Gowers U_2 norm of Boolean functions and their generalizations
(Extended Abstract)

Sugata Gangopadhyay[1], Constanza Riera[2],
Pantelimon Stănică[3]

[1] Department of Computer Science and Engineering,
Indian Institute of Technology Roorkee, Roorkee 247667, INDIA; `sugatfma@iitr.ac.in`
[2] Department of Computing, Mathematics, and Physics,
Western Norway University of Applied Sciences, 5020 Bergen, Norway; `csr@hvl.no`
[3] Department of Applied Mathematics, Naval Postgraduate School,
Monterey, CA 93943–5216, USA; `pstanica@nps.edu`

Abstract. In this paper we investigate the Gowers U_2 norm of order 2 for generalized Boolean functions, and $\mathbb{Z}$-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 $\mathbb{Z}$-bent functions, as proposed by Dobbertin and Leander [4], to provide a recursive framework to study bent functions. In the second part of the paper, we concentrate on $\mathbb{Z}$-bent functions and their U_2 norms. As a consequence of one of our results, we give an alternative proof to a known theorem of Dobbertin and Leander, and also find necessary and sufficient conditions for a function obtained by *gluing* $\mathbb{Z}$-bent functions to be bent in terms of the Gowers U_2 norms of its components.
Keywords: Gowers norms; Boolean functions; generalized Boolean functions; bent functions; $\mathbb{Z}$-bent functions

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 [7, 8, 10, 12–15, 18–23] 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 said to be bent functions [17]. 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 [4] 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 [4].

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 $f \in \mathcal{GB}_n^q$, $\chi_f : \mathbb{F}_2^n \to \mathbb{C}$, is defined by $\chi_f(\mathbf{x}) = \zeta_q^{f(\mathbf{x})}$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $\zeta_q = e^{\frac{2\pi i}{q}}$. The *algebraic normal form* (ANF) of $f \in \mathcal{B}_n$ is the polynomial representation $f(\mathbf{x}) = \bigoplus_{\mathbf{a}\in\mathbb{F}_2^n} \mu_{\mathbf{a}} x_1^{a_1} \ldots x_n^{a_n}$, where $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{a} = (a_1, \ldots, a_n)$, and $\mu_{\mathbf{a}} \in \mathbb{F}_2$. 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

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

The (Hamming) *weight* of $\mathbf{x} \in \mathbb{F}_2^n$, denoted by $wt(\mathbf{x})$, is the number of nonzero coordinates in $\mathbf{x}$, and the (Hamming) weight of a Boolean function f is $wt(f) = \#\{\mathbf{x} \in \mathbb{F}_2^n : f(\mathbf{x}) \neq 0\}$. The (Hamming) *distance* $d(f, g)$ between two functions f, g is the weight of their sum. The algebraic degree of f is $\deg(f) = \max\{wt(\mathbf{a}) : \mathbf{a} \in \mathbb{F}_2^n, \mu_{\mathbf{a}} \neq \mathbf{0}\}$. The Boolean functions having algebraic degree at most one are affine functions.
For a (generalized) Boolean function $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ we define the (*generalized*) *Walsh-Hadamard transform* to be the complex valued function

$$\mathcal{H}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_q^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}},$$

where $\mathbf{u} \cdot \mathbf{x} = \bigoplus_{1\leq i\leq n} u_i x_i$ For $q = 2$, we obtain the usual *Walsh-Hadamard transform* $\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}$. The autocorrelation of $f \in \mathcal{GB}_n^q$ is defined by $\mathcal{C}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_q^{f(\mathbf{x})-f(\mathbf{x}\oplus\mathbf{u})}$. We shall use the identity [21]

$$\mathcal{C}_f^{(q)}(\mathbf{u}) = 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f^{(q)}(\mathbf{x})|^2(-1)^{\mathbf{u}\cdot\mathbf{x}}. \tag{1}$$

A function $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f^{(q)}(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{F}_2^n$. Further, we say that $f \in \mathcal{GB}_n^q$ is called *s-plateaued* if $|\mathcal{H}_f^{(q)}(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{F}_2^n$, for a fixed integer s depending on f. For simplicity of notation, when q is fixed, we sometimes use ζ, $\mathcal{H}_f$, $\mathcal{C}_f$ instead of ζ_q, $\mathcal{H}_f^{(q)}$, and $\mathcal{C}_f^{(q)}$, respectively. We refer the reader to [7, 11, 12, 15] and references therein for more on generalized bent functions and their characterizations in terms of their components.

2.2 Gowers U_2 norm

Let $g : V \to \mathbb{C}$ 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. If $f : \mathbb{F}_2^n \to \mathbb{C}$ is a complex-valued function, we define the Gowers U_2 norm by

$$\begin{aligned}\|f\|_{U_2} &= \left(\mathbb{E}_{\mathbf{x},\mathbf{h}_1,\mathbf{h}_2\in\mathbb{F}_2^n}[f(\mathbf{x})\overline{f(\mathbf{x}\oplus\mathbf{h}_1)}\,\overline{f(\mathbf{x}\oplus\mathbf{h}_2)}f(\mathbf{x}\oplus\mathbf{h}_1\oplus\mathbf{h}_2)]\right)^{1/4}\\ &= \left(\mathbb{E}_{\mathbf{h}_1\in\mathbb{F}_2^n}|\mathbb{E}_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x})\overline{f(\mathbf{x}\oplus\mathbf{h}_1)}]|^2\right)^{1/4}.\end{aligned}$$

It is known (cf. [1, pp. 22–24]) that for $f : \mathbb{F}_2^n \to \mathbb{R}$, if there is a polynomial $P : \mathbb{F}_2^n \to \{0,1\}$ of degree d such that $|\mathbb{E}_{x\in\mathbb{F}_2^n} f(x)(-1)^{P(x)}| \geq \epsilon$, 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 $|\mathbb{E}_{x\in\mathbb{F}_2^n} f(x)(-1)^{P(x)}| \geq \epsilon$ 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 $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is a generalized Boolean function, we define the Gowers norm of f to be the Gowers norm for the character form $\chi_f := \zeta^f$ of 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 [1, pp. 22–24], to which we refer for a detailed discussion (for the Boolean case).

Theorem 1 *If $k \geq 1$ and $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$, then (with $\chi_f = \zeta^f$, where $\zeta = e^{2\pi\, i/2^k}$ is a 2^k-complex root of 1) $\|\chi_f\|_{U_2}^4 = 2^{-4n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^4 \leq 2^{-2n}\max_{\mathbf{x}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^2$. Moreover, the equality holds if and only if f is a bent ($k = 1$), respectively, gbent ($k > 1$) function, and, then, $\|\chi_f\|_{U_2}^4 = 2^{-n}$.*

Proof. If $f \in \mathcal{GB}_n^{2^k}$, using equation (1), we can see that the Gowers U_2 norm is

$$\begin{aligned}\|\chi_f\|_{U_2}^4 &= 2^{-3n}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{\mathbf{v}\in\mathbb{F}_2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\zeta^{f(\mathbf{x})}\overline{\zeta^{f(\mathbf{x}\oplus\mathbf{u})}}\sum_{\mathbf{v}\in\mathbb{F}_2^n}\overline{\zeta^{f(\mathbf{x}\oplus\mathbf{v})}}\zeta^{f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v})}\\ &= 2^{-3n}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{x}\in\mathbb{F}_2^n}\zeta^{f(\mathbf{x})-f(\mathbf{x}\oplus\mathbf{u})}\right)\left(\sum_{\mathbf{y}\in\mathbb{F}_2^n}\zeta^{-f(\mathbf{y})+f(\mathbf{y}\oplus\mathbf{u})}\right)\\ &= 2^{-5n}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{x}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^2(-1)^{\mathbf{u}\cdot\mathbf{x}}\right)\left(\sum_{\mathbf{y}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{y})|^2(-1)^{\mathbf{u}\cdot\mathbf{y}}\right)\\ &= 2^{-5n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^2|\mathcal{H}_f(\mathbf{y})|^2\sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y})} = 2^{-4n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^4. \qquad (2)\end{aligned}$$

Then, $2^{4n}\|\chi_f\|_{U_2}^4 = \sum_{x\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^4 \leq \max_{\mathbf{x}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^2\sum_{x\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^2 = 2^{2n}\max_{\mathbf{x}\in\mathbb{F}_2^n}|\mathcal{H}_f(\mathbf{x})|^2$.
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, $|\mathcal{H}_f(\mathbf{x})|^2 = 2^n$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Using (2), we infer

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

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

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

yielding a contradiction.
We only need to show that, if $||\chi_f||_{U_2}^4 = 2^{-n}$, the equality holds. Suppose that $||\chi_f||_{U_2}^4 = 2^{-n}$, but $||\chi_f||_{U_2}^4 = 2^{-4n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^4 > 2^{-2n} \max_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^2$. Then, $\max_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 < 2^n$, contradicting Parseval's identity. □

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

Proposition 2. *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 $\|\chi_f\|_{U_2}$ is $2^{(-n+2)/4}$, if n is even, and $2^{(-n+1)/4}$, if n is odd. In general, if $f \in \mathcal{GB}_n^q$ with $|\mathcal{H}_f(\mathbf{x})| \in \{0, \lambda_1, \ldots, \lambda_t\}$, 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 $|\mathcal{H}_f(\mathbf{x})| \in \{2^{(n+s)/2}, 0\}$. By Parseval's identity, $\sum_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 = 2^{2n} = a \cdot 2^{n+s}$, where a is the multiplicity of 2^{n+s} in $|\mathcal{H}_f(\mathbf{x})|$. Hence, $a = 2^{n-s}$. Then, by equation (2), $\|\chi_f\|_{U_2}^4 = 2^{-4n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^4 = 2^{-4n} \cdot a \cdot 2^{2(n+s)} = 2^{-n+s}$. 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 $nl(f) = 2^{n-1} - \frac{1}{2} \max_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{W}_f(\mathbf{x})|$, which means that if a function has high nonlinearity, then $\max_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|$ is small, and therefore $\|\chi_f\|_{U_2}$ is upper bounded by a relatively small number.
One can ask whether is it 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 $2h$ [16] (under $f(0) = 0$), then, by Proposition 2, $\|\chi_f\|_{U_2} = 2^{-2h}$. Thus, if f_1, f_2 are two quadratic Boolean functions of ranks $2h_1 < 2h_2$, respectively, then

$$nl(f_1) = 2^{n-1} - 2^{n-h_1-1} < 2^{n-1} - 2^{n-h_2-1} = nl(f_2), \|\chi_{f_1}\|^4 = 2^{-2h_1} > 2^{-2h_2} = \|\chi_{f_2}\|^4 .$$

We can certainly find an infinite class of pairs of Boolean functions (f, g) such that $nl(f) < nl(g)$ and $\|\chi_f\|_{U_2} > \|\chi_g\|_{U_2}$. For example, let n be even, g be any bent Boolean function, and so, by Theorem 1, $nl(g) = 2^{n-1} - 2^{n/2-1}$, $\|\chi_g\|_{U_2}^4 = 2^{-n}$. Let f now be any semibent Boolean function (with $f(0) = 0$) for n even, so, by Proposition 2, $\|\chi_f\|_{U_2} = 2^{(-n+2)/4}$, which implies that $nl(f) = 2^{n-1} - 2^{n/2}$, $\|\chi_f\|_{U_2}^4 = 2^{-4n} \max_{\mathbf{x}\in\mathbb{F}_2^n} \mathcal{W}_f(\mathbf{x})^4 = 2^{-4n} 2^{2(n+2)} 2^{n-2} = 2^{-n+2}$. Thus, $nl(f) < nl(g)$, 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 1 and Proposition 2 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 $\{E_0, \dots, E_{2^m}\}$ be a *spread* of $\mathbb{F}_2^n$, that is, E_i's, $0 \le i \le 2^m$, are m-dimensional subspaces of $\mathbb{F}_2^n$ with trivial intersection. Note that $\bigcup_{i=0}^{2^m} E_i = \mathbb{F}_2^n$ [3].

Theorem 3. *Let $\{E_0, \dots, E_{2^m}\}$ be a spread, and $f \in \mathcal{GB}_n^q$. Then:*

(i) If f is defined by $f(\mathbf{x}) = \begin{cases} c_i, & \mathbf{x} \in E_i^\star \\ c, & \mathbf{x} = \mathbf{0}, \end{cases}$ with arbitrary $c, c_i \in \mathbb{Z}_q$, $1 \le i \le m$, then

$$\|\chi_f\|_{U_2}^4 = 2^{-4n} \left((2^n - 1) \left| \zeta^c - A \right|^4 + \left| \zeta^c + (2^m - 1) A \right|^4 \right), \text{ where } A := \sum_{i=0}^{2^m} \zeta^{c_i}.$$

(ii) If f is defined by $f(\mathbf{x}) = \frac{q}{2} \mathbf{a}_i \cdot \mathbf{x}$, $\mathbf{x} \in E_i$, where $\{\mathbf{a}_0, \dots, \mathbf{a}_{2^m}\}$ are distinct arbitrary vectors in $\mathbb{F}_2^n$, then $\|\chi_f\|_{U_2}^4 = 2^{-2n} \left(2^{\frac{n}{2}} + 1 \right)$.

Proof. To show (i), we first write

$$\begin{aligned} \mathcal{H}_f(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{i=0}^{2^m} \sum_{\mathbf{x} \in E_i^\star} \zeta^{c_i} (-1)^{\mathbf{u} \cdot \mathbf{x}} + \zeta^c \\ &= \sum_{i=0}^{2^m} \zeta^{c_i} \sum_{\mathbf{x} \in E_i} (-1)^{\mathbf{u} \cdot \mathbf{x}} + \zeta^c - \sum_{i=0}^{2^m} \zeta^{c_i} = \zeta^c - A + \begin{cases} 2^m A & , \mathbf{u} = \mathbf{0} \\ 0 & , \mathbf{u} \ne \mathbf{0}. \end{cases} \end{aligned}$$

Then
$\|\chi_f\|_{U_2}^4 = 2^{-4n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^4 = 2^{-4n} \left((2^n - 1) \left| \zeta^c - A \right|^4 + \left| \zeta^c + (2^m - 1) A \right|^4 \right)$, and the first claim is shown.
To show (ii), we write $\mathcal{H}_f(\mathbf{u}) = \sum_{i=0}^{2^m} \sum_{\mathbf{x} \in E_i} \zeta^{\frac{q}{2} \mathbf{a}_i \cdot \mathbf{x}} (-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{i=0}^{2^m} \sum_{\mathbf{x} \in E_i} (-1)^{(\mathbf{a}_i + \mathbf{u}) \cdot \mathbf{x}} = 2^m$, if there exists i such that $\mathbf{u} = \mathbf{a}_i$, and 0 if $\mathbf{u} \ne \mathbf{a}_i, \forall i$. Therefore, we get $\|\chi_f\|_{U_2}^4 = 2^{-4n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^4 = 2^{-4n} 2^{4m} (2^m + 1) = 2^{-2n} \left(2^{\frac{n}{2}} + 1 \right)$, and the theorem is shown. □

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. Its proof is not shown here due to space restrictions, and will be available in the full paper.

Lemma 4. *Let $f_1, f_2 \in \mathcal{GB}_n^q$, $q = 2^k$, be n-variables generalized Boolean functions and ζ a q-complex root of 1. Then $\sum_{\mathbf{x} \in \mathbb{F}_2^n} |\mathcal{H}_{f_1}(\mathbf{x})|^2 |\mathcal{H}_{f_2}(\mathbf{x})|^2 = 2^n \sum_{\mathbf{w} \in \mathbb{F}_2^n} \mathcal{C}_{f_1}(\mathbf{w}) \mathcal{C}_{f_2}(\mathbf{w})$.*

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 5 *Let $f : \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{Z}_q$, 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, $f(x_1, \mathbf{x}) = (1 - x_1) f_1(\mathbf{x}) + x_1 f_2(\mathbf{x})$. The Gowers U_2 norm of f is given recursively by*

$$2^3 \|\chi_f\|_{U_2}^4$$

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

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

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

Proof. If $f : \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{Z}_q$ is given by $f(x_1, \mathbf{x}) = (1 - x_1)f_1(\mathbf{x}) + x_1 f_2(\mathbf{x})$, then, it is known (and easy to show) that $\mathcal{H}_f(u_1, \mathbf{u}) = \mathcal{H}_{f_1}(\mathbf{u}) + (-1)^{u_1}\mathcal{H}_{f_2}(\mathbf{u})$. The Gowers norm of f is then (below, we split the sums into $u_1 = 0$, $u_1 = 1$.)

$$2^{4(n+1)} \|\chi_f\|_{U_2}^4 = \sum_{(u_1,\mathbf{u})\in\mathbb{F}_2\times\mathbb{F}_2^n} |\mathcal{H}_f(u_1,\mathbf{u})|^4 = \sum_{(u_1,\mathbf{u})\in\mathbb{F}_2\times\mathbb{F}_2^n} |\mathcal{H}_{f_1}(\mathbf{u}) + (-1)^{u_1}\mathcal{H}_{f_2}(\mathbf{u})|^4$$

$$= \sum_{(u_1,\mathbf{u})\in\mathbb{F}_2\times\mathbb{F}_2^n} \left(|\mathcal{H}_{f_1}(\mathbf{u})|^2 + (-1)^{u_1}\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})} + \mathcal{H}_{f_2}(\mathbf{u})\overline{\mathcal{H}_{f_1}(\mathbf{u})}\right) + |\mathcal{H}_{f_1}(\mathbf{u})|^2\right)^2$$

$$= \sum_{(u_1,\mathbf{u})\in\mathbb{F}_2\times\mathbb{F}_2^n} \Bigg(|\mathcal{H}_{f_1}(\mathbf{u})|^4 + \left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})} + \mathcal{H}_{f_2}(\mathbf{u})\overline{\mathcal{H}_{f_1}(\mathbf{u})}\right)^2 + |\mathcal{H}_{f_2}(\mathbf{u})|^4$$

$$+2|\mathcal{H}_{f_1}(\mathbf{u})|^2|\mathcal{H}_{f_2}(\mathbf{u})|^2 + 2(-1)^{u_1}|\mathcal{H}_{f_1}(\mathbf{u})|^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})} + \mathcal{H}_{f_2}(\mathbf{u})\overline{\mathcal{H}_{f_1}(\mathbf{u})}\right)$$

$$+2(-1)^{u_1}|\mathcal{H}_{f_2}(\mathbf{u})|^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})} + \mathcal{H}_{f_2}(\mathbf{u})\overline{\mathcal{H}_{f_1}(\mathbf{u})}\right)\Bigg)$$

$$= \sum_{(u_1,\mathbf{u})\in\mathbb{F}_2\times\mathbb{F}_2^n} (|\mathcal{H}_{f_1}(\mathbf{u})|^4 + 4(-1)^{u_1}\mathcal{H}_{f_1}^3(\mathbf{u})\mathcal{H}_{f_2}(\mathbf{u})$$

$$+6\mathcal{H}_{f_1}^2(\mathbf{u})\mathcal{H}_{f_2}^2(\mathbf{u}) + 4(-1)^{u_1}\mathcal{H}_{f_1}(\mathbf{u})\mathcal{H}_{f_2}^3(\mathbf{u}) + |\mathcal{H}_{f_2}(\mathbf{u})|^4)$$

$$= 2\sum_{\mathbf{u}\in\mathbb{F}_2^n} \left(|\mathcal{H}_{f_1}(\mathbf{u})|^4 + |\mathcal{H}_{f_2}(\mathbf{u})|^4 + 2|\mathcal{H}_{f_1}(\mathbf{u})|^2|\mathcal{H}_{f_2}(\mathbf{u})|^2 + 4\Re^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})}\right)\right)$$

$$= 2^{4n+1}\|\chi_{f_1}\|_{U_2}^4 + 2^{4n+1}\|\chi_{f_2}\|_{U_2}^4 + 4\sum_{\mathbf{u}\in\mathbb{F}_2^n} \left(|\mathcal{H}_{f_1}(\mathbf{u})|^2|\mathcal{H}_{f_2}(\mathbf{u})|^2 + 2\Re^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})}\right)\right),$$

and by using Lemma 4, we infer the first claim. The second claim for $f_2 = f_1$ is easily obtained, since then $|\mathcal{H}_{f_2}(\mathbf{u})|^2 = |\mathcal{H}_{f_1}(\mathbf{u})|^2$, $\Re^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})}\right) = |\mathcal{H}_{f_1}(\mathbf{u})|^4$ and, so, $\sum_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{H}_{f_1}(\mathbf{u})|^2|\mathcal{H}_{f_2}(\mathbf{u})|^2 = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \Re^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})}\right) = 2^{4n}\|\chi_{f_1}\|_{U_2}$. If $f_2 = \bar{f}_1$, then $\mathcal{H}_{f_2} = \zeta\mathcal{H}_{f_1}$ and so, $\Re^2\left(\mathcal{H}_{f_1}(\mathbf{u})\overline{\mathcal{H}_{f_2}(\mathbf{u})}\right) = |\mathcal{H}_{f_1}(\mathbf{u})|^4\Re^2(\zeta)$, which, when used above renders the last claim. □

We now look at functions $f : \mathbb{F}_2^n \to \mathbb{Z}_4$, 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 [19] we can show the next theorem.

Theorem 6 *Let* $f \in \mathcal{GB}_n^4$, $f = a_0 + 2a_1$, $a_0, a_1 \in \mathcal{B}_n$. *Then*

$$2^4\|\chi_f\|_{U_2}^4 = \|\chi_{a_1}\|_{U_2}^4 + \|\chi_{a_0\oplus a_1}\|_{U_2}^4 + 2^{-4n+1}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathcal{W}_{a_1}^2(\mathbf{x})\mathcal{W}_{a_0\oplus a_1}^2(\mathbf{x})$$

$$= \|\chi_{a_1}\|_{U_2}^4 + \|\chi_{a_0\oplus a_1}\|_{U_2}^4 + 2^{-3n+1}\sum_{\mathbf{w}\in\mathbb{F}_2^n} \mathcal{C}_{a_1}(\mathbf{w})\mathcal{C}_{a_0\oplus a_1}(\mathbf{w}).$$

We can certainly derive an expression for the Gowers U_2 norm for a generalized $f \in \mathcal{GB}_n^{2^k}$. but the result is rather quite complicated, unfortunately. We will reserve it for the full paper.

4 Gowers U_2 norm and $\mathbb{Z}$-bent functions

4.1 $\mathbb{Z}$-bent functions

In this section, if f is an integer valued function, we will work with the Fourier transform $\widehat{f}(\mathbf{u}) = 2^{-n/2} \sum\limits_{\mathbf{x}\in\mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}$. The Gowers norm of f given by

$$\|f\|_{U_2}^4 = \mathbb{E}_{\mathbf{x},\mathbf{h}_1,\mathbf{h}_2\in\mathbb{F}_2^n}[f(\mathbf{x})f(\mathbf{x}\oplus\mathbf{h}_1)f(\mathbf{x}\oplus\mathbf{h}_2)f(\mathbf{x}\oplus\mathbf{h}_1\oplus\mathbf{h}_2)]$$

will render $\|f\|_{U_2}^4 = 2^{-2n}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{x})^4$.

Prompted by the observation that given two bent functions g, h in $n = 2k$ variables, $k > 1$, the function

$$f(\mathbf{x}) = \frac{\chi_g(\mathbf{x}) + \chi_h(\mathbf{x})}{2} \in \{-1, 0, 1\}, \tag{3}$$

for all $\mathbf{x} \in \mathbb{F}_2^n$ will also have its Fourier transform given by $\widehat{f}(\mathbf{u}) = \dfrac{\widehat{\chi}_g(\mathbf{u}) + \widehat{\chi}_h(\mathbf{u})}{2} \in \{-1, 0, 1\}$, for all $\mathbf{u} \in \mathbb{F}_2^n$, Dobbertin and Leander [4] defined the notion of $\mathbb{Z}$-bent function in the following way. Let $\mathcal{W}_0 = \{-1, 1\}$, $\mathcal{W}_r = \{\ell \in \mathbb{Z} : -2^{r-1} \le \ell \le 2^{r-1}\}$, for $r \ge 1$.A function $f : \mathbb{F}_2^n \to W_r \subseteq \mathbb{Z}$ is a *$\mathbb{Z}$-bent function of size k level r* if $\widehat{f}(\mathbf{x}) \in W_r$, for all $\mathbf{x} \in \mathbb{F}_2^n$. The set of all $\mathbb{Z}$-bent functions of size k level r is denoted by $\mathcal{B}F_r^k$. Any function belonging to $\bigcup_{r\ge 0} \mathcal{B}F_r^k$ is said to be a $\mathbb{Z}$-bent function of size k. If a $\mathbb{Z}$-bent function of level 1 can be written as in (3) then it is said to be *splitting*, otherwise it is said to be *non-splitting.* As Dobbertin and Leander did in [4], we refer to a ±1 function as bent (when we want to point that out we call it ±1-bent) even though it is the signature of a classical bent Boolean function.

Now, suppose that $h \in \mathcal{B}F_r^k$ is the concatenation $h = [h_{00}\|h_{01}\|h_{10}\|h_{11}]$, where $h_{\epsilon_1\epsilon_2}(\mathbf{x}) = h(\epsilon_1, \epsilon_2, \mathbf{x})$, for all $(\epsilon_1, \epsilon_2, \mathbf{x}) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{n-2}$, that is, $h(y, z, \mathbf{x}) = (y\oplus 1)(z\oplus 1)h_{00}(\mathbf{x}) + (y\oplus 1)zh_{01}(\mathbf{x}) + y(z\oplus 1)h_{10}(\mathbf{x}) + yzh_{11}(\mathbf{x})$. We define the functions $f_{\epsilon_1\epsilon_2}$ by using the following equations:

$$\textbf{Case 1.}\ \text{For } r \ge 1\text{:}\ \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} \tag{4}$$

$$\textbf{Case 2.}\ \text{For } r = 0\text{:}\ \begin{pmatrix} f_{00} & f_{10} \\ f_{01} & f_{11} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix} \tag{5}$$

Dobbertin and Leander [4, Proposition 2] showed that if h is a $\mathbb{Z}$-bent function of size k and level r, then the functions $f_{\epsilon_1\epsilon_2}$ are $\mathbb{Z}$-bent functions of size $k-1$ and level $r+1$, for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$. In other words, if $h \in \mathcal{B}F_r^k$, then $f_{\epsilon_1\epsilon_2} \in \mathcal{B}F_{r+1}^{k-1}$, for all $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$. Conversely, suppose we have $f_{\epsilon_1\epsilon_2} \in \mathcal{B}F_{r+1}^{k-1}$, 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 [4, Proposition 2] that all functions in $\mathcal{B}F_r^k$ are obtained by gluing functions in $\mathcal{B}F_{r+1}^{k-1}$. We derive the following condition connecting the $\mathbb{Z}$-bent functions of level 1 to (classical) bent functions as a special case of [4, Theorem 3].

Theorem 7 *Let four $\mathbb{Z}$-bent functions f_{00}, f_{01}, f_{10} and f_{11} of level* 1 *and size k be given such that*

$$\begin{aligned} f_{00}(\mathbf{x}) &\equiv f_{01}(\mathbf{x}) + 1 \pmod 2;\ f_{10}(\mathbf{x}) \equiv f_{11}(\mathbf{x}) + 1 \pmod 2; \\ \widehat{f_{00}}(\mathbf{x}) &\equiv \widehat{f_{10}}(\mathbf{x}) + 1 \pmod 2;\ \widehat{f_{01}}(\mathbf{x}) \equiv \widehat{f_{11}}(\mathbf{x}) + 1 \pmod 2. \end{aligned} \tag{6}$$

Then the function $h : \mathbb{F}_2\times\mathbb{F}_2\times\mathbb{F}_2^n \to \{-1, 1\}$ defined by $h(y, z, \mathbf{x}) = h_{yz}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_2^n$, where h_{ij}, f_{ij}, $0 \le i, j \le 1$ satisfy (5)*, is a* ±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 $\sum_{\mathbf{x}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{x})^2 = \sum_{\mathbf{x}\in\mathbb{F}_2^n} f(\mathbf{x})^2$.

4.2 Recurrences for Gowers U_2 norms of $\mathbb{Z}$-bent functions

Here, we will obtain some recurrences for the Gowers U_2 norms of $\mathbb{Z}$-bent functions $h \in \mathcal{B}F_r^k$ in terms of the U_2 Gowers norms of $f_{ij} \in \mathcal{B}F_{r+1}^{k-1}$, where h is obtained by gluing f_{ij}, $0 \le i, j \le 1$. Due to space restrictions, we state it without a proof, which will be available in the full paper.

Theorem 8 *Let $h : \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{Z}$ be the concatenation $h = [h_{00} \| h_{01} \| h_{10} \| h_{11}]$ of four n-variables integer valued functions h_{ij} $(0 \le i, j \le 1)$, satisfying equations* (4)–(5), *for some integer valued functions f_{ij}. Then, with $\gamma = \frac{1}{2}, 1$, if $r \ge 1$, respectively, $r = 0$, we have*

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

We can easily get a proof for Theorem 7 of Dobbertin-Leander [4].

Corollary 9. *If f_{ij} in the theorem above are $\mathbb{Z}$-bent functions and satisfy also equation* (6), *then the function h obtained from gluing f_{ij} is bent.*

4.3 An alternative proof of a theorem by Dobbertin and Leander

In Dobbertin-Leander Theorem 7, 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 8, we shall call it a theorem, due to its importance.

Theorem 10 *Let h_{ij}, f_{ij}, $0 \le i, j \le 1$, 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* $\|f_{00}\|_{U_2}^4 + \|f_{01}\|_{U_2}^4 + \|f_{10}\|_{U_2}^4 + \|f_{11}\|_{U_2}^4 + 3 \cdot 2^{-2n+1} \sum_{\mathbf{u} \in \mathbb{F}_2^n} (\widehat{f_{00}}^2(\mathbf{u}) \widehat{f_{10}}^2(\mathbf{u}) + \widehat{f_{01}}^2(\mathbf{u}) \widehat{f_{11}}^2(\mathbf{u})) = 2^{-n+1}$.

The next theorem uses a result of Kolomeec and Pavlov [9] who showed that $d(g, h) \ge 2^{\frac{n}{2}}$, for any two bent functions in n variables.

Theorem 11 *If f is a splitting $\mathbb{Z}$-bent function of level 1 such that $f(\mathbf{x}) = \frac{\chi_g(\mathbf{x}) + \chi_h(\mathbf{x})}{2}$ where g, h are bent functions, the U_2 Gowers norm is $\|f\|_{U_2}^4 = \frac{2^n - d\left(\widehat{g}, \widehat{h}\right)}{2^{2n}} = \frac{2^n - d(g,h)}{2^{2n}}$. If f is a splitting $\mathbb{Z}$-bent function of level 1 in n variables and not a bent function then $\|f\|_{U_2}^4 \le \frac{2^n - 2^{\frac{n}{2}}}{2^{2n}}$.*

While we were able to compute the U_2 Gowers norm of any bent function in Theorem 1 and give some necessary conditions for splitting $\mathbb{Z}$-bents in Theorem 11, 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 $\widehat{\chi_g}(\mathbf{u}) \cdot \widehat{\chi_h}(\mathbf{u}) = 0$, for any $\mathbf{u} \in \mathbb{F}_2^n$. Equivalently, $\widehat{\chi}_g(\mathbf{u}) = 0$ if and only if $\widehat{\chi}_h(\mathbf{u}) \ne 0$, since if n is odd then for any semibent, its Fourier spectrum has 2^{n-1} nonzero coefficients. In Theorem 3.2 of [6] 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 below Theorem 3.5 of [6] below, which states: Let n be even, and f_1, $f_2 \in \mathcal{B}_n$ be s_1-, respectively, s_2-plateaued functions that are neither bent nor both semibent, and so, $Spec(\chi_{f_i}) = \{0, \pm 2^{1+r_i}\}$, $r_i := \frac{s_i}{2} - 1 \geq 0$ $(i = 1, 2)$. Let α, β 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 $2\beta\epsilon_2 + \alpha\epsilon_1 \notin \{-1, 1\}$ (respectively, $2\alpha\epsilon_1 + \beta\epsilon_2 \notin \{-1, 1\}$), for at least one value of $x \in \mathbb{F}_2^n$; if $r_1 > 0$, $r_2 > 0$, we assume that $\alpha\widehat{\chi_{f_1}}(\mathbf{x}) + \beta\widehat{\chi_{f_2}}(\mathbf{x}) \notin \{0, \pm 2\}$, for at least one value $x \in \mathbb{F}_2^n$. Then, $f(\mathbf{x}) = \frac{\alpha\chi_{f_1}(\mathbf{x}) + \beta\chi_{f_2}(\mathbf{x})}{2}$ is a $\mathbb{Z}$-bent function of level $l := \lceil \log_2 M \rceil$, where $M = \max_{\mathbf{u} \in \mathbb{F}_2^n} \{|\alpha\widehat{\chi_{f_1}}(\mathbf{u}) + \beta\widehat{\chi_{f_2}}(\mathbf{u})|\}$, which cannot be split into two bent functions.

Theorem 12 *Let f be a $\mathbb{Z}$-bent function of level r, and write $f(\mathbf{x}) = \frac{\alpha\chi_g(\mathbf{x}) + \beta\chi_h(\mathbf{x})}{2}$.*

(i) If g, h are disjoint spectra functions that fulfill the conditions of [6, Theorem 3.5], *then $\|f\|_{U_2}^4 = 2^{-n-4}(\alpha^4 2^{s_1} + \beta^4 2^{s_2})$.*

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

$$\|f\|_{U_2}^4 = 2^{-n-4}(\alpha^4 2^{s_1} + \beta^4 2^{s_2}) + 2^{-2n-2}\alpha\beta(\alpha^2 2^{s_1} + \beta^2 2^{s_2})(2^n - 2d(g, h))$$
$$+ 2^{-2n-3}\alpha^2\beta^2 2^{s_1+s_2}|\{\mathbf{x} : \widehat{\chi}_g(\mathbf{x}) \cdot \widehat{\chi}_h(\mathbf{x}) \neq 0\}|.$$

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

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

Let $A = \#(\{\mathbf{u} \in \mathbb{F}_2^n : \widehat{\chi}_g(\mathbf{u}) = 2^{\frac{s_1}{2}}, \widehat{\chi}_h(\mathbf{u}) = 2^{\frac{s_2}{2}}\} \cup \{\mathbf{u} \in \mathbb{F}_2^n : \widehat{\chi}_g(\mathbf{u}) = -2^{\frac{s_1}{2}}, \widehat{\chi}_h(\mathbf{u}) = -2^{\frac{s_2}{2}}\})$, $B = \#(\{\mathbf{u} \in \mathbb{F}_2^n : \widehat{\chi}_g(\mathbf{u}) = 2^{\frac{s_1}{2}}, \widehat{\chi}_h(\mathbf{u}) = -2^{\frac{s_2}{2}}\} \cup \{\mathbf{u} \in \mathbb{F}_2^n : \widehat{\chi}_g(\mathbf{u}) = -2^{\frac{s_1}{2}}, \widehat{\chi}_h(\mathbf{u}) = 2^{\frac{s_2}{2}}\})$.
By Parseval's identity, $\sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{f}^2(\mathbf{x}) = 2^{-2} \sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} (\widehat{\chi}_g^2(\mathbf{x}) + 2\widehat{\chi}_g(\mathbf{x})\widehat{\chi}_h(\mathbf{x}) + \widehat{\chi}_h^2(\mathbf{x})) = \sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} f^2(\mathbf{x}) = 2^{-2} \sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} (\chi_g^2(\mathbf{x}) + 2\chi_g(\mathbf{x})\chi_h(\mathbf{x}) + \chi_h^2(\mathbf{x}))$. Further, $\sum_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{\chi}_g^2(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi_g^2(\mathbf{x})$, and $\sum_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{\chi}_h^2(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi_h^2(\mathbf{x})$, which implies that $\sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{\chi}_g(\mathbf{x})\widehat{\chi}_h(\mathbf{x}) = 2^{\frac{s_1+s_2}{2}}(A - B) = \sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} \chi_g(\mathbf{x})\chi_h(\mathbf{x}) = 2^n - 2d(g, h)$, so $A - B = 2^{-\frac{s_1+s_2}{2}}(2^n - 2d(g, h))$. Notice that $C := A + B$ is the number of positions where both $\widehat{\chi}_g$ and $\widehat{\chi}_h$ are nonzero. Then,

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{\chi}_g^3(\mathbf{x})\widehat{\chi}_h(\mathbf{x}) = 2^{\frac{3s_1}{2}} 2^{\frac{s_2}{2}}(A - B) = 2^{s_1}(2^n - 2d(g, h)),$$
$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{\chi}_g(\mathbf{x})\widehat{\chi}_h^3(\mathbf{x}) = 2^{\frac{s_1}{2}} 2^{\frac{3s_2}{2}}(A - B) = 2^{s_2}(2^n - 2d(g, h)).$$

Finally, $\sum\limits_{\mathbf{x} \in \mathbb{F}_2^n} \widehat{\chi}_g^2(\mathbf{x})\widehat{\chi}_h^2(\mathbf{x}) = 2^{s_1+s_2}(A+B) = C2^{s_1+s_2}$. Then, $\|f\|_{U_2}^4 = 2^{-2n-4}(\alpha^4 2^{2n} \|g\|_{U_2}^4 + \beta^4 2^{2n} \|h\|_{U_2}^4 + 4(\alpha^3\beta 2^{s_1} + \alpha\beta^3 2^{s_1}) \cdot (2^n - 2d(g, h)) + 6\alpha^2\beta^2 C 2^{s_1+s_2} = 2^{-n-4}(\alpha^4 2^{s_1} + \beta^4 2^{s_2}) + 2^{-2n-2}\alpha\beta(\alpha^2 2^{s_1} + \beta^2 2^{s_2})(2^n - 2d(g, h)) + 2^{-2n-3}\alpha^2\beta^2 2^{s_1+s_2} C$, where $C = |\{\mathbf{x} : \widehat{\chi}_g(\mathbf{x}) \cdot \widehat{\chi}_h(\mathbf{x}) \neq 0\}|$. The second claim is similar. $\square$

Corollary 13. *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* (4)–(5)*, for some integer valued* $\mathbb{Z}$*-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* $\mathbb{Z}$*-bent function* h *of level* r *is* $\|h\|_{U_2}^4 = 2^{-5}K$.

References

1. V. Y.-W. Chen, *The Gowers' norm in the testing of Boolean functions*, Ph.D. Thesis, Massachusetts Institute of Technology, June 2009.
2. T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, 2nd Ed. (Academic Press, San Diego, CA, 2017); 1st Ed., 2009.
3. J. F. Dillon, *Elementary Hadamard difference sets*, In: Proceedings of the Sixth S.E. Conference of Combinatorics, Graph Theory, and Computing, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, pp. 237–249 (1975).
4. H. Dobbertin and G. Leander, *Bent functions embedded into the recursive framework of* $\mathbb{Z}$*-bent functions*, Des. Codes Cryptogr. 49 (2008), 3–22.
5. S. Gangopadhyay, B. Mandal, P. Stănică, *Gowers* U_3 *norm of some classes of bent Boolean functions*, Des. Codes Cryptogr. 86 (2018), 1131–1148.
6. S. Gangopadhyay, E. Pasalic, P. Stănică, S. Datta, *A note on non-splitting* $\mathbb{Z}$*-functions*, Inf. Proc. Letters 121 (2017), 1–5.
7. S. Hodžić, W. Meidl, E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual and the Gray image*, IEEE Trans. Inf. Theory 64:7 (2018), 5432–5440.
8. S. Hodžić, E. Pasalic, *Generalized bent functions – Some general construction methods and related necessary and sufficient conditions*, Cryptogr. Commun. 7 (2015), 469–483.
9. N. Kolomeec, A. Pavlov, *Bent functions on the minimal distance*, IEEE Region 8 SIBIRCON-2010, Irkutsk Listvyanka, Russia, July 11–15, 2010.
10. P. V. Kumar, R. A. Scholtz, L. R. Welch, *Generalized bent functions and their properties*, J. Combin Theory – Ser. A 40 (1985), 90–107.
11. T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, *Decomposing generalized bent and hyperbent functions*, IEEE Trans. Inf. Theory 63:12 (2017), 7804–7812.
12. T. Martinsen, W. Meidl, A. Pott, P. Stănică, *On symmetry and differential properties of generalized Boolean functions*, Proc. WAIFI 2018: Arithm. of Finite Fields, 2018.
13. T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, Proc. WAIFI 2016: Arithm. Finite Fields, LNCS 10064 (2017), 160–173.
14. T. Martinsen, W. Meidl, P. Stănică, *Partial Spread and Vectorial Generalized Bent Functions*, Des. Codes Cryptogr. 85:1 (2017), 1–13.
15. S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, and K. Feng, *Further Results on Generalized Bent Functions and Their Complete Characterization*, IEEE Trans. Inform. Theory 64:7 (2018), 5441–5452.
16. B. Preneel, R. Govaerts, J. Vandewalle, *Cryptographic properties of quadratic boolean functions*, Int. Symp. Finite Fields and Appl., 1991.
17. O. S. Rothaus, *On bent functions*, J. Combin. Theory – Ser. A 20 (1976), 300–305.
18. K. U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA*, IEEE Trans. Inf. Theory 55:4 (2009), 1824–1832.
19. P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, Prikl. Diskr. Mat. 1 (2009), 16–18, (see also, http://eprint.iacr.org/2009/544.pdf).
20. P. Stănică, *Weak and strong* 2^k*-bent functions*, IEEE Trans. Inf. Theory 62:5 (2016), 2827–2835.
21. P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptogr. 69 (2013), 77–94.
22. C. Tang, C. Xiang, Y. Qi, K. Feng, *Complete characterization of generalized bent and* 2^k*-bent Boolean functions*, IEEE Trans. Inf. Theory 63:7 (2017), 4668–4674.
23. F. Zhang, S. Xia, P. Stănică, Y. Zhou, *Further results on constructions of generalized bent Boolean functions*, Inf. Sciences - China. 59 (2016), 1–3.