GOWERS $U_2$ NORM AS A MEASURE OF NONLINEARITY FOR BOOLEAN FUNCTIONS AND THEIR GENERALIZATIONS

SUGATA GANGOPADHYAY
Department of Computer Science and Engineering
Indian Institute of Technology Roorkee
Roorkee 247667, India

CONSTANZA RIERA
Department of Computer Science, Electrical Engineering and Mathematical Sciences
Western Norway University of Applied Sciences
5020 Bergen, Norway

PANTELIMON STĂNICĂ*
Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943, USA

(Communicated by Claude Carlet)

Abstract. In this paper, we investigate the Gowers $U_2$ norm for generalized Boolean functions, and $Z$-bent functions. The Gowers $U_2$ norm of a function is a measure of its resistance to affine approximation. Although nonlinearity serves the same purpose for the classical Boolean functions, it does not extend easily to generalized Boolean functions. We first provide a framework for employing the Gowers $U_2$ norm in the context of generalized Boolean functions with cryptographic significance, in particular, we give a recurrence rule for the Gowers $U_2$ norms, and an evaluation of the Gowers $U_2$ norm of functions that are affine over spreads. We also give an introduction to $Z$-bent functions, as proposed by Dobbertin and Leander [8], to provide a recursive framework to study bent functions. In the second part of the paper, we concentrate on $Z$-bent functions and their $U_2$ norms. As a consequence of one of our results, we give an alternate proof to a known theorem of Dobbertin and Leander, and also find necessary and sufficient conditions for a function obtained by gluing $Z$-bent functions to be bent, in terms of the Gowers $U_2$ norms of its components.

1. Introduction

Boolean functions are functions mapping binary strings to 0 or 1. Over the years, several generalizations of Boolean functions have been proposed. In this paper, we consider such a generalization for which the domain set remains the same as for classical Boolean functions but the range is the set of integers modulo a positive integer $q \geq 2$. These generalized Boolean functions have evolved to an active area of research [11, 12, 14, 16, 17, 18, 20, 23, 24, 25, 26, 27, 29] due to several possible applications in communications and cryptography.
Boolean functions which are maximally resistant to affine approximation have special significance. The idea of nonlinearity is developed and extensively studied for classical Boolean functions. In the case of classical Boolean functions on an even number of variables, the functions with the highest possible nonlinearity are called bent functions [22] (see [3] and references therein, for more recent work on the subject). The concept of nonlinearity does not extend easily to the generalized setup. In the first part of the paper we investigate the Gowers $U_2$ norm as a possible alternative to nonlinearity for measuring the resistance to affine approximation. As examples, we provide the expressions of the Gowers $U_2$ norms for the generalized bent functions, plateaued functions, functions that are affine over spreads, and a recurrence rule for the Gowers $U_2$ norms.

Characterization of bent Boolean functions is a longstanding open problem. One of the roadblocks faced by the researchers has been the absence of recurrence rules within the set of bent Boolean functions. Dobbertin and Leander [8] introduced the notion of $\mathbb{Z}$-bent functions in order to put bent functions in a recursive framework at the cost of leaving the space of Boolean functions, and replacing it with the one of $\mathbb{Z}$-bent functions of different levels. Here, we further obtain some recurrences of Gowers $U_2$ norms of $\mathbb{Z}$-bent functions, and a necessary and sufficient condition involving Gowers $U_2$ norms of four $\mathbb{Z}$-bent functions of level 1 so that bent functions are always obtained by the “gluing” process proposed by Dobbertin and Leander [8].

2. Preliminaries

2.1. Generalized Boolean functions. Let $\mathbb{F}_2$ be the finite field containing two elements; $\mathbb{C}, \mathbb{R}, \mathbb{Z}$ be the fields of complex numbers, real numbers, and the ring of integers respectively. The cardinality of a set $S$ is denoted by $\#S$. For any positive integer $n$, let $\mathbb{F}_2^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, 1 \leq i \leq n\}$ be a vector space over $\mathbb{F}_2$. Let $\mathbb{Z}_q$ be the ring of integers modulo $q$, where $q$ is a positive integer. By ‘$+$’ and ‘$-$’ we respectively denote addition and subtraction modulo $q$, whereas ‘$\oplus$’ denotes the addition over $\mathbb{F}_2^n$. Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, respectively, $\mathbb{Z}_q, q > 2$, is a Boolean, respectively, generalized Boolean function, in $n$ variables, and the set of all such functions is denoted by $\mathcal{B}_n$, respectively, $\mathcal{GB}_n^q$. The character form of a generalized Boolean function $f \in \mathcal{GB}_n^q$, $\chi_f : \mathbb{F}_2^n \rightarrow \mathbb{C}$, is defined by $\chi_f(x) = \zeta_q^{f(x)}$, for all $x \in \mathbb{F}_2^n$, where $\zeta_q = e^{2\pi i/q}$. The algebraic normal form (ANF) of $f \in \mathcal{B}_n$ is the polynomial representation $f(x) = \bigoplus_{a \in \mathbb{F}_2^n} \mu_a x_1^{a_1} \cdots x_n^{a_n}$, where $x = (x_1, \ldots, x_n), \ a = (a_1, \ldots, a_n)$, and $\mu_a \in \mathbb{F}_2$. If $q = 2^k$ for some $k \geq 1$ we can associate to any $f \in \mathcal{GB}_n^q$ a unique sequence of Boolean functions $a_i \in \mathcal{B}_n, 0 \leq i < k$, such that

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x),$$

for all $x \in \mathbb{F}_2^n$.

The (Hamming) weight of $x \in \mathbb{F}_2^n$, denoted by $wt(x)$, is the number of nonzero coordinates in $x$, and the (Hamming) weight of a Boolean function $f$ is $wt(f) = \#\{x \in \mathbb{F}_2^n : f(x) \neq 0\}$. The (Hamming) distance $d(f, g)$ between two functions $f, g$ is the weight of their sum. The algebraic degree of $f$ is $\deg(f) = \max\{wt(a) : a \in \mathbb{F}_2^n, \mu_a \neq 0\}$. The Boolean functions having algebraic degree at most one are affine functions.

For a (generalized) Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{Z}_q$ we define the (generalized) Walsh-Hadamard transform to be the complex valued function
\[ \mathcal{H}_f^{(q)}(u) = \sum_{x \in \mathbb{F}_q^n} \zeta_q(x) (-1)^{u \cdot x}, \]

where \( u \cdot x = \bigoplus_{1 \leq i \leq n} u_i x_i \). For \( q = 2 \), we obtain the usual Walsh-Hadamard transform \( W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{u \cdot x} \). The autocorrelation of \( f \in \mathcal{GB}_q^n \) is defined by

\[ C_f^{(q)}(u) = \sum_{x \in \mathbb{F}_q^n} \zeta_q(x) f(x) (-1)^{u \cdot u}. \]

We shall use the identity \[26\]

\[ C_f^{(q)}(u) = 2^{-n} \sum_{x \in \mathbb{F}_q^n} |\mathcal{H}_f^{(q)}(x)|^2 (-1)^{u \cdot x}. \]

A function \( f : \mathbb{F}_q^n \rightarrow \mathbb{Z}_q \) is called generalized bent (gbent) if \( |\mathcal{H}_f^{(q)}(u)| = 2^{n/2} \) for all \( u \in \mathbb{F}_q^n \). Further, we say that \( f \in \mathcal{GB}_q^n \) is called \( s \)-plateued if \( |\mathcal{H}_f^{(q)}(u)| \in \{0, 2^{(n+s)/2}\} \) for all \( u \in \mathbb{F}_q^n \), for a fixed integer \( s \) depending on \( f \). For simplicity of notation, when \( q \) is fixed, we sometimes use \( \zeta \), \( \mathcal{H} \), \( C \) instead of \( \zeta_q \), \( \mathcal{H}_f^{(q)} \), and \( C_f^{(q)} \), respectively. We refer the reader to \[11, 16, 15, 20\] and references therein for more on generalized bent functions and their characterizations in terms of their components.

### 2.2. Gowers \( U_2 \) Norm

Let \( g : V \rightarrow C \) be any function on a finite set \( V \) and \( B \subseteq V \). Then \( \mathbb{E}_{x \in B} [g(x)] := \frac{1}{|B|} \sum_{x \in B} g(x) \) is the average of \( f \) over \( B \). Let \( f : V \rightarrow \mathbb{R} \) be any function on a finite set \( V \) and \( B \subseteq V \). Then \( \mathbb{E}_{x \in B} [f(x)] := \frac{1}{|B|} \sum_{x \in B} f(x) \) is the average of \( f \) over \( B \). If \( f : \mathbb{F}_q^n \rightarrow \mathbb{R} \), as in \[5\], Definition 2.2.1, for every \( \ell \in \mathbb{Z}^+ \), we define the \( \ell \)th-order Gowers uniformity norm (the Gowers \( U_\ell \) norm, or simply the \( U_\ell \) norm) of \( f \) to be

\[ \|f\|_{U_\ell} = \left( \mathbb{E}_{x \in \mathbb{F}_q^n} \left[ \prod_{S \subseteq [\ell]} f \left( x \oplus \bigoplus_{i \in S} h_i \right) \right] \right)^{\frac{1}{2^\ell}}. \]

If \( f : \mathbb{F}_q^n \rightarrow \mathbb{C} \) is a complex-valued function, we define the Gowers norm by

\[ \|f\|_{U_\ell} = \left( \mathbb{E}_{x \in \mathbb{F}_q^n} \left[ \prod_{S \subseteq [\ell]} C^{\#S} f \left( x \oplus \bigoplus_{i \in S} h_i \right) \right] \right)^{\frac{1}{2^\ell}}, \]

where \( C \) is the complex conjugation operator, and \( [\ell] = \{1, \ldots, \ell\} \). Since in this paper we shall be using the Gowers \( U_2 \) norm for \( f : \mathbb{F}_2^n \rightarrow \mathbb{C} \), we give it explicitly below:

\[ \|f\|_{U_2} = \left( \mathbb{E}_{x \in \mathbb{F}_2^n} \left[ f(x) f(x \oplus h_1) f(x \oplus h_2) f(x \oplus h_1 \oplus h_2) \right] \right)^{1/4}, \]

\[ = \left( \mathbb{E}_{h_1 \in \mathbb{F}_2^n} \left[ \mathbb{E}_{x \in \mathbb{F}_2^n} \left[ f(x) f(x \oplus h_1) \right] \right] \right)^{1/4}. \]

We want to point out that the sum-of-squares indicator \[30\] is yet another measure of “nonlinearity” defined for Boolean functions. There is a large body of literature dedicated to this concept (and many others), and one can find such references in \[1, 2, 6, 19\]. We want to point out \[4\], where a nice asymptotic bound has been obtained for the sum-of-squares indicator. Surely, using the Cauchy inequality, one can find an upper bound of the Gowers \( U_2 \) norm in terms of the sum-of-squares indicator, but it will not achieve the purpose of this paper.
Theorem 2.1. It is known (cf. [5, pp. 22–24]) that for \( f : \mathbb{F}_2^n \rightarrow \mathbb{R} \), if there is a polynomial \( P : \mathbb{F}_2^n \rightarrow \{0, 1\} \) of degree \( d \) such that \( \|E_{x \in \mathbb{F}_2^n} f(x)(-1)^{P(x)}\| \geq \epsilon \), then \( \|f\|_{U_{d+1}} \geq \epsilon \), for any \( \epsilon > 0 \). It is also known that for \( d = 1 \) having \( \|f\|_{U_{d+1}} \geq \epsilon \) implies \( \|E_{x \in \mathbb{F}_2^n} f(x)(-1)^{P(x)}\| \geq \epsilon \) for some degree 1 Boolean polynomial. It is natural to investigate the Gowers \( U_2 \) norm as a possible measure of “nonlinearity” for generalized Boolean functions as well as \( \mathbb{Z} \)-bent functions. That is what we aim in this paper.

2.3. Gowers \( U_2 \) norm for generalized Boolean functions and the Walsh–Hadamard coefficients. In the remaining part of this section, and the next section we assume \( q = 2^k \), for some positive integer \( k \). If \( f : \mathbb{F}_2^n \rightarrow \mathbb{Z}_{2^k} \) is a generalized Boolean function, we define the Gowers norm of \( f \) to be the Gowers norm for the character form \( \chi_f := \zeta f \), where \( \zeta = e^{2\pi i/2^k} \) is a complex root of 1.

The first part of our next theorem shown for generalized Boolean functions can be (somewhat) adapted from Chen [5, pp. 22–24], to which we refer for a detailed discussion (for the Boolean case).

**Theorem 2.1.** If \( k \geq 1 \) and \( f : \mathbb{F}_2^n \rightarrow \mathbb{Z}_{2^k} \), then (with \( \chi_f = \zeta f \), where \( \zeta = e^{2\pi i/2^k} \) is a \( 2^k \)-complex root of 1)

\[
\|\chi_f\|_{U_2}^4 = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4 \leq 2^{-2n} \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2.
\]

Moreover, the equality holds if and only if \( f \) is a bent function (\( k = 1 \)), respectively, gbent function (\( k > 1 \)) function, and, then, \( \|\chi_f\|_{U_2}^4 = 2^{-n} \).

**Proof.** If \( f \in \mathcal{GB}_n^k \), using equation (1), we can see that the Gowers \( U_2 \) norm is

\[
\|\chi_f\|_{U_2}^4 = 2^{-3n} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} \zeta f(x) \overline{\zeta f(x \oplus u)} \sum_{v \in \mathbb{F}_2^n} \zeta f(x \oplus v) \overline{\zeta f(x \oplus u \oplus v)}
\]

\[
= 2^{-3n} \sum_{u \in \mathbb{F}_2^n} \left( \sum_{x \in \mathbb{F}_2^n} \zeta f(x) \overline{f(x \oplus u)} \right) \left( \sum_{y \in \mathbb{F}_2^n} \zeta f(y) \overline{f(y \oplus u)} \right)
\]

\[
= 2^{-5n} \sum_{u \in \mathbb{F}_2^n} \left( \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 (-1)^u x \right) \left( \sum_{y \in \mathbb{F}_2^n} |\mathcal{H}_f(y)|^2 (-1)^u y \right)
\]

\[
= 2^{-5n} \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 |\mathcal{H}_f(y)|^2 \left( \sum_{u \in \mathbb{F}_2^n} (-1)^u (x \oplus y) \right) = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4.
\]

Then, using Parseval’s identity, we get that

\[
2^{4n} \|\chi_f\|_{U_2}^4 = \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4 \leq \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 = 2^{2n} \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2.
\]

We will now show that the equality holds if and only if \( f \) is a bent function (\( k = 1 \)), or a gbent function (\( k > 1 \)). If \( f \) is bent (gbent), then, \( |\mathcal{H}_f(x)|^2 = 2^n \), for all \( x \in \mathbb{F}_2^n \). Using (3), we infer

\[
\|\chi_f\|_{U_2}^4 = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4 = 2^{-4n} \cdot 2^n \cdot 2^n = 2^{-n} = 2^{-2n} \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2.
\]

Suppose now that the equality holds, but \( f \) is not gbent (bent). Then, there exists some \( x_0 \) such that \( |\mathcal{H}_f(x_0)|^2 < \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 \). Since the equality holds, from
(3), we get that \( \| \chi_f \|_{U_2}^4 = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4 = 2^{-2n} \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 = 2^{-2n} \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 \). Thus,

\[
\max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 \cdot \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 = 2^{2n} \max_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 > \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4
\]

yielding a contradiction. The reciprocal is immediate. □

We say that \( f, g \in \mathcal{GB}_n^q \) are affine equivalent if \( g(x) = f(Ax \oplus b), \forall x \in \mathbb{F}_2^n \), where \( A \) is an \( n \times n \) nonsingular matrix, and \( b \in \mathbb{F}_2^n \).

**Corollary 1.** If \( f \) and \( g \) are affine equivalent, \( \| \chi_g \|_{U_2}^4 = \| \chi_f \|_{U_2}^4 \).

**Proof.** If \( f \) and \( g \) are affine equivalent, \( \mathcal{H}_g(x) = (-1)^b \cdot \mathcal{H}_f(x(A^{-1})^T) \). Then,

\[
\| \chi_g \|_{U_2}^4 = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_g(x)|^4 = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x(A^{-1})^T)|^4
\]

\[
= 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(y)|^4 = \| \chi_f \|_{U_2}^4,
\]

and the corollary is shown. □

**Corollary 2.** If \( f : \mathbb{F}_2^n \rightarrow \mathbb{C} \) is a complex valued function and the Fourier transform of \( f \) is \( \hat{f}(u) = 2^{-n/2} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{ux} \) then we have \( \| f \|_{U_2}^4 = 2^{-2n} \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)^4 \).

We can also obtain the Gowers \( U_2 \) norm of any plateaued function:

**Proposition 1.** If \( f \) is an \( s \)-plateaued generalized Boolean function in \( \mathcal{GB}_n^q \), where \( q = 2^k \) for some positive integer \( k \), then its Gowers norm is \( \| \chi_f \|_{U_2} = 2^{-(n+s)/4} \).

In particular, the Gowers \( U_2 \) norm of a semibent generalized Boolean function \( f \) is \( \| \chi_f \|_{U_2} = 2^{-(n+s)/4} \) if \( n \) is even, and \( 2^{-(n+1)/4} \) if \( n \) is odd. In general, if \( f \in \mathcal{GB}_n^q \) with \( |\mathcal{H}_f(x)| \in \{0, \lambda_1, \ldots, \lambda_t\} \), of respective multiplicities \( a, m_1, \ldots, m_t \), the Gowers \( U_2 \) norm is \( \| \chi_f \|_{U_2}^4 = \sum_{j=1}^t m_j \lambda_j 2^{-4n} \).

**Proof.** If \( f \) is an \( s \)-plateaued generalized Boolean function, then by definition \( |\mathcal{H}_f(x)| \in \{2^{(n+s)/2}, 0\} \). By Parseval's identity, \( \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^2 = 2^{2n} = a \cdot 2^{n+s} \), where \( a \) is the multiplicity of \( 2^{n+s} \) in \( |\mathcal{H}_f(x)| \). Hence, \( a = 2^{n-s} \). Then, by equation (3), \( \| \chi_f \|_{U_2}^4 = 2^{-4n} \sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_f(x)|^4 = 2^{-4n} \cdot a \cdot 2^{2(n+s)} = 2^{-n+s} \). Therefore, \( \| \chi_f \|_{U_2} = 2^{-(n+s)/4} \). By similar arguments, we can prove the last claim. □

It is well known that the nonlinearity of \( f \in \mathcal{B}_n \) is \( nl(f) = 2^{n-1} - \frac{1}{2} \max_{x \in \mathbb{F}_2^n} |\mathcal{W}_f(x)| \), which means that if a function has high nonlinearity, then \( \max_{x \in \mathbb{F}_2^n} |\mathcal{W}_f(x)| \) is small, and therefore \( \| \chi_f \|_{U_2} \) is upper bounded by a relatively small number.

One can ask whether it is true that \( \| \chi_f \|_{U_2} < \| \chi_g \|_{U_2} \), if \( f, g \in \mathcal{B}_n \) with \( nl(f) < nl(g) \). That is not necessarily true, and we provide an argument below. Let \( f \) be a quadratic Boolean function (so \( k = 1 \)) of rank \( 2h \) \[21\] (under \( f(0) = 0 \), then, by
Proposition 1. \( \|\chi_f\|_{U_2} = 2^{-2h} \). Thus, if \( f_1, f_2 \) are two quadratic Boolean functions of ranks \( 2h_1 < 2h_2 \), respectively, then
\[
\begin{align*}
 nl(f_1) &= 2^{n-1} - 2^{n-h_1-1} < 2^{n-1} - 2^{n-h_2-1} = nl(f_2), \\
 \|\chi_{f_1}\|^4 &= 2^{-2h_1} > 2^{-2h_2} = \|\chi_{f_2}\|^4.
\end{align*}
\]
We can certainly find an infinite class of pairs of Boolean functions \((f, g)\) such that
\[
\text{nl}(f) < \text{nl}(g) \quad \text{and} \quad \|\chi_f\|_{U_2} > \|\chi_g\|_{U_2},
\]
for example, let \( n \) be even, \( g \) be any bent Boolean function, and so, by Theorem 2.1, \( \|\chi_g\|_{U_2} = 2^n \). Let \( f \) now be any semibent Boolean function (with \( f(0) = 0 \)) for \( n \) even, so, by Proposition 1, \( \|\chi_f\|_{U_2} = 2^{-n+2}/4 \), which implies that \( \text{nl}(f) = 2^{n-1} - 2^{n/2} \), \( \|\chi_f\|_{U_2} = 2^{-4n} \max_{x \in F_2^n} W_f(x)^4 \leq 2^{-4n} 2^{(n+2)2n-2} = 2^{-n+2} \). Thus, \( \text{nl}(f) < \text{nl}(g) \), and \( \|\chi_g\|_{U_2} = 2^{-n/4} < \|\chi_f\|_{U_2} = 2^{-n+2}/4 \).

2.4. Gowers \( U_2 \) norm of functions that are affine over spreads. We found in Theorem 2.1 and Proposition 1 the Gowers \( U_2 \) norm of bent and, more generally, plateaued functions. It turns out we can precisely find the Gowers norm of a class of functions that extend in some direction the well-known class of partial spread bent functions, by allowing the function to be affine, not necessarily constant on the elements of a spread.

Let \( q = 2^k \). Let \( n = 2m \), and let \( \{E_0, \ldots, E_{2m}\} \) be a spread of \( F_2^n \), that is, \( E_i \)'s, \( 0 \leq i \leq 2m \), are \( m \)-dimensional subspaces of \( F_2^n \) with trivial intersection. Note that \( \bigcup_{i=0}^{2m} E_i = F_2^n \) [7].

**Theorem 2.1.** Let \( \{E_0, \ldots, E_{2m}\} \) be a spread, and \( f \in \mathcal{G}B^q \). Then:
\[(i)\] If \( f \) is defined by \( f(x) = \sum_{i \in E_i} c_i x \), with arbitrary \( c, c_i \in \mathbb{Z}_q \), then
\[
\|\chi_f\|_{U_2}^4 = 2^{-4n} \left( (2^n - 1) |c^c - A|^4 + |\zeta |^4 + (2^n - 1) A |^4 \right), \text{ where } A := \sum_{i=0}^{2m} \zeta^{c_i}.
\]
\[(ii)\] If \( f \) is defined by \( f(x) = \sum_{i \in E_i} a_i \cdot x \), then \( \|\chi_f\|_{U_2}^4 = 2^{-2n} (2^n + 1) \).

**Proof.** To show (i), we first write
\[
\mathcal{H}_f(u) = \sum_{x \in F_2^n} \zeta^{f(x)} (-1)^{u \cdot x} = \sum_{i=0}^{2m} \sum_{x \in E_i} \zeta^{c_i} (-1)^{u \cdot x} + \zeta^c
\]
\[
= \sum_{i=0}^{2m} \zeta^{c_i} \sum_{x \in E_i} (-1)^{u \cdot x} + \zeta^c = \sum_{i=0}^{2m} \zeta^c = \zeta^c - A + \begin{cases} 2^m A & u = 0, \\
0 & u \neq 0.
\end{cases}
\]
Then
\[
\|\chi_f\|_{U_2}^4 = 2^{-4n} \sum_{x \in F_2^n} |\mathcal{H}_f(x)|^4 = 2^{-4n} \left( (2^n - 1) |c^c - A|^4 + |\zeta |^4 + (2^n - 1) A |^4 \right),
\]
and the first claim is shown.

To show (ii), we write \( \mathcal{H}_f(u) = \sum_{i=0}^{2m} \sum_{x \in E_i} \zeta^{a_i \cdot x} (-1)^{u \cdot x} = \sum_{i=0}^{2m} \sum_{x \in E_i} (-1)^{a_i \cdot x} = 2^m, \) if there exists \( i \) such that \( u = a_i \), and 0 if \( u \neq a_i \) for all \( i \). Therefore, we get
We compute, using [6, Lemma 2.9], the Gowers $(1-\|f\|_U^4) = 2^{-4n} 2^{4m} (2^m + 1) = 2^{-2n} (2^\frac{m}{2} + 1)$, and the theorem is shown. \(\square\)

Note that, from the proof of (ii), it is easy to generalize this result to allow for repeated vectors. However, we do not state this result here, as it is notationally cumbersome.

3. Recurrences for Gowers $U_2$ norms of generalized Boolean functions

We start this section with a lemma, which will be used to derive a formula for the Gowers $U_2$ norms of concatenations of Boolean functions.

**Lemma 3.1.** Let $f_1, f_2 \in \mathcal{B}_n^q$, $q = 2^k$, be $n$-variables generalized Boolean functions and $\zeta$ a $q$-complex root of 1. Then

$$\sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_{f_1}(x)|^2 |\mathcal{H}_{f_2}(x)|^2 = 2^n \sum_{w \in \mathbb{F}_2^n} C_{f_1}(w) C_{f_2}(w).$$

**Proof.** We compute, using [6, Lemma 2.9],

$$\begin{align*}
\sum_{x \in \mathbb{F}_2^n} |\mathcal{H}_{f_1}(x)|^2 |\mathcal{H}_{f_2}(x)|^2 &= \sum_{x \in \mathbb{F}_2^n} \sum_{u \in \mathbb{F}_2^n} \zeta^{f_1(u) - f_1(t)} (-1)^{u \cdot t} x \sum_{v,s \in \mathbb{F}_2^n} \zeta^{f_2(s) - f_2(w)} (-1)^{(v \cdot s) - x} \\
&= \sum_{u,t,v,s \in \mathbb{F}_2^n} \zeta^{f_1(u) - f_1(t) + f_2(w) - f_2(v)} (-1)^{(u \cdot t + v \cdot s) - x} \\
&= 2^n \sum_{u,t,v,s \in \mathbb{F}_2^n} \zeta^{f_1(u) - f_1(t) + f_2(w) - f_2(v)} \\
&= 2^n \sum_{u,t \in \mathbb{F}_2^n} \zeta^{f_1(u) - f_1(t)} C_{f_2}(u \oplus t) 2^{-1} \sum_{u,w \in \mathbb{F}_2^n} \zeta^{f_1(u) - f_1(u \oplus w)} C_{f_2}(w) \\
&= 2^n \sum_{w \in \mathbb{F}_2^n} C_{f_2}(w) \sum_{u \in \mathbb{F}_2^n} \zeta^{f_1(u) - f_1(u \oplus w)} = 2^n \sum_{w \in \mathbb{F}_2^n} C_{f_1}(w) C_{f_2}(w),
\end{align*}$$

and the lemma follows. \(\square\)

We now derive a recurrence for Gowers $U_2$ norms of concatenations of generalized Boolean functions. We use $\Re(a+bi) = a$ for the real part of the complex argument.

**Theorem 3.1.** Let $f : \mathbb{F}_2 \times \mathbb{F}_2^n \rightarrow \mathbb{Z}_q$, where $q = 2^k$, be the concatenation $f = [f_1, f_2]$ of two $n$-variables generalized Boolean functions, $f_1, f_2$, that is, $f(x_1, x) = (1-x_1) f_1(x) + x_1 f_2(x)$. The Gowers $U_2$ norm of $f$ is given recursively by

$$2^4 \|\chi_f\|_{U_2}^4 = \|\chi_{f_1}\|_{U_2}^4 + \|\chi_{f_2}\|_{U_2}^4 + 2^{-4n+1} \sum_{u \in \mathbb{F}_2^n} |\mathcal{H}_{f_1}(u)|^2 |\mathcal{H}_{f_2}(u)|^2$$

$$+ 2^{-4n+2} \sum_{u \in \mathbb{F}_2^n} \Re^2 \left(\frac{\mathcal{H}_{f_1}(u) \overline{\mathcal{H}_{f_2}(u)}}{\|\chi_f\|_{U_2}^2}\right).$$

**Proof.** (Omitted for brevity.)
Proof. If \( f_2 = f_1 \), then \( \| \chi_f \|_{U_2} = \| \chi_{f_1} \|_{U_2} \). If \( f_2 = \bar{f}_1 \), then \( \| \chi_f \|_{U_2} = \frac{1 + \Re^2(\zeta)}{2} \| \chi_{f_1} \|_{U_2} \).

To show the theorem, we need to prove the following:

\[
\| \chi_f \|_{U_2}^4 = \| \chi_{f_1} \|_{U_2}^4 + 2^{3n+1} \sum_{u \in \mathbb{F}_2^n} C_{f_1}(u) C_{f_2}(u) + 2^{-4n+2} \sum_{u \in \mathbb{F}_2^n} \Re^2 \left( \mathcal{H}_{f_1}(u) \overline{\mathcal{H}_{f_2}(u)} \right).
\]

If \( f_2 = f_1 \), then \( \| \chi_f \|_{U_2} = \| \chi_{f_1} \|_{U_2} \). If \( f_2 = \bar{f}_1 \), then \( \| \chi_f \|_{U_2} = \frac{1 + \Re^2(\zeta)}{2} \| \chi_{f_1} \|_{U_2} \).

Using a decomposition result of [24] we can show the next theorem.

We now look at functions \( f : \mathbb{F}_2^n \to \mathbb{Z}_q \), where \( f = a_0 + 2a_1 \), with \( a_0, a_1 \in \mathcal{B}_n \) and find the Gowers \( U_2 \) norm of \( f \) in terms of those of the components \( a_0, a_0 \oplus a_1 \). Using a decomposition result of [24] we can show the next theorem.
Theorem 3.2. Let $f \in GB_n^4$, $f = a_0 + 2a_1$, $a_0, a_1 \in B_n$. Then

$$2^4 \| f \|_{U_2}^4 = \| \chi_{a_1} \|_{U_2}^4 + \| \chi_{a_0 \oplus a_1} \|_{U_2}^4 + 2^{-4n+1} \sum_{x \in F_2^n} \mathcal{W}^2_{a_1}(x) \mathcal{W}^2_{a_0 \oplus a_1}(x)$$

$$= \| \chi_{a_1} \|_{U_2}^4 + \| \chi_{a_0 \oplus a_1} \|_{U_2}^4 + 2^{-3n+1} \sum_{y \in F_2^n} \mathcal{C}_{a_1}(w) \mathcal{C}_{a_0 \oplus a_1}(w).$$

Proof. We know [24] that in the quartic case $| \mathcal{H}_f(x) |^2 = \frac{1}{2} \left( \mathcal{W}^2_{a_1}(x) + \mathcal{W}^2_{a_0 + a_1}(x) \right)$, so $| \mathcal{H}_f(x) |^4 = \frac{1}{4} \left( \mathcal{W}^4_{a_1}(x) + \mathcal{W}^4_{a_0 + a_1}(x) + 2 \mathcal{W}^2_{a_1}(x) \mathcal{W}^2_{a_0 + a_1}(x) \right)$, which by summation renders

$$2^{4(n+1)} \| f \|_{U_2}^4 = 2^{4n} \| \chi_{a_1} \|_{U_2}^4 + 2^{4n} \| \chi_{a_0 \oplus a_1} \|_{U_2}^4 + 2 \sum_{x \in F_2^n} \mathcal{W}^2_{a_1}(x) \mathcal{W}^2_{a_0 + a_1}(x).$$

Further, by Lemma 3.1, we get $\sum_{x \in F_2^n} \mathcal{W}^2_{a_1}(x) \mathcal{W}^2_{a_0 + a_1}(x) = 2^n \sum_{w \in F_2^n} \mathcal{C}_{a_1}(w) \mathcal{C}_{a_0 + a_1}(w),$ and the theorem follows. $\square$

We can certainly derive an expression for the Gowers $U_2$ norm for a generalized $f \in GB_n^k$, but the result is rather quite complicated, unfortunately. The proof is rather similar to the previous one.

Theorem 3.3. Let $f : F_2^k \rightarrow \mathbb{Z}_{2^k}$ given by $f = \sum_{i=0}^{k-1} a_i 2^i$, $a_i \in B_n$. Then,

$$2^{4(n+k-1)} \| f \|_{U_2}^4 = 2^{4n} \sum_{c \in F_2^{k-1}} \| \chi_{a_{k-1} \oplus c} \|_{U_2}^4 | \gamma_c |^4$$

$$+ \sum_{c \neq d \in F_2^{k-1}} \mathcal{W}^2_{a_{k-1} \oplus c}(u) \mathcal{W}^2_{a_{k-1} \oplus d}(u) | \gamma_c |^2 | \gamma_d |^2$$

$$+ \sum_{(c,d) \neq (x,y) \in F_2^{k-1} \times F_2^{k-1}} \mathcal{W}_{a_{k-1} \oplus c}(u) \mathcal{W}_{a_{k-1} \oplus d}(u) \mathcal{W}_{a_{k-1} \oplus x}(u) \mathcal{W}_{a_{k-1} \oplus y}(u) | \gamma_c | | \gamma_d | | \gamma_x | | \gamma_y |,$n

where $c = (c_0, \ldots, c_{k-2}) \in F_2^{k-1}$, $a = (a_0, \ldots, a_{k-2})$, $\gamma_z = \sum_{v \in F_2^{k-1}} (-1)^v \psi^v \zeta_{\sum_j v_j}^z \zeta_{v_j}^2$.}

4. Gowers $U_2$ norm and Z-bent functions

4.1. Z-bent functions. Dobbertin and Leander [8] introduced Z-bent functions to describe bent functions within a recursive framework. They used the normalized Fourier transform to define these functions. Since in this section we need to refer to many of their results, we choose to use the same convention, and work with the Fourier transform defined as $^1 \tilde{f}(u) = 2^{-n/2} \sum_{x \in F_2^n} f(x) (-1)^{u \cdot x}$. The Gowers norm of $f$ given by

$$\| f \|_{U_2}^4 = \left\langle \sum_{x \in F_2^n} \tilde{f}(x) \tilde{f}(x \oplus h_1) \tilde{f}(x \oplus h_2) \tilde{f}(x \oplus h_1 \oplus h_2) \right\rangle$$

will render $\| f \|_{U_2}^4 = 2^{-2n} \sum_{x \in F_2^n} \tilde{f}(x)^4$.

---

$^1$We use the normalized Fourier transform here to agree with the notation in [8].
Prompted by the observation that given two bent functions $g, h$ in $n = 2k$ variables, $k > 1$, the function
\begin{equation}
  f(x) = \frac{\chi_g(x) + \chi_h(x)}{2} \in \{-1, 0, 1\},
\end{equation}
for all $x \in \mathbb{F}_2^k$ will also have its Fourier transform given by $\hat{f}(u) = \frac{\hat{\chi}_g(u) + \hat{\chi}_h(u)}{2} \in \{-1, 0, 1\},$ for all $u \in \mathbb{F}_2^n.$ Dobbertin and Leander [8] defined the notion of $Z$-bent function in the following way. Let $\mathcal{W}_0 = \{-1, 1\}, \mathcal{W}_r = \{\ell \in \mathbb{Z} : -2^{r-1} \leq \ell \leq 2^{r-1}\},$ for $r \geq 1.$ A function $f : \mathbb{F}_2^2 \to \mathbb{Z}$ is a $Z$-bent function of size $k$ level $r$ if $\hat{f}(x) \in \mathcal{W}_r,$ for all $x \in \mathbb{F}_2^2.$ The set of all $Z$-bent functions of size $k$ level $r$ is denoted by $BF_k^r.$ Any function belonging to $\bigcup_{r \geq 0} BF_k^r$ is said to be a $Z$-bent function of size $k.$ If a $Z$-bent function of level $1$ can be written as in (4) then it is said to be splitting, otherwise it is said to be non-splitting. As Dobbertin and Leander did in [8], we refer to a $\pm 1$ function as bent (when we want to point that out we call it $\pm 1$-bent) even though it is the signature of a classical bent Boolean function.

Now, suppose that $h \in BF_k^r$ is the concatenation $h = [h_{00}][h_{01}][h_{10}][h_{11}],$ where $h_{\epsilon_1,\epsilon_2}(x) = h(\epsilon_1, \epsilon_2, x),$ for all $(\epsilon_1, \epsilon_2, x) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{n-2},$ that is, $h(y, z, x) = (y \oplus 1)(z \oplus 1)h_{00}(x) + (y \oplus 1)z h_{01}(x) + y(z \oplus 1)h_{10}(x) + yzh_{11}(x).$ We define the functions $f_{\epsilon_1,\epsilon_2}$ by using the following equations:
\begin{align}
\text{Case 1. For } r &\geq 1: \quad \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} \\
\text{Case 2. For } r &< 0: \quad \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}.
\end{align}

Dobbertin and Leander [8, Proposition 2] showed that if $h$ is a $Z$-bent function of size $k$ and level $r,$ then the functions $f_{\epsilon_1,\epsilon_2}$ are $Z$-bent functions of size $k - 1$ and level $r + 1,$ for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2.$ In other words, if $h \in BF_k^r,$ then $f_{\epsilon_1,\epsilon_2} \in BF_{k-1}^{r+1},$ for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2.$ Conversely, suppose we have $f_{\epsilon_1,\epsilon_2} \in BF_{k+1}^{r-1},$ for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2.$ If $h = [h_{00}][h_{01}][h_{10}][h_{11}],$ then we say that $h$ is obtained by gluing $f_{\epsilon_1,\epsilon_2},$ where $\epsilon_1, \epsilon_2 \in \mathbb{F}_2.$ Although the gluing process in general may not yield a Boolean function, it is known [8, Proposition 2] that all functions in $BF_k^r$ are obtained by gluing functions in $BF_{k+1}^{r-1}.$ We derive the following condition connecting the $Z$-bent functions of level $1$ to (classical) bent functions as a special case of [8, Theorem 3].

**Theorem 4.1.** Let four $Z$-bent functions $f_{00}, f_{01}, f_{10}$ and $f_{11}$ of level $1$ and size $k$ be given such that
\begin{equation}
  f_{00}(x) \equiv f_{01}(x) + 1 \pmod{2}; \quad f_{10}(x) \equiv f_{11}(x) + 1 \pmod{2};
\end{equation}
Then the function $h : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \to \{-1, 1\}$ defined by $h(y, z, x) = h_{yz}(x)$ for all $x \in \mathbb{F}_2^n,$ where $h_{ij}, f_{ij}, 0 \leq i, j \leq 1$ satisfy (6), is a $\pm 1$-bent function (of level $0$).

Due to normalization of the Walsh–Hadamard (Fourier) coefficients of $f : \mathbb{F}_2^n \to \mathbb{R},$ Parseval’s identity takes the form $\sum_{x \in \mathbb{F}_2^n} f(x)^2 = \sum_{x \in \mathbb{F}_2^n} g(x)^2.$

**4.2. Recurrences for Gowers $U_2$ norms of $Z$-bent functions.** Here, we will obtain some recurrences for the Gowers $U_2$ norms of $Z$-bent functions $h \in BF_k^r$ in terms of the $U_2$ Gowers norms of $f_{ij} \in BF_{k-1}^{r+1},$ where $h$ is obtained by gluing $f_{ij},$ $0 \leq i, j \leq 1.$
Theorem 4.2. Let $h : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^k \rightarrow \mathbb{Z}$ be the concatenation $h = [h_{00} \parallel h_{01} \parallel h_{10} \parallel h_{11}]$ of four $n$-variables integer-valued functions $h_{ij}$ $(0 \leq i, j \leq 1)$, satisfying equations (5)–(6), for some integer-valued functions $f_{ij}$. Then, with $\gamma = \frac{1}{2}, 1$, if $r \geq 1$, respectively, $r = 0$, we have

$$\gamma^{-4} \|h\|_{U_2}^4 = 2^{-3} \left( \|f_{00}\|_{U_2}^4 + \|f_{01}\|_{U_2}^4 + \|f_{10}\|_{U_2}^4 + \|f_{11}\|_{U_2}^4 \right) + 3 \cdot 2^{-2(n+1)} \sum_{u \in \mathbb{F}_2^k} \left( \hat{f}_{00}^{-2}(u) \hat{f}_{10}^{-2}(u) + \hat{f}_{01}^{-2}(u) \hat{f}_{11}^{-2}(u) \right).$$

**Proof.** First, observe that, similarly as in Theorem 3.1, the Fourier transform

$$2 \hat{h}(u_1, u_2, u) = \hat{h}_{00}(u) + (-1)^{u_2} \hat{h}_{01}(u) + (-1)^{u_1} \hat{h}_{10}(u) + (-1)^{u_1+u_2} \hat{h}_{11}(u).$$

Using the above identity, the $U_2$ Gowersnorm of $h$ is then

$$2^{2(n+2)} \|h\|_{U_2}^4 = \sum_{(u_1, u_2, u) \in \mathbb{F}_2^2} \hat{h}(u_1, u_2, u)$$

$$= 2^{-2} \sum_{u \in \mathbb{F}_2^k} \left( \hat{h}_{00}^{-2}(u) + \hat{h}_{01}^{-2}(u) + \hat{h}_{10}^{-2}(u) + \hat{h}_{11}^{-2}(u) \right)$$

$$+ 3 \cdot 2^{-1} \sum_{u \in \mathbb{F}_2^k} \left( \hat{h}_{00}^{-2}(u) \hat{h}_{01}^{-2}(u) + \hat{h}_{02}^{-2}(u) \hat{h}_{10}^{-2}(u) + \hat{h}_{00}^{-2}(u) \hat{h}_{11}^{-2}(u) \right)$$

$$+ 6 \sum_{u \in \mathbb{F}_2^k} \hat{h}_{00}(u) \hat{h}_{01}(u) \hat{h}_{10}(u) \hat{h}_{11}(u)$$

$$= 2^{2n-2} \left( \|h_{00}\|_{U_2}^4 + \|h_{01}\|_{U_2}^4 + \|h_{10}\|_{U_2}^4 + \|h_{11}\|_{U_2}^4 \right) + 3 \cdot 2^{-1} A + 6 B,$$

where $A$ and $B$ denote the last two sums in the previous equation. We will go further, and we shall replace these expressions in terms of the $U_2$ Gowers norms of $f_{ij}$ and the Fourier coefficients of the $f_{ij}$, $0 \leq i, j \leq 1$.

We treat concurrently equations (5) and (6) by denoting $\gamma = \frac{1}{2}, 1$, if $r \geq 1$, respectively, $r = 0$. Thus, $h_{00} = \gamma(f_{00} + f_{01}), h_{10} = \gamma(f_{10} + f_{11}), h_{01} = \gamma(f_{00} - f_{01}), h_{11} = \gamma(f_{01} - f_{11})$, and so, $h_{00} = \gamma(f_{00} + f_{01}), h_{10} = \gamma(f_{10} + f_{11}), h_{01} = \gamma(f_{00} - f_{01}), h_{11} = \gamma(f_{10} - f_{11})$. Using the last equation of (8), expanding and canceling terms (this is a straightforward, albeit cumbersome computation), we obtain

$$2^{2(n+2)} \|h\|_{U_2}^4 = 2^{\gamma^4} \sum_{u \in \mathbb{F}_2^k} \left( \hat{f}_{00}^{-4}(u) + \hat{f}_{01}^{-4}(u) + \hat{f}_{10}^{-4}(u) + \hat{f}_{11}^{-4}(u) \right)$$

$$+ 3 \cdot 2^{\gamma^4} \sum_{u \in \mathbb{F}_2^k} \left( \hat{f}_{00}^{-2}(u) \hat{f}_{10}^{-2}(u) + \hat{f}_{01}^{-2}(u) \hat{f}_{11}^{-2}(u) \right)$$

$$= 2^{2n+1} \gamma^4 \left( \|f_{00}\|_{U_2}^4 + \|f_{01}\|_{U_2}^4 + \|f_{10}\|_{U_2}^4 + \|f_{11}\|_{U_2}^4 \right)$$

$$+ 3 \cdot 2^{\gamma^4} \sum_{u \in \mathbb{F}_2^k} \left( \hat{f}_{00}^{-2}(u) \hat{f}_{10}^{-2}(u) + \hat{f}_{01}^{-2}(u) \hat{f}_{11}^{-2}(u) \right),$$

which gives, in particular, a recurrence between the $U_2$ Gowers norm of $h \in BF_r^k$ and the $U_2$ Gowers norms of $f_{ij} \in BF_r^{k-1}$.

We can easily get a proof for Theorem 4.1 of Dobbertin-Leander [8].
Corollary 3. If $f_{ij}$ in the theorem above are $\mathbb{Z}$-bent functions and satisfy also equation (7), then the function $h$ obtained from gluing $f_{ij}$ is bent.

Proof. If $f_{ij}$ in the theorem above satisfy equation (7) and have level 1 (that is, $r = 0$), then $f_{ij}, \hat{f}_{ij} \in \{0, \pm 1\}$, and, since $f_{00}(x) \equiv f_{01}(x) + 1 \pmod{2}$, $f_{10}(x) \equiv f_{11}(x) + 1 \pmod{2}$ the function $h$ has values $\pm 1$, and is then the signature of a Boolean function. Moreover, since

$$\hat{f}_{00}(u) \equiv \hat{f}_{10}(u) + 1 \pmod{2}, \quad \hat{f}_{01}(u) \equiv \hat{f}_{11}(u) + 1 \pmod{2},$$

and $f_{ij}, \hat{f}_{ij} \in \{0, \pm 1\}$, then the second powers also satisfy the same relations and further,

$$\hat{f}_{00}^2(u) + \hat{f}_{10}^2(u) = 1, \quad \hat{f}_{01}^2(u) + \hat{f}_{11}^2(u) = 1,$$

$$\hat{f}_{00}^4(u) + \hat{f}_{10}^4(u) = 1, \quad \hat{f}_{01}^4(u) + \hat{f}_{11}^4(u) = 1.$$

Thus, $\hat{f}_{00}^2(u)\hat{f}_{10}^2(u) = 0, \hat{f}_{01}^2(u)\hat{f}_{11}^2(u) = 0$. Using these equations in the first displayed identity of Theorem 4.2 renders (with $\gamma = 1$), $2^{2(n+2)} \|h\|_{U_2}^4 = 2 \cdot 2^{n+1} + 0 = 2^{n+2}$, yielding $\|h\|_{U_2}^4 = 2^{-n-2}$, which implies that $h$ is bent.

\[\square\]

4.3. An alternative proof and an extension of a theorem by Dobbertin and Leander. In this section, we first give an extension of a result of Dobbertin and Leander [8]. We next give an upper bound for the $U_2$ norm of a $\mathbb{Z}$-bent function of level 1 and under some technical condition of a $\mathbb{Z}$-bent of any level.

In Theorem 4.1 of Dobbertin and Leander, sufficient conditions on $f_{ij}$ for the bentness of $h$ are proposed. Using the above recurrence we can now easily get necessary and sufficient conditions for the bentness of $h$. Although, the next result is shown using Theorem 4.2, we shall call it a theorem, due to its importance.

Theorem 4.3. Let $h, f_{ij}, 0 \leq i, j \leq 1$, be as in the theorem above and $h$ obtained from gluing the $\mathbb{Z}$-bent functions $f_{ij}$ of level 1. Then $h$ is bent if and only if

$$2^{-n+1} = \|f_{00}\|_{U_2}^4 + \|f_{01}\|_{U_2}^4 + \|f_{10}\|_{U_2}^4 + \|f_{11}\|_{U_2}^4 + 3 \cdot 2^{-2n+1} \sum_{u \in \mathbb{F}_2^n} (\hat{f}_{00}^2(u)\hat{f}_{10}^2(u) + \hat{f}_{01}^2(u)\hat{f}_{11}^2(u)).$$

Proof. We need to prove that a function $f$ on $n$ variables is $\pm 1$-bent if and only if $\|f\|_{U_2}^4 = 2^{-n}$. If $f$ is $\pm 1$-bent, then $\|f\|_{U_2}^4 = 2^{-2n} \sum_{x \in \mathbb{F}_2^n} \hat{f}(x) = 2^{-2n} \cdot 2^n = 2^{-n}$. Suppose $f$ is not $\pm 1$-bent, but $\|f\|_{U_2}^4 = 2^{-n}$. Then, $\|f\|_{U_2}^4 = 2^{-2n} \sum_{x \in \mathbb{F}_2^n} \hat{f}(x) = 2^{-n}$, and $\hat{f}(x) = 2^n \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)$. Thus,

$$\|f\|_{U_2}^4 = 2^{-2n} \sum_{x \in \mathbb{F}_2^n} \hat{f}(x) \leq 2^{-2n} \max_{x \in \mathbb{F}_2^n} \hat{f}(x) \sum_{x \in \mathbb{F}_2^n} \hat{f}(x) = 2^{-n} \max_{x \in \mathbb{F}_2^n} \hat{f}(x),$$

and the result is shown. \[\square\]

The next theorem uses a result of Kolomeec and Pavlov [13] who showed that $d(g, h) \geq 2^n$, for any two bent functions in $n$ variables.
Theorem 4.4. If \( f \) is a splitting \( \mathbb{Z} \)-bent function of level 1 such that \( f(x) = \frac{\chi_g(x) + \chi_h(x)}{2} \) where \( g, h \) are bent functions, the \( U_2 \) Gowers norm is \( \|f\|_{U_2}^4 = \frac{2^n - d(\hat{g}, \hat{h})}{2^{2n}} = \frac{2^n - d(g, h)}{2^{2n}} \). If \( f \) is a splitting \( \mathbb{Z} \)-bent function of level 1 in \( n \) variables and not a bent function then \( \|f\|_{U_2}^4 \leq \frac{2^n - 2^2}{2^{2n}} \).

Proof. Since \( f(x) = \frac{\chi_g(x) + \chi_h(x)}{2} \in \{ -1, 0, 1 \} \), for all \( x \in \mathbb{F}_2^n \), we infer that the Fourier transform of \( f \) is given by \( \hat{f}(u) = \frac{\hat{\chi}_g(u) + \hat{\chi}_h(u)}{2} \in \{ -1, 0, 1 \} \), for all \( u \in \mathbb{F}_2^n \). By Parseval’s identity we have \( \sum_{x \in \mathbb{F}_2^n} \hat{f}^2(x) = \sum_{x \in \mathbb{F}_2^n} f^2(x) \). Therefore, \( \# \{ x \in \mathbb{F}_2^n : g(x) = \hat{h}(x) \} \)

The Gowers \( U_2 \) norm of \( f \) is then

\[
\|f\|_{U_2}^4 = 2^{-2n} \sum_{x \in \mathbb{F}_2^n} \hat{f}^4(x) = 2^{-2n} \# \{ x \in \mathbb{F}_2^n : g(x) = \hat{h}(x) \} = 2^{-2n} \left( 2^n - \# \{ x \in \mathbb{F}_2^n : g(x) \neq \hat{h}(x) \} \right) = \frac{2^n - d(\hat{g}, \hat{h})}{2^{2n}} = \frac{2^n - d(g, h)}{2^{2n}}.
\]

Kolomeec and Pavlov [13] have proved that \( d(g, h) \geq 2 \frac{n}{2} \) for any two bent functions in \( n \) variables. Therefore, if \( f \) is a splitting \( \mathbb{Z} \)-bent function of level 1 and not a bent function then \( \|f\|_{U_2}^4 \leq \frac{2^n - 2^2}{2^{2n}} \), and the theorem is shown. \( \Box \)

While we were able to compute the \( U_2 \) Gowers norm of any bent function in Theorem 2.1 and give some necessary conditions for splitting \( \mathbb{Z} \)-bents in Theorem 4.4, it is a natural question about the norm of a \( \mathbb{Z} \)-bent of any level. In our next result, we are able to compute the Gowers norms of \( \mathbb{Z} \)-bent functions of any level, under some technical conditions. In particular, we note that the next theorem implies that the norm of two types of \( \mathbb{Z} \)-bent functions of level 1 is not a function of \( n \) only, as it was the case for level 0.

Two Boolean functions \( g, h \in \mathfrak{B}_n \) are called disjoint spectra functions if \( \hat{\chi}_g(u) \cdot \hat{\chi}_h(u) = 0 \), for any \( u \in \mathbb{F}_2^n \). Equivalently, \( \hat{\chi}_g(u) = 0 \) if and only if \( \hat{\chi}_h(u) \neq 0 \), since if \( n \) is odd then for any semibent, its Fourier spectrum has \( 2^{n-1} \) nonzero coefficients. In Theorem 3.2 of [10], it is claimed that a \( \mathbb{Z} \)-bent function of level 1 constructed by using two disjoint spectra semibent functions in \( n \) variables, where \( n \) is even, is non-splitting. The proof of this theorem contains a serious flaw, and therefore proving the existence of non-splitting \( \mathbb{Z} \)-bent functions of level 1 is still an open problem.

We shall be using Theorem 3.5 of [10], which states: Let \( n \) be even, and \( f_1, f_2 \in \mathfrak{B}_n \) be \( s_1 \)-, respectively, \( s_2 \)-plateued functions that are neither bent nor both semibent, and so, \( \text{Spec}(f_i) = \{ 0, \pm 2^{1+r_i} \} \), \( r_i := \frac{n}{2^i} - 1 \geq 0 \) \( (i = 1, 2) \). Let \( \alpha, \beta \) be arbitrary nonzero integers with \( \alpha \equiv \beta \pmod{2} \). If \( r_1 = 0, r_2 = 1, \alpha = \pm 1 \) (or \( r_2 = 0, r_1 = 1, \beta = \pm 1 \)), we assume \( 2 \beta + \alpha \notin \{ -1, 1 \} \) (respectively, \( 2 \alpha + \beta \notin \{ -1, 1 \} \)), where \( \epsilon_i \in \{ 0, \pm 1 \} \), for at least one value of \( x \in \mathbb{F}_2^n \) (recall that \( \hat{\chi}_{f_1}(x) = \epsilon_1 2^{n/2} \); if \( r_1 > 0, r_2 > 0 \), we assume that \( \alpha \hat{\chi}_{f_1}(x) + \beta \hat{\chi}_{f_2}(x) \notin \{ 0, \pm 2 \} \), for at least one value \( x \in \mathbb{F}_2^n \). Then, \( f(x) = \alpha \hat{\chi}_{f_1}(x) + \beta \hat{\chi}_{f_2}(x) \) is a \( \mathbb{Z} \)-bent function of level \( l := \lceil \log_2 M \rceil \), where \( M = \max_{u \in \mathbb{F}_2^n} \{| \alpha \hat{\chi}_{f_1}(u) + \beta \hat{\chi}_{f_2}(u) \| \} \) that cannot be split into two bent functions.
Theorem 4.5. Let \( f \) be a \( Z \)-bent function of level \( r \), and write \( f(x) = \frac{\alpha \chi_g(x) + \beta \chi_h(x)}{2} \).

(i) If \( g, h \) are disjoint spectra functions that fulfill the conditions of \([10, \text{Theorem 3.5}]\), then \( \| f \|_{U_2}^4 = 2^{-n-4}(a^42^{s_1} + \beta^42^{s_2}) \).

(ii) In general, if \( g, h \) are not necessarily disjoint spectra functions, then

\[
\| f \|_{U_2}^4 = 2^{-n-4}(a^42^{s_1} + \beta^42^{s_2}) + 2^{-2n-2}\alpha \beta(\alpha^22^{s_1} + \beta^22^{s_2})(2^n - 2d(g, h))
+ 2^{-2n-3}\alpha^2\beta^22^{s_1+s_2}|\{x : \hat{\chi}_g(x) \cdot \hat{\chi}_h(x) \neq 0\}|.
\]

Proof. If \( g, h \) are not necessarily disjoint spectra functions, we obtain

\[
\| f \|_{U_2}^4 = 2^{-2n}\sum_{x \in \mathbb{F}_2^n} f^4(x) = 2^{-2n}\sum_{x \in \mathbb{F}_2^n} \left( \frac{\alpha \hat{\chi}_g(u) + \beta \hat{\chi}_h(u)}{2} \right)^4
= 2^{-2n-4}\sum_{x \in \mathbb{F}_2^n} \left( \alpha \hat{\chi}_g(x) \right)^4
+ 4\alpha^42^s\hat{\chi}_g(x)\hat{\chi}_h(x) + 6\alpha^2\beta^2\hat{\chi}_g(x)\hat{\chi}_h(x) + 4\alpha^3\beta\hat{\chi}_g(x)\hat{\chi}_h(x) + \beta^4\hat{\chi}_h(x).
\]

Let

\[
A = \#\{u \in \mathbb{F}_2^n : \hat{\chi}_g(u) = 2^{\frac{s_1}{2}} \neq \hat{\chi}_h(u) = 2^{\frac{s_2}{2}} \} \cup \{u \in \mathbb{F}_2^n : \hat{\chi}_g(u) = 2^{\frac{s_1}{2}}, \hat{\chi}_h(u) = -2^{\frac{s_2}{2}} \},
B = \#\{u \in \mathbb{F}_2^n : \hat{\chi}_g(u) = 2^{\frac{s_1}{2}}, \hat{\chi}_h(u) = -2^{\frac{s_2}{2}} \} \cup \{u \in \mathbb{F}_2^n : \hat{\chi}_g(u) = 2^{\frac{s_1}{2}} = -2^{\frac{s_2}{2}} \}.
\]

By Parseval’s identity,

\[
\sum_{x \in \mathbb{F}_2^n} f^2(x) = 2^{-2}\sum_{x \in \mathbb{F}_2^n} \left( \hat{\chi}_g(x) + 2\hat{\chi}_g(x)\hat{\chi}_h(x) + \hat{\chi}_h(x) \right)
= 2^{-2}\sum_{x \in \mathbb{F}_2^n} \left( \hat{\chi}_g(x)^2 + 2\hat{\chi}_g(x)\hat{\chi}_h(x) + \hat{\chi}_h(x)^2 \right).
\]

Further, \( \sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_g(x)^2 = \sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_h(x)^2 \), and \( \sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_g(x) = \sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_h(x) \), which implies that

\[
\sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_g(x)\hat{\chi}_h(x) = 2^{s_1+s_2}(A - B) = \sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_g(x)\hat{\chi}_h(x) = 2^n - 2d(g, h),
\]

so \( A - B = 2^{-s_1-s_2}(2^n - 2d(g, h)) \). Notice that \( C := A + B \) is the number of positions where both \( \hat{\chi}_g \) and \( \hat{\chi}_h \) are nonzero. Then,

\[
\sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_g(x)\hat{\chi}_h(x) = 2^{s_1+s_2}(A - B) = 2^{s_1}(2^n - 2d(g, h)),
\]

finally,

\[
\sum\sum_{x \in \mathbb{F}_2^n} \hat{\chi}_g(x)\hat{\chi}_h(x) = 2^{s_1+s_2}(A + B) = C2^{s_1+s_2}. \]

The second claim is similar. \( \square \)
Corollary 4. If $h : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{Z}$ is the concatenation $h = [h_{00}||h_{01}||h_{10}||h_{11}]$ of four $n$-variables integer-valued functions $h_{ij}$ ($0 \leq i, j \leq 1$), satisfying equations (5)–(6), for some integer-valued $Z$-bent functions $f_{ij}$ of level $r + 1 \geq 2$ of constant norm, say $\|f_{ij}\|_{U^2}^4 = K$, such that both pairs $f_{00}, f_{10}$, respectively, $f_{01}, f_{11}$ have disjoint spectra, then the $U_2$ Gowers norm of the $Z$-bent function $h$ of level $r$ is $\|h\|_{U^2}^4 = 2^{-5}K$.

Proof. From the recurrence of Theorem 4.2, since $\hat{f}_{00}^2(u)\hat{f}_{10}^2(u) = \hat{f}_{01}^2(u)\hat{f}_{11}^2(u) = 0$, then $\|h\|_{U^2}^4 = 2^{-3}\gamma^4 \left(\|f_{00}\|_{U^2}^4 + \|f_{01}\|_{U^2}^4 + \|f_{10}\|_{U^2}^4 + \|f_{11}\|_{U^2}^4\right) = 2^{-7} \cdot 2^2 \cdot K = 2^{-5}K$, which shows the corollary.

Acknowledgments

We would like to express our sincere appreciation for the anonymous reviewers, and the associate editor’s careful reading, beneficial comments and constructive suggestions. Many thanks to the organizers of the 2017 workshop on Boolean Functions and their Applications in Solstrand, Os, Norway, for bringing the authors together, which started this collaboration.

References

[1] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer, Cham, 2014.
[2] C. Carlet, Boolean functions for cryptography and error correcting codes, *Boolean Methods and Models, Cambridge Univ. Press, Cambridge*, (2010), 257–397.
[3] C. Carlet and S. Mesnager, *Four decades of research on bent functions*, *Des. Codes Cryptogr.*, **78** (2016), 5–50.
[4] F. Caullery and F. Rodier, Distribution of the absolute indicator of random Boolean functions, hal-01679358f, (2018), available at: https://hal.archives-ouvertes.fr/hal-01679358/document.
[5] V. Y.-W. Chen, *The Gowers Norm in the Testing of Boolean Functions*, Ph.D. Thesis, Massachusetts Institute of Technology, June 2009.
[6] T. W. Cusick and P. Stǎnicǎ, *Cryptographic Boolean Functions and Applications*, Elsevier/Academic Press, Amsterdam, 2009.
[7] J. F. Dillon, Elementary Hadamard difference sets, *Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Congressus Numerantium, Utilitas Math.*, Winnipeg, Man., **14** (1975), 237–249.
[8] H. Dobbertin and G. Leander, *Bent functions embedded into the recursive framework of Z-bent functions*, *Des. Codes Cryptogr.*, **49** (2008), 3–22.
[9] S. Gangopadhyay, B. Mandal and P. Stǎnicǎ, *Gowers $U_3$ norm of some classes of bent Boolean functions*, *Des. Codes Cryptogr.*, **86** (2018), 1131–1148.
[10] S. Gangopadhyay, E. Pasalic, P. Stǎnicǎ and S. Datta, *A note on non-splitting Z-functions*, *Inf. Proc. Letters*, **121** (2017), 1–5.
[11] S. Hodžić, W. Meidl and E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual and the Gray image*, *IEEE Trans. Inf. Theory*, **64** (2018), 5432–5440.
[12] S. Hodžić and E. Pasalic, *Generalized bent functions—Some general construction methods and related necessary and sufficient conditions*, *Cryptogr. Commun.*, **7** (2015), 469–483.
[13] N. Kolomeec and A. Pavlov, *Bent Functions on the Minimal Distance*, IEEE Region 8 SIBIRCON-2010, Irkutsk Listvyanka, Russia, 2010.
[14] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *J. Combin Theory Ser. A*, **40** (1985), 90–107.
[15] T. Martinsen, W. Meidl, S. Mesnager and P. Stǎnicǎ, *Decomposing generalized bent and hyperbent functions*, *IEEE Trans. Inf. Theory*, **63** (2017), 7804–7812.
[16] T. Martinsen, W. Meidl, A. Pott and P. Stǎnicǎ, *On symmetry and differential properties of generalized Boolean functions*, *Arithmetic of Finite Fields, Lecture Notes in Comput. Sci.*, **11321** (2018), 207–223.
[17] T. Martinsen, W. Meidl and P. Stanica, Generalized bent functions and their Gray images, *Arithmetic of Finite Fields, Lecture Notes in Comput. Sci.*, Springer, Cham, **10064** (2017), 160–173.

[18] T. Martinsen, W. Meidl and P. Stanica, Partial spread and vectorial generalized bent functions, *Des. Codes Cryptogr.*, **85** (2017), 1–13.

[19] S. Mesnager, *Bent Functions: Fundamentals and Results*, Springer-Verlag, 2016.

[20] S. Mesnager, C. M. Tang, Y. F. Qi, L. B. Wang, B. F. Wu and K. Q. Feng, Further results on generalized bent functions and their complete characterization, *IEEE Trans. Inform. Theory*, **64** (2018), 5441–5452.

[21] B. Preneel, R. Govaerts and J. Vandewalle, Cryptographic properties of quadratic Boolean functions, *Int. Symp. Finite Fields and Appl.*, (1991), 9pp.

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

[23] K. U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA, *IEEE Trans. Inf. Theory*, **55** (2009), 1824–1832.

[24] P. Solé and N. Tokareva, Connections between quaternary and binary bent functions, *Prikl. Diskr. Mat.*, **1** (2009), 16–18, [http://eprint.iacr.org/2009/544.pdf](http://eprint.iacr.org/2009/544.pdf).

[25] P. Stanica, Weak and strong $2^k$-bent functions, *IEEE Trans. Inf. Theory*, **62** (2016), 2827–2835.

[26] P. Stanica, T. Martinsen, S. Gangopadhyay and B. K. Singh, Bent and generalized bent Boolean functions, *Des. Codes Cryptogr.*, **69** (2013), 77–94.

[27] C. M. Tang, C. Xiang, Y. F. Qi and K. Q. Feng, Complete characterization of generalized bent and $2^k$-bent Boolean functions, *IEEE Trans. Inf. Theory*, **63** (2017), 4668–4674.

[28] N. Tokareva, *Bent Functions. Results and Applications to Cryptography*, Elsevier/Academic Press, Amsterdam, 2015.

[29] F. Zhang, S. Xia, P. Stanica and Y. Zhou, Further results on constructions of generalized bent Boolean functions, *Inf. Sciences-China*, **59** (2016), 1–3.

[30] X.-M. Zhang and Y. L. Zheng, GAC—the criterion for global avalanche characteristics of cryptographic functions, *J. UCS*, **1** (1995), 320–337.

Received July 2019; 1st revision October 2019; 2nd revision October 2019.

E-mail address: sugatfma@iitr.ac.in
E-mail address: csr@hvl.no
E-mail address: pstanica@nps.edu