次数最大的平衡相关免疫函数的构造

潘永涛 戚文峰
(郑州信息工程大学信息工程学院应用数学系 郑州 450002)

摘 要 Maitra 和 Sarkar 于 1999 年提出了一种递归构造 n 元平衡相关免疫布尔函数的方法。该文给出了一种新的递归构造方法，构造出非线性度很高的 n 元 m 阶 $n-m-1$ 次的平衡相关免疫函数。与原构造方法相比，该文构造方法得到的函数性质相同，数量更大。

关键词 布尔函数，代数次数，相关免疫，非线性度，平衡性
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)12-2355-04

Construction of Balanced Correlation-Immune Functions with Highest Degree

Pan Yong-tao Qi Wen-feng
(*Department of Applied Mathematics*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract Maitra and Sarkar provided a recursive construction method of balanced correlation-immune Boolean functions on n variables in 1999. In this paper, a new method is provided to construct balanced m-th order correlation-immune Boolean functions on n variables with high nonlinearity and algebraic degree $n-m-1$. Compared with the original one, this method can get more functions with the same characteristics.

Key words Boolean function, Algebraic degree, Correlation-immunity, Nonlinearity, Balancedness

1 引言

在密码应用中，所使用的布尔函数一般应满足平衡性，并且具有较高的相关免疫阶数、代数次数和非线性度，否则以此函数设计的密码系统就容易受到攻击。1984 年，Siegenthalar提出了相关免疫函数的概念[1]。此后相关免疫函数的构造问题一直是布尔函数的一个重要研究方向。到目前为止，此领域中已拥有了一系列重要研究成果。

1999 年Maitra和Sarkar提出了一种递归构造方法[2]，给定n和m，构造出一个n元m阶 $k=n-m-1$ 次的平衡相关免疫函数F，并使F的非线性度达到很大。但是这种构造方法所能构造的函数数量较少。

下面简要介绍一下 Maitra 和 Sarkar 的构造方法。

F_2 上 n 维向量空间记为 V_n，V_n 上布尔函数的集合记为 Ω_n。设 $f\in\Omega_n$，将 f 视为 $f(x)$ 的真值表，其中 $x=(x_n,\cdots,x_1)$，f^u 为 f 的前半段，f^l 为 f 的后半段。f^r 表示 f 首尾互换得到的序列，f^c 表示 f 中 01 取反得到的序列，并记 $f^{rc}=(f^r)^c=(f^c)^r$。

定义 1 设 $f,g\in\Omega_n$，Q: $\Omega_n\times\Omega_n\to\Omega_{n+1}$，$Q(f,g)=f^uf^lg^ug^l=f$；$R$: $\Omega_n\times\Omega_n\to\Omega_{n+1}$，$R(f,g)=f^ug^uf^lg^l$。

定义 2 给定 $h\in\Omega_k$ 和一个有限列 $(S_t)_{1\le t\le\lambda}$，其中 $S_t\in\{Q,R\}\times\{c,r,rc\}$，定义 $F\in\Omega_{k+\lambda}$ 如下：$F_0=h$，$F_t=P_t(F_{t-1},F_{t-1}^{\tau_t})$，其中 $S_t=(P_t,\tau_t)$，$F=F_\lambda$。称 F 的表示式为 $(h,S_1,\cdots,S_\lambda)$，并称 F 的表示式长为 λ。

Maitra 和 Sarkar 的构造(给定 n 和 m，要求构造一个 n 元 m 阶 $k=n-m-1$ 次的平衡相关免疫函数 F)：若 k 为偶数，取 $h\in\Omega_k$ 为一个 k 元 bent 函数加上 $x_k\cdots x_1$ 项；若 k 为奇数，取 $h\in\Omega_k$ 为两个 $k-1$ 元 bent 函数级联得到的函数再加上 $x_k\cdots x_1$ 项。令 $F\in\Omega_n$ 的表示式为 $(h,S_1,\cdots,S_{m+1})$，其中 $S_t=(P_t,\tau_t)$，$1\le t\le m+1$，t 为奇数时 $\tau_t\in\{c,r\}$，t 为偶数时 $\tau_t\in\{c,rc\}$，则 F 为一个 n 元 m 阶 $n-m-1$ 次的平衡相关免疫函数。

由 Maitra 和 Sarkar 的构造方法可以看出，构造过程的每步递归中 S_t 都是 $2\times2=4$ 种不同的选择，因此对一个给定的 $h\in\Omega_k$，所构造出的函数数量有限。本文提出了一种新的递归构造方法，对上述构造中一个给定的 $h\in\Omega_k$，先对 h 进行变换得到 h'，再将 h' 和 $(h')^\tau$ (τ 的选择与 Maitra 和 Sarkar 的构造中的选择方法相同)按某种特定的方式组合成一个 $k+1$ 元的函数；以这种方法递归下去，可以构造出一个 n 元 m 阶 $n-m-1$ 次的平衡相关免疫函数。因为每一步递归可以选择的变换与组合方式的数量都很大，所以对一个给定的 h，本方法可以构造出大量此类函数。

2 准备工作

设 $f\in\Omega_n$，f 的真值表中“1”的个数称为 f 的 Hamming 重量，记为 $\mathrm{wt}(f)$，若 $\mathrm{wt}(f)=2^{n-1}$，则称 f 是平衡的。两个布尔函数 f 与 g 的 Hamming 距离定义为 $d(f,g)=\left|\{x\in V_n\,|\,f(x)\ne g(x)\}\right|$。$f$ 与 g 的 Walsh 距离定义为 $\mathrm{wd}(f,g)=$

2005-05-16 收到， 2005-11-24 改回
国家自然科学基金 (60373092) 资助课题

$\left|\{x\in V_n \mid f(x)=g(x)\}\right|-\left|\{x\in V_n \mid f(x)\neq g(x)\}\right|$。$V_n$ 上形如 $f(x)=b_1x_1+b_2x_2+\cdots+b_nx_n+c$ 的函数称为仿射函数，记 $f\in L_n$，若 $c=0$，则称之为线性函数。布尔函数 f 与所有仿射函数之间的最小 Hamming 距离称为 f 的非线性度，记为 $\mathrm{nl}(f)$。于是 $\mathrm{nl}(f)=2^{n-1}-\frac{1}{2}\max_{H\in L_n}\left|\mathrm{wd}(f,H)\right|$。$f$ 的代数次数记为 $\deg(f)$。

定义 3[3] 称 $F(w)=\sum_{x\in V_n}(-1)^{f(x)+w\cdot x}$ 为布尔函数 f 的 Walsh 谱，其中 $w=(w_n,\cdots,w_1)$，$x=(x_n,\cdots,x_1)$，$w\cdot x$ 表示 w 与 x 的内积。若对任意 $w\in V_n$ 且 $1\le \mathrm{wt}(w)\le m$，有 $F(w)=0$，则称 $f(x)$ 为 m 阶相关免疫函数。记 $C_n(m)=\{f\in\Omega_n \mid f$ 为 m 阶相关免疫的，但不是 $m+1$ 阶相关免疫的$\}$，$HC_n(m)=\bigcup_{i=m}^{n}C_n(i)$。

命题 1[1] 设 n 元 d 次布尔函数 $f(x)$ 为 m 阶相关免疫函数，则 $d\le n-m$. 若 $f(x)$ 平衡，则 $d\le n-m-1$。

称次数为 $n-m-1$ 的 n 元 m 阶的平衡相关免疫函数为次数最大的平衡相关免疫函数。

定义 4 ($1/2^t$对折变换) 设 S 是 $\{1,2,\cdots,2^n\}$ 的一个全排列，给定 t，$1\le t\le n$，将 S 按顺序分成等长的 2^t 段，每段长为 2^{n-t}，第 $2k-1$ 段与第 $2k$ 段交换位置，$k=1,2,\cdots,2^{t-1}$，称此变换为 $1/2^t$ 对折变换。

定义 5 (对折) 设 S 是 $\{1,2,\cdots,2^n\}$ 的一个全排列，对 S 进行 k 次 $1/2^t$ 对折变换(t 的取值可以重复，依次为 $t_1,t_2,\cdots,t_k$)，称此变换为对 S 的一个对折，记为 $A=(t_1,t_2,\cdots,t_k)$。若 S 分别进行两个对折得到的排列相同，称这两个对折相等。

由定义 4 和定义 5 可以直接得到下面两个引理。

引理 1 设 S 是 $\{1,2,\cdots,2^n\}$ 的一个全排列，给定 t，$1\le t\le n$，则对 S 进行对折 (t,t) 得到的排列与 S 相同。

引理 2 设 S 是 $\{1,2,\cdots,2^n\}$ 的一个全排列，给定 t_1,t_2，$1\le t_1,t_2\le n$，则对 S 分别进行对折 (t_1,t_2) 和 (t_2,t_1) 得到的排列相同。

由引理 1 和引理 2 可知，在对 S 的一个对折 $A=(t_1,t_2,\cdots,t_k)$ 中，将两个重复的 t 值抵消，并改变顺序，得到的对折与原对折相同。

例如 $n\ge 3$，$A=(1,3,1,2,1,3)$，$A'=(1,2)$，则 $A=A'$。

因此可以将定义 5 改写为

定义 5′ (对折) 设 S 是 $\{1,2,\cdots,2^n\}$ 的一个全排列，给定 $t_1,\cdots,t_k$，$1\le t_1\le\cdots\le t_k\le n$，$1\le k\le n$，对 S 进行 k 次 $1/2^t$ 对折变换($t=t_1,t_2,\cdots,t_k$，不计顺序)，则此变换称为一个 n 维对折，记为 $A=(t_1,t_2,\cdots,t_k)$。令 $r=\sum_{i=1}^{k}2^{n-t_i}t_i$，则称 A 为第 r 个 n 维对折，记为 A_r。特别地，若 A 对 S 不作任何变换，称 A 为第 0 个 n 维对折。对 S 进行对折 A 得到的排列记为 $A(S)$。

由定义 5′可以看出，对正整数 n，共有 2^n 个不同的 n 维对折。

定义 6(B_t) 给定正整数 n，对任一整数 t，$1\le t\le n+1$，$B_t=\{i+2^tk \mid 1\le i\le 2^{t-1},0\le k\le 2^{n+1-t}-1\}$，并把 B_t 中的数按从小到大的顺序排列。

显然，$|B_t|=2^n$。

定义 7 设 $f,g\in\Omega_n$，$0\le i\le 2^n-1$，$1\le j\le n+1$，在一个长为 2^{n+1} 的序列中，将 $A_i(f)$ 按比特依次填入 B_j 对应的位置，再将 $A_i(g)$ 按比特依次填入 $\underline{B}_j=\{1,2,\cdots,2^{n+1}\}-B_j$ ($\underline{B}_j$ 和 B_j 类似，也按从小到大的顺序排列)对应的位置，得到一个 $n+1$ 元函数，记为 $P_{ij}(f,g)$。

3 非线性度、代数次数与平衡性

引理 3 设 $f\in\Omega_n$，对 f 进行 $1/2^t$ 对折变换，得到的函数记为 f'，则

$$f'(x_n,\cdots,x_1)=f(x_n,\cdots,x_{n+1-t}+1,\cdots,x_1)$$

证明 不妨对 $t=1$ 的情形证明。

因为 $f(x_n,\cdots,x_1)=(x_n+1)f(0,x_{n-1},\cdots,x_1)+x_nf(1,x_{n-1},\cdots,x_1)$ 所以

$$\begin{aligned}f(x_n+1,\cdots,x_1)&=((x_n+1)+1)f(0,x_{n-1},\cdots,x_1)\\&\quad+(x_n+1)f(1,x_{n-1},\cdots,x_1)\\&=x_nf(0,x_{n-1},\cdots,x_1)+(x_n+1)f(1,x_{n-1},\cdots,x_1)\\&=(x_n+1)f(1,x_{n-1},\cdots,x_1)+x_nf(0,x_{n-1},\cdots,x_1)\\&=f'(x_n,\cdots,x_1)\end{aligned}$$

证毕

由引理 3 可直接得到下面两个推论。

推论 1 设 $f\in\Omega_n$，对 f 进行对折 $A=(t_1,t_2,\cdots,t_k)$，$1\le t_1\le\cdots\le t_k\le n$，得到 f'，则

$$f'(x_n,\cdots,x_1)=f(x_n,\cdots,x_{n+1-t_1}+1,\cdots,x_{n+1-t_k}+1,\cdots,x_1)$$

推论 2 设 $H\in L_n$，且有 r 个变元在 H 的代数式中出现(即有 r 个变元在 H 的代数式中系数不为 0)，对 H 进行对折 A，则 $A(H)$ 为仿射函数，且 $A(H)$ 与 H 的代数式中出现的变元相同。

引理 4 对任意的 $H\in L_{n+1}$，从 H 中依次抽取 B_j 对应位置的值，则得到一个自变量为 $x'=(x_{n+1},x_n,\cdots,x_{n-j-2},x_{n-j},\cdots,x_1)$ 的 n 元仿射函数 $H\big|_{B_j}$：

$$H\big|_{B_j}(x')=H(x_{n+1},x_n,\cdots,x_{n-j-2},0,x_{n-j},\cdots,x_1)$$

依次抽取 $\underline{B}_j$ 对应位置的值也构成一个 n 元仿射函数，记为 $H\big|_{\underline{B}_j}$：

$$H\big|_{\underline{B}_j}(x')=H(x_{n+1},x_n,\cdots,x_{n-j-2},1,x_{n-j},\cdots,x_1)$$

推论 3 $H(x_n,\cdots,x_1)=\sum_{i=1}^{n+1}a_ix_i$，给定整数 j，$1\le j\le n+1$，若 $a_{n-j+1}=1$，则 $H\big|_{B_j}(x')=H\big|_{\underline{B}_j}(x')+1$；若 $a_{n-j+1}=0$，则 $H\big|_{B_j}(x')=H\big|_{\underline{B}_j}(x')$。

注：(1) $H\big|_{B_j}$ 与 $H\big|_{\underline{B}_j}$ 的代数式中出现的变元相同，若 $a_{n-j+1}=1$，则二者的代数式中出现的变元比 H 少 1 个，若 $a_{n-j+1}=0$，则与 H 相同。(2) 若 H 取遍 L_{n+1}，则 $H\big|_{B_j}$ 与 $H\big|_{\underline{B}_j}$ 都取遍 L_n。

定理 1　设 $f,g\in\Omega_n$，$F=P_{ij}(f,g)$，$0\le i\le 2^n-1$，$1\le j\le n+1$，则 $\mathrm{nl}(F)\ge \mathrm{nl}(f)+\mathrm{nl}(g)$；并且若 $g=f^r$ 或 f^c，则 $\mathrm{nl}(F)=2\mathrm{nl}(f)$。

证明　以下将 $H\big|_{B_j}$ 和 $H\big|_{\underline{B}_j}$ 分别简记为 H_1 和 H_2。

因为 $\mathrm{wd}(P_{ij}(f,g),H)=\mathrm{wd}(A_i(f),H_1)+\mathrm{wd}(A_i(g),H_2)=\mathrm{wd}\big(f,A_i(H_1)\big)+\mathrm{wd}\big(g,A_i(H_2)\big)$，所以

$$\begin{aligned}\mathrm{nl}(F)&=2^n-\frac{1}{2}\max_{H\in L_{n+1}}\left|\mathrm{wd}(P_{ij}(f,g),H)\right|\\&=2^n-\frac{1}{2}\max_{H\in L_{n+1}}\left|\mathrm{wd}(A_i(f),H_1)+\mathrm{wd}(A_i(g),H_2)\right|\\&\ge\left[2^{n-1}-\frac{1}{2}\max_{H\in L_{n+1}}\left|\mathrm{wd}(f,A_i(H_1))\right|\right]\\&\quad+\left[2^{n-1}-\frac{1}{2}\max_{H\in L_{n+1}}\left|\mathrm{wd}(g,A_i(H_2))\right|\right]\\&=\mathrm{nl}(f)+\mathrm{nl}(g)。\end{aligned}$$

若 $g=f^r$ 或 f^c，等号显然成立。　　证毕

定理 2　设 $f\in\Omega_n$，$F=P_{ij}(f,f^\tau)$，$0\le i\le 2^n-1$，$1\le j\le n+1$，$\tau\in\{c,r\}$，则 $\deg(F)=\deg(f)$。

证明　由推论 1 知，对任意的 $f\in\Omega_n$，任意一个 n 维对折都不改变 f 的次数，因此只需证明 $i=0$ 的情况。给定 j，$1\le j\le n+1$，对 $0\le t\le 2^{n-j+3}-1$，记 $c_t=(c_{t,0},\cdots,c_{t,n-j+1})$ 为 t 的二进制表示，即 $t=\sum_{k=0}^{n-j+2}c_{t,k}2^{n+2-j-k}$，则

$$\begin{aligned}&F(x_{n+1},x_n,\cdots,x_1)=P_{0j}(f,f^\tau)\\&=\sum_{k=0}^{2^{n-j+2}-1}(x_{n+1}+c_{2k,0}+1)(x_n+c_{2k,1}+1)\cdots(x_j+c_{2k,n-j+1}+1)\\&\quad\cdot f(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\\&\quad+\sum_{k=0}^{2^{n-j+2}-1}(x_{n+1}+c_{2k+1,0}+1)(x_n+c_{2k+1,1}+1)\cdots(x_j+c_{2k+1,n-j+1}+1)\\&\quad\cdot f^\tau(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\end{aligned}$$

注意到当 $1\le s\le n-j$ 时，$c_{2k,s}=c_{2k+1,s}=c_{k,s+1}$，$c_{2k,n-j+1}=0$，$c_{2k+1,n-j+1}=1$，于是

$$\begin{aligned}&F(x_{n+1},x_n,\cdots,x_1)\\&=\sum_{k=0}^{2^{n-j+2}-1}(x_{n+1}+c_{k,1}+1)(x_n+c_{k,2}+1)\cdots(x_j+0+1)\\&\quad\cdot f(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\\&\quad+\sum_{k=0}^{2^{n-j+2}-1}(x_{n+1}+c_{k,1}+1)(x_n+c_{k,2}+1)\cdots(x_j+1+1)\\&\quad\cdot f^\tau(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\end{aligned}$$

对 F 的变元作一个轮换 $(x_{n+1},x_n,\cdots,x_j)$，则得到的函数为

$$\begin{aligned}&F'(x_{n+1},x_n,\cdots,x_1)\\&=\sum_{k=0}^{2^{n-j+2}-1}(x_n+c_{k,1}+1)(x_{n-1}+c_{k,2}+1)\cdots(x_j+c_{k,n-j+1}+1)(x_{n+1}+1)\\&\quad\cdot f(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\\&\quad+\sum_{k=0}^{2^{n-j+2}-1}(x_n+c_{k,1}+1)(x_{n-1}+c_{k,2}+1)\cdots(x_j+c_{k,n-j+1}+1)x_{n+1}\\&\quad\cdot f^\tau(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\\&=(x_{n+1}+1)\sum_{k=0}^{2^{n-j+2}-1}(x_n+c_{k,1}+1)(x_{n-1}+c_{k,2}+1)\cdots(x_j+c_{k,n-j+1}+1)\\&\quad\cdot f(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\\&\quad+x_{n+1}\sum_{k=0}^{2^{n-j+2}-1}(x_n+c_{k,1}+1)(x_{n-1}+c_{k,2}+1)\cdots(x_j+c_{k,n-j+1}+1)\\&\quad\cdot f^\tau(c_{k,1},\cdots,c_{k,n-j+1},x_{j-1},\cdots,x_1)\\&=(x_{n+1}+1)f(x_n,\cdots,x_1)+x_{n+1}f^\tau(x_n,\cdots,x_1)\end{aligned}$$

显然 $\deg(F')=\deg(f)$。而变元轮换并不改变 F 的次数，因此结论成立。　　证毕

定理 3　设 $f\in\Omega_n$，$\deg(f)=n$，$0\le i\le 2^n-1$，$1\le j\le n+1$，则 $F=P_{ij}(f,f^r)$ 的代数式中有 n 个 n 次项。

证明　由 $\deg(f)=n$，易知函数 $P_{0,n+1}(f,f^r)=ff^r$ 的代数式中有 n 个 n 次项。$P_{i,n+1}(f,f^r)=P_{0,n+1}(A_i(f),A_i(f)^r)$，由推论 1 可知，$\deg(A_i(f))=\deg(f)=n$，所以 $P_{i,n+1}(f,f^r)$ 的代数式中有 n 个 n 次项。再由定理 2 的证明过程可知，F 经过一个变元轮换可以化成 $P_{i,n+1}(f,f^r)$ 的形式，所以结论成立。证毕

由定理 2 的证明过程易知下面的结论成立。

定理 4(平衡性)　设 $f,g\in\Omega_n$，$F=P_{ij}(f,g)$，$0\le i\le 2^n-1$，$1\le j\le n+1$，

(1) 若 $g=f^c$，则 F 平衡。

(2) 若 f 平衡，则当 $g=f^c,f^r$ 时 F 平衡。

4　相关免疫阶数

定理 5　设 $f\in C_n(m)$，$F=P_{ij}(f,f^c)$，$0\le i\le 2^n-1$，$1\le j\le n+1$，则 F 平衡，并且当 f 平衡时，$F\in C_{n+1}(m+1)$。

证明　F 平衡显然成立，下面证明当 f 平衡时，$F\in C_{n+1}(m+1)$。

先证 $i=0$ 的情况。由定理 2 的证明过程可知，每个 $F=P_{0j}(f,f^c)$ 经过一个变元轮换都可以变为 $j=n+1$ 的形式，即 $F'=P_{0,n+1}(f,f^c)=ff^c$。由文献 [4] 可知，$F'\in C_{n+1}(m+1)$，即当 $i=0$，$j=n+1$ 时结论成立。变元轮换保持函数的相关免疫阶数不变，所以当 $i=0$ 时结论对所有的 j 成立。

$F=P_{ij}(f,f^c)=P_{0j}(A_i(f),A_i(f)^c)$，由推论 1 可知，当 $f\in C_n(m)$ 时，$A_i(f)$，$A_i(f)^c\in C_n(m)$，所以 $F\in C_{n+1}(m+1)$，即结论对所有的 i 和 j 都成立。　　证毕

类似可以得到如下定理：

定理 6　设 $f\in C_n(m)$，$F=P_{ij}(f,f^\tau)$，$0\le i\le 2^n-1$，$1\le j\le n+1$，

(1) 若 $\tau=r$，则当 m 为偶数时，$F\in C_{n+1}(m+1)$，且当 f 平衡时 F 平衡。

(2) 若 $\tau=rc$，则当 m 为奇数时，$F\in C_{n+1}(m+1)$，且 F

平衡。

5 递归构造

定义 8 给定 $h\in\Omega_k$ 和一个有限列 $(S_t)_{1\le t\le\lambda}$，其中 $S_t\in\{0,1,\cdots 2^{k+t-1}-1\}\times\{1,\cdots,k+t\}\times\{c,r,rc\}$。定义 $F\in\Omega_{k+\lambda}$ 如下：$F_0=h$，$F_t=P_{i_tj_t}(F_{t-1},F_{t-1}^{\tau_t})$，其中 $S_t=(i_t,j_t,\tau_t)$。令 $F=F_\lambda$，称 F 的表示式为 $(h,S_1,\cdots,S_\lambda)$，并称 F 的表示式长为 λ。

定理 7 设 $h\in\Omega_k$，$F\in\Omega_{m+k+1}$ 的表示式为 $(h,S_1,\cdots,S_{m+1})$，其中 $S_t=(i_t,j_t,\tau_t)$，$1\le t\le m+1$，t 为奇数时 $\tau_t\in\{c,r\}$，t 为偶数时 $\tau_t\in\{c,rc\}$，则结论有：

(1) F 平衡。

(2) $\mathrm{nl}(f)=2^{m+1}\mathrm{nl}(h)$。

(3) $\deg(F)=\deg(f)$。

(4) 若 $m\ge 1$，则 $F\in HC_{m+k+1}(m)$。

(5) 若 $\deg(h)=k$，则 $F\in C_{m+k+1}(m)$。

证明 (1)由定理 4 可得；(2)由定理 1 可得；(3)由定理 2 可得；(4)由定理 5 和定理 6 可得；由(4)可知，F 的相关免疫阶数至少为 m，由(1)和命题 1 可知，F 的相关免疫阶数至多为 m，所以 F 的相关免疫阶数恰为 m，即 $F\in C_{m+k+1}(m)$，所以(5)成立。 证毕

构造方法(给定 n 和 m，要求构造一个 n 元 m 阶 $k=n-m-1$ 次的平衡相关免疫函数 F) 若 k 为偶数，取 $h\in\Omega_k$ 为一个 k 元 bent 函数加上 $x_k\cdots x_1$ 项；若 k 为奇数，取 $h\in\Omega_k$ 为两个 $k-1$ 元 bent 函数级联得到的函数再加上 $x_k\cdots x_1$ 项。令 $F\in\Omega_n$ 的表示式为 $(h,S_1,\cdots,S_{m+1})$，其中 $S_t=(i_t,j_t,\tau_t)$，$1\le t\le m+1$，t 为奇数时 $\tau_t\in\{c,r\}$，t 为偶数时 $\tau_t\in\{c,rc\}$。

定理 8 上述构造方法得到的 $F\in C_n(m)$ 满足：

(1)若 $n-m$ 为奇数，$\mathrm{nl}(F)=2^{n-1}-2^{(n+m-1)/2}-2^{m+1}$。

(2)若 $n-m$ 为偶数，$\mathrm{nl}(F)\ge 2^{n-1}-2^{(n+m)/2}-2^{m+1}$。

证明 (1)若 $n-m$ 为奇数，$k=n-m-1$ 为偶数，取 $u\in\Omega_k$ 为一个 k 元 bent 函数，$h(x_k,\cdots,x_1)=u(x_k,\cdots,x_1)+x_k\cdots x_1$，则 $\mathrm{nl}(h)=2^{k-1}-2^{k/2-1}-1$，于是由定理 7 中的结论(2)可知，$\mathrm{nl}(F)=2^{m+1}\mathrm{nl}(h)=2^{n-1}-2^{(n+m-1)/2}-2^{m+1}$。

(2)若 $n-m$ 为偶数，$k=n-m-1$ 为奇数，取 $u_1,u_2\in\Omega_{k-1}$ 为两个 $k-1$ 元 bent 函数，$h(x_k,\cdots,x_1)=(x_k+1)u_1(x_{k-1},\cdots,x_1)+x_ku_2(x_{k-1},\cdots,x_1)+x_k\cdots x_1$，则 $\mathrm{nl}(h)\ge 2^{k-1}-2^{(k-1)/2}-1$。于是由定理 7 中的结论(2)可知，$\mathrm{nl}(F)=2^{m+1}\mathrm{nl}(h)\ge 2^{n-1}-2^{(n+m)/2}-2^{m+1}$。 证毕

6 与前人构造方法的比较

Maitra 和 Sarkar 的构造方法相当于本文的构造方法作如下限制：对每一个 t，$1\le t\le m+1$，$i_t=0$，$j_t\in\{k+t,k+t-1\}$。于是每一步递归有 $1\times 2\times 2=4$ 种不同的选择，因此给定一个 $h\in\Omega_k$，可以构造出 $\mathrm{Num1}=4^{m+1}$ 个不同的函数表示式。

本构造中第 t 步递归有 $2^{k+t-1}\times(k+t)\times 2=(k+t)2^{k+t}$ 种不同的选择，因此，给定一个 $h\in\Omega_k$，可以构造出的不同函数表示式的个数为

$$\mathrm{Num2}=\prod_{t=1}^{m+1}(k+t)2^{k+t}=(n-m)(n-m+1)\cdots n\times 2^{(2n-m)(m+1)/2}$$

$$=\frac{n!}{(n-m-1)!}2^{(2n-m)(m+1)/2}$$

于是，$\mathrm{Num2}/\mathrm{Num1}=\dfrac{n!}{(n-m-1)!}2^{(2n-m-4)(m+1)/2}$。可以看出 Num2 要远远大于 Num1。

参 考 文 献

[1] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. on Information Theory*, 1984, 30(5): 776–780.

[2] Maitra S, Sarkar P. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In Advances in Cryptology - CRYPTO'99, LNCS.1666, Springer Verlag, 1999: 198–215.

[3] Xiao Guo-Zhen, Massey J. A spectral characterization of correlation immune combining functions. *IEEE Trans. on Information Theory*, 1988, 34(3): 569–571.

[4] Camion P, Carlet C, Charpin P, Sendrier N. On correlation immune functions. In Advances in Cryptology - CRYPTO'91, LNCS.576, Springer-Verlag, 1991: 86–100.

潘永涛： 男，1979 年生，硕士生，研究方向为布尔函数、信息安全.

戚文峰： 男，1963 年生，教授，博士生导师，主要研究方向为密码学、信息安全.