Separation Results for Boolean Function Classes

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

October 22, 2020

Abstract

We show (almost) separation between certain important classes of Boolean functions. The technique that we use is to show that the total influence of functions in one class is less than the total influence of functions in the other class. In particular, we show (almost) separation of several classes of Boolean functions which have been studied in the coding theory and cryptography from classes which have been studied in combinatorics and complexity theory.

Keywords: Boolean function, total influence, monotone functions, bent functions, strict avalanche criteria, propagation characteristic, plateaued function, constant depth circuits, linear threshold function.

1   Introduction

Boolean functions are one of the most basic objects in coding theory, cryptography and computer science. Several important classes of Boolean functions have been extensively studied in different areas. Some examples in the context of coding theory and cryptography are the classes of bent [15] functions, plateaued [19] functions, functions satisfying the strict avalanche criteria (SAC) [17], and functions satisfying propagation characteristics (PC) [14]. Examples in the context of combinatorics and complexity theory are monotone functions, bounded-depth circuits [11] and linear threshold functions [6].

If the intersection of two classes of Boolean functions is empty, then the classes are disjoint. For two infinite classes of Boolean functions, we say that they are almost disjoint, if their intersection is a finite set. Being almost disjoint implies that there is a positive integer n_0 such that for any $n \geq n_0$, there is no n-variable Boolean function which belongs to both the classes.

Our goal is to show that several pairs of classes of Boolean functions are almost disjoint. We use the notion of total influence [12] to show such separation. The technique that we use is to show that for sufficiently large n, the total influence of any n-variable Boolean function in one of the classes is less than the total influence of any n-variable Boolean function in the other class. The specific results that we obtain are the following. The class of Boolean functions consisting of bent functions and functions satisfying SAC and PC is almost disjoint from the class of monotone functions; the class of functions which can be implemented using constant depth, polynomial size circuits; and the class of linear threshold functions. Similar separation results are obtained for the class of plateaued functions.

The separation of bent and monotone functions was conjectured in [4] and proved in [3]. Our proof which is based on total influence is shorter. While [3] had considered cryptographic properties of

monotone functions, the classes of SAC, PC and plateaued functions were not considered in [3]. So, the separation results for these classes mentioned above are not present in [3].

2 Background and Notation

We use the notation $[n] = \{1, 2, \ldots, n\}$ and $2^{[n]}$ denotes the power set of $[n]$. Throughout we write $\log$ for $\log_2$. The expressions $0 \log 0$ and $0 \log \frac{1}{0}$ are to be interpreted as 0.

For $\mathbf{x} \in \{-1, 1\}^n$, the notation $\mathbf{x}^{\oplus i}$ denotes the vector $(x_1, \ldots, x_{i-1}, -x_i, x_{i+1}, \ldots, x_n)$. For $S \subseteq [n]$, the notation $\mathbf{x}^{\oplus S}$ denotes the vector $((-1)^{w_1} x_1, (-1)^{w_2} x_2, \ldots, (-1)^{w_n} x_n)$, where $w_i = 1$ if $i \in S$, and $w_i = 0$ otherwise.

We consider the domain of an n-variable Boolean function to be $\{-1, 1\}^n$ and the co-domain to be $\{-1, 1\}$, i.e., an n-variable Boolean function f is a map $f : \{-1, 1\}^n \to \{-1, 1\}$. Boolean functions are also considered to be maps from $\{0, 1\}^n$ to $\{0, 1\}$. The two representations of Boolean functions can be seen to be equivalent under the map from $\{0, 1\}$ to $\{-1, 1\}$ which takes $a \in \{0, 1\}$ to $(-1)^a$ and the inverse map which takes $b \in \{-1, 1\}$ to $(1 - b)/2$.

The Fourier transform of $f : \{-1, 1\}^n \to \{-1, 1\}$ is a map $\widehat{f} : 2^{[n]} \to [-1, 1]$ defined as follows. For $S \subseteq [n]$,

$$\widehat{f}(S) \;=\; \frac{1}{2^n} \sum_{\mathbf{x}=(x_1,\ldots,x_n)\in\{-1,1\}^n} f(\mathbf{x}) \prod_{i \in S} x_i. \tag{1}$$

From Parseval's identity, we have $\sum_{S \subseteq [n]} \widehat{f}^2(S) = 1$ and so the numbers $\widehat{f}^2(S)$ can be thought of as a probability distribution on $2^{[n]}$. The Fourier entropy $H(f)$ of f is defined to be the entropy of the probability distribution $\{\widehat{f}^2(S)\}_{S \subseteq [n]}$ and is equal to

$$H(f) \;=\; -\sum_{S \subseteq [n]} \widehat{f}^2(S) \log \widehat{f}^2(S). \tag{2}$$

The influence of variable i on $f : \{-1, 1\}^n \to \{-1, 1\}$ is defined as follows.

$$\mathsf{Inf}_i(f) = \Pr_{\mathbf{x} \in \{-1,1\}^n}[f(\mathbf{x}) \neq f(\mathbf{x}^{\oplus i})] = \sum_{\substack{S \subseteq [n] \\ i \in S}} \widehat{f}^2(S).$$

The total influence $I(f)$ of $f : \{-1, 1\}^n \to \{-1, 1\}$ is given by

$$I(f) = \sum_{i=1}^{n} \mathsf{Inf}_i(f) = \sum_{S \subseteq [n]} |S| \widehat{f}^2(S).$$

The influence of a set of variables S on $f : \{-1, 1\}^n \to \{-1, 1\}$ is defined to be

$$\mathsf{Inf}_S(f) = \Pr_{\mathbf{x} \in \{-1,1\}^n}[f(\mathbf{x}) \neq f(\mathbf{x}^{\oplus S})]$$

In Appendix A, we have stated the relationships between influence, auto-correlation and average sensitivity of a Boolean function.

2.1 Some Boolean Function Classes

We define the Boolean function classes that will be required in the present work. For some of the classes, the original definitions are different from, though equivalent to, the definitions that we provide.

An n-variable Boolean function f is said to be *monotone* if the following property holds. For $\mathbf{a}, \mathbf{b} \in \{-1, 1\}^n$, if $\mathbf{a} \leq \mathbf{b}$ (i.e., $a_i \leq b_i$, $i = 1, \ldots, n$), then $f(\mathbf{a}) \leq f(\mathbf{b})$. Let M denote the set of all monotone Boolean functions.

The following Boolean function classes have been studied in the context of coding theory and cryptography.

- For even n, an n-variable Boolean function f is said to be *bent* [15], if $\widehat{f}(S) = \pm \frac{1}{2^{n/2}}$, for all $S \in [n]$. Let B denote the set of all bent functions.

- An n-variable Boolean function f satisfies the *strict avalanche criterion* (SAC) [17], if $\mathsf{Inf}_i(f) = \frac{1}{2}$, for all i. Further, we say that an n-variable function satisfies SAC of order k, $0 \leq k \leq n-2$, (written as SAC(k)) if by fixing any k of the n variables to arbitrary values in $\{-1, 1\}$, the resulting function satisfies SAC. For $k \geq 0$, let S_k denote the set of all Boolean functions satisfying SAC(k), and define $\mathsf{S} = \cup_{k \geq 0} \mathsf{S}_k$.

- An n-variable Boolean function f satisfies *propagation characteristics* [14] of degree k, $0 \leq k \leq n$, (written as PC(k)) if $\mathsf{Inf}_S(f) = \frac{1}{2}$ for $1 \leq |S| \leq k$. For $k \geq 0$, let PC_k denote the set of all Boolean functions satisfying PC(k), and define $\mathsf{PC} = \cup_{k \geq 0} \mathsf{PC}_k$.

- An n-variable Boolean function f is said to be *k-plateaued* [19], for $k \in \{0, \ldots, n\}$ and $n \equiv k \bmod 2$, if for all $S \in [n]$, $\widehat{f}^2(S) \in \left\{ 0, \pm \frac{1}{2^{(n-k)/2}} \right\}$. For $k \geq 0$, let PL_k be the set of all k-plateaued Boolean functions, and define $\mathsf{PL} = \cup_{k \geq 0} \mathsf{PL}_k$.

We next define some Boolean functions classes which have been studied in the context of complexity theory.

- A bounded-depth circuit [11] for n variables is a Boolean circuit that consists of AND and OR gates, with inputs $x_1, \ldots, x_n$ and $\overline{x}_1, \ldots, \overline{x}_n$. Fan-in to the gates is unbounded but depth is bounded by a constant. Without loss of generality, the circuit is leveled, where gates at level i have all their inputs from level $i-1$; all gates at the same level have the same type, i.e., all gates at a particular level are either AND or OR; and the types of gates alternate between AND and OR for successive levels. The depth of such a circuit is the number of levels that it has. The size of a circuit is the number of gates in it. If the size of a bounded depth circuit is bounded by a polynomial in n, then it is called an AC^0 circuit [13]. The set of all Boolean functions computable by AC^0 circuits of depth d is denoted by $\mathsf{AC}^0[d]$.

- A Boolean function f is said to be a *linear threshold function* [6], if there are real constants $w_0, w_1, \ldots, w_n$ such that for any $\mathbf{x} = (x_1, \ldots, x_n) \in \{-1, 1\}^n$, $f(\mathbf{x}) = \mathsf{sign}(w_0 + w_1 x_1 + \cdots + w_n x_n)$, where $\mathsf{sign}(z) = 1$ if $z > 0$, and -1 if $z \leq 0$. Let LTF denote the set of all linear threshold function.

Below we collect together some relevant results on total influence that will be required for proving separation results. Some of these results were stated in terms of average sensitivity which is the same as total influence (see Appendix A).

Fact 1 [1]: For any n-variable function $f \in \mathsf{AC}^0[d]$, $I(f) = O((\log n)^{d-1})$.

Fact 2 [18]: For any non-constant n-variable monotone Boolean function f, $I(f) \le \binom{n}{\lfloor n/2 \rfloor} \lceil n/2 \rceil / 2^{n-1}$. Since $\binom{n}{\lfloor n/2 \rfloor} \lceil n/2 \rceil / 2^{n-1} = \Theta(\sqrt{n})$, we have $I(f) = O(\sqrt{n})$.

Fact 3 [8]: For any n-variable Boolean function f in LTF, $I(f) \le 2\sqrt{n}$.

Fact 4 [9]: For any n-variable Boolean function f in PL_k, $I(f) = \Omega(n-k)$.

3 Separation Results

For $n \in \mathbb{N}$, let $\mathcal{C}_n^1$ and $\mathcal{C}_n^2$, be two subsets of the set of all n-variable Boolean functions. Define $\mathcal{C}^1 \triangleq \bigcup_{n \ge 1} \mathcal{C}_n^1$ and $\mathcal{C}^2 \triangleq \bigcup_{n \ge 1} \mathcal{C}_n^2$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are two infinite classes of Boolean functions. Suppose there exists a constant n_0, such that for all $n \ge n_0$, $\mathcal{C}_n^1 \cap \mathcal{C}_n^2 = \emptyset$. If $n_0 = 1$, then the classes $\mathcal{C}^1$ and $\mathcal{C}^2$ are disjoint. If $n_0 > 1$, then we say that the classes are n_0-disjoint. Note that if the classes $\mathcal{C}^1$ and $\mathcal{C}^2$ are n_0-disjoint, then their intersection is finite, i.e., they are almost disjoint.

Let $\mathcal{C}^1$ and $\mathcal{C}^2$ be two classes of Boolean functions. To show separation between $\mathcal{C}^1$ and $\mathcal{C}^2$ we use the following idea. Suppose it is possible to find a function $\mathcal{P}$ from the set of all Boolean functions to the reals and a positive integer n_0 such that for all $n \ge n_0$ and for all $f \in \mathcal{C}_n^1$ and $g \in \mathcal{C}_n^2$, $\mathcal{P}(f) < \mathcal{P}(g)$. Then, it follows that $\mathcal{C}_n^1$ and $\mathcal{C}_n^2$ are n_0-disjoint. We use total influence as the function $\mathcal{P}$. To do so, we need results on total influence for both the classes. Results on total influence for some of the classes have been provided in Section 2. The following result provides the value of total influence for functions in $\mathsf{B} \cup \mathsf{PC} \cup \mathsf{PL}$.

Proposition 1 *If an n-variable Boolean function f is in $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$, then $I(f) = n/2$.*

Proof: For $f \in \mathsf{B}$, we have $\widehat{f}(S) = \pm \frac{1}{2^{n/2}}$, for all $S \in [n]$. Hence,

$$I(f) = \sum_{S \subseteq [n]} |S| \widehat{f}(S)^2 = \frac{n}{2}.$$

Suppose f satisfies $\mathrm{SAC}(k)$ for some $k \ge 0$. Then, it follows that f satisfies $\mathrm{SAC}(j)$ for $1 \le j < k$ (see [7]). So, in particular, f satisfies SAC. From the definition of SAC, we have $\mathsf{Inf}_i(f) = \frac{1}{2}$, for all i and so $I(f) = \frac{n}{2}$.

Suppose f satisfies $\mathrm{PC}(k)$ for some $k \ge 0$. From the defintion of PC, we have $\mathsf{Inf}_S(f) = \frac{1}{2}$, for $1 \le |S| \le k$. Therefore, $\mathsf{Inf}_{\{i\}}(f) = \mathsf{Inf}_i(f) = \frac{1}{2}$, for all i and consequently, $I(f) = \frac{n}{2}$. □

Theorem 1 *The following disjointness results hold for $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$.*

1. M *is 4-disjoint from* $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$.

2. LTF *is 16-disjoint from* $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$.

3. *Let d be any positive integer. Then there exists a positive integer $\mathfrak{n}_0$ (depending on d) such that $\mathsf{AC}^0[d]$ is $\mathfrak{n}_0$-disjoint from $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$.*

Proof: *Proof of the first point.* For any n-variable monotone Boolean function f, from Fact 2, we have $I(f) \le \binom{n}{\lfloor n/2 \rfloor} \lceil n/2 \rceil / 2^{n-1}$. Since, for $n \ge 4$, we have $\binom{n}{\lfloor n/2 \rfloor} \lceil n/2 \rceil / 2^{n-1} < n/2$, it follows that for $n \ge 4$, $I(f) < n/2$. On the other hand, from Proposition 1 for any n-variable Boolean function in $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$, the total influence is equal to $n/2$. So, f cannot be in $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$.

Proof of the second point. Let f be any n-variable Boolean function in LTF. From Fact 3, $I(f) \leq 2\sqrt{n}$. Now, for $n > 16$, $2\sqrt{n} < \frac{n}{2}$. Therefore, using Proposition 1, we obtain the desired result.

Proof of the third point. Let $f \in \mathsf{AC}^0[d]$. From Fact 1, we have $I(f) = O((\log n)^{d-1})$. Consequently, there is a constant c and a positive integer n_1, such that $I(f) \leq c(\log n)^{d-1}$. Since d is fixed, there is a positive integer $\mathfrak{n}_0$ such that $c(\log n)^{d-1} < n/2$ for all $n \geq \mathfrak{n}_0$. So, for $n \geq \mathfrak{n}_0$, $I(f) < n/2$. From Proposition 1, we have that for $n \geq \mathfrak{n}_0$, f does not belong to $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$. $\square$

The first point of Theorem 1 provides a shorter proof of the fact that no monotone function on $n \geq 4$ variables is bent, a result which was conjectured in [4] and originally proved in [3]. The third point of Theorem 1 shows that in general bent functions and also functions satisfying propagation characteristics and strict avalanche criteria cannot be realised using constant depth circuits.

The notion of linear threshold function has been extended to polynomial threshold function. An n-variable Boolean function f is said to be a degree d polynomial threshold function (PTF) [2] if there is a polynomial p such that $f(\mathbf{x}) = \mathsf{sign}(p(\mathbf{x}))$ for all $\mathbf{x} \in \{-1, 1\}$. It has been shown in [8] that if f is a degree d PTF, then $I(f) \leq 2^{O(d)} \cdot \log n \cdot n^{1-1/(4d+2)}$. Let PTF_d be the set of all degree d PTFs. In a manner similar to the proof of Theorem 1, it can be proved that for $d = \log^c n$ with $c < 1/2$, the class $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$ is almost disjoint from PTF_d. It has been conjectured in [10] that if f is any n-variable degree d PTF, then $I(f) \leq d\sqrt{n}$. If the conjecture is true, it will show that $\mathsf{B} \cup \mathsf{S} \cup \mathsf{PC}$ is $4d^2$-disjoint from PTF_d.

Theorem 2 *Let k be a non-negative integer. The following disjointness results hold for PL_k.*

1. *There exists a positive integer $\mathfrak{n}_0$ such that $\mathcal{M}$ and PL_k are $\mathfrak{n}_0$-disjoint.*

2. *There exists a positive integer $\mathfrak{n}_1$ such that LTF and PL_k are $\mathfrak{n}_1$-disjoint.*

3. *Let d be any positive integer. There exists a positive integer $\mathfrak{n}_2$ (depending on d) such that $\mathsf{AC}^0[d]$ and PL_k are $\mathfrak{n}_2$-disjoint.*

Proof: *Proof of the first point.* Choose an $\varepsilon \in (1/2, 1)$ and let n be a positive integer satisfying $n - n^\varepsilon \geq k$. For any n-variable function f in PL_k, from Fact 4, $I(f) = \Omega(n - k) = \Omega(n^\varepsilon)$. So, there is a constant c_1 and an integer n_1, such that $I(f) \geq c_1 n^\varepsilon$ for all $n \geq n_1$. Let g be any n-variable function in M. From Fact 2, we have $I(g) = O(\sqrt{n})$. This implies that there is a constant c_2 and an integer n_2, such that $I(g) \leq c_2 n^{1/2}$ for all $n \geq n_2$. Since $\varepsilon > 1/2$ and c_1 and c_2 are constants, there is an integer $\mathfrak{n}_0$ such that $c_1 n^\varepsilon > c_2 n^{1/2}$ for all $n \geq n_0$. Note that $\mathfrak{n}_0$ has to satisfy $\mathfrak{n}_0 - \mathfrak{n}_0^\varepsilon \geq k$. So, for $n \geq \mathfrak{n}_0$, $I(f) \geq c_1 n^\varepsilon > c_2 n^{1/2} \geq I(g)$ which implies that f cannot be equal to g. Consequently, f cannot be in M.

Proof of the second point. The proof is similar to the first point, with the only difference being that Fact 3 is used for the argument instead of Fact 2.

Proof of the third point. The proof is also similar to the first point, with the difference being that Fact 1 is used for the argument. $\square$

Total influence can be used to separate a few other classes of Boolean functions. We briefly mention these.

An n-variable Boolean function is said to have c-linearly high entropy [16] for real constant $c > 0$, if $H(f) \geq cn$. Let c-LHE denote the set of all Boolean functions having c-linearly high entropy. It has been shown in [16] that for $f \in \mathsf{LHE}_c$, with $c \in (0, \frac{1}{2})$, $H[f] \leq \frac{1+c}{h^{-1}(c^2)} \cdot I(f)$, where h^{-1} is the inverse

of binary entropy function. Consequently, using Fact 1, it follows that for any positive integer d and $c \in (0, \frac{1}{2})$, LHE_c and $\mathsf{AC}^0[d]$ are almost disjoint.

The notion of random LTF was considered in [5], where the parameters $w_0, w_1, \ldots, w_n$ are drawn independently from either the uniform distribution over $[-1, 1]$, or from the standard normal distribution. It has been shown [5] that for an n-variable random LTF f, $I(f) = \Omega(\sqrt{n})$ with high probability. Combining with Fact 1 we see that f is not in $\mathsf{AC}^0[d]$ with high probability, where d is any positive integer.

4 Conclusion

We have used total influence to separate classes of Boolean functions. In particular, we have shown separation of certain classes of Boolean functions of interest in coding theory and cryptography from classes of Boolean functions which have been considered in combinatorics and complexity theory.

References

[1] Boppana, R.B.: The average sensitivity of bounded-depth circuits. Information processing letters 63(5), 257–261 (1997)

[2] Bruck, J.: Harmonic analysis of polynomial threshold functions. SIAM Journal on Discrete Mathematics 3(2), 168–177 (1990)

[3] Carlet, C., Joyner, D., Stănică, P., Tang, D.: Cryptographic properties of monotone Boolean functions. Journal of Mathematical Cryptology 10(1), 1–14 (2016)

[4] Celerier, C., Joyner, D., Melles, C., Phillips, D., et al.: On the Walsh-Hadamard transform of monotone Boolean functions. Tbilisi Mathematical Journal 5(2), 19–35 (2012)

[5] Chakraborty, S., Karmalkar, S., Kundu, S., Lokam, S.V., Saurabh, N.: Fourier entropy-influence conjecture for random linear threshold functions. In: Latin American Symposium on Theoretical Informatics. pp. 275–289. Springer (2018)

[6] Chow, C.K.: On the characterization of threshold functions. In: 2nd Annual Symposium on Switching Circuit Theory and Logical Design (SWCT 1961). pp. 34–38. IEEE (1961)

[7] Cusick, T.W., Stanica, P.: Cryptographic Boolean functions and applications. Academic Press (2017)

[8] Diakonikolas, I., Raghavendra, P., Servedio, R.A., Tan, L.Y.: Average sensitivity and noise sensitivity of polynomial threshold functions. SIAM Journal on Computing 43(1), 231–253 (2014)

[9] Gangopadhyay, S., Stanica, P.: The Fourier entropy-influence conjecture holds for a log-density 1 class of cryptographic Boolean functions. IACR Cryptol. ePrint Arch. 2014, 54 (2014)

[10] Gotsman, C., Linial, N.: Spectral properties of threshold functions. Combinatorica 14(1), 35–50 (1994)

[11] Håstad, J.T.: Computational limitations for small-depth circuits. MIT press (1987)

[12] Kahn, J., Kalai, G., Linial, N.: The influence of variables on Boolean functions. In: [Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science. pp. 68–80 (1988)

[13] Linial, N., Mansour, Y., Nisan, N.: Constant depth circuits, Fourier transform, and learnability. Journal of the ACM (JACM) 40(3), 607–620 (1993)

[14] Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R., Vandewalle, J.: Propagation characteristics of Boolean functions. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 161–173. Springer (1990)

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

[16] Shalev, G.: On the Fourier Entropy Influence conjecture for extremal classes. arXiv preprint arXiv:1806.03646 (2018)

[17] Webster, A., Tavares, S.E.: On the design of S-boxes. In: Conference on the theory and application of cryptographic techniques. pp. 523–534. Springer (1985)

[18] Zhang, S.: Note on the average sensitivity of monotone Boolean functions. Preprint p. 4 (2011)

[19] Zheng, Y., Zhang, X.M.: Relationships between bent functions and complementary plateaued functions. In: International Conference on Information Security and Cryptology. pp. 60–75. Springer (1999)

A   Auto-Correlation, Influence and Average Sensitivity

Given an n-variable Boolean function f, its auto-correlation function $C_f : \{-1, 1\}^n \to [-2^n, 2^n]$ is defined to be

$$C_f(\mathbf{u}) = \sum_{\mathbf{x} \in \{-1,1\}^n} f(\mathbf{x}) f(\mathbf{x} \odot \mathbf{u})$$

where $\mathbf{x} \odot \mathbf{u}$ represents the pointwise multiplication of vectors $\mathbf{x}$ and $\mathbf{u}$. The auto-correlation function is related to the influence in the following manner. For $S \subseteq [n]$,

$$\mathsf{Inf}_S(f) = \frac{1}{2} - \frac{1}{2^{n+1}} C_f(\mathbf{w}_S).$$

where $\mathbf{w}_S = (w_1, \dots, w_n) \in \{-1, 1\}^n$ is such that $w_i = -1$ if $i \in S$ and $w_i = 1$ otherwise.

The sensitivity $s(f, \mathbf{x})$ of a Boolean function f on input $\mathbf{x} = (x_1, x_2, \dots x_n) \in \{-1, 1\}^n$ is defined in the following manner.

$$s(f, \mathbf{x}) = \#\{i \in [n] : f(\mathbf{x}) \neq f(\mathbf{x}^{\oplus \mathbf{i}})\}.$$

The average sensitivity $s(f)$ of f is given by

$$s(f) = \frac{1}{2^n} \sum_{\mathbf{x} \in \{-1,1\}^n} s(f, \mathbf{x}).$$

It is easy to see that $I(f) = s(f)$ [13].