中国科学: 数学 2017 年 第 47 卷 第 9 期: 995～1010
SCIENTIA SINICA Mathematica
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

一类 $\mathcal{PS}_{\mathrm{ap}}$ 向量 bent 函数的存在性

彭杰[1], TAN Chik How[2], 阚海斌[3*]

1. 上海师范大学数理学院, 上海 200234;
2. Temasek Laboratories, National University of Singapore, Singapore 117411, Singapore;
3. 复旦大学计算机科学技术学院, 上海 200433
E-mail: pengjie705@163.com, tsltch@nus.edu.sg, hbkan@fudan.edu.cn

收稿日期: 2016-07-18; 接受日期: 2017-02-22; 网络出版日期: 2017-06-09; * 通信作者
国家自然科学基金 (批准号: 61202471 和 61672166)、上海市优秀学术带头人计划 (批准号: 16XD1400200) 和上海市科技创新行动计划 (批准号: 16JC1402700) 资助项目

摘要 Bent 函数是非常特殊的组合对象, 在序列、差集、编码和密码等领域都有重要应用. 近年来, 形如 $\mathrm{Tr}_k^n(P(x))$ 的 bent 函数吸引了大量目光, 其中 $k=1$ 或 $k=n/2$ 且 $P(x)\in\mathbb{F}_{2^n}[x]$. 本文在前人研究的基础上进一步研究二项式函数 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+ax^{r(2^k-1)})$ $(k=n/2\geqslant 2)$ 的向量 bent 性, 其中 r 为奇数. 对于 $r\mid 2^k+1$ 的情形, 本文得到了 F 满足向量 bent 性的一个充要条件, 从而, 对所有 n 和 $a\in\mathbb{F}_{2^n}^*$ 都完全确定了 F 的向量 bent 性. 而对于 $r\nmid 2^k+1$ 的情形, Muratović-Ribić 等 (2014) 曾提出过不存在此类向量 bent 函数的猜想. 通过引入 Lucas 公式, 对 r 分别等于 5、7、9 及所有的 n 和 $a\in\mathbb{F}_{2^n}^*$, 本文也完全得到了 F 的向量 bent 性. 特别地, 本文找到了一些反例, 否定了 Muratović-Ribić 等 (2014) 提出的猜想.

关键词 向量 bent 函数 迹二项式函数 布尔函数 多项式系数 Lucas 公式
MSC (2010) 主题分类 11T06, 11T23, 11T71

1 引言

Bent 函数是由 Rothaus [1] 于 1976 年提出的一类非常重要的布尔函数. 这类函数和全体仿射布尔函数之间具有最大的 Hamming 距离. 它们在序列、差集、编码和密码等领域都有重要应用. 目前对 bent 函数已经有了大量研究, 但是对其进行完整的分类仍是一个遥不可及的目标, 并且看上去似乎是一项不可能完成的任务 (参见文献 [2]).

对迹函数表示的单项式 bent 函数, 即形如 $\mathrm{Tr}_1^n(ax^d)$ 的 bent 函数的构造已经有了较丰富的研究结果 (参见文献 [3–8]). 一些迹函数表示的二项式 bent 函数也已经被构造出来 (参见文献 [9–11]), 其中文献 [10,11] 是利用 Niho 型指数来进行构造.

Youssef 和 Gong [12] 提出了超 bent 函数的概念. 一个 n- 元布尔函数 f 称为是超 bent 的, 如果对任意与 2^n-1 互素的正整数 i, $f(x^i)$ 都是 bent 函数. 接着 Charpin 和 Gong [7] 利用 Dickson 多项式与 Kloosterman 和刻画了一类形如 $\sum_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^k-1)})$ 的超 bent 函数, 其中 $n=2k$, R 是模 2^k+1

英文引用格式: Peng J, Tan C H, Kan H B. On existence of vectorial bent functions from the $\mathcal{PS}_{\mathrm{ap}}$ class (in Chinese). Sci Sin Math, 2017, 47: 995–1010, doi: 10.1360/SCM-2016-0453

© 2017《中国科学》杂志社

的分圆陪集代表元集. 文献 [5] 证明了这样的超 bent 函数都属于 $\mathcal{PS}_{\rm ap}$ 类, 这是所谓的 partial spread ($\mathcal{PS}$) bent 函数类的一个子类 (参见文献 [13]). 近年来, 通过对这些函数添加一些小项得到了许多类似的超 bent 函数 (如文献 [14–19]).

布尔函数的 bent 和超 bent 性都可以很自然地推广到向量布尔函数上. 一个 m- 维的 n- 元向量布尔函数 $F=(f_1,\ldots,f_m):\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$ 称为是向量 bent 的, 如果它的分量函数 $f_1,\ldots,f_m$ 的所有非零线性组合都是 bent 函数, 等价地, 对任意的 $\lambda\in\mathbb{F}_{2^m}^*$, 布尔函数 $\mathrm{Tr}_1^m(\lambda F)$ 都是 bent 的. 函数 F 称为是向量超 bent 的, 如果对任意与 2^n-1 互素的正整数 i, $F(x^i)$ 都是向量 bent 函数. Nyberg [20] 证明了向量 bent 函数只有当 $m\leqslant n/2$ 时才存在, 还根据已知的 bent 函数构造了几类相应的向量 bent 函数. 此后又有更多的向量 bent 函数被找到 (参见文献 [21,22]). 这些构造都是通过合适地挑选出 m 个 bent 函数使得它们的所有非零线性组合都是 bent 函数的方法得到的. 此外, 形如

$$F(x)=\mathrm{Tr}_k^{2k}\left(\sum_{i=1}^{t}a_ix^{r_i(2^k-1)}\right)$$

的向量布尔函数的向量 bent 性还可以通过文献 [23] 介绍的方法直接验证.

对于单项式函数, 文献 [24] 证明了, 如果 x^d 是 $\mathbb{F}_{2^{2k}}$ 上的置换且 $\mathrm{Tr}_1^{2k}(ax^d)$ 是 bent 函数, 则 $\mathrm{Tr}_k^{2k}(ax^d)$ 是向量 bent 的. 多项式函数 $\mathrm{Tr}_m^n(\sum_{i=1}^r a_ix^{d_i})$ 的向量 bent 性与 $\mathrm{Tr}_1^n(\sum_{i=1}^r a_ix^{d_i})$ 的 bent 性之间也有类似的关系 (参见文献 [23]). 此外, 文献 [23] 还得到了 $F(x)=\mathrm{Tr}_m^n(\sum_{i=1}^t a_ix^{r_i(2^k-1)})$ 是向量 bent 函数的三个等价刻画. 其中一个非常重要的刻画是, F 为向量 bent 函数当且仅当 F 限制在 $\mathbb{F}_{2^{2k}}^*$ 的 2^k+1 阶子群 $\mathcal{U}$ 上时, $\mathbb{F}_{2^k}^*$ 中的每个元都恰好被取值一次而零元被取值两次. 从而, 判断 F 是否为向量 bent 函数的问题就转化成了确定一些与 F 在 $\mathcal{U}$ 上取值相关的初等对称多项式的系数的问题. 最终, 文献 [23] 得到了 F 满足向量 bent 性时, 参数 a_i 和 r_i 必须满足的一些条件. 例如, 所有的参数 r_i 都必须是奇数. 另一个重要工作是, 文献 [25] 证明了属于 $\mathcal{PS}_{\rm ap}$ 类的形如 $\mathrm{Tr}_k^{2k}(\sum_{i=1}^{2^k}a_ix^{i(2^k-1)})$ 的向量 bent 函数都是向量超 bent 的, 并且这种函数的确切数目为 $(2^k+1)!2^{k-1}$.

基于上述工作, 文献 [23,25] 提出了刻画形如 $\mathrm{Tr}_m^n(\sum_{i=1}^t a_ix^{r_i(2^k-1)})$ 且项数较少的向量 bent 函数的问题. 其中文献 [23] 证明了所有单项式函数 $\mathrm{Tr}_k^{2k}(ax^{r(2^k-1)})$ 都不是向量 bent 函数. 而对于二项式函数

$$F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+ax^{r(2^k-1)}),$$

若其满足向量 bent 性且 $r\mid 2^k+1$, 则 r 必为 3; 此外还得到了 $r=3$, $r\nmid 2^k+1$, 且 F 为向量 bent 函数时, 参数 a 需满足的一些条件.

本文继续探讨 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+ax^{r(2^k-1)})$ 的向量 bent 性, 证明了当 $r\mid 2^k+1$ 时, 文献 [23] 得到的必要条件是充要的, 从而完全确定了该情形下 F 的向量 bent 性. 对于 $r\nmid 2^k+1$ 的情形, 我们首先化简了文献 [23] 得到的计算关联 F 在 $\mathcal{U}$ 上取值的一些系数 s_l 的公式. 然后结合强有力的 Lucas 公式和 $\mathcal{U}$ 的群结构, 计算得到了一些关键的 s_l 的数值, 从而完全确定了 $r\nmid 2^k+1$ 及 r 分别等于 5、7 和 9 时 F 的向量 bent 性. 尤其值得一提的是, 针对文献 [23] 中提出的关于不存在此类二项式向量 bent 函数的猜想, 我们找到了一些反例.

本文的剩下内容安排如下: 第 2 节给出向量 bent 函数的背景和基本概念, 简单回顾关于 $F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+ax^{r(2^k-1)})$ 的向量 bent 性的结果, 并化简计算 s_l 的公式; 第 3 节完全确定 $r\mid 2^k+1$ 时 F 的向量 bent 性; 第 4–6 节依次分情形讨论并完全确定 $r\nmid 2^k+1$ 及 r 分别等于 5、7 和 9 时 F 的向量 bent 性; 第 7 节对本文作简要总结.

2 预备知识

本节简要介绍文献 [23] 得到的关于一类函数的向量 bent 性质的结果. 我们用 $\mathrm{Tr}_k^n(x)$ 表示从有限域 $\mathbb{F}_{2^n}$ 到其子域 $\mathbb{F}_{2^k}$ 的迹函数, 也即

$$\mathrm{Tr}_k^n(x) := \sum_{i=0}^{n/k-1} x^{2^{ik}} = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}.$$

设 $\mathcal{U}$ 是循环群 $\mathbb{F}_{2^{2k}}^*$ 的 2^k+1 阶子群, 则有 $\bigcup_{u\in\mathcal{U}} u\mathbb{F}_{2^k}^* = \mathbb{F}_{2^{2k}}^*$. 因此, 对每个 $x \in \mathbb{F}_{2^{2k}}^*$, 都存在唯一的 $u \in \mathcal{U}$ 和 $z \in \mathbb{F}_{2^k}^*$ 使得 $x = uz$.

关于向量布尔函数 $F(x) = \mathrm{Tr}_k^{2k}(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$ 的向量 bent 性有如下的刻画.

定理 1 (参见文献 [23, 定理 2]) 设 $n = 2k$ 且 $F(x) = \mathrm{Tr}_k^n(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$, 则下列结论等价:

(1) F 是 k 维向量 bent 函数;

(2) $\sum_{u\in\mathcal{U}}(-1)^{\mathrm{Tr}_1^k(\lambda F(u))} = 1, \forall\, \lambda \in \mathbb{F}_{2^k}$;

(3) 存在两个元 $u_1, u_2 \in \mathcal{U}$ 使得 $F(u_i) = 0$, $i = 1, 2$, 且 F 是从 $\mathcal{U} \setminus \{u_1\}$ 到 $\mathbb{F}_{2^k}$ 的双射;

(4) 在展开式

$$\prod_{u\in\mathcal{U}}(x - F(u)) = x^{2^k+1} + \sigma_1 x^{2^k} + \cdots + \sigma_e x^{2^k+1-e} + \cdots + \sigma_{2^k-1}x^2 + \sigma_{2^k}x + \sigma_{2^k+1}$$

中, 系数 σ_e 都是初等对称多项式, 满足 $\sigma_{2^k-1} = 1$, 且对任意奇数 $1 \leqslant e \leqslant 2^k+1$ 都有 $\sigma_e = 0$.

根据定理 1 给出的等价条件, 判断 F 是否为向量 bent 函数的问题就转化成了判断系数

$$\sigma_e = \sum_{0\leqslant i_1<i_2<\cdots<i_e\leqslant 2^k} F(\alpha^{i_1})F(\alpha^{i_2})\cdots F(\alpha^{i_e})$$

是否满足 $\sigma_{2^k-1} = 1$, 且对任意奇数 $1 \leqslant e \leqslant 2^k+1$ 都有 $\sigma_e = 0$, 其中 α 是 $\mathcal{U}$ 的一个生成元. 然而, 这些系数的计算是非常困难的.

令

$$s_i = \sum_{u\in\mathcal{U}} F(u)^i, \quad \forall\, 0 \leqslant i \leqslant 2^k+1, \tag{2.1}$$

则由 Newton 公式可得, 在有限域 $\mathbb{F}_{2^n}$ 中,

$$s_l + \sigma_1 s_{l-1} + \sigma_2 s_{l-2} + \cdots + l\sigma_l = 0, \quad \forall\, 1 \leqslant l \leqslant 2^k+1. \tag{2.2}$$

由 (2.2) 知, 判断系数 σ_e 是否满足 $\sigma_{2^k-1} = 1$, 且对其他满足 $1 \leqslant e \leqslant 2^k+1$ 的奇数 e 都成立 $\sigma_e = 0$ 的问题又转化成了判断 s_l 是否满足 $s_{2^k-1} = 1$, 且对其他满足 $1 \leqslant l \leqslant 2^k+1$ 的奇数 l 都成立 $s_l = 0$.

注意到对向量布尔函数

$$F(x) = \mathrm{Tr}_k^{2k}(x^{2^k-1} + \gamma z x^{r(2^k-1)}), \quad \gamma \in \mathcal{U}, \quad z \in \mathbb{F}_{2^k}^*,$$

以及任意的 $u \in \mathcal{U}$, 都有

$$F(u) = u^2 + u^{-2} + z\gamma u^{2r} + z\gamma^{-1}u^{-2r}. \tag{2.3}$$

由于 x^2 是 $\mathcal{U}$ 的一个置换, 根据定理 1 可知, F 为向量 bent 函数当且仅当

$$\widetilde{F}(u) = u + u^{-1} + z\gamma u^r + z\gamma^{-1}u^{-r} \tag{2.4}$$

限制在 $\mathcal{U}$ 上时, $\mathbb{F}_{2^k}^*$ 的每个元恰好被取值一次而零元被取值两次. 进一步, 若将 (2.1) 中的 $F(u)$ 都替换成 $\widetilde{F}(u)$, 和式的值不变. 从而可将 (2.1) 化为 (详见文献 [23])

$$s_l = \sum_{\substack{i_1+i_2+i_3+i_4=l;\\ i_1-i_2+r(i_3-i_4)\equiv 0 \pmod{2^k+1}}} \binom{l}{i_1,i_2,i_3,i_4} z^{i_3+i_4}\gamma^{i_3-i_4}, \tag{2.5}$$

其中的多项式系数定义为

$$\binom{l}{i_1,i_2,i_3,i_4} = \frac{l!}{i_1!i_2!i_3!i_4!}.$$

文献 [23] 还证明了, 对任意奇数 l, 成立

$$\sum_{\substack{i_1+i_2+i_3+i_4=l;\\ i_1-i_2+r(i_3-i_4)=0}} \binom{l}{i_1,i_2,i_3,i_4} z^{i_3+i_4}\gamma^{i_3-i_4} = 0.$$

因此, 当 l 为满足 $lr < 2^k+1$ 的奇数时, 总有 $s_l = 0$. 事实上, 我们还注意到对任意的奇数 l 和任意的偶数 d, 总有

$$\sum_{\substack{i_1+i_2+i_3+i_4=l;\\ i_1-i_2+r(i_3-i_4)=\pm d(2^k+1)}} \binom{l}{i_1,i_2,i_3,i_4} z^{i_3+i_4}\gamma^{i_3-i_4} = 0.$$

这是因为方程组

$$\begin{cases} i_1+i_2+i_3+i_4 = l, \\ i_1-i_2+r(i_3-i_4) = d(2^k+1) \end{cases}$$

无非负整数解. 从而, 若 l 为奇数且 $2^k+1 \leqslant lr < (2J+1)(2^k+1)$, 其中 J 为使得该不等式成立的最小的整数, 则 (2.5) 可进一步化简为

$$s_l = \sum_{0\leqslant j\leqslant J-1} \sum_{\substack{i_1+i_2+i_3+i_4=l;\\ i_1-i_2+r(i_3-i_4)=\pm(2j+1)(2^k+1)}} \binom{l}{i_1,i_2,i_3,i_4} z^{i_3+i_4}\gamma^{i_3-i_4}. \tag{2.6}$$

不难看出, 对每个给定的整数 j, $0 \leqslant j \leqslant J-1$, 关于 i_1、i_2、i_3 和 i_4 的线性方程组

$$\begin{cases} i_1+i_2+i_3+i_4 = l, \\ i_1-i_2+r(i_3-i_4) = (2j+1)(2^k+1) \end{cases} \tag{2.7}$$

和

$$\begin{cases} i_1+i_2+i_3+i_4 = l, \\ i_1-i_2+r(i_3-i_4) = -(2j+1)(2^k+1) \end{cases} \tag{2.8}$$

的非负整数解通过映射: $(i_1,i_2,i_3,i_4)\mapsto(i_2,i_1,i_4,i_3)$ 一一对应. 因此, 若 (i_1,i_2,i_3,i_4) 是 (2.7) 的一个满足 $\binom{l}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的非负整数解, 则 $z^{i_3+i_4}(\gamma^{i_3-i_4}+\gamma^{i_4-i_3})$ 必是 s_l 的表达式 (2.6) 中的一项. 并且 s_l 的每一项均可通过这种方式得到. 于是, 由 (2.6) 计算 s_l 时, 我们只需要对每个整数 $0\leqslant j\leqslant J-1$ 求得方程组 (2.7) 的所有非负整数解 (i_1,i_2,i_3,i_4), 并确定所有多项式系数 $\binom{l}{i_1,i_2,i_3,i_4}$ 的奇偶性. 后者比前者更困难. 为便于判断这些系数的奇偶性, 下面引入 Lucas 公式的一个结果.

设 a 和 b 均为非负整数且其二进制表示为 $a=(a_ma_{m-1}\cdots a_0)_2$, $b=(b_mb_{m-1}\cdots b_0)_2$, 也即

$$a=\sum_{i=0}^{m}a_i2^i,\quad b=\sum_{i=0}^{m}b_i2^i,$$

且 $a_i,b_i\in\{0,1\}$, $\forall\, 0\leqslant i\leqslant m$, 则有相应的 Lucas 公式

$$\binom{a}{b}\equiv\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_m}{b_m} \pmod 2,$$

从而, $\binom{a}{b}\equiv 1 \pmod 2$ 当且仅当对每个 $0\leqslant i\leqslant m$ 都有 $b_i\leqslant a_i$ (参见文献 [26]). 我们用记号 $b\preceq a$ 表示 $b_i\leqslant a_i$, $\forall\, 0\leqslant i\leqslant m$, 否则记作 $b\not\preceq a$.

文献 [23] 讨论了 $r\mid 2^k+1$, 以及 $r\nmid 2^k+1$ 且 $r=3$ 时, $F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+\gamma zx^{r(2^k-1)})$ 的向量 bent 性, 其中对于 $r\mid 2^k+1$ 的情形, 他们得到了下列主要结果.

定理 2 (参见文献 [23, 定理 9]) 设 $2^k+1=rD$, 其中 D 为正整数. 若 F 为向量 bent 函数, 则必有 $r=3$, $\gamma^D=1$, $\gamma\neq 1$ 且 $z=\mathrm{Tr}_k^n(\omega^D)(\mathrm{Tr}_k^n(\gamma))^{-1}$, 其中 ω 是 $\mathcal{U}$ 的一个生成元.

引理 1 (参见文献 [23, 引理 4]) 若定理 2 的条件满足, 则当 $D>4$ 时, $s_{D+4}=0$ 当且仅当

$$z^{D-2}(\gamma+\gamma^{-1})(\gamma+\gamma^{-1}+z(z^2+1))=0.$$

而对于 $r\nmid 2^k+1$ 且 $r=3$ 的情形, 设 $2^k+1=3D+2$, Muratović-Ribić 等[23] 也找到了一些使 F 成为向量 bent 函数的必要条件. 例如, 根据文献 [23, 引理 5] 知, 必须满足 $z=\mathrm{Tr}_k^n(\gamma^{D+1})$. 基于这些必要条件, 他们提出了如下猜想.

猜想 1 (参见文献 [23, 猜想 1]) 设 $k\geqslant 2$ 为偶数且 $n=2k$, 则对任意的 $\lambda\in\mathbb{F}_{2^n}^*$,

$$F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\lambda x^{r(2^k-1)})$$

都不是向量 bent 函数.

文献 [27] 试图证明该猜想 1 成立, 但随后文献 [28] 更正了一个错误并声明该猜想仍是一个公开问题.

在接下来的几节中, 我们继续深入研究二项式函数 $F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+\gamma zx^{r(2^k-1)})$ 在 $r\mid 2^k+1$ 以及 $r\nmid 2^k+1$ 且 r 分别等于 5、7 和 9 的情形下的向量 bent 性. 我们得到的主要结果是, 对于 $r\mid 2^k+1$ 的情形, 我们证明了由文献 [23] 得到的使得 F 成为向量 bent 函数的必要条件同时也是充分的, 从而完全确定了该情形下 F 的向量 bent 性. 而对于 $r\nmid 2^k+1$ 且 r 分别等于 5、7 和 9 的情形, 我们通过利用 Lucas 公式计算得到 s_l 的一些非常重要的数值, 也完全确定了 F 的向量 bent 性. 尤其重要的是, 我们得到了猜想 1 的一些反例.

3 $r\mid 2^k+1$ 的情形

当 $r\mid 2^k+1$ 时, 若 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{r(2^k-1)})$ 满足向量 bent 性, 则必有 $r=3$ (见本文定理 2), 从而 k 为奇数. 在下面的定理中, 我们将证明, 若 $r=3$, k 为奇数且 $k\geqslant 5$, 则不存在满足定理 2 和

引理 1 给出的所有条件的函数. 因此可得结论: 对于 $r \mid 2^k+1$ 的情形, F 满足向量 bent 性只可能是 $k=3$.

定理 3 设 $r=3$, k 为奇数且 $k \geqslant 5$, 则 F 不是向量 bent 函数.

证明 令 $2^k+1=3D$. 若 F 是向量 bent 函数, 由定理 2 可得 $\gamma^D=1$, $\gamma \neq 1$ 且

$$z=\mathrm{Tr}_k^{2k}(\omega^D)(\mathrm{Tr}_k^{2k}(\gamma))^{-1},$$

其中 ω 是 $3D$ 阶循环群 $\mathcal{U}$ 的一个生成元. 于是, ω^D 是 3 阶元, $\mathrm{Tr}_k^{2k}(\omega^D)=\omega^D+\omega^{-D}=1$, 可得

$$z=(\mathrm{Tr}_k^{2k}(\gamma))^{-1}=\frac{1}{\gamma+\gamma^{-1}}. \tag{3.1}$$

由于 $k \geqslant 5$, 根据引理 1, 有

$$\gamma+\gamma^{-1}+z(z^2+1)=0.$$

结合 (3.1) 并化简可得 $z^4+z^2+1=0$, 从而, $z \in \mathbb{F}_{2^k}^*$ 是 3 阶元, 于是 $3 \mid 2^k-1$. 又 $3 \mid 2^k+1$, 从而 $3 \mid 2$, 矛盾. 所以, F 不可能为向量 bent 函数. □

当 $k=r=3$ 时, $D=3$. 若 F 满足向量 bent 性, 根据定理 2 有 $\gamma^3=1$, $\gamma \neq 1$ 且 $z=(\gamma+\gamma^{-1})^{-1}=1$. 另一方面, 文献 [23, 例 2] 已经验证了 γ 为 3 阶元时函数 $F(x)=\mathrm{Tr}_3^6(x^7+\gamma x^{21})$ 是向量 bent 函数. 因此, 我们可总结上述结果如下.

定理 4 设 $r \mid 2^k+1$, 则

$$F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+\gamma z x^{r(2^k-1)})$$

为向量 bent 函数当且仅当 $r=k=3$, $z=\gamma^3=1$ 且 $\gamma \neq 1$.

4 $r \nmid 2^k+1$ 且 $r=5$ 的情形

本节考虑函数 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{5(2^k-1)})$ 在 $5 \nmid 2^k+1$ 时的向量 bent 性. 由于 $2 \in \mathbb{Z}_5^*$ 是 4 阶元, 因此, 对任意整数 m, 有

$$2^k+1 \bmod 5=\begin{cases} 2, & k=4m, \\ 3, & k=4m+1, \\ 0, & k=4m+2, \\ 4, & k=4m+3. \end{cases}$$

4.1 $k=4m$ 的情形

首先考虑 $k=4m$ 的情形. 可设 $2^k+1=5D+2$, 则

$$\begin{aligned} D&=\frac{2^{4m}-1}{5}=\frac{1}{5}(2^4-1+2^4(2^4-1)+\cdots+2^{4(m-1)}(2^4-1)) \\ &=3(1+2^4+\cdots+2^{4(m-1)})=(\underbrace{11001100\cdots110011}_{4m-2})_2. \end{aligned} \tag{4.1}$$

引理 2 设 $k=4m>4$, 则

$$s_{D+8}=z^{D-1}(\gamma^{D-1}+\gamma^{-(D-1)}).$$

证明 易知由 (2.6) 计算 s_{D+8} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $2i_1+3i_2+5i_4=19$, 结合 (4.1) 和 Lucas 公式可算得 (2.7) 的唯一满足 $\binom{D+8}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的非负整数解为 $i_1=8$, $i_2=1$, $i_4=0$, $i_3=D-1$. 因此, $s_{D+8}=z^{D-1}(\gamma^{D-1}+\gamma^{-(D-1)})$. □

定理 5 设 $k=4m>4$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{5(2^k-1)})$ 不是向量 bent 函数.

证明 假如 F 是向量 bent 函数, 则 $s_{D+8}=0$. 由引理 2 得 $z^{D-1}(\gamma^{D-1}+\gamma^{-(D-1)})=0$, 于是 $\gamma^{D-1}+\gamma^{-(D-1)}=0$, 进而 $\gamma^{D-1}=1$. 由于 $D-1=\frac{2^k-6}{5}$ 且 $7\nmid 2^k-6$, 可知

$$\gcd(D-1,5D+2)=\gcd(D-1,7)=1,$$

于是 $\gamma=1$, 矛盾. 事实上, 若 $\gamma=1$, 则对任意 $u\in\mathcal{U}$, 都有 $\widetilde{F}(u)=u+u^{-1}+zu^5+zu^{-5}$, 从而, $\widetilde{F}(u)=\widetilde{F}(u^{-1})$, 与定理 1(3) 矛盾. □

再考虑 $k=4$ 的情形, 此时 $2^k+1=17$, $2^k-1=15$, $D=3$.

定理 6 对任意的 z 和 γ, $F(x)=\mathrm{Tr}_4^8(x^{15}+\gamma zx^{75})$ 都不是向量 bent 函数.

证明 根据 (2.5) 可算得

$$s_{11}=\sum_{\substack{i_1+i_2+i_3+i_4=11;\\ i_1-i_2+5(i_3-i_4)=\pm 17,\pm 51}}\binom{11}{i_1,i_2,i_3,i_4}z^{i_3+i_4}\gamma^{i_3-i_4}=z^2(\gamma^2+\gamma^{-2})+z^{10}(\gamma^{10}+\gamma^{-10}),$$

$$s_{15}=\sum_{\substack{i_1+i_2+i_3+i_4=15;\\ i_1-i_2+5(i_3-i_4)=\pm 17,\pm 51}}\binom{15}{i_1,i_2,i_3,i_4}z^{i_3+i_4}\gamma^{i_3-i_4}=\mathrm{Tr}_1^4(z^6(\gamma^2+\gamma^{-2})+z^{14}(\gamma^{10}+\gamma^{-10})).$$

如果 F 是向量 bent 函数, 就有 $s_{11}=0$ 且 $s_{15}=1$. 而由 $s_{11}=0$ 显然可得 $s_{15}=0$, 矛盾. □

4.2 $k=4m+1$ 的情形

本小节假定 $k=4m+1$. 此时 $2^k+1=5D+3$, 且

$$D=\frac{2^{4m+1}-2}{5}=(\underbrace{11001100\cdots 1100110}_{4m-1})_2. \tag{4.2}$$

定理 7 若 $k=4m+1\geqslant 5$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{5(2^k-1)})$ 不是向量 bent 函数.

证明 根据 (2.6) 计算 s_{D+5}, 此时 $J=1$. 由线性方程组 (2.7) 可得 $2i_1+3i_2+5i_4=11$. 从而可得 (2.7) 的唯一满足 $\binom{D+5}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的非负整数解 $i_1=0$, $i_2=2$, $i_3=D+2$, $i_4=1$. 因此 $s_{D+5}=z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)})$.

若 F 是向量 bent 函数, 则 $s_{D+5}=0$, 即 $z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 从而 $\gamma^{D+1}=1$. 易见

$$\gcd(D+1,5D+3)=\gcd(D+1,2)=1,$$

所以 $\gamma=1$, 矛盾. □

4.3 $k=4m+3$ 的情形

本小节设 $k=4m+3$, 此时存在正整数 D 使得 $2^k+1=5D+4$.

定理 8 设 $k=4m+3$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{5(2^k-1)})$ 不是向量 bent 函数.

证明 由 (2.6) 计算 s_{D+2}, 此时 $J=1$, 且由线性方程组 (2.7) ($l=D+2$) 可得 $2i_1+3i_2+5i_4=3$, 从而, (2.7) 有唯一非负整数解 $(i_1,i_2,i_3,i_4)=(0,1,D+1,0)$. 由于 $\binom{D+2}{0,1,0,D+1}=\binom{D+2}{1}\equiv 1 \pmod 2$, 所以 $s_{D+2}=z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$.

若 F 是向量 bent 函数, 则 $s_{D+2}=0$, 即 $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 从而 $\gamma^{D+1}=1$. 又 $\gcd(D+1,5D+4)=\gcd(D+1,1)=1$, 于是 $\gamma=1$, 矛盾. □

综合定理 2 和 5–8 的结果, 可得本节主要结论如下.

定理 9 对任意整数 $k\geqslant 2$ 和任意 $a\in\mathbb{F}_{2^{2k}}$, $F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+ax^{5(2^k-1)})$ 都不是向量 bent 函数.

5 $r\nmid 2^k+1$ 且 $r=7$ 的情形

本节考虑 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{7(2^k-1)})$ 在 $7\nmid 2^k+1$ 时的向量 bent 性. 注意到 $2\in\mathbb{Z}_7^*$ 是 3 阶元, 对任意整数 m, 成立

$$2^k+1 \bmod 7=\begin{cases}2, & k=3m,\\ 3, & k=3m+1,\\ 5, & k=3m+2.\end{cases}$$

5.1 $k=3m$ 的情形

设 $k=3m$, 此时存在正整数 D 使得 $2^k+1=7D+2$, 且

$$\begin{aligned}D&=\frac{2^{3m}-1}{7}=\frac{1}{7}(2^3-1+2^3(2^3-1)+2^6(2^3-1)+\cdots+2^{3(m-1)}(2^3-1))\\&=1+2^3+2^6+\cdots+2^{3(m-1)}=(\underbrace{100100\cdots1001}_{3m-2})_2.\end{aligned}\tag{5.1}$$

引理 3 设 $k=3m$, 则 $s_{D+2}=z^D(\gamma^D+\gamma^{-D})$.

证明 由 (2.6) 计算 s_{D+2} 时, $J=1$. 由线性方程组 (2.7) ($l=D+2$) 可得 $3i_1+4i_2+7i_4=6$, 从而得到 (2.7) 的唯一非负整数解 $i_1=2, i_2=0, i_4=0, i_3=D$. 又由 (5.1) 可得 $\binom{D+2}{2,0,0,D}=\binom{D+2}{2}\equiv 1 \pmod 2$, 从而 $s_{D+2}=z^D(\gamma^D+\gamma^{-D})$. □

引理 4 设 $k=3m\geqslant 6$, 则 $s_{D+6}=z^D(\gamma^D+\gamma^{-D})+z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$.

证明 由 (2.6) 计算 s_{D+6} 时, $J=1$. 由线性方程组 (2.7) 可得 $3i_1+4i_2+7i_4=20$, 从而得到方程组 (2.7) 的所有满足 $\binom{D+6}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的非负整数解以及 s_{D+6} 的各项如下:

(1) $i_1=4, i_2=2, i_4=0, i_3=D$. 根据 (5.1) 可算得

$$\binom{D+6}{4,2,0,D}=\frac{(D+6)(D+5)}{2}\binom{D+4}{4}\equiv 1 \pmod 2,$$

从而, $z^D(\gamma^D+\gamma^{-D})$ 是 s_{D+6} 的项.

(2) $i_1=0$, $i_2=5$, $i_4=0, i_3=D+1$. 由 (5.1) 可得

$$\binom{D+6}{0,5,0,D+1}=\binom{D+6}{5}\equiv 1 \pmod 2,$$

从而, $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$ 也是 s_{D+6} 的项. 因此结论成立. □

定理 10 设 $k=3m$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{7(2^k-1)})$ 不是向量 bent 函数.

证明 假设 F 满足向量 bent 性, 则 $s_{D+2}=0$. 由引理 3 知, $z^D(\gamma^D+\gamma^{-D})=0$, 从而 $\gamma^D=1$. 当 $k=3$ 时, $D=1$, 则有 $\gamma=1$, 矛盾. 当 $k\geqslant 6$ 时, 还有 $s_{D+6}=0$. 由引理 4 可得 $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 从而 $\gamma^{D+1}=1$. 于是也有 $\gamma=1$, 矛盾. □

5.2 $k=3m+1$ 的情形

本小节假设 $k=3m+1$ 和 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{7(2^k-1)})$, 此时存在正整数 D 使得 $2^k+1=7D+3$, 且由 (5.1) 可知,

$$D=\frac{2^{3m+1}-2}{7}=(\underbrace{100100\cdots 10010}_{3m-1})_2. \tag{5.2}$$

引理 5 设 $k=3m+1\geqslant 4$, 则 $s_{D+5}=z^D(\gamma^D+\gamma^{-D})+z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$.

证明 由 (2.6) 计算 s_{D+5} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $3i_1+4i_2+7i_4=16$, 从而得方程组 (2.7) 的所有非负整数解以及 s_{D+6} 的各项如下:

(1) $i_1=4$, $i_2=1$, $i_4=0$, $i_3=D$. 由 (5.2) 可得 $4\preceq D+4$, 于是,

$$\binom{D+5}{4,1,0,D}=(D+5)\binom{D+4}{4}\equiv 1 \pmod 2,$$

从而, $z^D(\gamma^D+\gamma^{-D})$ 是 s_{D+6} 的一项.

(2) $i_1=3$, $i_2=0$, $i_4=1$, $i_3=D+1$. 由 (5.2) 可得 $3\not\preceq D+4$, 于是,

$$\binom{D+5}{3,0,1,D+1}=(D+5)\binom{D+4}{3}\equiv 0 \pmod 2.$$

(3) $i_1=0$, $i_2=4$, $i_4=0$, $i_3=D+1$. 由于 $4\preceq D+5$, 于是,

$$\binom{D+5}{0,4,0,D+1}=\binom{D+5}{4}\equiv 1 \pmod 2,$$

从而, $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$ 是 s_{D+6} 的一项. 因此结论成立. □

引理 6 设 $k=3m+1\geqslant 7$, 则 $s_{D+9}=z^{D-1}(\gamma^{D-1}+\gamma^{-(D-1)})$.

证明 由 (2.6) 计算 s_{D+9} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $3i_1+4i_2+7i_4=30$. 从而得到方程组 (2.7) 的唯一满足 $\binom{D+9}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的解 $(i_1,i_2,i_3,i_4)=(10,0,D-1,0)$. 因此, $s_{D+9}=z^{D-1}(\gamma^{D-1}+\gamma^{-(D-1)})$. □

定理 11 若 $k=3m+1\geqslant 7$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{7(2^k-1)})$ 不是向量 bent 函数.

证明 若 F 是向量 bent 函数, 则 $s_{D+5}=0$ 且 $s_{D+9}=0$. 由引理 6 得 $z^{D-1}(\gamma^{D-1}+\gamma^{-(D-1)})=0$, 进而 $\gamma^{D-1}=1$. 注意到 $\gcd(D-1,7D+3)=\gcd(D-1,5)$, 那么 $\gcd(D-1,7D+3)$ 只能是 1 或者 5, 从而 γ 的阶只能为 5. 于是有

$$(\gamma+\gamma^{-1})^3=\gamma^3+\gamma^{-3}+\gamma+\gamma^{-1}=1.$$

由引理 5 知, 成立 $z^D(\gamma^D+\gamma^{-D})+z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 并注意到 $\gamma^{D-1}+\gamma^{-(D-1)}=0$, 可得

$$z=\frac{\gamma^D+\gamma^{-D}}{\gamma^{D+1}+\gamma^{-(D+1)}}=\frac{1}{\gamma+\gamma^{-1}}.$$

所以 $z^3=1$, z 必为 3 阶元 (若 $z=1$, 可得 γ 为 3 阶元, 矛盾).

考虑从 $\mathcal{U}$ 到 $\mathbb{F}_{2^k}$ 的映射

$$\widetilde{F}(u)=u+u^{-1}+z\gamma u^7+z\gamma^{-1}u^{-7},$$

根据定理 1 知, $\mathbb{F}_{2^k}^*$ 中每个元必恰好取值一次, 而零元取值两次. 然而, 计算可得

$$\begin{aligned}&\widetilde{F}(\gamma^2)=\gamma^2+\gamma^{-2}+z(\gamma^{15}+\gamma^{-15})=(\gamma+\gamma^{-1})^2=z^{-2}=z,\\&\widetilde{F}(\gamma^4)=\widetilde{F}(\gamma^{-1})=\gamma+\gamma^{-1}+z(\gamma^6+\gamma^{-6})=(z+1)(\gamma+\gamma^{-1})=(z+1)z^{-1}=z.\end{aligned}$$

因此 $\widetilde{F}(\gamma^2)=\widetilde{F}(\gamma^4)$, 矛盾. 所以, F 不是向量 bent 函数. □

接下来考虑 $k=4$ 时 F 的向量 bent 性, 此时 $2^k+1=17$, $2^k-1=15$ 且 $D=2$.

定理 12 向量布尔函数 $F(x)=\mathrm{Tr}_4^8(x^{15}+\gamma zx^{105})$ 不是向量 bent 函数.

证明 由 (2.5) 可算得

$$s_{15}=\sum_{\substack{i_1+i_2+i_3+i_4=15;\\ i_1-i_2+7(i_3-i_4)=\pm17,\pm51,\pm85}}\binom{15}{i_1,i_2,i_3,i_4}z^{i_3+i_4}\gamma^{i_3-i_4}=\mathrm{Tr}_1^4(z(\gamma+\gamma^{-1})+z^3(\gamma^3+\gamma^{-3})).$$

若 F 是向量 bent 函数, 则 $s_7=0$ 且 $s_{15}=1$. 由引理 5 可得 $z^2(\gamma^2+\gamma^{-2})+z^3(\gamma^3+\gamma^{-3})=0$. 于是, $s_{15}=\mathrm{Tr}_1^4(z^2(\gamma^2+\gamma^{-2})+z^3(\gamma^3+\gamma^{-3}))=0$, 矛盾. □

5.3 $k=3m+2$ 的情形

本小节讨论 $k=3m+2$ 时 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{7(2^k-1)})$ 的向量 bent 性. 此时存在正整数 D 使得 $2^k+1=7D+5$, 且由 (5.1) 可知,

$$D=\frac{2^{3m+2}-4}{7}=(\underbrace{100100\cdots100100}_{3m})_2. \tag{5.3}$$

定理 13 设 $k=3m+2\geqslant5$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{7(2^k-1)})$ 不是向量 bent 函数.

证明 由 (2.6) 计算 s_{D+3} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $3i_1+4i_2+7i_4=8$. 因此, 方程组 (2.7) 有唯一非负整数解 $i_1=0$, $i_2=2$, $i_4=0$, $i_3=D+1$. 由 (5.3) 可得 $2\preceq D+3$, 从而 $\binom{D+3}{0,2,0,D+1}=\binom{D+3}{2}\equiv1\pmod 2$. 所以 $s_{D+3}=z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$.

若 F 为向量 bent 函数, 则 $s_{D+3}=0$, 即 $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 可得 $\gamma^{D+1}=1$. 而

$$\gcd(D+1,7D+5)=\gcd(D+1,2)=1,$$

于是 $\gamma=1$, 矛盾. □

下面考虑 $k=2$ 时 F 的向量 bent 性. 此时 $2^k+1=5$, $2^k-1=3$.

定理 14 函数 $F(x)=\mathrm{Tr}_2^4(x^3+\gamma zx^{21})$ 是向量 bent 函数当且仅当 $z=1$, $\gamma^5=1$ 且 $\gamma\neq1$.

证明 只需考虑 $z \neq 0$ 且 $\gamma \neq 1$ 的情形. 计算可得

$$F(1) = z(\gamma + \gamma^{-1}), \quad F(\gamma) = \gamma + \gamma^{-1} + z(\gamma^2 + \gamma^{-2}), \quad F(\gamma^2) = \gamma^2 + \gamma^{-2},$$
$$F(\gamma^3) = \gamma^2 + \gamma^{-2} + z(\gamma^2 + \gamma^{-2}), \quad F(\gamma^4) = \gamma + \gamma^{-1} + z(\gamma + \gamma^{-1}).$$

显然, 多重集

$$\{* \ F(1), F(\gamma), F(\gamma^2), F(\gamma^3), F(\gamma^4) \ *\} = \mathbb{F}_{2^2} \cup \{* \ 0 \ *\}$$

当且仅当 $z = 1$. 事实上, 一方面, 我们有 $F(1) \neq 0$; $F(\gamma^2) \neq 0$; $F(\gamma) = 0$ 当且仅当 $z = \frac{1}{\gamma+\gamma^{-1}}$; $F(\gamma^3) = 0$ 当且仅当 $z = 1$; 以及 $F(\gamma^4) = 0$ 当且仅当 $z = 1$. 另一方面, 当 $z = 1$ 时, 注意到 $\gamma + \gamma^{-1} \in \mathbb{F}_{2^2}^*$ 是 3 阶元, 则多重集

$$\{* \ F(1), F(\gamma), F(\gamma^2), F(\gamma^3), F(\gamma^4) \ *\} = \{* \ \gamma + \gamma^{-1}, 1, \gamma^2 + \gamma^{-2}, 0, 0 \ *\} = \mathbb{F}_{2^2} \cup \{* \ 0 \ *\}.$$

因此, F 是向量 bent 函数当且仅当 $z = 1$, $\gamma^5 = 1$ 且 $\gamma \neq 1$. □

注 1 定理 14 给出了猜想 1 在 $k = 2$ 时的一些反例. 从而猜想 1 至少在 $k = 2$ 时是不成立的.

综合定理 2 和 10–14 的结果, 可得本节的主要结论.

定理 15 函数 $F(x) = \mathrm{Tr}_k^{2k}(x^{2^k-1} + \gamma z x^{7(2^k-1)})$ 是向量 bent 函数当且仅当 $k = 2$, $z = 1$ 且 γ 为 5 阶元.

6 $r \nmid 2^k + 1$ 且 $r = 9$ 的情形

本节研究函数 $F(x) = \mathrm{Tr}_k^n(x^{2^k-1} + \gamma z x^{9(2^k-1)})$ 当 $9 \nmid 2^k + 1$ 时的向量 bent 性质. 注意到 $2 \in \mathbb{Z}_9^*$ 的阶为 6, 对任意的整数 m, 有

$$2^k + 1 \bmod 9 = \begin{cases} 2, & k = 6m, \\ 3, & k = 6m+1, \\ 5, & k = 6m+2, \\ 0, & k = 6m+3, \\ 8, & k = 6m+4, \\ 6, & k = 6m+5. \end{cases}$$

6.1 $k = 6m$ 的情形

本小节假定 $k = 6m$, 此时存在正整数 D 使得 $2^k + 1 = 9D + 2$, 并且

$$\begin{aligned} D &= \frac{2^{6m} - 1}{9} = \frac{1}{9}(2^6 - 1 + 2^6(2^6 - 1) + 2^{12}(2^6 - 1) + \cdots + 2^{6(m-1)}(2^6 - 1)) \\ &= 7(1 + 2^6 + 2^{12} + \cdots + 2^{6(m-1)}) = (\underbrace{111000\cdots111000111}_{6m-3})_2. \end{aligned} \tag{6.1}$$

定理 16 若 $k = 6m$, 则 $F(x) = \mathrm{Tr}_k^n(x^{2^k-1} + \gamma z x^{9(2^k-1)})$ 不可能是向量 bent 函数.

证明 由 (2.6) 计算 s_{D+4} 时, $J = 1$. 此时由线性方程组 (2.7) 可得 $4i_1 + 5i_2 + 9i_4 = 17$, 从而得到 (2.7) 的所有非负整数解以及 s_{D+4} 的所有项:

(1) $i_1=2$, $i_2=0$, $i_4=1$, $i_3=D+1$. 由 (6.1) 知 $2\preceq D+3$, 于是 $\binom{D+4}{2,0,1,D+1}=(D+4)\binom{D+3}{2}\equiv 1 \pmod 2$, 因此, $z^{D+2}(\gamma^D+\gamma^{-D})$ 是 s_{D+4} 的一项.

(2) $i_1=3$, $i_2=1$, $i_4=0$, $i_3=D$. 由 $3\not\preceq D+3$ 可得 $\binom{D+4}{3,1,0,D}=(D+4)\binom{D+3}{3}\equiv 0 \pmod 2$.

因此, $s_{D+4}=z^{D+2}(\gamma^D+\gamma^{-D})$. 若 F 是向量 bent 函数, 则 $s_{D+4}=0$, 即 $z^{D+2}(\gamma^D+\gamma^{-D})=0$, 从而 $\gamma^D=1$. 又

$$\gcd(D,9D+2)=\gcd(D,2)=1,$$

从而 $\gamma=1$, 矛盾. □

6.2 $k=6m+1$ 的情形

考虑 $k=6m+1$ 的情形, 此时存在正整数 D 使得 $2^k+1=9D+3$, 且由 (6.1) 知,

$$D=\frac{2^{6m+1}-2}{9}=(\underbrace{111000\cdots1110001110}_{6m-2})_2. \tag{6.2}$$

引理 7 设 $k=6m+1\geqslant 7$, 则

$$s_{D+9}=z^{D+4}(\gamma^D+\gamma^{-D})+z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)}).$$

证明 由 (2.6) 计算 s_{D+9} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $4i_1+5i_2+9i_4=39$. 计算可得 (2.7) 的所有满足 $\binom{D+9}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的非负整数解并得到 s_{D+9} 的各项如下:

(1) $i_1=4$, $i_2=1$, $i_4=2$, $i_3=D+2$. 此时,

$$\binom{D+9}{4,1,2,D+2}=\frac{(D+9)(D+8)(D+7)}{2}\binom{D+6}{4}\equiv 1 \pmod 2,$$

给出 s_{D+9} 的一项 $z^{D+4}(\gamma^D+\gamma^{-D})$.

(2) $i_1=0$, $i_2=6$, $i_4=1$, $i_3=D+2$. 此时,

$$\binom{D+9}{0,6,1,D+2}=(D+9)\binom{D+8}{6}\equiv 1 \pmod 2,$$

对应到 s_{D+9} 的一项 $z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)})$. 因此结论成立. □

引理 8 设 $k=6m+1\geqslant 7$, 则 $s_{D+13}=z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)})$.

证明 由 (2.6) 计算 s_{D+13} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $4i_1+5i_2+9i_4=57$. 易算得 (2.7) 的唯一使得 $\binom{D+13}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 成立的非负整数解 $(i_1,i_2,i_3,i_4)=(2,8,D+2,1)$. 因此, $s_{D+13}=z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)})$. □

定理 17 若 $k=6m+1$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{9(2^k-1)})$ 不是向量 bent 函数.

证明 若 F 是向量 bent 函数, 则 $s_{D+9}=0$ 且 $s_{D+13}=0$. 由引理 7 可得 $z^{D+4}(\gamma^D+\gamma^{-D})=0$, 从而 $\gamma^D=1$. 再由引理 8 得

$$z^{D+3}(\gamma^{D+1}+\gamma^{-(D+1)})=0,$$

从而 $\gamma^{D+1}=1$. 于是 $\gamma=1$, 矛盾. □

6.3 $k=6m+2$ 的情形

本小节考虑 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{9(2^k-1)})$ 在 $k=6m+2$ 时的向量 bent 性. 此时存在正整数 D 使得 $2^k+1=9D+5$, 且

$$D=\frac{2^{6m+2}-4}{9}=(\underbrace{111000\cdots11100011100}_{6m-1})_2. \tag{6.3}$$

引理 9 设 $k=6m+2\geqslant 8$, 则 $s_{D+11}=z^{D+7}(\gamma^{D+1}+\gamma^{-(D+1)})$.

证明 易知由 (2.6) 计算 s_{D+11} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $4i_1+5i_2+9i_4=47$. 算得 (2.7) 的唯一满足 $\binom{D+11}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的非负整数解 $(i_1,i_2,i_3,i_4)=(0,4,D+4,3)$, 从而 $s_{D+11}=z^{D+7}(\gamma^{D+1}+\gamma^{-(D+1)})$. □

定理 18 若 $k=6m+2\geqslant 8$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{9(2^k-1)})$ 不是向量 bent 函数.

证明 假如 F 是向量 bent 函数, 则 $s_{D+11}=0$. 由引理 9 得 $z^{D+7}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 从而 $\gamma^{D+1}=1$. 显然,

$$\gcd(D+1,9D+5)=\gcd(D+1,4)=1,$$

于是 $\gamma=1$, 矛盾. □

最后考虑 $k=2$ 时 F 的向量 bent 性, 此时 $2^k+1=5$, $2^k-1=3$, 从而 $\gamma^5=1$, $z^3=1$.

定理 19 函数 $F(x)=\mathrm{Tr}_2^4(x^3+\gamma z x^{27})$ 不是向量 bent 函数.

证明 设 $z\neq 0$ 且 $\gamma\neq 1$, 可算得

$$\begin{aligned}&F(1)=z(\gamma+\gamma^{-1}),\quad F(\gamma)=\gamma+\gamma^{-1},\quad F(\gamma^2)=\gamma^2+\gamma^{-2}+z(\gamma+\gamma^{-1}),\\&F(\gamma^3)=\gamma^2+\gamma^{-2}+z(\gamma^2+\gamma^{-2}),\quad F(\gamma^4)=\gamma+\gamma^{-1}+z(\gamma^2+\gamma^{-2}).\end{aligned}$$

由于 $F(1)\neq 0$; $F(\gamma)\neq 0$; $F(\gamma^2)=0$ 当且仅当 $z=\gamma+\gamma^{-1}$; $F(\gamma^3)=0$ 当且仅当 $z=1$; $F(\gamma^4)=0$ 当且仅当 $z=\frac{1}{\gamma+\gamma^{-1}}=\gamma^2+\gamma^{-2}$; 且 $\gamma+\gamma^{-1}\in\mathbb{F}_{2^2}^*$ 是 3 阶元, 因此, 多重集

$$\{*\ F(1),F(\gamma),F(\gamma^2),F(\gamma^3),F(\gamma^4)\ *\}=\mathbb{F}_{2^2}\cup\{*\ 0\ *\}$$

不成立, F 不是向量 bent 函数. □

6.4 $k=6m+4$ 的情形

本小节假定 $k=6m+4$, 则存在正整数 D 使得 $2^k+1=9D+8$.

引理 10 设 $k=6m+4$ 且 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{9(2^k-1)})$, 则 $s_{D+2}=z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$.

证明 易知由 (2.6) 计算 s_{D+2} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $4i_1+5i_2+9i_4=5$, 从而, (2.7) 有唯一非负整数解 $i_1=0$, $i_2=1$, $i_4=0$, $i_3=D+1$. 而 $\binom{D+2}{0,1,0,D+1}=\binom{D+2}{1}\equiv 1 \pmod 2$, 因此, $s_{D+2}=z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$. □

定理 20 设 $k=6m+4$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma z x^{9(2^k-1)})$ 不是向量 bent 函数.

证明 假如 F 是向量 bent 函数, 则 $s_{D+2}=0$. 由引理 10 得 $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 于是 $\gamma^{D+1}=1$. 又显然

$$\gcd(D+1,9D+8)=\gcd(D+1,1)=1,$$

从而 $\gamma=1$, 矛盾. □

6.5 $k=6m+5$ 的情形

考虑 $k=6m+5$ 时 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{9(2^k-1)})$ 的向量 bent 性. 此时存在正整数 D 使得 $2^k+1=9D+6$, 且

$$\begin{aligned}D&=\frac{2^{6m+5}-5}{9}=\frac{1}{9}(2^5-5+2^5(2^6-1)+2^{11}(2^6-1)+\cdots+2^{6(m-1)+5}(2^6-1))\\&=3+7(2^5+2^{11}+\cdots+2^{6(m-1)+5})=(\underbrace{111000\cdots11100011}_{6m+2})_2.\end{aligned}\tag{6.4}$$

引理 11 设 $k=6m+5$, 则 $s_{D+4}=z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$.

证明 易知由 (2.6) 计算 s_{D+11} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $4i_1+5i_2+9i_4=15$, 从而 (2.7) 有唯一的非负整数解 $i_1=0$, $i_2=3$, $i_4=0$, $i_3=D+1$. 而由 (6.4) 可得 $\binom{D+4}{0,3,0,D+1}=\binom{D+4}{3}\equiv 1 \pmod 2$, 因此 $s_{D+4}=z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})$. □

引理 12 设 $k=6m+5\geqslant 11$, 则

$$s_{D+12}=z^{D+2}(\gamma^D+\gamma^{-D})+z^{D+9}(\gamma^{D+1}+\gamma^{-(D+1)}).$$

证明 易知由 (2.6) 计算 s_{D+12} 时, $J=1$. 此时由线性方程组 (2.7) 可得 $4i_1+5i_2+9i_4=51$, 进而可得 (2.7) 的满足 $\binom{D+12}{i_1,i_2,i_3,i_4}\equiv 1 \pmod 2$ 的所有非负整数解以及 s_{D+12} 的各项如下:

(1) $i_1=8$, $i_2=2$, $i_4=1$, $i_3=D+1$. 由于 $\frac{D+11}{2}$ 是奇数且由 (6.4) 可得 $8\preceq D+9$, 从而,

$$\binom{D+12}{8,2,1,D+1}=\frac{(D+12)(D+11)(D+10)}{2}\binom{D+9}{8}\equiv 1 \pmod 2,$$

因此, $z^{D+2}(\gamma^D+\gamma^{-D})$ 是 s_{D+12} 的一项.

(2) $i_1=0$, $i_2=3$, $i_4=4$, $i_3=D+5$. 由于 $\frac{D+11}{2}$ 是奇数且 $4\preceq D+9$, 从而,

$$\binom{D+12}{0,3,4,D+5}=\frac{(D+12)(D+11)(D+10)}{3\cdot 2}\binom{D+9}{4}\equiv 1 \pmod 2,$$

因此, $z^{D+9}(\gamma^{D+1}+\gamma^{-(D+1)})$ 也是 s_{D+12} 的一项. 所以结论成立. □

定理 21 设 $k=6m+5$, 则 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+\gamma zx^{9(2^k-1)})$ 不是向量 bent 函数.

证明 假如 F 是向量 bent 的, 则 $s_{D+4}=0$. 由引理 11 可得 $z^{D+1}(\gamma^{D+1}+\gamma^{-(D+1)})=0$, 于是 $\gamma^{D+1}=1$. 若 $k=5$, 则 $D=3$, 于是 $\gamma^4=1$. 再由 $\gcd(4,2^k+1)=1$ 知 $\gamma=1$, 矛盾.

若 $k\geqslant 11$, 则还有 $s_{D+12}=0$. 由引理 12 可得

$$z^{D+2}(\gamma^D+\gamma^{-D})+z^{D+9}(\gamma^{D+1}+\gamma^{-(D+1)})=z^{D+2}(\gamma^D+\gamma^{-D})=0,$$

从而 $\gamma^D=1$. 因此 $\gamma=1$, 矛盾. □

综合定理 2 和 16–21 的结果, 可得本节的主要结论.

定理 22 对任意整数 $k\geqslant 2$ 和任意的 $a\in\mathbb{F}_{2^{2k}}$, $F(x)=\mathrm{Tr}_k^{2k}(x^{2^k-1}+ax^{9(2^k-1)})$ 都不是向量 bent 函数.

7 总结

本文在文献 [23] 的工作基础上继续深入研究了 $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+ax^{r(2^k-1)})$ 的向量 bent 性并得到了一些进一步的结果. 具体地, 对 $r\mid 2^k+1$ 的情形, 我们证明了文献 [23] 得到的必要条件是充要

条件, 从而完全确定了 F 的向量 bent 性. 而对于 $r \nmid 2^k+1$ 的情形, 我们通过引入 Lucas 公式并结合有限域的群结构, 最终完全确定了 F 在 r 分别等于 5、7 和 9 时的向量 bent 性. 特别地, 我们给出了一些反例, 否定了文献 [23] 提出的当 $k \geqslant 2$ 为偶数时不存在此类向量 bent 函数的猜想. 同时, 我们的研究结果表明, 二项式向量 bent 函数数量确实非常少. 事实上, 我们找到的反例都属于 $k=2$ 的情形. 因此, 当 $k \geqslant 4$ 时, 是否存在此类向量 bent 函数仍然是一个公开问题. 此外, 本文的方法能比较有效地解决 r 为某个特定奇数的情形, 例如, 还可类似地解决 $r=11,13,\ldots$ 的情形, 并对解决 $r=3$ 的情形也有帮助 (文献 [23] 中计算出了 $l=D+2$, $l=D+4$, $l=D+6$ 时 s_l 的值, 而利用 Lucas 公式, 我们算出了 $D+8 \leqslant l \leqslant D+34$ 时 s_l 的值, 但是这些数值未能提供关于 F 的向量 bent 性的进一步信息). 然而, 若想完全解决 $r \nmid 2^k+1$ 的情形, 还需要更进一步的研究, 在方法上进一步创新.

致谢 本文作者对审稿人提出的宝贵意见表示万分感谢. 本文的主要工作是第一作者在 2014 年访问新加坡国立大学淡马锡实验室期间合作完成的, 他借此对淡马锡实验室的诚挚邀请与热情接待表示感谢.

参考文献

1 Rothaus O S. On bent functions. J Combin Theory Ser A, 1976, 20: 300–305
2 Carlet C, Mesnager S. Four decades of research on bent functions. Des Codes Cryptogr, 2016, 78: 5–50
3 Canteaut A, Charpin P, Kyureghyan G. A new class of monomial bent functions. Finite Fields Appl, 2008, 14: 221–241
4 Carlet C, Charpin P, Zinoviev V. Codes, bent functions and permutations suitable for DES-like cryptosystems. Des Codes Cryptogr, 1998, 15: 125–156
5 Carlet C, Gabborit P. Hyperbent functions and cyclic codes. J Combin Theory Ser A, 2006, 113: 466–482
6 Charpin P, Kyureghyan G. Cubic monomial bent functions: A subclass of $\mathcal{M}$. SIAM J Discrete Math, 2008, 22: 650–665
7 Charpin P, Gong G. Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans Inform Theory, 2008, 54: 4230–4238
8 Leander N G. Monomial bent functions. IEEE Trans Inform Theory, 2006, 52: 738–743
9 Carlet C. Two new classes of bent functions. In: Workshop on the Theory and Application of Cryptographic Techniques, vol. 765. Berlin: Springer, 1993, 77–101
10 Dobbertin H, Leander G, Canteaut A, et al. Construction of bent functions via Niho power functions. J Combin Theory Ser A, 2006, 113: 779–798
11 Leander N G, Kholosha A. Bent functions with 2^r Niho exponents. IEEE Trans Inform Theory, 2006, 52: 5529–5532
12 Youssef A M, Gong G. Hyper-bent functions. In: International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2001, 406–419
13 Dillon J. Elementary Hadamard difference sets. PhD Thesis. Washington: University of Maryland, 1974
14 Mesnager S. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans Inform Theory, 2011, 57: 5996–6009
15 Cao X W, Hu L. A construction of hyperbent functions with polynomial trace form. Sci China Math, 2011, 54: 2229–2234
16 Li N, Helleseth T, Tang X H, et al. Several new classes of bent functions from Dillon exponents. IEEE Trans Inform Theory, 2013, 59: 1818–1831
17 Mesnager S. A new class of bent and hyper-bent Boolean functions in polynomial forms. Des Codes Cryptogr, 2011, 59: 265–279
18 Mesnager S, Flori J P. Hyperbent functions via Dillon-like exponents. IEEE Trans Inform Theory, 2013, 59: 3215–3232
19 Wang B C, Tang C M, Qi Y F, et al. A new class of hyper-bent Boolean functions in binomial forms. ArXiv:1112.0062, 2011
20 Nyberg K. Perfect nonlinear S-boxes. In: Advances in Cryptology-EUROCRYPT'91. Berlin: Springer-Verlag, 1991, 378–385
21 Feng K Q, Yang J. Vectorial Boolean functions with good cryptographic properties. Internat J Found Comput Sci, 2011, 22: 1271–1282
22 Wu J, Wei Y, Wang X. An optimized method for multiple output bent functions. Acta Electron Sinica, 2005, 33:

521–523
23 Muratović-Ribić A, Pasalic E, Bajrić S. Vectorial bent functions from multiple terms trace functions. IEEE Trans Inform Theory, 2014, 60: 1337–1347
24 Pasalic E, Zhang Y. On multiple output bent functions. Inform Process Lett, 2012, 112: 811–815
25 Muratović-Ribić A, Pasalic E, Ribić S. Vectorial hyperbent trace functions from the $\mathcal{PS}_{\rm ap}$ class—their exact number and specification. IEEE Trans Inform Theory, 2014, 60: 4408–4413
26 Fine N. Binomial coefficients modulo a prime. Amer Math Monthly, 1947, 54: 589–592
27 Pasalic E. A note on nonexistence of vectorial bent functions with binomial trace representation in the $\mathcal{PS}^-$ class. Inform Process Lett, 2015, 115: 139–140
28 Pasalic E. Corrigendum to "A note on nonexistence of vectorial bent functions with binomial trace representation in the $\mathcal{PS}^-$ class". Inform Process Lett, 2015, 115: 520–520

On existence of vectorial bent functions from the $\mathcal{PS}_{\rm ap}$ class

PENG Jie, TAN Chik How & KAN HaiBin

Abstract Bent functions are extremal combinatorial objects with wide applications. Recently, the research of bent functions of the form $\mathrm{Tr}_k^n(P(x))$ with $k=1$ or $k=n/2$ and $P(x)\in\mathbb{F}_{2^n}[x]$ has attracted much attention. In this paper, based on the existing results, we further study the vectorial bent property of the binomial trace functions $F(x)=\mathrm{Tr}_k^n(x^{2^k-1}+ax^{r(2^k-1)})$ with $k=n/2\geqslant 2$, r odd and $a\in\mathbb{F}_{2^n}^*$. For the case $r\mid 2^k+1$, we obtain a necessary and sufficient condition for F to be vectorial bent and thus completely determine the vectorial bent property of F for all n and all $a\in\mathbb{F}_{2^n}^*$. While for the case $r\nmid 2^k+1$, a conjecture on the nonexistence of binomial trace bent functions has been proposed by Muratović-Ribić et al. (2014). By employing the powerful Lucas formula, we completely determine the vectorial bent property of F for all n, all $a\in\mathbb{F}_{2^n}^*$, when r equals 5, 7 and 9. In particular, we find a few counter examples to the conjecture.

Keywords **vectorial bent function, binomial trace function, Boolean function, multinomial coefficient, Lucas formula**

MSC(2010) **11T06, 11T23, 11T71**

doi: 10.1360/SCM-2016-0453