# Plateaued 函数的正规性

王维琼[①②]　周　宇[①]　肖国镇[①]
[①](西安电子科技大学 ISN 国家重点实验室　西安　710071)
[②](长安大学理学院　西安　710064)

**摘　要**：Plateaued 函数作为 Bent 函数和部分 Bent 函数的扩展，是一类能实现多个密码学准则折中的性质优良的密码函数。该文基于布尔函数与其分解函数的 Walsh 谱之间的关系研究了 Plateaued 函数的复杂性度量指标之一的正规性，根据其正规性质给出了判定给定 Plateaued 函数是否正规的一个较为简单的算法，并分析了已知 Plateaued 函数类的正规性。

**关键词**：密码函数；非线性度；正规性；仿射子空间；Plateaued 函数
**中图分类号**：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2009)09-2283-04

# Normality of Plateaued Functions

Wang Wei-qiong[①②]　Zhou Yu[①]　Xiao Guo-zhen[①]
[①](*State Key Laboratory of Integrated Service Network*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*College of Science, Chang'an University*, *Xi'an* 710064, *China*)

**Abstract**: As a generalization of Bent functions and Partially Bent functions, Plateaued functions can achieve trade-off among many cryptographic criteria. Based on the relationships between the Walsh transform of a given function and the Walsh transform of its decomposing function, the normality of Plateaued functions is studied. Then a simpler algorithm for checking the normality of Plateaued functions is proposed. Finally, the normality of some known kind of Plateaued functions is discussed.

**Key words**: Cryptographic Boolean functions; Nonlinearity; Normality; Affine subspaces; Plateaued functions

## 1　引言

密码函数在流密码及分组密码的设计中发挥着重要的作用。基于 Shannon 提出的混淆及扩散思想，一个好的密码函数必须同时满足平衡性、高非线性性、好的扩散性、高的代数免疫阶、非正规等多个密码学性能指标。正规性这一指标是 Dobbertin[1] 在 1994 年构造高非线性的平衡函数时提出的，若一个 $n$ 元布尔函数在某一 $n/2$ 维仿射子空间上的限制为常数，则称其为正规的。显然，正规的布尔函数是有缺陷的，我们总希望一个好的密码函数在任意一个 $k$ 维子空间上的限制都不为常数或仿射函数，且 $k$ 越小表明该密码函数在这一方面的性质越好。自此正规性便受到大家广泛关注，文献[2,3]中相继给出了判定任一布尔函数正规性的算法及改进算法。文献[4,5]中研究了正规性和其他密码学指标之间的关系。也有不少学者开始关注一些高非线性密码函数的正规性，尤其是对达到非线性度上界的 Bent 函数正规性研究。起初 Dobbertin 猜想所有 Bent 函数都是正规的，但在文献[6]中作者找出了非正规的 Bent 函数，这一结果让密码研究者大受鼓舞。

虽然 Bent 能达到最大的非线性度，具有良好的差分分布均匀性，但其是不平衡的，也不是相关免疫的，而且仅在 $n$ 为偶数时才存在，这就限制了其直接应用。于是 Carlet 推广了 Bent 函数，提出了部分 Bent 函数的概念，指出部分 Bent 函数可为平衡的、具有高的非线性度，且具有良好的扩散性及相关免疫性，但遗憾的是当它不为 Bent 函数时都具有非零的线性结构。于是 Zheng 与 Zhang[7]又提出了 Plateaued 函数，指出某些 Plateaued 函数保持了部分 Bent 函数的良好性质，且不具有非零的线性结构，是一类性质良好的密码函数。文献[8–12]中对这类函数的性质及构造方法进行了大量研究。本文主要讨论 Plateaued 函数的正规性，针对其性质给出一个较简单的正规性判定算法，并分析已知 Plateaued 函数类的正规性。

## 2　预备知识

$n$ 元布尔函数 $f(x)$ 定义为映射：$F_2^n$，其中 $x=$

2008-05-15 收到，2009-06-08 改回
国家自然科学基金(60773003)资助课题

$(x_1, x_2, \cdots x_n) \in F_2^n$，并记 $B_n$ 为 $F_2^n$ 上所有 $n$ 元布尔函数的集合。

**定义 1** 对任意 $f(x) \in B_n$，定义 $f(x)$ 在点 $\alpha \in F_2^n$ 处的 Walsh 变换为

$$F(f+\varphi_\alpha) = \sum_{x \in F_2^n} (-1)^{f(x)+\varphi_\alpha(x)} \tag{1}$$

其中 $\varphi_\alpha$ 为 $B_n$ 中的线性函数：$x \mapsto \alpha \cdot x = \alpha_1 x_1 + \cdots \alpha_n x_n$。当 $F(f)=0$ 时，称 $f(x)$ 为平衡函数。$f(x)$ 的非线性度定义为其与 $B_n$ 上的所有仿射函数之间的最小汉明距离，可表为

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\alpha \in F_2^n} \left|F(f+\varphi_\alpha)\right| \tag{2}$$

Rothaus 证明了当 $n$ 为偶数时，$n$ 元布尔函数非线性度的最大值为 $2^{n-1} - 2^{(n/2)-1}$，并指出达到这一最大非线性度的布尔函数是唯一的，称为 Bent 函数。

**定义 2** 设 $V$ 为 $F_2^n$ 的一个 $k$ 维子空间，对 $\forall f(x) \in B_n$，称函数 $f\phi_V$ 为 $f(x)$ 在 $V$ 上的限制，其中 $\phi_V(x) = \begin{cases} 1, & x \in V \\ 0, & \text{其他} \end{cases}$。并定义 $f(x)$ 关于 $V$ 的分解函数序列为 $\{f\phi_{a+V} \mid a \in W\}$，其中 $V \times W = F_2^n$。

注意到，$f\phi_V(x) = 1$ 当且仅当对任意的 $x \in V$，都有 $f(x) = 1$；也可将 $f\phi_{a+V}$ 看作 $B_k (0 \le k \le n)$ 中的布尔函数。

**定义 3**[1] 若存在 $F_2^n$ 的一个 $\lceil n/2 \rceil$ 维仿射子空间 $V$，使 $f(x) \in B_n$ 在 $V$ 上的限制为常数(或仿射函数)，则称 $f(x)$ 是(弱)正规的。更一般地，若存在 $F_2^n$ 的一个 $k$ $(1 \le k \le n)$ 维仿射子空间 $V$，使 $f(x)$ 在 $V$ 上的限制为常数(仿射函数)，则称函数 $f(x)$ 为 $k$-(弱)正规的。

**定义 4**[7] 设 $f(x) \in B_n$，若存在一偶数 $r$ $(0 \le r \le n)$，使得对 $\forall \alpha \in F_2^n$，$F(f+\varphi_\alpha) \in \{0, \pm 2^{n-(r/2)}\}$，则称 $f(x)$ 为 $n$ 元 $r$ 阶的 Plateaued 函数，或裕度为 $2^{n-(r/2)}$ 的 Plateaued 函数。

由 Plateaued 函数的定义，不难得到下面的性质：

**性质 1** 设 $f(x) \in B_n$，

(1)若 $f(x)$ 为 $r$ 阶的 Plateaued 函数，则 $r$ 定为偶数；

(2) $f(x)$ 为 $n$ 阶的 Plateaued 函数当且仅当 $f(x)$ 为 Bent 函数；

(3) $f(x)$ 为 0 阶的 Plateaued 函数当且仅当 $f(x)$ 为仿射函数。

## 3 Plateaued 函数的正规性及其判定算法

文献[13]中给出了布尔函数与其分解函数的 Walsh 变换之间关系的一个重要结论：

**引理 1** 设 $f(x) \in B_n$，$V$ 为 $F_2^n$ 的一个 $k$ 维子空间，$f(x)$ 关于 $V$ 的分解函数序列为 $\{f\phi_{b+V} \mid b \in W\}$，简记为 $\{f_b \mid b \in W\}$，其中 $V \times W = F_2^n$，则

$$\sum_{v \in V^\perp} F^2(f+\varphi_v) = 2^{n-k} \sum_{b \in W} F^2(f_b) \tag{3}$$

$$\sum_{v \in V^\perp} (-1)^{b \cdot v} F(f+\varphi_v) = 2^{n-k} F(f_b) \tag{4}$$

由式(3)，不难推出：

$$\sum_{b \in W} F^2(f_b) \le \max_{\alpha \in F_2^n} \left|F^2(f+\varphi_\alpha)\right| \tag{5}$$

基于引理 1，我们可以得到 Plateaued 函数正规性的如下结论：

**定理 1** 设 $f(x) \in B_n$ 为一 $r$ 阶 Plateaued 函数 $(0 \le r \le n)$，令 $n - r/2 = k$，并设 $V$ 为 $F_2^n$ 的一个 $k$ 维子空间，$b+V$ 为 $V$ 的陪集，其中 $V \times W = F_2^n$，$b \in W$，则

(1) $f(x)$ 在 $b+V$ 上为常数当且仅当对 $\forall v \in V^\perp$，都有 $(-1)^{b \cdot v} F(f+\varphi_v) = 2^k$ 或 $-2^k$。

(2)若 $f(x)$ 在 $V$ 的某一陪集上为常数，则 $f(x)$ 在 $V$ 的其他陪集上为平衡函数。

**证明** (1)必要性因 $f(x)$ 在 $b+V$ 上为常数，则 $F(f_b) = \pm 2^k$，从而由式(4)，有

$$\sum_{v \in V^\perp} (-1)^{b \cdot v} F(f+\varphi_v) = 2^{n-k} F(f_b) = \pm 2^n \tag{6}$$

同时由 Plateaued 函数的定义可知，对 $\forall v \in V^\perp$，有 $\left|F(f+\varphi_v)\right| \le 2^k$，则要使式(6)成立其左端和式中的每一项都必同为 $2^k$ 或 $-2^k$。即对 $\forall v \in V^\perp$，都有 $(-1)^{b \cdot v} F(f+\varphi_V) = 2^k$ 或 $-2^k$。

充分性 因对 $\forall v \in V^\perp$，都有 $(-1)^{b \cdot v} F(f+\varphi_v) = 2^k$ 或 $-2^k$，根据式(4)可知，$\sum_{v \in V^\perp} (-1)^{b \cdot v} F(f+\varphi_v) = \pm 2^n = 2^{n-k} F(f_b)$，从而 $F(f_b) = \pm 2^k$，即 $f(x)$ 在 $b+V$ 上为常数。

(2)设 $\{f_b \mid b \in W\}$ 为 $f(x)$ 关于 $V$ 的分解序列，其中 $V \times W = F_2^n$，若 $f(x)$ 在 $b+V$ 上为常数，则 $F^2(f_b) = 2^{2k}$。由引理 1 中的式(5)可知，

$$2^{2k} \le \sum_{b \in W} F^2(f_b) \le \max_{\alpha \in F_2^n} \left|F^2(f+\varphi_\alpha)\right| = 2^{2k} \tag{7}$$

从而对 $\forall a \in W$ 且 $a \ne b$，有 $F(f_a) = 0$，即 $f(x)$ 在 $a+V$ 上为平衡函数。 证毕

定理 1 表明：

(1)若 $r$ 阶 Plateaued 函数 $f(x)$ 为 $k$- 正规的，则 $\left|F(f)\right| = 2^k$，即 $f(x)$ 为非平衡的，这也说明了这类函数的密码性质缺陷。同时也表明了非 $k$- 正规 Plateaued 函数的存在性，如：平衡的 Plateaued 函数便为非 $k$- 正规的。

(2)定理 1 刻画了 Plateaued 函数为 $k$- 正规时的情形，此时，$n/2 \le k = n - r/2 \le n$。显然，若 $f(x)$ 为 $k$- 正规的，则 $f(x)$ 定为正规的。

由定理 1 的结论(2)，我们不难得到如下的推论。

**推论 1** 设 $f(x) \in B_n$ 为一 $r$ 阶 Plateaued 函数 $(0 \le r \le n)$，并设 $V$ 为 $F_2^n$ 的一个 $k$ 维子空间，$b+V$ 为 $V$ 的陪集，其中 $V \times W = F_2^n$，$b \in W$，若 $f(x)$ 在 $V$ 的某一陪集 $b+V$ 上是不平衡的且不为常数，则 $f(x)$ 在 $V$ 的其他任一陪集上都不为常数。

文献[2,3]中分别给出了任一布尔函数正规性的判定算法及其改进算法，其算法都基于对所有的 $\le k$ 维的仿射子空间进行判断，而这是一项非常巨大的工程。基于定理 1 和推论 1 的结论，我们可以得到如下较为简单的判定 Plateaued 函数正规性的算法。本算法只需判断 $k$ 维的仿射子空间，且由推论 1，若存在 $V$ 的某一陪集 $b+V$，使得 $f(x)$ 在其上既不平衡又不为常数，则不需再判断 $V$ 的其他陪集。

**Input:** Plateaued function $f \in B_n$

**Output:** If $f$ is $k$-normal, return True; else return False

Return_Value=False;

For all the $k$-dimensional subspace $V$, do

If $F(f\phi_V) \in \{\pm 2^k\}$, Return_Value=True;

If Return_Value=True, Break;

For all $b \in W$, do

If $F(f\phi_V) \notin \{0, \pm 2^k\}$, Break;

Else if $F(f\phi_V) \in \{\pm 2^k\}$, Return_Value=True, Break;

同时，基于布尔函数与其分解函数非线性度之间的关系，我们可以得到 Plateaued 函数正规阶的上界。

**引理 2**[4] 设 $f(x) \in B_n$，$V$ 为 $F_2^n$ 的一个 $k$ 维子空间，$g(x)$ 为 $f(x)$ 在 $V$ 上的限制，则 $f(x)$ 与 $g(x)$ 之间的非线性度满足：

$$N_f \le 2^{n-1} - 2^{k-1} + N_g \tag{8}$$

由上引理及 Plateaued 函数的定义不难得到下面的推论。

**推论 2** 设 $f(x) \in B_n$ 为一 $r$ 阶 Plateaued 函数，则 $f(x)$ 不可能为 $l(l \ge n - r/2 + 1)$ 正规的。

## 4 已知 Plateaued 函数类的正规性

对 Plateaued 函数，主要有以下 3 类直接构造方法：

**构造法 1**：M-M 构造法，具有形式

$$f_{\phi,h}(x,y) = x \cdot \phi(y) \oplus h(y) \tag{9}$$

其中 $r,s$ 为任意的正整数，$n = r+s$，$x \in F_2^r$，$y \in F_2^s$，$\phi : F_2^s \to F_2^r$，$h : F_2^s \to F_2$。

Carlet[8] 指出，Zheng 和 Zhang[7] 提出的 Plateaued 函数的构造方法也是属于 M-M 类的。并指出当 $\phi$ 为单射(或 $\phi$ 为 $2 \to 1$)时，$f_{\phi,h}$ 便是裕度为 $2^r$ ($2^{r+1}$)的 Plateaued 函数。

显然，当取 $y$ 为常数时，$f_{\phi,h}$ 为 $x$ 的仿射函数，即 $f_{\phi,h}$ 为 $r$ 弱正规的，这类函数本质上为仿射函数的毗连，而仿射函数为密码性质弱函数，这就表明了这类函数的局限性。

**命题 1** 由 M-M 构造法所生成的 Plateaued 函数是 $r$ 弱正规的。

**构造法 2** $M'$ 构造法

基于 M-M 构造法毗连的是仿射函数这一弱点，Carlet 在文献[8]中提出了 $M'$ 构造法，通过毗连二次函数得到如下形式的函数：

$$f_{\psi,\phi,g}(x,y) = \bigoplus_{i=1}^{t} x_{2i-1}x_{2i}\psi_i(y) \oplus x \cdot \phi(y) \oplus g(y) \tag{10}$$

其中 $t = \lfloor r/2 \rfloor$，$s = n - r$，$x \in F_2^r, y \in F_2^s$，$\psi : F_2^s \to F_2^t$，$\phi : F_2^s \to F_2^r$，$g : F_2^s \to F_2$。

并指出，当满足一定条件时 $f_{\psi,\phi,g}$ 可为 Plateaued 函数。

表面上看，所构造的 $f_{\psi,\phi,g}$ 为二次函数的毗连，但当 $\bigcap_{i=1}^{t} \psi_i^{-1}(0)$ 非空时，$M'$ 变退化成了 M-M 型，为 $r$ 弱正规的。其次，若令 $x' = (x_1, x_3, \cdots x_{2t-1})$，$x'' = (x_2, x_4, \cdots, x_{2t})$，则当取 $(x', y)$ 或 $(x'', y)$ 为常数时，$f_{\psi,\phi,g}$ 也为 $x$ 的仿射函数，即 $f_{\psi,\phi,g}$ 为 $k = n - r/2$ 弱正规的。因而 $M'$ 构造法相对于 M-M 型构造法并没有本质上的突破。

**命题 2** 由 $M'$ 构造法所生成的 Plateaued 函数是 $k(k = n - r/2)$ 弱正规的。

**构造法 3** $Q$ 构造法

在文献[8]中，Carlet 还提出了一种毗连二次函数的方法，指出当满足一定条件时，由该方法也能得到 Plateaued 函数。所构造的函数具有形式

$$f_{\phi_1,\phi_2,\phi_3,g}(x,y) = (x \cdot \phi_1(y))(x \cdot \phi_2(y)) \oplus x \cdot \phi_3(y) \oplus g(y) \tag{11}$$

其中，$x \in F_2^r, y \in F_2^s$，$s + r = n$，$\phi_1, \phi_2, \phi_3 : F_2^s \to F_2^r$，$g : F_2^s \to F_2$。

形式上看，$Q$ 构造法所毗连的二次函数具有更一般的形式，但从正规性这一角度这类构造法所构造的函数与 $M'$ 构造法所构造出的函数相比并没有本质的不同。因为当取 $y$ 为常数时，$f_{\phi_1,\phi_2,\phi_3,g}(x,y) = (x \cdot \mu)(x \cdot \nu) \oplus x \cdot \phi_3(y) \oplus g(y)$ (其中 $\mu, \nu$ 为常数)，但文献[14]中指出所有的二次布尔函数都仿射等价于 $x_1x_2 + \cdots x_{2i-1}x_{2i} + \cdots x_{2t-1}x_{2t} + l(x)$，其中 $l(x)$ 为仿射函数。即就正规性而言，$M'$ 构造法和 $Q$ 构造法本质

上是一致的。

**命题 3** 由$Q$构造法所生成的 Plateaued 函数是$k(k=n-r/2)$弱正规的。

## 5 结束语

本文分析了具有良好密码学性质的 Plateaued 函数的正规性，指出非正规的 Plateaued 函数是存在的。给出了判定给定的 Plateaued 函数正规性的一个较为简单的算法，并分析了已知的 Plateaued 函数类的正规性。在后续的工作中，我们将研究更一般的非正规 Plateaued 函数的构造。

## 参 考 文 献


[1] Dobbertin H. Constructions of bent functions and balanced Boolean functions with high nonlinearity [C]. Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag, 1994, 1008: 61–74.

[2] Daum M, Dobbertin H, and Leander G. An algorithm for checking normality of Boolean functions [C]. Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003), Versailles, France, 2003: 133–142.

[3] Braeken A, Wolf C, and Preneel B. A randomised algorithm for checking the normality of cryptographic Boolean functions [C]. IFIP TCS, Kluwer, 2004: 51–66.

[4] Zheng Y, Zhang X M, and Imai H. Restriction, terms and nonlinearity of Boolean functions [J]. *Theoretical Computer Science*, 1999, 226(1): 207–223.

[5] 张卫国, 丁勇, 张宁,肖国镇. 代数免疫布尔函数的一个特征 [J]. 北京邮电大学学报, 2007, 30(5): 55–57.
Zhang Wei-guo, Ding Yong, Zhang Ning, and Xiao Guo-zhen. A characterization of algebraic immune Boolean functions [J]. *Journal of Beijing University of Posts and Telecommunications*, 2007, 30(5): 55–57.

[6] Canteaut A, Daum M, Dobbertin H, and Leauder G. Normal and Non Normal Bent Functions [C]. Proceedings of the 2003 Inernational Workshop on Coding and Cryptography (WCC 2003), Versailles, France, 2003: 91–100.

[7] Zheng Y, Zhang X M. Plateaued functions [C]. Advances in Cryptology, ICICS'99, Lecture Notes in Computer Science, Ed., Springer-Verlag, 1999, 1726: 284–300.

[8] Carlet C and Prouff E. On Plateaued functions and their constructions [C]. Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag, 2003, 2887: 54–73.

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

[10] Zhang W. Construction of plateaued functions satisfying multiple criteria [J]. *High Technology Letters*, 2005, 11(4): 364–366.

[11] 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 Bin, Jin Chen-hui, and Feng Chun-hai. Cryptographic properties of plateaued functions [J]. *Journal of Electronics & Information Technology*, 2008, 30(3): 660–664.

[12] 金栋梁, 赵亚群. 多输出 plateaued 函数的性质和构造[J]. 电子与信息学报, 2008, 30(12): 2991–2995.
Jin Dong-liang and Zhao Ya-qun. On properties and constructions of multi-output plateaued functions [J]. *Journal of Electronics & Information Technology*, 2008, 30(12): 2991–2995.

[13] Canteaut A, Carlet C, and Charpin P. On cryptographic properties of the cosets of R(1,m) [J]. *IEEE Transactions on Information Theory*, 2001, 47(4): 1494–1513.

[14] Mac Williams F J and Sloane N J. The Theory of Error-Correcting Codes [M], North-Holland, Amsterdam, 1977.



王维琼： 女，1979 年生，博士生，从事信息论与密码理论研究.

周 宇： 男，1980 年生，博士生，从事密码函数和序列密码理论研究.

肖国镇： 男，1934 年生，教授，博士生导师，主要从事密码理论、信息论与编码理论研究.