New Results on the Gowers Uniformity Norm of S-boxes

Deng Tang

1 Preliminaries

For any positive integer n, $\mathbb{F}_2^n$ denotes the vector space of n-tuples over the finite field $\mathbb{F}_2 = \{0, 1\}$. By $\mathbb{F}_{2^n}$, we denote the finite field of order 2^n. For simplicity, we denote by $\mathbb{F}_2^{n*}$ the set $\mathbb{F}_2^n \setminus \{\mathbf{0}_n\}$ where $\mathbf{0}_n$ is the all-zero vector, and $\mathbb{F}_{2^n}^*$ denotes the set $\mathbb{F}_{2^n} \setminus \{0\}$. It is known that the vector space $\mathbb{F}_2^n$ is isomorphic to the finite field $\mathbb{F}_{2^n}$ through the choice of some basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Indeed, if $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then every vector $x = (x_1, x_2 \ldots, x_n)$ of $\mathbb{F}_2^n$ can be identified with the element $x_1\lambda_1 + x_2\lambda_2 + \cdots + x_n\lambda_n \in \mathbb{F}_{2^n}$. The finite field $\mathbb{F}_{2^n}$ can then be viewed as an n-dimensional vector space over $\mathbb{F}_2$. The Hamming weight of an element $x \in \mathbb{F}_2^n$, denoted by $wt(x)$, is defined by $wt(x) = \sum_{i=1}^{n} x_i$, where the sum is over the integers. The cardinality of a set A is denoted by $\#A$. The inner product of $x, y \in \mathbb{F}_2^n$ is defined as $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$.

1.1 S-boxes over vector space $\mathbb{F}_2^n$ and finite field $\mathbb{F}_{2^n}$

Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function in n variables. We represent the set of all n-variable Boolean functions by $\mathcal{B}_n$. An $n \times m$ S-box $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, which is often called an (n, m)-function or a vectorial Boolean function if the values n and m are omitted, can be considered as m Boolean functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, where $1 \le i \le m$, such that $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ for all $x \in \mathbb{F}_2^n$. In addition, f_i's are called the coordinate functions of F. Further, the Boolean functions, which are the linear combinations with non all-zero coefficients of the coordinate functions of F, are called the component functions of F. The component functions of F can be expressed as $v \cdot F$, denoted by F_v, where $v \in \mathbb{F}_2^{m*}$. If we identify every element of $\mathbb{F}_2^m$ with an element of the finite field $\mathbb{F}_{2^m}$, then the nonzero component functions F_v of F can be expressed as $\mathrm{Tr}_1^m(vF)$, where $v \in \mathbb{F}_{2^m}^*$ and $\mathrm{Tr}_1^m(x) = \sum_{i=0}^{m-1} x^{2^i}$.

1.2 Cryptographic properties of S-boxes

We now briefly review the basic definitions regarding the cryptographic properties of Boolean functions and then extend those definitions to S-boxes by using component functions. The Hamming weight of $f \in \mathcal{B}_n$ is defined as the size of the support of

f in which the support of f is defined as $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) \neq 0\}$. A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if the cardinality of the support set of f is 2^{n-1}. Given two Boolean functions f and g in n variables, the Hamming distance between f and g is defined as $d_H(f,g) = \#\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}$. Any Boolean function f in n variables can also be expressed in terms of a polynomial in $\mathbb{F}_2[x_1,\ldots,x_n]/(x_1^2+x_1,\ldots,x_n^2+x_n)$:

$$f(x_1,\ldots,x_n) \;=\; \sum_{u\in\mathbb{F}_2^n} a_u\Big(\prod_{j=1}^{n} x_j^{u_j}\Big) = \sum_{u\in\mathbb{F}_2^n} a_u x^u,$$

where $a_u \in \mathbb{F}_2$. This representation is called the algebraic normal form (ANF) of f. The algebraic degree, denoted by $\deg(f)$, is the maximal value of $wt(u)$ such that $a_u \neq 0$. The algebraic degree of an S-box is defined as the maximum algebraic degree of its coordinate functions and it is also the maximum algebraic degree of its component functions. Recall that $\mathbb{F}_{2^n}$ is isomorphic as a $\mathbb{F}_2$-vector space to $\mathbb{F}_2^n$. A Boolean function defined over $\mathbb{F}_{2^n}$ can be uniquely expressed by a univariate polynomial over $\mathbb{F}_{2^n}[x]/(x^{2^n}+x)$:

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_0, a_{2^n-1} \in \mathbb{F}_2$, $a_i \in \mathbb{F}_{2^n}$ for $1 \leq i < 2^n - 1$ such that $a_i = a_{2i\,[\mathrm{mod}\ 2^n-1]}$. The algebraic degree $\deg(f)$ under this representation is equal to $\max\{wt(\bar{i}) : a_i \neq 0, 0 \leq i < 2^n\}$, where $\bar{i}$ is the binary expansion of i (see e.g., [?]). The r-th order nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is defined as its minimum Hamming distance from all the n-variable Boolean functions of degree at most r, $\mathrm{nl}_r(f) = \min_{g\in\mathcal{B}_n,\,\deg(g)\leq r}(d_H(f,g))$.

The nonlinearity profile of a function f is the sequence of those values $nl_r(f)$ for r ranging from integers 1 to $n-1$. The first order nonlinearity of f is simply called the nonlinearity of f and is denoted by $\mathrm{nl}(f)$. The nonlinearity $\mathrm{nl}(f)$ is the minimum Hamming distance between f and all the functions with algebraic degree at most 1. The nonlinearity of f can also be expressed by means of its Walsh–Hadamard transform. Let $x = (x_1, x_2, \ldots, x_n)$ and $\omega = (\omega_1, \omega_2, \ldots, \omega_n)$ both belonging to $\mathbb{F}_2^n$ and let $x \cdot \omega$ be the usual inner product in $\mathbb{F}_2^n$, then the Walsh–Hadamard transform of $f \in \mathcal{B}_n$ at point ω is defined by

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

The multiset constituted by the values of the Walsh–Hadamard transform is called the Walsh–Hadamard spectrum of f. Over $\mathbb{F}_{2^n}$, the Walsh–Hadamard transform of

f at point α can be defined by $\widehat{f}(\alpha) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(\alpha x)}$. It can be easily seen that, for any Boolean function $f \in \mathcal{B}_n$, its nonlinearity can be computed as

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n}|\widehat{f}(\omega)|, \tag{1}$$

when f is defined over $\mathbb{F}_2^n$, and $\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\max_{\alpha\in\mathbb{F}_{2^n}}|\widehat{f}(\alpha)|$, when f is defined over $\mathbb{F}_{2^n}$. The nonlinearity of an (n,m)-function F is defined by the minimum nonlineartiy of all its component functions, that is,

$$\mathrm{nl}(F) = \min_{\alpha\in\mathbb{F}_2^{m*}}\{\mathrm{nl}(\alpha\cdot F)\} = 2^{n-1} - \frac{1}{2}\max_{\beta\in\mathbb{F}_2^n,\alpha\in\mathbb{F}_2^{m*}}|\widehat{\alpha\cdot F}(\beta)|.$$

The nonlinearity $\mathrm{nl}(F)$ is upper bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$ when $m = n$. This upper bound is tight for odd $n = m$. For even $m = n$, the best known value of the nonlinearity of (n,n)-functions is $2^{n-1} - 2^{\frac{n}{2}}$. The r-th order nonlinearity of an (n,m)-function F is the minimum r-th order nonlineartiy of all its component functions.

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 $D_a f(x) = f(x+a) + f(x)$. By successively taking derivatives with respect to any k linearly independent vectors in $\mathbb{F}_2^n$ we obtain the kth-derivative of $f \in \mathcal{B}_n$. Suppose $u_1,\ldots,u_k$ are linearly independent vectors of $\mathbb{F}_2^n$ generating the subspace V_k 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_k, is defined as

$$D_{V_k}f(x) = D_{u_1,\ldots,u_k}f(x) = \sum_{(a_1,\ldots,a_k)\in\mathbb{F}_2^k} f(x + a_1u_1 + \cdots + a_ku_k) = \sum_{v\in V_k} f(x+v).$$

It can be seen that $D_{V_k}f$ is independent of the choice of basis for V_k. Similar with Boolean functions, we can define kth-derivative for S-boxes. The kth-derivative of an (n,m)-function F with respect to V_k is defined as $D_{V_k}F(x) = \sum_{v\in V_k}F(x+v)$. The k-th order differential of an S-box F [**?**, Definition 4.2] is related to the number of inputs $x \in \mathbb{F}_2^n$ such that

$$\sum_{v\in V_k} F(x+v) = \beta, \quad \beta \in \mathbb{F}_2^m. \tag{2}$$

Definition 1. *An $n\times m$ S-box F is called k-th order differentially δ_k-uniform if the equation $\sum_{v\in V_k}F(x+v) = \beta$ has at most δ_k solutions for all k-dimensional vector space V_k and $\beta \in \mathbb{F}_2^m$. Accordingly, δ_k is called k-th order differential uniformity of F.*

It is clear that if $x \in \mathbb{F}_2^n$ satisfies (2), then $x + v$, for any $v \in V$, satisfies (2) as well. Thus, the cardinality of the solution spaces of (2) for any k-dimensional subspace of $\mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^m$ is divisible by 2^k. The optimal value of δ_k is 2^k, and then the cardinality of the set $\{\sum_{v \in V_k} F(x+v) : x \in \mathbb{F}_2^n\}$ is 2^{n-k} for any k dimensional subspace V_k of $\mathbb{F}_2^n$.

Remark 1. *Let δ_k be the k-th order differential uniformity of an S-box F. Then $\delta_k \equiv 0 \pmod{2^k}$.*

The first order differential uniformity δ_1, simply denoted by δ, of F is well-known as differential uniformity which was introduced by Nyberg in [**?**] to evaluate the resistance of F to the differential attack [**?**]. The smaller δ is, the better is the contribution of F to resist the differential attack. The values of δ are always even since if x is a solution of equation $F(x) + F(x + \gamma) = \beta$ then $x + \gamma$ is also a solution. This implies that the differential uniformity of an (n, m)-function is greater or equal to 2^{n-m} and for $n = m$ the smallest possible value is 2. A function achieving this value is called an *almost perfect nonlinear* (APN) function. A cryptographically desirable S-box is expected to have low differential uniformity ($\delta = 2$ is optimal, $\delta = 4$ is good), which makes the probability of occurrence of a particular pair of input and output differences (γ, β) low, and hence provides resistance against differential cryptanalysis. For every k-dimensional vector space V_k and every $\beta \in \mathbb{F}_2^m$, we denote by $\delta_k(V_k, \beta)$ the size of the set $\{x \in \mathbb{F}_2^n : \sum_{v \in V_k} F(x + v) = \beta\}$ and therefore δ_k equals the maximum value of $\delta_k(V_k, \beta)$. The multi-set $[\delta_k(V_k, \beta) : V_k \subseteq \mathbb{F}_2^n, \dim(V_k) = k, \beta \in \mathbb{F}_2^m]$ is called the *k-th order differential spectrum* of F. For $k = 1$, this spectrum is represented as a well known table, called the difference distribution table (DDT), and the maximum value of the DDT is therefore the differential uniformity of F.

1.3 Gowers uniformity norms

In this section we introduce Gowers uniformity norms. Let $f : V \to \mathbb{R}$ be any function on a finite set V and $B \subseteq V$, say. Then $\mathbb{E}_{x \in B}[f(x)] = \frac{1}{\#B} \sum_{x \in B} f(x)$ is defined as the average of f over B. Gowers [**?**] introduced a new measure for Boolean functions, called the Gowers uniformity norms.

Definition 2. *[**?**, 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*

$$\|f\|_{U_k} = \left(\mathbb{E}_{x, u_1, \ldots, u_k \in \mathbb{F}_2^n} \left[\prod_{S \subseteq \{1,2,\ldots,k\}} f\left(x + \sum_{i \in S} u_i \right) \right] \right)^{\frac{1}{2^k}}. \tag{3}$$

Since for $k = 1$, Gowers uniformity norm may not be positive defined, it is a semi-norm for $k = 1$, and for other $k \geq 2$ Gowers norms satisfy all the norm properties. Gowers norms for $k = 1, 2, 3$ are explicitly presented below (see [?, ?]).

$$\begin{aligned}
\|f\|_{U_1} &= \mid \mathbb{E}_{x,u \in \mathbb{F}_2^n}[f(x)f(x+u)] \mid^{1/2} = \mid \mathbb{E}_{x \in \mathbb{F}_2^n}[f(x)] \mid . \\
\|f\|_{U_2} &= \mid \mathbb{E}_{x,u_1,u_2 \in \mathbb{F}_2^n}[f(x)f(x+u_1)f(x+u_2)f(x+u_1+u_2)] \mid^{1/4} \\
&= \mid \mathbb{E}_{u_1 \in \mathbb{F}_2^n} \mid \mathbb{E}_{x \in \mathbb{F}_2^n}[f(x)f(x+u_1)] \mid^2 \mid^{1/4} . \\
\|f\|_{U_3} &= \mid \mathbb{E}_{x,u_1,u_2,u_3 \in \mathbb{F}_2^n}[f(x)f(x+u_1)f(x+u_2)f(x+u_1+u_2) \\
&\qquad \times f(x+u_3)f(x+u_1+u_3)f(x+u_2+u_3)f(x+u_1+u_2+u_3)] \mid^{1/8} .
\end{aligned}$$

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

Theorem 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 $\|f\|_{U_{k+1}} \geq \epsilon$.*

Suppose $f \in \mathcal{B}_n$. From the above results, we get $nl_k(f) \leq 2^{n-1}(1-\epsilon) \Rightarrow \|(-1)^f\|_{U_{k+1}} \geq \epsilon$, that is, if the k-th order nonlinearity of a Boolean function is bounded above by high (low) value, then its Gowers U_{k+1} norm is bounded below by low (high) value. We know [?, ?] that the converse of Theorem 1 is also true for $k = 1, 2$. Samorodnitsky [?] proved that a Boolean function with a large Gowers U_3 norm is somewhat close to a quadratic polynomial.

Theorem 2. *[?, Theorem 2.3] Let $f \in \mathcal{B}_n$ such that $\|(-1)^f\|_{U_3} \geq \varepsilon$, $\varepsilon \geq 0$. Then there exists a quadratic Boolean function g such that the distance between f and g is at most $\frac{1}{2} - \varepsilon'$, where $\varepsilon' = \Omega(e^{-\varepsilon^{-C}})$ for an absolute constant C.*

Thus, the second order nonlinearity of a Boolean function is bounded above by high (low) value if and only if its Gowers U_3 norm is bounded below by low (high) value. Note that for any n-variable Boolean function g, $(-1)^g \in \{\pm 1\}$ is a two-valued function. Gangopadhyay et al. [?] first derived Gowers U_3 norms of some classes of Boolean functions with certain properties. Let n be a positive integer and f be an arbitrary n-variable Boolean function. One may note that for the two-valued function $(-1)^f \in \{-1, 1\} \subseteq \mathbb{R}$, we have

$$\left\|(-1)^f\right\|_{U_3} = 2^{-\frac{n}{2}} \left| \sum_{(\tau,\gamma) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+\tau)+f(x+\gamma)+f(x+\tau+\gamma)} \right)^2 \right|^{\frac{1}{8}} . \tag{4}$$

Lemma 1. *[?] For any integer $n > 0$, $\widehat{I_1}(1) = 1 - \sum_{t=0}^{\lfloor n/2 \rfloor} (-1)^{n-t} \frac{n}{n-t} \binom{n-t}{t} 2^t$.*

2 Gowers U_3 norm of the multiplicative inverse function

In this section we calculate the Gowers U_3 norm of the multiplicative inverse function. Let $f \in \mathcal{B}_n$ be any quadratic Boolean function. Since $\deg(f) \leq 2$, any second derivative of f is constant. Thus, from (4) we have $\|(-1)^f\|_{U_3} = 1$. Let us now consider the case of S-boxes. Suppose F is an S-box of input length n and output length m, and $f_i \in \mathcal{B}_n, 1 \leq i \leq m$, is the i-th coordinate function of F. Any nonzero component function of F can be written by $a \cdot F$, $a \in \mathbb{F}_2^{m*}$. Let us first define the Gowers uniformity norms for vectorial Boolean functions.

Definition 3 ([?]). *Let n, m be two positive integers and F be an (n, m)-function. For any positive integer k, the Gowers U_k norm of $(-1)^F$ is defined by*

$$\|(-1)^F\|_{U_k} = \max_{a\in\mathbb{F}_2^{m*}} \|(-1)^{a\cdot F}\|_{U_k} = \max_{a\in\mathbb{F}_2^{m*}} \left(\mathbb{E}_{x,u_1,\dots,u_k\in\mathbb{F}_2^n}\left[(-1)^{\sum_{S\subseteq\{1,2,\dots,k\}} a\cdot F\left(x+\sum_{i\in S} u_i\right)}\right]\right)^{\frac{1}{2^k}}.$$

Note that, it is clear that F being a vectorial Boolean function, $(-1)^F$ has no specific meaning. This is just a notation following the idea of single output Boolean function. Thus in the following text in this paper, $(-1)^F$ should only be considered as a notation. In particular for $k = 3$, the Gowers U_3 norm of $(-1)^F$ is

$$\begin{aligned}\|(-1)^F\|_{U_3} &= \max_{a\in\mathbb{F}_2^{m*}} \|(-1)^{a\cdot F}\|_{U_3} \\ &= 2^{-\frac{n}{2}} \max_{a\in\mathbb{F}_2^{m*}} \left|\sum_{(\tau,\gamma)\in\mathbb{F}_{2^n}^2} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{a\cdot F(x)+a\cdot F(x+\tau)+a\cdot F(x+\gamma)+a\cdot F(x+\tau+\gamma)}\right)^2\right|^{\frac{1}{8}}.\end{aligned}$$

Thus, the kth-dimension Gowers uniformity norm of an S-box is determined by the maximum kth-dimension Gowers uniformity norm among all the component functions.

Theorem 3 ([?]). *For any positive integer $n \geq 4$, we have*

$$\left\|(-1)^{I_1}\right\|_{U_3} = 2^{-\frac{n}{2}}\left|3\cdot 2^{3n+1} + 2^{n+3}\cdot\left[(-1)^n\left(3\widehat{I_1}(1) - 10\right) - 6\right]\right|^{\frac{1}{8}},$$

where $\widehat{I_1}(1)$ can be computed using Lemma 1.

3 Main results

Lemma 2. *Let F be an arbitrary (n,n)-function. For any $\gamma, \eta, \omega \in \mathbb{F}_2^n$, we define*

$$\mathcal{N}(\gamma,\eta,\omega) = \#\left\{x \in \mathbb{F}_{2^n} : F(x) + F(x+\gamma) + F(x+\eta) + F(x+\gamma+\eta) = \omega\right\}.$$

Then we have

$$\sum_{\gamma,\eta,\omega \in \mathbb{F}_2^n} \mathcal{N}(\gamma,\eta,\omega) = 2^{3n}$$

and

$$\sum_{\gamma,\eta,v \in \mathbb{F}_2^n} \left((-1)^{v\cdot(F(x)+F(x+\gamma)+F(x+\eta)+F(x+\gamma+\eta))}\right)^2 = 2^n \sum_{\gamma,\eta,\omega \in \mathbb{F}_2^n} \mathcal{N}(\gamma,\eta,\omega)^2.$$

Proof. Note that for any $v \in \mathbb{F}_2^n$ we have

$$\sum_{\gamma,\eta \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{v\cdot(F(x)+F(x+\gamma)+F(x+\eta)+F(x+\gamma+\eta))} = \sum_{\gamma,\eta \in \mathbb{F}_2^n} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{v\cdot\omega} \mathcal{N}(\gamma,\eta,\omega).$$

On the one hand, by applying this relation with $v = 0$, we get $\sum_{\gamma,\eta,\omega \in \mathbb{F}_2^n} \mathcal{N}(\gamma,\eta,\omega) = 2^{3n}$. On the other hand, by applying this relation with the Parseval's relation, we immediately get our rest assertion. This completes the proof. $\square$

Lemma 3. *Let F be an arbitrary (n,n)-function and $T = \{\mathbf{0}_n, \eta_1, \eta_2, \cdots, \eta_t\} \subseteq \mathbb{F}_2^n$, where $\eta_1, \eta_2, \cdots, \eta_t$ are any t vectors in $\mathbb{F}_2^{n*}$. For any $\omega \in \mathbb{F}_2^n$, we define*

$$\mathcal{N}_\omega(T) = \#\left\{x \in \mathbb{F}_{2^n} : \sum_{y \in T} F(x+y) = \omega\right\}.$$

Then we have

$$\sum_{\eta_1,\eta_2,\ldots,\eta_t \in \mathbb{F}_2^n} \sum_{\omega \in \mathbb{F}_2^n} \mathcal{N}_\omega(T) = 2^{n(t+1)}$$

and

$$\sum_{\eta_1,\eta_2,\cdots,\eta_t,v \in \mathbb{F}_2^n} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v\cdot\left(\sum_{y\in T} F(x+y)\right)}\right)^2 = 2^n \sum_{\eta_1,\eta_2,\ldots,\eta_t \in \mathbb{F}_2^n} \sum_{\omega \in \mathbb{F}_2^n} \left(\mathcal{N}_\omega(T)\right)^2.$$

Proof. Note that for any $v \in \mathbb{F}_2^n$ we have

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{v\cdot\left(\sum_{y\in T} F(x+y)\right)} = \sum_{\omega \in \mathbb{F}_2^n} (-1)^{v\cdot\omega} \mathcal{N}_\omega(T). \tag{5}$$

When $v = 0$ and all η_i range over $\mathbb{F}_2^n$ for $i = 1, 2, ..., t$, we have $\sum_{\eta_1,\eta_2,\ldots,\eta_t \in \mathbb{F}_2^n} \sum_{\omega \in \mathbb{F}_2^n} \mathcal{N}_\omega(T) = \sum_{x \in \mathbb{F}_2^n} (-1)^0 = 2^{n(t+1)}$. Furthermore, we can apply Parseval's relation to the right part of equation (5) since actually it is the value of Fourier Transform of $\mathcal{N}_\omega(T)$ at the point v. Then, we have

$$\sum_{v\in\mathbb{F}_2^n}\left(\sum_{\omega\in\mathbb{F}_2^n}(-1)^{v\cdot\omega}\mathcal{N}_\omega(T)\right)^2 = 2^n\sum_{\omega\in\mathbb{F}_2^n}\left(\mathcal{N}_\omega(T)\right)^2,$$

□

Corollary 1. *If f is a power permutation over the finite field $\mathbb{F}_{2^n}$, then*

Assume $f = x^d$ with $\gcd(d, 2^n-1) = 1$ is a power permutation over the finite field $\mathbb{F}_{2^n}$, then for all $v \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}\sum_{\eta_1,\eta_2,\cdots,\eta_t\in\mathbb{F}_{2^n}}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}_1^n\left(v\left(\sum_{y\in T}f(x+y)\right)\right)}\right)^2 &= \sum_{\eta_1,\eta_2,\cdots,\eta_t\in\mathbb{F}_{2^n}}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}_1^n\left(v\left(\sum_{y\in T}(x+y)^d\right)\right)}\right)^2\\ &= \sum_{\eta_1,\eta_2,\cdots,\eta_t\in\mathbb{F}_{2^n}}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}_1^n\left(\sum_{y\in T}\left(v^{\frac{1}{d}}x+v^{\frac{1}{d}}y\right)^d\right)}\right)^2\\ &= \sum_{\eta_1,\eta_2,\cdots,\eta_t\in\mathbb{F}_{2^n}}\left(\sum_{x'\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}_1^n\left(\sum_{y'\in T}(x'+y')^d\right)}\right)^2,\end{aligned}$$

which implies that the Gowers U_3 Norm of a power permutation is uniquely defined by the entries $\sum_{\eta_1,\eta_2,\cdots,\eta_t\in\mathbb{F}_{2^n}}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{tr}_1^n\left(\sum_{y\in T}f(x+y)\right)}\right)^2$.

Besides,

By equation (4) and Theorem 3, we can get

The Bracken-Leander function is a cubic permutation with differential uniformity 4. In the following, we determine the low bound of second-order of the Bracken-Leander function.

Theorem 4. *Let $F(x) = x^d \in \mathbb{F}_{2^n}[x]$, where $d = q^2+q+1$, $q = 2^m$ and $n = 4m$. Then for any nonzero u, v, the second-order*

Proof. For any $\gamma, \eta, \omega \in \mathbb{F}_{2^n}$, we have

$$\mathcal{N}_F(\gamma,\eta,\omega) = \#\left\{x\in\mathbb{F}_{2^n} : x^d+(x+\gamma)^d+(x+\eta)^d+(x+\gamma+\eta)^d = \omega\right\}.$$

First consider the simple cases, such that $\gamma = 0, \eta \neq 0$ or $\eta = 0, \gamma \neq 0$ or $\gamma = \eta \in \mathbb{F}_{2^n}$. In those three cases, it's easy to get that $\mathcal{N}_F(\gamma,\eta,\omega) = \#\left\{x\in\mathbb{F}_{2^n} : \omega = 0\right\}$.

So we have for $\gamma = 0, \eta \neq 0$ or $\eta = 0, \gamma \neq 0$ or $\gamma = \eta \in \mathbb{F}_{2^n}$, when ω ranges over $\mathbb{F}_{2^n}$, we have

$$\mathcal{N}_F(\gamma, \eta, \omega) = \begin{cases} 0, & (2^n - 1)(3 \cdot 2^n - 2) \text{ times} \\ 2^n, & (3 \cdot 2^n - 2) \text{ times} \end{cases} \tag{6}$$

Then for those $\gamma, \eta \in \mathbb{F}_{2^n}^*$ such that $\gamma \neq \eta$, we can rewrite $\mathcal{N}_F(\gamma, \eta, \omega)$ as

$$\mathcal{N}_F(\gamma, \eta, \omega') = \# \{x \in \mathbb{F}_{2^n} : f_{\gamma,\eta}(x) = \omega'\}$$

where

$$f_{\gamma,\eta}(x) = (\gamma^q \eta + \gamma \eta^q)\, x^{q^2} + \left(\gamma^{q^2} \eta + \gamma \eta^{q^2}\right) x^q + \left(\gamma^{q^2} \eta^q + \gamma^q \eta^{q^2}\right) x \tag{7}$$

and

$$\omega' = \omega + (\gamma + \eta)^{q^2+q+1} + \gamma^{q^2+q+1} + \eta^{q^2+q+1}.$$

Therefore, we consider $\mathcal{N}_F(\gamma, \eta, \omega')$ for all $\gamma, \eta, \omega \in \mathbb{F}_{2^n}$.

For equation (7) and for all $\omega \in \mathbb{F}_{2^n}$, we have

$$(\gamma^q \eta + \gamma \eta^q)\, x^{q^2} + \left(\gamma^{q^2} \eta + \gamma \eta^{q^2}\right) x^q + \left(\gamma^{q^2} \eta^q + \gamma^q \eta^{q^2}\right) x = \omega. \tag{8}$$

(1) If $\gamma^q \eta + \gamma \eta^q = 0$, i.e. $\frac{\gamma}{\eta} \in \mathbb{F}_q \setminus \mathbb{F}_2$, coefficients of equaiton (8) become zero, then the number of solutions of equaiton (8) is 0 if $\omega \neq 0$ and 2^n otherwise.

(2) If $\gamma^q \eta + \gamma \eta^q \neq 0$, i.e. $\frac{\gamma}{\eta} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, divides equation (8) by η^{q^2+q+1}, then we have

$$(\theta^q + \theta)\, y^{q^2} + \left(\theta^{q^2} + \theta\right) y^q + \left(\theta^{q^2} + \theta^q\right) y = \alpha, \tag{9}$$

where $\theta = \frac{\gamma}{\eta} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $y = \frac{x}{\eta}$ and $\alpha = \frac{\omega}{\eta^{q^2+q+1}}$.

Since

$$\begin{aligned} & (\theta^q + \theta)\, y^{q^2} + \left(\theta^{q^2} + \theta^q + \theta^q + \theta\right) y^q + \left(\theta^{q^2} + \theta^q\right) y \\ =& (\theta^q + \theta)\,(y^{q^2} + y^q) + \left(\theta^{q^2} + \theta^q\right)(y^q + y) \\ =& (\theta^q + \theta)\,(y^q + y)^q + (\theta^q + \theta)^q\,(y^q + y) \\ =& (\theta^q + \theta)^{q+1} \left[\left(\frac{y^q + y}{\theta^q + \theta} \right)^q + \frac{y^q + y}{\theta^q + \theta} \right] \\ =& \alpha. \end{aligned}$$

Equation (9) becomes

$$z^q + z = \beta \tag{10}$$

where $z = \frac{y^q+y}{\theta^q+\theta}$ and $\beta = \frac{\alpha}{(\theta^q+\theta)^{q+1}}$.

Note that both $y^q + y, z^q + z$ are q to 1 linearized polynomials, so when y ranges over $\mathbb{F}_{2^n}$, we have $2^{3m} = 2^n/q$ different $z = \frac{y^q+y}{\theta^q+\theta}$. And those z lead to $2^{2m} = 2^{3m}/q$ different β.

Indeed, if there exist z_1, z_2 such that $z_1^q+z_1 = z_2^q+z_2 = \beta$. we have $z_1+z_2 \in \mathbb{F}_q$, in other words, there are two y_1, y_2 such that $z_1 = \frac{y_1^q+y_1}{\theta^q+\theta}$ and $z_2 = \frac{y_2^q+y_2}{\theta^q+\theta}$, satisfying $(y_1 + y_2)^q + (y_1 + y_2) \in (\theta^q + \theta)\,\mathbb{F}_q$. Hence we assume $(y_1 + y_2)^q + (y_1 + y_2) = (\theta^q + \theta)\,v$ for $v \in \mathbb{F}_q$, so

$$(y_1 + y_2 + \theta v)^q + (y_1 + y_2 + \theta v) = 0,$$

implies that $y_1 + y_2 \in \theta v + \mathbb{F}_q$. In other words, if equation (9) has solutions, then the number of solutions is 2^{2m}.

Therefore, we obtain that there are 2^{2m} ω such that the number of solutions of equation (8) is 2^{2m}, besides, $2^n - 2^{2m}$ is the number of ω where equation (8) cannnot have solutions.

Therefore, for all $\gamma, \eta \in \mathbb{F}_{2^n}^*$ with $\gamma \neq \eta$, when ω ranges over $\mathbb{F}_{2^n}$, we have

(1) If $\frac{\gamma}{\eta} \in \mathbb{F}_q \setminus \mathbb{F}_2$,

$$\mathcal{N}_F(\gamma, \eta, \omega) = \begin{cases} 0, & 2^n - 1 \text{ times} \\ 2^n, & 1 \text{ times}, \end{cases} \tag{11}$$

(2) If $\frac{\gamma}{\eta} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$,

$$\mathcal{N}_F(\gamma, \eta, \omega) = \begin{cases} 0, & 2^n - 2^{2m} \text{ times} \\ 2^{2m}, & 2^{2m} \text{ times}, \end{cases} \tag{12}$$

So we conclude that for $\gamma, \eta \in \mathbb{F}_{2^n}^*$ and $\omega \in \mathbb{F}_{2^n}$, we have

$$\mathcal{N}_F(\gamma, \eta, \omega) = \begin{cases} 0, & (2^n - 1)(2^n - 1)(2^m - 2) + (2^n - 2^{2m})(2^n - 1)(2^n - 2^m) \text{ times} \\ 2^{2m}, & 2^{2m}(2^n - 1)(2^n - 2^m) \text{ times} \\ 2^n, & (2^n - 1)(2^m - 2) \text{ times} \end{cases}$$

Combine two results of $\mathcal{N}_F(\gamma, \eta, \omega)$, when γ, η, ω range over $\mathbb{F}_{2^n}$, we have

$$\mathcal{N}_F(\gamma, \eta, \omega) = \begin{cases} 0, & (2^n - 1)\left[(2^n - 1)(2^m - 2) + (2^n - 2^{2m})(2^n - 2^m) + 3 \cdot 2^n - 2\right] \text{ times} \\ 2^{2m}, & 2^{2m}(2^n - 1)(2^n - 2^m) \text{ times} \\ 2^n, & (2^n - 1)(2^m - 2) + 3 \cdot 2^n - 2 \text{ times} \end{cases}$$

□