第 15 卷 第 2 期　　电 子 科 学 学 刊　　Vol. 15, No. 2
1993 年 3 月　　JOURNAL OF ELECTRONICS　　Mar., 1993

相关免疫布尔函数的计数*

杨 义 先
(北京邮电学院信息工程系,北京 100088)

摘要　本文首次求出了重量为 4(或2^n-4) 和 6(或2^n-6) 的 n 元相关免疫布尔函数的精确个数。同时还用递归算法改进了现有的下界公式。

关键词　布尔函数;计数;密码;相关免疫

一、引　言

布尔函数是序列密码体制中的一类重要的密钥流生成器。为了使序列密码能抵抗"各个击破"式的相关攻击,就必须要求所用到的布尔函数具有相关免疫特性,并称这样的函数为"一阶"相关免疫函数,本文简称为 CIB 函数。由于 CIB 函数在密码中的重要作用,近年来国内外对 CIB 函数进行了大量的研究[1-13]。本文仅考虑 CIB 函数的计数问题。

CIB 函数的定义有多种等价的叙述形式,下面仅叙述两种直观易懂的形式。

定义 1[1]　n 元布尔函数 $f(x_1, \cdots, x_n)$ 称为一个 CIB 函数,当且仅当对任意 $i(1 \leqslant i \leqslant n)$ 和 $a(a=0$ 或 $1)$ 都成立如下等式:

$$W(f(x_1,\cdots,x_n)) = 2W(f(x_1,\cdots,x_n)|x_i = a)$$

这里 $W(f)$ 和 $W(f|x_i=a)$ 分别表示 n 元和 $n-1$ 元布尔函数 $f(x_1, \cdots, x_n)$ 和 $f(x_1,\cdots,x_{i-1},a,x_{i+1},\cdots,x_n)$ 的 Hamming 重量。

定义 2　设 $f(x_1,\cdots,x_n)$ 是 n 元布尔函数,记 $W=W(f)$,则称向量集合

$$D = \{d=(d_1,\cdots,d_n): f(d_1,\cdots,d_n)=1\}$$

为 $f(\cdot)$ 的特征集合。又记 $c_1=(c_{11},\cdots,c_{1n}),\cdots,c_W=(c_{W1},\cdots,c_{Wn})$ 为集合 D 中按字典序排列的 $f(\cdot)$ 的一切特征向量(注意到 $|D|=W(f)=W$),那么就称 $W\times n$ 阶 0,1 矩阵

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_W \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & & & \\ c_{W1} & c_{W2} & \cdots & c_{Wn} \end{pmatrix} \tag{1}$$

1991.12.17 收到,1992.10.05 定稿。
* 国家青年自然基金资助课题。
杨义先　男,1961 年出生,博士,教授,目前主要从事现代密码、纠错编码、信号理论、通信理论、人工神经网络和应用数学等方面的研究。

为 $f(\cdot)$ 的定序特征矩阵. 显然布尔函数与其定序特征矩阵是相互唯一确定的.

定义 3[13]　$(2k)\times n$ 阶 0,1 矩阵 $A=(a_{ij})$ 称为列平衡矩阵，当且仅当矩阵 A 的各行互异并且 A 的各列中刚好含有 k 个“0”和 k 个“1”.

列平衡矩阵曾在高维 Hadamard 矩阵的研究中起过重要作用[13]，下面将看到列平衡矩阵在 CIB 函数的计数方面也是十分有用的. 实际上由定义 1 和 CIB 函数的重量恒为偶数，又由文献[6]的推论 2 可知 CIB 函数还可等价地定义为：

定义 1　n 元布尔函数 $f(x_1,\cdots,x_n)$ 是 CIB 函数，当且仅当 $W(f)$ 为偶数(不妨记 $W(f)=2k$) 并且 $f(\cdot)$ 的定序特征矩阵是一个列平衡矩阵.

n 元 CIB 函数的计数问题难度很大，至今尚未彻底解决. 1986 年文献[10]中的结果是 $N(n)\geqslant 2^r$，$(r=2^{n-2})$；1990 年文献[12]中改进为 $N(n)\geqslant 2^p$，$(p=2^{n-1})$；1991 年文献[6]得到了在此之前的最好下界：

$$N(n)\geqslant\left[\sum_{j=2}^{n-1}\sum_{l=j}^{n-1}\binom{2^{l-1}}{2^{j-1}}\binom{2^{j-1}}{2^{j-2}}\binom{2^j}{2^{j-1}}^{n-l-1}\binom{2^{n-l-1}}{2^{j-1}}\right]+\binom{2^{n-1}}{2^{n-2}}-P(n)\qquad(2)$$

由此可见经过国内外学者的共同努力，$N(n)$ 的下界值虽然被不断的改进，但是始终未能求出其精确值. 本文将对几种极端情形首次给出 CIB 函数的精确计数公式，并利用递归方法极大地改进了现有的 $N(n)$ 值下界.

二、$W(f)=4$ 的情形

由定义 1 知 CIB 函数的重量恒为偶数，因此若对任意 $k(0\leqslant k\leqslant 2^{n-1})$ 求出了重量为 $2k$ 的 CIB 函数的精确个数 $N(2k,n)$，那么 n 元 CIB 函数的精确个数 $N(n)$ 就可表示为

$$N(n)=\sum_{k=0}^{2^{n-1}}N(2k,n)\qquad(3)$$

由文献[1]的引理 2 可得

$$N(2k,n)=N(2^n-2k,n)\qquad(4)$$

$$N(0,n)=N(2^n,n)=1\qquad(5)$$

由文献[6]的命题 1 还可得

$$N(2,n)=N(2^n-2,n)=2^{n-1}\qquad(6)$$

本节和下节将分别求出 $N(4,n)$ (或 $N(2^n-4,n)$) 和 $N(6,n)$ (或 $N(2^n-6,n)$) 的精确值. 结合定义 1′，定义 2 和定义 3 可知：

引理 1　若记 $M(2k,n)$ 为 $(2k)\times n$ 阶列平衡矩阵的个数，那么重量为 $2k$ 的 CIB 函数的个数为：

$$N(2k,n)=M(2k,n)/(2k)!\qquad(7)$$

为求出 $M(4,n)$ 的精确值，注意到重量为 2 的 4 维 0,1 列向量共有 6 个，即

$$a_1=\begin{pmatrix}0\\0\\1\\1\end{pmatrix},\quad a_2=\begin{pmatrix}0\\1\\0\\1\end{pmatrix},\quad a_3=\begin{pmatrix}0\\1\\1\\0\end{pmatrix},\quad a_4=\begin{pmatrix}1\\0\\0\\1\end{pmatrix},\quad a_5=\begin{pmatrix}1\\0\\1\\0\end{pmatrix},\quad a_6=\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$$

将各列取自 $a_1,\cdots,a_6$ 的 $4\times n$ 阶矩阵记为

$$B=(b_1,b_2,\cdots,b_n)=\begin{pmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\b_{31}&b_{32}&\cdots&b_{3n}\\b_{41}&b_{42}&\cdots&b_{4n}\end{pmatrix}\tag{8}$$

上述矩阵 B 的各列中已经刚好含 2 个“1”，因此只要 B 的各行互异，它就成为一个列平衡矩阵. 为求出这种列平衡矩阵的个数，分以下情况：

情况 1 B 中至少有两列 b_i 和 b_j 使得 $b_i=a_1$ 和 $b_j=a_2$（为书写简洁今后约定，如果 a_i 与 B 中的某列相同，就记为 $a_i\in B$；如果 $a_i\in B$ 并且 $a_j\in B$，就记 $\{a_i,a_j\}\in B$，依此类推. 同理如果 a_i 不等于 B 中的任何一列，就记 $a_i\bar{\in}B$. 此外诸如 $\{a_i,a_j\}\bar{\in}B$ 的含义可同法得到. 按此约定，情况 1 便可简记为 $\{a_1,a_2\}\in B$）.

由于 4×2 阶矩阵 $(a_1|a_2)=\begin{pmatrix}0&0&1&1\\0&1&0&1\end{pmatrix}^T$ 的各行已经互异，所以在情况 1 之下，B 的各行也是互异的. 由于不含 a_1 的 B 矩阵个数为 5^n；不含 a_2 的 B 矩阵个数为 5^n；同时不含 a_1 和 a_2 的 B 矩阵个数为 4^n. 所以同时含有 a_1 和 a_2 的 B 矩阵的个数 $E(1)$ 为

$$E(1)=6^n-2\times5^n+4^n\tag{9a}$$

情况 2 $\{a_1,a_3\}\in B$ 但 $a_2\bar{\in}B$. 注意到 4×2 阶矩阵 $(a_1|a_3)$ 的各行已经互异，所以仿情况 1，此时列平衡矩阵 B 的个数 $E(2)$ 为

$$E(2)=5^n-2\times4^n+3^n\tag{9b}$$

下面约定 $E(i)$ 表示在第 i 种情况下，列平衡矩阵 B 的个数.

情况 3 $\{a_1,a_4\}\in B$ 但 $\{a_2,a_3\}\bar{\in}B$.

$$E(3)=4^n-2\times3^n+2^n\tag{9c}$$

情况 4 $\{a_1,a_5\}\in B$ 但 $\{a_2,a_3,a_4\}\bar{\in}B$

$$E(4)=3^n-2\times2^n+1\tag{9d}$$

情况 5 $\{a_1,a_6\}\in B$，但 $\{a_2,a_3,a_4,a_5\}\bar{\in}B$. 或者 $a_1\in B$，但 $\{a_2,a_3,a_4,a_5,a_6\}\bar{\in}B$. 此时 B 矩阵的第 1 行和第 2 行始终相同，所以

$$E(5)=0\tag{9e}$$

情况 6 $\{a_2,a_3\}\in B$，但 $a_1\bar{\in}B$.

$$E(6)=5^n-2\times4^n+3^n\tag{9f}$$

情况 7 $\{a_2,a_4\}\in B$，但 $\{a_1,a_3\}\bar{\in}B$.

$$E(7)=4^n-2\times3^n+2^n\tag{9g}$$

情况 8 $\{a_2,a_6\}\in B$，但 $\{a_1,a_3,a_4\}\bar{\in}B$.

$$E(8) = 3^n - 2 \times 2^n + 1 \tag{9h}$$

情况 9　$\{a_2, a_5\} \in B$，但 $\{a_1, a_3, a_4, a_6\} \in B$ 或者 $a_2 \in B$，但 $\{a_1, a_3, a_4, a_5, a_6\} \in B$. 此时 B 的第一行和第3行始终相同. 所以

$$E(9) = 0 \tag{9i}$$

情况 10　$\{a_3, a_5\} \in B$，但 $\{a_1, a_2\} \in B$.

$$E(10) = 4^n - 2 \times 3^n + 2^n \tag{9j}$$

情况 11　$\{a_3, a_6\} \in B$，但 $\{a_1, a_2, a_5\} \in B$.

$$E(11) = 3^n - 2 \times 2^n + 1 \tag{9k}$$

情况 12　$\{a_3, a_4\} \in B$，但 $\{a_1, a_2, a_5, a_6\} \in B$ 或者 $a_3 \in B$，但 $\{a_1, a_2, a_4, a_5, a_6\} \in B$. 此时 B 矩阵的第 1 行和第 4 行相同，所以

$$E(12) = 0 \tag{9l}$$

情况 13　$\{a_4, a_5\} \in B$，但 $\{a_1, a_2, a_3\} \in B$.

$$E(13) = 3^n - 2 \times 2^n + 1 \tag{9m}$$

情况 14　$\{a_5, a_6\} \in B$，但 $\{a_1, a_2, a_3, a_4\} \in B$

$$E(14) = 2^n - 2 \tag{9n}$$

情况 15　$\{a_5\} \in B$，但 $\{a_1, a_2, a_4, a_6\} \in B$. 此时 B 的第 1 行和第 3 行相同，所以

$$E(15) = 0 \tag{9o}$$

情况 16　$\{a_4, a_6\} \in B$，但 $\{a_1, a_2, a_3, a_5\} \in B$.

$$E(16) = 2^n - 2 \tag{9p}$$

情况 17　只有 $a_4 \in B$ 或者只有 $a_6 \in B$.

$$E(17) = 0 \tag{9q}$$

以上 17 种情况概括了将列向量 $a_1, \cdots, a_6$ 放入(8)式的矩阵中所形成的一切列平衡矩阵. 综上所述可知：

定理 1　$4 \times n$ 阶列平衡矩阵的个数 $M(4,n)$ 为

$$M(4,n) = \sum_{i=1}^{17} E(i) = 6^n - 3 \times 2^n$$

更进一步由(7)和(4)式知，重量为 4 或 $2^n - 4$ 的 n 元 CIB 函数的精确个数为

$$N(4,n) = N(2^n - 4, n) = [6^n - 3 \times 2^n]/24 \tag{10}$$

三、$W(f)=6$ 的情形

上一节求出了 $N(4,n)$，现在计算 $N(6,n)$. 从原理上看，上节的方法是可行的，但是却要耗费巨大的工作量，所以必须采用新方法. 下面用递归方法计算 $N(6,n)$ 的精确值.

设 $6 \times (n+1)$ 阶 0,1 矩阵为

$$F = (F_1 | g) \tag{11}$$

这里 $g = (g_1, \cdots, g_n)^T$ 是一个 6 维列向量，而 F_1 是一个 $6 \times n$ 阶 0,1 矩阵，F_1 的第 i 行记为 $f_i (1 \leqslant i \leqslant 6)$. 并且已假定矩阵 F 中各列刚好含 3 个“1”和 3 个“0”. 为揭示

$6\times n$ 和 $6\times(n+1)$ 阶列平衡矩阵的个数 $M(6,n)$ 和 $M(6,n+1)$ 之间的关系，分以下情况：

情况 I (11)式中 F_1 的各行互异。此时任取一个重量为 3 的 6 维列向量作为 g 后，所得的矩阵 F 都是一个 $6\times(n+1)$ 阶的列平衡矩阵。而这时共有 $M(6,n)$ 个 F_1 矩阵。所以在情况 I 之下共有 $\binom{6}{3}M(6,n)=20M(6,n)$ 个 $6\times(n+1)$ 阶的列平衡矩阵。

情况 II (11)式中 F_1 至少有 3 行彼此相等。此时无论怎样选取列向量 g 都无法使矩阵 F 的各行互异，这时没有 $6\times(n+1)$ 阶列平衡矩阵。

情况 III (11)式中 F_1 的各行满足 $f_i=f_j$；$f_k=f_r$ 和 $f_p=f_q$ 并且 f_i,f_k,f_p 互异。（这里 $1\leqslant i,j,k,r,p,q\leqslant 6$ 并且互异）此时 F_1 的各列中所含"1"的个数为偶数，不可能等于 3，所以此时也没有 $6\times(n+1)$ 阶列平衡矩阵。

情况 IV (11)式中 F_1 的行满足 $f_i=f_j$，$f_k=f_r$ 并且 f_i，f_k，f_p 和 f_q 互异。当上述 i,j,k,r,p 和 q 给定之后，能使各列刚好含 3 个"1"和 3 个"0"的矩阵 F_1 的选取法共有 $2^n(2^n-2)$ 种。F_1 取定之后为使矩阵 F 的各行互异，共有 8 种方法选取列向量 g。最后由于 i,j,k,p,q 和 r 的可能排序法共有 $6!/(2!2!)=180$ 种，所以在情况 IV 之下共有 $8\times180\times2^n(2^n-2)$ 个 $6\times(n+1)$ 阶列平衡矩阵。

情况 V (11)式中的 F_1 满足 $f_i=f_j$ 并且 f_i,f_k,f_r,f_p 和 f_q 互异。此时矩阵 F_1 的取法共有 $\left\{\left[\binom{6}{3}\right]^n-(\text{情况 I 至情况 IV 时 } F_1 \text{ 的取法个数})\right\}$ 种。因此在情况 V 之下，F_1 的取法共有 $\{20^n-[M(6,n)+5\times2^{n+2}+45\times2^{n+2}(2^n-2)]\}$ 种。当 F_1 取定之后，为使 F 成为列平衡矩阵，共有 $2\times\binom{4}{2}$ 种方法选取 g。在情况 V 之下的 $6\times(n+1)$ 阶列平衡矩阵个数为：

$$12\times\{20^n-[M(6,n)+5\times2^{n+2}+45\times2^{n+2}(2^n-2)]\}.$$

综合以上各种情况可得：

定理 2 当 $n\geqslant3$ 时 $6\times n$ 和 $6\times(n+1)$ 阶列平衡矩阵的个数 $M(6,n)$ 和 $M(6,n+1)$ 之间满足

$$M(6,n+1)=8M(6,n)+g(n) \tag{12a}$$

这里 $g(n)$ 是 n 的如下函数：

$$g(n)=12\times20^n+75\times2^{n+4}-45\times4^{n+2} \tag{12b}$$

此外由(4)，(6)和(7)式还知：

$$M(6,3)=2880 \tag{13}$$

利用定理 2 和(13)式可得：

定理 3 对 $n\geqslant3$，$6\times n$ 阶列平衡矩阵的个数 $M(6,n)$ 和重量为 6（或 2^n-6）的 n 元 CIB 函数的个数 $N(6,n)$（或 $N(2^n-6,n)$）分别为

$$M(6,n)=\sum_{i=3}^{n-1}8^{n-i-1}g(i)+45\times8^{n-1} \tag{14}$$

$$N(6,n)=N(2^n-6,n)=M(6,n)/6! \tag{15}$$

此处 $g(i)$ 由（12 b）式给出。

四、几个一般性结果

由(5),(6),(10)和(15)式已知重量分别为0, 2, 4, 6, 2^n, 2^n-2, 2^n-4 和 2^n-6 的 n 元 CIB 函数的精确个数。但是要想利用(3)式求出 $N(n)$ 的精确值，还必须对 $4\leqslant k\leqslant 2^{n-1}-4$ 求出 $N(2k,n)$，可见 $N(n)$ 的精确值还远未求出。下面给出几个一般性的结果。

定理 4　当 $n\geqslant 4$ 时，n 元 CIB 函数的个数 $N(n)$ 满足下界：

$$N(n)\geqslant P(n)+2[N(0,n)+N(2,n)+N(4,n)+N(6,n)] \tag{16}$$

这里 $P(n)$ 由(2)式给出，$N(2k,n)$ $(0\leqslant k\leqslant 3)$ 分别由(5),(6),(10)和(15)式给出。

比较文献[6,10,12]，不难看出(16)式给出的下界是目前已知的最好下界。

上面(16)式中的下界还可以改进。实际上利用递归方法可以得到如下更好的结果。

将每列各含 k 个"1"和 k 个"0"的 $(2k)\times(n+1)$ 阶0,1矩阵记为 H：

$$H=(H_1|h) \tag{17}$$

这里 h 是 H 的最后一列。

在(17)式中若 H_1 的某 $2r$ 行 $(0\leqslant r\leqslant k)$ 是由互补向量对组成的，并且 H_1 中剩下的 $2(k-r)$ 行彼此互异，同时也与前述 $2r$ 个互补向量对互异，则当 r 固定之后，这样的 H_1 至少有 $\binom{2k}{2r}M(2(k-r),n)\binom{2^{n-1}-2(k-r)}{r}$ 个。而当 H_1 选定后，为使(17)式中的 H 为列平衡矩阵，至少有 $2^r\binom{2(k-r)}{k-r}$ 种方法去选取向量 h。因此当 $r(0\leqslant r\leqslant k)$ 固定之后，至少可以按上述方法得到

$$\binom{2k}{2r}\binom{2^{n-1}-2(k-r)}{r}\binom{2(k-r)}{k-r}2^rM(2(k-r),n)$$

个 $(2k)\times(n+1)$ 阶的列平衡矩阵。于是有

定理 5　$M(2k,n)$ 和 $M(2k,n+1)$ 之间以及 $N(2k,n)$ 和 $N(2k,n+1)$ 之间分别满足

$$N(2k,n+1)\geqslant\frac{1}{(2k)!}\left\{\sum_{r=0}^{k}\binom{2k}{2r}\binom{2^{n-1}-2(k-r)}{r}\binom{2(k-r)}{k-r}\times 2^r[2(k-r)]!N(2(k-r),n)\right\} \tag{18}$$

$$M(2k,n+1)\geqslant\left[\sum_{r=0}^{k}\binom{2k}{2r}\binom{2^{n-1}-2(k-r)}{r}\binom{2(k-r)}{k-r}\times 2^rM(2(k-r),n)\right] \tag{19}$$

显然反复利用递归式(18)式以及已经求出的各 $N(2k,n)$ $(0 \leqslant k \leqslant 3)$，并利用(3)式，便可以极大地改进 $N(n)$ 的下界公式.

参 考 文 献

[1] 杨义先，北京邮电学院学报，**13**(1990)3，27—35.
[2] 杨义先，电子科学学刊，**13**(1991)3，232—241
[3] Yang Yixian, *Electron. Lett.*, **23**(1987)25, 1335—1336.
[4] 杨义先，胡正名，通信学报，**8**(1987)6，1—4.
[5] 龚奇敏，黄月江，电子学报，**19**(1991)4，40—47.
[6] 单炜娟，应用数学学报，**20**(1991)3，331—366.
[7] 肖国镇，电子学报，**14**(1986)4，78—84.
[8] T. Siegenthaler, *IEEE Trans. on IT*, **IT-30**(1984)5, 776—780.
[9] C. Xiao, J. Massey, *IEEE Trans. on IT*, **IT-34**(1988)4,431—433.
[10] F. Pichier, Proc. of Eurocrypt' 86, 1986,pp. 237—241.
[11] R. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, (1986).
[12] C. Mitchell, *J. of Cryptology*, **2**(1990)3, 155—170.
[13] 杨义先，科学通报，**31**(1986)2，85—89.
[14] 杨义先，林须端，胡正名，编码与密码学，人民邮电出版社，北京，1992年，第1版.

ENUMERATING BOOLEAN FUNCTIONS WITH CORRELATION IMMUNITY

Yang Yixian

(Beijing University of Posts and Telecommunications, Beijing 100088)

Abstract The exact numbers of n-variable Boolean functions with correlational immunity are initially found for the cases of weight 4(or 2^n-4) and 6(or 2^n-6). The known lower bounds for the enumeration of such Boolean functions are also improved greatly by the recursive algorithms.

Key words Boolean functions; Enumeration; Cryptography; Correlation-immunity