Electronic Colloquium on Computational Complexity, Report No. 180 (2022)

A Lower Bound on the Constant in the Fourier Min-Entropy/Influence Conjecture

Aniruddha Biswas and Palash Sarkar
Indian Statistical Institute
203, B.T.Road, Kolkata
India 700108.
Email: {anib_r, palash}@isical.ac.in

December 15, 2022

Abstract

We describe a new construction of Boolean functions. A specific instance of our construction provides a 30-variable Boolean function having min-entropy/influence ratio to be $128/45 \approx 2.8444$ which is presently the highest known value of this ratio that is achieved by any Boolean function. Correspondingly, 128/45 is also presently the best known lower bound on the universal constant of the Fourier min-entropy/influence conjecture.
Keywords: Boolean function, Fourier transform, Walsh transform, Fourier entropy/influence conjecture, Fourier min-entropy/influence conjecture.

1 Introduction

A longstanding open problem in the field of analysis of Boolean functions is the Fourier Entropy/Influence (FEI) conjecture made by Friedgut and Kalai in 1996 [8]. The FEI conjecture states that there is a universal constant C such that $H(f) \leq C \cdot \mathsf{Inf}(f)$ for any Boolean function f, where $H(f)$ and $\mathsf{Inf}(f)$ denote the Fourier entropy and the total influence of f respectively. The conjecture was verified for various families of Boolean functions (e.g., symmetric functions [16], read-once formulas [15, 6], decision trees of constant average depth [21], read-k decision trees for constant k [21], functions with exponentially small influence or with linear entropy [19], random linear threshold functions [5], cryptographic Boolean functions [9], random functions [7]), but is still open for the class of all Boolean functions.

There has also been research in obtaining lower bounds on the constant C in the FEI conjecture. To show that C is at least some value δ it is sufficient to show the existence of a Boolean function whose entropy/influence ratio is δ. The first lower bound of 4.615 was obtained by O'Donnell et al. in [16]. Later O'Donnell and Tan [15] provided a recursive construction of Boolean functions which showed how to construct a function for which the value of the entropy/influence ratio is at least 6.278944 [11]. The presently best known lower bound on C is 6.454784. This bound was shown by Hod [11] using an extensive asymptotic analysis.

The Fourier min-entropy/influence (FMEI) conjecture was put forward by O'Donnell et al. in 2011 [16]. The FMEI conjecture states that there is a universal constant D such that $H_\infty(f) \leq D \cdot \mathsf{Inf}(f)$ for any Boolean function f, where $H_\infty(f)$ is the Fourier min-entropy of f. The FMEI conjecture is weaker than the FEI conjecture in the sense that settling the FEI conjecture will also settle the FMEI conjecture, but the converse is not true. It was observed in [5, 16] that as a consequence of the

ISSN 1433-8092

Kahn-Kalai-Linial theorem [12] the FMEI conjecture holds for monotone functions and linear threshold functions. The FMEI conjecture for "regular" read-k DNFs was established by Shalev [19]. More recently, Arunachalam et al. [1] have shown that the FMEI holds for read-k DNF for constant k.

To the best of our knowledge, till date there has been no work on obtaining lower bounds on the universal constant of the FMEI conjecture. Since the FMEI conjecture is weaker than the FEI conjecture, any upper bound on the universal constant of the FEI conjecture is also an upper bound on the universal constant of the FMEI conjecture. This, however, does not hold for lower bounds, i.e. a lower bound on the universal constant of the FEI conjecture is not necessarily a lower bound on the universal conjecture of the FMEI conjecture.

The purpose of the present paper is to obtain a lower bound on the universal constant D of the FMEI conjecture. As in the case of the FEI conjecture, to show that D is at least δ, it is sufficient to show the existence of a Boolean function for which the min-entropy/influence ratio is δ. An exhaustive search over all n-variable Boolean functions, with $1 \leq n \leq 5$, shows that the maximum value of min-entropy/influence ratio that is achieved by functions of at most 5 variables is $16/7 \approx 2.285714$. Since an exhaustive search becomes infeasible for $n \geq 6$, it is required to obtain some method of constructing Boolean functions for which the min-entropy/influence ratio is greater than $16/7$.

We first considered the recursive construction of O'Donnell and Tan [15], since this construction proved to be useful for showing a lower bound on the constant of the FEI conjecture. To analyse this construction in the context of the FMEI conjecture, we derived an expression for the min-entropy of the functions obtained using this construction. Since the construction is recursive, one needs an initial function to start the recursion. We performed an exhaustive search over all possible 5-variable initial functions. This yielded a 25-variable function having min-entropy/influence ratio equal to $512/225 \approx 2.275556$. This unfortunately is not useful since $512/225$ is less than $16/7$, the maximum value of min-entropy/influence ratio that is obtained by exhaustive search over all 5-variable functions. The 25-variable function is obtained in the first step of the O'Donnell-Tan recursion. Considering further steps of the recursion does not result in a higher value of the min-entropy/influence ratio. We identified an alternative recursive construction of Boolean functions which provides a lower bound on the constant of the FEI conjecture which is equal to that obtained from the O'Donnell-Tan construction. This alternative construction, however, does not improve upon the lower bound on the constant of the FMEI conjecture that is obtained from the O'Donnell-Tan construction. Further, we did not find any way to apply the asymptotic constructions given by Hod [11] in the context of the FEI conjecture for obtaining lower bounds on the constant in the FMEI conjecture.

Our main result is a new construction of Boolean functions. In simple terms, the construction takes an n-variable function g and constructs an $(n+1)$-variable palindromic function g_0. An $n(n+1)$-variable function G_0 is then constructed by taking the disjoint composition of g_0 and g. Under certain conditions on g, the min-entropy/influence ratio of G_0 is greater than that of g. By searching over all appropriate 5-variable functions g, we obtain a 30-variable function G_0 having min-entropy/influence ratio to be equal to $128/45 \approx 2.844444$. In fact, we obtain a total of 384 such functions G_0. The value $128/45$ is presently the highest achieved value of min-entropy/influence ratio and correspondingly is presently the best known lower bound on D.

In the final section, we provide a brief description of some experiments that we have carried out for symmetric and rotation-symmetric Boolean functions. Based on these experiments, we put forward a new conjecture on entropy/influence and the min-entropy/influence ratios of symmetric Boolean functions.

In Section 2, we describe the formal background and the notation. The technique of disjoint composition is required for our construction. In Section 3, we derive an expression for the min-entropy

of disjoint composition. The recursive construction of O'Donnell and Tan [15] and a new recursive construction is analysed in Section 4 and shown to be not useful for the FMEI conjecture. Section 5 presents the main construction of the paper and the description of the Boolean functions achieving the presently best known value of the min-entropy/influence ratio. In Section 6 we briefly describe our search experiments with symmetric and rotation-symmetric Boolean functions and state the new conjecture. Finally, in Section 7 we provide concluding remarks.

2 Background and notation

Let $\mathbb{F}_2 = \{0, 1\}$ denote the finite field consisting of two elements with addition represented by $\oplus$ and multiplication by $\cdot$; often, for $x, y \in \mathbb{F}_2$, the product $x \cdot y$ will be written as xy. The field of real numbers will be denoted by $\mathbb{R}$ and all logarithms are to the base 2.

For a positive integer n, by $[n]$ we will denote the set $\{1, \ldots, n\}$. For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, the support of $\mathbf{x}$ will be denoted by $\mathsf{supp}(\mathbf{x})$ which is the set $\{i : x_i = 1\}$; the weight of $\mathbf{x}$ will be denoted by $\mathsf{wt}(\mathbf{x})$ and is equal to $\#\mathsf{supp}(\mathbf{x})$. For $i \in [n]$, $\mathbf{e}_i$ denotes the vector in $\mathbb{F}_2^n$ whose i-th component is 1 and all other components are 0. By $\mathbf{1}_n$ and $\mathbf{0}_n$ we will denote the all-one and all-zero vectors of length n respectively. For $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, the inner product $\langle \mathbf{x}, \mathbf{y} \rangle$ of $\mathbf{x}$ and $\mathbf{y}$ is defined to be $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 \oplus \cdots \oplus x_n y_n$.

For a positive integer n, an n-variable Boolean function f is a map $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Variables will be written in upper case and vector of variables in bold upper case. For $\mathbf{X} = (X_1, \ldots, X_n)$, an n-variable Boolean function f will be written as $f(\mathbf{X})$ to denote the dependence on the variables $X_1, \ldots, X_n$.

The support of a Boolean function f will be denoted by $\mathsf{supp}(f)$ which is the set $\{\mathbf{x} : f(\mathbf{x}) = 1\}$; the weight of f will be denoted by $\mathsf{wt}(f)$ and is equal to $\#\mathsf{supp}(f)$. The expectation of f, denoted as $\mathbb{E}(f)$ (taken over a uniform random choice of $\mathbf{x} \in \mathbb{F}_2^n$), is equal to $\mathsf{wt}(f)/2^n$. The function f is said to be balanced if $\mathsf{wt}(f) = 2^{n-1}$.

The Fourier transform of a function $\psi : \mathbb{F}_2^n \to \mathbb{R}$ is the map $\widehat{\psi} : \mathbb{F}_2^n \to \mathbb{R}$, which is defined as follows. For $\boldsymbol{\alpha} \in \mathbb{F}_2^n$,

$$\widehat{\psi}(\boldsymbol{\alpha}) \quad = \quad \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} \psi(\mathbf{x}) (-1)^{\langle \mathbf{x}, \boldsymbol{\alpha} \rangle}. \tag{1}$$

The (normalised) Walsh transform of an n-variable Boolean function f is the map $W_f : \mathbb{F}_2^n \to \mathbb{R}$, which is defined as follows. For $\boldsymbol{\alpha} \in \mathbb{F}_2^n$,

$$W_f(\boldsymbol{\alpha}) \quad = \quad \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \langle \mathbf{x}, \boldsymbol{\alpha} \rangle}$$

In other words, the Walsh transform of f is the Fourier transform of $(-1)^f$.

From Parseval's theorem, it follows that $\sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^n} W_f^2(\boldsymbol{\alpha}) = 1$. So the values $\left\{ W_f^2(\boldsymbol{\alpha}) \right\}_{\boldsymbol{\alpha} \in \mathbb{F}_2^n}$ can be considered to be a probability distribution on $\mathbb{F}_2^n$, which assigns to $\boldsymbol{\alpha} \in \mathbb{F}_2^n$, the probability $W_f^2(\boldsymbol{\alpha})$. For an n-variable Boolean function f, its Fourier entropy $H(f)$ and min-entropy $H_\infty(f)$ are defined as follows.

$$H(f) = \sum_{\substack{\boldsymbol{\alpha} \in \mathbb{F}_2^n \\ W_f^2(\boldsymbol{\alpha}) \neq 0}} W_f^2(\boldsymbol{\alpha}) \log \frac{1}{W_f^2(\boldsymbol{\alpha})}, \qquad H_\infty(f) = \min_{\substack{\boldsymbol{\alpha} \in \mathbb{F}_2^n \\ W_f^2(\boldsymbol{\alpha}) \neq 0}} \log \frac{1}{W_f^2(\boldsymbol{\alpha})}. \tag{2}$$

For an n-variable Boolean function f, its influence $\mathsf{Inf}(f)$ is defined as follows.

$$\mathsf{Inf}(f) \quad = \quad \sum_{i=1}^{n} \Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq f(\mathbf{x} \oplus \mathbf{e}_i)]. \tag{3}$$

The connection of influence to the Walsh transform is given by the following (Theorem 2.38 in [14]).

$$\mathsf{Inf}(f) \quad = \quad \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n} \mathsf{wt}(\boldsymbol{\alpha}) W_f^2(\boldsymbol{\alpha}). \tag{4}$$

We next state the two conjectures connecting entropy and influence.

The Fourier entropy/influence (FEI) conjecture [8]. There exists a universal constant C such that for any integer $n \geq 1$ and for any n-variable Boolean function f, $H(f) \leq C \cdot \mathsf{Inf}(f)$.

The Fourier Min-entropy/influence (FMEI) conjecture [16]. There exists a universal constant D such that for any integer $n \geq 1$ and for any n-variable Boolean function f, $H_\infty(f) \leq D \cdot \mathsf{Inf}(f)$.

Since $H_\infty(f) \leq H(f)$, it follows that the FMEI is weaker than the FEI conjecture in the sense that settling the FEI conjecture will also settle the FMEI conjecture, but not vice versa.

Composition. For positive integers n and k, an (n,k) vectorial Boolean function (also called an S-box) is a map $\mathscr{G} : \mathbb{F}_2^n \to \mathbb{F}_2^k$. The function $\mathscr{G}$ can be written as $\mathscr{G}(\mathbf{X}) = (g_1(\mathbf{X}), \ldots, g_k(\mathbf{X}))$, where $g_1, \ldots, g_k$ are n-variable Boolean functions. Given a k-variable Boolean function f and an (n,k) vectorial Boolean function $\mathscr{G}$, their composition is the n-variable Boolean function $(f \circ \mathscr{G})(\mathbf{X}) = f(g_1(\mathbf{X}), \ldots, g_k(\mathbf{X}))$. The Walsh transform of $f \circ \mathscr{G}$ is given by the following result.

Theorem 1 *[10] Let $\mathscr{G}$ be an (n,k) vectorial Boolean function and f be a k-variable Boolean function. Then for any $\mathbf{u} \in \mathbb{F}_2^n$,*

$$W_{f\circ\mathscr{G}}(\mathbf{u}) \quad = \sum_{\mathbf{v}\in\mathbb{F}_2^k} W_f(\mathbf{v}) W_{(l_\mathbf{v}\circ\mathscr{G})}(\mathbf{u}), \tag{5}$$

where $(l_\mathbf{v} \circ \mathscr{G})(\mathbf{X}) = \langle \mathbf{v}, \mathscr{G}(\mathbf{X}) \rangle$.

Let k and l be positive integers and $n = kl$. For $\mathbf{x} \in \mathbb{F}_2^n$ and $1 \leq i \leq k$, by $\mathbf{x}^{(i)}$ we denote the vector $(x_{(i-1)l+1}, \ldots, x_{il}) \in \mathbb{F}_2^l$. By a slight abuse of notation, we will write $\mathbf{x} = (\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(k)})$. Let f and g be Boolean functions on k and l variables respectively and $n = kl$. Let $\mathscr{G}$ be the (n,k) vectorial Boolean function given by $\mathscr{G}(\mathbf{X}) = (g(\mathbf{X}^{(1)}), \ldots, g(\mathbf{X}^{(k)}))$. The *disjoint composition* of f and g, which we will denote as $f \diamond g$, is the n-variable Boolean function $f \circ \mathscr{G}$, i.e.

$$(f \diamond g)(\mathbf{X}) \quad = \quad (f \circ \mathscr{G})(\mathbf{X}) = f(g(\mathbf{X}^{(1)}), \ldots, g(\mathbf{X}^{(k)})).$$

The following result provides the entropy and influence of $f \diamond g$.

Theorem 2 (simplified form of Proposition 2 in [15]) *Let f and g be two Boolean functions. Then,*

1. $\mathsf{Inf}(f \diamond g) = \mathsf{Inf}(g) \cdot \mathsf{Inf}(f)$.
2. *If g is balanced, then $H(f \diamond g) = H(f) + H(g) \cdot \mathsf{Inf}(f)$.*

O'Donnell-Tan recursive construction. The following recursive construction of Boolean functions was introduced by O'Donnell and Tan [15]. Let g be an l-variable Boolean function. Using g, a sequence of Boolean functions f_m, $m \geq 0$, is defined in the following manner.

$$\left.\begin{array}{rcl} f_0 & = & g, \\ f_m & = & g \diamond f_{m-1} \quad \text{if } m \geq 1. \end{array}\right\} \tag{6}$$

It is easy to see that for $m \geq 0$, f_m is a map from $\mathbb{F}_2^{l^{m+1}} \to \mathbb{F}_2$. For the recursion defined in (6), in the case where the initial function g is balanced, the following was proved in [15].

$$\frac{H(f_m)}{\mathsf{Inf}(f_m)} = \frac{H(g)}{\mathsf{Inf}(g)} + \frac{H(g)}{\mathsf{Inf}(g)(\mathsf{Inf}(g)-1)} - \frac{H(g)}{\mathsf{Inf}(g)^{m+1}(\mathsf{Inf}(g)-1)}. \tag{7}$$

Consequently, $\lim_{m\to\infty} H(f_m)/\mathsf{Inf}(f_m) = H(g)/(\mathsf{Inf}(g)-1)$. So for any Boolean function g, $H(g)/(\mathsf{Inf}(g)-1)$ is a lower bound on the constant in the FEI conjecture.

3 Min-Entropy of disjoint composition

We wish to compute the min-entropy of disjoint composition. We start with the following result which is somewhat more general than what we need.

Theorem 3 *Let k and l be positive integers and $n = kl$. Let $\mathscr{G}$ be an (n,k) vectorial Boolean function such that $\mathscr{G}(\mathbf{X}) = (g_1(\mathbf{X}^{(1)}), \ldots, g_k(\mathbf{X}^{(k)}))$, where $g_1, \ldots, g_k$ are l-variable balanced Boolean functions. Then for any k-variable Boolean function f,*

$$W_{f\circ\mathscr{G}}(\mathbf{u}) = \begin{cases} W_f(\mathbf{0}_k) & \text{if } \mathbf{u} = \mathbf{0}_n, \\ W_f(\mathbf{w_u}) \prod_{i\in\mathsf{supp}(\mathbf{w_u})} W_{g_i}\left(\mathbf{u}^{(i)}\right) & \text{otherwise.} \end{cases} \tag{8}$$

In (8), for $\mathbf{u} \in \mathbb{F}_2^n$ written as $\mathbf{u} = (\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(k)})$, by $\mathbf{w_u}$ we denote the vector in $\mathbb{F}_2^k$ whose i-th position, $1 \leq i \leq k$, is 1 if and only if $\mathbf{u}^{(i)} \neq \mathbf{0}_l$, i.e. $\mathbf{w_u}$ encodes whether the l-bit blocks of $\mathbf{u}$ are zero or not.

Proof: The proof follows from an application of Theorem 1.

Note that for $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{F}_2^k$, $(l_\mathbf{v} \circ \mathscr{G})(\mathbf{X}) = v_1 \cdot g_1(\mathbf{X}^{(1)}) \oplus \cdots \oplus v_k \cdot g_k(\mathbf{X}^{(k)})$. So for $\mathbf{u} = (\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(k)}) \in \mathbb{F}_2^n$,

$$\begin{aligned} W_{(l_\mathbf{v}\circ\mathscr{G})}(\mathbf{u}) &= \frac{1}{2^n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{(l_\mathbf{v}\circ\mathscr{G})(\mathbf{x})\oplus\langle\mathbf{u},\mathbf{x}\rangle} \\ &= \frac{1}{2^n} \sum_{\mathbf{x}^{(1)},\ldots,\mathbf{x}^{(k)}\in\mathbb{F}_2^l} (-1)^{v_1\cdot g_1\left(\mathbf{x}^{(1)}\right)\oplus\langle\mathbf{u}^{(1)},\mathbf{x}^{(1)}\rangle\oplus\cdots\oplus v_k\cdot g_k\left(\mathbf{x}^{(k)}\right)\oplus\langle\mathbf{u}^{(k)},\mathbf{x}^{(k)}\rangle} \\ &= \prod_{i\in[k]} \frac{1}{2^l} \sum_{\mathbf{x}^{(i)}\in\mathbb{F}_2^l} (-1)^{v_i\cdot g_i\left(\mathbf{x}^{(i)}\right)\oplus\langle\mathbf{u}^{(i)},\mathbf{x}^{(i)}\rangle}. \end{aligned}$$

For $i \in [k]$, let $B_i\left(v_i, \mathbf{u}^{(i)}\right) = \frac{1}{2^l}\sum_{\mathbf{x}^{(i)}\in\mathbb{F}_2^l}(-1)^{v_i\cdot g_i\left(\mathbf{x}^{(i)}\right)\oplus\langle\mathbf{u}^{(i)},\mathbf{x}^{(i)}\rangle}$. Using (5) we have,

$$W_{f\circ\mathscr{G}}(\mathbf{u}) = \sum_{\mathbf{v}\in\mathbb{F}_2^k} W_f(\mathbf{v}) W_{(l_\mathbf{v}\circ\mathscr{G})}(\mathbf{u}) = \sum_{\mathbf{v}\in\mathbb{F}_2^k} W_f(\mathbf{v}) \prod_{i\in[k]} B_i\left(v_i, \mathbf{u}^{(i)}\right). \tag{9}$$

Let us now consider $B_i\left(v_i, \mathbf{u}^{(i)}\right)$. Note that $B_i\left(0, \mathbf{u}^{(i)}\right)$ is equal to 1 or 0 according as $\mathbf{u}^{(i)}$ is equal to $\mathbf{0}_l$ or not. Further, $B_i\left(1, \mathbf{u}^{(i)}\right) = W_{g_i}\left(\mathbf{u}^{(i)}\right)$. Since it is given that g_i is balanced, so $B_i\left(1, \mathbf{0}_l\right) = 0$.

For $\mathbf{u} \in \mathbb{F}_2^n$, the i-th bit of $\mathbf{w_u}$ is 1 if and only if the i-th block of $\mathbf{u}$ is non-zero. For $\mathbf{v} \in \mathbf{F}_2^k$ such that $\mathbf{v} \neq \mathbf{w_u}$, there is a $j \in [k]$ such that either $v_j = 0$ and $\mathbf{u}^{(j)} \neq \mathbf{0}_l$, or $v_j = 1$ and $\mathbf{u}^{(j)} = \mathbf{0}_l$; in either case, $B_j\left(v_j, \mathbf{u}^{(j)}\right) = 0$ and so $\prod_{i\in[k]} B_i\left(v_i, \mathbf{u}^{(i)}\right) = 0$. On the other hand, for $\mathbf{v} = \mathbf{w_u}$, if $v_i = 0$ then $\mathbf{u}^{(i)} = \mathbf{0}_l$ which implies $B_i\left(v_i, \mathbf{u}^{(i)}\right) = 1$; and if $v_i = 1$ then $\mathbf{u}^{(i)} \neq \mathbf{0}_l$ which implies $B_i\left(v_i, \mathbf{u}^{(i)}\right) = W_{g_i}\left(\mathbf{u}^{(i)}\right)$; so $\prod_{i\in[k]} B_i\left(v_i, \mathbf{u}^{(i)}\right) = \prod_{i\in\mathsf{supp}(\mathbf{v})} W_{g_i}\left(\mathbf{u}^{(i)}\right)$. From this, we get the required result. □

Suppose in Theorem 3, the g_i's are all equal, i.e. $g_1 = \cdots = g_k = g$. Then $f \circ \mathscr{G} = f \diamond g$ and Theorem 3 provides the Walsh transform of disjoint composition in the case where g is balanced. In this case, the min-entropy is given by the following result.

Theorem 4 *Let k and l be positive integers, f be a k-variable Boolean function, and g be an l-variable balanced Boolean function. For $0 \leq i \leq k$, let $a_i = \max_{\{\mathbf{w}:\mathsf{wt}(\mathbf{w})=i\}} W_f^2(\mathbf{w})$. Then*

$$H_\infty(f \diamond g) = \min_{i\in\{0,\ldots,k\}, a_i>0} (-\log(a_i) + i \cdot H_\infty(g)).$$

Proof: Let $n = kl$ and $\mathscr{G}$ be the (n, k) vectorial Boolean function $\mathscr{G}(\mathbf{X}) = (g(\mathbf{X}^{(1)}), \ldots, g(\mathbf{X}^{(k)}))$. Then $f \diamond g = f \circ \mathscr{G}$ and we can apply Theorem 3 to obtain the Walsh transform of $f \diamond g$. We have from Theorem 3, $W_{f\diamond g}(\mathbf{0}_n) = W_f(\mathbf{0}_k)$, and for $\mathbf{0}_n \neq \mathbf{u} \in \mathbb{F}_2^n$,

$$W_{f\diamond g}(\mathbf{u}) = W_f(\mathbf{w_u}) \prod_{j\in\mathsf{supp}(\mathbf{w_u})} W_g\left(\mathbf{u}^{(j)}\right).$$

From (2), to obtain the min-entropy of $f \diamond g$, it is required to obtain $\max_{\mathbf{u}\in\mathbb{F}_2^n}(W_{f\diamond g}(\mathbf{u}))^2$. Let $\boldsymbol{\alpha}_i = \arg\max_{\mathsf{wt}(\mathbf{w})=i} W_f^2(\mathbf{w})$ for $i \in [k]$ and let $\boldsymbol{\beta} = \arg\max_{\mathbf{v}} W_g^2(\mathbf{v})$ (breaking ties arbitrarily in both cases). Note that $a_i = W_f^2(\boldsymbol{\alpha}_i)$ and $H_\infty(g) = -\log W_g^2(\boldsymbol{\beta})$. For $\mathsf{wt}(\mathbf{w_u}) = i$, the maximum value of $\prod_{j\in\mathsf{supp}(\mathbf{w_u})} W_g^2\left(\mathbf{u}^{(j)}\right)$ is $\left(W_g^2(\boldsymbol{\beta})\right)^i$. So $\max_{\mathbf{0}_n\neq\mathbf{u}\in\mathbb{F}_2^n}(W_{f\diamond g}(\mathbf{u}))^2$ is equal to $\max_{i\in[k]} W_f^2(\boldsymbol{\alpha}_i)\left(W_g^2(\boldsymbol{\beta})\right)^i = \max_{i\in[k]} a_i \left(W_g^2(\boldsymbol{\beta})\right)^i$. The result now follows by taking logarithms. □

4 Recursive constructions

We wish to obtain a Boolean function f such that $H_\infty(f)/\mathsf{Inf}(f)$ is as high as possible. One way to obtain f is to perform an exhaustive search. Since the number of n-variable Boolean functions is 2^{2^n}, it is difficult to carry out the search for $n > 5$. For $n = 5$, we have performed an exhaustive search. This resulted in 3840 5-variable Boolean functions for which the min-entropy/influence ratio is 16/7. All the 3840 functions turned out to be unbalanced. For the purpose of illustration, we provide one of the 3840 functions that were obtained.

Example 1 *Let h be the following 5-variable Boolean function.*

$$h(X_5, X_4, X_3, X_2, X_1) \;=\; X_4X_3 \oplus X_5X_2 \oplus X_5X_4X_1 \oplus X_5X_4X_2 \oplus X_5X_4X_3. \tag{10}$$

For h defined in (10), $H_\infty(h) = 4$, $\mathsf{Inf}(h) = 7/4$ and so $H_\infty(h)/\mathsf{Inf}(h) = 16/7$.

The question now is whether it is possible to obtain a function whose min-entropy/influence ratio is greater than 16/7? In this section, we describe the approaches based on recursive constructions which did not provide such a function. In the next section, we describe a method which yields a function whose min-entropy/influence ratio is greater than that of h.

4.1 O'Donnell and Tan's Construction

We first consider the recursive construction of Boolean functions arising from the O'Donnell-Tan construction since this construction proved to be useful for the entropy/influence ratio. Using Theorem 4, we obtain the following result on the min-entropy of the O'Donnell-Tan recursive construction where the initial function satisfies the condition that there is a vector of weight 1 for which the corresponding Walsh transform value is the maximum.

Theorem 5 *Let g be an l-variable balanced Boolean function for which there is a $\boldsymbol{\beta} \in \mathbb{F}_2^l$ with $\mathsf{wt}(\boldsymbol{\beta}) = 1$ such that $W_g^2(\boldsymbol{\beta}) = \max_{\mathbf{v}} W_g^2(\mathbf{v})$. For $m \geq 0$, let f_m be the Boolean function constructed using (6) with $f_0 = g$. Then for $m \geq 0$,*

$$H_\infty(f_m) \;=\; (m+1) \cdot H_\infty(g). \tag{11}$$

Consequently,

$$\frac{H_\infty(f_m)}{\mathsf{Inf}(f_m)} = \left(\frac{H_\infty(g)}{\mathsf{Inf}(g)}\right)\left(\frac{m+1}{\mathsf{Inf}(g)^m}\right). \tag{12}$$

Proof: Note that $H_\infty(g) = -\log(W_g^2(\boldsymbol{\beta}))$. Further, since g is balanced, using Theorem 3, it follows that f_m is balanced for all $m \geq 1$.

We prove (11) by induction on m. For $m = 0$, this follows from the given condition on g. Suppose (11) holds for some $m \geq 0$. From Theorem 4 and the fact that f_{m+1} is balanced, $H_\infty(f_{m+1}) = H_\infty(g \diamond f_m) = \min_{i \in [l], a_i > 0}(-\log(a_i) + i \cdot H_\infty(f_m))$, where $a_i = \max_{\mathsf{wt}(\mathbf{w})=i} W_g^2(\mathbf{w})$ for $i = 1, \ldots, l$. For any $i \in [l]$, we have $-\log(a_i) + i \cdot H_\infty(f_m) \geq -\log(W_g^2(\boldsymbol{\beta})) + H_\infty(f_m) = H_\infty(g) + H_\infty(f_m)$ and since $\boldsymbol{\beta}$ has weight 1, equality is attained for $i = 1$. So using the induction hypothesis, $H_\infty(f_{m+1}) = \min_{i \in [l], a_i > 0}(-\log(a_i) + i \cdot H_\infty(f_m)) = H_\infty(g) + H_\infty(f_m) = (m+2)H_\infty(g)$.

The proof of (12) follows from (11) and Theorem 2. □

To use Theorem 5 as an amplifier of min-entropy/influence ratio it is required to obtain $m \geq 1$ such that $H_\infty(f_m)/\mathsf{Inf}(f_m) > H_\infty(g)/\mathsf{Inf}(g)$ which holds if and only if $\mathsf{Inf}(g) < (m+1)^{1/m}$. For $m = 1$, this condition becomes $\mathsf{Inf}(g) < 2$ and for higher values of m, the upper bound on $\mathsf{Inf}(g)$ is lower. Comparing (7) with (12), we see that unlike the case of the entropy/influence ratio, increasing m does not necessarily lead to a higher value of the min-entropy/influence ratio. In particular, the nice asymptotic analyses [15, 11] which has been done for the entropy/influence ratio is not applicable to the min-entropy/influence ratio.

To apply Theorem 5, we need an appropriate initial function g. We performed an exhaustive search over all possible 5-variable Boolean functions which satisfy the conditions of Theorem 5. For $m = 1$, we obtained 384 functions such that taking f_0 to be any of these functions leads to a 25-variable Boolean function f_1 with $H_\infty(f_1)/\mathsf{Inf}(f_1) = 512/225 \approx 2.275556$. Let $\mathcal{F}_5$ denote the set of these 384 functions. As an example, we provide one element of $\mathcal{F}_5$.

Example 2 *Let g be the following 5-variable Boolean function.*

$$\begin{aligned} & g(X_5, X_4, X_3, X_2, X_1) \\ &= \; X_3X_2X_1 \oplus X_4 \oplus X_4X_1 \oplus X_4X_2 \oplus X_4X_2X_1 \oplus X_4X_3X_1 \oplus X_4X_3X_2 \\ &\quad \oplus X_5 \oplus X_5X_1 \oplus X_5X_2X_1 \oplus X_5X_3 \oplus X_5X_3X_1 \oplus X_5X_3X_2 \oplus X_5X_4 \\ &\quad \oplus X_5X_4X_1 \oplus X_5X_4X_2 \oplus X_5X_4X_3. \end{aligned} \tag{13}$$

The function g defined in (13) is in $\mathcal{F}_5$. For g, $H_\infty(g) = 4$, $\mathsf{Inf}(g) = 15/8$. Taking $f_0 = g$ and $f_1 = f_0 \diamond f_0$, from Theorem 5 we have $H_\infty(f_1)/\mathsf{Inf}(f_1) = 32/15 \times 2/(15/8) = 512/225$.

We note the following points.

1. The 25-variable function f_1 obtained using the above method is not useful. The 5-variable function h given in (10) obtained using exhaustive search has a higher value of the min-entropy/influence ratio.

2. In our search over all 5-variable Boolean functions, considering $m > 1$ did not provide a result better than that obtained for $m = 1$.

3. In Theorem 5, the condition $\mathsf{wt}(\boldsymbol{\beta}) = 1$ is required to obtain the expression for f_m given by (11). Considering $\mathsf{wt}(\boldsymbol{\beta}) > 1$, on the other hand, does not seem to lead to a higher value of the min-entropy/influence ratio.

4.2 A different recursion

Let g be an l-variable Boolean function. We define a sequence $\{g_m\}_{m\geq 0}$ of Boolean functions as follows.

$$\left.\begin{array}{rcl} g_0 & = & g, \\ g_m & = & g_{m-1} \diamond g_{m-1} \quad \text{if } m \geq 1. \end{array}\right\} \tag{14}$$

For $m \geq 0$, g_m is a map from $\mathbb{F}_2^{l^{2^m}}$ to $\mathbb{F}_2$. If we start (6) and (14) with the same initial function g, then we obtain $f_1 = g_1$, but for $m > 1$, the two sequences are different. More generally, the sequence defined using (14) is not a sub-sequence of the sequence defined using (6).

Suppose g is a balanced function. Using Theorem 2, it is possible to show that $H(g_m) = H(g)(1 + \mathsf{Inf}(g_0))(1 + \mathsf{Inf}(g_1)) \ldots (1 + \mathsf{Inf}(g_{m-1}))$ and $\mathsf{Inf}(g_m) = \mathsf{Inf}(g)\mathsf{Inf}(g_0)\mathsf{Inf}(g_1) \ldots \mathsf{Inf}(g_{m-1}) = \mathsf{Inf}(g)^{2^m}$. From this it is possible to show that $H(g_m)/\mathsf{Inf}(g_m) = (H(g)/(\mathsf{Inf}(g) - 1)) \cdot (1 - 1/\mathsf{Inf}(g)^m)$. So as $m \to \infty$, $H(g_m)/\mathsf{Inf}(g_m)$ goes to $H(g)/(\mathsf{Inf}(g) - 1)$ which is the same limit as that obtained from the O'Donnell-Tan recursion. So the recursion given by (14) provides a different way of achieving the same limit for the entropy/influence ratio as that obtained using the O'Donnell-Tan recursion.

Suppose g is such that $W_g^2(\mathbf{v})$ is maximum for some $\mathbf{v}$ of weight 1. Let $\{g_m\}_{m\geq 0}$ be the sequence defined in (14) with $g_0 = g$. Then in a manner similar to the proof of Theorem 5 it can be shown that $H_\infty(g_m) = 2^m \cdot H_\infty(g)$. So $H_\infty(g_m)/\mathsf{Inf}(g_m) = (H(g)/\mathsf{Inf}(g)) \cdot (2^m/\mathsf{Inf}(g)^{2^m-1})$. For $m = 1$, this is the same as the O'Donnell-Tan construction and for $m > 1$, it does not lead to any improvement over the O'Donnell-Tan construction. So for the min-entropy/influence ratio, the new recursion does not provide anything better than the O'Donnell-tan construction.

5 Construction from palindromic functions

An n-variable Boolean function g can be represented by a bit string of length 2^n in the following manner: for $i \in \{0, \ldots, 2^n - 1\}$, the i-th bit of the string is $g(\boldsymbol{\alpha})$, where $\boldsymbol{\alpha}$ is the n-bit binary representation of i. We will denote the bit string representing g also by g. The reverse of the bit string representation of g is g^r, and g^r is given by $g^r(X_n, \ldots, X_1) = g(1 \oplus X_n, \ldots, 1 \oplus X_1)$. The following simple result relates the Walsh transforms of g and g^r.

Proposition 1 *Let g be an n-variable Boolean function and g^r be another n-variable Boolean function defined as $g^r(X_n, \ldots, X_1) = g(1 \oplus X_n, \ldots, 1 \oplus X_1)$. Then for $\boldsymbol{\alpha} \in \mathbb{F}_2^n$, $W_{g^r}(\boldsymbol{\alpha}) = (-1)^{\mathsf{wt}(\boldsymbol{\alpha})} W_g(\boldsymbol{\alpha})$.*

Given an n-variable Boolean function g, we may construct an $(n+1)$-variable Boolean f function in the following manner. Concatenate the bit string representing g and g^r to obtain a bit string of length

2^{n+1}. This string represents the desired $(n+1)$-variable Boolean function f. The bit string representing f is a palindrome and we call f to be a palindromic function. The following construction is a little more general than the method just described. For $b \in \mathbb{F}_2$, let

$$g_b(X_{n+1}, X_n, \ldots, X_1) \;=\; (1 \oplus X_{n+1})g(X_n, \ldots, X_1) \oplus X_{n+1}(b + g(1 \oplus X_n, \ldots, 1 \oplus X_1)). \quad (15)$$

If $b = 0$, then f_0 is the concatenation of g and g^r as described above, and if $b = 1$, then f_1 is the concatenation of g and the complement of g^r. The following result shows the relation between the relevant properties of g and g_b.

Proposition 2 *Let g be an n-variable Boolean function and $b \in \mathbb{F}_2$. Let g_b be the $(n+1)$-variable Boolean function constructed from g and b using* (15)*. Then the following holds.*

1. *For $\boldsymbol{\beta} \in \mathbb{F}_2^{n+1}$, where $\boldsymbol{\beta} = (a, \boldsymbol{\alpha})$, with $a \in \mathbb{F}_2$ and $\boldsymbol{\alpha} \in \mathbb{F}_2^n$,*

$$W_{g_b}(\boldsymbol{\beta}) \;=\; \left(\frac{(1 + (-1)^{b+\mathsf{wt}(\boldsymbol{\beta})})}{2}\right) W_g(\boldsymbol{\alpha}). \quad (16)$$

2. *$H_\infty(g_b) = H_\infty(g)$.*
3. *$\mathsf{Inf}(g_b) = \mathsf{Inf}(g) + \epsilon_b(g)$, where $\epsilon_b(g) = \displaystyle\sum_{\substack{\boldsymbol{\alpha} \in \mathbb{F}_2^n \\ \mathsf{wt}(\boldsymbol{\alpha}) \not\equiv b \bmod 2}} W_g^2(\boldsymbol{\alpha})$.*

Proof: By definition

$$W_{g_b}(\boldsymbol{\beta}) \;=\; \frac{1}{2^{n+1}} \sum_{\mathbf{x} \in \mathbb{F}_2^{n+1}} (-1)^{g_b(\mathbf{x}) \oplus \langle \boldsymbol{\beta}, \mathbf{x} \rangle}. \quad (17)$$

We simplify the exponent in the sum.

$$\begin{aligned} & g_b(x_{n+1}, x_n, \ldots, x_1) \oplus \langle (a, \boldsymbol{\alpha}), (x_{n+1}, x_n, \ldots, x_1) \rangle \\ &= (1 \oplus x_{n+1})g(x_n, \ldots, x_1) \oplus x_{n+1}(b \oplus g(1 \oplus x_n, \ldots, 1 \oplus x_1)) \oplus \langle (a, \boldsymbol{\alpha}), (x_{n+1}, x_n, \ldots, x_1) \rangle \\ &= \begin{cases} g(x_n, \ldots, x_1) \oplus \langle \boldsymbol{\alpha}, (x_n, \ldots, x_1) \rangle & \text{if } x_{n+1} = 0, \\ b \oplus g(1 \oplus x_n, \ldots, 1 \oplus x_1) \oplus a \oplus \langle \boldsymbol{\alpha}, (x_n, \ldots, x_1) \rangle & \text{if } x_{n+1} = 1. \end{cases} \end{aligned} \quad (18)$$

Writing $\mathbf{x} = (x_{n+1}, \mathbf{y})$, where $x_{n+1} \in \mathbb{F}_2$ and $\mathbf{y} \in \mathbb{F}_2^n$, we simplify (17) using (18) as follows.

$$\begin{aligned} W_{g_b}(\boldsymbol{\beta}) &= \frac{1}{2^{n+1}} \left(\sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{y}) \oplus \langle \boldsymbol{\alpha}, \mathbf{y} \rangle} + (-1)^{a \oplus b} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{1}_n \oplus \mathbf{y}) \oplus \langle \boldsymbol{\alpha}, \mathbf{y} \rangle} \right) \\ &= \frac{1}{2} \left(W_g(\boldsymbol{\alpha}) + (-1)^{a \oplus b} W_{g^r}(\boldsymbol{\alpha}) \right) \\ &= \frac{1}{2} \left(W_g(\boldsymbol{\alpha}) + (-1)^{a \oplus b} (-1)^{\mathsf{wt}(\boldsymbol{\alpha})} W_g(\boldsymbol{\alpha}) \right) \quad \text{(using Proposition 1)} \\ &= \frac{1}{2} \left(W_g(\boldsymbol{\alpha}) + (-1)^{b} (-1)^{\mathsf{wt}(a, \boldsymbol{\alpha})} W_g(\boldsymbol{\alpha}) \right). \end{aligned}$$

This proves the first point. The second point follows directly from the first.

For the third point, we use (4) to compute the influence of g_b from its Walsh transform.

$$\begin{aligned}
\mathsf{Inf}(g_b) &= \sum_{a\in\mathbb{F}_2,\boldsymbol{\alpha}\in\mathbb{F}_2^n} \mathsf{wt}(a,\boldsymbol{\alpha})W_{g_b}^2(a,\boldsymbol{\alpha}) \\
&= \sum_{a\in\mathbb{F}_2,\boldsymbol{\alpha}\in\mathbb{F}_2^n} \mathsf{wt}(a,\boldsymbol{\alpha}) \left(\frac{(1+(-1)^{b+\mathsf{wt}(a,\boldsymbol{\alpha})})}{2}\right)^2 W_g^2(\boldsymbol{\alpha}) \\
&= \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n} \mathsf{wt}(\boldsymbol{\alpha}) \left(\frac{(1+(-1)^{b+\mathsf{wt}(\boldsymbol{\alpha})})}{2}\right)^2 W_g^2(\boldsymbol{\alpha}) \\
&\quad + \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n} (1+\mathsf{wt}(\boldsymbol{\alpha})) \left(\frac{(1-(-1)^{b+\mathsf{wt}(\boldsymbol{\alpha})})}{2}\right)^2 W_g^2(\boldsymbol{\alpha}) \\
&= \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n,\mathsf{wt}(\boldsymbol{\alpha})\equiv b \bmod 2} \mathsf{wt}(\boldsymbol{\alpha})W_g^2(\boldsymbol{\alpha}) \\
&\quad + \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n,\mathsf{wt}(\boldsymbol{\alpha})\not\equiv b \bmod 2} (1+\mathsf{wt}(\boldsymbol{\alpha}))W_g^2(\boldsymbol{\alpha}) \\
&= \mathsf{Inf}(g) + \epsilon_b(g).
\end{aligned}$$

□

We note the following two points.

1. The Walsh transform of g_b is banded, i.e. it is zero for all vectors of weights congruent to $1-b$ modulo two.
2. From Parseval's theorem it follows that $0 \leq \epsilon_b(g) \leq 1$.

We recall two well known classes of Boolean function. See [3] for an extensive discussion on the various properties of these classes. Let f be an n-variable Boolean function.

- f is said to be t-resilient, $0 \leq t < n$, if $W_f(\boldsymbol{\alpha}) = 0$ for all $\boldsymbol{\alpha}$ with $\mathsf{wt}(\boldsymbol{\alpha}) \leq t$.
- f is said to be plateaued, if $W_f(\boldsymbol{\alpha})$ takes the values $0, \pm c$, for some c.

From (4), it follows that if f is t-resilient, then $\mathsf{Inf}(f) \geq t+1$.

Next we present the main result of the paper.

Theorem 6 *Let g be a balanced n-variable Boolean function, $b \in \mathbb{F}_2$ and g_b be constructed from g and b as in* (15)*. Let $G_b = g_b \diamond g$. Then*

$$\frac{H_\infty(G_b)}{\mathsf{Inf}(G_b)} = \frac{\min_{i\in\{0,\ldots,k\},a_i>0}(-\log(a_i) + iH_\infty(g))}{\mathsf{Inf}(g)(\mathsf{Inf}(g)+\epsilon_b(g))}, \tag{19}$$

where $a_i = \max_{\{\mathbf{w}:\mathsf{wt}(\mathbf{w})=i\}} W_{g_b}^2(\mathbf{w})$, $i = 0,\ldots,k$.

Further, suppose that there is a $t \geq 0$ such that $t \equiv b \bmod 2$ and g is a plateaued t-resilient function, which is not $(t+1)$-resilient. Then

$$\frac{H_\infty(G_b)}{\mathsf{Inf}(G_b)} = \frac{H_\infty(g)}{\mathsf{Inf}(g)}\left(\frac{t+3}{\mathsf{Inf}(g)+\epsilon_b(g)}\right). \tag{20}$$

Proof: Proposition 2 provides the expression for $\mathsf{Inf}(g_b)$ and Theorem 2 provides the expression for $\mathsf{Inf}(G_b)$. The expression for $H_\infty(G_b)$ is obtained from Theorem 4. This shows (19).

Now suppose g is a t-resilient plateaued function such that $t \equiv b \bmod 2$. Since g is plateaued, from (16), it follows that g_b is also plateaued and for $a_i > 0$, $-\log(a_i) = H_\infty(g)$. From the conditions g is t-resilient and $t \equiv b \bmod 2$, it follows that g_b is $(t+1)$-resilient. To see this, suppose $\boldsymbol{\beta} \in \mathbb{F}_2^{n+1}$ with $\mathsf{wt}(\boldsymbol{\beta}) \leq t+1$. If $\mathsf{wt}(\boldsymbol{\beta}) = t+1$, then since $t \equiv b \bmod 2$, we have $1 + (-1)^{b+\mathsf{wt}(\boldsymbol{\beta})} = 0$ and so $W_{g_b}(\boldsymbol{\beta}) = 0$; on the other hand, if $\mathsf{wt}(\boldsymbol{\beta}) < t+1$, then writing $\boldsymbol{\beta} = (a, \boldsymbol{\alpha})$ with $a \in \mathbb{F}_2$ and $\boldsymbol{\alpha} \in \mathbb{F}_2^n$, and using the fact that g is t-resilient, it follows that $\mathsf{wt}(\boldsymbol{\alpha}) \leq t$ and so $W_g(\boldsymbol{\alpha}) = 0$ which implies that $W_{g_b}(\boldsymbol{\beta}) = 0$. Further, since g is not $(t+1)$-resilient, it follows that g_b is not $(t+2)$-resilient. Since g_b is $(t+1)$-resilient, but not $(t+2)$-resilient, it follows that the minimum value of i such that $a_i > 0$ is $t+2$. Now using the fact that for $a_i > 0$, $-\log(a_i) = H_\infty(g)$, we have $\min_{i \in \{0,\ldots,k\}, a_i > 0}(-\log(a_i) + iH_\infty(g)) \geq H_\infty(g) + (t+2)H_\infty(g) = (t+3)H_\infty(g)$. This shows (20). □

5.1 Construction of a 30-variable Boolean function

By construction, if g is an n-variable Boolean function, then the function G_b in Theorem 6 is an $n(n+1)$-variable Boolean function. To use Theorem 6 as an amplifier of min-entropy/influence ratio, it is required to have $H_\infty(G_b)/\mathsf{Inf}(G_b) > H_\infty(g)/\mathsf{Inf}(g)$. If g is a plateaued t-resilient function, then the last condition holds if and only if $t + 3 \geq \mathsf{Inf}(g) + \epsilon_b(g)$. Note, however, that $\mathsf{Inf}(g) \geq t+1$ and so the condition $t+3 \geq \mathsf{Inf}(g) + \epsilon_b(g)$ offers only a limited scope for amplification of the min-entropy/influence ratio.

If g is balanced, but not 1-resilient, i.e. $t = 0$, then the amplification factor in Theorem 6 is $3/(\mathsf{Inf}(g) + \epsilon_b(g))$. We compare this condition with the amplification factor for $m = 1$ arising from the O'Donnell-Tan construction. From Theorem 5, the amplification factor in the O'Donnell-Tan construction is $2/\mathsf{Inf}(g)$. So if we use the same g in both Theorems 5 and 6, then the amplification provided by Theorem 6 is greater if and only if $\mathsf{Inf}(g) > 2\epsilon_b(g)$. The last condition holds for all $g \in \mathcal{F}_5$ (for the definition of $\mathcal{F}_5$ see the discussion before Example 2). So if we take any of the functions in $\mathcal{F}_5$ as the initial function and apply Theorem 6, we will obtain a function whose min-entropy/influence ratio is greater than what can be obtained by starting with the same initial function and using one step of the O'Donnell-Tan construction.

As a concrete example, we consider the 5-variable function g given in Example 2. Using this g and taking $b = 0$, from (15), we obtain a 6-variable function g_0. The function $G_0 = g_0 \diamond g$ is a 30-variable function. From Theorem 6, we have $H_\infty(G_0)/\mathsf{Inf}(G_0) = 128/45 \approx 2.8444$. Starting with any of the 384 functions in $\mathcal{F}_5$ and applying Theorem 6, we obtain a corresponding 30-variable function for which the min-entropy/influence ratio is also 128/45. This gives us a set of 384 30-variable functions each of which has min-entropy/influence ratio to be 128/45. Note that 128/45 is greater than 16/7, which is the maximum min-entropy/influence ratio that is achieved by any 5-variable function (see Example 1 and the discussion preceeding it). Presently, 128/45 is the highest known value of min-entropy/influence ratio that has been achieved. Correspondingly, 128/45 is also the best known lower bound on the universal constant of the min-entropy/influence conjecture.

6 Some further search results

A Boolean function f is said to be symmetric if it is invariant under any permutation of its input. The number of n-variable symmetric Boolean functions is 2^{n+1}. O'Donnell et al. [16] established the FEI conjecture for symmetric Boolean functions which also settles the FMEI conjecture for this class

of functions. Their proof showed that the entropy/influence ratio of any symmetric Boolean function is at most 12.04. We used exhaustive search to find the actual value of the ratio for symmetric functions on n variables with $n \leq 16$.

For $n \geq 2$, let $A_n(X_1, \ldots, X_n) = X_1 \cdots X_n$ (in terms of Boolean algebra A_n is the AND function). It is easy to show (see [11]) that $H(A_n)/\mathsf{Inf}(A_n) < 4$. Our search for $n \leq 16$ showed that if f is an n-variable symmetric Boolean function, then $H(f)/\mathsf{Inf}(f) \leq H(A_n)/\mathsf{Inf}(A_n)$. This suggests that the ratio 12.04 that was achieved in the proof of [16] is perhaps not the minimum possible value of the entropy/influence ratio for symmetric functions.

A Boolean function f is said to be bent [17] if all the Walsh transform values of f are equal. Such functions can exist only if n is even. If f is bent, then $H(f) = H_\infty(f) = n$. Further, $\mathsf{Inf}(f) = n/2$ (see [2]). So for a bent function f, $H(f)/\mathsf{Inf}(f) = H_\infty(f)/\mathsf{Inf}(f) = 2$. Symmetric functions can be bent and the class of symmetric bent functions have been characterised [18, 13]. Our search showed that if n is even, then for any n-variable symmetric Boolean function f, $H_\infty(f)/\mathsf{Inf}(f) \leq 2$ and equality is achieved if and only if f is bent; on the other hand, if n is odd, then for any n-variable symmetric Boolean function f, $H_\infty(f)/\mathsf{Inf}(f) < 2$.

Based on our observations, we put forth the following conjecture.

Conjecture 1 *Let f be an n-variable symmetric Boolean function. Then*

1. *$H(f)/\mathsf{Inf}(f) \leq H(A_n)/\mathsf{Inf}(A_n)$ and equality is achieved if and only if f equals A_n.*
2. *If n is even, then $H_\infty(f)/\mathsf{Inf}(f) \leq 2$ and equality is achieved if and only if f is bent; if n is odd, then $H_\infty(f)/\mathsf{Inf}(f) < 2$*

A closed form expression for the Walsh transform of symmetric Boolean function in terms of binomial coefficients is known [4]. We could not, however, find a way to use this expression to settle the above conjecture. We also tried to apply the techniques from [16] used for showing that the FEI conjecture holds for symmetric Boolean functions to settle Conjecture 1 but were not successful. The main problem is that the various inequalities used in the proof of [16] do not seem to be sufficiently sharp to establish the bounds stated in the above conjecture. As mentioned above, Conjecture 1 has been verified for $1 \leq n \leq 16$. It is possible to experimentally verify the conjecture for additional values of n, but this is unlikely to provide any insight into how to settle the conjecture.

A Boolean function is said to be rotation symmetric if it is invariant under a cyclic shift of its input. It is not known whether the FEI (or the FMEI) conjecture holds for rotation symmetric Boolean functions. See [20] for the number of rotation symmetric Boolean functions on n variables. We could perform an exhaustive search on rotation symmetric Boolean functions for $n \leq 7$. For $n = 6$ and $n = 7$, the maximum values of $H(f)/\mathsf{Inf}(f)$ are 3.739764 and 3.804357 respectively; and the maximum values of $H_\infty(f)/\mathsf{Inf}(f)$ are 2.168978 and 2.227449 respectively, where the maximums are over all n-variable rotation symmetric Boolean function. Compared to symmetric Boolean functions, we see that the maximum value of the entropy/influence ratio remains below 4, but the maximum value of the min-entropy/influence ratio is greater than 2. Since we could not run the experiment for higher values of n, we are unable to put forward any conjecture for rotation symmetric Boolean functions.

7 Concluding remarks

Our work has opened the interesting topic of obtaining lower bounds on the universal constant of the FMEI conjecture. We have provided one method of constructing Boolean functions which provides the presently best known lower bound. A future challenge is to obtain other construction methods which

yield functions with a higher value of the min-entropy/influence ratio. It is also interesting to look for sufficiently sharp techniques to settle Conjecture 1. A final open problem resulting from our work is to settle the FEI conjecture for rotation symmetric Boolean functions.

References

[1] Srinivasan Arunachalam, Sourav Chakraborty, Michal Koucký, Nitin Saurabh, and Ronald de Wolf. Improved bounds on Fourier entropy and min-entropy. *ACM Trans. Comput. Theory*, 13(4):22:1–22:40, 2021.

[2] Aniruddha Biswas and Palash Sarkar. Separation results for boolean function classes. *Cryptogr. Commun.*, 13(3):451–458, 2021.

[3] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, January 2021.

[4] Francis N. Castro, Luis A. Medina, and Pantelimon Stanica. Generalized walsh transforms of symmetric and rotation symmetric boolean functions are linear recurrent. *Appl. Algebra Eng. Commun. Comput.*, 29(5):433–453, 2018.

[5] Sourav Chakraborty, Sushrut Karmalkar, Srijita Kundu, Satyanarayana V. Lokam, and Nitin Saurabh. Fourier entropy-influence conjecture for random linear threshold functions. In Michael A. Bender, Martin Farach-Colton, and Miguel A. Mosteiro, editors, *LATIN 2018: Theoretical Informatics - 13th Latin American Symposium, Buenos Aires, Argentina, April 16-19, 2018, Proceedings*, volume 10807 of *Lecture Notes in Computer Science*, pages 275–289. Springer, 2018.

[6] Sourav Chakraborty, Raghav Kulkarni, Satyanarayana V Lokam, and Nitin Saurabh. Upper bounds on Fourier entropy. *Theoretical Computer Science*, 654:92–112, 2016.

[7] Bireswar Das, Manjish Pal, and Vijay Visavaliya. The entropy influence conjecture revisited. *arXiv preprint arXiv:1110.4301*, 2011.

[8] Ehud Friedgut and Gil Kalai. Every monotone graph property has a sharp threshold. *Proceedings of the American mathematical Society*, 124(10):2993–3002, 1996.

[9] Sugata Gangopadhyay and Pantelimon Stănică. Fourier Entropy-Influence Conjecture for Cryptographic Boolean Functions. *Special issue on Advances in Cryptology and Information Security in Transactions on Advanced Research*, 12(2):8–14, 2016.

[10] Kishan Chand Gupta and Palash Sarkar. Toward a general correlation theorem. *IEEE Trans. Inf. Theory*, 51(9):3297–3302, 2005.

[11] Rani Hod. Improved lower bounds for the Fourier entropy/influence conjecture via lexicographic functions. *arXiv preprint arXiv:1711.00762*, 2017.

[12] Jeff Kahn, Gil Kalai, and Nathan Linial. The influence of variables on boolean functions (extended abstract). In *29th Annual Symposium on Foundations of Computer Science, White Plains, New York, USA, 24-26 October 1988*, pages 68–80. IEEE Computer Society, 1988.

[13] Subhamoy Maitra and Palash Sarkar. Characterization of symmetric bent functions – an elementary proof. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 43:227–230, 2002.

[14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[15] Ryan O'Donnell and Li-Yang Tan. A composition theorem for the Fourier entropy-influence conjecture. In *International Colloquium on Automata, Languages, and Programming*, pages 780–791. Springer, 2013.

[16] Ryan O'Donnell, John Wright, and Yuan Zhou. The Fourier entropy–influence conjecture for certain classes of boolean functions. In *International Colloquium on Automata, Languages, and Programming*, pages 330–341. Springer, 2011.

[17] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.

[18] Peter Savický. On the bent boolean functions that are symmetric. *European Journal of Combinatorics*, 15(4):407–410, 1994.

[19] Guy Shalev. On the Fourier entropy influence conjecture for extremal classes. *arXiv preprint arXiv:1806.03646*, 2018.

[20] Pantelimon Stanica and Subhamoy Maitra. A constructive count of rotation symmetric functions. *Information Processing Letters*, 88(6):299–304, 2003.

[21] Andrew Wan, John Wright, and Chenggang Wu. Decision trees, protocols and the entropy-influence conjecture. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 67–80, 2014.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il