

p -元广义 plateaued 函数及其对偶

赵正俊 袁 哲 何 晴

安庆师范大学数理学院 安庆 246133

E-mail: ztywmm@aqnu.edu.cn; Yuanz2306@163.com; Heqing2225@163.com

摘 要 Plateaued 函数是一类具有理想密码学特性的密码函数. 在奇特征的情形下, 模仿经典 bent 函数的 Maiorana–McFarland 构造, 本文首先构造了广义 Walsh–Hadamard 变换具有两两互不相交支集的广义 s -plateaued 函数, 以此为基础, 构造了 p -元广义 bent 函数, 继而, 利用得到的广义 bent 函数, 构造支集两两互不相交的广义 plateaued 函数. 对于对偶函数是相对 (广义) bent 函数的 (广义) plateaued 函数 f , 利用代数数论中分圆域的相关结论, 本文证明了 $f^{**}(x) = f(-x)$.

关键词 广义 plateaued 函数; Walsh–Hadamard 变换; 弱正则; 对偶

MR(2020) 主题分类 11T71, 94A60, 06E30

中图分类 O156

On p -Ary Gplateaued Functions and Their Duals

Zhengjun Zhao Zhe Yuan Qing He

School of Mathematics and Physics, Anqing Normal University, Anqing 246133, P. R. China

E-mail: ztywmm@aqnu.edu.cn; Yuanz2306@163.com; Heqing2225@163.com

Abstract Plateaued functions are important cryptographic functions due to their various desirable cryptographic characteristics. Having provided a method to produce a set of s -gplateaued functions with Walsh–Hadamard transforms having pairwise disjoint support, p -ary gbent functions are constructed using gplateaued functions as building blocks. Recursively, the resulting functions are used as building blocks to construct gplateaued functions having pairwise disjoint supports. By a result on cyclotomic fields, a simple proof of $f^{**}(x) = f(-x)$ for plateaued functions and gplateaued functions is presented. Some properties of correlation spectrum of gbent function are presented also in this paper.

Keywords gplateaued funtions; Walsh–Hadamard transform; weakly regular; dual

MR(2020) Subject Classification 11T71, 94A60, 06E30

Chinese Library Classification O156

收稿日期: 2024-10-08; 接受日期: 2026-01-06

基金项目: 国家自然科学基金资助项目 (11971382); 安徽省高校学科 (专业) 拔尖人才项目 (gxbjZD2022035)

通讯作者: 赵正俊

1 引言

非线性性和平衡度是密码函数设计最重要的两个指标. 上世纪六十年代, Rothaus^[26] 引进了 Boolean bent 函数. 由于高非线性性, Boolean bent 函数在密码学和编码理论中起着重要的作用. 1985 年, Kumar 等人^[14] 将 Boolean bent 函数的概念推广至剩余类环上. 然而, 由于缺乏平衡度, bent 函数并非是完全令人满意的密码函数. 为了便于设计具有良好密码学特性的函数, Zheng 和 Zhang^[32] 引进了 Boolean plateaued 函数的概念. 此类函数具有理想的密码学特性, 例如, 高非线性性、低自相关性及高代数次数等. Boolean plateaued 函数和 p -元 plateaued 函数与编码理论、序列及图论也密切相关, 因此, 在过去的十年中, 受到研究者的广泛关注 (参见 [1, 4, 12, 21, 22, 24, 25, 30]).

设 p 是素数, n 是正整数, V_n 是有限域 $\mathbb{F}_p$ 上的 n 维线性空间. 对于函数 $f: V_n \rightarrow \mathbb{F}_p$, 当 $p=2$ 时, 称 f 是 V_n 上的 Boolean 函数, 否则, 称 f 是 V_n 上的 p -元函数. 令 $\langle \cdot, \cdot \rangle$ 是 V_n 上的 (非退化) 内积. 通常情况下, 当 $V_n = \mathbb{F}_p^n$ 时, $\langle a, x \rangle$ 表示向量的点乘 $a \cdot x$; 当 $V_n = \mathbb{F}_{p^n}$ 时, $\langle a, x \rangle$ 表示 $\text{Tr}_n(ax)$, 这里 Tr_n 表示有限域 $\mathbb{F}_{p^n}$ 上的绝对迹. 如果 $n = n_1 + \cdots + n_t$, $V_n = V_{n_1} \times \cdots \times V_{n_t}$, 对于 $a = (a_1, \dots, a_t)$, $x = (x_1, \dots, x_t) \in V_n$, V_n 上的内积定义为 $\langle a, x \rangle = \langle a_1, x_1 \rangle + \cdots + \langle a_t, x_t \rangle$.

众所周知, Walsh-Hadamard 变换是研究 V_n 上函数性质的重要工具. 设 $f: V_n \rightarrow \mathbb{F}_p$, $\zeta_p = e^{2\pi i/p}$ 是复数域中的本原 p 次单位根, 称函数

$$\hat{f}: V_n \rightarrow \mathbb{C}, \quad a \mapsto \sum_{x \in V_n} \zeta_p^{f(x) - \langle a, x \rangle}$$

是 f 的 **Walsh-Hadamard 变换**. 容易验证, 对任意 $x \in V_n$,

$$\zeta_p^{f(x)} = \frac{1}{p^n} \sum_{a \in V_n} \hat{f}(a) \zeta_p^{\langle a, x \rangle},$$

称之为 **Walsh-Hadamard 逆变换**. 如果对任意 $a \in V_n$, $|\hat{f}(a)| = p^{\frac{n}{2}}$, 称 f 是 **bent 函数**. 当 $p=2$ 时, 注意到 $\hat{f}(a)$ 是整数, 因此, 当 f 是 bent 函数时, n 是偶数. 而当 $p>2$ 时, 对任意正整数 n , V_n 上存在 bent 函数. 由于二元情形下奇数维线性空间上不存在 bent 函数, 研究人员提出了 near-bent 函数的概念^[15], 并将其推广至奇特征的情形^[3].

设 s 是非负整数, $f: V_n \rightarrow \mathbb{F}_p$. 如果对任意 $a \in V_n$, $|\hat{f}(a)| \in \{0, p^{\frac{n+s}{2}}\}$, 称 f 是 **s -plateaued 函数**. 由 Parseval 等式可知, 0-plateaued 函数即为 bent 函数. 1-plateaued 函数即为 near-bent 函数, 2-plateaued 函数称为 semi-bent 函数. 设 f 是 V_n 上的 s -plateaued 函数, 称

$$\text{supp}(\hat{f}) = \{a \in V_n : \hat{f}(a) \neq 0\}$$

为 $\hat{f}$ 的**支集**. 根据 Parseval 等式可知, $\text{supp}(\hat{f})$ 中元素个数为 p^{n-s} .

设 $f: V_n \rightarrow \mathbb{F}_p$ 是 p -元 s -plateaued 函数, $a \in \text{supp}(\hat{f})$. 根据定义容易计算,

$$\hat{f}(a) = \begin{cases} \pm p^{\frac{n+s}{2}} \zeta_p^{f^*(a)}, & p^{n+s} \equiv 1 \pmod{4}; \\ \pm i p^{\frac{n+s}{2}} \zeta_p^{f^*(a)}, & p^{n+s} \equiv 3 \pmod{4}, \end{cases}$$

这里 i 是复本原 4 次单位根, f^* 是定义在 $\text{supp}(\hat{f})$ 上的 p -元函数, 称之为 f 的**对偶函数** (参见 [10, 14, 24]). 为了方便讨论, 定义

$$\theta_f(a) = p^{-\frac{n+s}{2}} \zeta_p^{-f^*(a)} \hat{f}(a), \quad \epsilon_f(a) = \xi^{-1} \theta_f(a), \quad a \in \text{supp}(\hat{f}),$$

其中, 当 $p^{n+s} \equiv 1 \pmod{4}$ 时, $\xi = 1$, 当 $p^{n+s} \equiv 3 \pmod{4}$ 时, $\xi = i$, ϵ_f 是由 $\text{supp}(\hat{f})$ 到 $\{\pm 1\}$ 的函数. 类似于 bent 函数, 当 θ_f 是常值函数时, 称 f 是弱正则函数, 否则, 称之为非弱正则函数. 进一步地, 如果对任意 $a \in V_n$, $\theta_f(a) = 1$, 称 f 是正则函数. 通常情况下, 验证 p -元函数是否是 s -plateaued 函数是通过计算 $\hat{f}(a)$ 模的平方来实现. 但是, 这种方法不能说明函数的 (弱) 正则性. 事实上, 对 $a \in \text{supp}(\hat{f})$, 明确刻画 $\theta_f(a)$ 和 $f^*(a)$ 是非常困难的.

近二十年来, 理论计算机学家和从事密码学研究的代数学家对满足特定性质的 bent 函数的构造给予了极大的关注. 众所周知^[10, 30], 弱正则 bent 函数的对偶函数也是 bent 函数. 通过计算机验证, Helleseth 和 Kholosha^[10] 给出了第一个非弱正则 bent 函数的例子. 从已有的结果中可以看出, bent 函数的经典构造方法都构造出弱正则 bent 函数. Çeşmelioglu 等人在文献 [3] 中首次构造出无穷多个非弱正则 bent 函数. 2016 年, 利用所谓的 bent 函数的半直和, Çeşmelioglu 等人^[7] 首次构造出对偶函数不是 bent 函数的非弱正则 bent 函数. 最近, Wang 和 Fu^[30] 将文献 [7] 中的结果推广至广义 bent 函数的情形, 构造出对偶函数是或者不是广义 bent 函数的广义 bent 函数. 需要指出的是, 以上构造方法均以 bent 函数或者广义 bent 函数作为构造基础. 模拟经典 Lagrange 插值, Çeşmelioglu 等人^[4, 6] 以 near-bent 函数和 plateaued 函数为基础, 构造出弱正则和非弱正则 bent 函数.

受文献 [3, 4, 6] 及 [30] 中结果和方法的启发, 本文以广义 plateaued 函数为基础, 构造对偶函数是弱正则和非弱正则 bent 函数的广义 bent 函数. 继而, 再以得到的广义 bent 函数为基础, 构造 Walsh-Hadamard 变换支集两两互不相交的广义 plateaued 函数. 对任意 p -元弱正则 bent 函数 f , 由 Walsh-Hadamard 逆变换容易验证 $f^{**}(x) = f(-x)$. 通过细致的值分布计算, Özbudak 和 Pelen^[24] 证明该结论对对偶函数是 bent 函数的非弱正则 bent 函数和对偶函数是相对 bent 函数的 plateaued 函数也成立. 最近, 通过分析素数在分圆域中的分解状况, Wang 和 Fu^[30] 给出了该结论更为简洁的证明. 利用文献 [30] 中的想法, 本文将该结论推广至广义 p -元 s -plateaued 函数的情形.

本文的安排如下. 在第 2 节中, 简单回顾下文所需分圆域和 p -元函数的相关定义和结论. 为了文章的完整可读性, 第 3 节讨论了广义 p -元函数自相关谱的相关性质. 在第 4 节中, 以广义 s -plateaued 函数为基础, 构造弱正则和非弱正则广义 bent 函数, 同时, 明确刻画构造函数的对偶函数. 对于对偶函数是相对 bent 的 (广义) s -plateaued 函数 f , 第 5 节将证明 $f^{**}(x) = f(-x)$. 最后一节对本文进行总结.

2 预备知识

如无特别声明, 下文沿用本节所用记号和术语.

设 p 是奇素数, k, n 是正整数, $\zeta_{p^k} = e^{2\pi i/p^k}$ 是复本原 p^k 次单位根, $\mathbb{Z}_{p^k}$ 是模 p^k 的剩余类环. 首先简单回顾下文所需的分圆域的相关知识.

设 K 和 $\mathcal{O}_K$ 是 p^k 次分圆域 $\mathbb{Q}(\zeta_{p^k})$ 及其代数整数环, W_K 是 $\mathcal{O}_K$ 的单位根群. 不难计算,

$$W_K = \{\pm \zeta_{p^k}^j : 0 \leq j \leq p^k - 1\},$$

且 $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^k}]$ (参见 [8, 13]). 下列引理源于 [14] 中的性质 7, 该结论对 p -元函数的 bent 性与 Walsh-Hadamard 变换研究起着重要作用.

引理 2.1 ([23, 引理 2]) 设 $\alpha \in \mathcal{O}_K$, 如果 $|\alpha| = p^{\frac{n}{2}}$, 那么, $\frac{\alpha}{\sqrt{p^{*n}}} \in W_K$, 其中 $p^* = (-1)^{\frac{p-1}{2}} p$.

令 $\mathcal{P}$ 表示 $1 - \zeta_{p^k}$ 生成的主理想, 即, $\mathcal{P} = (1 - \zeta_{p^k})\mathcal{O}_K$. 由文献 [8] 中定理 2.14 可知, $\mathcal{P}$ 是素理想, $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, 且 $p\mathcal{O}_K = \mathcal{P}^{f(p^k)}$, 即, p 在 K 中完全分歧. 因此, 对于 $K/\mathbb{Q}$ 的任意中间域 M , p 在 M 中完全分歧. 注意到, 对任意正整数 $1 \leq l \leq k$ 及与 p 互素的正整数 m , $(1 - \zeta_{p^k}^m)\mathcal{O}_K = \mathcal{P}$, 且 $[K : \mathbb{Q}(\zeta_{p^l})] = p^{k-l}$. 下列关于分圆域的结论对本文 plateaued 函数对偶函数的讨论至关重要, 文献 [30] 给出了详细证明.

引理 2.2 ([30, 引理3]) 设 $1 \leq m < p^k$ 是正整数, $m = p^s \tilde{m}$, 其中, $0 \leq s < k$, $\gcd(p, \tilde{m}) = 1$. 那么, $1 + \zeta_{p^k}^m$ 是 $\mathcal{O}_K$ 中单位, 且 $(1 - \zeta_{p^k}^m)\mathcal{O}_K = \mathcal{P}^{p^s}$.

2018 年, Mesnager 等人 [23] 推广了广义 Boolean bent 函数, 提出了广义 p -元 bent 函数的概念. 利用划分产生的仿射空间, Mesnager 等人完全刻画了广义 p -元 bent 函数. 2022 年, 受文献 [7] 中相关工作的启发, Wang 和 Fu [30] 给出了广义 p -元 bent 函数的间接构造. 下面具体给出广义 p -元 bent 函数相关定义和结果.

沿用引言中的记号, V_n 到 $\mathbb{Z}_{p^k}$ 中的函数称为 V_n 上的 **广义 p -元函数**. 类似于 p -元函数的情形, 广义 Walsh-Hadamard 变换是研究广义 p -元函数的有力工具. 设 $f : V_n \rightarrow \mathbb{Z}_{p^k}$ 是广义 p -元函数, 对于 $a \in V_n$, 称

$$\hat{f} : V_n \rightarrow \mathbb{C}, \quad a \mapsto \sum_{x \in V_n} \zeta_{p^k}^{f(x)} \zeta_p^{-\langle a, x \rangle}$$

是 f 的 **广义 Walsh-Hadamard 变换**. 如果对每个 $a \in V_n$, $|\hat{f}(a)| = p^{\frac{n}{2}}$, 称 f 是 V_n 上的 **广义 p -元 bent 函数**, 简称 gbent 函数. 设 s 是非负整数, f 是 V_n 上的广义 p -元函数. 如果对任意 $a \in V_n$, 有 $|\hat{f}(a)| \in \{0, p^{\frac{n+s}{2}}\}$, 称 f 是 V_n 上的 **广义 p -元 s -plateaued 函数**, 简称 s -gplateaued 函数. Mesnager 等人在文献 [22] 中研究了 s -gplateaued 函数的性质, 利用广义 p -元函数的分支函数及 admissible plateaued 函数刻画了 s -gplateaued 函数.

类似于 s -plateaued 函数, s -gplateaued 函数的支集中也包含 p^{n-s} 个元素. 对于 $a \in V_n$, 利用引理 2.1 可得

$$\hat{f}(a) = \begin{cases} \pm p^{\frac{n+s}{2}} \zeta_{p^k}^{f^*(a)}, & p^{n+s} \equiv 1 \pmod{4}; \\ \pm i p^{\frac{n+s}{2}} \zeta_{p^k}^{f^*(a)}, & p^{n+s} \equiv 3 \pmod{4}. \end{cases}$$

由此, 定义

$$\theta_f(a) = p^{-\frac{n+s}{2}} \zeta_{p^k}^{-f^*(a)} \hat{f}(a), \quad \epsilon_f(a) = \xi^{-1} \theta_f(a), \quad a \in \text{supp}(\hat{f}),$$

其中, 当 $p^{n+s} \equiv 1 \pmod{4}$ 时, $\xi = 1$, 当 $p^{n+s} \equiv 3 \pmod{4}$ 时, $\xi = i$, ϵ_f 是由 $\text{supp}(\hat{f})$ 到 $\{\pm 1\}$ 的函数. 因此, 模拟 s -plateaued 函数, 可以类似地定义 s -gplateaued 函数的 (弱) 正则性与非弱正则性.

3 gbent 函数的相关谱

众所周知, 相关谱是研究 Boolean 函数 bent 性的另一个有力工具 (参见 [27]). 我们自然期望, 广义 p -元函数的相关谱也能成为研究该类函数 bent 性的有用工具. 为此, 首先给出下列记号和术语.

设 f, g 是 V_n 上的两个广义 p -元函数, $a \in V_n$, 称

$$C_{f,g}(a) = \sum_{x \in V_n} \zeta_{p^k}^{f(x+a)-g(x)}$$

为 f 与 g 在点 a 处的交叉相关, 并称 $C_{f,f}(a)$ 为 f 在点 a 处的自相关, 简记为 $C_f(a)$. 由定义容易验证 $\overline{C_{g,f}(a)} = C_{f,g}(-a)$.

下列论断反映了广义 p -元函数的交叉相关与广义 Walsh-Hadamard 变换之间的关系.

引理 3.1 设 f, g 是 V_n 上的两个广义 p -元函数, 那么, 对任意 $x \in V_n$,

$$C_{f,g}(x) = \frac{1}{p^n} \sum_{a \in V_n} \hat{f}(a) \overline{\hat{g}(a)} \zeta_p^{\langle a, x \rangle}.$$

证明 根据交叉相关和广义 Walsh-Hadamard 变换的定义直接计算可得

$$\begin{aligned} \frac{1}{p^n} \sum_{a \in V_n} \hat{f}(a) \overline{\hat{g}(a)} \zeta_p^{\langle a, x \rangle} &= \frac{1}{p^n} \sum_{a, y, z \in V_n} \zeta_{p^k}^{f(y)-g(z)} \zeta_p^{\langle a, x \rangle - \langle a, y \rangle + \langle a, z \rangle} \\ &= \frac{1}{p^n} \sum_{y, z \in V_n} \zeta_{p^k}^{f(y)-g(z)} \sum_{a \in V_n} \zeta_p^{\langle a, x-y+z \rangle} \\ &= \sum_{z \in V_n} \zeta_{p^k}^{f(z+x)-g(z)} \\ &= C_{f,g}(x). \end{aligned}$$

证毕.

由上述引理容易验证下列两个等式.

推论 3.2 同于上述引理的记号, 对任意 $x \in V_n$,

$$C_f(x) = \frac{1}{p^n} \sum_{a \in V_n} |\hat{f}(a)|^2 \zeta_p^{\langle a, x \rangle}, \quad \sum_{a \in V_n} C_{f,g}(a) \zeta_p^{-\langle a, x \rangle} = \hat{f}(x) \overline{\hat{g}(x)}.$$

证明 在上述引理中令 $f = g$ 可得第一个等式. 对于第二个等式,

$$\begin{aligned} \sum_{a \in V_n} C_{f,g}(a) \zeta_p^{-\langle a, x \rangle} &= \frac{1}{p^n} \sum_{a \in V_n} \sum_{y \in V_n} \hat{f}(y) \overline{\hat{g}(y)} \zeta_p^{\langle a, y \rangle - \langle a, x \rangle} \\ &= \frac{1}{p^n} \sum_{y \in V_n} \hat{f}(y) \overline{\hat{g}(y)} \sum_{a \in V_n} \zeta_p^{\langle a, y-x \rangle} \\ &= \hat{f}(x) \overline{\hat{g}(x)}. \end{aligned}$$

证毕.

类似于 Boolean 函数的情形, 广义 p -元函数的自相关可以用来判断函数是否是 gbent 函数. 利用上述引理, 不难得到下列结论.

定理 3.3 设 f 是 V_n 上的广义 p -元函数, 那么, f 是 gbent 函数当且仅当, 对任意非零元素 $a \in V_n$, $C_f(a) = 0$.

证明 设 f 是 gbent 函数, 根据上述推论, 对任意非零元素 $a \in V_n$,

$$C_f(a) = \sum_{b \in V_n} \zeta_p^{\langle b, a \rangle} = 0.$$

必要性得证. 注意到, 对任意 $b \in V_n$,

$$\begin{aligned} |\hat{f}(b)|^2 &= \sum_{x, y \in V_n} \zeta_{p^k}^{f(x)-f(y)} \zeta_p^{-\langle b, x \rangle + \langle b, y \rangle} \\ &= \sum_{x, y \in V_n} \zeta_{p^k}^{f(x)-f(y)} \zeta_p^{-\langle b, x-y \rangle} \end{aligned}$$

$$\begin{aligned} & \frac{z=x-y}{\sum_{z \in V_n}} \zeta_p^{-\langle b, z \rangle} \sum_{y \in V_n} \zeta_{p^k}^{f(y+z)-f(y)} \\ &= \sum_{z \in V_n} \zeta_p^{-\langle b, z \rangle} C_f(z). \end{aligned}$$

如果对任意非零元素 $z \in V_n$, $C_f(z) = 0$, 根据上述等式, 对任意 $b \in V_n$, $|\hat{f}(b)|^2 = p^n$, 从而, f 是 gbent 函数. 证毕.

设 $f: V_n \rightarrow \mathbb{Z}_{p^k}$ 是广义 p -元函数, $a \in V_n$, $\alpha \in \mathbb{Z}_{p^k}$, 令

$$V_{a,\alpha} = \{x \in V_n : f(x+a) - f(x) = \alpha\},$$

$N_{a,\alpha}$ 表示 $V_{a,\alpha}$ 中元素个数. 显然, 对任意非零元素 $a \in V_n$,

$$\sum_{\alpha \in \mathbb{Z}_{p^k}} N_{a,\alpha} = p^n.$$

如果 $k < n$, 且对任意 $\alpha, \beta \in \mathbb{Z}_{p^k}$, $N_{a,\alpha} = N_{a,\beta}$, 则 $N_{a,\alpha} = p^{n-k}$, 即, $f(x+a) - f(x)$ 作为 V_n 到 $\mathbb{Z}_{p^k}$ 中的函数, $\mathbb{Z}_{p^k}$ 中每个元素均有 p^{n-k} 个原像.

命题 3.4 设 $f: V_n \rightarrow \mathbb{Z}_{p^k}$ 是广义 p -元函数, $k < n$. 如果对任意非零元素 $a \in V_n$, $f(x+a) - f(x)$ 作为 V_n 到 $\mathbb{Z}_{p^k}$ 中的函数, $\mathbb{Z}_{p^k}$ 中每个元素均有 p^{n-k} 个原像, 那么, f 是 gbent 函数.

证明 注意到, 对任意非零元素 $a \in V_n$,

$$\begin{aligned} C_f(a) &= \sum_{x \in V_n} \zeta_{p^k}^{f(x+a)-f(x)} \\ &= \sum_{\alpha \in \mathbb{Z}_{p^k}} \sum_{x \in V_{a,\alpha}} \zeta_{p^k}^{f(x+a)-f(x)} \\ &= \sum_{\alpha \in \mathbb{Z}_{p^k}} N_{a,\alpha} \zeta_{p^k}^\alpha. \end{aligned}$$

如果对任意 $\alpha \in \mathbb{Z}_{p^k}$, $N_{a,\alpha} = p^{n-k}$, 则

$$C_f(a) = p^{n-k} \sum_{\alpha \in \mathbb{Z}_{p^k}} \zeta_{p^k}^\alpha = 0.$$

根据上述定理, f 是 gbent 函数. 证毕.

注 3.5 这里需要指出, 当 $k = 1$ 时, 上述命题的逆命题也成立, 即, 当 f 是 V_n 上的经典 bent 函数时, 对任意非零元素 $a \in V_n$, $f(x+a) - f(x)$ 作为 V_n 到 $\mathbb{Z}_p$ 中的函数, $\mathbb{Z}_p$ 中每个元素均有 p^{n-1} 个原像. 事实上, 满足这样条件的函数称之为完全非线性函数. 因此, 当 $k = 1$ 时, f 是 bent 函数当且仅当 f 是完全非线性函数. 更加一般地, 有下列结论成立.

命题 3.6 设 $f, g: V_n \rightarrow \mathbb{F}_p$ 是两个 p -元函数, $\alpha \in \mathbb{F}_p$, $a \in V_n$ 是非零元素, $V_{a,\alpha}$ 与 $N_{a,\alpha}$ 分别表示集合 $\{x \in V_n : f(x+a) - g(x) = \alpha\}$ 及其中元素个数. 那么, $C_{f,g}(a) = 0$ 当且仅当对任意 $\alpha \in \mathbb{F}_p$, $N_{a,\alpha} = p^{n-1}$.

证明 注意到,

$$\sum_{\alpha \in \mathbb{F}_p} N_{a,\alpha} = p^n, \quad C_{f,g}(a) = \sum_{\alpha \in \mathbb{F}_p} N_{a,\alpha} \zeta_p^\alpha.$$

充分性可由第二个等式直接得到. 因为 $\sum_{i=0}^{p-1} x^i$ 是 ζ_p 在 $\mathbb{Q}$ 上的极小多项式, 且 $N_{a,\alpha}$ 是整数, 所以, 当 $C_{f,g}(a) = 0$ 时, $\sum_{i=0}^{p-1} x^i$ 整除 $\sum_{\alpha \in \mathbb{F}_p} N_{a,\alpha} x^\alpha$, 从而, 对每个 $\alpha \in \mathbb{F}_p$, $N_{a,\alpha}$ 均相同. 结合该事实与上述第一个等式可知, 对任意 $\alpha \in \mathbb{F}_p$, $N_{a,\alpha} = p^{n-1}$. 证毕.

4 gbent 函数的构造

本节以 (plateaued 函数) gplateaued 函数为基础, 构造 (bent 函数) gbent 函数. 为了说明下列讨论的合理性, 模仿 Maiorana-McFarland 构造, 首先给出生成广义 Walsh-Hadamard 变换具有两两互不相交支集的 s -gplateaued 函数的方法.

设 $s < n$ 是正整数, $f: V_{n-s} \rightarrow \mathbb{Z}_{p^k}$ 是 gbent 函数. 对每个 $u = (u_1, \dots, u_s) \in \mathbb{F}_p^s$, 定义

$$f_u(x, y): V_{n-s} \times \mathbb{F}_p^s \rightarrow \mathbb{Z}_{p^k}, \quad (x, y) \mapsto f(x) + p^{k-1}u \cdot y.$$

对任意 $(a, b) \in V_{n-s} \times \mathbb{F}_p^s$, 有

$$\begin{aligned} \widehat{f_u}(a, b) &= \sum_{x \in V_{n-s}} \sum_{y \in \mathbb{F}_p^s} \zeta_{p^k}^{f_u(x, y)} \zeta_p^{-\langle a, x \rangle - b \cdot y} \\ &= \sum_{x \in V_{n-s}} \zeta_{p^k}^{f(x)} \zeta_p^{-\langle a, x \rangle} \sum_{y \in \mathbb{F}_p^s} \zeta_p^{(u-b) \cdot y} \\ &= \widehat{f}(a) \sum_{y \in \mathbb{F}_p^s} \zeta_p^{(u-b) \cdot y}, \end{aligned}$$

由此可得

$$\widehat{f_u}(a, b) = \begin{cases} p^s \widehat{f}(a), & b = u; \\ 0, & b \neq u. \end{cases}$$

因为 f 是 V_{n-s} 上的 gbent 函数, 所以, 当 $b = u$ 时, $|\widehat{f_u}(a, b)| = p^{\frac{n+s}{2}}$, 否则, $\widehat{f_u}(a, b) = 0$. 因此, f_u 是 $V_{n-s} \times \mathbb{F}_p^s$ 上的 s -gplateaued 函数, 且 $\text{supp}(\widehat{f_u}) = \{(a, u) \mid a \in V_{n-s}\}$. 这样可得到一族广义 Walsh-Hadamard 变换具有两两互不相交支集的 s -gplateaued 函数. 这里值得注意的是, 对每个 $u \in \mathbb{F}_p^s$, $\theta_{f_u} = \theta_f$, 且当 f 是 (弱, 非弱) 正则函数时, f_u 均为 (弱, 非弱) 正则函数. 进一步地, 对每个 $u \in \mathbb{F}_p^s$, 假设 $\tilde{f}_u: V_{n-s} \rightarrow \mathbb{Z}_{p^k}$ 是 gbent 函数, 则 $f_u(x, y) = \tilde{f}_u(x) + p^{k-1}u \cdot y$ 是 $V_{n-s} \times \mathbb{F}_p^s$ 上的 s -gplateaued 函数, 且对 $u \neq v \in \mathbb{F}_p^s$, $\text{supp}(\widehat{f_u}) \cap \text{supp}(\widehat{f_v}) = \emptyset$. 注意到, $\theta_{f_u} = \theta_{\tilde{f}_u}$, f_u 是否是弱正则函数取决于 $\tilde{f}_u$.

下面讨论利用 s -gplateaued 函数构造 gbent 函数. 对每个 $y \in \mathbb{F}_p^s$, 设 $f_y: V_n \rightarrow \mathbb{Z}_{p^k}$ 是 s -plateaued 函数, 且对任意 $y_1 \neq y_2 \in \mathbb{F}_p^s$, $\text{supp}(\widehat{f_{y_1}}) \cap \text{supp}(\widehat{f_{y_2}}) = \emptyset$. 结合条件与支集中的元素个数可知,

$$V_n = \bigcup_{y \in \mathbb{F}_p^s} \text{supp}(\widehat{f_y}).$$

定义

$$F(x, y): V_n \times \mathbb{F}_p^s \rightarrow \mathbb{Z}_{p^k}, \quad (x, y) \mapsto f_y(x).$$

易证, F 是 $V_n \times \mathbb{F}_p^s$ 上的 gbent 函数. 进一步地, 有下列结论成立.

定理 4.1 沿用上述记号和术语, $F(x, y)$ 是 $V_n \times \mathbb{F}_p^s$ 上的 gbent 函数, 且对偶函数为

$$F^*(x, y): V_n \times \mathbb{F}_p^s \rightarrow \mathbb{Z}_{p^k}, \quad (x, y) \mapsto f_z^*(x) - p^{k-1}y \cdot z,$$

其中 $x \in \text{supp}(\hat{f}_z)$. 若对每个 $y \in \mathbb{F}_p^s$, f_y 是 V_n 上的 gbent 函数, 那么, $F^*(x, y)$ 是 $V_n \times \mathbb{F}_p^s$ 上的 gbent 函数, 且 $F^{**}(x, y) = F(-x, -y)$.

证明 对任意 $(a, b) \in V_n \times \mathbb{F}_p^s$,

$$\begin{aligned}\hat{F}(a, b) &= \sum_{x \in V_n} \sum_{y \in \mathbb{F}_p^s} \zeta_{p^k}^{F(x, y)} \zeta_p^{-\langle a, x \rangle - b \cdot y} \\ &= \sum_{y \in \mathbb{F}_p^s} \zeta_p^{-b \cdot y} \sum_{x \in V_n} \zeta_{p^k}^{f_y(x)} \zeta_p^{-\langle a, x \rangle} \\ &= \sum_{y \in \mathbb{F}_p^s} \zeta_p^{-b \cdot y} \hat{f}_y(a).\end{aligned}$$

注意到, 存在唯一的 $z \in \mathbb{F}_p^s$ 使得 $a \in \text{supp}(\hat{f}_z)$. 对这样的 $z \in \mathbb{F}_p^s$ 有

$$\hat{F}(a, b) = \zeta_p^{-b \cdot z} \hat{f}_z(a).$$

因为 $\hat{f}_z(a) = \theta p^{\frac{n+s}{2}} \zeta_{p^k}^{f_z^*(a)}$, 其中 $\theta \in \{\pm 1, \pm i\}$ 取决于 a, z , 所以,

$$\hat{F}(a, b) = \theta p^{\frac{n+s}{2}} \zeta_{p^k}^{f_z^*(a) - p^{k-1}b \cdot z}, \quad |\hat{F}(a, b)| = p^{\frac{n+s}{2}},$$

从而, F 是 $V_n \times \mathbb{F}_p^s$ 上的 gbent 函数, 且对偶函数为 $f_z^*(x) - p^{k-1}y \cdot z$.

设对每个 $y \in \mathbb{F}_p^s$, f_y 是 V_n 上的 gbent 函数. 对任意 $(a, b) \in V_n \times \mathbb{F}_p^s$, 有

$$\begin{aligned}\widehat{F^*}(a, b) &= \sum_{x \in V_n} \sum_{y \in \mathbb{F}_p^s} \zeta_{p^k}^{F^*(x, y)} \zeta_p^{-\langle a, x \rangle - b \cdot y} \\ &= \sum_{y \in \mathbb{F}_p^s} \zeta_p^{-b \cdot y} \sum_{x \in V_n} \zeta_{p^k}^{F^*(x, y)} \zeta_p^{-\langle a, x \rangle} \\ &= \sum_{y \in \mathbb{F}_p^s} \zeta_p^{-b \cdot y} \sum_{z \in \mathbb{F}_p^s} \sum_{x \in \text{supp}(\hat{f}_z)} \zeta_{p^k}^{f_z^*(x) - p^{k-1}y \cdot z} \zeta_p^{-\langle a, x \rangle} \\ &= \sum_{z \in \mathbb{F}_p^s} \sum_{x \in \text{supp}(\hat{f}_z)} \zeta_{p^k}^{f_z^*(x)} \zeta_p^{-\langle a, x \rangle} \sum_{y \in \mathbb{F}_p^s} \zeta_p^{-y \cdot (b+z)} \\ &= p^s \sum_{x \in \text{supp}(\hat{f}_{-b})} \zeta_{p^k}^{f_{-b}^*(x)} \zeta_p^{-\langle a, x \rangle}.\end{aligned}\tag{4.1}$$

注意到, 对 V_n 上的弱正则 s -gplateaued 函数 f 及 $a \in \text{supp}(\hat{f})$, 有

$$\hat{f}(a) = \theta p^{\frac{n+s}{2}} \zeta_{p^k}^{f^*(a)},$$

其中 $\theta \in \{\pm 1, \pm i\}$ 与 a 无关, 且

$$\begin{aligned}p^n \zeta_{p^k}^{f(x)} &= \sum_{a \in V_n} \hat{f}(a) \zeta_p^{\langle a, x \rangle} \\ &= \sum_{a \in \text{supp}(\hat{f})} \hat{f}(a) \zeta_p^{\langle a, x \rangle} \\ &= \theta p^{\frac{n+s}{2}} \sum_{a \in \text{supp}(\hat{f})} \zeta_{p^k}^{f^*(a)} \zeta_p^{\langle a, x \rangle}.\end{aligned}$$

因此,

$$\sum_{a \in \text{supp}(\hat{f})} \zeta_{p^k}^{f^*(a)} \zeta_p^{\langle a, x \rangle} = \theta^{-1} p^{\frac{n-s}{2}} \zeta_{p^k}^{f(x)}.\tag{4.2}$$

结合 (4.1) 与 (4.2) 可得

$$\widehat{F^*}(a, b) = p^s \theta_b p^{\frac{n-s}{2}} \zeta_p^{f_{-b}(-a)} = \theta_b p^{\frac{n+s}{2}} \zeta_p^{f_{-b}(-a)},$$

其中 $\theta_b \in \{\pm 1, \pm i\}$ 取决于 b . 从而, F^* 是 $V_n \times \mathbb{F}_p^s$ 上的 gbent 函数, 且

$$F^{**}(x, y) = f_{-y}(-x) = F(-x, -y).$$

证毕.

由上述定理的证明过程可知, F 是弱正则 gbent 函数当且仅当, 对每个 $y \in \mathbb{F}_p^s$, f_y 是弱正则 s -gplateaued 函数, 且 θ_{f_y} 均相同, 即与 y 的选取无关. 根据本节第 2 段的论述, 满足这种条件的 s -gplateaued 函数存在. 上述定理的证明过程与文献 [3, 4, 6] 中由 near-bent 函数和 plateaued 函数构造 bent 函数的过程类似. 尽管 Çeşmelioglu 和 Meidl [4] 利用 Lagrange 插值给出了 F 的具体表达式, 但并未刻画 F 的对偶函数及其弱正则性. 这里给出的 gbent 函数的构造可以认为是文献 [3, 4, 6] 中部分结果的推广. 例如, 文献 [4] 中定理 2 是上述定理 $k=1$ 时结论的一部分, 而当 $k=s=1$ 时, 上述定理的结果即为文献 [3] 中定理 2.1 和文献 [6] 中定理 1.

设 $f_z : V_n \rightarrow \mathbb{Z}_{p^k}$ 是 gbent 函数, $z \in \mathbb{F}_p^s$. 定义

$$F_z(x, y) : V_n \times \mathbb{F}_p^s \rightarrow \mathbb{Z}_{p^k}, \quad (x, y) \mapsto f_z(x) + p^{k-1}y \cdot z. \quad (4.3)$$

由本节第 2 段的论述可知, F_z 是 $V_n \times \mathbb{F}_p^s$ 上的 s -gplateaued 函数, 且

$$\text{supp}(\widehat{F_z}) = \{(a, z) : a \in V_n\}.$$

因此, 如果对每个 $z \in \mathbb{F}_p^s$, f_z 是 V_n 上的 gbent 函数, F_z 是 $V_n \times \mathbb{F}_p^s$ 上的 s -gplateaued 函数, 且对任意 $z_1 \neq z_2 \in \mathbb{F}_p^s$, $\text{supp}(\widehat{F_{z_1}}) \cap \text{supp}(\widehat{F_{z_2}}) = \emptyset$. 定义

$$F(x, y, z) : V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s \rightarrow \mathbb{Z}_{p^k}, \quad (x, y, z) \mapsto F_z(x, y). \quad (4.4)$$

根据上述定理, F 是 $V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ 上的 gbent 函数. 事实上, 可以进一步刻画其对偶函数.

定理 4.2 设 $f_z : V_n \rightarrow \mathbb{Z}_{p^k}$ 是 gbent 函数, $z \in \mathbb{F}_p^s$. 按照 (4.3) 和 (4.4) 分别定义 F_z 和 F . 那么, F 是 $V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ 上的 gbent 函数, 且对偶函数为 $F^*(x, y, z) = f_y^*(x) - p^{k-1}y \cdot z$. 如果对每个 $z \in \mathbb{F}_p^s$, f_z 是 V_n 上的 gbent 函数, 那么, F^* 也是 $V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ 上的 gbent 函数, 且 $F^{**}(x, y, z) = f_{-z}^*(x) + p^{k-1}y \cdot z$.

证明 对任意 $(a, b, c) \in V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$, 有

$$\begin{aligned} \widehat{F}(a, b, c) &= \sum_{x \in V_n} \sum_{y \in \mathbb{F}_p^s} \sum_{z \in \mathbb{F}_p^s} \zeta_p^{f_z(x) + p^{k-1}y \cdot z} \zeta_p^{-\langle a, x \rangle - b \cdot y - c \cdot z} \\ &= \sum_{x \in V_n} \sum_{z \in \mathbb{F}_p^s} \zeta_p^{f_z(x)} \zeta_p^{-\langle a, x \rangle - c \cdot z} \sum_{y \in \mathbb{F}_p^s} \zeta_p^{(z-b) \cdot y} \\ &= p^s \zeta_p^{-b \cdot c} \sum_{x \in V_n} \zeta_p^{f_b(x)} \zeta_p^{-\langle a, x \rangle} \\ &= p^s \zeta_p^{-b \cdot c} \widehat{f_b}(a) \\ &= \theta_{b,c} p^{\frac{n+2s}{2}} \zeta_p^{f_b^*(a) - p^{k-1}b \cdot c}, \end{aligned}$$

其中 $\theta_{b,c} \in \{\pm 1, \pm i\}$ 取决于 b, c . 因此, F 是 $V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ 上的 gbent 函数, 并且, 对偶函数为 $F^*(x, y, z) = f_y^*(x) - p^{k-1}y \cdot z$. 设对每个 $z \in \mathbb{F}_p^s$, f_z 是 V_n 上的 gbent 函数, 结合 F^* 的表达式及

对 F 的证明过程可知, F^* 也是 $V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ 上的 gbent 函数, 且 $F^{**}(x, y, z) = f_{-z}^{**}(x) + p^{k-1}y \cdot z$. 证毕.

设 f 是 V_n 上的弱正则 bent 函数. 利用 Walsh-Hadamard 逆变换可知, 对任意 $x \in V_n$, $f^{**}(-x) = f(x)$. 事实上, 该结论对对偶函数是 bent 函数的非弱正则 bent 函数也成立. 通过分析对偶函数的值分布, Özbudak 和 Pelen^[24] 于 2020 年给出了该结论的证明. 最近, 利用分圆域中素理想的分解, Wang 和 Fu^[30] 给出了该结论一个简洁而优美的证明. 在下一节中, 我们将证明该结论对对偶函数是相对 gbent 函数的 gplateaued 函数也是成立的. 利用该论断容易得到下列结论.

推论 4.3 设对每个 $z \in \mathbb{F}_p^s$, $f_z(x) : V_n \rightarrow \mathbb{Z}_{p^k}$ 是对偶函数是 gbent 函数的 gbent 函数, 按照 (4.3) 和 (4.4) 定义 F_z 和 F . 那么,

$$F^{**}(-x, -y, -z) = F(x, y, z), \quad F^{****}(x, y, z) = F(x, y, z).$$

证明 由定理 4.2 可知, F^* 是 $V_n \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ 上的 gbent 函数. 结合 F^* 的 gbent 性及前段的论述, 两个等式容易验证. 证毕.

注意到, 第一个等式可由 F^{**} 的表达式直接验证. 因为 $F^{**}(x, y, z) = f_{-z}^{**}(x) + p^{k-1}y \cdot z$, 所以

$$\begin{aligned} F^{**}(-x, -y, -z) &= f_{-z}^{**}(-x) + p^{k-1}(-y) \cdot (-z) \\ &= f_z(x) + p^{k-1}y \cdot z \\ &= F(x, y, z). \end{aligned}$$

下面给出两个 gbent 函数构造的例子结束本节.

例 4.4 设 $p = 3$, $n = 6$, $s = 2$, $k = 3$. 对任意 $u = (u_1, u_2) \in \mathbb{F}_3^2$, 定义

$$f_u(x) : \mathbb{F}_3^6 \rightarrow \mathbb{Z}_{3^3}, \quad x = (x_1, \dots, x_6) \mapsto (x_1x_3 + x_2x_4 + u_1x_5 + u_2x_6)3^2 + x_43 + x_3.$$

对 $x = (x_1, \dots, x_6) \in \mathbb{F}_3^6$, 令 $\tilde{x} = (x_3, \dots, x_6) \in \mathbb{F}_3^4$. 则, 对任意 $a = (a_1, \dots, a_6) \in \mathbb{F}_3^6$, 有

$$\begin{aligned} \widehat{f_u}(a) &= \sum_{x \in \mathbb{F}_3^6} \zeta_{3^3}^{f_u(x)} \zeta_3^{-a \cdot x} \\ &= \sum_{\tilde{x} \in \mathbb{F}_3^4} \zeta_{3^3}^{x_43 + x_3} \zeta_3^{-\tilde{a} \cdot \tilde{x} + u_1x_5 + u_2x_6} \sum_{x_1, x_2 \in \mathbb{F}_3} \zeta_3^{(x_3 - a_1, x_4 - a_2) \cdot (x_1, x_2)} \\ &= 3^2 \zeta_{3^3}^{a_23 + a_1} \zeta_3^{-a_1a_3 - a_2a_4} \sum_{x_5, x_6 \in \mathbb{F}_3} \zeta_3^{(u_1 - a_5, u_2 - a_6) \cdot (x_5, x_6)}. \end{aligned}$$

由此可得

$$\widehat{f_u}(a) = \begin{cases} 3^4 \zeta_{3^3}^{(-a_1a_3 - a_2a_4)3^2 + a_23 + a_1}, & (a_5, a_6) = u; \\ 0, & (a_5, a_6) \neq u. \end{cases}$$

因此, f_u 是由 $\mathbb{F}_3^6$ 到 $\mathbb{Z}_{3^3}$ 的正则 2-gplateaued 函数, 且广义 Walsh-Hadamard 变换的支集为

$$\text{supp}(\widehat{f_u}) = \{(\tilde{a}, u) : \tilde{a} \in \mathbb{F}_3^4\}.$$

由此得到 9 个广义 Walsh-Hadamard 变换的支集两两互不相交的 2-gplateaued 函数. 下面, 再以这些 gplateaued 函数为基础, 利用定理 4.1 构造正则 gbent 函数. 定义

$$F(x, y) : \mathbb{F}_3^6 \times \mathbb{F}_3^2 \rightarrow \mathbb{Z}_{3^3}, \quad (x, y) \mapsto (x_1x_3 + x_2x_4 + y_1x_5 + y_2x_6)3^2 + x_43 + x_3,$$

其中, $x = (x_1, \dots, x_6) \in \mathbb{F}_3^6, y = (y_1, y_2) \in \mathbb{F}_3^2$. 根据定理 4.1 可知, F 是 $\mathbb{F}_3^8$ 上的正则 gbent 函数. 继而, 再以这些 gbent 函数为基础构造 gbent 函数. 定义

$$G(x, y, z) : \mathbb{F}_3^6 \times \mathbb{F}_3^2 \times \mathbb{F}_3^2 \rightarrow \mathbb{Z}_{3^3},$$

$$(x, y, z) \mapsto (x_1x_3 + x_2x_4 + z_1x_5 + z_2x_6 + y_1z_1 + y_2z_2)3^2 + x_43 + x_3,$$

其中, $x = (x_1, \dots, x_6) \in \mathbb{F}_3^6, y = (y_1, y_2), z = (z_1, z_2) \in \mathbb{F}_3^2$. 根据定理 4.2 可知, G 是 $\mathbb{F}_3^{10}$ 上的 gbent 函数.

Helleseth 和 Kholosha^[10] 给出了第一个非弱正则 bent 函数的例子. 下面, 以这个非弱正则 bent 函数为基础, 给出构造非弱正则 gbent 函数的例子.

例 4.5 令 ω 是 $\mathbb{F}_{3^6}$ 的本原元素, 则 $f(x) = \text{Tr}_6(\omega^7 x^{98})$ 是 $\mathbb{F}_{3^6}$ 上的非弱正则 bent 函数. 设 $u = (u_1, u_2) \in \mathbb{F}_3^2$, 定义

$$f_u(x, y) : \mathbb{F}_{3^6} \times \mathbb{F}_3^2 \rightarrow \mathbb{Z}_{3^3}, \quad (x, y) \mapsto 3^2(f(x) + u \cdot y).$$

对任意 $a \in \mathbb{F}_{3^6}, b = (b_1, b_2) \in \mathbb{F}_3^2$, 根据本节第 2 段中的 Walsh-Hadamard 逆变换公式可得

$$\widehat{f_u}(a, b) = \widehat{f}(a) \sum_{y \in \mathbb{F}_3^2} \zeta_3^{(u-b) \cdot y},$$

从而,

$$\widehat{f_u}(a, b) = \begin{cases} 3^2 \widehat{f}(a), & b = u; \\ 0, & b \neq u. \end{cases}$$

由此可得 $|\widehat{f_u}(a, b)| \in \{0, 3^{\frac{8+2}{2}}\}$, 即, f_u 是 $\mathbb{F}_{3^6} \times \mathbb{F}_3^2$ 上的 2-gplateaued 函数, 且

$$\text{supp}(\widehat{f_u}) = \{(x, u) : x \in \mathbb{F}_{3^6}\}.$$

由此得到 9 个广义 Walsh-Hadamard 变换的支集两两互不相交的非弱正则 2-gplateaued 函数. 定义

$$F(x, y, z) : \mathbb{F}_{3^6} \times \mathbb{F}_3^2 \times \mathbb{F}_3^2 \rightarrow \mathbb{Z}_{3^3}, \quad (x, y, z) \mapsto 3^2(f(\omega^7 x^{98}) + y \cdot z).$$

则 F 是 $\mathbb{F}_{3^6} \times \mathbb{F}_3^2 \times \mathbb{F}_3^2$ 上的非弱正则 gbent 函数. 进一步地, 定义

$$G(x, y, z, w) : \mathbb{F}_{3^6} \times \mathbb{F}_3^2 \times \mathbb{F}_3^2 \times \mathbb{F}_3^2 \rightarrow \mathbb{Z}_{3^3}, \quad (x, y, z, w) \mapsto 3^2(f(\omega^7 x^{98}) + (y + w) \cdot z).$$

则 G 是 $\mathbb{F}_{3^6} \times \mathbb{F}_3^2 \times \mathbb{F}_3^2 \times \mathbb{F}_3^2$ 上的非弱正则 2-gplateaued 函数.

5 plateaued 函数与 gplateaued 函数的对偶

正如在上一节所指出的, 当 $f : V_n \rightarrow \mathbb{F}_p$ 是对偶函数为 bent 函数的 bent 函数时, 对任意 $x \in V_n$, 有 $f^{**}(x) = f(-x)$. Özbudak 和 Pelen^[24] 证明了该结论对 s -plateaued 函数也成立. 借助文献 [30] 中的方法, 本节给出该结论一个简洁的证明, 并且证明该结论对 s -gplateaued 函数也成立. 为此, 首先引入下列记号和定义.

对于 V_n 上的 s -plateaued 函数 f 及 $a \in \text{supp}(\widehat{f})$, $\theta_f(a)$ 可以表示为 $\xi \epsilon_f(a)$, 其中, $\xi \in \{1, i\}$, $\epsilon_f(a) \in \{\pm 1\}$. 注意到, 当 $p \equiv 1 \pmod{4}$ 或者 n 是偶数时, $\xi = 1$, 当 $p \equiv 3 \pmod{4}$ 且 n 是奇数时, $\xi = i$. 因为 f^* 是 $\text{supp}(\widehat{f})$ 上的 p -元函数, 且 $\text{supp}(\widehat{f})$ 中有 p^{n-s} 个元素, 下列定义可以认为是 bent 函数概念的推广 (参见 [24]).

定义 5.1 设 S 是 V_n 的含有 N 个元素的子集, $f: S \rightarrow \mathbb{F}_p$ 是 p -元函数, $a \in V_n$, 定义

$$\hat{f}(a) = \sum_{x \in S} \zeta_p^{f(x) - \langle a, x \rangle}.$$

如果对任意 $a \in V_n$, $|\hat{f}(a)| = N^{1/2}$, 称 f 是相对于 S 的 bent 函数.

相对 bent 函数在 plateaued 函数构造过程中是常见的. 下面给出一个相对 bent 函数的例子.

例 5.2 设 p 是奇素数, m 是正整数, 定义

$$f: \mathbb{F}_p^{2m+1} \rightarrow \mathbb{F}_p, \quad (x_1, x_2, \dots, x_{2m+1}) \mapsto \sum_{i=1}^m x_i x_{i+m}.$$

不难验证, $-f$ 是相对 bent 函数. 事实上, $-f$ 是相对于 $\text{supp}(f)$ 的 bent 函数. 注意到, 对任意 $a = (a_1, a_2, \dots, a_{2m+1}) \in \mathbb{F}_p^{2m+1}$,

$$\begin{aligned} \hat{f}(a) &= \sum_{x \in \mathbb{F}_p^{2m+1}} \zeta_p^{f(x) - \langle a, x \rangle} \\ &= \sum_{x_{2m+1} \in \mathbb{F}_p} \zeta_p^{-a_{2m+1} x_{2m+1}} \sum_{(x_1, \dots, x_{2m}) \in \mathbb{F}_p^{2m}} \zeta_p^{\sum_{i=1}^m x_i x_{i+m} - \sum_{i=1}^{2m} a_i x_i}. \end{aligned}$$

当 $a_{2m+1} \neq 0$ 时, $\hat{f}(a) = 0$. 而当 $a_{2m+1} = 0$ 时,

$$\begin{aligned} \hat{f}(a) &= p \sum_{(x_1, \dots, x_m) \in \mathbb{F}_p^m} \zeta_p^{-\sum_{i=1}^m a_i x_i} \sum_{(x_{m+1}, \dots, x_{2m}) \in \mathbb{F}_p^m} \zeta_p^{\sum_{i=1}^m (x_i - a_i) x_{i+m}} \\ &= p p^m \zeta_p^{-\sum_{i=1}^m a_i a_{i+m}}. \end{aligned}$$

因此, f 是 1-plateaued 函数, 且 $\text{supp}(f) = \{(a_1, \dots, a_{2m}, 0) : a_i \in \mathbb{F}_p, 1 \leq i \leq 2m\}$. 由上述计算可知, 对任意 $x = (x_1, \dots, x_{2m}, 0) \in \text{supp}(f)$,

$$f^*(x) = -\sum_{i=1}^m x_i x_{i+m} = -f(x).$$

从而, 对任意 $a = (a_1, a_2, \dots, a_{2m+1}) \in \mathbb{F}_p^{2m+1}$,

$$\begin{aligned} \widehat{f^*}(a) &= \sum_{x \in \text{supp}(f)} \zeta_p^{f^*(x) - \langle a, x \rangle} \\ &= \sum_{(x_1, \dots, x_{2m}) \in \mathbb{F}_p^{2m}} \zeta_p^{-\sum_{i=1}^m x_i x_{i+m} - \sum_{i=1}^{2m} a_i x_i} \\ &= p^m \zeta_p^{-\sum_{i=1}^m a_i a_{i+m}}. \end{aligned}$$

进而, $|\widehat{f^*}(a)| = p^m = |\text{supp}(f)|^{1/2}$. 这说明, f^* 是相对于 $\text{supp}(f)$ 的 bent 函数, 且对任意 $x \in \mathbb{F}_p^{2m+1}$, $f^{**}(x) = f(x) = f(-x)$.

设 $N = p^m$, $m < n$, f 是相对于 S 的 bent 函数. 根据引理 2.1, 对任意 $a \in V_n$,

$$\hat{f}(a) = \xi_{\epsilon_f(a)} p^{\frac{m}{2}} \zeta_p^{f^*(a)}.$$

对于相对于 S 的 bent 函数, 可以类似于 bent 函数和 plateaued 函数定义其 (非) 弱正则性.

定理 5.3 设 $s < n$ 是正整数, $f: V_n \rightarrow \mathbb{F}_p$ 是 s -plateaued 函数, 且对偶函数 f^* 是相对于 $\text{supp}(\hat{f})$ 的 bent 函数. 那么, 对任意 $x \in V_n$, $f^{**}(x) = f(-x)$.

证明 注意到, 对任意 $x \in \text{supp}(\hat{f})$, $\hat{f}(x) = \xi \epsilon_f(x) p^{\frac{n+s}{2}} \zeta_p^{f^*(x)}$. 因此,

$$\zeta_p^{f^*(x)} = \xi^{-1} \epsilon_f(x) p^{-\frac{n+s}{2}} \hat{f}(x). \quad (5.1)$$

因为 f^* 是相对于 $\text{supp}(\hat{f})$ 的 bent 函数, 由定理前的论述可知, 对任意 $a \in V_n$,

$$\widehat{f^*}(a) = \xi \epsilon_{f^*}(a) p^{\frac{n-s}{2}} \zeta_p^{f^{**}(a)}. \quad (5.2)$$

另一方面,

$$\begin{aligned} \widehat{f^*}(a) &= \sum_{x \in \text{supp}(\hat{f})} \zeta_p^{f^*(x) - \langle a, x \rangle} \\ &\stackrel{(5.1)}{=} \xi^{-1} p^{-\frac{n+s}{2}} \sum_{x \in \text{supp}(\hat{f})} \epsilon_f(x) \hat{f}(x) \zeta_p^{-\langle a, x \rangle} \\ &= \xi^{-1} p^{-\frac{n+s}{2}} \sum_{x \in V_n} \epsilon_f(x) \hat{f}(x) \zeta_p^{-\langle a, x \rangle} \\ &= \xi^{-1} p^{-\frac{n+s}{2}} \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} - \xi^{-1} p^{-\frac{n+s}{2}} \sum_{\epsilon_f(x)=-1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} \\ &= 2\xi^{-1} p^{-\frac{n+s}{2}} \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} - \xi^{-1} p^{-\frac{n+s}{2}} \sum_{x \in V_n} \hat{f}(x) \zeta_p^{-\langle a, x \rangle}. \end{aligned} \quad (5.3)$$

由 Walsh-Hadamard 逆变换可得

$$\sum_{x \in V_n} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} = p^n \zeta_p^{f(-a)}. \quad (5.4)$$

结合 (5.3) 和 (5.4) 可知

$$\widehat{f^*}(a) = 2\xi^{-1} p^{-\frac{n+s}{2}} \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} - \xi^{-1} p^{\frac{n-s}{2}} \zeta_p^{f(-a)}. \quad (5.5)$$

再由 (5.2) 和 (5.5) 可得

$$2 \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} = p^n \zeta_p^{f(-a)} (1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{f^{**}(a) - f(-a)}). \quad (5.6)$$

为了简化记号, 令

$$T = \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle}, \quad \delta_a = f^{**}(a) - f(-a).$$

这样, (5.6) 可以表示为

$$2T = p^n \zeta_p^{f(-a)} (1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{\delta_a}). \quad (5.7)$$

下证, 对任意 $a \in V_n$, $\delta_a = 0$.

令 K 和 $\mathcal{O}_K$ 分别表示 p 次分圆域 $\mathbb{Q}(\zeta_p)$ 及其代数整数环. 由引理 2.2 可知, 对任意 $i \in \mathbb{F}_p^*$ (这里将 $\mathbb{F}_p$ 等同于 $\mathbb{Z}_p$), $1 + \zeta_p^i$ 是 $\mathcal{O}_K$ 中单位, 且 $(1 - \zeta_p^i)\mathcal{O}_K = (1 - \zeta_p)\mathcal{O}_K$ 是素理想. 显然, T 与 $p^n \zeta_p^{f(-a)} (1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{\delta_a})$ 是 K 中的代数整数. 假设存在 $a \in V_n$, 使得 $\delta_a \neq 0$. 因为 $\xi^2 \epsilon_{f^*}(a) = \pm 1$, 所以

$$(\zeta_p^{f(-a)} (1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{\delta_a}))\mathcal{O}_K = \mathcal{O}_K \quad \text{或} \quad (1 - \zeta_p)\mathcal{O}_K.$$

下面考虑 $2T$ 和 $p^n \zeta_p^{f(-a)}(1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{\delta_a})$ 生成的主理想. 注意到, $p\mathcal{O}_K = ((1 - \zeta_p)\mathcal{O}_K)^{p-1}$, 且 $(1 - \zeta_p)\mathcal{O}_K$ 是素理想. 则, 以上论述说明

$$(p^n \zeta_p^{f(-a)}(1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{\delta_a}))\mathcal{O}_K = ((1 - \zeta_p)\mathcal{O}_K)^{n(p-1)+\epsilon},$$

其中, 当 $\xi^2 \epsilon_{f^*}(a) = 1$ 时, $\epsilon = 0$, 当 $\xi^2 \epsilon_{f^*}(a) = -1$ 时, $\epsilon = 1$. 由于 Dedekind 整环中每个非零理想可以唯一地分解成素理想的乘积, 从而, 素理想 $(1 - \zeta_p)\mathcal{O}_K$ 整除 $2\mathcal{O}_K$, 进而, $(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = 2\mathbb{Z}$. 而 $(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$, 因此, $p = 2$, 矛盾. 定理得证.

上述定理的证明过程中等式 (5.7) 迫使 $\delta_a = 0$, 且 $1 + \xi^2 \epsilon_{f^*}(a) \zeta_p^{\delta_a} = 0$, 从而, 对任意 $a \in V_n$, $\sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} = 0$. 事实上, 上述定理的结论对 gplateaued 函数也成立. 类似地, 首先需要给出 s-gplateaued 函数的相对 gbent 的定义.

定义 5.4 设 S 是 V_n 的含有 N 个元素的子集, $f: S \rightarrow \mathbb{Z}_{p^k}$ 是广义 p -元函数, $a \in V_n$. 定义

$$\hat{f}(a) = \sum_{x \in S} \zeta_{p^k}^{f(x)} \zeta_p^{-\langle a, x \rangle}.$$

如果对任意 $a \in V_n$, $|\hat{f}(a)| = N^{1/2}$, 称 f 是相对于 S 的 gbent 函数.

类似于上述定理的证明, 不难验证下列结论.

推论 5.5 设 $s < n$ 是正整数, $f: V_n \rightarrow \mathbb{Z}_{p^k}$ 是 s -gplateaued 函数, 且对偶函数 f^* 是相对于 $\text{supp}(\hat{f})$ 的 gbent 函数. 那么, 对任意 $x \in V_n$, $f^{**}(x) = f(-x)$.

证明 该推论的证明过程与上述定理类似, 这里简要叙述. 同于上述定理的计算过程, 对任意 $a \in V_n$,

$$2 \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle} = p^n \zeta_{p^k}^{f(-a)} (1 + \xi^2 \epsilon_{f^*}(a) \zeta_{p^k}^{f^{**}(a) - f(-a)}). \quad (5.8)$$

令

$$T = \sum_{\epsilon_f(x)=1} \hat{f}(x) \zeta_p^{-\langle a, x \rangle}, \quad \delta_a = f^{**}(a) - f(-a).$$

假设存在 $a \in V_n$, 使得 $\delta_a \neq 0$. 沿用引理 2.2 的记号, T 是 K 中的代数整数. 再由该引理的结论可知,

$$(p^n \zeta_{p^k}^{f(-a)}(1 + \xi^2 \epsilon_{f^*}(a) \zeta_{p^k}^{\delta_a}))\mathcal{O}_K = \mathcal{P}^{n\varphi(p^k)+\epsilon},$$

其中, 当 $\xi^2 \epsilon_{f^*}(a) = 1$ 时, $\epsilon = 0$, 当 $\xi^2 \epsilon_{f^*}(a) = -1$ 时, $\epsilon = p^s$. 这里, s 是 δ_a 的分解中 p 的指数. 因此, 素理想 $\mathcal{P}$ 整除 2, 从而, $p = 2$, 矛盾. 因此, 对任意 $a \in V_n$, $\delta_a = 0$. 证毕.

6 总结

本文主要关注广义 p -元函数的相关问题. 相关谱是分析 Boolean 函数 bent 性的有力工具. 利用广义 p -元函数的交叉相关, 本文讨论了广义 p -元函数的 bent 性. 对于经典 p -元函数 f , f 是 bent 函数当且仅当 f 是完全非线性函数. 但对广义 p -元函数, 该结论不成立. 模仿 Maiorana-McFarland 构造方法, 本文给出了构造 Walsh-Hadamard 变换支集两两互不相交的 s -gplateaued 函数族的方法, 由此构造 gbent 函数, 并通过两个例子说明构造过程. 设 f 是对

偶函数相对于 Walsh-Hadamard 变换支集 gbent 的 s -gplateaued 函数, 利用分圆域中素理想的分解, 本文证明了 $f^{**}(x) = f(-x)$. 该结论推广了文献 [24] 中的定理 4.2.

致谢 感谢审稿人对本文提出的修改意见和建议.

参 考 文 献

- [1] Carlet C., Boolean and vectorial plateaued functions and APN functions, *IEEE Trans. Inform. Theory*, 2015, **61**(11): 6272–6289.
- [2] Carlet C., Mesnager S., Four decades of research on bent functions, *Des. Codes Cryptogr.*, 2016, **78**(1): 5–50.
- [3] Çeşmelioglu A., McGuire G., Meidl W., A construction of weakly and non-weakly regular bent functions, *J. Combinat. Theory A*, 2012, **119**(2): 420–429.
- [4] Çeşmelioglu A., Meidl W., A construction of bent functions from plateaued functions, *Des. Codes Cryptogr.*, 2013, **66**: 231–242.
- [5] Çeşmelioglu A., Meidl W., Pott A., A survey on bent functions and their duals, In: *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, Schmidt K.-U. and Winterhof A., Eds. Berlin, Germany: De Gruyter, 2019, 39–56.
- [6] Çeşmelioglu A., Meidl W., Pott A., On the dual of (non)-weakly regular bent functions and self-dual bent functions, *Adv. Math. Commun.*, 2013, **7**(4): 425–440.
- [7] Çeşmelioglu A., Meidl W., Pott A., There are infinitely many bent functions for which the dual is not bent, *IEEE Trans. Inform. Theory*, 2016, **62**(9): 5204–5208.
- [8] Feng K., *Algebraic Number Theory*, Harbin Institute Technology Press, Harbin, 2018.
- [9] Feng K., Luo J., Value distributions of exponential sums from perfect nonlinear functions and their applications, *IEEE Trans. Inform. Theory*, 2007, **53**(9): 3035–3041.
- [10] Helleseth T., Kholosha A., Monomial and quadratic bent functions over finite fields of odd characteristic, *IEEE Trans. Inform. Theory*, 2006, **52**(5): 2018–2032.
- [11] Hou X., p -ary and q -ary version of certain results about bent functions and resilient functions, *Finite Fields Appl.*, 2004, **10**(4): 566–582.
- [12] Hyun J., Lee J., Lee Y., Explicit criteria for construction of plateaued functions, *IEEE Trans. Inform. Theory*, **62**(12): 7555–7565.
- [13] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Springer, New York, 1990.
- [14] Kumar P., Scholtz R., Welch L., Generalized bent functions and their properties, *J. Combinat. Theory A*, 1985, **40**(1): 90–107.
- [15] Leander G., McGuire G., Construction of bent functions from near-bent functions, *J. Combinat. Theory A*, 2009, **116**(4): 960–970.
- [16] Lidl R., Niederreiter H., *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [17] Meidl W., A survey on p -ary and generalized bent functions, *Cryptogr. Commun.*, 2022, **14**: 737–782.
- [18] Meier W., Staffelbach O., Fast correlation attacks on stream ciphers, In: *Advances in Cryptology (Lecture Notes in Computer Science)*, Springer, Berlin, 1998, 301–314.
- [19] Mesnager S., *Bent Functions—Fundamentals Results*, Springer, Cham. Switzerland, 2016.
- [20] Mesnager S., On generalized hyper-bent functions, *Cryptogr. Commun.*, 2020, **12**: 455–468.
- [21] Mesnager S., Özbudak F., Sinak A., et al., On q -ary plateaued functions over $\mathbb{F}_q$ and their explicit characterizations, *European J. Combina.*, 2019, **80**: 71–81.
- [22] Mesnager S., Tang C., Qi Y., Generalized plateaued functions and admissible (plateaued) function, *IEEE Trans. Inform. Theory*, 2017, **63**(10): 6139–6148.
- [23] Mesnager S., Tang C., Qi Y., et al., Further results on generalized bent functions and their complete characterization, *IEEE Trans. Inform. Theory*, 2018, **64**(7): 5441–5452.
- [24] Özbudak F., Pelen R., Duals of non-weakly regular bent functions are not weakly regular and generalization to plateaued functions, *Finite Fields Appl.*, 2020, **64**: 101668.
- [25] Potapov V., On q -ary bent and plateaued functions, *Des. Codes Cryptogr.*, 2020, **88**: 2037–2049.

- [26] Rothaus O., On “bent” functions, *J. Combinat. Theory A*, 1976, **20**(3): 300–305.
- [27] Stănică P., Martinsen T., Gangopadhyay S., et al., Bent and generalized bent Boolean functions, *Des. Codes Cryptogr.*, 2013, **69**: 77–94.
- [28] Tan Y., Yang J., Zhang X., A recursive construction of p -ary bent function which are not weakly regular, In: Proc. IEEE Int. Conf. Inform. Theory Inf. Secur., Beijing, China, IEEE Computer Society, Piscataway, 2010, 156–159.
- [29] Tang C., Xiang C., Qi Y., et al., Complete characterization of generalized bent and 2^k -bent Boolean functions, *IEEE Trans. Inform. Theory*, 2017, **63**(7): 4668–4674.
- [30] Wang J., Fu F., On the duals of generalized bent functions, *IEEE Trans. Inform. Theory*, 2022, **68**(7): 4770–4781.
- [31] Zheng Y., Zhang X., On plateaued functions, *IEEE Trans. Inform. Theory*, 2001, **47**(3): 1215–1223.
- [32] Zheng Y., Zhang X., Plateaued functions, In: Information and Communication Security, Lecture Notes in Computer Science, Vol. 1726, Springer-Verlag, Berlin, 1999, 284–300.