密码学中 3 类具有特殊 Walsh 谱值布尔函数的关系

胡斌，金晨辉，邵增玉
（解放军信息工程大学 电子技术学院，河南 郑州 450004）

摘 要：从函数结构角度对 Bent 函数与 Plateaued 函数、部分 Bent 函数与 Plateaued 函数的关系进行了研究，指出了任意一个 Bent 函数都可拆分成 2 个 Plateaued 函数的链接，而 Plateaued 函数在满足一定条件下也可拆分成 Bent 函数的链接。给出了 $n-1$ 阶 Plateaued 函数具有非零线性结构时与 Bent 函数的特殊关系，讨论了部分 Bent 函数可表示成 2 个 Plateaued 函数链接时的条件。研究结果进一步说明了这 3 类具有特殊 Walsh 谱值密码函数之间有着紧密的内在联系，为密码设计中使用此类函数提供了重要依据。

关键词：Bent 函数；部分 Bent 函数；Plateaued 函数；Walsh 谱
中图分类号：TN918 **文献标识码**：B **文章编号**：1000-436X(2010)07-0104-06

Relationship among three kinds of cryptographic Boolean functions with special Walsh spectrum

HU Bin, JIN Chen-hui, SHAO Zeng-yu
(Electronic Technology Institute, Information Engineering University, Zhengzhou 450004, China)

Abstract: The relationship among Bent functions, partially Bent functions and Plateaued functions was discussed, point out that any Bent functions could be divided into two Plateaued functions, and Plateaued function satisfying certain conditions could also be divided into two Bent functions.Propose the special relation between Plateaued of $n-1$ order with non-zero linear structure and Bent functions, and show that partially Bent functions satisfying certain conditions Could be divided into two Plateaued functions. These results show the close connection among the three cryptographic Boolean functions with special Walsh spectrum, which propose the important basis for designing cipher using these functions.

Key words: Bent functions; partially Bent functions; Plateaued functions; Walsh spectrum

1 引言

Bent 函数是非线性度达到最大的一类布尔函数，Bent 函数的 Walsh 谱只取 2 个值，由于其具有较好的扩散性和极大的非线性度和稳定性，在密码设计和通信领域得到广泛应用。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。为弥补 Bent 函数的这一不足，1992 年 C.Carlet 提出了部分 Bent 函数[1]，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，其 Walsh 谱只取 3 个值。但是，除了 Bent 函数的那部分外，部分 Bent 函数都有非零的线性结构，而在密码学上通常是不希望具有的一个性质。2001 年 Y. Zheng 等在文献[2]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，它的 Walsh 谱也只取 3 个值。

这 3 类密码函数的 Walsh 谱取值均比较特殊，

收稿日期：2008-12-15；修回日期：2010-04-25

即只取 2 个或 3 个值，且均具有较好的非线性度，在密码学中有重要的应用。3 类函数间有紧密的联系，但在这 3 类函数的结构关系研究方面，目前国内外公开的文献中只是给出了初步刻画，如文献[2]中指出了 3 类函数间的包含关系及互相转化条件，指出部分 Bent 函数是线性维数达到最大的 Plateaued 函数，从线性维数方面指出了 2 类函数的结构关系。文献[3]中对部分 Bent 函数和 Plateaued 函数的结构关系进行了进一步刻画，给出了 n 元 Plateaued 函数为 n 元部分 Bent 函数的一个充分必要条件，即若设 H 是 n 元 Plateaued 函数所有非零的 Walsh 谱点集，则 Plateaued 函数是部分 Bent 函数的充分必要条件是存在一个 $t\in F_2^n$，使得 $t+H$ 为 F_2^n 的线性子空间。文献[4]中利用 Walsh 谱进一步对二者的关系进行了研究，给出了 Plateaued 函数为部分 Bent 函数时其非线性度所满足的条件，文献[5]对多输出 Plateaued 函数的性质进行了分析。

以上结果主要是从线性维数与非零谱值点集方面讨论了部分 Bent 函数和 Plateaued 函数的关系，从结构方面仅指出了部分 Bent 函数与 Plateaued 函数三者间的关系。但这些研究结果均是给出了 3 类函数的间的基本结构关系，关于它们之间深入的内在联系目前国内外还没有人进行研究。本文在此基础上进一步对 3 类密码函数的深入关系进行了研究，主要从函数结构角度对 Bent 函数与 Plateaued 函数、部分 Bent 函数与 Plateaued 函数的关系进行了深入分析，指出了任意一个 Bent 函数都可拆分成 2 个 Plateaued 函数的链接，而 Plateaued 函数在满足一定条件下也可拆分成 Bent 函数的链接。给出了 $n-1$ 阶 Plateaued 函数具有非零线性结构时与 Bent 函数的特殊关系，讨论了部分 Bent 函数可表示成 2 个 Plateaued 函数链接时的条件。研究结果进一步说明了这 3 类具有特殊 Walsh 谱值密码函数之间有着紧密的内在联系，为密码设计中使用此类函数提供了重要依据。

2　主要结果

n 个变元的布尔函数 $f(x)$ 是从 F_2^n 到 F_2 的一个函数或映射，记为 $f(x)\colon F_2^n\to F_2$。

定义 1[6]　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[6]　设 $f(x)\colon F_2^n\to F_2$，则称

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

为 $f(x)$ 在 α 点的自相关系数。

定义 3[2]　设 $f(x)\colon F_2^n\to F_2$，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 $w\in F_2^n$，$S_{(f)}(w)=0$或$\pm 2^{\frac{r}{2}}$，则称 $f(x)$ 为 r 阶 Plateaued 函数，其中 $\#\{A\}$ 表示集合 A 的计数。

由定义 3 及部分 Bent 函数的谱特征[7]知，部分 Bent 函数是 Plateaued 函数的子集，因此 Plateaued 函数是比部分 Bent 函数范围更广的一类函数。关于 Bent 函数和部分 Bent 函数的关系较简单，本文主要讨论 Plateaued 函数和 Bent 函数以及 Plateaued 函数和部分 Bent 函数的关系。对于 Plateaued 函数和部分 Bent 函数的关系，现有的主要结果如下[2~4]。

定理 1[2]　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 $k\leqslant n-r$，其中等号成立当且仅当 $f(x)$ 为部分 Bent 函数。

定理 2[3]　设 $f(x)$ 为 F_2^n 上的 r 阶 Plateaued 函数，记 $\Im_f=\{\alpha\in F_2^n: S_{(f)}(\alpha)\neq 0\}$，则 $f(x)$ 为部分 Bent 函数的充要条件是存在 $t\in F_2^n$，使得 $t+\Im_f$ 构成 F_2^n 的子空间。

定理 3[4]　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 $N_f/2^{n-1}+1/\sqrt{2^{n-k}}\geqslant 1$，其中等号成立当且仅当 $f(x)$ 为部分 Bent 函数。

上述 3 个定理从不同角度指出了 Plateaued 函数为部分 Bent 函数的条件，刻画了二者之间存在的一定关系。但其主要是从线性维数或非零谱值点集的性质方面进行刻画，未给出函数的结构方面的联系，也未能指出 Plateaued 函数与 Bent 函数间的明确关系，下面从函数结构角度给出 Plateaued 函数与 Bent 函数和部分 Bent 函数之间的联系。

首先从函数结构角度来刻画 Plateaued 函数与 Bent 函数间的关系。

对于 F_2^n 上的任意布尔函数 $f(x)=f(x_1,\cdots,x_n)$，令 $f_1(x_1,\cdots,x_{n-1})=f(x_1,\cdots,x_{n-1},0)$，$f_2(x_1,\cdots,x_{n-1})=$

$f(x_1,\cdots,x_{n-1},1)$，则有 $f(x_1,\cdots,x_n)=(x_n+1)\ f_1(x_1,\cdots,x_{n-1})+x_nf_2(x_1,\cdots,x_{n-1})$，这种表示实际上是将 $f(x_1,\cdots,x_n)$ 表示成 $f_1(x_1,\cdots,x_{n-1})$ 和 $f_2(x_1,\cdots,x_{n-1})$ 的链接形式。利用此表示形式，可给出 Plateaued 函数与 Bent 函数结构上的关系。

定理 4 设 n 为偶数，$f(x_1,x_2,\cdots,x_n)$ 是 F_2^n 上任意一个 Bent 函数，且可表示成 F_2^{n-1} 上的 2 个 $n-1$ 元布尔函数的链接，即 $f(x_1,x_2,\cdots,x_n)=(x_n+1)f_1(x_1,x_2,\cdots,x_{n-1})+x_nf_2(x_1,x_2,\cdots,x_{n-1})$，则 f_1,f_2 均为 $n-2$ 阶 $n-1$ 元 Plateaued 函数。

证明 考查 $f(x_1,x_2,\cdots,x_n)$ 在任一点 $u=(\alpha,\beta)$ 处的 Walsh 谱值，$\alpha\in F_2^{n-1},\beta\in F_2$，令 $x=(y,x_n)$，其中 $y=(x_1,x_2,\cdots,x_{n-1})$，则有：

$$\begin{aligned}S_{(f)}(u)&=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{f(x)+u\cdot x}\\&=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{(x_n+1)f_1(x_1,x_2,\ldots,x_{n-1})+x_nf_2(x_1,x_2,\ldots,x_{n-1})+u\cdot x}\\&=\frac{1}{2^n}\sum_{y\in F_2^{n-1}}\sum_{x_n\in F_2}(-1)^{(x_n+1)f_1(x_1,x_2,\cdots,x_{n-1})+x_nf_2(x_1,x_2,\cdots,x_{n-1})+u\cdot x}\\&=\frac{1}{2^n}\sum_{y\in F_2^{n-1}}(-1)^{f_1(y)+\alpha\cdot y}+\frac{1}{2^n}\sum_{y\in F_2^{n-1}}(-1)^{f_2(y)+y\cdot\alpha+\beta}\\&=\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)\cdot(-1)^{\beta}\end{aligned}\tag{1}$$

由于 $f(x_1,x_2,\cdots,x_n)$ 为 Bent 函数，故其在任何一点的谱值为 $\pm2^{-\frac{n}{2}}$，因此式（1）的结果有 4 种可能，即：

$$\text{第 1 种：}\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=2^{-\frac{n}{2}}\\\frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=2^{-\frac{n}{2}}\end{cases}$$

$$\text{第 2 种：}\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=2^{-\frac{n}{2}}\\\frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=-2^{-\frac{n}{2}}\end{cases}$$

$$\text{第 3 种：}\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=-2^{-\frac{n}{2}}\\\frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=2^{-\frac{n}{2}}\end{cases}$$

$$\text{第 4 种：}\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=-2^{-\frac{n}{2}}\\\frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=-2^{-\frac{n}{2}}\end{cases}$$

对于第 1 种情形，有 $S_{(f_1)}(\alpha)=2^{-\frac{n}{2}+1}$，$S_{(f_2)}(\alpha)=0$；第 2 种情形，有 $S_{(f_1)}(\alpha)=0$，$S_{(f_2)}(\alpha)=2^{-\frac{n}{2}+1}$；第 3 种情形，有 $S_{(f_1)}(\alpha)=0$，$S_{(f_2)}(\alpha)=-2^{-\frac{n}{2}+1}$；第 4 种情形，有 $S_{(f_1)}(\alpha)=-2^{-\frac{n}{2}+1}$，$S_{(f_2)}(\alpha)=0$。

即对于任意的 $\alpha\in F_2^{n-1}$，总有 $S_{(f_1)}(\alpha)$，$S_{(f_2)}(\alpha)\in\{-2^{-\frac{n}{2}+1},0,2^{-\frac{n}{2}+1}\}$，因此 f_1,f_2 均为 $n-2$ 阶 $n-1$ 元 Plateaued 函数。

定理 4 说明，任意一个 Bent 函数均可表示成 2 个 Plateaued 函数的链接，这从函数结构上刻画了 2 种函数之间的联系。反之，当 Plateaued 函数在满足一定条件时，也可表示成 2 个 Bent 函数的链接。

定理 5 设 $f(x)$ 为 F_2^n 上的 $n-1$ 阶 Plateaued 函数，n 为奇数，且对任意的 $\alpha'=(\alpha_1,\cdots,\alpha_{n-1})\in F_2^{n-1}$，有 $|S_{(f)}(\alpha',0)|\neq|S_{(f)}(\alpha',1)|$，则

1) 设 $f(x)=(1+x_n)g(x_1,\cdots,x_{n-1})+x_nh(x_1,\cdots,x_{n-1})$，则 $g(x_1,\cdots,x_{n-1})$ 和 $h(x_1,\cdots,x_{n-1})$ 均为 $n-1$ 元 Bent 函数。

2) 存在一个 $n-1$ 维子空间 $H\subset F_2^n$，使得对 $\forall\alpha\in H$，$r_f(\alpha)=0$。

证明 1) 设 $\alpha'=(\alpha_1,\cdots,\alpha_{n-1})\in F_2^{n-1}$，$x'=(x_1,\cdots,x_{n-1})\in F_2^{n-1}$，考查 $f(x)$ 在任一点 $\alpha\in F_2^n$ 处的 Walsh 谱值：

$$\begin{aligned}S_{(f)}(\alpha)&=\frac{1}{2^n}\sum_{x\in F_2^n}(-1)^{(1+x_n)g(x_1,\cdots,x_{n-1})+x_nh(x_1,\cdots,x_{n-1})+\alpha\cdot x}\\&=\frac{1}{2^n}\sum_{x'\in F_2^{n-1}}\sum_{x_n\in F_2}(-1)^{(1+x_n)g(x_1,\cdots,x_{n-1})+x_nh(x_1,\cdots,x_{n-1})+\alpha\cdot x}\\&=\frac{1}{2^n}\sum_{x'\in F_2^{n-1}}(-1)^{g(x_1,\cdots,x_{n-1})+\alpha'\cdot x'}+\frac{1}{2^n}\sum_{x'\in F_2^{n-1}}(-1)^{h(x_1,\cdots,x_{n-1})+\alpha'\cdot x'+\alpha_n}\end{aligned}$$

于是有：

$$S_{(f)}(\alpha',0)=\frac{1}{2}S_{(g)}(\alpha')+\frac{1}{2}S_{(h)}(\alpha')$$

$$S_{(f)}(\alpha',1)=\frac{1}{2}S_{(g)}(\alpha')-\frac{1}{2}S_{(h)}(\alpha')$$

由于 $f(x)$ 为 F_2^n 上的 $n-1$ 阶 Plateaued 函数，故对任意的 $\alpha\in F_2^n$，$|S_{(f)}(\alpha)|=2^{-\frac{n-1}{2}}$ 或 0，且对任意的 $\alpha'=(\alpha_1,\cdots,\alpha_{n-1})\in F_2^{n-1}$，有 $|S_{(f)}(\alpha',0)|\neq|S_{(f)}(\alpha',1)|$，

于是有以下 2 种情形：

① $S_{(f)}(\alpha',0)=0, S_{(f)}(\alpha',1)=\pm 2^{\frac{n-1}{2}}$，此时可得 $S_{(g)}(\alpha')=-S_{(h)}(\alpha')=\pm 2^{\frac{n-1}{2}}$；

② $S_{(f)}(\alpha',1)=0, S_{(f)}(\alpha',0)=\pm 2^{\frac{n-1}{2}}$，此时可得 $S_{(g)}(\alpha')=S_{(h)}(\alpha')=\pm 2^{\frac{n-1}{2}}$。

在上面 2 情形下，都可得 $g(x_1,\cdots,x_{n-1}), h(x_1,\cdots,x_{n-1})$ 均为 $n-1$ 元 Bent 函数。

2) 对于任意的 $\alpha=(\alpha_1,\cdots,\alpha_{n-1},\alpha_n)\in F_2^n$，有：

$$\begin{aligned}&f(x)+f(x+\alpha)\\&=(1+x_n)g(x_1,\cdots,x_{n-1})+x_n h(x_1,\cdots,x_{n-1})+\\&(1+x_n+\alpha_n)g((x_1,\cdots,x_{n-1})+\alpha')+\\&(x_n+\alpha_n)h((x_1,\cdots,x_{n-1})+\alpha')\\&=(1+x_n)[g(x_1,\cdots,x_{n-1})+g((x_1,\cdots,x_{n-1})+\alpha')]+\\&x_n[h(x_1,\cdots,x_{n-1})+h((x_1,\cdots,x_{n-1})+\alpha')]+\\&\alpha_n[g((x_1,\cdots,x_{n-1})+\alpha')+h((x_1,\cdots,x_{n-1})+\alpha')]\end{aligned}$$

当 $\alpha_n=0$ 时，可得：

$$\begin{aligned}&f(x)+f(x+\alpha)=\\&(1+x_n)[g(x_1,\cdots,x_{n-1})+g((x_1,\cdots,x_{n-1})+\alpha')]+\\&x_n[h(x_1,\cdots,x_{n-1})+h((x_1,\cdots,x_{n-1})+\alpha')]\end{aligned}$$

由于 $g(x_1,\cdots,x_{n-1})$ 和 $h(x_1,\cdots,x_{n-1})$ 均为 $n-1$ 元 Bent 函数，故对任意的 $\alpha'=(\alpha_1,\cdots,\alpha_{n-1})\in F_2^{n-1}$，$g(x_1,\cdots,x_{n-1})+g((x_1,\cdots,x_{n-1})+\alpha')$ 和 $h(x_1,\cdots,x_{n-1})+h((x_1,\cdots,x_{n-1})+\alpha')$ 均为平衡函数，因此 $(1+x_n)[g(x_1,\cdots, x_{n-1})+g((x_1,\cdots,x_{n-1})+\alpha')]+x_n[h(x_1,\cdots,x_{n-1})+h((x_1,\cdots,x_{n-1})+\alpha')]$ 也为平衡函数，也就是说，对任意的 $\alpha=(\alpha_1,\cdots,\alpha_{n-1},0)\in F_2^n$，均有 $r_f(\alpha)=0$。于是令 $H=\{\alpha\in F_2^n,\ \alpha=(\alpha_1,\cdots,\alpha_{n-1},0)\}$，显然 H 为 F_2^n 的一个子空间，且对任意的 $\alpha\in H$，$r_f(\alpha)=0$。

定理 5 指出了 $n-1$ 阶 Plateaued 函数在满足一定条件时，可以拆成 2 个 $n-1$ 元 Bent 函数的链接，且此时函数的扩散性质也比较理想。进一步地，当 $n-1$ 阶 Plateaued 函数具有非零线性结构时，其与 Bent 函数的关系可由以下定理给出。

定理 6　设 n 为奇数，$f(x)$ 为 F_2^n 上的 $n-1$ 阶 Plateaued 函数，则其具有一个非 0 的线性结构等价于存在一个线性双射 φ 和 F_2^{n-1} 上的一个 $n-1$ 元 Bent 函数 $h(x_1,\cdots,x_{n-1})$，使得：

$$g(x)=f(\varphi(x))=h(x_1,x_2,\cdots,x_{n-1})+cx_n$$

证明　由文献[6]知，当 $f(x)$ 具有一个非 0 的线性结构时，必存在一个线性双射 φ 和 F_2^{n-1} 上的一个 $n-1$ 元布尔函数 $h(x_1,\cdots,x_{n-1})$，使得 $g(x)=f(\varphi(x))=h(x_1,x_2,\cdots,x_{n-1})+cx_n$，不妨设 $c=1$，于是有：$g(x)=h(x_1,x_2,\cdots,x_{n-1})+x_n$，并且由于 φ 为线性双射，故由文献[2]知，$g(x)$ 仍为 $n-1$ 阶 Plateaued 函数。再由定理 5 的证明可知，$g(x_1,x_2,\cdots,x_n)$ 在任一点 $u=(\alpha,\beta)$（$\alpha\in F_2^{n-1},\beta\in F_2$）处的 Walsh 谱值为：

$$\begin{aligned}S_{(g)}(u)&=\frac{1}{2}S_{(h)}(\alpha)+\frac{1}{2}S_{(h)}(\alpha)\cdot(-1)^{1+\beta}\\&=\begin{cases}0 & ,\ \beta=0\\S_{(h)}(\alpha) & ,\ \beta=1\end{cases}\end{aligned}$$

由于 $g(x)$ 为 F_2^n 上的 $n-1$ 阶 Plateaued 函数，故在 2^n 个点中有 2^{n-1} 个点处的 Walsh 谱值为 0。再由上式知，$S_{(g)}(u)$ 恰在 $\beta=0$ 时为 0，这样的点也恰为 2^{n-1} 个，因此对任意的 $\alpha\in F_2^{n-1}$，有 $S_{(h)}(\alpha)\neq 0$，故有 $S_{(h)}(\alpha)=\pm 2^{\frac{n-1}{2}}$，于是 $h(x_1,\cdots,x_{n-1})$ 为 F_2^{n-1} 上的 $n-1$ 元 Bent 函数。

定理 4 到定理 6 从函数结构角度刻画了 Plateaued 函数与 Bent 函数间的关系，下面给出 Plateaued 函数与部分 Bent 函数间的结构关系。

定理 7　设 $f(x_1,x_2,\cdots,x_n)$ 是 F_2^n 上任意一个部分 Bent 函数，且可表示成 F_2^{n-1} 上的 2 个 $n-1$ 元布尔函数的链接，即 $f(x_1,x_2,\cdots,x_n)=(x_n+1)f_1(x_1,x_2,\cdots,x_{n-1})+x_n f_2(x_1,x_2,\cdots,x_{n-1})$，且其所有线性结构所构成的线性子空间的维数为 k，如果对任意的 $\alpha\in F_2^{n-1}$，$S_{(f_1)}(\alpha)$ 和 $S_{(f_2)}(\alpha)$ 或者同时为 0 或者同时不为 0，则 $f_1(x_1,x_2,\cdots,x_{n-1})$ 和 $f_2(x_1,x_2,\cdots,x_{n-1})$ 均为 $n-k$ 阶 $n-1$ 元 Plateaued 函数。

证明　由定理 5 的证明可知，$f(x_1,x_2,\cdots,x_n)$ 在任一点 $u=(\alpha,\beta)$（$\alpha\in F_2^{n-1},\beta\in F_2$）处的 Walsh 谱值为

$$S_{(f)}(u)=\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)\cdot(-1)^{\beta}\qquad(2)$$

由于 $f(x_1,x_2,\cdots,x_n)$ 为部分 Bent 函数，且其所有的线性结构所构成的线性子空间的维数为 k，故由文献[7]知，其在任何一点的谱值为 0 或 $\pm 2^{\frac{k-n}{2}}$，此时式(2)的结果共有 9 种可能，即：

第 1 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=0\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=0\end{cases}$

第 2 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=0\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}\end{cases}$

第 3 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=0\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}\end{cases}$

第 4 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=0\end{cases}$

第 5 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}\end{cases}$

第 6 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}\end{cases}$

第 7 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=0\end{cases}$

第 8 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}\end{cases}$

第 9 种：$\begin{cases}\frac{1}{2}S_{(f_1)}(\alpha)+\frac{1}{2}S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}\\ \frac{1}{2}S_{(f_1)}(\alpha)-\frac{1}{2}S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}\end{cases}$

在这 9 种可能的取值中，对应于 $S_{(f_1)}(\alpha)$ 和 $S_{(f_2)}(\alpha)$ 的取值分别为：

1) $S_{(f_1)}(\alpha)=0,\ S_{(f_2)}(\alpha)=0$；

2) $S_{(f_1)}(\alpha)=2^{\frac{k-n}{2}},\ S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}$；

3) $S_{(f_1)}(\alpha)=-2^{\frac{k-n}{2}},\ S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}$；

4) $S_{(f_1)}(\alpha)=2^{\frac{k-n}{2}},\ S_{(f_2)}(\alpha)=2^{\frac{k-n}{2}}$；

5) $S_{(f_1)}(\alpha)=2^{\frac{k-n}{2}+1},\ S_{(f_2)}(\alpha)=0$；

6) $S_{(f_1)}(\alpha)=0,\ S_{(f_1)}(\alpha)=2^{\frac{k-n}{2}+1}$；

7) $S_{(f_1)}(\alpha)=-2^{\frac{k-n}{2}},\ S_{(f_2)}(\alpha)=-2^{\frac{k-n}{2}}$；

8) $S_{(f_1)}(\alpha)=0,\ S_{(f_1)}(\alpha)=-2^{\frac{k-n}{2}+1}$；

9) $S_{(f_1)}(\alpha)=-2^{\frac{k-n}{2}+1},\ S_{(f_2)}(\alpha)=0$。

由于对任意的 $\alpha\in F_2^{n-1}$，$S_{(f_1)}(\alpha)$ 和 $S_{(f_2)}(\alpha)$ 或者同时为 0 或者同时不为 0，故在上述的 9 种结果中，情形 5)、6)、8）和 9）这 4 种情形不可能出现，故只有 1）~4）和 7）这 5 种可能情形，对于这 5 种情形中的任一种，均有 $S_{(f_1)}(\alpha)=0$ 或 $\pm2^{\frac{k-n}{2}}$，$S_{(f_2)}(\alpha)=0$ 或 $\pm2^{\frac{k-n}{2}}$，因此 $f_1(x_1,x_2,\cdots,x_{n-1})$ 和 $f_2(x_1,x_2,\cdots,x_{n-1})$ 均为 $n-k$ 阶 $n-1$ 元 Plateaued 函数。

定理 7 给出了部分 Bent 函数与 Plateaued 函数之间的结构关系。由此定理可以得到 n 元 r 阶 Plateaued 函数与 n–1 元 r 阶 Plateaued 函数之间的结构关系。

推论 1 设 $f(x_1,x_2,\cdots,x_n)$ 为 n 元 r 阶 Plateaued 函数，且可表示成 F_2^{n-1} 上的 2 个 $n-1$ 元布尔函数的链接，$f(x_1,x_2,\cdots,x_n)=(x_n+1)f_1(x_1,x_2,\cdots,x_{n-1})+x_nf_2(x_1,x_2,\cdots,x_{n-1})$，若如果对任意的 $\alpha\in F_2^{n-1}$，$S_{(f_1)}(\alpha)$ 和 $S_{(f_2)}(\alpha)$ 或者同时为 0 或者同时不为 0，则 $f_1(x_1,x_2,\cdots,x_{n-1})$ 和 $f_2(x_1,x_2,\cdots,x_{n-1})$ 均为 $n-1$ 元 r 阶 Plateaued 函数。

证明 由定理 7 知，当 $f(x_1,x_2,\cdots,x_n)$ 为 n 元 r 阶 Plateaued 函数时，其 Walsh 谱值只取 0，$\pm2^{-\frac{r}{2}}$ 这 3 个值，当对任意的 $\alpha\in F_2^{n-1}$，$S_{(f_1)}(\alpha)$ 和 $S_{(f_2)}(\alpha)$ 或者同时为 0 或者同时不为 0 时，有 $S_{(f_1)}(\alpha)=0$ 或 $\pm2^{-\frac{r}{2}}$，$S_{(f_2)}(\alpha)=0$ 或 $\pm2^{\frac{-r}{2}}$，故 $f_1(x_1,x_2,\cdots,x_{n-1})$ 和 $f_2(x_1,x_2,\cdots,x_{n-1})$ 均为 $n-1$ 元 r 阶 Plateaued 函数。

3 结束语

本文从函数结构角度对 Bent 函数与 Plateaued 函数、部分 Bent 函数与 Plateaued 函数的关系进行了研究，指出了任意一个 Bent 函数都可拆分成 2 个 Plateaued 函数的链接，而 Plateaued 函数在满足

一定条件下也可拆分成 Bent 函数的链接。给出了 $n-1$阶 Plateaued 函数具有非零线性结构时与 Bent 函数的特殊关系，讨论了部分 Bent 函数可表示成 2 个 Plateaued 函数链接时的条件。研究结果进一步说明了这 3 类具有特殊 Walsh 谱值密码函数之间有着紧密的内在联系，为密码设计中使用此类函数提供了重要依据。此外，这 3 类密码函数在计数方面有何联系，还有待于进一步研究。

参考文献：

[1] CARLET C. Partially Bent functions[A]. Advance in Cryptology-Crytpo'93[C]. Berlin: Springer-Verlag, 1993.77-101.

[2] ZHENG Y, ZHANG X M. On Plateaued functions[J]. IEEE Transactions on Information Theory, 2001,47(3): 1215-1223.

[3] 滕吉红. 密码学中逻辑函数有关非线性准则的研究[D]. 解放军信息工程大学博士学位论文, 2003.
TENG J H. The Research of Nonlinear Criterion of Cryptographic Logic Functions[D]. University of Information Engineering, 2003.

[4] 胡斌, 金晨辉, 冯春海. Plateaued 函数的密码学性质[J]. 电子与信息学报, 2008, 30(3):660-664.
HU B, JIN C H, FENG C H. The peoperties of Plateaued functions[J]. Journal of Electronics , 2008, 30(3):660-664.

[5] 胡斌, 金晨辉, 史建红. 多输出 Plateaued 函数的密码学性质[J]. 电子与信息学报, 2009, 31(6):1433-1437.
HU B, JIN C H, SHI J H. The peoperties of multi-plateaued functions[J]. Journal of Electronics , 2009, 31(6):1433-1437.

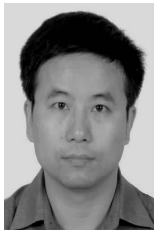
[6] 冯登国. 频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000.
FENG D G. Spectrum Theory and the Application in Cryptography[M]. Beijing: Publishing Company of Science,2000.

[7] JIN C H. Spectral characteristics of partially-bent functions[A]. Advanced in Cryptology—Chinacrypt'94[C]. 1994.48-51.

[8] CARLET C. On an improved correlation analysis of stream ciphers using muti-output Boolean functions and the related generalized notion of nonlinearity[EB/OL]. http://eprint.iacr.org,2007.

[9] CHARPIN P, PASALIC E, TAVERNIER C. On bent and semi-bent quadratic Boolean functions[J]. IEEE Transactions on Information Theory, 2005, 51(12):4286-4298.

作者简介：



胡斌（1971-），男，河南新县人，博士，解放军信息工程大学副教授，主要研究方向为密码学与信息安全。

金晨辉（1965-），男，河南周口人，解放军信息工程大学教授、博士生导师，主要研究方向为密码学与信息安全。

邵增玉（1965-）男，河南郑州人，解放军信息工程大学副教授，主要研究方向为密码学与信息安全。