最高非线性度旋转对称布尔函数与最优代数免疫函数

黄景廉 王 卓
(西北民族大学电气工程学院 兰州 730030)

摘 要 研究了旋转对称布尔函数的最高扩散次数、最高非线性度、代数免疫性和最优代数免疫函数的存在性与构造等问题。利用导数和e-导数证明了非线性度达到最高的旋转对称布尔函数的存在性,并利用导数,由扩散性达到最高n次的Bent函数来验证一类旋转对称Bent函数的存在性。同时证明了1阶代数免疫和2阶以上代数免疫旋转对称布尔函数的存在性。另外,利用旋转对称Bent函数构造了非齐次完全旋转对称最优代数免疫布尔函数以及一类众多的最优代数免疫布尔函数,并证明了这两类函数的存在性。同时,也得到了非齐次完全旋转对称相关免疫布尔函数。

关键词 旋转对称布尔函数,Bent函数,导数,最优代数免疫函数,相关免疫性

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.045

Highest Nonlinearity Rotation Symmetric Boolean Functions and Optimal Algebraic Immunity Function

HUANG Jing-lian WANG Zhuo
(School of Electrical Engineering, Northwest University for Nationalities, Lanzhou 730030, China)

Abstract In this paper, we studied the cryptographic properties of RSBFs, including the highest number of propagation, the highest nonlinearity and algebraic immunity, and also studied the problems of the existence and the construction of the optimal algebraic immunity function. Using the derivative and the e-derivative of the Boolean functions, we proved that there exist RSBFs whose nonlinearity is the highest, and verified the existence of a type of RSBFs from Bent functions whose propagation reaches n degree. Moreover, we also proved the existence of RSBFs with algebraic immunity by one-order or higher than two-order. We constructed inhomogeneous complete RSBFs with the optimal algebraic immunity and a large number of the optimal algebraic immunity Boolean functions from rotation symmetric Bent functions, and proved the existence of the two types of functions. Meanwhile, we also obtained inhomogeneous complete RSBFs with correlation immunity.

Keywords RSBFs, Bent function, Derivative, Optimal algebraic immunity function, Correlation immunity

1 引言

代数免疫性、最优代数免疫、非线性度、最高非线性度、扩散性、高次扩散性、相关免疫性都是密码函数非常重要的安全性质。对这些性质的研究一直都在进行,特别是近些年提出的抵抗代数攻击的代数免疫性[1],受到了人们更多的关注并涌现了许多方法[2-7]。除此之外,在构造布尔函数时也需要考虑其它密码学性质,如扩散性、相关免疫性和非线性度等。

Bent函数和旋转对称布尔函数(Rotation Symmetric Boolean Functions, RSBFs)都是密码学中的重要函数,是密码学界一直在认真研究的对象[8-14]。Bent函数是一类结构最简单的完全非线性函数,具有最优的非线性性,能够有效抵抗线性密码攻击[15]。旋转对称布尔函数由于具有良好的密码性质[11],从而成为密码学函数的一类优良选择,在密码学的多个方面有着广泛的应用。而旋转对称布尔函数中是否也含有Bent函数,如何用Bent函数构造出最优代数免疫旋转对称布尔函数等是需要研究的重要问题。如果以导数和e-导数作为新的研究工具,这些问题就较容易解决。本文将利用导数和e-导数来讨论旋转对称布尔函数的非线性度、扩散性、代数免疫性、旋转对称Bent函数的存在性和结构、最优代数免疫旋转对称布尔函数的存在性及构造等问题。

2 预备知识

布尔函数的导数是人们所熟知的[16]。需要给出布尔函数e-导数的概念。e-导数与导数的关系及e-导数的性质可参阅文献[17-19]。

定义1 设$n\in I_+$,对任意$x=(x_1,x_2,\cdots,x_n)\in GF(2)^n$,$k\in I_+$,且$0\leqslant k\leqslant n-1$,定义$\rho_n^k(x)=(\rho_n^k(x_1),\rho_n^k(x_2),\cdots,\rho_n^k(x_n))$,其中

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

若对任意$x=(x_1,x_2,\cdots,x_n)\in GF(2)^n$,有$f(\rho_n^k(x))=f(x)$,$0\leqslant k\leqslant n-1$,则称$f(x)$为旋转对称布尔函数。

定义2 若n元布尔函数$f(x)=f(x_1,x_2,\cdots,x_n)\in$

到稿日期:2015-09-05 返修日期:2015-11-06 本文受国家自然科学基金项目(61262085)资助。

黄景廉(1968-),女,教授,主要研究方向为计算机网络通信与信息安全、密码学,E-mail:huangjlstudy@163.com;王 卓(1944-),男,教授,主要研究方向为数学、布尔代数、分布式系统、计算机信息安全。

$GF(2)^{GF(2)^n}$，有且仅有 $k(k\in I_+)$ 次项，称 $f(x)$ 为 k 次齐次布尔函数；若 $f(x)$ 有且仅有 $\binom{n}{k}$ 个不同的 k 次项，则称 $f(x)$ 为完全 k 次齐次布尔函数，记为 $f_0^k(x)(k\in I_+)$。

由定义 1 可知，$f_0^k(x)$ 是旋转对称布尔函数，所以也称 $f_0^k(x)(k\in I_+)$ 为完全 k 次齐次旋转对称布尔函数。显然，完全 k 次齐次旋转对称布尔函数只是 k 次齐次旋转对称布尔函数中的一种函数。$f_0^r(x)+f_0^k(x)(r,k\in I_+,r\neq k)$ 可称为非齐次完全旋转对称布尔函数，或完全旋转对称布尔函数。

定义 3[16] n 元布尔函数 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ 对 r 个变元 $x_{i1},x_{i2},\cdots,x_{ir}$ 的导数（偏导数）表示和定义为：

$$\frac{\partial f(x)}{\partial(x_{i1},x_{i2},\cdots,x_{ir})}=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)+f(x_1,x_2,\cdots,\overline{x_{i1}},\overline{x_{i2}},\cdots,\overline{x_{ir}},\cdots,x_n)$$

$$1\leqslant i\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n,1\leqslant r\leqslant n \quad (1)$$

当 $r=1$ 时，式(1)即为 $f(x)=f(x_1,x_2,\cdots,x_n)$ 对单个变元的导数，记为 $\frac{df(x)}{dx_i}(i=1,2,\cdots,n)$。经简单的计算化简，可得到如下便于使用的形式：

$$\frac{df(x)}{dx_i}=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)+f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n),i=1,2,\cdots,n$$

定义 4[17,18] n 元布尔函数 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ 对 r 个变元 $x_{i1},x_{i2},\cdots,x_{ir}$ 的 e-导数（e-偏导数）表示和定义为：

$$\frac{ef(x)}{e(x_{i1},x_{i2},\cdots,x_{ir})}=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)\cdot f(x_1,x_2,\cdots,\overline{x_{i1}},\overline{x_{i2}},\cdots,\overline{x_{ir}},\cdots,x_n)$$

$$1\leqslant i\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n,1\leqslant r\leqslant n \quad (2)$$

当 $r=1$ 时，式(2)即为 $f(x)=f(x_1,x_2,\cdots,x_n)$ 对单个变元的 e-导数，记为 $ef(x)/ex_i(i=1,2,\cdots,n)$。经简单的计算化简，可得到如下便于使用的形式：

$$\frac{ef(x)}{ex_i}=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n),i=1,2,\cdots,n$$

定义 5 若 $f(x)\in GF(2)^{GF(2)^n}$ 对所有 $\alpha\in GF(2)^n(1\leqslant w_t(\alpha)\leqslant k,k\in I_+)$ 都有 $w_t(f(x+\alpha)+f(x))=2^{n-1}$，则称 $f(x)$ 满足 k 次扩散准则，或 $f(x)$ 是 k 次扩散函数。

Bent 函数是密码学中重要的函数，也能用扩散准则来定义。即称函数 $f(x)\in GF(2)^{GF(2)^n}$ 为 Bent 函数，当且仅当 $f(x)$ 是 n 次扩散函数[16]。

定义 6 对任意满足 $1\leqslant w_t(\omega)\leqslant m$ 的 n 元向量 $\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in GF(2)^n$，函数 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ 都有 $w_t(f(x)+\omega x)=2^{n-1}(\omega x=\omega_1x_1+\omega_2x_2+\cdots+\omega_nx_n)$，则称 $f(x)$ 为 m 阶相关免疫函数，m 称为阶数。

定义 7 对函数 $f(x)\in GF(2)^{GF(2)^n}$，若有 $g(x)\in GF(2)^{GF(2)^n}$ 使 $g(x)f(x)=0$，则称 $g(x)$ 是 $f(x)$ 的零化子。$f(x)$ 和 $1+f(x)$ 的所有非零零化子中最低代数次数零化子的代数次数，称为 $f(x)$ 的代数免疫阶，记为 $AI(f(x))$ 或 $AI(f)$。若 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$，则称 $f(x)$ 为最优代数免疫函数。

通常以 $\deg f(x)$ 表示 $f(x)$ 的代数次数。

设 $L_n[x]=\{\omega x+\omega_0\mid\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in GF(2)^n,x=(x_1,x_2,\cdots,x_n)\in GF(2)^n,\omega_0\in GF(2)\}$，即 $L_n(x)$ 是 $GF(2)$ 上所有 n 元线性函数为元素的集合。

定义 8 对 $f(x)\in GF(2)^{GF(2)^n}$，定义 $N_f=\min\limits_{l(x)\in L_n[x]}w_t(f(x)+l(x))$ 为 $f(x)$ 的非线性度。

也可用非线性度来定义 Bent 函数。对 $f(x)\in GF(2)^{GF(2)^n}$，若 $N_f=2^{n-1}-2^{\frac{n}{2}-1}$，则称 $f(x)$ 为 Bent 函数。

根据上述定义，可容易地得到引理 1—引理 3。

引理 1 布尔函数 $f(x)\in GF(2)^{GF(2)^n}$ 是 k 次扩散函数的充分必要条件是，对一切 $1\leqslant r\leqslant k$，都有 $w_t(\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir}))=2^{n-1}(i\in I_+,r\in I_+,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_k\leqslant k\leqslant n)$。

引理 2 对任意布尔函数 $f(x)\in GF(2)^{GF(2)^n}$，有

$$f(x)=f(x)\frac{\partial f(x)}{\partial(x_{i1},x_{i2},\cdots,x_{ir})}+\frac{ef(x)}{e(x_{i1},x_{i2},\cdots,x_{ir})}=f(x)\frac{df(x)}{dx_j}+\frac{ef(x)}{ex_j}$$

$$1\leqslant i\leqslant n,1\leqslant r\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n,j\in I_+$$

引理 3 设 $x'=(x_2,x_3,\cdots,x_n)$，记 $f_{0,n-1}^e(x')$ 为 $n-1$ 元完全 2 次齐次旋转对称布尔函数，$f_{0,n-1}^1(x')$ 为 $n-1$ 元完全 1 次齐次旋转对称布尔函数。则有

$$\begin{aligned}f_{0,n}^e(x)&=f_{0,n-1}^e(x')+x_1\sum_{i=2}^{n}x_i\\&=f_{0,n-1}^e(x')+x_1(f_{0,n-1}^e(x')+\sum_{i=2}^{n}x_i+f_{0,n-1}^e(x'))\\&=(1+x_1)f_{0,n-1}^e(x')+x_1(f_{0,n-1}^1(x')+f_{0,n-1}^e(x'))\end{aligned}$$

利用这一递推公式，容易推出 n 为偶数时，$f_0^e(x)$ 的重量为 $w_t(f_0^e(x))=2^{n-1}\pm2^{\frac{n}{2}-1}$（“+”或“−”依赖于 n 的取值。如 $n=4$、$n=6$ 时取的是“+”，$n=8$、$n=10$ 时取的是“−”）。

因本文后面要用到 $f_0^e(x)$ 的重量，故这里简略推出。

3 完全 2 次齐次旋转对称布尔函数与 Bent 函数、相关免疫函数

定理 1 先讨论完全 2 次齐次旋转对称布尔函数的性质。

定理 1 对元数 n 为偶数的完全 2 次齐次旋转对称布尔函数 $f_0^2(x)$：

1) 当 $w_t(f_0^2(x))=2^{n-1}+2^{\frac{n}{2}-1}$ 时，对 $l_{01}(x)=1+\frac{df_0^2(x)}{dx_n}$，有

$$N_{f_0^2}=w_t(f_0^2(x)+l_{01}(x))=\min_{l(x)\in L_n[x]}w_t(f_0^2(x)+l(x))=2^{n-1}-2^{\frac{n}{2}-1}$$

2) 当 $w_t(f_0^2(x))=2^{n-1}-2^{\frac{n}{2}-1}$ 时，对 $l_{02}(x)=\frac{df_0^2(x)}{dx_n}$，有

$$N_{f_0^2}=w_t(f_0^2(x)+l_{02}(x))=\min_{l(x)\in L_n[x]}w_t(f_0^2(x)+l(x))=2^{n-1}-2^{\frac{n}{2}-1}$$

证明：

1) 由引理 2，经简单计算推导，有

$$w_t(f_0^2(x)+l(x))=w_t(f_0^2(x)\frac{df_0^2(x)}{dx_n}+l(x))+w_t(\frac{ef_0^2(x)}{ex_n+l(x)})-w_t(l(x))$$

由于 $f_0^2(x)$ 是完全 2 次齐次旋转对称布尔函数，含变量

x_n 的项有且仅有 $x_n\sum_{i=1}^{n-1}x_i$。所以有

$$\deg\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}=\deg\sum_{i=1}^{n-1}x_i=1$$

$$w_t\left(\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}\right)=2^{n-1}$$

$$w_t\left(f_0^2(x)\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}\right)=2^{n-2}$$

和

$$w_t\left(\frac{\mathrm{e}f_0^2(x)}{\mathrm{e}x_n}\right)=2^{n-2}\pm2^{\frac{n}{2}-1}$$

故当 $w_t(f_0^2(x))=2^{n-1}+2^{\frac{n}{2}-1}$，即 $w_t\left(\frac{\mathrm{e}f_0^2(x)}{\mathrm{e}x_n}\right)=2^{n-2}+2^{\frac{n}{2}-1}$ 时，取 $l_{01}(x)=1+\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}$，有

$$w_t\left(f_0^2(x)\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}+l_{01}(x)\right)=2^{n-1}+2^{n-2}$$

$$w_t\left(\frac{\mathrm{e}f_0^2(x)}{\mathrm{e}x_n}+l_{01}(x)\right)=2^{n-2}-2^{\frac{n}{2}-1}$$

所以有

$$\begin{aligned}N_{f_0^2}&=w_t(f_0^2(x)+l_{01}(x))\\&=(2^{n-1}+2^{n-2})+(2^{n-2}-2^{\frac{n}{2}-1})-2^{n-1}\\&=2^{n-1}-2^{\frac{n}{2}-1}\end{aligned}$$

2）当 $w_t(f_0^2(x))=2^{n-1}-2^{\frac{n}{2}-1}$，即 $w_t\left(\frac{\mathrm{e}f_0^2(x)}{\mathrm{e}x_n}\right)=2^{n-2}-2^{\frac{n}{2}-1}$ 时，取 $l_{02}(x)=\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}$，有

$$w_t\left(f_0^2(x)\frac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_n}+l_{02}(x)\right)=2^{n-2},$$

$$w_t\left(\frac{\mathrm{e}f_0^2(x)}{\mathrm{e}x_n}+l_{02}(x)\right)=2^{n-1}+2^{n-2}-2^{\frac{n}{2}-1}$$

所以有

$$\begin{aligned}N_{f_0^2}&=w_t(f_0^2(x)+l_{02}(x))\\&=(2^{n-2})+(2^{n-1}+2^{n-2}-2^{\frac{n}{2}-1})-(2^{n-1})\\&=2^{n-1}-2^{\frac{n}{2}-1}\end{aligned}$$

证毕。

由 Bent 函数的定义可知，$f_0^2(x)$（n 为偶数）是 Bent 函数，从而 $f_0^2(x)$（n 为偶数）是 n 次扩散函数，这一点利用导数也容易直接证明：

对 n 为偶数，$1\leqslant r\leqslant n$，当 r 为奇数时，有

$$\begin{aligned}&w_t\left(\frac{\partial f_0^2(x)}{\partial(x_{i1},x_{i2},\cdots,x_{ir})}\right)\\&=w_t(\underbrace{(1+1+\cdots+1)}_{\binom{r}{1}\uparrow1}+\sum_{p=1}^{n}x_p+x_{i1}+x_{i2}+\cdots+x_{ir})\\&=2^{n-1}\end{aligned}$$

而当 r 为偶数时，有

$$\begin{aligned}&w_t\left(\frac{\partial f_0^2(x)}{\partial(x_{i1},x_{i2},\cdots,x_{ir})}\right)\\&=w_t(\underbrace{(1+1+\cdots+1)}_{\binom{r}{2}\uparrow1}+x_{i1}+x_{i2}+\cdots+x_{ir})\\&=2^{n-1}\end{aligned}$$

注意到是对任意 $1\leqslant r\leqslant n$ 的 r 求导，并由引理 1 即知 $f_0^2(x)$（n 为偶数）是 n 次扩散函数。

推论 1 n 为偶数时，$f_0^2(x)$ 是 Bent 函数。

推论 2 偶数元完全 2 次齐次旋转对称布尔函数是 n 次扩散函数。

当 n 为奇数时，$f_0^2(x)$ 是相关免疫函数，有定理 2。

定理 2 元数 $n\geqslant5$ 且 n 为奇数时，完全 2 次齐次旋转对称布尔函数是相关免疫函数。

证明：在 n 元完全 2 次齐次旋转对称布尔函数 $f_0^2(x)$ 的所有项中，含每一个变元 x_i 的项为 $n-1$ 项，即含 $n-1$ 个 x_i。当 n 为奇数时，$n-1$ 为偶数。所以

$$\frac{\partial f_0^2(x)}{\partial(x_1,x_2,\cdots,x_n)}=\sum_{1\leqslant i<j\leqslant n}(1+x_i+x_j)=0$$

故有

$$w_t(f_0^2(x)|x_i=0)=w_t(f_0^2(x)|x_i=1)=2^{-1}w_t(f_0^2(x))$$

故对所有 $w_t(\omega)=1$ 的 ωx，有 $w_t(f_0^2(x)+\omega x)=2^{n-1}$。因此，$n$ 为奇数时，$f_0^2(x)$ 是相关免疫函数。证毕。

从定理 1、定理 2 可以看出，完全 2 次齐次旋转对称布尔函数 $f_0^2(x)$ 有多种良好密码学性质。由于 $f_0^2(x)$ 具有完全 2 次齐次旋转对称的特点，因此利用 $f_0^2(x)$ 易于构造出最优代数免疫旋转对称布尔函数（$f_0^2(x)$ 本身是 2 阶代数免疫函数）。本文将在后面讨论这一问题。

4 旋转对称布尔函数与最优代数免疫函数

本节讨论旋转对称布尔函数的代数免疫问题及构造最优代数免疫函数问题。

定理 3 若有非齐次完全旋转对称布尔函数

$$f(x)=f_0^0(x)+f_0^3(x)+f_0^4(x)+\cdots+f_0^{n-1}(x)+f_0^n(x)$$

且 n 为奇数，则 $f_0^1(x)$ 是 $f(x)$ 的最低代数次数零化子，$AI(f)=1$。

证明：对任意奇数 i，$f_0^1(x)f_0^{i-1}(x)$ 乘积项可有 $i-1$ 次项和 i 次项，其中 $i-1$ 为偶数。于是乘积中每个 $i-1$ 次项共有 $\binom{i-1}{1}=i-1$ 个项，故和为 0，即乘积结果无 $i-1$ 次数。又因乘积中每个 i 次项共有 $\binom{i}{1}=i$ 个项，故每个 i 次项都最终存在。又 $f_0^1(\rho_n^k(x))f_0^{i-1}(\rho_n^k(x))=f_0^1(x)f_0^{i-1}(x)$，所以，$f_0^1(x)f_0^{i-1}(x)=f_0^i(x)$。

而 $f_0^1(x)f_0^i(x)$ 同样由于 $\binom{i}{1}=i$，$\binom{i+1}{1}=i+1$ 而必有 $f_0^1(x)f_0^i(x)=f_0^i(x)$，故必有

$$f_0^1(x)(f_0^{i-1}(x)+f_0^i(x))=f_0^i(x)+f_0^i(x)=0$$

又知 i 任意，所以

$$\begin{aligned}f_0^1(x)f(x)=&f_0^1(x)f_0^2(x)+f_0^1(x)f_0^3(x)+f_0^1(x)f_0^4(x)+\\&f_0^1(x)f_0^5(x)+\cdots+f_0^1(x)f_0^{n-1}(x)+f_0^1(x)\\&f_0^n(x)\\=&0\end{aligned}$$

又 $\deg f_0^1(x)=1$，所以 $f_0^1(x)$ 是 $f(x)$ 的最低代数次数零化子，$AI(f)=1$。

证毕。

根据定理 3 易得到定理 4。

定理 4 若有非齐次完全旋转对称布尔函数

$$f(x)=f_0^0(x)+f_0^3(x)+f_0^4(x)+\cdots+f_0^{n-1}(x)+f_0^n(x)$$

且 n 为偶数，则必有 $AI(f)\geqslant2$。

证明：由于 $f(x)$ 中 n 为偶数，由定理 3 的证明可知，有

$f_0^1(x)f(x)=f_0^1(x)f_0^n(x)=f_0^{n+1}(x)$，即 $f_0^1(x)$不是 $f(x)$的零化子。

对任意不为 $f_0^1(x)$的非旋转对称的1次函数 $g(x)$，$g(x)$必含有 $f_0^1(x)$的部分项而不含 $f_0^1(x)$的某些1次项。为简便且不失一般性，不妨设 $g(x)=f_0^1(x)+x_1$，则

$$\begin{aligned}g(x)f(x)=&\overbrace{(f_0^{n+1}(x)+f_0^{n+1}(x)+\cdots+f_0^{n+1}(x))}^{\text{偶数项}(n-1)-1\text{项}}+\\&f_0^1(x)f_0^n(x)+x_1(f_0^2(x)+f_0^3(x)+\cdots+\\&f_0^{n-1}(x)+f_0^n(x))\\=&f_0^1(x)f_0^n(x)+x_1(f_0^2(x)+f_0^3(x)+\cdots+\\&f_0^{n-1}(x)+f_0^n(x))\\=&f_0^{n+1}(x)+x_1(f_0^2(x)+f_0^3(x)+\cdots+\\&f_0^{n-1}(x)+f_0^n(x))\\\neq&0\end{aligned}$$

故 $f(x)$没有1次零化子，所以 $AI(f)\geqslant 2$。证毕。

推论3 对于非齐次完全旋转对称布尔函数

$$f(x)=f_0^1(x)+f_0^3(x)+(f_0^4(x)+f_0^6(x))+(f_0^8(x)+f_0^{10}(x))+\cdots+(f_0^{2k+2}(x)+f_0^{2k+4}(x)),k=1,2,\cdots$$

有 $AI(f)=2$，且 $f_0^2(x)$是 $f(x)$的最低代数次数零化子。

推论3的证明与定理3、定理4相似，不再详证。

定理5讨论旋转对称布尔函数的最优代数免疫函数问题。

定理5

1）2^n元的非齐次完全旋转对称布尔函数

$$f(x)=f_0^2(x)+f_0^4(x)+f_0^8(x)+\cdots+f_0^{2^{n-1}}(x)$$

是最优代数免疫函数。

2）用2次齐次完全旋转对称 Bent 函数 $f_0^2(x)$可构造出一族最优代数免疫函数。

证明：

1）由于对任何 $r<i(i=4,8,\cdots,2^{n-1})$，由杨辉三角中组合数的性质知，必有 $f_0^{2^r}(x)f_0^{2^i}(x)=f_0^{2^i+2^r}(x)(i=4,8,\cdots,2^{n-1})$。因此对任意代数次数 2^r 次的函数 $f_{2^r}(x)$，只要 $f_{2^r}(x)f_0^2(x)$，$f_{2^r}(x)f_0^4(x)$，$\cdots$，$f_{2^r}(x)f_0^{2^{n-1}}(x)$这些乘积不全为0，则必有 $f_{2^r}(x)f_0^{2^i}(x)=f_{2^r+2^i}(x)$，即 $\deg f_{2^r+2^i}(x)=2^r+2^i$。因此 $f(x)$的非零零化子有 $1+f(x)$和使 $g(x)f_0^2(x)$，$g(x)f_0^4(x)$，$\cdots$，$g(x)f_0^{2^{n-1}}(x)$均为0的非零 $g(x)$。

由于 $\dfrac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_{2^n}}=f_0^1(x')(x'=x_1x_2\cdots x_{2^n-1})$，即 x'是 2^{n-1}元的变量向量。同样，$\dfrac{\mathrm{d}(1+f_0^2(x))}{\mathrm{d}x_{2^n}}=\dfrac{\mathrm{d}f_0^2(x)}{\mathrm{d}x_{2^n}}=f_0^1(x')(x'=x_1x_2\cdots x_{2^n-1})$。因此 $f_0^2(x)$只有2次最低代数次数零化子。4元的 $f_0^2(x)$的最低代数次数零化子为2次，设为 $g'(x)$。但

$$\begin{aligned}&g'(x)[f_0^2(x)+x_1x_2x_3x_4]\\&=g'(x)f_0^2(x)+g'(x)x_1x_2x_3x_4\\&=g'(x)x_1x_2x_3x_4=x_1x_2x_3x_4\neq 0\end{aligned}$$

所以4元函数 $f_0^2(x)+x_1x_2x_3x_4$ 的最低代数次数零化子为3次。设4元函数 $f_0^2(x)+x_1x_2x_3x_4$ 的最低代数次数零化子3次多项式为 $g''(x)$。

由于

$$\begin{aligned}&f_0^2(x)f_0^4(x)=f_0^6(x),f_0^2(x)f_0^8(x)\\&=f_0^{10}(x),\cdots,f_0^2(x)f_0^{2^{n-1}}(x)\\&=f_0^{2^n}(x)\end{aligned}$$

因此 $f_0^2(x)$和 $f_0^{2^i}(x)$的零化子也是 $f_0^{2^i+2}(x)$的零化子。故4元 $f_0^2(x)+x_1x_2x_3x_4$ 的零化子 $g''(x)$经逐级与0级联变为 2^n 元多项式时的多项式 $g(x)$有 $\deg g(x)>2^{n-1}$。而 $g(x)$便是使 $g(x)f_0^2(x)$，$g(x)f_0^4(x)$，$g(x)f_0^8(x)$，$\cdots$，$g(x)f_0^{2^{n-1}}(x)$均为0的最低代数次数多项式，即为 $f(x)$的零化子。

因此，$f(x)$除了零化子 $1+f(x)$和 $g(x)$外，再无其它零化子。故 $f(x)$只有最低代数次数零化子 $1+f(x)$。同理，$1+f(x)$只有最低代数次数零化子 $f(x)$。所以 $AI(f(x))=2^{n-1}$。又因 $f(x)$是 2^n 元函数，故 $f(x)$是最优代数免疫函数。显然，正是由于 $f(x)$是 2^n 元函数，才保证了 $\deg g(x)>2^{n-1}$。

2）若记 $(f_0^8(x))'$，$(f_0^{16}(x))'$，$\cdots$，$(f_0^{2^{n-1}}(x))'$分别为从 $f_0^8(x)$，$f_0^{16}(x)$，$\cdots$，$f_0^{2^{n-1}}(x)$中各自取出的适当的项构成的相应的函数，则由1）的证明可知，可使函数

$$f'(x)=f_0^2(x)+f_0^4(x)+(f_0^8(x))'+(f_0^{16}(x))'+\cdots+(f_0^{2^{n-1}}(x))'$$

只有最低代数次数零化子 $1+f'(x)$。同样，$1+f'(x)$也只有最低代数次数零化子 $f'(x)$。故 2^n 元函数 $f'(x)$是最优代数免疫函数。$f'(x)$中，$f_0^2(x)$是2次齐次完全旋转对称 Bent 函数（由定理1知）。而对 $(f_0^8(x))'$，$(f_0^{16}(x))'$，$\cdots$，$(f_0^{2^{n-1}}(x))'$做不同的选取，则构成不同的 $f'(x)$。所以 $f'(x)$是一族由 Bent 函数 $f_0^2(x)$构成的最优代数免疫函数。证毕。

例 $f_0^2(x)+f_0^4(x)+f_0^8(x)$是 $AI(f)=4$ 的8元最优代数免疫函数。

结束语 旋转对称布尔函数和 Bent 函数都是密码学中的重要函数。本文研究了旋转对称 Bent 函数的相关性质，证明了1阶代数免疫和2阶以上代数免疫完全旋转对称布尔函数的存在性。并且，在本文得到的一类相关免疫的齐次完全旋转对称布尔函数的基础上，构造出了非齐次完全旋转对称最优代数免疫函数和一类众多的最优代数免疫函数。以上结果反映出了旋转对称布尔函数的一些组合性质具有很大意义。同时，本文运用导数和e-导数来证明相关定理，说明导数和e-导数是很有用的研究工具。

参 考 文 献

[1] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback[C]// Advances in Cryptology-EUROCRYPT 2003. Warsaw, Poland, 2003, LNCS, 2656: 345-359

[2] Carlet C, Zeng X Y. 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. A method of construction of balanced functions with optimum algebraic immunity[C]// Proceedings of the First International Workshop on Coding and Cryptography. Fujian, 2007: 25-43

[4] Li Y, Yang M, Kan H B. Constructing and counting Boolean functions on even variables with maximum algebraic immunity [J]. IEICE Transactions on Fundamentals, 2010, 93-A(3): 640-643

（下转第241页）

的模型与方法[D]. 昆明:云南大学,2012

[17] Miladi M N, Jmaiel M, Kacem M H. A UML profile and a FUJABA plugin for modelling dynamic software architectures[C]// Proc. of the Workshop on Model-Driven Software Evolution. Washington: IEEE Press, 2007: 20-26

[18] Kacem M H, Kacem A H, Jmaiel M, et al. Describing dynamic software architectures using an extended UML model[C]// Proc. of the Symp. on Applied Computing. New York: ACM Press, 2006: 1245-1249

[19] Bruni R, Bucchiarone A, Gnesi S, et al. Modelling dynamic software architectures using typed graph grammars[J]. Electronic Notes in Theoretical Computer Science, 2008, 213(1): 39-53

[20] Abi-Antoun M, Aldrich J, Garlan D, et al. Modeling and implementing software architecture with acme and archJava[C]// Proc. of the 27th Int'l Conf. on Software Engineering. New York: ACM Press, 2005: 676-677

[21] Mei H, Chen F, Wang Q X, et al. ABC/ADL: An ADL supporting component composition[C]// ICFEM 2002. Shanghai, 2002: 38-47

[22] Ding Bo, Wang Huai-min, Shi Dian-xi, et al. Component Model Supporting Trustworthiness-Oriented Software Evolution[J]. Journal of Software, 2011, 22(1): 17-27(in Chinese)
丁博,王怀民,史殿习,等. 一种支持软件可信演化的构件模型[J]. 软件学报,2011,22(1):17-27

[23] Zhao Hui-qun, Sun Jing. An Algebraic Model of Service Oriented Trustworthy Software Architecture[J]. Chinese Journal of Computer, 2010, 33(5): 890-899(in Chinese)
赵会群,孙晶. 面向服务的可信软件体系结构代数模型[J]. 计算机学报,2010,33(5):890-899

[24] Wang Ying-hui, Liu Yu, Wang Li-fu. SA Dynamic Evolution Model Based on Static-Point Transition[J]. Chinese Journal of Computer, 2004, 27(11): 1451-1456(in Chinese)
王映辉,刘瑜,王立福. 基于不动点转移的 SA 动态演化模型[J]. 计算机学报,2004,27(11):1451-1456

[25] OSGi Service platform [OL]. http://core.ac.uk/display/38522655

[26] Huang G, Mei H, Yang F Q. Runtime software architecture based on reflective middleware[J]. Science in China(Series E), 2004, 34(2): 121-138(in Chinese)
黄罡,梅宏,杨芙清. 基于反射式软件中间件的运行时软件体系结构[J]. 中国科学(E 辑),2004,34(2):121-138

[27] Ma X X, Cao C, Yu P, et al. A supporting environment based on graph grammar for dynamic software architectures[J]. Journal of Software, 2008, 19(8): 1881−1892(in Chinese)
马晓星,曹春,余萍,等. 基于图文法的动态软件体系结构支撑环境[J]. 软件学报,2008,19(8):1881-1892

[28] Xie Zhong-wen, Li Tong, Dai Fei, et al. Modelling Dynamic Evolution-oriented Software Architecture Based on Petri Net[J]. Computer Applications and Software, 2012, 29(10): 36-39, 127(in Chinese)
谢仲文,李彤,代飞,等. 基于 Petri 网的面向动态演化的软件体系结构建模[J]. 计算机应用与软件,2012,29(10):36-39,127

(上接第 233 页)

[5] Rizomiliotis P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation[J]. IEEE Transactions on Information Theory, 2010, 56(8): 4014-4024

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

[7] Wang Q, Peng J, Kan H, et al. Constructions of cryptographically significant Boolean functions using primitive polynomials[J]. IEEE Transactions on Information Theory, 2010, 56(6): 3048-3053

[8] Li C L, Zhang H G, Zeng X Y, et al. The lower bound on the second-order nonlinearity for a class of Bent functions[J]. Chinese Journal of Computers, 2012, 35(8): 1588-1593(in Chinese)
李春雷,张焕国,曾祥勇,等. 一类 Bent 函数的二阶非线性度下界[J]. 计算机学报,2012,35(8):1588-1593

[9] Sarkar S, Gangopadhyay S. On the second order nonlinearity of a cubic Maiorana-McFarland Bent Functions[J]. International Journal of Foundations of Computer Science, 2010, 21(3): 243-254

[10] Su S H, Tang X H. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity[J]. Designs, Codes and Cryptography, 2014, 71(2): 183-199

[11] Chen Y D, Zhang Y N, Tian W. Construction of Even-variable Rotation Symmetric Boolean Functions with Optimal Algebraic Immunity[J]. Journal of Cryptologic Research, 2014, 1(5): 437-448(in Chinese)
陈银冬,张亚楠,田威. 具有最优代数免疫度的偶数元旋转对称布尔函数的构造[J]. 密码学报,2014,1(5):437-448

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

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

[14] Dong D S, Li C, Qu L J, et al. Rotation symmetric Boolean functions in even-variable maximum algebraic immunity[J]. Journal of National University of Defense Technology, 2012, 34(4): 85-89(in Chinese)
董德帅,李超,屈龙江,等. 偶变元 MAI 旋转对称布尔函数[J]. 国防科技大学学报,2012,34(4):85-89

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

[16] 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

[17] Li W, Wang Z, Huang J. The e-derivative of boolean functions and its application in the fault detection and cryptographic system[J]. Kybernetes, 2011, 40(5/6): 905-911

[18] Huang J L, Wang Z. The relationship between correlation immune and weight of H Boolean function[J]. Journal on Communications, 2012, 33(2): 110-118(in Chinese)
黄景廉,王卓. H 布尔函数的相关免疫性与重量的关系[J]. 通信学报,2012,33(2):110-118

[19] Zhao M L. Method of detecting special logic function based on Boolean e-derivative[J]. Journal of Zhejiang University (Science Edition), 2014, 41(4): 424-426(in Chinese)
赵美玲. 基于布尔 e 导数的特殊逻辑函数检测方法[J]. 浙江大学学报(理学版),2014,41(4):424-426