On the Fourier Entropy–Influence Conjecture for Boolean Plateaued Functions

Vladimir N. Potapov [1]

[1]Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Istanbul,Türkiye,
e-mail: quasigroup349@gmail.com

Abstract

We prove the following inequality for Boolean functions:

$$2\sum_{x\in\mathbb{F}_2^n} f(x)\mathrm{wt}(x) \geq \mathrm{wt}(f)(n-\deg_{alg}(f)).$$

Using this inequality, we establish the Fourier Entropy–Influence (FEI) conjecture for Boolean plateaued functions. In particular, we show that the sharp FEI constant for the class of plateaued functions is 4. We also prove the FEI conjecture for partially bent functions and show that the corresponding sharp constant is 2. Finally, we derive several estimates for the p-biased distribution on the Boolean hypercube.
Keywords: Fourier entropy, total influence, average sensitivity, plateaued function, algebraic degree, Reed–Muller code, p-biased distribution.

1 Introduction

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Throughout the paper, we use the *Walsh–Hadamard (Fourier) transform* of f, normalized by the factor 2^{-n}. It is defined by

$$W_f(z) = \frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus(x,z)},$$

where $(x,z) = x_1z_1 \oplus \cdots \oplus x_nz_n$. Thus, $W_f : \mathbb{F}_2^n \to \mathbb{R}$. By Parseval's identity, $\sum_{z\in\mathbb{F}_2^n} W_f^2(z) = 1$. Therefore, the values $W_f^2(z)$ define a probability distribution on $\mathbb{F}_2^n$. The *Fourier entropy* of f is defined by $H(f) = \sum_{z\in\mathbb{F}_2^n} W_f^2(z)\log_2\frac{1}{W_f^2(z)}$. The quantity $I(f) = \sum_{z\in\mathbb{F}_2^n} W_f^2(z)\mathrm{wt}(z)$ is called the *total influence* or *average sensitivity* of f, where $\mathrm{wt}(z)$ denotes the Hamming weight of z.

The Fourier Entropy–Influence (FEI) conjecture was introduced by Friedgut and Kalai in 1996 [4]. The conjecture asserts the existence of a universal constant C such that $H(f) \leq C\cdot I(f)$ for every Boolean function f. Restricted versions of the FEI conjecture have been proved for several important classes of Boolean functions (see [6]). In particular, the FEI conjecture is true for monomial Boolean functions with $C = 4$, which is the best possible (see [5]). Recently, Li and Tang [6] constructed s-plateaued functions whose FEI constants are strictly smaller than 4, but arbitrarily close to 4.

In the present paper, we prove the following inequality

$$2\sum_{x\in\mathbb{F}_2^n} f(x)\mathrm{wt}(x) \geq \mathrm{wt}(f)(n-\deg_{alg}(f)), \tag{1}$$

which relates the average Hamming weight of the support of a Boolean function to its algebraic degree. Here $\mathrm{wt}(x)$ is the Hamming weight of $x \in \mathbb{F}_2^n$ and $\mathrm{wt}(f) = \sum_{x\in\mathbb{F}_2^n} f(x)$, i.e., $\mathrm{wt}(f)$ is the total number of values 1 of a Boolean function f.

Using this inequality, we prove that the FEI constant for plateaued functions is at most 4 (Theorem 2). Combined with the recent construction of plateaued functions whose Fourier min-entropy/influence ratios approach 4 [6], this shows that the sharp FEI constant for the class of plateaued functions is exactly 4. Furthermore, we prove the FEI conjecture for partially bent functions and show that the sharp FEI constant in this case is equal to 2 (Theorem 1). Additional relations between total influence and algebraic degree can be found in [7].

Local probabilistic testing is a powerful instrument to determine an algebraic degree of Boolean functions [8]. Codewords of a Reed–Muller code of order d correspond to Boolean functions of degree at most d. A code is locally testable if there is a way to indicate with high probability that a vector is far enough from any codeword by checking only a small number of the vector's bits. In [1] authors proved that the Reed–Muller codes of constant order are locally testable. In [3] the authors proposed to use the p-biased distribution $\mu(p)$ instead the standard uniform distribution $\mu(1/2)$ distribution on the Boolean hypercube. In Section 5 we consider how useful new inequality for an estimating of probabilities under $\mu(p)$.

2 FEI Conjecture for Plateaued Functions

A Boolean function is called *s-plateaued* if $|W_f(z)| = 2^{\frac{s-n}{2}}$ (equivalently $W_f^2(z) = 2^{s-n}$) or 0 for every $z \in \mathbb{F}_2^n$. In the case $s = 0$, an s-plateaued function is called *bent*. An s-plateaued function f is called *partially bent* function if $\mathrm{supp}(W_f)$ is an affine subspace. The following statements are immediate

Proposition 1 *$H(f) = n - s$ for each s-plateaued function f.*

Proof. Since every nonzero Walsh coefficient satisfies $W_f^2(z) = 2^{s-n}$, and the support size equals 2^{n-s}, we obtain $H(f) = 2^{s-n} \cdot 2^{n-s} \cdot (n-s)$. □

Corollary 1 *$H(f) = 2I(f)$ holds for every bent function f.*

It is well known that all directed derivatives of any bent function are balanced. In [5], the FEI conjecture was proven with constant 2 under weaker conditions: it is sufficient that an n-variable function possesses n linearly independent directions whose derivatives are balanced.

Proposition 2 *[2, equality (2.41)] For any face $\Gamma \subset \mathbb{F}_2^n$, $0 \in \Gamma$, and a Boolean function f it holds*

$$\sum_{z\in\Gamma} W_f(z) = 2^{\dim(\Gamma)-n} \sum_{x\in\Gamma^\perp} (-1)^{f(x)}.$$

Every Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented in *algebraic normal form* (ANF)

$$f(x_1,\ldots,x_n) = \bigoplus_{y\in\mathbb{F}_2^n} M_f(y)x^y = \bigoplus_{y\in\mathbb{F}_2^n} M_f(y)x_1^{y_1}\cdots x_n^{y_n}, \tag{2}$$

where $x^0 = 1, x^1 = x$, and the function $M_f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called the *Möbius transform* of f. $\deg_{alg}(f)$ is the maximum degree of the polynomial (2). It is well known (see [2, Section 2.2.1]) that for every function the ANF is unique.

Proposition 3 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. $|\mathrm{supp}(f)|$ is odd if and only if $\deg_{alg}(f) = n$.*

This proposition follows from the definition of ANF immediately.

It is well known that

$$M_f(y) = \bigoplus_{x \in \Gamma_y} f(x), \tag{3}$$

where the face Γ_y, $\dim(\Gamma_y) = \mathrm{wt}(y)$, contained 0 and y. Let $\geq$ be a natural partial order on $\mathbb{F}_2^n$, i. e., for $x, y \in \mathbb{F}_2^n$ inequality $x \leq y$ implies that $y_1 = 1$ if $x_i = 1$. Note that Γ_y is the set of vectors x such that x is less than y in this order.

The maximal degree of the monomial in ANF of f is called the *algebraic degree* of f, i. e., $\deg_{alg}(f) = \max\limits_{M_f(y)=1} \mathrm{wt}(y)$.

Let $S_f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an indicator function of $\mathrm{supp}(W_f)$.

Proposition 4 *If f is an s-plateaued function then $\deg_{alg}(S_f) \leq \frac{n+s}{2}$.*

Proof. Let $\Gamma \subset \mathbb{F}_2^n$ be a face containing the zero vector. By Proposition 2 we see that if $\dim(\Gamma) - n > \frac{s-n}{2}$ then Γ contained zero or even number of nonzero coefficient W_f. Then we obtain $\deg_{alg}(S_f) \leq \frac{n+s}{2}$ by using (3). □

Theorem 1 *If f is a partially bent function then $H(f) \leq 2I(f)$.*

Proof. Let f be a s-plateaued and partially bent function. Then S_f is an $(n-s)$-affine subspace by the definition. Let h be an indicator function of a k-dimensional affine subspace then $\deg_{alg}(h) = n - k$. By (1) $2 \sum\limits_{x \in \mathbb{F}_2^n} h(x)\mathrm{wt}(x) \geq \mathrm{wt}(h)(n - (n-k))$ Then

$$I(f) = \sum_{z \in \mathbb{F}_2^n} W_f^2(z)\mathrm{wt}(z) = 2^{s-n} \sum_{z \in \mathbb{F}_2^n} S_f(z)\mathrm{wt}(z) \geq 2^{s-n}\mathrm{wt}(S_f)\frac{n-s}{2} = \frac{n-s}{2}.$$

Since $H(f) = n - s$ by Proposition 1, we complete the proof. □

Theorem 2 *$H(f) \leq 4I(f)$ for every plateaued function f.*

Proof. $W_f^2(z) = 2^{s-n}$ or $W_f^2(z) = 0$ for any $z \in \mathbb{F}_2^n$. By Parseval's identity $\mathrm{wt}(S_f) = 2^{n-s}$. By (1) we have that

$$I(f) = \sum_{z \in \mathbb{F}_2^n} W_f^2(z)\mathrm{wt}(z) = 2^{s-n} \sum_{z \in \mathbb{F}_2^n} S_f(z)\mathrm{wt}(z) \geq \frac{n - \deg_{alg}(S_f)}{2}.$$

By Proposition 2 we have $I(f) \geq \frac{n-s}{4}$. Since $H(f) = n - s$ by Proposition 1, we complete the proof. □

Note that in [6], the authors proved that $\sup \frac{H(f)}{I(f)} \geq 4$, where the supremum is taken over all plateaued functions. Consequently, the FEI constanf 4 is tight for plateaued functions.

3 Proof of the Main Inequality

Let $S \subseteq \mathbb{F}_2^n$ and $u, v \in \mathbb{F}_2^n$. Define $T_S(a,b) = \{x \in S, x \geq a, x \geq b\}$.

Lemma 1 *For every $S \subset \mathbb{F}_2^n$ there exists a permutation $\pi : S \to S$ such that for every $y \in S$ the cardinality $|T_S(y, \pi(y))|$ is odd.*

Proof. Suppose that elements of S are enumerated by integers such that if $x < y$ then the number of x is less than the number of y. Define a matrix M of size $|S| \times |S|$ by the equation

$$M_{xy} = \begin{cases} 1 & \text{if } x \leq y, \\ 0 & \text{otherwise.} \end{cases}$$

We consider M as a matrix over $\mathbb{F}_2$. By definition, M is an upper triangle matrix with units on the main diagonal. Therefore, $\det(M) = 1$ and $\det(MM^{\mathsf{T}}) = 1$. So, there exists a permutation π such that $MM^{\mathsf{T}}(y, \pi(y)) = 1$ for every $y \in S$.

By definition

$$(MM^{\mathsf{T}})_{uv} = \langle \mathbf{1}_{S \cap \{u \leq y\}}, \mathbf{1}_{S \cap \{v \leq y\}} \rangle = |T_S(u,v)| \bmod 2.$$

Thus, the cardinality $|T_S(y, \pi(y))|$ is odd for every $y \in S$. $\square$

Lemma 2 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function and let $|T_{\mathrm{supp}(f)}(u,v)|$ be odd. Then* $\mathrm{wt}(u) + \mathrm{wt}(v) \geq n - \deg_{alg}(f)$.

Proof. Consider the indicator function h of $T_{\mathrm{supp}(f)}(u,v)$. By definition $h(x) = f(x)x^u x^v$ because of x^z is an indicator function of the set $\{x \in \mathbb{F}_2^n : x \geq z\}$. Therefore, $\deg_{alg}(h) \leq \deg_{alg}(f) + \mathrm{wt}(u) + \mathrm{wt}(v)$. By Proposition 3 $\deg_{alg}(h) = n$. Then $\mathrm{wt}(u) + \mathrm{wt}(v) \geq n - \deg_{alg}(f)$. $\square$

Theorem 3 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function then*

$$2 \sum_{x \in \mathbb{F}_2^n} f(x)\mathrm{wt}(x) \geq \mathrm{wt}(f)(n - \deg_{alg}(f)).$$

Proof. Let $S = \mathrm{supp}(f)$. By Lemmas 1 and 2 there exists a permutation π of S such that

$$\mathrm{wt}(y) + \mathrm{wt}(\pi(y)) \geq n - \deg_{alg}(f)$$

for every $y \in S$. Then

$$\sum_{y \in S} (\mathrm{wt}(y) + \mathrm{wt}(\pi(y))) \geq \sum_{y \in S} (n - \deg_{alg}(f)).$$

It is easy to see that $\sum\limits_{y \in S} (\mathrm{wt}(y) + \mathrm{wt}(\pi(y))) = 2 \sum\limits_{x \in \mathbb{F}_2^n} f(x)\mathrm{wt}(x)$ and $\sum\limits_{y \in S} (n - \deg_{alg}(f)) = \mathrm{wt}(f)(n - \deg_{alg}(f))$. $\square$

We can treat Theorem 3 as an estimation of mean weight of 1s of Boolean functions with known degree. Below we clarify details of the distribution of 1s.

Consider a vector space $\mathbb{F}_2^S$ consist of functions $h|_S$, where h are n-variables Boolean functions. Let $\langle u, v \rangle$ be a bilinear form on $\mathbb{F}_2^S$ defined by the equation

$$\langle u, v \rangle = \bigoplus_{x \in S} u(x)v(x).$$

This form is nondegenerate because for every $u \neq \mathbf{0}$ there exists v such that $\langle u, v\rangle = 1$. Indeed, if $u(x_0) = 1$ then we can take an indicator function of x_0 as v. Then the equation $\dim(L) + \dim(L^\perp) = |S|$ is true for every linear subspace $L \subset \mathbb{F}_2^S$.

Proposition 5 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function of degree d and $0 \leq t \leq \min(n-d, d-1)$. Then* $\sum_{x,\mathrm{wt}(x)\leq\frac{n-d-t}{2}} f(x) \leq \sum_{x,\mathrm{wt}(x)\geq\frac{n-d+t}{2}} f(x)$.

Proof. Let $S = \mathrm{supp}(f)$, and let $L_m = \{h|_S : \deg_{alg}(h) \leq m\}$ denote the space of restrictions to S of Boolean functions of algebraic degree at most m. By Lemma 2, if $m + k < n - d$, then $L_m \subseteq L_k^\perp$. Since the bilinear form on $\mathbb{F}_2^S$ is nondegenerate, $\dim(L_k) + \dim(L_m) \leq |S|$.

We next show that $\{x^u|_S : u \in S,\ \mathrm{wt}(u) \leq k\}$ is a linearly independent set. Enumerate the elements of S as $S = \{u^1, \ldots, u^{|S|}\}$ in nonincreasing order of Hamming weight, with arbitrary ordering among elements of equal weight. Suppose that $\{x^{u^1}|_S, \ldots, x^{u^m}|_S\}$ is linearly independent, and put $v = u^{m+1}$. For every $j \leq m$, either $\mathrm{wt}(u^j) > \mathrm{wt}(v)$, in which case $u^j \not\leq v$, or $\mathrm{wt}(u^j) = \mathrm{wt}(v)$ and $u^j \neq v$, in which case again $u^j \not\leq v$. Hence $x^{u^j}(v) = 0$ if $j \leq m$, whereas $x^v(v) = 1$. Thus the enlarged set is linearly independent. Consequently,

$$\dim(L_k) \geq \big|\{u \in S : \mathrm{wt}(u) \leq k\}\big|.$$

Therefore, whenever $m + k < n - d$,

$$\big|\{u \in S : \mathrm{wt}(u) \leq k\}\big| + \big|\{u \in S : \mathrm{wt}(u) \leq m\}\big| \leq |S|.$$

Equivalently,

$$\big|\{u \in S : \mathrm{wt}(u) \leq k\}\big| \leq \big|\{u \in S : \mathrm{wt}(u) \geq m+1\}\big|.$$

Now put $k = \left\lfloor \frac{n-d-t}{2} \right\rfloor$ and $m = n - d - k - 1$. Then $m + k = n - d - 1 < n - d$, and

$$m + 1 = n - d - \left\lfloor \frac{n-d-t}{2} \right\rfloor = \left\lceil \frac{n-d+t}{2} \right\rceil.$$

Since Hamming weights are integers, $\mathrm{wt}(u) \geq m + 1$ if and only if $\mathrm{wt}(u) \geq \frac{n-d+t}{2}$. The desired inequality follows. □

4 Equivalent Forms of the Main Inequality

Proposition 6 *The inequality (1) is equivalent to inequality*

$$2\sum_{x\in\mathbb{F}_2^n} f(x)\mathrm{wt}(x) \leq \mathrm{wt}(f)(n + \deg_{alg}(f)).$$

Proof. If we change variables x_i to $x_i \oplus 1$ for all $i \in 1, \ldots, n$ we obtain this inequality from (1) and preserve the set of all n-variable functions of degree d. □

We will use the following well-known property.

Proposition 7 *For any Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and any nondegenerate affine transformation $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ we have $\deg_{alg}(f \circ L) = \deg_{alg}(f)$.*

Proposition 8 *The inequality (1) is equivalent to inequality*

$$-\deg_{alg}(f)\mathrm{wt}(f) \le 2^{n-1}\sum_{i=1}^{n} W_f(u_i) \le \deg_{alg}(f)\mathrm{wt}(f), \tag{4}$$

where $\{u_1, u_2, \ldots, u_n\}$ *is an arbitrary basis of* $\mathbb{F}_2^n$

Proof. It is easy to see that $\sum\limits_{i=1}^{n}(-1)^{x_i} = n - 2\mathrm{wt}(x)$. Then

$$-\deg_{alg}(f)\mathrm{wt}(f) \le -\sum_{x\in\mathbb{F}_2^n} f(x)\sum_{i=1}^{n}(-1)^{x_i} \le \deg_{alg}(f)\mathrm{wt}(f).$$

Since $f(x) = \frac{1}{2}(1-(-1)^{f(x)})$ we have

$$-\sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{x_i} = -\frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(1-(-1)^{f(x)})(-1)^{x_i} = \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus(x,e_i)} = 2^{n-1}W_f(e_i),$$

where $e_i = (0,\ldots,0,1,0,\ldots,0)$ is a standard unit vector. Therefore, we prove (4) for the standard basis. By Proposition 7 we obtain inequalities (4) are true for every basis. By a similar way we can conclude that the inequalities (1) follow from (4). □

Note that we can take $|W_f(u_i)|$ instead of $W_f(u_i)$ in the right inequality (4) because $W_g(z) = (-1)^{(a,z)}W_f(z)$, where $g(x) = f(x)\oplus(a,x)$.

5 p-Biased Distribution

Let $X_1,\ldots,X_n$ be independent binary random variables such that $X_i = 1$ with probability p for $i = 1,\ldots,n$, where $0 \le p \le 1$. Define symmenric probabilistic distribution on $\mathbb{F}_2^n$ by the formula: $\Pr\{X = x\} = p^{\mathrm{wt}(x)}(1-p)^{n-\mathrm{wt}(x)}$. For function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ define

$$\mu_f(p) = \Pr(\mathrm{supp}(f)) = \mathsf{E}(f) = \sum_{x\in\mathbb{F}_2^n} f(x)\Pr\{X = x\}.$$

It is easy to see that $\mu_{f\oplus 1}(p) = \mu_f(1-p)$. So, we will consider only $0 \le p \le 1/2$. By definition, we have $\mu_f(1/2) = \frac{\mathrm{wt}(f)}{2^n}$. It is well-known that

$$\mathrm{wt}(f) \ge 2^{n-\deg_{alg}(f)} \tag{5}$$

if f is not a zero constant. This bound is known as a minimal code distance of Reed–Muller code. In other words this bound implies $\mu_f(1/2) \ge \frac{1}{2^{\deg_{alg}(f)}}$ (Schwartz–Zippel lemma). Recently this inequality was generalized by the following way.

Proposition 9 ([3], Claim 6.8) *For* $0 \le p \le 1/2$ *and every Boolean function* f, $f \ne \mathbf{0}$, *it holds* $\mu_f(p) \ge p^{\deg_{alg}(f)}$.

We propose further improvement of this inequality.

Proposition 10 *Let* $0 \le p, q \le 1/2$ *and let* f, $f \ne \mathbf{0}$, *be a Boolean function* f *of degree* d. *It holds* $\mu_f(pq) \ge q^d\mu_f(p)$.

Proof. Let $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ be independent binary random variables such that $X_i = 1$ with probability p and where $Y_i = 1$ with probability q, where $0 \leq p, q \leq 1/2$. Then $X_i Y_i$ are independent binary random variables with $\Pr\{X_i Y_i = 1\}$ for $i = 1, \ldots, n$.

Let $x \cdot y = (x_1 y_1, \ldots, x_n y_n)$. We have

$$\mu_f(pq) = \sum_{x,y \in \mathbb{F}_2^n} f(xy) \Pr\{XY = xy\} = \sum_{x,y \in \mathbb{F}_2^n} f(xy) \Pr\{XY = xy | X = x\} \Pr\{X = x\}$$

$$= \sum_{x \in \mathbb{F}_2^n} \Pr\{X = x\} \sum_{y \in \mathbb{F}_2^n} f(xy) \Pr\{XY = xy | X = x\}.$$

Define functions $f_x(y)$ by the equation $f_x(y) = f(xy)$. By definition $\deg_{alg}(f_x) \leq \deg_{alg}(f)$. Moreover, $f_x \neq \mathbf{0}$ if $f(x) = 1$. By Proposition 9 we obtain that $\mu_{f_x}(q) \geq q^d$. If $f(x) = 1$ then

$$\sum_{y \in \mathbb{F}_2^n} f(xy) \Pr\{XY = xy | X = x\} = \mu_{f_x}(q) \geq q^d.$$

Then

$$\mu_f(pq) = \sum_{x \in \mathbb{F}_2^n} \Pr\{X = x\} \sum_{y \in \mathbb{F}_2^n} f(xy) \Pr\{XY = xy | X = x\} \geq q^d \sum_{x \in \mathbb{F}_2^n} f(x) \Pr\{X = x\} = q^d \mu_f(p).$$

□

Corollary 2 *For $0 \leq s \leq 1/4$ and every n-variable Boolean function f, $f \neq \mathbf{0}$, of degree d, it holds $\mu_f(s) \geq \frac{s^d \mathrm{wt}(f)}{2^{n-d}}$.*

Proof. We use Proposition 10 with $p = 1/2$ and $q = 2s$. □

Proposition 11 *For $0 \leq p \leq 1/2$ and every Boolean function f, $f \neq \mathbf{0}$, of degree d it holds $\mu_f(p) \geq \mathrm{wt}(f) p^{(n+d)/2} (1-p)^{(n-d)/2}$.*

Proof. The function $h(t) = \alpha^t$ is convex. Thus, by Jensen's inequality we obtain that

$$\frac{1}{\mathrm{wt}(f)} \sum_{x \in \mathrm{supp}(f)} \left(\frac{p}{1-p}\right)^{\mathrm{wt}(x)} \geq \left(\frac{p}{1-p}\right)^{\sum_{x \in \mathrm{supp}(f)} \frac{\mathrm{wt}(x)}{\mathrm{wt}(f)}}.$$

Since $\frac{p}{1-p} \leq 1$ by Proposition 6 we have

$$\left(\frac{p}{1-p}\right)^{\sum_{x \in \mathrm{supp}(f)} \frac{\mathrm{wt}(x)}{\mathrm{wt}(f)}} \geq \left(\frac{p}{1-p}\right)^{\frac{n+d}{2}}.$$

Then

$$\mu_f(p) = \sum_{x \in \mathrm{supp}(f)} p^{\mathrm{wt}(x)} (1-p)^{n - \mathrm{wt}(x)} \geq wt(f) p^{(n+d)/2} (1-p)^{n-(n+d)/2}.$$

□

Note that

$$\frac{p^d}{2^{n-d}} \geq p^{(n+d)/2} (1-p)^{(n-d)/2} \tag{6}$$

and, consequently, the bound from Corollary 2 is better than the bound from Proposition 11. Indeed, (6) is equivalent to $1 \geq 4p(1-p)$. However, the bound from Corollary 2 is valid only if $p \leq 1/4$. For the case $1/4 \leq p \leq 1/2$, the bound from Proposition 11 is better than the bound from Proposition 9 if $p^d < \mathrm{wt}(f) p^{(n+d)/2} (1-p)^{(n-d)/2}$, i. e., $\mathrm{wt}(f) \geq (p(1-p))^{(d-n)/2}$. For $p = 1/2$ the last equation coincide with (5), so itis holds for all functions of degree d.

6 Acknowledgements

The author thanks Storozhuk for his continued interest in his work. The main inequality was proved with the assistance of ChatGPT.

References

[1] Alon N., Kaufman T., Krivelevich M., Litsyn S., and Ron D., Testing Reed-Muller codes, IEEE Trans. Inform. Theory, vol. 51 (2005), pp. 4032–4039. https://doi.org/10.1109/TIT.2005.856958,

[2] Carlet C., *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 562 pages, 2020.

[3] Dinur I., Filmus Y., Harsha P., Agreement tests on graphs and hypergraphs, SIAM Journal on Computing, vol. 54 iss. 2 (2025). https://doi.org/10.1137/21M1397684

[4] Friedgut E., Kalai G., Every monotone graph property has a sharp threshold. Proceedings of the American mathematical Society, 124(10) (1996), pp. 2993-3002.

[5] Gangopadhyay S., Stănică P. Fourier entropy-influence conjecture for cryptographic Boolean functions. Trans. Adv. Res.(Special issue on Advances in Cryptology and Information Security), vol. 12(2), (2016), pp. 8-14.

[6] Li Z., Tang D., A note on the FMEI of the Boolean functions in the Generalized Maiorana-McFarland construction, Discrete Applied Mathematics, vol. 387 (2026), pp. 106-115. https://doi.org/10.1016/j.dam.2026.02.052.

[7] Potapov V.N., On the number of relevant variables for discrete functions, Cryptography and Communications, vol.17 (2025), pp. 989–998. https://doi.org/10.1007/s12095-025-00797-4

[8] Sălăgean A., Reyes-Paredes P., Bounds for the average degree-k monomial density of Boolean functions. Cryptogr. Commun. vol. 18, no. 1 (2026), pp. 187-211. https://doi.org/10.1007/s12095-025-00839-x