arXiv:2303.01118v1 [math.CO] 2 Mar 2023

关于$\mathcal{PS}_{ap}^{\#}$类向量值超弯函数的构造与枚举

Jingkun Zhou[a,*]、Chunming Tang[b]、Fengrong Zhang[c,d]

[a]浙江大学数学科学学院，中国浙江杭州 310027[b]西南交通大学信息科学与技术学院，中国成都 610031[c]西安电子科技大学综合业务网国家重点实验室，中国西安 710071[d]中国矿业大学计算机科学与技术学院，中国江苏徐州 221116

摘要

本文旨在给出 $\mathcal{PS}_{ap}^{\#}$ 类向量值超弯函数的显式构造。据我们所知，目前已知的显式构造仅适用于非常特殊的情形。为此，我们给出了这族向量值函数为超弯函数的充分必要条件，并用群环来表达这些条件。基于这一刻画，我们通过平衡函数提出了 $\mathcal{PS}_{ap}^{\#}$ 类向量值超弯函数的显式构造。此外，我们还确定了 $\mathcal{PS}_{ap}^{\#}$ 类向量值超弯函数的准确数量。本文结果改进了此前的一些工作。此外，我们解决了 Muratovi´c-Ribi´c、Pasalic 和 Ribi´c 在 [《IEEE 信息论汇刊》60（2014），第 4408-4413] 页中提出的向量值超弯函数计数问题。

关键词：布尔函数，弯函数，超弯函数，向量函数，最大非线性度。

1. 引言

超弯函数最初由 A.M. Youssef 和 G. Gong [8] 于 2001 年提出，是一种布尔函数 $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$，其扩展沃尔什-哈达玛变换

$$\widehat{\chi}_f(\lambda,t)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(\lambda x^t)}$$

仅取 $\pm 2^{\frac{n}{2}}$ 中的值，其中 $\lambda\in\mathbb{F}_{2^n}$ 和 t 是与 2^n-1 互素的整数。超弯函数被定义为弯曲函数的一个特殊类别，旨在避免通过双射单项式函数进行逼近。[8] 中提出的超弯函数类属于 Dillon [10] 引入的 $\mathcal{PS}_{ap}$ 类弯曲函数，也是迄今为止已知的唯一一个无限超弯函数类。

*通讯作者电子邮箱：jingkunz@zju.edu.cn（Jingkun Zhou）、tangchunmingmath@163.com（Chunming Tang）、zhfl203@163.com（Fengrong Zhang）

布尔函数的超弯性质可以扩展到向量值函数。对于向量值函数 F： $\mathbb{F}_{2^n} \to \mathbb{F}_2^k$，如果 F 的分量函数的所有非零组合都是超弯函数，则称 F 是超弯的。也就是说，一个向量值函数

$$F(x) = (f_1(x), \ldots, f_k(x))$$

如果对任意选择的$a_i \in \mathbb{F}_2$， $a_1 f_1(x) + \cdots + a_k f_k(x)$都是超弯函数，则称其为超弯的，其中并非所有 a_i都为零。

迹函数是研究弯曲函数的有用工具。Carlet 和 Gaborit[9] 证明， $\mathcal{PS}_{ap}^{\#}$ 类的超弯曲布尔函数具有如下形式

$$f(x) = \mathrm{Tr}_1^{2m}\left(\sum_{i=1}^{2^m} a_i x^{i(2^m-1)} + a_0\right),$$

其中 $a_i \in \mathbb{F}_{2^n}$。 Charpin 和 Gong [16] 给出了 $\mathbb{F}_{2^{2m}}$ 上形如$\sum_{r\in R}\mathrm{Tr}_1^{2m}(a_r x^{r(2^m-1)})$的超弯曲布尔函数的刻画，该刻画基于 Dickson 多项式和 Kloosterman 和，其中 $a_r \in \mathbb{F}_{2^m}$。关于具有 Dillon 型指数的超弯曲布尔函数的最新进展，参见论文 [17],[11] 。Carlet 等人通过采用 M¨obius 变换，刻画了系数取遍整个 $\mathbb{F}_{2^{2m}}$ [1]的 Dillon 型指数函数的超弯性质。

在 [6, 15] 中，给出了具有 Dillon 类指数的向量值弯曲函数的一些必要条件。在 [7], 中，作者研究了向量情形，并得到了函数 $F(x) = \mathrm{Tr}_m^{2m}(\sum_{i=1}^{2^m} a_i x^{i(2^m-1)})$为向量值弯曲函数的充分必要条件。他们还证明，这种形式的每个向量值弯曲函数都是向量值超弯函数。此外，作者精确计算了形式为 $F(x) = \mathrm{Tr}_m^{2m}(\sum_{i=1}^{2^m} a_i x^{i(2^m-1)} + c)$的向量值超弯函数的数量。他们还将一般情形 $k|n$ 下向量值超弯函数的基数问题留作一个开放问题。

本文研究一类向量值函数F的超弯性质：对于 F 的分量函数的每个非零线性组合 f, $f(\gamma^{2^m+1}x) = f(x)$均成立，且 $F(0) = 0$。在此条件下，向量值超弯函数的概念是 $\mathcal{PS}_{ap}^{\#}$ 类超弯曲布尔函数的推广。我们得到了这类向量值函数具有超弯性质的充分必要条件。本文给出了典型形式的向量值超弯函数的数值结果，从而解决了关于计数 [7],中向量值超弯函数的开放问题，并构造了任意维数的向量值超弯函数。

本文其余部分安排如下。第2节介绍群环和向量值超弯函数的一些预备知识。第3节为一类向量函数是超弯函数建立充分必要条件。计数了一种典型形式的向量值超弯函数的数量，并利用平衡函数给出了向量值超弯函数的一种显式构造。最后，第4节对全文进行总结。

2. 预备知识

2.1. 群环与傅里叶分析

本节介绍群环的一些基本结果。

定义 2.1. 设 G 是一个阿贝尔群。群环 $\mathbb{Q}[G]$ 定义为由 G 中元素构成、系数取自 $\mathbb{Q}$ 的形式和所组成的集合。$\mathbb{Q}[G]$ 中的加法、数乘和乘法分别定义如下:

$$\sum_{g\in G} a_g \cdot g + \sum_{g\in G} b_g \cdot g = \sum_{g\in G} (a_g + b_g) \cdot g,$$
$$a \sum_{g\in G} a_g \cdot g = \sum_{g\in G} (a a_g) \cdot g,$$

and

$$\left(\sum_{g\in G} a_g \cdot g\right) \cdot \left(\sum_{g\in G} b_g \cdot g\right) = \sum_{g\in G} \left(\sum_{h\in G} a_h b_{gh^{-1}}\right) \cdot g.$$

通常会约定将 S 同时视为 G 的子集以及 $\mathbb{Q}[G]$ 中相应的元素 $\sum_{s\in S} s$。阿贝尔群 G 的一个特征 χ 是从 G 到复数域 $\mathbb{C}$ 的乘法群的群同态。将 G 的所有特征的集合记为 G。令 $A = \sum_{g\in G} a_g \cdot g \in \mathbb{Q}[G]$。$\chi$ 在 A 上的特征和为 $\chi(A) = \sum_{g\in G} a_g \chi(g)$。下面的反演公式表明，如果对于每个特征，两个元素在其上的特征和取值都相等，则 $\mathbb{Q}[G]$ 中的这两个元素相同。

命题 2.1。设 $A = \sum_{g\in G} a_g g$ 是有限阿贝尔群 G 的群环 $\mathbb{Q}[G]$ 中的一个元素，则 A 的系数 a_g 可由下式显式计算:

$$a_g = \frac{1}{|G|} \sum_{\chi\in \hat{G}} \chi(A)\chi(g^{-1}),$$

其中，G 表示 G 的特征群。特别地，如果 A、$B \in \mathbb{Q}[G]$ 满足对于所有特征 $\chi \in G$ 均有 $\chi(A) = \hat{\chi}(B)$，则 $A = B$。

由于域 $\mathbb{F}_{2^k}$ 与 $\mathbb{F}_2^k$ 作为 $\mathbb{F}_2$ 上的向量空间是相同的，因此描述初等阿贝尔群的所有特征集合主要有两种方法：一种使用点积，另一种使用迹函数。

命题 2.2. 设 k 为正整数。

(1) 对每个 $a = (a_1, \ldots, a_k) \in \mathbb{F}_2^k$，定义函数 $\chi_a\colon \mathbb{F}_2^k \to \{\pm 1\}$，使得

$$\chi_a(x) = (-1)^{\sum_{i=1} a_i x_i} = (-1)^{\langle a,x\rangle}$$

对每个 $x = (x_1, \ldots, x_k) \in \mathbb{F}_2^k$，其中 $\langle a, x\rangle$ 是通常的点积。于是

$$\widehat{\mathbb{F}_2^k} = \{\chi_a : a \in \mathbb{F}_2^k\}.$$

(2) 对每个 $a \in \mathbb{F}_{2^k}$，定义函数 $\rho_a\colon \mathbb{F}_{2^k} \to \{\pm 1\}$，使得

$$\rho_a(x) = (-1)^{\mathrm{Tr}_1^k(ax)}$$

对每个 $x \in \mathbb{F}_{2^k}$ 均如此。于是集合 $\{\rho_a\colon\ a \in \mathbb{F}_{2^k}\}$ 包含 G 的所有特征，其中 G 是 $\mathbb{F}_{2^k}$ 的加法群。

2.2. 超弯函数

我们建立两个有用的命题，将在第3节中使用。设 $n = 2m$ 是一个偶数正整数。我们可以将 $\mathbb{F}_{2^n}^*$ 直接划分如下:

$$\mathbb{F}_{2^n}^* = \bigcup_{u \in U} u\mathbb{F}_{2^m}^*,$$

其中， U 是 $\mathbb{F}_{2^n}^*$ 中阶为 $2^m + 1$的循环子群。

以下命题是众所周知的，在 [18]中可以找到其略有不同的形式。为完整起见，我们在此给出其证明。

命题 2.3. 设 γ 是 $\mathbb{F}_{2^n}$的本原元。设 f 是定义在 $\mathbb{F}_{2^n}$ 上的布尔函数，使得

$$f(\gamma^{2^m+1}x) = f(x) \tag{1}$$

对于每个 $x \in \mathbb{F}_{2^n}$ 和 $f(0) = 0$。那么，当且仅当 f 是超弯函数时，

$$\sum_{u \in U} (-1)^{f(u)} = 1,$$

在这种情况下， f 被称为属于 $\mathcal{PS}_{ap}^{\#}$ 类。

证明。记 $q = 2^m$。由于 γ^{q+1} 是 $\mathbb{F}_q$的本原元，由 (1) 可知，对每个$u \in U$，函数 f 在 $u\mathbb{F}_q^*$ 上的限制是常数。

设 i 是一个与 $q^2 - 1$ 和 $a \in \mathbb{F}_{q^2}^*$互素的整数。则有

$$\sum_{x \in \mathbb{F}_{q^2}^*} (-1)^{f(x)+\mathrm{Tr}_1^n(ax^i)} = \sum_{u \in U} (-1)^{f(u)} \sum_{x \in u\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^n(ax^i)} = \sum_{u \in U} (-1)^{f(u)} \sum_{y \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^n(au^iy^i)}.$$

对于 $a \in \mathbb{F}_{q^2}^*$、 $u \in U$和 $y \in \mathbb{F}_q^*$，有

$$\mathrm{Tr}_1^n(au^iy^i) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(au^iy^i)) = \mathrm{Tr}_1^m(au^iy^i + a^qu^{qi}y^{qi}),$$

根据迹的传递性。由于 $u^q = u^{-1}$ 和 $y^q = y$，有

$$\mathrm{Tr}_1^n(au^iy^i) = \mathrm{Tr}_1^m(au^iy^i + a^qu^{qi}y^{qi}) = \mathrm{Tr}_1^m((au^i + a^qu^{-i})y^i).$$

于是， $au^i + a^qu^{-i} = 0$ 当且仅当 $u = a^{t(q-1)}$，其中 t 是 $2i$模 $q^2 - 1$的乘法逆元。

令 $u_0 = a^{t(q-1)}$。若 $u = u_0$，则对任意 $y \in \mathbb{F}_q^*$，有 $\mathrm{Tr}_1^n(au^iy^i) = 0$，因此

$$\sum_{y \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^n(au^iy^i)} = q - 1.$$

若 $u \in U \setminus \{u_0\}$，则有 $au^i + a^qu^{-i} \neq 0$。那么集合

$$\{y \in \mathbb{F}_q^* : \mathrm{Tr}_1^m((au^i + a^qu^{-i})y^i) = 0\}$$

的大小为 $q/2-1$，且集合

$$\{y \in \mathbb{F}_q^* : \mathrm{Tr}_1^m((au^i + a^q u^{-i})y^i) = 1\}$$

其大小为 $q/2$，因为 $y \mapsto y^i$ 是一个双射。因此我们得到

$$\sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^n(au^i y^i)} = 1 \times (q/2-1) + (-1) \times q/2 = -1$$

对每个 $u \in U \setminus \{u_0\}$ 都成立。因此

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{q^2}^*} (-1)^{f(x)+\mathrm{Tr}_1^n(ax^i)} &= \sum_{u\in U} (-1)^{f(u)} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^n(au^i y^i)} \\
&= (q-1)\cdot(-1)^{f(u_0)} - \sum_{u\in U\setminus\{u_0\}} (-1)^{f(u)} \\
&= q\cdot(-1)^{f(u_0)} - \sum_{u\in U} (-1)^{f(u)} \\
&= \pm q - \sum_{u\in U} (-1)^{f(u)}.
\end{aligned}$$

因此，我们有

$$\sum_{x\in\mathbb{F}_{q^2}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax^i)} = \pm q + 1 - \sum_{u\in U} (-1)^{f(u)}.$$

然后根据超弯函数的定义，我们得出：f 是超弯函数，当且仅当

$$\sum_{u\in U} (-1)^{f(u)} = 1,$$

这就完成了该命题的证明。 □

命题 2.4。设 f 是 $\mathcal{PS}_{ap}^{\#}$ 中的超弯函数，且 $f(0) = 0$。则存在一个从 U 到 $\mathbb{F}_2$ 的函数 g，使得

$$f(x) = g(x^{2^m-1})$$

对于 $x \in \mathbb{F}_{2^n}^*$，以及

$$\sum_{u\in U} (-1)^{g(u)} = 1.$$

反之，若 g 是一个从 U 到 $\mathbb{F}_2$ 的函数，满足 $\sum_{u\in U}(-1)^{g(u)} = 1$，则从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 的函数 f 满足：对于 $x \in \mathbb{F}_{2^n}^*$ 和 $f(0) = 0$，$f(x) = g(x^{2^m-1})$，是一个从 $\mathcal{PS}_{ap}^{\#}$ 到 $\mathcal{PS}_{ap}^{\#}$ 的超弯函数。

证明。首先假设 f 是 $\mathcal{PS}_{ap}^{\#}$ 中的超弯函数，且 $f(0) = 0$。取 s 为 2^m-1 模 2^m+1 的乘法逆元，并定义 $g:\ U \to \mathbb{F}_2$，使得

$g(u) = f(u^s)$ 对每个 $u \in U$成立。对于 $x \in \mathbb{F}_{2^n}^*$，取 $u \in U$和 $y \in \mathbb{F}_q^*$，使得 $x = uy$。于是我们有

$$f(x) = f(u) = f(u^{s(2^m-1)}) = f((u^{2^m-1})^s) = g(u^{2^m-1}) = g(x^{2^m-1}).$$

并且我们看到

$$\sum_{u\in U}(-1)^{g(u)} = \sum_{u\in U}(-1)^{f(u^s)} = \sum_{u\in U}(-1)^{f(u)} = 1$$

由命题 2.3 及 $\gcd(2^m+1, s) = 1$。

现在假设 g 是从 U 到 $\mathbb{F}_2$ 的函数，满足 $\sum_{u\in U}(-1)^{g(u)} = 1$，且 f是 $\mathbb{F}_{2^n}$ 上的布尔函数，满足对于 $x \in \mathbb{F}_{2^n}^*$， $f(x) = g(x^{2^m-1})$，并且 $f(0) = 0$。注意到

$$f(\alpha^{q+1}x) = f(x)$$

其中 α 是 $\mathbb{F}_{2^n}$的本原元，并且

$$\sum_{u\in U}(-1)^{f(u)} = \sum_{u\in U}(-1)^{g(u^{2^m-1})} = \sum_{u\in U}(-1)^{g(u)} = 1$$

因为 $\gcd(2^m-1, 2^m+1) = 1$。由命题 2.3， f 是从 $\mathcal{PS}_{ap}^{\#}$到.....的超弯函数。证明至此完成。 □

3. 向量值超弯函数的构造与枚举 s

令 n、m、γ 和 U 如第 2.2 节所述。在群环的背景下，我们得到向量值超弯函数的以下刻画。

定理 3.1。令 $n = 2m$。令 $F(x)$ 为从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2^k$ 的向量函数，使得对于 F 的分量函数的每个非零组合 f，$f(\gamma^{2^m+1}x) = f(x)$ 成立，且 $F(0) = 0$。则以下条件等价:

(1) F 是维数为 k 的向量值超弯函数。(2) 对所有 $v \in \mathbb{F}_2^k \setminus \{0\}$，$\sum_{u\in U}(-1)^{\langle v,}$ $^{F(u)\rangle} = 1$。(3) 在群环 $\mathbb{Z}[H]$ 中，$\sum_{u\in U} F(u) = 2^{m-k}H + 0_H$ 成立，其中 H 是 $\mathbb{F}_2^k$ 的加法群。

证明。根据向量值超弯函数的定义，我们推得 F 当且仅当对所有 $v \in \mathbb{F}_2^k \setminus \{0\}$， $\langle v, F(u)\rangle$ 都是弯函数时，才是向量值超弯函数；根据命题 2.3，这等价于 (2)。因此，(1) 与 (2) 等价。

假设 $\sum_{u\in U} F(u) = 2^{m-k}H + 0_H$ 成立。取 H 的任意非主特征χ_v ，可得

$$\sum_{u\in U}(-1)^{\langle v,F(u)\rangle} = \sum_{u\in U}\chi_v(F(u)) = \chi_v(2^{m-k}H + 0_H) = 1,$$

其中 $\chi_v(x) = (-1)^{\langle v,\ x\rangle}$。

假设对所有 $v \in \mathbb{F}_2^k \setminus \{0\}$，$\sum_{u\in U}(-1)^{\langle v,\ F(u)\rangle} = 1$。则对每个非主特征 χ_v，有 $\chi_v(\sum_{u\in U} F(u))$ $= \chi_v(2^{m-k}H + 0_H) = 1$。此外，我们还有 $\psi(\sum_{u\in U} F(u) = \psi(2^{m-k}H + 0_H) = 2^m + 1$，其中 ψ 表示 H的主特征。由命题 2.1 可得 (3) 成立。因此，(2) 和 (3) 等价，证明至此完成。

□

由于来自 $\mathcal{PS}_{ap}^{\#}$ 的 $\mathbb{F}_{2^n}$ 的每个超弯曲布尔函数都具有如下形式

$$f(x)=\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_ix^{i(2^m-1)}+a_0\right),$$

任何满足定理 3.1 所给条件的从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2^k$ 的向量超弯函数均具有如下表达式:

$$F(x)=\left(\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_{1,i}x^{i(2^m-1)}+a_{1,0}\right),\ldots,\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_{k,i}x^{i(2^m-1)}+a_{k,0}\right)\right).$$

下面的定理统计这种形式的向量超弯函数的数量。

定理 3.2. 设 $n=2m$。设 $\mathcal{N}_{n,k}$ 表示具有如下形式的向量超弯函数的数量

$$F(x)=\left(\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_{1,i}x^{i(2^m-1)}+a_{1,0}\right),\ldots,\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_{k,i}x^{i(2^m-1)}+a_{k,0}\right)\right).$$

那么,

$$\mathcal{N}_{n,k}=2^k\cdot\binom{2^m+1}{2^{m-k}+1}\cdot\prod_{i=1}^{2^k-1}\binom{2^m-i\cdot2^{m-k}}{2^{m-k}}.$$

证明。我们首先考虑满足给定形式且 $F(0)=0$的向量超弯函数的数量 N F。由定理 3.1 可得

$$N=\binom{2^m+1}{2^{m-k}+1}\cdot\prod_{i=1}^{2^k-1}\binom{2^m-i\cdot2^{m-k}}{2^{m-k}}.$$

由于每个具有给定形式的向量超弯函数都是一个具有给定形式且满足 $F(0)=0$的向量超弯函数 $F(x)$ 的平移 $F(x)+r$, $r\in\mathbb{F}_{2^k}$, 并且每个这样的 $F(x)$ 恰有 2^k 个平移, 因此得到所需结果。

□

设 k 是一个正整数。给定 $\mathbb{F}_{2^k}$ 在 $\mathbb{F}_2$ 上的一组有序基 $A=(\alpha_1,\ldots,\alpha_k)$, 其对偶基定义为满足以下条件的一组基 $B=(\beta_1,\ldots,\beta_k)$:

$$\mathrm{Tr}_1^k(\alpha_i\beta_j)=\delta_{i,j}\text{ for }i,j=1,2,\ldots,k,$$

其中 $\delta_{i,\ j}$ 表示克罗内克 δ 函数。众所周知, $\mathbb{F}_{2^k}$ 在 $\mathbb{F}_2$ 上的每一组基都有唯一的对偶基。

令 $n=2m$ 和 k 为满足 $k|m$的整数。记 $\mathcal{HB}_{n,k}$ 为所有从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2^k$的超弯函数的集合, 其形式为

$$F(x)=\left(\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_{1,i}x^{i(2^m-1)}+a_{1,0}\right),\ldots,\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m}a_{k,i}x^{i(2^m-1)}+a_{k,0}\right)\right),$$

其中 $a_{i,j} \in \mathbb{F}_{2^n}$ 对于 $i \in \{1, \ldots, k\}$ 和 $j \in \{0, \ldots, 2^m\}$成立。令 $\mathcal{HB}_{n,k}$ 表示所有从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_{2^k}$的超弯函数的集合，其形式为

$$\widetilde{F}(x) = \mathrm{Tr}_k^n \left(\sum_{i=1}^{2^m} b_i x^{i(2^m-1)} + b_0 \right),$$

其中 $b_i \in \mathbb{F}_{2^n}$ 适用于 $i \in \{0, \ldots, 2^m\}$。设 $A = (\alpha_1, \ldots, \alpha_k)$ 是 $\mathbb{F}_{2^k}$ 在 $\mathbb{F}_2$ 上的一组基，且 $B = (\beta_1, \ldots, \beta_k)$ 是其对偶基。我们定义映射 π，从 $\mathcal{HB}_{n,k}$ 到 $\mathcal{HB}_{n,k}$，如下：$\pi(f_1(x) \ldots, f_k(x)) = \sum_{j=1}^{k} f_j(x)\alpha_j$，其中 $(f_1(x) \ldots, f_k(x)) \in \mathcal{HB}_{n,k}$。并定义映射 σ，从 $\widetilde{\mathcal{HB}}_{n,k}$ 到 $\mathcal{HB}_{n,k}$，如下：$\sigma(\widetilde{F}(x)) = \left(\mathrm{Tr}_1^k(\beta_1 \widetilde{F}(x)) \ldots, \mathrm{Tr}_1^k(\beta_k \widetilde{F}(x))\right)\widetilde{}$，其中 $F(x) \in \mathcal{HB}_{n,k}$。简单验证可知，$\pi\sigma(F(x)) = F(x)$，且 $\sigma\pi(f_1(x) \ldots, f_k(x)) = (f_1(x) \ldots, f_k(x))$，对于 $F(x) \in \mathcal{HB}_{n,k}$ 以及 $(f_1(x) \ldots, f_k(x)) \in \mathcal{HB}_{n,k}$ 均成立。因此，从 $\mathcal{HB}_{n,k}$ 得到的超弯函数恰好是 $\mathcal{HB}_{n,k}$ 中的那些元素。

注记 3.1. 设 $n = 2m$。$\mathcal{HB}_{n,m}$ 中向量超弯函数的数量由 *[7],* 计数，因此我们的结果是情形 $k = m$的推广。

定理 3.3. 设 $n = 2m$ 且 $u_0 \in U \setminus \{1\}$。设 T_{u_0} 为定义在 $\mathbb{F}_{2^n}$ 上的向量函数，其定义为

$$T_{u_0}(x) = \mathrm{Tr}_m^n \left(u_0 \sum_{i=1}^{2^{m-1}} x^{i(2^m-1)} \right).$$

则 T_{u_0} 是一个向量值超弯函数。

证明. 记

$$g(u) = \mathrm{Tr}_m^n \left(u_0 \sum_{i=1}^{2^{m-1}} u^i \right) \text{ for } u \in U$$

并注意到 $g(1) = 0$。根据命题 2.4，只需证明 $g|_{U\setminus\{1\}}$ 将 $U \setminus \{1\}$映射到 $\mathbb{F}_{2^m}$上。假设存在 $u_1 \neq u_2 \in U \setminus \{1\}$ 使得

$$\mathrm{Tr}_m^n \left(u_0 \sum_{i=1}^{2^{m-1}} u_1^i \right) = \mathrm{Tr}_m^n \left(u_0 \sum_{i=1}^{2^{m-1}} u_2^i \right). \tag{2}$$

既然

$$\begin{aligned}
\mathrm{Tr}_m^n \left(u_0 \sum_{i=1}^{2^{m-1}} u_1^i \right) &= \mathrm{Tr}_m^n \left(u_0 u_1 \frac{1 + u_1^{2^{m-1}}}{1 + u_1} \right) \\
&= u_0 u_1 \frac{1 + u_1^{2^{m-1}}}{1 + u_1} + u_0^{2^m} u_1^{2^m} \frac{1 + u_1^{2^{2m-1}}}{1 + u_1^{2^m}} \\
&= u_0 u_1 \frac{1 + u_1^{2^{m-1}}}{1 + u_1} + u_0^{-1} \frac{1 + u_1^{-2^{m-1}}}{1 + u_1},
\end{aligned}$$

我们计算得出

$$\begin{aligned}\left(\mathrm{Tr}_m^n\left(u_0\sum_{i=1}^{2^{m-1}}u_1^i\right)\right)^2 &= u_0^2u_1^2\frac{1+u_1^{-1}}{1+u_1^2}+u_0^{-2}\frac{1+u_1}{1+u_1^2}\\ &= u_0^2\frac{1+u_1^{-1}}{1+u_1^{-2}}+u_0^{-2}\frac{1+u_1}{1+u_1^2}\\ &= \frac{u_0^2}{1+u_1^{-1}}+\frac{u_0^{-2}}{1+u_1}.\end{aligned}$$

同理，我们有

$$\left(\mathrm{Tr}_m^n\left(u_0\sum_{i=1}^{2^{m-1}}u_2^i\right)\right)^2 = \frac{u_0^2}{1+u_2^{-1}}+\frac{u_0^{-2}}{1+u_2}.$$

于是，由（2）可得

$$\frac{u_0^2}{1+u_1^{-1}}+\frac{u_0^{-2}}{1+u_1}=\frac{u_0^2}{1+u_2^{-1}}+\frac{u_0^{-2}}{1+u_2},$$

也就是说,

$$\frac{u_0^2u_1+u_0^{-2}}{1+u_1}=\frac{u_0^2u_2+u_0^{-2}}{1+u_2}.$$

Then

$$(u_0^2u_1+u_0^{-2})(1+u_2)=(u_0^2u_2+u_0^{-2})(1+u_1).$$

由此可得

$$(u_0^2+u_0^{-2})(u_1+u_2)=0.$$

由于 $u_0\neq 1$，我们有 $u_0^2\neq u_0^{-2}$。因此 $u_1=u_2$，这与假设矛盾。于是 $g|_{U\setminus\{1\}}$ 是单射；又因为 $U\setminus\{1\}$ 和 $\mathbb{F}_{2^m}$ 的大小相同，所以它也是满射。证明至此完成。

□

若对任意 $b\in\mathbb{F}_2^k$，都有 $\#\{x\in\mathbb{F}_{2^m}:\ h(x)=b\}=2^{m-k}$，则称函数 h 从 $\mathbb{F}_{2^m}$ 到 $\mathbb{F}_2^k$ 为平衡函数。下面给出一个从 $\mathbb{F}_{2^{2m}}$ 到 $\mathbb{F}_2^k$构造向量值超弯函数的直接方法。

定理 3.4。设 T_{u_0} 如定理 3.3 中所定义。设 h 是从$\mathbb{F}_{2^m}$ 到 $\mathbb{F}_2^k$ 的平衡函数，且 $h(0)=0$。那么 $h(T_{u_0}(x))$ 是从 $\mathbb{F}_{2^n}$ 到$\mathbb{F}_2^k$的向量值超弯函数。

证明。由定理 3.1 和定理 3.3 可直接得出。 □

最后，我们利用置换多项式和二元 m 序列给出若干超弯函数的无限类。

若其关联的多项式函数 $h\colon x\mapsto f(x)$ 从 $\mathbb{F}_{2^m}$ 到其自身构成 $\mathbb{F}_{2^m}$ 的一个置换，则称多项式 $h(X)\in\mathbb{F}_{2^m}[X]$ 是 $\mathbb{F}_{2^m}$ 上的置换多项式（PP）。置换性质已得到充分研究的一类重要多项式

是 Dickson 多项式，下面我们将对其进行定义。我们回顾一下， r 阶二元 Dickson 多项式 $D_r(x) \in \mathbb{F}_2[x]$ 定义为

$$D_r(x) = \sum_{i=0}^{\lfloor r/2 \rfloor} \frac{r}{r-i} \binom{r-i}{i} x^{r-2i},$$

其中， $\lfloor r/2 \rfloor$表示小于或等于 $r/2$的最大整数。对于 $r = 0$，我们设$D_0(x) = 0$。前八个二元狄克森多项式为

$$D_0(x) = 0, \quad D_1(x) = x, \quad D_2(x) = x^2, \quad D_3(x) = x^3 + x, \quad D_4(x) = x^4,$$
$$D_5(x) = x^5 + x^3 + x, \quad D_6(x) = x^6 + x^2, \quad D_7(x) = x^7 + x^5 + x.$$

我们记$x = \frac{1}{y}$，其中 $y \neq 0$ 为一个不定元。于是，二元狄克森多项式通常可以改写为（也称为函数表达式）

$$D_r(x) = D_r\left(y + \frac{1}{y}\right) = y^r + \frac{1}{y^r}.$$

对于任意非零正整数 r 和 s，Dickson 多项式满足：

$$D_r(D_s(x)) = D_{rs}(x).$$

Dickson 多项式中的置换多项式已得到完整分类。我们陈述以下由 N¨obauer [19] 提出的定理。Dickson 在其 1896年博士论文中观察到并部分证明了该定理。

定理 3.5。Dickson 多项式 $D_r(x)$是 $\mathbb{F}_{2^m}$ 上的置换多项式，当且仅当 $\gcd(r, 2^{2m} - 1) = 1$。

结合定理 3.4和定理 3.5，可得到以下由 Dickson 多项式构造向量超弯函数的方法。

推论 3.1. 设 $n = 2m$，且 r 为满足 $\gcd(r, 2^{2m} - 1) = 1$的正整数。设 T_{u_0} 如定理 3.3 中所定义，且 $D_r(x)$为第 r 个二元 Dickson 多项式。那么， $D_r(T_{u_0}(x))$ 是从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_{2^m}$的向量值超弯函数。

将 [14] 中提出的任意置换二项式或置换三项式代入定理 3.4，即可得到一个从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_{2^m}$的向量值超弯函数。

周期为 $2^m - 1$ 的二元 m 序列是 $\mathbb{F}_2$ 中的元素序列，其形式为$\left\{\mathrm{Tr}_1^m\left(\gamma^{di+t}\right)\right\}_{i\in\mathbb{Z}}$，其中 γ 是 $\mathbb{F}_{2^m}^*$的生成元， t 是整数，且抽取 d 满足 $\gcd(d, 2^m - 1) = 1$。利用迹函数表示，两个 m 序列 $\{\mathrm{Tr}_1^m(\gamma^i)\}_{i\in\mathbb{Z}}$和 $\left\{\mathrm{Tr}_1^m\left(\gamma^{di}\right)\right\}_{i\in\mathbb{Z}}$之间的互相关 $C_d(t)$ 可由以下指数和描述

$$\begin{aligned} C_d(t) &= \sum_{i=0}^{2^m-2} (-1)^{\mathrm{Tr}\left(\gamma^{t+i} + \gamma^{di}\right)} \\ &= \sum_{x\in\mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}\left(x^d + cx\right)}, \end{aligned}$$

其中 $c = \gamma^t$。我们称 $C_d(t)$ 是 v 值的，这意味着 $\#\{C_d(t): \ t \in \mathbb{Z}\} = v$。Katz [13]证明了，如果互相关函数 $C_d(t)$ 是三值的，那么 $C_d(t)$ 总会取 -1 作为其中一个值。因此，我们得到如下由三值 m 序列构造超弯函数的方法。

推论 3.2. 设 $n = 2m$ 和 $u_0 \in U \setminus \{1\}$。设 d 为任意正整数，使得 $\gcd(d, 2^m - 1) = 1$，且 $C_d(t)$ 是三值的。那么总存在 $\lambda \in \mathbb{F}_{2^m}^*$，使得 $\mathrm{Tr}_1^m\left(\left(\mathrm{Tr}_m^n\left(u_0 \sum_{i=1}^{2^{m-1}} x^{i(2^m-1)}\right)\right)^d\right) + \mathrm{Tr}_1^n\left(\lambda u_0 \sum_{i=1}^{2^{m-1}} x^{i(2^m-1)}\right)$ 是一个超弯函数。

对于长度为 $2^m - 1$ 的二元 m 序列，以下是已知能产生三值互相关的所有抽取指数的完整列表。要确定该列表是否完整，是一个具有挑战性的开放问题。

(i) Gold [5]: $d = 2^k + 1$, $\frac{m}{\gcd(k,m)}$ 为奇数。

(ii) Kasami [20]: $d = 2^{2k} - 2^k + 1$, $\frac{m}{\gcd(k,m)}$ 为奇数。

(iii) Cusick 和 Dobbertin [2]: $d = 2^{\frac{m}{2}} + 2^{\frac{m+2}{4}} + 1$, $m \equiv 2$ (模 4)。

(iv) Cusick 和 Dobbertin [2]: $d = 2^{\frac{m+2}{2}} + 3$, $m \equiv 2$ (模 4)。

(v) Canteaut、Charpin 和 Dobbertin [3]: $d = 2^{\frac{m-1}{2}} + 3$, m 为奇数。

(vi) Dobbertin [4], Hollmann 和 Xiang [12]:

$$d = \begin{cases} 2^{\frac{m-1}{2}} + 2^{\frac{m-1}{4}} - 1, & m \equiv 1 \pmod 4 \\ 2^{\frac{m-1}{2}} + 2^{\frac{3m-1}{4}} - 1, & m \equiv 3 \pmod 4 \end{cases}.$$

4. 结论

本文致力于推导向量超弯函数的一个充分必要条件，这是对 [7] 中定理 1 在 $k = n/2$ 情形下的推广。我们还得到了形如以下形式的向量超弯函数个数的数值结果 $\mathcal{N}_{n,\ k}$

$$F(x) = \left(\mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m} a_{1,i} x^{i(2^m-1)} + a_{1,0}\right), \ldots, \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^m} a_{k,i} x^{i(2^m-1)} + a_{k,0}\right)\right),$$

这推广了 [7] 中定理 4 的结果。根据定理 3.4，寻找向量超弯函数 $\mathbb{F}_{2^n}$ 的问题可归结为寻找从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2^k$ 的平衡函数 $\mathbb{F}_2^k$。

致谢。本工作得到国家自然科学基金委员会项目（批准号：12171428、12231015 和 61972400）的资助。

参考文献

[1] C. Carlet、P. Han、S. Mesnager 和 C. Tang。具有扩域系数的 Dillon 型指数超弯函数的 Möbius 变换及其刻画。 *Advances in Mathematics of Communications*, 16(4), 709-720, 2022。[2] T.W. Cusick 和 H. Dobbertin。二元 m 序列的一些新的三值互相关函数。*Inf. Theory* 42 4 1238 1240, 1996 *IEEE Trans.* ,

（），–。[3] A. Canteaut、P. Charpin 和 H. Dobbertin。具有三值互相关的二元 m 序列：Welch 猜想的证明。 *IEEE Trans. Inf. Theory*, 46(1), 4-8, 2000。

[4] H. Dobbertin。GF(2^n) 上的几乎完美非线性幂函数：Welch 情形。 *IEEE Trans. Inf. Theory*，45(4)，1271–1275，1999。[5] R. Gold。具有 3 *IEEE Trans. Inf.* 值递归 *Theory* 14 1 154 156, 1968 互相关函数的极大递归序列（通信）。，（），第 - 页。[6] A. Muratovi *IEEE* c-Ric、E. *Trans. Inf. Theory* 60 2 1337 1347, 2014 Pasalic 和 S. Bajric。由多项迹函数构造的向量值弯曲函数。，（），–。[7] A. Muratovi´c-Ribi´c、E. Pasalic 和 S. Ribi´c。 PS_{ap} 类的向量超弯曲迹函数——其确切数量与刻画。 *IEEE Trans. Inf. Theory*，60(7)，4408-4413，2014。[8] A.M. Youssef 和 G. Gong。超弯函数。《密码学进展——EUROCRYPT 2001》，《计算机科学讲义》，第 2045 卷。施普林格，柏林，406–419，2001。[9] C. Carlet 和 P. Gaborit。超弯函数与循环码。 *Journal of Combinatorial Theory A* 113 3 466 482, , 2006 （），-。[10] J.F.Dillon。初等 Hadamard 差集。博士学位论文，马里兰大学，大学公园市，1974。[11] J.-P. Flori 和 S. Mesnager。具有多项迹的超弯函数族的高效刻画。*J. Math. Cryptol.*，7(1)，43–68，2013。[12] H.D. Hollmann 和 Q. Xiang。关于二元 m 序列互相关的 Welch 猜想和 Niho 猜想的证明。有限域及其应用，7(2)，253-286，2001。[13] D.J. Katz。二项式的 Weil 和、三值互相关以及 Helleseth 猜想。 *Journal of Combinatorial Theory Series A* 119 8 1644 1659, 2012 , , （），–。[14] K. Li、L. Qu 和 X. Chen。有限域上的新型置换二项式和置换三项式。 *Finite Fields and Their Applications* 43 69 85, 2017 ，–。[15] L. Lapierre 和 P. Lison˘ek。关于具有 Dillon 型指数的向量值弯曲函数。2016 年 IEEE 国际信息论研讨会论文集，西班牙巴塞罗那，2016 年 7 月，第 490–494 页。[16] P. Charpin 和 G. Gong。超弯函数、Kloosterman 和与 Dickson 多项式。 *IEEE Trans. Inf.*，（），–。[17] *Theory* 54 9 4230 4238, 2008 S. Mesnager 和 J.-P. Flori。通过 Dillon 型指数构造超弯函数。 *IEEE Trans. Inf. Theory*，59(5)，3215–3232，2013。[18] S. Mesnager。《弯曲函数：基础与结果》。瑞士查姆：施普林格，2016。[19] W. N obauer。关于一类 *J. Reine Angew. Math.* 231 215 置换多项式及其表示的群。，，–219，1968。[20] T. Kasami。 2 阶二元 *Infor- mation and Control* 18 4 369 394, 1971 Reed-Muller 码若干子码的重量枚举多项式。，（），–。