arXiv:2304.03884v1 [cs.DM] 8 Apr 2023

Dillon 函数的瑞利商

阿迪蒂·卡尔·冈戈帕迪亚[1], 曼西[1],比马尔·曼达尔[2],亚历山大·库岑科[3], 苏加塔·冈戈帕迪亚[4]

[1] 印度鲁尔基理工学院数学系，印度鲁尔基 247667；{aditi.gangopadhyay, mansi}@ma.iitr.ac.in[2] 印度焦特布尔理工学院数学系，印度焦特布尔 342030；bimalmandal@iitj.ac.in[3] 俄罗斯新西伯利亚国立大学，俄罗斯新西伯利亚 630090；alexandrkutsenko@bk.ru[4] 印度鲁尔基理工学院计算机科学与工程系，印度鲁尔基 247667；sugata.gangopadhyay@cs.iitr.ac.in

摘要。弯曲函数的沃尔什–哈达玛谱唯一确定一个对偶函数。弯曲函数的对偶函数也为弯曲函数。与其对偶函数相等的弯曲函数称为自对偶函数。弯曲函数与其对偶函数之间的汉明距离与其瑞利商相关。Carlet、Danielsen、Parker 和 Sol´e [2] 在 $\mathcal{PS}_{ap}$中研究了弯曲函数的瑞利商，并得到了一个用特征和表示的表达式 [6]。我们采用另一种方法，利用 Desarguesian 扩张，求得弯曲函数瑞利商的完整谱 $\mathcal{PS}_{ap}$。

关键词：布尔函数、沃尔什–哈达玛变换、自对偶弯曲函数、瑞利商、Desarguesian 扩张

1 引言

设 $\mathbb{F}_2$ 为特征为 2 的素域，并设 $[n] = \{1, 2, \ldots, n\}$。我们将 $\mathbb{F}_{2^n}$ 记为 $\mathbb{F}_2$上的 n 次扩域。由 n 元组 $\mathbb{F}_2$ 构成的 n 维向量空间为 $\mathbb{F}_2^n$ =$\{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_2$，其中对所有 $i \in [n]\}$均成立。我们约定，将 $\mathbb{F}_2^n$中的向量 x 写作 x $=(x_1, x_2, \ldots, x_n)$，其中 $x_i \in \mathbb{F}_2$为各坐标。向量 x $\in \mathbb{F}_2^n$的重量为 $_n$wt(x) $= \sum x_i$ ，其中求和在整数范围内进行。令 $E_e = \{$x $\in \mathbb{F}_2^n :$ wt(x) 为偶数$\}$ ，并令 $E_o = \{$x $\in \mathbb{F}_2^n :_{i=1}$wt(x) 为奇数$\}$。 $\mathbb{F}_2^n$上的内积定义为 x $\cdot$ y $= \oplus_{i=1}^n x_i y_i$，对所有 x, y $\in \mathbb{F}_2^n$均成立，其中 $\oplus$表示模 2 加法。

迹函数 Tr_1^n: $\mathbb{F}_{2^n} \to \mathbb{F}_2$ 由 $\mathrm{Tr}_1^n(x) = x + x^2 + \cdots + x^{2^{n-1}}$定义，其中对所有 $x \in \mathbb{F}_{2^n}$均成立。 $\mathbb{F}_{2^n}$上的内积定义为 $(x, y) \mapsto \mathrm{Tr}_1^n(xy)$，其中对所有 x、$y \in \mathbb{F}_{2^n}$均成立。根据我们对布尔函数定义域的选择，使用上述内积中的一种。设 U 是 $\mathbb{F}_2^n$的一个子空间。 U 的对偶空间为

$$U^\perp = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \cdot \mathbf{y} = 0, \text{ for all } \mathbf{y} \in U\},$$

或者，等价地，如果将 U 视为 $\mathbb{F}_{2^n}$的一个向量子空间，则 U 的对偶空间为

$$U^\perp = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(xy) = 0, \text{ for all } y \in U\}.$$

定义 1. *A Boolean function in n variables is an $\mathbb{F}_2$-valued function from $\mathbb{F}_2^n$, or equivalently from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.*

Carlet [1], 、Cusick 和 St˘anic˘a [3] 是研究与密码学和编码理论相关的布尔函数的优秀参考资料。任意一个含有 n 个变量的布尔函数 f 都有唯一的多项式表示，称为 f 的代数正规形（ANF），其形式为

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\mathbf{a}\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \prod_{i=1}^{n} x_i^{a_i},$$

其中，对于所有 a $=(a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$，系数为 $\mu_{\mathbf{a}} \in \mathbb{F}_2$。令 $\mathfrak{B}_n$ 为 n f $f = | f |$ $f = \{ \in \mathbb{F}_2^n$ f $\neq$个变0$\}$ f $f \in \mathfrak{B}_n$ $f = 2^{n-1}$量上所有布尔函数的集合。函数的重量为 wt( ) supp( )，其中 supp( ) x : (x) 称为函数的支撑集。若 wt( )，则称函数为平衡函数。 f的代数次数为 $deg(f) =$max{wt(a) : $\mu_{\mathbf{a}} \neq 0$}。次数至多为 1 的布尔函数称为仿射函数。所有 n变量仿射布尔函数的集合记为 $\mathfrak{A}_n$。 n 变量上的仿射函数具有形式 $f(x_1, x_2, \ldots, x_n)$ $= \oplus_{i=1}^{n} a_i x_i \oplus \varepsilon$，其中对于所有 $i = 1, 2, \ldots, n$， $a_i, \varepsilon \in \mathbb{F}_2$。若 $\varepsilon = 0$，则称 f为一个 n变量线性函数，所有此类函数的集合记为 $\mathfrak{L}_n$。两个布尔函数 $f, g \in \mathfrak{B}_n$ 之间的汉明距离为 $dist(f, g) = |\{$x $\in \mathbb{F}_2^n$: f(x) $\neq g$(x)$\}|$。 f与仿射函数集合之间的汉明距离的最小值称为其非线性度，即 $nl_f = dist(f, \mathfrak{A}_n) =min\{dist$ $(f, g) : g \in \mathfrak{A}_n\}$。 $f \in \mathfrak{B}_n$ 的沃尔什–哈达玛变换是一个取整数值的函数 $W_f : \mathbb{F}_2^n \to \mathbb{Z}$，定义为

$$W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}},$$

对于所有 u $\in \mathbb{F}_2^n$。多重集 $[W_f$(u) : u $\in \mathbb{F}_2^n]$称为 f的沃尔什–哈达玛谱。对于每个 u $\in \mathbb{F}_2^n$， W_f (u) 用于计算 f与线性函数 u $\cdot$x 之间的距离。 f 的非线性度与其沃尔什–哈达玛谱之间的关系如下:

$$nl_f = 2^{n-1} - \frac{1}{2} \max_{\mathbf{u}\in\mathbb{F}_2^n} |W_f(\mathbf{u})|.$$

由于高非线性度函数在设计多种密码学原语方面的应用，对这类函数的研究已十分深入。对于任意正偶整数 n，一类称为弯曲函数的函数可达到非线性度的上界。Mesnager [8] 是研究弯曲函数最全面的参考资料。与之相反，Tokareva [10] 对弯曲函数理论进行了简明回顾，并提供了若干引人入胜的历史见解。本文着重研究某些特殊类别弯曲函数及其对偶函数的汉明距离分布。

1.1 弯曲函数、对偶性与瑞利商

任意布尔函数 $f \in \mathfrak{B}_n$都满足帕塞瓦尔恒等式 $\sum_{\mathbf{u}\in\mathbb{F}_2^n} |W_f(u)|^2 = 2^{2n}$。换言之，沃尔什–哈达玛系数的平方的平均值为 2^n。由于非负整数数据集中的最大值总是大于或等于平均值，即 max $\mathbf{u}\in\mathbb{F}_2^n |W_f \quad | \geq$(u)。因此，$2^{\frac{n}{2}}$ $2^{n-1}-2^{\frac{n}{2}-1}$任意布尔函数的非线性度都有上界，即对于任意 $f \in \mathfrak{B}_n$

$$nl_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

当 n 为偶数时，一类称为弯曲布尔函数的函数可以达到此上界。

定义 **2** *Let n be a positive even integer. A Boolean function $f \in \mathfrak{B}_n$ that has nonlinearity*。 $nl_f = 2^{n-1} - 2^{\frac{n}{2}-1}$ *is said to be bent.*

等价地，当且仅当对所有 u $\in \mathbb{F}_2^n$， n变量上的布尔函数称为弯曲函数，其中 $|W_f$(u)$| = 2^{\frac{n}{2}}$。因此，弯曲函数定义在变量个数为偶数的情形下，其沃尔什–哈达玛谱仅包含两个值。

˜定义 3. *If $f \in \mathfrak{B}_n$ is a bent function, then there exists a unique function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ suchthat*

$$W_f(\mathbf{u}) = (-1)^{\widetilde{f}(\mathbf{u})} 2^{\frac{n}{2}}, \text{ for all } \mathbf{u} \in \mathbb{F}_2^n.$$

The function $\widetilde{f}$ is said to be the dual of f, and it is also a bent function in n variables.

特别地，如果 $f=\widetilde{f}$那么 f称为自对偶；如果 $f=\widetilde{f}\oplus 1$，即 $\widetilde{f}$是 f的补函数，那么f称为反自对偶。Rothaus [13] 首次构造了一类弯曲函数，称为 Maiorana– McFarland 弯曲函数。令 $n=2k$。函数 $f:\mathbb{F}_2^k\times\mathbb{F}_2^k\to\mathbb{F}_2$ 属于 Maiorana–McFarland 弯曲函数类，当且仅当

$$f(\mathbf{x},\mathbf{y})=\mathbf{x}\cdot\pi(\mathbf{y})\oplus g(\mathbf{y}),$$

对所有的 $\mathbf{x},\mathbf{y}\in\mathbb{F}_2^k$，其中 $\pi:\mathbb{F}_2^k\to\mathbb{F}_2^k$ 是一个置换，$g:\mathbb{F}_2^k\to\mathbb{F}_2$ 是 k 元变量上的任意布尔函数。Maiorana–McFarland 函数 f 的对偶函数也属于同一类型，定义如下：

$$\widetilde{f}(\mathbf{x},\mathbf{y})=\mathbf{x}\cdot\pi^{-1}(\mathbf{y})\oplus g(\pi^{-1}(\mathbf{y})),$$

对所有Dillon [4,5]构造了另一类弯曲函数，称为部分扩张（$\mathcal{PS}$），其支撑集是 $\mathbb{F}_2^n$的部分扩张中各元素的并集。此外，Dillon 还构造了部分扩张函数的一个子类，该子类由扩张中的元素组成。我们称这些函数为 Dillon 函数 [6]。

定义

4 *Let $n=2k$ be an even integer. A partial spread of $\mathbb{F}_2^n$ consists of pairwise supplementary k-dimensional subspaces of $\mathbb{F}_2^n$. A partial spread is a full spread if the union of its elements equals $\mathbb{F}_2^n$.*

。$\mathcal{PS}^-$ $\mathcal{PS}^+$ $\mathcal{PS}$ =类分为两个互不相交的函数类，分别称为 $\mathcal{PS}^-\cup\mathcal{PS}^+$ S 和，即。我们首先定义集合的示性函数如下：

$$\phi_S(\mathbf{x})=\begin{cases}1 & \text{if } \mathbf{x}\in S;\\ 0 & \text{if } \mathbf{x}\notin S.\end{cases}$$

设 U和 V是 $\mathbb{F}_2^n$的两个子空间。如果 $U\cap V=\{\mathbf{0}\}$，其中 0 是 $\mathbb{F}_2^n$中的全零向量，则称 U和 V“不相交”。设 E_i、 $i=1$、2、.....、2^{k-1}是 $\mathbb{F}_2^n$中两两“互不相交”的 k维子空间。若弯曲函数 $f\in\mathfrak{B}_n$具有如下形式，则称其属于 $\mathcal{PS}^-$类：

$$f(\mathbf{x})=\sum_{i=1}^{2^{k-1}}\phi_{E_i}(\mathbf{x})-2^{k-1}\phi_{\{\mathbf{0}\}}(\mathbf{x}).$$

2^{k-1} $f\in\mathcal{PS}^-$ 的对偶函数具有如下形式：$\widetilde{f}(\mathbf{x})=\sum\phi_{E_i^\perp}(\mathbf{x})-2^{k-1}\phi_{\{\mathbf{0}\}}(\mathbf{x})$。若弯曲函数 $f\in\mathfrak{B}_n$属于 $\mathcal{PS}^+$ 类，则其具有如下形式：$i=1$

$$f(\mathbf{x})=\sum_{i=1}^{2^{k-1}+1}\phi_{E_i}(\mathbf{x})-2^{k-1}\phi_{\{\mathbf{0}\}}(\mathbf{x}),$$

其中 E_i、 $i=1$、2、.....、$2^{k-1}+1$是 $\mathbb{F}_2^n$中两两“互不相交”的 k维子空间。$f\in\mathcal{PS}^+$ 的对偶函数具有如下形式：

$$\widetilde{f}(\mathbf{x})=\sum_{i=1}^{2^{k-1}+1}\phi_{E_i^\perp}(\mathbf{x})-2^{k-1}\phi_{\{\mathbf{0}\}}(\mathbf{x}).$$

弯曲函数与其对偶函数之间的距离是一个有趣的研究问题。Danielsen 等人 [6] 提出了弯曲布尔函数的归一化瑞利商，用以衡量弯曲函数与其对偶函数之间的距离。

定义 5。 *The Rayleigh quotient S_f of a Boolean function f in n variables is*

$$S_f=\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{y})\oplus\mathbf{x}\cdot\mathbf{y}}=\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})}W_f(\mathbf{x}).$$

对于弯曲函数，我们使用瑞利商的归一化形式。 N_f 个变量的弯曲函数 f 的归一化瑞利商为

$$N_f=\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus\widetilde{f}(\mathbf{x})}=2^{-\frac{n}{2}}S_f.$$

对于一个 n变量的弯曲布尔函数 f，当且仅当 $N_f = 2^n$ 为自对偶函数时， f 为自对偶；当 f 为反自对偶时， $N_f = -2^n$ 为 f 。弯曲函数 f 与其对偶函数 $\widetilde{f}$ 之间的汉明距离为

$$\begin{aligned}\mathrm{dist}(f,\widetilde{f}) = |\{\mathbf{x}\in\mathbb{F}_2^n : f(\mathbf{x}) \neq \widetilde{f}(\mathbf{x})\}| &= 2^{n-1} - \frac{N_f}{2} \\ &= \begin{cases} 0 & \text{if } f \text{ is self-dual} \\ 2^n & \text{if } f \text{ is anti self-dual} \end{cases}\end{aligned}$$

Now，我们将讨论一些与对称弯曲函数的瑞利商相关的结果 c-
tions.

1.2 对称弯曲函数的瑞利商分布

如果布尔函数 $f \in \mathfrak{B}_n$ 的输出在其输入的任意排列下保持不变，则称其为对称布尔函数。1994年，Savick´y [9] 推导出了对称弯曲函数的如下刻画。

定理1. [9,定理3.3] *If* $f(\mathbf{x}) = c_k$, $\mathrm{wt}(\mathbf{x}) = k$, *is a symmetric function of an even numberof variable* n, *then The following statements are equivalent:*

1. *The function* f *is a bent function;*
2. *For all* $k = 0\ 1\ \ldots\ n-2$, , , *the identity* $c_{k+2} = c_k \oplus 1$ *is satisfied;*
3. *There exist* $\varepsilon_1\ \varepsilon_2 \in \mathbb{F}_2$ f $= \oplus_{1\le i<j\le n} x_i x_j \oplus \varepsilon_1 \oplus_{i=1}^{n} x_i \oplus \varepsilon_2$, , $(\mathbf{x})$ ( ) , *for all* $\mathbf{x} \in \mathbb{F}_2^n$.

我们首先明确推导对称弯曲函数的对偶函数。然后计算对称弯曲函数可能的瑞利商。我们发现，对称弯曲函数的对偶函数要么是自对偶，要么是反自对偶，要么其输出中恰有一半与该函数的输出相同，另一半不同。这些情况取决于变量的数量以及与常数项和线性项相关的系数。结果见以下命题。

命题1. *Let* $f \in \mathfrak{B}_n$ *be a symmetric bent function then the dual of* f *is*

$$\tilde{f}(\mathbf{x}) = \begin{cases} \mathrm{wt}(\mathbf{x}) \oplus c_{\mathrm{wt}(\mathbf{x})} \oplus \frac{n}{4} & \text{if } \frac{n}{2} \text{ is even} \\ \begin{cases} \mathrm{wt}(\mathbf{x}) \oplus c_{\mathrm{wt}(\mathbf{x})+1} \oplus \lfloor \frac{n}{4} \rfloor & \text{if } \mathrm{wt}(\mathbf{x}) \le n-1 \\ n \oplus 1 \oplus c_1 \oplus \lfloor \frac{n}{4} \rfloor & \text{if } \mathrm{wt}(\mathbf{x}) = n \end{cases} & \text{if } \frac{n}{2} \text{ is odd} \end{cases}.$$

命题2. *Let* $f \in \mathfrak{B}_n$ *be a symmetric bent Boolean function, then the Rayleigh quotient of* f *is*

$$N_f = \begin{cases} 0 & \text{if } \frac{n}{2} \text{ is even} \\ \begin{cases} 2^n & \begin{cases} \text{either } \lfloor \frac{n}{4} \rfloor \text{ is even and } c_0 = c_1 \\ \text{or } \lfloor \frac{n}{4} \rfloor \text{ is odd and } c_0 = c_1 \oplus 1 \end{cases} \\ -2^n & \begin{cases} \text{either } \lfloor \frac{n}{4} \rfloor \text{ is odd and } c_0 = c_1 \\ \text{or } \lfloor \frac{n}{4} \rfloor \text{ is even and } c_0 = c_1 + 1 \end{cases} \end{cases} & \text{if } \frac{n}{2} \text{ is odd} \end{cases},$$

where c_0 *and* c_1 *are the output value of function for input of weight* 0 *and* 1 *respectively and* $\lfloor\cdot\rfloor$ *is* , , *the floor function.*

有关这些命题的详细内容，请参阅 [12,9] 。根据以上结果，我们得到了对称弯曲布尔函数的完整瑞利商谱。为方便起见，无需进行大量计算，只要给定一个对称弯曲布尔函数，我们就能求出它的瑞利商。但 Dillon 函数并非如此。 [2]给出了求 Dillon 函数瑞利商的方法。我们希望采用另一种方法，求出 Dillon 函数与其对偶函数之间可能的距离。因此，我们根据弯曲函数与其对偶函数之间的距离，将弯曲函数划分为不同的集合。此处值得注意的是，Kolomeec [7] 证明，两个弯曲函数之间的最小汉明距离为 $2^{\frac{n}{2}}$。因此，两个弯曲函数之间可能的最大汉明距离为 $2^n - 2^{\frac{n}{2}}$，反自对偶弯曲函数除外。

2 弯曲函数及其对偶函数的性质

本节研究弯曲函数及其对偶函数的一些度量性质。这些表达式有助于刻画弯曲函数与其对偶函数之间的距离。记$E_e = \{\mathbf{x} \in \mathbb{F}_2^n\colon \mathrm{wt}(\mathbf{x}) \text{ 为偶数}\}$，以及 $E_o = \{\mathbf{x} \in \mathbb{F}_2^n\colon \mathrm{wt}(\mathbf{x}) \text{ 为奇数}\}$。布尔函数 $f \in \mathfrak{B}_n$ 在 $\in \mathbb{F}_2^n$处的 $A \subset \mathbb{F}_2^n$上的限制沃尔什–哈达玛变换记为 $W_f(\mathbf{a})|_A$，定义为$W_f(\mathbf{a})|_A = \sum_{\mathbf{x}\in A}(-1)^{f(\mathbf{x})\oplus \mathbf{a}\cdot\mathbf{x}}$。

命题 3. *Let $f \in \mathfrak{B}_n$ where $n = 2k \geq 4$ be a bent function and its dual $\widetilde{f}$. The distance , , between $\widetilde{f}$ and f can be written as*

$$\begin{aligned}\mathrm{dist}(f,\widetilde{f}) &= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{0})} + \frac{1}{2^k}\sum_{\mathbf{u}\in \mathrm{supp}(f)} W_f(\mathbf{u}) \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{D_\mathbf{u}f}(\mathbf{u}) + \frac{1}{2^k}\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{D_\mathbf{u}f}(\mathbf{u})|_{E_o}.\end{aligned}$$

Proof. 设 $f \in \mathfrak{B}_n$是一个弯曲函数，$n = 2k \geq 4$，且 $W_f(\mathbf{u}) = 2^k(-1)^{\tilde{f}(\mathbf{u})}$，对所有 $\mathbf{u} \in \mathbb{F}_2^n$。$\widetilde{}$与 f 之间的汉明距离为 f

$$\begin{aligned}\mathrm{dist}(f,\widetilde{f}) = |\{\mathbf{x}\in\mathbb{F}_2^n : f(\mathbf{x}) \neq \widetilde{f}(\mathbf{x})\}| &= 2^{n-1} - \frac{1}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus\widetilde{f}(\mathbf{x})} \\ &= 2^{n-1} - \frac{1}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(1-2f(\mathbf{x}))(-1)^{\widetilde{f}(\mathbf{x})} \\ &= 2^{n-1} - \frac{1}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\widetilde{f}(\mathbf{x})} + \sum_{\mathbf{x}\in\mathbb{F}_2^n} f(\mathbf{x})(-1)^{\widetilde{f}(\mathbf{x})} \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n} W_f(\mathbf{x}) + \frac{1}{2^k}\sum_{\mathbf{x}\in\mathrm{supp}(f)} W_f(\mathbf{x}) \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{x}} + \frac{1}{2^k}\sum_{\mathbf{x}\in\mathrm{supp}(f)} W_f(\mathbf{x}) \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{y})}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\mathbf{y}\cdot\mathbf{x}} + \frac{1}{2^k}\sum_{\mathbf{x}\in\mathrm{supp}(f)} W_f(\mathbf{x}) \\ &= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{0})} + \frac{1}{2^k}\sum_{\mathbf{x}\in\mathrm{supp}(f)} W_f(\mathbf{x}),\end{aligned}$$

and

$$\begin{aligned}\mathrm{dist}(f,\widetilde{f}) = 2^{n-1} - \frac{1}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus\widetilde{f}(\mathbf{x})} &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})}W_f(\mathbf{x}) \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{x}} \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{y})}(-1)^{\mathbf{y}\cdot\mathbf{x}} \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{u})}(-1)^{(\mathbf{x}\oplus\mathbf{u})\cdot\mathbf{x}} \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{D_\mathbf{u}f(\mathbf{x})}(-1)^{\mathrm{wt}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= 2^{n-1} - \frac{1}{2^{k+1}}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\left\{\sum_{\mathbf{x}\in E_e}(-1)^{D_\mathbf{u}f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} - \sum_{\mathbf{x}\in E_o}(-1)^{D_\mathbf{u}f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\right\}\end{aligned}$$

$$= 2^{n-1} - \frac{1}{2^{k+1}} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \left\{ \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_{\mathbf{u}}f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} - 2 \sum_{\mathbf{x}\in E_o} (-1)^{D_{\mathbf{u}}f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} \right\}$$
$$= 2^{n-1} - \frac{1}{2^{k+1}} \sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{D_{\mathbf{u}}f}(\mathbf{u}) + \frac{1}{2^k} \sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{D_{\mathbf{u}}f}(\mathbf{u})|_{E_o}.$$

推论 1. *For any bent function $f \in \mathfrak{B}_n$ where $n \geq 4$ is a positive even integer, we ha ve*

$$2 \sum_{\mathbf{u}\in \mathrm{supp}(f)} W_f(\mathbf{u}) + \sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{D_{\mathbf{u}}f}(\mathbf{u}) - 2 \sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{D_{\mathbf{u}}f}(\mathbf{u})|_{E_o} - 2^n(-1)^{f(\mathbf{0})} = 0.$$

弯曲函数的集合可以利用弯曲函数与其对偶函数之间的距离进行划分。我们来定义弯曲函数的等价类。

定义 6。 *Two bent functions f, $g \in \mathfrak{B}_n$ are called distance equivalent if* $\mathrm{dist}(f, f) = \mathrm{dist}(g, \widetilde{g})$ *and are denoted by $f \sim g$.*

对于任意弯曲函数 f、g、$h \in \mathfrak{B}_n$、$f \sim f$，若 $f \sim g$，则 $g \sim f$；若 $f \sim g$ 且 $g \sim h$，则 $f \sim h$。因此，“$\sim$”是弯曲函数集合上的一个等价关系。我们将与此等价关系相对应的弯曲函数等价类定义为

$$cl(i) = \{f \in \mathfrak{B}_n : f \text{ is bent and } \mathrm{dist}(f, \widetilde{f}) = i\}, \text{ for all } 0 \leq i \leq 2^n.$$

自对偶函数和反自对偶函数的等价类分别为 $cl(0)$ 和 $cl(2^n)$。除反自对偶函数外，$\mathrm{dist}(f, \widetilde{f}) \leq 2^n - 2^{\frac{n}{2}}$。对于每个 $0 \leq i \neq j \leq 2^n$，$cl(i) \cap cl(j) = \emptyset$。因此，$n$ 变量上的所有弯曲函数的集合为 $\cup_{i=0}^{2^n} cl(i)$。由此产生了以下两个显而易见的问题:

– 同一类别的弯曲函数，即固定 $0 \leq i \leq 2^n$ 时的 $cl(i)$，是否仿射等价? 或者，是否可能找到一个非奇异仿射变换，使两个弯曲函数属于同一类别? – 某一特定类别的弯曲函数可能具有哪些距离?

本文将探讨这两个问题。现在，我们证明这些距离类通常并非仿射不变。在下一节中，我们将确定某一类弯曲函数可能所属类别的具体情况。

设 f 是一个定义在 $n = 2k$ 个变量上的弯曲函数，并且对所有 $\mathbf{x} \in \mathbb{F}_2^n$，都有 $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b})$，其中 A 是一个 n 阶非奇异二元矩阵，且 $\mathbf{b} \in \mathbb{F}_2^n$。那么 $g(\mathbf{0}) = f(\mathbf{b})$，$\mathrm{supp}(g) = \mathrm{supp}(f)B \oplus \mathbf{b}B = \{\mathbf{x}B \oplus \mathbf{b}B : f(\mathbf{x}) = 1\}$，其中 $B = A^{-1}$，并且对任意 $\mathbf{u} \in \mathbb{F}_2^n$，

$$W_g(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x}A\oplus\mathbf{b})\oplus\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})\oplus\mathbf{u}\cdot(\mathbf{y}B\oplus\mathbf{b}B)}$$
$$= (-1)^{\mathbf{u}B^T\cdot\mathbf{b}} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})\oplus\mathbf{u}B^T\cdot\mathbf{y}} = (-1)^{\mathbf{u}B^T\cdot\mathbf{b}} W_f(\mathbf{u}B^T).$$

因此，

$$\mathrm{dist}(g, \widetilde{g}) = 2^{n-1} - 2^{k-1}(-1)^{g(0)} + \frac{1}{2^k} \sum_{\mathbf{u}\in\mathrm{supp}(g)} W_g(\mathbf{u})$$
$$= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{b})} + \frac{1}{2^k} \sum_{\mathbf{u}\in\mathrm{supp}(f)B+\mathbf{b}B} (-1)^{\mathbf{u}B^T\cdot\mathbf{b}} W_f(\mathbf{u}B^T)$$
$$= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{b})}$$
$$+ \frac{1}{2^k} \sum_{\mathbf{u}'\in\mathrm{supp}(f)} (-1)^{(\mathbf{u}'\oplus\mathbf{b})BB^T\cdot\mathbf{b}} W_f((\mathbf{u}' \oplus \mathbf{b})BB^T)$$
$$\neq \mathrm{dist}(f, \widetilde{f}), \text{ in general.}$$

设 A 为正交二元矩阵。则 $BB^T = (A^TA)^{-1} = I_n$，并且

$$\mathrm{dist}(g, \widetilde{g}) = 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{b})} + \frac{(-1)^{\mathrm{wt}(\mathbf{b})}}{2^k} \sum_{\mathbf{u}'\in\mathrm{supp}(f)} (-1)^{\mathbf{u}'\cdot b} W_f(\mathbf{u}' \oplus \mathbf{b}).$$

特别地，如果 $\mathbf{b} = \mathbf{0}$，则 $\mathrm{dist}(g, \widetilde{g}) = \mathrm{dist}(f, \widetilde{f})$。我们可以直接从上述表达式得出以下结果。

定理 2 *Let* $f \in \mathfrak{B}_n$ *be bent and* $g = f A \oplus$ *for all* $\in \mathbb{F}_2^n$ *where* A *is a binary*。 (x) (x b) x, b b, , *orthogonal matrix of order* n *and* $\in \mathbb{F}_2^n$. *If* $= \mathbf{0}$ *then it preserves the distance and if* $\neq \mathbf{0}$ b, *then* $=$ $\mathrm{dist}(f, \widetilde{f})$ $\mathrm{dist}(g, \widetilde{g})$ *if and only if one of the following condition holds.*

1. *If* $f(\mathbf{0}) = f(\mathbf{b})$, *then* $\sum_{\mathbf{u}\in \mathrm{supp}(f)} W_f(\mathbf{u}) = (-1)^{\mathrm{wt}(\mathbf{b})} \sum_{\mathbf{u}\in \mathrm{supp}(f)} (-1)^{\mathbf{b}\cdot\mathbf{u}} W_f(\mathbf{u}\oplus\mathbf{b})$.
2. *If* $f(\mathbf{0}) \neq f(\mathbf{b})$, *then* $\sum_{\mathbf{u}\in \mathrm{supp}(f)} W_f(\mathbf{u}) - (-1)^{\mathrm{wt}(\mathbf{b})} \sum_{\mathbf{u}\in \mathrm{supp}(f)} (-1)^{\mathbf{b}\cdot\mathbf{u}} W_f(\mathbf{u}\oplus\mathbf{b}) = 2^{2k}(-1)^{f(\mathbf{0})}$.

由上述定理可知，经过适当的非奇异仿射变换后，自对偶弯曲函数可能不再是自对偶弯曲函数。类似地，也可以利用适当的非奇异仿射变换，从非自对偶弯曲函数构造出自对偶弯曲函数。

例如，考虑 $n = 4$、 f(x) $= x_1x_3 + x_2x_4$，对所有 x $\in \mathbb{F}_2$，，以及两个阶数为 4 的二进制非奇异矩阵 A和 A'，如下所示:

$$A = \begin{bmatrix} 1&1&1&0 \\ 1&1&0&1 \\ 1&0&1&1 \\ 0&1&1&1 \end{bmatrix}, \qquad A' = \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&0 \\ 1&1&1&1 \end{bmatrix}.$$

这里， f是一个自对偶弯曲函数， A是一个正交矩阵，但 A'不是。设对所有 x 都有 $g =$ $f A g' = f A' h = f A \oplus 0,1,1,1 \in \mathbb{F}_2^4$ g (x) (x)、(x) (x)，以及 (x) (x ( ))。那么， 也是自对偶弯曲函数，但 g'和 h 不是自对偶函数。这里 $\mathrm{dist}(g', \widetilde{g'}) = 8$，且 $\mathrm{dist}(h, \widetilde{h}) = 8$。

3 Dillon 函数瑞利商的分布

弯曲函数的部分扩展类记为 $\mathcal{PS}$，由 Dillon [4,5] 构造。Dillon 还构造了 $\mathcal{PS}$ 的一个重要子类，称为 $\mathcal{PS}_{ap}$，其中“ap”表示一个仿射平面。

定义 7. *Let* $x, y \in F_{2^k}$, *where* $k = \frac{n}{2}$. *The class denoted by* $\mathcal{PS}_{ap}$ *in* [2] *consists function of the type* $f\ x\ y = g\ x/y$ *with the convention that* $x/y = 0$ *if* $y = 0$ *and where* g *is balanced* (,) ( ) , ( ) *Boolean function and* $g\ 0 = 0$.

定理 3. [2,定理 4.5] *A Boolean function* f *as defined above is self-dual bent if* g *satisfies* $g(1) = 0$, *and, for all* $u \neq 0$ *the relation* $g(u) = g(1/u)$. *There are exactly* $\binom{2^{\frac{n}{2}-1}-1}{2^{\frac{n}{2}-2}}$ *such functions.*

Danielsen、Parker 和 Sol´e [6] 研究了 Dillon 函数的瑞利商，并得到了一个以特征和表示的表达式。这些函数的特征和在 [11]中定义如下

$$K_g := \sum_u (-1)^{g(u)+g(1/u)}. \tag{1}$$

若 $g = Tr_1^k$，则 K_g 是 Kloosterman 和。

定理 4 [6, 7] *Let* f *be a bent function constructed from a Dillon* g *as above then its* . 定理 , ( ) $N_f = 2^k + 2^{k-1} K_g$.

本节推导部分扩散 Bent 函数与其对偶函数之间距离的表达式。在本文余下部分，我们设 $n = 2k \geq 4$ 和 $f \in \mathfrak{B}_n$ 为一个弯曲函数，其对偶函数记为 $\widetilde{f}$。

3.1 PS$^+$ 弯曲函数与其对偶函数之间的距离

设 $f \in \mathfrak{B}_n$ 是任意 $\mathcal{PS}^+$ 类弯曲函数，满足 $\mathrm{supp}(f) = \cup_{i=1}^{2^{k-1}+1} E_i$，其中 E_i 是 $\mathbb{F}_2^n$ 中“互不相交”的 k 维子空间。若 f 的对偶函数是 $\widetilde{f}$，则 $\mathrm{supp}(\widetilde{f}) = \cup_{i=1}^{2^{k-1}+1} E_i^{\perp}$。显然， $f(0) = \widetilde{f}(0) = 1$。

定理 5. *Let $f \in \mathfrak{B}_n$, $n = 2k \geq 4$, be a $\mathcal{PS}^+$ class bent function with its dual $\widetilde{f}$ and* $\mathrm{supp}(f) = \cup_{i=1}^{2^{k-1}+1} E_i$, *where E_i's are defined as above. Then*

$$\mathrm{dist}(f, \widetilde{f}) = 2^n + 2^k - 2 - 2\sum_{i=1}^{2^{k-1}+1} |\{\mathbf{x} \in E_i^{\perp} \setminus \{\mathbf{0}\} : f(\mathbf{x}) = 1\}|.$$

Proof. f的支撑集可写为 $\mathrm{supp}(f) = (\mathrm{supp}(f) \setminus \{\mathbf{0}\}) \cup \{\mathbf{0}\}$，其中 $\mathrm{supp}(f) \setminus \{\mathbf{0}\} = \cup_{i=1}^{2^{k-1}+1} E_i \setminus \{\mathbf{0}\} = \cup_{i=1}^{2^{k-1}+1} (E_i \setminus \{\mathbf{0}\})$。显然，$W_f(\mathbf{0}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (1 - 2f(\mathbf{x})) = 2^n - 2((2^{k-1}+1)(2^k-1)+1) = -2^k$。根据命题 3，我们有

$$\begin{aligned}
\mathrm{dist}(f, \widetilde{f}) &= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{0})} + \frac{1}{2^k} \sum_{\mathbf{a}\in\mathrm{supp}(f)} W_f(\mathbf{a}) \\
&= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{0})} + \frac{1}{2^k} \sum_{\mathbf{a}\in\mathrm{supp}(f)\setminus\{\mathbf{0}\}} W_f(\mathbf{a}) + \frac{1}{2^k} W_f(\mathbf{0}) \\
&= 2^{n-1} + 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}+1} \sum_{\mathbf{a}\in E_i\setminus\{\mathbf{0}\}} W_f(\mathbf{a}) + \frac{1}{2^k}(-2^k) \\
&= 2^{n-1} + 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}+1} \sum_{\mathbf{a}\in E_i\setminus\{\mathbf{0}\}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{a}\cdot\mathbf{x}} - 1 \\
&= 2^{n-1} + 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}+1} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})} \sum_{\mathbf{a}\in E_i\setminus\{\mathbf{0}\}} (-1)^{\mathbf{a}\cdot\mathbf{x}} - 1 \\
&= 2^{n-1} + 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}+1} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})} \left(\sum_{\mathbf{a}\in E_i} (-1)^{\mathbf{a}\cdot\mathbf{x}} - 1 \right) - 1 \\
&= 2^{n-1} + 2^{k-1} + \sum_{i=1}^{2^{k-1}+1} \sum_{\mathbf{x}\in E_i^{\perp}} (-1)^{f(\mathbf{x})} + 2^{k-1} + 1 - 1 \\
&= 2^{n-1} + 2^k + \sum_{i=1}^{2^{k-1}+1} \sum_{\mathbf{x}\in E_i^{\perp}} (1 - 2f(\mathbf{x})) \\
&= 2^{n-1} + 2^k + (2^{n-1} + 2^k) - 2\sum_{i=1}^{2^{k-1}+1} |\{\mathbf{x} \in E_i^{\perp} : f(\mathbf{x}) = 1\}| \\
&= 2^n + 2^{k+1} - 2\sum_{i=1}^{2^{k-1}+1} |\{\mathbf{x} \in E_i^{\perp} : f(\mathbf{x}) = 1\}| \\
&= 2^n + 2^{k+1} - 2\sum_{i=1}^{2^{k-1}+1} (1 + |\{\mathbf{x} \in E_i^{\perp} \setminus \{\mathbf{0}\} : f(\mathbf{x}) = 1\}|) \\
&= 2^n + 2^k - 2 - 2\sum_{i=1}^{2^{k-1}+1} |\{\mathbf{x} \in E_i^{\perp} \setminus \{\mathbf{0}\} : f(\mathbf{x}) = 1\}|.
\end{aligned}$$

推论 2。 *Let $f \in \mathfrak{B}_n$, $n = 2k \geq 4$, be a $\mathcal{PS}^+$ bent function and $\widetilde{f}$ be dual of f. Then* $\mathrm{dist}(f, \widetilde{f}) \leq 2^n - 2^k$.

Proof. 令 $f \in \mathfrak{B}_n, n = 2k \geq 4$, 为一个 $\mathcal{PS}^+$ 弯曲函数，使得 $\mathrm{supp}(f) = \cup_{i=1}^{2^{k-1}+1} E_i$，其中 E_i's 是 $\mathbb{F}_2^n$ 中互不相交的 k 维子空间。若 $\widetilde{f}$ 是 f 的对偶函数，则 $|\mathrm{supp}(\widetilde{f})| = 2^{n-1} + 2^{k-1} = (2^{n-1} - 2^{k-1}) + 2^k$。因此，至少存在 $2^k - 1$ 个非零元素 $\mathbf{x} \in \mathrm{supp}(\widetilde{f})$，使得

$^{2^{k-1}+1}f(\mathbf{x}) = 1$ 作为 $|\mathrm{supp}(f)| = 2^{n-1} + 2^{k-1}$。因此，$\sum |\{\mathrm{x} \in E_i^{\perp} \setminus \{\mathbf{0}\} : f(\mathrm{x}) = 1\}| \geq 2^k - 1$，并且根据$_{i=1}$推论 5，我们有 $\mathrm{dist}(f, \widetilde{f}) \leq 2^n + 2^k - 2 - 2(2^k - 1) = 2^n - 2^k$。

例如，考虑 $n = 4$ 以及 $\mathbb{F}_2^4$ 的二维“互异”子空间

$$E_1 = \{0000, 0001, 0100, 0101\},\ E_2 = \{0000, 0010, 1000, 1010\}$$
$$E_3 = \{0000, 0011, 1101, 1110\},\ E_4 = \{0000, 0110, 1001, 1111\}$$
$$E_5 = \{0000, 0111, 1011, 1100\}.$$

显然，$E_1^{\perp} = E_2$, $E_3^{\perp} = E_5$ 和 $E_4^{\perp} = E_4$。设 $g_1, g_2, g_3 \in \mathfrak{B}_4$ 是 $\mathcal{PS}^+$ 弯曲函数，使得 $\mathrm{supp}(g_1) = E_1 \cup E_2 \cup E_4$, $\mathrm{supp}(g_2) = E_1 \cup E_2 \cup E_3$，且 $\mathrm{supp}(g_3) = E_1 \cup E_3 \cup E_4$。那么 g_1 是自对偶弯曲函数，即 $\mathrm{dist}(g_1, \widetilde{g_1}) = 0$，并且

$$\mathrm{dist}(g_2, \widetilde{g_2}) = 6,\ \mathrm{dist}(g_3, \widetilde{g_3}) = 12.$$

3.2 PS^- 弯曲函数与其对偶函数之间的距离

设 $f \in \mathfrak{B}_n$ 是 $\mathcal{PS}^-$ 上的弯曲函数，且 E_i 的 $i = 1, \ldots, 2^{k-1}$ 是 $\mathbb{F}_2^n$ 的两两“互不相交”的 k 维子空间，使得 $\mathrm{supp}(f) = \bigcup_{i=1}^{2^{k-1}} E_i \setminus \{\mathbf{0}\}$。显然，当且仅当以下条件成立时，$f$ 是自对偶函数

$$\bigcup_{i=1}^{2^{k-1}} E_i = \bigcup_{i=1}^{2^{k-1}} E_i^{\perp}. \tag{2}$$

不过，确定 $\mathcal{PS}^-$ 中一个弯曲函数与其对偶函数之间所有可能的距离颇有意义。下面给出一个技术性结果。

定理 **6** *Let $n = 2k \geq 4$ and $f \in \mathfrak{B}_n$ be a $\mathcal{PS}^-$ bent function such that $f = \cup_{i=1}^{2^{k-1}} E_i \setminus .\mathrm{supp}() , , , \{\mathbf{0}\}$ where E_i's $1 \leq i \leq 2^{k-1}$ are mutually "disjoint" k-dimensional subspaces of $\mathbb{F}_2^n$. Then*

$$\mathrm{dist}(f, \widetilde{f}) = 2^n - 2^k - 2\sum_{i=1}^{2^{k-1}} |\{\mathbf{x} \in E_i^{\perp} : f(\mathbf{x}) = 1\}|.$$

Proof. 对于任意 $i \in \{1, 2, \ldots, 2^{k-1}\}$，我们有

$$\sum_{\mathbf{x} \in E_i^{\perp}} (-1)^{f(\mathbf{x})} = 2^k - 2|\{\mathbf{x} \in E_i^{\perp} : f(\mathbf{x}) = 1\}|,$$

且 $\mathrm{supp}(f) = \cup_{i=1}^{2^{k-1}} E_i \setminus \{\mathbf{0}\} = \cup_{i=1}^{2^{k-1}} E_i^*$，其中 $E_i^* = E_i \setminus \{\mathbf{0}\}$。由命题 3 可得

$$\begin{aligned}
\mathrm{dist}(f, \widetilde{f}) &= 2^{n-1} - 2^{k-1}(-1)^{f(\mathbf{0})} + \frac{1}{2^k} \sum_{\mathbf{u} \in \mathrm{supp}(f)} W_f(\mathbf{u}) \\
&= 2^{n-1} - 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}} \sum_{\mathbf{u} \in E_i^*} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \\
&= 2^{n-1} - 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})} \sum_{\mathbf{u} \in E_i^*} (-1)^{\mathbf{u} \cdot \mathbf{x}} \\
&= 2^{n-1} - 2^{k-1} + \frac{1}{2^k} \sum_{i=1}^{2^{k-1}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})} \left(\sum_{\mathbf{u} \in E_i} (-1)^{\mathbf{u} \cdot \mathbf{x}} - 1 \right) \\
&= 2^{n-1} - 2^{k-1} + \sum_{i=1}^{2^{k-1}} \sum_{\mathbf{x} \in E_i^{\perp}} (-1)^{f(\mathbf{x})} - \frac{1}{2^k} \sum_{i=1}^{2^{k-1}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})}
\end{aligned}$$

$$= 2^{n-1} - 2^{k-1} + 2^{n-1} - 2\sum_{i=1}^{2^{k-1}} |\{\mathbf{x} \in E_i^{\perp} : f(\mathbf{x}) = 1\}| - 2^{k-1}$$

$$= 2^n - 2^k - 2\sum_{i=1}^{2^{k-1}} |\{\mathbf{x} \in E_i^{\perp} : f(\mathbf{x}) = 1\}|.$$

推论 **3** *Let* $f \in \mathfrak{B}_n$ $n = 2k \geq 4$ f ≤。,, *be a* $2^n - 2^k$*-bent function with its dual* $\widetilde{f}$*. Then* dist(, $\widetilde{f}$)

Proof. 我们知道，对所有 $i = 1$，有 $|\{\mathbf{x} \in E_i^{\perp}: f(\mathbf{x}) = 1\}| \geq 0$，2，....., 2^{k-1}。因此，根据定理 6，可得此结果。

例如，设 E_i、 $1 \leq i \leq 5$ 是 $\mathbb{F}_2^4$ 的子空间，定义如上。假设 f_1、f_2、f_3 是 4 变量中的三个 $\mathcal{PS}^-$ 弯曲函数，且 $\mathrm{supp}(f_1) = E_1 \cup E_2 \setminus \{\mathbf{0}\}$、$\mathrm{supp}(f_2) = E_3 \cup E_4 \setminus \{\mathbf{0}\}$ 和 $\mathrm{supp}(f_3) = E_1 \cup E_3 \setminus \{\mathbf{0}\}$。那么 f_1 是自对偶弯曲函数，即 $\mathrm{dist}(f_1, \widetilde{f_1}) = 0$，并且

$$\mathrm{dist}(f_2, \widetilde{f_2}) = 6,\ \mathrm{dist}(f_3, \widetilde{f_3}) = 12.$$

3.2.1 $\mathcal{PS}_{ap}$ 弯曲函数与其对偶函数之间的距离

根据推论 2 和推论 3，我们得知，$\mathcal{PS}$ 类中一个 n 变量的 $n \geq 4$ 弯曲函数与其对偶函数之间的距离为偶数，且不超过 $2^n - 2^{\frac{n}{2}}$。Dillon [4,5] 构造了 $\mathcal{PS}$ 的一个子类，称为 $\mathcal{PS}_{ap}$ 类。下标“ap”表示“仿射平面”。

本节中，我们得到了这一类函数的瑞利商的显式分布。首先，我们借助 Desarguesian 射影平面介绍 Dillon 函数的构造。

令我们将 $\mathbb{F}_2^n$ 与 $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ 视为同一对象，其中 $n = 2k$。对于每个 $a \in \mathbb{F}_{2^k}$，定义 $E_a = \{(x, xa): x \in \mathbb{F}_{2^k}\}$。显然，对于每个 $a \in \mathbb{F}_{2^k}$， E_a 是 $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ 的 k 维子空间，并且对于所有满足 $a \neq b$ 的 a，都有 $E_a \cap E_b = \{\mathbf{0}\}$ $b \in \mathbb{F}_{2^k}$。令 $E_\infty = \{(0, y): y \in \mathbb{F}_{2^k}\}$。注意，对于所有 $a \in \mathbb{F}_{2^k}$， $E_\infty \cap E_a = \{\mathbf{0}\}$。

$\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ 中的 Desarguesian 扩张为以下集合

$$\mathfrak{D} = \{E_a : a \in \mathbb{F}_{2^k}\} \cup \{E_\infty\}. \tag{3}$$

对于任意 $\mathfrak{C} \subseteq \mathfrak{D}$ 和 $|\mathfrak{C}| = 2^{k-1}$，形式如下的函数

$$f(\mathbf{x}) = \sum_{E \in \mathfrak{C}} \mathbf{1}_E(\mathbf{x}) - 2^{k-1}\mathbf{1}_{\{\mathbf{0}\}}(\mathbf{x}), \tag{4}$$

是 $\mathcal{PS}^-$ 中的一个弯曲函数。所有此类弯曲函数构成一个子类，记为 $\mathcal{PS}_{ap}$。有限域 $\mathbb{F}_{2^k}$ 被视为 $\mathbb{F}_2$ 上的向量空间，并赋予内积 $(x, y) \mapsto \mathrm{Tr}_1^k(xy)$。该内积可扩展为内积 $\langle \cdot, \cdot \rangle : (\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}) \times (\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}) \to \mathbb{F}_2$，其定义为

$$\langle (x, y), (x', y') \rangle = \mathrm{Tr}_1^k(xx') + \mathrm{Tr}_1^k(yy').$$

我们注意到 $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ 中关于 Desarguesian 扩张的以下结果。我们可以对利用 Desarguesian 扩张构造的 $\mathcal{PS}_{ap}$ 弯曲函数进行划分。令 $\mathcal{PS}_{ap}^{ds}(2k)$ 表示在 $\mathcal{PS}_{ap}$ 中利用式 (3) 定义的 Desarguesian 扩张 $\mathfrak{D}$ 构造的 $2k$ 变量弯曲函数的集合。定义

$$cl(i) = \{f \in \mathcal{PS}_{ap}^{ds}(2k) : \mathrm{dist}(f, \widetilde{f}) = (2^{k+1} - 2)(2^{k-1} - i)\},$$

对所有 $i = 0$，1，...，2^{k-1} 均成立。因此，$\mathcal{PS}_{ap}^{ds}(2k)$ 中所有自对偶弯曲函数构成 $cl(2^{k-1})$。显然，对于所有 $0 \leq i \neq j \leq 2^{k-1}$，$cl(i) \cap cl(j) = \emptyset$，且 $\mathcal{PS}_{ap}^{ds}(2k) = \cup_{i=0}^{2^{k-1}} cl(i)$。

引理 1. *For any* $E \in \mathfrak{D}$*, its dual* $E^{\perp} \in \mathfrak{D}$.

Proof. 首先，考虑 $E = E_a$ 对某个 $a \in \mathbb{F}_{2^k}^*$ 成立的情形。令 $(y, z) \in E_a^\perp$，于是

$$\langle (y, z), (x, xa) \rangle = 0,$$

对所有 $x \in \mathbb{F}_{2^k}$。也就是说

$$\mathrm{Tr}_1^k(yx) + \mathrm{Tr}_1^k(zxa) = \mathrm{Tr}_1^k((y + za)x) = 0,$$

对所有 $x \in \mathbb{F}_{2^k}$。
这意味着 $y + za = 0$，也就是说，$z = ya^{-1}$。因此

$$E_a^\perp = \{(y, ya^{-1}) : y \in \mathbb{F}_{2^k}\} = E_{a^{-1}} \in \mathfrak{D}.$$

注意到 E_0、$E_\infty \in \mathfrak{D}$ 彼此正交，即可完成证明。

自对偶 $\mathcal{PS}_{ap}$ 的直接计数见 [2, 定理 4。5]。但下一个定理刻画了自对偶 $\mathcal{PS}_{ap}$ 弯曲函数及其数量。我们的方法不仅能统计自对偶 $\mathcal{PS}_{ap}$ 函数的总数，还能得出 $\mathcal{PS}_{ap}$ 中函数的瑞利商完整分布。

定理 7。 *Let $\mathfrak{D}$ be the Desarguesian spread defined in* (3). *A $\mathcal{PS}_{ap}$ class of bent functionf : $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ defined in* (4) *is self-dual if and only if the following conditions are satisfied*

1. $E_1 \notin \mathfrak{C}$;
2. $\{E_0, E_\infty\} \cap \mathfrak{C} \in \{\emptyset, \{E_0, E_\infty\}\}$;
3. *For all* $a \in \mathbb{F}_{2^k}^* \setminus \{1\}$, $E_a \in \mathfrak{C}$ *if and only if* $E_{a^{-1}} \in \mathfrak{C}$.

The number of self-dual $\mathcal{PS}_{ap}$-bent functions is $\binom{2^{k-1}-1}{2^{k-2}}$.

Proof. f 在式（4）中定义的对偶函数是

$$\widetilde{f}(\mathbf{x}) = \sum_{E \in \mathfrak{C}} \phi_{E^\perp}(\mathbf{x}) - 2^{k-1}\mathbf{1}_{\{\mathbf{0}\}}(\mathbf{x}).$$

设 $\mathfrak{I} = \{E_a : a \in \mathbb{F}_{2^k} \cup \{\infty\}, a \neq 1\}$。要使 f 成为自对偶弯曲函数，$|\mathfrak{C} \cap \mathfrak{I}|$ 必须是偶数。这是因为 $E_a \in \mathfrak{C}$ 当且仅当 $E_{a^{-1}} \in \mathfrak{C}$，其中 $a \in \mathbb{F}_{2^k}^* \setminus \{1\}$；并且 $E_0 \in \mathfrak{C}$ 当且仅当 $E_\infty \in \mathfrak{C}$。因此，$\mathfrak{I}$ 中的子空间要么成对出现，要么都不出现。如果 $E_1 \in \mathfrak{C}$，那么 $|\mathfrak{I}| = 2^{k-1} - 1$。这是不可能的。

如果 f 是自对偶函数，则 E_0、$E_\infty \in \mathfrak{C}$ 或 E_0、$E_\infty \notin \mathfrak{C}$ 必须同时成立。此外，对于所有 $a \in \mathbb{F}_{2^k}^* \setminus \{1\}$，当且仅当 $E_{a^{-1}} \in \mathfrak{C}$ 时，$E_a \in \mathfrak{C}$。因此，这三个条件均得到满足。不难验证，这些条件也是自对偶性的充分条件。

如果 $\{E_0, E_\infty\} \subseteq \mathfrak{C}$，那么其余子空间会从集合 $\mathfrak{D} \setminus \{E_0, E_1, E_\infty\}$ 中成对出现。元素个数为 $\left|\mathfrak{D} \setminus \{E_0, E_1, E_\infty\}\right| = 2^k - 2$。因此，可以从 $\mathfrak{D} \setminus \{E_0, E_1, E_\infty\}$ 中选出的子空间对数为 $2^{k-1} - 1$。要构造 $\mathfrak{C}$，我们需要 $2^{k-2} - 1$ 对子空间，因为 $\{E_0, E_\infty\} \subseteq \mathfrak{C}$。这可以通过 $\binom{2^{k-1}-1}{2^{k-2}-1}$ 种方式完成。

在 $\{E_0, E_\infty\} \cap \mathfrak{C} = \{\emptyset\}$ 的情况下，我们必须从 $\mathfrak{D} \setminus \{E_0, E_1, E_\infty\}$ 中选取所有 2^{k-2} 对 $\mathfrak{C}$。这可以通过 $\binom{2^{k-1}-1}{2^{k-2}}$ 完成。因此，自对偶 $\mathcal{PS}_{ap}$-弯曲函数的总数为

$$\binom{2^{k-1}-1}{2^{k-2}-1} + \binom{2^{k-1}-1}{2^{k-2}} = \binom{2^{k-1}}{2^{k-2}}$$

考虑式 (3) 中定义的 $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ Desarguesian 扩张时，我们可以计算一个 $\mathcal{PS}_{ap}$ 弯曲函数与其对偶函数之间的距离分布。令 $\mathfrak{C}^\perp = \{E^\perp : E \in \mathfrak{C}\}$，其中 $\mathfrak{C} \subseteq \mathfrak{D}$。

定理 8。 *Let $\mathfrak{D}$ be the Desarguesian spread defined in* (3). *A $\mathcal{PS}_{ap}$ bent function f : $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ defined in* (4) *with its dual $\widetilde{f}$ of the form $\widetilde{f}(\mathbf{x}) = \sum_{E \in \mathfrak{C}^\perp} \mathbf{1}_E(\mathbf{x}) - 2^{k-1}\mathbf{1}_{\{\mathbf{0}\}}(\mathbf{x})$。*

1. *If $E_1 \notin \mathfrak{C}$ and $|\mathfrak{C} \cap \mathfrak{C}^\perp| = i \;\; 0 \leq i \leq 2^{k-1}$ then $N_f = 2^n - 4\ 2^{k-1} - i \;\; 2^k - 1$. , , ( )() , , ( )$(2^k - 1)$.*
2. *If $E_1 \in \mathfrak{C}$ and $|\mathfrak{C} \cap \mathfrak{C}^\perp| = 1 + j \;\; 0 \leq j \leq 2^{k-1} - 1$ then $N_f = 2^n - 4\ 2^{k-1} - j - 1$*

Proof. 令 $E_1 \notin \mathfrak{C}$ 和 $\left|\mathfrak{C} \cap \mathfrak{C}^{\perp}\right| = i$，其中 $i \in \{0, 1, \cdots, 2^{k-1}\}$。 f与 $\widetilde{f}$之间的汉明距离为 dist$(f, \widetilde{f})$ $= 2(2^{k-1} - i)(2^k - 1)$。因此

$$N_f = 2^n - 4(2^{k-1} - i)(2^k - 1).$$

设 $E_1 \in \mathfrak{C}$ 和 $\left|\mathfrak{C} \cap \mathfrak{C}^{\perp}\right| = 1 + j$，其中 $j \in \{0, 1, \cdots, 2^{k-1} - 1\}$。 f和 $\widetilde{f}$之间的汉明距离为 dist$(f, \widetilde{f})$ $= 2(2^{k-1} - j - 1)(2^k - 1)$。因此

$$N_f = 2^n - 4(2^{k-1} - j - 1)(2^k - 1).$$

根据上述定理，我们得到 $\mathcal{PS}_{ap}$ 类 Dillon 函数的 N_f 的显式表达式。Danielsen、Parker 和 Sol´e 在前面也提到过的定理7], 中，关于 $\mathcal{PS}_{ap}$ 上瑞利商的表达式是特征和的形式，并非显式形式。由此我们得到以下观察:

– 若函数 f 属于 $2k$ 个变量的 $\mathcal{PS}_{ap}$，则当 $i = 2^{k-1}$ 或 $j = 2^{k-1} - 1$ 时，即对于 $i = 2^{k-1}$ 或 $j = 2^{k-1} - 1$，函数 f 是自对偶函数。– 由 Desarguesian 扩张定义的 $2k$ 变量弯曲函数与其对偶函数之间的距离是 $2^{k+1} - 2$ 的倍数。例如，若 $k = 2$，则此类距离可能仅为 0、6 和 12。若 $k = 3$，则此类距离可能仅为 0、14、28、42 和 56。

命题 4. *There is no anti-self-dual bent function in* $\mathcal{PS}_{ap}$.

Proof. 我们将用反证法证明这一点。令 $n = 2k$ 且 $n \geq 4$。设 $f \in \mathcal{PS}_{ap}$ 为一个 n 元反自对偶弯曲函数，使得 $E_1 \notin \mathfrak{C}$ 且 $|\mathfrak{C} \cap \mathfrak{C}^{\perp}| = i$， $0 \leq i \leq 2^{k-1}$，则

$$N_f = 2^n - 4(2^{k-1} - i)(2^k - 1).$$

因此，对于某个 i， $0 \leq i \leq 2^{k-1}$， f 是一个反自对偶函数 $\Rightarrow N_f = -2^n$。

$$\begin{aligned}
&\Rightarrow 2^n - 4(2^{k-1} - i)(2^k - 1) = -2^n \\
&\Rightarrow 2^{n+1} = 4(2^{k-1} - i)(2^k - 1) \\
&\Rightarrow 2^{n-1} = (2^{k-1} - i)(2^k - 1)
\end{aligned}$$

但这就产生了矛盾，因为 $n \geq 4 \Rightarrow k \geq 2 \Rightarrow (2^k - 1) > 1$，所以右侧乘积有一个不为 1 的奇因子，而左侧没有这样的因子。类似地，当 $E_1 \in \mathfrak{C}$时，我们也可以证明同样的结论。因此，对于任意函数 $f \in \mathcal{PS}_{ap}$， $N_f \neq -2^n$。

对于较小的 $n \geq 4$ 和 $f \in \mathcal{PS}_{ap}$，我们已计算出 N_f 和 dist(f, f) 的所有可能取值，结果汇总在下表中:

n	N_f	dist($f, \widetilde{f}$)
4	-8, 4, 16	0, 6, 12
6	-48, -20, 8, 36, 64	0, 14, 28, 42, 56
8	-224, -164, -104, -44, 16, 76, 136, 196, 256	0, 30, 60, 90, 120, 150, 180, 210, 240
10	-960, -836, -712, -588, -464, -340, -216, -92, 32, 156, 280, 404, 528, 652, 776, 900, 1024	0, 62, 124, 186, 248, 310, 372, 434, 496, 558, 620, 682, 744, 806, 868, 930, 992
12	-3968, -3716, -3464, -3212, -2960, -2708, -2456, -2204, -1952, -1700, -1448, -1196, -944, -692, -440, -188, 64, 316, 568, 820, 1072, 1324, 1576, 1828, 2080, 2332, 2584, 2836, 3088, 3340, 3592, 3844, 4096	0, 126, 252, 378, 504, 630, 756, 882, 1008, 1134, 1260, 1386, 1512, 1638, 1764, 1890, 2016, 2142, 2268, 2394, 2520, 2646, 2772, 2898, 3024, 3150, 3276, 3402, 3528, 3654, 3780, 3906, 4032
14	-16128, -15620, -15112, -14604, -14096, -13588, -13080, -12572, -12064, -11556, -11048, -10540, -10032, -9524, -9016, -8508, -8000, -7492, -6984, -6476, -5968, -5460, -4952, -4444, -3936, -3428, -2920, -2412, -1904, -1396, -888, -380, 128, 636, 1144, 1652, 2160, 2668, 3176, 3684, 4192, 4700, 5208, 5716, 6224, 6732, 7240, 7748, 8256, 8764, 9272, 9780, 10288, 10796, 11304, 11812, 12320, 12828, 13336, 13844, 14352, 14860, 15368, 15876, 16384	0, 254, 508, 762, 1016, 1270, 1524, 1778, 2032, 2286, 2540, 2794, 3048, 3302, 3556, 3810, 4064, 4318, 4572, 4826, 5080, 5334, 5588, 5842, 6096, 6350, 6604, 6858, 7112, 7366, 7620, 7874, 8128, 8382, 8636, 8890, 9144, 9398, 9652, 9906, 10160, 10414, 10668, 10922, 11176, 11430, 11684, 11938, 12192, 12446, 12700, 12954, 13208, 13462, 13716, 13970, 14224, 14478, 14732, 14986, 15240, 15494, 15748, 16002, 16256

4 结论

据我们所知，检查 $\mathcal{PS}$ 中弯曲函数的瑞利商分布仍是一个未解决的问题。上述结果表明，我们可以通过检查有限域上的不同扩张和部分扩张来研究这一问题。

致谢。
Aleksandr Kutsenko 的工作由 Akademgorodok 数学中心根据与俄罗斯联邦科学与高等教育部签订的协议（编号 075-15-2022-282）资助。Mansi 的工作由印度政府科学与工业研究理事会（CSIR）提供的奖学金资助（09/143(1028)/2020-EMR-I）。

参考文献

1. Claude Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press（2021 9781108606806 2 10 1017），https://doi.org/。/。Claude Carlet、Lars Eirik Danielsen、Matthew G. Parker 和 Patrick Sol ´ e。*Self-dual bent func-tions.* International Journal of Information and Coding Theory（ ）–（ ）。1 4 384 399 2010。3. Thomas Cusick 和 Pantelimon St ˘ ˘ anica。*Cryptographic Boolean functions and Applications.* 第版。2 2017 9780128111291 Elsevier，。isbn：。4. J. F. Dillon。*A survey of bent function.* NSA Technical Journal Special Issue（1972），191–217。5. J. F. Dillon。初等 Hadamard 差集。博士论文，马里兰大学帕克分校（1974）。6. Lars Eirik Danielsen、Matthew G. Parker 和 Patrick Sol ´ e。*The Rayleigh Quotient of Bent Function.* IMA International Conference, Cryptography and Coding LNCS –（2009）。2009, 5921 418 432。7. Nikolay Kolomeec。*The graph of minimal distances of bent functions and its properties.* Designs, Codes and Cryptography 85 395–410（2017）。8. Sihem Mesnager。*Bent Functions: Fundamentals and Results* Springer（2016），https://doi.org/ 10 1007 978 3 319 32595 8 。/ - - - -。Peter Savicky。*On the Bent Boolean Functions That are Symmetric.* European Journal of Com-binatorics 15(4) 407–410（1994）。9 ´

10. Natalia Tokareva。 *Bent Functions: Results and Applications to Cryptography*。Academic Press（2015年）, https://doi.org/10.1016/C2014-0-02922-X 11. Hans Dobbertin 和 Gregor Leander。 *Bent functions embedded into the recursive framework of Z–bent functions* 49 3 22 2008 。Designs, Codes and Cryptography –（ ）。12. Josep Rif`a 和 Victor A. Zinoviev。 *On two families of binary quadratic bent functions.* arXiv: 1211 5257 [ ], 10 48550 1211 5257 。cs.IT https://doi.org/。/arXiv。。O. S. 13 *On bent functions.* Rothaus。Journal of Combinatorial Theory, Series A 20(3) 300–305（1976年）。