第 19 卷 第 6 期 电 子 科 学 学 刊 Vol.19 No.6
1997 年 11 月 JOURNAL OF ELECTRONICS Nov. 1997

# $m$ 阶相关免疫函数的计数问题 [1]

温巧燕 肖国镇

(西安电子科技大学信息保密所 西安 710071)

**摘 要** 主要讨论 $m$ 阶相关免疫函数的构造和计数问题，并给出了 $m$ 阶相关免疫函数个数的一个新的下界和一些特殊情况下的精确值.

**关键词** 相关免疫，流密码，正交矩阵，布尔函数

**中图号** TN918.1

## 1 引 言

在文献 [1] 中我们首次讨论了 $m$ 阶相关免疫函数的构造和计数问题，并给出了 $m$ 阶相关免疫函数个数的下界公式:

$$N^{(m)}(n) \geq 2 + 2^{2^{n-m-1}} + 2\sum_{k=2}^{r}(2^k!)^{2^{n-mk-1}}, \qquad r = \left[\frac{n-1}{m}\right]$$

$N^{(m)}(n)$ 表示 $n$ 元 $m$ 阶相关免疫函数的个数，则用 $N^{(1)}(n)$ 表示 1 阶相关免疫函数的个数。

本文通过分析 $m$ 阶相关免疫函数的结构特征，揭示了 $N^{(m)}(n)$ 与 $N^{(1)}(n)$ 的本质区别，给出了几种特殊情况下 $N^{(m)}(n)$ 的精确值，并将 $N^{(m)}(n)$ 的下界改进为

$$N^{(m)}(n) \geq 2 + 2^{2^{n-m-1}} + 2\sum_{k=2}^{r}(2^k!)^{2^{n-mk-1}} + \sum_{k=3}^{r}\sum_{l\in I_k}(C_{2^k}^{t})^{2^{n-mk-1}},$$

这里 $I_k = \{t | t$为奇数,且$3 \leq t \leq 2^k - 3\}$ .

## 2 几种特殊情况下的精确计数

用 $N^{(m)}(w,n)$ 表示重量为 $w$ 的 $n$ 元 $m$ 阶相关免疫函数的个数，则

$$N^{(m)}(n) = \sum_{k=0}^{2^{n-m}} N^{(m)}(2^m k, n). \tag{1}$$

由文献[1] 有

$$N^{(m)}(w,n) = N^{(m)}(2^n - w, n), \tag{2}$$

$$N^{(m)}(0,n) = N^{(m)}(2^n, n) = 1. \tag{3}$$

由文献 [3], 对任意 $k$, 重量为 2k 的 1 阶相关免疫函数皆存在，即 $N^{(1)}(2k,n) \neq 0$, 但当 $m \geq 2$ 时，情况则大不一样，比如 $m = 2$ 时， $N^{(2)}(4,n)$ 只有当 $n = 2,3$ 时，不为 0, 即 $n > 3$ 时 $N^{(2)}(4,n) = 0$, 一般地，有如下结论:

[1] 1996-04-05 收到， 1997-03-06 定稿

**定理 1**

$$N^{(m)}(2^m,n)=\begin{cases}1, & n=m\text{时};\\ 2, & n=m+1\text{时};\\ 0, & \text{其它}.\end{cases}$$

证明略去.

**定理 2**　设 $m\geq 2$, 则对任意 $w$, 存在 $w_0$, 使得当 $n\geq w_0$ 时, $N^{(m)}(w,n)=0$ .

证明是显然的. 因为 $m$ 阶相关免疫函数的特征阵中, 各列互不相同, 且不能有共轭对出现, 故 $w_0$ 至少可取为 $2^{w-1}$ .

两个向量 $\alpha$ 、 $\beta$ 称为共轭的是指: $\alpha+\beta=(1,1,\cdots,1)$ .

当 $w$ 不大时, 通过计算表明 $w_0$ 可取为 $w$, 但对任意 $w,w_0$ 是否可取为 $w$ 还有待证明, 特提出以下猜想.

**猜想**　设 $m\geq 2$, 则当 $n\geq w$ 时 $N^{(m)}(w,n)=0$ .

## 3　$N^{(m)}(n)$ 的下界公式

**引理 1** [1]　对任意 $m\geq 1,k\geq 1$, 有 $\mathrm{GF}(2)^{mk+1}=\begin{bmatrix}C_1\\ \vdots\\ C_{2^k}\end{bmatrix}$, $C_i$ 是 $(2^{(m-1)k+1},mk+1,2,m)$ 正交阵, $\mathrm{GF}(2)^n$ 表示以该空间全体向量为行之阵.

**引理 2** [1]　对任意的 $k\leq(n-1)/m,(m\geq 2)$, 有 $N^{(m)}(2^{n-k},n)\geq(2^k!)^{2^{n-mk-1}}$ .

**引理 3**　对任意 $m\geq 1,k\geq 1$, 有 $2^k$ 个互无相同行的 $(2^{(m-1)k+1},mk+1,2,m)$ 正交阵.

证明见文献 [1] 中引理 3.1 和定理 3.4 之证明过程.

**引理 4**　对任意 $k\leq(n-1)/m,m\geq 2$, 有 $2^k$ 个互无相同行的 $(2^{n-k},n,2,m)$ 正交矩阵.

**证明**　若 $A,B$ 是互无相同行的 $(w,n,2,m)$ 正交阵, 则

$$C_1=\begin{bmatrix}1 & A\\ 0 & A\end{bmatrix},\qquad C_2=\begin{bmatrix}1 & B\\ 0 & B\end{bmatrix}$$

是两个互无相同行的 $(2w,n+1,2,m)$ 正交阵, 再由引理 3 可证本引理.

**引理 5**　若 $A$ 、 $B$ 是 $(w,n,2,m)$ 正交阵, 且 $A$ 与 $B$ 无相同行, 则 $C=\begin{bmatrix}A\\ B\end{bmatrix}$ 是 $(2w,n,2,m)$ 正交阵.

由定义可证.

由引理 5 和文献 [1] 中定理 3.5 可得

**引理 6**　对任意 $0\leq t\leq 2^k,k\geq 1,m\geq 2$, 有

$$N^{(m)}(2^{(m-1)k+1}t,mk+1)\geq\begin{cases}2^k!, & t=1,2^k-1;\\ C_{2^k}^t, & t\neq 1,2^k-1.\end{cases}$$

由引理 6 和文献 [1] 中定理 3.2 可证.

**引理 7**　对任意 $m\geq 2,k\geq 1,0\leq t\leq 2^k$, 有

$$N^{(m)}(2^{n-k}t,n)\geq\begin{cases}(2^k!)^{2^{n-mk-1}}, & t=1,2^k-1;\\ (C_{2^k}^t)^{2^{n-mk-1}}, & t\neq 1,2^k-1.\end{cases}$$

由引理 7 并利用 (1)、(2)、(3) 式，有

$$N^{(m)}(n)=\sum_{k=0}^{2^{n-m}}N^{(m)}(2^mk,n)\geq\sum_{k=0}^{[(n-1)/m]}\sum_{t\in J_k}N^{(m)}(2^{n-k}t,n)$$

$$\geq 2+2^{2^{n-m-1}}+2\sum_{k=2}^{[(n-1)/m]}(2^k!)^{2^{n-mk-1}}+\sum_{k=3}^{[(n-1)/m]}\sum_{t\in I_k}(C_{2^k}^t)^{2^{n-mk-1}}.$$

这里，$I_k=\{3,5,7,\cdots,2^k-3\}, J_k=I_kU\{1,2^k-1\}$ .

从而得

**定理** 3　$n$ 个变元的 $m$ 阶相关免疫函数的个数至少为

$$2+2^{2^{n-m-1}}+2\sum_{k=2}^{[(n-1)/m]}(2^k!)^{2^{n-mk-1}}+\sum_{k=3}^{[(n-1)/m]}\sum_{t\in I_k}(C_{2^k}^t)^{2^{n-mk-1}}$$

## 4 结 语

本文给出的下界是相当好的. 截止目前 1 阶相关免疫函数的个数 $N^{(1)}(n)$ 最好的下界表达式为

$$2^{2^{n-1}}+g_1(n)2^{2^{n-2}}+g_2(n)2^{2^{n-3}}+\cdots.$$

最高项为 $2^{2^{n-1}}$, 那么，自然的问题是，$m$ 阶时最高项能否从文中的 $2^{2^{n-m-1}}$ 改进为 $2^{2^{n-m}}$ 呢？回答是否定的. 通过直接计算可知，$N^{(2)}(4)=12<16=2^{2^{4-2}}$ . 因此最高项只能达到 $2^{2^{n-m-1}}$, 文中下界首项为 $2^{2^{n-m-1}}$, 因此这个下界是比较紧的. 当然，对 $2^{2^{n-m-1}}$ 的系数是否可以改进，还有待于进一步研究.

## 参 考 文 献


[1] 温巧燕，肖国镇. $m$ 阶相关免疫函数的构造与计数，西安电子科技大学学报，1997, 24(1): 36–39.

[2] Mitchell C. Enumerating Boolean functions of cryptographic significance. J of Crytology, 1990, 2(3): 155–170.

[3] 丁存生，肖国镇. 流密码学及其应用. 北京：国防工业出版社，1994, 161–173.

[4] 杨义先，胡正名，用于序列密码的布尔函数计数问题. 通信学报，1992, 13(4): 18–24.

[5] 杨义先. 相关免疫布尔函数的计数. 电子科学学刊，1993, 15(2): 140–146.

[6] 王建宇. 线性结构函数与一阶相关免疫函数的计数. 通信学报，1996, 17(1): 87–91.


## THE ENUMERATION OF CORRELATION-IMMUNE BOOLEAN FUNCTIONS OF $m$-ORDER


Wen Qiaoyan　Xiao Guozhen

(*Xidian university, Xi'an* 710071)



**Abstract**　Construction and enumeration of correlation-immune Boolean functions of $m$-order are discussed in this paper and the formula of lower bounds given by the authors (1997) formerly is improved greatly.



**Key words**　Correlation-immune, Stream ciphers, Orthogonal array, Boolean functions



温巧燕：女，1959 年生，副教授，博士生，现从事密码学、编码学，应用数学等方面的教学和研究.

肖国镇：男，1935 年生，教授，博士生导师，现从事密码学，编码学、信息论和应用数学等方面的教学和研究工作.