代数免疫度最优的旋转对称布尔函数的构造*

李 超[1,2],薛朝红[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,为了抵挡代数攻击,密码算法中所使用的布尔函数应当具有较高的代数免疫度。本文利用"轨道交换"技术,给出了一类具有最优代数免疫度的旋转对称布尔函数的构造,该类函数对于代数攻击具有较强的抵抗能力,同时具有较高的非线性度和最优代数次数。

关键词:代数免疫度;旋转对称;非线性度;代数次数
中图分类号:TN918.1 **文献标志码**:A **文章编号**:1001-2486(2012)02-0034-05

Construction of rotation symmetric Boolean function with maximum algebraic immunity

LI Chao[1,2], *XUE Chaohong*[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 cryptographic properties for Boolean functions. In order to resist algebraic attack, high algebraic immunity is necessary for those Boolean functions used in symmetric cipher algorithms. Based on "orbit exchange" technique, this research presents a construction of rotation symmetric Boolean functions with the maximum algebraic immunity on even number of variables. These functions have strong resistance against algebraic attacks. These functions also have much better nonlinearity and optimal algebraic degree.

Key words: algebraic immunity; rotation symmetric; nonlinearity; algebraic degree

代数攻击的提出和发展被认为是近年来密码分析技术最重要的突破之一,代数免疫度也成为衡量密码函数安全性的一个重要指标,如何构造代数免疫度最优的函数(简称 MAI 函数)已经成为近年来研究的一个重点问题[1-9]。旋转对称布尔函数(简称 RotS 函数)由于其良好的结构特性,在密码学中有着广泛的应用,因而构造代数免疫度最优且具有其他良好密码学性质的 RotS 函数具有重要意义。文献[10]给出了一种代数免疫度最优的 RotS 函数的构造方法,本文利用"轨道交换"技术,构造了一类代数免疫度最优的 RotS 函数,并给出了所构造函数的非线性度下界,与文献[10]中结果相比,构造函数的非线性度得到了一定提升,同时代数次数达到最优。

1 预备知识

对于 $x_i \in \mathbb{F}_2 (1 \leqslant i \leqslant n)$,以及 $0 \leqslant k \leqslant n-1$,定义

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

ρ_n^k 的定义可以推广到向量 $x=(x_1,x_2,\cdots,x_n) \in \mathbb{F}_2^n$ 上,$\rho_n^k(x_1,x_2,\cdots,x_n) = (\rho_n^k(x_1),\rho_n^k(x_2),\cdots,\rho_n^k(x_n))$.

定义 1 如果对于任意的 $x=(x_1,x_2,\cdots,x_n) \in \mathrm{F}_2^n$,以及 $0 \leqslant k \leqslant n-1$,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。

记 $G_n(x_1,x_2,\cdots,x_n) = \{\rho_n^k(x_1,x_2,\cdots,x_n) \mid 0 \leqslant k \leqslant n-1\}$,即 $(x_1,x_2,\cdots,x_n)$ 在 ρ_n 作用下的轨道。显然 $\mathbb{F}_2^n$ 中的所有向量被分为不同的轨道,如果 $|G_n(x_1,x_2,\cdots,x_n)| = t$,称 $G_n(x_1,x_2,\cdots,x_n)$ 是一个 t-轨道,容易验证 t 是 n 的一个因子。

记 $\bar{x} = (x_1+1, x_2+1, \cdots, x_n+1)$,易知 $G_n(\bar{x}) = \overline{G_n(x)}$,$\overline{G_n(x)}$ 称为轨道 $G_n(x)$ 的共轭轨道。如果 $G_n(x) = G_n(\bar{x})$,则称 $G_n(x)$ 为自共轭轨道。

* **收稿日期**:2011-07-28
基金项目:国家自然科学基金资助项目(61070215,61103191)
作者简介:李超(1966—),男,湖南汨罗人,教授,博士,博士生导师,E-mail: lichao_nudt@sina.com

定义 2　对 $f\in B_n$,则 f 的代数免疫度(记为 $AI(f)$)是指使得 $fg=0$ 或者 $(f+1)g=0$ 成立的非零布尔函数 g 的最小代数次数,即 $AI(f)=\min\{\deg(g)\mid 0\neq g\in \mathrm{Ann}(f)\cup \mathrm{Ann}(1+f)\}$。可以证明 $AI(f)\leqslant\lceil\frac{n}{2}\rceil$,因而称 $AI(f)=\lceil\frac{n}{2}\rceil$ 的布尔函数为代数免疫度最优的(MAI)。

2　一类代数免疫度最优 RotS 函数的构造

在文献[10]中,孟强等提出了一种代数免疫度最优函数的构造方法。令 n 为偶数,并记

$$W^{<\frac{n}{2}}=\left\{x\,\middle|\,x\in\mathbb{F}_2^n,w(x)<\frac{n}{2}\right\},$$

$$W^{\frac{n}{2}}=\left\{x\,\middle|\,x\in\mathbb{F}_2^n,w(x)=\frac{n}{2}\right\},$$

$$W^{>\frac{n}{2}}=\left\{x\,\middle|\,x\in\mathbb{F}_2^n,w(x)>\frac{n}{2}\right\}.$$

令 T,U,S 和 V 为 $\mathbb{F}_2^n$ 的不相交子集,其中

$$T=\{\alpha_1,\cdots,\alpha_{l_1}\}\subseteq W^{<\frac{n}{2}},$$

$$U=\{u_1,\cdots,u_{l_2}\}\subseteq W^{\frac{n}{2}},$$

$$S=\{\beta_1,\cdots,\beta_{l_3}\}\subseteq W^{>\frac{n}{2}},$$

$$V=\{v_1,\cdots,v_{l_4}\}\subseteq W^{\frac{n}{2}}.$$

这里,$l_1\leqslant l_2$,$l_3\leqslant l_4$. 定义有限域 F_2 上的两个矩阵 $A=(a_{ij})_{l_2\times l_1}$ 与 $B=(b_{ij})_{l_4\times l_3}$,满足:

(1)对任意的 $1\leqslant i\leqslant l_2$,$1\leqslant j\leqslant l_1$,如果 $\mathrm{supp}(\alpha_j)\subset\mathrm{supp}(u_i)$,则定义 $a_{ij}=1$,否则定义 $a_{ij}=0$。

(2)对任意的 $1\leqslant i\leqslant l_4$,$1\leqslant j\leqslant l_3$,如果 $\mathrm{supp}(v_i)\subset\mathrm{supp}(\beta_j)$,则定义 $b_{ij}=1$,否则定义 $b_{ij}=0$。

引理 1[10]　设 $f\in B_n$,且

$$f(x)=\begin{cases}1, & W^{<\frac{n}{2}}\cup S\cup U\backslash T,\\ a(x), & W^{\frac{n}{2}}\backslash(U\cup V),\\ 0, & W^{>\frac{n}{2}}\cup T\cup V\backslash S.\end{cases}$$

其中,$a(x)$ 是任一定义在 $w^{\frac{n}{2}}\backslash(U\cup V)$ 上的布尔值函数。如果上面定义的矩阵 $A=(a_{ij})_{l_2\times l_1}$ 与 $B=(b_{ij})_{l_4\times l_3}$ 均为列满秩矩阵,那么 f 具有最优的代数免疫度。

我们对上述构造进行改进,选取偶数 n 满足 $n\geqslant 12$,令 $N=\lfloor\frac{n}{4}\rfloor-1$,设 $\lambda_p\in\mathbb{F}_2^n(1\leqslant p\leqslant N)$ 满足:

$$\mathrm{supp}(\lambda_p)=\begin{cases}\{1,2,\cdots,2p\}\cup\left\{\frac{n}{2}+p\right\}, & \frac{n}{2}\text{为奇数};\\ \{1,2,\cdots,2p-1\}\cup\left\{\frac{n}{2}+p\right\}, & \frac{n}{2}\text{为偶数}。\end{cases}$$

记 $T=\bigcup\limits_{1\leqslant p\leqslant N}G_n(\lambda_p)$,对于 $1\leqslant p\leqslant N$,设向量 $\nu_p\in\mathbb{F}_2^n$ 满足:

$$\mathrm{supp}(\nu_p)=\left\{1,2,\cdots,\frac{n}{2}-1\right\}\cup\left\{\frac{n}{2}+p\right\}$$

记 $U=\bigcup\limits_{1\leqslant p\leqslant N}(G_n(\nu_p)\cup G_n(\overline{\nu_p}))$.

定理 1　$a(x)$ 定义在 $W^{\frac{n}{2}}$ 上且满足:

(1)$a(x)=a(\bar{x})$;

(2)$a(x)=a(\rho_n^k(x))$;

(3)$a(x)=1,\forall x\in U$;

(4)$a(x)$ 在 $W^{\frac{n}{2}}$ 上平衡,或者 $a(x)$ 在 $W^{\frac{n}{2}}$ 上接近平衡,即 $\big|\,|E(a(x)=1)|-|E(a(x)=0)|\,\big|\leqslant n$。记

$$f(x)=\begin{cases}1, & W^{<\frac{n}{2}}\backslash T,\\ a(x), & W^{\frac{n}{2}},\\ 0, & W^{>\frac{n}{2}}\cup T.\end{cases}\tag{1}$$

则 $f(x)$ 为代数免疫度最优函数。

证明　首先简要说明 $a(x)$ 是存在的。取 $x\in W^{\frac{n}{2}}$,则 $|G_n(x)|$ 可能的取值为 $1,2,\cdots,k,\cdots,\frac{n}{2},n$,记 $A_x=G_n(x)\cup G_n(\bar{x})$,$B_k=\{x\in W^{\frac{n}{2}}\mid|G_n(x)|=k\}=\bigcup\limits_{i=1}^{l_k}A_{x_{ki}}$,这里 $k\mid n$,则 $W^{\frac{n}{2}}=\bigcup\limits_{1\leqslant k\leqslant n}B_k$。我们来考虑 $a(x)$ 的构造,当 $k=n$ 时,记 $A_i=A_{x_{ki}}$,B_n 可分为非自共轭(l_{n1} 个)和自共轭($l_{n2}=(l_n-l_{n1})$ 个)两部分,不妨假定

$$B_{n1}\triangleq\bigcup_{i=1}^{l_{n1}}A_i,G_n(x)\neq G_n(\bar{x}),x\in A_i,$$

$$B_{n2}\triangleq\bigcup_{i=l_{n1}+1}^{l_n}A_i,G_n(x)=G_n(\bar{x}),x\in A_i$$

易知 $l_{n1}\neq 0$,$l_{n2}\neq 0$,记

$$C_n=\big|\{x\in B_n\mid a(x)=1\}\big|-\big|\{x\in B_n\mid a(x)=0\}\big|$$

下面分情况讨论:

(1)当 l_{n1},l_{n2} 为偶数时,令

$$a(x)=1,x\in A_i,i=1,\cdots,\frac{l_{n1}}{2},$$

$$a(x)=1,x\in A_i,i=l_{n1}+1,\cdots,l_{n1}+\frac{l_{n2}}{2},$$

$$a(x)=0,x\in A_i,i=\frac{l_{n1}}{2}+1,\cdots,l_{n1},$$

$$a(x)=0,x\in A_i,i=l_{n1}+\frac{l_{n2}}{2}+1,\cdots,l_{n1}+l_{n2},$$

$C_n=0$;

(2)当 l_{n1} 为偶数,l_{n2} 为奇数时,令

$$a(x)=1,x\in A_i,i=1,\cdots,\frac{l_{n1}}{2},$$

$$a(x)=1,x\in A_i,i=l_{n1}+1,\cdots,l_{n1}+\frac{l_{n2}+1}{2},$$

$$a(x)=0,x\in A_i,i=\frac{l_{n1}}{2}+1,\cdots,l_{n1},$$

$$a(x)=0,x\in A_i,i=l_{n1}+\frac{l_{n2}+3}{2},\cdots,l_{n1}+l_{n2},$$

$C_n = n$;

(3)当 l_{n1} 为奇数,l_{n2} 为偶数时,令

$a(x) = 1, x \in A_i, i = 1, \cdots, \frac{l_{n1}+1}{2}$,

$a(x) = 1, x \in A_i, i = l_{n1}+1, \cdots, l_{n1}+\frac{l_{n2}}{2}-1$,

$a(x) = 0, x \in A_i, i = \frac{l_{n1}+3}{2}, \cdots, l_{n1}$,

$a(x) = 0, x \in A_i, i = l_{n1}+\frac{l_{n2}}{2}, \cdots, l_{n1}+l_{n2}, C_n = 0$;

(4)当 l_{n1}, l_{n2} 为奇数时,令

$a(x) = 1, x \in A_i, i = 1, \cdots, \frac{l_{n1}+1}{2}$,

$a(x) = 1, x \in A_i, i = l_{n1}+1, \cdots, l_{n1}+\frac{l_{n2}-1}{2}$,

$a(x) = 0, x \in A_i, i = \frac{l_{n1}+3}{2}, \cdots, l_{n1}$,

$a(x) = 0, x \in A_i, i = l_{n1}+\frac{l_{n2}+1}{2}, \cdots, l_{n1}+l_{n2}$,

$C_n = n$;

当 $k = \frac{n}{2}$ 时,采用类似的处理方法,使得 $C_{\frac{n}{2}} = -n$($l_{\frac{n}{2}1}$ 为奇数,$l_{\frac{n}{2}2} = 0$),$C_{\frac{n}{2}} = -\frac{n}{2}$ 或者 $C_{\frac{n}{2}} = 0$;……

当 $C_k \neq 0, k = n, \frac{n}{2}, \cdots, 2, 1, k \mid n$ 时,C_k 是正负交替的,$\big||E(a(x)=1)| - |E(a(x)=0)|\big| = \Big|\sum_{k \mid n} C_k\Big| \leqslant n$,这样,我们就得到了满足(1)、(2)、(4)的 $a(x)$。同时 U 仅是 B_n 的很小一部分,因而条件(3)容易满足,此即表明满足条件的 $a(x)$ 是存在的。再证 $f(x)$ 为代数免疫度最优函数。

当 $\frac{n}{2}$ 为奇数时,取

$$T = \{\lambda_1, \cdots, \rho^{n-1}(\lambda_1), \cdots, \lambda_p, \cdots, \rho^{n-1}(\lambda_p)\},$$
$$U = \{\nu_1, \cdots, \rho^{n-1}(\nu_1), \cdots, \nu_p, \cdots, \rho^{n-1}(\nu_p), \overline{\nu_1}, \cdots, \rho^{n-1}(\overline{\nu_1}), \cdots, \overline{\nu_p}, \cdots, \rho^{n-1}(\overline{\nu_p})\}$$

下面证 $A = (a_{ij})_{l_2 \times l_1}$ 的前 np 行是一个 $np \times np$ 的下三角矩阵。由 $A = (a_{ij})_{l_2 \times l_1}, T, U$ 的定义,易知 $a_{ii} = 1 (1 \leqslant i \leqslant np)$。同时

$$a_{ij} = 1 \Leftrightarrow \mathrm{supp}(\alpha_j) \subset \mathrm{supp}(u_i)$$

当 $i < j$ 时,α_j, μ_i 可能的取值情况有两种:

(1)$\alpha_j = \rho^{k_2}(\lambda_p), \mu_i = \rho^{k_1}(\nu_p), 0 \leqslant k_1 < k_2 < n$,若 $(k_2 - k_1) + \frac{n}{2} + p \leqslant n$,则 $\mathrm{supp}(\rho^{k_2}(\lambda_p)) \subset \mathrm{supp}(\rho^{k_1}(\nu_p))$ 与 $\begin{cases}(k_2-k_1)+\frac{n}{2}+p \in \mathrm{supp}(\rho^{k_2-k_1}(\lambda_p)),\\ (k_2-k_1)+\frac{n}{2}+p \notin \mathrm{supp}(\nu_p).\end{cases}$ 矛盾;

若 $(k_2 - k_1) + \frac{n}{2} + p > n$,则 $(k_2 - k_1) + p > \frac{n}{2}$,此时 $\mathrm{supp}(\rho^{k_2}(\lambda_p)) \subset \mathrm{supp}(\rho^{k_1}(\nu_p))$ 与 $\begin{cases}\{(k_2-k_1)+2p, (k_2-k_1)+2p-1\} \subseteq \mathrm{supp}(\rho^{k_2-k_1}(\lambda_p)),\\ \{(k_2-k_1)+2p, (k_2-k_1)+2p-1\} \not\subset \mathrm{supp}(\nu_p).\end{cases}$ 矛盾。

(2)$\alpha_j = \rho^{k_2}(\lambda_{p_2}), \mu_i = \rho^{k_1}(\nu_{p_1}), 1 \leqslant p_1 < p_2 \leqslant N, 0 \leqslant k_1, k_2 < n$,如果 $k_1 - k_2 \geqslant 0$,有

$$\mathrm{supp}(\rho^{k_2}(\lambda_{p_2})) \not\subset \mathrm{supp}(\rho^{k_1}(\nu_{p_1})) \Leftrightarrow \mathrm{supp}(\lambda_{p_2}) \not\subset \mathrm{supp}(\rho^{k_1-k_2}(\nu_{p_1}));$$

如果 $k_1 - k_2 < 0$,有

$$\mathrm{supp}(\rho^{k_2}(\lambda_{p_2})) \not\subset \mathrm{supp}(\rho^{k_1}(\nu_{p_1})) \Leftrightarrow \mathrm{supp}(\lambda_{p_2}) \not\subset \mathrm{supp}(\rho^{k_1-k_2+n}(\nu_{p_1})).$$

由 λ_{p_2}, ν_{p_1} 的定义有 $\{1, 2, \frac{n}{2}+p_2\} \subseteq \mathrm{supp}(\lambda_{p_2})$,对于任意的 k,$\{1, 2, \frac{n}{2}+p_2\} \not\subset \mathrm{supp}(\rho^k(\nu_{p_1}))$,从而 $\mathrm{supp}(\lambda_{p_2}) \not\subset \mathrm{supp}(\rho^k(\nu_{p_1}))$ 对于任意的 k 都成立。所以 $\mathrm{supp}(\rho^{k_2}(\lambda_{p_2})) \not\subset \mathrm{supp}(\rho^{k_1}(\lambda_{p_1}))$。因而当 $i < j$ 时,$a_{ij} = 0$。这就证明了 $A = (a_{ij})_{l_2 \times l_1}$ 的前 np 行为一 $np \times np$ 的下三角矩阵,则 $A = (a_{ij})_{l_2 \times l_1}$ 为列满秩矩阵。由引理 2 可得 $f(x)$ 为代数免疫度最优函数。

当 $\frac{n}{2}$ 为偶数时,类似可证明 $f(x)$ 为代数免疫度最优函数。

3　所构造函数的非线性度

首先介绍引理。根据 ρ_n^k 和 G_n 的定义,直接可得:

引理 2　对于 $1 \leqslant p \leqslant N$,有

(1)若 $\frac{n}{2}$ 是奇数,那么 $|G_n(\lambda_p)| = n$;

(2)若 $\frac{n}{2}$ 是偶数,那么

$|G_n(\lambda_1)| = \frac{n}{2}$ 且当 $p \neq 1$ 时 $|G_n(\lambda_p)| = n$.

设 $\mu \in \mathbb{F}_2^n$,并且 $w(\mu) = k$,令

$$K_i(k,n) = \sum_{w(x)=i} (-1)^{\mu \cdot x} = \sum_{j=0}^{i} (-1)^j \binom{k}{j}\binom{n-k}{i-j},$$

这里 $K_i(k,n)$ 是 Krawtchouk 多项式。

引理 3[4]　Krawtchouk 多项式有以下性质:

(1)$\binom{n}{k} K_i(k,n) = \binom{n}{i} K_k(i,n)$;

(2)对偶数 n,

$$K_i(\frac{n}{2}, n) = \begin{cases} 0, & i \text{ 为奇数}, \\ (-1)^{i/2}\binom{n/2}{i/2}, & i \text{ 为偶数}。\end{cases}$$

定理 2　设 $f(x)$ 是定理 1 中构造的函数,那么 $N(f) \geqslant 2^{n-1} - \binom{n-1}{n/2-1} + \frac{1}{8}(n^2 - 16n + 12)$。

证明　由 $G_n(\nu_p)$ 的定义,易知 $G_n(\nu_p)$ 是非自共轭轨道,存在 $W^{\frac{n}{2}}$ 的子集 A 满足:

$$G_n(\nu_p) \subset A, A \cup \bar{A} = W^{\frac{n}{2}} \text{ 且 } A \cap \bar{A} = \varnothing.$$

$$W_f(\mu) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x) \oplus \mu \cdot x}$$

$$= \sum_{W^{<\frac{n}{2}}} (-1)^{1 \oplus \mu \cdot x} - \sum_{T} (-1)^{1 \oplus \mu \cdot x} + \sum_{W^{\frac{n}{2}}} (-1)^{a(x) \oplus \mu \cdot x} + \sum_{W^{>\frac{n}{2}}} (-1)^{\mu \cdot x} + \sum_{T} (-1)^{\mu \cdot x}$$

$$= \begin{cases} -2K_{\frac{n}{2}-1}(t-1, n-1) + 2\sum_{T} (-1)^{\mu \cdot x}, & w(\mu) \text{ 为奇数}, \\ \sum_{W^{\frac{n}{2}}} (-1)^{a(x) \oplus \mu \cdot x} + 2\sum_{T} (-1)^{\mu \cdot x}, & w(\mu) \text{ 为偶数}。 \end{cases}$$

分别计算 $\sum_{T} (-1)^{\mu \cdot x}$ 与 $\sum_{W^{\frac{n}{2}}} (-1)^{a(x) \oplus \mu \cdot x}$,由引理 3 可得

(1) $w(\mu) = 0$ 时,有

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

$$= \begin{cases} N \cdot n, & \frac{n}{2} \text{ 为奇数}, \\ (N-1) \cdot n + \frac{n}{2}, & \frac{n}{2} \text{ 为偶数}。 \end{cases}$$

(2) $w(\mu) = 1$ 时,有

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

$$= \begin{cases} \sum_{1 \leqslant p \leqslant N} (n - 4p - 2) = \frac{n^2 - 8n + 12}{8}, & \frac{n}{2} \text{ 为奇数}, \\ \frac{n-4}{2} + \sum_{2 \leqslant p \leqslant N} (n - 4p) = \frac{(\frac{n}{2} - 2)^2}{2}, & \frac{n}{2} \text{ 为偶数}。 \end{cases}$$

(3) $w(\mu) = n$ 时,注意到

$$\sum_{x \in G_n(\lambda_q)} (-1)^{\mu \cdot x} = n - 2w(x),$$

所以若 $\frac{n}{2}$ 是奇数,

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

若 $\frac{n}{2}$ 是偶数,

$$\sum_{T} (-1)^{\mu \cdot x} = \sum_{1 \leqslant p \leqslant N} \sum_{x \in G_n(\lambda_p)} (-1)^{\mu \cdot x} = \frac{n-4}{2} + \sum_{2 \leqslant p \leqslant N} (n - 4p) = \frac{n}{2} + (N-1)n$$

(4) 当 $2 \leqslant w(\mu) \leqslant n-1$ 时,有

$$\left| \sum_{T} (-1)^{\mu \cdot x} \right| = \left| \sum_{1 \leqslant p \leqslant N} \sum_{x \in G_n(\lambda_p)} (-1)^{\mu \cdot x} \right| \leqslant N \cdot n$$

若 $a(x)$ 在 $W^{\frac{n}{2}}$ 上为平衡函数,则

$$\left| \sum_{W^{\frac{n}{2}}} (-1)^{a(x) \oplus \mu \cdot x} \right| \leqslant |W^{\frac{n}{2}}| - \left| \sum_{W^{\frac{n}{2}}} (-1)^{\mu \cdot x} \right| = |W^{\frac{n}{2}}| - |K_{n/2}(t, n)|$$

$$= |W^{\frac{n}{2}}| - \frac{\binom{n}{n/2}}{\binom{n}{t}} K_t(\frac{n}{2}, n) \leqslant \binom{n}{n/2} - \frac{\binom{n/2}{t/2}\binom{n}{n/2}}{\binom{n}{t}}$$

若 $a(x)$ 在 $W^{\frac{n}{2}}$ 上不平衡,则取 $a'(x)$ 为 $W^{\frac{n}{2}}$ 上的平衡函数且 $|a'(x) \neq a(x)| \leqslant \frac{n}{2}$,从而

$$\left| \sum_{W^{\frac{n}{2}}} (-1)^{a(x) \oplus \mu \cdot x} \right| \leqslant \left| \sum_{W^{\frac{n}{2}}} (-1)^{a'(x) \oplus \mu \cdot x} \right| + n$$

$$\leqslant |W^{\frac{n}{2}}| - \left| \sum_{W^{\frac{n}{2}}} (-1)^{\mu \cdot x} \right| + n$$

$$\leqslant \binom{n}{n/2} - \frac{\binom{n/2}{t/2}\binom{n}{n/2}}{\binom{n}{t}} + n$$

综上所述,当 $a(x)$ 在 $W^{\frac{n}{2}}$ 上为平衡函数时,有

$$|W_f(\mu)| = \begin{cases} n^2/2 - 3n, & w(u) = 0, \\ 2\binom{n-1}{n/2-1} - \frac{1}{4}(n^2 - 8n + 12), & w(u) = 1, n/2 \text{ 为奇数} \\ 2\binom{n-1}{n/2-1} - (n/2-2)^2, & w(u) = 1, n/2 \text{ 为偶数} \\ \left| -2K_{n/2}(t-1, n-1) + 2\sum_{T} (-1)^{\mu \cdot x} \right| \leqslant \frac{2}{n-1}\binom{n-1}{n/2-1} + \frac{n^2 - 6n}{2}, & 2 \leqslant w(u) \leqslant n-1, n/2 \text{ 为奇数} \\ \left| \sum_{W^{\frac{n}{2}}} (-1)^{a(x) \oplus \mu \cdot x} + 2\sum_{T} (-1)^{\mu \cdot x} \right| \leqslant \binom{n}{n/2} - \frac{\binom{n/2}{t/2}\binom{n}{n/2}}{\binom{n}{t}} + \frac{n^2 - 4n}{2}, & 2 \leqslant w(u) \leqslant n-1, n/2 \text{ 为偶数} \\ \left| 2\sum_{T} (-1)^{\mu \cdot x} \right| \leqslant \frac{n^2 - 6n}{2}, & w(\mu) = n \end{cases}$$

即 $|W_f(\mu)| \leqslant \binom{n}{n/2} - \frac{1}{4}(n^2 - 8n + 12)$；若 $a(x)$ 在 $W^{\frac{n}{2}}$ 上不平衡，则

$$|W_f(\mu)| \leqslant \binom{n}{n/2} - \frac{1}{4}(n^2 - 8n + 12) + n,$$

从而

$$N(f) \geqslant 2^{n-1} - \binom{n-1}{n/2-1} + \frac{1}{8}(n^2 - 12n + 12)$$

最后，我们对定理 2 中得到的下界和已有的下界结果进行了比较。当 n 为偶数时，文献[10]中推论 1 的下界结果为 $2^{n-1} - \binom{n-1}{n/2-1} - 1$，从表 1 中可知，本文所给出的下界有较大提升。

表 1 代数免疫度最优布尔函数的非线性度比较

Tab. 1 Comparison of nonlinearity of MAI functions

n	文献[10]	定理 2
14	$2^{13} - \binom{13}{6} - 1$	$2^{13} - \binom{13}{6} + 5$
16	$2^{15} - \binom{15}{7} - 1$	$2^{15} - \binom{15}{7} + \frac{19}{2}$
20	$2^{19} - \binom{19}{9} - 1$	$2^{19} - \binom{19}{9} + \frac{43}{2}$
28	$2^{27} - \binom{27}{13} - 1$	$2^{27} - \binom{27}{13} + \frac{115}{2}$
60	$2^{59} - \binom{59}{29} - 1$	$2^{59} - \binom{59}{29} + \frac{723}{2}$
80	$2^{79} - \binom{79}{39} - 1$	$2^{79} - \binom{79}{39} + \frac{1363}{2}$

4 所构造函数的代数次数

本节我们讨论构造函数的代数次数。对于布尔函数 f，$\deg f = n$ 当且仅当 f 的重量为奇数。如果定理 1 中 f 的重量 $w(f)$ 为奇数，则 $\deg f = n$，即 f 的代数次数达到最优，否则，只需对 f 稍作修改即可使其代数次数达到最优。由定理 1 中 f 的构造，存在 $y_0 \in W^{\frac{n}{2}} \backslash U$，$a(y_0) = 0$ 且 $G_n(y_0)$ 是非自共轭轨道。令

$$f(x) = \begin{cases} 1, & W^{<\frac{n}{2}} \cup \{(1,1,\cdots,1)\} \backslash T, \\ a(x), & W^{<\frac{n}{2}}, \\ 0, & W^{<\frac{n}{2}} \cup T \backslash \{(1,1,\cdots,1)\}. \end{cases} \tag{2}$$

此时 $w(f)$ 为奇数，$\deg f = n$，即代数次数达到最优。由引理 2 及定理 1 易得式(2)为代数免疫度最优函数，同时由于只是修改了一个点，非线性度至多减少 1。

5 结束语

旋转对称布尔函数是指在旋转变换作用输入变量时，函数取值不变的一类特殊布尔函数，这类函数具有良好的密码学性质。本文研究了旋转对称布尔函数的构造问题，我们构造了一类代数免疫度最优的偶数元 RotS 函数，与文献[10]中结果比较，非线性度有所提升，代数次数也可达到最优。然而，我们构造的布尔函数不是平衡的，同时也没有考虑弹性要求，如何构造高非线性度且满足弹性要求的布尔函数是我们下一步研究的重点。

参考文献(References)

[1] Carlet C. A method of construction of balanced functions with optimum algebraic Immunity [C] // Proceedings of the International Workshop on Coding and Cryptography, Wuyi Mountain, Fujian, China, June 11 – 15, 2007.

[2] Carlet C, Zeng X Y, et al. Further properties of several classes of boolean functions with optimum algebraic immunity [J]. Designs, Codes and Cryptography, 2009,52(3): 303 – 338.

[3] Carlet C, Dalai D K, Gupta K C, et al. Algebraic immunity for cryptographically significant boolean functions: analysis and construction[J]. IEEE Trans. Inf. Theory, 2006,52(7): 3105 – 3121.

[4] Dalai D K, Gupta K C, et al. Cryptographically significant boolean functions: construction and analysis in terms of algebraic immunity [G]. FSE, 2005,LNCS 3557:98 – 111

[5] Li N, Qu L J, et al. On the construction of boolean functions with optimal algebraic immunity [J]. IEEE Trans. on Information Theory,2008,54(3):1330 – 1334.

[6] Qu L J, Feng K Q, et al. Construction symmetric boolean functions with maximum algebraic immunity[J]. IEEE Trans. on Information Theory, 2009,55(5):2406 – 2412.

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

[8] Tu Z R, Deng Y P. A Class of 1-resilient function with high nonlinearity and algebraic immunity[EB/OL]. [2011 – 05 – 03] Cryptography ePrint. Archive, Report 2010/179, 2010. http://eprint. iacr. org.

[9] Zeng X Y, Carlet C, Shan J Y, et al. Balanced boolean functions with optimum algebraic immunity and high nonlinearity[EB/OL]. [2011 – 08 – 15] Cryptology ePrint Archive, Report 2010/534, 2010. http://eprint. iacr. org.

[10] 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 Qiang, CHEN Lusheng, FU Fangwei. Construction of Boolean functions with maximum algebraic immunity [J]. Journal of software, 2010, 21 (7): 1758 – 1767. (in Chinese)