doi:10.3969/j.issn.1000-436x.2013.01.010

一类对称布尔函数的研究

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

摘 要：主要讨论了一类对称布尔函数(记为$\hat{A}$)的性质。提供了不同的方法证明$\hat{A}$的一个子类具有最大代数免疫阶。给出了$\hat{A}$中函数达到最大代数免疫阶的一个必要条件，并得到了满足此必要条件的布尔函数个数的下界。同时给出了$\hat{A}$中大部分函数的代数次数，分析了$\hat{A}$中函数的线性结构和相关免疫性。结果表明，$\hat{A}$中函数没有非零的线性结构且仅有 2 个函数具有一阶相关免疫性。

关键词：对称布尔函数；代数免疫阶；相关免疫性；非线性度
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2013)01-0089-07

On one class of symmetric Boolean functions

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

Abstract: The properties of one class of symmetric Boolean funct which was denoted by$\hat{A}$ was discussed, a different method for proving that one subclass of $\hat{A}$ having maximum algebraic immunity was presented. A necessary condition was proposed for the functions of $\hat{A}$ with maximum algebraic immunity, of which a lower bound of the number was also given. Meanwhile, the algebraic degree of most functions of $\hat{A}$ was determined and linear structure and correlation immunity of$\hat{A}$ were also analyzed. The results show that the functions of $\hat{A}$ have no non-zero linear structure and only two functions of$\hat{A}$ have 1-correlation immunity.

Key words: symmetric Boolean functions; algebraic immunity; corre ion immunity; nonlinearity

1 引言

自 Courtois 和 Meier[1]利用代数攻击方法有效攻击 LILI-128 算法和 Toyocrypt 算法以来，作为一种新的密码分析方法，代数攻击便成为了密码分析领域的研究焦点。它的总体思想具有很强的一般性，对公钥、分组和序列密码都具有潜在的威胁，特别是对分组和序列密码具有很大的威胁。为抵抗此种攻击，Meier 等提出了布尔函数的代数免疫阶的概念[2]。由于代数攻击的复杂度随布尔函数代数免疫阶的增加而急剧增加，在密码设计中，使用高代数免疫阶的布尔函数是一个必要条件。因此，构造高代数免疫阶的布尔函数已经成为密码算法设计和密码系统设计的重要内容。然而，对于 n 元布尔函数，文献[1]、文献[2]同时指出其代数免疫阶不大于$\lceil n/2 \rceil$。确定所有代数免疫阶达到最大的 n 元布尔函数是十分重要的，但一般来说这是十分困难的，因而这方面的研究多集中在特殊的布尔函数上。

对称布尔函数作为布尔函数的一个子类，一方面，在函数的存储上占用较少的内存空间；另一方面，实际应用中需要的逻辑门个数与变元个数呈线性关系，因此，寻找良好密码学性质的对称布尔函数是十分有意义的。择多函数作为基本的对称布尔函数已被证明具有最大的代数免疫阶[3]；许多具有最大代数免疫阶的布尔函数的构造都是在择多函数的基础上修改而来的[4~10]。文献[8]、文献[10]利用重量支撑分析方法分析了 2^m 元对称布尔函数，文献[7]、文献[8]给出了一些对称布尔函数达到最大代数免疫

收稿日期：2011-11-16；修回日期：2012-04-09
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)

阶的必要条件。另外，由于在实际应用中，要求布尔函数具有良好的综合性能以抵抗各种攻击，如：线性攻击、差分攻击等。因此，布尔函数的其他密码学性质也常常被考虑，如：线性结构、代数次数、非线性度、相关免疫性等，文献[5]、文献[10]、文献[12]等讨论了对称布尔函数的上述密码学性质。

设$F_2=\{0,1\}$为二元域，n元布尔函数f是指F_2^n到F_2的映射，表示为$f(x)$，其中，$x=(x_1,x_2,\cdots x_n)\in F_2^n$为输入变元，$F_2^n$为$n$个$F_2$的笛卡尔积。$wt(x)=|\{1\le i\le n|x_i=1\}|$称为$x$的汉明重量。如果布尔函数的值是输入置换下的不变量则称其为对称布尔函数，记SB_n为n元对称布尔函数的集合，$T_i=\{a\in F_2^n\mid wt(a)=i\}$，易知任一$n$元对称布尔函数$f$可由$n+1$元向量$v_f=(v_f(0),v_f(1),\cdots,v_f(n))$表示，其中，$v_f(i)=f(x)$，$wt(x)=i$，$1\le i\le n$。设$e_i\in F_2^{n+1}$，它的第$i$个分量为1，其他分量为0，定义$s_{k-m}=e_{k-m}+e_{k+m}$。文献[4]证明了函数$v_f=(1\{1\cdots1\}_k0\{0\cdots0\}_k)+s_{k-3\cdot2^t}+s_{k-2^t}$的代数免疫阶达到最大，其中，$4\cdot2^t\le k<5\cdot2^t$，$t\ge0$，$a\in F_2$，但没有讨论此类函数的其他密码学性质。对$0<t\le k$，文献[5]给出了函数$v_f=(0\{0\cdots0\}_k1\{1\cdots1\}_{k+1})+s_{k-t}$代数免疫阶达到最大的充要条件，并讨论了此类函数的代数次数。在文献[4]、文献[5]的基础之上，本文做了进一步的研究。为讨论方便，定义$\hat{A}$为如下n元布尔函数的集合。

$$\hat{A}=\{f\mid v_f=(1\{1\cdots1a\}_k0\{0\cdots0\}_k)+s_{k-m}+s_{k-s},\ 0<s<m\le k,n=2k,a\in F_2\}$$

易知$\hat{A}$中的函数为对称布尔函数的一个子类且包含文献[4]中的函数。

2 $\hat{A}$中一类函数具有最大代数免疫阶的不同证明

设f是n元布尔函数，f的代数免疫阶记为$AI(f)$，是指能零化f或$f+1$的非零布尔函数的代数次数的最小值，即$AI(f)=\min\{\deg(g)\mid g\ne0;\ gf=0$或$g(f+1)=0\}$，其中，$\deg(g)$为布尔函数$g$的代数次数。

定义1[5] 如果$a=(a_1,\cdots a_n)\in F_2^n$，$b=(b_1,\cdots b_n)\in F_2^n$，定义$\begin{cases}a\preceq b\Leftrightarrow a_i\le b_i,(i=1,\cdots,n)\\ a\prec b\Leftrightarrow a\preceq b,a\ne b\end{cases}$；如果$a$，$b$是非负整数，它们的二进制展开为$a=(a_n,\cdots,a_0)$，$b=(b_n,\cdots,b_0)$，同样定义$\begin{cases}a\preceq b\Leftrightarrow a_i\le b_i,(i=0,\cdots,n)\\ a\prec b\Leftrightarrow a\preceq b,a\ne b\end{cases}$；定义$a\not\preceq b$当且仅当存在$i$使得$a_i>b_i$。

任一n元布尔函数g可以表示成如下形式$g(x)=\sum_{a\in F_2^n}c_g(a)x^a$，$c_g(a)\in F_2$，其中，$a=(a_1,\cdots a_n)$，$x^a=x_1^{a_1}\cdots x_n^{a_n}$，规定$0^0=1$，则对于$b\in F_2^n$，必有$g(b)=\sum_{a\in F_2^n,a\preceq b}c_g(a)$。

引理1[11] 设k，t是2个非负整数，$k\ge t$，它们有二进制展开$k=(k_l,\cdots,k_0)$，$t=(t_l,\cdots,t_0)$则$\binom{k}{t}\equiv\binom{k_l}{t_l}\binom{k_{l-1}}{t_{l-1}}\cdots\binom{k_0}{t_0}\bmod2\equiv\begin{cases}1\bmod2,\ t\preceq b\\ 0\bmod2,\ t\not\preceq b\end{cases}$。

对于对称布尔函数，当变元数是2的幂次时，文献[8]提出了一个使其达到最大代数免疫阶的充要条件的猜想，这个猜想包含了下面的定理1，文献[10]利用重量支撑分析法证明了这个猜想。文献[4]给出了两类代数免疫阶达到最大的对称布尔函数，用文献[4]的思想证明下面的定理1。

定理1 设$f\in\hat{A}$，$v_f=(1\{1\cdots1a\}_k0\{0\cdots0\}_k)+s_{k-m}+s_{k-s}$ $(k=m=2s=2^{t+1},n=2k,t>0,a\in F_2)$，则$AI(f)=k$。

证明 假设$AI(f)<k$，必有非零的n元布尔函数g且$\deg(g)<k$使得$gf=0$或$g(f+1)=0$。

若$gf=0$，设$c(a)\in F_2$，$g(x)=\sum_{a\in F_2^n,wt(a)<k}c(a)x^a$。下面证明当$wt(a)<k$时$c(a)=0$，从而$g=0$。

1) 断言当$0<wt(b)<k-s$时$c(b)=c(0)$，下面利用归纳法证明。

当$wt(b)=1$时，$0=g(b)=\sum_{wt(a)<k,a\preceq b}c(a)=c(b)+c(0)$，即$c(b)=c(0)$。假定$0<l<k-s-1$，当$0<wt(b)\le l$时有$c(b)=c(0)$，则当$wt(b)=l+1$时

$$0=g(b)=\sum_{0\le wt(a)\le l+1,a\preceq b}c(a)=c(0)+c(b)+\sum_{0<wt(a)\le l,a\prec b}c(a)=c(0)+c(b)+c(0)(2^{wt(b)}-2)$$

故$c(b)=c(0)$。

2) 断言当$k-s<wt(b)<k$时$c(b)=\sum_{wt(a)=k-s,a\prec b}c(a)$，下面利用归纳法证明。

当$wt(b)=k-s+1$时，由1)可得

$$0=g(b)=\sum_{0\le wt(a)\le k-s+1,a\preceq b}c(a)=c(0)+c(b)+\sum_{0<wt(a)<k-s,a\prec b}c(a)+\sum_{wt(a)=k-s,a\prec b}c(a)=c(0)+c(b)+c(0)(2^{wt(b)}-3-k+s)+$$

$\sum_{wt(a)=k-s,a\preceq b}c(a)$。

即 $c(b)=\sum_{wt(a)=k-s,a\preceq b}c(a)$。

假定 $k-s<l\le k-1$，当 $k-s<wt(b)\le l-1$ 时有 $c(b)=\sum_{wt(a)=k-s,a\preceq b}c(a)$ 成立，则当 $wt(b)=l$ 时

$$0=g(b)=\sum_{0\le wt(a)\le l,a\preceq b}c(a)=c(0)+c(b)+\sum_{wt(a)=k-s,a\preceq b}c(a)+\sum_{0<wt(a)<k-s,a\preceq b}c(a)+\sum_{k-s<wt(a)\le l-1,a\preceq b}c(a)$$

由于 $k-s<l\le k-1$，可令 $l=2^t+d$，$0<d<2^t$，故由 1)及引理 1 知

$$\sum_{0<wt(a)<k-s,a\preceq b}c(a)=c(0)\sum_{i=1}^{2^t-1}\binom{2^t+d}{i}\equiv c(0)\bmod 2。$$

由归纳假设知

$$\sum_{k-s<wt(a)\le l-1,a\preceq b}c(a)=\sum_{k-s<wt(a)\le l-1,a\preceq b}\ \sum_{wt(b)=k-s,b\preceq a}c(b)$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)\sum_{k-s<wt(a)\le l-1,b\preceq a\preceq b}1$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)(2^{l-(k-s)}-2)\equiv 0\bmod 2。$$

从而 $c(b)=\sum_{wt(a)=k-s,a\preceq b}c(a)$。

3) 断言当 $wt(b)=k+s$，$k+m$ 时 $c(0)+\sum_{wt(a)=k-s,a\preceq b}c(a)=0$。

当 $wt(b)=k+s$ 时，

$$0=g(b)=\sum_{0\le wt(a)\le k-1,a\preceq b}c(a)$$

$$=c(0)+\sum_{wt(a)=k-s,a\preceq b}c(a)+\sum_{0<wt(a)<k-s,a\preceq b}c(a)+\sum_{k-s<wt(a)\le k-1,a\preceq b}c(a)。$$

而由 1)及引理 1 知

$$\sum_{0<wt(a)<k-s,a\preceq b}c(a)=c(0)\sum_{i=1}^{k-s-1}\binom{k+s}{i}$$

$$\equiv c(0)\sum_{i=1}^{2^t-1}\binom{2^t}{i}\bmod 2\equiv 0\bmod 2$$

同样由 2)及引理 1 可得

$$\sum_{k-s<wt(a)\le k-1,a\preceq b}c(a)=\sum_{k-s<wt(a)\le k-1,a\preceq b}\ \sum_{wt(b)=k-s,b\preceq a}c(b)=\sum_{wt(b)=k-s,b\preceq b}c(b)\sum_{k-s<wt(a)\le k-1,b\preceq a\preceq b}1$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)\Big(\sum_{i=1}^{k-1-(k-s)}\binom{wt(b)-(k-s)}{i}\Big)$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)\Big(\sum_{i=1}^{2^t-1}\binom{2^{t+1}}{i}\Big)\equiv 0\bmod 2$$

故 $c(0)+\sum_{wt(a)=k-s,a\preceq b}c(a)=0$。

当 $wt(b)=k+m$ 时，相似 $wt(b)=k+s$ 时的证明，可得

$$0=g(b)=\sum_{0\le wt(a)\le k-1,a\preceq b}c(a)$$

$$=c(0)+\sum_{wt(a)=k-s,a\preceq b}c(a)+\sum_{0<wt(a)<k-s,a\preceq b}c(a)+\sum_{k-s<wt(a)\le k-1,a\preceq b}c(a)$$

由 1)及引理 1 知

$$\sum_{0<wt(a)<k-s,a\preceq b}c(a)=c(0)\sum_{i=1}^{k-s-1}\binom{k+m}{i}$$

$$=c(0)\sum_{i=1}^{2^t-1}\binom{2^{t+2}}{i}\bmod 2\equiv 0\bmod 2$$

同样由 2)及引理 1 知

$$\sum_{k-s<wt(a)\le k-1,a\preceq b}c(a)=\sum_{k-s<wt(a)\le k-1,a\preceq b}\ \sum_{wt(b)=k-s,b\preceq a}c(b)$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)\sum_{k-s<wt(a)\le k-1,b\preceq a\preceq b}1$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)\Big(\sum_{i=1}^{k-1-(k-s)}\binom{wt(b)-(k-s)}{i}\Big)$$

$$=\sum_{wt(b)=k-s,b\preceq b}c(b)\Big(\sum_{i=1}^{2^t-1}\binom{2^{t+1}+2^t}{i}\Big)\equiv 0\bmod 2$$

故 $c(0)+\sum_{wt(a)=k-s,a\preceq b}c(a)=0$。

4) 断言当 $wt(b)=k+s$ 或 $k+m$ 跑遍时，方程组 $c(0)+\sum_{wt(a)=k-s,a\preceq b}c(a)=0$ 只有零解，即 $c(0)=0$，且对所有 $wt(a)=k-s=2^t$，$a\in F_2^n$ 有 $c(a)=0$。要证此方程组只有零解，只需证系数矩阵可逆即可。由于系数矩阵为 $\boldsymbol{M}=(m_{a,b})_{a\in T_{k+s}\cup T_{k+m},b\in T_{k-s}\cup T_{k-m}}$，$m_{a,b}=\begin{cases}1, b\preceq a\\ 0, \text{否则}\end{cases}$。将矩阵 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{M}$ 分块，可得 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{M}=(n_{b,c})=\begin{pmatrix}X & Y\\ Y^{\mathrm{T}} & Z\end{pmatrix}$，其中，$Z=(z_{b,c})$，$b,c\in T_{k-m}=T_0$；$Y=(y_{b,c})$，$b\in T_{k-s},c\in T_{k-m}=T_0$；$X=(x_{b,c})$，$b,c\in T_{k-s}$。对于 $Z=(z_{b,c})$，$Y=(y_{b,c})$，和 $X=(x_{b,c})$，有如下结论。

$$z_{b,c}=\sum_{a\in T_{k+s}\cup T_{k+m},b\preceq a,c\preceq a}1\equiv 1\bmod 2；$$

$$y_{b,c}=\sum_{a\in T_{k+s}\cup T_{k+m},b\preceq a,c\preceq a}1$$

$$=\binom{n-(k-s)}{k+s-(k-s)}+\binom{n-(k-s)}{n-(k-s)}$$

$$=\binom{2^{t+1}+2^t}{2^{t+1}}+\binom{2^{t+1}+2^t}{2^{t+1}+2^t}\equiv 0 \bmod 2$$；

$x_{b,c}=\sum_{a\in T_{k+s}\cup T_{k+m},b\preceq a,c\preceq a}1$，此时设 $d=(b\vee c)$，其中，“$\vee$”为“或”运算，则有 $2^{t+2}-wt(d)=2^{t+1}+l$ 且 $0\le l\le 2^t$，从而 $x_{b,c}=\sum_{a\in T_{k+s}\cup T_{k+m},d\preceq a}1=1+\binom{n-wt(d)}{k+s-wt(d)}=1+\binom{2^{t+1}+l}{2^t}\equiv 1+\binom{l}{2^t}\bmod 2$，可得 $x_{b,c}\equiv 0\bmod 2\Leftrightarrow l=2^t$，即 $x_{b,c}\equiv 0\bmod 2$ 当且仅当 $b=c$，故矩阵 $\boldsymbol{X}$ 除对角线上元素为 0 外其他位置均为 1。由引理 1 知 $\boldsymbol{X}$ 的阶数 $\binom{n}{k+s}=\binom{2^{t+2}}{2^t}\equiv 0\bmod 2$ 是偶数，故 $\boldsymbol{X}$ 可逆，从而 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{M}=\begin{pmatrix}X & Y\\ Y^{\mathrm{T}} & Z\end{pmatrix}=\begin{pmatrix}X & 0\\ 0 & 1\end{pmatrix}$ 可逆，进而系数矩阵 $\boldsymbol{M}$ 可逆。

从而，$c(0)=0$，$c(a)=0$ 对所有 $wt(a)=k-s=2^t$。

又由 1)、2)、3)可知对任何 $a\in F_2^n$，$wt(a)<k$ 有 $c(a)=0$，即当 $gf=0$ 时假设不成立，命题得证。

若 $g(f+1)=0$，令 $f_1(x_1,\cdots,x_n)=f(x_1+1,\cdots,x_n+1)+1$，$g_1(x_1,\cdots,x_n)=g(x_1+1,\cdots,x_n+1)$，则 f_1 具有如下形式：$v_{f_1}=(\underbrace{1,\cdots,1}_{k}\underbrace{0,\cdots,0}_{2^k-k-1})+s_{k-m}+s_{k-s}$，且 $g_1f_1=0$，从而利用上述同样的证法可得 $g_1(x)=0$，进而 $g(x)=0$，即 $g(f+1)=0$ 时假设不成立，命题得证。

综合上面的证明可知原命题得证。

3 $\hat{A}$ 中函数达最大代数免疫阶的一个必要条件

利用文献[5]的思想，下面给出一个使 $\hat{A}$ 中的函数达到最大代数免疫阶的必要条件，并初步估计了满足此必要条件的函数个数的下界。

引理 2[4] 设 k 是一个非负整数，则 $\binom{2k}{k}\equiv 2\bmod 4$ 当且仅当 k 是 2 的某个幂次。

定理 2 设 $f\in\hat{A}$，若 $AI(f)=k$，则必有 $\binom{k+s}{k-s}\binom{2s}{s}\equiv 2\bmod 4$ 或 $\binom{k+m}{k-s}\sum_{i=0}^{s-1}\binom{m+s}{i}\equiv 1\bmod 2$。

证明 假设定理不成立，令 $g(x)=\sum_{a\in F_2^n}c(a)x^a$，其中，$c(a)=\begin{cases}0, & wt(a)<k-s,wt(a)>k-1\\ 1, & wt(a)=k-s\\ \sum_{wt(b)=k-s,b\preceq a}1\bmod 2, & k-s<wt(a)<k\end{cases}$，显然有 $\deg(g)<k$ 且 $g\neq 0$。

若 $a=0$，下面证明 $g(x)f(x)=0$。

当 $wt(b)<k-s$ 时，易知 $g(b)=0$。

当 $k-s<wt(b)<k$ 时

$$\begin{aligned}g(b)&=\sum_{k-s\le wt(a)\le wt(b),a\preceq b}c(a)\\&=\sum_{k-s\le wt(a)\le wt(b),a\preceq b}\ \sum_{wt(b)=k-s,b\preceq a}1\\&=\sum_{i=k-s}^{wt(b)}\binom{wt(b)}{i}\binom{i}{k-s}\\&=\sum_{i=k-s}^{wt(b)}\binom{wt(b)}{k-s}\binom{wt(b)-(k-s)}{i-(k-s)}\\&=\binom{wt(b)}{k-s}2^{wt(b)-(k-s)}\equiv 0\bmod 2\end{aligned}$$

当 $wt(b)=k+s$ 时，由引理 2，类似地可得

$$\begin{aligned}g(b)&=\sum_{i=k-s}^{k-1}\binom{k+s}{i}\binom{i}{k-s}=\binom{k+s}{k-s}\sum_{i=0}^{s-1}\binom{2s}{i}\\&=\binom{k+s}{k-s}\left(2^{2s-1}-\frac{1}{2}\binom{2s}{s}\right)\equiv 0\bmod 2\end{aligned}$$

当 $wt(b)=k+m$ 时，同样可得 $g(b)\equiv 0\bmod 2$。即得 $g(x)f(x)=0$，这与 $AI(f)=k$ 矛盾。

若 $a=1$，令 $f_1(x_1,\cdots x_n)=f(x_1+1,\cdots,x_n+1)+1$，$g_1(x_1,\cdots x_n)=g(x_1+1,\cdots,x_n+1)$ 由于代数次数是线性变换下的不变量，故 $g_1\neq 0$，$\deg(g_1)<k$ 而 $v_{f_1}=(\underbrace{1,\cdots,1}_{k}\underbrace{0,\cdots,0}_{2^k-k-1})+s_{k-m}+s_{k-s}$，相似的证明可得 $gf_1=0$，从而 $g_1(f+1)=0$，这与 $AI(f)=k$ 矛盾。综上可知假设不成立，原命题得证。

下面求满足上述定理中必要条件的函数个数的下界，即对于固定的 k 下式中 $|A|$ 的下界。

$$A=\left\{(m,s)\mid 0<s<m\le k,\binom{k+s}{k-s}\binom{2s}{s}\equiv 2\bmod 4\right\}\cup\left\{(m,s)\mid 0<s<m\le k,\binom{k+m}{k-s}\sum_{i=0}^{s-1}\binom{m+s}{i}\equiv 1\bmod 2\right\}=B\cup C。$$

先做如下准备工作，对于固定的 $k=2^{k_p}+\cdots+2^{k_1}$，$k_p>\cdots>k_1$，设 $t_i=k_{v_i+1}-k_{v_i}\ge 2$，$v_i>v_j$ 如果 $i>j$，$t=(t_1,\cdots,t_q)$。对于 $1\le z\le t_1+\cdots+t_q-q$ 及 $w=(w_1,\cdots,w_q)$，定义 $w<t\Leftrightarrow 0\le w_i\le t_i-1$，

$i=1,\L,q$ 且 $w_1+\L+w_q=z$。令 $V_z=\{w=(w_1,\L,w_q)\mid w<t\}$，$u_w=\max\{v_j\mid w_j\neq 0,\ j=1,\L,q\}$。对于组合数$\binom{k}{t}$，规定$\binom{0}{0}=1$，$\binom{k}{t}=0$若 $k<0$ 或者 $t>k$，在下面定理中规定$k_0=-1$。

定理 3　如果 $p=1$，$k_1>0$，则$|A|\geq 2^{k_1-1}$；如果 $p>1$，则

$$|A|\geq\sum_{z=1}^{t_1+\L+t_q-q}\sum_{w=(w_1,\L,w_q)\in V_z}[(2^{u_w}-1)\prod_{i=1}^{q}\binom{t_i-1}{w_i}]+\sum_{k_i-1>k_{i-1}\geq -1,1\leq i\leq p}\ \sum_{1\leq t\leq z\leq p}\binom{p+1-i}{t}\binom{i-1}{z-t}$$

证明　当 $p=1$，$k_1>0$ 时，设 $s=2^{k_1-1}$，$s<m\leq k$，则此时$(m,s)\in B$，个数为$k-s=2^{k_1-1}$，定理成立。当 $p>1$ 时，对于$1\leq z\leq t_1+\L+t_q-q$，$w=(w_1,\L,w_q)\in V_z$，s 按如下方法取：取 $s=2^{s_l}+2^{s_{l-1}}+\L+2^{s_1}$，其中，$1\leq l\leq u_w$，$s_i\in\{k_{u_w},k_{u_w-1},\L,k_1\}$，$i=1,2,\L,l$，$s_i\neq s_j$ 如果$i\neq j$；m 按如下方法取：在区间(k_{v_i},k_{v_i+1})中取 w_i 个不同的数作为 m 的二进制展开中 2 的幂次，其中，$i=1,2,\L,q$，则此时有 $(m,s)\in C$ 且这样的(m,s)个数为

$$\sum_{z=1}^{t_1+\L+t_q-q}\sum_{w=(w_1,\L,w_q)\in V_z}[(\sum_{i=1}^{u_w}\binom{u_w}{i})\prod_{i=1}^{q}\binom{t_i-1}{w_i}]=\sum_{z=1}^{t_1+\L+t_q-q}\sum_{w=(w_1,\L,w_q)\in V_z}[(2^{u_w}-1)\prod_{i=1}^{q}\binom{t_i-1}{w_i}]$$

另外，对于 $k_i-1>k_{i-1}\geq -1$，$1\leq i\leq p$，$1\leq z\leq p$，取$m=2^{m_z}+2^{m_{z-1}}+\L+2^{m_1}$，$s=2^{k_i-1}$，其中，$m_i\in\{k_1,k_2,\L,k_p\}$，$i=1,2,\L,z$，$m_i\neq m_j$ 如果 $i\neq j$。由于 $m>s$，则 $m_1,\L,m_z$ 中必有若干个（设为$t\geq 1$个）取自$\{k_i,k_{i+1},\L,k_p\}$，有若干个（为 $z-t$ 个）取自 $\{k_1,k_2,\L,k_{i-1}\}$，这种$(m,\ s)$个数为 $\sum_{k_i-1>k_{i-1}\geq -1,1\leq i\leq p}\ \sum_{1\leq t\leq z\leq p}\binom{p+1-i}{t}\binom{i-1}{z-t}$，此时 $(m,s)\in B$ 且 $(m,s)\notin C$，即当 $p>1$ 时结论成立。综合可知定理得证。

定理 3 中的下界公式是复杂的，对其进行再简化是困难的。从证明过程可见当 k 的二进制展开中的“1”越稀疏时，其下界更可能越大。为了直观的感受，当 $k<2^{24}$ 时，给出一些例子，如表 1 所示。

表 1　　一些下界的例子

$n=2k$	下界	$n=2k$	下界
14	0	9 268	1 752
32	8	20 076	4 016
88	14	44 002	12 301
234	65	90 044	23 544
408	36	196 000	5 632
672	24	262 142	0
850	153	524 288	131 072
1 908	396	2 097 166	917 505
3 564	828	8 388 654	3 932 177
4 094	0	33 554 348	6 291 460

4　$\hat{A}$ 中函数的密码学性质

为了探讨定理 1 中函数的其他密码学性质，结合文献[5]的思想，下面更一般地讨论$\hat{A}$ 中函数的密码学性质。这也是文献[5]指出的后续工作的一部分。

4.1　线性结构

n 元布尔函数 f 的汉明重量定义为 $wt(f)=|\{x\in F_2^n\mid f(x)=1\}|$，它能反映 f 的平衡性。如果 $w\in F_2^n$ 使得 $f(w+x)+f(x)$ 恒为常数，则称 w 为 f 的线性结构，定义 $\bar{\bar{0}}=(0,\L,0)\in F_2^n$，$\bar{1}=(1,\L,1)\in F_2^n$。

性质 1　设 $f\in\hat{A}$，则 f 没有除 $\bar{0}$ 之外的其他线性结构。

证明　当 $a=1$ 时，易知 $wt(f)=2^{n-1}+\frac{1}{2}\binom{n}{k}$；当 $a=0$ 时，易知 $wt(f)=2^{n-1}-\frac{1}{2}\binom{n}{k}$。由文献[12]知对于非仿射的对称布尔函数，它们没有除 $\bar{0}$ 和 $\bar{1}$ 之外的线性结构。而此时 $wt(f)\neq 2^{n-1}$，即知 f 不是仿射函数，又 $f(x)+f(x+\bar{1})=\begin{cases}0, wt(x)=k\\ 1, wt(x)\neq k\end{cases}$，故 $\bar{1}$ 也不是 f 的线性结构，从而 f 没有除 $\bar{0}$ 之外的其他线性结构。

4.2　代数次数

引理 3[12]　$f\in SB_n$ 当且仅当 $f(x)=\sum_{i=0}^{n}l_f(i)X_{i,n}$，$l_f(i)\in F_2$，其中，$X_{i,n}$ 为 i 次基本对称布尔函数，即 $X_{i,n}=\sum_{1\leq j_1<\L<j_i\leq n}x_{j_1}x_{j_2}\L x_{j_i}$，易知 $\deg(f)=\max\{i\mid l_f(i)=1,0\leq i\leq n\}$。

引理 4[12] 设 $f(x)=\sum_{i=0}^{n} l_f(i)X_{i,n}$，$v_f=(v_f(0), v_f(0), \cdots, v_f(n))$，则 $l_f(i)=\sum_{j \underline{p} i} v_f(j)$，$v_f(j)=\sum_{j \underline{p} i}^{n} l_f(i)$。

引理 5[8] 设 $f \in SB_n$，$f(x)=\sum_{i=0}^{n} l_f(i)X_{i,n}$，$v_f=(v_f(0), v_f(1), \cdots, v_f(n))$，则 $l_f(i)=\sum_{j \underline{p} i} v_f(j)$，$v_f(i)=\sum_{j \underline{p} i} l_f(j)$。

引理 6[5] 设 k 是非负整数，$l=\lfloor \mathrm{lb}k \rfloor$，则

1) $\{t \mid t \underline{p} k\}=\{t \mid t \underline{p} k, 0 \le t \le k-2^l\} \cup \{t \mid t \underline{p} k, 2^l \le t \le k\}$；

2) $|\{t \mid t \underline{p} k, 0 \le t \le k-2^l\}| = |\{t \mid t \underline{p} k, 2^l \le t \le k\}| = 2^{wt(k)-1}$。

对于非负整数 i，r，设 $i \lozenge r=\begin{cases}1, & i \underline{p} r \\ 0, & i \not\underline{p} r\end{cases}$，$g_n(i,j,p,q)=\max\{r \mid (i \lozenge r)+(j \lozenge r)+(p \lozenge r)+(q \lozenge r)=1 \text{或} 3, 0 \le r \le n\}$。

定理 4 设 $f \in \hat{A}$，当 n 不是 2 的幂次时，令 $d=2^{\lfloor \mathrm{lb}n \rfloor}$，$m$，$s \notin \{d-k, k\}$。则当 n 是 2 的幂次时 $\deg(f)=n$；当 n 不是 2 的幂次时 $\deg(f)=\max\{d, g_n(k-s, k-m, k+s, k+m)\}$。

证明 当 n 是 2 的幂次时，由引理 4 知 $l_f(n)=\sum_{i \underline{p} n} v_f(i)=v_f(0)+v_f(n)=\begin{cases}0+1=1, m=k \\ 1+0=1, m \ne k\end{cases}$，故结论成立。当 n 不是 2 的幂次时，由于 m，$s \notin \{d-k, k\}$，有 $l_f(d)=\sum_{i \underline{p} d} v_f(d)=v_f(0)+v_f(d)=1+0=1$。令 $i \in \{d+1, d+2, \cdots, n\}$，则 $wt(i)>1$，由引理 5 和引理 6 知

$$\begin{aligned} l_f(i)&=\sum_{i \underline{p} n} v_f(i)=\sum_{j \underline{p} i, j \le i-d} v_f(j)+\sum_{j \underline{p} i, d \le j \le i} v_f(j) \\ &=2^{wt(i)-1} \cdot 1-\sum_{j \underline{p} i, j=k-s} 1-\sum_{j \underline{p} i, j=k-m} 1+2^{wt(i)-1} \cdot 0+ \\ &\quad \sum_{j \underline{p} i, j=k+s} 1-\sum_{j \underline{p} i, j=k+m} 1 \equiv \sum_{j=k-m, k-s, k+m, k+s} 1 \bmod 2。 \end{aligned}$$

故 $l_f(i) \equiv 1 \bmod 2$ 当且仅当式子 $k-m \underline{p} i$，$k-s \underline{p} i$，$k+s \underline{p} i$，$k+m \underline{p} i$ 中有奇数个成立，从而结论成立。

4.3 非线性度

布尔函数的非线性度即是布尔函数与所有仿射函数的最小距离。n 元布尔函数 f 的非线性度记为 $NL(f)=\min_{g \in A_n}\{|\{x \mid f(x) \ne g(x)\}|\}$，其中，$A_n$ 为所有 n 元仿射函数的集合。文献[13]已经给出了 $\hat{A}$ 中函数的非线性度，但为了性质的完整性，仍把它列在下面。

定理 5[13] 设 $f \in \hat{A}$，则 $NL(f)=2^{2k-1}-\frac{1}{2}\binom{2k}{k}$。

4.4 相关免疫性

设 f 是 n 元布尔函数，它在点 $w \in F_2^n$ 的 Walsh 循环谱记为 $S_{(f)}(w)=\sum_{x \in F_2^n}(-1)^{f(x)+wx}$，如果对任何 $w \in F_2^n$，$1 \le wt(w) \le t$，都有 $S_{(f)}(w)=0$，则称 f 是 t 阶相关免疫的。$\sum_{j=0}^{i}(-1)^j\binom{x}{j}\binom{n-x}{i-j}=K_i(x,n)$，$(i=0,1,\cdots,n)$ 被称为 Krawtchouk 多项式[14]。若 $w \in F_2^n$，$wt(w)=k$，则有 $\sum_{x \in F_2^n, wt(x)=i}(-1)^{wx}=\sum_{j=0}^{i}(-1)^j\binom{k}{j}\binom{n-k}{i-j}=K_i(k,n)$，从而，对于 $f \in SB_n$ 有 $S_{(f)}(w)=\sum_{x \in F_2^n}(-1)^{f(x)+wx}=\sum_{i=0}^{n}(-1)^{v_f(i)}K_i(wt(w),n)$。下面列出 Krawtchouk 多项式的一些性质，在接下来的证明中将用到它们。

性质 2[5, 14]

1) 对于偶数 n 和奇数 h，$K_{n/2}(h,n)=0$；

2) $K_i(h,n)=(-1)^h K_{n-i}(n-h,n)$。

引理 7 设 $f \in \hat{A}$，$w \in F_2^n$，$wt(w)=h$，若 $a=0$，则

$$S_{(f)}(w)=\begin{cases}K_k(h,n), h \equiv 0 \bmod 2 \\ -2\sum_{i=0}^{k-1}K_i(h,n)+4K_{k-s}(h,n)+4K_{k-m}(h,n), \\ h \equiv 1 \bmod 2\end{cases}$$

若 $a=1$，则

$$S_{(f)}(w)=\begin{cases}-K_k(h,n), h \equiv 0 \bmod 2 \\ -2\sum_{i=0}^{k-1}K_i(h,n)+4K_{k-s}(h,n)+4K_{k-m}(h,n), \\ h \equiv 1 \bmod 2\end{cases}$$

证明 若 $a=0$，由性质 2 可得

$$\begin{aligned} S_{(f)}(w)&=\sum_{i=0}^{n}(-1)^{v_f(i)}K_i(h,n) \\ &=-\sum_{i=0}^{k-1}K_i(h,n)+\sum_{i=k}^{n}K_i(h,n) \end{aligned}$$

$$+2\sum_{i=k-m,k-s}K_i(h,n)-2\sum_{i=k+s,k+m}K_i(h,n)$$

$$=-\sum_{i=0}^{k-1}K_i(h,n)+\sum_{i=0}^{k}(-1)^h K_i(h,n)$$

$$+2\sum_{i=k-m,k-s}K_i(h,n)-2\sum_{i=k-s,k-m}(-1)^h K_i(h,n)$$

$$=\begin{cases}K_k(h,n), h\equiv 0 \bmod 2\\ -2\sum_{i=0}^{k-1}K_i(h,n)+4K_{k-s}(h,n)+4K_{k-m}(h,n), h\equiv 1 \bmod 2\end{cases}$$

若 $a=1$，由性质 2 同样可得结论。

引理 8　设 t, k 为整数且 $0<t<k$，令 $F(t)=\binom{2k-1}{t}-\binom{2k-1}{t-1}$，则 $F(t)$ 是关于 t 的增函数。

证明　由于 $F(t+1)-F(t)=\binom{2k-1}{t+1}-\binom{2k-1}{t-1}$

$=\dfrac{(2k-1)![4(t-k+1/2)^2+k-1]}{(t+1)!(2k-t)!}\geq 0$，故结论得证。

定理 6　设 $f\in\hat{A}$，仅有 k=7、m=3、s=1 或 k=m=3、s=2 时 f 具有 1 阶相关免疫性，其他情况下 f 不具有相关免疫性。

证明　令 $w\in F_2^n$，$wt(w)$=1。当 $a=0$ 时，若 $m\neq k$ 并且 $k\geq 9$，则由引理 7 可得

$$S_{(f)}(w)=-2\binom{2k-1}{k-1}+4\binom{2k-1}{k-m}-4\binom{2k-1}{k-m-1}+4\binom{2k-1}{k-s}-4\binom{2k-1}{k-s-1}$$

又由引理 8 可得

$$S_{(f)}(w)\leq -2\binom{2k-1}{k-1}+4\binom{2k-1}{k-1}-4\binom{2k-1}{k-2}+4\binom{2k-1}{k-2}-4\binom{2k-1}{k-3}$$

$$=\frac{-2(2k-1)![(k-9/2)^2-73/4]}{(k+2)!(k-1)!}<0$$

故此时 f 没有相关免疫性。

若 $m\neq k$ 并且 k<9，由计算机可穷尽算得仅有 k=7、m=3、s=1 时 f 有 1 阶相关免疫性。

若 $m=k$ 并且 $k\leq 4$，同样由计算机可穷尽算得仅有 k=m=3、s=2 时 f 有 1 阶相关免疫性。

若 m=k 并且 k>4，则由引理 7 可得 $S_{(f)}(w)=-2\binom{2k-1}{k-1}+4+4\binom{2k-1}{k-s}-4\binom{2k-1}{k-s-1}$。又由引理 8 可得 $S_{(f)}(w)\leq -2\binom{2k-1}{k-1}+4+4\binom{2k-1}{k-1}-4\binom{2k-1}{k-2}$

$=4-\dfrac{2k-6}{k+1}\binom{2k-1}{k-1}<0$。故此时 f 没有相关免疫性。

这样即证明了当 $a=0$ 时结论成立，同样地，当 $a=1$ 时相似地可证结论成立。

5　结束语

本文给出了 $\hat{A}$ 中一类函数达到代数免疫阶的不同证明，给出了 $\hat{A}$ 中函数达最大代数免疫阶的必要条件，同时给出了满足此条件的函数个数的一个下界。另外，给出了 $\hat{A}$ 中大部分函数的代数次数，分析了 $\hat{A}$ 中函数的相关免疫性，证明了仅在 k=7、m=3、s=1 或 k=m=3、s=2 时 $\hat{A}$ 中函数具有 1 阶相关免疫性，还分析了 $\hat{A}$ 中函数的线性结构等性质。对此类对称布尔函数有了一个较全面的认识。由 4.4 节算得的 $\hat{A}$ 中函数的 Walsh 循环谱表达式，还可深入讨论此类函数的其他性质。

参考文献：

[1] COURTOIS N, MEIER W. Algebraic attacks on stream ciphers with linear feedbake[A]. Advances in Cryptology-Eurocrypt 2003[C]. Warsaw, Poland, 2003. 345-359.

[2] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[EB/OL]. http://www.iacr.org/cryptodb/archive/2004/EUROCRYPT/2645/2645.pdf, 2004.

[3] DALAI D K, MAITRA S, SARKAR S. Basic theory in constructions with maximum possible annihilator immunity[J]. Designs, Codes and Cryptography, 2006, 40(1): 41-58.

[4] QU L J, FENG K Q, LIU F. Constructing symmetric Boolean functions with maximum algebraic immunity[J]. IEEE Trans I f Theory, 2009, 55(5): 2406-2412.

[5] CHEN Y D, LU P Z. Two classes of symmetric Boolean functions with optimum algebraic immunity: construction and analysis[J]. IEEE Trans Inf Theory, 2011, 57(4): 2522-2538.

[6] LI N, QI W. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity[J]. IEEE Trans Inf Theory, 2006, 52(5): 2271-2273.

[7] QU L J, LI C. Weight support technique and the symmetric Boolean functions with maximum algebraic immunity on even number of variables[A]. Information Security and Cryptology 2007[C]. Xining, China, 2008.271-282.

[8] QU L J, Li C. On the 2^m -variable symmetric Boolean functions with maximum algebraic immunity[J]. Sci China F: Inf Sci, 2008, 51(2): 120-127.

[9] QU L J, LI L, FENG K Q. A note on symmetric Boolean functionswith maximum algebraic immunity in odd number of variables[J]. IEEE Trans Inf Theory, 2007, 53(8): 2908-2910.

（下转第 104 页）

[7] CHOI Y H. Improved adaptive nulling of coherent interference without spatial smoothing[J]. IEEE Transactions on Signa ing, 2004, 52(12):3464-3469.

[8] **赵永波**, **张守宏**. **存在相干信号时的最优波束成形**[J]. **通信学报**, 2002, 23(2) : 113-121.
ZHAO Y B, ZHANG S H, Optimum beamforming for coherent ignals[J].Journal on Communications, 2002, 23(2): 113-121.

[9] HE J, JIANG S L, WANG J T, *et al*. Polarization difference smoothing for direction finding of coherent signals[J]. IEEE Transactions on Aerospace and Electronic Systems, 2010, 46(1) : 469-480.

[10] RAHAMIM D, TABRIKIAN J. Source localization using vector sensor array in a multipath environment[J]. IEEE Transactions on Signal Processing,2004,52 (11):3096-3103.

[11] **庄钊文**, **徐振海**, **肖顺平等**. **极化敏感阵列信号处理**[M]. **北京**: **国防工业出版社**, 2005.28-37.
ZHUANG Z W, XU Z H, XIAO S P, *et al*. Signal Processing of Polarization Sensitive Array[M]. Beijing: National Defense Press, 2005.28-37.

[12] HarryL VanTrees. **最优阵列处理技术**[M]. **北京**: **清华大学出版社**, 2008.455-467.
HarryL VanTrees.Optimum Array Processing[M]. Beijing: singhua University Press, 2008.455-467.

[13] KAY S M **著**. **罗鹏飞等译**. **统计信号处理基础——估计与检测理论**[M]. **北京**: **电子工业出版社**, 2006.416-421.
KAY S M. Fundamentals of Statistical Signal Processing—Estimation Theory[M]. Beijing: Electronics Industry Press, 2006.416-421.

[14] TSAI C J, YANG J F, SHIU T H. Performance analyses of beamformers using effective SINR on array parameters[J]. IEEE Transactions on Signal Processing,1995,43(1):300-303.

作者简介：

林智勇（1986-），男，福建漳州人，空军航空大学硕士生，主要研究方向为阵列信号处理。

陶建武（1959-），男，吉林省吉林市人，博士，空军航空大学教授、博士生导师，主要研究方向为阵列信号处理、传感器与智能信号处理。

（上接第 95 页）

[10] **李超**, **屈龙江**, **周悦等**. **密码函数的安全性指标分析**[M]. **北京**: **科学出版社**, 2011.256-262.
LI C, QU L J, ZHOU Y, *et al*. Analysis on Security Index of Cryptographic Functions[M]. Beijing: Science Press, 2011.256-262.

[11] WILSON R M. A diagonal form for the incidence matrices of *t*-subsets vs *k*-subsets[J]. European Journal of Combinatorics, 1990, 11(6): 609-614.

[12] CANTEAUT A, MARION V. Symmetric Boolean functions[J]. IEEE Trans Inf Theory, 2005, 51(8):2791-2811.

[13] **陈银东**, **陆佩忠**. **互补对称布尔函数的非线性度**[J]. **计算机工程与科学**, 2011, 33(10):51-56.
CHEN Y D, LU P Z. The nonlinearity of complementary symmetric Boolean functions[J]. Computer Engineering & Science, 2011, 33(10): 51-56.

[14] MACWILLIAMS F J, SLOANE N J. The Theory of Error–Correcting Codes[M].Amsterdam: Elsevier, 1977.

作者简介：

欧智慧（1985-），男，河南周口人，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。

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。