Tighter Relations between Sensitivity and Other Complexity Measures

Andris Ambainis[1,⋆], Mohammad Bavarian[2,⋆⋆], Yihan Gao[3], Jieming Mao[4], Xiaoming Sun[5,⋆⋆⋆], and Song Zuo[6]

[1] University of Latvia, Riga, Latvia
[2] Massachusetts Institute of Technology, Cambridge, MA, USA
[3] University of Illinois at Urbana-Champaign, IL, USA
[4] Princeton University, NJ, USA
[5] Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China
[6] Tsinghua University, Beijing, China

Abstract. The sensitivity conjecture of Nisan and Szegedy [12] asks whether the maximum sensitivity of a Boolean function is polynomially related to the other major complexity measures of Boolean functions.[1] Despite major advances in analysis of Boolean functions in the past decade, the problem remains wide open with no positive result toward the conjecture since the work of Kenyon and Kutin from 2004 [11].

In this work, we prove tighter upper bounds for various complexity measures in terms of sensitivity. More precisely, we show that $\deg(f)^{1-o(1)} = O(2^{s(f)})$ and $C(f) \leq 2^{s(f)-1}s(f)$; these in turn imply various corollaries regarding the relation between sensitvity and other complexity measures, such as block sensitivity, via known results. The gap between sensitivity and other complexity measures remains exponential but these results are the first improvement for this difficult problem that has been achieved in a decade.

1 Introduction

Sensitivity conjecture is a well-known and challenging open problem in the study of complexity measures of Boolean functions. As explaind in detail in various works, the conjecture has many equivalent (or morally equivallent) formulations. Although in this work we shall be mostly concerned with the original formulation of the conjecture in terms of complexity measures of Boolean functions, let us begin by stating the combinatorial formulations of the problem— as this formulation perhaps has the benefit of being more immediately accessible. In the

⋆ Supported by the European Commission under the project QALGO (Grant No. 600700) and the ERC Advanced Grant MQC (Grant No. 320731).
⋆⋆ Supported by NSF STC Award 0939370.
⋆⋆⋆ Supported in part by the National Natural Science Foundation of China Grant 61170062, 61222202.

[1] This includes deterministic, randomized or quantum query complexity, block sensitivity or Fourier degree which are all known to be polynomially related to one another.

J. Esparza et al. (Eds.): ICALP 2014, Part I, LNCS 8572, pp. 101–113, 2014.
© Springer-Verlag Berlin Heidelberg 2014

language of extremal combinatorics, the problem is about a certain conjectured Ramsey-type phenomenon over the Hamming cube as follows: does there exists a $\delta > 0$ such that any unbalanced two-coloring of vertices of hypercube $\{0,1\}^n$ contains a verctex $x \in \{0,1\}^n$ such that x has $\geq n^\delta$ neighbors in the same color class as x?

In the original form of Nisan and Szegedy [12], the conjecture takes the following form:

Conjecture 1 (sensitivity conjecture). There exists a constant $d \in \mathbb{R}^+$ such that for any Boolean function $f : \{-1,1\}^n \to \{-1,1\}$ we have

$$bs(f) = O(s(f)^d),$$

where $s(f)$ and $bs(f)$ denote the sensitivity and the block sensitivity (defined in Section 2) of the function f .

We shall note that the equivalence between these two seemingly different problems, first observed by Gotsman and Linial [8], is not at all that difficult. Moreover, the equivalence is very direct, and there is almost no cost in parameters for switching from one setting to the other. Thus, one may choose to work in whichever setting one finds more convenient. As such, we shall work exclusively in the complexity theoretic framework, though we shall note that our arguements in Section 4 is inspired and is a refinement of an arguement of Chung et al. from [6] which takes place in the combinatorial setting.

We shall make one final remark about the formulation of the problem before moving on to the discussion of previous works and our results. In the statement of the conjecture, we can replace the block sensitivity by several other widely used complexity measure of Boolean functions (such as deterministic and randomized query complexity, certificate complexity, Fourier degree, etc.) which are all polynomially related to block sensitivity (and to each other), as shown by Nisan and Szegedy [12].

Background. As mentioned above, through the work of various researchers by now many different equivalent forms of the sensitivity conjecture are available. Fortunately, almost all of these different formulations and various approaches to the conjecture are discussed in the recent survey of P. Hatami et al. [10] (see also the blogpost of Aaronson [1] which played an important role in the recent surge of attention to the problem). We refer to these works for a more detailed exposition of the background and the prior works. We briefly recall some of the more immediately relevant facts:

The best known upper bound on block sensitivity is

$$bs(f) \leq (\frac{e}{\sqrt{2\pi}})e^{s(f)}\sqrt{s(f)}, \tag{1}$$

given by Kenyon and Kutin [11]. In the other direction, the first progress on the lower bound was made by Rubinstein [13] who gave the first quadratic separation for block sensitivity and sensitivity by constructing a Boolean function f with $bs(f) = \frac{1}{2}s(f)^2$. Currently, the best lower bound is due to Ambainis and Sun who in [3] exhibited a function with $bs(f) = \frac{2}{3}s(f)^2 - \frac{1}{2}s(f)$.

Results. Our first result in this paper is the following estimate regarding the relation between the maximum sensitivity and Fourier degree of a Boolean function.

Theorem 1. *Let $f : \{0,1\}^n \to \{-1,1\}$ be a Boolean function. Then*

$$\deg(f)^{1-o(1)} \leq s(f)2^{s(f)},$$

where $o(1)$ denotes a term that vanishes as $\deg(f) \to \infty$.

The proof of the above theorem is a mixture of techniques from Fourier analysis and combinatorics. The argument is partly inspired by the arguments in the paper of Chung et al. [6] which recently played an important role in solving a question about the query complexity of restrictions of parity function in [2].

For sensitivity versus certificate complexity, we can prove a somewhat stronger theorem which has direct consequences for sensitivity versus block sensitivity problem (which is the original formulation of sensitivity conjecture by Nisan and Szegedy [12]).

Theorem 2. *For any Boolean function f,*

$$C_1(f) \leq 2^{s_0(f)-1}s_1(f), \quad C_0(f) \leq 2^{s_1(f)-1}s_0(f). \tag{2}$$

Here $C_0(f)$ and $C_1(f)$ denote the 0-certificate complexity and 1-certificate complexity of f. These notions – along with the rest of the background material on complexity measures of Boolean functions – are presented in Section 2.

Using the known relations between various complexity measures of Boolean functions, we can derive several consequences from the above result.

Corollary 1. *For any Boolean function f,*

$$bs(f) \leq C(f) \leq 2^{s(f)-1}s(f).$$

Combining Theorem 2 and some previous results, we can also give another upper bound for block sensitivity.

Corollary 2. *For any Boolean function f,*

$$bs(f) \leq \min\{2^{s_0(f)}, 2^{s_1(f)}\}s_1(f)s_0(f). \tag{3}$$

Hence, we see that our Theorems 1 and 2 and their corollaries show an improved exponent in relation between sensitivity and various complexity measures of Boolean functions compared to the previous best bound shown in equation (1). Beside being the first positive result toward the sensitivity conjecture since the work of Kenyon and Kutin from 2004, we believe our results have the merit of introducing new ideas and techniques which could be valuable elesewhere as well as in the future works on this fundamental conjecture.

Although the bounds obtained in Theorems 1 and Theorem 2 look quite similar, the theorems do not follow one from another by using the known relations

between certificate complexity and Fourier degree. On the contrary, the two theorems are obtained by using rather different techniques. However, we shall note that despite their differences both proofs of Theorem 1 and 2 crucially rely on the small set expansion properties of Boolean hypercube. It is plausible that better analytic estimates along the lines of [7] could be useful to slightly improve our results— though a significant improvement is likely to require new ideas.

Organization. In Section 2 we recall some basic definitions and concepts relevant to this work. In Section 3, we prove Theorem 1 and in Section 4, we prove Theorem 2 and its corollaries. Both Sections 3 and 4 are self-contained and can be read in any order.

2 Preliminaries

In this paper, we work with total Boolean functions over the hypercube and their measures of complexity. We assume some basic familiarity with the complexity measures of Boolean functions (as described in the survey [5]). For completeness, we briefly recall some basic definitions.

We work with the usual graph structure on the hypercube by connecting $x, y \in \{0,1\}^n$ if and only if x, y differ in a single coordinate. We always denote by $\log(\cdot)$ the logarithm with the base 2.

Definition 1. *The pointwise sensitivity $s(f,x)$ of a function f on input x is defined as the number of bits on which the function is sensitive, i.e.*

$$s(f,x) = \left|\{i \in [n] | f(x) \neq f(x^{(i)})\}\right|,$$

where $x^{(i)}$ is obtained by flipping the i-th bit of x. We define the total sensitivity by

$$s(f) = \max\left\{s(f,x) | x \in \{0,1\}^n\right\},$$

and the 0-sensitivity and 1-sensitivity by

$$s_0(f) = \max\left\{s(f,x) | x \in \{0,1\}^n, f(x) = 0\right\}, \quad s_1(f) = \max\left\{s(f,x) | x \in \{0,1\}^n, f(x) = 1\right\}.$$

Block sensitivity is another important complexity measure which is obtained by relaxing the requirement that we have to only flip single coordinates by allowing flipping disjoint blocks. More formally block sensitivity is defined as follows:

Definition 2. *The pointwise block sensitivity $bs(f,x)$ of f on input x is defined as maximum number of pairwise disjoint subsets $B_1, ..., B_k$ of $[n]$ such that $f(x) \neq f(x^{(B_i)})$ for all $i \in [k]$. Here $x^{(B_i)}$ is obtained by flipping all the bits $\{x_j | j \in B_i\}$ of x. Define the block sensitivity of f as*

$$bs(f) = \max\left\{bs(f,x) | x \in \{0,1\}^n\right\},$$

and the 0-block sensitivity and 1-block sensitivity, analogously to Definition 1, by

$$bs_0(f) = \max\left\{bs(f,x) | x \in \{0,1\}^n, f(x) = 0\right\}, \quad bs_1(f) = \max\left\{bs(f,x) | x \in \{0,1\}^n, f(x) = 1\right\}.$$

The certificate complexity is another very useful complexity measure with a more non-deterministic type of definition. It is defined as follows:

Definition 3. *The certificate complexity $C(f,x)$ of f on input x is defined as the minimum length of a partial assignment of x such that f is constant on this restriction. Define the certificate complexity of f by*

$$C(f) = \max\left\{C(f,x) | x \in \{0,1\}^n\right\},$$

and the 0-certificate and 1-certificate by

$$C_0(f) = \max\left\{C(f,x) | x \in \{0,1\}^n, f(x) = 0\right\}, \quad C_1(f) = \max\left\{C(f,x) | x \in \{0,1\}^n, f(x) = 1\right\}.$$

Another important notion for us is Fourier degree. It is also polynomially related to block-sensitivity and certificate complexity. To define Fourier degree, recall that any function $f : \{0,1\}^n \to \mathbb{C}$ can be expanded in terms of Fourier characters as follows

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\, \chi_S(x)\,,$$

where $\chi_S(x) = (-1)^{\sum_{i \in S} x_i}$.

Definition 1. *Let $f : \{-1,1\}^n \to \mathbb{R}$ and let $\hat{f}(\cdot)$ denote its Fourier transform. We define Fourier degree of f by*

$$\deg(f) = \max_{\hat{f}(S) \neq 0} |S|\,.$$

Finally, we mention an important and well-known combinatorial result over the hypercube, usually attributed to Harper [9].

Lemma 1 (Hamming Cube Isoperimetry [9]). *Assume $\emptyset \neq A \subseteq \{0,1\}^n$. Let d be the average degree of vertices of A with graph structure on A induced from the natural Hamming graph of $\{0,1\}^n$. Then we have*

$$|A| \geq 2^d\,.$$

The above lemma is quite easy to prove by induction. For a detailed proof which covers the application to combinatorics, we recommend consulting the book by Bollobás [4].

The above theorem implies that if $|A|$ is small, the average degree d must also be relatively small. In this case, the ratio between the number of the edges leaving the set A and the total number of incident edges to A, which is equal to $1 - d/n$, is relatively large. This justifies the alternative name given to the above theorem as the "small set expansion" property of the Hamming cube.

In Section 4, we need an equivalent formulation of discrete isoperimetric inequality, Lemma 1, which will be a more convenient for our purposes there.

Lemma 2. *For any $A \subseteq \{0,1\}^n$, the edges between A and $\bar{A} = \{0,1\}^n \setminus A$ is lower bounded by*

$$|E(A,\bar{A})| \geq |A|(n - \log_2 |A|).$$

3 Sensitivity versus Degree

In this section, we shall prove Theorem 1. Let $f : \{0,1\}^n \to \{-1,1\}$ be a Boolean function. To prove Theorem 1, the key idea is to count the following objects.

Definition 4. *An (l,r) S-triple consists of a point $x \in \{0,1\}^n$ and two sets $L \subseteq R \subseteq [n]$ with $|L| = l$ and $|R| = r$ such that $f(x) \neq f(x^i)$ for any $i \in L$.*

In our application, the two parameters $l \leq r$ are chosen as follows: $l = c \log r$, for some $c > 0$ an appropriately chosen constant, and r will be a slowly growing function of n which will be asymptotically $\log \log n$. The upper bound on the number of S-triples is easy to establish.

Lemma 3. *The number of (l,r) S-triples is bounded by*

$$2^n \frac{s(f)^l \, n^{r-l}}{l!(r-l)!}.$$

Proof. We can assume $s(f) \geq l$ as otherwise the number of S-triples is zero. Consider any $x \in \{0,1\}^n$. The number of S-triples involving x is bound by $\max_{1 \leq q \leq s(f)} \binom{q}{l} \binom{n-l}{r-l}$. This is clearly bounded by $\frac{s(f)^l \, n^{r-l}}{l!(r-l)!}$ which implies the above lemma. □

The main part of proving Theorem 1 is to prove a lower bound on the number of S-triples which coupled with the above lemma gives the desired lower bound on $s(f)$. The key idea here is study of restriction of function f to subcubes of dimension r. To be able to carry out our argument we will need a few definition regarding restrictions of functions over the discrete cube.

Restrictions of Boolean functions.

Definition 5. *Given $z \in \{0,1,*\}^n$ and $R \subseteq [n]$, we call them a* compatible pair *if $R = \{i \in [n] : z(i) = *\}$. Each $z \in \{0,1,*\}^n$ naturally corresponds to $|R|$-dimensional subcube $Q_z \subseteq \{0,1\}^n$ defined as follows:*

$$Q_z = \{y \in \{0,1\}^n : z_i \neq * \Rightarrow y_i = z_i\},$$

i.e. Q_z is constructed by freezing the coordinates of y in $[n] \setminus R$ according to z, and letting the rest of coordinates y_i for $i \in R$ to be free.

Let $f : \{0,1\}^n \to \mathbb{R}$. Given a compatible pair $z \in \{0,1,*\}^n$ and $R = \{i \in [n] : z(i) = *\}$ we obtain a restriction function $f|_z$ given by restricting f to Q_z

Definition 6. *Given $z \in \{0,1,*\}^n$ and $x \in \{0,1\}^n$ (here x is not necessarily in Q_z), define $y = (x \downarrow z)$ to be projection of x to Q_z given by $y_i = z_i$ for any $i \in [n]$ such that $z(i) \neq *$ and $y_i = x_i$ for all the other $i \in [n]$. We define*

$$f|_z(x) = f(x \downarrow z).$$

Notice that $f|_z(x)$ is a function over whole $\{0,1\}^n$ though its value only depends on R the coordinates which $z(i) = *$. Given the above definition one can easily infer the Fourier expansion of the restriction function $f|_z(\cdot)$ from that of f as follows.

$$(f|_z)(x) = \sum_{S \subseteq R} \chi_S(x) \sum_{U \cap R = S} \hat{f}(U) \chi_{U \setminus S}(z)\,.$$

We need the following lemma regarding the degree of restrictions of a function.

Lemma 4. *Let $f : \{-1,1\}^n \to \{-1,1\}$ be function of degree n. Let $R \subseteq [n]$. Then there exist $z \in \{-1,1,*\}^n$ compatible with R such that $(f|_z)$ is also full-degree $|R|$.*

Proof. The coefficient of the highest monomial in Fourier expansion of $(f|_z)$ is given by

$$\sum_{R \subseteq U} \hat{f}(U) \chi_{U \setminus R}(z).$$

Now we calculate the expectation of the square of this value for a random z compatible with R.

$$\mathop{\mathbf{E}}_{z} \left(\sum_{R \subseteq U} \hat{f}(U) \chi_{U \setminus R}(z) \right)^2 = \sum_{R \subseteq U} \hat{f}(U)^2 \geq \hat{f}([n])^2 > 0$$

where for the last inequality we used the fact that f is full-degree. □

The importance of the above lemma is that it allows us to use *induction*:[2] Fix some $R \subseteq [n]$. By the lemma above, there exists $z \in \{0,1,*\}^n$ compatible with R such that $f|_z$ is full-degree. The importance of existence of z is that Q_z always contain an S-triple which was the object we were interested to count. More precisely, since $f|_z$ is full-degree by induction on the degree in Theorem 1 there exists subset $L \subseteq R$ with $|L| \geq \frac{1}{3} \log |R|$ such that there exist $x \in Q_z$ such that $f|_z(x) \neq f|_z(x^i)$ for every $i \in L$. Taking $l = |L|$ and $r = |R|$ we see that (x, L, R) constitutes an S-triple. We use the existence of z and Harper's lemma 1 to prove that for every R there exists not only one such z but in fact many. This is the key estimate we need to prove our result.

The Main Proof of Sensitivity versus Fourier Degree Estimate

Proof (Theorem 1). Without loss of generality we can assume f is full-degree. If this is not the case, choose $S \subseteq [n]$ with $|S| = \deg(f)$ such that $\hat{f}(S) \neq 0$,

[2] It is worth noting that for our induction we do not need the full strength of Theorem 1; in fact, a weaker bound of (say) $\deg(f) \leq 10^{s(f)}$, which follows from [11] and the know relations between Fourier degree and block sensitivity, here suffices. If we were able to change our methods to exploit the sharper induction hypothesis provided by Theorem 1, this may be useful for achieving some improved estimate.

then set the coordinates outside S arbitrary to get a Boolean function on $|S|$-dimensional hypercube of full-degree. This reduces the problem to the full-degree case as restricting a function can only decrease the sensitivity.

Let $r = \omega(1)$ be a very slowly growing function of n to be specified later. Fix a set $R \subseteq [n]$ with $|R| = r$. By Lemma 4 there exist $z \in \{0,1,*\}^n$ compatible with R such that the restricted function $(f|_z)$ has degree r. Now by induction $s(f|_z) \geq l$ where $l = \Theta(\log r)$. (we can take $l = \frac{1}{3}\log r$ for concreteness.) This means we can find a point $x \in Q_z$ with l neighbors $x_1, x_2, \ldots, x_l$ such that

$$(f|_z)(x_1) = (f|_z)(x_2) = \ldots = (f|_z)(x_l) \neq (f|_z)(x)\,.$$

Let $L = \{i_1, i_2, \ldots, i_l\} \subseteq R$ be the direction of the edges $(x, x_1), (x, x_2), \ldots, (x, x_l)$ respectively. Then (x, L, R) constitutes a (l, r) S-triple.

So far for any $R \subseteq [n]$ we have shown the existence of one such S-triple. Now we show there are many such triples. Consider Z_R which is the set of all $z \in \{0,1,*\}^n$ compatible with R. Notice that Z_R can be naturally associated with a $(n-r)$-hypercube with $z_1, z_2 \in Z_R$ said to be *neighbors* in direction $j \in [n] \setminus R$ if $z_1(i) = z_2(i)$ for $i \in [n] \setminus \{j\}$ and $z_1(j) \neq z_2(j)$. (Clearly $z_1(j) \neq *$ and $z_2(j) \neq *$ as both z_1 and z_2 are compatible with R.)

We call a $\widetilde{z} \in Z_R$ *good* if

$$(f|_{\widetilde{z}})(x_1) = (f|_{\widetilde{z}})(x_2) = \ldots = (f|_{\widetilde{z}})(x_l) \neq (f|_{\widetilde{z}})(x)\,.$$

Let A be the set of all good $\widetilde{z}$ in Z_R. Notice that if $\widetilde{z}$ is good, $((x \downarrow \widetilde{z}), L, R)$ constitutes an S-triple. We have shown so far that $z \in A$ so A is non-empty. Now we prove all elements of A have high degree when seen as a subset of $(n-r)$-hypercube. Indeed, notice that for any $\bar{z} \in Z_R$ and any $\bar{x}$, there are at most $s(f)$ directions $j \in [n] \setminus R$ such that $(f|_{\bar{z}})(\bar{x}^{(j)}) \neq (f|_{\bar{z}})(\bar{x})$. Applying the same reasoning to all $x, x_1, x_2, \ldots, x_l$, we see that for any $z \in A$ there is at least $n - r - s(f)(l+1)$ neighbors of z in A. Now applying our isoperimetric inequality (Lemma 1) to A we see that there are at least $2^{n-r-(l+1)s(f)}$ such special triples for a fixed $R \subseteq [n]$ of size$r$.

On the other hand, the number of such special triples is bounded above by Lemma 3. So we have

$$\binom{n}{r} 2^{n-r-s(f)(l+1)} \leq 2^n \frac{s(f)^l\, n^{r-l}}{l!(r-l)!}.$$

As $r \ll n$ we have $\binom{n}{r} \geq \frac{n^r}{2^r r!}$. Simplifying we see $n^{\frac{l}{l+1}} \leq 4^r \binom{r}{l} s(f) 2^{s(f)}$. Choosing $r \log r = \log n$ and $l = \frac{\log r}{3}$ we get

$$n^{1 - O\left(\frac{1}{\log\log n}\right)} \leq s(f) 2^{s(f)}\,,$$

which is our desired result. □

4 Sensitivity versus Certificate Complexity

In this section we prove Theorem 2. Actually, we prove a slightly stronger result.

Theorem 3. *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, then*

$$C_1(f) \leq 2^{s_0(f)-1}s_1(f) - (s_0(f)-1),\ C_0(f) \leq 2^{s_1(f)-1}s_0(f) - (s_1(f)-1).^3$$

Proof. By symmetry we only need to prove $C_1(f) \leq 2^{s_0(f)-1}s_1(f) - (s_0(f)-1)$. Without the loss of generality, we assume $C_1(f) = C(f, 0^n)$, i.e. the 1-certificate complexity is achieved on the input 0^n. We have $f(0^n) = 1$. We assume that the minimal certificate of 0^n consists of $x_1 = 0, x_2 = 0, \ldots, x_m = 0$, where $m = C(f, 0^n) = C_1(f)$.

Let Q_0 be the set of inputs x that satisfies $x_1 = x_2 = \ldots = x_m = 0$. Since $x_1 = 0, x_2 = 0, \ldots, x_m = 0$ is a 1-certificate, we have $\forall\ x \in Q_0,\ f(x) = 1$.

For each $i \in [m]$, let Q_i be the set of inputs x with $x_1 = \ldots = x_{i-1} = x_{i+1} = \ldots = x_m = 0$ and $x_i = 1$. Let S be the total sensitivity of all inputs $x \in \bigcup_{i=1}^m Q_i$. It consists of three parts: sensitivity between Q_i and Q_0 (denoted by S_1), sensitivity inside Q_i (denoted by S_2) and sensitivity between Q_i and other input (denoted by S_3), i.e.

$$S = \sum_{i=1}^{m} \sum_{x \in Q_i} s(f, x) = S_1 + S_2 + S_3. \tag{4}$$

In the following we estimate S_1, S_2 and S_3 separately. We use $A_1, \ldots, A_m$ to denote the set of 0-inputs in $Q_1, \ldots, Q_m$, respectively, i.e. $A_i = \{x \in Q_i | f(x) = 0\}$ $(i \in [m])$. Since $x_1 = \ldots = x_m = 0$ is the minimal certificate, i.e. Q_0 is maximal, thus $A_1, \ldots, A_m$ are all nonempty.

We also need the following lemma which follows from Lemma 2 but can be also proven without using it [14]:

Lemma 5. *For any $i \in [m]$,*

$$|A_i| \geq 2^{n-m-s_0(f)+1}.$$

The sensitivity between Q_i and Q_0 is $|A_i|$. By summing over all possible i we get:

$$S_1 = \sum_{i=1}^{m} |A_i|. \tag{5}$$

Sensitivity Inside $Q_1, \ldots, Q_m$: By Lemma 2, for each $i \in [m]$, the number of edges between A_i and $Q_i \setminus A_i$ is bounded by:

$$|E(A_i, Q_i \setminus A_i)| \geq |A_i|(\log_2 |Q_i| - \log_2 |A_i|) = |A_i|(n - m - \log_2 |A_i|).$$

[3] If $s_0(f) = 0$ or $s_1(f) = 0$, then f is constant, hence $s(f) = bs(f) = C(f) = 0$.

Therefore,

$$S_2 = 2\sum_{i=1}^{m} |E(A_i, Q_i \setminus A_i)|$$
$$\geq 2\sum_{i=1}^{m} |A_i|(n - m - \log_2 |A_i|). \quad (6)$$

Sensitivity between Q_i and Other Inputs (i.e. $\{0,1\}^n \setminus \bigcup_{j=0}^{m} Q_j$): For each $1 \leq i < j \leq m$, let $Q_{i,j}$ be the set of inputs (not in Q_0) that are *adjacent* to both Q_i and Q_j, i.e. $Q_{i,j}$ is the set of inputs x that satisfy $x_1 = \ldots x_{i-1} = x_{i+1} = \ldots x_{j-1} = x_{j+1} = \ldots x_m = 0$ and $x_i = x_j = 1$. The sensitivity between Q_i, Q_j and $Q_{i,j}$ is lower bounded by

$$\sum_{x \in Q_0} |f(x + e_i) - f(x + e_j)|.$$

where e_i is the unit vector with the i-th coordinate equal to 1 and all other coordinates equal to 0. Then, $x + e_i$, $x + e_j$ are the neighbors of x in Q_i and Q_j, respectively. Summing over all possible pairs of (i, j) we get

$$S_3 \geq \sum_{1 \leq i < j \leq m} \sum_{x \in Q_0} |f(x + e_i) - f(x + e_j)|$$
$$= \sum_{x \in Q_0} \left(\sum_{i=1}^{m} f(x + e_i) \right) \left(m - \sum_{i=1}^{m} f(x + e_i) \right)$$
$$= \sum_{x \in Q_0} s(f, x)(m - s(f, x)). \quad (7)$$

If we combine inequalities (5)-(7), we get

$$S = \sum_{i=1}^{m} \sum_{x \in Q_i} s(f, x)$$
$$\geq \sum_{i=1}^{m} |A_i| + 2\sum_{i=1}^{m} |A_i|(n - m - \log_2 |A_i|) + \sum_{x \in Q_0} s(f, x)(m - s(f, x)). \quad (8)$$

Since $s(f, x)$ is upper bounded by $s_0(f)$ or $s_1(f)$ (depending on whether $f(x) = 0$ or $f(x) = 1$), we have

$$\sum_{x \in Q_i} s(f, x) \leq |A_i| s_0(f) + (|Q_i| - |A_i|) s_1(f)$$
$$= |A_i| s_0(f) + (2^{n-m} - |A_i|) s_1(f)$$

Thus,

$$S = \sum_{i=1}^{m} \sum_{x \in Q_i} s(f, x) \leq \sum_{i=1}^{m} \Big(|A_i| s_0(f) + (2^{n-m} - |A_i|) s_1(f) \Big). \quad (9)$$

We use w to denote the total number of 0-inputs in $Q_1, \ldots, Q_m$. Then,

$$w = \sum_{i=1}^{m} |A_i| = \sum_{x \in Q_0} s(f, x).$$

The inequality (9) can be rewritten as

$$S \leq w \cdot s_0(f) + (m \cdot 2^{n-m} - w) s_1(f). \tag{10}$$

Also, $s(f, x) \leq s_1(f)$ for each $x \in Q_0$. Thus, the right-hand side of inequality (8) is

$$\begin{aligned}
&\sum_{i=1}^{m} |A_i| + 2 \sum_{i=1}^{m} |A_i|(n - m - \log_2 |A_i|) + \sum_{x \in Q_0} s(f, x)(m - s(f, x)) \\
&\geq w + 2 \sum_{i=1}^{m} |A_i|(n - m - \log_2 |A_i|) + (m - s_1(f)) \sum_{x \in Q_0} s(f, x) \\
&= w + 2w(n - m) - 2 \sum_{i=1}^{m} |A_i| \log_2 |A_i| + (m - s_1(f))w \\
&= w(1 + 2n - m - s_1(f)) - 2 \sum_{i=1}^{m} |A_i| \log_2 |A_i|. \qquad (11)
\end{aligned}$$

By combining inequalities (8)-(11) we get

$$w(1 + 2n - m - s_1(f)) - 2 \sum_{i=1}^{m} |A_i| \log_2 |A_i| \leq w \cdot s_0(f) + (m \cdot 2^{n-m} - w) s_1(f).$$

By rearranging the inequality we get

$$w(1 + 2n - m - s_0(f)) \leq 2 \sum_{i=1}^{m} |A_i| \log_2 |A_i| + m \cdot 2^{n-m} s_1(f). \tag{12}$$

Since the function $g(x) = x \log_2 x$ is convex and we know that $|A_i| \leq |Q_i| = 2^{n-m}$, from Lemma 5 $|A_i| \geq 2^{n-m-s_0(f)+1}$. Therefore,

$$\begin{aligned}
g(|A_i|) &= g\left(\frac{|A_i| - 2^{n-m-s_0(f)+1}}{2^{n-m} - 2^{n-m-s_0(f)+1}} \cdot 2^{n-m} + \frac{2^{n-m} - |A_i|}{2^{n-m} - 2^{n-m-s_0(f)+1}} \cdot 2^{n-m-s_0(f)+1} \right) \\
&\leq \frac{|A_i| - 2^{n-m-s_0(f)+1}}{2^{n-m} - 2^{n-m-s_0(f)+1}} \cdot g(2^{n-m}) + \frac{2^{n-m} - |A_i|}{2^{n-m} - 2^{n-m-s_0(f)+1}} \cdot g(2^{n-m-s_0(f)+1}) \\
&= \frac{|A_i| - 2^{n-m-s_0(f)+1}}{2^{n-m} - 2^{n-m-s_0(f)+1}} \cdot 2^{n-m}(n - m) \\
&\quad + \frac{2^{n-m} - |A_i|}{2^{n-m} - 2^{n-m-s_0(f)+1}} \cdot 2^{n-m-s_0(f)+1}(n - m - s_0(f) + 1) \\
&= \frac{|A_i| - 2^{n-m-s_0(f)+1}}{2^{s_0(f)-1} - 1} \cdot 2^{s_0(f)-1}(n - m) + \frac{2^{n-m} - |A_i|}{2^{s_0(f)-1} - 1}(n - m - s_0(f) + 1) \\
&= \left(\frac{|A_i| - 2^{n-m-s_0(f)+1}}{2^{s_0(f)-1} - 1} 2^{s_0(f)-1} + \frac{2^{n-m} - |A_i|}{2^{s_0(f)-1} - 1} \right)(n - m) - \frac{2^{n-m} - |A_i|}{2^{s_0(f)-1} - 1}(s_0(f) - 1) \\
&= |A_i|(n - m) - \frac{2^{n-m} - |A_i|}{2^{s_0(f)-1} - 1}(s_0(f) - 1).
\end{aligned}$$

Hence

$$\sum_{i=1}^{m} |A_i| \log_2 |A_i| = \sum_{i=1}^{m} g(|A_i|)$$
$$\leq \sum_{i=1}^{m} \left(|A_i|(n-m) - \frac{2^{n-m} - |A_i|}{2^{s_0(f)-1}-1}(s_0(f)-1) \right)$$
$$= w(n-m+\frac{s_0(f)-1}{2^{s_0(f)-1}-1}) - m \cdot 2^{n-m} \frac{s_0(f)-1}{2^{s_0(f)-1}-1}. \quad (13)$$

By combining inequalities (12) and (13), we get

$$w(1+2n-m-s_0(f))$$
$$\leq 2\left(w(n-m+\frac{s_0(f)-1}{2^{s_0(f)-1}-1}) - m \cdot 2^{n-m} \frac{s_0(f)-1}{2^{s_0(f)-1}-1} \right) + m \cdot 2^{n-m} s_1(f).$$

It implies that

$$w\left(1+m-s_0(f) - \frac{2(s_0(f)-1)}{2^{s_0(f)-1}-1}\right) \leq m \cdot 2^{n-m}\left(s_1(f) - \frac{2(s_0(f)-1)}{2^{s_0(f)-1}-1}\right),$$

Substituting $w = \sum_{i=1}^{m} |A_i| \geq m \cdot 2^{n-m-s_0(f)+1}$, we get

$$m \cdot 2^{n-m-s_0(f)+1}\left(1+m-s_0(f) - \frac{2(s_0(f)-1)}{2^{s_0(f)-1}-1}\right) \leq m \cdot 2^{n-m}\left(s_1(f) - \frac{2(s_0(f)-1)}{2^{s_0(f)-1}-1}\right),$$

i.e.

$$1+m-s_0(f) - \frac{2(s_0(f)-1)}{2^{s_0(f)-1}-1} \leq 2^{s_0(f)-1}\left(s_1(f) - \frac{2(s_0(f)-1)}{2^{s_0(f)-1}-1}\right),$$

which implies

$$m \leq 2^{s_0(f)-1} s_1(f) - s_0(f) + 1.$$

□

4.1 Proof of Corollary 2

To prove Corollary 2, we need the following Lemma by Kenyon and Kutin.[4]

Lemma 6. *[11]* $bs_0(f) \leq 2(C_1(f) - \frac{1}{2})s_0(f)$, $bs_1(f) \leq 2(C_0(f) - \frac{1}{2})s_1(f)$.

Proof. (of Corollary 2) From Theorem 2 $bs_0(f) \leq C_0(f) \leq 2^{s_1(f)-1}s_0(f)$. From Corollary 6 we have $bs_0(f) \leq 2(C_1(f) - \frac{1}{2})s_0(f)$, together with Theorem 2 we get $bs_0(f) \leq 2(2^{s_0(f)-1}s_1(f) - \frac{1}{2})s_0(f)$. Therefore, $bs_0(f) \leq \min\{2^{s_1(f)}s_0(f),\ 2^{s_0(f)}s_1(f)s_0(f)\}$. Similarly we can show that $bs_1(f) \leq \min\{2^{s_1(f)}s_0(f)s_1(f),\ 2^{s_0(f)}s_1(f)\}$. □

[4] In their original paper there is no "$-\frac{1}{2}$" term, but a careful analysis will provide it.

References

1. Aaronson, S.: My philomath project: Sensitivity versus block-sensitivity, Shtetl Optimized blog (June 13, 2010), http://www.scottaaronson.com/blog/?p=453
2. Aaronson, S., Ambainis, A., Balodis, K., Bavarian, M.: Weak Parity. In: ICALP (to appear, 2014)
3. Ambainis, A., Sun, X.: New separation between $s(f)$ and $bs(f)$. Electronic Colloquium on Computational Complexity (ECCC) 18, 116 (2011)
4. Bollobás, B.: Combinatorics: set systems, hypergraphs, families of vectors and combinatorial probability. Cambridge University Press, Cambridge (1986)
5. Buhrman, H., de Wolf, R.: Complexity measures and decision tree complexity: a survey. Theoretical Computer Science 288(1), 21–43 (2002)
6. Chung, F.R.K., Füredi, Z., Graham, R.L., Seymour, P.: On induced subgraphs of the cube. J. Comb. Theory Ser. A 49 (1988)
7. Falik, D., Samorodnitsky, A.: Edge-isoperimetric inequalities and influences. Combinatorics, Probability & Computing 16(5), 693–712 (2007)
8. Gotsman, C., Linial, N.: The equivalence of two problems on the cube. Journal of Combinatorial Theory, Series A 61(1), 142–146 (1992)
9. Harper, L.: Optimal numberings and isoperimetric problems on graphs. Journal of Combinatorial Theory 1 (1966)
10. Hatami, P., Kulkarni, R., Pankratov, D.: Variations on the Sensitivity Conjecture. Theory of Computing Library, Graduate Surveys (4), 1–27 (2011)
11. Kenyon, C., Kutin, S.: Sensitivity, block sensitivity, and l-block sensitivity of Boolean functions. Information and Computation 189(1), 43–53 (2004)
12. Nisan, N., Szegedy, M.: On the degree of boolean functions as real polynomials. Computational Complexity 4, 301–313 (1994)
13. Rubinstein, D.: Sensitivity vs. Block Sensitivity of Boolean functions. Combinatorica 15(2), 297–299 (1995)
14. Simon, H.U.: A Tight $\Omega(\log \log n)$-Bound on the Time for Parallel Ram's to Compute Nondegenerated Boolean Functions. In: Karpinski, M. (ed.) FCT 1983. LNCS, vol. 158, pp. 439–444. Springer, Heidelberg (1983)