Fourier Entropy-Influence Conjecture for Cryptographic Boolean Functions

Gangopadhyay, Sugata and Stănică, Pantelimon

Abstract—*Using methods from the area of cryptographic Boolean functions we provide a sharper estimate of the constant term involved in the Fourier Entropy-Influence inequality involving quadratic Boolean functions. We also consider the conjecture for plateaued Boolean functions.*

Index Terms—*Boolean functions, Fourier Entropy-Influence conjecture, Fourier spectrum.*

1. Introduction

Let $\mathbb{F}_2, \mathbb{Z}, \mathbb{Z}^+$ be the two-element field, the set of integers and the set of positive integers, respectively. For any $n \in \mathbb{Z}^+$, we use the notation $[n] := \{1, \ldots, n\}$. Let $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for all } i \in [n]\}$ be the vector space of dimension n over $\mathbb{F}_2$. The additive identity $\mathbf{0} \in \mathbb{F}_2^n$ is the vector with each component equal to $0 \in \mathbb{F}_2$. Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a *Boolean function* in 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 $\mathbb{Z}$ is denoted by "$+$". The (Hamming) weight of $\mathbf{x} \in \mathbb{F}_2^n$ is $\mathrm{wt}(\mathbf{x}) = \sum_{i \in [n]} x_i$. The algebraic normal form (ANF), or $\mathbb{F}_2$-representation 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 $\mu_{\mathbf{a}} \in \mathbb{F}_2$, 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 $\mathbf{u} \cdot \mathbf{x} = \bigoplus_{i \in [n]} u_i x_i$ 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 and $[|\widehat{f}(\mathbf{u})| : \mathbf{u} \in \mathbb{F}_2^n]$ is referred as the *absolute Fourier spectrum* of f. The *Walsh–Hadamard transform* of $f \in \mathfrak{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is $W_f(\mathbf{u}) = 2^n \widehat{f}(\mathbf{u})$. 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. Whenever convenient, we will consider the spectrum $\mathrm{Spec}(f)$ as the set of distinct Walsh–Hadamard coefficients. The mentioned transforms are invertible, that is, for all $\mathbf{x} \in \mathbb{F}_2^n$,

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

Since for any $f \in \mathfrak{B}_n$ $\widehat{f}(\mathbf{u})^2 \in [0, 1]$ and $\sum_{\mathbf{u} \in \mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2 = 1$ (Parseval's identity), the function $\mathbf{u} \mapsto \widehat{f}(\mathbf{u})^2$, for all $\mathbf{u} \in \mathbb{F}_2^n$ can be thought of as a probability mass function. 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

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

It is known that the maximum possible entropy that a function in $\mathfrak{B}_n$ can have is n (cf. [16, Theorem 2.6]). This happens when all the Fourier coefficients of the function have the same absolute value equal to $2^{-n/2}$, i.e., the function has a flat absolute Fourier spectrum. Such functions, called *bent functions*, were first constructed by Rothaus [15] for even n, whereas the the problem is open for n odd. We refer to [4] for details on bent and Boolean functions in general.

Let $\mathbf{e}_i \in \mathbb{F}_2^n$ be the vector whose ith component is 1 and all the other components are 0. The influence of the ith variable 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 equiprobably, and the *total influence* is then

$$\mathsf{Inf}(f) = \sum_{i\in[n]} \mathsf{Inf}_i(f).$$

The influence of the ith variable and the total influence on f is related to the Fourier coefficients of f (cf. [14]) as

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

and

$$\mathsf{Inf}(f) = \sum_{i\in[n]} \mathsf{Inf}_i(f) = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathsf{wt}(\mathbf{u})\widehat{f}(\mathbf{u})^2.$$

The *derivative* of $f \in \mathfrak{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$ is

$$D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{a}) \oplus f(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

An expression of the total influence of f involving the derivatives of f with respect to the weight 1 vectors in $\mathbb{F}_2^n$ is

$$\mathsf{Inf}(f) = \frac{n}{2} - \frac{1}{2^{n+1}} \sum_{i\in[n]} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_{\mathbf{e}_i}f(\mathbf{x})}. \quad (1)$$

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

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

$$\mathbb{H}(f) \le C \cdot \mathsf{Inf}(f).$$

The FEI conjecture is known to imply the well–known Kahn-Kalai-Linial theorem (in fact, it implies even a strengthening of it due to Talagrand [17]).

Theorem 1 (KKL '88)**.** *For every Boolean function f there exists $1 \le i \le n$ such that*

$$\mathsf{Inf}_i(f) = \mathsf{Var}[f] \cdot \Omega\left(\frac{\log n}{n}\right)$$

where $\mathsf{Var}[f] = \sum_{\mathbf{0}\neq\mathbf{a}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{a})^2$ *is the variance of f.*

The FEI conjecture also implies a version of Mansour's conjecture (see [10], [14]), which states that given a Boolean function f whose disjunctive normal form (DNF) has t terms, then most of the nonzero Fourier coefficients are also concentrated on polynomial poly(t) number of coefficients. We state below Mansour's conjecture (without being precise on the dependence upon ϵ).

Conjecture 2 (Mansour '94)**.** *Let f be a Boolean function computed by a t-term DNF formula. For any constant $\epsilon > 0$, there exists a collection of vectors $\mathcal{V} \subseteq \mathbb{F}_2^n$ of cardinality* poly(t) *such that $\sum_{\mathbf{a}\in\mathcal{V}} \widehat{f}(\mathbf{a})^2 \ge 1-\epsilon$.*

The FEI conjecture (and variations) generated a lot of research in the past twenty years (see [7], [8], [9], [12], [13], [14], [21] and the references therein). We mention here that O'Donnell et al. [14] have verified the conjecture for symmetric functions and functions computable by read–once decision trees. The results from [9] make significant progress showing that the conjecture is true for randomly chosen DNF formulas and read-k DNF formulas for constant k, among other classes.

In this paper, we provide a sharper estimate of the constant term involved in the FEI inequality involving monomial Boolean functions. We also consider the conjecture for plateaued Boolean functions.

Suppose $g, h : \mathbb{Z}^+ \to \mathbb{R}^+$, the set of positive real numbers. We write $h = \Omega(g)$ (equivalently, $g = O(h)$) if there exist $n_0, c \in \mathbb{Z}^+$ such that $cg(n) \le h(n)$, for all $n \ge n_0$. If both $h = \Omega(g)$ and $h = O(g)$ hold, then we say that $h = \Theta(g)$.

2. The FEI conjecture for monomial Boolean functions

In this section we provide our sharp estimate for the constant involved in FEI 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 3. *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

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

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

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

For $\ell = 1$ we have $\mathsf{Inf}_i(f) = \frac{1}{2} - \frac{1}{2^{n+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{e}_i)}$. If $i \in [k]$, then $f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{e}_i) = x_1\dots x_k \oplus x_1\dots x_k \oplus x_1\dots x_{i-1}x_{i+1}\dots x_k = x_1\dots x_{i-1}x_{i+1}\dots x_k$, 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 $f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\mathbf{e}_i) = x_1\dots x_k \oplus x_1\dots x_k = 0$, 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

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

The total influence becomes

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

Thus we have

$$\begin{aligned}
\frac{\mathbb{H}(f)}{\mathsf{Inf}(f)} &= \left(1-\frac{1}{k}\right)(2^k-1)2^{2-k} \\
&\quad + 2^k\left(1-\frac{1}{2^{k-1}}\right)^2\left(\left(1-\frac{1}{k}\right) - \frac{\log_2(2^{k-1}-1)}{k}\right).
\end{aligned} \tag{2}$$

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

$$\frac{\mathbb{H}(f)}{\mathsf{Inf}(f)} = \frac{2\left((s+1)^2\ln(s+1) - s^2\ln s\right)}{(s+1)\ln(2(s+1))}, \tag{3}$$

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

$$\begin{aligned}
&\frac{2\left((s+1)^2\ln(s+1) - s^2\ln s\right)}{(s+1)\ln(2(s+1))} \le 4 \\
\iff &(s+1)^2\ln(s+1) - s^2\ln s \\
&\quad \le 2(s+1)\ln(2(s+1)) \\
\iff &s\ln\left(1+\frac{1}{s}\right)^s + (2s+1)\ln(s+1) \\
&\quad \le 2(s+1)\ln(2(s+1)) \\
\iff &s\ln\left(1+\frac{1}{s}\right)^s - \ln(s+1) \\
&\quad \le 2(s+1)\ln 2 \\
\iff &s\left(\ln\left(1+\frac{1}{s}\right)^s - 2\ln 2\right) \\
&\quad \le \ln(s+1) + 2\ln 2,
\end{aligned}$$

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 $\frac{\mathbb{H}(f)}{\mathsf{Inf}(f)}$ 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 (2) 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 (3), 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 (2) (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, $\lim_{k\to\infty}\frac{\mathbb{H}(f)}{\mathsf{Inf}(f)} = 4$. This proves the FEI conjecture for monomials with (the best possible constant) $C = 4$. ■

3. 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 [19] 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 $D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})$ (with respect to any vector $\mathbf{a}$ with $\mathsf{wt}(\mathbf{a}) = 1$) is balanced [4, Chapter 3]. Further, we say that a function satisfies the SAC of order $1\leq k\leq n-2$ (with notation SAC(k)) if and only if by fixing k variables, the resulting function in $n-k$ variables is SAC. Also, if f satisfies SAC(k), then its algebraic degree satisfies $2\leq\deg(f)\leq n-k-1$. If for a function f, by changing k variables the output changes with probability $1/2$, we say that the function satisfies PC(k). It is known [4] that if a function satisfies the SAC(k), then it satisfies SAC(j), $1\leq j\leq k$. Equivalently, a function is PC(k) if and only if all the directional derivatives $D_{\mathbf{a}}f(\mathbf{x})$ (with respect to any vector $\mathbf{a}$ with $1\leq\mathsf{wt}(\mathbf{a})\leq k$) are balanced [4, Chapter 3].

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 $\lim_{n\to\infty}\frac{\log_2 L_n}{2^n} = 1$, so, the set of SAC functions has log-density 1.

Lemma 4. *We have*

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

$$\mathsf{Inf}^{[\ell]}(f) = \frac{1}{2}\sum_{i=1}^{\ell}\binom{n}{i} - \frac{1}{2^{n+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\substack{\mathbf{u}\in\mathbb{F}_2^n\\ 1\leq\mathsf{wt}(\mathbf{u})\leq\ell}}(-1)^{D_{\mathbf{u}}f(\mathbf{x})}.$$

Proof: It is easy to show that (see also [4, p.9]])

$$\mathsf{Prob}[f(\mathbf{x})\neq f(\mathbf{x}\oplus\mathbf{u})] =$$

$$frac12 - \frac{1}{2^{n+1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{D_{\mathbf{u}}f(\mathbf{x})},$$

which, by summing, implies

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

and the lemma is shown. ■

Theorem 5. *The FEI conjecture is true for the SAC Boolean functions (a log-density* 1 *set).*

Proof: Using Lemma 4, we restate the FEI conjecture as

$$\mathbb{H}(f) = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2 \log_2 \frac{1}{\widehat{f}(\mathbf{u})^2} \leq C\left(\frac{n}{2} - \frac{1}{2^{n+1}} \sum_{\substack{\mathbf{a}\in\mathbb{F}_2^n \\ \mathsf{wt}(\mathbf{a})=1}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_{\mathbf{a}}f(\mathbf{x})}\right), \tag{4}$$

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 (4) 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 (4) becomes $\frac{C}{2}n$, and so, the FEI conjecture is shown, with $C = 2$, for the set of SAC Boolean functions. ■

Remark 6. *Certainly, if f satisfies PC(ℓ), the ℓ-level and ℓ-total FEI conjectures are also true.*

Remark 7. *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 $\sum_{\mathbf{a}\in\mathbb{F}_2^n:\mathsf{wt}(\mathbf{a})=1} d_{\mathbf{a}}(f) \leq cn2^n$, $c < 1$, because then, by* (4) *we get*

$$\left(\frac{n}{2} - \frac{1}{2^{n+1}} \sum_{\substack{\mathbf{a}\in\mathbb{F}_2^n \\ \mathsf{wt}(\mathbf{a})=1}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_{\mathbf{a}}f(\mathbf{x})}\right) \geq \frac{n}{2} - \frac{1}{2^{n+1}} c\, n\, 2^n = \frac{1-c}{2}\, n,$$

and so, since $\mathbb{H}(f)$ is upper bounded by n, the FEI conjecture follows.

4. The FEI conjecture for plateaued functions

A Boolean function f is called *plateaued* (the concept was introduced by Zheng and Zhang [20] to generalize bent and semibent functions) if the set of Fourier coefficients $\mathrm{Spec}(f) \subseteq \{0, \pm\lambda\}$, for some $\lambda \neq 0$ (called the amplitude of f). If f is neither bent nor affine the inclusion above is equality. 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).

We consider general plateaued functions (under some technical condition on their level: precisely, we show the FEI conjecture if the level k of the plateaued function is either small or large).

Theorem 8. *For any fixed but arbitrary constant $0 < \epsilon < 1/2$, the Fourier Entropy–Influence conjecture is true for the class of plateaued Boolean functions of level k such that $n - k = O(1)$, or $\sum_{i=0}^{\lfloor \epsilon n \rfloor} \binom{n}{i} \leq 2^{n-k}$.*

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

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} 2^{-n} \log_2 2^n = n \leq C \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathsf{wt}(\mathbf{u}) 2^{-n} = C 2^{-n} \sum_{i=0}^{n} i \binom{n}{i} = \frac{C}{2} n, \tag{5}$$

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 $\mathrm{Spec}(f) = \{0, \pm 2^{(k-n)/2}\}$, $1 \leq k < n$. It is known that the number of nonzero vectors $\mathbf{u}$ for which $\widehat{f}(\mathbf{u}) \neq 0$ is exactly 2^{n-k}. The FEI conjecture for the plateaued functions is written as

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})^2 \log_2 \frac{1}{\widehat{f}(\mathbf{u})^2} \leq C \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathsf{wt}(\mathbf{u}) \widehat{f}(\mathbf{u})^2 \tag{6}$$

$$\iff \sum_{\mathbf{u}\in\mathbb{F}_2^n:\widehat{f}(\mathbf{u})\neq 0} 2^{k-n} \log_2 2^{n-k} \leq C \sum_{\mathbf{u}\in\mathbb{F}_2^n:\widehat{f}(\mathbf{u})\neq 0} \mathsf{wt}(\mathbf{u}) 2^{k-n} \tag{7}$$

$$\iff n - k \leq C\, 2^{k-n} \sum_{\mathbf{u}\in\mathbb{F}_2^n:\widehat{f}(\mathbf{u})\neq 0} \mathsf{wt}(\mathbf{u}) \tag{8}$$

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

$\sum_{i=0}^{T_{n,k}} \binom{n}{i} \geq 2^{n-k}$. It may be worth showing that $T_{\cdot,\cdot}$ is in fact increasing. Using $\binom{n}{i} < 2\binom{n-1}{i}$ (for $i \leq T_{n,k} \leq n/2$) 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 immediately implies that $T_{n-1,k} \leq T_{n,k} \leq T_{n-1,k} + 1$.

Next, using the identity $i\binom{n}{i} = n\binom{n-1}{i-1}$, the right hand side of the inequality (6) becomes

$$\begin{aligned} \mathsf{Inf}(f) &\geq 2^{k-n} \sum_{i=1}^{T_{n,k}-1} i\binom{n}{i} \\ &= 2^{k-n} n \sum_{j=0}^{T_{n,k}-2} \binom{n-1}{j}. \end{aligned}$$

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

$$\sum_{i=0}^{T_{n,k}-2} \binom{n-1}{i} \geq C 2^{n-k}. \qquad (9)$$

First, we observe that, if $n-k = O(1)$, since the left hand side of the above inequality (9) is certainly increasing and unbounded with n, 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 $n \geq n_0$.

We next assume that $\sum_{i=0}^{\lfloor \epsilon n \rfloor} \binom{n}{i} \leq 2^{n-k}$. It then implies that $\lfloor \epsilon\, n \rfloor \leq T_{n,k} \leq n/2$.

For brevity, let $T := T_{n,k}$. Next, we observe that the function $T \mapsto \frac{n-T+1}{T-1}$ is decreasing, and so, for $\epsilon\, n \leq T \leq n$, we get $\frac{n-T+1}{T-1} \leq \frac{n-\epsilon n+1}{\epsilon n-1} \leq \frac{1}{\epsilon}$ (for $n \geq \frac{\epsilon+1}{\epsilon^2}$), along with $\frac{n}{T} \leq \frac{n}{\epsilon\, n} = \frac{1}{\epsilon}$, then we get that

$$\begin{aligned} \binom{n}{T} &= \frac{n(n-T+1)}{T(T-1)} \binom{n-1}{T-2} \\ &\leq \frac{1}{\epsilon^2} \binom{n-1}{T-2} \end{aligned}$$

when $n \geq \frac{\epsilon+1}{\epsilon^2}$. Therefore, $\binom{n}{T} \leq C_1 \sum_{i=0}^{T-2} \binom{n-1}{i}$ from some constant C_1, and so from the definition of $T_{n,k}$, we get

$$\begin{aligned} 2^{n-k-1} &\leq \sum_{i=0}^{T} \binom{n-1}{i} \\ &= \sum_{i=0}^{T-2} \binom{n-1}{i} + \binom{n}{T} \qquad (10) \\ &\leq (1+C_1) \sum_{i=0}^{T-2} \binom{n-1}{i} \end{aligned}$$

from which (9) follows. ■

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

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] A. Canteaut, P. Charpin and G. M. Kyureghyan, *A new class of monomial bent functions*, Finite Fields Appl. 14 (2008), 221–241.

[3] C. Carlet, *Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications*, IEEE Trans. Inform. Theory 54 (3) (2008), 1262–1272.

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

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

[6] 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.

[7] G. Kalai, *The entropy/influence conjecture*, Posted on Terence Tao's *What's new* blog, http://terrytao.wordpress.com/2007/08/16/gil-kalai-the-entropyinfluence-conjecture, 2007.

[8] N. Keller, E. Mossel, and T. Schlank, *A note on the entropy/influence conjecture*, Discrete Math. 312:22 (2012), 3364–3372.

[9] A. Klivans, H. Lee, and A. Wan, *Mansour's Conjecture is true for random DNF formulas*, In Proc. of the 23rd Annual Conference on Learning Theory, pages 368–380, 2010.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] O. S. Rothaus, *On bent functions*, J. Combin. Theory – Ser. A 20 (1976), 300–305 (appeared originally as IDA CRD W.P. No. 169, 1966).

[16] D. R. Stinson, Cryptography – Theory and practice (3rd Ed.), Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[17] M. Talagrand, *On Russo's approximate zero-one law*, Annals of Probability, 22:3 (1994), 1576–1587.

[18] E. Viola, *On the power of small-depth computation*, Foundations and Trends in Theoretical Computer Science, 5(1) (2009) 1–72. http://www.ccs.neu.edu/home/viola/papers/shallow.pdf.

[19] A. F. Webster and S. E. Tavares, *On the design of* S*-boxes*, Advances in Cryptology-Crypto '85, LNCS 218 (Springer, Berlin, 1986), pp. 523–534.

[20] Y. Zheng and X. M. Zhang, *Plateaued functions*, in Advances in Cryptology–ICICS '99, LNCS 1726 (Springer-Verlag, 1999), pp. 284–300.

[21] A. Wan, J. Wright, and C. Wu, *Decision Trees, Protocols, and the Fourier Entropy-Influence Conjecture*, arxiv.org/abs/1312.3003, 2013.

Sugata Gangopadhyay received MSc degree in Mathematics in the year 1993 from the Indian Institute of Technology Kharagpur. He completed PhD from the Indian Institute of Technology Kharagpur in 1998. Currently he is an Associate Professor at the Department of Computer Science and Engineering of the Indian Institute of Technology Roorkee. His research interests are in Cryptology and Discrete Mathematics.

Pantelimon Stănič a received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. Currently, he is a Professor at the Naval Postgraduate School, in Monterey, California. His research interests are in Cryptology, Number Theory and Discrete Mathematics.