Further Cryptographic Properties of the Multiplicative Inverse Function

Deng Tang[1,2], Bimal Mandal[3], and Subhamoy Maitra[4]

[1] School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China
[3] Department of Mathematics, Indian Institute of Technology Madras,
Chennai,600036, India
[4] Indian Statistical Institute, Kolkata, 700108, India
dtang@foxmail.com, bimalmandal90@gmail.com, subho@isical.ac.in

Abstract. Differential analysis is an important cryptanalytic technique on block ciphers. In one form, this measures the probability of occurrence of the differences between certain inputs vectors and the corresponding outputs vectors. For this analysis, the constituent S-boxes of Block cipher need to be studied carefully. In this direction, we derive further cryptographic properties of inverse function, especially higher-order differential properties here. This improves certain results of Boukerrou et al [ToSC 2020(1)]. We prove that inverse function defined over $\mathbb{F}_{2^n}$ has an error (bias) in its second-oder differential spectrum with probability $\frac{1}{2^{n-2}}$, and that error occurs in more than one places. To the best of our knowledge, this result was not known earlier. Further, for the first time, we analyze the Gowers uniformity norm of S-boxes which is also a measure of resistance to higher order approximations. Finally, the bounds related to the nonlinearity profile of multiplicative inverse function are derived using both Gowers U_3 norm and Walsh–Hadamard spectrum. Some of our findings provide slightly improved bounds over the work of Carlet [IEEE-IT, 2008]. All our results might have implications towards non-randomness of a block cipher where the inverse function is used as a primitive.

Keywords: Block Cipher, Boolean function, Differential uniformity, Gowers uniformity norm, Nonlinearity, S-box.

1 Introduction

Towards designing secure symmetric ciphers, especially block ciphers, S-boxes are used as the basic building blocks. Cryptanalysis on such ciphers are broadly considered in two directions. One is differential cryptanalysis [2], and the other one is linear cryptanalysis [27]. The basic idea of differential cryptanalysis of a cipher E is to measure the probability of occurance of input messages M satisfying $E(M) + E(M + \varDelta) = \delta$, where $\varDelta$ and δ are inputs and corresponding outputs differences, respectively. This probability with significant value is hard to find for some ciphers when we consider a certain rounds. That is, well defined ciphers may not have an “easy to find” differential path.

One of the most important attacks on block ciphers is the boomerang attack [36], and recently, Cid *et al.* [12] significantly improved this attack by introducing the boomerang connectivity table (BCT) on bijective S-boxes. Boukerrou *et al.* [5] extended this idea to Feistal ciphers, where the S-boxes may not be bijective, and introduced the Feistal Boomerang connectivity table (FBCT). The coefficient of FBCT is related to the number of vanishing second-order derivative of S-boxes used in the cipher. Here, the authors consider the inputs vectors that have zero second-order derivative. However, there are some particular cases where we do not get discover such distinguisher, that is, the number of input vectors that have zero second-order derivative at non trivial points is very low or may be zero. For example, if we consider an APN S-box, all the non trivial coefficients at FBCT is 0, and for inverse function in even variables, it is 4. However, it might happen that we get a sufficiently larger value at the extended FBCT table by considering non zero second-order derivatives. In this direction, Nyberg [29] extended the boomerang connectivity table by considering all 2^n BCTs. Langford and Hellman [24] first proposed the differential-linear cryptanalysis which is a combination of differential and linear distinguishers. Many block ciphers [4,13,18,25] are attacked using this cryptanalytic approach. Bar-On *et al.* [1] proposed a new connectivity table of S-boxes, differential-linear connectivity table (DLCT), to obtain a good differential-linear distinguisher. Recently, a new class of S-boxes with very low differential-linear uniformity has been constructed [35], i.e., those functions should have supposedly good resistance against the differential-linear cryptanalysis. Very recently, Boukerrou *et al.* [5] derived a relation between the DLCT and Feistel Boomerang connectivity table (FBCT). To provide related references, Daemen *et al.* [14] introduced the concept of integral distinguisher to evaluate the security of a block cipher SQUARE. Later Knudsen *et al.* [19] formalized this concept and proved that AES has the 4-round integral distinguishers with 2^{32} chosen plaintexts. To identify integral distinguisher for a block cipher, we first consider a set of chosen plaintexts that contains all possible values for some bits and constant value for the other bits. Then the corresponding ciphertexts are calculated from plaintexts in the set by using an encryption oracle. If the XOR of the corresponding ciphertexts always becomes 0, we say that this cipher has an integral distinguisher. Thus, it involves the higher derivatives of the underlying S-box. Todo [34] generalized the concept of integral and higher-order differential distinguisher, and discovered a new distinguishing property against block ciphers, called the division property. This property was used to present new generic distinguishers against both SPN and Feistel constructions. All these distinguishers are mainly dependent on the derivatives of the functions or the S-boxes. A summary of related results are presented below.

The basic idea of such cryptanalysis comes from the fundamental concept of Shannon [30]. Shannon [30] introduced two basic properties of symmetric ciphers, called confusion and diffusion, which are related to their nonlinearity and

Distinguisher/ Tool/ Remark	year	Author	Paper
Differential	1990	Biham *et al.*	[2]
Differential (Attack on DES full rounds)	1992	Biham *et al.*	[3]
Higher-order differential	1994	Lai	[38]
Truncated differential	1994	Knudsen	[20]
Integral	1997	Daemen *et al.*	[14]
Impossible differential	1998	Knudsen	[21]
Impossible differential (Rump Session, Crypto'98)	1998	Shamir	[31]
Division property	2015	Todo	[34]
Boomerang	1999	Wagner	[36]
BCT	2018	Cid *et al.*	[12]
Results on Boomerang uniformity	2018	Boura *et al.*	[6]
Boomerang switch	2019	Wang *et al.*	[37]
FBCT	2020	Boukerrou *et al.*	[5]
Differential-linear	1994	Langford *et al.*	[24]
DLCT	2019	Bar-On *et al.*	[1]
Construction of S-boxes resisting differential-linear attack	2019	Tang *et al.*	[35]
Extended BCT	2019	Nyberg	[29]

autocorrelation, respectively. A secure cryptosystem must have high nonlinearity, low autocorrelation spectrum and a flat differential spectrum. Nyberg [28] proved that the inverse function is an APN permutation for odd n, and if n is even, differential uniformity of inverse function is 4. In particular, for a nonzero fixed input difference of inverse function, we have exactly one output difference that have four solutions when n is even. Thus, it is difficult to explore a differential path with good probability in a block cipher that uses the inverse function as a primitive. In this direction, it is important to identify the higher-order differential properties of S-boxes to resist different variants of differential attack. In this paper we look at the most popular S-box, called the inverse function, and derive its higher-order cryptographic properties. We identify an error in second-order spectrum of such function and that error occurs in several places. This error might be useful to identify some second-order differential paths in a block cipher that uses the inverse function as a primitive. In this direction, we introduce the Gowers uniformity norms of vectorial Boolean functions that can be exploited as a measure of resistance against higher order approximate. The Gowers U_3 norm of inverse functions are derived and subsequently we show that this norm value is larger than optimal Gowers U_3 norm for a vectorial Boolean function. This implies that the correlation, between the components of the inverse function and certain quadratic Boolean functions, is higher than the optimal case. Finally, we derive the nonlinearity bounds of inverse function using both Gowers uniformity norm and Walsh–Hadamard spectrum. In particular, we check that our bounds on second-order and third-order nonlinearity are slightly improved than that bounds provided by Carlet in [8].

1.1 Contribution and Organization

We mainly focus on two properties, the k-th order differential spectrum and the nonlinearity profile of the inverse function. This is used in Advanced Encryption

Standard (AES) with input length is 8. These properties are dependent on the properties of its component functions. To start with, some basic definitions and notations are presented in Section 2. We also introduce the definition of Gowers uniformity norm of S-boxes. The contributory sections of this paper are as follows.

– The second-order differential spectrum of multiplicative inverse function are calculated in Section 3, and prove that there are many tuples (η, γ, ω) in $\mathbb{F}_{2^n}^3$ such that the second-order spectrum value is 8. We also derive a relation between second-order differential spectrum and difference distribution table of multiplicative inverse function.

  From [5, Table 2], we know that for inverse function the value of $\mathcal{N}(\gamma, \eta, 0)$, defined in (5), is 0 when n is odd, for all $\gamma, \eta \in \mathbb{F}_{2^n}^*$ with $\gamma \neq \eta$. When n is even, there exist $\gamma, \eta \in \mathbb{F}_{2^n}^*$ with $\gamma \neq \eta$ such that $\mathcal{N}(\gamma, \eta, 0) = 4$. Thus, there exist $\gamma, \eta \in \mathbb{F}_{2^n}^*$ with $\gamma \neq \eta$ having probability $\Pr[\{x \in \mathbb{F}_{2^n} : \frac{1}{x} + \frac{1}{x+\gamma} + \frac{1}{x+\eta} + \frac{1}{x+\gamma+\eta} = 0\}] = \frac{1}{2^{n-2}}$, which is an optimal value.

  Instead of 0, if we consider a nonzero ω, then from Lemma 7 and Theorem 3, we have the maximum value of $\mathcal{N}(\gamma, \eta, \omega)$ is 8. Thus, there exist $\gamma, \eta, \omega \in \mathbb{F}_{2^n}^*$ with $\gamma \neq \eta$ having probability $\Pr[\{x \in \mathbb{F}_{2^n} : \frac{1}{x} + \frac{1}{x+\gamma} + \frac{1}{x+\eta} + \frac{1}{x+\gamma+\eta} = \omega\}] = \frac{2}{2^{n-2}}$. So, we get an error in second-order spectrum of inverse function with probability $\frac{1}{2^{n-2}}$. Thus, $O(2^{n-2})$ ($p = \frac{1}{2^{n-2}}$ and $q = 1$ since $\frac{2}{2^{n-2}} = \frac{1}{2^{n-2}}(1+1)$, so $O(\frac{1}{pq^2}) = O(2^{n-2})$) many inputs are required to identify this error with a success probability significantly higher that half. This might be exploited to identify weaknesses of a block cipher where the inverse function is used as a primitive.

  Our findings improve the results given in [5] related to the higher-order profiles of an inverse function.

– We further calculate the Gowers uniformity norm, in particular Gowers U_3 norm, for inverse function in Section 4. The main result is presented in Theorem 5. This norm is related to the correlation between the components of the inverse function and certain quadratic Boolean functions. We note that this is higher than the optimal case. This is the first time the Gowers norm is studied in detail in analysing a vector Boolean function, and in particular for the inverse function.

– The bounds of nonlinearity profile of multiplicative inverse function are derived in Section 5. In this case we consider Walsh–Hadamard spectrum of higher order derivatives. With the help of computer, we check that our bounds on second-order and third-order nonlinearity are slightly improved than the bounds provided by Carlet in [8]. The Gowers norm is also used to study higher order nonlinearity.

Section 6 concludes the paper.

Our results in this paper provide more detailed understanding about the inverse function, which is used as S-box in many block cipher designs, most importantly in AES. Thus, these results will have importance in understanding the strength and weaknesses of block ciphers better where inverse functions are used.

Before proceeding further let us present some background material.

2 Preliminaries

For any positive integer n, we denote by $\mathbb{F}_2^n$ the vector space of n-tuples over the finite field $\mathbb{F}_2 = \{0, 1\}$, and by $\mathbb{F}_{2^n}$ the finite field of order 2^n. For simplicity, we denote by ${\mathbb{F}_2^n}^*$ the set $\mathbb{F}_2^n \setminus \{(0, 0, \ldots, 0)\}$, 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 $x = (x_1, \ldots, x_n)$ 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 $wt(x) = \sum_{i=1}^n x_i$, the sum is over integer. The cardinality of any set A is denoted by $\#A$. The inner product of $x, y \in \mathbb{F}_2^n$ is defined by $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$.

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

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 the parallelization of m Boolean functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, where $1 \leq i \leq m$, such that $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ for all $x \in \mathbb{F}_2^n$. In addition, the Boolean functions 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 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 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 $\mathrm{Tr}_1^m(x) = \sum_{i=0}^{m-1} x^{2^i}$.

2.2 Cryptographic properties of S-boxes

We now briefly review the basic definitions regarding to the cryptographic properties of Boolean functions and then extend those definitions to S-boxes by using component functions.

We represent the set of all n-variable Boolean functions by $\mathcal{B}_n$. Any Boolean function $f \in \mathcal{B}_n$ can be expressed by its truth table, i.e.,

$$f = \big[f(0,\dots,0,0), f(0,\dots,0,1),\dots,f(1,\dots,1,1)\big].$$

We say that a Boolean function $f \in \mathcal{B}_n$ is balanced if its truth table contains an equal number of ones and zeros, that is, if its Hamming weight equals 2^{n-1}, where the Hamming weight of f is defined as the size of the support of f in which the support of f is defined as $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) \neq 0\}$. 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 $\mathbb{F}_2[x_1,\dots,x_n]/(x_1^2 + x_1,\dots,x_n^2 + x_n)$:

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

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 $w_H(u)$ such that $a_u \neq 0$, where $w_H(u)$ denotes the Hamming weight of u which is defined as the number of nonzero coordinates of $u \in \mathbb{F}_2^n$. Recall that $\mathbb{F}_{2^n}$ is isomorphic as a $\mathbb{F}_2$-vector space to $\mathbb{F}_2^n$. The Boolean functions defined over $\mathbb{F}_{2^n}$ can also 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 $\max\{w_H(\bar{i}) : a_i \neq 0, 0 \leq i < 2^m\}$, where $\bar{i}$ is the binary expansion of i (see e.g. [9]). The *rth-order nonlinearity* of a Boolean function $f \in \mathcal{B}_n$ is defined as its minimum Hamming distance from f to 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 $x = (x_1, x_2, \dots, x_n)$ and $\omega = (\omega_1, \omega_2, \dots, \omega_n)$ both belong 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

$$\widehat{f}(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(\alpha x)}.$$

It can be easily seen that, for any Boolean function $f \in \mathcal{B}_n$, its nonlinearity can be computed as

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

when f is defined over $\mathbb{F}_2^n$, and its nonlinearity can be computed as

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

when f is defined over $\mathbb{F}_{2^n}$. The nonlinearity of an (n, m)-function F is dependent on its component functions, and is defined by the minimum nonlineartiy of its all component functions, that is,

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

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 rth order nonlinearity of an (n, m)-function F is the minimum rth order nonlineartiy of its all component functions.

The derivative of $f \in \mathbb{B}_n$ 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 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

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

It can be easily seen that $D_V f$ is independent of the choice of basis for V.

2.3 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 $B \subseteq V$. 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 [15] introduced a new measure of Boolean functions, called Gowers uniformity norms.

Definition 1 ([11], 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*

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

It is semi-norm $k = 1$, and for other $k \geq 2$ Gowers norms satisfied all the norm properties. Gowers norms for $k = 1, 2, 3$ are explicitly presented below (see [11,33]).

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

The connection between the Gowers uniformity norms and correlation of a function with polynomials with a certain degree bound is described by results obtained by Gowers, Green and Tao [15,16]. For a survey we refer to Chen [11].

Theorem 1 ([11,15,16]). *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 kth order nonlinearity of a Boolean function bounded above by high (low) value, then its Gowers U_{k+1} norm bounded below by low (high) value. We know [16,32] that the converse part of Theorem 1 is also true for $k = 1, 2$. Samorodnitsky [32] proved that a Boolean function with a large Gowers U_3 norm is somewhat close to a quadratic polynomial.

Theorem 2. [32, 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 bounded above by high (low) value if and only if its Gowers U_3 norm 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. The Gowers norm on Boolean functions first used by Gangopadhyay *et al.* [17], and derived Gowers U_3 norms of some classes of Boolean functions with some properties. Let n be a positive integer and f be an arbitrary n-variable

Boolean function. For the two-valued function $(-1)^f \in \{-1,1\} \subseteq \mathbb{R}$, we have

$$\left\|(-1)^f\right\|_{U_3} = 2^{-\frac{n}{2}} \left| \sum_{(\tau,\gamma)\in\mathbb{F}_{2n}^2} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+f(x+\tau)+f(x+\gamma)+f(x+\tau+\gamma)} \right)^2 \right|^{\frac{1}{8}}. \quad (3)$$

Let us now consider the case of S-boxes. Suppose F is a S-box of input length n and output length m, and $f_i \in \mathcal{B}_m, 1 \le i \le m$, is the 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 2. *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*

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

In particular for $k=3$, the Gowers U_3 norm of $(-1)^F$ is

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

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. The algebraic degree of an S-box is defined as the maximum algebraic degree of the coordinate functions and it is also the maximum algebraic degree of the component functions. Similar with Boolean functions, we can define kth-derivative for S-boxes. Let $V_k \subseteq \mathbb{F}_2^n$ be a vector space with dimension k and F be an arbitrary (n,m)-function. The kth-derivative of F with respect to V_k is defined as $D_{V_k}F = \sum_{v\in V_k} F(x+v)$. Let V be an k dimensional subspace of $\mathbb{F}_2^n$. The kth order differential of a S-box F [22, Definition 4.2] is the number of inputs $x \in \mathbb{F}_2^n$ such that

$$\sum_{v\in V} F(x+v) = \beta, \quad \beta \in \mathbb{F}_2^n. \quad (4)$$

Definition 3. *An $n\times m$ S-box F is called the kth-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 the kth-order differential uniformity of F.*

It is clear that if $x \in \mathbb{F}_2^n$ satisfy (4), then $x+v$, $v \in V$ are also satisfied. Thus, the cardinality of the solution spaces of (4) for any k-dimensional subspace of $\mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^n$ is divisible by 2^k.

Remark 1. Let δ_k be the kth-order differential uniformity of a 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 [28] for considering the quality of F to resist the differential attack [2]. 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 smallest possible value of δ of (n,m)-functions is 2 and the functions achieving this value are called *almost perfect nonlinear* (APN) functions. A cryptographically desirable S-box is required 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 $[\delta_k(V_k, \beta) : V_k \subseteq \mathbb{F}_2^k, \beta \in \mathbb{F}_2^m]$ is called the *kth-order differential spectrum* of F. For $k=1$, this spectrum is represented as a well known table, called difference distribution table (DDT), and the maximum value of DDT is called differential uniformity of F.

2.4 The multiplicative inverse function

For any finite field $\mathbb{F}_{2^n}$, the multiplicative inverse function of $\mathbb{F}_{2^n}$, denoted by I, is defined as $I(x) = x^{2^n-2}$. In the sequel, we will use x^{-1} or $\frac{1}{x}$ to denote x^{2^n-2} with the convention that $x^{-1} = \frac{1}{x} = 0$ when $x = 0$. We can see that, for any $v \neq 0$, $I_v(x) = \mathrm{Tr}_1^n(vx^{-1})$ is a component function of I. The Walsh–Hadamard transform of I_1 at any point α is well known as a Kloosterman sum over $\mathbb{F}_{2^n}$ at α, which is usually denoted by $\mathcal{K}(\alpha)$, i.e., $\mathcal{K}(\alpha) = \widehat{I_1}(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{-1}+\alpha x)}$. In fact, the original Kloosterman sums are generally defined on the multiplicative group $\mathbb{F}_{2^n}^*$. We extend them to 0 by assuming $(-1)^0 = 1$. Regarding the Kloosterman sums, the following results are well known and we will use them in the sequel.

Lemma 1 ([7]). *For any integer $n > 0$, $\widehat{I_1}(1) = 1 - \sum_{t=0}^{\lfloor n/2 \rfloor} (-1)^{n-t} \frac{n}{n-t} \binom{n-t}{t} 2^t$.*

Lemma 2 ([23]). *For any positive integer n and arbitrary $a \in \mathbb{F}_{2^n}^*$, the Walsh–Hadamard spectrum of $I_1(x)$ defined on $\mathbb{F}_{2^n}$ can take any value divisible by 4 in the range $[-2^{n/2+1}+1, 2^{n/2+1}+1]$.*

Let $n = 2t+1$ be odd integer and P be a largest positive integer such that $P \equiv 0 \pmod 4$ and $P \leq 2^{t+1}\sqrt{2}+1$.

Remark 2. The possible maximum absolute value of Walsh–Hadamard spectrum of I_1 over $\mathbb{F}_{2^n}$ is

$$\max_{\alpha \in \mathbb{F}_{2^n}^*} |\widehat{I_1}(\alpha)| = \begin{cases} 2^{\frac{n}{2}+1}, & \text{if } n \text{ is even} \\ P, & \text{if } n \text{ is odd} \end{cases},$$

where P is defined in above.

3 Second-order differential spectrum of the multiplicative inverse function

The second-order differential spectrum of any (n,m)-function is related to its second derivatives. Let $V_{\eta,\gamma} = \{0, \eta, \gamma, \eta+\gamma\} \subset \mathbb{F}_{2^n}$. It is clear that if $\eta = 0$ or $\gamma = 0$ or $\eta = \gamma$, $V_{\eta,\gamma}$ is a multiset and the cardinality of $\{x \in \mathbb{F}_{2^n} : \sum_{\upsilon \in V_{\eta,\gamma}} F(x+\upsilon) = 0\}$ is $\delta_2(V_{\eta,\gamma}, 0) = 2^n$ for all (n,m)-function F. These particular values of η and γ we usually called trivial points. In cryptography we are interested to calculate the values of $\delta_2(V_{\eta,\gamma}, 0)$ for all $\eta, \gamma \in \mathbb{F}_{2^n}^*$ with $\eta \neq \gamma$. Recently, Boukerrou et al. [5] calculated the values of $\delta_2(V_{\eta,\gamma}, 0)$ for inverse function. They proved that the values of $\delta_2(V_{\eta,\gamma}, 0)$ for inverse function at any nontrivial point is 0 when n is odd, and if n is even, its only nonzero value is 4. Thus, inverse function have best known $\delta_2(V_{\eta,\gamma}, 0)$ values. In this section we further calculate the values of $\delta_2(V_{\eta,\gamma}, \beta)$ at any nontrivial point and $\beta \in \mathbb{F}_{2^n}^*$.

Lemma 3 ([26]). *For any $(\alpha, \beta) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we define a polynomial $\mu(x) = \alpha x^2 + \beta x + \gamma \in \mathbb{F}_{2^n}[x]$. Then the equation $\mu(x) = 0$ has 2 solutions if and only if $\mathrm{Tr}_1^n(\beta^{-2}\alpha\lambda) = 0$.*

Lemma 4. *Let n be a positive integer and $T_0 = \{\upsilon^2 + \upsilon : \upsilon \in \mathbb{F}_{2^n}\}$. Then we have*

$$\sum_{x \in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)} = \frac{1}{2}(-1)^{\mathrm{Tr}_1^n(1)}\widehat{I_1}(1).$$

Proof. Note that

$$\sum_{x \in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)} + \sum_{x \in \mathbb{F}_{2^n} \setminus T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)} = 0$$

and

$$\sum_{x \in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)} - \sum_{x \in \mathbb{F}_{2^n} \setminus T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)}$$
$$= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}+x\right)} = (-1)^{\mathrm{Tr}_1^n(1)}\widehat{I_1}(1).$$

We can obtain that

$$\sum_{x\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)}=\frac{1}{2}(-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1).$$

This completes the proof.

Lemma 5. *Let n be a positive integer. We have*

$$\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2}{\upsilon^2+\upsilon+1}\right)}=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2+1}{\upsilon^2+\upsilon+1}\right)}=(-1)^{\mathrm{Tr}_1^n(1)}\left(\widehat{I}_1(1)-2\right).$$

Proof. It can be easily seen that

$$\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2}{\upsilon^2+\upsilon+1}\right)}=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2+1}{\upsilon^2+\upsilon+1}\right)}$$

by changing υ into $\upsilon+1$. We now consider the value of $\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2}{\upsilon^2+\upsilon+1}\right)}$. We have

$$\begin{aligned}\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2}{\upsilon^2+\upsilon+1}\right)}&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\upsilon^2+\upsilon+1}\right)}\quad(\text{replacing }\upsilon\text{ by }\upsilon^{-1})\\&=2\sum_{x\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)}-2(-1)^{\mathrm{Tr}_1^n(1)}\quad(\text{replacing }\upsilon^2+\upsilon\text{ by }x)\\&=(-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1)-2(-1)^{\mathrm{Tr}_1^n(1)}=(-1)^{\mathrm{Tr}_1^n(1)}\left(\widehat{I}_1(1)-2\right).\end{aligned}$$

where Lemma 4 is used in the last identity. This completes the proof.

Lemma 6. *Let $n\geq 4$ be an arbitrary integer. We define*

$$L=\#\left\{c\in\mathbb{F}_{2^n}:\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)=\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)=0\right\}.$$

Then we have $L=2^{n-2}+\frac{3}{4}(-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1)+\frac{1}{2}\left(1-(-1)^{\mathrm{Tr}_1^n(1)}\right)$, where $\widehat{I}_1(1)$ is given by Lemma 1.

Proof. For any $(i,j,k)\in\mathbb{F}_2^3$, we define $L_{(i,j,k)}$ as

$$\#\left\{c\in\mathbb{F}_{2^n}:\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)=i,\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)=j,\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)=k\right\}.$$

Note that $\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)+\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)=\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)$. So we have $L=L_{(0,0,0)}=2^n-L_{(0,1,1)}-L_{(1,0,1)}-L_{(1,1,0)}$. Note that

$$\sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)}=\sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)}$$

by changing c into $c+1$. Then the Hamming weight of Boolean functions $\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)$ and $\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)$ on variables c is equal, that is, $wt\left(\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)\right)$ $= wt\left(\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)\right)$. So we have $L_{(0,1,1)}+L_{(1,1,0)} = L_{(0,1,1)}+L_{(1,0,1)}$ and thus

$$L_{(1,1,0)} = L_{(1,0,1)} = \frac{1}{2}wt\left(\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)\right) = \frac{1}{4}\left(2^n - \sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)}\right).$$

Note that

$$L_{(1,0,1)}+L_{(0,1,1)} = wt\left(\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)\right) = \frac{1}{2}\left(2^n - \sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)}\right).$$

Therefore, we have

$$\begin{aligned} L = L_{(0,0,0)} &= 2^n - L_{(0,1,1)} - L_{(1,0,1)} - L_{(1,1,0)} \\ &= 2^{n-2} + \frac{1}{4}\sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)} + \frac{1}{2}\sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)}. \end{aligned}$$

By Lemma 4 we have

$$\sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right)} = 2\sum_{x\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)} = (-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1),$$

where $T_0 = \{\upsilon^2+\upsilon : \upsilon\in\mathbb{F}_{2^n}\}$. From Lemma 5 we have

$$\sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{c^2+1}{c^2+c+1}\right)} = \sum_{c\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right)} = (-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1) - (-1)^{\mathrm{Tr}_1^n(1)} + 1,$$

So we have $L = 2^{n-2} + \frac{3}{4}(-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1) + \frac{1}{2}\left(1-(-1)^{\mathrm{Tr}_1^n(1)}\right)$. This completes the proof.

Let F be an (n,m)-function. For any $\gamma,\eta\in\mathbb{F}_{2^n}$ and $,\omega\in\mathbb{F}_{2^m}$, let us define

$$\mathcal{N}_F(\gamma,\eta,\omega) = \#\left\{x\in\mathbb{F}_{2^n} : F(x)+F(x+\gamma)+F(x+\eta)+F(x+\eta+\gamma)=\omega\right\}. \tag{5}$$

It is clear that for $\gamma=0$ or $\eta=0$ or $\gamma=\eta$, we have $\mathcal{N}_F(\gamma,\eta,0)=2^n$, and when $\omega\neq 0$, $\mathcal{N}_F(\gamma,\eta,\omega)=0$. If F is an inverse function over $\mathbb{F}_{2^n}$, we denote $\mathcal{N}_I(\gamma,\eta,\omega)$ by $\mathcal{N}(\gamma,\eta,\omega)$.

Lemma 7. *Let $n\geq 3$ be a positive integer and $\mathcal{N}(\gamma,\eta,\omega)$ be defined as (5). Let γ,η be two elements of $\mathbb{F}_{2^n}^*$ such that $\gamma\neq\eta$. Then for any $\omega\in\mathbb{F}_{2^n}$, we have $\mathcal{N}(\gamma,\eta,\omega)\in\{0,4,8\}$. Moreover, the number of $(\gamma,\eta,\omega)\in\mathbb{F}_{2^n}^3$ such that $\mathcal{N}(\gamma,\eta,\omega)=8$ is*

$$\left(2^{n-2}+\frac{3}{4}(-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1)-\frac{5}{2}(-1)^{\mathrm{Tr}_1^n(1)}-\frac{3}{2}\right)(2^n-1).$$

Proof. Let us consider the solutions of equation

$$\frac{1}{y} + \frac{1}{y+\gamma} + \frac{1}{y+\eta} + \frac{1}{y+\eta+\gamma} = \omega \tag{6}$$

over $\mathbb{F}_{2^n}$, where $\eta, \gamma \in \mathbb{F}_{2^n}^*$ with $\eta \neq \gamma$. If y is a solution of (6), then $y+\eta$, $y+\gamma$ and $y+\eta+\gamma$ are also solutions.

Case 1. Suppose $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta = 0$. Then $0, \eta, \gamma$ and $\eta+\gamma$ are the solution of (6) then we have $\frac{1}{\gamma}+\frac{1}{\eta}+\frac{1}{\gamma+\eta} = \omega$ which is equivalent to $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta = 0$ since γ, η are two distinct nonzero elements of $\mathbb{F}_{2^n}$. We can always find $\omega \in \mathbb{F}_{2^n}$ such that $\omega = \frac{\gamma^2+\eta^2+\gamma\eta}{\gamma\eta(\gamma+\eta)}$. Thus, $\delta_2 \geq 4$ for inverse function.

Case 2. Let $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta \neq 0$. It can be easily verified that any element in $\{0, \gamma, \eta, \gamma+\eta\}$ is not a solution of (6) otherwise $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta = 0$. So in this case if (6) has solutions then every solution belongs to $\mathbb{F}_{2^n} \setminus \{0, \gamma, \eta, \gamma+\eta\}$. Then (6) becomes

$$\frac{\gamma}{y^2+\gamma y} + \frac{\gamma}{y^2+\gamma y+\eta^2+\gamma\eta} = \omega. \tag{7}$$

Let us define $z = y^2+\gamma y$. We have $z \neq 0$ since $y \in \mathbb{F}_{2^n} \setminus \{0, \gamma, \eta, \gamma+\eta\}$, and $y^2+\gamma y+\eta^2+\gamma\eta \neq 0$ when $y \in \mathbb{F}_{2^n} \setminus \{0, \gamma, \eta, \gamma+\eta\}$ since $y^2+\gamma y+\eta^2+\gamma\eta = 0$ has at most two distinct solutions in $\mathbb{F}_{2^n}$ and we can see that η and $\gamma+\eta$ are two distinct solutions. Multiplying both sides of (7) by $z(z+\eta^2+\gamma\eta)$ yields

$$\omega z^2 + (\omega\eta^2+\omega\gamma\eta)z + (\gamma\eta^2+\gamma^2\eta) = 0. \tag{8}$$

We have $\omega \neq 0$ since if $\omega = 0$ in (7) then we have $\gamma = \eta$ which contradicts to our assumption that γ, η are two distinct nonzero elements of $\mathbb{F}_{2^n}$. Multiplying both sides of (8) by $\frac{1}{\omega}$ gives

$$z^2 + (\eta^2+\gamma\eta)z + \frac{\gamma\eta^2+\gamma^2\eta}{\omega} = 0. \tag{9}$$

This leads to

$$\begin{aligned} &\left(\frac{z}{\eta^2+\gamma\eta}\right)^2 + \frac{z}{\eta^2+\gamma\eta} + \frac{\gamma\eta+\gamma^2}{\omega\eta^3+\omega\gamma^2\eta} = 0 \\ \Leftrightarrow\ &\left(\frac{z}{\eta^2+\gamma\eta}\right)^2 + \frac{z}{\eta^2+\gamma\eta} + \frac{\gamma}{\omega\eta(\eta+\gamma)} = 0 \end{aligned} \tag{10}$$

by multiplying $\frac{1}{(\eta^2+\gamma\eta)^2}$ to both sides of (9). It follows from Lemma 3 that (10) has no solution if $\mathrm{Tr}_1^n\left(\frac{\gamma}{\omega\eta(\eta+\gamma)}\right) = 1$ and has two solutions, denoted by u and $u+1$, if $\mathrm{Tr}_1^n\left(\frac{\gamma}{\omega\eta(\eta+\gamma)}\right) = 0$. Recall that $z = y^2+\gamma y$. We have $\frac{y^2+\gamma y}{\eta^2+\gamma\eta}$ equals u or

$u+1$. It is clear that $u \neq 0, 1$, otherwise from (10) $\gamma = 0$. Note that $\frac{y^2+\gamma y}{\eta^2+\gamma\eta} = u$ is equivalent to

$$\left(\frac{y}{\gamma}\right)^2 + \frac{y}{\gamma} + u\left(\left(\frac{\eta}{\gamma}\right)^2 + \frac{\eta}{\gamma}\right) = 0, \tag{11}$$

and $\frac{y^2+\gamma y}{\eta^2+\gamma\eta} = u+1$ is equivalent to

$$\left(\frac{y}{\gamma}\right)^2 + \frac{y}{\gamma} + (u+1)\left(\left(\frac{\eta}{\gamma}\right)^2 + \frac{\eta}{\gamma}\right) = 0. \tag{12}$$

Note that $\mathrm{Tr}_1^n\left((u+1)((\frac{\eta}{\gamma})^2 + \frac{\eta}{\gamma})\right) = \mathrm{Tr}_1^n\left(u((\frac{\eta}{\gamma})^2 + \frac{\eta}{\gamma})\right) = 0$. By Lemma 3, we have two solutions of (11) and (12) each if $\mathrm{Tr}_1^n\left(u((\frac{\eta}{\gamma})^2 + \frac{\eta}{\gamma})\right) = 0$. Suppose the solutions of (11) are u' and $u'+1$, and the solutions of (12) are u'' and $u''+1$. Then from (11), we have $y = \gamma u'$ or $y = \gamma(u'+1)$, and from (12), we have $y = \gamma u''$ or $y = \gamma(u''+1)$. From (11) and (12), we have $u', u'' \notin \{0, 1, \frac{\eta}{\gamma}, \frac{\eta}{\gamma}+1\}$ and $u' \notin \{u'', u''+1\}$. Thus, these solutions not belong to the set $\{0, \eta, \gamma, \eta+\gamma\}$. Thus, if there exist nonzero elements $\gamma, \eta, \omega \in \mathbb{F}_{2^n}$ with $\gamma \neq \eta$ such that $\mathrm{Tr}_1^n\left(\frac{\gamma}{\omega\eta(\eta+\gamma)}\right) = 0$ and $\mathrm{Tr}_1^n\left(u((\frac{\eta}{\gamma})^2 + \frac{\eta}{\gamma})\right) = 0$, (7) has 4 distinct solutions in this case.

Indeed, if $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta = 0$, the discussion of (6) with solutions in $\mathbb{F}_{2^n} \setminus \{0, \eta, \gamma, \eta+\gamma\}$ is the same as Case 2. Thus, form Cases 1 and 2 we can see that, for any $\eta, \gamma \in \mathbb{F}_{2^n}^*$ with $\eta \neq \gamma$, (6) has 0 or 4 solutions if $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta \neq 0$, and has 4 or 8 solutions if $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta = 0$.

In what follows, we determine the number of $(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3$ such that $\mathcal{N}(\gamma, \eta, \omega) = 8$ with $\eta^2+\gamma^2+\omega\gamma\eta^2+\omega\eta\gamma^2+\gamma\eta = 0$. We can see that any element in $\{0, \eta, \gamma, \eta+\gamma\}$ is a solution of (6). We now consider the solutions of (6) in $\mathbb{F}_{2^n} \setminus \{0, \eta, \gamma, \eta+\gamma\}$. Let us denote by $\eta = \gamma c$. Then we have $\gamma \in \mathbb{F}_{2^n}^*$, $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ and $w = \frac{c^2+c+1}{\gamma(c^2+c)} \neq 0$. Form Case 2, (6) has solutions in $\mathbb{F}_{2^n} \setminus \{0, \eta, \gamma, \eta+\gamma\}$ if and only if $\mathrm{Tr}_1^n\left(\frac{\gamma}{\omega\eta(\eta+\gamma)}\right) = 0$ and $\mathrm{Tr}_1^n\left(u((\frac{\eta}{\gamma})^2 + \frac{\eta}{\gamma})\right) = 0$. Note that

$$\mathrm{Tr}_1^n\left(\frac{\gamma}{\omega\eta(\eta+\gamma)}\right) = 0 \Leftrightarrow \mathrm{Tr}_1^n\left(\frac{1}{c^2+c+1}\right) = 0$$

and

$$\begin{aligned}\mathrm{Tr}_1^n\left(u\left(\left(\frac{\eta}{\gamma}\right)^2 + \frac{\eta}{\gamma}\right)\right) = 0 &\Leftrightarrow \mathrm{Tr}_1^n(u(c^2+c)) = 0 \Leftrightarrow \mathrm{Tr}_1^n((u^2+u)c^2) = 0 \\ &\Leftrightarrow \mathrm{Tr}_1^n\left(\frac{c^2\gamma}{\omega\eta(\eta+\gamma)}\right) = 0 \Leftrightarrow \mathrm{Tr}_1^n\left(\frac{c^2}{c^2+c+1}\right) = 0,\end{aligned}$$

where $c \in \mathbb{F}_{2^n}$ for odd n and $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ for even n since $c \in \mathbb{F}_4$ will lead to $\omega = 0$. Then by Lemma 6, we can get the number of such c. Note that for any such c, γ can range over $\mathbb{F}_{2^n}^*$, so we can get the number of $(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3$ such that $\mathcal{N}(\gamma, \eta, \omega) = 8$. The proof is completed.

Theorem 3. *Let $n \geq 3$ be a positive integer. When (γ, η, ω) ranges over $\mathbb{F}_{2^n}^3$ such that $\gamma, \eta \in \mathbb{F}_{2^n}^*$ and $\gamma \neq \eta$, we have*

$$\mathcal{N}(\gamma, \eta, \omega) = \begin{cases} 0, \; 3 \cdot 2^{3n-2} - 2^{2n+1} - \Big(10(-1)^{\mathrm{Tr}_1^n(1)} - 3(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) + 1\Big) \cdot 2^{n-2} \\ \quad -\frac{3}{4}(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) + \frac{5}{2}(-1)^{\mathrm{Tr}_1^n(1)} + \frac{3}{2} \text{ [times]} \\ 4, \; 2^{3n-2} - 5 \cdot 2^{2n-2} + \Big(10(-1)^{\mathrm{Tr}_1^n(1)} - 3(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) + 8\Big) \cdot 2^{n-1} \\ \quad +\frac{3}{2}(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) - 5(-1)^{\mathrm{Tr}_1^n(1)} - 3 \text{ [times]} \\ 8, \; 2^{2n-2} + \Big(3(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) - 10(-1)^{\mathrm{Tr}_1^n(1)} - 7\Big) \cdot 2^{n-2} \\ \quad -\frac{3}{4}(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) + \frac{5}{2}(-1)^{\mathrm{Tr}_1^n(1)} + \frac{3}{2} \text{ [times]} \end{cases},$$

where $\widehat{I_1}(1)$ is given by Lemma 1.

Proof. For any $\gamma, \eta, \omega \in \mathbb{F}_{2^n}$, we have $\mathcal{N}(\gamma, \eta, 0) = 2^n$ if $\gamma = 0$ or $\eta = 0$ or $\gamma = \eta$. So the number of $(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3$ such that $\mathcal{N}(\gamma, \eta, 0) = 2^n$ is $3 \cdot 2^n - 2$. Let us define $c = \#\{(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3 : \mathcal{N}(\gamma, \eta, \omega) = 4\}$ and $d = \#\{(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3 : \mathcal{N}(\gamma, \eta, \omega) = 8\}$. We have $4c + 8d + 2^n(3 \cdot 2^n - 2) = 2^{3n}$ since $\sum_{\gamma, \eta, \omega \in \mathbb{F}_{2^n}} \mathcal{N}(\gamma, \eta, \omega) = 2^{3n}$. Then by Lemma 7 the value of c is

$$\frac{2^{3n} - 2^n \cdot (3 \cdot 2^n - 2) - 8 \cdot (2^{n-2} + \frac{3}{4}(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) - \frac{5}{2}(-1)^{\mathrm{Tr}_1^n(1)} - \frac{3}{2})(2^n - 1)}{4}$$
$$= 2^{3n-2} - 5 \cdot 2^{2n-2} + \Big(10(-1)^{\mathrm{Tr}_1^n(1)} - 3(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) + 8\Big) \cdot 2^{n-1}$$
$$+\frac{3}{2}(-1)^{\mathrm{Tr}_1^n(1)} \widehat{I_1}(1) - 5(-1)^{\mathrm{Tr}_1^n(1)} - 3.$$

Moreover, the number of (γ, η, ω) ranging over $\mathbb{F}_{2^n}^3$ such that $\gamma, \eta \in \mathbb{F}_{2^n}^*$, $\gamma \neq \eta$ and $\mathcal{N}(\gamma, \eta, \omega) = 0$ is equal to $(2^{2n} - (3 \cdot 2^n - 2)) \cdot 2^n - c - d$. This completes the proof.

Remark 3. When $n = 4$ and $n = 5$, there is no $(\gamma, \eta, \omega) \in \mathbb{F}_{2^n}^3$ such that $\mathcal{N}(\gamma, \eta, \omega) = 8$.

Let $n \geq 3$ be an odd positive integer. It is clear that $\eta^2 + \gamma^2 + \eta\gamma = 0$ where $\eta, \gamma \in \mathbb{F}_{2^n}$ if and only if $\eta = 0$ and $\gamma = 0$. Thus, the above results for odd variables and $\omega = 0$ follow from the result given in [5]. Suppose for an (n, m)-function F, $\Delta_F(\alpha, \beta) = \{x \in \mathbb{F}_{2^n} : F(x) + F(x + \alpha) = \beta\}$. We derive the relation between $\mathcal{N}_F(\gamma, \eta, \omega)$, defined as (5), and the cardinality of some fixed intersection sets $\Delta_I(\alpha, \beta)$ which is generalized of [5, Theorem 3].

Theorem 4. *Let $n \geq 3$ be a positive integer and F be an (n, m)-function. For any $\gamma, \eta \in \mathbb{F}_{2^n}^*$ with $\gamma \neq \eta$ and $\omega \in \mathbb{F}_{2^m}$, we have*

$$\mathcal{N}_F(\gamma, \eta, \omega) = \sum_{\beta \in \mathbb{F}_{2^m}} \# \Delta_F(\gamma, \beta) \cap (\eta + \Delta_F(\gamma, \beta + \omega)).$$

Proof. We know that $\mathit{\Delta}_F(\gamma,\beta)\cap\mathit{\Delta}_F(\gamma,\beta')=\emptyset$ for all $\gamma\in\mathbb{F}_{2^n}$ and $\beta,\beta'\in\mathbb{F}_{2^m}$ with $\beta\neq\beta'$. For any $\gamma,\eta\in\mathbb{F}_{2^n}^*$ with $\gamma\neq\eta$ and $\omega\in\mathbb{F}_{2^m}$,

$$\begin{aligned}\mathcal{N}_F(\gamma,\eta,\omega)&=\#\{x\in\mathbb{F}_{2^n}:F(x)+F(x+\gamma)+F(x+\eta)+F(x+\gamma+\eta)=\omega\}\\&=\#\{x\in\mathbb{F}_{2^n}:F(x)+F(x+\gamma)+F(x+\eta)+F(x+\gamma+\eta)+\omega\}\\&=\#\cup_{\beta\in\mathbb{F}_{2^m}}\{x\in\mathbb{F}_{2^n}:F(x)+F(x+\gamma)=\beta\}\\&\qquad\qquad\cap\{x\in\mathbb{F}_{2^n}:F(x+\eta)+F(x+\gamma+\eta)=\beta+\omega\}\\&=\#\cup_{\beta\in\mathbb{F}_{2^m}}\mathit{\Delta}_F(\gamma,\beta)\cap\{x+\eta\in\mathbb{F}_{2^n}:F(x)+F(x+\gamma)=\beta+\omega\}\\&=\#\cup_{\beta\in\mathbb{F}_{2^m}}\mathit{\Delta}_F(\gamma,\beta)\cap(\eta+\mathit{\Delta}_F(\gamma,\beta+\omega))\\&=\sum_{\beta\in\mathbb{F}_{2^m}}\#\mathit{\Delta}_F(\gamma,\beta)\cap(\eta+\mathit{\Delta}_F(\gamma,\beta+\omega)).\end{aligned}$$

We consider the set $\mathit{\Delta}_F(\alpha,\beta)$ at (α,β) instead of their cardinality in DDT of an (n,m)-function F, then the value $\mathcal{N}_F(\eta,\gamma,\omega)$ of F dependent on the set $\mathit{\Delta}_F(\gamma,\beta)\cap(\eta+\mathit{\Delta}_F(\gamma,\beta+\omega))$ for all $\beta\in\mathbb{F}_{2^m}$. Suppose $\mathit{\Delta}_F(\gamma,\beta)=V_\beta+\{0,\gamma\}$ and $\mathit{\Delta}_F(\gamma,\beta+\omega)=V_{\beta+\omega}+\{0,\gamma\}$. From Theorem 4, we have $\mathcal{N}_F(\gamma,\eta,\omega)=2\sum_{\beta\in\mathbb{F}_{2^m}}\#V_\beta\cap V_{\beta+\omega}$. For example let $\mathcal{N}(\gamma_1,\eta_1,\omega_1)=4$ for an inverse function defined over odd number of variables, where $\gamma_1,\eta_1,\omega_1\in\mathbb{F}_{2^n}^*$ with $\gamma_1\neq\eta_1$. From Theorem 4, there exist two distinct $\beta_1,\beta_2\in\mathbb{F}_{2^n}^*$ such that the sets $\mathit{\Delta}_I(\gamma_1,\beta_1)\cap(\eta_1+\mathit{\Delta}_I(\gamma_1,\beta_1+\omega_1))$ and $\mathit{\Delta}_I(\gamma_1,\beta_2)\cap(\eta_1+\mathit{\Delta}_I(\gamma_1,\beta_2+\omega_1))$ are nonempty. Suppose $\mathit{\Delta}_I(\gamma_1,\beta_1)=x_{\beta_1}+\{0,\gamma_1\}$ and $\eta_1+\mathit{\Delta}_I(\gamma_1,\beta_1+\omega_1)=\eta_1+x_{\beta_1+\omega_1}+\{0,\gamma_1\}$. Then $x_{\beta_1}+x_{\beta_1+\omega_1}=\eta_1$. Here $V_{\beta_1}=\{x_{\beta_1}\}$ and $V_{\beta_1+\omega_1}=\{x_{\beta_1+\omega_1}\}$. Similarly, if $\mathit{\Delta}_I(\gamma_1,\beta_2)=x_{\beta_2}+\{0,\gamma_1\}$ and $\eta_1+\mathit{\Delta}_I(\gamma_1,\beta_2+\omega_1)=\eta_1+x_{\beta_2+\omega_1}+\{0,\gamma_1\}$, then $x_{\beta_2}+x_{\beta_2+\omega_1}=\eta_1=x_{\beta_1}+x_{\beta_1+\omega_1}$. We know that if F is a bijective function over $\mathbb{F}_{2^n}$ and $\gamma\neq 0$, then $\mathit{\Delta}_F(\gamma,0)=\emptyset$. Thus, $\mathcal{N}_F(\gamma,\eta,\omega)=\sum_{\beta\in\mathbb{F}_{2^m}}\#\mathit{\Delta}_F(\gamma,\beta)\cap(\eta+\mathit{\Delta}_F(\gamma,\beta+\omega))$.

4 Gowers U_3 norm of the multiplicative inverse function

In this section we calculate the Gowers U_3 norm of inverse function. Let $f\in\mathcal{B}_n$ be any quadratic Boolean function. Then $\deg(f)\leq 2$, so any second derivative of f is constant. Thus, from (3) we have $\|(-1)^f\|_{U_3}=1$. We first derive some results that are used to prove our main claim.

Lemma 8 ([26]). *For any n-variable Boolean function f, we have $\sum_{a\in\mathbb{F}_{2^n}}\widehat{f}^{\,2}(a)=2^{2n}$.*

Lemma 9. *Let f be an arbitrary n-variable Boolean function. For any $\alpha,\beta\in\mathbb{F}_{2^n}^*$, we have*

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(\alpha x)+f(\beta x)}=2^{-n}\sum_{u\in\mathbb{F}_{2^n}}\widehat{f}(\alpha^{-1}u)\widehat{f}(\beta^{-1}u).$$

Proof. For any $\alpha, \beta \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}\sum_{u \in \mathbb{F}_{2^n}} \widehat{f}(\alpha^{-1}u)\widehat{f}(\beta^{-1}u) &= \sum_{u \in \mathbb{F}_{2^n}} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\alpha^{-1}ux)} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(y)+\mathrm{Tr}_1^n(\beta^{-1}uy)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(y)} \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n((\alpha^{-1}x+\beta^{-1}y)u)} \\ &= 2^n \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(\beta\alpha^{-1}x)} = 2^n \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(\alpha x)+f(\beta x)}.\end{aligned}$$

Lemma 10. *Let n be a positive integer and $U = \{(0, y) \in \mathbb{F}_{2^n}^2 : y \in \mathbb{F}_{2^n}^*\} \cup \{(x, 0) \in \mathbb{F}_{2^n}^2 : x \in \mathbb{F}_{2^n}^*\} \cup \{(x, x) \in \mathbb{F}_{2^n}^2 : x \in \mathbb{F}_{2^n}\}$. For any $(\tau, \gamma) \in \mathbb{F}_{2^n}^2 \setminus U$, we have*

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\frac{1}{x+\gamma}+\frac{1}{x+\tau+\gamma}\right)} &= \widehat{I_1}\left(\frac{\tau}{\gamma^2+\tau\gamma}\right) + \widehat{I_1}\left(\frac{\tau y^2}{\gamma^2+\tau\gamma}\right) \\ &\quad + \widehat{I_1}\left(\frac{\tau(y^2+1)}{\gamma^2+\tau\gamma}\right) + 4\left((-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\tau\gamma}+\frac{1}{\tau}\right)} - 1\right),\end{aligned}$$

where $y = \gamma\tau^{-1}$ or $\gamma\tau^{-1} + 1$.

Proof. For any $(\tau, \gamma) \in \mathbb{F}_{2^n}^2 \setminus U$

$$\begin{aligned}&\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\frac{1}{x+\gamma}+\frac{1}{x+\tau+\gamma}\right)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\frac{1}{\tau x+\gamma}+\frac{1}{\tau x+\tau+\gamma}\right)} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1,\gamma\tau^{-1},1+\gamma\tau^{-1}\}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\frac{1}{\tau x+\gamma}+\frac{1}{\tau x+\tau+\gamma}\right)} + 4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)} \\ &= \sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1,\gamma\tau^{-1},1+\gamma\tau^{-1}\}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\frac{1}{\tau(x^2+x)+\gamma^2\tau^{-1}+\gamma}\right)} + 4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\frac{1}{\tau(x^2+x)+\gamma^2\tau^{-1}+\gamma}\right)} - 4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)} + 4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)} \\ &= 2\sum_{z \in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)} - 4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)} + 4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)},\end{aligned}$$

where $T_0 = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(x) = 0\}$. Note that

$$\begin{aligned}&\sum_{z \in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)} + \sum_{z \in \mathbb{F}_{2^n} \setminus T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)} \\ &\quad= \sum_{z \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)} = \sum_{z \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{z}+\frac{1}{z+\gamma^2\tau^{-1}+\gamma}\right)} \\ &\quad= \widehat{I_1}\left(\frac{\tau}{\gamma^2+\tau\gamma}\right) + 2\Big((-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\tau\gamma}\right)} - 1\Big),\end{aligned}$$

where the last identity follows from Theorem 8. Note also that

$$\begin{aligned}
&\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)}-\sum_{z\in\mathbb{F}_{2^n}\setminus T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)}\\
&\quad=\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+z\right)}=\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{z}+\frac{1}{z+\gamma^2\tau^{-1}+\gamma}+\frac{z}{\tau}\right)}\\
&\quad=\widehat{I}_1\left(\frac{\tau y^2}{\gamma^2+\tau\gamma}\right)+\widehat{I}_1\left(\frac{\tau(y^2+1)}{\gamma^2+\tau\gamma}\right)+2\Big((-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\tau\gamma}\right)}-1\Big),
\end{aligned}$$

where $y=\gamma\tau^{-1}$ or $\gamma\tau^{-1}+1$, and in the last identity we make use of Theorem 8. So we have

$$\begin{aligned}
&\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)}\\
&=\frac{1}{2}\left[\widehat{I}_1\left(\frac{\tau}{\gamma^2+\tau\gamma}\right)+\widehat{I}_1\left(\frac{\tau y^2}{\gamma^2+\tau\gamma}\right)+\widehat{I}_1\left(\frac{\tau(y^2+1)}{\gamma^2+\tau\gamma}\right)\right]+2\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\tau\gamma}\right)}-1\right].
\end{aligned}$$

Then we can obtain our assertion.

We now present the third-dimension Gowers uniformity norm of the two-valued function $(-1)^{I_1}$ derived from the multiplicative inverse function.

Theorem 5. *For any positive integer $n\geq 4$, we have*

$$\left\|(-1)^{I_1}\right\|_{U_3}=2^{-\frac{n}{2}}\left|3\cdot 2^{3n+1}+2^{n+3}\cdot\left[(-1)^{\mathrm{Tr}_1^n(1)}\left(3\widehat{I}_1(1)-10\right)-6\right]\right|^{\frac{1}{8}},$$

where $\widehat{I}_1(1)$ is given by Lemma 1.

Proof. Note that $\mathbb{F}_{2^n}^2=\bigcup_{v\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\{(\tau,v\tau):\tau\in\mathbb{F}_{2^n}^*\}\bigcup U$, where $U=\{(0,y)\in\mathbb{F}_{2^n}^2:y\in\mathbb{F}_{2^n}^*\}\cup\{(x,0)\in\mathbb{F}_{2^n}^2:x\in\mathbb{F}_{2^n}^*\}\cup\{(x,x)\in\mathbb{F}_{2^n}^2:x\in\mathbb{F}_{2^n}\}$. Define

$$S_1=\sum_{(\tau,\gamma)\in\mathbb{F}_{2^n}^2\setminus U}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{I_1(x)+I_1(x+\tau)+I_1(x+\gamma)+I_1(x+\tau+\gamma)}\right)^2$$

and

$$S_2=\sum_{(\tau,\gamma)\in U}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{I_1(x)+I_1(x+\tau)+I_1(x+\gamma)+I_1(x+\tau+\gamma)}\right)^2.$$

It can be easily seen that $\mathbb{F}_{2^n}^2 \setminus U = \{(\tau, \upsilon\tau) : \upsilon \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2, \tau \in \mathbb{F}_{2^n}^*\}$. Then by Lemma 10 with $\gamma = \upsilon\tau$ we have

$$
\begin{aligned}
S_1 = &\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[\widehat{I_1}^2\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}^2\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}^2\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\right]\\
&+2\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[\widehat{I_1}\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)\widehat{I_1}\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\right.\\
&\left.+\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)\widehat{I_1}\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\right]+16\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right]^2\\
&+8\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[\widehat{I_1}\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\right]\\
&\times\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right].
\end{aligned}
$$

It can be easily seen that, for any fixed $\upsilon \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, when τ ranges over $\mathbb{F}_{2^n}^*$ we have $\frac{1}{(\upsilon^2+\upsilon)\tau}$, $\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}$ and $\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}$ range over $\mathbb{F}_{2^n}^*$. Note that $\sum_{z\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(z)} = -1$ and $\widehat{I_1}(0) = 0$. Then by Lemma 8 we have

$$
\begin{aligned}
&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[\widehat{I_1}^2\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}^2\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I_1}^2\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\right]\\
&\qquad=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{z\in\mathbb{F}_{2^n}^*}\left(\widehat{I_1}^2(z)+\widehat{I_1}^2\left(z\upsilon^2\right)+\widehat{I_1}^2\left(z(\upsilon^2+1)\right)\right)\\
&\qquad=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}3\cdot\left(2^{2n}-\widehat{I_1}^2(0)\right)=3\cdot 2^{2n}\cdot(2^n-2)\,.
\end{aligned}
$$

By Lemma 9, we have

$$
\begin{aligned}
&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I_1}\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)\\
&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(\sum_{u\in\mathbb{F}_{2^n}}\widehat{I_1}(u)\widehat{I_1}(u\upsilon^2)-\widehat{I_1}^2(0)\right)=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(\sum_{u\in\mathbb{F}_{2^n}}\widehat{I_1}(u)\widehat{I_1}(u\upsilon^2)\right)\\
&=2^n(2^n-2)\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\frac{1}{x}+\frac{\upsilon^2}{x})}=2^n(2^n-2)\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\frac{1+\upsilon^2}{x})}=0.
\end{aligned}
$$

Similarly, we have

$$
\begin{aligned}
&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I_1}\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)\widehat{I_1}\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\\
&\qquad=2^n(2^n-2)\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\frac{1}{x}+\frac{\upsilon^2+1}{x})}=0
\end{aligned}
$$

and

$$\begin{aligned}&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)\widehat{I_1}\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\\&=2^n(2^n-2)\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\frac{\upsilon^2}{x}+\frac{\upsilon^2+1}{x})}=0.\end{aligned}$$

We have

$$\begin{aligned}&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right]^2\\
&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left(2-2(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}\right)\\
&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(-2\sum_{\tau\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}+2\left(2^n-1\right)\right)\\
&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(-2\sum_{\tau\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2+\upsilon+1}{(\upsilon^2+\upsilon)\tau}\right)}+2\left(2^n-1\right)\right)\\
&=\begin{cases}\sum\limits_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(-2\sum\limits_{z\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(z)}+2\left(2^n-1\right)\right), & \text{if } n\equiv 1\pmod 2\\
\sum\limits_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_4}\left(-2\sum\limits_{z\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(z)}+2\left(2^n-1\right)\right)\\
+\sum\limits_{\upsilon\in\mathbb{F}_4\setminus\mathbb{F}_2}\left(-2\sum\limits_{z\in\mathbb{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(0)}+2\left(2^n-1\right)\right), & \text{if } n\equiv 0\pmod 2\end{cases}\\
&=\left(2^n-3-(-1)^{\mathrm{Tr}_1^n(1)}\right)2^{n+1}.\end{aligned}$$

We can obtain that

$$\begin{aligned}&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right]\\
&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2+\upsilon+1}{(\upsilon^2+\upsilon)\tau}\right)}-\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I_1}\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)\right)\\
&=\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\left(\sum_{u\in\mathbb{F}_{2^n}}\widehat{I_1}\left(u\right)(-1)^{\mathrm{Tr}_1^n\left(u\frac{\upsilon^2+\upsilon+1}{\upsilon^2}\right)}-\sum_{u\in\mathbb{F}_{2^n}}\widehat{I_1}\left(u\right)\right)\\
&=2^n\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2}{\upsilon^2+\upsilon+1}\right)}-2^n(2^n-2).\end{aligned}$$

Similarly, we have

$$\begin{aligned}&\sum_{\upsilon,\tau\in\mathbb{F}_{2^n}^*:\upsilon\neq 1}\widehat{I}_1\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right]\\&\quad=2^n\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{\mathrm{Tr}_1^n\left(\frac{\upsilon^2+1}{\upsilon^2+\upsilon+1}\right)}-2^n(2^n-2)\end{aligned}$$

and

$$\begin{aligned}&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\widehat{I}_1\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right]\\&\quad=2^n\left(\sum_{\upsilon\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\upsilon^2+\upsilon+1}\right)}-2(-1)^{\mathrm{Tr}_1^n(1)}\right)-2^n(2^n-2)\\&\quad=2^n\left(2\sum_{x\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+1}\right)}-2(-1)^{\mathrm{Tr}_1^n(1)}\right)-2^n(2^n-2)\\&\quad=2^n\left((-1)^{\mathrm{Tr}_1^n(1)}\widehat{I}_1(1)-2(-1)^{\mathrm{Tr}_1^n(1)}\right)-2^n(2^n-2),\end{aligned}$$

where T_0 is defined by Lemma 4 and we make use of this lemma in the last identity. Therefore, by Lemma 5 we immediately get

$$\begin{aligned}&\sum_{\upsilon\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\sum_{\tau\in\mathbb{F}_{2^n}^*}\left[\widehat{I}_1\left(\frac{1}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I}_1\left(\frac{\upsilon^2}{(\upsilon^2+\upsilon)\tau}\right)+\widehat{I}_1\left(\frac{\upsilon^2+1}{(\upsilon^2+\upsilon)\tau}\right)\right]\\&\quad\times\left[(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{(\upsilon^2+\upsilon)\tau}+\frac{1}{\tau}\right)}-1\right]=3\cdot 2^n\left[(-1)^{\mathrm{Tr}_1^n(1)}(\widehat{I}_1(1)-2)-2^n+2\right].\end{aligned}$$

Therefore, we have

$$\begin{aligned}S_1&=3\cdot 2^{2n}\cdot(2^n-2)+2\cdot 0+16\cdot(2^n-3-(-1)^{\mathrm{Tr}_1^n(1)})\cdot 2^{n+1}\\&\quad+8\left[3\cdot 2^n((-1)^{\mathrm{Tr}_1^n(1)}(\widehat{I}_1(1)-2)-2^n+2))\right]\\&=3\cdot 2^{3n}+2^{2n+1}+\left[(-1)^{\mathrm{Tr}_1^n(1)}(3\widehat{I}_1(1)-10)-6\right]\cdot 2^{n+3}.\end{aligned}$$

We now consider the value of S_2. Recall that $U=\{(0,y)\in\mathbb{F}_{2^n}^2:y\in\mathbb{F}_{2^n}^*\}\cup\{(x,0)\in\mathbb{F}_{2^n}^2:x\in\mathbb{F}_{2^n}^*\}\cup\{(x,x)\in\mathbb{F}_{2^n}^2:x\in\mathbb{F}_{2^n}\}$. We have

$$\begin{aligned}S_2&=\sum_{(\tau,\gamma)\in U}\left(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+f(x+\tau)+f(x+\gamma)+f(x+\tau+\gamma)}\right)^2\\&=\sum_{\gamma\in\mathbb{F}_{2^n}^*}2^{2n}+\sum_{\tau\in\mathbb{F}_{2^n}^*}2^{2n}+\sum_{x\in\mathbb{F}_{2^n}}2^{2n}=3\cdot 2^{3n}-2^{2n+1}.\end{aligned}$$

According to what has been discussed above, it can be concluded that

$$S_1+S_2=3\cdot 2^{3n+1}+\left[(-1)^{\mathrm{Tr}_1^n(1)}\left(3\widehat{I}_1(1)-10\right)-6\right]\cdot 2^{n+3}.$$

Then by (3) we can immediately get our assertion and this completes the proof.

Let $g \in \mathcal{B}_n, n \geq 4$, be any quadratic Boolean function. From above result and Theorem 2 we get a bound of distant between I_1 and g. The optimal values of $\|(-1)^{I_1}\|_{U_3}$ is $2^{-\frac{n}{4}}|3 \cdot 2^n - 1|^{\frac{1}{8}}$, that is, $S_1 = 2^{-\frac{n}{4}}|3 \cdot 2^n - 1|^{\frac{1}{8}}$ and $S_2 = 0$.

Now we prove that the Gowers U_3 norm of I_v, $v \in \mathbb{F}_{2^n}^*$, is same as the the Gowers U_3 norm of I_1. It is clear that $\mathbb{F}_{2^n} = \{v^{-1}x : x \in \mathbb{F}_{2^n}\}$ for any nonzero $v \in \mathbb{F}_{2^n}$.

Theorem 6. *Let $n \geq 4$. For any nonzero $v \in \mathbb{F}_{2^n}$, we have $\|(-1)^{I_v}\|_{U_3} = \|(-1)^{I_1}\|_{U_3}$.*

Proof. Let $v \in \mathbb{F}_{2^n}$ be any nonzero element and $u = v^{-1}$. Then we have

$$\begin{aligned}
\|(-1)^{I_v}\|_{U_3} &= 2^{-\frac{n}{2}} \left| \sum_{(\tau,\gamma)\in\mathbb{F}_{2^n}^2} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{I_v(x)+I_v(x+\tau)+I_v(x+\gamma)+I_v(x+\tau+\gamma)} \right)^2 \right|^{\frac{1}{8}} \\
&= 2^{-\frac{n}{2}} \left| \sum_{(\tau,\gamma)\in\mathbb{F}_{2^n}^2} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{v}{x}+\frac{v}{x+\tau}+\frac{v}{x+\gamma}+\frac{v}{x+\tau+\gamma}\right)} \right)^2 \right|^{\frac{1}{8}} \\
&= 2^{-\frac{n}{2}} \left| \sum_{(\tau,\gamma)\in\mathbb{F}_{2^n}^2} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{ux}+\frac{1}{ux+u\tau}+\frac{1}{ux+u\gamma}+\frac{1}{ux+u\tau+u\gamma}\right)} \right)^2 \right|^{\frac{1}{8}} \\
&= 2^{-\frac{n}{2}} \left| \sum_{(\tau',\gamma')\in\mathbb{F}_{2^n}^2} \left(\sum_{x'\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x'}+\frac{1}{x'+\tau'}+\frac{1}{x'+\gamma'}+\frac{1}{x'+\tau'+\gamma'}\right)} \right)^2 \right|^{\frac{1}{8}} \\
&= \|(-1)^{I_1}\|_{U_3},
\end{aligned}$$

where $x' = ux, \tau' = u\tau$ and $\gamma' = u\gamma$.

By Theorem 6, we immediately have the following result.

Corollary 1. *Let $n \geq 4$ be a positive integer. The Gowers U_3 norm of inverse function I over $\mathbb{F}_{2^n}$ is*

$$\|(-1)^{I}\|_{U_3} = 2^{-\frac{n}{2}} \left| 3 \cdot 2^{3n+1} + 2^{n+3} \cdot \left[(-1)^{\mathrm{Tr}_1^n(1)} \left(3\widehat{I_1}(1) - 10 \right) - 6 \right] \right|^{\frac{1}{8}},$$

where $\widehat{I_1}(1)$ is given by Lemma 1.

5 On the nonlinearity profile of the multiplicative inverse function

In this section we derive the nonlinearity profile of inverse function. It is known that nonlinearity of an n-variable Boolean function f is related to its maximum absolute Walsh–Hadamard value, that is, $\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\max_{\alpha\in\mathbb{F}_{2^n}} |\widehat{f}(\alpha)|$. In the next results we prove that the Walsh–Hadamard spectrum of some derivatives of the component functions I_v are invariant over nonzero $v \in \mathbb{F}_{2^n}$.

Theorem 7. *Let n be a positive integer and $\tau, \gamma, v \in \mathbb{F}_{2^n}^*$. Then*

$$\widehat{D_\tau(I_v)}(\alpha) = \widehat{D_{v^{-1}\tau}(I_1)}(\alpha v) \text{ and } \widehat{D_{\tau,\gamma}(I_v)}(\alpha) = \widehat{D_{v^{-1}\tau,v^{-1}\gamma}(I_1)}(\alpha v),$$

where $\alpha \in \mathbb{F}_{2^n}$.

Proof. For any $\tau, v \in \mathbb{F}_{2^n}^*$ and $\alpha \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\widehat{D_\tau(I_v)}(\alpha) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{v}{x}+\frac{v}{x+\tau}+\alpha x\right)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{v^{-1}x}+\frac{1}{v^{-1}x+v^{-1}\tau}+\alpha x\right)}\\ &= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{y}+\frac{1}{y+v^{-1}\tau}+(\alpha v)y\right)} = \widehat{D_{v^{-1}\tau}(I_1)}(\alpha v), \text{ where } y = v^{-1}x.\end{aligned}$$

Similarly, for any $\tau, \gamma, v \in \mathbb{F}_{2^n}^*$ and $\alpha \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\widehat{D_{\tau,\gamma}(I_v)}(\alpha) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{v}{x}+\frac{v}{x+\tau}+\frac{v}{x+\gamma}+\frac{v}{x+\tau+\gamma}+\alpha x\right)}\\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{v^{-1}x}+\frac{1}{v^{-1}x+v^{-1}\tau}+\frac{1}{v^{-1}x+v^{-1}\gamma}+\frac{1}{v^{-1}x+v^{-1}\tau+v^{-1}\gamma}+(\alpha v)v^{-1}x\right)}\\ &= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{y}+\frac{1}{y+v^{-1}\tau}+\frac{1}{y+v^{-1}\gamma}+\frac{1}{y+v^{-1}\tau+v^{-1}\gamma}+(\alpha v)y\right)}\\ &= \widehat{D_{v^{-1}\tau,v^{-1}\gamma}(I_1)}(\alpha v), \text{ where } y = v^{-1}x.\end{aligned}$$

By Theorem 7, it is sufficient to calculate the Walsh–Hadamard spectrum of first and second derivative functions of I_1 to derive the nonlinearity of $D_\tau I_v$ and $D_{\tau,\gamma} I_v$, respectively, for any $\tau, \gamma, v \in \mathbb{F}_{2^n}^*$.

Theorem 8. *For any positive integer n and arbitrary $\tau \in \mathbb{F}_{2^n}^*$, we have*

$$\widehat{D_\tau(I_1)}(\alpha) = \begin{cases} 0, & \text{if } \mathrm{Tr}_1^n(\alpha\tau) = 1\\ \widehat{I_1}\left(\frac{y^2}{\tau}\right) + \widehat{I_1}\left(\frac{y^2+1}{\tau}\right) + 2\Big((-1)^{\mathrm{Tr}_1^n(\frac{1}{\tau})} - 1\Big), & \text{if } \mathrm{Tr}_1^n(\alpha\tau) = 0\end{cases},$$

where y is a solution of the equation $y^2 + y + \alpha\tau = 0$.

Proof. Note that for any $\tau \in \mathbb{F}_{2^n}^*$ we have

$$\widehat{D_\tau(I_1)}(\alpha) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\alpha x\right)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+\tau}+\frac{1}{x}+\alpha x+\alpha\tau\right)},$$

where the last identity is obtained replacing x by $x+\tau$. Thus we have $\widehat{D_\tau(I_1)}(\alpha) = 0$ if $\mathrm{Tr}_1^n(\alpha\tau) = 1$. In what follows, we assume that $\mathrm{Tr}_1^n(\alpha\tau) = 0$. From Lemma 3, we have the equation $y^2 + y + \alpha\tau = 0$ have two solutions if $\mathrm{Tr}_1^n(\alpha\tau) = 0$, otherwise no solution. We have

$$\begin{aligned}
\widehat{D_\tau(I_1)}(\alpha) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\alpha x\right)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\alpha\tau x\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1\}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\alpha\tau x\right)} + 2(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1\}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\alpha\tau x\right)} + 2(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\alpha\tau x\right)} + 2\left((-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)} - 1\right) \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+(y^2+y)x\right)} + 2\left((-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)} - 1\right) \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+(x^2+x)y^2\right)} + 2\left((-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)} - 1\right) \\
&= 2\sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} + 2\left((-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)} - 1\right),
\end{aligned}$$

where $T_0 = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(x) = 0\}$ and y is the solution of $y^2 + y + \alpha\tau = 0$. Note that

$$\begin{aligned}
\sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} + \sum_{z\in\mathbb{F}_{2^n}\setminus T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} \\
&= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{z}+\frac{y^2}{\tau} z\right)} = \widehat{(I_1)}\left(\frac{y^2}{\tau}\right),
\end{aligned}$$

and,

$$\begin{aligned}
\sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} - \sum_{z\in\mathbb{F}_{2^n}\setminus T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+(y^2+1)z\right)} \\
&= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{z}+\frac{y^2+1}{\tau} z\right)} = \widehat{(I_1)}\left(\frac{y^2+1}{\tau}\right).
\end{aligned}$$

From above two relations we get

$$2\sum_{z\in T_0} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+y^2 z\right)} = \widehat{(I_1)}\left(\frac{y^2}{\tau}\right) + \widehat{(I_1)}\left(\frac{y^2+1}{\tau}\right),$$

and using this value we get

$$\widehat{D_\tau(I_1)}(\alpha) = \begin{cases} 0, & \text{if } \mathrm{Tr}_1^n(\alpha\tau) = 1 \\ \widehat{I_1}\left(\frac{y^2}{\tau}\right) + \widehat{I_1}\left(\frac{y^2+1}{\tau}\right) + 2\Big((-1)^{\mathrm{Tr}_1^n(\frac{1}{\tau})} - 1\Big), & \text{if } \mathrm{Tr}_1^n(\alpha\tau) = 0 \end{cases}.$$

Corollary 2. *The nonlinearity of two-values functions $D_\tau(I_1)$, $\tau \in \mathbb{F}_{2^n}^*$, is*

$$\mathrm{nl}(D_\tau(I_1)) \geq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}+1}, & \textit{if } n \textit{ is even} \\ 2^{n-1} - P, & \textit{if } n \textit{ is odd} \end{cases},$$

where P is defined in Remark 2.

Proof. We know that for any $\tau \in \mathbb{F}_{2^n}^*$, there always exist a $\alpha \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_1^n(\tau\alpha) = 0$. From Remark 2 and Theorem 8, we get

$$\max_{\alpha \in \mathbb{F}_{2^n}} |\widehat{D_\tau(I_1)}(\alpha)| \leq \begin{cases} 2^{\frac{n}{2}+2}, & \text{if } n \text{ is even} \\ 2P, & \text{if } n \text{ is odd} \end{cases},$$

and from (1) we get the claim.

It is clear that $D_{\tau,\gamma}I_1(x) = \mathrm{Tr}_1^n(\frac{1}{x} + \frac{1}{x+\tau} + \frac{1}{x+\gamma} + \frac{1}{x+\tau+\gamma}) = 0$ for $\tau = 0$ or $\gamma = 0$ or $\tau = \gamma$, so $\widehat{D_{\tau,\gamma}(I_1)}(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\alpha x)} = 2^n$, if $\alpha = 0$, otherwise 0. Thus, we are interested to calculate the Walsh–Hadamard spectrum of $D_{\tau,\gamma}I_1$ for any $\tau, \gamma \in \mathbb{F}_{2^n}^*$ with $\tau \neq \gamma$.

Theorem 9. *Let n be a positive integer and $U = \{(0,\mu) \in \mathbb{F}_{2^n}^2 : \mu \in \mathbb{F}_{2^n}^*\} \cup \{(x,0) \in \mathbb{F}_{2^n}^2 : x \in \mathbb{F}_{2^n}^*\} \cup \{(x,x) \in \mathbb{F}_{2^n}^2 : x \in \mathbb{F}_{2^n}\}$. For any $(\tau,\gamma) \in \mathbb{F}_{2^n}^2 \setminus U$, we have $\widehat{D_{\tau,\gamma}(I_1)}(\alpha) = 0$ if $\mathrm{Tr}(\alpha\tau) = 1$ or $\mathrm{Tr}(\alpha\gamma) = 1$, and*

$$\begin{aligned} \widehat{D_{\tau,\gamma}(I_1)}(\alpha) = {} & \widehat{I_1}\left(\frac{\mu^2}{\gamma^2\tau^{-1}+\gamma}\right) + \widehat{I_1}\left(\frac{\mu^2+1}{\gamma^2\tau^{-1}+\gamma}\right) + \widehat{I_1}\left(\frac{\mu^2+\gamma^2\tau^{-2}}{\gamma^2\tau^{-1}+\gamma}\right) \\ & + \widehat{I_1}\left(\frac{\mu^2+\gamma^2\tau^{-2}+1}{\gamma^2\tau^{-1}+\gamma}\right) + 4\Big((-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)} - 1\Big) \end{aligned}$$

otherwise, where μ is a solution of the equation $\mu^2 + \mu + \gamma^2 y^2 \tau^{-2} + \gamma y^2 \tau^{-1} = 0$ in which y is a solution of the equation $y^2 + y + \alpha\tau = 0$.

Proof. Note that for any $(\tau,\gamma) \in \mathbb{F}_{2^n}^2 \setminus U$, we have

$$\begin{aligned} \widehat{D_{\tau,\gamma}(I_1)}(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\frac{1}{x+\gamma}+\frac{1}{x+\tau+\gamma}+\alpha x\right)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+\tau}+\frac{1}{x}+\frac{1}{x+\tau+\gamma}+\frac{1}{x+\gamma}+\alpha x+\alpha\tau\right)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x+\gamma}+\frac{1}{x+\gamma+\tau}+\frac{1}{x}+\frac{1}{x+\tau}+\alpha x+\alpha\gamma\right)}, \end{aligned}$$

where the second identity is obtained replacing x by $x+\tau$ and the last one is obtained replacing x by $x+\gamma$. Thus we have $\widehat{D_{\tau,\gamma}(I_1)}(\alpha)=0$ if $\mathrm{Tr}_1^n(\alpha\tau)=1$ or $\mathrm{Tr}_1^n(\alpha\gamma)=1$. Thus we assume that $\mathrm{Tr}_1^n(\alpha\tau)=0$ and $\mathrm{Tr}_1^n(\alpha\gamma)=0$ in what follows. We have

$$\begin{aligned}
&\widehat{D_{\tau,\gamma}(I_1)}(\alpha)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\frac{1}{x+\gamma}+\frac{1}{x+\tau+\gamma}+\alpha x\right)}\\
&=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\frac{1}{\tau x+\gamma}+\frac{1}{\tau x+\tau+\gamma}+\alpha\tau x\right)}\\
&=\sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1,\gamma\tau^{-1},1+\gamma\tau^{-1}\}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\frac{1}{\tau x+\gamma}+\frac{1}{\tau x+\tau+\gamma}+\alpha\tau x\right)}+4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)}\\
&=\sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1,\gamma\tau^{-1},1+\gamma\tau^{-1}\}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\frac{1}{\tau(x^2+x)+\gamma^2\tau^{-1}+\gamma}+\alpha\tau x\right)}+4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)}\\
&=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\frac{1}{\tau(x^2+x)+\gamma^2\tau^{-1}+\gamma}+\alpha\tau x\right)}-4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)}+4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)}\\
&=2\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+y^2z\right)}-4(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)}\left(1-(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)}\right),
\end{aligned}$$

where $T_0=\{x\in\mathbb{F}_{2^n}:\mathrm{Tr}_1^n(x)=0\}$ and y is a solution of the equation $y^2+y+\alpha\tau=0$. Note that

$$\begin{aligned}
&\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+y^2z\right)}+\sum_{z\in\mathbb{F}_{2^n}\setminus T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+y^2z\right)}\\
&=\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{z}+\frac{1}{z+\gamma^2\tau^{-1}+\gamma}+\frac{y^2}{\tau}z\right)}\\
&=\begin{cases}0, & \text{if } \mathrm{Tr}_1^n(\alpha\gamma)=1\\ \widehat{I_1}\left(\frac{\mu^2}{\gamma^2\tau^{-1}+\gamma}\right)+\widehat{I_1}\left(\frac{\mu^2+1}{\gamma^2\tau^{-1}+\gamma}\right)+2\left((-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\gamma^2\tau^{-1}+\gamma}\right)}-1\right), & \text{if } \mathrm{Tr}_1^n(\alpha\gamma)=0\end{cases},
\end{aligned}$$

where μ is a solution of the equation $\mu^2+\mu+\gamma^2y^2\tau^{-2}+\gamma y^2\tau^{-1}=0$ and we make use of Theorem 8 in the last identity with $\mathrm{Tr}_1^n((\gamma^2\tau^{-1}+\gamma)y^2\tau^{-1})=\mathrm{Tr}_1^n(\gamma^2y^2\tau^{-2}+\gamma^2y^4\tau^{-2})=\mathrm{Tr}_1^n(\gamma^2\tau^{-2}(y^2+y^4))=\mathrm{Tr}_1^n(\alpha\gamma)$. Similarly, we have

$$\begin{aligned}
&\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+y^2z\right)}-\sum_{z\in\mathbb{F}_{2^n}\setminus T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+y^2z\right)}\\
&=\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{z}+\frac{1}{z+\gamma^2\tau^{-1}+\gamma}+\frac{y^2+1}{\tau}z\right)}\\
&=\begin{cases}0, & \text{if } \mathrm{Tr}_1^n(\alpha\gamma)=1\\ \widehat{I_1}\left(\frac{\nu^2}{\gamma^2\tau^{-1}+\gamma}\right)+\widehat{I_1}\left(\frac{\nu^2+1}{\gamma^2\tau^{-1}+\gamma}\right)+2\left((-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\gamma^2\tau^{-1}+\gamma}\right)}-1\right), & \text{if } \mathrm{Tr}_1^n(\alpha\gamma)=0\end{cases},
\end{aligned}$$

where ν is a solution of the equation $\nu^2+\nu+\gamma^2\tau^{-2}(y^2+1)+\gamma\tau^{-1}(y^2+1)=0$. Note that $\nu=\mu+\gamma\tau^{-1}$ or $\nu=\mu+\gamma\tau^{-1}+1$. Therefore, in the case of $\mathrm{Tr}_1^n(\alpha\tau)=0$

and $\mathrm{Tr}_1^n(\alpha\gamma) = 0$ we have

$$2\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}+y^2z\right)} = \widehat{I_1}\left(\frac{\mu^2}{\gamma^2\tau^{-1}+\gamma}\right)+\widehat{I_1}\left(\frac{\mu^2+1}{\gamma^2\tau^{-1}+\gamma}\right)$$
$$+\widehat{I_1}\left(\frac{\mu^2+\gamma^2\tau^{-2}}{\gamma^2\tau^{-1}+\gamma}\right)+\widehat{I_1}\left(\frac{\mu^2+\gamma^2\tau^{-2}+1}{\gamma^2\tau^{-1}+\gamma}\right)+4\Big((-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)}-1\Big),$$

and hence we can immediately get the value of $\widehat{D_{\tau,\gamma}(I_1)}(\alpha)$ in the case of $\mathrm{Tr}_1^n(\alpha\tau) = 0$ and $\mathrm{Tr}_1^n(\alpha\gamma) = 0$. Recall that $\widehat{D_{\tau,\gamma}(I_1)}(\alpha) = 0$ if $\mathrm{Tr}_1^n(\alpha\tau) = 1$ or $\mathrm{Tr}_1^n(\alpha\gamma) = 1$. This completes the proof.

From above Theorem and Remark 2, we have

$$\max_{\alpha\in\mathbb{F}_{2^n}}|\widehat{D_{\tau,\gamma}(I_1)}(\alpha)|\leq\begin{cases}2^{\frac{n}{2}+3}, & \text{if } n \text{ is even}\\ 4P, & \text{if } n \text{ is odd}\end{cases},$$

where $\tau,\gamma\in\mathbb{F}_{2^n}^*$ with $\tau\neq\gamma$, and we get the next result.

Corollary 3. *Let n be a positive integer and $U = \{(0,\mu)\in\mathbb{F}_{2^n}^2 : \mu\in\mathbb{F}_{2^n}^*\}\cup\{(x,0)\in\mathbb{F}_{2^n}^2 : x\in\mathbb{F}_{2^n}^*\}\cup\{(x,x)\in\mathbb{F}_{2^n}^2 : x\in\mathbb{F}_{2^n}\}$. For any $(\tau,\gamma)\in\mathbb{F}_{2^n}^2\setminus U$, the nonlinearity of two-values functions $D_{\tau,\gamma}(I_1)$ is*

$$\mathrm{nl}(D_{\tau,\gamma}(I_1))\geq\begin{cases}2^{n-1}-2^{\frac{n}{2}+2}, & \textit{if } n \textit{ is even}\\ 2^{n-1}-2P, & \textit{if } n \textit{ is odd}\end{cases},$$

where P is defined in Remark 2.

We now consider lower bounds on the higher-order nonlinearity of the multiplicative inverse function. It is difficult to determine the rth-order nonlinearity of a general function with algebraic degree no less than $r+1$. In [8], Carlet presented a method for obtaining a lower bound on the rth-order nonlinearity of an n-variable Boolean function f, provided that a lower bound on the $(r-1)$th-order nonlinearity of its derivatives $D_\gamma f(x) = f(x)+f(x+\gamma)$, $\gamma\in\mathbb{F}_{2^n}^*$, is known.

Lemma 11 ([8]). *Let f be any n-variable Boolean function and r be a positive integer smaller than n. Then we have*

$$\mathrm{nl}_r(f)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2\sum_{\gamma\in\mathbb{F}_{2^n}}\mathrm{nl}_{r-1}(D_\gamma f)}.$$

By Corollary 2 and Lemma 11 we can get a lower bound on the second-order nonlinearity of the multiplicative inverse function.

Theorem 10. *For any arbitrary integer $n\geq 4$, we have*

$$\mathrm{nl}_2(I_1)\geq\begin{cases}2^{n-1}-\frac{1}{2}\sqrt{2^{\frac{3n}{2}+2}-2^{\frac{n}{2}+2}+2^n}, & \textit{if } n \textit{ is even}\\ 2^{n-1}-\frac{1}{2}\sqrt{2^{n+1}P-2P+2^n}, & \textit{if } n \textit{ is odd}\end{cases},$$

where P is defined in Remark 2.

Let $f \in \mathcal{B}_n$ be an arbitrary Boolean function, applying two times Lemma 11, we can obtain that

$$\mathrm{nl}_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\gamma \in \mathbb{F}_{2^n}} \sqrt{2^{2n} - 2\sum_{\eta \in \mathbb{F}_{2^n}} \mathrm{nl}_{r-2}\left(D_{\gamma,\eta}(f)\right)}}. \qquad (13)$$

Then by Corollary 3 we can get a lower bound on the third-order nonlinearity of the multiplicative inverse function.

Theorem 11. *For any arbitrary integer $n \geq 5$, we have*

$$\mathrm{nl}_3(I_1) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{\frac{3n}{2}+3} + 2^{n+1} - 2^{\frac{n}{2}+4}}}, & \textit{if } n \textit{ is even} \\ 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{n+2}P + 2^{n+1} - 8P}}, & \textit{if } n \textit{ is odd} \end{cases},$$

where P is defined in Remark 2.

Proof. Let us first consider even n. Note that $\mathrm{nl}\left(D_{\gamma,\eta}(I_1)\right) = 0$ if $\gamma = 0$ or $\eta = 0$ or $\gamma = \eta$. By (13) and Corollary 3 we have

$$\begin{aligned}\mathrm{nl}_3(I_1) &\geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\gamma \in \mathbb{F}_{2^n}} \sqrt{2^{2n} - 2\sum_{\eta \in \mathbb{F}_{2^n}} \mathrm{nl}\left(D_{\gamma,\eta}(I_1)\right)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^n + \sum_{\gamma \in \mathbb{F}_{2^n}^*} \sqrt{2^{2n} - 2\sum_{\eta \in \mathbb{F}_{2^n}} \mathrm{nl}\left(D_{\gamma,\eta}(I_1)\right)}} \\ &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{2n} - 2(2^n-2)\left(2^{n-1} - 2^{\frac{n}{2}+2}\right)}} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{\frac{3n}{2}+3} + 2^{n+1} - 2^{\frac{n}{2}+4}}}.\end{aligned}$$

Similarly, we can get a lower bound on the third-order nonlinearity of the multiplicative inverse function for odd n. This completes the proof.

In what follows, we consider the the nonlinearity profile of the multiplicative inverse function. Let $\tau, \gamma \in \mathbb{F}_{2^n}^*$ such that $\tau \neq \gamma$ and $g \in \mathcal{B}_n$ be an arbitrary function with algebraic degree at most r. We have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\frac{1}{x+\gamma}+\frac{1}{x+\tau+\gamma}\right)+g(x)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\frac{1}{\tau x+\gamma}+\frac{1}{\tau x+\tau+\gamma}\right)+g(\tau x)}\\
&= \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1,\gamma\tau^{-1},1+\gamma\tau^{-1}\}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau x}+\frac{1}{\tau x+\tau}+\frac{1}{\tau x+\gamma}+\frac{1}{\tau x+\tau+\gamma}\right)+g(\tau x)}+(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)}\\
&\qquad\times\left((-1)^{g(0)}+(-1)^{g(\tau)}+(-1)^{g(\gamma)}+(-1)^{g(\tau+\gamma)}\right)\\
&= \sum_{x\in\mathbb{F}_{2^n}\setminus\{0,1,\gamma\tau^{-1},1+\gamma\tau^{-1}\}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\frac{1}{\tau(x^2+x)+\gamma^2\tau^{-1}+\gamma}\right)+g(\tau x)}+(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}+\frac{1}{\tau}\right)}\\
&\qquad\times\left((-1)^{g(0)}+(-1)^{g(\tau)}+(-1)^{g(\gamma)}+(-1)^{g(\tau+\gamma)}\right)\\
&= \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau(x^2+x)}+\frac{1}{\tau(x^2+x)+\gamma^2\tau^{-1}+\gamma}\right)+g(\tau x)}-(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)}\left(1-(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)}\right)\\
&\qquad\times\left((-1)^{g(0)}+(-1)^{g(\tau)}+(-1)^{g(\gamma)}+(-1)^{g(\tau+\gamma)}\right)\\
&= 2\sum_{z\in T_0}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau z}+\frac{1}{\tau z+\gamma^2\tau^{-1}+\gamma}\right)+g'(\tau z)}-(-1)^{\mathrm{Tr}_1^n\left(\frac{\tau}{\gamma^2+\gamma\tau}\right)}\left(1-(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{\tau}\right)}\right)\\
&\qquad\times\left((-1)^{g(0)}+(-1)^{g(\tau)}+(-1)^{g(\gamma)}+(-1)^{g(\tau+\gamma)}\right)\\
&\le 2\sum_{y\in T_0'}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{y}+\frac{1}{y+\gamma^2\tau^{-1}+\gamma}\right)+g'(y)}+8,
\end{aligned}$$

where $T_0=\{x^2+x : x\in\mathbb{F}_{2^n}\}$, $T_0'=\{\tau z : z\in T_0\}$, and $g'(\tau z)=g(\tau\mathcal{L}(z))$ where $\mathcal{L}(z)$ is the root of $x^2+x+z=0$ expressed by z which is linear over $\mathbb{F}_{2^n}$ (see, e.g. [10]) and hence both $g'(\tau z)$ and $g'(y)$ still have algebraic degree at most r. Note that

$$\begin{aligned}
d_H\left(D_{\tau,\gamma}(I_1),g\right) &= 2^{n-1}-\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\frac{1}{x+\tau}+\frac{1}{x+\gamma}+\frac{1}{x+\tau+\gamma}\right)+g(x)}\\
&\ge 2^{n-1}-\sum_{y\in T_0'}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{y}+\frac{1}{y+\gamma^2\tau^{-1}+\gamma}\right)+g'(y)}-4.
\end{aligned}$$

It was pointed by Carlet in [8, Proposition 1] that, for any n-variable Boolean function f and an affine hyperplane $\mathcal{H}$ of $\mathbb{F}_{2^n}$, the rth-order nonlinearity of the restriction of f to $\mathcal{H}$ (viewed as an $(n-1)$-variable function), denoted by $f|\mathcal{H}$, satisfies $\mathrm{nl}_r(f|\mathcal{H})\ge\mathrm{nl}_r(f)-2^{n-2}$. Note that T_0' is a hyperplane of $\mathbb{F}_{2^n}$ and $g'(y)$ has algebraic degree at most r when it restricts to an affine hyperplane (viewed as an $(n-1)$-variable function). Then we have

$$\sum_{y\in T_0'}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{y}+\frac{1}{y+\gamma^2\tau^{-1}+\gamma}\right)+g'(y)}$$

$$\begin{aligned}
&= 2^{n-1} - 2w_H\left(\mathrm{Tr}_1^n\left(\frac{1}{y} + \frac{1}{y+\gamma^2\tau^{-1}+\gamma}\right) + g'(y)\right)\\
&\le 2^{n-1} - 2\mathrm{nl}_r(D_{\gamma^2\tau^{-1}+\gamma}(I_1)|T_0')\\
&\le 2^{n-1} - 2\left(\mathrm{nl}_r(D_{\gamma^2\tau^{-1}+\gamma}(I_1)) - 2^{n-2}\right)\\
&= 2^n - 2\mathrm{nl}_r(D_{\gamma^2\tau^{-1}+\gamma}(I_1)).
\end{aligned}$$

So we have

$$d_H\left(D_{\tau,\gamma}(I_1), g\right) \ge 2\mathrm{nl}_r(D_{\gamma^2\tau^{-1}+\gamma}(I_1)) - 2^{n-1} - 4.$$

Moreover, Carlet proved in [8] that, for any $a \in \mathbb{F}_{2^n}^*$, $\mathrm{nl}_r(D_a(I_1)) \ge 2\mathrm{nl}_r(I_{a^{-1}}) - 2^{n-1} - 2 = 2\mathrm{nl}_r(I_1) - 2^{n-1} - 2$. Therefore, we have $\mathrm{nl}_r(D_{\tau,\gamma}(I_1)) \ge 2\mathrm{nl}_r(D_{\gamma^2\tau^{-1}+\gamma}(I_1))$ $-2^{n-1} - 4 \ge 4\mathrm{nl}_r(I_1) - 3\cdot 2^{n-1} - 8$. Thus, we can present a recursive lower bound on the nonlinearity profile of the multiplicative inverse function.

Theorem 12. *Let $n \ge 6$ be an arbitrary integer. Then for any $4 \le r \le n-2$, we have*

$$\mathrm{nl}_r(I_1) \ge 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{2n+2} - (2^{n+3}-16)\,\mathrm{nl}_{r-2}(I_1) + 3\cdot 2^{n+1} - 32}},$$

where $\mathrm{nl}_2(I_1)$ and $\mathrm{nl}_3(I_1)$ are given by Theorems 10 and 11 respectively.

Proof. By (13) we have

$$\begin{aligned}
\mathrm{nl}_r(I_1) &\ge 2^{n-1} - \frac{1}{2}\sqrt{\sum_{\gamma\in\mathbb{F}_{2^n}}\sqrt{2^{2n} - 2\sum_{\eta\in\mathbb{F}_{2^n}}\mathrm{nl}_{r-2}\left(D_{\gamma,\eta}(I_1)\right)}}\\
&= 2^{n-1} - \frac{1}{2}\sqrt{2^n + \sum_{\gamma\in\mathbb{F}_{2^n}^*}\sqrt{2^{2n} - 2\sum_{\eta\in\mathbb{F}_{2^n}}\mathrm{nl}_{r-2}\left(D_{\gamma,\eta}(I_1)\right)}}\\
&\ge 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{2n} - 2(2^n-2)\left(4\mathrm{nl}_{r-2}(I_1) - 3\cdot 2^{n-1} - 8\right)}}\\
&= 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^n-1)\sqrt{2^{2n+2} - (2^{n+3}-16)\,\mathrm{nl}_{r-2}(I_1) + 3\cdot 2^{n+1} - 32}}.
\end{aligned}$$

This completes the proof.

Remark 4. With the help of computer, we check that our bounds on second-order and third-order nonlinearity are little better than that bounds given by Carlet in [8]. For rth-order nonlinearity with $r \ge 4$, the expression becomes more and more complex when r increases.

6 Conclusion

In this paper we study certain cryptographic properties of S-boxes. We derive the second-order differential spectrum of the inverse function and prove that the function defined over $\mathbb{F}_{2^n}$ have an error (bias) with probability $\frac{1}{2^{n-2}}$ and that error occurs for several values of inputs. These errors (biases) were not identified in [5], where the authors derived several properties of FBCT of inverse function. Next, we introduce the Gowers uniformity norm on S-boxes, which is also dependent on the derivatives of its component functions. Correlation with degree two functions can be identified in this manner. For the first time, we used the Gowers norm to study the properties of the inverse function. Further, the nonlinearity profile of inverse function are presented using Gowers norm and Walsh–Hadamard spectrum of its component functions and their linear combinations. In certain cases our bounds slightly improve the ones in [8]. Our results have implications towards Block cipher cryptanalysis where inverse functions are used as basic components.

References

1. A. Bar-On, O. Dunkelman, N. Keller, and A. Weizman. *DLCT: A new tool for differential-linear cryptanalysis.* Eurocrypt 2019, LNCS, 11476:313–342, 2019.
2. E. Biham and A. Shamir. *Differential cryptanalysis of DES-like cryptosystems.* Journal of Cryptology, 4(1):3–72 1991.
3. E. Biham and A. Shamir. *Differential cryptanalysis of the full 16-round DES.* Crypto 1992, LNCS, 740:487–496 1992.
4. E. Biham, O. Dunkelman, and N. Keller. *Enhancing differential-linear cryptanalysis.* Asiacrypt 2002, LNCS, 2501:254–266 2002.
5. H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier. *On the Feistel Counterpart of the Boomerang Connectivity Table Introduction and Analysis of the FBCT.* IACR Transactions on Symmetric Cryptology 2020(1):331–362 2020.
6. C. Boura and A. Canteaut. *On the boomerang uniformity of cryptographic S-boxes.* IACR Transactions on Symmetric Cryptology, 2018(3):290310, 2018.
7. L. Carlitz. *Kloosterman sums and finite field extensions.* Acta Arithmetica, 2(16):179–194 1969.
8. Claude Carlet. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. *IEEE Transactions on Information Theory*, 54(3):1262–1272, 2008.
9. C. Carlet. *Boolean functions for cryptography and error correcting codes.* Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 2:257–397 2010.
10. Chin-Long Chen. Formulas for the solutions of quadratic equations over GF(2^m). *IEEE Trans. Information Theory*, 28(5):792–794, 1982.
11. V. Y-W. Chen. *The Gowers' norm in the testing of Boolean functions.* PhD thesis, Massachusetts Institute of Technology, 2009.
12. C. Cid, T. Huang, T. Peyrin,Y. Sasaki and L. Song. *Boomerang connectivity table: a new cryptanalysis tool.* Eurocrypt 2018, LNCS, 10821:683–714 2018.

13. O. Dunkelman, S. Indesteege, and N. Keller. *A differential-linear attack on 12-Round Serpent.* Indocrypt 2008, LNCS, 5365:308–321 2008.
14. J. Daemen, L. Knudsen, V. Rijmen. *The block cipher Square.* FSE 1997, LNCS, 1267:149–165 1997.
15. W. T. Gowers. *A new proof of szemeredi's theorem.* Geometric and Functional Analysis, 11(3):465–588 2001.
16. B. Green and T. Tao. *An inverse theorem for the Gowers $U^(G)$ norm.* Proceedings of the Edinburgh Mathematical Society, 51(1):73–153 2008.
17. S. Gangopadhyay, B. Mandal and P. Stănică. *Gowers U_3 norm of of some classes of bent Boolean functions.* Designs, Codes and Cryptography, 86(5):1131–1148 2018.
18. T. Huang, I. Tjuawinata, and H. Wu. *Differential-linear cryptanalysis of ICE-POLE.* FSE 2015, LNCS, 9054:243–263 2015.
19. L. Knudsen, D. Wagner. *Integral cryptanalysis (extended abstract)* FSE 2002, LNCS, 2365:112-127 2002.
20. L. Knudsen. *Truncated and higher order differentials.* FSE 1994, LNCS, 1008:196–211 1995.
21. L. Knudsen. *DEAL–a 128-bit block cipher.* Technical report no. 151. Department of Informatics, University of Bergen, Norway.
22. L. R. Knudsen. *Partial and higher order differentials and applications to the DES.* BRICS Report Series, RS–95–9 1995.
23. G. Lachaud and J. Wolfmann. *The weights of the orthogonals of the extended quadratic binary goppa codes.* IEEE Transactions on Information Theory, 36(3):686–692 1990.
24. S. K. Langford and M. E. Hellman. *Differential-linear cryptanalysis.* Crypto 1994, LNCS, 839:17–25 1994.
25. G. Leurent. *Improved differential-linear cryptanalysis of 7-round Chaskey with partitioning.* Eurocrypt 2016, LNCS, 9665:344–371 2016.
26. F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes,* 16, Elsevier 1977.
27. M. Matsui. *Linear cryptanalysis method for DES cipher.* Eurocrypt 1993, LNCS, 765:386–397 1993.
28. K. Nyberg. *Differentially uniform mappings for cryptography.* Eurocrypt 1993, LNCS, 765:55–64 1994.
29. K Nyberg. *The extended autocorrelation and Boomerang tables and Links between nonlinearity properties of vectorial Boolean functions.* Cryptology ePrint Archive 1381 2019.
30. C. E. Shannon, *A mathematical theory of cryptography,* Bell System Technical Memo MM 45-110-02, September 1, 1945.
31. A Shamir. *Impossible differential attacks.* Crypto 1998 rump session.
32. A. Samorodnitsky. *Low-degree tests at large distances.* STOC 2007: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, 506–515 2007.
33. T. Tao. *Structure and randomness in combinatorics.* FOCS 2007, IEEE Computer Society, 3–15 2007.
34. Y. Todo. *Structural evaluation by generalized integral property.* Eurocrypt 2015, LNCS, 9056:287–314 2015.
35. D. Tang, B. Mandal and S. Maitra. *Vectorial Boolean functions with very low differential-linear uniformity using Maiorana–McFarland type construction.* Indocrypt 2019, LNCS, 11898:341–360 2019.
36. D. Wagner. *The boomerang attack.* FSE 1999, LNCS, 1636:156–170 1999.
37. H. Wang and T. Peyrin. *Boomerang switch in multiple rounds.* IACR Transactions on Symmetric Cryptology, 2019(1):142–169, 2019.

38. X. Lai. *Higher order derivatives and differential cryptanalysis.* Communications and Cryptography, 276:227–233 1994.