Plateaued 函数谱支撑集的性质

胡 斌[1],行红明[2]
(1.解放军信息工程大学,河南郑州 450004;2.河南林业职业学院,河南洛阳 471002)

摘 要: 本文对 Plateaued 函数的谱支撑集的结构与性质进行了深入研究,给出了 r 阶 Plateaued 函数的全体非 0 谱值点集合与线性结构集的维数之间的关系.利用谱指标对 2 阶 Plateaued 函数和 4 阶 Plateaued 函数的自相关性进行了详细分析,给出了其自相关系数的分布.分析了 r 阶 Plateaued 函数的谱支撑集和零谱值点集的结构特征,给出了多个 r 阶 Plateaued 函数的谱支撑集在不相交时自相关系数之间的关系以及谱支撑集与函数平衡性的关系.

关键词: Plateaued 函数; 谱支撑集; 扩散性
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2014)05-0948-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.05.017

The Spectrum Support's Properties of Plateaued Functions

HU Bin[1], XING Hong-ming[2]
(1. *Information Engineering University of PLA*, *Zhengzhou*, *Henan* 450004, *China*; 2. *Henan Forestry Vocational College*, *Luoyang*, *Henan* 471002, *China*)

Abstract: This paper discusses the structure and properties of spectrum support for plateaued functions. We give the relationship between the set of rth-order plateaued functions' all nonzero walsh spectrum points and the dimension of linear structure set. Meanwhile, we utilize spectrum index to analyze the autocorrelation properties of both second-order and 4th-order plateaued functions. And the distribution of their autocorrelation coefficient is given. Moreover, we talk about the structure characteristics of rth-order plateaued functions' spectrum support and zero walsh spectrum points set. We present the relationship among their autocorrelation coefficients and point out the relationship between the spectrum support and the balance property when more rth-order plateaued functions' spectrum supports are not cross.

Key words: Plateaued functions; Walsh spectrum support; propagation properties

1 引言

在密码函数的设计中,我们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 C. 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,S 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 Y. 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.Plateaued 函数、Bent 函数和部分 Bent 函数的 Walsh 谱的取值均比较特殊,即只取两个或三个值.文献[6]从函数结构角度对这三类密码函数之间的关系进行了深入分析,研究结果进一步说明了这三类具有特殊 Walsh 谱值密码函数之间有着紧密的内在联系.文献[7]对两类半 Bent 函数的自相关系数进行了研究,

收稿日期:2012-05-15;修回日期:2013-08-29;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61272041,No.61202491,No.61272488)

对于 Plateaued 函数来说,由于其 Walsh 谱值只取三个值,且非 0 谱值的绝对值相等,因而非 0 谱值点是一个非常特殊的集合,我们有必要对其进行深入的研究.本文对 Plateaued 函数的谱支撑集的结构与性质进行了深入研究,给出了 r 阶 Plateaued 函数的全体非 0 谱值点集合与线性结构集的维数之间的关系.利用谱指标对 2 阶 Plateaued 函数和 4 阶 Plateaued 函数的自相关性进行了详细分析,给出了其自相关系数的分布.分析了 r 阶 Plateaued 函数的谱支撑集和零谱值点集的结构特征,给出了多个 r 阶 Plateaued 函数的谱支撑集在不相交时自相关系数之间的关系以及谱支撑集与函数平衡性的关系.

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 $f(x):F_2^n\to F_2$.

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 $x\cdot w=w_1x_1+w_2x_2+\cdots+w_nx_n$, 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 $f(x):F_2^n\to F_2$,则称

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

为 $f(x)$ 的在 α 点的自相关系数.

定义 3　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数,称集合 $\Im_f=\{\alpha\in F_2^n:S_{(f)}(\alpha)\neq 0\}$ 为函数 $f(x)$ 的 Walsh 谱支撑集.

定义 4[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 $w\in F_2^n$, $S_{(f)}(w)=0$ 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.

我们首先给出一般的布尔函数的全体非 0 谱值点集合与线性结构集的维数之间的关系.

引理 1[9]　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数, U 为 F_2^n 的一个线性子空间,且其维数为 l, $v\in F_2^n$,则有:

(1) $\sum_{\alpha\in F_2^n}S_{(f)}(\alpha)=(-1)^{f(0)}$

(2) $\sum_{\alpha\in U}S_{(f)}^2(\alpha)=2^{l-n}\sum_{v\in U^\perp}r_f(v)$

(3) $\sum_{\alpha\in U}S_{(f)}(\alpha)=2^{l-n}\sum_{v\in U^\perp}(-1)^{f(v)}$

(4) $\sum_{\alpha\in U+v}S_{(f)}(\alpha)=2^{l-n}\sum_{x\in U^\perp}(-1)^{f(x)+v\cdot x}$

引理 2　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:

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

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, $c=0$.

定理 1　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数,其谱支撑集为 $\Im_f=\{\alpha\in F_2^n:S_{(f)}(\alpha)\neq 0\}$, $f(x)$ 的全体不变线性结构所构成的集合为 $U_f=\{\alpha:f(x+\alpha)+f(x)=0,\ \forall x\in F_2^n\}$,设 $\dim U_f=k$, E 为 $f(x)$ 的谱支撑集所生成的线性子空间,则有 $\dim E=n-k$.

证明　对任意的 $b\in E^\perp$, $b\neq 0$,令 $H=\{x:b\cdot x=0\}$,则显然有 $E\subset H$,且 H 构成 F_2^n 的一个 $n-1$ 维线性子空间.于是由引理 1 知:

$$\sum_{\alpha\in H}S_{(f)}^2(\alpha)=2^{-1}(r_f(0)+r_f(b))=2^{-1}(1+r_f(b))$$

由于 $E\subset H$,故 $\sum_{\alpha\in H}S_{(f)}^2(\alpha)=2^{-1}(1+r_f(b))=1$,故 $r_f(b)=1$,即 b 为 $f(x)$ 的一个非 0 的线性结构,可得: $E^\perp\subset U_f$.

另一方面,若对任意的 $b\in U_f$,则有 $r_f(b)=1$.由引理 1, $\sum_{\alpha\in H}S_{(f)}^2(\alpha)=2^{-1}(1+r_f(b))=1$,于是可得 $E\subset H$,因此一定有 $H^\perp\subset E^\perp$.由 H 的定义可知 $b\in H^\perp$,故 $b\in E^\perp$,因而有 $U_f\subset E^\perp$.于是有 $U_f=E^\perp$,故 $\dim E^\perp=k$,因此 $\dim E=n-k$.

推论 1　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数,若其线性维数为 k,令

$$t=\begin{cases}n-k, & f(x)\text{不存在恒变线性结构}\\ n-k+1, & f(x)\text{存在恒变线性结构}\end{cases}$$

则存在一个线性双射 φ,使得 F_2^n 上的 r 阶 Plateaued 函数 $f(x)$ 可经由仿射变换后退化为 F_2^t 上的 r 阶 Plateaued 函数 $g(x)=f(\varphi(x))$.

在讨论 F_2^n 上的 r 阶 Plateaued 函数的谱支撑集结构时,我们通常是讨论其非 0 谱值的分布情形.为了研究方便,我们首先给出一个定义.

定义 5　设 $f(x)$ 为 F_2^n 上的 n 元布尔函数,称

$$\varphi(a)=2^{\frac{r}{2}}S_{(f)}(a)$$

为 $f(x)$ 在 a 点的 Walsh 谱指标,简称谱指标.

由该定义知,Plateaued 函数 $f(x)$ 在任意一点 a 处的谱指标为 1、-1 或 0,实际上,Plateaued 函数 $f(x)$ 在某一点的谱指标为 1 说明函数在该点的谱值为正,谱指标为 -1 说明函数在该点的谱值为负,谱指标为 0 说明函数在该点的谱值为 0.

记 $\Re_f=\{\alpha\in F_2^n:r_f(\alpha)\neq 0\}$,利用引理 1 可很容易地得到 r 阶 Plateaued 函数 $f(x)$ 关于谱指标的一个简单结论.

定理 2 设 $f(x)$为 F_2^n 上的 r 阶 Plateaued 函数，$\varphi(a)$为其在点 a 处的谱指标，则有：

$$\sum_{a\in F_2^n}\varphi(a)\in\{-2^{r/2},2^{r/2}\}$$

证明 由引理 1(1)知，$\sum_{a\in F_2^n}\varphi(a)=2^{r/2}\cdot\sum_{a\in F_2^n}S_{(f)}(a)=2^{r/2}\cdot(-1)^{f(0)}\in\{-2^{r/2},2^{r/2}\}$.

推论 2 F_2^n 上的 2 阶 Plateaued 函数非 0 的 Walsh 谱点共有 4 个，且在这 4 个点中，谱值为正的点 3 个、为负的点 1 个；或谱值为正的点 1 个、为负的点 3 个. 4 阶 Plateaued 函数非 0 的 Walsh 谱点共有 16 个，且在这 16 个点中，谱值为正的点 10 个、为负的点 6 个；或谱值为正的点 6 个、为负的点 10 个.

下面再对 2 阶 Plateaued 函数 $f(x)$的自相关性进行分析.

由于 2 阶 Plateaued 函数 $f(x)$的谱支撑集中有 4 个元素，不妨设其谱支撑集为 $\Im_f=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$，记 $\Im_f$ 的秩为 $R(\Im_f)$，显然 $R(\Im_f)$只可能取 2,3,4 这三个值，下面我们分别对其进行分析.

对于 $R(\Im_f)=2$ 和 3 时的情形较为简单，这里不再详细讨论. 当 $R(\Im_f)=4$ 时，设 $f(x)$的 4 个非 0 的 Walsh 谱值点为 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$，同理可知，存在可逆线性变换 B，使 $g(x)=f(xB)$的非 0 谱值点为 $\beta_1,\beta_2,\beta_3,\beta_4$，且 $\beta_1=(1,0,0,0,\cdots,0,0)$，$\beta_2=(0,1,0,0,\cdots,0,0)$，$\beta_3=(0,0,1,0,\cdots,0,0)$，$\beta_4=(0,0,0,1\cdots,0,0)$. 于是对任意的 $a=(a_1,a_2,\cdots,a_n)\in F_2^n$，有：

$$r_h(a)=\sum_{x\in F_2^n}S_{(h)}^2(x)(-1)^{a\cdot x}=\frac{1}{4}\sum_{x\in\{\beta_1,\beta_2,\beta_3,\beta_4\}}(-1)^{a\cdot x}$$
$$=\frac{1}{4}[(-1)^{a_1}+(-1)^{a_2}+(-1)^{a_3}+(-1)^{a_4}]$$

即 $r_h(a)$的取值只与 a_1,a_2,a_3,a_4 有关，于是当 (a_1,a_2,a_3,a_4)遍历 F_2^4 时，$[(-1)^{a_1}+(-1)^{a_2}+(-1)^{a_3}+(-1)^{a_4}]$的 16 个取值中有 6 个为 0，4 个为 2，4 个为 -2，1 个为 4，1 个为 -4. 于是 $r_h(a)$的所有 2^n 个取值中有 $6\cdot2^{n-4}$个为 0，2^{n-2}个为$\frac{1}{2}$，2^{n-2}个为$-\frac{1}{2}$，2^{n-4}个为 1，2^{n-4}个为 -1. 于是我们可知，$f(x)$的 2^n 个自相关系数的取值中，也有 $6\cdot2^{n-4}$个为 0，2^{n-2}个为$\frac{1}{2}$，2^{n-2}个为$-\frac{1}{2}$，2^{n-4}个为 1，2^{n-4}个为 -1.

我们再考查 4 阶 Plateaued 函数 $f(x)$的自相关性.

由文献[10]可知，4 阶 Plateaued 函数 $f(x)$的谱支撑集 $\Im_f$ 的秩 $R(\Im_f\le7$，由于 $\Im_f$ 中有 16 个元素，显然 $R(\Im_f)\ge4$，即 $4\le R(\Im_f)\le7$，若 $R(\Im_f)=4$，则显然 $\Im_f$ 构成一个线性子空间，类似于上面的讨论可知，此时对于任意的 $\alpha\in F_2^n$，其自相关系数为 1 或为 0，且自相关系数为 1 点的个数为 $\#\Re_f=\left|\Im_f^{\perp}\right|=2^{n-4}$，于是有$(\#\Im_f)(\#\Re_f)=2^n$，即此时 $f(x)$为部分 Bent 函数.

对于 $R(\Im_f)=5$ 时，16 个元素中 5 个是线性无关的，另外 11 个元素可通过这 5 个线性无关的元素表示，在计算任一点 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)\in F_2^n$ 的自相关系数时，类似于上面的讨论，由：

$$r_h(\boldsymbol{a})=\sum_{x\in F_2^n}S_{(h)}^2(x)(-1)^{\boldsymbol{a}\cdot\boldsymbol{x}}=\frac{1}{16}\sum_{x\in\{\beta_1,\beta_2,\cdots,\beta_{16}\}}(-1)^{\boldsymbol{a}\cdot\boldsymbol{x}}$$
$$=\frac{1}{16}[(-1)^{a_1}+(-1)^{a_2}+(-1)^{a_3}+(-1)^{a_4}$$
$$+(-1)^{a_5}+(-1)^{a_6'}+\cdots+(-1)^{a_{16}'}]$$

由于 $a_6',\cdots,a_{16}'$这 11 个元素是 $a_1,\cdots,a_5$ 的线性组合，且其线性组合的所有可能为 $26\times25\times24\times\cdots\times17\times16\approx2^{49}$，(在 32 种可能选择中除去 0，$a_1,\cdots,a_5$ 等 6 种选择)当计算任意一点的自相关系数时还需要考虑 5 个线性无关的元素遍历 F_2^5，故其计算复杂度约为 2^{54}，显然计算量太大，在这里难于给出具体分布.

同样对于 $R(\Im_f)=6,7$ 时也由于计算量太大而难于给出具体分布.

定理 3 设 $f(x)$为 F_2^n 上的 r 阶 Plateaued 函数，其谱支撑集为 $\Im_f$，H 为 F_2^n 任意的一个 $n-1$ 维线性子空间，如果 $\Im_f\cap H\neq\varnothing$且 $\Im_f\cap H\neq\Im_f$，则有 $2^{r/2}\le|\Im_f\cap H|\le2^r-2^{r/2}$.

证明 由于 H 为 F_2^n 的 $n-1$ 维线性子空间，故可设 $H^{\perp}=\{0,v\}$，$v\in F_2^n$，$v\neq0$，于是由引理 1(2)知

$$=\sum_{a\in H}|\varphi(a)|=2^r\sum_{a\in H}|S_{(f)}{}^2(a)|=2^{r-1}\sum_{x\in H^{\perp}}r_f(x)$$
$$=2^{r-1}(r_f(0)+r_f(v))=2^{r-1}(1+r_f(v))$$

因此，当 v 为 $f(x)$的不变线性结构时，$r_f(v)=1$，此时有 $\sum_{a\in H}|\varphi(a)|=2^r$，说明在 H 中有 2^r 个非 0 的谱值点，又由于 $f(x)$为 r 阶 Plateaued 函数，其谱值不为 0 的点的个数为 2^r，即这 2^r 个非 0 谱值的点均在 H 中，于是有 $\Im_f\cap H=\Im_f$. 当 v 为 $f(x)$的恒变线性结构时，$r_f(v)=-1$，此时有 $\sum_{a\in H}|\varphi(a)|=0$，即说明 H 中所有点的谱值均为 0，即谱值非 0 的点均不在 H 中，于是有 $\Im_f\cap H=\varnothing$.

当 v 不是 $f(x)$的线性结构时，由已知的结论知，此时 $2^{1-\frac{r}{2}}-1\le r_f(v)\le1-2^{1-\frac{r}{2}}$，因此有 $2^{r/2}\le\sum_{a\in H}|\varphi(a)|\le2^r-2^{r/2}$，这实际上给出了 H 中所有非 0 谱值点的个数的上下界，于是可得：

$$2^{r/2}\le|\Im_f\cap H|\le2^r-2^{r/2}$$

由于 r 阶 Plateaued 函数的非零谱值点的个数比较特殊，均为 2 的幂次方，根据这一性质我们可讨论 Plateaued 函数的所有取值为零的点所构成的集合的基本性质. 有以下结论.

定理 4　设 $f(x)$为 F_2^n 上的 r 阶 Plateaued 函数,设 E 为$f(x)$的所有 Walsh 谱值为 0 的点所构成的集合,即 $E=\{\alpha\in F_2^n, S_{(f)}(\alpha)=0\}$,记集合 E 的秩为 k,则:

(1)当 n 为偶数,且 E 为空集时,$k=0$,$f(x)$为 F_2^n 上的 Bent 函数;

(2)当 $f(x)$不为 Bent 函数时,有 $k\geq n-1$,且 $k=n-1$ 的充分必要条件是 $f(x)$为 F_2^n 上的 $n-1$ 阶 Plateaued 函数,此时 E 构成 F_2^n 的一个线性子空间.

证明　(1)显然,当 E 为空集时,$k=0$ 时,此时 $f(x)$在任意一点的 Walsh 谱值不为0,又由于 $f(x)$为 F_2^n 上的 Plateaued 函数,故在所有谱值不为 0 点的谱值相等,因此 $f(x)$为 F_2^n 上的 Bent 函数.

(2)当 $f(x)$不为 Bent 函数时,此时 $r\leq n-1$,$f(x)$的非 0 的 Walsh 谱值点的个数至多为 2^{n-1},即 $f(x)$的 Walsh 谱取值为 0 的点的个数至少为 2^{n-1},故必定有 $k\geq n-1$.若 $k=n-1$,说明 $f(x)$的 Walsh 谱取值为 0 的点的个数恰为 2^{n-1},故 E 构成 F_2^n 的一个线性子空间.此时 $f(x)$的 Walsh 谱取值不为 0 的点的个数也为 2^{n-1},所以 $f(x)$为 F_2^n 上的 $n-1$ 阶 Plateaued 函数.

反之,若 $f(x)$为 F_2^n 上的 $n-1$ 阶 Plateaued 函数,此时有 $|E|=2^{n-1}$,又由于 $k\geq n-1$,所以此时有 $k=n-1$,显然 E 构成 F_2^n 的一个线性子空间.

下面我们可进一步给出当 n 为奇数时,n 元 $n-1$ 阶 Plateaued 函数的所有非 0 谱值点构成集合的秩的具体情形,有以下结论.

定理 5　设 n 为奇数,$f(x)$为 F_2^n 上的 n 元 $n-1$ 阶 Plateaued 函数,若 $f(x)$没有非 0 的线性结构,则秩$(\Im_f)=n$.

证明　由于 $f(x)$为 F_2^n 上的 n 元 $n-1$ 阶 Plateaued 函数,故 $\#\Im_f=2^{n-1}$,因此秩$(\Im_f)\geq n-1$.

由定理 4 知,若秩$(\Im_f)=n-1$,则 $\Im_f$ 构成 F_2^n 的一个线性子空间.于是由引理 2 可知,

$$r_f(\alpha)=\sum_{x\in F_2^n}S_{(f)}{}^2(x)(-1)^{\alpha\cdot x}=2^{-(n-1)}\sum_{x\in\Im_f}(-1)^{\alpha\cdot x}$$
$$=\begin{cases}1, & \alpha\in\Im_f^{\perp}\\ 0, & \alpha\notin\Im_f^{\perp}\end{cases}$$

即此时 $f(x)$存在非 0 的线性结构,与已知矛盾,于是有秩$(\Im_f)=n$.

上面我们讨论了 r 阶 Plateaued 函数的谱支撑集所具有的一些基本性质,初步刻画了此类函数自身的特性.那么函数簇中不同 Plateaued 函数的谱支撑集间有何关系呢? 经研究发现,对于多个 r 阶 Plateaued 函数的谱支撑集,若其各谱支撑集之间不相交,则此时多个 r 阶 Plateaued 函数的自相关系数之间有特殊的关系,具体地,我们有如下结论.

定理 6　设函数 $g_1(x),g_2(x),\cdots,g_{2^k}(x)$是 F_2^n 上的 2^k 个 $n-k$ 阶 Plateaued 函数,设 $\Im_{g_i}=\{\alpha\in F_2^n, S_{(g_i)}(\alpha)\neq 0\}$,$i=1,2,\cdots,2^k$,则对任意的 $1\leq p,q\leq 2^k$,$\Im_{g_p}\cap\Im_{g_q}=\varnothing$的充分必要条件是对任意非 0 的 $\alpha\in F_2^n$,有:

$$\sum_{i=1}^{2^k}r_{g_i}(\alpha)=0$$

证明　先证必要性.由于对任意的 $1\leq i\leq 2^k$,$g_i(x)$均为 n-k 阶 Plateaued 函数,故对任意的非 0 的 $\alpha\in F_2^n$,有:

$$r_{g_i}(\alpha)=\sum_{x\in F_2^n}S_{(g_i)}(x)(-1)^{\alpha\cdot x}=2^{k-n}\sum_{x\in\Im_{g_i}}(-1)^{\alpha\cdot x}$$

记 $s_i=\{x\in\Im_{g_i},\alpha\cdot x=0\}$,$t_i=\{x\in\Im_{g_i},\alpha\cdot x=1\}$,显然 $s_i+t_i=\#\Im_{g_i}$.

由于 $g_i(x)$均为 $n-k$ 阶 Plateaued 函数,故 $\#\Im_{g_i}=2^{n-k}$,且对任意的 $1\leq p,q\leq 2^k$,$\Im_{g_p}\cap\Im_{g_q}=\varnothing$,故

$$\Im_{g_1}\cup\Im_{g_2}\cup\cdots\cup\Im_{g_{2^k}}=F_2^n$$

因此有:$\sum_{i=1}^{2^k}(s_i+t_i)=2^n$,并且可得:$\sum_{i=1}^{2^k}s_i=\sum_{i=1}^{2^k}t_i=2^{n-1}$,于是 $\sum_{i=1}^{2^k}s_i-\sum_{i=1}^{2^k}t_i=0$

由于

$$r_{g_i}(\alpha)=\sum_{x\in F_2^n}S_{(g_i)}(x)(-1)^{\alpha\cdot x}=2^{k-n}\sum_{x\in\Im_{g_i}}(-1)^{\alpha\cdot x}=2^{k-n}(s_i-t_i)$$

因此

$$\sum_{i=1}^{2^k}r_{g_i}(\alpha)=2^{k-n}\sum_{i=1}^{2^k}(s_i-t_i)=2^{k-n}\Big(\sum_{i=1}^{2^k}s_i-\sum_{i=1}^{2^k}t_i\Big)=0$$

再证充分性.此时对任意非 0 的 $\alpha\in F_2^n$,有:$\sum_{i=1}^{2^k}r_{g_i}(\alpha)=0$,由上面必要性的证明中可知,

$$\sum_{i=1}^{2^k}r_{g_i}(\alpha)=2^{k-n}\sum_{i=1}^{2^k}(s_i-t_i)=2^{k-n}\Big(\sum_{i=1}^{2^k}s_i-\sum_{i=1}^{2^k}t_i\Big)=0$$

即 $\sum_{i=1}^{2^k}s_i-\sum_{i=1}^{2^k}t_i=0$,由于 $s_i+t_i=\#\Im_{g_i}=2^{n-k}$,故 $\sum_{i=1}^{2^k}(s_i+t_i)=2^k\cdot 2^{n-k}=2^n$,并且 $\sum_{i=1}^{2^k}s_i=\sum_{i=1}^{2^k}t_i$.

设 $A=\Im_{g_1}\cup\Im_{g_2}\cup\cdots\cup\Im_{g_{2^k}}$,则对任意非 0 的 $\alpha\in F_2^n$,有:

$$\sum_{x\in A}(-1)^{\alpha\cdot x}=\sum_{i=1}^{2^k}s_i-\sum_{i=1}^{2^k}t_i=0.$$

因此可得此时集合 A 即是整个 n 维向量空间 F_2^n,即 $\Im_{g_1}\cup\Im_{g_2}\cup\cdots\cup\Im_{g_{2^k}}=F_2^n$,于是:

对任意的 $1\leq p,q\leq 2^k$,有:

$$\Im_{g_p}\cap\Im_{g_q}=\varnothing$$

进一步地,我们可得以下结论.

定理 7　设函数 $g_1(x),g_2(x),\cdots,g_{2^k}(x)$ 是 F_2^n 上

的 2^k 个 $n-k$ 阶 Plateaued 函数，设 $\Im_{g_i}=\{\alpha\in F_2^n, S_{(g_i)}(\alpha)\neq 0\}$，$i=1,2,\cdots,2^k$，若对任意的 $1\leq p,q\leq 2^k$，$\Im_{g_p}\bigcap\Im_{g_q}=\varnothing$，则这 2^k 个 n-k 阶 Plateaued 函数中有且仅有一个函数为非平衡函数.

证明 由于 $g_i(x)$ 均为 n-k 阶 Plateaued 函数，故 $\#\Im_{g_i}=2^{n-k}$，且对任意的 $1\leq p,q\leq 2^k$，$\Im_{g_p}\bigcap\Im_{g_q}=\varnothing$，故

$$\Im_{g_1}\bigcup\Im_{g_2}\bigcup\cdots\bigcup\Im_{g_{2^k}}=F_2^n$$

于是，存在一个 i，$1\leq i\leq 2^k$，全 0 向量 $(0,0,\cdots,0)$ 属于且仅属于 $\Im_{g_i}$，即 $S_{(g_i)}(0)\neq 0$，因此 $g_i(x)$ 为非平衡函数.

而对于其他的 2^k-1 个函数，由于全 0 向量 $(0,0,\cdots,0)$ 均不属于 $\Im_{g_j}$，$1\leq j\leq 2^k$，$j\neq i$，于是有 $S_{(g_j)}(0)=0$，于是这 2^k-1 个函数均为平衡函数.

利用定理 6 和定理 7 显然有以下推论.

推论 3 设函数 $g_1(x),g_2(x),\cdots,g_{2^k}(x)$ 是 F_2^n 上的 2^k 个 $n-k$ 阶 Plateaued 函数，若对任意非 0 的 $\alpha\in F_2^n$，有 $\sum_{i=1}^{2^k} r_{g_i}(\alpha)=0$，则这 2^k 个 n-k 阶 Plateaued 函数中有且仅有一个函数为非平衡函数.

3 结束语

本文对 Plateaued 函数的谱支撑集的结构与性质进行了深入研究，通过对 r 阶 Plateaued 函数的谱支撑集与线性结构集、谱支撑集元素的自相关特性以及零谱值点集的结构特征的分析与刻画，掌握了 Plateaued 函数谱支撑集的基本性质. 对多个 Plateaued 函数的谱支撑集的关系进行了初步研究，给出了在不相交时自相关系数之间的关系以及谱支撑集与函数平衡性的关系. 对于高阶 Plateaued 函数的谱支撑集的结构特征，如扩散特性以及自相关特征如何分类刻画或给出快速计算算法，还需进一步深入研究. 在研究中，可根据 Plateaued 函数的特性，利用二阶自相关特性进行深入刻画[11,12]. 另外，对于 Plateaued 函数的代数免疫性，目前还缺乏研究，文献[13,14]对布尔函数的代数免疫性进行了深入研究，如何借鉴其方法与结果给出 Plateaued 函数的代数免疫性质可进一步研究.

参考文献

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

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

[3] S Chee, S Lee. Semi-bent functions[A]. Advance in Cryptology-Asiacrytp'94[C]. Berlin: Springer-Verlag, 1995. 107 – 118.

[4] 秦静，赵亚群. 半 Bent 函数的密码学特性[J]. 山东大学学报(理学版)，2002，37(12)：480 – 483.
QinJing, Zhaoyachen. Cryptographicproperties of Semi-bent functions[J]. Journal of Shandong University (Natural Science), 2002, 37(12): 480 – 483. (in Chinese).

[5] Y. Zheng, XM Zhang. On plateaued functions[J]. IEEE Transactions on Information Theory, 2001, 47(3): 1215 – 1223.

[6] 胡斌，金晨辉，邵增玉. 密码学中三类具有特殊 Walsh 谱值布尔函数的关系[J]. 通信学报，2010，31(7)：104 – 109.
Hu Bin, et al. Relationship among three kinds of cryptographic Boolean functions with special walsh spectrum[J]. Journal on Communications, 2010, 31(7): 104 – 109. (in Chinese)

[7] X Li, Y Hu , J Gao. Autocorrelation coefficient of two classes of semi-bent functions[J]. Applied Mathematics and Information Sciences, 2011, 5(1): 85 – 97.

[8] 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.

[9] Claude Carlet, Pascale Charpin. Cubic Boolean function with highest resiliency[J]. IEEE Transactions on Information Theory, 2007, 53(2): 562 – 571.

[10] Yuriy Tarannikov. On affine rank of spectrum support for plateaued function[DB/OL]. http://eprint.org/2005/399.pdf, 2012-05-15.

[11] S. Gangopadhyay, B K Singh. On second-order nonlinearities of some D0 type bent functions[J]. Fundamenta Informaticae, 2012, 114(3): 271 – 285.

[12] M. Garg, S Gangopadhyay. A lower bound of the second-order nonlinearities of Boolean bent functions[J]. Fundamenta Informaticae, 2011, 111(4), 413 – 422.

[13] X Zeng, C Carlet, J Shan, L Hu. More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks[J]. IEEE Transactions on Information Theory, 2011, 57(9): 6310 – 6320.

[14] Z Tu, Y Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity[J]. Designs, Codes and Cryptography, 2011, 60(1): 1 – 14.

作者简介

胡 斌 男，1971 年生，教授，博士生导师，主要研究方向为密码学与信息安全.
E-mail: hb2110@126.com

行红明 男，1970 年生，副教授，主要研究方向为应用教学.