Asymptotic Lower Bounds On The Number Of Bent Functions Having Odd Many Variables Over Finite Fields of Odd Characteristic

V. N. Potapov * and Ferruh Özbudak**

*Sobolev Institute of Mathematics, Novosibirsk, Russia e-mail: vpotapov@math.nsc.ru
**Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Istanbul, and Middle East Technical University, 06800, Ankara, Turkey, e-mail:ozbudak@metu.edu.tr

Abstract

Using recent deep results of Keevash et al. [8] and Eberhard et al. [6] together with further new detailed techniques in combinatorics, we present constructions of two concrete families of generalized Maiorana-McFarland bent functions. Our constructions improve the lower bounds on the number of bent functions in n variables over a finite field $\mathbb{F}_p$ if p is odd and n is odd in the limit as n tends to infinity.

Let p be a prime. Let $\mathbb{F}_p$ be the finite field with p elements. For a set A, let $|A|$ denote its cardinality. Let $\ln(\cdot)$ be the natural logarithm function.

Bent functions were first introduced by Rothaus in 1976 [14] over $\mathbb{F}_2$. In 1985, Kumar et al. generalized the notion of bent function to arbitrary finite fields [9]. We prefer to introduce bent functions as a special class of functions, namely, plateaued functions.

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 $0 \le m$ be an integer. We say that f is m-plateaued if

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

for all $\alpha \in \mathbb{F}_{p^n}$. Here $|\cdot|$ denotes the absolute value in complex numbers. Let $\mathrm{Supp}(\hat{f})$ denote the subset of $\mathbb{F}_{p^n}$ consisting of α such that $\hat{f}(\alpha) \neq 0$. The following facts (definitions) are well known (see, for example, [4], [12])

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

It seems we have rather limited knowledge in construction of plateaued functions over arbitrary finite field (see, for example, [3], [7]). A direct, but still very powerful construction of a strict subclass of plateaued functions is for the class of partially bent functions [2]. If $f : \mathbb{F}_{p^s} \to \mathbb{F}_p$ is a bent function, then for any integer $m \ge 1$, the function

$$\begin{aligned} g : \mathbb{F}_{p^s} \times \mathbb{F}_{p^m} &\to \mathbb{F}_p \\ (x, y) &\mapsto f(x) \end{aligned}$$

is a partially bent function and m-plateaued function in $m+s$ many variables over $\mathbb{F}_p$. Moreover, given any affine space U_1 of dimension s in $\mathbb{F}_q^{m+s}$, it is easy to modify g to g_1 such that $\mathrm{Supp}(\hat{g}_1)$ is U_1.

Bent functions and plateaued functions are central objects for a variety of topics related to cryptography, coding theory and combinatorics. We refer, for example, to [4], [11], [12] and the references therein for further information.

It is an interesting open problem to count bent functions, even for rather moderate values of n (see, [10], [13]). Hence the asymptotic number of bent functions is a natural and actually difficult problem to consider (see [13] and the references therein).

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 following are well known (see, for example, [4], [12] and [13]):

- Case n is even:

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

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

- Case n is odd:

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

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

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

Let $\mathcal{B}(p,n)$ denote the family of bent functions in n variables over $\mathbb{F}_p$. Let $\mathcal{GMM}(p,n)$ denote the family of generalized Maiorana-McFarland bent functions in n variables over $\mathbb{F}_p$ (see [1] and [5]). Note that the notions of completed Maiorana-McFarland bent functions (see [4]) and generalized Maiorana-McFarland bent functions are different.

We have the obvious bound that

$$|\mathcal{B}(p,n)| \geq |\mathcal{GMM}(p,n)|. \tag{3}$$

In [13], the authors obtain that, if $p=2$, then

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

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

In particular they improve the lower bound in (1) so that the coefficient of the main term $np^{n/2}\ln(p)$ is increased from $\frac{1}{2}$ to $\frac{3}{4}$.

Combining (3) and (4) we obtain an asymptotic lower bound on the number of bent functions over $\mathbb{F}_2$, which is the best known asymptotic lower bound on the number of bent functions over $\mathbb{F}_2$.

The methods of [13] do not generalize to odd characteristic. In this paper we improve (2) and we obtain an asymptotic lower bounds on the number of bent functions in odd n variables over $\mathbb{F}_p$ as $n \to \infty$ and p is odd.

We construct two families of generalized bent functions using two different methods related to the results of [8] and [6], respectively.

Using results of [8] and further detailed techniques we prove our first main result in the following.

Theorem 0.1 *Let p be 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*

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

as $n \to \infty$.

We present a sketch of the proof of Theorem 0.1 in Section 2 below.

Remark 0.2 *In Theorem 0.1, we improve the lower bound in (2) by increasing the coefficient of the main term* $np^{n/2}\ln(p)$ *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* $\frac{1}{\sqrt{p}}\left(1-\frac{1}{2(p^2-1)}\right) = \frac{1}{\sqrt{3}}\frac{15}{16}$*. This also gives an improved lower bound in the number of bent functions over* $\mathbb{F}_p$ *for odd number of variables* n *using (3) in the limit as* $n\to\infty$ *if* $p>3$*.*

Using results of [6] and further different detailed techniques we prove our second main result in the following.

Theorem 0.3 *Recall that* $\mathbb{F}_3$ *is the finite field with* 3 *elements. 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*

$$\ln\left(|\mathcal{F}_2(n)|\right) \geq \frac{n3^{n/2}}{\sqrt{3}}\ln(3)(1+o(1))$$

as $n\to\infty$*.*

We present a sketch of the proof of Theorem 0.3 in Section 3 below.

Remark 0.4 *In Theorem 0.3, we improve the lower bound in Theorem 0.1 (and hence the lower bound in (2) by increasing the coefficient of the main term* $n3^{n/2}\ln(3)$ *from* $\frac{1}{\sqrt{3}}\frac{15}{16}$ *to* $\frac{1}{\sqrt{3}}$*. This also gives an improved lower bound in the number of bent functions over* $\mathbb{F}_3$ *for odd number of variables* n *using (3) in the limit as* $n\to\infty$*.*

1 Why do we use only partially bent functions?

In this section we explain why we only use partially bent functions and not arbitrary plateaued functions shortly. Let $s\geq 1$ be an integer. Let $n_1\geq 1$ be a variable integer which runs and tends infinity over a sequence. We construct bent functions with $2n_1+s$ many variables over $\mathbb{F}_p$. Hence our number of variables tends to infinity as n_1 tends to infinity.

Let $\mathcal{P}=(A_1,\ldots,A_{p^{n_1}})$ be an ordered partition of $\mathbb{F}_{p^{n_1+s}}$ into subsets of size exactly p^s. We will need a huge number of such partitions that we can control.

By control we mean the following. Given such $\mathcal{P}$, we need to design a corresponding ordered set of n_1-plateaued functions $(g_1,\ldots,g_{p^{n_1}})$ such that $g_i:\mathbb{F}_{p^{s+n_1}}\to\mathbb{F}_p$ and

$$\mathrm{Supp}(\hat{g}_i)=A_i \tag{5}$$

for each $1\leq i\leq p^{n_1}$.

Let $\phi:\mathbb{F}_{p^{n_1}}\to\{1,2,\ldots,p^{n_1}\}$ be a fixed bijection. A generalized Maiorana-McFarland bent function in $(2n_1+s)$ variables over $\mathbb{F}_p$ is defined as (see [1], [5])

$$\begin{array}{rcl} f:\mathbb{F}_p^{s+n_1}\times\mathbb{F}_p^{n_1} & \to & \mathbb{F}_p \\ (y,z) & \mapsto & g_{\phi(z)}(y). \end{array}$$

If $(A_1,\ldots,A_{p^{n_1}})$ and $(B_1,\ldots,B_{p^{n_1}})$ are two distinct ordered partitions of $\mathbb{F}_{p^{n_1+s}}$ into subsets of size exactly p^s, i.e. $A_i\neq B_i$ for at least one i, then independent from the corresponding ordered set of n_1-plateaued functions (provided they exist), the constructed bent functions f_A and f_B in $(2n_1+s)$ variables are distinct. Moreover assume that we fix an ordered partition $(A_1,\ldots,A_{p^{n_1}})$ of $\mathbb{F}_{p^{n_1+s}}$ into subsets of size exactly p^s. Assume also that there are two corresponding ordered set of n_1-plateaued functions $(g_1,\ldots,g_{p^{n_1}})$ and $(h_1,\ldots,h_{p^{n_1}})$ such that $g_i,h_i:\mathbb{F}_{p^{s+n_1}}\to\mathbb{F}_p$ and

$$\mathrm{Supp}(\hat{g}_i)=\mathrm{Supp}(\hat{h}_i)=A_i \tag{6}$$

for each $1 \leq i \leq p^{n_1}$. Then if $g_i \neq h_i$ for some i, then the constructed bent functions f_g and f_h in $(2n_1 + s)$ variables are distinct.

An important problem is to have a large number of such partitions $\mathcal{P}$ that we make sure existence of a large number of corresponding ordered sequences of n_1-plateaued functions.

We know sufficiently large number of such partitions using affine subspaces of $\mathbb{F}_{p^{n_1+s}}$ of dimension s. This implies that we use only partially bent functions [2]. It is still not an easy problem to count even this particular subject as n_1 tends to infinity. We use methods from [8], [6] together with many new and further techniques to have a good asymptotic lower bound. It seems difficult to improve these asymptotic lower bounds making also use of non partially bent but plateaued functions.

2 Sketch of proof of Theorem 0.1

Let $s \geq 1$ be an integer. Let m be an integer such that $(s+1) \mid m$. Recall that a spread $\mathbb{S}$ of dimension $(s+1)$ in $\mathbb{F}_{p^m}$ is a collection of $(s+1)$-dimensional subspaces of $\mathbb{F}_{p^m}$ such that any one dimensional subspace of $\mathbb{F}_{p^m}$ lies in exactly one of the elements of $\mathbb{S}$. Note that $\mathbb{S}$ should have exactly $\frac{1+p+\cdots+p^{m-1}}{1+p+\cdots+p^s}$ many elements. As $m \to \infty$ and $(s+1) \mid m$, Keevash et al. [8] proved existence of $M_1(s,m)$ many spreads such that

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

as $m \to \infty$.

Take $m = n_1 + s + 1$. 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

$$\ln\left(M_2(s,n_1)\right) \geq \left(p^{n_1} - \delta(s)p^{n_1-s-1}\right)(n_1+s)s\ln(p)(1+o(1)) + p^{n_1}n_1\ln(p)(1+o(1)) \tag{7}$$

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

Using generalized Maiorana-McFarland construction and (7) we obtain that the number $M_3(s,n_1)$ of bent functions in $(2n_1+s)$ variables gives

$$\ln(M_3(s,n_1)) \geq p^{n_1}\left(n_1 s + n_1 + s^2 - \frac{(n_1+s)s\delta(s)}{p^{s+1}}\right)\ln(p)(1+o(1))$$

as $n_1 \to \infty$. Putting $s = 1$ we complete the proof.

3 Sketch of proof of Theorem 0.3

Using results of Eberhald et al. [6] we obtain exact number of transversals of the 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 affine subspaces satisfies

$$\ln(M_4(m)) \geq 3^{m-1}m\ln(3) - 2\cdot 3^{m-1}\ln(3)(1+o(1)) \tag{8}$$

as $m \to \infty$. Take $m = n_1 + 1$. Using generalized Maiorana-McFarland construction and (8) we obtain that the number $M_5(n_1)$ of $(2n_1+1)$-variable bent functions over $\mathbb{F}_3$ satisfies

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

as $n_1 \to \infty$. This completes the proof.

References

[1] S. Agievich. Bent rectangles. *Boolean functions in cryptology and information security*, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 18, pp. 3–22, Amsterdam, 2008.

[2] C. Carlet. Partially-bent functions. *Advances in cryptology'CRYPTO '92 (Santa Barbara, CA, 1992)*, 280-291, Lecture Notes in Comput. Sci., 740, Springer, Berlin, 1993.

[3] C. Carlet. Boolean and vectorial plateaued functions and APN functions. *IEEE Transactions on Information Theory*, vol. 61, no. 11. pp. 6272–6289, 2015.

[4] C. Carlet. *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2021.

[5] A.Çesmelioğlu, W. Meidl and A. Pott. Generalized Maiorana-McFarland class and normality of p-ary bent functions. *Finite Fields and Their Applications*, vol. 24, pp. 105–117, 2013.

[6] S. Eberhard, F. Manners and R. Mrazovic. An asymptotic for the Hall-Paige conjecture. *Advances in Mathematics*, Part A, Paper No. 108423, 73 pp, 2022.

[7] S. Hodžić, E. Pasalic, Y. Wei, F. Zhang. Designing plateaued Boolean functions in Spectral Domain and Their Classification. *IEEE Transactions on Information Theory*, vol. 65, no. 9. pp. 5865–5879, 2019.

[8] P. Keevash, M. Sah and M. Sawhney. The existence of subspace designs. arXiv: 2212.00870, 61 pp, 2022.

[9] P. V. Kumar, R. A. Scholtz, L. R. Welch, "Generalized bent functions and their properties", J. Combinatorial Theory Ser. A vol. 40, no. 1, pp. 90–107, 1985.

[10] P. Langevin and G. Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes and Cryptography*, vol. 59, no. 1-3, pp. 193–205, 2011.

[11] W. Meidl. A survey on p-ary and generalized bent functions. *Cryptography and Communications*, vol. 14, pp. 737–782, 2022.

[12] S. Mesnager. *Bent Functions. Fundamentals and Results*, Springer International Publishing, 2016.

[13] V. N. Potapov, A. A. Taranenko and Yu. V. Tarannikov. An asymptotic lower bound on the number of bent functions. *Designs, Codes and Cryptography*, 2023. DOI: 10.1007/s10623-023-01239-z

[14] O. S. Rothaus "On 'bent' functions" J. Combinatorial Theory Ser. A vol. 20, no. 3, pp. 300–305, 1976.