Sensitivity Versus Certificate Complexity of Boolean Functions

Andris Ambainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs(✉)

Faculty of Computing, University of Latvia, Raiņa bulv. 19, Rīga LV-1586, Latvia
jevgenijs.vihrovs@lu.lv

Abstract. Sensitivity, block sensitivity and certificate complexity are basic complexity measures of Boolean functions. The famous sensitivity conjecture claims that sensitivity is polynomially related to block sensitivity. However, it has been notoriously hard to obtain even exponential bounds. Since block sensitivity is known to be polynomially related to certificate complexity, an equivalent of proving this conjecture would be showing that the certificate complexity is polynomially related to sensitivity. Previously, it has been shown that $bs(f) \le C(f) \le 2^{s(f)-1} s(f) - (s(f) - 1)$. In this work, we give a better upper bound of $bs(f) \le C(f) \le \max\left(2^{s(f)-1}\left(s(f) - \frac{1}{3}\right), s(f)\right)$ using a recent theorem limiting the structure of function graphs. We also examine relations between these measures for functions with 1-sensitivity $s_1(f) = 2$ and arbitrary 0-sensitivity $s_0(f)$.

1 Introduction

Sensitivity and *block sensitivity* are two well-known combinatorial complexity measures of Boolean functions. The sensitivity of a Boolean function, $s(f)$, is just the maximum number of variables x_i in an input assignment $x = (x_1, \ldots, x_n)$ with the property that changing x_i changes the value of f. Block sensitivity, $bs(f)$, is a generalization of sensitivity to the case when we are allowed to change disjoint blocks of variables.

Sensitivity and block sensitivity are related to the complexity of computing f in several different computational models, from parallel random access machines or PRAMs [7] to decision tree complexity, where block sensitivity has been useful for showing the complexities of deterministic, probabilistic and quantum decision trees are all polynomially related [5,6,13].

A very well-known open problem is the *sensitivity vs. block sensitivity conjecture* which claims that the two quantities are polynomially related. This problem is very simple to formulate (so simple that it can be assigned as an undergraduate research project). At the same time, the conjecture appears quite difficult to

This work was supported by the European Union Seventh Framework Programme (FP7/2007-2013) under projects RAQUEL (Grant Agreement No. 323970) and ERC Advanced Grant MQC, and the Latvian State Research Programme NeXIT project No. 1.

A.S. Kulikov and G.J. Woeginger (Eds.): CSR 2016, LNCS 9691, pp. 16–28, 2016.
DOI: 10.1007/978-3-319-34171-2_2

solve. It has been known for over 25 years and the best upper and lower bounds are still very far apart. We know that block sensitivity can be quadratically larger than sensitivity [3,14,16] but the best upper bounds on block sensitivity in terms of sensitivity are still exponential [1,11,15].

Block sensitivity is polynomially related to a number of other complexity measures of Boolean functions: *certificate complexity*, *polynomial degree* and the number of queries to compute f either deterministically, probabilistically or quantumly [6]. This gives a number of equivalent formulations for the sensitivity vs. block sensitivity conjecture: it is equivalent to asking whether sensitivity is polynomially related to any one of these complexity measures.

Among the many equivalent forms of the conjecture, relating sensitivity to certificate complexity $C(f)$ might be the combinatorially simplest one. Certificate complexity being at least c simply means that there is an input $x = (x_1, \ldots, x_n)$ that is not contained in an $(n-(c-1))$-dimensional subcube of the Boolean hypercube on which f is constant. Therefore, in this paper we focus on the "sensitivity vs. certificate complexity" form of the conjecture.

1.1 Related Work

New Approaches to the Sensitivity Conjecture. Recently, there have been multiple developments in various approaches to the sensitivity conjecture. Gilmer et. al. interpret the problem through the cost of a novel communication game [8]. Gopalan et. al. investigate the properties of Boolean functions with low sensitivity [9]. Lin and Zhang give a bound on block sensitivity in terms of sensitivity and the alternating number of the function [12].

Upper Bounds on $bs(f)$ and $C(f)$ in Terms of $s(f)$. There has been a substantial amount of work on reducing the gap between sensitivity and block sensitivity measures. The first non-trivial upper bound is due to Simon [15]:

$$bs(f) \leq 4^{s(f)} s(f). \tag{1}$$

Kenyon and Kutin [11] improved the bound to

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

Recently, Ambainis et. al. [1] showed an even better estimate:

$$bs(f) \leq 2^{s(f)-1} s(f) - (s(f) - 1). \tag{3}$$

The essense of this result lies in the following relation between certificate complexity and sensitivity:

$$C_0(f) \leq 2^{s_1(f)-1} s_0(f) - (s_1(f) - 1). \tag{4}$$

Note that any bound for $C_0(f)$ also holds for $C_1(f)$ symmetrically (in this case, $C_1(f) \leq 2^{s_0(f)-1} s_1(f) - (s_0(f) - 1)$).[1]

[1] Here, C_0 (C_1) and s_0 (s_1) stand for certificate complexity and sensitivity, restricted to inputs x with $f(x) = 0$ ($f(x) = 1$).

1.2 Our Results

In this work, we give improved upper bounds for the "sensitivity vs. certificate complexity" problem. Our main technical result is

Theorem 1. *Let f be a Boolean function which is not constant. If $s_1(f) = 1$, then $C_0(f) = s_0(f)$. If $s_1(f) > 1$, then*

$$C_0(f) \le 2^{s_1(f)-1}\left(s_0(f) - \frac{1}{3}\right). \tag{5}$$

A similar bound for $C_1(f)$ follows by symmetry. This implies a new upper bound on block sensitivity and certificate complexity in terms of sensitivity:

Corollary 1. *Let f be a Boolean function. Then*

$$bs(f) \le C(f) \le \max\left(2^{s(f)-1}\left(s(f) - \frac{1}{3}\right), s(f)\right). \tag{6}$$

On the other hand, the function of Ambainis and Sun [3] gives the separation of

$$C_0(f) = \left(\frac{2}{3} + o(1)\right) s_0(f)s_1(f) \tag{7}$$

for arbitrary values of $s_0(f)$ and $s_1(f)$. For $s_1(f) = 2$, we show an example of f that achieves

$$C_0(f) = \left\lfloor \frac{3}{2}s_0(f) \right\rfloor = \left\lfloor \frac{3}{4}s_0(f)s_1(f) \right\rfloor. \tag{8}$$

We also study the relation between $C_0(f)$ and $s_0(f)$ for functions with low $s_1(f)$, as we think these cases may provide insights into the more general case.

If $s_1(f) = 1$, then $C_0(f) = s_0(f)$ follows from (4). So, the easiest non-trivial case is $s_1(f) = 2$, for which (4) becomes $C_0(f) \le 2s_0(f) - 1$.

For $s_1(f) = 2$, we prove a slightly better upper bound of $C_0(f) \le \frac{9}{5}s_0(f)$. We also show that $C_0(f) \le \frac{3}{2}s_0(f)$ for $s_1(f) = 2$ and $s_0(f) \le 6$ and thus our example (8) is optimal in this case. We conjecture that $C_0(f) \le \frac{3}{2}s_0(f)$ is a tight upper bound for $s_1(f) = 2$.

Our results rely on a recent "gap theorem" by Ambainis and Vihrovs [4] which says that any sensitivity-s induced subgraph G of the Boolean hypercube must be either of size 2^{n-s} or of size at least $\frac{3}{2}2^{n-s}$ and, in the first case, G can only be a subcube obtained by fixing s variables. Using this theorem allows refining earlier results which used Simon's lemma [15] – any sensitivity-s induced subgraph G must be of size at least 2^{n-s} – but did not use any more detailed information about the structure of such G.

We think that further research in this direction may uncover more interesting facts about the structure of low-sensitivity subsets of the Boolean hypercube, with implications for the "sensitivity vs. certificate complexity" conjecture.

2 Preliminaries

Let $f:\{0,1\}^n \to \{0,1\}$ be a Boolean function on n variables. The i-th variable of an input x is denoted by x_i. For an index set $P \subseteq [n]$, let x^P be the input obtained from an input x by flipping every bit x_i, $i \in P$.

We briefly define the notions of sensitivity, block sensitivity and certificate complexity. For more information on them and their relations to other complexity measures (such as deterministic, probabilistic and quantum decision tree complexities), we refer the reader to the surveys by Buhrman and de Wolf [6] and Hatami et al. [10].

Definition 1. *The* sensitivity complexity $s(f,x)$ *of* f *on an input* x *is defined as*

$$s(f,x) = \left| \left\{ i \,\middle|\, f(x) \neq f\left(x^{\{i\}}\right) \right\} \right|. \tag{9}$$

The b-sensitivity $s_b(f)$ *of* f*, where* $b \in \{0,1\}$*, is defined as* $\max(s(f,x) \mid x \in \{0,1\}^n, f(x)=b)$*. The* sensitivity $s(f)$ *of* f *is defined as* $\max(s_0(f), s_1(f))$.

We say that a vertex x has *full sensitivity* if $s(f,x) = s_{f(x)}(f)$.

Definition 2. *The* block sensitivity $bs(f,x)$ *of* f *on an input* x *is defined as the maximum number* t *such that there are* t *pairwise disjoint subsets* $B_1,\ldots,B_t$ *of* $[n]$ *for which* $f(x) \neq f\left(x^{B_i}\right)$*. We call each* B_i *a* block*. The* b-block sensitivity $bs_b(f)$ *of* f*, where* $b \in \{0,1\}$*, is defined as* $\max(bs(f,x) \mid x \in \{0,1\}^n, f(x)=b)$*. The* block sensitivity $bs(f)$ *of* f *is defined as* $\max(bs_0(f), bs_1(f))$.

Definition 3. *A* certificate c *of* f *on an input* x *is defined as a partial assignment* $c:P \to \{0,1\}, P \subseteq [n]$ *of* x *such that* f *is constant on this restriction. We call* $|P|$ *the* length *of* c*. If* f *is always 0 on this restriction, the certificate is a* 0-certificate*. If* f *is always 1, the certificate is a* 1-certificate.

Definition 4. *The* certificate complexity $C(f,x)$ *of* f *on an input* x *is defined as the minimum length of a certificate that* x *satisfies. The* b-certificate complexity $C_b(f)$ *of* f*, where* $b \in \{0,1\}$*, is defined as* $\max(C(f,x) \mid x \in \{0,1\}^n, f(x)=b)$*. The* certificate complexity $C(f)$ *of* f *is defined as* $\max(C_0(f), C_1(f))$.

In this work we look at $\{0,1\}^n$ as a set of vertices for a graph Q_n (called the *n-dimensional Boolean cube* or *hypercube*) in which we have an edge (x,y) whenever $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)$ differ in exactly one position. We look at subsets $S \subseteq \{0,1\}^n$ as subgraphs (induced by the subset of vertices S) in this graph.

Definition 5. *Let* c *be a partial assignment* $c:P \to \{0,1\}, P \subseteq [n]$*. An* $(n-|P|)$-dimensional subcube *of* Q_n *is a subgraph* G *induced on a vertex set* $\{x \mid \forall i \in P\,(x_i = c(i))\}$*. It is isomorphic to* $Q_{n-|P|}$*. We call the value* $\dim(G) = n-|P|$ *the* dimension *and the value* $|P|$ *the* co-dimension *of* G.

For example, a subgraph induced on the set $\{x \mid x_1 = 0, x_2 = 1\}$ is a $(n-2)$-dimensional subcube. Note that each certificate of length l corresponds to a subcube of Q_n with co-dimension l.

Definition 6. *Let G be a subcube defined by a partial assignment $c : P \to \{0,1\}, P \subseteq [n]$. Let $c' : P \to \{0,1\}$ where $c'(i) \neq c(i)$ for exactly one $i \in P$. Then we call the subcube defined by c' a* neighbour subcube *of G.*

For example, the sets $\{x \mid x_1 = 0, x_2 = 0\}$ and $\{x \mid x_1 = 0, x_2 = 1\}$ induce two neighbouring subcubes, since their union is a subcube induced on the set $\{x \mid x_1 = 0\}$.

We also extend the notion of Hamming distance to the subcubes of Q_n:

Definition 7. *Let G and H be two subcubes of Q_n. Then the* Hamming distance *between G and H is defined as $d(G,H) = \min_{\substack{x \in G \\ y \in H}} d(x,y)$, where $d(x,y)$ is the Hamming distance between x and y.*

Definition 8. *Let G and H be induced subgraphs of Q_n. By $G \cap H$ denote the* intersection *of G and H that is the graph induced on $V(G) \cap V(H)$. By $G \cup H$ denote the* union *of G and H that is the graph induced on $V(G) \cup V(H)$. By $G \setminus H$ denote the* complement *of G in H that is the graph induced by $V(G) \setminus V(H)$.*

Definition 9. *Let G and H be induced subgraphs of Q_n. By $R(G,H)$ denote the relative size of G in H:*

$$R(G,H) = \frac{|V(G \cap H)|}{|V(H)|}. \tag{10}$$

We extend the notion of sensitivity to the induced subgraphs of Q_n:

Definition 10. *Let G be a non-empty induced subgraph of Q_n. The* sensitivity *$s(G, Q_n, x)$ of a vertex $x \in Q_n$ is defined as $\left|\left\{i \,\middle|\, x^{\{i\}} \notin G\right\}\right|$, if $x \in G$, and $\left|\left\{i \,\middle|\, x^{\{i\}} \in G\right\}\right|$, if $x \notin G$. Then the* sensitivity *of G is defined as $s(G, Q_n) = \max(s(G, Q_n, x) \mid x \in G)$.*

Our results rely on the following generalization of Simon's lemma [15], proved by Ambainis and Vihrovs [4]:

Theorem 2. *Let G be a non-empty induced subgraph of Q_n with sensitivity at most s. Then either $R(G, Q_n) = \frac{1}{2^s}$ and G is an $(n-s)$-dimensional subcube or $R(G, Q_n) \geq \frac{3}{2} \cdot \frac{1}{2^s}$.*

3 Upper Bound on Certificate Complexity in Terms of Sensitivity

In this section we prove Corollary 1. In fact, we prove a slightly more specific result.

Theorem 1. *Let f be a Boolean function which is not constant. If $s_1(f) = 1$, then $C_0(f) = s_0(f)$. If $s_1(f) > 1$, then*

$$C_0(f) \leq 2^{s_1(f)-1}\left(s_0(f) - \frac{1}{3}\right). \tag{11}$$

Note that a similar bound for $C_1(f)$ follows by symmetry. For the proof, we require the following lemma.

Lemma 1. *Let H_1, H_2, …, H_k be distinct subcubes of Q_n such that the Hamming distance between any two of them is at least 2. Take*

$$T = \bigcup_{i=1}^{k} H_i, \qquad T' = \left\{x \,\middle|\, \exists i \left(x^{\{i\}} \in T\right)\right\} \setminus T. \tag{12}$$

If $T \neq Q_n$, then $|T'| \geq |T|$.

Proof. If $k = 1$, then the co-dimension of H_1 is at least 1. Hence H_1 has a neighbour cube, so $|T'| \geq |T| = |H_1|$.

Assume $k \geq 2$. Then $n \geq 2$, since there must be at least 2 bit positions for cubes to differ in. We use an induction on n.

Base case. $n = 2$. Then we must have that H_1 and H_2 are two opposite vertices. Then the other two vertices are in T', hence $|T'| = |T| = 2$.

Inductive step. Divide Q_n into two adjacent $(n-1)$-dimensional subcubes Q_n^0 and Q_n^1 by the value of x_1. We will prove that the conditions of the lemma hold for each $T \cap Q_n^b$, $b \in \{0, 1\}$. Let $H_u^b = H_u \cap Q_n^b$. Assume $H_u^b \neq \varnothing$ for some $u \in [k]$. Then either $x_1 = b$ or x_1 is not fixed in H_u. Thus, if there are two non-empty subcubes H_u^b and H_v^b, they differ in the same bit positions as H_u and H_v. Thus the Hamming distance between H_u^b and H_v^b is also at least 2. On the other hand, $Q_n^b \not\subseteq T$, since then k would be at most 1.

Let $T_b = T \cap Q_n^b$ and $T'_b = \left\{x \,\middle|\, x \in Q_n^b, \exists i \left(x^{\{i\}} \in T_b\right)\right\} \setminus T_b$. Then by induction we have that $|T'_b| \geq |T_b|$. On the other hand, $T_0 \cup T_1 = T$ and $T'_0 \cup T'_1 \subseteq T'$. Thus

$$|T'| \geq |T'_0| + |T'_1| \geq |T_0| + |T_1| = |T|. \tag{13}$$

□

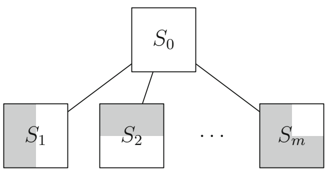

Fig. 1. A schematic representation of the 0-certificate S_0 and its neighbour cubes $S_1, S_2, \ldots, S_m$. The shaded parts represent the vertices in the subcubes for which the value of f is 1.

Proof of Theorem 1. Let z be a vertex such that $f(z) = 0$ and $C(f, z) = C_0(f)$. Pick a 0-certificate S_0 of length $C_0(f)$ and $z \in S_0$. It has $m = C_0(f)$ neighbour subcubes which we denote by $S_1, S_2, \ldots, S_m$ (Fig. 1).

We work with the graph G induced on the vertex set $\{x \mid f(x) = 1\}$. Since S_0 is a minimum certificate for z, $S_i \cap G \neq \varnothing$ for $i \in [m]$.

As S_0 is a 0-certificate, it gives 1 sensitive bit to each vertex in $G \cap S_i$. Then $s(G \cap S_i, S_i) \leq s_1(f) - 1$.

Suppose $s_1(f) = 1$, then for each $i \in [m]$ we must have that $G \cap S_i$ equals to the whole S_i. But then each vertex in S_0 is sensitive to its neighbour in $G \cap S_i$, so $m \leq s_0(f)$. Hence $C_0(f) = s_0(f)$.

Otherwise $s_1(f) \geq 2$. By Theorem 2, either $R(G, S_i) = \frac{1}{2^{s_1(f)-1}}$ or $R(G, S_i) \geq \frac{3}{2^{s_1(f)}}$ for each $i \in [m]$. We call the cube S_i either *light* or *heavy* respectively. We denote the number of light cubes by l, then the number of heavy cubes is $m - l$. We can assume that the light cubes are $S_1, \ldots, S_l$.

Let the average sensitivity of the inputs in S_0 be $as(S_0) = \frac{1}{|S_0|} \sum_{x \in S_0} s_0(x)$. Since each vertex of G in any S_i gives sensitivity 1 to some vertex in S_0, $\sum_{i=1}^{m} R(G, S_i) \leq as(S_0)$. Clearly $as(S_0) \leq s_0(f)$. We have that

$$l \frac{1}{2^{s_1(f)-1}} + (m - l) \frac{3}{2^{s_1(f)}} \leq as(S_0) \leq s_0(f) \tag{14}$$

$$m \frac{3}{2^{s_1(f)}} - l \frac{1}{2^{s_1(f)}} \leq as(S_0) \leq s_0(f). \tag{15}$$

Then we examine two possible cases.

Case 1. $l \leq (s_0(f) - 1) 2^{s_1(f)-1}$. Then we have

$$m \frac{3}{2^{s_1(f)}} - (s_0(f) - 1) \frac{2^{s_1(f)-1}}{2^{s_1(f)}} \leq as(S_0) \leq s_0(f) \tag{16}$$

$$m \frac{3}{2^{s_1(f)}} \leq s_0(f) + \frac{1}{2}(s_0(f) - 1) \tag{17}$$

$$m \frac{3}{2^{s_1(f)}} \leq \frac{3}{2} s_0(f) - \frac{1}{2} \tag{18}$$

$$m \leq 2^{s_1(f)-1} \left(s_0(f) - \frac{1}{3} \right). \tag{19}$$

Case 2. $l = (s_0(f) - 1) 2^{s_1(f)-1} + \delta$ for some positive integer δ. Since $s_1(f) \geq 2$, the number of light cubes is at least $2(s_0(f) - 1) + \delta$, which in turn is at least $s_0(f)$.

Let $\mathcal{F} = \{F \mid F \subseteq [l], |F| = s_0(f)\}$. Denote its elements by $F_1, F_2, \ldots, F_{|\mathcal{F}|}$. We examine $H_1, H_2, \ldots, H_{|\mathcal{F}|}$ – subgraphs of S_0, where H_i is the set of vertices whose neighbours in S_j are in G for each $j \in F_i$. By Theorem 2, $G \cap S_i$ are subcubes for $i \leq l$. Then so are the intersections of their neighbours in S_0, including each H_i.

Let $N_{i,j}$ be the common neighbour cube of S_i and S_j that is not S_0. Suppose $v \in S_0$. Then by v_i denote the neighbour of v in S_i. Let $v_{i,j}$ be the common neighbour of v_i and v_j that is in $N_{i,j}$.

Next we will show the following:

Proposition 1. *The Hamming distance between any two subcubes H_i and H_j, $i \neq j$ is at least 2.*

Proof. Assume there is an edge (u, v) such that $u \in H_i$ and $v \in H_j$. Then $u_k \in G$ for each $k \in F_i$. Since $i \neq j$, there is an index $t \in F_j$ such that $t \notin F_i$. The vertex u is sensitive to S_k for each $k \in F_i$ and, since $|F_i| = s_0(f)$, has full sensitivity. Thus $u_t \notin G$. On the other hand, since each S_k is light, u_k has full 1-sensitivity, hence $u_{k,t} \in G$ for all $k \in F_i$. This gives full 0-sensitivity to u_t. Hence $v_t \notin G$, a contradiction, since $v \in H_j$ and $t \in F_j$.

Thus there are no such edges and the Hamming distance between H_i and H_j is not equal to 1. That leaves two possibilities: either the Hamming distance between H_i and H_j is at least 2 (in which case we are done), or both H_i and H_j are equal to a single vertex v, which is not possible, as then v would have a 0-sensitivity of at least $s_0(f) + 1$.

Let $T = \bigcup_{i=1}^{|\mathcal{F}|} H_i$. We will prove that $T \neq S_0$. If each of H_i is empty, then $T = \varnothing$ and $T \neq S_0$. Otherwise there is a non-empty H_j. As $s_1(f) \geq 2$, by Theorem 2 it follows that $\dim(G \cap S_k) = \dim(S_k) - s_1(f) + 1 \leq \dim(S_0) - 1$ for each $k \in [l]$. Thus $\dim(H_j) \leq \dim(S_0) - 1$, and $H_j \neq S_0$. Then it has a neighbour subcube H'_j in S_0. But since the Hamming distance between H_j and any other H_i is at least 2, we have that $H'_j \cap H_i = \varnothing$, thus T is not equal to S_0.

Therefore, $H_1, H_2, \ldots, H_{|\mathcal{F}|}$ satisfy all the conditions of Lemma 1. Let T' be the set of vertices in $S_0 \setminus T$ with a neighbour in T. Then, by Lemma 1, $|T'| \geq |T|$ or, equivalently, $R(T', S_0) \geq R(T, S_0)$.

Then note that $R(T', S_0) \geq R(T, S_0) \geq \frac{\delta}{2^{s_1(f)-1}}$, since $R(G, S_i) = \frac{1}{2^{s_1(f)-1}}$ for all $i \in [l]$, there are a total of $(s_0(f) - 1)2^{s_1(f)-1} + \delta$ light cubes and each vertex in S_0 can have at most $s_0(f)$ neighbours in G.

Let S_h be a heavy cube, and $i \in [|\mathcal{F}|]$. The neighbours of H_i in S_h must not be in G, or the corresponding vertex in H_i would have sensitivity $s_0(f) + 1$.

Let $k \in F_i$. As S_k is light, all the vertices in $G \cap S_k$ are fully sensitive, therefore all their neighbours in $N_{k,h}$ are in G. Therefore all the neighbours of H_i in S_h already have full 0-sensitivity. Then all their neighbours must also not be in G.

This means that vertices in T' can only have neighbours in G in light cubes. But they can have at most $s_0(f) - 1$ such neighbours each, otherwise they would be in T, not in T'. As $R(T', S_0) \geq \frac{\delta}{2^{s_1(f)-1}}$, the average sensitivity of vertices in S_0 is at most

$$as(S_0) \leq s_0(f) R(S_0 \setminus T', S_0) + (s_0(f) - 1) R(T', S_0) \tag{20}$$

$$\leq s_0(f) \left(1 - \frac{\delta}{2^{s_1(f)-1}}\right) + (s_0(f) - 1) \frac{\delta}{2^{s_1(f)-1}} \tag{21}$$

$$= s_0(f) - \frac{\delta}{2^{s_1(f)-1}}. \tag{22}$$

Then by inequality (15) we have

$$m \frac{3}{2^{s_1(f)}} - \left((s_0(f) - 1)2^{s_1(f)-1} + \delta\right) \frac{1}{2^{s_1(f)}} \leq s_0(f) - \frac{\delta}{2^{s_1(f)-1}}. \tag{23}$$

Rearranging the terms, we get

$$m\frac{3}{2^{s_1(f)}} \leq \left((s_0(f)-1)2^{s_1(f)-1}+\delta\right)\frac{1}{2^{s_1(f)}} + s_0(f) - \frac{\delta}{2^{s_1(f)-1}} \tag{24}$$

$$m\frac{3}{2^{s_1(f)}} \leq s_0(f) + \frac{1}{2}(s_0(f)-1) - \frac{\delta}{2^{s_1(f)}} \tag{25}$$

$$m\frac{3}{2^{s_1(f)}} \leq \frac{3}{2}s_0(f) - \frac{1}{2} - \frac{\delta}{2^{s_1(f)}} \tag{26}$$

$$m \leq 2^{s_1(f)-1}\left(s_0(f)-\frac{1}{3}\right) - \frac{\delta}{3}. \tag{27}$$

□

Theorem 1 immediately implies Corollary 1:

Proof of Corollary 1. If f is constant, then $C(f) = s(f) = 0$ and the statement is true. Otherwise by Theorem 1

$$C(f) = \max(C_0(f), C_1(f)) \tag{28}$$

$$\leq \max_{b\in\{0,1\}}\left(\max\left(2^{s_{1-b}(f)-1}\left(s_b(f)-\frac{1}{3}\right), s_b(f)\right)\right) \tag{29}$$

$$\leq \max\left(2^{s(f)-1}\left(s(f)-\frac{1}{3}\right), s(f)\right) \tag{30}$$

On the other hand, $bs(f) \leq C(f)$ is a well-known fact. □

4 Relation Between $C_0(f)$ and $s_0(f)$ for $s_1(f) = 2$

Ambainis and Sun exhibited a class of functions that achieves the best known separation between sensitivity and block sensitivity, which is quadratic in terms of $s(f)$ [3]. This function also produces the best known separation between 0-certificate complexity and 0/1-sensitivity:

Theorem 3. *For arbitrary $s_0(f)$ and $s_1(f)$, there exists a function f such that*

$$C_0(f) = \left(\frac{2}{3}+o(1)\right)s_0(f)s_1(f). \tag{31}$$

Thus it is possible to achieve a quadratic gap between the two measures. As $bs_0(f) \leq C_0(f)$, it would be tempting to conjecture that quadratic separation is the largest possible. Therefore we are interested both in improved upper bounds and in functions that achieve quadratic separation with a larger constant factor.

In this section, we examine how $C_0(f)$ and $s_0(f)$ relate to each other for small $s_1(f)$. If $s_1(f) = 1$, it follows by Theorem 1 that $C_0(f) = s_0(f)$. Therefore we consider the case $s_1(f) = 2$.

Here we are able to construct a separation that is better than (31) by a constant factor.

Theorem 4. *There is a function f with $s_1(f) = 2$ and arbitrary $s_0(f)$ such that*

$$C_0(f) = \left\lfloor \frac{3}{4} s_0(f) s_1(f) \right\rfloor = \left\lfloor \frac{3}{2} s_0(f) \right\rfloor . \tag{32}$$

Proof. Consider the function that takes value 1 iff its 4 input bits are in either ascending or descending sorted order. Formally,

$$\textsc{Sort}_4(x) = 1 \Leftrightarrow (x_1 \leq x_2 \leq x_3 \leq x_4) \vee (x_1 \geq x_2 \geq x_3 \geq x_4). \tag{33}$$

One easily sees that $C_0(\textsc{Sort}_4) = 3$, $s_0(\textsc{Sort}_4) = 2$ and $s_1(\textsc{Sort}_4) = 2$.

Denote the 2-bit logical AND function by $\textsc{And}_2$. We have $C_0(\textsc{And}_2) = s_0(\textsc{And}_2) = 1$ and $s_1(\textsc{And}_2) = 2$.

To construct the examples for larger $s_0(f)$ values, we use the following fact (it is easy to show, and a similar lemma was proved in [3]):

Fact 1. *Let f and g be Boolean functions. By composing them with OR to $f \vee g$ we get*

$$C_0(f \vee g) = C_0(f) + C_0(g), \tag{34}$$
$$s_0(f \vee g) = s_0(f) + s_0(g), \tag{35}$$
$$s_1(f \vee g) = \max(s_1(f), s_1(g)). \tag{36}$$

Suppose we need a function with $k = s_0(f)$. Assume k is even. Then by Fact 1 for $g = \bigvee_{i=1}^{\frac{k}{2}} \textsc{Sort}_4$ we have $C_0(g) = \frac{3}{2}k$. If k is odd, consider the function $g = \left(\bigvee_{i=1}^{\frac{k-1}{2}} \textsc{Sort}_4 \right) \vee \textsc{And}_2$. Then by Fact 1 we have $C_0(g) = 3 \cdot \frac{k-1}{2} + 1 = \left\lfloor \frac{3}{2}k \right\rfloor$. □

A curious fact is that both examples of (31) and Theorem 4 are obtained by composing some primitives using OR. The same fact holds for the best examples of separation between $bs(f)$ and $s(f)$ that preceded the [3] construction [14,16].

We are also able to prove a slightly better upper bound in case $s_1(f) = 2$.

Theorem 5. *Let f be a Boolean function with $s_1(f) = 2$. Then*

$$C_0(f) \leq \frac{9}{5} s_0(f). \tag{37}$$

Proof. Let z be a vertex such that $f(z) = 0$ and $C(f, z) = C_0(f)$. Pick a 0-certificate S_0 of length $m = C_0(f)$ and $z \in S_0$. It has m neighbour subcubes which we denote by $S_1, S_2, \ldots, S_m$. Let $n' = n - m = \dim(S_i)$ for each S_i.

We work with a graph G induced on a vertex set $\{x \mid f(x) = 1\}$. Let $G_i = G \cap S_i$. As S_0 is a minimal certificate for z, we have $G_i \neq \varnothing$ for each $i \in [m]$. Since any $v \in G_i$ is sensitive to S_0, we have $s(G_i, S_i) \leq 1$. Thus by Theorem 2 either G_i is an $(n'-1)$-subcube of S_i with $R(G_i : S_i) = \frac{1}{2}$ or $R(G_i : S_i) \geq \frac{3}{4}$. We call S_i *light* or *heavy*, respectively.

Let $N_{i,j}$ be the common neighbour cube of S_i, S_j that is not S_0. Let $G_{i,j} = G \cap N_{i,j}$. Suppose $v \in S_0$. Let v_i be the neighbour of v in S_i. Let $v_{i,j}$ be the neighbour of v_i and v_j in $N_{i,j}$.

Let S_i, S_j be light. By G_i^0, G_j^0 denote the neighbour cubes of G_i, G_j in S_0. We call $\{S_i, S_j\}$ a *pair*, iff $G_i^0 \cup G_j^0 = S_0$. In other words, a pair is defined by a single dimension. Also we have either $z_i \notin G$ or $z_j \notin G$: we call the corresponding cube the *representative* of this pair.

Proposition 2. *Let $\mathcal{P}$ be a set of mutually disjoint pairs of the neighbour cubes of S_0. Then there exists a 0-certificate S_0' such that $z \in S_0'$, $\dim(S_0') = \dim(S_0)$ and S_0' has at least $|\mathcal{P}|$ heavy neighbour cubes.*

Proof. Let $\mathcal{R}$ be a set of mutually disjoint pairs of the neighbour cubes of S_0. W.l.o.g. let $S_1, \ldots, S_{|\mathcal{R}|}$ be the representatives of $\mathcal{R}$. Let F_i be the neighbour cube of $S_i \setminus G$ in S_0. Let $B_\mathcal{R} = \bigcap_{i=1}^{|\mathcal{R}|} F_i$. Suppose $S_0 + x$ is a coset of S_0 and $x_t = 0$ if the t-th dimension is not fixed in S_0: let $B_\mathcal{R}(S_0 + x)$ be $B_\mathcal{R} + x$.

Pick $\mathcal{R} \subseteq \mathcal{P}$ with the largest size, such that for each two representatives S_i, S_j of $\mathcal{R}$, $B_\mathcal{R}(N_{i,j})$ is a 0-certificate.

Next we prove that the subcube S_0' spanned by $B_\mathcal{R}, B_\mathcal{R}(S_1), \ldots, B_\mathcal{R}\left(S_{|\mathcal{R}|}\right)$ is a 0-certificate. It corresponds to an $|\mathcal{R}|$-dimensional hypercube $Q_{|\mathcal{R}|}$ where $B_\mathcal{R}(S_0 + x)$ corresponds to a single vertex for each coset $S_0 + x$ of S_0.

Let $T \subseteq Q_{|\mathcal{R}|}$ be the graph induced on the set $\{v \mid v$ corresponds to $B_\mathcal{R}(S_0 + x), B_\mathcal{R}(S_0 + x)$ is not a 0-certificate$\}$. Then we have $s(T, Q_{|\mathcal{R}|}) \leq 2$. Suppose $B_\mathcal{R}$ corresponds to $0^{|\mathcal{R}|}$. Let L_d be the set of $Q_{|\mathcal{R}|}$ vertices that are at distance d from $0^{|\mathcal{R}|}$. We prove by induction that $L_d \cap T = \varnothing$ for each d.

Proof. **Base case.** $d \leq 2$. The required holds since all $B_\mathcal{R}, B_\mathcal{R}(S_i), B_\mathcal{R}(N_{i,j})$ are 0-certificates.

Inductive step. $d \geq 3$. Examine $v \in L_d$. As v has d neighbours in L_{d-1}, $L_{d-1} \cap T = \varnothing$ and $s(T, Q_{|\mathcal{R}|}) \leq 2$, we have that $v \notin T$.

Let k be the number of distinct dimensions that define the pairs of $\mathcal{R}$, then $k \leq |\mathcal{R}|$. Hence $\dim(S_0') = |\mathcal{R}| + \dim(B_\mathcal{R}) = |\mathcal{R}| + (\dim(S_0) - k) \geq \dim(S_0)$. But S_0 is a minimal 0-certificate for z, therefore $\dim(S_0') = \dim(S_0)$.

Note that a light neighbour S_i of S_0 is separated into a 0-certificate and a 1-certificate by a single dimension, hence we have $s(G, S_i, v) = 1$ for every $v \in S_i$. As S_i neighbours S_0, every vertex in its 1-certificate is fully sensitive. The same holds for any light neighbour S_i' of S_0'.

Now we will prove that each pair in $\mathcal{P}$ provides a heavy neighbour for S_0'. Let $\{S_a, S_b\} \in \mathcal{P}$, where S_a is the representative. We distinguish two cases:

- $B_\mathcal{R}(S_b)$ is a 1-certificate. Since S_b is light, it has full 1-sensitivity. Therefore, $v \in G$ for all $v \in B_R(N_{i,b})$, for each $i \in [|\mathcal{R}|]$. Let S_b' be the neighbour of S_0' that contains $B_\mathcal{R}(S_b)$ as a subcube. Then for each $v \in B_\mathcal{R}(S_b)$ we have $s(G, S_b', v) = 0$. Hence S_b' is heavy.
- Otherwise, $\{S_a, S_b\}$ is defined by a different dimension than any of the pairs in $\mathcal{R}$. Let $\mathcal{R}' = \mathcal{R} \cup \{S_a, S_b\}$. Examine the subcube $B_{\mathcal{R}'}$. By definition of $\mathcal{R}$, there is a representative S_i of $\mathcal{R}$ such that $B_{\mathcal{R}'}(N_{i,a})$ is not a 0-certificate. Let S_a' be the neighbour of S_0' that contains $B_\mathcal{R}(S_a)$ as a subcube. Then there is a vertex $v \in B_{\mathcal{R}'}(S_a)$ such that $s(G, S_a', v) \geq 2$. Hence S_a' is heavy. $\square$

Let $\mathcal{P}$ be the largest set of mutually disjoint pairs of the neighbour cubes of S_0. Let l and $h = m - l$ be the number of light and heavy neighbours of S_0, respectively. Each pair in $\mathcal{P}$ gives one neighbour in G to each vertex in S_0. Now examine the remaining $l - 2|\mathcal{P}|$ light cubes. As they are not in $\mathcal{P}$, no two of them form a pair. Hence there is a vertex $v \in S_0$ that is sensitive to each of them. Then $s_0(f) \geq s_0(f, v) \geq |\mathcal{P}| + (l - 2|\mathcal{P}|) = l - |\mathcal{P}|$. Therefore $|\mathcal{P}| \geq l - s_0(f)$.

Let q be such that $m = qs_0(f)$. Then there are $qs_0(f) - l$ heavy neighbours of S_0. On the other hand, by Proposition 2, there exists a minimal certificate S_0' of z with at least $l - s_0(f)$ heavy neighbours. Then z has a minimal certificate with at least $\frac{(qs_0(f)-l)+(l-s_0(f))}{2} = \frac{q-1}{2} \cdot s_0(f)$ heavy neighbour cubes.

W.l.o.g. let S_0 be this certificate. Then $l = qs_0(f) - h \leq (q - \frac{q-1}{2})s_0(f) = \frac{q+1}{2} \cdot s_0(f)$. As each $v \in G_i$ for $i \in [m]$ gives sensitivity 1 to its neighbour in S_0,

$$l\frac{1}{2} + h\frac{3}{4} \leq s_0(f). \tag{38}$$

Since the constant factor at l is less than at h, we have

$$\frac{q+1}{2} \cdot s_0(f) \cdot \frac{1}{2} + \frac{q-1}{2} \cdot s_0(f) \cdot \frac{3}{4} \leq s_0(f) \tag{39}$$

By dividing both sides by $s_0(f)$ and simplifying terms, we get $q \leq \frac{9}{5}$. □

This result shows that the bound of Corollary 1 can be improved. However, it is still not tight. For some special cases, through extensive casework we can also prove the following results:

Theorem 6. *Let f be a Boolean function with $s_1(f) = 2$ and $s_0(f) \geq 3$. Then*

$$C_0(f) \leq 2s_0(f) - 2. \tag{40}$$

Theorem 7. *Let f be a Boolean function with $s_1(f) = 2$ and $s_0(f) \geq 5$. Then*

$$C_0(f) \leq 2s_0(f) - 3. \tag{41}$$

The proofs of these theorems are available online in the full version of the paper [2].

These theorems imply that for $s_1(f) = 2$, $s_0(f) \leq 6$ we have $C_0(f) \leq \frac{3}{2}s_0(f)$, which is the same separation as achieved by the example of Theorem 4. This leads us to the following conjecture:

Conjecture 1. Let f be a Boolean function with $s_1(f) = 2$. Then

$$C_0(f) \leq \frac{3}{2}s_0(f). \tag{42}$$

We consider $s_1(f) = 2$ to be the simplest case where we don't know the actual tight upper bound on $C_0(f)$ in terms of $s_0(f), s_1(f)$. Proving Conjecture 1 may provide insights into relations between $C(f)$ and $s(f)$ for the general case.

References

1. Ambainis, A., Bavarian, M., Gao, Y., Mao, J., Sun, X., Zuo, S.: Tighter relations between sensitivity and other complexity measures. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (eds.) ICALP 2014. LNCS, vol. 8572, pp. 101–113. Springer, Heidelberg (2014)
2. Ambainis, A., Prūsis, K., Vihrovs, J.: Sensitivity versus certificate complexity of Boolean functions. CoRR, abs/1503.07691 (2016)
3. Ambainis, A., Sun, X.: New separation between $s(f)$ and $bs(f)$. CoRR, abs/1108.3494 (2011)
4. Ambainis, A., Vihrovs, J.: Size of sets with small sensitivity: a generalization of simon's lemma. In: Jain, R., Jain, S., Stephan, F. (eds.) TAMC 2015. LNCS, vol. 9076, pp. 122–133. Springer, Heidelberg (2015)
5. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM **48**(4), 778–797 (2001)
6. Buhrman, H., de Wolf, R.: Complexity measures and decision tree complexity: a survey. Theor. Comput. Sci. **288**(1), 21–43 (2002)
7. Cook, S., Dwork, C., Reischuk, R.: Upper and lower time bounds for parallel random access machines without simultaneous writes. SIAM J. Comput. **15**, 87–97 (1986)
8. Gilmer, J., Koucký, M., Saks, M.E.: A communication game related to the sensitivity conjecture. CoRR, abs/1511.07729 (2015)
9. Gopalan, P., Nisan, N., Servedio, R.A., Talwar, K., Wigderson, A.: Smooth Boolean functions are easy: Efficient algorithms forlow-sensitivity functions. In: Proceedings of the 2016 ACM Conference on Innovations inTheoretical Computer Science, ITCS 2016, pp. 59–70. ACM, New York, NY, USA (2016)
10. Hatami, P., Kulkarni, R., Pankratov, D.: Variations on the sensitivity conjecture. In: Number 4 in Graduate Surveys. Theory of Computing Library (2011)
11. Kenyon, C., Kutin, S.: Sensitivity, block sensitivity, and ℓ-block sensitivity of Boolean functions. Inf. Comput. **189**(1), 43–53 (2004)
12. Lin, C., Zhang, S.: Sensitivity conjecture and log-rank conjecture for functions with small alternating numbers. CoRR, abs/1602.06627 (2016)
13. Nisan, N.: CREW PRAMS and decision trees. In: Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing, STOC 1989, pp. 327–335. ACM, New York, NY, USA (1989)
14. Rubinstein, D.: Sensitivity vs. block sensitivity of Boolean functions. Combinatorica **15**(2), 297–299 (1995)
15. 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, London (1983)
16. Virza, M.: Sensitivity versus block sensitivity of Boolean functions. Inf. Process. Lett. **111**(9), 433–435 (2011)

http://www.springer.com/978-3-319-34170-5

Computer Science – Theory and Applications
11th International Computer Science Symposium in Russia, CSR 2016, St. Petersburg, Russia, June 9-13, 2016, Proceedings
Kulikov, A.S.; Woeginger, G.J. (Eds.)
2016, XXI, 425 p. 49 illus., Softcover
ISBN: 978-3-319-34170-5