Asymptotic lower bounds on the number of bent functions having odd many variables over finite fields of odd characteristic

Vladimir N. Potapov and Ferruh Özbudak

1 Sobolev Institute of Mathematics, Russia

2 Sabanci University and Middle East Technical University, Turkey

Boolean Functions and their Applications, Voss, Norway, September 3-8, 2023

Walsh Transform

Let p be a prime. Let $\mathbb{F}_p$ be the finite field with p elements. For a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and $\alpha \in \mathbb{F}_p^n$, let $\hat{f} : \mathbb{F}_{p^n} \to \mathbb{C}$ be the Walsh Transform of f at α defined as

$$\hat{f}(\alpha) = \sum_{x \in \mathbb{F}_p^n} e^{\frac{2\pi\sqrt{-1}}{p}(f(x) - \alpha \cdot x)},$$

where $\alpha \cdot x$ is the inner product $\alpha_1 x_1 + \cdots + \alpha_n x_n$ of $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $x = (x_1, \ldots, x_n)$.
Let $0 \leq m$ be an integer. We say that f is m-plateaued if

$$|\hat{f}(\alpha)| \in \{0, p^{\frac{n+m}{2}}\}$$

for all $\alpha \in \mathbb{F}_{p^n}$. Let $\mathrm{Supp}(\hat{f})$ denote the subset of $\mathbb{F}_{p^n}$ consisting of α such that $\hat{f}(\alpha) \neq 0$.

- f is bent if and only if f is 0-plateaued.
- If f is m-plateaued, then $|\mathrm{Supp}(\hat{f})| = p^{n-m}$.

Maiorana-McFarland family

Let $\mathcal{M}^\sharp(p,n)$ denote the family of completed Maiorana-McFarland bent functions in n variables over $\mathbb{F}_p$. Note that n is even if $p=2$. The followings are well known:

- Case n is even:

$$\ln\left|\mathcal{M}^\sharp(p,n)\right| = \frac{n}{2}p^{n/2}\ln(p)\,(1+o(1)) \tag{1}$$

  as $n\to\infty$ and n is even.

- Case n is odd:

$$\ln\left|\mathcal{M}^\sharp(p,n)\right| = \frac{n-1}{2}p^{(n-1)/2}\ln(p)\,(1+o(1)) \tag{2}$$

  as $n\to\infty$ and n is odd.

Here $o(\cdot)$ stands for the small o notation as $n\to\infty$.

Generalized MMF

Agievich (2008), Çeşmelioğlu and Meidl (2013), Baksova and Tarannikov (2020)
Let $\{C_a\}_{a\in\mathbb{F}_p^{n_1}}$, $C_a \subseteq \mathbb{F}_p^{n_2}$ be an ordered partition of $\mathbb{F}_p^{n_2}$ into affine subspaces of dimensions $n_2 - n_1$ (OPAS).
Let $\mathcal{F} = \{f_a\}_{a\in\mathbb{F}_p^{n_1}}$ be a family of plateaued functions such that the support of the Walsh spectrum of f_a is exactly C_a.

Generalized construction

Define a function f on n variables as a sum

$$f_{\mathcal{F}}(x, y) = \sum_{a\in\mathbb{F}_p^{n_1}} f_a(y)\mathbf{1}(x - a),$$

where $x \in \mathbb{F}_p^{n_1}, y \in \mathbb{F}_p^{n_2}$, $a \in \mathbb{F}_p$, $\mathbf{1}$ is the indicator function of $\mathbb{F}_p^{n_2} \times \bar{0} \subset \mathbb{F}_p^{n_2} \times \mathbb{F}_p^{n_1}$, $n = n_1 + n_2$, $n_2 \geq n_1$, n and $n_2 - n_1$ are even, $\{C_a\}_{a\in\mathbb{F}_p^{n_1}}$ is OPAS, $f_a \in \mathcal{F}$.

Generalized MMF

Let $\mathcal{GMM}(p, n)$ denote the family of generalized Maiorana-McFarland bent functions in n variables over $\mathbb{F}_p$

Theorem (P., Taranenko, Tarannikov 2023)

If $p = 2$, then

$$\ln\left(|\mathcal{GMM}(p, n)|\right) \geq \frac{3}{4} n p^{n/2} \ln(p) \left(1 + o(1)\right)$$

as $n \to \infty$ and n is even.

Main results

Theorem 1

Let p an odd prime. There exists a sequence of odd integers n (moreover $n \equiv 3 \mod 4$), $n \to \infty$ and a corresponding sequence of families $\mathcal{F}_1(n)$ of generalized Maiorana-McFarland bent functions in n variables over $\mathbb{F}_p$ satisfying

$$\ln\left(|\mathcal{F}_1(n)|\right) \geq \frac{np^n}{\sqrt{p}}\left(1 - \frac{1}{2(p^2-1)}\right)\ln(p)(1+o(1))$$

as $n \to \infty$.

Remark

In Theorem 1, we improve the lower bound in (2) by increasing the coefficient of the main term $np^n \ln(p)$ from $\frac{1}{2\sqrt{p}}$ to $\frac{1}{\sqrt{p}}\left(1 - \frac{1}{2(p^2-1)}\right)$. Note that if $p = 3$, then $\frac{1}{\sqrt{p}}\left(1 - \frac{1}{2(p^2-1)}\right) = \frac{1}{\sqrt{3}}\frac{15}{16}$.

Proof of Theorem1

Let $s \geq 1$ be an integer. Let n_1 be an integer such that $(s+1) \mid n_1$. Recall that a spread $\mathbb{S}$ of dimension $(s+1)$ in $\mathbb{F}_{p^{n_1}}$ is a collection of $(s+1)$ dimensional subspaces of $\mathbb{F}_{p^{n_1}}$ such that any one dimensional subspace of $\mathbb{F}_{p^{n_1}}$ lies in exactly one of the elements of $\mathbb{S}$. Note that $\mathbb{S}$ should have exactly $\frac{1+p+\cdots+p^{n_1-1}}{1+p+\cdots p^s}$ many elements. As $n_1 \to \infty$ and $(s+1) \mid n_1$, Keevash et al. (2023) proved existence of $M_1(s, n_1)$ many spreads such that

$$\ln\left(M_1(s, n_1)\right) = p^{n_1-s-1}(n_1-1)s\ln(p)(1+o(1))$$

as $n_1 \to \infty$.

Using an hyperplane restriction of these spreads and using also more techniques from perfect matchings we obtain that the number $M_2(s, n_1)$ of ordered partitions of $\mathbb{F}_{p^{n_1+s}}$ into s dimensional affine subspaces satisfies

$$\ln\left(M_2(s, n_1)\right) \geq \left(p^{n_1} - p^{n_1-s-1}\delta(s)\right)(n_1+s)s\ln(p) + p^{n_1}n_1\ln(p)(1+o(1))$$

as $n_1 \to \infty$. Here $\delta(s) = \frac{p^{s+1}}{(p^{s+1}-1)}$.

Main results

Recall that $\mathbb{F}_3$ is the finite field with 3 elements.

Theorem 2

There exists a sequence of odd integers $n \to \infty$ and a corresponding sequence of families $\mathcal{F}_2(n)$ of generalized Maiorana-McFarland bent functions in n variables over $\mathbb{F}_3$ satisfying

$$\ln\left(|\mathcal{F}_2(n)|\right) \geq \frac{n3^n}{\sqrt{3}} \ln(3)(1 + o(1))$$

as $n \to \infty$.

Proof of Theorem 2

Using results of Eberhald et al. (2022) we obtain exact number of transversal of Cayley table of $\mathbb{F}_3^n$. This implies that the number $M_4(m)$ of unordered partitions of $\mathbb{F}_{3^m}$ into 1-dimensional subspaces satisfies

$$\ln(M_4(m) \geq 3^{m-1} m \ln(3)(1 + o(1))$$

as $m \to \infty$. Using also definition of transversal we obtain that for the number $M_5(n_1)$ of $2n_1 + 1$ many variable bent functions over $\mathbb{F}_3$ satisfies

$$\ln(M_5(n_1)) \geq 3^{n_1} 2n_1 \ln(3) - 2 \cdot 3^{n_1}(1 + o(1))$$

as $n_1 \to \infty$.