满足严格雪崩准则相关免疫函数的代数免疫阶

黄景廉[1] 王 卓[1] 张志杰[2]
(西北民族大学计算机科学与信息工程学院 兰州 730030)[1]
(辽宁工程技术大学软件学院 阜新 123000)[2]

摘 要 以布尔函数的导数和自定义的e-导数为研究工具,讨论满足严格雪崩准则、具有相关免疫性、重量为$2^{n-1}+2^{n-2}$的H布尔函数的代数免疫问题。得出这类函数奇数($n\geqslant 17$)元、偶数($n\geqslant 16$)元的最优代数免疫函数及其构造方法,给出了代数免疫阶$AI(f)\geqslant 8$的n元代数免疫函数的构造方法;还给出了零化子及最低代数次数零化子的求法及其与布尔函数的导数的关系等结果。

关键词 H布尔函数,相关免疫性,子函数,最优代数免疫,代数免疫阶
中图法分类号 TP309 **文献标识码** A

Algebraic Immune Order of Correlation Immune Functions Satisfying Strict Avalanche Criterion

HUANG Jing-lian[1] WANG Zhuo[1] ZHANG Zhi-jie[2]
(College of Computer Science and Information Engineering, Northwest University for Nationalities, Lanzhou 730030, China)[1]
(College of Software, Liaoning Technical University, Fuxin 123000, China)[2]

Abstract Using the derivative of Boolean functions and custom e-derivative as a research tool, we discussed the issue of algebraic immunity of H Boolean function with correlation immunity and weight of $2^{n-1}+2^{n-2}$ which meets the strict avalanche criterion. We got the optimal algebraic immunity function and its construction method of these functions with odd($n\geqslant 17$) variables and even($n\geqslant 16$) variables and gave the construction method of algebraic immunity function with n variables that the algebraic immunity order is $AI(f)\geqslant 8$, also gave the method of solving the annihilator and the minimum algebraic degree annihilators and the derivative relations of annihilator and the Boolean function. The derivative of the Boolean function and the e-derivative defined with derivative can directly and explicitly depict the weight of the Boolean functions as research tools, in-depth to the internal structure of the value of the Boolean function.

Keywords H Boolean function, Correlation immune, Subfunction, Optimal algebraic immunity, Algebraic immunity order

1 引言

弹性函数的代数免疫阶、弹性函数的最优代数免疫函数构造,是当前正在认真研究的问题。近来文献[1]给出偶数元一阶弹性最优代数免疫函数的构造;文献[2]运用计算机搜索,给出了2个10元二阶弹性函数。而奇数元弹性最优代数免疫函数问题的解决多年未见进展,近来文献[1]给出1个5元一阶弹性最优代数免疫函数的例子。因此,需要对弹性函数的代数免疫问题进行进一步研究,以给出更进一步的新的结果。而解决满足严格雪崩准则相关免疫函数的更高维的奇数元最优代数免疫函数构造问题,将为奇数元最优代数免疫弹性函数的构造问题得出更好的结果打下基础。

下面将对Hamming重量$2^{n-1}+2^{n-2}$的相关免疫H布尔函数的奇数元和偶数元的最优代数免疫函数的构造、代数免疫阶、最低代数次数零化子的求法等问题进行讨论。

2 预备知识和一些基本定理

布尔函数的导数是人们所熟知的[3-6]。这里给出布尔函数的e-导数的定义[7-10]。

定义1 n元布尔函数$f(x)$对变元$x_{i1},x_{i2},\cdots,x_{ir}$($1\leqslant r\leqslant n, 1\leqslant i_1<i_2<\cdots<i_r\leqslant n$)的e-导数定义为

$$ef(x)/e(x_{i1},\cdots,x_{ir})=f(x_1,\cdots,x_{i1},\cdots,x_{ir},\cdots,x_n)f(x_1,\cdots,x_{i1},\cdots,\bar{x}_{i1},\cdots,\bar{x}_{ir},x_{ir+1},\cdots,x_n)(1\leqslant r\leqslant n,1\leqslant i_1<i_2<\cdots<i_r\leqslant n) \quad (1)$$

式中,$f(x)$对单个变元x_i($i=1,2,\cdots,n$)的e-导数,经简单推导,有如下便于使用的形式:

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

为便于使用布尔函数的导数和e-导数展开讨论,本文对两个n元布尔函数$f_1(x)$和$f_2(x)$的级联函数作如下定义。

到稿日期:2012-06-05 返修日期:2012-09-21 本文受国家自然科学基金项目(61262085),中央高校基本科研业务费专项资金项目(ZYZ2011055)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;张志杰(1973-),女,硕士,讲师,主要研究方向为计算机密码学与网络安全、密码学。

定义 2 两个 n 元布尔函数 $f_1(x)$ 和 $f_2(x)$ 的 $n+1$ 元级联函数 $f(x)$ 定义为

$$f(x)=(1+x_0)f_1(x)+x_0f_2(x) \tag{3}$$

n 元 H 布尔函数按重量的定义[3]和导数的重量定义是等价的，于是有定理 1。

定理 1 n 元布尔函数 $f(x)$ 是 H 布尔函数，当且仅当对一切 $x_i(i=1,2,\cdots,n)$，有

$$w_t(\mathrm{d}f(x)/\mathrm{d}x_i)=2^{n-1}(i=1,2,\cdots,n) \tag{4}$$

由导数、e-导数的定义即可直接得出用导数、e-导数表示函数 $f(x)$ 的表示式及函数重量的表示，如定理 2。

定理 2 对任意 n 元布尔函数 $f(x)$，有

$$f(x)=f(x)\mathrm{d}f(x)/\mathrm{d}x_i+ef(x)/ex_i(i=1,2,\cdots,n)$$

$$w_t(f(x))=2^{-1}w_t(\mathrm{d}f(x)/\mathrm{d}x_i)+w_t(ef(x)/ex_i)(i=1,2,\cdots,n) \tag{5}$$

由定理 1、定理 2 即可得到定理 3。

定理 3 (1) n 元布尔函数是 Hamming 重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数的充要条件是

$$w_t(\mathrm{d}f(x)/\mathrm{d}x_i)=2^{n-1}\text{且}\ w_t(ef(x)/ex_i)=2^{n-1}(i=1,2,\cdots,n) \tag{6}$$

(2) n 元布尔函数 $f(x)$ 是 Hamming 重量为 2^{n-2} 的 H 布尔函数的充要条件是

$$w_t(\mathrm{d}f(x)/\mathrm{d}x_i)=2^{n-1}\text{且}\ w_t(e_f(x)/ex_i)=0(i=1,2,\cdots,n) \tag{7}$$

3 Hamming 重量 $2^{n-1}+2^{n-2}$ 的 H 布尔函数的构造

对 $w_t(f(x))=2^{n-1}+2^{n+2}$ 的 H 布尔函数，根据定理 3，有 $w_t(\mathrm{d}f(x)/\mathrm{d}x_n)=2^{n-1}$ 和 $w_t(ef(x)/ex_n)=2^{n-1}$，故线性函数 $h_1(x)=\sum_{i=2}^{n}x_i$ 和常数函数 $h_2(x)=1$ 的级联函数 $f(x)=(1+x_1)h_1(x)+x_1h_2(x)$ 有 $w_t(\mathrm{d}f(x)/\mathrm{d}x_i)=w_t(1+x_1)=2^{n-1}$，$w_t(ef(x)/ex_i)=w_t(x_1)=2^{n-1}(i=n,n-1,\cdots,2)$。$w_t(\mathrm{d}f(x)/\mathrm{d}x_1)=w_t(h_1(x)+h_2(x))=w_t(\sum_{i=2}^{n}x_i+1)=2^{n-1}$，$w_t(ef(x)/ex_1)=w_t(h_2(x)h_1(x))=w_t(h_1(x))=2^{n-1}$，故有定理 4。

定理 4 $n-1$ 维布尔函数 $h_1(x_2,x_3,\cdots,x_n)=\sum_{i=2}^{n}x_i$，$h_2(x_2,x_3,\cdots,x_n)=1$ 的 n 维级联函数

$$f(x)=(1+x_1)h_1(x_2,x_3,\cdots,x_n)+x_1h_2(x_2,x_3,\cdots,x_n) \tag{8}$$

是重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数。

于是由定理 4 可知，由二元函数 $g_{01}=x_{n-1}+x_n$（或 $1+x_{n-1}+x_n$）与 $g_{02}=1$ 经 $n-2$ 次逐步级联成的 n 元布尔函数是重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数。

将 $f(x)=(1+x_{n-2})g_{01}+x_{n-2}g_{02}$ 中的值按 $w_t(\mathrm{d}f(x)/\mathrm{d}x_n)=2^2$，$w_t(ef(x)/ex_n)=2^2$ 的要求进行所有可能的排列，在所有可能的 $c_2^2c_2^1+c_2^1c_2^1c_3^1=14$ 种排列中，能满足 $w_t(\mathrm{d}f(x)/\mathrm{d}x_i)=2^2$，$w_t(ef(x)/ex_i)=2^2(i=n-1,n-2)$ 要求的二元函数除 g_{01}、g_{02} 外，还有 $g_{11}=x_{n-1}+x_n+x_{n-1}x_n$ 和 $g_{12}=1+x_{n-1}x_n$ 及 $g_{21}=1+x_n+x_{n-1}x_n$ 和 $g_{22}=1+x_{n-1}+x_{n-1}x_n$。可知定理 4 中的级联函数也是由 g_{01} 和 g_{02} 逐步级联构成的。由 g_{01} 和 g_{02}、g_{21}、g_{22}、g_{11}、g_{12} 进行满足定理 3 要求的级联构成 n 元函数，总共有 $c_{2^{n-2}}^2c_2^1+c_{2^{n-3}}^4(c_4^2+c_4^3+c_4^4)$ 个，是指数级的函数，数量是很大的，这就是所有 Hamming 重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数的数量。

4 最优代数免疫的相关免疫 H 布尔函数

若 $w_t(f)=r\neq0$，设 $g(1+f)=0$ 且 $g\neq0$，即 g 也是 f 的零化子。故知 g 必是与 f 有 1 个 1 值，或 2 个 1 值，…，或 $r-1$ 个 1 值，或 r 个 1 值取值相同，其余值为 0 的 n 维函数。为方便考虑，不妨称 g 为 f 的子函数。于是，可把 f 的子函数分别记为 $g_1,g_2,\cdots,g_r$，以对应 g_i 与 f 的 i 个 1 值取值相同。可知，子函数一定是零化子，但零化子不全是子函数。

定理 5 对 $w_t(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数 $f(x)$（简记为 f），设 $g(x)$（简记为 g）是 f 的子函数，且有 $f=g+h$，$hg=0$。若 g 是线性函数，则对一切 $i=1,2,\cdots,n$，有

$$w_t(\mathrm{d}h/\mathrm{d}x_i)=2^{n-1} \tag{9}$$

证明：因 g 是线性函数，则

$$\frac{\mathrm{d}g}{\mathrm{d}x_i}=\begin{cases}1, & \text{当 } g \text{ 中含有 } x_i \text{ 项}\\ 0, & \text{当 } g \text{ 中不含 } x_i \text{ 项}\end{cases} \tag{10}$$

又因 $f(x)$ 是 H 布尔函数，$f=g+h$，$gh=0$，故必有

$$w_t(\mathrm{d}f/\mathrm{d}x_i)=w_t(\mathrm{d}g/\mathrm{d}x_i)+w_t(\mathrm{d}h/\mathrm{d}x_i)-2w_t(\mathrm{d}g/\mathrm{d}x_i\mathrm{d}h/\mathrm{d}x_i)=2^{n-1}(i=1,2,\cdots,n) \tag{11}$$

故由式(10)、式(11)知，对一切 $i=1,2,\cdots,n$，都有式(9)成立。

定理 5 告诉我们，对重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数 f，当 f 有线性子函数时，f 的线性子函数（线性零化子）要在 $\mathrm{d}f/\mathrm{d}x_n$ 和 ef/ex_n 中同时取值，否则就取不到线性子函数（线性零化子），这就为求 f 可能具有的线性零化子给出了方向。由于定理 5 的条件是必要条件，因此 f 中不一定就有线性子函数（线性零化子），这就为寻找代数免疫阶较高的 f 提供了理论依据。

推论 1 在定理 5 的条件中，若 g 还含有变量 x_i，则

$$\mathrm{d}h/\mathrm{d}x_i=1+\mathrm{d}f/\mathrm{d}x_i \tag{12}$$

例 1 $f(x)=(x_{n-1}+x_n)+\sum_{i=1}^{n-2}x_i+x_{n-1}\sum_{i=1}^{n-2}x_i+x_n\sum_{i=1}^{n-1}x_i$，则 $f(x)$ 有线性子函数（线性零化子）$g=x_{n-1}+x_n$。

定理 6 设 $f_1(x)$ 和 $f_2(x)$ 是两个 n 元布尔函数，有 $\deg f_1(x)=m_1$，$\deg f_2(x)=m_2$，级联函数为

$$f(x)=(1+x_0)f_1(x)+x_0f_2(x) \tag{13}$$

(1)若 $m_1\neq m_2$，则 $\deg f(x)=\max(m_1,m_2)+1$。

(2)若 $m_1=m_2=m$：

① 又若 $f_1(x)=f_2(x)$，或 $f_1(x)+f_2(x)=1$，则 $\deg f(x)=m$；

② 而若 $f_1(x)\neq f_2(x)$，$f_1(x)+f_2(x)\neq1$，且 $f_1(x)$ 的最高次项 $\neq f_2(x)$ 的最高次项，则 $\deg f(x)=m+1$；

定理 6 是明显的，不再证明。

推论 2 若 $h_1(x)\neq h_2(x)\neq h_3(x)$，$h_1(x)\neq1+h_2(x)$，$h_2(x)\neq1+h_3(x)$，$\deg h_1(x)=m_1$，$\deg h_2(x)=m_2$，$\deg h_3(x)=m_3$，$m_1>m_2=m_3$，但 $h_2(x)$ 的最高次项 $\neq h_3(x)$ 的最高次项，则对级联函数

$$f_1(x)=(1+x_{i+1})((1+x_i)h_1(x)+x_ih_2(x))+x_{i+1}((1+x_i)h_2(x)+x_ih_3(x))$$

$$f_2(x)=(1+x_{i+1})((1+x_i)h_1(x)+x_ih_2(x))+x_{i+1}((1+x_i)h_2(x)+x_ih_1(x)) \tag{14}$$

必有 $\deg f_1(x)=m_1+2$，$\deg f_2(x)=m_2+1=m_3+1$。

推论 2 的证明很简单，不再证明。定理 6 和推论 2 虽然简单，但对下面构造具有较高的代数免疫阶的相关免疫 H 布尔函数却起着基础性的重要作用。

因要寻找的代数免疫函数还要求具有相关免疫性，故先给出一个级联函数的相关免疫性的定理。

定理 7 若 n 元函数 $f(x)$ 是由 2 个 $n-1$ 元函数 $f_1(x)$、$f_2(x)$ 级联构成，即

$$f(x)=(1+x_0)f_1(x)+x_0f_2(x) \tag{15}$$

则 $f(x)$ 是 k 阶相关免疫函数的充要条件是：对一切 $1\leqslant\omega\leqslant k$，$\omega\in GF(2)$，${}^n x\in GF(2)^n$，

$$w_t(f_1(x)+\omega x)+w_t(f_2(x)+\omega x)=2^n \tag{16}$$

证明：经推导，有

$$\begin{aligned}w_t(f(x)+\omega x)&=w_t((1+x_0)f_1(x)+x_0f_2(x)+\omega x+\omega x\\&\quad+\omega x)\\&=w_t((1+x_0)f_1(x)+\omega x+(x_0f_2(x)+\\&\quad\omega x)+\omega x)\\&=w_t(f_1(x)+\omega x)+w_t(f_2(x)+\omega x)-w_t\\&\quad(\omega x)\end{aligned} \tag{17}$$

因 $w_t(\omega x)=2^{n-1}$，故由式(17)、式(16)知，$w_t(f(x)+\omega x)=2^{n-1}$，当且仅当

$$w_t(f_1(x)+\omega x)+w_t(f_2(x)+\omega x)=2^n$$

即定理结论成立。

下面用构造性的方法来证明在 Hamming 重量为 $2^{n-1}+2^{n-2}$ 的相关免疫 n 元 H 布尔函数中，存在 $n\geqslant16$ 元(偶数元)和 $n\geqslant17$ 元(奇数元)的最优代数免疫函数，以及 $\{f(x)\}$ 中的相关免疫 H 布尔函数的最高代数免疫阶 $AI(f)\geqslant8$。

定理 8 在 Hamming 重量为 $2^{n-1}+2^{n-2}$ 的相关免疫 H 布尔函数 $\{f(x)\}$ 中，存在 $n\geqslant16$ 元(偶数元)和 $n\geqslant17$ 元(奇数元)的相关免疫的最优代数免疫 H 布尔函数，$\{f(x)\}$ 中的相关免疫 H 布尔函数的最高代数免疫阶 $\max AI(f)\geqslant8$。

证明：在第 3 节中已证明 Hamming 重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数只能由 $g_{01}=x_{n-1}+x_n$，$g_{02}=1$，$g_{21}=1+x_n+x_{n-1}x_n$，$g_{22}=1+x_{n-1}+x_{n-1}x_n$ 级联构成，或 $g_{11}=x_{n-1}+x_n+x_{n-1}x_n$，$g_{12}=1+x_{n-1}x_n$ 与 g_{21}，g_{22} 级联构成。又根据定理 6 知，需要在级联时保证每一参与级联的函数的零化子都与其它参与级联的函数不同，以使各级联函数的零化子也不同。于是可得 5 元 H 布尔函数如下。

$$\begin{aligned}f_1&=(1+x_{n-4})((1+x_{n-3})((1+x_{n-2})g_{01}+x_{n-2}g_{21})+\\&\quad x_{n-3}((1+x_{n-2})g_{21}+x_{n-2}g_{02}))+x_{n-4}((1+x_{n-3})\\&\quad((1+x_{n-2})g_{21}+x_{n-2}g_{22})+x_{n-3}((1+x_{n-2})g_{02}+\\&\quad x_{n-2}g_{01}))\\f_2&=(1+x_{n-4})((1+x_{n-3})((1+x_{n-2})g_{21}+x_{n-2}g_{22})+\\&\quad x_{n-3}((1+x_{n-2})g_{22}+x_{n-2}g_{21}))+x_{n-4}((1+x_{n-3})\\&\quad((1+x_{n-2})g_{22}+x_{n-2}g_{21})+x_{n-3}((1+x_{n-2})g_{21}+\\&\quad x_{n-2}g_{22}))\\f_3&=(1+x_{n-4})((1+x_{n-3})((1+x_{n-2})g_{22}+x_{n-2}g_{21})+\\&\quad x_{n-3}((1+x_{n-2})g_{21}+x_{n-2}g_{22}))+x_{n-4}((1+x_{n-3})\\&\quad((1+x_{n-2})g_{21}+x_{n-2}g_{22})+x_{n-3}((1+x_{n-2})g_{22}+\\&\quad x_{n-2}g_{21}))\end{aligned} \tag{18}$$

式中，f_1，f_2，f_3 分别有最低代数次数的零化子 $g_1=\sum_{i=n-4}^{n}x_i+x_{n-4}x_{n-2}$，$g_2=g_3=1+x_{n-1}+x_n$。

又由于要使这些 5 元函数经级联构成更多元的级联函数是相关免疫函数，则根据定理 6 和推论 2 构造如下 f_4。

$$\begin{aligned}f_4&=(1+x_{n-4})((1+x_{n-3})((1+x_{n-2})g_{02}+x_{n-2}g_{22})+\\&\quad x_{n-3}((1+x_{n-2})g_{22}+x_{n-2}g_{01}))+x_{n-4}((1+x_{n-3})\\&\quad((1+x_{n-2})g_{01}+x_{n-2}g_{02})+x_{n-3}((1+x_{n-2})g_{21}+\\&\quad x_{n-2}g_{22}))\end{aligned} \tag{19}$$

f_4 有最低代数次数的零化子 $g_4=\sum_{i=n-3}^{n}x_i+x_{n-4}x_{n-2}$。

由于

$$w_t(df_i/dx_r)=2^{n-1}(i=1,2,3,4;r=n,n-1,n-2,n-3,n-4) \tag{20}$$

因此由定理 1 知，$f_i(i=1,2,3,4)$ 均为 H 布尔函数。又由于

$$w_t(ef_i/ex_r)=2_{n-1}(i=1,2,3,4;r=n,n-1,n-2,n-3,n-4;n=5) \tag{21}$$

因此由定理 3 知，$f_i(i=1,2,3,4)$ 重量均为 $2^{n-1}+2^{n-2}(n=5)$。

由于

$$w_t(f_i+x_r)=2^{n-1}(i=2,3;r=n,n-1,n-2,n-3,n-4;n=5) \tag{22}$$

因此 f_2 和 f_3 是相关免疫函数。故 f_2 和 f_3 的级联函数是相关免疫函数。又由于

$$w_t(f_1+x_r)+w_t(f_4+x_r)=2^n(r=n,n-1,n-2,n-3,n-4;n=5) \tag{23}$$

因此由定理 7 知，f_1 和 f_4 级联构成的级联函数是相关免疫函数。

根据定理 6、推论 2，再构造 5 元 H 布尔函数 f_5 如下。

$$\begin{aligned}f_5&=(1+x_{n-4})((1+x_{n-3})((1+x_{n-2})g_{22}+x_{n-2}g_{02})+\\&\quad x_{n-3}((1+x_{n-2})g_{01}+x_{n-2}g_{22}))+x_{n-4}((1+x_{n-3})\\&\quad((1+x_{n-2})g_{02}+x_{n-2}g_{01})+x_{n-3}((1+x_{n-2})g_{22}+\\&\quad x_{n-2}g_{21})\end{aligned} \tag{24}$$

同样，有

$$w_t(df_5/dx_i)=2^{n-1},w_t(ef_5/ex_i)=2^{n-1}(i=n,n-1,n-2,n-3,n-4;n=5) \tag{25}$$

故 f_5 是重量为 $2^{n-1}+2^{n-2}(n=5)$ 的 H 布尔函数。又

$$w_t(f_1+x_i)+w_t(f_5+x_i)=2^n(i=n,n-1,n-2,n-3,n-4;n=5) \tag{26}$$

因此由定理 7 知，f_1 和 f_5 的级联函数是相关免疫函数。

作级联函数

$$\begin{aligned}F_1&=(1+x_{n-8})\ ((1+x_{n-7})((1+x_{n-6})((1+x_{n-5})f_1+\\&\quad x_{n-5}f_4)+x_{n-6}((1+x_{n-5})f_4+x_{n-5}f_3))+x_{n-7}((1\\&\quad+x_{n-6})((1+x_{n-5})f_5+x_{n-5}f_1))+x_{n-6}((1+x_{n-5})\\&\quad f_1+x_{n-5}f_2)))+x_{n-8}((1+x_{n-7})((1+x_{n-6})((1+\\&\quad x_{n-5})f_4+x_{n-5}f_3)+x_{n-6}((1+x_{n-5})f_1+x_{n-5}f_2))\\&\quad+x_{n-7}((1+x_{n-6})((1+x_{n-5})f_1+x_{n-5}f_4)+x_{n-6}\\&\quad((1+x_{n-5})f_5+x_{n-5}f_1)))\\F_2&=(1+x_{n-8})((1+x_{n-7})((1+x_{n-6})((1+x_{n-5})f_1+\\&\quad x_{n-5}f_4)+x_{n-6}((1+x_{n-5})f_4+x_{n-5}f_5))+x_{n-7}((1\\&\quad+x_{n-6})((1+x_{n-5})f_5+x_{n-5}f_1))+x_{n-6}((1+x_{n-5})\\&\quad f_1+x_{n-5}f_4)))+x_{n-8}(1+x_{n-7})((1+x_{n-6})((1+\\&\quad x_{n-5})f_2+x_{n-5}f_1)\ +x_{n-6}((1+x_{n-5})f_3+x_{n-5}f_4))\\&\quad+x_{n-7}((1+x_{n-6})((1+x_{n-5})f_1+x_{n-5}f_2)+x_{n-6}\\&\quad((1+x_{n-5})f_2+x_{n-5}f_1)))\end{aligned}$$

$$F_3=(1+x_{n-8})((1+x_{n-7})((1+x_{n-6})((1+x_{n-5})f_2+x_{n-5}f_3)+x_{n-6}((1+x_{n-5})f_3+x_{n-5}f_4))+x_{n-7}((1+x_{n-6})((1+x_{n-5})f_1+x_{n-5}f_2))+x_{n-6}((1+x_{n-5})f_2+x_{n-5}f_3)))+x_{n-8}((1+x_{n-7})((1+x_{n-6})((1+x_{n-5})f_3+x_{n-5}f_2)+x_{n-6}((1+x_{n-5})f_2+x_{n-5}f_3))+x_{n-7}((1+x_{n-6})((1+x_{n-5})f_2+x_{n-5}f_3)+x_{n-6}((1+x_{n-5})f_1+x_{n-5}f_4))) \quad (27)$$

由于

$$w_t(\mathrm{d}F_r/\mathrm{d}x_i)=2^{n-1}(n=9;r=1,2,3;i=n,n-1,\cdots,n-8) \quad (28)$$

因此 $F_r(r=1,2,3)$均为 H 布尔函数，且因 $f_i(i=1,2,3,4,5)$均为 $2^{n-1}+2^{n-2}(n=6)$ 重量，故 $F_r(r=1,2,3)$也是 $2^{n-1}+2^{n-2}(n=9)$ 重量。又由于[11]

$$w_t(x_iF_r\mathrm{d}F_r/\mathrm{d}x_s)=2^{n-3},w_t(x_ieF_r/ex_s)=2^{n-2}\ (n=9;r=1,2,3;s,i=n,n-1,\cdots,n-8,s\neq i) \quad (29)$$

因此由定理 2 及相关免疫定义知，$F_r(r=1,2,3)$均为相关免疫函数。

作级联函数

$$P_1(x)=(1+x_{n-9})F_1+x_{n-9}F_3=F_1+x_{n-9}(F_1+F_3)$$
$$P_2(x)=(1+x_{n-9})F_3+x_{n-9}F_1=F_3+x_{n-9}(F_1+F_3) \quad (30)$$

可求得 f_1,f_2,f_3,f_4,f_5 分别有最低代数次数的子函数(零化子)，分别为

$$g_1=x_{n-4}+x_{n-3}+x_{n-2}+x_{n-1}+x_n+x_{n-4}x_{n-2}$$
$$g_2=g_3=1+x_{n-1}+x_n \quad (31)$$
$$g_4=g_5=x_{n-3}+x_{n-2}+x_{n-1}+x_n+x_{n-4}x_{n-2}$$

于是根据定理 6、推论 2 及式(31)，可求得 P_1 的最低代数次数的零化子的最高代数次数的项为 $x_{n-8}x_{n-7}x_{n-5}x_{n-4}x_{n-2},x_{n-9}x_{n-7}x_{n-6}x_{n-4}x_{n-2},x_{n-9}x_{n-8}x_{n-5}x_{n-4}x_{n-2}$，为 5 次，即 P_1 的代数免疫阶为 $AI(P_1)=5$。求得 P_2 的最低代数次数的零化子的最高代数次数的项为 $x_{n-8}x_{n-6}x_{n-5}x_{n-4}x_{n-2},x_{n-9}x_{n-7}x_{n-6}x_{n-4}x_{n-2},x_{n-9}x_{n-8}x_{n-5}x_{n-4}x_{n-2}$，为 5 次，即 P_2 的代数免疫阶为 $AI(P_2)=5$。再作级联函数

$$r_1=F_1+x_{n-9}(F_1+F_3)+x_{n-10}(F_1+F_3)+x_{n-10}x_{n-9}(0)$$
$$r_2=F_3+x_{n-9}(F_3+F_1)+x_{n-10}(F_3+F_1)+x_{n-10}x_{n-9}(0)$$
$$h_1=F_1+x_{n-9}(F_1+F_3)+x_{n-10}(F_1+F_3)+x_{n-10}x_{n-9}(0)+x_{n-11}(F_1+F_3)+x_{n-11}x_{n-9}(0)+x_{n-11}x_{n-10}(0)+x_{n-11}x_{n-10}x_{n-9}(0)$$
$$h_2=F_3+x_{n-9}(F_3+F_1)+x_{n-10}(F_3+F_1)+x_{n-10}x_{n-9}(0)+x_{n-11}(F_3+F_1)+x_{n-11}x_{n-9}(0)+x_{n-11}x_{n-10}(0)+x_{n-11}x_{n-10}x_{n-9}(0) \quad (32)$$

由定理 6、推论 2 及式(32)可知，$AI(r_1)=AI(r_2)=AI(h_1)=AI(h_2)=5$。又 P_1,P_2 是 $n=10$ 元(偶数元)布尔函数，r_1,r_2 是 $n=11$ 元(奇数元)布尔函数，故 P_1,P_2,r_1,r_2 是最优代数免疫函数。同式(28)、式(29)的证明相仿，P_1,P_2,r_1,r_2(还包括 h_1,h_2)都是 Hamming 重量 $2^{n-1}+2^{n+2}$ 的、具有相关免疫性的 H 布尔函数。

从 r_1,r_2,h_1,h_2 的级联结果可知，用归纳法证明，由 h_1,h_2 进一步作 n 元级联函数，可得到 n 元的代数免疫阶为 $AI(f(x))=5$ 的代数免疫函数 $f(x)$。而与式(28)、式(29)的证明相仿，$f(x)$是 Hamming 重量 $2^{n-1}+2^{n-2}$ 的、具有相关免疫性的 H 布尔函数。

根据定理 6 及推论 2，加入 F_2 与 F_1 和 F_3 一起级联可以提高代数免疫阶数。于是由 F_1,F_2,F_3 构造

$$S_1=(1+x_{n-11})((1+x_{n-10})((1+x_{n-9})F_1+x_{n-9}F_3)+x_{n-10}((1+x_{n-9})F_3+x_{n-9}F_2))+x_{n-11}((1+x_{n-10})((1+x_{n-9})F_3+x_{n-9}F_2)+x_{n-10}((1+x_{n-9})F_2+x_{n-9}F_3))$$
$$S_2=(1+x_{n-11})((1+x_{n-10})((1+x_{n-9})F_3+x_{n-9}F_2)+x_{n-10}((1+x_{n-9})F_2+x_{n-9}F_3))+x_{n-11}((1+x_{n-10})((1+x_{n-9})F_2+x_{n-9}F_3)+x_{n-10}((1+x_{n-9})F_3+x_{n-9}F_2)) \quad (33)$$

对 S_1 和 S_2 作级联函数

$$f(x)=(1+x_{n-15})((1+x_{n-14})((1+x_{n-13})S_1+x_{n-13}S_2)+x_{n-14}((1+x_{n-13})S_2+x_{n-13}S_1))+x_{n-15}((1+x_{n-14})((1+x_{n-13})S_2+x_{n-13}S_1)+x_{n-14}((1+x_{n-13})S_1+x_{n-13}S_2))$$
$$g(x)=(1+x_{n-16})((1+x_{n-15})((1+x_{n-14})((1+x_{n-13})S_1+x_{n-13}S_2)+x_{n-14}((1+x_{n-13})S_2+x_{n-13}S_1))+x_{n-15}((1+x_{n-14})((1+x_{n-13})S_2+x_{n-13}S_1)+x_{n-14}((1+x_{n-13})S_1+x_{n-13}S_2)))+x_{n-16}((1+x_{n-15})((1+x_{n-14})((1+x_{n-13})S_2+x_{n-13}S_1)+x_{n-14}((1+x_{n-13})S_1+x_{n-13}S_2))+x_{n-15}((1+x_{n-14})((1+x_{n-13})S_1+x_{n-13}S_2)+x_{n-14}((1+x_{n-13})S_1+x_{n-13}S_2))) \quad (34)$$

因 $w_t(\mathrm{d}f(x)/\mathrm{d}x_i)=2^{n-1},w_t(ef(x)/ex_i)=2^{n-1}(n=16,i=n,n-1,\cdots,n-15)$，故由定理 3 知，$f(x)$是重量为 $2^{n-1}+2^{n-2}$ 的 H 布尔函数。又由于

$$w_t(x_if(x)\mathrm{d}f(x)/\mathrm{d}x_r)=2^{n-3},w_t(x_ie_f(x)/ex_r)=2^{n-2}\ (n=16(\text{偶数});r,i=n,n-1,\cdots,n-15,r\neq i) \quad (35)$$

故 $f(x)$是相关免疫函数[7]。

同样的计算证明，可知 $g(x)$是奇数元 $n=17$ 的重量为 $2^{n-1}+2^{n-2}$ 的相关免疫 H 布尔函数。

由定理 6、推论 2 及式(34)，可求得 $f(x)$的代数次数最低的零化子的最高次项中的一项为 $x_{n-15}x_{n-11}x_{n-10}x_{n-8}x_{n-7}x_{n-5}x_{n-4}x_{n-2}$，故 $AI(f(x))=8$，故知 $f(x)$是 $n=16$(偶数)元的最优代数免疫函数。求得 $g(x)$的代数次数最低的零化子的最高次项中的一项为 $x_{n-16}x_{n-11}x_{n-9}x_{n-8}x_{n-6}x_{n-5}x_{n-4}x_{n-2}$，故 $AI(g(x))=8$，故知 $g(x)$是 $n=17$(奇数)元的最优代数免疫函数。

从 $f(x)$和 $g(x)$的级联过程可知，对 S_1 和 S_2 的级联可以继续进行到变量 x_1。经归纳法证明，$(1+x_1)((1+x_2)(\cdots((1+x_{n-13})S_1+x_{n-13}S_2)+\cdots)+x_1((1+x_2)(\cdots((1+x_{n-13})S_2+x_{n-13}S_1)+\cdots)$ 级联函数是重量为 $2^{n-1}+2^{n-2}$ 的 n 元的代数免疫阶为 $AI(f)=8$ 的相关免疫 H 布尔函数。

由 r_1,r_2,h_1,h_2 和 S_1,S_2 的级联计算可知，在保证满足定理 1 和定理 7 的条件下，构造 12 元相关免疫 H 布尔函数 S_3 如下。

$$S_3=(1+x_{n-11})((1+x_{n-10})((1+x_{n-9})F_2+x_{n-9}F_3)+x_{n-10}((1+x_{n-9})F_3+x_{n-9}F_2))+x_{n-11}((1+x_{n-10})((1+x_{n-9})F_3+x_{n-9}F_2)+x_{n-10}((1+x_{n-9})F_2+x_{n-9}F_3)) \quad (36)$$

将 S_3, S_2, S_1 一起级联，可以得到代数免疫阶 $AI(f)$ 更高的奇数元和偶数元的最优代数免疫函数和 n 元代数免疫函数。限于篇幅，而且前述方法已很明显，不再继续构造。因而只证明到代数免疫阶 $AI(f)\geqslant 8$ 的结果。证毕。

定理 9 在 Hamming 重量 2^{n-2} 的布尔函数中，存在代数免疫阶 $AI(f)=8$ 的奇数元 $n=17$ 和偶数元 $n=16$ 的最优代数免疫相关免疫 H 布尔函数。

证明：由定理 8，设 $g(x)$ 为定理 8 中的代数免疫阶 $AI(f)=8$ 的 $n=17$ 元(奇数元)的最优代数免疫相关免疫 H 布尔函数。由于 $w_t(g(x))=2^{n-1}+2^{n-2}$，故对 $g_1(x)=1+g(x)$，有

$$w_t(g_1(x))=2^n-w_t(g(x))=2^{n-2} \tag{37}$$

又 $w_t(\mathrm{d}g(x)/\mathrm{d}x_i)=2^{n-1}$，$w_t(eg(x)/ex_i)=2^{n-1}$ $(i=1,2,\cdots,n)$，故

$$w_t(\mathrm{d}g_1(x)/\mathrm{d}x_i)=w_t(\mathrm{d}g(x)/\mathrm{d}x_i)=2^{n-1}$$

$$w_t(eg_1(x)/ex_i)=w_t(1)(wt(\mathrm{d}g(x)/\mathrm{d}x_i)-w_t(eg(x)/ex_i)=0$$

$$(i=1,2,\cdots,n) \tag{38}$$

故由式(37)、式(38)及定理 3 知，$g_1(x)$ 是重量 2^{n-2} 的 H 布尔函数，且 $g_1(x)=g_1(x)\mathrm{d}g_1(x)/\mathrm{d}x_i(i=1,2,\cdots,n)$，故

$$\begin{aligned}&w_t(x_i\mathrm{d}g_1(x)/\mathrm{d}x_k)\\&=w_t(x_i(1+g(x))\mathrm{d}(1+g(x))/\mathrm{d}x_k)\\&=w_t(x_i\mathrm{d}g(x)/\mathrm{d}x_k)-w_t(x_ig(x)\mathrm{d}g(x)/\mathrm{d}x_k)\\&=2^{n-2}-2^{n-3}=2^{n-3}\\&(i,k=1,2,\cdots,n,i\neq k)\end{aligned} \tag{39}$$

故 $g_1(x)$ 是相关免疫函数[7]。

由于 $g_1(x)=1+g(x)$，因此 $g(x)$ 的零化子是 $g_1(x)$ 的零化子。$g(x)$ 是 $n=17$(奇数)元最优代数免疫函数，故 $g_1(x)$ 也是 $n=17$(奇数)元最优代数免疫函数。

又设 $f(x)$ 是定理 8 中的代数免疫阶 $AI(f)=8$ 的 $n=16$(偶数)元的最优代数免疫相关免疫 H 布尔函数，又设 $f_1(x)=1+f(x)$。与前面 $g_1(x)$ 的证明相同，仅仅维数小 1。可知 $f_1(x)$ 是 $w_t(f_1(x))=2^{n-2}$ 的 $n=16$ 元的最优代数免疫相关免疫 H 布尔函数。

结束语 H 布尔函数中，还有更多其它重量的 H 布尔函数[11]。重量 $2^{n-1}+2^{n-2}$ 和 2^{n-2} 的相关免疫 H 布尔函数的最优代数免疫性的结果，可为其它重量相关免疫及弹性 H 布尔函数代数免疫性研究打下基础。

参 考 文 献

[1] 杜蛟，温巧燕，张勤，等. 5 元 1 阶弹性函数的代数免疫阶[J]. 通信学报，2011，32(4)：17-24

[2] Liu W M，Youssef . On the existence of (10，2，7 488) resilient functions[J]. IEEE Trans Information Theory，2009，55(1)：411-412

[3] Xiao Guo-zhen，Massey J L. A Spectral Characterization of Correlation-Immune Combining Functions[J]. IEEE Trans. on Inform，1988，34(3)：215-220

[4] 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

[5] 李世取，曾本胜，廉玉忠，等. 密码学中的逻辑函数[M]. 北京：北京中软电子出版社，2003

[6] 温巧燕，张勤，钮心忻，等. 现代密码学中的布尔函数研究综述[J]. 电信科学，2004，20(12)：43-46

[7] 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

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

[9] 何亮，王卓，李卫卫. 减小平衡 H 布尔函数相关度的算法和相关问题研究[J]. 通信学报，2010，31(2)：93-99

[10] Ding Y J，Wang Z，Ye J H. Initial-value problem of the Boolean function's primary function and its application in cryptographic system[J]. Kybernetes，2010，39(6)：900-906

[11] Delfs H，Knebl H. Introduction to Cryptography[M]. Springer-Verlag，2002

(上接第 121 页)

数据进行等维新息处理，利用马尔可夫链模型预测出结果的波动范围。本文构建的等维新息灰色马尔可夫模型具有如下优点：

(1)等维新息灰色预测模型既克服了传统灰色预测模型的数据来源固定不变的弊病，又利用了传统灰色预测模型对近期数据预测精度高的优点。

(2)通过建立状态转移概率矩阵可确定互联网上网人数位于不同区间的可能性，通过综合考虑区间预测中值与区间发生概率可更加准确地把握未来上网人数的发展趋势。

虽然该模型计算量较大，但最终取得了较好的结果，为互联网的网络建设和管理提供了决策依据，并为相关方案的制定奠定了基础。

参 考 文 献

[1] Dang Yue-chen，Xu Juan. Research on the Number of Internet Users Forecast Model Based on matlab[J]. Journal of Beijing Institute of Technology：Social Sciences Edition，2010，12(2)：47-49

[2] 陈晶晶，毛谦，刘国辉. 我国互联网用户数预测研究[J]. 光通信研究，2007(01)：1-3

[3] 丁洁. 基于灰色灾变原理的互联网用户人数预测模型[J]. 情报理论与实践，2005，28(5)：482-484

[4] 朱苗苗，牛国锋，乐德广. 基于灰色 Verhulst 的互联网上网人数动态预测模型[J]. 微型机与应用，2011，30(23)：91-93

[5] 连飞. 基于 GM(1，1)模型的我国互联网上网人数灰色预测[J]. 统计与咨询，2008(04)：28-29

[6] 张宗国. 马尔可夫链预测方法及其应用研究[D]. 南京：河海大学，2005，6：14-15

[7] 熊岗，陈章潮. 灰色预测模型的缺陷及改进方法[J]. 系统工程，1992，10(2)：42-44

[8] 邓聚龙. 灰预测与灰决策[M]. 武汉：华中理工大学出版社，2002

[9] 李东，苏小红，马双全. 基于新维灰色马尔科夫预测模型的股价预测算法[J]. 哈尔滨工业大学学报，2003，35(2)：244-248

[10] 赵晓梅，盖美. 基于等维新息灰色马尔可夫模型的大连城市用水量预测[J]. 水文，2011，31(1)：66-69