Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 111 (2021)

Influence of a Set of Variables on a Boolean Function

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

June 15, 2022

Abstract

The influence of a variable is an important concept in the analysis of Boolean functions. The more general notion of influence of a set of variables on a Boolean function has four separate definitions in the literature. In the present work, we introduce a new definition of influence of a set of variables which is based on the auto-correlation function and develop its basic theory. Among the new results that we obtain are generalisations of the Poincaré inequality and the edge expansion property of the influence of a single variable. Further, we obtain new characterisations of resilient and bent functions using the notion of influence. We show that the previous definition of influence due to Fischer et al. (2002) and Blais (2009) is half the value of the auto-correlation based influence that we introduce. Regarding the other prior notions of influence, we make a detailed study of these and show that each of these definitions do not satisfy one or more desirable properties that a notion of influence may be expected to satisfy.

Keywords: Boolean function, influence, Fourier transform, Walsh transform, auto-correlation, junta, bent functions, resilient functions.

1 Introduction

Boolean functions play an important role in diverse areas of mathematics and computer science, including combinatorics, probability, complexity theory, learning theory, cryptography and coding theory. We refer to two excellent books on Boolean functions, namely [11] and [6]. The first book focuses on Boolean functions in the context of theoretical computer science, while the second book focuses on Boolean functions in relation to cryptography and coding theory.

The notion of influence of a variable on a Boolean function was introduced by Ben-Or and Linial [2]. Subsequently, this concept has become central to the study of Boolean functions in various contexts. See [11] for a very comprehensive account of such applications. The notion of influence, however, has not received much attention in the context of cryptographic applications of Boolean functions. We know of only two works [9, 3] which have studied influence in relation to cryptographic properties.

The notion of influence of a variable on a function has been extended to consider the influence of a set of variables on a function. We have been able to locate four different definitions of the influence of a set of variables on a Boolean function. The first definition appears in the work of Ben-Or and Linial [2] itself in 1989. A different definition due to Fischer et al. [7] appeared in 2002 and the same definition was considered in 2009 by Blais [4]. A third definition was given by Gangyopadhyay and Stănică [9] in 2016 and a fourth definition was given by Tal [16] in 2017. All of these definitions coincide with each

ISSN 1433-8092

other in the case of a single variable, but in the case of more than one variable, in general the values provided by the four definitions of influence are different.

The motivation of our work is to make a systematic and comprehensive study of the notion of influence of a set of variables on a Boolean function. To this end, we introduce a definition of influence based on the auto-correlation function, which is a very useful tool for analysing certain cryptographic properties of Boolean functions. Two Walsh transform based characterisations of influence are obtained and some basic intuitive properties are derived. Several results on the influence of a single variable are generalised. These include Poincaré inequality and edge expansion property of influence of a variable. In the context of cryptographic properties, we provide characterisations of resilient and bent functions using the notion of influence.

The definition of influence given in [7, 4] is shown to be half the value of the notion of influence that we introduce. We also argue that the definition of influence considered in [9] does not satisfy a basic desirable property, namely that the influence of a set of variables can be zero even if the function is not degenerate on these variables.

Next we define a quantity called pseudo-influence, obtain its Walsh transform based characterisation and derive certain basic properties. We show that the pseudo-influence does not satisfy some intuitive properties that one would expect a notion of influence to satisfy, which is why we call it pseudo-influence. From the Walsh transform based characterisation, it follows that the definition of influence considered by Tal [16] is the notion of pseudo-influence that we introduce. Our motivation for introducing pseudo-influence and analysing it is to show that the notion of influence considered in [16] is not satisfactory.

Lastly, we make a systematic study of the Ben-Or and Linial (BL) notion of influence [2]. We show that the BL notion of influence satisfies some desirable properties, but it does not satisfy sub-additivity. Further, we argue that compared to the auto-correlation based definition, the BL notion of influence is a more coarse measure.

Section 2 introduces the background and the notation and also describes the previous definitions of influence of a set of variables. The definition of influence from auto-correlation is introduced in Section 3 and its Walsh transform based characterisations and basic properties are derived. The concept is further developed in several subsections. The path expansion property of influence is derived in Section 3.1, two probabilistic interpretations of influence are given in Section 3.2, the relation of influence to juntas and cryptographic properties are described in Section 3.3 and 3.4 respectively, and a general form the Fourier entropy/influence conjecture is mentioned in Section 3.5. The notion of pseudo-influence is introduced in Section 4 and its properties as well as its relation to influence are studied. Section 5 makes a detailed investigation of the notion of influence introduced by Ben-Or and Linial and its relation to the auto-correlation based notion of influence. Finally, Section 6 concludes the paper.

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.

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 $\mathbf{0}_n$ and $\mathbf{1}_n$ we will denote the all-zero and all-one vectors of length n respectively. For $\mathbf{x} = (x_1, \ldots, x_2), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, we write $\mathbf{x} \leq \mathbf{y}$ if $x_i = 1$ implies $y_i = 1$ for $i = 1, \ldots, n$. The inner product $\langle \mathbf{x}, \mathbf{y} \rangle$ of $\mathbf{x}$ and $\mathbf{y}$ is defined to be $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 \oplus \cdots \oplus x_ny_n$. For a subspace E of $\mathbb{F}_2^n$, $E^\perp$ will denote the subspace $\{\mathbf{x} \in \mathbb{F}_2^n : \langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{0}_n,$ for all $\mathbf{y} \in E\}$. For $T \subseteq [n]$, χ_T denotes the vector in

$\mathbb{F}_2^n$ where the i-th component of χ_T is 1 if and only if $i \in T$; further, $\overline{T}$ will denote the set $[n] \setminus T$.

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 $f(\mathbf{X})$. 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 $\mathsf{wt}(f) = 2^{n-1}$, i.e., $\mathbb{E}_{\mathbf{x}\in\mathbb{F}_2^n}(f) = 1/2$. Noting that $f^2 = f$, the variance of f, denoted as $\mathsf{Var}(f)$ is equal to $\mathbb{E}(f^2) - \mathbb{E}(f)^2 = \mathbb{E}(f)(1 - \mathbb{E}(f))$.

Remark 1 *In the literature, n-variable Boolean functions have variously been considered to be maps from $\{-1,1\}^n$ to $\{-1,1\}$, or maps from $\{-1,1\}^n$ to $\{0,1\}$, or maps from $\{0,1\}^n$ to $\{-1,1\}$. As stated above, in this paper, we will consider Boolean functions to be maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Results stated in this representation will be somewhat different from, though equivalent to, the results stated in the other representations.*

Let $\mathbf{X} = (X_1, \ldots, X_n)$ be a vector of variables and suppose $\emptyset \neq T = \{i_1, \ldots, i_t\} \subseteq [n]$, where $i_1 \leq \cdots \leq i_t$. By $\mathbf{X}_T$ we denote the vector of variables $(X_{i_1}, \ldots, X_{i_t})$. Suppose $f(\mathbf{X})$ is an n-variable Boolean function. For $\boldsymbol{\alpha} \in \mathbb{F}_2^t$, by $f_{\mathbf{X}_T \leftarrow \boldsymbol{\alpha}}(\mathbf{X}_{\overline{T}})$ we denote the Boolean function on $n - t$ variables obtained by setting the variables in $\mathbf{X}_T$ to the respective values in $\boldsymbol{\alpha}$. The function f is said to be degenerate on the set of variables $\{X_{i_1}, \ldots, X_{i_t}\}$ if these variables do not influence the output of the function f, i.e., for any $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}_2^t$ if we set $f_{\boldsymbol{\alpha}} = f_{\mathbf{X}_T \leftarrow \boldsymbol{\alpha}}(\mathbf{X}_{\overline{T}})$ and $f_{\boldsymbol{\beta}} = f_{\mathbf{X}_T \leftarrow \boldsymbol{\beta}}(\mathbf{X}_{\overline{T}})$, then the functions $f_{\boldsymbol{\alpha}}$ and $f_{\boldsymbol{\beta}}$ are equal.

Let $\psi : \mathbb{F}_2^n \to \mathbb{R}$. The Fourier transform of ψ is a map $\widehat{\psi} : \mathbb{F}_2^n \to \mathbb{R}$ which is defined as follows.

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

The Poisson summation formula (see Page 58 of [6]) provides a useful relation between a function $\psi : \mathbb{F}_2^n \to \mathbb{R}$ and its Fourier transform. Let E be a subspace of $\mathbb{F}_2^n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$. Then

$$\sum_{\mathbf{w}\in\mathbf{a}+E} (-1)^{\langle \mathbf{b}, \mathbf{w} \rangle} \widehat{\psi}(\mathbf{w}) \quad = \quad \frac{\#E}{2^n} (-1)^{\langle \mathbf{a}, \mathbf{b} \rangle} \sum_{\mathbf{u}\in\mathbf{b}+E^{\perp}} (-1)^{\langle \mathbf{a}, \mathbf{u} \rangle} \psi(\mathbf{u}). \tag{2}$$

The (normalised) Walsh transform of a Boolean function f is a map $W_f : \mathbb{F}_2^n \to [-1, 1]$ which is defined as follows.

$$W_f(\boldsymbol{\alpha}) \quad = \quad \frac{1}{2^n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \langle \mathbf{x}, \boldsymbol{\alpha} \rangle} = 1 - \frac{\mathsf{wt}(f(\mathbf{X}) \oplus \langle \boldsymbol{\alpha}, \mathbf{X} \rangle)}{2^{n-1}}. \tag{3}$$

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

Note that $W_f(\boldsymbol{\alpha}) = 0$ if and only if the function $f(\mathbf{X}) \oplus \langle \boldsymbol{\alpha}, \mathbf{X} \rangle$ is balanced. From Parseval's theorem (see Page 79 of [6]), it follows that

$$\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n} (W_f(\boldsymbol{\alpha}))^2 \quad = \quad 1. \tag{4}$$

So the values $\left\{ (W_f(\boldsymbol{\alpha}))^2 \right\}$ 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 $(W_f(\boldsymbol{\alpha}))^2$. For $k \in \{0, \ldots, n\}$, let

$$\widehat{p}_f(k) \quad = \quad \sum_{\{\mathbf{u}\in\mathbb{F}_2^n : \mathsf{wt}(\mathbf{u}) = k\}} (W_f(\mathbf{u}))^2 \tag{5}$$

be the probability assigned by the Fourier transform of f to the integer k. Note that $\widehat{p}_f(\mathbf{0}_n) = (1-2\mathbb{E}(f))^2$ and so $1-\widehat{p}_f(\mathbf{0}_n) = 4\mathbb{E}(f)(1-\mathbb{E}(f)) = 4\,\mathsf{Var}(f)$.

The (normalised) auto-correlation function of f is a map $C_f : \mathbb{F}_2^n \to [-1,1]$ defined as follows.

$$\begin{aligned} & C_f(\boldsymbol{\alpha}) \\ &= \frac{1}{2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\boldsymbol{\alpha})} = 1 - \frac{\mathsf{wt}(f(\mathbf{X})\oplus f(\mathbf{X}\oplus\boldsymbol{\alpha}))}{2^{n-1}} = 1 - 2\Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq f(\mathbf{x}\oplus\boldsymbol{\alpha})]. \end{aligned} \quad (6)$$

Note that $C_f(\mathbf{0}) = 1$.

For a Boolean function f, the Wiener-Khintchine formula (see Page 80 of [6]) relates the Walsh transform to the auto-correlation function.

$$(W_f(\boldsymbol{\alpha}))^2 \;=\; \widehat{C}_f(\boldsymbol{\alpha}) = \frac{1}{2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\langle\boldsymbol{\alpha},\mathbf{x}\rangle}C_f(\mathbf{x}). \quad (7)$$

Applying (2) with $\psi = C_f$ and $\mathbf{a} = \mathbf{b} = \mathbf{0}_n$ and then using (7), we obtain the following result (see Proposition 5 of [5]).

$$\sum_{\mathbf{w}\in E}(W_f(\mathbf{w}))^2 \;=\; \frac{\#E}{2^n}\sum_{\mathbf{u}\in E^{\perp}}C_f(\mathbf{u}). \quad (8)$$

Let $T \subseteq [n]$ with $\#T = t$ and for $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, let $f_{\boldsymbol{\alpha}}$ denote $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}(\mathbf{X}_T)$. Then $f_{\boldsymbol{\alpha}}$ is a t-variable function. From the second order Poisson summation formula (see Page 62 of [6] for the general statement of this result), we have

$$\sum_{\mathbf{w}\leq\chi_{\overline{T}}}(W_f(\mathbf{w}))^2 \;=\; \frac{1}{2^{n-t}}\sum_{\boldsymbol{\alpha}\leq\chi_{\overline{T}}}\left(W_{f_\alpha}(\mathbf{0}_t)\right)^2. \quad (9)$$

Remark 2 *We have normalised the Walsh transform and the auto-correlation function by 2^n so that the values lie in the range $[-1,1]$. The non-normalised versions have also been used in the literature. We note in particular that [6] uses the non-normalised versions. When we use results from [6], we normalise them appropriately.*

Some Boolean function classes. Let f be an n-variable Boolean function.

- The function f is said to be bent [13] if $W_f(\boldsymbol{\alpha}) = \pm 2^{-n/2}$ for all $\boldsymbol{\alpha} \in \mathbb{F}_2^n$. Bent functions exist if and only if n is even.
- The function f is said to satisfy propagation characteristics [12] of degree $k \geq 1$, written as PC(k), if $C_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $1 \leq \mathsf{wt}(\mathbf{u}) \leq k$.
- The function f is said to be m-resilient [15, 17] if $W_f(\boldsymbol{\alpha}) = 0$ for all $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ with $0 \leq \mathsf{wt}(\boldsymbol{\alpha}) \leq m$.
- The function f is said to be an s-junta if there is a subset $S \subseteq [n]$ with $\#S \leq s$ such that f is degenerate on the variables indexed by $\overline{S}$.

2.1 Influence

Let $f(\mathbf{X})$ be an n-variable Boolean function where $\mathbf{X} = (X_1, \ldots, X_n)$. For $i \in [n]$, the influence of X_i on f is denoted by $\mathsf{inf}_i(f)$ and is defined to be the probability (over a uniform random choice of $\mathbf{x} \in \mathbb{F}_2^n$) that $f(\mathbf{x})$ is not equal to $f(\mathbf{x} \oplus \mathbf{e}_i)$, i.e.,

$$\mathsf{inf}_i(f) \quad = \quad \Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq f(\mathbf{x} \oplus \mathbf{e}_i)]. \tag{10}$$

The total influence $\mathsf{inf}(f)$ of the individual variables is defined to be the sum of the influences of the individual variables, i.e. $\mathsf{inf}(f) = \sum_{i\in[n]} \mathsf{inf}_i(f)$.

Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$ with $t = \#T$. The influence of the set of variables indexed by T on f has been defined in the literature in four different ways. These definitions are given below.

Ben-Or and Linial [2]. The definition of influence introduced in [2] is the following.

$$\mathcal{I}_f(T) \quad = \quad \Pr_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}}\left[f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}(\mathbf{X}_T) \text{ is not constant}\right]. \tag{11}$$

Fischer et al. [7] and Blais [4]. The same quantity has been defined in two different ways in Fischer et al. [7] and Blais [4]. In [7], this quantity was called 'variation' and in [4], it was termed 'influence'. Here we provide the formulation as given in [4]. For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, let $Z(T, \mathbf{x}, \mathbf{y})$ denote the vector $\mathbf{z} \in \mathbb{F}_2^n$, where $z_i = y_i$, if $i \in T$ and $z_i = x_i$ otherwise. The definition of influence given in [4] is the following.

$$I_f(T) \quad = \quad \Pr_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}\left[f(\mathbf{x}) \neq f(Z(T, \mathbf{x}, \mathbf{y}))\right]. \tag{12}$$

Gangopadhyay and Stănică [9]. The definition of influence introduced in [2] is the following.

$$\mathcal{J}_f(T) \quad = \quad \Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq f(\mathbf{x} \oplus \chi_T)] = \frac{1}{2}\left(1 - C_f(\chi_T)\right). \tag{13}$$

Tal [16]. For $\boldsymbol{\beta} \in \mathbb{F}_2^t$, let $f_{\boldsymbol{\beta}}$ denote the function $f_{\mathbf{X}_T\leftarrow\boldsymbol{\beta}}$. Let $D_T f : \{0,1\}^{n-t} \to [-1, 1]$ be defined as follows. For $\mathbf{y} \in F_2^{n-t}$, $(D_T f)(\mathbf{y}) = 1/2^t \times \sum_{\boldsymbol{\beta}\in\mathbb{F}_2^t}(-1)^{\mathsf{wt}(\boldsymbol{\beta})+f_{\boldsymbol{\beta}}(\mathbf{y})}$. The definition of influence given in [16] is the following.

$$J_f(T) \quad = \quad \mathop{\mathbb{E}}_{\mathbf{y}\in\mathbb{F}_2^{n-t}}\left[\left(D_T f(\mathbf{y})\right)^2\right]. \tag{14}$$

3 Influence from Auto-Correlation

The auto-correlation function is a very useful tool for expressing various properties of Boolean functions. We refer to [6] for the many uses of the auto-correlation function in the context of cryptographic properties of Boolean functions. Given an n-variable Boolean function f and $\boldsymbol{\alpha} \in \mathbb{F}_2^n$, the value of the auto-correlation function C_f at $\boldsymbol{\alpha}$, i.e., $C_f(\boldsymbol{\alpha})$ is the number of places $f(\mathbf{X})$ and $f(\mathbf{X} \oplus \boldsymbol{\alpha})$ are equal minus the number of places they are unequal (normalised by 2^n). So the auto-correlation function at $\boldsymbol{\alpha}$ to some extent captures the effect on f of flipping all the bits in the support of $\boldsymbol{\alpha}$. This suggests that the auto-correlation function is an appropriate mechanism to capture the influence of a set of variables on a Boolean function. We note that for $i \in [n]$, $\mathsf{inf}_i(f)$ can be written as follows.

$$\mathsf{inf}_i(f) \quad = \quad \frac{1}{2}\left(1 - C_f(\mathbf{e}_i)\right) = 1 - \frac{1}{2}\left(C_f(\mathbf{0}) + C_f(\mathbf{e}_i)\right). \tag{15}$$

Let $f(X_1, \ldots, X_n)$ be an n-variable Boolean function and $\emptyset \neq T = \{i_1, \ldots, i_t\} \subseteq [n]$. We denote the influence of the set of variables $\{X_{i_1}, \ldots, X_{i_t}\}$ corresponding to $T = \{i_1, \ldots, i_t\}$ on the Boolean function f by $\mathsf{inf}_f(T)$. Following the auto-correlation based expression of the influence of a single variable on a Boolean function given by (15), we put forward the following definition of $\mathsf{inf}_f(T)$.

$$\mathsf{inf}_f(T) \quad = \quad 1 - \frac{1}{2^{\#T}}\left(\sum_{\boldsymbol{\alpha} \leq \chi_T} C_f(\boldsymbol{\alpha})\right). \tag{16}$$

It is easy to note that for a singleton set $T = \{i\}$, $\mathsf{inf}_f(T) = \mathsf{inf}_i(f)$. Further, one may note that $\mathsf{inf}_f(T) = 2^{1-t} \times \sum_{S \subseteq T} \mathcal{J}_f(S)$.

Remark 3 *We note that $\mathsf{inf}_f(T)$, $\mathcal{I}_f(T)$, $J_f(T)$ and $\mathcal{J}_f(T)$ (defined in 2.1) agree with each other when $\#T = 1$. Also, we later show that $I_f(T) = \mathsf{inf}_f(T)/2$.*

It is perhaps not immediately obvious that the definition of influence given by (16) is appropriate. We later show in Theorem 4 that this definition satisfies a set of intuitive desiderata that any notion of influence may be expected to satisfy.

Let f be an n-variable function and t be an integer with $1 \leq t \leq n$. Then the t-influence of f is the total influence (scaled by $\binom{n}{t}$) obtained by summing the influence of every set of t variables on the function f, i.e.,

$$t\text{-}\mathsf{inf}(f) \quad = \quad \frac{\sum_{\{T \subseteq [n] : \#T = t\}} \mathsf{inf}_f(T)}{\binom{n}{t}}. \tag{17}$$

Note that 1-$\mathsf{inf}(f)$ is equal to $\mathsf{inf}(f)/n$, i.e., 1-$\mathsf{inf}(f)$ is the sum of the influences of the individual variables scaled by a factor of n.

The following result provides a characterisation of influence in terms of the Walsh transform.

Theorem 1 *Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$. Then*

$$\mathsf{inf}_f(T) \quad = \quad \sum_{\{\mathbf{u} \in \mathbb{F}_2^n : \mathsf{supp}(\mathbf{u}) \cap T \neq \emptyset\}} \left(W_f(\mathbf{u})\right)^2. \tag{18}$$

Proof: Let $\#T = t$. Let E be the subspace $\{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \leq \chi_{\overline{T}}\}$. Then $\#E = 2^{n-t}$ and $E^\perp = \{\mathbf{y} \in \mathbb{F}_2^n : \mathbf{y} \leq \chi_T\}$. Using (8), we obtain

$$\sum_{\mathbf{x} \leq \chi_{\overline{T}}} \left(W_f(\mathbf{x})\right)^2 \quad = \quad \frac{2^{n-t}}{2^n} \sum_{\mathbf{y} \leq \chi_T} C_f(\mathbf{y}) = \frac{1}{2^{\#T}} \sum_{\mathbf{y} \leq \chi_T} C_f(\mathbf{y}). \tag{19}$$

Using (19) with (16) and (4) we have

$$\mathsf{inf}_f(T) \quad = \quad 1 - \sum_{\mathbf{x} \leq \chi_{\overline{T}}} \left(W_f(\mathbf{x})\right)^2 = \sum_{\mathbf{w} \in \mathbb{F}_2^n} \left(W_f(\mathbf{w})\right)^2 - \sum_{\mathbf{x} \leq \chi_{\overline{T}}} \left(W_f(\mathbf{x})\right)^2 = \sum_{\mathbf{u} \not\leq \chi_{\overline{T}}} \left(W_f(\mathbf{u})\right)^2.$$

The condition $\mathbf{u} \not\leq \chi_{\overline{T}}$ is equivalent to $\mathsf{supp}(\mathbf{u}) \cap T \neq \emptyset$. □

It is a well known result (see Page 52 of [11]) that for an n-variable Boolean function, the total influence of the individual variables, i.e., $\mathsf{inf}(f)$ is the expected value of a random variable which takes the value k with probability $\widehat{p}_f(k)$ for $k = 0, \ldots, n$. We generalise this result to the case of t-$\mathsf{inf}(f)$ for $t \geq 1$.

For positive integer n, t and k with, $1 \leq t \leq n$ and $0 \leq k \leq n$, let $N_{n,t,k}$ be the number of subsets of $[n]$ of size t which contains at least one element of $[k]$. Then

$$N_{n,t,k} \quad = \quad \binom{n}{t} - \binom{n-k}{t} = \sum_{i=1}^{\min(k,t)} \binom{k}{i}\binom{n-k}{t-i}. \tag{20}$$

It follows that $N_{n,t,0} = 0$, $N_{n,t,k} = \binom{n}{t}$ for $n - t + 1 \leq k \leq n$, and $N_{n,1,k} = k$ for $k = 0, \ldots, n$.

Theorem 2 *Let f be an n-variable function and $t \in [n]$. Then*

$$t\text{-}\mathsf{inf}(f) \quad = \quad \frac{1}{\binom{n}{t}} \mathbb{E}[Z], \tag{21}$$

where Z is a random variable which takes the value $N_{n,t,k}$ with probability $\widehat{p}_f(k)$.

Proof: Consider $\mathbf{u} \in \mathbb{F}_2^n$ with $\#\mathsf{supp}(\mathbf{u}) = k$. For $1 \leq i \leq \min(k,t)$, the number of subsets T of $[n]$ of cardinality t whose intersection with $\mathsf{supp}(\mathbf{u})$ is of size i is $\binom{k}{i}\binom{n-k}{t-i}$. Summing over i provides the number of subsets T of $[n]$ of cardinality t with which $\mathsf{supp}(\mathbf{u})$ has a non-empty intersection.

$$\begin{aligned}
t\text{-}\mathsf{inf}(f) \quad &= \quad \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} \sum_{\{\mathbf{u} \in \mathbb{F}_2^n : \mathsf{wt}(\mathbf{u}) = k\}} \sum_{i=1}^{\min(k,t)} \binom{k}{i}\binom{n-k}{t-i} \left(W_f(\mathbf{u})\right)^2 \\
&= \quad \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} \sum_{i=1}^{\min(k,t)} \binom{k}{i}\binom{n-k}{t-i} \sum_{\{\mathbf{u} \in \mathbb{F}_2^n : \mathsf{wt}(\mathbf{u}) = k\}} \left(W_f(\mathbf{u})\right)^2 \\
&= \quad \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} N_{n,t,k} \widehat{p}_f(k) \qquad (22) \\
&= \quad \frac{1}{\binom{n}{t}} \mathbb{E}[Z].
\end{aligned}$$

□

Poincaré inequality (see Page 52 of [11]) states that the total influence of the individual variables, i.e., $\mathsf{inf}(f)$ is bounded below by $4\,\mathsf{Var}(f)$. We obtain a generalisation of this result as a corollary of Theorem 2.

Corollary 1 *Let f be an n-variable Boolean function and $t \in [n]$. Then*

$$t\text{-}\mathsf{inf}(f) \quad \geq \quad \frac{4t}{n} \mathsf{Var}(f). \tag{23}$$

Equality is achieved for $t = n$.

Proof: It is easy to check that for $k \in [n]$, $N_{n,t,k}/\binom{n}{t} \geq t/n$, where equality is achieved for $t = n$. So from (22),

$$t\text{-}\mathsf{inf}(f) \quad \geq \quad \frac{t}{n}\sum_{k=1}^{n}\widehat{p}_f(k) = \frac{t}{n}(1-\widehat{p}_f(\mathbf{0}_n)) = \frac{4t}{n}\mathsf{Var}(f).$$

□

An alternative Walsh transform based characterisation of influence is given by the following result.

Theorem 3 *Let f be an n-variable function and $\emptyset \neq T \subseteq [n]$. Then*

$$\mathsf{inf}_f(T) \quad = \quad 1 - \frac{1}{2^{n-t}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}}\left(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t)\right)^2, \tag{24}$$

where $f_{\boldsymbol{\alpha}}$ denotes $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}$.

Proof: Let $\#T = t$. Let $E = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \leq \chi_{\overline{T}}\}$ and so $E^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \leq \chi_T\}$. Using (8) and (9) we have

$$\frac{1}{2^t}\sum_{\mathbf{u}\leq\chi_T} C_f(\mathbf{u}) \quad = \quad \frac{1}{2^{n-t}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}}\left(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t)\right)^2.$$

Using the definition of influence given in (16), we obtain the required result. □

Remark 4 *Theorems 1 and 3 provide two different Walsh transform based characterisations of* $\mathsf{inf}_f(T)$*. The expression for* $\mathsf{inf}_f(T)$ *given by (24) can be computed in $O(2^n)$ time, while the expression given by (18) in general will require $O(n2^n)$ time using the fast Fourier transform algorithm to compute the required values of the Walsh transform.*

We obtain the following corollary of Theorem 3.

Corollary 2 *Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$. Then*

$$\mathsf{inf}_f(T) \quad = \quad \frac{1}{2^{n-2-t}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}}\mathsf{Var}(f_{\boldsymbol{\alpha}}) \tag{25}$$

where $f_{\boldsymbol{\alpha}}$ denotes $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}$.

Proof: Using (24), we have

$$\begin{aligned}
\mathsf{inf}_f(T) \quad &= \quad 1 - \frac{1}{2^{n-t}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}}\left(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t)\right)^2 \\
&= \quad \frac{1}{2^{n-t}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}}\left(1-\left(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t)\right)^2\right) \\
&= \quad \frac{1}{2^{n-t}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}} 4\mathbb{E}\left(f_{\boldsymbol{\alpha}}\right)\left(1-\mathbb{E}\left(f_{\boldsymbol{\alpha}}\right)\right)
\end{aligned}$$

$$= \frac{1}{2^{n-2-t}} \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}} \mathsf{Var}(f_{\boldsymbol{\alpha}}). \tag{26}$$

□

One may consider some basic desiderata that any reasonable measure of influence should satisfy. Since we are considering normalised measures, the value of influence should be in the set $[0,1]$ and it should take the value 0 if and only if the function is degenerate on the set of variables. Further, by expanding a set of variables, the value of influence should not decrease, i.e. influence should be monotonic non-decreasing. Also, sub-additivity is a desirable property. The following result shows these properties for $\mathsf{inf}_f(T)$ and also characterises the condition under which $\mathsf{inf}_f(T)$ takes its maximum value 1.

Theorem 4 *Let f be an n-variable Boolean function and $\emptyset \neq T, S \subseteq [n]$. Then*

1. $0 \leq \mathsf{inf}_f(T) \leq 1$.
2. $\mathsf{inf}_f(T) = 0$ *if and only if the function f is degenerate on the variables indexed by T.*
3. $\mathsf{inf}_f(T) = 1$ *if and only if $f_{\boldsymbol{\alpha}}$ is balanced for each $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, where $f_{\boldsymbol{\alpha}}$ denotes $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}$.*
4. $\mathsf{inf}_f(S \cup T) \geq \mathsf{inf}_f(T)$.
5. $\mathsf{inf}_f(S \cup T) = \mathsf{inf}_f(S) + \mathsf{inf}_f(T) - \sum_{\mathbf{u}\in\mathcal{U}} (W_f(\mathbf{u}))^2$, *where $\mathcal{U} = \{\mathbf{u} \in \mathbb{F}_2^n : \mathsf{supp}(\mathbf{u}) \cap S \neq \emptyset \neq \mathsf{supp}(\mathbf{u}) \cap T\}$. Consequently, $\mathsf{inf}_f(S\cup T) \leq \mathsf{inf}_f(S) + \mathsf{inf}_f(T)$ (i.e., $\mathsf{inf}_f(T)$ satisfies sub-additivity).*

Proof: The first point follows from Theorem 1 and Parseval's theorem. The fourth and fifth points also follow from Theorem 1. The third point follows from Theorem 3.

Consider the second point. From (24), $\mathsf{inf}_f(T) = 0$ if and only if $\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}} (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 = 2^{n-t}$. Since $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 \leq 1$, it follows that $\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^{n-t}} (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 = 2^{n-t}$ if and only if $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 = 1$ (equivalently, $f_{\boldsymbol{\alpha}}$ is constant) for all $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$. The last condition is equivalent to the statement that f is degenerate on the set of variables indexed by T. □

Remark 5 *For the Gangopadhyay and Stănică notion of influence $\mathcal{J}_f(T)$ (see 13) the second point of Theorem 4 does not hold. It is possible that f is not degenerate on the variables indexed by T, yet $\mathcal{J}_f(T) = 0$. For example, let $f(X_1, X_2, X_3, X_4) = (1 \oplus X_1)X_2(X_3 \oplus X_4)$ and $T = \{3, 4\}$. Then it may be checked that $\mathcal{J}_f(T) = 0$, but f is not degenerate on the set of variables $\{X_3, X_4\}$ as $f(0,1,0,0) = 0 \neq f(0,1,0,1)$.*

If a function is not degenerate on the set of variables indexed by T, then these variables have an effect on value of f. Any reasonable measure of influence should ensure that if f is not degenerate on a set of variables, then the value of the measure for this set of variables is positive. Since this condition does not hold for $\mathcal{J}_f(T)$, this measure cannot be considered to be a satisfactory measure of influence of a set of variables.

Theorem 5 *Let f be an n-variable Boolean function and t be an integer with $1 \leq t \leq n$.*

1. *t-$\mathsf{inf}(f)$ takes its maximum value 1 if and only if f is $(n-t)$-resilient.*
2. *t-$\mathsf{inf}(f)$ takes its minimum value 0 if and only if f is a constant function.*

Proof: From (22) and recalling that $N_{n,t,0} = 0$ and $N_{n,t,k} = \binom{n}{t}$ for $n - t + 1 \leq k \leq n$, we have

$$
\begin{aligned}
t\text{-}\mathsf{inf}(f) &= \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} N_{n,t,k}\widehat{p}_f(k) \\
&= \frac{1}{\binom{n}{t}} \left(\sum_{k=0}^{n-t} \left(\binom{n}{t} - \binom{n-k}{t} \right) \widehat{p}_f(k) + \sum_{k=n-t+1}^{n} \binom{n}{t} \right) \widehat{p}_f(k) \\
&= \frac{1}{\binom{n}{t}} \left(\sum_{k=0}^{n} \binom{n}{t} \widehat{p}_f(k) - \sum_{k=0}^{n-t} \binom{n-k}{t} \widehat{p}_f(k) \right) \\
&= 1 - \frac{1}{\binom{n}{t}} \sum_{k=0}^{n-t} \binom{n-k}{t} \widehat{p}_f(k). \qquad (27)
\end{aligned}
$$

From (27), $t\text{-}\mathsf{inf}(f)$ takes its maximum value of 1 if and only if $\sum_{k=0}^{n-t} \binom{n-k}{t} \widehat{p}_f(k) = 0$ which holds if and only if $\widehat{p}_f(k) = 0$ for $k = 0, \ldots, n - t$, i.e., if and only if f is $(n - t)$-resilient. This shows the first point.

For the second point, from (27), $t\text{-}\mathsf{inf}(f) = 0$ if and only if

$$
\binom{n}{t} \widehat{p}_f(0) + \binom{n-1}{t} \widehat{p}_f(1) + \cdots + \binom{t}{t} \widehat{p}_f(t) = \binom{n}{t}. \qquad (28)
$$

If f is a constant function, then $\widehat{p}_f(0) = 1$ and $\widehat{p}_f(k) = 0$ for $k \in [n]$. So (28) holds. On the other hand, if f is not a constant function, then $\widehat{p}_f(0) < 1$. In this case,

$$
\begin{aligned}
&\binom{n}{t} \widehat{p}_f(0) + \binom{n-1}{t} \widehat{p}_f(1) + \cdots + \binom{t}{t} \widehat{p}_f(t) \\
&\leq \binom{n}{t} \widehat{p}_f(0) + \binom{n-1}{t} (\widehat{p}_f(1) + \cdots + \widehat{p}_f(n)) \\
&= \binom{n}{t} \widehat{p}_f(0) + \binom{n-1}{t} (1 - \widehat{p}_f(0)) < \binom{n}{t}.
\end{aligned}
$$

□

The next result shows that as t increases, the value of $t\text{-}\mathsf{inf}(f)$ is non-decreasing.

Theorem 6 *Let f be an n-variable Boolean function. For $t \in [n]$, $t\text{-}\mathsf{inf}(f)$ increases monotonically with t.*

Proof: For $t \in [n - 1]$, the following calculations show that $t\text{-}\mathsf{inf}(f)$ is at most $(t + 1)\text{-}\mathsf{inf}(f)$.

$$
\begin{aligned}
&t\text{-}\mathsf{inf}(f) \leq (t+1)\text{-}\mathsf{inf}(f) \\
\iff\ & 1 - \sum_{k=0}^{n-t} \frac{\binom{n-k}{t}}{\binom{n}{t}} \widehat{p}_f(k) \leq 1 - \sum_{k=0}^{n-t-1} \frac{\binom{n-k}{t+1}}{\binom{n}{t+1}} \widehat{p}_f(k) \\
\iff\ & \sum_{k=0}^{n-t} \frac{\binom{n-k}{t}}{\binom{n}{t}} \widehat{p}_f(k) \geq \sum_{k=0}^{n-t-1} \frac{\binom{n-k}{t+1}}{\binom{n}{t+1}} \widehat{p}_f(k) \\
\iff\ & \frac{1}{\binom{n}{t}} \widehat{p}_f(n-t) + \sum_{k=0}^{n-t-1} \left(\frac{\binom{n-k}{t}}{\binom{n}{t}} - \frac{\binom{n-k}{t+1}}{\binom{n}{t+1}} \right) \widehat{p}_f(k) \geq 0
\end{aligned}
$$

$$\iff \quad \frac{1}{\binom{n}{t}}\widehat{p}_f(n-t) + \sum_{k=0}^{n-t-1}\left(\frac{(n-k)!(n-t-1)!}{n!(n-k-t-1)!}\frac{k}{n-t-k}\right)\widehat{p}_f(k) \geq 0. \tag{29}$$

For k in the range 0 to $n-t-1$, it follows that $k/(n-t-k) \geq 0$. So the relation in (29) holds showing that $t\text{-}\mathsf{inf}(f) \leq (t+1)\text{-}\mathsf{inf}(f)$.

□

3.1 Geometric Interpretation

Let H_n be the n-dimensional hypercube, i.e., H_n is a graph whose vertex set is $\mathbb{F}_2^n$ and two vertices $\mathbf{u}$ and $\mathbf{v}$ are connected by an edge if $\mathbf{v}$ can be obtained from $\mathbf{u}$ by flipping one of the bits of $\mathbf{u}$, i.e., if $\mathsf{wt}(\mathbf{u} \oplus \mathbf{v}) = 1$. Let A be a subset of the vertices of H_n and $\overline{A} = \mathbb{F}_2^n \setminus A$. Let $e(A, \overline{A})$ be the number of edges between A and $\overline{A}$. Suppose f is an n-variable Boolean function such that $\mathsf{supp}(f) = A$. It is known that $\mathsf{inf}(f) = e(A, \overline{A})/2^{n-1}$ (see [10] and Page 52 of [11]). This relation is called the edge expansion property of influence. In this section, we obtain a general form of this relation for $t\text{-}\mathsf{inf}(f)$.

Suppose $\mathbf{u}$ is a vertex of H_n and $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ with $T = \mathsf{supp}(\boldsymbol{\alpha})$ and $t = \#T$. Let $\mathbf{v} = \mathbf{u} \oplus \boldsymbol{\alpha}$. Then $\mathbf{v}$ is obtained from $\mathbf{u}$ by flipping the bits of $\mathbf{u}$ which are indexed by T. Since these bits can be flipped in any order, there are a total of $t!$ paths of length t in H_n between $\mathbf{u}$ and $\mathbf{v}$.

Let A be a subset of H_n and f be an n-variable Boolean function such that $\mathsf{supp}(f) = A$. For $\boldsymbol{\alpha} \in \mathbb{F}_2^n$, let $n_{\boldsymbol{\alpha}}$ be the number of paths between A and $\overline{A}$ such that the two ends $\mathbf{u}$ and $\mathbf{v}$ of any such path satisfy $\mathbf{u} \oplus \mathbf{v} = \boldsymbol{\alpha}$. The following result relates $n_{\boldsymbol{\alpha}}$ to the autocorrelation of f at $\boldsymbol{\alpha}$.

Proposition 1 $C_f(\boldsymbol{\alpha}) = 1 - \dfrac{n_{\boldsymbol{\alpha}}}{(\mathsf{wt}(\boldsymbol{\alpha}))!2^{n-2}}$.

Proof: Let $x_{\boldsymbol{\alpha}} = \#\{(\mathbf{u}, \mathbf{v}) : \mathbf{u} \in A,\ \mathbf{v} \in \overline{A},\ \mathbf{u} \oplus \mathbf{v} = \boldsymbol{\alpha}\}$. Then

$$n_{\boldsymbol{\alpha}} \quad = \quad (\mathsf{wt}(\boldsymbol{\alpha}))! x_{\boldsymbol{\alpha}}. \tag{30}$$

Note that $x_{\boldsymbol{\alpha}} = \#\{\mathbf{u} \in \mathbb{F}_2^n : f(\mathbf{u}) = 1 \text{ and } f(\mathbf{u} \oplus \boldsymbol{\alpha}) = 0\}$. Let $g(\mathbf{X}) = f(\mathbf{X}) \oplus f(\mathbf{X} \oplus \boldsymbol{\alpha})$. Then

$$\begin{aligned}
\mathsf{wt}(g) &= \#\{\mathbf{u} \in \mathbb{F}_2^n : \text{ either } f(\mathbf{u}) = 1 \text{ and } f(\mathbf{u} \oplus \boldsymbol{\alpha}) = 0, \text{ or } f(\mathbf{u}) = 0 \text{ and } f(\mathbf{u} \oplus \boldsymbol{\alpha}) = 1\} \\
&= 2\#\{\mathbf{u} \in \mathbb{F}_2^n : f(\mathbf{u}) = 1 \text{ and } f(\mathbf{u} \oplus \boldsymbol{\alpha}) = 0\} \\
&= 2x_{\boldsymbol{\alpha}}.
\end{aligned} \tag{31}$$

From the definition of $C_f(\boldsymbol{\alpha})$ given in (6), it follows that $\mathsf{wt}(g) = 2^{n-1}(1 - C_f(\boldsymbol{\alpha}))$ which combined with (30) and (31) shows the result. □

Remark 6 *Proposition 1 connects auto-correlation to number of paths and consequently provides a geometric interpretation of the auto-correlation function. Combining Proposition 1 with* (7)*, we obtain*

$$(W_f(\boldsymbol{\beta}))^2 \quad = \quad \Delta_{\boldsymbol{\beta}} - \frac{1}{2^{2n-2}} \sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^n} (-1)^{\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle} \frac{n_{\boldsymbol{\alpha}}}{(\mathsf{wt}(\boldsymbol{\alpha}))!},$$

where $\Delta_{\boldsymbol{\beta}} = 1$ if $\boldsymbol{\beta} = \mathbf{0}_n$ and 0 *otherwise. This provides a geometric interpretation of the Walsh transform. To the best of our knowledge, these geometric interpretations of the auto-correlation function and the Walsh transform do not appear earlier in the literature.*

Now we are ready to state the path expansion property of $t\text{-}\mathsf{inf}(f)$.

Theorem 7 *Let f be an n-variable Boolean function and $t \in [n]$. Then*

$$t\text{-}\mathsf{inf}(f) \;=\; 1 - \frac{1}{2^{n+t-2}\binom{n}{t}} \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n} \binom{n-\mathsf{wt}(\boldsymbol{\alpha})}{t-\mathsf{wt}(\boldsymbol{\alpha})} \left(2^{n-2} - \frac{n_{\boldsymbol{\alpha}}}{(\mathsf{wt}(\boldsymbol{\alpha}))!}\right). \tag{32}$$

Proof: Using Proposition 1 in the definition of $\mathsf{inf}_T(f)$ given by (16), we have

$$\begin{aligned}
\mathsf{inf}_T(f) &= 1 - \frac{1}{2^t}\left(\sum_{\boldsymbol{\alpha}\leq\chi_T} C_f(\boldsymbol{\alpha})\right) \\
&= 1 - \frac{1}{2^t}\sum_{k=0}^{t}\left(\sum_{\boldsymbol{\alpha}\leq\chi_T,\mathsf{wt}(\boldsymbol{\alpha})=k} C_f(\boldsymbol{\alpha})\right) \\
&= 1 - \frac{1}{2^t}\sum_{k=0}^{t}\left(\sum_{\boldsymbol{\alpha}\leq\chi_T,\mathsf{wt}(\boldsymbol{\alpha})=k} \left(1 - \frac{n_{\boldsymbol{\alpha}}}{k!2^{n-2}}\right)\right). \qquad (33)
\end{aligned}$$

For $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ with $\mathsf{wt}(\boldsymbol{\alpha}) = k$, there are exactly $\binom{n-k}{t-k}$ subsets T of $[n]$ such that $\alpha \leq \chi_T$. Using this observation, we have

$$\begin{aligned}
t\text{-}\mathsf{inf}(f) &= \frac{1}{\binom{n}{t}} \sum_{T\subseteq[n],\#T=t} \mathsf{inf}_f(T) \\
&= 1 - \frac{1}{2^t\binom{n}{t}}\sum_{k=0}^{t}\left(\sum_{\{\boldsymbol{\alpha}:\mathsf{wt}(\boldsymbol{\alpha})=k\}} \binom{n-k}{t-k}\left(1 - \frac{n_{\boldsymbol{\alpha}}}{k!2^{n-2}}\right)\right) \\
&= 1 - \frac{1}{2^{n+t-2}\binom{n}{t}} \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^n} \binom{n-\mathsf{wt}(\boldsymbol{\alpha})}{t-\mathsf{wt}(\boldsymbol{\alpha})} \left(2^{n-2} - \frac{n_{\boldsymbol{\alpha}}}{(\mathsf{wt}(\boldsymbol{\alpha}))!}\right).
\end{aligned}$$

□

Putting $t = 1$ in (32), we obtain $1\text{-}\mathsf{inf}(f) = \sum_{i\in[n]} n_{\mathbf{e}_i}/(n2^{n-1}) = e(A,\overline{A})/(n2^{n-1})$ which is the previously mentioned edge expansion property for $\mathsf{inf}(f)$ scaled by a factor of n.

3.2 Probabilistic Interpretation

We have defined the influence of a set of variables using the auto-correlation function. In this section, we provide two probabilistic interpretations of the influence.

Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$, with $\#T = t$. We define two probabilities.

$$\begin{aligned}
\mu_f(T) &= \Pr_{\boldsymbol{\alpha}\leq\chi_T,\mathbf{u}\in\mathbb{F}_2^n}[f(\mathbf{u}) \neq f(\mathbf{u}\oplus\boldsymbol{\alpha})], \qquad (34)\\
\nu_f(T) &= \Pr_{\boldsymbol{\beta}\in\mathbb{F}_2^{n-t},\mathbf{w},\mathbf{z}\in\mathbb{F}_2^t}[f_{\boldsymbol{\beta}}(\mathbf{w}) \neq f_{\boldsymbol{\beta}}(\mathbf{z})], \qquad (35)
\end{aligned}$$

where $f_{\boldsymbol{\beta}}$ denotes $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\beta}}$.

Remark 7 *The definition of influence given by Fischer et al. [7] and Blais [4] is $I_f(T)$ and is given by (12). This definition is made in terms of the function $Z(T,\mathbf{x},\mathbf{y})$. For $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^n$, both $\mathbf{x}$ and $Z(T,\mathbf{x},\mathbf{y})$ agree on the bits indexed by $\overline{T}$. In particular, the bits of $\mathbf{y}$ indexed by $\overline{T}$ do not play any role in the probability $\Pr_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq f(Z(T,\mathbf{x},\mathbf{y}))]$. So this probability is the same as the probability of the event arising from choosing $\boldsymbol{\beta}$ uniformly at random from $\mathbb{F}_2^{n-t}$, choosing $\mathbf{w}$ and $\mathbf{z}$ independently and uniformly from $\mathbb{F}_2^t$ and considering $f_{\boldsymbol{\beta}}(\mathbf{w}) \neq f_{\boldsymbol{\beta}}(\mathbf{z})$. This shows that $I_f(T) = \nu_f(T)$.*

The following result relates the above two probabilities to influence.

Theorem 8 *Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$. Then $\mu_f(T) = \nu_f(T) = \mathsf{inf}_f(T)/2$.*

Proof: We separately show that $\mu_f(T) = \mathsf{inf}_f(T)/2$ and $\nu_f(T) = \mathsf{inf}_f(T)/2$. Let $t = \#T$.

$$
\begin{aligned}
\mu_f(T) &= \frac{1}{2^t} \sum_{\boldsymbol{\alpha} \leq \chi_T} \Pr_{\mathbf{u} \in \mathbb{F}_2^n} [f(\mathbf{u}) \neq f(\mathbf{u} \oplus \boldsymbol{\alpha})] \\
&= \frac{1}{2^t} \sum_{\boldsymbol{\alpha} \leq \chi_T} \frac{1 - C_f(\alpha)}{2} \qquad \text{(using (6))} \\
&= \frac{1}{2} \left(1 - \frac{1}{2^t} \sum_{\boldsymbol{\alpha} \leq \chi_T} C_f(\alpha) \right) \\
&= \frac{\mathsf{inf}_f(T)}{2}. \qquad (36)
\end{aligned}
$$

$$
\begin{aligned}
\nu_f(T) &= \frac{1}{2^{n-t}} \sum_{\boldsymbol{\beta} \in \mathbb{F}_2^{n-t}} \Pr_{\mathbf{w}, \mathbf{z} \in \mathbb{F}_2^t} [f_{\boldsymbol{\beta}}(\mathbf{w}) \neq f_{\boldsymbol{\beta}}(\mathbf{z})] \\
&= \frac{1}{2^{n-t}} \sum_{\boldsymbol{\beta} \in \mathbb{F}_2^{n-t}} 2 \times \frac{\mathsf{wt}(f_{\boldsymbol{\beta}})}{2^t} \left(1 - \frac{\mathsf{wt}(f_{\boldsymbol{\beta}})}{2^t} \right) \\
&= \frac{1}{2^{n-1-t}} \sum_{\boldsymbol{\beta} \in \mathbb{F}_2^{n-t}} \mathbb{E}(f_{\boldsymbol{\beta}})(1 - \mathbb{E}(f_{\boldsymbol{\beta}})) \\
&= \frac{1}{2^{n-1-t}} \sum_{\boldsymbol{\beta} \in \mathbb{F}_2^{n-t}} \mathsf{Var}(f_{\boldsymbol{\beta}}) \\
&= \frac{\mathsf{inf}_f(T)}{2} \qquad \text{(from (25)).}
\end{aligned}
$$

□

Using the third point of Theorem 4, a consequence of Theorem 8 is that both the probabilities $\mu_f(T)$ and $\nu_f(T)$ are at most $1/2$.

Remark 8 *From Remark 7 and Theorem 8, it follows that $I_f(T) = \mathsf{inf}_f(T)/2$. Some of the results for $\mathsf{inf}_T(f)$ that we have proved have been obtained for $I_f(T)$ in [7, 4]. In particular, it has been shown that $I_f(T)$ is equal to half the right hand side of* (18) *using a somewhat long proof which is different from the one that we given. Since we defined influence using the auto-correlation function, we were able to use known results on Walsh transform which make our proof simpler. Further, it has been proved in [7, 4] that $I_f(T) \leq I_f(S \cup T) \leq I_f(S) + I_f(T)$, i.e., monotonicity and sub-additivity properties hold for I_f. These properties for $\mathsf{inf}_f(T)$ are covered by Points 4 and 5 of Theorem 4.*

3.3 Juntas

The total influence of the individual variable, i.e. $\mathsf{inf}(f)$, for an s-junta f is known to be at most s. The following result generalises this to provide an upper bound on t-$\mathsf{inf}(f)$ for an s-junta.

Proposition 2 *Let f be an n-variable function which is an s-junta for some $s \in [n]$. For $t \in [n]$, $t\text{-}\mathsf{inf}(f) \leq 1 - \binom{n-s}{t}/\binom{n}{t}$.*

Proof: Let $T \subseteq [n]$ with $\#T = t$. Since f is an s-junta, there is a subset $S \subseteq [n]$, with $\#S \leq s$ such that f is degenerate on the variables indexed by $\overline{S}$. So $\mathsf{inf}_f(T) = 0$ if T is a subset of $\overline{S}$. This means that for $\binom{n-s}{t}$ possible subsets T, $\mathsf{inf}_f(T) = 0$. For the other $\binom{n}{t} - \binom{n-s}{t}$ possible subsets T, $\mathsf{inf}_f(T) \leq 1$. The result now follows from the definition of $t\text{-}\mathsf{inf}(f)$ given in (17). □

For $t = 1$, the upper bound on $1\text{-}\mathsf{inf}(f)$ given by Proposition 2 is s/n which is a scaled version of the bound $\mathsf{inf}(f) \leq s$. Note that the upper bound on $t\text{-}\mathsf{inf}(f)$ increases as t increases and reaches 1 for $t > n - s$.

An n-variable Boolean function f is said to be ϵ-far from being a s-junta if for every n-variable s-junta g, $\Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq g(\mathbf{x})] \geq \epsilon$. It was proved in [4] that if f is ϵ-far from being an s-junta, then for any set $S \subseteq [n]$ with $\#S \leq s$, $I_f(\overline{S}) \geq \epsilon$. The following result provides an equivalent statement for $\mathsf{inf}_f(\overline{S})$. The reason for stating the result in the present work is that our proof is simpler than that in [4].

Proposition 3 *If an n-variable Boolean function f is ϵ-far from being an s-junta, then for any set $S \subseteq [n]$ with $\#S \leq s$, $\mathsf{inf}_f(\overline{S}) \geq 2\epsilon$.*

Proof: Among all the s-juntas on the variables indexed by S, let g be the closest s-junta to f. For $\boldsymbol{\alpha} \in \mathbb{F}_2^s$, let $f_{\boldsymbol{\alpha}} = f_{\mathbf{X}_S \leftarrow \boldsymbol{\alpha}}(\mathbf{X}_{\overline{S}})$ and $g_{\boldsymbol{\alpha}} = g_{\mathbf{X}_S \leftarrow \boldsymbol{\alpha}}(\mathbf{X}_{\overline{S}})$ be functions on $(n-s)$-variables. Since g is a junta on S, it is degenerate on all variables indexed by $\overline{S}$. So $g_{\boldsymbol{\alpha}}$ is a constant function for all $\boldsymbol{\alpha} \in \mathbb{F}_2^s$. Since among all the juntas on the variables indexed by S, g is the closest s-junta to f, it follows that for each $\boldsymbol{\alpha} \in \mathbb{F}_2^s$, $g_{\boldsymbol{\alpha}}$ is either the constant function 0 or the constant function 1 according as $\mathsf{wt}(f_{\boldsymbol{\alpha}}) \leq 2^{n-s-1}$ (i.e. $\mathbb{E}(f_{\boldsymbol{\alpha}}) \leq 1/2$) or $\mathsf{wt}(f_{\boldsymbol{\alpha}}) > 2^{n-s-1}$ (i.e. $\mathbb{E}(f_{\boldsymbol{\alpha}}) > 1/2$) respectively. So

$$\begin{aligned} \Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq g(\mathbf{x})] &= \frac{\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^s} \mathsf{wt}(f_{\boldsymbol{\alpha}} \oplus g_{\boldsymbol{\alpha}})}{2^n} \\ &= \frac{1}{2^s} \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^s} \min\left(\mathbb{E}(f_{\boldsymbol{\alpha}}), 1 - \mathbb{E}(f_{\boldsymbol{\alpha}})\right). \qquad (37) \end{aligned}$$

Since f is ϵ-far from being an s-junta, it follows that $\epsilon \leq \Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq g(\mathbf{x})]$. Using $\mathsf{Var}(f_{\boldsymbol{\alpha}}) = \mathbb{E}(f_{\boldsymbol{\alpha}})(1 - \mathbb{E}(f_{\boldsymbol{\alpha}}))$, it is easy to check that $\min\left(\mathbb{E}(f_{\boldsymbol{\alpha}}), 1 - \mathbb{E}(f_{\boldsymbol{\alpha}})\right) \leq 2\mathsf{Var}(f_{\boldsymbol{\alpha}})$. The result now follows by taking $T = \overline{S}$ in (25) and combining with (37). □

3.4 Cryptographic Properties

An n-variable Boolean function f is δ-close to an s-junta if there is an s-junta g such that $\Pr_{\mathbf{x}\in\mathbb{F}_2^n}[f(\mathbf{x}) \neq g(\mathbf{x})] \leq \delta$. From the point of view of cryptographic design, it is undesirable for f to be δ-close to an s-junta for δ close to 0 and s smaller than n. Since otherwise, g is a good approximation of f and a cryptanalyst may replace f by g which may help in attacking a cipher which uses f as a building block. For example, in linear cryptanalysis the goal is to obtain g to be a linear function on a few variables such that it is a good approximation of f. To defend against such attacks, one usually requires f to not have any good linear approximation on a small number of variables. In particular, an m-resilient function cannot be approximated with probability different from 1/2 by any linear function on m or smaller number of variables. A characterisation of resilient functions in terms of influence is given by Theorem 5 which shows that an n-variable function is m-resilient if and only if $(n-m)\text{-}\mathsf{inf}(f)$ takes its maximum value of 1.

The next result provides a characterisation of bent functions in terms of influence.

Theorem 9 *Let f be an n-variable Boolean function. Then f is bent if and only if for any non-empty $T \subseteq [n]$, $\mathsf{inf}_f(T) = 1 - 2^{\#T}$.*

Proof: First suppose that f is bent. Then it follows from (16) that for any non-empty $T \subseteq [n]$, $\mathsf{inf}_f(T) = 1 - 2^{\#T}$.

Next we prove the converse. From (16), it follows that $\mathsf{inf}_f(T) = 1 - 2^{\#T}$ if and only if

$$\sum_{\mathbf{0}_n \neq \boldsymbol{\alpha} \leq \chi_T} C_f(\boldsymbol{\alpha}) \quad = \quad 0. \tag{38}$$

For $0 \leq i \leq 2^n - 1$, let $\mathsf{bin}_n(i)$ denote the n-bit binary representation of i. Let $\mathbf{M}$ be the $(2^n - 1) \times (2^n - 1)$ matrix whose rows and columns are indexed by the integers in $[2^n - 1]$ such that the (i, j)-th entry of $\mathbf{M}$ is 1 if $\mathsf{bin}_n(j) \leq \mathsf{bin}_n(i)$ and otherwise the entry is 0. It is easy to verify that $\mathbf{M}$ is a lower triangular matrix whose diagonal elements are all 1. In particular, $\mathbf{M}$ is invertible.

Let $\mathbf{C} = [C_f(\mathsf{bin}_n(i))]_{i \in [2^n - 1]}$ be the vector of auto-correlations of f at all the non-zero points in $\mathbb{F}_2^n$. The set of relations of the form (38) for all non-empty $T \subseteq [n]$ can be expressed as $\mathbf{M}\mathbf{C}^\top = \mathbf{0}^\top$. Since $\mathbf{M}$ is invertible, it follows that $\mathbf{C} = \mathbf{0}$, i.e. $C_f(\boldsymbol{\alpha}) = 0$ for all non-zero $\boldsymbol{\alpha} \in \mathbb{F}_2^n$. From (7), it now follows that $W_f(\boldsymbol{\beta}) = \pm 2^{n/2}$ for all $\boldsymbol{\beta} \in \mathbb{F}_2^n$ which shows that f is bent. □

For functions satisfying propogation characteristics, somewhat less can be said. From (16), it follows that if f satisfies PC(k) then for any subset $\emptyset \neq T \subseteq [n]$ with $\#T = t \leq k$, $\mathsf{inf}_f(T) = 1 - 2^{-t}$ and so $t\text{-}\mathsf{inf}(f) = 1 - 2^{-t}$.

3.5 The Fourier Entropy/Influence Conjecture

The Fourier entropy $H(f)$ of f is defined to be the entropy of the probability distribution $\{W_f^2(\boldsymbol{\alpha})\}$ and is equal to

$$H(f) \quad = \quad -\sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^n} W_f^2(\boldsymbol{\alpha}) \log W_f^2(\boldsymbol{\alpha}), \tag{39}$$

where log denotes $\log_2$ and the expressions $0 \log 0$ and $0 \log \frac{1}{0}$ are to be interpreted as 0. For $t \in [n]$, let

$$\rho_t(f) \quad = \quad \frac{H(f)/n}{t\text{-}\mathsf{inf}(f)}. \tag{40}$$

The Fourier entropy/influence conjecture [8] states that there is a universal constant C, such that for all Boolean functions f, $\rho_1(f) \leq C$. A general form of this conjecture is that there is a universal constant C_t, such that for all Boolean functions f and $t \in [1, n]$, $\rho_t(f) \leq C_t$. Since $t\text{-}\mathsf{inf}(f)$ increases monotonically with t, it follows that $\rho_t(f)$ decreases monotonically with t. So if the FEI conjecture holds, then the conjecture on $\rho_t(f)$ also holds for $t \geq 1$. The converse, i.e if the conjecture holds for some ρ_t with $t > 1$ then it also holds for ρ_1, need not be true.

Remark 9 *A weaker variant of the FEI conjecture replaces $H(f)$ by the min-entropy of the distribution $\widehat{p}_f(\omega)$. In a similar vein, one may consider the conjecture on $\rho_t(f)$ to be a weaker variant of the FEI conjecture.*

4 Pseudo-Influence

In this section, we introduce a quantity which we call the pseduo-influence of a Boolean function. The main reason for considering this notion is that it turns out to be the same as the notion of influence $J_f(T)$ introduced in [16]. We make a thorough study of the basic properties of pseudo-influence. A consequence of this study is that pseudo-influence does not satisfy some of the basic desiderata that a notion of influence may be expected to satisfy, which is why we call it pseudo-influence. This shows that even though the quantity was termed 'influence' in [16], it is not a satisfactory notion of influence.

Suppose $f(\mathbf{X})$ is an n-variable Boolean function where $\mathbf{X} = (X_1, \ldots, X_n)$ and $\emptyset \neq T = \{i_1, \ldots, i_t\} \subseteq [n]$. We define pseudo-influence $\mathsf{PI}_f(T)$ of the set of variables $\{X_{i_1}, \ldots, X_{i_t}\}$ indexed by T on f in the following manner.

$$\mathsf{PI}_f(T) \quad = \quad \frac{1}{2^{\#T}} \left(\sum_{\boldsymbol{\alpha} \leq \chi_T} (-1)^{\mathsf{wt}(\alpha)} C_f(\boldsymbol{\alpha}) \right). \tag{41}$$

For a singleton set $T = \{i\}$, $\mathsf{PI}_f(T) = \mathsf{inf}_f(T) = \mathsf{inf}_i(f)$.

Let f be an n-variable function and t be an integer with $1 \leq t \leq n$. Then the t-pseudo-influence of f is the total pseudo-influence (scaled by $\binom{n}{t}$) obtained by summing the pseudo-influence of every set of t variables on the function f, i.e.,

$$t\text{-}\mathsf{PI}(f) \quad = \quad \frac{\sum_{\{T \subseteq [n]: \#T = t\}} \mathsf{PI}_f(T)}{\binom{n}{t}}. \tag{42}$$

The characterisation of pseudo-influence in terms of the Walsh transform is given by the following result.

Theorem 10 *Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$. Then*

$$\mathsf{PI}_f(T) \quad = \quad \sum_{\mathbf{u} \geq \chi_T} \left(W_f(\mathbf{u})\right)^2. \tag{43}$$

Consequently, for an integer t with $1 \leq t \leq n$,

$$t\text{-}\mathsf{PI}(f) \quad = \quad \frac{1}{\binom{n}{t}} \sum_{k=t}^{n} \binom{k}{t} \widehat{p}_f(k) \tag{44}$$

Proof: Let $\#T = t$. Let $E = \{\boldsymbol{\beta} \in \mathbb{F}_2^n : \boldsymbol{\beta} \leq \chi_{\overline{T}}\}$. Then $\#E = 2^{n-t}$ and $E^{\perp} = \{\boldsymbol{\alpha} \in \mathbb{F}_2^n : \boldsymbol{\alpha} \leq \chi_T\}$. From (41) and putting $\mathbf{a} = \mathbf{1}_n$, $\mathbf{b} = \mathbf{0}_n$ and $\psi = C_f$ in (2) we obtain the following:

$$\mathsf{PI}_f(T) \quad = \quad \frac{1}{2^t} \sum_{\boldsymbol{\alpha} \leq \chi_T} (-1)^{\mathsf{wt}(\boldsymbol{\alpha})} C_f(\boldsymbol{\alpha}) = \frac{1}{2^t} \sum_{\boldsymbol{\alpha} \leq \chi_T} (-1)^{\langle \mathbf{1}_n, \boldsymbol{\alpha} \rangle} C_f(\boldsymbol{\alpha}) = \sum_{\boldsymbol{\beta} \in \mathbf{1}_n + E} \widehat{C_f}(\boldsymbol{\beta}) = \sum_{\boldsymbol{\beta} \geq \chi_T} \widehat{C_f}(\boldsymbol{\beta}).$$

The result now follows from (7).

The expression for t-$\mathsf{PI}(f)$ can be seen as follows.

$$t\text{-}\mathsf{PI}(f) \quad = \quad \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} \sum_{\{\mathbf{u}: \mathsf{wt}(\mathbf{u}) = k\}} \binom{k}{t} \left(W_f(\mathbf{u})\right)^2$$

$$\begin{aligned} &= \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} \binom{k}{t} \sum_{\{\mathbf{u}:\mathsf{wt}(\mathbf{u})=k\}} (W_f(\mathbf{u}))^2 \\ &= \frac{1}{\binom{n}{t}} \sum_{k=1}^{n} \binom{k}{t} \widehat{p}_f(k) \\ &= \frac{1}{\binom{n}{t}} \sum_{k=t}^{n} \binom{k}{t} \widehat{p}_f(k). \qquad (45) \end{aligned}$$

□

The following result states the basic properties of the pseudo-influence.

Theorem 11 *Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq S \subseteq [n]$. Then*

1. $0 \leq \mathsf{PI}_f(T) \leq 1$.
2. *If the function f is degenerate on the variables indexed by T, then $\mathsf{PI}_f(T) = 0$.*
3. $\mathsf{PI}_f(S) \leq \mathsf{PI}_f(T)$.

Proof: The first point follows from Theorem 10 and Parseval's theorem. The third point also follows from Theorem 1.

Consider the second point. Suppose π is any permutation of $[n]$ and define $g(\mathbf{X})$ to be the function $f(X_{\pi(1)}, \ldots, X_{\pi(n)})$. Then f is degenerate on the variables indexed by a set $U = \{i_1, \ldots, i_t\}$ if and only if g is degenerate on the variables indexed by the set $V = \{\pi(i_1), \ldots, \pi(i_t)\}$. Also, $\mathsf{inf}_f(U) = \mathsf{inf}_g(V)$. In view of this, we consider the set T to be $\{1, \ldots, t\}$.

For $\boldsymbol{\alpha} \in \mathbb{F}_2^t$ and $\mathbf{Y} = (X_{t+1}, \ldots, X_n)$, let $f_{\boldsymbol{\alpha}}(\mathbf{Y}) = f(\boldsymbol{\alpha}, \mathbf{Y})$. The function f is degenerate on the variables indexed by T, if and only if $f_{\boldsymbol{\alpha}}(\mathbf{Y}) = f_{\boldsymbol{\beta}}(\mathbf{Y})$ for any $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}_2^t$. We show that the latter condition is equivalent to $f(\mathbf{X}) = f(\mathbf{X} \oplus \boldsymbol{\gamma})$ for any $\boldsymbol{\gamma} \leq \chi_T$. Note that by the choice of T, we have that for $\boldsymbol{\gamma} \leq \chi_T$, $\boldsymbol{\gamma} = (\boldsymbol{\delta}, \mathbf{0})$ for some $\boldsymbol{\delta} \in \mathbb{F}_2^t$. So it is sufficient to show that $f(\boldsymbol{\alpha}, \mathbf{Y}) = f((\boldsymbol{\alpha}, \mathbf{Y}) \oplus (\boldsymbol{\delta}, \mathbf{0}))$ for all $\boldsymbol{\alpha} \in \mathbb{F}_2^t$. The latter condition is equivalent to $f_{\boldsymbol{\alpha}}(\mathbf{Y}) = f_{\boldsymbol{\alpha} \oplus \boldsymbol{\delta}}(\mathbf{Y}) = f_{\boldsymbol{\beta}}(\mathbf{Y})$ where $\boldsymbol{\beta} = \boldsymbol{\alpha} \oplus \boldsymbol{\delta}$. This completes the proof that f is degenerate on the variables indexed by T if and only if $f(\mathbf{X}) = f(\mathbf{X} \oplus \boldsymbol{\gamma})$ for all $\boldsymbol{\gamma} \leq \chi_T$.

The condition $f(\mathbf{X}) = f(\mathbf{X} \oplus \boldsymbol{\gamma})$ for all $\boldsymbol{\gamma} \leq \chi_T$ is equivalent to $C_f(\boldsymbol{\gamma}) = 1$ for all $\boldsymbol{\gamma} \leq \chi_T$. So f is degenerate on the set of variables indexed by T if and only if $C_f(\boldsymbol{\gamma}) = 1$ for all $\boldsymbol{\gamma} \leq \chi_T$. Using this in the definition of pseudo-influence given by (41), we obtain the the second point. □

Theorem 11 states that if f is degenerate on the variables indexed by T, then $\mathsf{PI}_f(T) = 0$. The converse, however, is not true. Suppose f is an n-variable function such that $W_f(\mathbf{1}_n) = 0$ and let $T = [n]$. Then from (43), $\mathsf{PI}_f(T) = 0$. This example can be generalised. Suppose g is an n-variable, m-resilient function and let $f(\mathbf{X}) = \langle \mathbf{1}, \mathbf{X} \rangle \oplus g(\mathbf{X})$. Using (3), we have $W_f(\boldsymbol{\alpha}) = W_g(\mathbf{1} \oplus \boldsymbol{\alpha})$ for all $\boldsymbol{\alpha} \in \mathbb{F}_2^n$. Since, g is m-resilient, $W_g(\boldsymbol{\omega}) = 0$ for all $\boldsymbol{\omega}$ with $\mathsf{wt}(\boldsymbol{\omega}) \leq m$. So $W_f(\boldsymbol{\alpha}) = 0$ for all $\boldsymbol{\alpha}$ with $\mathsf{wt}(\boldsymbol{\alpha}) \geq n - m$. Consequently, for any $\emptyset \neq T \subseteq [n]$, with $\#T \geq n - m$, it follows that $\mathsf{PI}_f(T) = 0$. There are known examples of non-degenerate resilient functions. See for example [14].

Remark 10 *By the above discussion, $\mathsf{PI}_f(T)$ can be zero even if f is non-degenerate on the variables indexed by T. Further, the third point of Theorem 11 shows that $\mathsf{PI}_f(T)$ is non-increasing with T. As a consequence, sub-additivity does not hold for $\mathsf{PI}_f(T)$. So $\mathsf{PI}_f(T)$ violates some of the basic desiderata that one may expect a notion of influence to fulfill.*

For $\mathbf{u} \in \mathbb{F}_2^n$ and $\emptyset \neq T \subseteq [n]$, $\mathbf{u} \geq \chi_T$ is equivalent to $\mathsf{supp}(\mathbf{u}) \supseteq T$ which in particular implies that $\mathsf{supp}(u) \cap T \neq \emptyset$. So from (18) and (43), we have the following result which states that influence is always at least as large as the pseudo-influence.

Proposition 4 *Let f be an n-variable Boolean function and $\emptyset \neq T \subseteq [n]$. Then $\mathsf{inf}_f(T) \geq \mathsf{PI}_f(T)$.*

Theorem 12 *Let $f(\mathbf{X})$ be an n-variable Boolean function where $\mathbf{X} = (X_1, \ldots, X_n)$ and t be an integer with $1 \leq t \leq n$.*

1. *t-$\mathsf{PI}(f)$ takes its maximum value of 1 if and only if f is of the form $f(\mathbf{X}) = \langle \mathbf{1}, \mathbf{X} \rangle$.*
2. *t-$\mathsf{PI}(f)$ takes its minimum value of 0 if and only if f is of the form $f(\mathbf{X}) = \langle \mathbf{1}, \mathbf{X} \rangle \oplus g(\mathbf{X})$, where $g(\mathbf{X})$ is $(n-t)$-resilient.*

Proof: From (44), t-$\mathsf{PI}(f)$ takes its maximum value of 1 if and only if

$$\sum_{k=t}^{n} \binom{k}{t} \widehat{p}_f(k) \quad = \quad \binom{n}{t}. \tag{46}$$

If $f(\mathbf{X}) = \langle \mathbf{1}, \mathbf{X} \rangle$, then $\widehat{p}_f(n) = 1$ and $\widehat{p}_f(k) = 0$ for $0 \leq k \leq n-1$. On the other hand, if $f(\mathbf{X}) \neq \langle \mathbf{1}, \mathbf{X} \rangle$, then $\widehat{p}_f(n) < 1$ and we have

$$\begin{aligned}
& \binom{t}{t}\widehat{p}_f(t) + \binom{t+1}{t}\widehat{p}_f(t+1) + \cdots + \binom{n}{t}\widehat{p}_f(n) \\
\leq \quad & \binom{n-1}{t}(\widehat{p}_f(0) + \cdots + \widehat{p}_f(n-1)) + \binom{n}{t}\widehat{p}_f(n) \\
= \quad & \binom{n-1}{t}(1 - \widehat{p}_f(n)) + \binom{n}{t}\widehat{p}_f(n) < \binom{n}{t}.
\end{aligned}$$

This completes the proof of the first point.

For the second point, from (44), one may note that the values $\widehat{p}_f(0), \ldots, \widehat{p}_f(t-1)$ do not affect the expression for t-$\mathsf{PI}(f)$. So t-$\mathsf{PI}(f) = 0$ if and only if $\widehat{p}_f(t) = \cdots = \widehat{p}_f(n) = 0$. The latter condition holds if and only if f is of the stated form. □

From the second point of Theorem 12, it is possible to obtain examples of non-degenerate functions f such that t-$\mathsf{PI}(f)$ is 0.

Remark 11 *The quantity $J_f(T)$ (see (14)) was put forward by Tal [16] as a measure of influence of the set of variables indexed by T on the function f. It was shown in [16] that $J_f(T)$ is equal to the right hand side of (43). So it follows that $J_f(T) = \mathsf{PI}_f(T)$. This is somewhat surprising since the definition of $J_f(T)$ given in (14) and that of $\mathsf{PI}_f(T)$ given in (41) are very different. It is perhaps only through the characterisations of both these quantities in terms of the Walsh transform that they can be seen to be equal. The quantity $\sum_{\{T:\#T=t\}} J_f(T)$ was considered in [16] and the expression (44) was also obtained in [16]. Since $J_f(T) = \mathsf{PI}_f(T)$, from Remark 10 it follows that $J_f(T)$ is not a satisfactory notion of influence.*

5 Ben-Or and Linial Definition of Influence

The first notion of influence of a set of variables on a Boolean function was proposed by Ben-Or and Linial in [2]. In this section, we introduce this notion, prove some of its basic properties and show its relationship with the notion of influence defined in Section 3.

For an n-variable function f and $\emptyset \neq T \subseteq [n]$, with $t = \#T$, the notion of influence introduced in [2] is $\mathcal{I}_f(T)$ and is given by (11). For $t \in [n]$, we define

$$t\text{-}\mathcal{I}(f) \;=\; \frac{\sum_{\{T\subseteq[n]:\#T=t\}} \mathcal{I}_f(T)}{\binom{n}{t}}. \tag{47}$$

The following result provides an alternative description of $\mathcal{I}_f(T)$.

Proposition 5 *For an n-variable function f and $\emptyset \neq T \subseteq [n]$, with $t = \#T$,*

$$\begin{aligned} \mathcal{I}_f(T) &= 1 - \frac{\#\left\{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 = 1\right\}}{2^{n-t}} & (48)\\ &= \frac{\#\left\{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 \neq 1\right\}}{2^{n-t}}, & (49) \end{aligned}$$

where $f_{\boldsymbol{\alpha}}$ denotes $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}$.

Proof: From (11), it clearly follows that

$$\begin{aligned} \mathcal{I}_f(T) &= 1 - \frac{\#\{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : f_{\boldsymbol{\alpha}} \text{ is constant}\}}{2^{n-t}}\\ &= 1 - \frac{\#\{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : \mathsf{wt}(f_{\boldsymbol{\alpha}}) = 0, \text{ or } 2^t\}}{2^{n-t}}\\ &= 1 - \frac{\#\{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t) = \pm 1\}}{2^{n-t}}. \end{aligned}$$

This shows (48), and (49) follows directly from (48). □

Some basic properties of $\mathcal{I}_f(T)$ are as follows.

Theorem 13 *Let f be an n-variable function and $\emptyset \neq T \subseteq S \subseteq [n]$. Let $\#T = t$.*

1. $0 \leq \mathcal{I}_f(T) \leq 1$.
2. $\mathcal{I}_f(T) = 0$ *if and only if f is degenerate on the variables indexed by T.*
3. $\mathcal{I}_f(T) = 1$ *if and only if $f_{\boldsymbol{\alpha}}$ is a non-constant function for every $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, where $f_{\boldsymbol{\alpha}}$ denotes $f_{\mathbf{X}_{\overline{T}}\leftarrow\boldsymbol{\alpha}}$. In particular, if $T = [n]$, then $\mathcal{I}_f(T) = 1$.*
4. $\mathcal{I}_f(T) \leq \mathcal{I}_f(S)$.

Proof: The first point is obvious.

For the second point, using (48) note that $\mathcal{I}_f(T) = 0$ if and only if for every $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, $W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t) = \pm 1$, i.e., if and only if $\mathsf{wt}(f_{\boldsymbol{\alpha}}) = 0, \text{ or } 2^t$, i.e., if and only if $f_{\boldsymbol{\alpha}}$ is constant. The latter condition holds if and only if the variables indexed by T have no effect on the value of f, i.e., if and only if f is degenerate on the variables indexed by T.

To see the third point, note that $\mathcal{I}_f(T) = 1$ if and only if for every $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 \neq 1$, which holds if and only if $f_{\boldsymbol{\alpha}}$ is a non-constant function.

Let $\#S = s$. For the fourth point, it is sufficient to consider $s = t + 1$, since otherwise, we may define a sequence of sets $T \subset S_1 \subset S_2 \subset \cdots \subset S$, with $\#T + 1 = \#S_1$, $\#S_1 + 1 = \#S_2$, ..., and argue $\mathcal{I}_f(T) \leq \mathcal{I}_f(S_1) \leq \cdots \leq \mathcal{I}_f(S)$. Further, without loss of generality, we assume $T = \{n - t + 1, \ldots, n\}$

and $S = \{n-t, \ldots, n\}$ as otherwise, we may apply an appropriate permutation on the variables to ensure this condition. Then $\overline{T} = \{1, \ldots, n-t\}$ and $\overline{S} = \{1, \ldots, n-t-1\}$.

Let $\mathcal{T} = \{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : f_{\boldsymbol{\alpha}} \text{ is constant}\}$ and $\mathcal{S} = \{\boldsymbol{\beta} \in \mathbb{F}_2^{n-t-1} : f_{\boldsymbol{\beta}} \text{ is constant}\}$, where $f_{\boldsymbol{\beta}}$ is a shorthand for $f_{\mathbf{X}_{\overline{S}} \leftarrow \boldsymbol{\beta}}$. Note that if $\boldsymbol{\beta} \in \mathcal{S}$, then $(\boldsymbol{\beta}, 0), (\boldsymbol{\beta}, 1) \in \mathcal{T}$. So $\#\mathcal{T} \geq 2\#\mathcal{S}$ which implies

$$\frac{\#\mathcal{T}}{2^{n-t}} \geq \frac{2\#\mathcal{S}}{2^{n-t}} \geq \frac{\#\mathcal{S}}{2^{n-t-1}}.$$

Consequently,

$$\mathcal{I}_f(T) = 1 - \frac{\#\mathcal{T}}{2^{n-t}} \leq 1 - \frac{\#\mathcal{S}}{2^{n-t-1}} = \mathcal{I}_f(S).$$

□

Remark 12 *We note that the sub-additivity property does not hold for $\mathcal{I}_f(T)$. As an example, consider a 6-variable function f which maps $\mathbf{0}_6$ to 1 and all other elements of $\mathbb{F}_2^6$ to 0; let $S = \{4, 5, 6\}$ and $T = \{2, 3, 6\}$. Then $\mathcal{I}_f(S \cup T) = 1/2 > 1/8 + 1/8 = \mathcal{I}_f(S) + \mathcal{I}_f(T)$.*

Next, we show that the Ben-Or and Linial notion of influence is always at least as much as the notion of influence defined in (16).

Theorem 14 *Let f be an n-variable function and $\emptyset \neq T \subseteq [n]$. Then $\mathsf{inf}_f(T) \leq \mathcal{I}_f(T)$. Further, equality holds if and only if $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 = 0$ or 1 for each $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, where $f_{\boldsymbol{\alpha}}$ denotes $f_{\mathbf{X}_{\overline{T}} \leftarrow \boldsymbol{\alpha}}$.*

Proof: We rewrite (24) in the following form.

$$\mathsf{inf}_f(T) = \frac{1}{2^{n-t}} \sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}} \left(1 - (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2\right). \tag{50}$$

Consider the expressions for $\mathsf{inf}_f(T)$ and $\mathcal{I}_f(T)$ given by (50) and (49) respectively. Both the expressions are sums over $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$. Suppose $\boldsymbol{\alpha}$ is such that $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 = 1$. The contribution of such an $\boldsymbol{\alpha}$ to both (50) and (49) is 0. Next suppose $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 \neq 1$; the contribution of such an $\boldsymbol{\alpha}$ to (49) is 1 and the contribution to (50) is at most 1, and the value 1 is achieved if and only if $W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t) = 0$. □

One may compare the properties of $\mathcal{I}_f(T)$ given by Theorem 13 to the desiderata that a notion of influence may be expected to satisfy (see the discussion before Theorem 4). The measure $\mathcal{I}_f(T)$ satisfies some of the desiderata, namely, it is between 0 and 1; takes the value 0 if and only if f is degenerate on the variables indexed by T; and it is monotone increasing with the size of T. On the other hand, as noted above, it does not satisfy the sub-additivity property.

Compared to $\mathsf{inf}_f(T)$, the value of $\mathcal{I}_f(T)$ rises quite sharply. To see this, it is useful to view the following expressions for the two quantities.

$$2^{n-t} \times \mathsf{inf}_f(T) = \sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}} \left(1 - (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2\right), \tag{51}$$

$$2^{n-t} \times \mathcal{I}_f(T) = \#\left\{\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t} : (W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 \neq 1\right\}. \tag{52}$$

Suppose $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$ is such that $f_{\boldsymbol{\alpha}}$ is a non-constant function, so that $(W_{f_{\boldsymbol{\alpha}}}(\mathbf{0}_t))^2 \neq 1$. Then such an $\boldsymbol{\alpha}$ contributes 1 to (52), while it contributes a value which is at most 1 to (51). More generally, $\boldsymbol{\alpha}$ contributes either 0 or 1 to (52) according as $f_{\boldsymbol{\alpha}}$ is constant or non-constant; on the other hand, the contribution of $\boldsymbol{\alpha}$ to (51) is more granular. Consequently, the value of $\mathcal{I}_f(T)$ rises more sharply than the value of $\mathsf{inf}_f(T)$. In particular, if f and g are two distinct functions such that for all $\boldsymbol{\alpha}$, both $f_{\boldsymbol{\alpha}}$ and $g_{\boldsymbol{\alpha}}$ are non-constant functions, then both $\mathcal{I}_f(T)$ and $\mathcal{I}_g(T)$ will be necessarily be equal to 1, whereas the values of $\mathsf{inf}_f(T)$ and $\mathsf{inf}_g(T)$ are neither necessarily 1 nor necessarily equal. In other words, the discerning power of $\mathcal{I}_f(T)$ as a measure of influence is less than that of $\mathsf{inf}_f(T)$, i.e., $\mathcal{I}_f(T)$ is a more coarse measure of influence. So while both $\mathsf{inf}_f(T)$ and $\mathcal{I}_f(T)$ share some intuitive basic properties expected of a definition of influence, the facts that $\mathcal{I}_f(T)$ does not satisfy sub-additivity and has less discerning power make it a less satisfactory measure of influence compared to $\mathsf{inf}_f(T)$.

The following result characterises the minimum and maximum values of t-$\mathcal{I}(f)$.

Theorem 15 *Let f be an n-variable Boolean function and t be an integer with $1 \leq t \leq n$.*

1. *t-$\mathcal{I}(f)$ takes its maximum value of 1 if and only if for every subset T of $[n]$ of size t, and for every $\boldsymbol{\alpha} \in \mathbb{F}_2^{n-t}$, the function $f_{\mathbf{X}_{\overline{T}} \leftarrow \boldsymbol{\alpha}}(\mathbf{X}_T)$ is non-constant.*
2. *t-$\mathcal{I}(f)$ takes its minimum value of 0 if and only if f is a constant function.*

Proof: The proof of the first point follows from the third point of Theorem 13.

For the second point, we note that if f is a constant function, then from (11), $\mathcal{I}_f(T) = 0$ for every subset T of $[n]$ and so t-$\mathcal{I}(f)$. On the other hand, if t-$\mathcal{I}(f) = 0$, then from Theorem 14, it follows that t-$\mathsf{inf}(f) = 0$ and so from the second point of Theorem 5 we have that f is a constant function. □

Remark 13 *Upper bounds on $\mathcal{I}_f(T)$ for T with bounded size have been proved in [1]. Since $\mathsf{inf}_f(T) \leq \mathcal{I}_f(T)$, it follows that these upper bounds also hold for $\mathsf{inf}_f(T)$.*

6 Conclusion

We introduced a definition of influence of a set of variables on a Boolean function using the auto-correlation function. The basic theory around the notion of influence has been carefully developed and several well known results on the influence of a single variable have been generalised. New characterisations of resilient and bent functions in terms of influence have been obtained. A previously introduced [7, 4] measure of influence of a set of variables is shown to be half the value of the influence that we introduce. We also defined a notion of pseudo-influence, argued that it is not a satisfactory measure of influence and showed that pseudo-influence is equal to a measure of influence previously defined in [16]. Finally, we studied in details the definition of influence given by Ben-Or and Linial [2] and brought out its relation to the auto-correlation based notion of influence.

Acknowledgement

We thank the reviewers of an earlier version for providing helpful comments.

References

[1] Miklós Ajtai and Nathal Linial. The influence of large coalitions. *Combinatorica*, 13(2):129–145, 1993.

[2] Michael Ben-Or and Nathan Linial. Collective coin flipping. *Adv. Comput. Res.*, 5:91–115, 1989.

[3] Aniruddha Biswas and Palash Sarkar. Separation results for boolean function classes. *Cryptography Commun.*, 13(3):451458, may 2021.

[4] Eric Blais. Testing juntas nearly optimally. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 151–158. ACM, 2009.

[5] Anne Canteaut, Claude Carlet, Pascale Charpin, and Caroline Fontaine. Propagation characteristics and correlation-immunity of highly nonlinear boolean functions. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 507–522. Springer, 2000.

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

[7] Eldar Fischer, Guy Kindler, Dana Ron, Shmuel Safra, and Alex Samorodnitsky. Testing juntas. In *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*, pages 103–112. IEEE Computer Society, 2002.

[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] Gil Kalai. Boolean functions: Influence, threshold and noise. In *European Congress of Mathematics (2016)*, pages 85–110. European Mathematical Society, 2018.

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

[12] Bart Preneel, Werner Van Leekwijck, Luc Van Linden, René Govaerts, and Joos Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques*, volume 473, pages 161–173. Springer, 1990.

[13] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[14] Palash Sarkar and Subhamoy Maitra. Construction of nonlinear resilient boolean functions using "small" affine functions. *IEEE Trans. Inf. Theory*, 50(9):2185–2193, 2004.

[15] Thomas Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inf. Theory*, 30(5):776–780, 1984.

[16] Avishay Tal. Tight bounds on the Fourier spectrum of AC0. In Ryan O'Donnell, editor, *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, volume 79 of *LIPIcs*, pages 15:1–15:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[17] Guo-Zhen Xiao and James L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inf. Theory*, 34(3):569–571, 1988.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il