Plateaued 函数的密码学性质

胡 斌　金晨辉　冯春海
(解放军信息工程大学电子技术学院　郑州　450004)

摘　要：Plateaued 函数是包含 Bent 函数和部分 Bent 函数的更大函数类，是一类密码学性质优良的密码函数，在非线性组合函数的设计中有重要的应用。该文以 Walsh 谱和自相关系数为工具，从密码函数的角度证明了 r 阶 Plateaued 函数的全体线性结构构成的子空间维数的上界为 $n-r$，且等号成立当且仅当 $f(x)$ 为部分 Bent 函数，同时还给出了 Plateaued 函数的其他一些密码学性质。

关键词：密码函数；Bent 函数；部分 Bent 函数；Plateaued 函数
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2008)03-0660-05

Cryptographic Properties of Plateaued Functions

Hu Bin　Jin Chen-hui　Feng Chun-hai
(*Electronic Technology Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: Plateaued functions include Bent functions and partially bent functions, but are wider than them. They have good cryptographic properties, and are important in the design of nonlinear combining functions. This paper proves some properties of Plateaued functions with Walsh spectrum and auto-correlation coefficient, and presents some other properties of Plateaued functions.

Key words: Cryptographic function; Bent functions; Partially Bent functions; Plateaued functions

1　引言

在密码函数的设计中，总是希望其能满足多个非线性准则，但是有的非线性准则之间存在着一定的制约关系，因此要设计出兼顾各种性质的非线性密码函数有一定的难度。如密码函数的非线性度是一个重要的非线性准则，非线性度达到最大的函数是 Bent 函数，Bent 函数对任意的非零向量均满足扩散性准则。但 Bent 函数又有其明显的弱点，如它不是平衡的，不满足相关免疫性，只能是偶数维函数，而且所有非仿射的部分Bent函数都可以通过Bent函数来构造[1]等。为弥补 Bent 函数的这一不足，1992 年 Carlet 提出了部分 Bent 函数[2]，Bent 函数是部分 Bent 函数的子集。部分 Bent 函数也具有很高的非线性度，而且可以具有平衡性、相关免疫性和一定的扩散性。但是，除了为 Bent 函数的那部分外，部分 Bent 函数都有非零的线性结构，而这通常是在密码学上不希望具有的一个性质。1994 年，Chee 等通过将一个 Bent 函数和一个与其仿射等价的另一个 Bent 函数进行链接而得到一类新的函数，即半 Bent 函数[3,4]。n 维半 Bent 函数是平衡的，具有很好的非线性度，并且满足 $n-1$ 次扩散准则，但其只能是奇数维的，实用性受到很大限制。2001 年，Zheng 等在文献[5]中提出了 Plateaued 函数，该函数是包含 Bent 函数和部分 Bent 函数的更大函数类。它具有很好的非线性度，可以满足相关免疫性、平衡性。而且可以不具有非零的线性结构，是一类密码学性质优良的密码函数，在密码学上有重要的应用，如一种可变长的杂凑算法 HAVAL 中所选择的密码函数均是七元一阶 Plateaued 函数[1]。因此，对其进行深入研究，掌握其基本的密码学特性及构造方法等问题在密码学上均具有重要意义。文献[5]对 Plateaued 函数的一些密码学性质进行了初步的研究，如非线性度、代数次数、线性维数等，得出了一些结论。并给出了 Plateaued 函数的一种构造方法。滕吉红给出了 Plateaued 函数的矩阵表示形式的一些性质，讨论了其构造方法及应用[6,7]。本文在文献[5]讨论的基础上进一步对其密码学性质进行了探讨，以 Walsh 谱和自相关系数为工具，证明了 Plateaued 函数的一些性质。

2007-01-19 收到，2007-07-19 改回

2　基本定义

定义 1[8]　设 $x=(x_1,x_2,\cdots,x_n)$，$w=(w_1,w_2,\cdots,w_n)\in F_2^n$，$x$ 和 w 的点积定义为 $w\cdot x=w_1x_1+w_2x_2+\cdots+w_nx_n$，$n$ 个变元的布尔函数 $f(x)$ 的循环 Walsh 谱定义为

$$S_{(f)}(w)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(x)+w\cdot x}$$

定义 2[8]　设 $f(x):F_2^n\to F_2$，$a\in F_2^n$，如果对一切 $x\in F_2^n$，都有

$$f(x+a)-f(x)=f(a)-f(0)$$

则称 a 为 $f(x)$ 的一个线性结构。

令 $f(x)$ 的全体线性结构所构成的集合为 U_f，则 U_f 为 F_2^n 的一个线性子空间，再令

$$U_f^{(0)}=\{a\in F_2^n \mid f(x+a)-f(x)=0,\text{对一切}x\in F_2^n\}$$

$$U_f^{(1)}=\{a\in F_2^n \mid f(x+a)-f(x)=1,\text{对一切}x\in F_2^n\}$$

显然，$U_f=U_f^{(0)}\cup U_f^{(1)}$，且$U_f^{(0)}$为$U_f$的一个子空间，我们称$U_f^{(0)}$中的元素为$f(x)$的不变线性结构，$U_f^{(1)}$中的元素为$f(x)$的恒变线性结构。称线性子空间$U_f$的维数为$f(x)$的线性维数。

定义 3[8]　设$f(x):F_2^n\to F_2$，称$r_f(\alpha)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(x)+f(x+\alpha)}$为$f(x)$在$\alpha$点的自相关系数。

记$\Im_f=\{\alpha\in F_2^n:S_{(f)}(\alpha)\neq 0\}$，$\Re_f=\{\alpha\in F_2^n:r_f(\alpha)\neq 0\}$

定义 4[8]　设$f(x):F_2^n\to F_2$，如果对任意的$\alpha\in F_2^n$，均有 $|S_{(f)}(\alpha)|=2^{-n/2}$，则称$f(x)$为 Bent 函数。

定义 5[2]　设$f(x):F_2^n\to F_2$，如果$(\#\Im_f)(\#\Re_f)=2^n$，则称$f(x)$为部分 Bent 函数。其中$\#S$表示集合S中点的个数。

由于对于任意的 Bent 函数，$\#\Im_f=2^n$，$\#\Re_f=1$，故$(\#\Im_f)(\#\Re_f)=2^n$，所以 Bent 函数是部分 Bent 函数的子集。

定义 6[4]　设$f_1(x),f_2(x):F_2^n\to F_2$均是 Bent 函数($n$为偶数)，若$S_{(f_1)}(0)+S_{(f_2)}(0)=0$，则称$n+1$元函数

$$g(x,x_{n+1})=x_{n+1}f_1(x)+(x_{n+1}+1)f_2(x)$$

为半 Bent 函数。其中$x\in F_2^n, x_{n+1}\in F_2$。由定义知，半 Bent 函数是奇数元函数。

3　Plateaued 函数的密码学性质

定义 7[5]　设$f(x):F_2^n\to F_2$，如果存在一个偶数r，使得$\#\{w\in F_2^n \mid S_{(f)}(w)\neq 0\}=2^r$且对任意的$w\in F_2^n, S_{(f)}\cdot(w)=0$或$\pm 2^{-r/2}$，则称$f(x)$为$r$阶 Plateaued 函数。

由定义 7 及部分 Bent 函数的谱特征知[9]，部分 Bent 函数是 Plateaued 函数的子集，当n为奇数时，半 Bent 函数是$n-1$阶的n元 Plateaued 函数。因此，Plateaued 函数是比部分 Bent 函数和半 Bent 函数范围更广的一类函数。

文献[5]中对 Plateaued 函数的性质进行了初步研究，给出了其非线性度和代数次数的上界。

引理 1[5]　设$f(x)$为r阶 Plateaued 函数，则其非线性度$N_f=2^{n-1}-2^{n-r/2-1}$。

引理 2[5]　设$f(x)$为r阶 Plateaued 函数，则其代数次数不超过$\frac{r}{2}+1$。

引理 3[5]　设$f(x)$为r阶 Plateaued 函数，$\boldsymbol{A}$为一非奇异矩阵，则$f(\boldsymbol{A}x+b)$也为一r阶 Plateaued 函数。

文献[5]中还给出了关于r阶 Plateaued 函数的全体线性结构构成的子空间维数的上界，并利用了函数序列的性质给出了证明。本文以 Walsh 谱和自相关系数为工具，从一般的函数结构角度对该性质进行详细的证明。为证明该结论，首先给出以下几个引理。

引理 4　设$f(x)$是n元布尔函数，双射$\varphi(x)$是仿射变换，则α是$f(\varphi(x))$的线性结构的充要条件是$\varphi(\alpha)+\varphi(0)$是$f(x)$的线性结构。且$\alpha$是$f(\varphi(x))$的不变线性结构当且仅当$\varphi(\alpha)+\varphi(0)$是$f(x)$的不变线性结构。

引理 5　设$f(x)$为F_2^n上的n元布尔函数，$f(x)$的全体线性结构构成的子空间的维数为k，则必存在一个线性双射φ和F_2^{n-k}上的一个$n-k$元布尔函数$g_1(x)$，使得

$$g(x)=f(\varphi(x))=g_1(x_1,x_2,\cdots,x_{n-k})+cx_{n-k+1} \tag{1}$$

且当$f(x)$存在恒变线性结构时，c=1；当$f(x)$不存在恒变线性结构时，c=0。

证明　由于$f(x)$的线性维数为k，故不妨设存在$f(x)$的一个恒变线性结构α_1及$f(x)$的$k-1$个不变线性结构$\alpha_2,\cdots,\alpha_k$，使得$\alpha_1,\alpha_2,\cdots,\alpha_k$线性无关。作一个$n$维线性双射$\varphi$，使得

$$\varphi(e_i)=\begin{cases}e_i, & i\le n-k\\ \alpha_{i-(n-k)}, & i>n-k\end{cases} \tag{2}$$

其中e_i是第i维分量为 1，其他维分量为 0 的n维向量，$1\le i\le n$。

当$i>n-k$时，$\varphi(e_i)$是$f(x)$的线性结构，从而由引理 4 知$e_{n-k+1},\cdots,e_n$是$f(\varphi(x))$的线性结构，且$e_{n-k+2},\cdots,e_n$还是$f(\varphi(x))$的不变线性结构。令

$$c=f(\alpha_1)+f(0),\quad h(x_1,\cdots,x_n)=f(\varphi(x))+cx_{n-k+1} \tag{3}$$

则$e_{n-k+1},\cdots,e_n$是$h(x)$的不变线性结构，故有$h(x_1,\cdots,x_n)=h(x_1,\cdots,x_{n-k},0,\cdots,0)$，记$g_1(x_1,\cdots,x_{n-k})=h\cdot(x_1,\cdots,x_{n-k},0,\cdots,0)$，则有

$$f(\varphi(x))=g_1(x_1,\cdots,x_{n-k})+cx_{n-k+1} \tag{4}$$

且$c=0$当且仅当α_1是$f(x)$的不变线性结构。

引理 6　设$f(x)$为F_2^n上的n元布尔函数，$r<n$，则

(1)如果存在F_2^r上的一个布尔函数$g(x_1,x_2,\cdots x_r)$，使得$f(x)=g(x_1,x_2,\cdots x_r)$，则对任意的$\alpha\in F_2^r$，有

$$S_{(f)}(\alpha,\beta)=\begin{cases}0, & \beta\neq 0\\ S_{(g)}(\alpha), & \beta=0\end{cases} \tag{5}$$

(2)如果存在F_2^r上的一个布尔函数$g(x_1,x_2,\cdots x_r)$，使得$f(x)=g(x_1,x_2,\cdots x_r)+x_{r+1}$，则对任意的$\alpha\in F_2^r$，$\beta\in F_2^{n-r-1}$，有

$$S_{(f)}(\alpha,0,\beta)=0,\ S_{(f)}(\alpha,1,\beta)=\begin{cases}0, & \beta\neq 0\\ S_{(g)}(\alpha), & \beta=0\end{cases} \tag{6}$$

证明　(1)设$x=(x',x'')=((x_1,x_2,\cdots x_r),(x_{r+1},x_{r+2},\cdots x_n))$，于是对任意的$\alpha\in F_2^r$，$\beta\in F_2^{n-r}$，有

$$S_{(f)}(\alpha,\beta)=\frac{1}{2^n}\sum_{x'}\sum_{x''}(-1)^{g(x')+\alpha x'+\beta x''}$$
$$=\frac{1}{2^n}\sum_{x'}(-1)^{g(x')+\alpha x'}\sum_{x''}(-1)^{\beta x''}$$
$$=\begin{cases}0, & \beta\neq 0\\ S_{(g)}(\alpha), & \beta=0\end{cases}$$

(2)设 $x=(y,z,z')=((x_1,x_2,\cdots,x_r),x_{r+1},(x_{r+2},x_{r+3},\cdots,x_n))$，于是对任意的 $\alpha\in F_2^r$，$\beta\in F_2^{n-r-1}$，有

$$S_{(f)}(\alpha,0,\beta)=\frac{1}{2^n}\sum_{y}\sum_{z}\sum_{z'}(-1)^{g(y)+\alpha y+z+\beta z'}$$
$$=\frac{1}{2^n}\sum_{y}(-1)^{g(y)+\alpha y}\sum_{z}(-1)^{z}\sum_{z'}(-1)^{\beta z'}=0$$
$$S_{(f)}(\alpha,1,\beta)=\frac{1}{2^n}\sum_{y}\sum_{z}\sum_{z'}(-1)^{g(y)+\alpha y+\beta z'}$$
$$=\frac{1}{2^{n-1}}\sum_{y}(-1)^{g(y)+\alpha y}\sum_{z'}(-1)^{\beta z'}$$
$$=\begin{cases}0, & \beta\neq 0\\ S_{(g)}(\alpha), & \beta=0\end{cases}$$

引理 7 设 $f(x)$ 为 F_2^n 上的 n 元布尔函数

(1)设 φ 为一个线性双射，$g(x)=f(\varphi(x))$，$\alpha\in F_2^n$，则 $r_g(\alpha)=r_f(\varphi(\alpha))$

(2)如果存在 F_2^r 上的一个布尔函数 $g(x_1,x_2,\cdots x_r)$，使得 $f(x)=g(x_1,x_2,\cdots x_r)$，则对任意的 $\alpha\in F_2^r$，$\beta\in F_2^{n-r}$，有 $r_f(\alpha,\beta)=r_g(\alpha)$；

(3)如果存在 F_2^r 上的一个布尔函数 $g(x_1,x_2,\cdots x_r)$，使得 $f(x)=g(x_1,x_2,\cdots x_r)+x_{r+1}$，则对任意的 $\alpha\in F_2^r$，$\beta\in F_2^{n-r-1}$，有 $r_f(\alpha,0,\beta)=r_g(\alpha)$，$r_f(\alpha,1,\beta)=-r_g(\alpha)$。

证明 (1)由于 φ 为一个线性双射，故由定义知：

$$r_g(\alpha)=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{g(x)+g(x+\alpha)}=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(\phi(x))+f(\phi(x+\alpha))}$$
$$=\frac{1}{2^n}\sum_{y\in F_2^n}(-1)^{f(y)+f(y+\phi(\alpha))}=r_f(\phi(\alpha))$$

(2)设 $x=(y,z),y\in F_2^r,z\in F_2^{n-r}$，则对任意的 $\alpha\in F_2^r$，$\beta\in F_2^{n-r}$，有

$$r_f(\alpha,\beta)=\frac{1}{2^n}\sum_{y}\sum_{z}(-1)^{g(y)+g(y+\alpha)}$$
$$=\frac{1}{2^r}\sum_{y}(-1)^{g(y)+g(y+\alpha)}=r_g(\alpha)$$

(3)设 $x=(y,t,z)$，$y\in F_2^r,t\in F_2,z\in F_2^{n-r-1}$，则对任意的 $\alpha\in F_2^r$，$\beta\in F_2^{n-r-1}$，有

$$r_f(\alpha,0,\beta)=\frac{1}{2^n}\sum_{y}\sum_{t}\sum_{z}(-1)^{g(y)+g(y+\alpha)}$$
$$=\frac{1}{2^r}\sum_{y}(-1)^{g(y)+g(y+\alpha)}=r_g(\alpha)$$
$$r_f(\alpha,1,\beta)=\frac{1}{2^n}\sum_{y}\sum_{t}\sum_{z}(-1)^{g(y)+g(y+\alpha)+1}$$
$$=\frac{1}{2^r}\sum_{y}(-1)^{g(y)+g(y+\alpha)+1}=-r_g(\alpha)$$

定理 1 设 $f(x)$ 为 F_2^n 上的 r 阶 Plateaued 函数，$f(x)$ 的全体线性结构构成的子空间的维数为 k，则有 $k\le n-r$，其中等号成立当且仅当 $f(x)$ 为部分 Bent 函数。

证明 由于 $f(x)$ 的线性维数为 k，故由引理 5 知，必存在一个线性双射 φ 和 F_2^{n-k} 上的一个 $n-k$ 元布尔函数 $g_1(x)$，使得：

$$g(x)=f(\varphi(x))=g_1(x_1,x_2,\cdots,x_{n-k})+cx_{n-k+1}\qquad(7)$$

由于 $f(x)$ 为 r 阶 Plateaued 函数，而 φ 为一线性变换，由于 Walsh 谱值经过线性变换只是改变了其分布，而值不变，故 $g(x)$ 仍为 r 阶 Plateaued 函数。

当 $c=0$ 时，此时 $g_1(x_1,x_2,\cdots,x_{n-k})=g(x_1,x_2,\cdots,x_n)$，由引理 6，对任意的 $\alpha\in F_2^{n-k}$，有

$S_{(g_1)}(\alpha)=S_{(g)}(\alpha\underbrace{0\cdots0}_{k})$，于是 $\max_{\alpha}|S_{(g_1)}(\alpha)|=\max_{\alpha}|S_{(g)}(\alpha\underbrace{0\cdots0}_{k})|=2^{-r/2}$，由于 $g_1(x)$ 的最大 Walsh 谱值的下界为 $2^{-(n-k)/2}$，因此 $2^{-r/2}\ge 2^{-(n-k)/2}$，于是可得 $k\le n-r$。

当 $c=1$ 时，此时 $g(x)=g_1(x_1,x_2,\cdots,x_{n-k})+x_{n-k+1}$，由引理 6，对任意的 $\alpha\in F_2^{n-k}$，有

$S_{(g)}(\alpha,1,\underbrace{0\cdots0}_{k-1})=S_{(g_1)}(\alpha)$，于是，$\max_{\alpha}|S_{(g_1)}(\alpha)|=|S_{(g)}(\alpha,1,\underbrace{0\cdots0}_{k-1})|=2^{-r/2}$，由于 $g_1(x)$ 的最大 Walsh 谱值的下界为 $2^{-(n-k)/2}$，因此 $2^{-r/2}\ge 2^{-(n-k)/2}$，于是可得 $k\le n-r$。

由上面的证明可知，当 $r=n-k$ 时，$g_1(x)$ 为 F_2^{n-k} 上的 Bent 函数，如果 $c=0$，此时，$g(x_1,x_2,\cdots,x_n)=g_1(x_1,x_2,\cdots,x_{n-k})$，对任意的 $\gamma=(\alpha,\beta)$，$\alpha\in F_2^{n-k},\beta\in F_2^k$，由引理 6，此时使 $S_{(g)}(\gamma)\neq 0$ 的点的个数为 2^{n-k}，即 $\#\Im_g=2^{n-k}$，由引理 7，$r_g(\alpha,\beta)=r_{g_1}(\alpha)$，由于 $g_1(x)$ 为 F_2^{n-k} 上的 Bent 函数，故 $r_{g_1}(\alpha)\neq 0$ 的点个数只有 1 个，因此使 $r_g(\alpha,\beta)\neq 0$ 的点的个数有 2^k 个，即 $\#\Re_g=2^k$，$(\#\Im_g)(\#\Re_g)=2^{n-k}\cdot 2^k=2^n$，所以 $g(x)$ 为部分 Bent 函数，再由引理 7 的第一部分结论知 $f(x)$ 也为部分 Bent 函数。

如果 $c=1$，此时，$g(x)=g_1(x_1,x_2,\cdots,x_{n-k})+x_{n-k+1}$，由引理 7，对任意的 $\alpha\in F_2^{n-k}$，$\beta\in F_2^{k-1}$，有 $r_g(\alpha,0,\beta)=r_{g_1}(\alpha)$，$r_g(\alpha,1,\beta)=-r_{g_1}(\alpha)$，由于 $g_1(x)$ 为 F_2^{n-k} 上的 Bent 函数，故 $r_{g_1}(\alpha)\neq 0$ 的点个数只有 1 个，因此使 $r_g(\alpha,t,\beta)\neq 0(t\in F_2)$的点的个数有 2^k 个，即 $\#\Re_g=2^k$；又由引理 6，对任意的 $\gamma=(\alpha,t,\beta)$，$\alpha\in F_2^{n-k},t\in F_2,\beta\in F_2^{k-1}$，使得 $S_{(g)}(\gamma)\neq 0$ 的点的个数为 2^{n-k}，即 $\#\Im_g=2^{n-k}$。于是 $(\#\Im_g)(\#\Re_g)=2^{n-k}\cdot 2^k=2^n$，所以 $g(x)$ 为部分 Bent 函数，再由引理 7 的第一部分结论知 $f(x)$ 也为部分 Bent 函数。

若 $f(x)$ 为部分 Bent 函数，则由部分 Bent 函数的谱特征知[9]，其非 0 的谱值为 $|S_{(f)}(\alpha)|=2^{-(n-k)/2}$，显然是一 $n-k$ 阶 Plateaued 函数，即 $r=n-k$。

下面我们给出一个关于 Plateaued 函数的自相关系数的一个性质。

引理 8　设 $f(x)$为F_2^n 上的 n 元布尔函数，则有 $r_f(\alpha)=\sum_{x\in F_2^n} S_{(f)}^2(x)(-1)^{\alpha x}$。

定理 2　设 $f(x)$ 为 r 阶 Plateaued 函数，$r_f(\alpha)$ 为其在 α 点的自相关系数，则有

$$\sum_{\alpha=0}^{2^n-1} r_f^2(\alpha)=2^{n-r} \tag{8}$$

证明　因 $f(x)$ 为 r 阶 Plateaued 函数，故对任意的 $w\in F_2^n, S_{(f)}(w)=0$或 $\pm 2^{-r/2}$，由引理 8 知 $r_f(\alpha)=\sum_{x\in F_2^n} S_{(f)}^2(x)\cdot(-1)^{\alpha x}$，所以有

$$\begin{aligned}\sum_{\alpha=0}^{2^n-1} r_f^2(\alpha)&=\sum_{\alpha=0}^{2^n-1}\sum_{x\in F_2^n} S_{(f)}^2(x)(-1)^{\alpha x}\sum_{y\in F_2^n} S_{(f)}^2(y)(-1)^{\alpha y}\\&=2^{-2r}\sum_{\alpha=0}^{2^n-1}\sum_{x\in F_2^n:S_{(f)}(x)\neq 0}\ \sum_{y\in F_2^n:S_{(f)}(y)\neq 0}(-1)^{\alpha(x+y)}\\&=2^{-2r}\sum_{x:S_{(f)}(x)\neq 0}\ \sum_{y:S_{(f)}(y)\neq 0}\ \sum_{\alpha=0}^{2^n-1}(-1)^{\alpha(x+y)}\\&=2^{n-2r}\sum_{x:S_{(f)}(x)\neq 0}\ \sum_{y:S_{(f)}(y)\neq 0,y=x} 1=2^{n-2r}2^r=2^{n-r}\end{aligned}$$

引理 9　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数，设其非线性度为 N_f，则有

$$N_f/2^{n-1}+1/\sqrt{\#\Im_f}\le 1 \tag{9}$$

其中等号成立当且仅当 $f(x)$ 为 F_2^n 上的 Plateaued 函数。

证明　由于 $N_f=2^{n-1}(1-\max_w|S_{(f)}(w)|)$，$\#\Im_f=\#\{w\in F_2^n: S_{(f)}(w)\neq 0\}$，故由能量守恒定理 $\sum_w S_{(f)}^2(w)=1$，可得：$(\#\Im_f)(\max_w S_{(f)}^2(w))\ge 1$，所以有

$$\begin{aligned}N_f/2^{n-1}+1/\sqrt{\#\Im_f}&=1-\max_w|S_{(f)}(w)|)\\&+1/\sqrt{\#\Im_f}\le(1-\max_w|S_{(f)}(w)|)+\max_w|S_{(f)}(w)|=1\end{aligned}$$

若 $f(x)$ 为 F_2^n 上的 r 阶 Plateaued 函数，则有 $\#\Im_f=2^r$，且 $N_f=2^{n-1}\left(1-2^{-r/2}\right)$，于是有

$$N_f/2^{n-1}+1/\sqrt{\#\Im_f}=1-2^{-r/2}+2^{-r/2}=1$$

反之，若 $N_f/2^{n-1}+1/\sqrt{\#\Im_f}=1$，即 $1-\max_w|S_{(f)}\cdot(w)|)+1/\sqrt{\#\Im_f}=1$，可得

$$(\#\Im_f)(\max_w S_{(f)}^2(w))=1 \tag{10}$$

于是可知 $f(x)$ 在每一个非零点的谱值的绝对值均相等，且设 $\max_w|S_{(f)}(w)|=\frac{k}{2^n}$，即有 $(\#\Im_f)k^2=2^{2n}$，于是 $\#\Im_f$ 的个数必为 2 的方幂，不妨设 $\#\Im_f=2^r$，则可得 $k=2^{n-r/2}$，于是 $f(x)$ 为 F_2^n 上的 r 阶 Plateaued 函数。

推论 1　设 $f(x)$ 为 F_2^n 上的 r 阶 Plateaued 函数，$f(x)$ 的全体线性结构构成的子空间的维数为 k，则有 $N_f/2^{n-1}+1/\sqrt{2^{n-k}}\ge 1$，其中等号成立当且仅当 $f(x)$ 为部分 Bent 函数。

证明　由引理 9 知，$N_f/2^{n-1}+1/\sqrt{\#\Im_f}=1$，$\#\Im_f=2^r$，又由定理 1 知，$r\le n-k$，等号成立当且仅当 $f(x)$ 为部分 Bent 函数，故 $N_f/2^{n-1}+1/\sqrt{2^{n-k}}\ge 1$ 且等号成立当且仅当 $f(x)$ 为部分 Bent 函数。

推论 2　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数，v 为 $f(x)$ 的 Walsh 谱值为 0 的点的个数，则有 $v\le 2^n-\frac{1}{\max_\alpha|S_{(f)}^2(\alpha)|}$，其中等号成立当且仅当 $f(x)$ 为 Plateaued 函数。特别地，当 n 为偶数时，如果 $\max_\alpha|S_{(f)}(\alpha)|\le 2^{-(n-2)/2}$，则有 $v\le 2^{n-1}+2^{n-2}$，等号成立当且仅当 $f(x)$ 为 $n-2$ 阶 Plateaued 函数；当 n 为奇数时，如果 $\max_\alpha|S_{(f)}(\alpha)|\le 2^{-\frac{n-1}{2}}$，则有 $v\le 2^{n-1}$，等号成立当且仅当 $f(x)$ 为 $n-1$ 阶 Plateaued 函数；

证明　由能量守恒定理(Parseval 定理)知：$\sum_\alpha S_{(f)}^2(\alpha)=1$，因而有：$(2^n-v)\max_\alpha S_{(f)}^2(\alpha)\ge 1$，于是可得：$v\le 2^n-\frac{1}{\max_\alpha|S_{(f)}^2(\alpha)|}$，且等号成立当且仅当 $f(x)$ 在所有非 0 点的 Walsh 谱值均相等。

当 n 为偶数时，如果 $\max_\alpha|S_{(f)}(\alpha)|\le 2^{-(n-2)/2}$ 时，有 $v\le 2^n-2^{n-2}=2^{n-1}+2^{n-2}$，且等号成立当且仅当 $f(x)$ 在所有非 0 点的 Walsh 谱值均为 $\pm 2^{-(n-2)/2}$，故 $f(x)$ 为 $n-2$ 阶 Plateaued 函数。当 n 为奇数时，如果 $\max_\alpha|S_{(f)}(\alpha)|\le 2^{-(n-2)/2}$，则有 $v\le 2^n-2^{n-1}=2^{n-1}$。且等号成立当且仅当 $f(x)$ 在所有非 0 点的 Walsh 谱值均为 $\pm 2^{-(n-1)/2}$，故 $f(x)$ 为 $n-1$ 阶 Plateaued 函数。

4　结束语

本文在文献[5]讨论的基础上进一步对 Plateaued 函数的密码学性质进行了探讨，以密码函数中经常使用的 Walsh 谱为工具对，从密码函数的角度证明了 r 阶 Plateaued 函数的全体线性结构构成的子空间维数的上界为 $n-r$，且等号成立当且仅当 $f(x)$ 为部分 Bent 函数，并给出了 Plateaued 函数的另外一些性质。对于 Plateaued 函数，还有许多问题需进一步讨论。如其自相关系数的上界，谱支集的结构等。关于该函数的构造目前已有一些文章进行了讨论[5,6,10]，但构造的方法思路基本一致，深入地研究其他构造方法是很有意义的问题，值得进一步研究和探讨。

参 考 文 献

[1] Li Shi-Qi and Zhao Ya-Qun. The relation between partially-Bent and Bent functions. Proceedings of CCICS'99, Beijing, 1999: 196–201(in Chinese).

[2] Carlet. C. Partially Bent functions. Advance in Cryptology-Crytpo'93, Berlin: Springer–Verlag, 1993: 77–101.

[3] Chee S, Lee S, and Kin K. Semi-Bent functions. Advance in Cryptology-Asiacrytp'94. Berlin: Springer-Verlag, 1995: 107–118.

[4] 秦静, 赵亚群. 半 Bent 函数的密码学特性. 山东大学学报(理学版), 2002, 37(12): 480–483.
Qin Jing and ZhaoYa-qun. The Cryptographic properties of Semi-Bent functions. *Journal of Shandong University* (Natural Science), 2002, 37(12): 480–483.

[5] Zheng Y and Zhang X M. On Plateaued functions. *IEEE Trans. on Information Theory*, 2001, 47(3): 1215–1223.

[6] 滕吉红, 李世取, 刘文芬. k 阶拟 Bent 函数在密码设计和通信中的应用. 通信学报, 2003, 24(12): 58–66.
Teng Ji-hong, Li Shi-qu, and Liu Wen-fen. k order Quasi-Bent function's application in Cryptography and communication. *Journal of Commuications*. 2003, 24(12): 58–66.

[7] 滕吉红, 张文英, 李世取, 黄晓英. 一类 k 阶拟 Bent 函数密码性质的矩阵特征. 计算机学报, 2004, 27(4): 58–66.
Teng Ji-hong, Zhang Wen-ying, Li Shi-qu, and Huang Xiao-ying. The matrix characteristics of the Cryptographic properties of a special kind of k-order Quasi-Bent functions, *Journal of Computers*, 2004, 27(4): 58–66.

[8] 冯登国, 裴定一. 密码学导引. 北京: 科学出版社, 1999, 73–85.
Feng Deng-gou and Pei Ding-yi. Cryptography, published by Science Publishing Company, Beijing，1999: 73–85.

[9] Jin Chenhui. Spectral characteristics of partially-bent functions. CHINACRYPT'94, Xidian, China, 11-15, Nov 1994: 48–51.

[10] Carlet. C and Prouff. E. On plateaued functions and their constructions, FSE'2003, LNCS, 2887: 54–73.

胡 斌： 男，1971 年生，博士生，副教授，研究方向为密码学与信息安全.

金晨辉： 男，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.

冯春海： 男，1964 年生，副教授，研究方向为密码学.