一类H布尔函数的代数次数、相关免疫性与代数免疫性的关系

黄景廉 王 卓 李 娟
(西北民族大学电气工程学院 兰州 730030)

摘 要 以布尔函数的导数和自定义的e-导数为研究工具,研究了一类特定Hamming重量的H布尔函数的代数次数、代数免疫性、相关免疫性之间的关联问题。得出H布尔函数的组成部分e-导数的代数次数决定了H布尔函数的代数次数;H布尔函数的e-导数与H布尔函数的代数免疫阶的大小紧密关联;H布尔函数的e-导数可将H布尔函数的代数免疫性、零化子、相关免疫性、代数次数联系到一起等。同时,导出了公式法和级联法两类求解H布尔函数最低代数次数零化子的不同方法。

关键词 H布尔函数,e-导数,导数,代数次数,代数免疫,相关免疫,关系
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.032

On Relationship of Algebraic Degree, Correlation Immunity and Algebraic Immunity for a Class of H Boolean Functions

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

Abstract Using the derivative of the Boolean function and the e-derivative defined by ourselves as research tools, we studied the relationship of algebraic degree, algebraic immunity and correlation immunity for H Boolean functions with a specific Hamming weight. We obtained the algebraic degree of the e-derivative which is a component of H Boolean functions deciding the algebraic degree of H Boolean functions. Besides, we determined the e-derivative of H Boolean functions which is closely related to the order of the algebraic immunity of H Boolean functions. We also checked the e-derivative of H Boolean functions which can put algebraic immunity, annihilators, correlation immunity and algebraic degree of H Boolean functions together. Meanwhile, we also deduced two kinds of methods which are formula method and cascade method. By using these two methods we could solve annihilators of the lowest algebraic degree of H Boolean functions.

Keywords H Boolean functions, e-derivative, Derivative, Algebraic degree, Algebraic immunity, Correlation immunity, Relationship

1 引言

从20世纪60年代起,为研究和构造具有良好安全性的现代密码系统,学者们陆续提出了对密码系统进行攻击的Berlekamp-Massey算法、线性逼近攻击、差分攻击、相关攻击、代数攻击等一系列攻击技术,并随之提出了抵抗各种攻击的相应的布尔函数的高代数次数、高非线性度、平衡性、严格雪崩准则、扩散性、相关免疫性、代数免疫性等密码安全性质。为使设计的密码系统具有抵抗多种密码攻击的能力,需求用以设计非线性组合函数的布尔函数具有多种良好的密码学性质。但研究发现,一些密码安全性质之间往往存在相互制约的关系。如布尔函数的相关免疫阶与代数次数之和小于等于维数,当维数确定时,二者相互制约,一个增大,另一个就减小[1];又如Bent函数是n次扩散函数,但却是0阶相关免疫函数[2]。因此,布尔函数对多种密码安全性质的相容性,一直是备受关注的问题。对多种布尔函数密码安全性质相容性的研究,大多是以研究布尔函数一种密码安全性质为主,同时包含对其它密码安全性质的相容性的研究。如目前人们对弹性布尔函数的代数免疫性的研究[3],对Plateaued函数(或Bent函数)的代数免疫性的研究[4],都是如此。

自Meier等人于2004年提出抵抗代数攻击的布尔函数代数免疫性的概念[5]以来,代数免疫性及代数次数最低的零化子的求法一直都是密码安全性研究中的一个热点问题。同时,代数免疫性与其它密码安全性质的相互关联、零化子的求法是研究的重要内容。采用的主要研究方法有:代数分析方法、频谱方法、矩阵方法、重量分析方法、线性子空间方法、级联方法等[6]。对最低代数次数零化子的求法,有待定系数算法[5]、利用Grobner基来寻找零化子的算法[7]、矩阵推算法[8]、用子函数零化子求原函数零化子的概率性算法[9]、利用零点集和支撑集及零点集的K维子空间的方法[10]等。这些

到稿日期:2014-04-05 返修日期:2014-06-06 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;李 娟(1984-),女,讲师,主要研究方向为密码学、计算机网络安全。

研究方法都需要按步骤进行多步计算才能求得结果，计算较为繁琐。

布尔函数的导数是早已有定义的概念[6,11,12]。在对布尔函数密码学性质的研究中，单独使用导数所起作用不大。为研究布尔函数的密码安全性质，我们提出了布尔函数的e-导数的概念。本文将e-导数和导数结合起来作为主要的研究工具，对Hamming重量为$2^{n-1}+2^{n-2}$的H布尔函数$f(x)$的代数次数、代数免疫性与相关免疫性之间的关系进行讨论；同时，对$f(x)$的相关免疫性、代数免疫性与$f(x)$的e-导数、导数的代数次数之间的关系，以及$f(x)$的最低代数次数零化子与$f(x)$的e-导数、导数的关系进行讨论，目的是得出布尔函数的严格雪崩准则、相关免疫性、代数免疫性、代数次数等性质之间具有相容性的一些新结果；还将得到求解$f(x)$的代数免疫阶、最低代数次数零化子较为简便的、新的求解方法。

2 预备知识

布尔函数的导数是人们所熟知的[6,11,12]。下面给出布尔函数的e-导数的概念。e-导数与导数的关系及e-导数的性质可参考文献[13,14]。

定义1 n维布尔函数$f(x_1,x_2,\cdots,x_n)$对$k(1\leqslant k\leqslant n)$个变元$x_{i_1},x_{i_2},\cdots,x_{i_k}(1\leqslant i\leqslant n)$的e-导数(e-偏导数)表示和定义为

$$\begin{aligned}&ef(x_1,x_2,\cdots,x_n)/e(x_{i_1}x_{i_2}\cdots x_{i_k})\\&=f(x_1,x_2,\cdots,x_{i_1},x_{i_2},\cdots,x_{i_k},\cdots,x_n)\cdot f(x_1,x_2,\\&\quad\cdots,\overline{x_{i_1}},\overline{x_{i_2}},\cdots,\overline{x_{i_k}},\cdots,x_n),1\leqslant i\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\\&\quad\cdots\leqslant i_k\leqslant n,1\leqslant k\leqslant n\end{aligned}\tag{1}$$

当$k=1$时，式(1)即为$f(x)=f(x_1,x_2,\cdots,x_n)$对单个变元$x_i$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：

$$\begin{aligned}&ef(x_1,x_2,\cdots,x_n)/ex_i\\&=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot f(x_1,x_2,\cdots,x_{i-1},\\&\quad 0,x_{i+1},\cdots,x_n),i=1,2,\cdots,n\end{aligned}$$

由布尔函数的导数和e-导数，可得到引理1－3。

引理1 布尔函数$f(x)$是r次扩散函数，当且仅当$w_t(\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir}))=2^{n-1}(1\leqslant i\leqslant n,1\leqslant r\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n)$。

引理2 布尔函数$f(x)$是H布尔函数，当且仅当：对一切$x_i(i=1,2,\cdots,n)$，有$w_t(df(x)/dx_i)=2^{n-1}$。

引理3 对任意布尔函数$f(x)$有

$$\begin{aligned}f(x)=f(x)\partial f(x)/\partial(x_{i_1}x_{i_2}\cdots x_{i_k})+ef(x)/e(x_{i_1}x_{i_2}\cdots\\x_{i_k}),1\leqslant i\leqslant n,1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_k\leqslant n,1\leqslant k\leqslant n\end{aligned}\tag{2}$$

$$f(x)=f(x)df(x)/dx_i+ef(x)/ex_i,i=1,2,\cdots,n\tag{3}$$

$$\begin{aligned}w_t(f(x))&=w_t(f(x)df(x)/dx_i)+w_t(ef(x)/ex_i)\\&=2^{-1}w_t(df(x)/dx_i)+w_t(ef(x)/ex_i)\\&\quad i=1,2,\cdots,n\end{aligned}\tag{4}$$

定义2 设有n维函数$f_1(x)=f_1(x_1,x_2,\cdots,x_n)$和$f_2(x)=f_2(x_1,x_2,\cdots,x_n)$，称$n+1$维函数

$$f(x)=(1+x_0)f_1(x)+x_0f_2(x)\tag{5}$$

为$f_1(x)$和$f_2(x)$的级联函数。

定义3[5] 对布尔函数$f(x)$，若有$g_1(x)$使$g_1(x)f(x)=0$，称$g_1(x)$是$f(x)$的零化子；若有$g_2(x)$使$g_2(x)(1+f(x))=0$，称$g_2(x)$是$1+f(x)$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$AI(f)$。

3 H布尔函数的代数次数、代数免疫性和相关免疫性的关系

下面讨论重量为$2^{n-1}+2^{n-2}$的H布尔函数的代数次数与相关免疫性、代数免疫性的关系，以及重量为$2^{n-1}+2^{n-2}$的H布尔函数的代数次数、相关免疫性、代数免疫性与e-导数、导数的关系。

定理1 对于Hamming重量为$2^{n-1}+2^{n-2}$的H布尔函数$f(x)$，

1)$\deg ef(x)/ex_n=1$当且仅当$\deg f(x)=2$。

2)若$\deg f(x)=2$，且$CI(f(x))=m\geqslant 1$，则

$$AI(f(x))\leqslant CI(f(x))<ef(x)/ex_n\tag{6}$$

3)若

$$\partial f(x)/\partial(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)=0\tag{7}$$

且

$$ef(x)/e(x_{n-5}x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)=\sum_{i=1}^{n-3}x_i+x_{n-1}+x_n\tag{8}$$

则$AI(f(x))=1$，$CI(f(x))=1$，$\deg ef(x)/ex_n>1$和$\deg f(x)>2$。

证明：1)的结论显然成立，不再证明。

对于2)，由于$\deg f(x)=2$，由定理1的1)知，$\deg ef(x)/ex_n=1$。由引理3，有

$$\begin{aligned}&ef(x)/ex_n(1+f(x))\\&\quad=ef(x)/ex_n+ef(x)/ex_nf(x)df(x)/dx_n+ef(x)/ex_nef(x)/ex_n\\&\quad=0\end{aligned}\tag{9}$$

由$\deg ef(x)/ex_n=1$及式(9)知

$$AI(f(x))=1\tag{10}$$

对于任意$w_t(\omega)\geqslant 1$的$\omega x(\omega,x\in GF(2)^n)$，可推得

$$\begin{aligned}w_t(f(x)+\omega x)=&w_t(f(x)df(x)/dx_n+\omega x)+\\&w_t(ef(x)/ex_n+\omega x)-w_t(\omega x)\end{aligned}\tag{11}$$

由于$\max\limits_{\omega x}w_t(f(x)df(x)/dx_n+\omega x)=2^{n-1}+2^{n-2}$，由式(11)及已知$f(x)$相关免疫可知，必有

$$w_t(ef(x)/ex_n+\omega x)\neq 0\tag{12}$$

由已知$CI(f(x))=m\geqslant 1$、m阶相关免疫的概念、式(12)和$ef(x)/ex_n$为1次函数知，必有

$$CI(f(x))<ef(x)/ex_n\tag{13}$$

由式(10)、式(13)便知，式(6)成立。

对于3)，由引理3知

$$\begin{aligned}f(x)=&f(x)\partial f(x)/\partial(x_{n-5}x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)+\\&ef(x)/e(x_{n-5}x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)\end{aligned}$$

记

$$\begin{aligned}&\partial f(x)/\partial(x_{n-5}x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)=h_1(x)\\&ef(x)/e(x_{n-5}x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)=h_2(x)\end{aligned}\tag{14}$$

则

$$h_2(x)(1+f(x))=h_2(x)+h_2(x)f(x)h_1(x)+$$

$$h_2(x)h_2(x)=0 \tag{15}$$

可求得

$$\deg(f(x)df(x)/dx_n)=2 \tag{16}$$

由式(14)、式(16)知，$\deg h_2(x)=1$。由式(15)知，$h_2(x)$是$1+f(x)$的最低代数次数的零化子，故有$AI(f(x))=1$。

由已知式(11)成立知，可将$f(x)$分为2^{n-5}个五元函数$f_5^1(x),f_5^2(x),\cdots,f_5^{(n-5)}(x)$的级联。为记述方便且不至引起意义不清，将这$2^{n-5}$个五元函数一律称为$f_5(x)$。由于每个$f_5(x)$均满足式(11)，因此对于每个$f_5(x)$均有

$$w_t(f_5(x)|x_i=0)=w_t(f_5(x)|x_i=1)$$
$$=2^{-1}w_t(f_5(x)),i=n-4,n-3,n-2,n-1,n \tag{17}$$

又由于H布尔函数$f(x)$有$w_t(f(x))=2^{n-1}+2^{n-2}$，且有式(11)、式(12)成立，又有式(17)成立，因此对一切$i=1,2,\cdots,n$，必有

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

故$CI(f(x))=1$。

由于H布尔函数$f(x)$有$w_t(f(x))=2^{n-1}+2^{n-2}$，由引理3有$w_t(ef(x)/ex_n)=2^{n-1}$。

可假设$\deg ef(x)/ex_n=1$。则由e-导数的定义知，$ef(x)/ex_n$必为$x_{n-1},x_i+x_{n-1}(i=1,2,\cdots,n-2),x_i+x_j+x_{n-1}(i,j=1,2,\cdots,n-2,i\neq j),\cdots,x_1+x_2+\cdots+x_{n-2}+x_{n-1}$及$x_1+x_2+\cdots+x_{n-2}$等一次函数(或相应仿射函数)中的1个函数，这与式(10)矛盾。故必有$\deg ef(x)/ex_n>1$。

由定理1的1)，及$\deg ef(x)/ex_n>1$可知，$\deg f(x)>2$。

证毕。

由于式(11)、式(12)对任意非线性布尔函数都成立，且$\max ef(x)/ex_n$所含变元个数等于$n-1$，因此有推论1。

推论1 对布尔函数$f(x)$，有$\max\limits_{f(x)} CI(f(x))=n-2$。

由定理1的1)，还可得到推论2。

推论2 $f(x)$是Hamming重量为$2^{n-1}+2^{n-2}$的H布尔函数。若$AI(f(x))>1$，则必有$\deg f(x)>2$。

注意：推论2的条件和结论反过来不一定成立。

定理2 $f(x)$是Hamming重量为$2^{n-1}+2^{n-2}$的H布尔函数，且$\deg ef(x)/ex_n=1$，则$1+f(x)$有3个一次函数零化子$g_1(x)$、$g_2(x)$和$g_3(x)$，且

$$\begin{cases} g_1(x)=ef(x)/ex_n \\ g_2(x)=f(x)df(x)/dx_n+f_1(x) \\ g_3(x)=f(x)df(x)/dx_n+f_2(x) \end{cases} \tag{18}$$

其中，$f_1(x)+f_2(x)=ef(x)/ex_n$，$f_1(x)f_2(x)=0$，$w_t(f_1(x))=w_t(f_2(x))=2^{n-2}$，且$f_1(x)$使$dg_2(x)/dx_{n-1}=0$(或$dg_2(x)/dx_{n-2}=0$)，$f_2(x)$使$\partial g_3(x)/\partial(x_{n-1}x_n)=0$。

证明：由于$w_t(f(x))=2^{n-1}+2^{n-2}$，因此$w_t(1+f(x))=2^{n-2}$。故只有$1+f(x)$可以有一次函数零化子。假设$1+f(x)$的一次函数零化子为$g(x)$，有$(1+f(x))g(x)=0$，$w_t(g(x))=2^{n-1}$，$\deg g(x)=1$。由引理3有

$$(1+f(x))g(x)=g(x)+g(x)f(x)df(x)/dx_n+$$
$$g(x)ef(x)/ex_n=0 \tag{19}$$

式(19)的可能为一次函数的非零解为

$$\begin{cases} g_1(x)=ef(x)/ex_n \\ g_2(x)=f(x)df(x)/dx_n+f_1(x) \\ g_3(x)=f(x)df(x)/dx_n+f_2(x) \end{cases}$$

其中，$f_1(x)+f_2(x)=ef(x)/ex_n$，$f_1(x)f_2(x)=0$，$w_t(f_1(x))=w_t(f_2(x))=2^{n-2}$，且$f_1(x)$使$dg_2(x)/dx_{n-1}=0$(或$dg_2(x)/dx_{n-2}=0$)，$f_2(x)$使$\partial g_3(x)/\partial(x_{n-1}x_n)=0$。

由于$f(x)$有已知条件$w_t(f(x))=2^{n-1}+2^{n-2}$，$w_t(f(x)df(x)/dx_n)=2^{n-2}$，$w_t(ef(x)/ex_n)=2^{n-1}$和$w_t(df(x)/dx_i)=2^{n-1}(i=1,2,\cdots,n)$，且有$\deg ef(x)/ex_n=1$。于是，$ef(x)/ex_n$可以为$x_{n-1},x_i+x_{n-1}(i=1,2,\cdots,n-2),x_i+x_j+x_{n-1}(i,j=1,2,\cdots,n-2,i\neq j),\cdots,x_1+x_2+\cdots+x_{n-2}+x_{n-1}$及$x_1+x_2+\cdots+x_{n-2}$等一次函数中的任1个函数(当$ef(x)/ex_n$为$x_1+x_2+\cdots+x_{n-2}$时，显然$g_2(x)=x_{n-1}+x_n$，$g_3(x)=\sum\limits_{i=1}^{n}x_i$，故结论成立。因此后面不再讨论$ef(x)/ex_n$为$x_1+x_2+\cdots+x_{n-2}$的情况)。又由于$dg_2(x)/dx_{n-1}=0$，因此若将$f(x)df(x)/dx_n$和$f_1(x)$均以小项表示，则当$f(00\cdots0)=1$时，对应于$f(x)df(x)/dx_n$中的小项$\cdots(1+x_{n-1})(1+x_n)$，$\cdots(1+x_{n-1})x_n$，$\cdots x_{n-1}(1+x_n)$，$\cdots x_{n-1}x_n$，$f_1(x)$中必有小项$\cdots x_{n-1}(1+x_n)$，$\cdots x_{n-1}x_n$，$\cdots(1+x_{n-1})(1+x_n)$，$\cdots(1+x_{n-1})x_n$，且在$02^2-1,2^22^3-1,\cdots,2^n-2-12^n-1$每个小区间均有$f(x)df(x)/dx_n$的1个小项与$f_1(x)$的1个小项相对应。故有

$$g_2(x)=f(x)df(x)/dx_n+f_1(x)$$
$$=(1+x_1+x_2+\cdots+x_{n-2})+x_n((1+x_1)(1+x_2)$$
$$\cdots(1+x_{n-3})(1+x_{n-2})+(1+x_1)(1+x_2)\cdots(1$$
$$+x_{n-3})x_{n-2}+\cdots+x_1x_2x_3\cdots x_{n-3}x_{n-2})$$
$$=1+\sum_{i=1}^{n-2}x_i+x_n$$

$\partial g_3(x)/\partial(x_{n-1}x_n)=0$，则$f_2(x)$也可用小项表示。对应于$f(x)df(x)/dx_n$中的小项$\cdots(1+x_{n-1})(1+x_n)$，$\cdots(1+x_{n-1})x_n$，$\cdots x_{n-1}(1+x_n)$，$\cdots x_{n-1}x_n$，$f_2(x)$中必有小项$\cdots x_{n-1}x_n$，$\cdots x_{n-1}(1+x_n)$，$\cdots(1+x_{n-1})x_n$，$\cdots(1+x_{n-1})(1+x_n)$，同样在$02^2-1,2^22^3-1,\cdots,2^n-2-12^n-1$每个小区间均有$f(x)df(x)/dx_n$的1个小项与$f_2(x)$的1个小项相对应。故有

$$g_3(x)=f(x)df(x)/dx_n+f_2(x)=1+\sum_{i=1}^{n}x_i$$

而当$f(00\cdots0)=0$时，同样有$g_2(x)=\sum\limits_{i=1}^{n-2}x_i+x_n$和$g_3(x)=\sum\limits_{i=1}^{n}x_i$。

可知，$1+f(x)$有一次函数零化子式(18)。

证毕。

定理3 H布尔函数$f(x)$有

$$w_t(f(x))=2^{n-1}+2^{n-2} \tag{20}$$

$$\partial f(x)/\partial(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)=0 \tag{21}$$

$$\begin{cases} w_t(\partial f(x)/\partial(x_{n-1}x_n))=2^{n-2} \\ w_t(ef(x)/e(x_{n-1}x_n))=2^{n-1}+2^{n-3} \end{cases} \tag{22}$$

则$CI(f(x))=1$，且$1+f(x)$有一次函数零化子：

$$(x_{n-1}+x_n)ef(x)/e(x_{n-1}x_n)+e((1+x_{n-1}+x_n)ef(x)$$
$$/e(x_{n-1}x_n))/ex_{n-2}=x_{n-4}+x_{n-3}+x_{n-1}+x_n \tag{23}$$

证明：由于$f(x)$是满足式(20)的H布尔函数，由引理3有

$$\begin{cases} w_t(f(x)df(x)/dx_i)=2^{n-2} \\ w_t(ef(x)/ex_i)=2^{n-1} \end{cases},i=1,2,\cdots,n \tag{24}$$

由于 $f(x)$满足式(21),有

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

因此 $f(x)$为一阶相关免疫函数,有 $CI(f(x))=1$。

由于 $f(x)$是 H 布尔函数,因此对一切 $\omega x(\omega,x\in GF(2)^n)$,有

$$w_t(d(f(x)+\omega x)/dx_i)=2^{n-1}(x_i\neq\omega x) \tag{25}$$

由于 $f(x)$是一阶相关免疫函数,且有式(25)及引理3,因此当 $\omega x\neq x_i$ 时,对一切 $w_t(\omega)=1$ 的 $\omega x(\omega,x\in GF(2)^n)$,有

$$\begin{aligned}&w_t(e(f(x)+\omega x)/ex_i)\\&=w_t(ef(x)/ex_i)-2w_t(\omega xef(x)/ex_i)-\\&\quad w_t(\omega xdf(x)/dx_i)+w_t(\omega x)\\&=2^{n-2}\end{aligned} \tag{26}$$

由式(24)和式(26),便有

$$\begin{aligned}&w_t(\omega xdf(x)/dx_i)+2w_t(\omega xef(x)/ex_i)\\&=2^{n-1}+2^{n-2}\end{aligned} \tag{27}$$

由于 $f(x)$是满足式(20)的 H 布尔函数,由引理2有

$$\begin{aligned}&w_t(\omega xdf(x)/dx_i)+w_t(\omega xef(x)/ex_i)\\&=w_t(\omega x)=2^{n-1}\end{aligned} \tag{28}$$

式(27)与式(28)的联立方程组的解为:

$$\begin{cases}w_t(\omega xdf(x)/dx_i)=2^{n-2}\\w_t(\omega xef(x)/ex_i)=2^{n-2}\end{cases} \tag{29}$$

故

$$\begin{cases}w_t(x_{n-1}df(x)/dx_n)=2^{n-2}\\w_t(x_{n-1}ef(x)/ex_n)=2^{n-2}\end{cases} \tag{30}$$

由 $f(x)$一阶相关免疫及引理3知,对一切 $w_t(\omega)=1$ 的 $\omega x(\omega,x\in GF(2)^n)$,有

$$\begin{aligned}&w_t(f(x)+\omega x)\\&=w_t(f(x)df(x)/dx_n)-2w_t(\omega xf(x)df(x)/dx_n)+\\&\quad w_t(ef(x)/ex_n)-2w_t(\omega xef(x)/ex_n)+w_t(\omega x)\\&=2^{n-1}\end{aligned} \tag{31}$$

由式(24)、式(31)、式(29),便有

$$\begin{aligned}w_t(\omega xf(x)df(x)/dx_n)&=2^{-1}w_t(f(x)df(x)/dx_n)\\&=2^{n-3}\end{aligned}$$

故有

$$\begin{aligned}&w_t(x_{n-1}f(x)df(x)/dx_n)\\&=2^{-1}w_t(f(x)df(x)/dx_n)=2^{n-3}\end{aligned} \tag{32}$$

由式(22)、式(30)、式(32)及式(20)、式(24)有

$$\begin{cases}w_t((x_{n-1}+x_n)\partial f(x)/\partial(x_{n-1}x_n))=2^{n-2}\\w_t((x_{n-1}+x_n)ef(x)/ex_n)=2^{n-2}\\w_t((1+x_{n-1}+x_n)\partial f(x)/\partial(x_{n-1}x_n))=0\\w_t((1+x_{n-1}+x_n)ef(x)/ex_n)=2^{n-2}+2^{n-3}\end{cases} \tag{33}$$

由式(33)、式(20)、式(24)及式(21)知,$1+f(x)$有一次零化子:$g=x_{n-4}+x_{n-3}+x_{n-1}+x_n$,且 g 与 $f(x)$有式(34)的关系。

$$\begin{aligned}g=&(x_{n-1}+x_n)ef(x)/e(x_{n-1}x_n)+e((1+x_{n-1}+x_n)\\&ef(x)/e(x_{n-1}x_n))/ex_{n-2}\end{aligned} \tag{34}$$

证毕。

定理4 若 $f(x)$为 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数,且 $f(x)=f_1(x)\parallel f_2(x)\parallel f_3(x)\parallel f_4(x)$。其中 $f_1(x),f_2(x),f_3(x)$和 $f_4(x)$均为 $n-2$ 维的 Hamming 重量为 $2^{n-3}+2^{n-4}$的 H 布尔函数。

$$\begin{cases}g_1(x)(1+f_1(x))=0\\g_2(x)(1+f_2(x))=0\\g_3(x)(1+f_3(x))=0\\g_4(x)(1+f_4(x))=0\end{cases} \tag{35}$$

在式(35)中,$g_1(x)$、$g_2(x)$、$g_3(x)$和 $g_4(x)$分别表示 $f_1(x)$、$f_2(x)$、$f_3(x)$和 $f_4(x)$各自所有的最低代数次数的零化子。若 $g_1(x)\neq g_4(x)$,$g_2(x)\neq g_3(x)$,

$$\begin{cases}\deg g_1(x)=\deg g_4(x)=\left\lceil\dfrac{n-4}{2}\right\rceil\\\deg g_2(x)=\deg g_3(x)=\left\lceil\dfrac{n-2}{2}\right\rceil\end{cases}$$

且 $g_1(x)$和 $g_4(x)$的最高次项、$g_2(x)$和 $g_3(x)$的最高次项不完全相等,则 $f(x)$与 $1+f(x)$有最低代数次数零化子$g(x)$:

$$g(x)=g_1(x)\parallel 0\parallel 0\parallel g_4(x)\text{或 }g(x)=g_1(x)\parallel 0\parallel 0\parallel 0 \tag{36}$$

且 $g(x)(1+f(x))=0$,$\deg g(x)=\left\lceil\dfrac{n}{2}\right\rceil$,即 $f(x)$是最优代数免疫函数。

显然,由式(36)易求出 $\deg g(x)=\left\lceil\dfrac{n-4}{2}\right\rceil+2=\left\lceil\dfrac{n}{2}\right\rceil$。所以,定理4的结果是显然的,不再证明。

从定理3可以看到,$f(x)$的最低代数次数零化子用式(27)即可表示并求出。从定理4可以看到,$f(x)$的最低代数次数的零化子不可能由1个公式1步求出,必须用级联的方法分步求出。由此可知,求解布尔函数的代数免疫性和最低代数次数的零化子时,需要根据布尔函数的不同实际情况,采用不同的方法来处理。

例1 有 $f(x)=f_1(x)\parallel f_2(x)\parallel f_3(x)\parallel f_4(x)$。其中

$$\begin{aligned}f_1(x)=&x_3+x_4+x_5+x_6+x_7+x_4x_6+x_3x_4+x_3x_6+\\&x_3x_5+x_4x_5+x_5x_6+x_5x_7+x_4x_6x_7+x_3x_6x_7+\\&x_3x_4x_6+x_3x_4x_7\end{aligned}$$

$$\begin{aligned}f_2(x)=&1+x_3+x_3x_5+x_3x_6+x_3x_7+x_3x_4+x_4x_5+\\&x_4x_6+x_5x_7+x_3x_4x_5+x_3x_5x_6+x_4x_5x_7+\\&x_4x_6x_7+x_5x_6x_7+x_3x_4x_5x_7+x_3x_5x_6x_7\end{aligned}$$

$$\begin{aligned}f_3(x)=&1+x_7+x_6x_7+x_5x_6+x_5x_7+x_4x_6+x_4x_7+\\&x_1x_6+x_1x_7\end{aligned}$$

$$\begin{aligned}f_4(x)=&1+x_4+x_6+x_3x_5+x_3x_6+x_3x_7+x_4x_5+x_4x_7\\&+x_5x_6+x_6x_7+x_3x_4x_5+x_3x_5x_7+x_4x_5x_6+\\&x_4x_5x_7+x_4x_6x_7+x_5x_6x_7+x_3x_5x_6x_7\end{aligned}$$

可得到:

$$ef_1(x)/ex_7=x_5+x_4x_6+x_3x_4+x_3x_6$$

$$g_1(x)=x_3+x_4+x_6+x_7$$

$$\begin{aligned}ef_2(x)/ex_7=&1+x_3+x_5+x_4x_6+x_5x_6+x_3x_4x_5+\\&x_3x_5x_6\end{aligned}$$

$$g_2(x)=x_4+x_5+x_6+x_7+x_3x_5$$

$$ef_3(x)/ex_7=x_3+x_4+x_5+x_6$$

$$g_3(x)=x_3+x_4+x_5+x_6$$

$$\begin{aligned}ef_4(x)/ex_7=&1+x_4+x_6+x_5x_6+x_4x_5+x_4x_6+x_3+\\&x_3x_5x_6+x_3x_4x_5\end{aligned}$$

$$g_4(x)=1+x_4+x_5+x_6+x_7+x_3x_5$$

故有

$$g(x)=g_1(x)\parallel 0\parallel g_3(x)\parallel 0$$

$$=x_3+x_4+x_6+x_7+x_2x_3+x_2x_4+x_2x_6+x_2x_7+x_1x_5+x_1x_7+x_1x_2x_5+x_1x_2x_7$$

或

$$g(x)=g_1(x)\,\|\,0\,\|\,0$$
$$=x_3+x_4+x_6+x_7+x_2x_3+x_2x_4+x_2x_6+x_2x_7+x_1x_3+x_1x_4+x_1x_6+x_1x_7+x_1x_2x_3+x_1x_2x_4+x_1x_2x_6+x_1x_2x_7$$

有 $\deg g(x)=3$。

可求得 $f(x)$的最高次项为 $x_1x_2x_3x_4x_5x_7$，$\deg f(x)=6$。又可求得 $w_t(df(x)/dx_i)=2^{7-1}=64$ $(i=1,2,\cdots,7)$，$\left\lceil\frac{n}{2}\right\rceil=3$。故知 $f(x)$是最优代数免疫 H 布尔函数。

例 2　有 $f(x)=\sum_{i=1}^{5}x_i+x_1\sum_{i=2}^{4}x_i+x_2x_3+x_2x_4+x_3x_4+x_3x_5+x_1x_2x_4+x_1x_2x_5+x_1x_4x_5+x_2x_4x_5$。$f(x)$满足定理 3 的条件，的确有 $CI(f(x))=1$。$1+f(x)$有一次零化子 $g=x_1+x_2+x_4+x_5$，有 $AI(f(x))=1$。

由定理 1－4 可以发现，$\deg ef(x)/ex_n+1=\deg(f(x)df(x)/dx_n)=\deg f(x)$，这是必然的性质。因为 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数 $f(x)$，均是由一些 $w_t(f_i(x))=3$ 和 $w_t(f_j(x))=2$，或 $w_t(f_i(x))=4$ 和 $w_t(f_j(x))=2$(且 $f_i(x)$和 $f_j(x)$成对出现)的二元函数级联构成。当构成三元 H 布尔函数时，有：若 $w_t(ef(x)/ex_n)=4$，则 $w_t(f(x)df(x)/dx_n)=2$，$d(f(x)df(x)/dx_n)/dx_n=df(x)/dx_n=1+ef(x)/ex_n$，$f(x)=f(x)df(x)/dx_n+ef(x)/ex_n$。$f(x)$的最低代数次数零化子 $g(x)$可以由式(36)的取 0 的级联方法进行级联得到。

因此，下面不加证明地给出定理 5。

定理 5　$f(x)$是 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数。设 $g(x)$为 $f(x)$的最低代数次数的零化子，则

$$\deg g(x)\leqslant\deg ef(x)/ex_n$$
$$=\deg(f(x)df(x)/dx_n)-1=\deg f(x)-1$$

推论 3　$f(x)$是 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数，$g(x)$是 $f(x)$的最低代数次数的零化子。若 $\partial f(x)/\partial(x_1x_2\cdots x_n)=0$，$\deg ef(x)/ex_n=2$，则有 $CI(f(x))=1$，$AI(f(x))=1$ 和 $\deg f(x)=3$。

结束语　本文得到了 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数的代数次数、代数免疫性与相关免疫性的关联关系。从前述的定理和证明可以看出，其能对这些性质起决定性作用，从而将这些性质联系到一起的是构成 $f(x)$的组成部分 $ef(x)/ex_n$(e-导数)，及 $f(x)df(x)/dx_n$ 与 $ef(x)/ex_n$ 的某种结合。本文对 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数对多种密码学性质相容性的研究，可为下一步研究 Bent 函数、弹性 H 布尔函数、旋转对称 H 布尔函数对多种密码学性质的相容性打下基础。从文中 e-导数对 $f(x)$的密码学性质起着关键影响这一结果来看，在下一步研究 Bent 函数、弹性 H 布尔函数、旋转对称 H 布尔函数对多种密码学性质的相容性时，$ef(x)/ex_n$ 和 $f(x)df(x)/dx_n$ 也必定会起关键性作用，成为研究相关问题的锁钥。

另外，文中另一重要结果就是利用 e-导数和导数，导出了公式法和级联法两种求解 Hamming 重量为 $2^{n-1}+2^{n-2}$的 H 布尔函数最低代数次数零化子的方法，并给出了两种方法适用的函数类别及特点。这些结果也将作为我们今后对其它类别 H 布尔函数、一般布尔函数的代数次数及代数免疫性研究的一个方法性的基础。因此，本文的研究结果是重要的。

参 考 文 献

[1] Xiao G, Massey J. A Spectral Characterization of Correlation-Immune Combining Functions[J]. IEEE Trans. on Inform. Theory, 1988, 34(3): 569-571

[2] Preneel B, Leekwijck W, Linden L, et al. Propagation Characteristics of Boolean Functions[M]// Advances in Cryptology-EUROCRYPT'90, 1991, 473: 161-173

[3] Pan S, Fu X, Zhang W. Construction of 1-Resilient Boolean Functions with Optimal Algebraic Immunity and Good Nonlinearity[J]. Journal of Computer Science and Technology, 2011, 26(2): 269-275

[4] Zheng Y, Zhang X. Plateaued functions: Information and Communication Security Second International Conference [C]// ICICS'99. Sydney, Australia, 1999, LNCS, 1726: 284-300

[5] Meier W, Pasalic E, Carle C. Algebraic attacks and decomposition of Boolean functions[C]// Advances in Cryptology-EUROCRYPT 2004. Interlaken, Switzerland, 2004, LNCS, 3027: 474-491

[6] 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

[7] Batten L M. Algebraic Attacks over GF(q)[C]// Progress in Cryptology-INDOCRYPT 2004. Chennai, India, 2005, LNCS, 3348: 84-91

[8] Armknecht F, Carlet C, Gaborit P, et al. Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks [C]// Advances in Cryptology-EUROCRYPT 2006St. Petersburg, Russia, 2006, LNCS, 4004: 147-164

[9] Didier F, Tillich J. Computing the algebraic immunity efficiently [M]// Fast Software Encryption 2006, 2006, 4047: 359-374

[10] Zhang W, Wu C, Yu J. On the Annihilators of Cryptographic Boolean Functions[J]. Acta Electronica Sinica, 2006, 34(1): 51-54

[11] Reed I S. A class of multiple-error-correcting codes and the decoding scheme[J]. IRE Transactions on Information Theory, 1954, 4(4): 38-49

[12] Akers S B. On a theory of Boolean functions[J]. Journal of the Society for Industrial and Applied Mathematics, 1959, 7(4): 487-498

[13] 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

[14] 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