弯曲划分 s，向量值对偶弯函数与部分差集†

Jiaxin Wang、Fang-Wei Fu、Yadi Wei

arXiv:2301.00581v1 [cs.IT] 2 Jan 2023

摘要

$V_{(p)^n}$ 的弯曲划分在构造弯曲函数、向量值弯曲函数和广义 Bent 函数方面十分有力，其中 $V_n^{(p)}$是定义在 $\mathbb{F}_p$ 上的 n 维向量空间， n 是偶正整数， p 是素数。众所周知，部分扩散是一类弯曲划分。在 [4], [18],中，提出了两类形式类似于部分扩散的弯曲划分。在 [3], 中，又从（预）半域出发提出了更多弯曲划分 Γ_1、Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2，其中包括 [4], [18]中给出的弯曲划分。本文研究弯曲划分与向量值对偶弯函数之间的关系。对于任意素数 p，我们证明，可以由某些向量值对偶弯函数（称为满足条件 A 的向量值对偶弯函数）生成某些弯曲划分（称为满足条件 $\mathcal{C}$ 的弯曲划分）。特别地，当 p 为奇素数时，我们证明，满足条件 $\mathcal{C}$ 的弯曲划分与满足条件 A 的向量值对偶弯函数一一对应。我们以向量值对偶弯函数的形式，给出 Γ_1、Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2 为弯曲划分的另一种证明。我们提出一种向量值对偶弯函数的二次构造，可用于生成更多弯曲划分。我们证明，任意 2-形式的三元弱正则弯曲函数 $f\colon V_n^{(3)} \to \mathbb{F}_3$ （n 为偶数）都能生成一个弯曲划分。当这样的 f 是弱正则但非正则时，由 f 生成的弯曲划分并非源自正规弯曲划分，从而回答了 [4]中提出的一个未解决问题。我们给出从弯曲划分构造部分差集的一个充分条件；当 p 为奇素数时，还从部分差集的角度刻画了满足条件 $\mathcal{C}$ 的弯曲划分。

索引词

弯曲划分；弯曲函数；向量值弯曲函数；向量对偶弯曲函数；半域；部分差集

Jiaxin Wang、Fang-Wei Fu 和 Yadi Wei 就职于中国天津 300071 南开大学陈省身数学研究所和 LPMC，电子邮箱：wjiaxin@mail.nankai.edu.cn、fwfu@nankai.edu.cn、wydecho@mail.nankai.edu.cn。

†本研究得到国家重点研发计划（项目编号：2018YFA0704703 和 2022YFA1005001）、国家自然科学基金（项目编号：12141108、61971243、12226336）、天津市自然科学基金（20JCZDJC00610）、中央高校基本科研业务费（南开大学）以及南开至德基金的资助。

I. 引言

布尔弯曲函数由 Rothaus 引入 [21]，随后由 Kumar、Scholtz 和 Welch [15], 推广为 p元弯曲函数，其中 p 为任意素数。由于 p元弯曲函数在密码学、编码理论、序列和组合学中的应用，它们得到了广泛研究。关于 p元弯曲函数及其推广（如向量 Bent 函数和广义 Bent 函数），可参阅综述 [5], [17] 和专著 [19] 。

在 [10], Ç.es¸melio˘glu 等人首次提出了向量值对偶弯函数，这是向量值弯曲函数的一个特殊类别。在 [7], [8], [22], 中，向量值对偶弯函数被用于构造部分差集。特别地，Wang 和 Fu [22] 证明，对于某些向量值对偶弯函数 $F: V_{(n}^{p} \to V_s^{(p))}$（其中 $V_{(p)n}$ 是素域$\mathbb{F}_p$上的一个 n维向量空间），任意 $V_s^{(p)}$的子集在 F 下的原像集都是一个部分差集。

最近，文献 [4], [18], 引入了 $V_n^{(p)}$ 的弯曲划分，它们在构造弯曲函数、向量值弯曲函数和广义 Bent 函数方面颇为有力。众所周知，部分扩散是弯曲划分的一类。在 [18], 中，Meidl 和 Pirsic 首次提出了两类不同于部分扩散的弯曲划分。在 [4], 中，Anbar 和 Meidl 将 [18] 中的研究推广到 p 为奇数的情形，并给出了相应的两类奇数 p 的弯曲划分。在 [3], 中，Anbar、Kalaycı 和 Meidl 提出了更多由（预）半域得到的弯曲划分 Γ_1 $\Gamma_2\Gamma_1^\bullet\Gamma_2^\bullet\Theta_1\Theta_2$，其中包括 [4], [18] 中给出的弯曲划分。在 [2], 中，Anbar、Kalaycı 和 Meidl 证明， [4], [18] 中给出的弯曲划分里的任意若干个元素之并都会构成一个部分差集。在构造部分差集方面，某些向量值对偶弯曲函数和某些弯曲划分似乎发挥着相同的作用。因此，研究向量值对偶弯曲函数与弯曲划分之间的关系颇有意义。本文证明，利用某些向量值对偶弯曲函数（称为满足条件 A 的向量值对偶弯曲函数），可以为任意素数 p 构造具有某些性质的 $V_n^{(p)}$ 弯曲划分（称为满足条件 $\mathcal{C}$ 的弯曲划分）。特别地，当 p 为奇素数时，我们证明，满足条件 $\mathcal{C}$ 的 $V_n^{(p)}$ 弯曲划分与满足条件 A 的向量值对偶弯曲函数一一对应。以向量值对偶弯曲函数为出发点，我们给出另一种证明，说明 [3] 中给出的 $\Gamma_1\Gamma_2\Gamma_1^\bullet\Gamma_2^\bullet\Theta_1\Theta_2$ 是弯曲划分。我们给出一种向量值对偶弯曲函数的二次构造，可用于生成更多弯曲划分。我们证明，任意三元弱正则弯曲函数 $f: V_n^{(3)} \to \mathbb{F}_3$（$n$ 为偶数）若具有 2-形式，都能生成一个弯曲划分。在特殊情形下

若 f 弱正则但非正则，则由 f 生成的弯曲划分并非源自正规弯曲划分，这回答了 [4] 中提出的一个未解决问题。我们利用向量值对偶弯曲函数作为弯曲划分与部分差集之间的桥梁，给出了从弯曲划分构造部分差集的一个充分条件。当 p 为奇素数时，我们从部分差集的角度刻画了满足条件 $\mathcal{C}$ 的弯曲划分。

本文其余部分安排如下。在第二节中，我们陈述一些关于向量值对偶弯曲函数和弯曲划分的必要结果。在第三节中，我们介绍某些弯曲划分与某些向量值对偶弯曲函数之间的关系。在第四节中，我们给出一种向量值对偶弯曲函数的二次构造方法，该方法可用于生成更多弯曲划分。在第五节中，我们介绍某些弯曲划分与某些部分差集之间的关系。在第六节中，我们作出总结。

II. 预备知识

本节陈述一些关于向量值对偶弯曲函数和弯曲划分的基本结果。首先，我们固定本文中通用的一些记号。

- p 是一个素数。
- $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ 是一个复数的 p次本原单位根。注意， $\zeta_2 = -1$。
- $\mathbb{F}_{p^n}$ 是含有 p^n 个元素的有限域。
- $\mathbb{F}_p^n$ 是 $\mathbb{F}_p$上由 n元组构成的向量空间。
- $V_{(p)n}$ 是 $\mathbb{F}_p$上的 n维向量空间。
- $\langle\cdot\rangle_n$ 表示 $V_{(p)n}$ 的一个（非退化）内积。本文中，当 $V_{(p)n} = \mathbb{F}_{p^n}$时，令 $\langle a, b\rangle_n = Tr_1^n(ab)$，其中 $a, b \in \mathbb{F}_{p^n}$, $Tr_k^n(\cdot)$表示从 $\mathbb{F}_{p^n}$到$\mathbb{F}_{p^k}$, $k \mid n$的迹函数；当 $V_{(p)n} = \mathbb{F}_p^n$时，令 $\langle a, b\rangle_n = a \cdot b = \sum_{i=1}^n a_i b_i$，其中 $a = (a_1, \ldots, a_n)$ $b = (b_1, \ldots, b_n) \in \mathbb{F}_p^n$；当 $V_{(p)n} = V_{(p)n_1} \times \cdots \times V_{(p)n_m} (n = \sum_{i=1}^m n_i)$时，令 $\langle a, b\rangle_n = \sum_{i=1}^m \langle a_i, b_i\rangle_{n_i}$，其中 $a = (a_1, \ldots, a_m)$ $b = (b_1, \ldots, b_m) \in V_{(p)n}$。
- 对于任意集合 $A \subseteq V_{(p)n}$ 和 $u \in V_{(p)n}$，令 $\chi_u(A) = \sum_{x\in A} \chi_u(x)$，其中 χ_u 表示特征标 $\chi_u(x) = \zeta^{\langle u, x\rangle_n}$。

A. 向量对偶弯曲函数

函数 $F: V_n^{(p)} \to V_s^{(p)}$ 称为向量值 p 元函数；当 $s = 1$ 时，简称为 p 元函数。 p 元函数 $f: V_n^{(p)} \to \mathbb{F}_p$ 的 Walsh 变换是一个复值

函数，定义为

$$W_f(a) = \sum_{x \in V_n^{(p)}} \zeta_p^{f(x)-\langle a,x\rangle_n}, a \in V_n^{(p)}. \tag{1}$$

若 p 元函数 $f: V(p)_n \to \mathbb{F}_p$ 满足对所有 $a \in V(p)_n$ 都有 $|W_f(a)| = p^{\frac{n}{2}}$，则称其为弯曲函数。注意，当 f 是布尔弯曲函数，即 $p = 2$ 时，n 必为偶数，因为此时 W_f 是一个取整数值的函数。若向量值 p 元函数 $F: V_n^{(p)} \to V(p)_s$ 的所有分量函数 $F_c: V(p)_n \to \mathbb{F}_p$（$c \in V(s^p \setminus \{0\}$）定义为 $F_c(x) = \langle c, F(x)\rangle_s$）均为弯曲函数，则称其为向量值弯曲函数。已知，若 $F: V(p)_n \to V_s^{(p)}$) 是向量值弯曲函数，则当 $p = 2$ 时有 $s \le \frac{n}{2}$；若 p 是奇素数，则有 $s \le n$。若 $f: V(p)_n \to \mathbb{F}_p$ 是弯曲函数，则 cf、$c \in \mathbb{F}_p^*$ 也都是弯曲函数；也就是说，任意 p 元弯曲函数都是向量值弯曲函数。对于 $F: V_n^{(p)} \to V(p)_s$，F 是否为向量值弯曲函数，与 $V_n^{(p)}$ 和 $V(p)_s$ 的内积无关。p 元弯曲函数 $f: V(p)_n \to \mathbb{F}_p$ 的 Walsh变换满足：对任意 $a \in V_n^{(p)}$，当 $p = 2$ 时，我们有

$$W_f(a) = 2^{\frac{n}{2}}(-1)^{f^*(a)}, \tag{2}$$

且当 p 是一个奇素数时，我们有

$$W_f(a) = \begin{cases} \pm p^{\frac{n}{2}} \zeta_p^{f^*(a)} & \text{if } p \equiv 1 \ (mod\ 4) \text{ or } n \text{ is even}, \\ \pm\sqrt{-1} p^{\frac{n}{2}} \zeta_p^{f^*(a)} & \text{if } p \equiv 3 \ (mod\ 4) \text{ and } n \text{ is odd}, \end{cases} \tag{3}$$

其中，f^* 是从 $V(p)_n$ 到 $\mathbb{F}_p$ 的函数，称为 f 的对偶。若 $f: V(p)_n \to \mathbb{F}_p$ 是一个 p 元弯曲函数，并且满足 $W_f(a) = \varepsilon_f p^{\frac{n}{2}} \zeta_p^{f^*}(a)$，其中 ε_f 是一个与 a 无关的常数，则称其为弱正则；否则，称 f 为非弱正则。特别地，若 $\varepsilon_f = 1$, f 称为正则。f 的（非）弱正则性与 $V_n^{(p)}$ 的内积无关；若 f 是弱正则的，则 ε_f 与 $V_n^{(p)}$ 的内积无关。根据（2），所有布尔弯曲函数都是正则的。若 f 是一个 p 元弱正则弯曲函数，则 f 的对偶 f^* 也是弱正则弯曲函数，且满足 $(f^*)^*(x) = f(-x)$（见 [9]）。

2018年，C¸es¸melio˘glu 等人 [10] 引入了向量对偶弯曲函数。

定义1. 若存在一个向量值弯曲函数 $G: V_n^{(p)} \to V_{(p)s}$，使得对于任意 $c \in V_{(s^p} \setminus \{0\}_)$，均有 $(F_c)^* = G_{\sigma(c)}$，其中 $(F_c)^*$ 是分量函数 $\langle c, F(x)\rangle_s$ 的对偶，且 σ 是 $V_s^{(p)} \setminus \{0\}$ 上的某个置换，则称向量值 p 元弯曲函数 $F: V_n^{(p)} \to V_{(p)s}$ 为向量值对偶弯曲函数。向量值弯曲函数 G 称为 F 的向量值对偶，记作 F^*。

已知 [10] ，向量值对偶弯曲这一性质与 $V_n^{(p)}$和 $V_{(p)s}$ 的内积无关。注意，对于向量值对偶弯曲函数，其向量值对偶并不唯一，因为函数是向量值弯曲且向量值对偶弯曲的性质，取决于由所有分量函数构成的向量空间（见 [10]中的注释1）。例如，若一个p元函数 f （视为取值于 $V_1^{(p)}$ 的向量值函数， p 为奇数）在任意固定内积下都是向量值对偶弯曲的，则其对偶 f^* 是唯一的，但其向量值对偶并不唯一，因为对于任意$c \in \mathbb{F}_p^*$， cf^*都是 f的一个向量值对偶。称一个 p元函数 f: $V_{(p)n} \to \mathbb{F}_p$为 l形式，若对于任意 $a \in \mathbb{F}_p^*$ 和 $x \in V_{(p)n}$，均有$f(ax) = a^l f(x)$，其中 $1 \le l \le p-1$为整数。根据 [7], [22], 中的结果，我们有以下命题。

命题1（ [7], [22]）。若一个 p 元函数 f 满足 $f(0) = 0$ ，则它是弱正则向量值对偶弯曲函数，当且仅当 f 是 l 形式的弱正则弯曲函数，且 $gcd(l-1, p-1) = 1$。特别地，对于任意 $c \in \mathbb{F}_p^*$，一个 p 元函数 f 满足 $(cf)^* = cf^*$，当且仅当 f 是 $(p-1)$ 形式的弱正则弯曲函数时，它是弱正则向量值对偶弯曲函数。

在本小节余下部分，我们回顾一类重要的 p 元弯曲函数，称为 Maiorana-McFarland 弯曲函数。

- 令 f: $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_p$ 定义如下:

$$f(x, y) = Tr_1^n(\alpha x \pi(y)) + g(y),$$

其中 $\alpha \in \mathbb{F}_{p^n}^*$, π 是 $\mathbb{F}_{p^n}$ 上的一个置换，而 $g: \mathbb{F}_{p^n} \to \mathbb{F}_p$ 是任意函数。
则 f 是弯曲函数，称为 Maiorana-McFarland 弯曲函数。 f 的对偶 f^* 为

$$f^*(x, y) = Tr_1^n(-\pi^{-1}(\alpha^{-1}x)y) + g(\pi^{-1}(\alpha^{-1}x)). \tag{4}$$

所有 Maiorana-McFarland 弯曲函数都是正则的（见 [15]）。

B. 弯曲划分

最近，人们引入了 $V_n^{(p)}$的弯曲划分这一概念 [4], [18]。

定义2. 设 n 为偶正整数， K 为可被 p整除的正整数。

- 设 $\Gamma = \{A_1, \ldots, A_K\}$是 $V_{(p)n}$的一个划分。假设对于每个满足以下条件的函数 f: 每个$i \in \mathbb{F}_p$ 在其原像中恰好包含 $\frac{K}{p}$ 个来自 Γ 的集合 A_j ，该函数都是一个 p元弯曲函数。那么， Γ 称为 $V_{(p)n}$ 的一个深度为 K 的弯曲划分，而每个这样的弯曲函数 f 称为由弯曲划分 Γ构造的弯曲函数。

• 设 $\Gamma = \{U, A_1, \ldots, A_K\}$ 是 $V_{(p)n}$ 的一个划分。假设每个满足以下性质的函数 f 都是弯曲函数：

(1) 每个 $c \in \mathbb{F}_p$ 的原像集中恰好包含集合 A_1、……、A_K 中的 $\frac{K}{p}$ 个集合；

(2) 对所有 $x \in U$， $f(x) = c_0$，其中 $c_0 \in \mathbb{F}_p$ 为某个固定值。

于是，我们称 Γ 为 $V_n^{(p)}$ 的深度为 K 的正规弯曲划分。

弯曲划分在构造弯曲函数、向量值弯曲函数和广义 Bent 函数方面非常强大。本文着重研究弯曲划分与向量值弯曲函数之间的关系。

命题2（ [4]）。设 $\Gamma = \{A_1, \ldots, A_{p^s}\}$ 是 $V_{(p)^n}$ 的一个弯曲划分。那么，每个函数 F：$V_{(p)^n} \to V_{(p)^s}$，若每个元素 $i \in V_s^{(p)}$ 的原像中包含 A_j、$1 \le j \le p^s$ 中的某一个集合的元素，且恰好对应一个集合，则该函数是向量值弯曲函数。

已知部分扩散是一类弯曲划分（例如参见 [4]的第2节）。在[4], [18], 中，介绍了两类不同于部分扩散的显式弯曲划分。在[3], 中，给出了来自某些（预）半域的弯曲划分 Γ_1、Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2，其中包括 [4], [18]中给出的弯曲划分。我们将回顾 Γ_1、Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2 中给出的弯曲划分 [3]。首先，我们需要介绍一些关于（预）半域的基本知识。

定义3. 设 $\circ$ 是定义在（$V_{(p)^n}, +$）上的二元运算，使得

(i) $x \circ y = 0$ 推出 $x = 0$ 或 $y = 0$, (ii) $(x + y) \circ z = (x \circ z) + (y \circ z)$, ($z \circ (x + y) = (z \circ x) + (z \circ y)$, 分别),

对所有 $x, y, z \in V_{(p)^n}$ 均成立。则$(V_{(p)^n}, +, \circ)$称为右（分别为左）预拟域。如果$(V_{(p)^n}, +, \circ)$既是右预拟域又是左预拟域，则称为预半域。如果$(V_{(p)^n}, +, \circ)$是预半域，且存在元素 $e \neq 0$，使得对所有 $x \in V_{(p)^n}$， $e \circ x = x \circ e = x$ 均成立，则称为半域。

设 $P = (\mathbb{F}_{p^n}, +, \circ)$ 是一个预半域。则可由 P 得到预半域 $P^\bullet = (\mathbb{F}_{p^n}, +, \bullet)$ 和 $P^\star = (\mathbb{F}_{p^n}, +, \star)$，其中 $\bullet$ 和 $\star$ 由下式给出

$$x \bullet y = y \circ x \text{ for all } x, y \in \mathbb{F}_{p^n},$$

and

$$Tr_1^n(z(x \circ y)) = Tr_1^n(x(z \star y)) \text{ for all } x, y, z \in \mathbb{F}_{p^n},$$

分别为。预半域 $P^\star$ 被称为 P 的对偶。设 s 是 n 的一个正因子。若对于任意 x、$y \in \mathbb{F}_{p^n}$、$c \in \mathbb{F}_{p^s}$，均有 $x \circ (cy) = c(x \circ y)$ 成立，则称 P 为右 $\mathbb{F}_{p^s}$-线性的。每个预半域 $P = (\mathbb{F}_{p^n}, +, \circ)$ 都可通过以下变换诱导出一个半域 $P' = (\mathbb{F}_{p^n}, +, *)$：任取 $\alpha \in \mathbb{F}_{p^n}^*$，并令 $*$ 为

$$(x \circ \alpha) * (\alpha \circ y) = x \circ y \text{ for all } x, y \in \mathbb{F}_{p^n}.$$

根据 [3], 的引理2，若 P 是右 $\mathbb{F}_{p^s}$-线性的，则 P' 也为右 $\mathbb{F}_{p^s}$-线性。有限域 $\mathbb{F}_{p^n}$ 是右 $\mathbb{F}_{p^s}$-线性半域（即 $\circ$ 是域乘法）。更多右 $\mathbb{F}_{p^s}$-线性（预）半域的内容，请参阅 [3] 的第 3 节。

现在回顾 [3] 中给出的弯曲划分 Γ_1、Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2。

- 令 n、s 为满足 $s \mid n$ 且 $gcd(p^n-1,\ p^s+p-1) = 1$ 的正整数。设 $u = p^s+p-1$，并令 d 为满足 $du \equiv 1\ mod\ (p^n-1)$ 的整数。令 $P = (\mathbb{F}_{p^n},\ +,\ \circ)$ 为一个（预）半域，使其对偶 $P^\star = (\mathbb{F}_{p^n},\ +,\ \star)$ 是右 $\mathbb{F}_{p^s}$-线性的。对于给定的 $x \in \mathbb{F}_{p^n}$，若 $x = 0$，则令$\eta_x = 0$；若 $x \neq 0$，则令 η_x 由 $x \star \eta_x^{-1} = 1$ 给出。

- 定义
$$U_t = \{(x, t \circ x^u) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } U = \{(0, y) : y \in \mathbb{F}_{p^n}\}.$$
令 $i_0 \in \mathbb{F}_{p^s}$ 为任意元素。定义
$$\Gamma_1 = \{A_i, i \in \mathbb{F}_{p^s}\}, \tag{5}$$
其中 $A_i = \bigcup_{t \in \mathbb{F}_{p^n}: Tr_s^n(t) = i} U_t$若 $i \neq i_0$, $A_{i_0} = \bigcup_{t \in \mathbb{F}_{p^n}: Tr_s^n(t) = i_0} U_t \bigcup U$。

- 定义
$$U_t^\bullet = \{(x, x^u \circ t) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } U = \{(0, y) : y \in \mathbb{F}_{p^n}\}.$$
令 $i_0 \in \mathbb{F}_{p^s}$ 为任意元素。定义
$$\Gamma_1^\bullet = \{A_i^\bullet, i \in \mathbb{F}_{p^s}\}, \tag{6}$$
其中 $A_i^\bullet = \bigcup_{t \in \mathbb{F}_{p^n}: Tr_s^n(t) = i} U_t^\bullet$若 $i \neq i_0$, $A_{i_0}^\bullet = \bigcup_{t \in \mathbb{F}_{p^n}: Tr_s^n(t) = i_0} U_t^\bullet \bigcup U$。

- 定义
$$V_t = \{(t \circ x^d, x) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } V = \{(x, 0) : x \in \mathbb{F}_{p^n}\}.$$
令 $i_0 \in \mathbb{F}_{p^s}$ 为任意元素。定义
$$\Gamma_2 = \{B_i, i \in \mathbb{F}_{p^s}\}, \tag{7}$$

其中 $B_i = \bigcup_{t\in\mathbb{F}_{p^n}:\ Tr_s^n(t)=i} V_i$当 $i \neq i_0$时， $B_{i_0} = \bigcup_{t\in\mathbb{F}_{p^n}:\ Tr_s^n(t)=i_0} V_i \bigcup V$。

- 定义

$$V_t^\bullet = \{(x^d \circ t, x) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } V = \{(x, 0) : x \in \mathbb{F}_{p^n}\}.$$

设 $i_0 \in \mathbb{F}_{p^s}$ 为任意元素。定义

$$\Gamma_2^\bullet = \{B_i^\bullet, i \in \mathbb{F}_{p^s}\}, \tag{8}$$

其中 $B_i^\bullet = \bigcup_{t\in\mathbb{F}_{p^n}:Tr_s^n(t)=i} V_i^\bullet$若 $i \neq i_0$, $B_{i_0} = \bigcup_{t\in\mathbb{F}_{p^n}:Tr_s^n(t)=i_0} V_i^\bullet \bigcup V$。

- 定义

$$X_t = \{(t\eta_x^d, x) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } X = \{(x, 0) : x \in \mathbb{F}_{p^n}\}.$$

设 $i_0 \in \mathbb{F}_{p^s}$ 为任意元素。定义

$$\Theta_1 = \{S_i, i \in \mathbb{F}_{p^s}\}, \tag{9}$$

其中 $S_i = \bigcup_{t\in\mathbb{F}_{p^n}:Tr_s^n(t)=i} X_t$若 $i \neq i_0$, $S_{i_0} = \bigcup_{t\in\mathbb{F}_{p^n}:Tr_s^n(t)=i_0} X_t \bigcup X$。

- 定义

$$Y_t = \{(x, t\eta_x^u) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } Y = \{(0, y) : y \in \mathbb{F}_{p^n}\}.$$

令 $i_0 \in \mathbb{F}_{p^s}$ 为任意元素。定义

$$\Theta_2 = \{T_i, i \in \mathbb{F}_{p^s}\}, \tag{10}$$

其中 $T_i = \bigcup_{t\in\mathbb{F}_{p^n}:\ Tr_s^n(t)=i} Y_t$若 $i \neq i_0$, $T_{i_0} = \bigcup_{t\in\mathbb{F}_{p^n}:\ Tr_s^n(t)=i_0} Y_t \bigcup Y$。

注释1. 在有限域情形下，也就是说， $\circ$ 和 $\star$ 是域乘法，则 $\Gamma_1 = \Gamma_1^\bullet = \Theta_2, \Gamma_2 = \Gamma_2^\bullet = \Theta_1$，这可化为 *[4], [18]*中给出的两类弯曲划分。

注释2. 事实上，对于弯曲划分 $\Gamma_1, \Gamma_1^\bullet, \Gamma_2, \Gamma_2^\bullet, \Theta_1, \Theta_2$中的参数 u ，根据 *[3]*中的证明，可以考虑更一般的形式 $u \equiv p^j \ mod\ (p^s - 1)$。

III. 某些弯曲划分与某些向量值函数之间的关系

对偶弯函数

本节中，我们分别考虑满足以下条件的弯曲划分和向量对偶弯曲函数。

条件 $\mathcal{C}$: 设 n 为偶正整数， s 为正整数，且 $s \leq \frac{n}{2}$。设$\Gamma = \{A_i, i \in V_{(s}{}^p\}$)为 $V_{(p)n}$ 的弯曲划分，并满足 $\mathbb{F}_p^* A_i = A_i$ 对所有 $i \in V_{(p)s}$

并且由 Γ 构造的所有弯曲函数 f 都是正则的（即 $\varepsilon_f = 1$），或是弱正则但非正则的（即 $\varepsilon_f = -1$）。我们用 $\varepsilon = \varepsilon_f$ 表示由 Γ 构造的所有弯曲函数 f。

条件 A：设 n 为偶正整数，s 为满足 $s \le \frac{n}{2}$ 的正整数。设F：$V_{(p)n} \to V_{(p)s}$为一个向量值对偶弯曲函数，满足 $(F_c)^* = (F^*)_c, c \in V_{(s^p \setminus \{0\})}$，其中 F 的向量值对偶为 F^*，且所有分量函数均为正则或弱正则但非正则，即 $\varepsilon_{F_c}, c \in V_{(s^p \setminus \{0\})}$都相同。对于所有 $c \in V_{(s^p \setminus \{0\})}$，记作 $\varepsilon = \varepsilon_{F_c}$。

不难看出，已知的弯曲划分，包括部分扩散以及由 (5)-(10) 定义的 $\Gamma_i, \Gamma_i^\bullet, \Theta_i, i = 1, 2$, 均满足 $\mathbb{F}_p^* A_i = A_i, i \in V_{(p)s}$。根据 [3], [11], [14], 中的结果，所有由部分扩散和 $\Gamma_i, \Gamma_i^\bullet$, $\Theta_i, i = 1, 2$ 构造的弯曲函数都是正则的。因此，已知的弯曲划分均满足条件 $\mathcal{C}$，其中 $\varepsilon = 1$。此外，当 $p = 2$时，容易看出，对于深度为 2 的幂的 $V_n^{(2)}$的任意弯曲划分，条件 $\mathcal{C}$ 都是平凡的。本节将介绍满足条件 $\mathcal{C}$ 的弯曲划分与满足条件 A 的向量值对偶弯曲函数之间的关系。首先，我们需要一个引理。

引理 1. 设 n 为偶正整数，s 为满足 $s \le \frac{n}{2}$ 的正整数，且 F：$V_{(p)n} \to V_s^{(p)}$。那么以下两个陈述等价。

(1) F 是满足条件 A 的向量值对偶弯曲函数。

(2) 存在两两不交集 $W_i \subseteq V_{(p)n}, i \in V_{(p)s}$，其中 $\bigcup_{i \in V_s^{(p)}} W_i = V_{(p)n}$，以及常数 $\varepsilon \in \{\pm 1\}$（若 $p = 2$，则 $\varepsilon = 1$），使得对于任意非空集合 $I \subseteq V_s^{(p)}$,

$$\chi_u(D_{F,I}) = p^{n-s}\delta_{\{0\}}(u)|I| + \varepsilon p^{\frac{n}{2}-s}(p^s \delta_{W_I}(u) - |I|), u \in V_n^{(p)}, \tag{11}$$

其中 $D_{F,I} = \{x \in V_{(p)n}: F(x) \in I\}$, $W_I = \bigcup_{i \in I} W_i$; 对于任意集合 S, δ_S 表示 S 的示性函数。

证明. 根据 [22] 的命题 3（注意，尽管 [22] 的命题 3 只考虑 p 为奇数的情形，但 $p = 2$ 也成立），对于任意 $u \in V_{(p)n}, i \in V_{(p)s}$，我们有

$$\chi_u(D_{F,i}) = p^{n-s}\delta_{\{0\}}(u) + p^{-s} \sum_{c \in V_s^{(p)} \setminus \{0\}} W_{F_c}(-u)\zeta_p^{-\langle c,i \rangle_s}, \tag{12}$$

其中 $D_{F,\ i} = \{x \in V_{\ (p)\ n}: F(x) = i\}$。

（1） ⇒ （2）：若 F 是满足条件 A 的向量值对偶弯曲函数（注意，若 $p=2$，则 $\varepsilon=1$，因为所有布尔弯曲函数都是正则的），那么

$$\begin{aligned}\chi_u(D_{F,i}) &= p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}\sum_{c\in V_s^{(p)}\backslash\{0\}}\zeta_p^{(F_c)^*(-u)-\langle c,i\rangle_s}\\ &= p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}\sum_{c\in V_s^{(p)}\backslash\{0\}}\zeta_p^{(F^*)_c(-u)-\langle c,i\rangle_s}\\ &= p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}\sum_{c\in V_s^{(p)}\backslash\{0\}}\zeta_p^{\langle c,F^*(-u)-i\rangle_s}\\ &= p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}(p^s\delta_{\{0\}}(F^*(-u)-i)-1).\end{aligned} \tag{13}$$

定义 $W_i=\{x\in V_{(p)n}: F^*(-x)=i\}, i\in V_{(p)s}$。那么，对于任意 $i\neq j$ 和 $\bigcup_{i\in V_s^{(p)}}W_i=V_{(p)n}$，都有 $W_i\bigcap W_j=\emptyset$。由（13），对于任意非空集合 $I\subseteq V_{(p)s}$ 和 $u\in V_{(p)n}$，我们有

$$\begin{aligned}\chi_u(D_{F,I}) &= \sum_{i\in I}\chi_u(D_{F,i})\\ &= \sum_{i\in I}p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}(p^s\delta_{W_i}(u)-1)\\ &= p^{n-s}\delta_{\{0\}}(u)|I|+\varepsilon p^{\frac{n}{2}-s}(p^s\delta_{W_I}(u)-|I|).\end{aligned}$$

（2） ⇒ (1)：根据关于 W_i 的假设，$i\in V_{(p)s}$，我们可知，对于任意 $x\in V_{(p)n}$，存在唯一的 $i\in V_{(p)s}$ 使得 $x\in W_i$。定义 $G: V_n^{(p)}\to V_{(p)s}$ 为

$$G(x)=i \text{ if } -x\in W_i.$$

根据 G 的定义，对于任意 $u\in V_{(p)n}$，$i\in V_{(p)s}$，我们有

$$\chi_u(D_{F,i})=p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}(p^s\delta_{\{0\}}(G(-u)-i)-1). \tag{14}$$

对于任意 $c\in V_s^{(p)}\backslash\{0\}$,

$$\begin{aligned}W_{F_c}(-u) &= \sum_{x\in V_n^{(p)}}\zeta_p^{\langle c,F(x)\rangle_s+\langle u,x\rangle_n}\\ &= \sum_{i\in V_s^{(p)}}\sum_{x\in V_n^{(p)}:F(x)=i}\zeta_p^{\langle c,i\rangle_s+\langle u,x\rangle_n}\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i\in V_s^{(p)}} \zeta_p^{\langle c,i\rangle_s}\chi_u(D_{F,i}) \\
&= \sum_{i\in V_s^{(p)}\backslash\{G(-u)\}} \zeta_p^{\langle c,i\rangle_s}(p^{n-s}\delta_{\{0\}}(u)-\varepsilon p^{\frac{n}{2}-s}) + (p^{n-s}\delta_{\{0\}}(u)+\varepsilon p^{\frac{n}{2}-s}(p^s-1))\zeta_p^{\langle c,G(-u)\rangle_s} \\
&= (p^{n-s}\delta_{\{0\}}(u)-\varepsilon p^{\frac{n}{2}-s})\sum_{i\in V_s^{(p)}} \zeta_p^{\langle c,i\rangle_s} + \varepsilon p^{\frac{n}{2}}\zeta_p^{G_c(-u)} \\
&= \varepsilon p^{\frac{n}{2}}\zeta_p^{G_c(-u)}.
\end{aligned} \tag{15}
$$

由 (15) 以及假设 $\varepsilon = 1$ if $p = 2$, F 是一个向量值弯曲函数，满足 $\varepsilon_{F_c} = \varepsilon$ 且对于任意 $c \in V_s^{(p)}\backslash\{0\}$，有 $(F_c)^* = G_c$。由于 F_c 是一个弱正则弯曲函数，我们有 $G_c =(F_c)^*$ 也是弱正则弯曲函数，且 G 是向量值弯曲函数。因此， F 是向量值对偶弯曲函数，满足 $\varepsilon_{F_c} = \varepsilon$，并且对于任意 $c \in V_{(s^p}\backslash\{0\})$，有 $(F_c)^* =(F^*)_c$，其中 $F^* = G$，也就是说，F 满足条件 A。

□

根据引理 1，我们有以下定理。

定理 1. 设 $F:\ V_n^{(p)} \to V_s^{(p)}$是满足条件 A 的向量值对偶弯曲函数。定义

$$A_i = D_{F,i},\ i \in V_s^{(p)},$$

其中 $D_{F,\ i} = \{x \in V_{(p)n}:\ F(x) = i\}$。则 $\Gamma = \{A_i, i \in V_{(s^p}\})$是满足条件 $\mathcal{C}$ 的弯曲划分。

证明. 根据引理 1 及其证明，对于任意 $i \in V_s^{(p)}$和 $u \in V_n^{(p)}$，

$$\chi_u(A_i) = \chi_u(D_{F,i}) = p^{n-s}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-s}(p^s\delta_{\{0\}}(F^*(-u)-i)-1),$$

其中，当 $p = 2$ 时 $\varepsilon = 1$，因为所有布尔弯曲函数都是正则的。对于由 $\{A_i:\ i \in V_s^{(p)}\}$ 中的 p^{s-1} 个集合构成的任意并集 S，我们有

$$\chi_u(S) = \begin{cases} p^{n-1}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-1}(p-1), \text{ if } A_{F^*(-u)} \subseteq S, \\ p^{n-1}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-1}, \text{ if } A_{F^*(-u)} \nsubseteq S. \end{cases} \tag{16}$$

设 f 是任意函数，使得对于每个 $j \in \mathbb{F}_p$，其原像中恰有 p^{s-1} 个集合 A_i 属于 Γ。定义 $g(u) = f(A_{F^*(-u)})$。注意， g 是从 $V_{(p)n}$ 到 $\mathbb{F}_p$ 的 p 元函数。于是，由 (16) 可得

$$\chi_u(D_{f,j}) = \begin{cases} p^{n-1}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-1}(p-1), \text{ if } j = g(u), \\ p^{n-1}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-1}, \text{ if } j \neq g(u). \end{cases} \tag{17}$$

由 (17)，对于任意 $u \in V_n^{(p)}$，我们有

$$\begin{aligned} W_f(-u) &= \sum_{x\in V_n^{(p)}} \zeta_p^{f(x)+\langle u,x\rangle_n} \\ &= \sum_{j\in\mathbb{F}_p} \zeta_p^j \sum_{x\in V_n^{(p)}:f(x)=j} \zeta_p^{\langle u,x\rangle_n} \\ &= \sum_{j\in\mathbb{F}_p} \zeta_p^j \chi_u(D_{f,j}) \\ &= \sum_{j\in\mathbb{F}_p\setminus\{g(u)\}} \zeta_p^j(p^{n-1}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-1}) + \zeta_p^{g(u)}(p^{n-1}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-1}(p-1)) \\ &= (p^{n-1}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-1}) \sum_{j\in\mathbb{F}_p} \zeta_p^j + \varepsilon p^{\frac{n}{2}} \zeta_p^{g(u)} \\ &= \varepsilon p^{\frac{n}{2}} \zeta_p^{g(u)}. \end{aligned} \tag{18}$$

由 (18) 和 $\varepsilon = 1$，若 $p = 2$，则 f 是一个满足 $\varepsilon_f = \varepsilon$ 且 $f^*(x) = g(-x)$ 的弱正则弯曲函数。令

$$W_j = \{u \in V_n^{(p)} : g(u) = j\}, j \in \mathbb{F}_p,$$

则 W_j、$j \in \mathbb{F}_p$ 两两不相交，且 $\bigcup_{j\in\mathbb{F}_p} W_j = V_{(p)n}$。由 (17)，对于任意 $u \in V_{(p)n}$ 和非空集合 $J \subseteq \mathbb{F}_p$，有

$$\chi_u(D_{f,J}) = p^{n-1}\delta_{\{0\}}(u)|J| + \varepsilon p^{\frac{n}{2}-1}(p\delta_{W_J}(u) - |J|), \tag{19}$$

其中 D_f、$_J = \{x \in V_{(p)n}: f(x) \in J\}$，$W_J = \bigcup_{j\in J} W_j$。由 (19) 和引理 1，$f$ 是向量值对偶弯曲的，且对某个 $\beta \in \mathbb{F}_p^*$，有 $(cf)^* = c(\beta f^*)$ $c \in \mathbb{F}_p^*$（因为 f 的所有向量值对偶都是 cf^*、$c \in \mathbb{F}_p^*$）。令 $c = 1$，可得 $\beta = 1$，即 f 是向量值对偶弯曲的，且 $(cf)^* = cf^*$，$c \in \mathbb{F}_{p^*}$。由命题1，f 是一个 $(p-1)$-型。特别地，对于任意 $c \in \mathbb{F}_{p^s}^*$，F_c 都是一个 $(p-1)$-型，由此可得，对于任意 $\alpha \in \mathbb{F}_p^*$ 和 $\mathbb{F}_p^* A_i = A_i$，$F(\alpha x) = F(x)$，$i \in V_{(p)s}$。因此，Γ 是满足条件 $\mathcal{C}$ 的弯曲划分。

□

由定理 1 可得以下推论。

推论1. 设 n 为偶正整数。设 $f: V_n^{(p)} \to \mathbb{F}_p$ 为 $(p-1)$-型弱正则弯曲函数，则 $\{D_{f,j}, j \in \mathbb{F}_p\}$ 是 $V_{(p)n}$ 的弯曲划分，其中 $D_{f,j} = \{x \in V_{(p)n}: f(x) = j\}$。

证明。根据命题1，f 是一个弱正则向量值对偶弯曲函数，且满足（cf）$^* = cf^*$。由于 n 是偶数，对所有 $c \in \mathbb{F}_p^*$ 都有 $\varepsilon_{cf} = \varepsilon_f$（参见 [6]的定理1）。于是由定理1可得结论。

□

如果存在某个 i 使得 $\{U, A_1, \ldots, A_{i-1}, A_i \backslash U, A_{i+1}, \ldots, A_K\}$ 是正规弯曲划分，则称深度为 K 的弯曲划分 $\Gamma = \{A_1, \ldots, A_K\}$ 源自正规弯曲划分。在 [4], 中有一个未解决问题：是否存在不源自深度为 $K > 2$的正规弯曲划分的弯曲划分？下文将对这个未解决问题给出肯定答案。根据 l-形式的定义，三元函数 f 是2-形式，当且仅当$f（x）= f（-x）$。令 n为一个偶正整数。若 f： $V_{(3)n} \to \mathbb{F}_3$，且 $f（x）= f（-x）$是一个弱正则但非正则的三元弯曲函数（即 $\varepsilon_f = -1$），则由推论1可知，$\{D_{f,0}, D_{f,1}, D_{f,2}\}$ 是一个深度为3的弯曲划分。存在这样的三元弯曲函数 f，例如参见 [7], [17]:

- $$f(x) = Tr_1^n(\alpha x^2), x \in \mathbb{F}_{3^n}, \tag{20}$$

  其中 n 为偶数；当 $4 \mid n$ 时， $\alpha \in \mathbb{F}_{3^n}^*$ 为平方元；当 $4 \nmid n$ 时， $\alpha \in \mathbb{F}_{3^n}^*$ 为非平方元；

- $$f(x) = Tr_1^n(ax^{\frac{3^n-1}{4}+3^m+1}), x \in \mathbb{F}_{3^n}, \tag{21}$$

  其中 $n = 2m$、 m 为奇数， $a = \alpha^{\frac{3^m+1}{4}}$ 是 $\mathbb{F}_{3^n}$ 的一个本原元 α；

- $$f(x) = Tr_1^n(\alpha(x^{3^{3k}+3^{2k}-3^k+1} + x^2)), x \in \mathbb{F}_{3^n}, \tag{22}$$

  其中 $n = 4k$ 对任意正整数 k， $\alpha \in \mathbb{F}_{3^{2k}}^*$；

- $$f(x, y, z) = (g(x) - h(x))z^2 + yz + g(x), (x, y, z) \in \mathbb{F}_{3^n} \times \mathbb{F}_3 \times \mathbb{F}_3, \tag{23}$$

  其中 n 为偶数；若 $4 \mid n$，则 g 和 h 是由 (20) 或 (22) 构造的两个不同弯曲函数；若 $4 \nmid n$，则 g和 h 是由 (20) 或 (21) 构造的两个不同弯曲函数。

对于任意三元弱正则但非正则弯曲函数 f： $V_n^{(3)} \to \mathbb{F}_3$ （n 为偶数），且$f（x）= f（-x）$，根据 [4], 的定理4（i），相应的弯曲划分 $\{D_{f,0}, D_{f,1}, D_{f,2}\}$ 并非来源于正规弯曲划分；该结果为 [4] 中提出的上述未解决问题给出了肯定答案。我们首先回顾 [4] 的定理4（i），然后给出一个例子来说明这一事实。

引理2（ [4]）。设 $\Gamma = \{U, A_1, \ldots, A_K\}$是 $V_{(p)^n}$的正规弯曲划分。则 $|U| = p^{\frac{n}{2}}$和 $|A_j| = \frac{p^n - p^{\frac{n}{2}}}{K}$， $1 \le j \le K$。

例1。设 f： $\mathbb{F}_{3^4} \to \mathbb{F}_3$由 $f(x) = Tr_1^4(x^2)$定义。则 f是三元弱正则弯曲函数，且 $f(x) = f(-x)$以及 $\varepsilon_f = -1$。根据推论1， $\{D_{f,0}, D_{f,1}, D_{f,2}\}$是一个弯曲划分。根据Nyberg的结果，对于任意弱正则 p元弯曲函数 g： $V_n^{(p)} \to \mathbb{F}_p$ ，当n为偶数时，有 $\{|D_{g,i}|, i \in \mathbb{F}_p\} = \{p^{n-1} + \varepsilon_f p^{\frac{n}{2}-1}(p-1)\ p^{n-1} - \varepsilon_f p^{\frac{n}{2}-1}\}$。对于我们的例子，$|D_{f,\ 0}| = 21$, $|D_{f,\ 1}| = |D_{f,\ 2}| = 30$。根据引理2，很容易看出 $\{D_{f,0}, D_{f,1}, D_{f,2}\}$ 不可能来自正规弯曲划分。

接下来，基于定理 1，我们给出另一种证明，证明 $\Gamma_i, \Gamma_i^\bullet, \Theta_i, i = 1, 2$（由 [3] 中给出的 (5)-(10) 定义）是弯曲划分。

设 s, n 为正整数， $s \mid n$, u 为满足 $u \equiv p^{j_0}\ mod\,(p^s - 1)$ 的整数，其中某个 $0 \le j_0 \le s-1$ ，且 $gcd(u, p^n - 1) = 1$；再设 d 为满足 $du \equiv 1\ mod\,(p^n - 1)$ 的整数。令 $P = (\mathbb{F}_{p^n}, +, \circ)$ 为一个（预）半域，使其对偶 $P^\star = (\mathbb{F}_{p^n}, +, \star)$ 是右 $\mathbb{F}_{p^s}$-线性的。对于给定的 $x \in \mathbb{F}_{p^n}$，若 $x = 0$，则令 $\eta_x = 0$；若 $x \ne 0$，则令 η_x 由 $x \star \eta_x^{-1} = 1$ 给出（按惯例，设 $\eta_0^{-1} = \eta_0^{p^n-2} = 0$）。对于任意 $\alpha \in \mathbb{F}_{p^n}^*$ 和 $i_0 \in \mathbb{F}_{p^s}$，定义

$$F(x,y) = Tr_s^n(\alpha a(x,y)) + i_0(1 - x^{p^n-1}), (x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, \tag{24}$$

其中，对于给定的 (x, y)，若 $x = 0$，则 $a(x, y) = 0$；若 $x \ne 0$，则 $a(x, y)$ 由$a(x, y) \circ x^u = y$ 给出，且

$$F^\bullet(x,y) = Tr_s^n(\alpha a^\bullet(x,y)) + i_0(1 - x^{p^n-1}), (x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, \tag{25}$$

其中，对于给定的 (x, y)，若 $x = 0$，则 $a^\bullet(x, y) = 0$；若 $x \ne 0$，则 $a^\bullet(x, y)$ 由$x^u \circ a^\bullet(x, y) = y$ 给出，且

$$G(x,y) = Tr_s^n(\alpha b(x,y)) + i_0(1 - y^{p^n-1}), (x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, \tag{26}$$

其中，对于给定的 (x, y)，若 $y = 0$，则 $b(x, y) = 0$；若 $y \ne 0$，则 $b(x, y)$ 由$b(x, y) \circ y^d = x$ 给出，且

$$G^\bullet(x,y) = Tr_s^n(\alpha b^\bullet(x,y)) + i_0(1 - y^{p^n-1}), (x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, \tag{27}$$

其中，对于给定的（x， y），若 $y = 0$，则 $b^\bullet(x,\ y) = 0$；若 $y \ne 0$，则 $b^\bullet(x,\ y)$ 由 $y^d \circ b^\bullet(x,\ y) = x$给出，并且

$$M(x,y) = Tr_s^n(\alpha \eta_x^{-u} y) + i_0(1 - x^{p^n-1}), (x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, \tag{28}$$

and

$$N(x,y) = Tr_s^n(\alpha x \eta_y^{-d}) + i_0(1 - y^{p^n-1}), (x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}. \tag{29}$$

命题 3. 设 F、 $F^{\bullet}$、 G、 $G^{\bullet}$、 M、 N如上定义。则它们都是满足条件 A 且具有 $\varepsilon = 1$ 的向量对偶弯曲函数。

证明。我们只证明 F和 M的结果，因为 $F^{\bullet}$、 G、 $G^{\bullet}$的证明与 F的证明类似，而 N 的证明与 M的证明类似。

- 对于 F:

对于任意 $c \in \mathbb{F}_{p^s}^*$，我们有

$$F_c(x,y) = Tr_1^n(c\alpha a(x,y)) + Tr_1^s(ci_0)(1 - x^{p^n-1}).$$

对于任意 $c \in \mathbb{F}_{p^s}^*$和 $(w,v) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$，我们有

$$\begin{aligned} W_{F_{c^u}}(w,v) &= \sum_{x\in\mathbb{F}_{p^n}^*}\sum_{y\in\mathbb{F}_{p^n}} \zeta_p^{Tr_1^n(c^u\alpha a(x,y))-Tr_1^n(wx+vy)} + \zeta_p^{Tr_1^s(c^u i_0)}\sum_{y\in\mathbb{F}_{p^n}} \zeta_p^{-Tr_1^n(vy)} \\ &= \sum_{x\in\mathbb{F}_{p^n}}\sum_{y\in\mathbb{F}_{p^n}} \zeta_p^{Tr_1^n(c^u\alpha a(x,y))-Tr_1^n(wx+vy)} + p^n(\zeta_p^{Tr_1^s(c^u i_0)} - 1)\delta_{\{0\}}(v) \\ &= W_h(w,v) + p^n(\zeta_p^{Tr_1^s(c^u i_0)} - 1)\delta_{\{0\}}(v), \end{aligned}$$

其中 $h(x,y) = Tr_1^n(c^u\alpha a(x,y))$。对于给定的 $x \in \mathbb{F}_{p^n}$，若 $x = 0$，则令 $\lambda_x = 0$；若 $x \neq 0$，则令 λ_x由 $x \star \lambda_x^{-1} = \alpha$给出（按照惯例，我们设 $\lambda_0^{-1} = \lambda_0^{p^n-2} = 0$）。定义$\rho(x) = \lambda_x^{-d}$。那么 ρ 是 $\mathbb{F}_{p^n}$上的一个置换。对于任意 $x \in \mathbb{F}_{p^n}^*$，令 $z = \rho^{-1}(c^{-1}x)$。那么 $\lambda_z^{-d} = \rho(z) = c^{-1}x$。由 $du \equiv 1 \ mod\ (p^n - 1)$，我们有 $\lambda_z^{-1} = c^{-u}x^u$。由于 $z \neq 0$ 和 $P^{\star}$ 是右 $\mathbb{F}_{p^s}$-线性的，我们有 $\alpha = z \star \lambda_z^{-1} = z \star (c^{-u}x^u) = c^{-u}(z \star x^u)$，即对任意 $x \neq 0$， $\rho^{-1}(c^{-1}x) \star x^u = \alpha c^u$。因此，当 $x \neq 0$时， $Tr_1^n(c^u\alpha a(x,y)) = Tr_1^n(a(x,y)(\rho^{-1}(c^{-1}x) \star x^u))$ $= Tr_1^n(\rho^{-1}(c^{-1}x)(a(x,y) \circ x^u)) = Tr_1^n(\rho^{-1}(c^{-1}x)y)$。当 $x = 0$时，由 $a(0,y) = \rho^{-1}(0) = 0$，我们有 $Tr_1^n(c^u\alpha a(x,y)) = Tr_1^n(\rho^{-1}(c^{-1}x)y) = 0$。因此， $h(x,y) = Tr_1^n(\rho^{-1}(c^{-1}x)y)$，这是一个 Maiorana-McFarland 弯曲函数，并且由 (4),

$$W_h(w,v) = p^n\zeta_p^{-Tr_1^n(cw\rho(v))}.$$

因此，对于任意 $c \in \mathbb{F}_{p^s}^*$,

$$\begin{aligned} W_{F_{c^u}}(w,v) &= p^n(\zeta_p^{-Tr_1^n(cw\rho(v))} + (\zeta_p^{Tr_1^s(c^u i_0)} - 1)\delta_{\{0\}}(v)) \\ &= p^n\zeta_p^{-Tr_1^n(cw\rho(v))+Tr_1^s(c^u i_0)(1-v^{p^n-1})}. \end{aligned} \tag{30}$$

由（30）和 $ud \equiv 1 \ mod\ (p^n - 1)$ 可知，对于任意 $c \in \mathbb{F}_{p^s}^*$, F_c 都是一个正则弯曲函数，且满足

$$\begin{aligned} (F_c)^*(x,y) &= -Tr_1^n(c^d x\rho(y)) + Tr_1^s(ci_0)(1 - y^{p^n-1}) \\ &= -Tr_1^n(c^{dp^{j_0}}(x\rho(y))^{p^{j_0}}) + Tr_1^s(ci_0)(1 - y^{p^n-1}). \end{aligned}$$

由于 $u \equiv p^{j_0} \ mod\ (p^s-1)$ 和 $du \equiv 1 \ mod\ (p^n-1)$，我们有 $d \equiv p^{s-j_0} \ mod\ (p^s-1)$，因此对于任意 $c \in \mathbb{F}_{p^s}^*$，都有 $(c^d)^{p^{j_0}} = c$。所以，F 是一个向量值弯曲函数，满足 $\varepsilon_{F_c} = 1$，并且对于所有 $c \in \mathbb{F}_{p^s}^*$，都有 $(F_c)^* = H_c$，其中

$$H(x,y) = -Tr_s^n((x\rho(y))^{p^{j_0}}) + i_0(1-y^{p^n-1}) = -(Tr_s^n(x\rho(y)))^{p^{j_0}} + i_0(1-y^{p^n-1}).$$

由于 F_c 是正则弯曲函数，因此 $(F_c)^* = H_c$ 也是正则弯曲函数，且 H 是向量值弯曲函数。因此，F 是向量值对偶弯曲函数，其中 $\varepsilon_{F_c} = 1$，并且对于所有 $c \in \mathbb{F}_{p^s}^*$，$(F_c)^* = (F^*)_c$，其中 $F^* = H$，也就是说，F 满足条件 A。

- 对于 M:

对于任意 $c \in \mathbb{F}_{p^s}^*$,

$$M_c(x,y) = Tr_1^n(c\alpha\eta_x^{-u}y) + Tr_1^s(ci_0)(1-x^{p^n-1}).$$

与对 F的讨论类似，对于任意 $c \in \mathbb{F}_{p^s}^*$和 $(w,v) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$，我们有

$$W_{M_c}(w,v) = W_g(w,v) + p^n(\zeta_p^{Tr_1^s(ci_0)} - 1)\delta_{\{0\}}(v),$$

其中 $g(x,y) = Tr_1^n(c\alpha\eta_x^{-u}y)$。令 $\pi(x) = \eta_x^{-u}$，则 π是 $\mathbb{F}_{p^n}$上的一个置换。由于 g是 Maiorana-McFarland 弯曲函数，由 (4) 可得,

$$W_g(w,v) = p^n\zeta_p^{-Tr_1^n(w\pi^{-1}(c^{-1}\alpha^{-1}v))}.$$

对于任意给定的 $y \in \mathbb{F}_{p^n}^*$，令 $\pi^{-1}(c^{-1}\alpha^{-1}y) = z$。则 $c^{-1}\alpha^{-1}y = \pi(z) = \eta_z^{-u}$。由 $ud \equiv 1 \ mod\ (p^n-1)$，可得 $\eta_z^{-1} = c^{-d}\alpha^{-d}y^d$。由于 $z \neq 0$ 且 $P^\star$ 是右 $\mathbb{F}_{p^s}$-线性的，我们有$1 = z \star \eta_z^{-1} = z \star (c^{-d}\alpha^{-d}y^d) = c^{-d}(z \star \alpha^{-d}y^d)$，也就是说，$\pi^{-1}(c^{-1}\alpha^{-1}y) \star \alpha^{-d}y^d = c^d$。对于给定的 $(x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$，若 $y = 0$，则令 $r(x,y) = 0$；若 $y \neq 0$，则令 $r(x,y)$ 由$r(x,y) \circ \alpha^{-d}y^d = x$给出。当 $v \neq 0$时，我们有 $Tr_1^n(w\pi^{-1}(c^{-1}\alpha^{-1}v)) = Tr_1^n(\pi^{-1}(c^{-1}\alpha^{-1}v)(r(w,v) \circ \alpha^{-d}v^d)) = Tr_1^n(r(w,v)(\pi^{-1}(c^{-1}\alpha^{-1}v) \star \alpha^{-d}v^d)) = Tr_1^n(c^d r(w,v)) = Tr_1^n(c(r(w,v))^{p^{j_0}})$。当$v = 0$时，由于 $\pi^{-1}(0) = 0$且 $r(w,0) = 0$，我们有 $Tr_1^n(w\pi^{-1}(c^{-1}\alpha^{-1}v)) = Tr_1^n(c(r(w,v))^{p^{j_0}}) = 0$。因此，$-Tr_1^n(w\pi^{-1}(c^{-1}\alpha^{-1}v)) = -Tr_1^n(c(r(w,v))^{p^{j_0}})$，并且

$$\begin{aligned} W_{M_c}(w,v) &= p^n(\zeta_p^{-Tr_1^n(c(r(w,v))^{p^{j_0}})} + (\zeta_p^{Tr_1^s(ci_0)} - 1)\delta_{\{0\}}(v)) \\ &= p^n\zeta_p^{-Tr_1^n(c(r(w,v))^{p^{j_0}}) + Tr_1^s(ci_0)(1-v^{p^n-1})}, \end{aligned}$$

这意味着 M 是一个向量值对偶弯曲函数，满足 $\varepsilon_{M_c} = 1$，并且对所有$c \in \mathbb{F}_{p^s}^*$，都有 $(M_c)^* = (M^*)_c$，其中

$$M^*(x,y) = -Tr_s^n((r(x,y))^{p^{j_0}}) + i_0(1-y^{p^n-1}),$$

也就是说， M 满足条件 A。 □

根据定理 1 和命题 3，可知 $\{D_{F,i}, i \in \mathbb{F}_{p^s}\}$、$\{D_{F^\bullet,i}, i \in \mathbb{F}_{p^s}\}$、$\{D_{G,i}, i \in \mathbb{F}_{p^s}\}$、$\{D_{G^\bullet,i}, i \in \mathbb{F}_{p^s}\}$、$\{D_{M,i}, i \in \mathbb{F}_{p^s}\}$和 $\{D_{N,i}, i \in \mathbb{F}_{p^s}\}$都是弯曲划分。容易验证

$$D_{F,i} = \begin{cases} \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i} U_t, & \text{if } i \neq i_0, \\ \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i_0} U_t \bigcup U, & \text{if } i = i_0, \end{cases}, \; D_{F^\bullet,i} = \begin{cases} \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i} U_t^\bullet, & \text{if } i \neq i_0, \\ \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i_0} U_t^\bullet \bigcup U, & \text{if } i = i_0, \end{cases},$$

$$D_{G,i} = \begin{cases} \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i} V_t, & \text{if } i \neq i_0, \\ \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i_0} V_t \bigcup V, & \text{if } i = i_0, \end{cases}, \; D_{G^\bullet,i} = \begin{cases} \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i} V_t^\bullet, & \text{if } i \neq i_0, \\ \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i_0} V_t^\bullet \bigcup V, & \text{if } i = i_0, \end{cases},$$

$$D_{M,i} = \begin{cases} \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i} X_t, & \text{if } i \neq i_0, \\ \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i_0} X_t \bigcup X, & \text{if } i = i_0, \end{cases}, \; D_{N,i} = \begin{cases} \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i} Y_t, & \text{if } i \neq i_0, \\ \bigcup\limits_{t\in\mathbb{F}_{p^n}:Tr_s^n(\alpha t)=i_0} Y_t \bigcup Y, & \text{if } i = i_0, \end{cases}$$

其中

$$U_t = \{(x, t \circ x^u) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } U = \{(0, y) : y \in \mathbb{F}_{p^n}\},$$

$$U_t^\bullet = \{(x, x^u \circ t) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } U = \{(0, y) : y \in \mathbb{F}_{p^n}\},$$

$$V_t = \{(t \circ x^d, x) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } V = \{(x, 0) : x \in \mathbb{F}_{p^n}\},$$

$$V_t^\bullet = \{(x^d \circ t, x) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } V = \{(x, 0) : x \in \mathbb{F}_{p^n}\},$$

$$X_t = \{(t\eta_x^d, x) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } X = \{(x, 0) : x \in \mathbb{F}_{p^n}\},$$

$$Y_t = \{(x, t\eta_x^u) : x \in \mathbb{F}_{p^n}^*\} \text{ if } t \in \mathbb{F}_{p^n}, \text{ and } Y = \{(0, y) : y \in \mathbb{F}_{p^n}\}.$$

对于由向量值对偶弯曲函数 $F, F^\bullet, G, G^\bullet, M, N$得到的上述弯曲划分，通过令 $\alpha = 1$, $u = p^s + p - 1$ 满足 $gcd(u, p^n - 1) = 1$，我们便可分别得到由 (5)-(10) 定义的弯曲划分$\Gamma_1, \Gamma_1^\bullet, \Gamma_2, \Gamma_2^\bullet, \Theta_1, \Theta_2$。因此，根据上述分析，我们给出了另一种推导，说明 $\Gamma_1, \Gamma_1^\bullet, \Gamma_2, \Gamma_2^\bullet$, Θ_1, Θ_2 是弯曲划分。

当 p 为奇素数时，我们证明定理 1 的逆命题也成立。

定理 2. 设 p 为奇素数。设 $\Gamma = \{A_i, i \in V_{(s^p)}\}$是 $V_{(p)n}$ 的一个满足条件 $\mathcal{C}$的弯曲划分。定义 F: $V_n^{(p)} \to V_s^{(p)}$如下:

$$F(x) = i \text{ if } x \in A_i.$$

那么， F 是一个满足条件 A 的向量值对偶弯曲函数。

证明。由于 $\mathbb{F}_p^* A_i = A_i$对任意 $i \in V_{(p)s}$均成立，由 Γ构造的所有弯曲函数都是 $(p-1)$-型。当 $s = 1$时，结论由命题1得出。下面我们考虑 $s \geq 2$的情形。

设 f 是由 Γ 构造的任意弯曲函数。根据 [13]，的引理 3.4，对于任意 $u \in V_n^{(p)}$ 和 $j \in \mathbb{F}_p$，我们有

$$\chi_u(D_{f,j}) = \begin{cases} p^{n-1}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-1}(p-1), \text{ if } f^*(u) = j, \\ p^{n-1}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-1}, \text{ if } f^*(u) \neq j, \end{cases} \tag{31}$$

其中 $D_{f,\ j} = \{x \in V_{(p)n} :\ f(x)\ = j\}, j \in \mathbb{F}_p$。对于任意固定的 $u \in V_{(p)n}$，由于

$$\{\chi_u(D_{f,j}), j \in \mathbb{F}_p\} = \{p^{n-1}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-1}(p-1), p^{n-1}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-1}\}$$

对于任意由 Γ 构造的弯曲函数 f，我们有：对于任意固定的 $u \in V_n^{(p)}$，存在唯一的 $G(u) \in V_{(p)s}$，使得 $\chi_u(A_i)\ i \neq G(u)$ 都相同，且 $\chi_u(A_i)\ \neq \chi_u(A_{G(u)})\ i \neq G(u)$。注意，$G$ 是从 $V_{(p)n}$ 到 $V_{(p)s}$ 的函数。此外，由 (31)，对于任意固定的 $u \in V_n^{(p)}$，我们有

$$\chi_u(A_i) = \begin{cases} p^{n-s}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}-s}(p^s-1), \text{ if } i = G(u), \\ p^{n-s}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-s}, \text{ if } i \neq G(u). \end{cases} \tag{32}$$

定义

$$W_i = \{u \in V_n^{(p)} : G(u) = i\}, i \in V_s^{(p)}.$$

那么显然，$W_i, i \in V_{(p)s}$ 两两不相交，且 $\bigcup_{i \in V_s^{(p)}} W_i = V_{(p)n}$。由 (32)，对于任意 $u \in V_{(p)n}$ 和非空集合 $I \subseteq V_s^{(p)}$，我们有

$$\chi_u(D_{F,I}) = \sum_{i \in I} \chi_u(A_i) = p^{n-s}\delta_{\{0\}}(u)|I| + \varepsilon p^{\frac{n}{2}-s}(p^s\delta_{W_I}(u) - |I|), \tag{33}$$

其中 $D_{F,I} = \{x \in V_{(p)n} :\ F(x)\ \in I\}$, $W_I = \bigcup_{i \in I} W_i$。由 (33) 和引理 1，结论成立。

□

当 p 是奇素数时，由定理 1 和定理 2 可得到满足条件 $\mathcal{C}$ 的弯曲划分的一个向量值对偶弯曲函数刻画。

定理 3. 设 p 是奇素数。设 $\Gamma = \{A_i, i \in V_{(s^{\ p}\ \}\ )}$是 $V_{(p)n}$ 的一个划分，其中 n 为偶数，$s \leq \frac{n}{2}$。定义 F：$V_{(p)n}\ \ \to V_{(p)s}$ 如下

$$F(x) = i \textit{ if } x \in A_i.$$

那么，当且仅当 F 是满足条件 A 的向量值对偶弯曲函数时，Γ 是满足条件 $\mathcal{C}$ 的弯曲划分。

IV. 由 向量值对偶弯曲函数构造弯曲划分

I本节中，我们从向量值对偶弯曲函数构造弯曲划分。 s.

下面的定理给出了向量值对偶弯曲函数的一种二次构造，可用于生成更多弯曲划分。

定理 4. 设 n、m、s 为正整数，满足 n 为偶数且 $s \le \frac{n}{2}$、$s \mid m$、$s \ne m$。对于任意 $i \in \mathbb{F}_{p^s}$，设 $F(i;\ x)\colon V_{(p)n} \to \mathbb{F}_{p^s}$ 为一个向量值对偶弯曲函数，满足 $((F(i;\ x))_c)^* = ((F(i;\ x))^*)_c$，并且对任意 $c \in \mathbb{F}_{p^s}^*$ 有 $\varepsilon_{(F(i;x))_c} = \varepsilon$，其中 $(F(i;\ x))^*$ 是 $F(i;\ x)$ 的向量值对偶，且 $\varepsilon \in \{\pm 1\}$ 是独立于 i、c 的常数。设 α、$\beta \in \mathbb{F}_{p^m}$ 在 $\mathbb{F}_{p^s}$ 上线性无关。设 R 是 $\mathbb{F}_{p^m}$ 上的一个置换，满足 $R(0) = 0$，且 $T\colon \mathbb{F}_{p^s} \to \mathbb{F}_{p^s}$ 为任意函数。定义 $H\colon V_n^{(p)} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^s}$ 为

$$H(x, y_1, y_2) = F(Tr_s^m(\alpha R(y_1 y_2^{p^m-2})); x) + Tr_s^m(\beta R(y_1 y_2^{p^m-2})) + T(Tr_s^m(\alpha R(y_1 y_2^{p^m-2}))).$$

那么，H 是满足条件 A 的向量值对偶弯曲函数，$\Gamma = \{A_i, i \in \mathbb{F}_{p^s}\}$ 是满足条件 $\mathcal{C}$ 的弯曲划分，其中 $A_i = \{(x, y_1, y_2) \in V_{(p)n} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}\colon\ H(x, y_1, y_2) = i\}$。

证明。记

$$d(y) = Tr_s^m(\beta R(y_1 y_2^{p^m-2})), e(y) = Tr_s^m((\beta - \alpha) R(y_1 y_2^{p^m-2})), y = (y_1, y_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}.$$

对于任意 $c \in \mathbb{F}_{p^s}^*$ 以及 $(a, b) = (a, b_1, b_2) \in V_{(p)n} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$，有

$$\begin{aligned}
&W_{H_c}(a, b)\\
&= \sum_{x \in V_n^{(p)}} \sum_{y=(y_1,y_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}} \zeta_p^{Tr_1^s(cF(d(y)-e(y);x)) + Tr_1^s(cd(y)) + Tr_1^s(cT(d(y)-e(y)))} \zeta_p^{-\langle a,x\rangle_n - Tr_1^m(b_1 y_1 + b_2 y_2)}\\
&= \sum_{i \in \mathbb{F}_{p^s}} \sum_{y=(y_1,y_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} : d(y)-e(y)=i} \sum_{x \in V_n^{(p)}} \zeta_p^{Tr_1^s(cF(i;x)) + Tr_1^s(cd(y)) + Tr_1^s(cT(i))} \zeta_p^{-\langle a,x\rangle_n - Tr_1^m(b_1 y_1 + b_2 y_2)}\\
&= p^{-s} \sum_{i \in \mathbb{F}_{p^s}} W_{(F(i;x))_c}(a) \zeta_p^{Tr_1^s(cT(i))} \sum_{y=(y_1,y_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}} \zeta_p^{Tr_1^s(cd(y)) - Tr_1^m(b_1 y_1 + b_2 y_2)} \sum_{j \in \mathbb{F}_{p^s}} \zeta_p^{Tr_1^s(cj(i-(d(y)-e(y))))}\\
&= p^{-s} \sum_{i \in \mathbb{F}_{p^s}} W_{(F(i;x))_c}(a) \zeta_p^{Tr_1^s(cT(i))} \sum_{j \in \mathbb{F}_{p^s}} \zeta_p^{Tr_1^s(ijc)} \sum_{y=(y_1,y_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}} \zeta_p^{Tr_1^s(c((1-j)d(y) + je(y))) - Tr_1^m(b_1 y_1 + b_2 y_2)}.
\end{aligned}$$

根据定理 3，[10],对于任意 $j \in \mathbb{F}_{p^s}$, $J(j;\ y) = (1-j)d(y) + je(y)$ 是一个具有 $\varepsilon_{(J(j;y))_c} = 1$ 且满足 $((J(j;\ y))_c)^* = ((1-j)d^*(y) + je^*(y))_c$（对任意 $c \in \mathbb{F}_{p^s}^*$）的部分扩散向量值对偶弯曲函数,

其中 $d^*(y) = Tr_s^m(\beta R(-y_1^{p^m-2}y_2))$, $e^*(y) = Tr_s^m((\beta-\alpha)R(-y_1^{p^m-2}y_2))$. 因此 e,

$$\begin{aligned}
&W_{H_c}(a,b)\\
&= p^{m-s}\sum_{i\in\mathbb{F}_{p^s}} W_{(F(i;x))_c}(a)\zeta_p^{Tr_1^s(cT(i))}\sum_{j\in\mathbb{F}_{p^s}}\zeta_p^{Tr_1^s(ijc)}\zeta_p^{Tr_1^s(c((1-j)d^*(b)+je^*(b)))}\\
&= p^{m-s}\zeta_p^{Tr_1^s(cd^*(b))}\sum_{i\in\mathbb{F}_{p^s}} W_{(F(i;x))_c}(a)\zeta_p^{Tr_1^s(cT(i))}\sum_{j\in\mathbb{F}_{p^s}}\zeta_p^{Tr_1^s(cj(i-(d^*(b)-e^*(b))))}\\
&= p^m\zeta_p^{Tr_1^s(cd^*(b))}W_{(F(d^*(b)-e^*(b);x))_c}(a)\zeta_p^{Tr_1^s(cT(d^*(b)-e^*(b)))}\\
&= \varepsilon p^{\frac{n}{2}+m}\zeta_p^{((F(Tr_s^m(\alpha R(-b_1^{p^m-2}b_2));x))_c)^*(a)+Tr_1^s(cTr_s^m(\beta R(-b_1^{p^m-2}b_2)))+Tr_1^s(cT(Tr_s^m(\alpha R(-b_1^{p^m-2}b_2))))}\\
&= \varepsilon p^{\frac{n}{2}+m}\zeta_p^{((F(Tr_s^m(\alpha R(-b_1^{p^m-2}b_2));x))^*)_c(a)+Tr_1^s(cTr_s^m(\beta R(-b_1^{p^m-2}b_2)))+Tr_1^s(cT(Tr_s^m(\alpha R(-b_1^{p^m-2}b_2))))}.
\end{aligned} \tag{34}$$

注意, $\varepsilon = 1$ 若 $p = 2$, 这是因为所有布尔弯曲函数都是正则的。由 (34) 可知, H 是一个向量值弯曲函数, 具有 $(H_c)^* = G_c$, 且对任意 $c \in \mathbb{F}_{p^s}^*$, $\varepsilon_{H_c} = \varepsilon$ 均成立, 其中

$$G(a,b_1,b_2) = (F(Tr_s^m(\alpha R(-b_1^{p^m-2}b_2));x))^*(a) + Tr_s^m(\beta R(-b_1^{p^m-2}b_2)) + T(Tr_s^m(\alpha R(-b_1^{p^m-2}b_2))$$

由于 H_c 是弱正则弯曲函数, 因此 $G_c = (H_c)^*$ 也是弱正则弯曲函数, 且 G 是向量值弯曲函数。因此, H 是向量值对偶弯曲函数, 具有 $(H_c)^* = (H^*)_c$, 且对任意 $c \in \mathbb{F}_{p^s}^*$, $\varepsilon_{H_c} = \varepsilon$ 均成立, 其中 $H^* = G$, 也就是说, H 满足条件 A。根据定理 1, 由 H 生成的划分 Γ 是一个满足条件 $\mathcal{C}$的弯曲划分。

□

下面给出的弯曲划分的显式构造是命题 3 和定理 4 的直接推论。

定理 5. 设 n, m, s 为正整数, 满足 $s \mid n, s \mid m, s \neq m$, 且 $u_i, i \in \mathbb{F}_{p^s}$ 为整数, 使得对任意 $i \in \mathbb{F}_{p^s}$, 存在某个 $0 \leq j_i \leq s-1$ 使 $u_i \equiv p^{j_i} \ mod\ (p^s-1)$, 并且 $gcd(u_i, p^n-1) = 1$。对于任意 $i \in \mathbb{F}_{p^s}$, 设 d_i 为满足 $u_i d_i \equiv 1 \ mod\ (p^n-1)$ 的整数, 并设 $P_i = (\mathbb{F}_{p^n}, +, \circ_i)$ 为一个（预）半域, 其对偶 $P_i^\star$是右 $\mathbb{F}_{p^s}$-线性的。对于任意 $i \in \mathbb{F}_{p^s}$, 令 $F(i; x_1, x_2) : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^s}$ 为一个由命题 3 构造的任意向量值对偶弯曲函数, 其中 $u = u_i, d = d_i$, $P = P_i$。设 $\alpha, \beta \in \mathbb{F}_{p^m}$ 在 $\mathbb{F}_{p^s}$上线性无关, R是 $\mathbb{F}_{p^m}$ 上的一个置换, 满足 $R(0) = 0$, 且 $T : \mathbb{F}_{p^s} \to \mathbb{F}_{p^s}$ 为任意函数。定义$H : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^s}$ 为

$$H(x_1,x_2,y_1,y_2) = F(Tr_s^m(\alpha R(y_1y_2^{p^m-2})); x_1, x_2) + Tr_s^m(\beta R(y_1y_2^{p^m-2})) + T(Tr_s^m(\alpha R(y_1y_2^{p^m-2}))).$$

Then

$$\Gamma = \{A_i, i \in \mathbb{F}_{p^s}\}$$

是满足条件 $\mathcal{C}$的弯曲划分, 其中

$$A_i = \{(x_1,x_2,y_1,y_2) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} : H(x_1,x_2,y_1,y_2) = i\}.$$

注 3。采用与定理 4 相同的记号。注意，在定理 4 中，将由定理 5 构造的向量对偶弯曲函数 H 作为构造块（即作为 $F(i;\ x)$），我们可以得到更明确的向量对偶弯曲函数，并通过定理 4 生成更多弯曲划分。

我们利用定理 5 给出一个例子。

例 2. 设 $p=3, s=4, n=m=8$。设 α 是 $\mathbb{F}_{3^8}$ 的本原元，且 $\beta=1$, R 是恒等映射和 $T=0$。对于任意 $i\in\mathbb{F}_{3^4}$，令

$$F(i;x_1,x_2)=\begin{cases} Tr_4^8(x_1^{-89}x_2),\ \textit{if}\ i\in\mathbb{F}_{3^4}^*, \\ Tr_4^8(x_1x_2^{-83}),\ \textit{if}\ i=0. \end{cases}$$

Then

$$H(x_1,x_2,y_2,y_2)=(Tr_4^8(\alpha y_1y_2^{6559}))^{80}(Tr_4^8(x_1^{-89}x_2-x_1x_2^{-83}))+Tr_4^8(x_1x_2^{-83}+y_1y_2^{6559}$$

并且 $\Gamma=\{D_{H,i}, i\in\mathbb{F}_{3^4}\}$ 是满足条件 $\mathcal{C}$的弯曲划分，其中 $D_{H,\ i}=\{(x_1,x_2,y_1,y_2)\ \in(\mathbb{F}_{3^8})^4:\ H(x_1,x_2,y_1,y_2)\ =i\}$。

五、弯曲划分与部分差集之间的关系

本节以向量值对偶弯曲函数作为弯曲划分与部分差集之间的纽带，给出由弯曲划分构造部分差集的一个充分条件。当 p 是奇素数时，我们用部分差集刻画满足条件 $\mathcal{C}$的弯曲划分。

定义 4. 设 $(G,+)$ 是一个阶为 v 的有限阿贝尔群，且 D 是 G 的一个含有 k 个元素的子集。如果对于 d_1 和 d_2 属于 D 且满足 $d_1\neq d_2$，表达式 d_1-d_2 恰好将 D 中的每个非零元素表示 λ 次，并将 $G\setminus D$ 中的每个非零元素表示 μ 次，则称 D 为 G 的一个 (v,k,λ,μ) 部分差集。当 $\lambda=\mu$ 时，称 D 为一个 (v,k,λ) 差集。

注意，若 D 是 G 的一个部分差集，且具有 $-D=D$，那么 $D\cup\{0\}$、$D\setminus\{0\}$和 $G\setminus D$也都是部分差集（见 [16]）。有一种重要工具可以用特征标来刻画部分差集。

引理 3（ [16]）。设 G 是一个阶为 v的阿贝尔群。假设 D 是 G 的一个子集，含有k个元素，并满足 $-D = D$和 $0 \notin D$。那么， D是一个（v， k， λ， μ）部分差集，当且仅当对于 G的每个非主特征标 χ ，

$$\chi(D) = \frac{\beta \pm \sqrt{\Delta}}{2},$$

其中 $\chi(D) = \sum_{x \in D} \chi(x)$, $\beta = \lambda - \mu, \gamma = k - \mu, \Delta = \beta^2 + 4\gamma$。

当 p 是奇素数或 $s \geq 2$时，我们给出满足条件 A 的向量值对偶弯函数的值分布。

命题 4. 设 F: $V_n^{(p)} \to V_{(p)s}$ 是满足条件 A 的向量值对偶弯函数，其中 p 为奇数或 $s \geq 2$。则

$$|D_{F,F(0)}| = p^{n-s} + \varepsilon p^{\frac{n}{2}-s}(p^s - 1), \ |D_{F,i}| = p^{n-s} - \varepsilon p^{\frac{n}{2}-s} \text{ if } i \neq F(0).$$

证明。注意，若 f 是弱正则 p 元弯曲函数，则对任意 $a \in \mathbb{F}_p$， $f - a$ 是一个弱正则弯曲函数，且 $(f - a)^* = f^* - a$ 和 $\varepsilon_{f-a} = \varepsilon_f$。由于 F 是一个向量值对偶弯曲函数，满足 $(F_c)^* = (F^*)_c$， $c \in V_{(s^p \setminus \{0\})}$，因此 $F(x) - F(0)$ 是一个向量值弯曲函数，并且对任意 $c \in V_s^{(p)} \setminus \{0\}$,

$$((F - F(0))_c)^* = (F_c)^* - \langle c, F(0) \rangle_s = (F^*)_c - \langle c, F(0) \rangle_s = (F^* - F(0))_c,$$

这意味着 $F(x) - F(0)$ 是一个向量值对偶弯曲函数，且 $((F - F(0))_c)^* = (F^* - F(0))_c$，并且对任意 $c \in V_{(s^p \setminus \{0\})}$，都有 $\varepsilon_{(F-F(0))_c} = \varepsilon$。根据定理 1 的证明，对任意 $a \in \mathbb{F}_p^*$， $F(ax) = F(x)$，因此 $F(x) = F(-x)$。根据 [22] 的推论1（注意，尽管 [22] 的推论1仅考虑 p 为奇数的情况，但 [22] 的推论 1 对 $p = 2$、 $s \geq 2$ 也成立），我们有

$$|D_{F-F(0),0}| = p^{n-s} + \varepsilon p^{\frac{n}{2}-s}(p^s - 1), \ |D_{F-F(0),i}| = p^{n-s} - \varepsilon p^{\frac{n}{2}-s} \text{ if } i \neq 0,$$

也就是说,

$$|D_{F,F(0)}| = p^{n-s} + \varepsilon p^{\frac{n}{2}-s}(p^s - 1), \ |D_{F,i}| = p^{n-s} - \varepsilon p^{\frac{n}{2}-s} \text{ if } i \neq F(0).$$

□

接下来，我们将用部分差集刻画满足条件 A 的向量值对偶弯曲函数。

定理 6. 设 n 为偶正整数， s 为满足 $s \le \frac{n}{2}$ 的正整数，并且 $F: V_n^{(p)} \to V_s^{(p)}$。以下两个命题等价。

(1) F 是满足条件 A 的向量值对偶弯曲函数。

(2) 当 $p=2, s=1$ 时，由 $supp(F)=\{x \in V_{(2)n}: F(x)=1\}$ 定义的 F 的支撑集 $supp(F)$ 是一个 $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$ 差集；并且当 p 为奇数或 $s \ge 2$ 时，对于任意非空集合 $I \subseteq V_{(p)s}$， $D_{F,I} \backslash \{0\}$ 是一个 (p^n, k, λ, μ) 部分差集，其中 $-D_{F,I} = D_{F,I}$；若 $F(0) \in I$，则

$$\begin{aligned} k &= p^{n-s}|I| + \varepsilon p^{\frac{n}{2}-s}(p^s - |I|) - 1, \\ \lambda &= p^{n-2s}|I|^2 + \varepsilon p^{\frac{n}{2}-s}(p^s - |I|) - 2, \\ \mu &= p^{n-2s}|I|^2 + \varepsilon p^{\frac{n}{2}-s}|I|, \end{aligned} \tag{35}$$

若 $F(0) \notin I$，则

$$\begin{aligned} k &= p^{n-s}|I| - \varepsilon p^{\frac{n}{2}-s}|I|, \\ \lambda &= p^{n-2s}|I|^2 + \varepsilon p^{\frac{n}{2}-s}(p^s - 3|I|), \\ \mu &= p^{n-2s}|I|^2 - \varepsilon p^{\frac{n}{2}-s}|I|, \end{aligned} \tag{36}$$

其中 $D_{F,I} = \{x \in V_{(p)n}: F(x) \in I\}$，且 $\varepsilon \in \{\pm 1\}$ 是一个常数（若 $p=2$，则为 $\varepsilon = 1$）。

证明。容易看出，布尔函数 F 是满足条件 A 的向量值对偶弯曲函数，当且仅当 F 是弯曲的；也就是说，对于任意布尔弯曲函数，条件 A 都是平凡的。根据众所周知的结论，布尔函数 $F: V_n^{(2)} \to \mathbb{F}_2$ 是弯曲的，当且仅当其支撑集 $supp(F)=\{x \in V_{(2)n}: F(x)=1\}$ 是一个 $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$ 差集（见 [11]），显然可得，对于 $p=2, s=1$，结论成立。下文证明，当 p 为奇数或 $s \ge 2$ 时，结论成立。

(1) $\Rightarrow$ (2)：根据定理 1 的证明， $F(-x)=F(x)$，即 $-D_{F,I} = D_{F,I}$。对于任意 $u \in V_n^{(p)} \backslash \{0\}$，采用与 [22], 中定理 2 的证明相同的论证

$$\chi_u(D_{F,I}) = \begin{cases} \varepsilon p^{\frac{n}{2}} - \varepsilon p^{\frac{n}{2}-s}|I|, & \text{if } F^*(-u) \in I, \\ -\varepsilon p^{\frac{n}{2}-s}|I|, & \text{if } F^*(-u) \notin I. \end{cases}$$

其中 $\varepsilon = 1$ 如果 $p=2$ 因为所有布尔弯曲函数都是正则的。

若 $F(0) \in I$，则 $|D_{F,I} \backslash \{0\}| = |D_{F,I}| - 1$ 且 $\chi_u(D_{F,I} \backslash \{0\}) = \chi_u(D_{F,I}) - 1$。根据命题 4, $|D_{F,I} \backslash \{0\}| = (|I|-1)(p^{n-s} - \varepsilon p^{\frac{n}{2}-s}) + (p^{n-s} + \varepsilon p^{\frac{n}{2}-s}(p^s - 1) - 1) = p^{n-s}|I| + \varepsilon p^{\frac{n}{2}-s}(p^s - |I|) - 1$。根据引理 3， $D_{F,I} \backslash \{0\}$ 是一个 (p^n, k, λ, μ) 部分差集，其中 k、 λ、 μ 由 (35) 给出。

若 $F(0) \notin I$，则 $|D_{F,\ I}\backslash\{0\}| = |D_{F,\ I}|$ 且 $\chi_u(D_{F,\ I}\backslash\{0\}) = \chi_u(D_{F,\ I})$。根据命题 4，$|D_{F,\ I}\backslash\{0\}| = |I|(p^{n-s} - \varepsilon p^{\frac{n}{2}-s})$。根据引理 3，$D_{F,\ I}\backslash\{0\}$ 是一个 (p^n, k, λ, μ) 部分差集，其中 k、λ、μ 由 (36) 给出。

(2) $\Rightarrow$ (1)：根据引理 3，对于任意 $u \in V_{(p)n}$ 以及非空集合 $I \subseteq V_s^{(p)}$，我们有

$$\chi_u(D_{F,I}) = p^{n-s}\delta_{\{0\}}(u)|I| + \varepsilon p^{\frac{n}{2}} - \varepsilon p^{\frac{n}{2}-s}|I| \text{ or } \chi_u(D_{F,I}) = p^{n-s}\delta_{\{0\}}(u)|I| - \varepsilon p^{\frac{n}{2}-s}|I|. \quad (37)$$

对于任意 $i \in V_{(p)s}$，定义 $W_i = \{u \in V_{(p)n}: \chi_u(D_{F,i}) = p^{n-s}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}} - \varepsilon p^{\frac{n}{2}-s}\}$，其中 $D_{F,i} = \{x \in V_{(p)n}: F(x) = i\}$。我们断言，对于任意 $i \neq i'$，都有 $W_i \bigcap W_{i'} = \emptyset$，且 $\bigcup_{i \in V_s^{(p)}} W_i = V_{(p)n}$。事实上，若存在 $i \neq i'$ 使得 $W_i \bigcap W_{i'} \neq \emptyset$，即存在 $u \in V_{(p)n}$ 使得 $\chi_u(D_{F,i}) = \chi_u(D_{F,i'}) = p^{n-s}\delta_{\{0\}}(u) + \varepsilon p^{\frac{n}{2}} - \varepsilon p^{\frac{n}{2}-s}$，则 $\chi_u(D_{F,i} \bigcup D_{F,i'}) = 2p^{n-s}\delta_{\{0\}}(u) + 2\varepsilon p^{\frac{n}{2}} - 2\varepsilon p^{\frac{n}{2}-s}$，这与 (37) 矛盾。因此，对任意 $i \neq i'$，都有 $W_i \bigcap W_{i'} = \emptyset$。若存在 $u \in V_{(p)n}$ 使得对于任意 $i \in V_{(p)s}$，都有 $u \notin W_i$，即对于任意 $i \in V_{(p)s}$，都有 $\chi_u(D_{F,i}) = p^{n-s}\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}-s}$，则 $\chi_u(V_{(p)n}) = \sum_{i \in V_s^{(p)}} \chi_u(D_{F,i}) = p^n\delta_{\{0\}}(u) - \varepsilon p^{\frac{n}{2}}$，这与 $\chi_u(V_{(p)n}) = \sum_{x \in V_n^{(p)}} \zeta_p^{\langle u, x\rangle_n} = p^n\delta_{\{0\}}(u)$ 矛盾。因此，$\bigcup_{i \in V_s^{(p)}} W_i = V_{(p)n}$。根据上述分析，我们有

$$\chi_u(D_{F,I}) = p^{n-s}\delta_{\{0\}}(u)|I| + \varepsilon p^{\frac{n}{2}-s}(p^s\delta_{W_I}(u) - |I|), \quad (38)$$

其中 $W_I = \sum_{i \in I} W_i$。由 (38) 和引理 1，F 是满足条件 A 的向量值对偶弯曲函数。

□

下述定理给出了从弯曲划分构造部分差集的一个充分条件。

定理 7. 设 n 为偶正整数，s 为满足 $s \leq \frac{n}{2}$ 的正整数。假设 $\Gamma = \{A_i, i \in V_{(s}{}^{p}\}_{)}$ 是 $V_{(p)n}$ 的一个弯曲划分，其中函数 $F: V_{(p)n} \to V_{(p)s}$ 定义为

$$F(x) = i \text{ if } x \in A_i$$

是满足条件 A 的向量值对偶弯曲函数。因此，当 $p = 2$、$s = 1$、A_0 和 A_1 分别是 $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$ 差集和 $(2^n, 2^{n-1} \mp 2^{\frac{n}{2}-1}, 2^{n-2} \mp 2^{\frac{n}{2}-1})$ 差集，且 p 为奇数或 $s \geq 2$ 时，对于任意非空集合 $I \subseteq V_{(p)s}$，$A_I\backslash\{0\} = \bigcup_{i \in I} A_i\backslash\{0\}$ 是一个 (p^n, k, λ, μ) 部分差集，其中，当 $0 \in A_I$ 时，(k, λ, μ) 由式 (35) 给出；当 $0 \notin A_I$ 时，(k, λ, μ) 由式 (36) 给出。

证明。注意，若 D 是有限阿贝尔群 G上的一个 (v,k,λ) 差集，则 $G\backslash D$ 是 G 上的一个 $(v,v-k,v-2k+\lambda)$ 差集（例如参见 [12]）。结论由定理 6 得出。

□

注 4. 根据命题 3，弯曲划分 Γ_1（分别地，Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2）满足定理 7 中的条件。根据定理 7，从 Γ_1（分别地，Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2）中取集合的任意并集均构成一个部分差集。因此，*[1]* 的推论 15 中关于从 Γ_1（分别地，Γ_2、$\Gamma_1^\bullet$、$\Gamma_2^\bullet$、Θ_1、Θ_2）构造部分差集的结果（其中包括 *[2]* 的定理 2 中关于从有限域中的 Γ_1（分别地，Γ_2）构造部分差集的结果）也可以由我们的结果加以说明。

由于定理 5 中构造的弯曲划分满足定理 7 中的条件，我们由定理 7 得到以下推论。

推论 2. 设 $\Gamma=\{A_i,i\in\mathbb{F}_{p^s}\}$ 是由定理 5 构造的弯曲划分。那么，当 $p=2$、$s=1$、A_0 和 A_1 分别为（2^n、$2^{n-1}\pm2^{\frac{n}{2}-1}$、$2^{n-2}\pm2^{\frac{n}{2}-1}$）差集和（$2^n$、$2^{n-1}\mp2^{\frac{n}{2}-1}$、$2^{n-2}\mp2^{\frac{n}{2}-1}$）差集，且当 p 为奇数或 $s\geq2$ 时，对于任意非空集合 $I\subseteq\mathbb{F}_{p^s}$，$A_I\backslash\{0\}=\bigcup_{i\in I}A_i\backslash\{0\}$ 是一个（p^n、k、λ、μ）部分差集，其中（k、λ、μ）在 $0\in A_I$ 时由（35）给出，而（k、λ、μ）在 $0\notin A_I$ 时由（36）给出。

由推论 2 可得一个例子。

例 3。设 $\Gamma=\{D_{H,i},i\in\mathbb{F}_{3^4}\}$ 是例 2 中构造的弯曲划分。根据推论 2，$D_{H,\,i}$ 对于任意 $i\in\mathbb{F}_{3^4}^*$，$D_{H,\,0}\backslash\{0\}$ 都是一个(1853020188851841，22876834970240，282472051759，282430067922)部分差集，$(D_{H,\,0}\bigcup D_{H,\,1})\backslash\{0\}$ 是一个(1853020188851841，45753626893760，1129760129761，1129719208806)部分差集。

当 p 为奇素数时，由定理 3 和定理 6，我们立即得到满足条件 $\mathcal{C}$ 的 $V_n^{(p)}$弯曲划分的如下刻画。

定理 8. 设 p 为奇素数。设 $\Gamma=\{A_i,i\in V_{(s^p)}\}$是 $V_{(p)n}$ 的一个划分，其中 n 为偶数且 $s\leq\frac{n}{2}$。那么以下两个陈述等价。

(1) Γ 是满足条件 $\mathcal{C}$的弯曲划分。

（2）对于任意非空集合 $I\subseteq V_{(p)s}$，$A_I\backslash\{0\}=\bigcup_{i\in I}A_i\backslash\{0\}$ 是一个参数为（p^n，k，λ，μ）的部分差

集，其中 $-A_I = A_I$；若 $0 \in A_I$，则（k，λ，μ）由（35）给出；若 $0 \notin A_I$，则（k，λ，μ）由（36）给出。

VI. 结论

本文研究了弯曲划分与向量值对偶弯曲函数之间的关系（定理1、2、3），并给出了满足条件 $\mathcal{C}$的弯曲划分的一些新构造（推论1、定理4和5）。我们说明，对于任意三元弱正则弯曲函数f：$V_{(3)n} \to \mathbb{F}_3$（$n$偶）满足 f（x）、$= f$（$-x$）和 $\varepsilon_f = -1$时，由 f生成的弯曲划分并非源自正规弯曲划分（见例1），从而回答了 [4]提出的一个未解决问题。我们以向量值对偶弯曲函数作为弯曲划分与部分差集之间的纽带，给出了从弯曲划分构造部分差集的一个充分条件（定理 7）。当 p 为奇素数时，我们利用部分差集刻画了满足条件 $\mathcal{C}$ 的弯曲划分（定理 8）。

参考文献

[1]N. Anbar、T. Kalaycı，《由弯曲划分构造的非形关联方案》，可获取：https://www.researchgate.net/publication/366593699 Amorphic association schemes from bent partitions[2] N. Anbar、T. Kalaycı 和 W. Meidl，《弯曲划分与部分差集》，IEEE 信息论汇刊，第 68 卷，第 10 期，第 6894-6903 页，2022年[3] N. Anbar、T. Kalaycı 和 W. Meidl，《广义半域铺展》，《设计、码与密码学》，在线发表。DOI：10.1007/s10623- 022-01115-2[4] N. Anbar 和 W. Meidl，《弯曲划分》，《设计、码与密码学》，第 90 卷，第 4 期，第 1081-1101 页，2022年。[5] C. Carlet 和 S. Mesnager，《弯曲函数研究的四十年》，《设计、码与密码学》，第 78 卷，第 1 期，第 5-50 页，2016年。[6] A. Ç.es.melio˘glu，W. Meidl，《一种由平台函数构造弯曲函数的方法》，《设计、码与密码学》，第 66 卷，第 231-242 页，2013年。[7] A. Ç.es.melio˘glu，W. Meidl，《弯曲函数与向量值弯曲函数、部分差集和强正则图》，《高级数学通讯》，第 12 卷，第 691-705 页，2018年。[8] A. Ç.es.melio˘glu，W. Meidl，I. Pirsic，《向量值弯曲函数与部分差集》，《设计、码与密码学》，第 89 卷，第 10 期，第 2313-2330 页，2021年。[9] A. Ç.es.melio˘glu，W. Meidl 和 A. Pott，《关于（非）弱正则弯曲函数的对偶及自对偶弯曲函数》，《高级数学通讯》，第 7 卷，第 4 期，第 425-440 页，2013年。[10] A. Ç.es.melio˘glu，W. Meidl 和 A. Pott，《向量值弯曲函数及其对偶》，《线性代数及其应用》，第 548 卷，第 305-320 页，2018年。[11] J. F. Dillon，《初等 Hadamard 差集》，博士论文，马里兰大学，1974年。[12] C. Ding，《由差集构造的码》，世界科技出版公司，新加坡，2015年。[13] J. Y. Hyun、J. Lee 和 Y. Lee，《由 p 元弯曲函数构造的拉马努金图与扩展图族》，《设计、码与密码学》，第 88 卷，第 2 期，第 453-470 页，2020年。

[14] P. Lisonˇek 和 H. Y. Lu，《部分扩散上的弯曲函数》，《设计、码与密码学》，第 73 卷，第 1 期，第 209-216 页，2014年。[15] P. V. Kumar、R. A. Scholtz 和 L. R. Welch，《广义 Bent 函数及其性质》，《组合理论杂志》A辑，第 40 卷，第 1 期，第 90-107 页，1985年。[16] S. L. Ma，《部分差集综述》，《设计、码与密码学》，第 4 卷，第 4 期，第 221-261 页，1994年。[17] W. Meidl，《 p 元及广义弯曲函数综述》，《密码学通讯》，第 14 卷，第 4 期，第 737-782 页，2022年。[18] W. Meidl 和 I. Pirsic，《由类扩张划分构造的弯曲函数与 $\mathbb{Z}_{2^k}$ 弯曲函数》，《设计、码与密码学》，第 89 卷，第 1 期，第 75-89 页，2021年。[19] S. Mesnager，《弯曲函数：基础与结果》，施普林格，瑞士，2016年。[20] K. Nyberg，《弯曲函数与差集的构造》，载于：密码学进展——EUROCRYPT' 90，《计算机科学讲义》473，施普林格，柏林，第 151-160 页，1991年。[21] O. S. Rothaus，《关于“弯曲”函数》，《组合理论杂志》A辑，第 20 卷，第 3 期，第 300-305 页，1976年。[22] J. Wang 和 F.-W.Fu，《向量值对偶弯曲函数与部分差集的新结果》，《设计、码与密码学》，在线发表。DOI：10.1007/s10623-022-01103-6