2<n/2-5$,则易知 $\bar{\nu}_{p_2}$ 是由两段重量不小于 3 的连续 1 片段构成,而 ν_{p_1} 其中一连续 1 片段的重量不超过 2,故二者所在轨道不可能相等;若 $p_2=n/2-5$,则 $\bar{\nu}_{p_2}$ 支撑中两个 1 片段之间的距离为 1 或 2(等于 $|l_p|$),而 ν_{p_1} 支撑中两个片段之间的距离不小于 $n/2+2-(n/2-1)=3$,且二者都是长片段在前,故二者所在轨道也不可能相等,从而假设不成立,结论得证。

构造 3

Step 1 选取偶数 $n,n\geqslant 14$;

Step 2 设 $N=n/2-5,S=\{1,2,\cdots,N\}$,对于所有的 $p(1\leqslant p\leqslant N)$,构造 $\lambda_p,v_p\in F_2^n$ 如式(5)、(6)所示;

Step 3 令 $\bar{\lambda}_p,\bar{\nu}_p$ 分别为 λ_p,v_p 的补,设
$A=\cup_{p\in S}G_n(\lambda_p)$,$B=\cup_{p\in S}G_n(\bar{\lambda}_p)$,
$C=\cup_{p\in S}G_n(\bar{\nu}_p)$;

Step 4 构造布尔函数 f,满足

$$f(x)=\begin{cases}F_n(x)+1, & x\in A\cup B\cup C\\ F_n(x), & \text{其他}\end{cases},$$

定理 3:构造 3 所得到的布尔函数 f 为 MAI 旋转对称函数,且有

$$nl_f=\begin{cases}2^{n-1}-\binom{n-1}{n/2}+\dfrac{n^2-16n+60}{2}, & \dfrac{n}{2}\text{为奇数}\\ 2^{n-1}-\binom{n-1}{n/2}+\dfrac{n^2-16n+48}{2}, & \dfrac{n}{2}\text{为偶数}\end{cases}$$

证明:旋转对称是显然的,MAI 的证明与定理 1 类似,不再详述。易知此时有

$$W_f(\mu)=\sum_{x\in A\cup B\cup C}(-1)^{F_n(x)+1+x\cdot\mu}+\sum_{x\notin A\cup B\cup C}(-1)^{F_n(x)+x\cdot\mu}=\sum_{x\in F_2^n}(-1)^{F_n(x)+x\cdot\mu}+2\sum_{x\in A\cup B\cup C}(-1)^{F_n(x)+1+x\cdot\mu}=W_{F_n}(\mu)+2\sum_{x\in B}(-1)^{x\cdot\mu}-2\sum_{x\in A}(-1)^{x\cdot\mu}-2\sum_{x\in C}(-1)^{x\cdot\mu}$$

分情况讨论之:

1. 若 $\mu=0$:此时 $W_{F_n}(\mu)=\binom{n}{n/2}$,
   $\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=|G_n(\lambda_p)|=n$,而
   $W_f(\mu)=W_{F_n}(\mu)+2\sum_{x\in B}(-1)^{x\cdot\mu}-2\sum_{x\in A}(-1)^{x\cdot\mu}-2\sum_{x\in C}(-1)^{x\cdot\mu}=\binom{n}{n/2}+2N\cdot n-2N\cdot n-2N\cdot n$
   所以 $|W_f(\mu)|=\binom{n}{n/2}-2N\cdot n$.

2. 若 $wt(\mu)=1$:此时 $W_{F_n}(\mu)=\binom{n}{n/2}$,
   $\sum_{x\in G_n(\lambda_q)}(-1)^{x\cdot\mu}=n-2wt(\lambda_q)$,从而 $\sum_{x\in C}(-1)^{x\cdot\mu}=0$,若 $n/2$ 为奇数,易计算有 $2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}-2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=4\sum_{1\leqslant p\leqslant N}(2wt(\lambda_p)-n)=8\sum_{1\leqslant i\leqslant(n-10)/4}(n-4i-6)=16n-n^2-60$;
   若 $n/2$ 为偶数,同样易有 $2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}-2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=4\sum_{1\leqslant p\leqslant N}(2wt(\lambda_p)-n)=16n-n^2-48$。从而

$$|W_f(\mu)|=\begin{cases}\binom{n}{n/2}-n^2+16n-60, & \dfrac{n}{2}\text{为奇数}\\ \binom{n}{n/2}-n^2+16n-48, & \dfrac{n}{2}\text{为偶数}\end{cases}$$

3. 若 $wt(\mu)=n$:当 $n/2$ 为奇数时,$W_{F_n}(\mu)=-\binom{n}{n/2}$;$n/2$ 为偶数时,$W_{F_n}(\mu)=\binom{n}{n/2}$。若

$n/2$ 为奇数,则 $wt(\lambda_p)$ 恒奇, 故 $wt(\bar{\lambda}_p)$ 也恒奇,从而

$$2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=2\sum_{1\leqslant p\leqslant N}-n=-2Nn$$

若 $n/2$ 为偶数,由于 $wt(\lambda_p)$ 恒为偶数,则 $wt(\bar{\lambda}_p)$ 也恒为偶数,故

$$2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\lambda_p)}(-1)^{x\cdot\mu}=2\sum_{1\leqslant p\leqslant N}n=2Nn$$

另一方面

$$2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\nu_p)}(-1)^{x\cdot\mu}=2\sum_{1\leqslant p\leqslant N}\sum_{x\in G_n(\nu_p)}(-1)^{n/2}=2Nn(-1)^{n/2}$$

故此时总有 $|W_f(\mu)|=\binom{n}{n/2}-2Nn.$

4. 若 $2\leqslant wt(\mu)\leqslant n-1$:由文献[7]知 $|W_{F_n}(\mu)|\leqslant\frac{1}{n-1}\binom{n-1}{n/2}$,又 $n\geqslant 14$,故

$$|W(\mu)|\leqslant|W_{F_n}(\mu)|+|2\sum_{x\in B}(-1)^{x\cdot\mu}|+|2\sum_{x\in A}(-1)^{x\cdot\mu}|+|2\sum_{x\in C}(-1)^{x\cdot\mu}|$$

$$\leqslant\frac{1}{n-1}\binom{n-1}{n/2}+6Nn\leqslant\binom{n-1}{n/2}-2Nn.$$

当 $n\geqslant 14$ 时,易知 $2Nn>n^2-16n+60$,故 f 的Walsh谱的绝对值仍在 $wt(\mu)=1$ 时达到最大,代入非线性度的计算公式可得。

表 1　非线性度的比较

Tab. 1　The comparison of nonlinearity

n	文献[5]的构造	构造 3
18	106 798	106 810
20	431 974	431 974
22	1 744 500	1 744 532
24	7 036 630	7 036 650

4　结　论

本文给出了具有最大代数免疫度的偶数元旋转对称布尔函数的两种构造方法,并研究了特殊情形时所构造的旋转对称布尔函数的非线性度。当然,仍有许多的问题值得进一步研究,如怎样使得所构造的 MAI 旋转对称布尔函数达到平衡以及怎样构造奇数变元的 MAI 旋转对称布尔函数等,这些都是我们下一步研究的方向。

参考文献(References)

[1] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback[C]//Eurocrypt 2003, LNCS 2656, Springer-Verlag, 2003:345 - 359.

[2] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions[C]//EUROCRYPT 2004, LNCS 3027,2004: 474 - 491.

[3] Fu S J, Li C, Matsuura K, et al. Construction of rotation symmetric Boolean functions with maximum algebraic immunity [C]//CANS 2009, LNCS 5888,2009:402 - 412.

[4] Sarkar S, Maitra S. Construction of rotation symmetric Boolean functions with optimal algebraic immunity[J]. Computation Systems, 2009, 12(3): 267 - 284.

[5] Fu S J, Li C, Matsuura K,et al. Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity[J]. Science in China (F), accepted.

[6] Carlet C. A method of construction of balanced functions with optimum algebraic immunity [C] // Proceedings of the International Workshop on Coding and Cryptography, Fujiang, China, June, 2007.

[7] Dalai D K, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J]. Des. Codes Cryptogr., 2006, 40: 41 - 58.

[8] Li N, Qu L J. On the construction of Boolean functions with optimal algebraic immunity [J]. IEEE Transactions on Information Theory, 2008, 53(3): 1330 - 1334.

[9] Carlet C, Feng K Q. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity[C]// Asiacrypt 2008, LNCS 5350, 2008:425 - 440.

[10] Qu L J, Feng K Q, Liu F, et al. Construction symmetric Boolean functions with maximum algebraic immunity[J]. IEEE Transactions on Information Theory, 2009, 55(5): 2406 - 2412.

[11] Tu Z R, Deng Y P. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity[J]. Des. Codes Cryptogr.,2011,60:1 - 14.

[12] Tu Z R, Deng Y P. A class of 1 - resilient function with high nonlinearity and algebraic immunity [EB]. Cryptography ePrint Archive, Report 2010/179, 2010.