2014-01-25

The Fourier Entropy-Influence Conjecture Holds for a Log-Density 1 Class of Cryptographic Boolean Functions

Stănică, Pantelimon

THE FOURIER ENTROPY-INFLUENCE CONJECTURE HOLDS FOR A LOG–DENSITY 1 CLASS OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS

SUGATA GANGOPADHYAY AND PANTELIMON STĂNICĂ

Abstract. We consider the Fourier Entropy-Influence (FEI) conjecture in the context of cryptographic Boolean functions. We show that the FEI conjecture is true for the functions satisfying the strict avalanche criterion, which forms a subset of asymptotic log–density 1 in the set of all Boolean functions. Further, we prove that the FEI conjecture is satisfied for plateaued Boolean functions, monomial algebraic normal form (with the best involved constant), direct sums, as well as concatenations of Boolean functions. As a simple consequence of these general results we find that each affine equivalence class of quadratic Boolean functions contains at least one function satisfying the FEI conjecture. Further, we propose some "leveled" FEI conjectures.

1. Introduction

Let $\mathbb{F}_2$ be the prime field of characteristic 2. Let $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2\}$ be the vector space of dimension n over $\mathbb{F}_2$. Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a *Boolean function* on n variables, whose set is denoted by $\mathfrak{B}_n$. The additions over $\mathbb{F}_2$ and $\mathbb{F}_2^n$ are both denoted by $\oplus$ whereas the addition over integers is denoted by $+$. For any positive integer n, the set $[n] := \{1, \ldots, n\}$. For any $\mathbf{x} \in \mathbb{F}_2^n$, the weight of $\mathbf{x}$ is $\mathrm{wt}(\mathbf{x}) = \sum_{i=1}^n x_i$. The algebraic normal form (ANF) of a Boolean function $f \in \mathfrak{B}_n$ is

$$f(x_1, \ldots, x_n) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} x_1^{a_1} \ldots x_n^{a_n}$$

where $\mu_{\mathbf{a}} \in \mathbb{F}_2^n$, for all $\mathbf{a} \in \mathbb{F}_2^n$. The algebraic degree of f is $\deg(f) = \max_{\mathbf{a}\in\mathbb{F}_2^n}\{\mathrm{wt}(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0\}$. The *Fourier transform* or the *Fourier coefficient* of $f \in \mathfrak{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is

$$\widehat{f}(\mathbf{u}) = 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}$$

where $\mathbf{u} \cdot \mathbf{x} = \bigoplus_{i=1}^n u_i x_i$ is the inner product of $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{x} = (x_1, \ldots, x_n)$. The multiset of Fourier coefficients $[\widehat{f}(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is said to be the *Fourier spectrum* of f. The *Walsh–Hadamard transform* of $f \in \mathfrak{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$

Date: January 25, 2014.

2010 *Mathematics Subject Classification.* Primary: 94C10, 94A17; Secondary: 05A10, 94A60.

This paper was written during an enjoyable visit of S. G. at the Applied Mathematics Department of Naval Postgraduate School in December, 2013. During the preparation of this paper, S. G. was supported in part by VSP award no. N62909-13-1-V105 (Department of the US Navy, ONR-Global).

is $W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n\widehat{f}(\mathbf{u})$. The multiset of Walsh–Hadamard coefficients $[W_f(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n]$ is said to be the *Walsh–Hadamard spectrum* of f. These transforms are invertible, that is, for all $\mathbf{x} \in \mathbb{F}_2^n$, $(-1)^{f(\mathbf{x})} = 2^{-n}\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}}$. The *crosscorrelation* of $f, g \in \mathfrak{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is

$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})}(-1)^{g(\mathbf{x}\oplus\mathbf{u})}. \tag{1}$$

If $f = g$, then $C_{f,f}(\mathbf{u})$ is said to be the *autocorrelation* of f at $\mathbf{u} \in \mathbb{F}_2^n$. The Walsh–Hadamard transform and autocorrelation of f are related by (referred to as Wiener-Khintchine Theorem [3, Theorem 2.8, p.8])

$$C_{f,f}(\mathbf{y}) = 2^{-n}\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f(\mathbf{u})^2(-1)^{\mathbf{u}\cdot\mathbf{y}}.$$

The correlation between the functions f and g is measured by $C_{f,g}(\mathbf{0})$. Thus the Fourier coefficients of f measure the correlations between f and the affine functions in $\mathfrak{B}_n$. A desirable property of Boolean functions employed as cryptographic primitives is lowest possible correlation to all the affine functions. The construction of such functions $f \in \mathfrak{B}_n$ is constrained by Parseval's identity

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{x})^2 = 1. \tag{2}$$

It is known that a Boolean function on n variables maximally resist affine approximations, if the squares of its Fourier coefficients are all equal to 2^{-n}. Such functions exist (if n is even) and are called *bent functions* [15].

For any $f \in \mathfrak{B}_n$, it is clear that $\widehat{f}(\mathbf{u})^2 \in [0, 1]$. This, along with the Parseval's identity (2) associates to f a probability distribution with the probability mass function $\mathbf{u} \mapsto \widehat{f}(\mathbf{u})^2$, for all $\mathbf{u} \in \mathbb{F}_2^n$. A high value of $\widehat{f}(\mathbf{u})^2$ means that $\mathbf{u}\cdot\mathbf{x}$ or its complement is a good approximation of f. The entropy of the probability distribution corresponding to a Boolean function f, referred to as the entropy of f, is

$$\mathbb{H}(f) = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2 \log_2 \frac{1}{\widehat{f}(\mathbf{u})^2}.$$

The maximum entropy is attained by functions with flat spectrum [16, Theorem 2.6], which are bent functions. If f is bent, then its Fourier coefficients are all $\pm 2^{-n/2}$ and so, that maximum entropy becomes

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} 2^{-n}\log_2 2^n = n.$$

Suppose $\mathbf{e}_i \in \mathbb{F}_2^n$ is the vector whose ith component is 1 and all the other components are 0. The influence of the ith variables x_i of $f \in \mathfrak{B}_n$ is defined as

$$\mathrm{Inf}_i(f) = \mathrm{Prob}[f(\mathbf{x}) \neq f(\mathbf{x} \oplus \mathbf{e}_i)]$$

where $\mathbf{x} \in \mathbb{F}_2^n$ is chosen at random, and the *total influence* is then

$$\mathrm{Inf}(f) = \sum_{i=1}^{n} \mathrm{Inf}_i(f). \tag{3}$$

Recall the Dirac symbol

$$\delta_1(x) = \begin{cases} 0, & \text{if } x \neq 1 \\ 1, & \text{if } x = 1. \end{cases}$$

The influence of the ith variable and the total influence on f is related to the Fourier coefficients of f as

$$\mathrm{Inf}_i(f) = \sum_{\mathbf{u} \in \mathbb{F}_2^n} \delta_1(\mathbf{u} \cdot \mathbf{e}_i) \widehat{f}(\mathbf{u})^2, \tag{4}$$

and

$$\mathrm{Inf}(f) = \sum_{i=1}^{n} \mathrm{Inf}_i(f) = \sum_{\mathbf{u} \in \mathbb{F}_2^n} \mathrm{wt}(\mathbf{u}) \widehat{f}(\mathbf{u})^2. \tag{5}$$

A very important conjecture involving the total influence and the entropy of a Boolean function is as follows.

Fourier Entropy–Influence (FEI) Conjecture (Friedgut and Kalai [5]): *There exists a universal constant C such that for any Boolean function f we have*

$$\mathbb{H}(f) \leq C \cdot \mathrm{Inf}(f).$$

The FEI conjecture implies a version of Mansour's conjecture (see [9, 13]), which states that given a Boolean function f whose conjunctive normal form has a number of terms which is polynomial in n, then most of the nonzero Fourier coefficients are also concentrated on polynomial number of input variables. The FEI conjecture (and variations) generated a lot of research in the past twenty years (see [8, 11, 12, 13] and the references therein). We only mention here that O'Donnell et al. [13] have verified the conjecture for symmetric functions and functions computable by read–once decision trees.

We generalize the notion of the influence concept in the following way. We define the *derivative* of f with respect to any vector $\mathbf{a}$ by $D_{\mathbf{a}} f(x) = f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})$. For a fixed k, and a vector $\mathbf{u}$ whose weight $\mathrm{wt}(\mathbf{u}) = k$, we define the (generalized) influence with respect to $\mathbf{u}$ as

$$\mathrm{Inf}_{\mathbf{u}}(f) = \mathrm{Prob}[f(\mathbf{x}) \neq f(\mathbf{x} \oplus \mathbf{u})],$$

We define the *ℓ-level influence*, respectively, *ℓ-total influence* by

$$\mathrm{Inf}_{[\ell]}(f) = \sum_{\mathbf{u}, \mathrm{wt}(\mathbf{u}) = \ell} \mathrm{Inf}_{\mathbf{u}}(f), \text{ respectively,}$$

$$\mathrm{Inf}^{[\ell]}(f) = \sum_{i=1}^{\ell} \mathrm{Inf}_{[i]}(f) = \sum_{i=1}^{\ell} \sum_{\mathbf{u}, \mathrm{wt}(\mathbf{u}) = i} \mathrm{Inf}_{\mathbf{u}}(f).$$

We propose the following *level* versions of the FEI conjecture.

ℓ-Level FEI Conjecture. *There exists a universal constant C such that for any Boolean function f we have*

$$\mathbb{H}(f) \leq C \cdot \mathrm{Inf}_{[\ell]}(f)$$

ℓ-Total FEI Conjecture. *There exists a universal constant C such that for any Boolean function f we have*

$$\mathbb{H}(f) \leq C \cdot \mathrm{Inf}^{[\ell]}(f)$$

It is obvious that if $\ell = 1$, we recover the original FEI conjecture, and that for any ℓ, the ℓ-Level FEI Conjecture implies the ℓ-Total FEI Conjecture. For a subset $S \subseteq \mathfrak{B}_n$ of Boolean functions, if $\lim_{n\to\infty} \frac{\log \# S}{2^n} = L$ exists, then we call this limit $L \leq 1$ to be the *log-density* of S. In this paper we prove the ℓ-level FEI conjecture for a class of Boolean functions of log-density 1, for any $\ell \geq 1$.

Throughout this paper, we use the Vinogradov symbols $\gg$, $\ll$ and the Landau symbols O, Ω, o, $\asymp$ with their usual meanings. We recall that $f \ll g$, $g \gg f$ and $f = O(g)$ are all equivalent and mean that $|f(x)| < c|g(x)|$ holds with some constant c, for x sufficiently large, while $A \asymp B$ (we sometimes use $A = \Theta(B)$, or $B = \Theta(A)$) means that both $A \ll B$ and $B \ll A$ hold. Also, $f = \Omega(g)$ is equivalent to $g = O(f)$, and $f = o(g)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

2. The FEI conjecture is true for functions satisfying SAC and PC(ℓ)

In this section we will show the Fourier Entropy–Influence Conjecture is true for a class of log-density 1. Throughout, we assume that $n \geq 4$.

The Strict Avalanche Criterion (SAC) was introduced by Webster and Tavares [17] in a study of design criteria for certain cryptographic functions. A Boolean function f satisfies the SAC if and only if by changing any input bit the output changes with probability 1/2. Equivalently, a function is SAC if and only if the derivative $D_{\mathbf{a}}f(x) = f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})$ (with respect to any vector $\mathbf{a}$ with $\mathrm{wt}(\mathbf{a}) = 1$) is balanced [3]. Further, we say that a function satisfies the SAC of order $0 \leq k \leq n-2$ (with notation SAC(k)) if and only if by fixing k variables, the resulting function is SAC. If for a function f, by fixing k variables the output changes with probability 1/2, we say that the function satisfies PC(k). It is known [3] that if a function satisfies the SAC(k), then it satisfies SAC(j), $1 \leq j \leq k$. Also, if f satisfies SAC(k), then its algebraic degree satisfies $2 \leq \deg(f) \leq n-k-1$.

Lemma 1. *We have*

$$\begin{aligned}
\mathrm{Inf}_{[\ell]}(f) &= \frac{1}{2}\binom{n}{i} - \frac{1}{2^{n+1}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{\mathbf{u},\mathrm{wt}(\mathbf{u})=\ell} (-1)^{D_{\mathbf{u}}f(\mathbf{x})} \\
\mathrm{Inf}^{[\ell]}(f) &= \frac{1}{2}\sum_{i=1}^{\ell}\binom{n}{i} - \frac{1}{2^{n+1}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{\mathbf{u},1\leq\mathrm{wt}(\mathbf{u})\leq\ell} (-1)^{D_{\mathbf{u}}f(\mathbf{x})}.
\end{aligned}$$

Proof. It is easy to show that (see also [3, p.9]])

$$\mathrm{Prob}[f(\mathbf{x}) \neq f(\mathbf{x} \oplus \mathbf{u})] = \frac{1}{2} - \frac{1}{2^{n+1}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_{\mathbf{u}}f(\mathbf{x})},$$

which, by summing, implies

$$\mathrm{Inf}_{[\ell]}(f) = \frac{1}{2}\binom{n}{\ell} - \frac{1}{2^{n+1}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{\mathbf{u},\mathrm{wt}(\mathbf{u})=\ell} (-1)^{D_{\mathbf{u}}f(\mathbf{x})},$$

and the lemma is shown. □

Theorem 2. *The FEI conjecture is true for a Boolean functions class of log-density* 1 *(that is, the class of SAC functions).*

Proof. Using Lemma 1, we restate the FEI conjecture as

$$\mathbb{H}(f) = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2 \log_2 \frac{1}{\widehat{f}(\mathbf{u})^2} \leq C\left(\frac{n}{2} - \frac{1}{2^{n+1}} \sum_{\mathbf{a},\mathrm{wt}(\mathbf{a})=1} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_\mathbf{a} f(\mathbf{x})}\right), \tag{6}$$

for some universal constant C. Thus, since the entropy is upper bounded by n, to show the FEI conjecture for a class of functions it is sufficient to show that the right hand side of the expression (6) is lower bounded by n (for some constant C). Thus, if we assume that f is SAC, therefore $D_\mathbf{a} f(\mathbf{x})$ is balanced, we get $\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{D_\mathbf{a} f(\mathbf{x})} = 0$. Then the right hand side of (6) becomes $\frac{C}{2}n$, and so, the FEI conjecture is shown, with $C = 2$, for the set of SAC Boolean functions.

Further, it was shown in [1] that the number of SAC functions L_n satisfies

$$L_n \geq \binom{2^{n-1}}{2^{n-2}}^n 2^{2^n - n2^{n-1}} \asymp \frac{1}{\pi^{n/2}} 2^{2^n - \frac{n^2}{2} + n},$$

where the last approximation uses Stirling's formula. Thus, the number of SAC functions in n variables satisfies $\lim_{n\to\infty} \dfrac{\log_2 L_n}{2^n} = 1$, so, the set of SAC functions has log-density 1.

□

Remark 3. *Certainly, if f satisfies PC(ℓ), the ℓ-level and ℓ-total FEI conjectures are also true.*

Remark 4. *We observe that the FEI conjecture is fully proven for any f if one can show (denoting $d_\mathbf{a}(f) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_\mathbf{a} f(\mathbf{x})}$) that $\sum_{\mathbf{a},\mathrm{wt}(\mathbf{a})=1} d_\mathbf{a}(f) = \Omega(n2^n)$, with the involved constant strictly smaller than $1/2$.*

3. The FEI conjecture is true for plateaued Functions

In this section we will show the Fourier Entropy–Influence Conjecture for the class of plateaued functions, a class of functions introduced by Zheng and Zhang [18], which generalizes bent and semibent functions. A Boolean function f is called *plateaued* if the set of Fourier coefficients $Spec(f) = \{0, \pm\lambda\}$, for some $\lambda \neq 0$ (called the amplitude of f). Using Parseval's identity, it is easy to see that λ must be of the form $2^{(k-n)/2}$, where $0 \leq k \leq n$ is such that $n \equiv k \pmod 2$ (we shall refer to k as the level of f).

Theorem 5. *The Fourier Entropy–Influence Conjecture is true for the class of plateaued Boolean functions.*

Proof. If f is affine, then the FEI conjecture is obviously satisfied. If f is bent, then its Fourier coefficients are all $2^{-n/2}$ and so, the FEI conjecture becomes

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} 2^{-n} \log_2 2^n = n \leq C \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathrm{wt}(\mathbf{u}) 2^{-n} = C 2^{-n} \sum_{i=0}^{n} i\binom{n}{i} = \frac{C}{2}n,$$

and so, we can take $C = 2$, for the class of bent functions.

Next, we assume that f is a plateaued function that is neither affine, nor bent, of $Spec(f) = \{0, \pm 2^{(k-n)/2}\}$, $1 \leq k < n$. It is known that the number of nonzero

vectors $\mathbf{u}$ for which $\hat{f}(\mathbf{u}) \neq 0$ is exactly 2^{n-k}. The FEI for the plateaued functions is written as

$$\begin{aligned} & \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \widehat{f}(\mathbf{u})^2 \log_2 \frac{1}{\widehat{f}(\mathbf{u})^2} \leq C \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathrm{wt}(\mathbf{u})\widehat{f}(\mathbf{u})^2 \\ \iff \quad & \sum_{\mathbf{u},\widehat{f}(\mathbf{u})\neq 0} 2^{k-n} \log_2 2^{n-k} \leq C \sum_{\mathbf{u},\widehat{f}(\mathbf{u})\neq 0} \mathrm{wt}(\mathbf{u}) 2^{k-n} \\ \iff \quad & n-k \leq C\, 2^{k-n} \sum_{\mathbf{u},\widehat{f}(\mathbf{u})\neq 0} \mathrm{wt}(\mathbf{u}) \end{aligned} \tag{7}$$

for some universal constant C.

In the worst case, we assume that all nonzero Fourier coefficients are clustered in the smallest weight input vectors. We take $T_{n,k}$ the smallest integer such that $\sum_{i=0}^{T_{n,k}} \binom{n}{i} \geq 2^{n-k}$. Certainly, since $k \geq 1$, then $T_{n,k} \leq n/2$. Using the identity $i\binom{n}{i} = n\binom{n-1}{i-1}$, the right hand side of the inequality (7) becomes

$$\mathrm{Inf}(f) \quad \geq \quad 2^{k-n} \sum_{i=1}^{T_{n,k}} i\binom{n}{i} = 2^{k-n} n \sum_{j=0}^{T_{n,k}-1} \binom{n-1}{j}.$$

We need to show that there exists a universal constant $C > 0$ such that

$$\sum_{i=0}^{T_{n,k}-1} \binom{n-1}{i} \geq C 2^{n-k}. \tag{8}$$

As a simple observation, if $n-k = O(1)$, then the left hand side of the above inequality (8) is certainly increasing and unbounded with n, so it will overcome $2^{n-k} = 2^{O(1)}$, for $n \geq n_0$. One can choose $C = 1$, and the FEI conjecture holds, for $n \geq n_0$.

Using $\binom{n}{i} < 2\binom{n-1}{i}$ and the definitions of $T_{n-1,k}$ and $T_{n,k}$, we obtain

$$\begin{aligned} & 2^{n-k} \leq \sum_{i=0}^{T_{n,k}} \binom{n}{i} < 2 \sum_{i=0}^{T_{n,k}} \binom{n-1}{i}, \\ & 2^{n-k} < 2^{n-k} + \binom{n-1}{T_{n-1,k}+1} \leq 2 \sum_{i=0}^{T_{n-1,k}} \binom{n-1}{i} + \binom{n-1}{T_{n-1,k}+1} = \sum_{i=0}^{T_{n-1,k}+1} \binom{n}{i}, \end{aligned}$$

which shows that $T_{n-1,k} \leq T_{n,k} \leq T_{n-1,k} + 1$.

If $T_{n,k} = T_{n-1,k} + 1$, then the inequality (8) is obviously satisfied with $C = 1/2$. Assume next that $T_{n,k} = T_{n-1,k} := T \leq n/2$. Using the known estimate [6]

$$\sum_{i=0}^{N} \binom{m}{i} = \begin{cases} \Theta(2^m) & \text{if } N \geq m/2 - \sqrt{m} \\ \Theta\left((1-\frac{2N}{m})^{-1}\binom{m}{N}\right) & \text{if } N < m/2 - \sqrt{m}, \end{cases} \tag{9}$$

and taking all k such that $T \geq \frac{n+1}{2} - \sqrt{n-1}$, we obtain that

$$\sum_{i=0}^{T-1} \binom{n-1}{i} = \Theta(2^{n-1}) \geq C_1 \cdot 2^{n-k},$$

for some constant C_1. Now, take all k such that $T < \frac{n+1}{2} - \sqrt{n-1}$, then by (9), we get

$$\sum_{i=0}^{T-1} \binom{n-1}{i} = \Theta\left(\left(1 - \frac{2(T-1)}{n-1}\right)^{-1} \binom{n-1}{T-1}\right),$$

Let $S := \sum_{i=0}^{T-1} \binom{n-1}{i}$. We obtain that

$$\binom{n-1}{T} = \frac{n-T}{T}\binom{n-1}{T-1} = \Theta\left(\frac{n-T}{T}\left(1 - \frac{2(T-1)}{n-1}\right) S\right),$$

which means that the term $\binom{n-1}{T}$ is smaller than a constant multiple of S. Using

$$\sum_{i=0}^{T} \binom{n-1}{i} = \sum_{i=0}^{T-1} \binom{n-1}{i} + \binom{n-1}{T} \geq 2^{n-k-1},$$

we obtain that equation (8) holds, for some constant C_2. Thus the FEI conjecture holds with $C := \min\{C_1, C_2\}$. □

4. The FEI conjecture for some more classes of functions

O'Donnell, Wright and Zhou, [13] have proved the FEI conjecture for symmetric Boolean functions and read-once decision trees. O'Donnell and Tan [14] proved that if $g_1, \ldots, g_k$ are functions over disjoint sets of variables, denoted by $x^1, \ldots, x^k$, and $F \in \mathfrak{B}_k$, all satisfying the FEI conjecture, then their composition $F(g_1(x^1), \ldots, g_k(x^k))$ satisfies the FEI conjecture. In fact O'Donnell and Tan [14] have proved the FEI conjecture for more general μ-biased Fourier coefficients.

Definition 6 (Definition 5, [14])**.** *Let $\mathcal{B}$ be a set of Boolean functions. We say that a Boolean function f is a formula over the basis $\mathcal{B}$ if f is computable with gates belonging to $\mathcal{B}$. We say that f is a read-once formula over $\mathcal{B}$ if every variable appears at most once in the formula for f.*

As an application of their result, O'Donnell and Tan [14] show that the FEI conjecture holds for read-once formulas over arbitrary gates of bounded parity which extends the result in [13].

The fact that Boolean functions having monomial ANF satisfy the FEI conjecture is known [13, 14]. In this section we revisit this problem and prove that the universal constant C is 4 for monomial Boolean functions.

Finally we prove that if f and g are two Boolean functions having disjoint Fourier spectra and satisfy the FEI conjecture then their concatenation also satisfies the FEI conjecture.

4.1. The FEI conjecture for monomial functions.

In this section we consider the case when the algebraic normal form (ANF) of $f \in \mathfrak{B}_n$ is a monomial (i.e., contains only one term). Without loss of generality, we assume $f(\mathbf{x}) = x_1 \ldots x_k$, where $k < n$. Let $\mathbb{V}$ be the span of the elementary basis vectors $\mathbf{e}_{k+1}, \ldots, \mathbf{e}_n$, that is, $\mathbb{V} = \langle \mathbf{e}_{k+1}, \ldots, \mathbf{e}_n \rangle$ and $\mathbf{u}_k = \mathbf{e}_1 \oplus \ldots \oplus \mathbf{e}_k$. The indicator function of any $S \subseteq \mathbb{F}_2^n$ is $\mathbf{1}_S(\mathbf{x})$, which is 0, if $\mathbf{x} \notin S$, and 1, if $\mathbf{x} \in S$. Then f becomes

$$f(\mathbf{x}) = x_1 \ldots x_k = \mathbf{1}_{(\mathbf{u}_k \oplus \mathbb{V})}(\mathbf{x}).$$

Theorem 7. *The FEI conjecture is true for monomial Boolean functions with $C = 4$, which is the best possible.*

Proof. It will be sufficient to show the conjecture for $f(\mathbf{x}) = \mathbf{1}_{\mathbf{u}_k \oplus \mathbb{V}}(\mathbf{x})$. The Walsh-Hadamard transform of f is

$$\begin{aligned} W_f(\mathbf{u}) &= \sum_{\mathbf{x}\in \mathbf{u}_k\oplus\mathbb{V}} (-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\notin \mathbf{u}_k+\mathbb{V}} (-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} = (-2)\sum_{\mathbf{x}\in \mathbf{u}_k\oplus\mathbb{V}} (-1)^{\mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= 2(-1)^{1\oplus \mathbf{u}\cdot\mathbf{u}_k}\sum_{\mathbf{x}\in\mathbb{V}} (-1)^{\mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2(-1)^{1\oplus \mathbf{u}\cdot\mathbf{u}_k}\sum_{\mathbf{x}\in\mathbb{V}} (-1)^{\mathbf{u}\cdot\mathbf{x}} + 2^n\delta_{\mathbf{0}}(\mathbf{u}) \\ &= 2^{n-k+1}(-1)^{1\oplus \mathbf{u}\cdot\mathbf{u}_k}\mathbf{1}_{\mathbb{V}^\perp}(\mathbf{u}) + 2^n\delta_{\mathbf{0}}(\mathbf{u}) = \begin{cases} 2^n - 2^{n-k+1} \text{ if } \mathbf{u} = \mathbf{0}, \\ (-1)^{1\oplus \mathbf{u}\cdot\mathbf{u}_k} 2^{n-k+1} \text{ if } \mathbf{0}\neq \mathbf{u}\in\mathbb{V}^\perp, \\ 0 \text{ otherwise.} \end{cases} \end{aligned}$$

Therefore

$$\widehat{f}(\mathbf{u}) = \begin{cases} 1 - 2^{1-k} \text{ if } \mathbf{u} = \mathbf{0}, \\ (-1)^{1\oplus \mathbf{u}\cdot\mathbf{u}_k} 2^{1-k} \text{ if } \mathbf{u}\neq \mathbf{0}, \mathbf{u}\in\mathbb{V}^\perp, \\ 0 \text{ otherwise,} \end{cases}$$

that is,

$$\widehat{f}(\mathbf{u})^2 = \begin{cases} (1 - 2^{1-k})^2 \text{ if } \mathbf{u} = \mathbf{0}, \\ 2^{2(1-k)} \text{ if } \mathbf{u}\neq \mathbf{0}, \mathbf{u}\in\mathbb{V}^\perp, \\ 0 \text{ otherwise.} \end{cases}$$

Thus, $f(\mathbf{u})^2$ is $(1-2^{1-k})^2$ at 1 element in $\mathbb{F}_2^n$ and $2^{2(1-k)}$ at 2^k-1 elements of $\mathbb{F}_2^n$, that is, at all the nonzero elements of $\mathbb{V}^\perp$. The entropy of f is

$$\begin{aligned} \mathbb{H}(f) &= (2^k-1)2^{2(1-k)}2(1-k) + (1-2^{1-k})^2\log_2\frac{1}{(1-2^{1-k})^2} \\ &= (2^k-1)2^{3-2k}(1-k) + 2(1-2^{1-k})^2\log_2\frac{2^{k-1}}{2^{k-1}-1} \\ &= (2^k-1)2^{3-2k}(1-k) + 2(1-2^{1-k})^2(k-1) - 2(1-2^{1-k})^2\log_2(2^{k-1}-1). \end{aligned}$$

Using Lemma 1 for $\ell = 1$ we have $\mathrm{Inf}_i(f) = \frac{1}{2} - \frac{1}{2^{n+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{e}_i)}$. If $i\in[k]$, then $f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{e}_i) = x_1\ldots x_k \oplus x_1\ldots x_k \oplus x_1\ldots x_{i-1}x_{i+1}\ldots x_k = x_1\ldots x_{i-1}x_{i+1}\ldots x_k$, that is,

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{e}_i)} = (2^n - 2^{n-k+1}) - 2^{n-k+1} = 2^n - 2^{n-k+2}.$$

If $i\in[n]\setminus[k]$, then $f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{e}_i) = x_1\ldots x_k \oplus x_1\ldots x_k = 0$, that is,

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{e}_i)} = 2^n.$$

The influence of x_i on f is

$$\mathrm{Inf}_i(f) = \begin{cases} \frac{1}{2} - \frac{1}{2^{n+1}}(2^n - 2^{n-k+2}) \text{ if } i\in[k] \\ 0 \text{ if } i\in[n]\setminus[k]. \end{cases}$$

The total influence becomes

$$\begin{aligned} \mathrm{Inf}(f) &= \sum_{i=1}^n \mathrm{Inf}_i(f) = \sum_{i=1}^k\left(\frac{1}{2} - \frac{1}{2^{n+1}}(2^n - 2^{n-k+2})\right) \\ &= \frac{k}{2} - \frac{1}{2^{n+1}}(k2^n - k2^{n-k+2}) = k2^{1-k}. \end{aligned}$$

Thus we have

$$\frac{\mathbb{H}(f)}{\mathrm{Inf}(f)} = \left(1-\frac{1}{k}\right)(2^k-1)2^{2-k} + 2^k\left(1-\frac{1}{2^{k-1}}\right)^2\left(\left(1-\frac{1}{k}\right) - \frac{\log_2(2^{k-1}-1)}{k}\right). \tag{10}$$

Using the transformation $k = 1+\log_2(s+1)$ in the expression $\frac{\mathbb{H}(f)}{\mathrm{Inf}(f)}$, we see that

$$\frac{\mathbb{H}(f)}{\mathrm{Inf}(f)} = \frac{2\left((s+1)^2\ln(s+1) - s^2\ln s\right)}{(s+1)\ln(2(s+1))}, \tag{11}$$

(A more delicate Calculus analysis shows that this expression is in fact increasing, but we will not need that.) We show that

$$\begin{aligned}
&\frac{\mathbb{H}(f)}{\mathrm{Inf}(f)} = \frac{2\left((s+1)^2\ln(s+1) - s^2\ln s\right)}{(s+1)\ln(2(s+1))} \le 4\\
\iff\ & (s+1)^2\ln(s+1) - s^2\ln s \le 2(s+2)\ln(2(s+1))\\
\iff\ & s\ln\left(1+\frac{1}{s}\right)^s + (2s+1)\ln(s+1) \le 2(s+2)\ln(2(s+1))\\
\iff\ & s\ln\left(1+\frac{1}{s}\right)^s - \ln(s+1) \le 2(s+2)\ln 2\\
\iff\ & s\left(\ln\left(1+\frac{1}{s}\right)^s - 2\ln 2\right) \le \ln(s+1) + 4\ln 2,
\end{aligned}$$

which is certainly true, since $\ln\left(1+\frac{1}{s}\right)^s - 2\ln 2 < 0$ using the fact that the sequence $\left\{\left(1+\frac{1}{s}\right)^s\right\}_s$ is increasing with the limit $\lim_{s\to\infty}\left(1+\frac{1}{s}\right)^s = e$ (Euler's constant). (Certainly, when $k\to\infty$, then $s = 2^{k-1}-1\to\infty$.)

Certainly, since the quotient $\frac{\mathbb{H}(f)}{\mathrm{Inf}(f)}$ depends upon k only, to show that $C=4$ is the best possible, it will be sufficient to investigate what happens when $k\to\infty$. The limit of the first term in (10) is 4, as $k\to\infty$. We will show that the limit of the second term is 0, as $k\to\infty$. (We could have used L'Hôpital's rule in (11), together with some elementary considerations, but we preferred a more direct approach below.) With $k = 1+\log_2(s+1)$, the limit of the second term in (10) (disregarding $2\left(1-\frac{1}{2^{k-1}}\right)^2\to 2$, as $k\to\infty$) becomes

$$\begin{aligned}
&\lim_{s\to\infty}\frac{(s+1)\left(\log_2(s+1)-\log_2 s\right)}{1+\log_2(s+1)} = \lim_{s\to\infty}\frac{(s+1)\log_2(1+1/s)}{1+\log_2(s+1)}\\
=\ &\lim_{s\to\infty}\frac{\log_2(1+1/s)^{s+1}}{1+\log_2(s+1)} = \lim_{s\to\infty}\frac{\log_2(1+1/s)^s + \log_2(1+1/s)}{1+\log_2(s+1)} = 0,
\end{aligned}$$

since the numerator of the last fraction approaches $\log_2 e$, and the denominator approaches infinity, as $s\to\infty$. Therefore, $\lim_{k\to\infty}\frac{\mathbb{H}(f)}{\mathrm{Inf}(f)} = 4$. This proves the FEI conjecture for monomials with (the best possible constant) $C=4$. □

The fact that the direct sum of two Boolean functions satisfying the FEI conjecture also satisfies the FEI conjecture is a consequence of the results proved by O'Donnell and Tan [14], although, using our method, the proof takes just a couple of paragraphs. Given any positive integer n, the representatives of the affine

non-equivalent quadratic Boolean functions in n variables [10, p. 438] can be chosen

$$\sum_{i=1}^{h} x_{2i-1}x_{2i} + \ell(x_1, x_2, \ldots, x_n),\ h \leq \left\lfloor \frac{n}{2} \right\rfloor,$$

where ℓ is an affine function (we can disregard it – we simply inserted it to show dependence on n). Since all of these terms (disregarding the affine terms) are direct sums of monomials it is clear that for any positive integer n each affine non-equivalent class of quadratic Boolean functions contains a function which satisfies the FEI conjecture.

4.2. **FEI conjecture for concatenations of Boolean functions.** Finally we obtain a sufficient condition under which the concatenations of two Boolean functions satisfying the FEI conjecture also satisfies the FEI conjecture.

Theorem 8. *Suppose $f, g \in \mathfrak{B}_n$ have disjoint Fourier spectra which satisfy the FEI conjecture. Then $h \in \mathfrak{B}_{n+1}$ defined by*

$$h(\mathbf{u}, v) = f(\mathbf{u}) \oplus v(f(\mathbf{u}) \oplus g(\mathbf{u})),\ \textit{for all } \mathbf{u} \in \mathbb{F}_2^n, v \in \mathbb{F}_2,$$

satisfies the FEI conjecture.

Proof. Since f and g satisfy the FEI conjecture there is a constant C such that $\mathbb{H}(f) \leq C \cdot \mathrm{Inf}(f)$ and $\mathbb{H}(g) \leq C \cdot \mathrm{Inf}(g)$ (we assume that $C \geq 2$). It is known [3, Chapter 4, p.66] that the Fourier transform of h at $(\mathbf{u}, v) \in \mathbb{F}_2^n \times \mathbb{F}_2$ is

$$\widehat{h}(\mathbf{u}, v) = \frac{1}{2}\widehat{f}(\mathbf{u}) + (-1)^v \frac{1}{2}\widehat{g}(\mathbf{u}).$$

Taking squares of both sides we have

$$\begin{aligned}\widehat{h}(\mathbf{u}, v)^2 &= \frac{1}{4}(\widehat{f}(\mathbf{u}) + (-1)^v\widehat{g}(\mathbf{u}))^2 = \frac{1}{4}(\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2 + 2(-1)^v\widehat{f}(\mathbf{u})\widehat{g}(\mathbf{u})) \\ &= \frac{1}{4}(\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2) \quad \text{(since, } f \text{ and } g \text{ have disjoint Fourier spectra).}\end{aligned}$$

The entropy becomes

$$\begin{aligned}\mathbb{H}(h) &= -\sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2} \widehat{h}(\mathbf{u}, v)^2 \log_2(\widehat{h}(\mathbf{u}, v)^2) \\ &= -\frac{1}{4}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2} (\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2) \log_2\left(\frac{\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2}{4}\right) \\ &= -\frac{1}{2}\sum_{\mathbf{u}\in\mathbb{F}_2^n} (\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2) \log_2\left(\frac{\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2}{4}\right) \\ &\leq -\frac{1}{2}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\widehat{f}(\mathbf{u})^2 \log_2\frac{\widehat{f}(\mathbf{u})^2}{2} + \widehat{g}(\mathbf{u})^2 \log_2\frac{\widehat{g}(\mathbf{u})^2}{2}\right) \quad \text{(using log-sum inequality)} \\ &= -\frac{1}{2}\left(\sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2(\log_2(\widehat{f}(\mathbf{u})^2) - 1) + \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{g}(\mathbf{u})^2(\log_2(\widehat{g}(\mathbf{u})^2) - 1)\right) \\ &= -\frac{1}{2}\left(\sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2 \log_2(\widehat{f}(\mathbf{u})^2) + \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{g}(\mathbf{u})^2 \log_2(\widehat{g}(\mathbf{u})^2) - 2\right)\end{aligned}$$

$$= \frac{1}{2}(\mathbb{H}(f) + \mathbb{H}(g)) + 1 \leq \frac{1}{2}C \cdot (\mathrm{Inf}(f) + \mathrm{Inf}(g)) + 1$$

The total influence is then

$$\begin{aligned}
\mathrm{Inf}(h) &= \sum_{\mathbf{u}\in\mathbb{F}_2^n} \sum_{v\in\mathbb{F}_2} \widehat{h}(\mathbf{u}, v)^2 \mathrm{wt}(\mathbf{u}, v) \\
&= \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{h}(\mathbf{u}, 0)^2 \mathrm{wt}(\mathbf{u}) + \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{h}(\mathbf{u}, 1)^2 \mathrm{wt}(\mathbf{u}, v) \\
&= \frac{1}{4} \sum_{\mathbf{u}\in\mathbb{F}_2^n} (\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2) \mathrm{wt}(\mathbf{u}) + \frac{1}{4} \sum_{\mathbf{u}\in\mathbb{F}_2^n} (\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2) \mathrm{wt}(\mathbf{u}) \\
&\qquad + \frac{1}{4} \sum_{\mathbf{u}\in\mathbb{F}_2^n} (\widehat{f}(\mathbf{u})^2 + \widehat{g}(\mathbf{u})^2) = \frac{1}{2}(\mathrm{Inf}(f) + \mathrm{Inf}(g) + 1).
\end{aligned}$$

Therefore (since $C \geq 2$),

$$\mathbb{H}(f) \leq \frac{C}{2} \cdot (\mathrm{Inf}(f) + \mathrm{Inf}(g) + 1) + 1 - \frac{C}{2} = C \cdot \mathrm{Inf}(f) - (\frac{C}{2} - 1) \leq C \cdot \mathrm{Inf}(f),$$

and the claim is shown. □

References

[1] D. K. Biss, *A lower bound on the number of functions satisfying the strict avalanche criterion*, Discrete Math. 185 (1998), no. 1–3, 29–39.

[2] S. Chakraborty, R. Kulkarni, S. V. Lokam and N. Saurabh, *Upper bounds on Fourier entropy*, Elec. Colloq. Comput. Compl., Rev. 1 of Report No. 52 (2013).

[3] T. W. Cusick and P. Stănică, Cryptographic Boolean functions and applications, Elsevier–Academic Press, 2009.

[4] B. Das, M. Pal and V. Visavaliya, *The entropy influence conjecture revisited*, arXiv:1110.4301v2 [math.CO], 20 Oct 2011.

[5] E. Friedgut and Gil Kalai, *Every monotone graph property has a sharp threshold*, Proc. AMS 124(10) (1996), 2293–3002.

[6] E. Jeřábek, *Dual weak pigeonhole principle, Boolean complexity, and derandomization*, Annals of Pure and Applied Logic 129, Issues 1–3 (2004), 1–37.

[7] J. Kahn, G. Kalai and N. Linial, *The influence of variables on Boolean functions*, in: Proceedings of the 29th IEEE Symp. Found. Comp. Sci., 1988, 68–80.

[8] N. Keller, E. Mossel and T. Schlank, *A note on the entropy/influence conjecture*, Discrete Math. 312 (2012), no. 22, 3364–3372.

[9] Y. Mansour, *Learning Boolean functions via the Fourier Transform*, Theoretical Advances in Neural Computation and Learning (V. Roychowdhury, K.-Y. Siu, A. Orlitsky, eds.), chapter 11, pp. 391–424, Kluwer Academic Publishers, 1994.

[10] F. J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[11] R. O'Donnell, The lecture notes of the course "analysis of Boolean function", Lecture 29: Open problems, 2007.

[12] R. O'Donnell, *Some topics in analysis of Boolean functions*, in: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, 2008, 569–578.

[13] R. O'Donnell, J. Wright and Y. Zhou, *The Fourier entropy–influence conjecture for certain classes of Boolean functions*, in: Proceedings of Automata, Languages and Programming – 38th International Colloquium, 2011, 330–341.

[14] R. O'Donnell and L-Y. Tan, *A composition theorem for the Fourier entropy-influence conjecture*, ICALP (1) 2013, 780–791. (Available at: arXiv:1304.1347v1 [cs.CC] 4 Apr 2013).

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

[16] D. R. Stinson, Cryptography. Theory and practice. Third edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[17] A. F. Webster and S. E. Tavares, *On the design of S-boxes*, Advances in Cryptology-Crypto '85, LNCS 218 (Springer, Berlin, 1986), 523–534.
[18] Y. Zheng and X. M. Zhang, *Plateaued functions*, in Advances in Cryptology–ICICS 1999, LNCS 1726, Springer-Verlag, 1999, pp. 284–300.

Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, INDIA
E-mail address: gsugata@gmail.com

Applied Mathematics Department, Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA
E-mail address: pstanica@nps.edu