# Gowers $U_3$ norm of some classes of bent Boolean functions*

Sugata Gangopadhyay[1], Bimal Mandal[2] and Pantelimon Stănică[3]
[1]Department of Computer Science and Engineering
[2]Department of Mathematics
Indian Institute of Technology Roorkee
[3]Department of Applied Mathematics
Naval Postgraduate School, Monterey, CA 93943–5216, USA
sugatfma@iitr.ac.in, bimalmandal90@gmail.com, pstanica@nps.edu

June 23, 2017

**Abstract**

The Gowers $U_3$ norm of a Boolean function is a measure of its resistance to quadratic approximations. It is known that smaller the Gowers $U_3$ norm for a Boolean function larger is its resistance to quadratic approximations. Here, we compute Gowers $U_3$ norms for some classes of Maiorana–McFarland bent functions. In particular, we explicitly determine the value of the Gowers $U_3$ norm of Maiorana–McFarland bent functions obtained by using APN permutations. We prove that this value is always smaller than the Gowers $U_3$ norms of Maiorana–McFarland bent functions obtained by using differentially $\delta$-uniform permutations, for all $\delta \geq 4$. We also compute the Gowers $U_3$ norms for a class of cubic monomial functions, not necessarily bent, and show that for $n = 6$, these norm values are less than that of Maiorana–McFarland bent functions. Further, we computationally show that there exist 6-variable functions in this class which are not bent but achieve the maximum second-order nonlinearity for 6 variables.

**Keywords:** Gowers uniformity norms, second-order nonlinearity, Maiorana–McFarland bent functions, differentially $\delta$-uniform functions, APN functions.
**Mathematics Subject Classification:** 06E30, 94C10.

# 1 Introduction

## 1.1 Boolean functions

We denote by $\mathbb{F}_2$ the finite field with 2 elements and by $\mathbb{F}_2^n = \{x = (x_1, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{F}_2\}$ the $n$-dimensional $\mathbb{F}_2$-vector space consisting of $n$-tuples of elements of $\mathbb{F}_2$. The $n$-degree extension field of $\mathbb{F}_2$ is denoted by $\mathbb{F}_{2^n}$, and $\mathbb{F}_{2^n}^*$ is the group of units of $\mathbb{F}_{2^n}$. Any function from $\mathbb{F}_2^n$ (or, from $\mathbb{F}_{2^n}$) to $\mathbb{F}_2$ is said to be a Boolean function in $n$ variables and their set is denoted by $\mathcal{B}_n$. Let $\mathbb{Z}$ and $\mathbb{R}$ denote the set of integers and real numbers, respectively. Let $\mathbb{Z}^+$ be the set of positive integers. The character form associated to $F \in \mathcal{B}_n$, denoted by the corresponding lower case letter $f$, is defined by $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$. The

*Sections 1–2 were presented in Fq11, The 11th International Conference on Finite Fields and their Applications, Magdeburg, Germany, July 22–26, 2013.

weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is $wt(x) := \sum_{i=1}^n x_i$, where the sum is over the integers. The Hamming distance $d : \mathcal{B}_n \times \mathcal{B}_n \to \mathbb{Z}^+ \cup \{0\}$ is $d(F, G) = |\{x \in \mathbb{F}_2^n : F(x) \neq G(x)\}|$. The algebraic normal form of a Boolean function $F \in \mathcal{B}_n$ is

$$F(x_1, \ldots, x_n) = \sum_{u=(u_1,\ldots,u_n)} \lambda_u \left( \prod_{i=1}^n x_i^{u_i} \right), \lambda_u \in \mathbb{F}_2,$$

where the sum is over $\mathbb{F}_2$. The algebraic degree, $\deg(F)$ of $F$ is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$. The inner product of $x, y \in \mathbb{F}_2^n$, respectively, $x, y \in \mathbb{F}_{2^n}$, is denoted by $x \cdot y$ and defined by $x \cdot y = x_1 y_1 + \cdots + x_n y_n$ (the sum being over $\mathbb{F}_2$), respectively, $x \cdot y = Tr_1^n(xy)$, where the trace function $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

For any $a \in \mathbb{F}_2^n$, $\varphi_a \in \mathcal{B}_n$ is the linear function defined by $\varphi_a(x) = a \cdot x$, for all $x \in \mathbb{F}_2^n$. The Walsh–Hadamard transform of $F \in \mathcal{B}_n$ at $a \in \mathbb{F}_2^n$ is

$$\mathcal{F}(F + \varphi_a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x) + \varphi_a(x)} = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\varphi_a(x)}.$$

The Fourier transform of $f$ at $a \in \mathbb{F}_2^n$ is defined as

$$\widehat{f}(a) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\varphi_a(x)} = \frac{1}{2^n} \mathcal{F}(F + \varphi_a).$$

The Walsh–Hadamard spectrum of $F$ is the multiset $[\mathcal{F}(F + \varphi_a) : a \in \mathbb{F}_2^n]$ and the Fourier spectrum of $f$ (or, of $F$) is $[\widehat{f}(a) : a \in \mathbb{F}_2^n]$.

**Definition 1.1.** *A Boolean function $F \in \mathcal{B}_n$ (n even) is said to be bent if and only if there exists another Boolean function $\widetilde{F} \in \mathcal{B}_n$ such that $\mathcal{F}(F + \varphi_a) = (-1)^{\widetilde{F}(a)} 2^{\frac{n}{2}}$. The Boolean function $\widetilde{F}$ is called the dual of $F$ and it is also a bent function.*

The first generic technique for constructing bent functions was proposed by Rothaus [13]. The functions so obtained are referred to as Maiorana–McFarland bent functions.

**Definition 1.2.** *Suppose $m = 2n$ where $n \in \mathbb{Z}^+$, $\pi$ is a permutation on $\mathbb{F}_{2^n}$ and $g \in \mathcal{B}_n$. A function of the form $F(x, y) = \pi(x) \cdot y + g(x)$, for all $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, is said to be a Maiorana–McFarland bent function.*

Bent functions are interesting objects of study in coding theory and cryptography, since they maximally resist affine approximations, being furthest away from the set of all affine functions.

The derivative of a Boolean function is defined as follows.

**Definition 1.3.** *The derivative of $F \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_2^n$, denoted by $D_a F$, is defined by*

$$D_a F(x) = F(x + a) + F(x), \text{ for all } x \in \mathbb{F}_2^n. \tag{1}$$

If $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$, then $D_a f(x) = (-1)^{D_a F(x)} = (-1)^{F(x+a)+F(x)} = f(x) f(x + a)$. By successively taking derivatives with respect to $k$ linearly independent vectors in $\mathbb{F}_2^n$ we obtain the $k$th-derivatives of $F \in \mathcal{B}_n$.

**Definition 1.4.** *Suppose $u_1, \ldots, u_k$ are linearly independent vectors of $\mathbb{F}_2^n$ generating the subspace $V$ of $\mathbb{F}_2^n$. The kth-derivative of $F \in \mathcal{B}_n$ with respect to $u_1, \ldots, u_k$, or alternatively with respect to the subspace $V$, is defined as*

$$D_V F(x) = D_{u_1,\ldots,u_k} F(x) = \sum_{(a_1,\ldots,a_k)\in\mathbb{F}_2^k} F(x + a_1u_1 + \cdots + a_ku_k), \text{ for all } x \in \mathbb{F}_2^n. \tag{2}$$

From the right hand side of (2) it follows that $D_V F$ is independent of the choice of basis for $V$. The Walsh–Hadamard transform of a bent function $F$ is related to the Walsh–Hadamard transform of its dual $\widetilde{F}$ as we see next.

**Proposition 1.5** ( [4, Lemma 2])**.** *Let $F$ be a bent function on $n$ variables and $\widetilde{F}$ be its dual. Then, for any $a, b \in \mathbb{F}_2^n$, we have*

$$\mathcal{F}(D_a\widetilde{F} + \varphi_b) = \mathcal{F}(D_bF + \varphi_a). \tag{3}$$

### 1.2 Higher-order nonlinearities of Boolean functions

The (first-order) nonlinearity of a Boolean function $F \in \mathcal{B}_n$, denoted by $nl(F)$, is the minimum of its Hamming distances from all the functions in $\mathcal{B}_n$ having algebraic degree at most one, i.e., the affine functions. The nonlinearity $F$ and its Walsh–Hadamard spectrum are related by

$$nl(F) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_{2^n}} |\mathcal{F}(F + \varphi_a)|. \tag{4}$$

The $r$th-order nonlinearity of $F \in \mathcal{B}_n$, denoted by $nl_r(F)$, is its Hamming distance from the set of Boolean functions in $\mathcal{B}_n$ with algebraic degrees at most $r$.

### 1.3 Gowers uniformity norms

Let $f : V \to \mathbb{R}$ be any function on a finite set $V$ and $B \subseteq V$. Then $\mathbb{E}_{x\in B}[f(x)] := \frac{1}{|B|}\sum_{x\in B} f(x)$ is the average of $f$ over $B$. The connection between the expected values of $F : \mathbb{F}_2^n \to \mathbb{F}_2$ and its character form $f$ is given in the lemma below.

**Lemma 1.6.** *We have $\mathbb{E}_{x\in B}[f(x)] = 1 - 2\,\mathbb{E}_{x\in B}[F(x)]$.*

*Proof.* Using the fact that $(-1)^b = 1 - 2b$, for $b \in \{0, 1\}$, we write

$$\begin{aligned}\mathbb{E}_{x\in B}[f(x)] &= \frac{1}{|B|}\sum_{x\in B} f(x) = \frac{1}{|B|}\sum_{x\in B}(-1)^{F(x)} \\ &= \frac{1}{|B|}\sum_{x\in B}(1 - 2F(x)) = 1 - 2\,\mathbb{E}_{x\in B}[F(x)].\end{aligned}$$

□

**Definition 1.7** ([7, Definition 2.2.1])**.** *Let $f : \mathbb{F}_2^n \to \mathbb{R}$. For every $k \in \mathbb{Z}^+$, we define the kth-dimension Gowers uniformity norm (the $U_k$ norm) of $f$ to be*

$$\|f\|_{U_k} = \left(\mathbb{E}_{x,x_1,\ldots,x_k\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f\left(x + \sum_{i\in S} x_i\right)\right]\right)^{\frac{1}{2^k}}. \tag{5}$$

Gowers norms for $k = 1, 2, 3$ are explicitly presented below (cf. [7, 15]):

$$\begin{aligned}
\|f\|_{U_1} &=| \mathbb{E}_{x,h\in\mathbb{F}_2^n}[f(x)f(x+h)] \,|^{1/2} \\
&=| \mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)] \,| \,. \\
\|f\|_{U_2} &=| \mathbb{E}_{x,h_1,h_2\in\mathbb{F}_2^n}[f(x)f(x+h_1)f(x+h_2)f(x+h_1+h_2)] \,|^{1/4} \\
&=| \mathbb{E}_{h_1\in\mathbb{F}_2^n} \,| \mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)f(x+h_1)] \,|^2|^{1/4}, \\
\|f\|_{U_3} &=| \mathbb{E}_{x,h_1,h_2,h_3\in\mathbb{F}_2^n}[f(x)f(x+h_1)f(x+h_2)f(x+h_1+h_2) \\
&\qquad \times f(x+h_3)f(x+h_1+h_3)f(x+h_2+h_3)f(x+h_1+h_2+h_3)] \,|^{1/8} \,.
\end{aligned}$$

It is not difficult (and we will encounter some instances of this claim later) to see that one can recursively define the Gowers norms by

$$\begin{aligned}
\|f\|_{U_1} &= |\mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)]|, \\
\|f\|_{U_{k+1}} &= \left(\mathbb{E}_{h\in\mathbb{F}_2^n}[\|D_h f\|_{U_k}^{2^k}]\right)^{1/2^{k+1}} .
\end{aligned} \tag{6}$$

The connection between the Gowers uniformity norms and correlation of a function with polynomials with a certain degree bound is described by results obtained by Gowers, Green and Tao [11, 12]. For a survey we refer to Chen [7].

**Theorem 1.8** ([7, Fact 2.2.1])**.** *Let $k \in \mathbb{Z}^+$, $\epsilon > 0$. Let $P : \mathbb{F}_2^n \to \mathbb{F}_2$ be a polynomial of degree at most $k$, and $f : \mathbb{F}_2^n \to \mathbb{R}$. Suppose $\left|\mathbb{E}_x[f(x)(-1)^{P(x)}]\right| \geq \epsilon$. Then $\|f\|_{U_{k+1}} \geq \epsilon$.*

Theorem 1.8 implies that if a Boolean function has low Gowers $U_{k+1}$ norm, then it has low correlation with all the polynomials functions on $\mathbb{F}_2^n$ of degrees at most $k$. In other words it has high $k$th-order nonlinearity.

It is known that the $U_k$, for $k > 1$, is a norm, that is, it is homogeneous, nonnegative, nondegenerate and respects the triangle inequality. It is also known that the sequence of norms $\{U_k\}_k$ is monotonically increasing, that is, $\|f\|_{U_k} \leq \|f\|_{U_{k+1}}$, $k \geq 0$.

It is known that the Gowers $U_2$ norm of a function is the $\ell_4$ norm of its Fourier transform, more precisely:

**Theorem 1.9** ([7, 11])**.** *Let $f : \mathbb{F}_2^n \to \mathbb{R}$. Then*

$$\|f\|_{U_2}^4 = \sum_{x\in\mathbb{F}_2^n} \widehat{f}(x)^4. \tag{7}$$

The following is an extension of Theorem 1.9.

**Theorem 1.10.** *Let $k \in \mathbb{Z}^+$, $k \geq 2$. Let $F \in \mathcal{B}_n$ and $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$. Then*

$$\|f\|_{U_k}^{2^k} = \frac{1}{2^{(k-2)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{D_{h_1,\cdots,h_{k-2}}f}(x)^4. \tag{8}$$

*Proof.* Let $g = D_{h_1,\cdots,h_{k-2}}f$, where $h_1, \cdots, h_{k-2} \in \mathbb{F}_2^n$. For any $k \in \mathbb{Z}^+$, the $k$th dimensional

Gowers uniformity norm of $f$ is

$$\begin{aligned}
\|f\|_{U_k}^{2^k} &= \mathbb{E}_{x,h_1,\cdots,h_k\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f(x+\sum_{i\in S} h_i)\right]\\
&= \frac{1}{2^{(k+1)n}} \sum_{x,h_1,\cdots,h_k\in\mathbb{F}_2^n} g(x)g(x+h_{k-1})g(x+h_k)g(x+h_{k-1}+h_k)\\
&= \frac{1}{2^{(k+1)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} g(x)g(x+h_{k-1}) \sum_{h_k\in\mathbb{F}_2^n} g(x+h_k)g(x+h_{k-1}+h_k)\\
&= \frac{1}{2^{(k+1)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} g(x)g(x+h_{k-1}) \sum_{y\in\mathbb{F}_2^n} g(y)g(y+h_{k-1})\\
&= \frac{1}{2^{(k-1)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{g}(x)^2\,(-1)^{h_{k-1}\cdot x} \sum_{y\in\mathbb{F}_2^n} \widehat{g}(y)^2\,(-1)^{h_{k-1}\cdot y}\\
&= \frac{1}{2^{(k-1)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^n} \widehat{g}(x)^2\,\widehat{g}(y)^2\,(-1)^{h_{k-1}\cdot(x+y)}\\
&= \frac{1}{2^{(k-1)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^n} \widehat{g}(x)^2\,\widehat{g}(y)^2 \sum_{h_{k-1}\in\mathbb{F}_2^n} (-1)^{h_{k-1}\cdot(x+y)}\\
&= \frac{1}{2^{(k-2)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{g}(x)^4\\
&= \frac{1}{2^{(k-2)n}} \sum_{h_1,\cdots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{D_{h_1,\cdots,h_{k-2}} f}(x)^4,
\end{aligned}$$

where we used the fact (see [8]) that the autocorrelation

$$C_g(u) = \sum_{x\in\mathbb{F}_2^n} g(x)g(x+u) = 2^n \sum_x \hat{g}(x)^2(-1)^{u\cdot x},\ u\in\mathbb{F}_2^n,$$

as well as [8, Lemma 2.6] giving $\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot w} = 2^n$ if $w=0$, and 0, if $w\neq 0$. □

## 1.4 Gowers $U_3$ norm of the dual of a bent function

It is known that the dual of a bent function is bent. However, it is not known whether a bent function and its dual have the same second-order nonlinearity. We prove that the Gowers $U_3$ norms of a bent and it dual are equal and therefore they provide equal "resistance" to quadratic approximations.

**Proposition 1.11.** *Let the character forms associated to a bent function $F\in\mathcal{B}_n$ and its dual $\widetilde{F}$ be $f$ and $\widetilde{f}$, respectively. Then*

$$\|f\|_{U_3} = \|\widetilde{f}\|_{U_3}. \tag{9}$$

*Proof.* Applying (6), (7) and (3) we obtain

$$\|f\|_{U_3}^8 = \frac{1}{2^n}\sum_{h\in\mathbb{F}_2^n}\|D_hf\|_{U_2}^4 = \frac{1}{2^n}\sum_{h\in\mathbb{F}_2^n}\sum_{a\in\mathbb{F}_2^n}\widehat{D_hf}(a)^4 = \frac{1}{2^{5n}}\sum_{h\in\mathbb{F}_2^n}\sum_{a\in\mathbb{F}_2^n}\mathcal{F}(D_hF+\varphi_a)^4$$
$$= \frac{1}{2^{5n}}\sum_{a\in\mathbb{F}_2^n}\sum_{h\in\mathbb{F}_2^n}\mathcal{F}(D_a\widetilde{F}+\varphi_h)^4 = \|\widetilde{f}\|_{U_3}^8.$$

□

## 2 Gowers $U_3$ norm of Maiorana–McFarland bents of the form $Tr_1^n(yx^{2^i+1})$

Gangopadhyay et al. [9] employed the recursive framework developed by Carlet to identify cubic Maiorana–McFarland bent functions having high second-order nonlinearities. Below we describe the subclass of Maiorana–McFarland bent functions considered in [9] which was originally constructed by Canteaut and Charpin [1]. It is shown in [9] that bent functions on 10 variables having maximum known second-order nonlinearity exist within this class.

Let $m = 2n$. We identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^m$ with $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. In the next theorem we consider cubic Maiorana–McFarland bent functions of the form

$$F_i(x,y) = Tr_1^n(yx^{2^i+1}) \tag{10}$$

where $x, y \in \mathbb{F}_{2^n}$, $m \geq 6$, $i$ is an integer such that $1 \leq i < n$, $\gcd(2^n-1, 2^i+1) = 1$ and $\gcd(i,n) = e$.

**Theorem 2.1.** *If $F_i \in \mathcal{B}_m$ is a function of the form given by (10) and $f_i$ is the associated character form, then*

$$\|f_i\|_{U_3}^8 = \frac{2^m + 2^{n+e}(2^e+1)(2^n-1)}{2^{2m}}. \tag{11}$$

*Consequently, the Gowers $U_3$ norm is minimum if and only if $e = 1$.*

*Proof.* For any function $F \in \mathcal{B}_m$ with $f$ as the associated character form, the Gowers $U_3$ norm can be written as

$$\|f\|_{U_3}^8 = \left|\frac{1}{2^{4m}}\sum_{h,h_1,h_2,x\in\mathbb{F}_2^m}(-1)^{D_{h,h_1,h_2}F(x)}\right|$$
$$= \left|\frac{1}{2^{4m}}\sum_{h_1,h_2\in\mathbb{F}_2^m}\sum_{h,x\in\mathbb{F}_2^m}(-1)^{D_h(D_{h_1,h_2}F)(x)}\right|$$
$$= \frac{1}{2^{4m}}\left|\sum_{h_1,h_2\in\mathbb{F}_2^m}\left(\sum_{x\in\mathbb{F}_2^m}(-1)^{D_{h_1,h_2}F(x)}\right)^2\right|.$$

Let $S(h_1,h_2;F) := \sum_{x\in\mathbb{F}_2^m}(-1)^{D_{h_1,h_2}F(x)}$. We note that $S(h_1,h_2;F) = 2^m$ if either $h_1 = h_2$

or exactly one of $h_1$, $h_2$ is 0, so

$$\begin{aligned}
\|f\|_{U_3}^8 &= \frac{1}{2^{4m}}\left|\sum_{h_1,h_2\in\mathbb{F}_2^m} S(h_1,h_2;F)^2\right| \\
&= \frac{1}{2^{4m}}\left|2^{2m}\left(\sum_{h_1\in\mathbb{F}_2^m} 1 + \sum_{\substack{h_2\in\mathbb{F}_2^m\setminus\{0\}\\ h_1=0}} 1 + \sum_{\substack{h_1\in\mathbb{F}_2^m\setminus\{0\}\\ h_2=0}} 1\right) + \sum_{\substack{h_1,h_2\in\mathbb{F}_2^m\setminus\{0\}\\ h_1\neq h_2}} S(h_1,h_2;F)^2\right| \\
&= \frac{1}{2^{4m}}\left|2^{2m}(3\cdot 2^m-2) + \sum_{\substack{h_1,h_2\in\mathbb{F}_2^m\setminus\{0\}\\ h_1\neq h_2}} S(h_1,h_2;F)^2\right|.
\end{aligned}$$

Replacing $F$ by $F_i$ we note that, since $F_i$ is a cubic function, $S(h_1,h_2;F_i)$ is either 0 or $\pm 2^m$. Therefore we have to count the pairs $(h_1,h_2)$ for which $S(h_1,h_2;F_i)=\pm 2^m$. Similar counting is performed in [9] and [10, Theorem 4]. However, for completeness we recall the basic steps.

Let $h_1=(b,a)$ and $h_2=(d,c)$, where $a,b,c,d\in\mathbb{F}_{2^n}$.

$$\begin{aligned}
D_{(b,a),(d,c)}F_i(x,y) = {}& Tr_1^n(((ad+cb)+(ad^{2^i}+cb^{2^i})^{2^i})x^{2^i}) + Tr_1^n((bd^{2^i}+b^{2^i}d)y) \\
&+ Tr_1^n(ad^{2^i+1}+cb^{2^i+1}) + Tr_1^n((a+c)(bd^{2^i}+b^{2^i}d)).
\end{aligned} \tag{12}$$

*Case* 1*:* If $b=d=0$, then $D_{(b,a),(d,c)}F_i(x,y)=0$, for all $(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. The number of such points is $(2^n-1)(2^n-2)$.

*Case* 2*:* If $b=0$ and $d\neq 0$, then

$$D_{(d,c),(0,a)}F_i(x,y) = Tr_1^n((ad+(ad^{2^i})^{2^i})x^{2^i}) + Tr_1^n(ad^{2^i+1}),$$

which is constant if and only if

$$\begin{aligned}
& ad+(ad^{2^i})^{2^i} = ad + a^{2^i}d^{2^{2i}} = 0, \\
\text{i.e.,}\quad & a^{2^i-1}d^{2^{2i}-1} = (ad^{2^i+1})^{2^i-1} = 1, && \text{since } d\neq 0 \text{ and } a\neq 0, \\
\text{i.e.,}\quad & ad^{2^i+1}\in\mathbb{F}_{2^e}^*, && \text{where } \gcd(i,n)=e.
\end{aligned}$$

Thus, given any $a\in\mathbb{F}_{2^n}\setminus\{0\}$, $c$ and $d$ can be chosen in $2^n$ and $2^e-1$ ways, respectively, such that the second-derivative under consideration is 0. Therefore, among all the derivatives of the form $D_{(d,c),(0,a)}F_i$, exactly $2^n(2^n-1)(2^e-1)$ are constants.

Similarly, if $b\neq 0$ and $d=0$ among all the derivatives of the form $D_{(0,c),(b,a)}F_i$, then exactly $2^n(2^n-1)(2^e-1)$ are constants.

*Case* 3*:* Suppose $b\neq 0$ and $d\neq 0$. Let $b=d$. Then $D_{(d,c),(b,a)}F_i = D_{(0,c+a),(b,a)}F_i = D_{(d,c),(0,a+c)}F_i$. In this case $a\neq c$, since otherwise $(b,a)=(d,c)$ which is already dealt with. Thus, among all the derivatives of the form $D_{(d,c),(b,a)}F_i$, exactly $2^n(2^n-1)(2^e-1)$ are constants.

Suppose $b\neq 0$ and $d\neq 0$. Let $b\neq d$. The second-derivative $D_{(d,c),(b,a)}F_i$ is constant if and only if

$$(ad+cb)+(ad^{2^i}+cb^{2^i})^{2^i}=0 \quad\text{and}\quad bd^{2^i}+b^{2^i}d=0.$$

From the second condition we obtain $(b^{-1}d)^{2^i-1}=1$. Since $b,d\in\mathbb{F}_{2^n}$, $(b^{-1}d)^{2^n-1}=1$. Combining these two we obtain $(b^{-1}d)^{2^e-1}=1$, which implies that $b^{-1}d\in\mathbb{F}_{2^e}^*$. Thus, $d=\gamma b$

where $\gamma \in \mathbb{F}_{2^e}^*$. Since $b \neq d$, $\gamma \neq 1$. Therefore, for each choice of $b$ it is possible to choose $d$ in $2^e - 2$ different ways. From the first condition we obtain:

$$\begin{aligned} & ad + cb + (ad^{2^i} + cb^{2^i})^{2^i} = b(a\gamma + c) + (b^{2^i}(a\gamma + c))^{2^i} = 0, \\ \text{i.e.,} \quad & (b^{2^i+1}(a\gamma + c))^{2^i-1} = 1, \text{ if } a\gamma + c \neq 0. \\ \text{i.e.,} \quad & b^{2^i+1}(a\gamma + c) =: \gamma' \in \mathbb{F}_{2^e}^*, \text{ so, } c = a\gamma + \tfrac{\gamma'}{b^{2^i+1}}. \end{aligned}$$

Note that $a$ can be chosen in $2^n$ ways, $b$ in $2^n - 1$ ways, $d$ in $2^e - 2$ ways and $c$ in $2^e$ ways (including the case for which $a\gamma + c = 0$). So the total number of ways in which $(b, a), (d, c)$ can be chosen is

$$2^{n+e}(2^n - 1)(2^e - 2).$$

Combining all the above counts we obtain

$$\|f_i\|_{U_3}^8 = \frac{2^m + 2^{n+e}(2^e + 1)(2^n - 1)}{2^{2m}}.$$

□

It is observed from (11) that for $e = 1$, the Gowers $U_3$ norm of $F_i$

$$\|f_i\|^8 = \frac{7 \cdot 2^n - 6}{2^{3n}}$$

is minimum. It has been experimentally checked in [9, Section 3] that for $m = 2n = 10$, $1 \leq i \leq 4$ (therefore $e = 1$), the functions $F_i$'s have the largest known second-order nonlinearity.

## 3 Gowers $U_3$ norms of Maiorana–McFarland bent functions constructed by using APN and differentially 4-uniform permutations

A vectorial Boolean function $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$, also referred to as an $(n, n)$-function, is said to be differentially $\delta$-uniform if

$$\delta(a, b) = |\{x \in \mathbb{F}_2^n : \phi(x) + \phi(x + a) = b\}| \leq \delta$$

for all $a, b \in \mathbb{F}_2^n$ with $a \neq 0$. We denote the set $\{x \in \mathbb{F}_2^n : \phi(x) + \phi(x + a) = b\}$ by $\Delta(a, b)$ for all $a, b \in \mathbb{F}_2^n$ with $a \neq 0$. If $\phi$ is differentially 2-uniform then it is said to be an *almost perfect nonlinear* (APN) function. If $\phi$ is an APN function and a permutation then we refer to it as an APN permutation on $\mathbb{F}_2^n$. There are several applications of APN functions, but perhaps the most significant is that if the $S$-box (vectorial Boolean function) is based upon an APN function, the probability of success for the differential attack is minimized [6]. Certainly, in block cipher design, invertibility is essential, so the $S$-boxes must be permutations. There are very few classes of APN functions, like monomials APN, which are completely described, and there are many APN questions still open (like the existence of APN permutations in *all* even dimensions; in fact, we barely know of a single example in dimension 6). The connection with linear codes is well-known via a result of Carlet, Charpin and Zinoviev [3], stating that $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $f(0) = 0$ is APN if and only if the binary linear code with parity check matrix of columns $(\alpha^i, f(\alpha^i))^T$, $1 \leq i \leq 2^n - 1$, has minimum distance 5 ($\alpha$ is a primitive element of $\mathbb{F}_{2^n}$). We refer the reader to the huge body of literature on APN functions, listed in this paper, and elsewhere.

Let

$$E_i = \{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : a \neq 0 \text{ and } \delta(a,b) = i\}, \tag{13}$$

for all nonnegative integers $i$. It is easy to see that $E_i = \emptyset$, if $i \equiv 1 \pmod 2$.

**Lemma 3.1.** *Suppose that $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. Then the cardinality of $E_2 = \{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : a \neq 0$ and $\delta(a,b) = 2\}$ is $|E_2| = 2^{n-1}(2^n - 1)$.*

*Proof.* Let $a \in \mathbb{F}_2^n \setminus \{0\}$. We know that $D_a\phi(x) = D_a\phi(x+a) = b \in \mathbb{F}_2^n$, for all $x \in \mathbb{F}_2^n$. Therefore, the cardinality of the range of the function $D_a\phi$ is at most $2^{n-1}$. Suppose that $\{x_i : i = 1, \ldots, 2^{n-1}\} \subseteq \mathbb{F}_2^n$ such that $x_j \neq x_i$ and $x_j \neq x_i + a$, for all $i \neq j$ and $D_a\phi(x_i) = D_a\phi(x_i + a) = b_i$, for all $i = 1, \ldots, 2^{n-1}$. Then

$$\begin{aligned}
b_i = b_j \Longleftrightarrow & D_a\phi(x_i) = D_a\phi(x_j) \\
\Longleftrightarrow & D_a(\phi(x_i) + \phi(x_j)) = 0 \\
\Longleftrightarrow & D_a(\phi(x_i) + \phi(x_i + b)) = 0, \text{ where } b = x_i + x_j, \\
\Longleftrightarrow & D_aD_b\phi(x_i) = 0,
\end{aligned}$$

which is not possible, since $\phi$ is APN (cf. [6, p. 417]). Therefore, for each choice of $a \in \mathbb{F}_2^n \setminus \{0\}$ we obtain exactly $2^{n-1}$ distinct $b$'s in $\mathbb{F}_2^n \setminus \{0\}$ such that $\delta(a,b) = 2$. Since $a$'s can be chosen in $2^n - 1$ many ways, $|E_2| = 2^{n-1}(2^n - 1)$. □

**Lemma 3.2.** *Let $\phi$ be a differentially $\delta$-uniform $(n,n)$-function, where $\delta = 2k$, and*

$$E_{2i} = \{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : a \neq 0 \text{ and } \delta(a,b) = 2i\},$$

*for all $i \in \{0, 1, \ldots, k\}$. Then $\displaystyle\sum_{i=1}^{k} i\,|E_{2i}| = 2^{n-1}(2^n - 1)$.*

*Proof.* For each $a \in \mathbb{F}_2^n \setminus \{0\}$, it is possible to find a set $\{x_1, \ldots, x_{2^{n-1}}\}$ such that $x_i + a \neq x_j$, whenever $i \neq j$, so that $\mathbb{F}_2^n = \{x_1, \ldots, x_{2^{n-1}}\} \cup \{(x_1 + a), \ldots, (x_{2^{n-1}} + a)\}$. We construct a list of differences as follows:

| No. | Output differences |
|---|---|
| 1 | $\phi(x_1) + \phi(x_1 + a) \quad = \quad b_1$ |
| 2 | $\phi(x_2) + \phi(x_2 + a) \quad = \quad b_2$ |
| $\vdots$ | $\ldots\ldots\ldots$ |
| $j$ | $\phi(x_j) + \phi(x_j + a) \quad = \quad b_j$ |
| $\vdots$ | $\ldots\ldots\ldots$ |
| $2^{n-1}$ | $\phi(x_{2^{n-1}}) + \phi(x_{2^{n-1}} + a) \quad = \quad b_{2^{n-1}}$ |

Table 1: List of (not necessarily distinct) output differences when the input difference is $a$.

If $\delta(a,b) \neq 0$, then $(a,b) \in E_{2i}$ for a unique $i \in \{1, \ldots, k\}$, and we have a subset $S_{(a,b)}^{(i)} \subseteq \{1, \ldots, 2^{n-1}\}$, with $|S_{(a,b)}^{(i)}| = i$, such that $\phi(x_j) + \phi(x_j + a) = b_j = b$, for all $j \in S_{(a,b)}^{(i)}$. We say that $i$ rows of $S^{(i)}_{(a,b)}$ are covered by $(a,b)$. If we consider the collection of all tables like Table 1, one for each $a \in \mathbb{F}_2^n \setminus \{0\}$, then for each $(a,b) \in E_{2i}$, $i$ rows of $S^{(i)}_{(a,b)}$ are covered. It can be checked that $S^{(i)}_{(a,b)} = S^{(i')}_{(a,b')}$ if and only if $i = i'$ and $b = b'$, otherwise, $S^{(i)}_{(a,b)} \cap S^{(i')}_{(a,b')} = \emptyset$.

The total number of rows covered (considering all the distinct $2^n - 1$ tables, one corresponding to each $a \in \mathbb{F}_2^n \setminus \{0\}$) if we vary $(a,b)$ over the whole of $E_{2i}$ is $i\,|E_{2i}|$. If we repeat this process for each $i \in \{1, \ldots, k\}$, eventually all the rows of all the $2^{n-1}$ tables will be exhausted and the claimed identity is shown. □

**Theorem 3.3.** *Let $F \in \mathcal{B}_m$ be a Maiorana–McFarland bent function of the form*

$$F(x,y) = \phi(x) \cdot y + h(x),$$

*for all $x, y \in \mathbb{F}_2^n$, where $h \in \mathcal{B}_n$ and $\phi$ is an APN permutation on $\mathbb{F}_2^n$. Then the Gowers $U_3$ norm of the character form $f = (-1)^F$ is*

$$\|f\|_{U_3}^8 = \frac{7 \cdot 2^n - 6}{2^{3n}}. \tag{14}$$

*Proof.* Using Theorem 1.10,

$$\begin{aligned}
\|f\|_{U_3}^8 &= \frac{1}{2^m} \sum_{(\alpha,\beta)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \widehat{D_{(\alpha,\beta)}f}(a,b)^4 \\
&= \frac{1}{2^{5m}} \sum_{(\alpha,\beta)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left( \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(\alpha,\beta)}F(x,y)+a\cdot x+b\cdot y} \right)^4 \\
&= \frac{1}{2^{5m}}(A+B+C),
\end{aligned}$$

where

$$\begin{aligned}
A &= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left( \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(0,0)}F(x,y)+a\cdot x+b\cdot y} \right)^4, \\
&= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left( \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{a\cdot x+b\cdot y} \right)^4 = 2^{4m}, \\
B &= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left( \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(0,\beta)}F(x,y)+a\cdot x+b\cdot y} \right)^4, \\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left( \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x+b\cdot y} \right)^4 \\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left( \sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x} \sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot y} \right)^4
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{a\in\mathbb{F}_2^n} \left(2^n \sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x}\right)^4 \\
&= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x}\right)^4 - 2^{2m} \sum_{a\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x}\right)^4 \\
&= 2^{2m}(3\cdot 2^{4n} - 2\cdot 2^{3n} - 2^{4n}),\ (\text{cf. [6, p. 418]}) \\
&= 2^{3m+n+1}(2^n-1),
\end{aligned}
$$

$$
\begin{aligned}
C &= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(\alpha,\beta)}F(x,y)+a\cdot x+b\cdot y}\right)^4 \\
&= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{a\cdot x+\beta\cdot\phi(x+\alpha)+h(x)+h(x+\alpha)+(\phi(x)+\phi(x+\alpha)+b)\cdot y}\right)^4 \\
&= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x+\beta\cdot\phi(x+\alpha)+h(x)+h(x+\alpha)} \sum_{y\in\mathbb{F}_2^n} (-1)^{(\phi(x)+\phi(x+\alpha)+b)\cdot y}\right)^4 \\
&= 2^{2m} \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\phi(x+\alpha)+h(x)+h(x+\alpha)}\right)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\phi(x)+b\cdot\beta+h(x)+h(x+\alpha)}\right)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \left(\sum_{x\in\Delta(\alpha,b)=\{x_{\alpha b},x_{\alpha b}+\alpha\}} (-1)^{a\cdot x+\beta\cdot\phi(x)+h(x)+h(x+\alpha)}\right)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \Big((-1)^{a\cdot x_{\alpha b}+\beta\cdot\phi(x_{\alpha b})+h(x_{\alpha b})+h(x_{\alpha b}+\alpha)} \\
&\qquad\qquad +(-1)^{a\cdot(x_{\alpha b}+\alpha)+\beta\cdot\phi(x_{\alpha b}+\alpha)+h(x_{\alpha b}+\alpha)+h(x_{\alpha b})}\Big)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \Big((1+(-1)^{a\cdot\alpha+b\cdot\beta})(-1)^{a\cdot x_{\alpha b}+\beta\cdot\phi(x_{\alpha b})+h(x_{\alpha b})+h(x_{\alpha b}+\alpha)}\Big)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \Big(8+8(-1)^{a\cdot\alpha+b\cdot\beta}\Big) \\
&= 2^{2m} \sum_{(\alpha,b)\in E_2} \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} 8 + 2^{2m+3} \sum_{(\alpha,b)\in E_2} \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} (-1)^{b\cdot\beta+\alpha\cdot a} \\
&= 2^{3m+3}\,|E_2|\,,\ \text{since } (\alpha,b)\neq(0,0), \text{ the sum } \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} (-1)^{b\cdot\beta+\alpha\cdot a} = 0.
\end{aligned}
$$

From Lemma 3.1 we have $|E_2| = 2^{n-1}(2^n-1)$. So

$$
\|f\|_{U_3}^8 = \frac{1}{2^{2m}}(2^m + 2^{n+1}(2^n-1) + 8\,|E_2|) = \frac{7\cdot 2^n - 6}{2^{3n}},
$$

and the claim is shown. □

**Corollary 3.4.** *Let $\|f_i\|_{U_3}^8$ and $\|f\|_{U_3}^8$ be defined as in equation* (11) *and* (14) *respectively. Then*

$$\|f_i\|_{U_3}^8 - \|f\|_{U_3}^8 = \frac{(2^n-1)(2^e+3)(2^e-2)}{2^{3n}}.$$

*Therefore, $\|f_i\|_{U_3}^8 \geq \|f\|_{U_3}^8$, with equality holding only when $e=1$, that is,* $\gcd(n,i)=1$.

**Theorem 3.5.** *Let $G \in \mathcal{B}_m$ be a Maiorana–McFarland bent function of the form*

$$G(x,y) = \psi(x)\cdot y + h(x),$$

*for all $x, y \in \mathbb{F}_2^n$, where $h \in \mathcal{B}_n$ and $\psi$ is a differentially 4-uniform permutation and not an APN permutation on $\mathbb{F}_2^n$. Then the Gowers $U_3$ norm of the character form $g = (-1)^G$ is*

$$\|g\|_{U_3}^8 > \frac{7\cdot 2^n - 6}{2^{3n}}.$$

*Proof.* Using similar arguments as in the proof of Theorem 3.3,

$$\|g\|_{U_3}^8 = \frac{1}{2^{5m}}(A_1 + B_1 + C_1),$$

where

$$\begin{aligned}
A_1 &= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}\left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}(-1)^{D_{(0,0)}G(x,y)+a\cdot x+b\cdot y}\right)^4 = 2^{4m},\\
B_1 &= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}}\sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}\left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}(-1)^{D_{(0,\beta)}G(x,y)+a\cdot x+b\cdot y}\right)^4\\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}}\sum_{a\in\mathbb{F}_2^n}\left(2^n\sum_{x\in\mathbb{F}_2^n}(-1)^{\beta\cdot\psi(x)+a\cdot x}\right)^4\\
&\geq 2^{3m+n+1}(2^n-1), \quad \text{(cf. [6, p. 415])},\\
C_1 &= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}}\sum_{\beta\in\mathbb{F}_2^n}\sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}\left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}(-1)^{D_{(\alpha,\beta)}G(x,y)+a\cdot x+b\cdot y}\right)^4\\
&= 2^{2m}\sum_{a\in\mathbb{F}_2^n}\sum_{\beta\in\mathbb{F}_2^n}\sum_{i=1}^{2}\sum_{(\alpha,b)\in E_{2i}}\left(\sum_{x\in\Delta(\alpha,b)}(-1)^{a\cdot x+\beta\cdot\psi(x)+h(x)+h(x+\alpha)}\right)^4\\
&= C_{11} + C_{12},\\
C_{11} &= 2^{2m}\sum_{a\in\mathbb{F}_2^n}\sum_{\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_2}\left(\sum_{x\in\Delta(\alpha,b)}(-1)^{a\cdot x+\beta\cdot\psi(x)+h(x)+h(x+\alpha)}\right)^4 = 2^{3m+3}|E_2|,\\
C_{12} &= 2^{2m}\sum_{a\in\mathbb{F}_2^n}\sum_{\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_4}\left(\sum_{x\in\Delta(\alpha,b)}(-1)^{a\cdot x+\beta\cdot\psi(x)+h(x)+h(x+\alpha)}\right)^4.
\end{aligned}$$

For each $(\alpha, b) \in E_4$, there exist four distinct elements $x_1, x_1+\alpha, x_2, x_2+\alpha \in \mathbb{F}_2^n$ such that $D_\alpha\psi(x_j) = D_\alpha\psi(x_j+\alpha) = b$ where $j = 1$ and 2. For $j = 1$ and 2,

$$\begin{aligned} S_j &= (-1)^{a\cdot x_j+\beta\cdot\psi(x_j)+h(x_j)+h(x_j+\alpha)} + (-1)^{a\cdot(x_j+\alpha)+\beta\cdot\psi(x_j+\alpha)+h(x_j+\alpha)+h(x_j)} \\ &= (1+(-1)^{a\cdot\alpha+\beta\cdot b})(-1)^{\epsilon_j}, \end{aligned}$$

where $\epsilon_j = a\cdot x_j + \beta\cdot\psi(x_j) + h(x_j) + h(x_j+\alpha)$. Further,

$$\begin{aligned} C_{12} &= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (S_1+S_2)^4 \\ &= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (1+(-1)^{a\cdot\alpha+\beta\cdot b})^4((-1)^{\epsilon_1}+(-1)^{\epsilon_2})^4 \\ &= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (8+8(-1)^{a\cdot\alpha+\beta\cdot b})(1+(-1)^{\epsilon_1+\epsilon_2})^4 \\ &= 2^{2m+6} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (1+(-1)^{a\cdot\alpha+\beta\cdot b})(1+(-1)^{\epsilon_1+\epsilon_2}) \\ &= 2^{2m+6} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (1+(-1)^{a\cdot\alpha+\beta\cdot b}+(-1)^{\epsilon_1+\epsilon_2}+(-1)^{a\cdot\alpha+\beta\cdot b+\epsilon_1+\epsilon_2}) \\ &= 2^{3m+6}|E_4|. \end{aligned}$$

We note that $\sum_{a\in\mathbb{F}_2^n}((-1)^{a\cdot\alpha+\beta\cdot b}+(-1)^{\epsilon_1+\epsilon_2}+(-1)^{a\cdot\alpha+\beta\cdot b+\epsilon_1+\epsilon_2}) = 0$, since $\alpha \neq 0, x_1+x_2 \neq 0$ and $x_1+x_2+\alpha \neq 0$. Thus,

$$\begin{aligned} C_1 = C_{11}+C_{12} &= 2^{3m+3}(|E_2|+8|E_4|) \\ &= 2^{3m+n+2}(2^n-1) + 3\cdot 2^{3m+4}|E_4| > 2^{3m+n+2}(2^n-1), \end{aligned}$$

and the claimed inequality follows. □

**Corollary 3.6.** *The Gowers $U_3$ norm of a Maiorana–McFarland bent function constructed by using a differentially 4-uniform permutation is always larger than the Gower norm of any Maiorana–McFarland bent function obtained by using an APN permutation.*

*Proof.* The proof is immediate from the results of Theorems 3.3 and 3.5. □

**Theorem 3.7.** *Let $K$ be a bent function on $\mathbb{F}_2^m \cong \mathbb{F}_2^n \times \mathbb{F}_2^n$, $m = 2n$, defined by*

$$K(x,y) = \phi_\delta(x)\cdot y, \tag{15}$$

*where $\phi_\delta$ is a differentially $\delta$-uniform permutation on $\mathbb{F}_2^n$, where $\delta = 2t$. The Gowers $U_3$ norm of $k(x,y) = (-1)^{K(x,y)}$, $(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, is $\|k\|_{U_3}^8 \geq \dfrac{7\cdot 2^n - 6}{2^{3n}}$.*

*Proof.* Using similar arguments as in Theorem 3.3,

$$\|k\|_{U_3}^8 = \frac{1}{2^{5m}}(A_1^{'} + B_1^{'} + C_1^{'}),$$

where

$$
\begin{aligned}
A_1^{'} &= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}\left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}(-1)^{D_{(0,0)}K(x,y)+a\cdot x+b\cdot y}\right)^4 = 2^{4m},\\
B_1^{'} &= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}}\sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}\left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}(-1)^{D_{(0,\beta)}K(x,y)+a\cdot x+b\cdot y}\right)^4\\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}}\sum_{a\in\mathbb{F}_2^n}\left(2^n\sum_{x\in\mathbb{F}_2^n}(-1)^{\beta\cdot\phi_\delta(x)+a\cdot x}\right)^4\\
&\geq 2^{3m+n+1}(2^n-1),\quad (cf.[6,p.415]),\\
C_1^{'} &= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}}\sum_{\beta\in\mathbb{F}_2^n}\sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}\left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n}(-1)^{D_{(\alpha,\beta)}K(x,y)+a\cdot x+b\cdot y}\right)^4\\
&= 2^{2m}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{i=1}^{t}\sum_{(\alpha,b)\in E_{2i}}\left(\sum_{x\in\Delta(\alpha,b)}(-1)^{a\cdot x+\beta\cdot\phi_\delta(x)}\right)^4\\
&= C_{11}^{'}+C_{12}^{'}+\cdots+C_{1t}^{'},
\end{aligned}
$$

where,

$$
C_{1j}^{'} = 2^{2m}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(\sum_{x\in\Delta(\alpha,b)}(-1)^{a\cdot x+\beta\cdot\phi_\delta(x)}\right)^4, 1\leq j\leq t.
$$

Now we claim that $C_{1j}^{'}\geq 2^{3m+3}(j|E_{2j}|)$, for all $j\in\{1,2,\cdots,t\}$. Since $C_{11}^{'}=2^{3m+3}|E_2|$ and $C_{12}^{'}\geq 2^{3m+3}(2|E_4|)$, for each $(\alpha,b)\in E_{2j}$, there exist $2j$ distinct elements $x_1,x_1+\alpha,x_2,x_2+\alpha,\ldots,x_j,x_j+\alpha\in\mathbb{F}_2^n$ such that $D_\alpha\phi_\delta(x_s)=D_\alpha\phi_\delta(x_s+\alpha)=b$, $s\in\{1,2,\ldots,j\}$. Let

$$
S_s=(-1)^{a\cdot x_s+\beta\cdot\phi_\delta(x_s)}+(-1)^{a\cdot(x_s+\alpha)+\beta\cdot\phi_\delta(x_s+\alpha)}=\left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)(-1)^{\epsilon_s},
$$

where $\epsilon_s=a\cdot x_s+\beta\cdot\phi_\delta(x_s)$, for all $s\in\{1,2,\ldots,j\}$. Thus,

$$
\begin{aligned}
C_{1j}^{'} &= 2^{2m}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}(S_1+S_2+\cdots+S_j)^4\\
&= 2^{2m}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)^4((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\cdots+(-1)^{\epsilon_j})^4\\
&= 2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\cdots+(-1)^{\epsilon_j})^4.
\end{aligned}
$$

First,

$$\begin{aligned}
&\left((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\cdots+(-1)^{\epsilon_j}\right)^4\\
=&\left(1+(-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\cdots+(-1)^{\epsilon_1+\epsilon_j}\right)^4\\
=&1+4\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\cdots+(-1)^{\epsilon_1+\epsilon_j}\right)\\
&+6\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\cdots+(-1)^{\epsilon_1+\epsilon_j}\right)^2\\
&+4\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\cdots+(-1)^{\epsilon_1+\epsilon_j}\right)^3\\
&+\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\cdots+(-1)^{\epsilon_1+\epsilon_j}\right)^4.
\end{aligned}$$

Next,

$$\begin{aligned}
&\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\cdots+(-1)^{\epsilon_1+\epsilon_j}\right)^4\\
=&\left(1+(-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\cdots+(-1)^{\epsilon_2+\epsilon_j}\right)^4\\
=&1+4\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\cdots+(-1)^{\epsilon_2+\epsilon_j}\right)\\
&+6\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\cdots+(-1)^{\epsilon_2+\epsilon_j}\right)^2\\
&+4\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\cdots+(-1)^{\epsilon_2+\epsilon_j}\right)^3\\
&+\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\cdots+(-1)^{\epsilon_2+\epsilon_j}\right)^4.
\end{aligned}$$

After $(j-2)$ similar steps, we get,

$$\left((-1)^{\epsilon_{j-2}+\epsilon_{j-1}}+(-1)^{\epsilon_{j-2}+\epsilon_j}\right)^4=\left(1+(-1)^{\epsilon_{j-1}+\epsilon_j}\right)^4=8+8(-1)^{\epsilon_{j-1}+\epsilon_j}.$$

Therefore, $\left((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\cdots+(-1)^{\epsilon_j}\right)^4=(j-2)+8+P_1=j+P$, where $P=P_1+6$ is the sum of some positive integer and terms of the form $(-1)^{\sum_{l\in E}\epsilon_l}$, $E\subseteq[j]$ with some multiplicity. Since for any $E\subseteq[j]$, $\sum_{a\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}x_l)\cdot a}$, $\sum_{a\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}x_l+\alpha)\cdot a}$, $\sum_{\beta\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}\phi_\delta(x_l))\cdot\beta}$ and $\sum_{\beta\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}\phi_\delta(x_l)+b)\cdot\beta}$ are nonnegative integers,

$$\begin{aligned}
C_{1j}^{'}&=2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)(j+P)\\
&=2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(j+P+j(-1)^{a\cdot\alpha+b\cdot\beta}+P(-1)^{a\cdot\alpha+b\cdot\beta}\right)\\
&=2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}j+2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(P+P(-1)^{a\cdot\alpha+b\cdot\beta}\right)\\
&\geq 2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}j=2^{3m+3}(j|E_{2j}|),
\end{aligned}$$

as $\sum_{a\in\mathbb{F}_2^n}\sum_{\beta\in\mathbb{F}_2^n}\left(P+P(-1)^{a\cdot\alpha+b\cdot\beta}\right)\geq 0$. Thus,

$$\begin{aligned}
C_1^{'}&=C_{11}^{'}+C_{12}^{'}+\cdots+C_{1t}^{'}\\
&\geq 2^{3m+3}(|E_2|+2|E_4|+\cdots+t|E_{2t}|)\\
&=2^{3m+n+2}(2^n-1),
\end{aligned}$$

and the theorem follows. □

The proof of the next corollary follows directly from Theorem 3.3 and Theorem 3.7.

**Corollary 3.8.** *The Gowers $U_3$ norm of a Maiorana–McFarland bent function defined as in Theorem* 3.7 *is always larger than the norm of a Maiorana–McFarland bent function obtained by using an APN permutation.*

## 4 Gowers $U_3$ norm for a class of cubic monomial function

This section is aimed at demonstrating how we envision the use of Gowers $U_3$ norm to identify the classes of functions with potentially high second-order nonlinearity. This section also shows that the largest second-order nonlinearity may not be observed within the class of bent functions. We consider a class of cubic monomial function similar to those considered by Canteaut, Charpin and Kyureghyan [2].

**Theorem 4.1.** *Let $m = 3r$, $r > 1$ be a positive integer. Let $F_r \in \mathcal{B}_m$ be a cubic Boolean function defined by*

$$F_r(x) = Tr_1^n(\lambda x^{2^{2r}+2^r+1}), \tag{16}$$

*for all $x \in \mathbb{F}_{2^m}$ where $\lambda \in \mathbb{F}_{2^r}^*$ and $f_r(x) = (-1)^{F_r(x)}$, for all $x \in \mathbb{F}_{2^m}$. Then the Gowers $U_3$ norm of $f_r$ is*

$$\|f_r\|_{U_3} = \frac{2^m + 2^r(2^m-1)}{2^{2m}}.$$

*Proof.* The Gowers $U_3$ norm of $f_r$ can be written as

$$\begin{aligned}
\|f_r\|_{U_3}^8 &= \frac{1}{2^{4m}}\left|\sum_{a,b,h,x\in\mathbb{F}_{2^m}}(-1)^{D_{a,b,h}F_r(x)}\right| \\
&= \frac{1}{2^{4m}}\left|\sum_{a,b\in\mathbb{F}_{2^m}}\sum_{h,x\in\mathbb{F}_{2^m}}(-1)^{D_{a,b}F_r(x)+D_{a,b}F_r(x+h)}\right| \\
&= \frac{1}{2^{4m}}\left|\sum_{a,b\in\mathbb{F}_{2^m}}\left(\sum_{x\in\mathbb{F}_{2^m}}(-1)^{D_{a,b}F_r(x)}\right)^2\right| \\
&= \frac{1}{2^{4m}}\left|2^{2m}\left(\sum_{a\in\mathbb{F}_{2^m}}1+\sum_{\substack{b\in\mathbb{F}_{2^m}\setminus\{0\}\\ a=0}}1+\sum_{\substack{a\in\mathbb{F}_{2^m}\setminus\{0\}\\ b=0}}1\right)+\sum_{\substack{a,b\in\mathbb{F}_{2^m}\setminus\{0\}\\ a\neq b}}\left(\sum_{x\in\mathbb{F}_{2^m}}(-1)^{D_{a,b}F_r(x)}\right)^2\right| \\
&= \frac{1}{2^{4m}}\left|2^{2m}(3\cdot 2^m-2)+\sum_{\substack{a,b\in\mathbb{F}_{2^m}\setminus\{0\}\\ a\neq b}}\left(\sum_{x\in\mathbb{F}_{2^m}}(-1)^{D_{a,b}F_r(x)}\right)^2\right|.
\end{aligned}$$

Since $\deg(D_{a,b}F_r)$ is at most 1, $D_{a,b}F_r$ is either balanced or constant. We find those nonzero $a, b \in \mathbb{F}_{2^m}$ with $a \neq b$ such that $D_{a,b}F_r(x)$ is constant for all $x \in \mathbb{F}_{2^m}$.

$$D_{a,b}F_r(x) = Tr_1^m(\lambda(a^{2^r}b+ab^{2^r})x)+Tr_1^m\left(\lambda\left((a^{2^{2r}}b^{2^r+1}+a^{2^r+1}b^{2^{2r}})+(a^{2^{2r}}+b^{2^{2r}})(a^{2^r}b+ab^{2^r})\right)\right)$$

$D_{a,b}F_r(x)$ is constant for all $x \in \mathbb{F}_{2^m}$ if and only if

$$\lambda\left(a^{2^r}b + ab^{2^r}\right) = 0 \Leftrightarrow a^{2^r}b + ab^{2^r} = 0 \Leftrightarrow \left(\frac{b}{a}\right)^{2^r-1} = 1 \Leftrightarrow \frac{b}{a} \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2 \Leftrightarrow b = \beta a$$

where $\beta \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Thus, given any $a \in \mathbb{F}_{2^m}^*$, $b$ can be chosen in $2^r - 2$ ways. Therefore, the total number of ways in which $a, b$ can be chosen is $(2^m - 1)(2^r - 2)$. Thus,

$$\|f_r\|_{U_3} = \frac{2^m + 2^r(2^m - 1)}{2^{2m}},$$

which shows the theorem. □

We compare Gowers $U_3$ norms of a cubic Maiorana–McFarland bent function, $f$ say, constructed by using APN permutations as in Theorem 3.3, and cubic monomial Boolean functions considered above. Let $m = 2n = 3r$, i.e., $n = \frac{3r}{2}$.

$$\begin{aligned}\|f_r\|_{U_3}^8 - \|f\|_{U_3}^8 &= \frac{2^m + 2^r(2^m - 1)}{2^{2m}} - \frac{7 \cdot 2^n - 6}{2^{3n}}\\ &= \frac{2^m + 2^{m+r} - 2^r - 7 \cdot 2^m + 6 \cdot 2^n}{2^{2m}}\\ &= \frac{6 \cdot 2^n + 2^m(2^r - 6) - 2^r}{2^{2m}}.\end{aligned}$$

It can be directly checked that if $r = 2$, then $\|f_r\|_{U_3}^8 < \|f\|_{U_3}^8$ and if $r \geq 3$, then $\|f_r\|_{U_3}^8 > \|f\|_{U_3}^8$. This suggests that the second-order nonlinearity of $f_r$ is greater than the one of $f$ if $m = 6$ and for $m \geq 10$ such is not the case.

There are three known affine inequivalent classes of cubic bent functions in 6 variables [13]. It is also known that all the cubic bents are affine equivalent to Maiorana-McFarland bent functions. By direct computation we have found that their second-order nonlinearities are 8, 12 and 16. Motivated by low Gowers $U_3$ norm of $F_2$, obtained by substituting $r = 2$ in (16), we have computed the second-order nonlinearity of $F_2$. We find that while it is not bent, having nonlinearity 22, its second-order nonlinearity has the maximum possible value in $\mathcal{B}_6$, namely 18. However, the reversal of the inequality sign for $r \geq 3$ indicates that this trend will not extend to 12 variables, i.e., for $r = 4$.

## 5 Further comments

The problem of constructing Boolean functions in $n$ variables with highest possible second-order nonlinearity is connected to the covering radius problem of second-order Reed–Muller codes. Both these problems are difficult and remain far from being settled. In this paper we locate some functions with low Gowers $U_3$ norms, since this is also a measure of resistance to second-order approximation of a Boolean function. This norm seems to be dependent more on the differential uniformity of the permutations associated to the Maiorana–McFarland bent functions rather than the algebraic degrees. Similarly, in the recent past, Tang, Carlet and Tang [14] have demonstrated that lower bound of second-order nonlinearities of the Maiorana–McFarland bents obtained by using APN permutations is greater than or equal to the functions considered by Gangopadhyay et al. [9]. It should be interesting to check whether the Maiorana-McFarland APN-based functions have the largest second-order nonlinearity among the class of bent functions.

**Acknowledgement:** The authors thank Palash Sarkar for suggesting the problem and for several long discussions. We are also thankful for the useful comments of the reviewers that has immensely helped us to significantly improve both technical and editorial quality of the manuscript. Bimal Mandal acknowledges IIT Roorkee for supporting his research.

# References

[1] A. Canteaut and P. Charpin, *Decomposing Bent Functions*, IEEE Trans. Inform. Theory 49(8) (2003), 2004–2019.

[2] A. Canteaut, P. Charpin and G. M. Kyureghyan, *A new class of monomial bent functions*, Finite Fields Appl. 14 (2008), 221–241.

[3] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. 15(2) (1998), 125–156.

[4] C. Carlet, *On Cryptographic Propagation Criteria for Boolean Functions*, Information and Computation 151(1-2) (1999), 32–56.

[5] C. Carlet, *Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications*, IEEE Trans. Inform. Theory 54 (3) (2008), 1262–1272.

[6] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monograph: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge Univ. Press, Yves Crama and Peter L. Hammer (eds.) (2010), 257–397.

[7] V. Y-W. Chen, *The Gowers' norm in the testing of Boolean functions*, Ph.D. Thesis, Massachusetts Institute of Technology, June 2009.

[8] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, 2nd Ed. (Academic Press, San Diego, CA, 2017); 1st Ed., 2009.

[9] S. Gangopadhyay, S. Sarkar and R. Telang, *On the lower bounds of the second order nonlinearities of some Boolean functions*, Inform. Sci. 180 (2010), 266–273.

[10] S. Gangopadhyay,*Affine inequivalence of cubic Maiorana–McFarland type bent functions*, Discrete Appl. Math., 161(7-8) (2013), 1141–1146.

[11] T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. 11(3) (2001), 465–588.

[12] B. Green and T. Tao, *An inverse theorem for the Gowers' $U^3(G)$ norm*, arXiv:0503014v3 [math.NT], 5 Aug 2006.

[13] O. S. Rothaus, *On bent functions*, J. Combin. Theory – Ser. A 20 (1976), 300–305.

[14] D. Tang, C. Carlet and X. Tang, *On the second-order nonlinearities of some bent functions*, Inform. Sci. 223 (2013), 322–330.

[15] T. Tao, *Structure and randomness in combinatorics*, arXiv:0707.4269v2 [math.CO], 3 Aug 2007.