H 布尔函数的相关免疫性与重量的关系

黄景廉，王卓
（西北民族大学 计算机科学与信息工程学院，甘肃 兰州 730030）

摘 要：将布尔函数的导数和与导数一起便可直接明确刻画布尔函数的重量而定义的 *e*-导数一起作研究工具，深入到布尔函数取值的内部结构中去，讨论了在 H 布尔函数存在的一个大重量范围内，所有不同重量的 H 布尔函数的一阶、任意 *m* 阶相关免疫函数存在与否的问题。对存在 *m* 阶相关免疫性的 H 布尔函数，它的相关免疫阶数 *m* 与维数 *n* 的具体关系，以及 *m* 的最大值问题。给出了 *m* 阶相关免疫 H 布尔函数只存在于 2 种重量的 H 布尔函数中，其相关免疫阶数 *m* 的最大值为 *n*−2，以及其余重量的 H 布尔函数中不存在二阶以上（包括二阶）相关免疫函数等一系列结果。同时，也给出了一些判断布尔函数相关免疫性的方法。

关键词：H 布尔函数；*e*-导数；导数；扩散性；相关免疫阶数；重量；阶数最大值
中图分类号：TP309 **文献标识码**：B **文章编号**：1000-436X(2012)02-0110-09

Relationship between correlation immune and weight of H Boolean functions

HUANG Jing-lian, WANG Zhuo
(College of Computer Science and Information Engineering, Northwest University for Nationalities, Lanzhou 730030, China)

Abstract: The Boolean function derivative and *e*-derivative which together with the derivative so that the weight of Boolean functions can be directly clear characterized and defined as the tools for research and deep into the internal structure of Boolean function value, to discuss a large range in which the H-Boolean functions exist, the issue of whether all different weights of first-order and m-order H Boolean functions exist. For H Boolean functions with *m*-order correlation immunity, the relationship between its correlation immune order m and dimension *n*, and the maximum problem of *m*. Gives the *m*-order correlation immune H Boolean function exists only in the H Boolean function that with two kinds of weight. The maximum value of correlation immune *m* is *n*-2, and the rest of the weight of H Boolean function does not exist above the second-order (including the second-order) correlation immune fuction and a series of results.

Key words: H Boolean functions; *e*-derivative; derivative; propagation; correlation immune order; weight; maximum value of order

1 引言

在现代密码学中，杨义先教授提出的 H 布尔函数及对 H 布尔函数的研究[1~4]，为布尔函数密码学性质的研究开辟了一个重要的、新的研究方向和研究领域。由于密码系统抵抗各种攻击的综合能力的要求，要求设计的布尔函数要兼具扩散性、相关免疫性、代数免疫性等密码学性质。可知，直接讨论 H 布尔函数的相关免疫性要比单纯地、孤立地讨论布尔函数的相关免疫性更有意义，能更直接地对扩

收稿日期：2010-08-23；**修回日期**：2010-12-14
基金项目：中央高校基本科研业务费专项基金资助项目（ZYZ2011055）
Foundation Item: The Fundamental Research Funds for the Central Universities (ZYZ2011055)

散性、相关免疫性等直接进行综合性研究。H 布尔函数为各种密码学性质的综合研究提供了一个方向性工具，有重要的密码学价值。本文正是在这一方向上来讨论扩散性、重量和相关免疫性的关系问题。在 H 布尔函数存在的重量范围内，H 布尔函数的相关免疫性及其阶数与它的重量有何直接关系的问题，是一个可以直接从 H 布尔函数的重量即可便捷地、明确判定 H 布尔函数的相关免疫性及其阶数的重要问题，也是人们尚未顾及研究的问题。由于布尔函数 $f(x)$的导数只能反映 $f(x)$在 $\mathrm{d}f(x)/\mathrm{d}x_i=1$（这时相应有 $ef(x)/ex_i=0$）的取值情况，只有定义布尔函数 $f(x)$的 e-导数[5~7]，才能反映 $f(x)$在 $ef(x)/ex_i=1$（而这时相应有 $\mathrm{d}f(x)/\mathrm{d}x_i=0$）时的另一种取值情况。本文将导数和与导数一起才能完整刻画布尔函数的重量而定义的 e-导数相结合作为研究工具，讨论了在 $2^{n-2}\leqslant w(f(x))\leqslant 2^{n-1}+2^{n-2}$ 这一大的重量范围内，各种重量 H 布尔函数的相关免疫性及其阶数的存在性问题，以及 m ($m\geqslant 2$) 阶相关免疫函数的阶数 m 与函数的维数 n 有何关系的问题，得到一系列有用的明确结果。

2　预备性概念

布尔函数的导数是布尔代数、逻辑设计和密码学中早已有定义的概念[8,9]，但 e-导数是为刻画布尔函数的重量才定义的新概念。为后面讨论各种不同重量 H 布尔函数的相关免疫性及其阶数的需要和阅读方便，下面给出导数和 e-导数的定义以及它们与布尔函数、重量、扩散性、相关免疫性的一些最基本的简单关系。

定义 1　n 元布尔函数 $f(x)$对变元 $x_{i1},\cdots,x_{ir}$ 的 e-导数，记为 $ef(x)/e(x_{i1},\cdots,x_{ir})$，并定义为

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

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

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

由定义 1 和布尔函数的导数的定义，可直接得到下面的引理 1 和引理 2。

引理 1　有乘积关系 $\mathrm{d}f(x)/\mathrm{d}x_i e\, f(x)/ex_i=0$，($i=1,2,\cdots,n$)。

引理 2　对任意 n 元布尔函数 $f(x)$，有如下关系。

1) $f(x)=f(x)\partial f(x)/\partial(x_{i1},\cdots,x_{ir})+ef(x)/e(x_{i1},\cdots,x_{ir})$，($1\leqslant r\leqslant n,\ 1\leqslant i_1<i_2<\cdots<i_r\leqslant n$)。

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

3) $w(f(x))=w(f(x)\,\partial\, f(x)/\partial(x_{i1},\cdots,x_{ir}))+w(ef(x)/e(x_{i1},\cdots,x_{ir}))=2^{-1}w(\partial f(x)/\partial(x_{i1},\cdots,x_{ir}))+w(e\, f(x)/e(x_{i1},\cdots,x_{ir}))$，($1\leqslant r\leqslant n,\ 1\leqslant i_1<i_2<\cdots<i_r\leqslant n$)。

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

参考文献[4]关于扩散性的定义显然可由导数来描述，于是可得出关于 $f(x)$的扩散性的等价定义引理 3。

引理 3　布尔函数 $f(x)$满足 k ($1\leqslant k\leqslant n$)次扩散准则，当且仅当对一切 $x_{i1},\cdots,x_{ik}$，($1\leqslant k\leqslant n,\ 1\leqslant i_1<i_2\cdots<i_k\leqslant n$)，有

$$w(\partial f(x)/\partial(x_{i1},\cdots,x_{ik})=2^{n-1},\ (1\leqslant k\leqslant n,\ 1\leqslant i_1<i_2<\cdots<i_k\leqslant n)$$

特别地，$f(x)$满足一次扩散准则，当且仅当对一切 x_i，($i=1,2,\cdots,n$)，有

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

由引理 2 的 4)和引理 3，可以用导数和 e-导数来导出和参考文献[4]p19、p133、p22 关于平衡 H 布尔函数的定义等价的定义，即引理 4。

引理 4　$f(x)$是平衡 H 布尔函数，当且仅当对一切 x_i ($i=1,2,\cdots,n$)，有

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

下面的引理 5 是一些文献中已有的结果，这里引入是因为本文的讨论要用。本文也将给出用导数性质进行的证明。

引理 5　布尔函数 $f(x)$是 H 布尔函数的必要条件是 $2^{n-2}\leqslant w(f(x))\leqslant 2^{n-1}+2^{n-2}$。

证明　若 $f(x)$是 H 布尔函数，则由引理 3 知，必有 $w(\mathrm{d}f(x)/\mathrm{d}x_n)=2^{n-1}$，又由引理 2 的 4)知，必有 $w(f(x))\geqslant 2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_n)=2^{n-2}$。

对 $w(f(x))\leqslant 2^{n-1}+2^{n-2}$ 用反证法证明。

假设 $w(f(x))>2^{n-1}+2^{n-2}$，则有 $w(1+f(x))=2^n-w(f(x))<2^{n-2}$，故由引理 2，必有 $w(\mathrm{d}(1+f(x))/\mathrm{d}x_n)<2^{n-1}$。但由导数的性质知，有 $w(\mathrm{d}f(x)/\mathrm{d}x_n)=w(\mathrm{d}(1+f(x))/\mathrm{d}x_n)<2^{n-1}$，故由引理 3 知，这与 $f(x)$是 H 布尔函数矛盾，故必有 $w(f(x))\leqslant 2^{n-1}+2^{n-2}$。

故若 $f(x)$是 H 布尔函数，必有 $2^{n-2}\leqslant w(f(x))\leqslant 2^{n-1}+2^{n-2}$。

3 对 H 布尔函数的重量与相关免疫性及其阶数关系的讨论

下面对 $2^{n-2}\leqslant w(f(x))\leqslant 2^{n-1}+2^{n-2}$ 中所有 H 布尔函数的相关免疫性及其阶数进行讨论，同时给出一些有关的辅助性定理。

定理 1 对布尔函数 $f(x)$（$x\in \mathrm{GF}(2)^n$，$f(x)\neq c$，$c\in \mathrm{GF}(2)$），若

$$\partial f(x)/\partial(x_1,\cdots,x_n)=0 \tag{3}$$

则 $f(x)$必为一阶相关免疫函数。

证明 若 $f(x)$满足式(3)，则对一切 $i=1,2,\cdots,n$，显然必有

$$w(f(x)|x_i=0)=w(f(x)|x_i=1)=2^{-1}w(f(x)) \tag{4}$$

故知 $f(x)$为一阶相关免疫函数。

定理 1 及式(4)是参考文献[4]p47 中相关免疫的一个充要条件。式(3)是式(4)的一个充分条件，故式(3)只是 $f(x)$一阶相关免疫的充分条件，而不是必要条件。

例如：$f(x)=x_4+x_1x_4+x_2x_4+x_2x_5+x_3x_4+x_4x_5+x_1x_2x_4+x_1x_2x_5+x_1x_3x_4+x_1x_3x_5+x_1x_4x_5+x_2x_3x_4+x_2x_3x_5+x_3x_4x_5$

$f(x)$是一阶相关免疫函数，但不满足式(3)。

定理 2 若 n 元布尔函数 $f_1(x)$和 $f_2(x)$有 $w(f_1(x))=w(f_2(x))$，且

$$\partial f_1(x)/\partial(x_1,\cdots,x_n)=0,\partial f_2(x)/\partial(x_1,\cdots,x_n)=0 \tag{5}$$

则 $f_1(x)$和 $f_2(x)$的级联函数

$$f(x)=(1+x_0)f_1(x)+x_0f_2(x) \tag{6}$$

是 $n+1$ 元一阶相关免疫函数。

这里要注意的是，式(6)与一些参考文献[4]P163、参考文献[1]P16、P48 中定义的级联函数

$$f(x)=(1+x_{n+1})f_1(x)+x_{n+1}f_2(x) \tag{7}$$

不仅形式不同，而且有本质的差异，这一点是显然的。

证明 由于 $w(f_1(x))=w(f_2(x))$，则由式(6)知有

$$w(f(x)|x_0=0)=w(f_1(x))=2^{-1}w(f(x))=w(f_2(x))=w(f(x)|x_0=1) \tag{8}$$

由于式(5)，则由定理 1 知 $f_1(x)$和 $f_2(x)$均为 n 元一阶相关免疫函数。故对 $i=1,2,\cdots,n$，$a_i\in \mathrm{GF}(2)$，必有

$$w(f(x)|x_i=a_i)=w(f_1(x)|x_i=a_i)+w(f_2(x)|x_i=a_i)=2^{-1}w(f_1(x))+2^{-1}w(f_2(x))=2^{-1}w(f(x)) \tag{9}$$

结合式(8)、式(9)，便知 $f(x)$是 $n+1$ 元一阶相关免疫函数。证毕。

定理 1 和定理 2 说明了一阶相关免疫函数 $f(x)$取值的某种对称性。而由一阶相关免疫定义的充要条件式(4)来看，这种对称性是充分必要的性质。显然，定理 2 还可作进一步的多次级联的推理。限于篇幅，这里省略。

有了上面的准备，下面来讨论各种重量 H 布尔函数的相关免疫性。

下面对 $w(f(x))=2^{n-1}+2^{n-2}$ 的 m 阶($m\geqslant 1$)相关免疫性分成几个定理来证明。

定理 3 在 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数中，存在二阶相关免疫的 H 布尔函数。

证明 为推导公式明晰的需要，这里要从一阶相关免疫推起（因为由定理 1 和定理 2 知，一阶肯定存在）。设 $f(x)$是 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数，经简单推导，有

$$w(\mathrm{d}f(x)+x_i)/\mathrm{d}x_k)=w(\mathrm{d}f(x)/\mathrm{d}x_k+\mathrm{d}x_i/\mathrm{d}x_k)=w(\mathrm{d}f(x)/\mathrm{d}x_k)=2^{n-1},\ (i,k=1,2,\cdots,n;\ k\neq i) \tag{10}$$

$$w(ef(x)+x_i)/ex_k)=w(x_i)+w(ef(x)/ex_k)-w(x_i\,\mathrm{d}f(x)/\mathrm{d}x_k)-2w(x_i\,ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i) \tag{11}$$

于是由式(10)、式(11)、引理 4 和相关免疫的条件（$w(f(x)+x_i)=2^{n-1}$）要求知，$f(x)$一阶相关免疫，当且仅当

$$w(x_i\mathrm{d}f(x)/\mathrm{d}x_k)+2w(x_ief(x)/ex_k)=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)+w(ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i) \tag{12}$$

由于 $f(x)$是 H 布尔函数，且 $w(f(x))=2^{n-1}+2^{n-2}$，则由引理 2、引理 3 知，必有

$w(\mathrm{d}f(x)/\mathrm{d}x_k)=2^{n-1}$，$w(ef(x)/ex_k)=2^{n-1}$，($k=1,2,\cdots,n$)，故由引理 1 知，必有

$$w(\mathrm{d}f(x)/\mathrm{d}x_k+ef(x)/ex_k)=w(\mathrm{d}f(x)/\mathrm{d}x_k)+w(ef(x)/ex_k)=2^n,\ (i,k=1,2,\cdots,n;\ k\neq i) \tag{13}$$

反之，显然满足式(13)的 H 布尔函数，必有 $w(f(x))=2^{n-1}+2^{n-2}$，$w(ef(x)/ex_k)=2^{n-1}$ 。

又由于 $w(x_i)=2^{n-1}$, ($i,=1,2,\cdots,n$)，故由式(13)知，必有

$$w(x_i(\mathrm{d}f(x)/\mathrm{d}x_k+ef(x)/ex_k))=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k+ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i) \tag{14}$$

将式(14)展开，并由引理 1 知有

$$w(x_i(\mathrm{d}f(x)/\mathrm{d}x_k)+w(x_ief(x)/ex_k)=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{-1}w(ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i) \tag{15}$$

解式(12)、式(15)两式组成的联立方程组，则对一切 $i,k=1,2,\cdots,n$，$k\neq i$，有解

$w(x_i ef(x)/ex_k)=2^{-1}w(ef(x)/ex_k)$, $w(x_i \mathrm{d}f(x)/\mathrm{d}x_k)$
$=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)$，$(i,k=1,2,\cdots,n;\ k\neq i)$ (16)

于是可知，当 $f(x)$一阶相关免疫时，必有式(12)成立，而式(15)是必成立的。故必有式(16)两式均成立。反之，若式(16)成立时，显然将式(16)代入式(12)，式(12)必成立。故 $f(x)$一阶相关免疫，当且仅当式(16)成立。

由于式(15)必成立及式(16)是方程组唯一解，可知，式(16)中有一式成立，则另一式也必成立。于是取 $f_e(x)=ef(x)/ex_n$, 即 $f_1(x)$是由 $f(x)$中 $ef(x)/ex_n=1$ 且 $\mathrm{d}f(x)/\mathrm{d}x_n=0$ 的那些值的函数，即有 $w(f_e(x))=w(ef(x)/ex_n)=2^{n-1}$。而满足式(16)第一式的 $f_e(x)$显然是存在的。比如满足定理 1 的条件 $\partial f_e(x)/\partial(x_1,\cdots,x_n)=0$，或满足定理 2 的条件 $\partial f_e(x)/\partial(x_1,\cdots,x_n)=0$，或满足对定理 2 进行推广的条件 $\partial f_e(x)/\partial(x_{n-2}x_{n-1}x_n)=0$ 的 $f_e(x)$（由于 $w(f_e(x))=2^{n-1}$, $f_e(x))=ef(x)/ex_n$）是存在的。这时，$f_e(x)$显然都满足式(16)的第一式。故知相应的 $f(x)$也满足式(16)的第一式，故 $f(x)$也满足式(16)的第二式。事实上，取 $\partial f_e(x)/\partial(x_{n-2}x_{n-1}x_n)=0$ 的条件，便知 $f(x)$可由 $f_1(x)=x_{n-1}+x_n+x_{n-1}x_n$；$f_2(x)=1+x_{n-1}+x_{n-1}x_n$；$f_3(x)=1+x_{n-1}x_n$；$f_4(x)=1+x_n+x_{n-1}x_n$ 这 4 个 2 元布尔函数按保证 $f(x)$是 H 布尔函数，及满足 $\partial f_e(x)/\partial(x_{n-2}x_{n-1}x_n)=0$ 的某种次序逐步级联构成。故知由式(16)第一式，易于构造出一阶相关免疫函数，即一阶相关免疫的 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数是存在的。

于是取 $f(x)$是 $w(f(x))=2^{n-1}+2^{n-2}$ 的一阶相关免疫的 H 布尔函数，并对它的二阶相关免疫性进行讨论。经简单推导，有

$$w(\mathrm{d}(f(x)+x_i+x_j)/\mathrm{d}x_k)=w(\mathrm{d}f(x)/\mathrm{d}x_k)=2^{n-1},\quad (i,j,k=1,2,\cdots,n;\ k\neq i\neq j) \tag{17}$$

$$w(e(f(x)+x_i+x_j)/ex_k)=w(x_i+x_j)+w(ef(x)/ex_k)-w(x_i\mathrm{d}f(x)/dx_k)-2w(x_i ef(x)/ex_k)-w(x_j\mathrm{d}f(x)/\mathrm{d}x_k)-2w(x_j ef(x)/ex_k)+2w(x_ix_j\mathrm{d}f(x)/\mathrm{d}x_k)+4w(x_ix_j ef(x)/ex_k),\quad (i,j,k=1,2,\cdots,n;k\neq i\neq j) \tag{18}$$

由引理 4 和式(12)、式(13)、式(17)、式(18)及二阶相关免疫条件知，$f(x)$二阶相关免疫，当且仅当

$$w(x_ix_j\mathrm{d}f(x)/\mathrm{d}x_k)+2w(x_ix_j ef(x)/ex_k)=2^{-2}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{-1}w(ef(x)/ex_k),(i,j,k=1,2,\cdots,n;k\neq i\neq j) \tag{19}$$

由于式(13)必成立，又由于 $w(x_ix_j)=2^{n-2}$, $(i,j=1,2,\cdots,n;\ i\neq j)$，故必有

$$w(x_ix_j(\mathrm{d}f(x)/\mathrm{d}x_k+ef(x)/ex_k))=w(x_ix_j\mathrm{d}f(x)/\mathrm{d}x_k)+w(x_ix_j ef(x)/ex_k)=2^{-2}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{-2}w(ef(x)/ex_k),\quad (i,j,k=1,2,\cdots,n;k\neq i\neq j) \tag{20}$$

求解式(19)、式(20)两式组成的联立方程组，则对一切 $i,j,k=1,2,\cdots,n$，$k\neq i\neq j$，有解

$$w(x_ix_j ef(x)/ex_k)=2^{-2}w(ef(x)/ex_k),\ w(x_ix_j\mathrm{d}f(x)/\mathrm{d}x_k)=2^{-2}w(\mathrm{d}f(x)/\mathrm{d}x_k),(i,j,k=1,2,\cdots,n;k\neq i\neq j) \tag{21}$$

显然，通过和前面一阶相关免疫相同的讨论，可得结论：$f(x)$ 二阶相关免疫，当且仅当式(21)成立。

利用前面一阶相关免疫时得出的 $f_1(x)$、$f_2(x)$、$f_3(x)$、$f_4(x)$，便能轻易构造 $w(f(x))=2^{n-1}+2^{n-2}$ 的二阶相关免疫函数。为对任意 n 元能更清楚地证明存在性，先构造 2 个低元的二阶相关免疫函数，然后再逐步级联成任意 n 元的方法来构造。为此，先证明如下关系。

若 $f_{i1}(x)$和 $f_{i2}(x)$均为 $m(m\geqslant 1)$阶相关免疫 n 元 H 布尔函数，且 $w(f_{i1}(x)+f_{i2}(x))=2^{n-1}$，则 $f_{i1}(x)$ 和 $f_{i2}(x)$的级联函数：

$$f(x)=(1+x_0)f_{i1}(x)+x_0 f_{i2}(x) \tag{22}$$

仍至少是 m 阶相关免疫的 $n+1$ 元 H 布尔函数，这是由于，对 ωx $(1\leqslant w(\omega)\leqslant m)$，经推导，有 $w(f(x)+\omega x)=w((1+x_0)f_{i1}(x)+\omega x)+w(x_0 f_{i2}(x)+\omega x)-w(\omega x)$，故知 $f(x)$仍为 $m(m\geqslant 1)$阶 $n+1$ 元布尔函数。又

$$w(\mathrm{d}f(x)/\mathrm{d}x_k)=w(\mathrm{d}f_{i1}(x)/\mathrm{d}x_k)+w(\mathrm{d}f_{i2}(x)/\mathrm{d}x_k)=2^{(n+1)-1},\quad (i=1,2,\cdots,n)$$

$$w(\mathrm{d}f(x)/\mathrm{d}x_0)=2w(f_{i1}(x)+f_{i2}(x))=2^n$$

即 $f(x)$为 $n+1$ 元 H 布尔函数。

于是由一阶相关免疫时得到的 $f_1(x)$、$f_2(x)$、$f_3(x)$、$f_4(x)$，根据式(21)第一式的要求，按 $f_1(x)$、$f_2(x)$、$f_3(x)$、$f_4(x)$、$f_4(x)$、$f_3(x)$、$f_2(x)$、$f_1(x)$的次序构造得

$$f_t(x)=1+x_1+x_2+x_3+x_4+x_5+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_2x_5+x_3x_5+x_4x_5$$

又按 $f_3(x)$、$f_4(x)$、$f_1(x)$、$f_2(x)$、$f_2(x)$、$f_1(x)$、$f_4(x)$、$f_3(x)$的次序构造得 $f_r(x)=1+x_2+x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_2x_5+x_3x_5+x_4x_5$，其中，$f_t(x)$和 $f_r(x)$均为 $n=5$ 元二阶相关免疫 H 布尔函数。于是，将 $f_t(x)$和 $f_r(x)$按次序 $f_t(x)$、$f_r(x)$、$f_r(x)$、$f_t(x)$、$f_r(x)$、$f_t(x)$、$f_t(x)$、$f_r(x)$、…两两逐步级联，便可得到任意 n 元二阶相关免疫的 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数。

故定理 3 成立。证毕。

从定理 3 证明中的式(16)、式(21)的推导，可以看出，$w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数的三阶相关免疫的充要条件，也有

$w(x_ix_jx_k\mathrm{d}f(x)/\mathrm{d}x_r)=2^{-3}w(\mathrm{d}f(x)/\mathrm{d}x_r)$；$w(x_ix_jx_kef(x)/ex_r)=2^{-3}w(ef(x)/ex_r)$，$(i,j,k,r=1,2,\cdots,n$；$k\neq i\neq j\neq r)$ (23)

如果用归纳法来证明，显然可以得到任意 m ($m\geqslant 1$)阶相关免疫的充要条件。限于篇幅，不作详细推导，直接给出如下定理 4。

定理 4 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数 $f(x)$任意 m ($m\geqslant 1$)阶相关免疫的充要条件是，对一切 $S_1\neq S_2\neq\cdots\neq S_m\neq k$，$m\geqslant 1$，有

$$w(x_{S1}x_{S2}\cdots x_{Sm}\mathrm{d}f(x)/\mathrm{d}x_k)=2^{-m}w(\mathrm{d}f(x)/\mathrm{d}x_k),$$
$$w(x_{S1}x_{S2}\cdots x_{Sm}ef(x)/ex_k)=2^{-m}w(ef(x)/ex_k),$$
$$(k\neq S_i,i=1,2,\cdots,m;\ 1\leqslant S_i\leqslant n) \quad (24)$$

现在需要用 $w(f(x))=2^{n-1}$ 且 $ef(x)/ex_n=2^{n-1}$，$\mathrm{d}f(x)/\mathrm{d}x_n=0$ 的布尔函数中，存在任意 m ($m\geqslant 1$)阶相关免疫布尔函数及定理 4，来证明存在 $w(f(x))=2^{n-1}+2^{n-2}$ 的任意 m ($m\geqslant 1$)阶相关免疫 H 布尔函数。下面先给出定理 3、定理 4 的推论，然后再给出解决上述问题的定理 5。

推论 1 若 $f_t(x)$和 $f_r(x)$均为 m ($m\geqslant 1$)阶相关免疫 n 元 H 布尔函数，且 $w(f_t(x)+f_r(x))=2^{n-1}$，则 $f_t(x)$和 $f_r(x)$的级联函数：

$$f(x)=(1+x_0)f_t(x)+x_0f_r(x) \quad (25)$$

仍至少是 m 阶相关免疫的 $n+1$ 元 H 布尔函数。

推论 1 在定理 3 中式(22)已证明，这里不再重复证明。

推论 2 若 $f(x)$为 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数，则 $f(x)$为 m ($m\geqslant 1$)阶相关免疫函数的充分必要条件是式(24)的第二式（或第一式）

$$w(x_{S1}x_{S2}\cdots x_{Sm}ef(x)/ex_k)=2^{-m}w(ef(x)/ex_k),$$
$$(k\neq S_i,i=1,2,\cdots,m;\ 1\leqslant S_i\leqslant n)$$

成立。

证明 从定理 3 的推导便可知，$f(x)$为 m ($m\geqslant 1$)阶相关免疫函数的充分必要条件是

$$w(x_{S1}x_{S2}\cdots x_{Sm}\mathrm{d}f(x)/\mathrm{d}x_k)+2w(x_{S1}x_{S2}\cdots x_{Sm}ef(x)/ex_k)=2^{-m}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{-m}w(ef(x)/ex_k),$$
$$(k\neq S_i,i=1,2,\cdots,m;\ 1\leqslant S_i\leqslant n) \quad (26)$$

由于 $w(f(x))=2^{n-1}+2^{n-2}$，$w(\mathrm{d}f(x)/\mathrm{d}x_k)=2^{n-1}$，$w(ef(x)/ex_k)=2^{n-1}$，$(k=1,2,\cdots,n)$，则定理 3 有式(13)必成立，于是和定理 3 由式(13)推出式(14)、式(15)相仿。由于 $w(x_{S1}x_{S2}\cdots x_{Sm})=2^{n-m}$，$(1\leqslant S_i\leqslant n$，$i=1,2,\cdots,m)$，必有

$$w(x_{S1}x_{S2}\cdots x_{Sm}\mathrm{d}f(x)/\mathrm{d}x_k)+w(x_{S1}x_{S2}\cdots x_{Sm}ef(x)/ex_k)=2^{-m}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{-m}w(ef(x)/ex_k),$$
$$(k\neq S_i,i=1,2,\cdots,m;\ 1\leqslant S_i\leqslant n) \quad (27)$$

将式(26)、式(27)两式联立成方程组并解之，得唯一解式(24)，故 $f(x)$为 m ($m\geqslant 1$)阶相关免疫函数的充分必要条件是式(24)的两式均成立。由于式(24)是方程组式(26)、式(27)的唯一解，故推论 2 成立。

显然，特别提出推论 2，是为以后判断 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数 $f(x)$是否 m ($m\geqslant 1$)阶相关免疫时，只需对 $ef(x)/ex_n=f_S(x)$ 进行判断，这比同时判断式(24)的 2 个式子要省一半工作量。

定理 4 和推论 2 只是给出了判断 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数是不是 m ($m\geqslant 1$)阶相关免疫函数的充分必要条件，并没有给出它存在的结论。但推论 2 给出了判断它的存在性的简便方法。为此，下面给出定理 5。

定理 5 在 $w(f(x))=2^{n-1}$，且 $w(ef(x)/ex_n)=2^{n-1}$，$\mathrm{d}f(x)/\mathrm{d}x_n=0$ 的 n ($n\geqslant 3$)元布尔函数 $f(x)$中（即 $f(x)=ef(x)/ex_n$），存在任意 m ($m\geqslant 1$) 阶相关免疫函数，且相关免疫阶数最高为 $m=n-2$ 阶，即

$$\max m_i=m=n-2$$

证明 由定理条件 $w(f(x))=w(ef(x)/ex_n)=2^{n-1}$，$f(x)=ef(x)/ex_n$，则当 $n\geqslant 3$ 时，取 $f(x)$满足

$$\partial f(x)/\partial(x_{n-2}x_{n-1}x_n)=0 \quad (28)$$

显然，即相应有

$$ef(x)/e(x_{n-2}x_{n-1}x_n)=2^{n-1} \quad (29)$$

则由定理 1、定理 2 及推论 1 知，$f(x)$必为一阶相关免疫函数。而且还可知，$f(x)$这时必定是由 $f_{21}(x)=x_{n-1}$ 和 $f_{22}(x)=1+x_{n-1}$ 按式(25)让 x_0 依次取为 $x_{n-2},x_{n-3},\cdots,x_2,x_1$ 逐步级联得到的函数。而且由式(28)、式(29)知，$f(x)$必须在 $n\geqslant 3$ 时，才至少是一阶相关免疫的。有以上结果后，下面便可用归纳法来推导 $f(x)$的表示式及相应的相关免疫性质。

当 $n=3$，即 $x=x_{n-2}x_{n-1}x_n$ 时，利用式(25)，取 $x_0=x_{n-2}$，对 $f_{21}(x_{n-1}x_n)=x_{n-1}$ 和 $f_{22}(x_{n-1}x_n)=1+x_{n-1}$ 作级联，得

$$f_{31}(x)=(1+x_{n-2})f_{21}(x)+x_{n-2}f_{22}(x)=(1+x_{n-2})x_{n-1}+x_{n-2}(1+x_{n-1})=x_{n-2}+x_{n-1} \quad (30)$$

和

$$f_{32}(x)=(1+x_{n-2})f_{22}(x)+x_{n-2}f_{21}(x)=(1+x_{n-2})(1+x_{n-1})+x_{n-2}x_{n-1}=1+x_{n-2}+x_{n-1} \quad (31)$$

式(30)、式(31)中，$f_{21}(x)$和 $f_{22}(x)$是二元函数。显然，$f_{31}(x)$和 $f_{32}(x)$ 仍然是仿射函数[3,6]（线性函数）。

根据相关免疫的定义[3]：$f(x)$为 m 阶相关免疫，

当且仅当对任意的 $1\leqslant i_1\leqslant i_2\leqslant\cdots\leqslant i_r\leqslant n$ 和满足 $1\leqslant w(\omega)\leqslant m$ 的 $\omega=(\omega_1,\cdots,\omega_n)\in GF(2)^n$，

$$w(f(x)+\sum_{i=1}^{n}\omega_i x_i))=w(f(x)+\omega x)=2^{n-1} \tag{32}$$

显然可知，三元函数（即 $n=3$）$f_{31}(x)$和 $f_{32}(x)$ 均为一阶相关免疫线性函数，但一定不是二阶相关免疫函数。

同样，取 $n=4$，即 $x=x_{n-3}\,x_{n-2}\,x_{n-1}\,x_n$ 时，有

$$f_{41}(x)=(1+x_{n-3})\,f_{31}(x)+x_{n-3}f_{32}(x)=x_{n-3}+x_{n-2}+x_{n-1} \tag{33}$$

$$f_{42}(x)=(1+x_{n-3})\,f_{32}(x)+x_{n-3}f_{31}(x)=1+x_{n-3}+x_{n-2}+x_{n-1} \tag{34}$$

其中，$f_{31}(x)$和 $f_{32}(x)$是三元布尔函数。于是，显然由相关免疫的定义式(32)可知，$f_{41}(x)$和 $f_{42}(x)$ 均为二阶相关免疫线性函数，但一定不是三阶相关免疫函数。

现在用归纳法，假设 $n=k$ 时，依 $x_0=x_{n-4},\,x_{n-5},\cdots,x_k$ 的顺序，按式(25)的级联方式逐步级联，得到的 $n=k$ 元布尔函数为

$$f_{k1}(x)=x_{n-k+1}+\cdots+x_{n-3}+x_{n-2}+x_{n-1} \tag{35}$$

$$f_{k2}(x)=1+x_{n-k+1}+\cdots+x_{n-3}+x_{n-2}+x_{n-1} \tag{36}$$

且显然 $f_{k1}(x)$和 $f_{k2}(x)$均为 $n-2=k-2$ 阶相关免疫函数。

则当 $n=k+1$ 时，按式(25)的级联方式，对 $f_{k1}(x)$和 $f_{k2}(x)$ 进行级联，得

$$f_{(k+1),1}(x)=(1+x_{n-k})\,f_{k1}(x)+x_{n-k}f_{k2}(x)$$
$$=x_{n-k}+x_{n-k-1}+\cdots+x_{n-3}+x_{n-2}+x_{n-1} \tag{37}$$

$$f_{(k+1),2}(x)=(1+x_{n-k})\,f_{k2}(x)+x_{n-k}f_{k1}(x)$$
$$=1+x_{n-k}+x_{n-k-1}+\cdots+x_{n-3}+x_{n-2}+x_{n-1} \tag{38}$$

得到的仍是 $k+1$ 元线性函数（仿射函数），且显然 $f_{(k+1),1}(x)$和 $f_{(k+1),2}(x)$是 $n-2=(k+1)-2=k-1$ 阶相关免疫函数。

故对于 n 元的，$w(f(x))=w(ef(x)/ex_n)=2^{n-1}$ 的布尔函数 $f(x)$中，存在 $m=n-2$ 阶相关免疫函数。

除由上面 $f_{21}(x)$和 $f_{22}(x)$逐步级联构成的 $w(f(x))=w(ef(x)/ex_n)=2^{n-1}$ 的函数 $f(x)$外，尚可由 $f'_{21}(x)=0$ 和 $f'_{22}(x)=1$ 构成的级联函数 $f'(x)$，由级联式(25)可知，$f'(x)$一定少含变量 x_{n-2}，x_{n-1}，x_n 3 个，由于上面的函数是按二阶相关免疫来构造的，还必须满足 $w(f(x))=w(ef(x)/ex_n)=2^{n-1}$，所以显然再不可能构造出其他结构的二阶相关免疫函数了。故相关免疫阶数一定小于 $m=n-2$。限于篇幅，不详证。故知，相关免疫阶数最高为 $m=n-2$。

由推论 2 和定理 4，显然可得到下面的定理 6 。

定理 6　在 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数中，存在任意 m $(1\leqslant m\leqslant n-2)$ 阶相关免疫 H 布尔函数。

证明　设 $f(x)$是 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数，则显然 $f(x)$可由 $f_1(x)=x_{n-1}+x_n+x_{n-1}x_n$；$f_2(x)=1+x_{n-1}+x_{n-1}x_n$；$f_3(x)=1+x_{n-1}x_n$；$f_4(x)=1+x_n+x_{n-1}x_n$ 这 4 个二元布尔函数逐步级联构成。这在定理 3 中已经看到过。由引理 2 的 2)，有

$$f(x)=f(x)\mathrm{d}f(x)/\mathrm{d}x_n+ef(x)/ex_n=f_{\mathrm{d}}(x)+f_e(x) \tag{39}$$

其中，$f_{\mathrm{d}}(x)=f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n$；$f_e(x)=ef(x)/ex_n$，且 $w(f_{\mathrm{d}}(x))=2^{n-2}$，$w(f_e(x))=w(ef(x)/ex_n)=2^{n-1}$。显然，使 $f_e(x)=ef(x)/ex_n$ （$w(f_e(x))=w(ef(x)/ex_n)=2^{n-1}$）满足定理 5 的式(28)、式(29)的 $f(x)$是存在的，并且是易于由定理 3 中的 $f_1(x)$、$f_2(x)$、$f_3(x)$、$f_4(x)$按式(25)级联构造的。故由定理 4 知，可以构造 $f_e(x)$是任意 m $(1\leqslant m\leqslant n-2)$ 阶相关免疫函数。即有

$$w(f_e(x)+\omega x)=w(f_e(x))+w(\omega x)-2w(\omega x\,f_e(x))=2^{n-1} \tag{40}$$

其中，$1\leqslant w(\omega)\leqslant n-2=m$，$\omega\in GF(2)^n$。故知有

$$w(\omega x\,f_e(x))=w((x_{S1}+x_{S2}+\cdots+x_{S\mathrm{m}})\,ef_e(x)/ex_n)$$
$$=2^{-1}w(f_e(x))=2^{-1}w(ef(x)/ex_n)$$

于是，必有

$$w(x_{S_i}f_e(x))=2^{-1}w(ef(x)/ex_n),\quad (S_i=1,2,\cdots,n) \tag{41}$$

又有 $w((x_{S_i}+x_{S_j})ef(x)/ex_n)=w(x_{S_i}\,ef(x)/ex_n)+w(x_{S_j}\,ef(x)/ex_n)-2w(x_{S_i}x_{S_j}ef(x)/ex_n)=2^{-1}w(ef(x)/ex_n)$，故由式(41)知，必有

$$w(x_{S_i}x_{S_j}\,ef(x)/ex_n)=2^{-2}w(ef(x)/ex_n),$$
$$(S_i,S_j=1,2,\cdots,n;\quad S_i\neq S_j) \tag{42}$$

继续这一推导，且由于又有

$$w((x_{S1}+x_{S2}+\cdots+x_{Sm})\;ef(x)/ex_n)=\sum_{S_i=1}^{n}w(x_{Si}ef(x)/ex_n)+$$
$$(-1)^1 2^1\sum_{1\leqslant S_i<S_j\leqslant n}w(x_{Si}x_{Sj}ef(x)/ex_n)+(-1)^2 2^2\sum_{1\leqslant S_i<S_j<S_k\leqslant n}$$
$$w(x_{Si}\;x_{Sj}\;x_{Sk}\;ef(x)/ex_n)+\cdots+(-1)^{m-2}\,2^{m-2}$$
$$\sum_{1\leqslant S_1<S_2<\cdots<S_{m-1}\leqslant n}w(x_{S1}\cdots x_{Sm-1}ef(x)/ex_n)+(-1)^{m-1}\,2^{m-1}$$
$$w(x_{S1}x_{S2}x_{Sm}ef(x)/ex_n)=2^{-1}w(ef(x)/ex_n) \tag{43}$$

故由式(43)知，当 $f_e(x)=ef(x)/ex_n$ 为 m $(1\leqslant m\leqslant n-2)$ 阶相关免疫函数时，必有

$$w(x_{S1}x_{S2}\cdots\;x_{Sm}ef(x)/ex_n)=2^{-m}w(ef(x)/ex_n) \tag{44}$$

其中，$1\leqslant S_1<S_2<\cdots<S_m\leqslant n$。

由于 $f_e(x)=ef(x)/ex_n$ 是满足定理 5 的式(28)、式(29)的要求，按定理 5 的方式构造的，故 $f_e(x)$必如定理 5 中式(37)、式(38)的形式的如下函数：

$$f_e(x)=(1+x_1)(x_2+x_3+\cdots+x_{n-2}+x_{n-1})+ x_1(1+x_2+x_3+\cdots+x_{n-2}+x_{n-1}) \quad (45)$$

故显然有

$ef_e(x)/ex_k=0$，$(k=1,2,\cdots,n-1)$；

$$ef_e(x)/ex_n)=f_e(x)=ef(x)/ex_n \quad (46)$$

故由式(44)、式(46)，知，必有

$$w(x_{S1}x_{S2}\cdots x_{S\,m}\,ef(x)/ex_k)=2^{-m}w(ef(x)/ex_k),\ (1\leqslant S_1<S_2<\cdots<S_m\leqslant n,\ k\neq S_i,\ (i=1,2,\cdots,n)) \quad (47)$$

于是由式(47)，$f(x)$的构成及推论 2 知，$f(x)$是 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数中的任意 m $(1\leqslant m\leqslant n-2)$阶相关免疫函数，证毕。

定理 7 在 $w(f(x))=2^{n-2}$ 的 H 布尔函数中，存在任意 m $(1\leqslant m\leqslant n-2)$ 阶相关免疫 H 布尔函数。

证明 设 $g(x)$为 $w(g(x))=2^{n-1}+2^{n-2}$ 的 m $(1\leqslant m\leqslant n-2)$阶相关免疫的 H 布尔函数。则由相关免疫的定义知，对 $\omega x(1\leqslant w(\omega)\leqslant m,\ 1\leqslant m\leqslant n-2)$，有 $w(g(x)+\omega x)=2^{n-1}$。取 $f(x)=1+g(x)$，有

$$w(f(x))=w(1+g(x))=2^n-(2^{n-1}+2^{n-2})=2^{n-2} \quad (48)$$

$$w(f(x)+\omega x)=w(1+g(x)+\omega x)=2^n-w(g(x)+\omega x)=2^{n-1} \quad (49)$$

$$w(\mathrm{d}f(x)/\mathrm{d}x_i)=w(\mathrm{d}(1+g(x))/\mathrm{d}x_i)=w(\mathrm{d}g(x)/\mathrm{d}x_i)=2^{n-1},\ (i=1,2,\cdots,n) \quad (50)$$

故由式(48)、式(49)、式(50)知，$f(x)$是 $w(f(x))=2^{n-2}$ 的任意 m $(1\leqslant m\leqslant n-2)$ 阶相关免疫的 H 布尔函数。证毕。

现在来讨论 $2^{n-2}<w(f(x))<2^{n-1}+2^{n-2}$ 中 H 布尔函数的相关免疫性。

定理 8 在 $w(f(x))=w(ef(x)/ex_n)<2^{n-1}$（即 $f(x)=ef(x)/ex_n$, $\mathrm{d}f(x)/\mathrm{d}x_n=0$）的布尔函数中，不存在二阶相关免疫函数。

证明 由于定理条件有 $f(x)=ef(x)/ex_n$，可知 $f(x)$必由 $f_{10}(x_{n-1}\,x_n)=x_{n-1}$, $f_{20}(x_{n-1}\,x_n)=1+x_{n-1}$, $f_{30}(x_{n-1}\,x_n)=0$, $f_{40}(x_{n-1}\,x_n)=1$ 按式(6)、式(25)，即定理 5 中的级联方式逐步级联构成。由定理 1、定理 2 及其推理可知，若 $f_{10}(x_{n-1}\,x_n)$ 与 $f_{20}(x_{n-1}\,x_n)$ 成对出现，$f_{30}(x_{n-1}\,x_n)$和 $f_{40}(x_{n-1}\,x_n)$ 成对出现，其余均取 0 级联时，$f(x)$必为一阶相关免疫函数。由于 $w(f(x))=w(ef(x)/ex_n)<2^{n-1}$，因而级联时要有较多的 0 值二元函数参与级联。于是 $f(x)$必为如下形式：

$$f(x)=x_{n-r}+f'(x) \quad (51)$$

其中，x_{n-r}是 x_i $(i=1,2,\cdots,n-1)$ 中的某一个，$f'(x)$中既含有 x_i $(i=1,2,\cdots,n-1)$ 中除 x_{n-r} 外的其余某些一次函数项，也含有不包括 x_n 的一些二次及二次以上的函数项（其实，一定含有 x_{n-1} 这一项，只是为了一般性的考虑，以 x_{n-r} 来进行标记）。以上所述的结果，只需做一些维数 n 较小的级联即可明显得出，然后通过归纳法即可轻易证明。由于结果很明显，限于篇幅，不再详证。由于 $f(x)$一阶相关免疫，故由相关免疫的定义及式(51)知，必有

$$w(f'(x))=w(f(x)+x_{n-r})=w(f(x))+w(x_{n-r})-2w(x_{n-r}f(x))=2^{n-1} \quad (52)$$

$$\therefore w(f(x))=2w(x_{n-r}f(x))<2^{n-1} \quad 及 \quad w(f'(x))=2^{n-1} \quad (53)$$

现在来讨论 $f(x)$是否二阶相关免疫。由式(51)，并经简单的重量公式推导，有

$$\begin{aligned}&w(f(x)+x_{n-r}+x_i)=w(f'(x)+x_i)\\&=w((f(x)+x_i)+(x_{n-r}+x_i)+x_i)\\&=w((f(x)+x_i)+w(x_{n-r}+x_i)-2w(x_{n-r}f(x))+\\&4w(x_i x_{n-1}f(x))-w(x_i)\\&=w((f(x)+x_i)-2w(x_{n-r}f(x))+\\&4w(x_i x_{n-1})-4w(x_i x_{n-r}f'(x))\end{aligned} \quad (54)$$

由式(53)知，$w(f'(x))=2^{n-1}$，故 $w(x_i x_{n-r}f'(x))\leqslant 2^{n-2}$，又显然 $0<2w(x_{n-r}f(x))<2^{n-1}$，故代入式(54)知，式(54)必不等于 2^{n-1}，故由二阶相关免疫的定义知，$f(x)$一定不是二阶相关免疫函数。

推论 3 若 $f(x)=ef(x)/ex_n$（即 $\mathrm{d}f(x)/\mathrm{d}x_n=0$）且 $w(f(x))=w(ef(x)/ex_n)<2^{n-2}$，则 $f(x)$中存在一阶相关免疫函数，但 $f(x)$一定不是二阶相关免疫函数。

由式(2)，对 $f(x)$，若记 $f_{10}(x)=f(x)\mathrm{d}f(x)/\mathrm{d}x_n$, $f_{20}(x)=ef(x)/ex_n$, 则

$$f(x)=f(x)\mathrm{d}f(x)/\mathrm{d}x_n+ef(x)/ex_n=f_{10}(x)+f_{20}(x) \quad (55)$$

由式(55)对 $f(x)$分解后，下面来证明重要的定理 9。

定理 9 将 H 布尔函数 $f(x)$分解成式(55)的 $f_{10}(x)=f(x)\mathrm{d}f(x)/\mathrm{d}x_n$ 和 $f_{20}(x)=ef(x)/ex_n$，则 $f(x)$一阶相关免疫，则 $f_{10}(x)$和 $f_{20}(x)$ 均必为一阶相关免疫函数；$f(x)$二阶相关免疫，则 $f_{10}(x)$和 $f_{20}(x)$均必为二阶相关免疫函数。

证明 同式(10)、式(11)、式(12)的推导相同，也有结果：$f(x)$一阶相关免疫，当且仅当

$$w(x_i\,\mathrm{d}f(x)/\mathrm{d}x_k)+2w(x_i\,ef(x)/ex_k)=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)+w(ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i) \quad (56)$$

显然，若 H 布尔函数 $f(x)$满足

$$w(x_i\,\mathrm{d}f(x)/\mathrm{d}x_k)=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k),\ w(x_i\ ef(x)/ex_k)$$
$$=2^{-1}w(ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i)\quad(57)$$

时，$f(x)$必满足式(56)，则$f(x)$必为一阶相关免疫函数。

反之，当$f(x)$为一阶相关免疫的 H 布尔函数，且 $w(ef(x)/ex_k)<2^{n-1}$时，用反证法，假设式(57)不成立，不妨设 $w(x_i\,\mathrm{d}f(x)/\mathrm{d}x_k)=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{n-r}$, 则由于$f(x)$为 H 布尔函数，有 $w(\mathrm{d}f(x)/\mathrm{d}x_k)=2^{n-1}$，故必有 $w(x_i\ ef(x)/ex_k)=2^{-1}w(ef(x)/ex_k)-2\times2^{n-r}$（这一结果对 n=4 时是显然的。对任意的 n 时，用归纳法是易于证明的。限于篇幅，不再详证）。将这一结果代入式(56)左端，有

$$w(x_i\,\mathrm{d}f(x)/\mathrm{d}x_k)+2w(x_i\ ef(x)/ex_k)=2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)+$$
$$2^{n-r}+2(2^{-1}w(ef(x)/ex_k)-2\times2^{n-r})=2^{-1}(\mathrm{d}f(x)/\mathrm{d}x_k)+$$
$$w(ef(x)/ex_k)-(2^2-2)2^{n-r}<2^{-1}w(\mathrm{d}f(x)/\mathrm{d}x_k)+$$
$$w(ef(x)/ex_k),\ (i,k=1,2,\cdots,n;\ k\neq i)\quad(58)$$

即式(56)不成立，$f(x)$不是一阶相关免疫 H 布尔函数，与$f(x)$是一阶相关免疫 H 布尔函数矛盾，故必有式(57)成立。

由于$f(x)$一阶相关免疫，必有 $w(x_n f(x))=2^{-1}w(f(x))$，又由式(2)，必有

$$w(x_n f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n)+w(x_n\ ef(x)/ex_n)$$
$$=2^{-1}w(f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n)+2^{-1}w(ef(x)/ex_n)\quad(59)$$

同式(57)必成立的证明相同，也必有

$$w(x_n f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n)=2^{-1}w(f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n),$$
$$w(x_n\ ef(x)/ex_n)=2^{-1}w(ef(x)/ex_n)\quad(60)$$

对式(57)，显然也有：$f(x)$一阶相关免疫，则必有

$$w(x_i f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n)=2^{-1}w(f(x)\,\mathrm{d}f(x)/\mathrm{d}x_n),$$
$$w(x_i\ ef(x)/ex_n)=2^{-1}w(ef(x)/ex_n)$$
$$(i=1,2,\cdots,n-1)\quad(61)$$

故由式(60)、式(61)知，$f(x)$一阶相关免疫，必有$f_{10}(x)$和$f_{20}(x)$均为一阶相关免疫函数。

在 $2^{n-2}<w(f(x))<2^{n-1}+2^{n-2}$ 范围中，也普遍存在一阶相关免疫的 H 布尔函数，而且由定理 1、定理 2 及其级联构造方法(6)知，一阶相关免疫的 H 布尔函数不仅存在，而且是易于构造的。于是，现在来讨论一阶相关免疫的 H 布尔函数的二阶相关免疫性。有了前面对一阶相关免疫性的必要条件的讨论，对二阶相关免疫性的讨论，由于与一阶相关免疫相仿，和定理 3 已有的对 $w(f(x))=2^{n-1}+2^{n-2}$ 的 H 布尔函数的讨论相同，已很显然。限于篇幅，这里只做简略的讨论。和定理 3 中式(19)的讨论相同，对任意的一阶相关免疫 H 布尔函数$f(x)$，根据参考文献[4]的 p19、p133 和参考文献[1]的 p39、p40、p50 的定义：

$$w(f(x)+x_i+x_j)=w(f(x))+w(x_i+x_j)-2w(x_i f(x))-$$
$$2w(x_j f(x))+4w(x_i x_j f(x))=2^{n-1}$$
$$(i,j=1,2,\cdots,n;\quad j\neq i)\quad(62)$$

同定理 3 的推导相同，也有：$f(x)$ 二阶相关免疫，当且仅当

$$w(x_i x_j\,\mathrm{d}f(x)/\mathrm{d}x_k)+2w(x_i x_j\ ef(x)/ex_k)$$
$$=2^{-2}w(\mathrm{d}f(x)/\mathrm{d}x_k)+2^{-1}w(ef(x)/ex_k)$$
$$(i,j,k=1,2,\cdots,n;\quad k\neq j\neq i)\quad(63)$$

和式(57)的讨论相同，$f(x)$ 二阶相关免疫，当且仅当

$$w(x_i x_j\,\mathrm{d}f(x)/\mathrm{d}x_k)=2^{-2}w(\mathrm{d}f(x)/\mathrm{d}x_k),$$
$$w(x_i x_j\ ef(x)/ex_k)=2^{-2}w(ef(x)/ex_k)$$
$$(i,j,k=1,2,\cdots,n;\quad k\neq j\neq i)\quad(64)$$

和式(60)、式(61)的讨论相同，$f(x)$ 二阶相关免疫，也必有

$$w(x_i x_j f(x)\mathrm{d}f(x)/\mathrm{d}x_n)=2^{-2}w(f(x)\mathrm{d}f(x)/\mathrm{d}x_n),$$
$$w(x_i x_j\ ef(x)/ex_n)=2^{-2}w(ef(x)/ex_n)$$
$$(i,j=1,2,\cdots,n;\quad j\neq i)\quad(65)$$

即 $f(x)$ 二阶相关免疫，则$f_{10}(x)$和$f_{20}(x)$也必为二阶相关免疫函数。证毕。

由定理 8 及推论 3 和定理 9，显然可直接得到定理 10。

定理 10　在 $2^{n-2}<w(f(x))<2^{n-1}+2^{n-2}$ 中的 H 布尔函数中，不存在二阶相关免疫的 H 布尔函数。

显然，这时有 $w(f_{20}(x))=w(ef(x)/ex_n)<2^{n-1}$，$f_{20}(x)$不是二阶相关免疫的，则再由定理 9 即得出结论。但由于结论很重要，故作为定理给出。

4　结束语

H 布尔函数存在于一个很大的重量范围内，数量庞大[10]。H 布尔函数的相关免疫性及其阶数与重量有无联系？有何联系？m 阶相关免疫的 H 布尔函数的相关免疫阶数 m 与它的维数 n 有无关系？有何关系？本文对这些问题进行解决，给出了具体的结果，即只有在 $w(f(x))=2^{n-1}+2^{n-2}$ 和 $w(f(x))=2^{n-2}$ 的 H 布尔函数中，存在任意 $m(m\geqslant1)$ 阶相关免疫的 H 布尔函数，m 和维数 n 的关系为 $\max m_i=n-2$。而在 $2^{n-2}<w(f(x))<2^{n-1}+2^{n-2}$ 这样一个大范围内的各种重

量的 H 布尔函数中，只存在一阶相关免疫的 H 布尔函数，但不存在二阶相关免疫的 H 布尔函数。这些结果使 H 布尔函数的相关免疫性和重量明确联系起来，能够按重量进行分类，这对构造具有良好密码学性质的布尔函数有实际意义，由此也可知，H 布尔函数在密码学研究中有重要作用。

参考文献：

[1] 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.
LI S Q, ZENG B S, LIAN Y Z, *et al*. Logic Function in Cryptography[M]. Beijing: Beijing Soft Electronic Publishing House, 2003.

[2] 杨义先. *N* 元 H 布尔函数[J]. 北京邮电大学学报,1988,11(3):1-9.
YANG Y X. On the H-Boolean functions[J]. Journal of Beijing University of Posts and Telecommunications, 1988,11(3):1-9.

[3] 杨义先,邢育森. N 元 H 布尔函数(Ⅱ)[J].电子科学学刊,1997, 19(2): 214-216.
YANG Y X,XING Y S. On the H Boolean function(Ⅱ)[J]. Journal of Electronics,1997,19(2): 214-216.

[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.
WEN Q Y, NIU X X, YANG Y X. Boolean Function in Modern Cryptoloy[M]. Beijing: Science Publishing House, 2000.

[5] LI W W, WANG Z. The *e*-derivative of boolean functions and its application in the fault detection and cryptographic system[A]. The 5th IIGSS Workshop, Kybernetes[C]. 2007. 245-249.

[6] 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.
HE L, WANG Z, LI W W.　Algorithm of reducing the balanced H-Boolean function correlation_measure and research on correlation issue[J]. Journal on Communications, 2010, 31(2): 93-99.

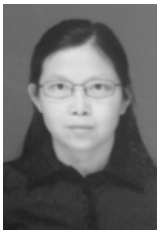
[7] DING Y J, WANG Z, YE J H. Initial-value problem of the Boolean function's primary function and its application in cryptographic system[J]. Kybernetes, 2010, 39(6): 900-906.

[8] XIAO G Z, MASSEY J L. A spectral characterization of correlation-immune combining functions[A]. IEEE Trans on Inform[C]. 1988.

[9] 温巧燕, 张劼, 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.
WEN Q Y, ZHANG J, NIU X X, *et al*. Review of Boolean functions of modern cryptography[J]. Telecommunication Science, 2004, 20(12): 43-46.

[10] DELFS H, KNEBL H. Introduction to Cryptography[M]. Springer-Verlag, 2002.

作者简介：



黄景廉（1968-），女，四川南充人，西北民族大学教授，主要研究方向为计算机网络通信与信息安全。

王卓（1944-），男，贵州贵阳人，西北民族大学教授、硕士生导师，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。