高校应用数学学报
APPLIED MATHEMATICS A JOURNAL
OF CHINESE UNIVERSITIES
1999年 第14卷 第4期 Vol.14 No.4 1999

Bent函数的一般构造法

王隽　李世取

摘　要　本文用概率方法给出小项表示的布尔函数谱的性质，据此得到了Bent函数的特征矩阵的等价刻画，原则上给出了Bent函数的一般构造法，并为Bent函数的计数问题提供了一个模型.文中还提出了Bent矩阵的概念，考察了Bent矩阵的性质，并借助Bent矩阵得到由已知Bent函数构造新的Bent函数的方法.
关键词　布尔函数，Walsh谱，Bent函数，Bent矩阵.
分类号　(中图) TN918.1;　(1991MR)94A60.

A GENERAL CONSTRUCTION OF BENT FUNCTIONS

Wang Jun　Li Shiqu
(Dept.of Appl.Math.,Zhengzhou Information Engineering Institute,450002)

Abstract　With probability methods,spectrum properties of Boolean functions represented by minor term is studied in this paper.On the basis of this an equivalent description of the characteristic matrix of bent functions is given,then a general method of constructing and counting bent functions is discussed in principle.Bent matrix is introduced for the first time and its properties are examined.At last some methods of constructing new bent functions from known bent functions are presented by bent matrixes.
Keywords　Boolean Function, Walsh Spectrum, Bent Function, Bent Matrix.
Subject Classification　(CL)TN918.1;(1991MR)94A60.

§1　引　言

在流密码中，为研究密钥流序列的线性复杂度稳定性和使一些流密码能抗BAA(最佳仿射逼近)攻击，1987年，丁存生等提出了布尔函数稳定性的概念[1]，后来发现这种稳定函数就是Rothaus于1976年提出的Bent函数[2].由于Bent函数与每个仿射函数的符合率(相等的概率)均为$\frac{1}{2}\pm\frac{1}{2\cdot 2^{\frac{n}{2}}}$,即Bent函数与所有仿射函数保持了平衡，所以，以Bent函数为非线性滤波函数和非线性组合函数的流密码能抗BAA攻击，故文献[3]“断言Bent函数是较为理想的非线性滤波和非线性组合函数”，专著[4]也指出“怎样寻找更多更好的Bent函数”“是很有价值的课题”.但从以往国内外公开发表的文章来看，人们大多用代数方法研究Bent函数，且很少见研究Bent函数的一般构造法的.本文则注重概率方法在研究Bent函数构造中的应用，先用概率方法得到谱的性质，再据此用特征矩阵研究Bent函数的结构，为解决Bent函数的一般构造及计数问题提供了一个模型，文中提出了Bent矩阵的概念，考察了Bent矩阵的性质，并借助Bent矩阵得到由已知Bent函数构造新的Bent函数的方法.

§2　Bent函数的结构分析

记GF(2)为二元域，$\Omega=GF^n(2)$,$F=\{A:A\subseteq\Omega\}$,可测空间(Ω,F)上的概率测度P满足：$P\{(x_1,\cdots,x_n)\}=\frac{1}{2^n}$,$(x_1,\cdots,x_n)\in\Omega$,在概率空间$(\Omega,F,P)$上，定义$X_k(x_1,\cdots,x_n)=x_k$,$1\leqslant k\leqslant n$,$(x_1,\cdots,x_n)\in\Omega$,易知$X_1,\cdots,X_n$是$(\Omega,F,P)$上相互独立且具有均匀分布的布尔随机变量.以下凡$X=(X_1,\cdots,X_n)$都表示上述意义的布尔随机向量.

定义1[3]　设$f(x),x\in GF^n(2)$是布尔函数，则f(x)的Walsh循环谱定义为：

$$S_{(f)}(\omega)=\frac{1}{2^n}\sum_{x\in GF^n(2)}(-1)^{f(x)+\omega x},$$

(1)

其中，$w\in GF^n(2)$, $wx=\sum_{j=1}^{n}w_jx_j \bmod 2$.

$S_{(f)}(w)$有如下概率表示式[5]

$$S_{(f)}(w)=P\{f(X)=wX\}-P\{f(X)=wX+1\},$$

(2)

结合$P\{f(X)=wX\}+P\{f(X)=wX+1\}=1$, 则有

$$S_{(f)}(w)=2P\{f(X)=wX\}-1,$$

(3)

及

$$S_{(f)}(w)=1-2P\{f(X)=wX+1\}.$$

(4)

设布尔函数$f(x)$, $x\in GF^n(2)$的Hamming重量为$W(f)$, $f^{-1}(1)=\{c^{(1)}, c^{(2)}, \cdots, c^{(W(f))}\}$, 其中, $c^{(j)}=(c^{(j)}_1, \cdots, c^{(j)}_n)\in GF^n(2)$, $j=1, 2, \cdots, W(f)$, 记

$$f_j(x)=x^{c^{(j)}}=(x_1+c^{(j)}_1+1)\cdots(x_n+c^{(j)}_n+1),$$

(5)

则$f(x)$有小项表示

$$f(x)=f_1(x)+\cdots+f_{W(f)}(x)=x^{c^{(1)}}+\cdots+x^{c^{(W(f))}}.$$

(6)

下面我们借助$f(x)$的小项表示式，用概率方法研究布尔函数的Walsh谱的性质，并据此分析Bent函数的结构.

引理1　设单项式布尔函数$f(x)=x^c=(x_1+c_1+1)(x_2+c_2+1)\cdots(x_n+c_n+1)$, $w\in GF^n(2)$的Hamming重量$W(w)=k$, $1\leqslant k\leqslant n$, w中不为0的分量是$w_{i_1}, w_{i_2}, \cdots, w_{i_k}$, 则对此$w$, 相应的Walsh谱为

$$S_{(f)}(w)=\frac{(-1)^{c_{i_1}+c_{i_2}+\cdots+c_{i_k}+1}}{2^{n-1}}.$$

(7)

证　不妨设$(i_1, i_2, \cdots, i_k)=(1, 2, \cdots, k)$，我们对$k$作归纳法. 当$k=1$时，若$c_1=0$，则

$$P\{f(X)=wX\}=P\{f(X)=X_1\}=$$
$$P\{X_1=0, (X_1+1)(X_2+c_2+1)\cdots(X_n+c_n+1)=X_1\}+$$
$$P\{X_1=1, (X_1+1)(X_2+c_2+1)\cdots(X_n+c_n+1)=X_1\}=$$

$P\{X_1=0\}\cdot P\{(X_2+c_2+1)\cdots(X_n+c_n+1)=0\}=$

$$\frac{1}{2}\left\{1-\frac{1}{2^{n-1}}\right\},$$

若$c_1=1$，则

$$P\{f(X)=wX\}=P\{f(X)=X_1\}=$$
$$P\{X_1=0, X_1\cdot(X_2+c_2+1)\cdots(X_n+c_n+1)=X_1\}+$$
$$P\{X_1=1, X_1\cdot(X_2+c_2+1)\cdots(X_n+c_n+1)=X_1\}=$$
$$P\{X_1=0\}+P\{X_1=1\}\cdot P\{(X_2+c_2+1)\cdots(X_n+c_n+1)=1\}=$$
$$\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2^{n-1}},$$

故据(3)式知

$$S_{(f)}(w)=\frac{(-1)^{c_1+1}}{2^{n-1}},$$

所以，k=1时结论成立，假设结论对k成立，则在k+1时有

$$P\{f(X)=wX\}=P\{f(X)=X_1+X_2+\cdots+X_{k+1}\}=$$
$$P\{X_{k+1}=c_{k+1}, (X_1+c_1+1)\cdots(X_n+c_n+1)=X_1+X_2+\cdots+X_{k+1}\}+$$
$$P\{X_{k+1}=c_{k+1}+1, (X_1+c_1+1)\cdots(X_n+c_n+1)=X_1+X_2+\cdots+X_{k+1}\}=$$
$$P\{X_{k+1}=c_{k+1}\}\cdot P\{(X_1+c_1+1)\cdots(X_k+c_k+1)(X_{k+2}+c_{k+2}+1)\cdots$$
$$(X_n+c_n+1)=X_1+\cdots+X_k+c_{k+1}\}+$$
$$P\{X_{k+1}=c_{k+1}+1\}\cdot P\{X_1+X_2+\cdots+X_k+c_{k+1}+1=0\}=$$
$$\frac{1}{2}\left\{\frac{1}{2}+\frac{(-1)^{c_{k+1}}}{2}\cdot\frac{(-1)^{c_1+\cdots+c_k+1}}{2^{n-2}}\right\}+\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{2}+\frac{1}{2}\cdot\frac{(-1)^{c_1+c_2+\cdots+c_{k+1}+1}}{2^{n-1}},$$

据(3)式有$S_{(f)}(w)=\frac{(-1)^{c_1+c_2+\cdots+c_{k+1}+1}}{2^{n-1}}$，可见对任一正整数k≥1，引理1都成立.

引理2　设布尔函数f(x), x∈$GF^n(2)$的小项表示形如(6)式，w∈$GF^n(2)$的Hamming重量W(w)=k, 1≤k≤n，w中不为0的分量是$w_{i_1}, w_{i_2}, \cdots, w_{i_k}$，则对此w, 相应的Walsh谱为

$$S_{(f)}(w)=\sum_{j=1}^{W(f)}\frac{(-1)^{c_1^{(j)}+\cdots+c_k^{(j)}+1}}{2^{n-1}}.$$

(8)

证　由文献［3］知：当w≠0时，$S_{(f_1+f_2)}(w)=S_{(f_1)}(w)+S_{(f_2)}(w)-2S_{(f_1\cdot f_2)}(w)$，注意到对任意x∈$GF^n(2)$, $f_1(x)\cdot f_2(x)\equiv 0$, 故$S_{(f_1\cdot f_2)}(w)=\frac{1}{2^n}\sum_{x\in GF^n(2)}(-1)^{wx}=0$, 从而，$S_{(f_1+f_2)}(w)=S_{(f_1)}(w)+S_{(f_2)}(w)$. 再用归纳法不难证明对一般的正整数m>2, w≠0时，有$S_{(f_1+\cdots+f_m)}(w)=S_{(f_1)}(w)+\cdots+S_{(f_m)}(w)$，故据引理1知引理2成立.

注　引理1和引理2揭示了单项式布尔函数和一般布尔函数的谱的性质，其结论和方法都具有普遍意义，如据此还可以得到相关免疫函数和部分Bent函数的矩阵刻画，进一步，凡性质能用Walsh谱刻画的布尔函数，都能由引理1、引理2得到其特征矩阵的等价刻画：在多值逻辑函数情形，也可以用类似的思想和方法研究Chrestenson谱的性质.

定义2[〖STBZ 2〗] 设f(x),x∈GF^n(2)是布尔函数，若对任意w∈GF^n(2),都有$|S_{(f)}(w)|=2^{-\frac{n}{2}}$,则称f(x)为Bent函数.

定理1 设布尔函数f(x),x∈GF^n(2)的小项表示形如(6)式，则f(x)是Bent函数的充要条件是$W(f)=2^{n-1}\pm 2^{\frac{n}{2}-1}$,且对任意w∈GF^n(2),W(w)=k,1≤k≤n,设w中不为0的分量是$w_{i_1},w_{i_2},\cdots,w_{i_k}$,则有

$$\sum_{j=1}^{W(f)}(-1)^{c_{i_1}^{(j)}+\cdots+c_{i_k}^{(j)}}=\pm 2^{\frac{n}{2}-1}. \tag{9}$$

证 必要性 设f(x)是Bent函数，则由(4)式和定义2知

$$P\{f(X)=1\}=\frac{1}{2}(1-S_{(f)}(0))=\frac{1}{2}\left(1\pm 2^{-\frac{n}{2}}\right).$$

故

$$W(f)=2^n\cdot P\{f(X)=1\}=2^{n-1}\pm 2^{(n)/(2)-1},$$

且对任意w∈GF^n(2),W(w)=k,1≤k≤n,设w中不为0的分量是$w_{i_1},w_{i_2},\cdots,w_{i_k}$,则据(8)式及定义2，有

$\sum_{j=1}^{W(f)}\frac{(-1)^{c_{i_1}^{(j)}+\cdots+c_{i_k}^{(j)}+1}}{2^{n-1}}=\pm 2^{-\frac{n}{2}}$,即$\sum_{j=1}^{W(f)}(-1)^{c_{i_1}^{(j)}+\cdots+c_{i_k}^{(j)}}=\pm 2^{\frac{n}{2}-1}$.

充分性 由$W(f)=2^{n-1}\pm 2^{\frac{n}{2}-1}$知$P\{f(X)=1\}=\frac{W(f)}{2^n}=\frac{1}{2}\pm\frac{1}{2\cdot 2^{\frac{n}{2}}}$,故由(4)式得$S_{(f)}(0)=\pm 2^{-\frac{n}{2}}$,又由(8),(9)式知：对任意w∈GF^n(2),w≠0，都有$S_{(f)}(w)=\pm 2^{-\frac{n}{2}}$,所以，据定义2有f(x)是Bent函数.

§3 Bent函数的一般构造法

设布尔函数f(x),x∈GF^n(2)的小项表示形如(6)式，则称矩阵$c_f=\begin{bmatrix} c_1^{(1)} & \cdots & c_n^{(1)} \\ \vdots & & \\ c_1^{(k)} & \cdots & c_n^{(k)} \end{bmatrix}$为f(x)的特征矩阵，其中,k=W(f).显然，矩阵c_f中行向量互不相同，且改变矩阵c_f的行序，其对应的函数不变，但若改变矩阵c_f的列序，则得到不同的函数.将定理1用特征矩阵的语言叙述，则有

定理2 设布尔函数f(x),x∈GF^n(2)的小项表示形如(6)式，其特征矩阵为c_f，则f(x)是Bent函数的充要条件是矩阵c_f有$2^{n-1}\pm 2^{\frac{n}{2}-1}$行，且其中各列向量的非零线性组合中0，1个数之差为$\pm 2^{\frac{n}{2}-1}$.

称满足定理2条件的矩阵c_f为n阶Bent矩阵.由定理2知n元Bent函数和n阶Bent矩阵相互唯一确定，故定理2原则上为解决Bent函数的一般构造和计数问题提供了一个模型.如当n=2时，设f(x)为二元布尔函数，不妨设W(f)=1(此时，W(f+1)=3)，在特征矩阵$c_f=c^{(1)}{}_1,\ c^{(1)}{}_2$中，$(c^{(1)}{}_1,c^{(1)}{}_2)$的不同取法共有$C^1{}_4=4$种，经验证，任一种取法都满足定理2，故特征矩阵$c_f$所对应的布尔函数是Bent函数，这样，4个不同的$c_f$就对应4个不同的Bent函数，而当f(x)是Bent函数时，f(x)+1也是Bent函数，所以，二元Bent函数共有2×4=8个.

以下我们考察Bent矩阵的性质，同时给出一些由已知Bent函数构造新的Bent函数的方法.

定理3 设$A=(\alpha_1,\cdots,\alpha_n)=(a_{ij})_{k\times n}$是Bent矩阵，其中$k=2^{n-1}\pm 2^{\frac{n}{2}-1}$,$a_{ij}\in$GF(2)，i=1,…,k,j=1,

…,n,又设M=$(m_{ij})_{n\times n}$是n阶非奇异矩阵，$m_{ij}\in GF(2)$,i,j=1,2,…,n,V=$\begin{pmatrix} v_1 & \cdots & v_n \\ v_1 & \cdots & v_n \\ \vdots & & \\ v_1 & \cdots & v_n \end{pmatrix}=(\bar{v}_1,\cdots,\bar{v}_n)_{n\times n}$,$v_1,\cdots,v_n\in GF(2)$，则B=AM+V也是Bent矩阵.

证　先验证B中没有相同的行向量.B=AM+V$\left(\sum_{j=1}^{n}a_{ij}m_{jl}+v_l\right)_{k\times n}$,i=1,…,k,l=1,…,n,若B中第$i_1$行和第$i_2$行相同，$i_1\neq i_2$，则有

$$(a_{i_11}+a_{i_21},\cdots,a_{i_1n}+a_{i_2n})\begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & & \\ m_{n1} & \cdots & m_{nn} \end{pmatrix}=0.$$

由$M=(m_{ij})_{n\times n}$是可逆矩阵，$m_{ij}\in GF(2)$,i,j=1,…,n知$(a_{i_11}\cdots,a_{i_1n})=(a_{i_21}\cdots,a_{i_2n})$,这与A是Bent矩阵矛盾，所以，B中没有相同行.即B的行数与A的行数相同，也是$2^{n-1}\pm 2^{\frac{n}{2}-1}$，且其行向量都不相同.

再看B的列向量非零线性组合中0，1个数之差.设$A=(\alpha_1,\cdots,\alpha_n)$,$B=(\beta_1,\cdots,\beta_n)$,则$\beta_1=\sum_{j=1}^{n}m_{j1}\alpha_j+\bar{v}_1$.任取$w=(w_1,\cdots,w_n)\in GF^n(2)\setminus\{0\}$，有

$$\sum_{l=1}^{n}w_l\beta_l=\sum_{l=1}^{n}w_l\left(\sum_{j=1}^{n}m_{jl}\alpha_j+\bar{v}_l\right)=\sum_{j=1}^{n}\left(\sum_{l=1}^{n}w_lm_{jl}\right)\alpha_j+\sum_{l=1}^{n}w_l\bar{v}_l,$$

因为$A=(\alpha_1,\cdots,\alpha_n)$是Bent矩阵，$M=(m_{ij})_{n\times n}$是非奇异矩阵，且$w=(w_1,\cdots,w_n)\neq 0$,所以，$\sum_{j=1}^{n}\left(\sum_{l=1}^{n}w_lm_{jl}\right)\cdot\alpha_j$是$\alpha_1,\cdots,\alpha_n$的非零线性和，其中0，1个数之差为$\pm 2^{\frac{n}{2}-1}$,故$\sum_{j=1}^{n}\left(\sum_{l=1}^{n}w_lm_{jl}\right)\cdot\alpha_j+\sum_{l=1}^{n}w_l\bar{v}_l$中0，1个数之差也为$\pm 2^{\frac{n}{2}-1}$,即$\sum_{l=1}^{n}w_l\beta_l$中0，1个数之差为$\pm 2^{\frac{n}{2}-1}$,由定理2知B是Bent矩阵.

注　由Bent矩阵和Bent函数的定义可以证明定理3与文献[2]中有关Bent函数的一个经典结论等价，即：如果f(x)是n元Bent函数，M是GF(2)上的n阶非奇异矩阵，v是GF(2)上的n维向量，则f(xM+v)也是Bent函数.

特别地，当M=I是单位矩阵时，$B=A+V=(\alpha_1+\bar{v}_1,\cdots,\alpha_n+\bar{v}_n)$，当$\bar{v}_i=0$时，$\alpha_i+\bar{v}_i=\alpha_i$,当$\bar{v}_i=1$时，$\alpha_i+\bar{v}_i=\begin{pmatrix} a_{1i}+1 \\ \vdots \\ a_{ni}+1 \end{pmatrix}$,即第i列的各元素相反，故由定理3知有

推论1　设$A=(\alpha_1,\cdots,\alpha_n)$是Bent矩阵，A中任意1个列向量的各分量取补后得到矩阵B，$1\leqslant 1\leqslant n$,则B也是Bent矩阵.

由定理2我们可以作n元Bent函数的全部构造，而推论1则可以使这种构造得以简化.如在n=4时，$W(f)=2^{n-1}\pm 2^{\frac{n}{2}-1}=10$或6，所以，只要找到所有不同的6×4阶Bent矩阵(不考虑行序)，就可构造全部4元Bent函数.根据推论1不妨设要找的6×4阶矩阵的各列都由两个0和4个1组成，不难验证这样的矩阵共有28个，故由推论1得到满足定理2条件的不同的6×4阶矩阵共有$2^4\times 28=448$个，而当f(x)是Bent函数时，f(x)+1也是Bent函数，且W(f(x)+1)=10≠W(f(x)),所以，4元Bent函数的总数为448×2=896个，经上机搜索验证，这个结果正确.

在定理3中取V=0，则有B=AM是Bent矩阵，其中，M是非奇异矩阵.设L(A)为由A的列向量$\alpha_1,\cdots,\alpha_n$生成的$GF^k(2)$上的线性子空间，$k=2^{n-1}\pm 2^{\frac{n}{2}-1}$，$\beta_1,\cdots,\beta_n$是L(A)中任一极大无关组，则由线性代数理论知有n阶非奇异0，1矩阵M，使$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)M$,故由定理3即有

推论2　设$A=(\alpha_1,\cdots,\alpha_n)_{k\times n}$是Bent矩阵，$k=2^{n-1}\pm 2^{\frac{n}{2}-1}$，记$\alpha_1,\cdots,\alpha_n$生成$GF^k(2)$上的线性子空间为$L(A)$，若$\beta_1,\cdots,\beta_n$是$L(A)$中任一极大无关组，则$B=(\beta_1,\cdots,\beta_n)$是Bent矩阵.

由推论2我们可以通过分析子空间中极大无关组的个数来计算n元Bent函数的个数.如n=4时，4元Bent函数对应的特征矩阵为6×4阶或10×4阶，我们现在计算满足定理2条件的6×4阶矩阵个数.在向量空间$GF^6(2)$中，所有Hamming重量为偶数的向量组成了$GF^6(2)$的一个5维线性子空间$\underline{S}$，不难验证其中不含全1向量的不同的4维子空间共有16个，在每个这样的子空间中，任意向量的非零线性组合都由全0或两个0四个1或两个1四个0组成，故由定理2及推论2知其任一极大无关组组成的矩阵都对应一个Bent函数，而其不同的极大无关组有$n_1=(2^4-1)(2^4-2)(2^4-4)(2^4-8)$个，且特征矩阵的行序不影响其所对应的函数，所以，Hamming重量为6的不同的Bent函数共有$\frac{16\cdot n_1}{6!}$=448个，因而不同的4元Bent函数共有2×448=896个.

事实上，用文献[6]中的典型方法可以具体写出所有4元Bent函数.设

$$f(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4+(ax_1+bx_2)(cx_3+dx_4)+\sum_{i=1}^{4}w_ix_i+v,$$

$$f_1(x_1,x_2,x_3,x_4)=x_1x_3+x_2x_4+(ax_1+bx_3)(cx_2+dx_4)+\sum_{i=1}^{4}w_ix_i+v,$$

$$f_2(x_1,x_2,x_3,x_4)=x_1x_4+x_2x_3+(ax_1+bx_4)(cx_2+dx_3)+\sum_{i=1}^{4}w_ix_i+v,$$

其中,$a,b,c,d,v,w_i\in GF(2)$, i=1,2,3,4,则不难验证上述函数$f(x_1,x_2,x_3,x_4)$，$f_1(x_1,x_2,x_3,x_4)$和$f_2(x_1,x_2,x_3,x_4)$实际上表示了所有896个不同的4元Bent函数.

§4　结束语

自从70年代中期提出Bent函数以来，人们用多种方法对其作了大量研究，如有用Hadamard矩阵研究其性质和构造的[7,8]，有用Fourier变换研究的[2, 9]，也有用Walsh谱方法对Bent函数加以研究的[3]，本文则用特征矩阵揭示了Bent函数的结构，得到了Bent函数的一般构造法，从我们的研究结果看，当变元个数较大时，用特征矩阵研究Bent函数的构造不很方便，但从理论上一般性地探讨Bent函数的计数问题则有其独到之处，类似于特征矩阵在相关免疫函数的计数中所发挥的作用[3,10]，我们相信特征矩阵在Bent函数的计数中也将发挥重要作用.

衷心感谢俞佳恩教授对本文工作的支持和帮助.

作者单位：武昌吴家湾特一号(甲)　邮编 430074
郑州信息工程学院应用数学系

参考文献

1　丁存生，肖国镇，单炜娟，The Stability Theory of Stream Ciphers,Heidelberg:Springer,1991.
2　Rothaus,O.S.,On“Bent”functions,J.Combin.Theory Ser.A.,1976,20:300～305.
3　丁存生，肖国镇，流密码学及其应用，国防工业出版社，北京，1994，25～27,136～142,163～169.
4　杨义先，林须端，编码密码学，人民邮电出版社，北京，1992，203～231.
5　李世取，曾本胜，多值逻辑函数相关免疫的充要条件，密码学进展—Chinacrypt　94,科学出版社，北京，1994，257～264.
6　曾本胜，李世取，李坤，一类布尔函数Walsh谱的分解式及其应用，密码学进展—Chinacrypt　98,科学出版社，北京，1998，257～264.
7　Adams,C.M.,Tavares,S.E.,Generating and counting binary bent sequences,IEEE Trans.Inform.Theory,1990,36(5):1170～1173.
8　Seberry,J.,Zhang,X.M.,Zheng,Y.,Nonlinearily balanced Boolean functions and their propagation characteristics,Advances in Cryptology-Crypt　93,Springer,1994,49～60.
9　Chee Seongtaek,Lee Sangjin,Kim Kwangjo,Semi-bent functions,Advances in Cryptology-Asiacrypt　94,Springer,1995,107～118.
10　温巧燕，肖国镇，2阶相关免疫函数的构造与计数，通信学报，1998，19(8)：39～44.

收稿：1998-11-24.修回：1999-01-27.