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

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 certificate complexity is polynomially related to sensitivity. Previously, it has been shown that $bs(f) \leq C(f) \leq 2^{s(f)} - 1$. In this work, we give a better upper bound of $bs(f) \leq C(f) \leq \max \left( \frac{2^{s(f)}}{3}, s(f) \right)$ using a recent theorem limiting the structure of function graphs. We also examine relations between these measures for functions with small 1-sensitivity $s_1(f)$ 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 [10, 15, 6].

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 to be quite difficult to solve. It has been known for more than 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 [11, 13, 14] but the best upper bounds on block sensitivity in terms of sensitivity are still exponential (of the form $bs(f) \leq c^{s(f)}$) [12, 02].
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.

Which of those equivalent forms of the conjecture is the most promising one? We think that certificate complexity, $C(f)$, is the combinatorially simplest among all of these complexity measures. Certificate complexity being at least $c$ simply means that there is an input $x = (x_1, \ldots, x_n)$ that is not contained in a $(n - (c - 1))$-dimensional subcube of the Boolean hypercube on which $f$ is constant. Therefore, we now focus on the “sensitivity vs. certificate complexity” form of the conjecture.

1.1 Prior Work

The best upper bound on certificate complexity in terms of sensitivity is

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

(1)

due to Ambainis et al. [2]. The bounds for $C_0(f)$ also hold for $C_1(f)$ symmetrically (in this case, $C_1(f) \leq 2^{s_0(f) - 1} s_1(f) - (s_0(f) - 1)$), so it is sufficient to focus on the former.

Since $bs(f) \leq C(f)$, this immediately implies that

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

(2)

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 not identical to 1. Then

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

(3)

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

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

(4)

1 Here, $C_0$ ($C_1$) and $s_0$ ($s_1$) stand for certificate complexity and sensitivity, restricted to inputs $x$ with $f(x) = 0$ ($f(x) = 1$).
On the other hand, we show the examples of functions that give the largest known separations between $C_0(f)$ and $s_0(f), s_1(f)$. The function of Ambainis and Sun [3] gives the separation of

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

(5)

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

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

(6)

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 (1). So, the easiest non-trivial case is $s_1(f) = 2$, for which (1) becomes $C_0(f) \leq 2s_0(f) - 1$.

For $s_1(f) = 2$ and $s_0(f) \leq 5$, we show that our example is optimal. Therefore we conjecture that our example is optimal for any $s_0(f)$ when $s_1(f) = 2$, however, for larger values of $s_0(f)$ we can only show that $C_0(f) \leq 2s_0(f) - 2$, very slightly improving the best known upper bound.

Our results rely on a recent “gap theorem” by Ambainis and Vihrovs [4] which says that any sensitivity-$s$ subset $S$ of the Boolean hypercube must be either of size $2^n - s$ or of size at least $\frac{3}{4} 2^n - s$ and, in the first case, $S$ can only be a subcube obtained by fixing $s$ variables. Using this theorem allows refining earlier results which used Simon’s lemma [12]—any sensitivity-$s$ subset $S$ must be of size at least $2^{n-s}$—but did not use any more detailed information about the structure of such $S$.

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 input $x$ is denoted by $x_i$. For an index set $S \subseteq [n]$, let $x_S$ be the input obtained from $x$ by flipping every bit $x_i$, $i \in S$.

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. [8].

**Definition 1.** The sensitivity complexity $s(f, x)$ of $f$ on an input $x$ is defined as $|\{i \mid f(x) \neq f(x^{(i)})\}|$. The $z$-sensitivity $s_z(f)$ of $f$, where $z \in \{0,1\}$, is defined as $\max(s(f, x) \mid x \in \{0,1\}^n, f(x) = z)$. The sensitivity $s(f)$ of $f$ is defined as $\max(s_0(f), s_1(f))$. 
Definition 2. The block sensitivity $bs(f, x)$ of $f$ on input $x$ is defined as the maximum number $b$ such that there are $b$ pairwise disjoint subsets $B_1, \ldots, B_b$ of $[n]$ for which $f(x) \neq f(x^{B_i})$. We call each $B_i$ a block. The $z$-block sensitivity $bs_z(f)$, where $z \in \{0,1\}$, is defined as $\max( bs(f, x) \mid x \in \{0,1\}^n, f(x) = z )$. 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 input $x$ is defined as a partial assignment $c : S \to \{0,1\}, S \subseteq [n]$ of $x$ such that $f$ is constant on this restriction. 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 input $x$ is defined as the minimum length of a certificate that $x$ satisfies. The $z$-certificate complexity $C_z(f)$, where $z \in \{0,1\}$, is defined as $\max( C(f, x) \mid x \in \{0,1\}^n, f(x) = z )$. 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 $S \subseteq \{0,1\}$ as subgraphs (induced by the subset of vertices $S$) in this graph.

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

Note that there each certificate of length $l$ corresponds to one subcube of $Q_n$ with co-dimension $l$.

Definition 6. Let $X$ and $Y$ be induced subgraphs of $Q_n$. By $X \cap Y$ denote the intersection of $X$ and $Y$ that is the graph induced on $V(X) \cap V(Y)$. By $X \cup Y$ denote the union of $X$ and $Y$ that is the graph induced on $V(X) \cup V(Y)$. By $X^c$ denote the complement of $Y$ in $X$ that is the graph induced by $V(X) \setminus V(Y)$.

Definition 7. Let $X$ and $Y$ be induced subgraphs of $Q_n$. By $R(X, Y)$ denote the relative size of $X$ in $Y$:

$$R(G, Q_n) = \frac{|X \cap Y|}{|Y|}.$$  

(7)

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

Definition 8. Let $G$ be a non-empty induced subgraph of $Q_n$. The sensitivity $s(G, x)$ of a vertex $x$ is defined as $|\{ i \mid x^{(i)} \notin G \}|$, if $x \in G$, and $|\{ i \mid x^{(i)} \in G \}|$, if $x \notin G$. The sensitivity of $G$ is defined as $\max( s(G, x) \mid x \in G )$.

Our results rely on the following generalization of Simon’s lemma [12], proved by Ambainis and Vihrovs [3].

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


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 not identical to 1. Then

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

(8)

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

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

$$S = \{ x \mid \exists u \ (x \in H_u) \},$$

(9)

$$S' = \{ x \mid \exists i \ (x^{(i)} \in S) \} \setminus S.$$  

(10)

If $S \neq Q_n$, then $|S'| \geq |S|$.

Proof. If $k = 1$, then the co-dimension of $H_1$ is at least 1. Hence $H_1$ has a neighbour cube, so $|S'| \geq |S| = |H_1|.$

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 $S'$, hence $|S'| = |S| = 2$.

Inductive step. Divide $Q_n$ into two adjacent $(n - 1)$-dimensional subcubes $Q_0$ and $Q_1$ by the value of $x_1$. We will prove that the conditions of the lemma hold for each $S \cap Q_b$, $b \in \{0, 1\}$. Let $H_u^b = H_u \cap Q_b.$ Assume $H_u^b \neq \emptyset$ 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, $Q_b \subseteq S$, since then $k$ would be at most 1.

Let $S_b = S \cap Q_b$ and $S_b^i = \{ x \mid \exists i \ (x^{(i)} \in S_h) \} \setminus S_b.$ Then by induction we have that $|S_b^i| \geq |S_b|$. On the other hand, $S_0 \cup S_1 = S$ and $S_0' \cup S_1' \subseteq S'$. Thus we have

$$|S'| \geq |S_0'| + |S_1'| \geq |S_0| + |S_1| = |S|.$$  

(11)

Proof of Theorem 1. Further assume $f$ is not always 0, since then $C_0(f) = s_0(f) = 0$ and the statement holds.

We work with a graph $G$ induced on a vertex set $\{ x \mid f(x) = 1 \}$. 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 $S_1, S_2, \ldots, S_m$. Since $S_0$ is a minimum certificate for $z$, $S_i \cap G \neq \emptyset$ 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 within \( S_i \) each vertex in \( G \) has 1-sensitivity at most \( s_1(f) - 1 \).

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 \( G \cap S_1 \), so \( m \leq s_0(f) \).

Otherwise \( s_1(f) \geq 2 \). By Theorem 2, either \( R(G, S_i) = \frac{1}{2^{s_1(f)-1}} \) or \( R(G, S_i) \geq \frac{1}{2s_1(f)} \) 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 \( x \in S_0 \) be \( as(S_0) \). Since each vertex of \( G \) in any \( S_i \) gives sensitivity 1 to some vertex in \( S_0 \), \( \sum_{i=1}^{m} R(G, S_i) \leq as(S_0) \). Obviously \( as(S_0) \leq s_0(f) \). We have that

\[
\frac{1}{2^{s_1(f)-1}} + (m - l) \left( \frac{3}{2^{s_1(f)}} \right) \leq as(S_0) \leq s_0(f)
\]

(12)

\[
m \left( \frac{3}{2^{s_1(f)}} \right) - l \left( \frac{1}{2^{s_1(f)}} \right) \leq as(S_0) \leq s_0(f).
\]

(13)

Then we examine two possible cases.

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

\[
m \left( \frac{3}{2^{s_1(f)}} \right) - (s_0(f) - 1)2^{s_1(f)-1} \leq as(S_0) \leq s_0(f)
\]

(14)

\[
m \left( \frac{3}{2^{s_1(f)}} \right) \leq s_0(f) + \frac{1}{2}(s_0(f) - 1)
\]

(15)

\[
m \left( \frac{3}{2^{s_1(f)}} \right) \leq \frac{3}{2}s_0(f) - \frac{1}{2}
\]

(16)

\[
m \leq 2^{s_1(f)-1} \left( s_0(f) - \frac{1}{3} \right).
\]

(17)

**Case 2.** \( l = (s_0(f) - 1)2^{s_1(f)-1} + \epsilon \) for some \( \epsilon > 0 \). Since \( s_1(f) \geq 2 \), the number of light cubes is at least \( 2(s_0(f) - 1) + \epsilon \), 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 \( T_1, T_2, \ldots, T_\|\mathcal{F}\| \) - subgraphs of \( S_0 \), where \( T_i \) 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 their intersections and \( T_i \).

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 \( N_{i,j} \).

We will show that the Hamming distance between any two subcubes \( T_i \) and \( T_j, i \neq j \) is at least 2.

Assume there is an edge \((u, v)\) such that \( u \in T_i \) and \( v \in T_j \). 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 $u_t \not\in G$. 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 $v_t \not\in G$, a contradiction, since $v \in T_j$ and $t \in F_j$.

Thus there are no such edges, and the Hamming distance between $T_i$ and $T_j$ is not equal to 1. That leaves two possibilities: either the Hamming distance between $T_i$ and $T_j$ is at least 2 (in which case we are done), or both $T_i$ and $T_j$ 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 $T = \bigcup_{i=1}^{n} T_i$. We will prove that $T \neq S_0$. Since $s_1(f) \geq 2$, by Theorem 2 it follows that $\dim(G \cap S_i) = \dim(S_i) - s_1(f) + 1 \leq \dim(S_0) - 1$ for each $i \in [l]$. Thus $\dim(T_i) \leq \dim(S_0) - 1$, and $T_i \neq S_0$. Then it has a neighbour subcube $T'_i$ in $S_0$. But since the Hamming distance between $T_i$ and any other $T_i$ is at least 2, we have that $T'_i \cap T_i = \emptyset$, thus $T$ is not equal to $S_0$.

Therefore $T_1, T_2, \ldots, T_{|F|}$ and $T$ 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 $R(T', S_0) \geq R(T, S_0)$.

Then note that $R(T', S_0) \geq R(T, S_0) \geq \frac{\epsilon}{2^{s_1(f)}}$, since $R(G, S_i) = \frac{1}{2^{s_1(f)}}$ for all $i \in [l]$, there are a total of $(s_0(f) - 1)2^{s_1(f)} + \epsilon$ 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 $i \in [l]$ $F$. The neighbours of $T_i$ in $S_h$ must not be in $G$, otherwise the corresponding vertex in $T_i$ would have sensitivity $s_0(f) + 1$.

Let $j \in F_i$. As $S_j$ is light, all the vertices in $G \cap S_j$ are fully sensitive, therefore all their neighbours in $N_{j,h}$ are in $G$. Therefore all the neighbours of $T_i$ in $S_h$ already have full 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 $R(T', S_0) \geq \frac{\epsilon}{2^{s_1(f)}}$, the average sensitivity of vertices in $S_0$ is at most

$$as(S_0) \leq s_0(f)R(S_0 \setminus T', S_0) + (s_0(f) - 1)R(T', S_0) \leq s_0(f)\left(1 - \frac{\epsilon}{2^{s_1(f)}}\right) + (s_0(f) - 1)\frac{\epsilon}{2^{s_1(f)}-1}$$

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

Then by inequality (13) we have

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

Then by inequality (13) we have

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

(21)
Rearranging the terms, we get

\[ m \frac{3}{2^{s(f)}} \leq \left( (s_0(f) - 1)2^{s_1(f) - 1} + \epsilon \right) \frac{1}{2^{s_1(f)}} + s_0(f) - \frac{\epsilon}{2^{s_1(f) - 1}} \]  

(22)

\[ m \frac{3}{2^{s(f)}} \leq s_0(f) + \frac{1}{2}(s_0(f) - 1) - \frac{\epsilon}{2^{s_1(f)}} \]  

(23)

\[ m \frac{3}{2^{s(f)}} \leq \frac{3}{2} s_0(f) - \frac{1}{2} - \frac{\epsilon}{2^{s_1(f)}} \]  

(24)

\[ m \leq 2^{s_1(f) - 1} \left( s_0(f) - \frac{1}{3} \right) - \frac{\epsilon}{3} \]  

(25)

\[ \square \]

Theorem 1 immediately implies Corollary 1.

**Proof of Corollary 1** If \( f \) is always constant, then \( C(f) = s(f) = 0 \) and the statement is true. Otherwise \( s_0(f), s_1(f) \geq 1 \) and by Theorem 1

\[ C(f) = \max(C_0(f), C_1(f)) \leq \]  

(26)

\[ \leq \max_{z \in \{0,1\}} \left( \max \left( 2^{s_1-1}(f) - 1 \left( s_z(f) - \frac{1}{3} \right), s_z(f) \right) \right) \leq \]  

(27)

\[ \leq \max \left( 2^{s(f) - 1} \left( s(f) - \frac{1}{3} \right), s(f) \right) \]  

(28)

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

\[ \square \]

4 Quadratic Separation between Certificate Complexity and Sensitivity

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

One can easily check that for this type of function we have

\[ C_0(f) = \left( \frac{2}{3} + o(1) \right) s_0(f)s_1(f). \]  

(29)

Here we have the nice property that \( s_0(f) \) and \( s_1(f) \) can be arbitrary.

Thus it is possible to achieve a quadratic gap between these two measures. As \( bs_0(f) \leq C_0(f) \), it would be tempting to conjecture that the quadratic separation is the largest possible.
5  Relation between $C_0(f)$ and $s_0(f)$ for Small Values of $s_1(f)$

In this section, we examine how $C_0(f)$ and $s_0(f)$ relate to each other for small fixed values of $s_1(f)$. If $s_1(f) = 1$, it follows by (1) that $C_0(f) \leq s_0(f)$, hence $C_0(f) = s_0(f)$. Next we consider the cases $s_1(f) = 2$ and $s_1(f) = 3$.

5.1  Case $s_1(f) = 2$

Here we are able to construct a separation that is better than (29) by a constant factor.

**Theorem 3.** There is a function $f$ with $s_1(f) = 2$ and arbitrary $s_0(f)$ such that

$$C_0(f) = \left\lfloor \frac{3}{4}s_0(f)s_1(f) \right\rfloor = \left\lfloor \frac{3}{2}s_0(f) \right\rfloor. \tag{30}$$

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

$$\text{Sort}_4(x) = 1 \Leftrightarrow (x_1 \leq x_2 \leq x_3 \leq x_4) \lor (x_1 \geq x_2 \geq x_3 \geq x_4). \tag{31}$$

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

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

To construct the examples for larger $s_0(f)$ values, we use the following fact:

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

$$C_0(f \lor g) = C_0(f) + C_0(g), \tag{32}$$

$$s_0(f \lor g) = s_0(f) + s_0(g), \tag{33}$$

$$s_1(f \lor g) = \max(s_1(f), s_1(g)). \tag{34}$$

This fact is easy to show, and a similar lemma was proved in [3].

Suppose we need a function with $k = s_0(f)$. Assume $k$ is even. Then by Fact 1 for $g = \bigvee_{i=1}^{\frac{3}{2}k} \text{Sort}_4$ we have $C_0(g) = \frac{3}{4}k$. If $k$ is odd, consider the function $g = \left(\bigvee_{i=1}^{\frac{3}{2}k} \text{Sort}_4\right) \lor \text{And}_2$. Then by Fact 1 we have $C_0(g) = 3 \cdot \frac{k-1}{2} + 1 = \left\lfloor \frac{3}{2}k \right\rfloor$. \hfill $\square$

A curious fact is that both examples of (29) and Theorem 3 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 Ambainis’ and Sun’s construction [11,13].

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

2 The Sort$_4$ function was first introduced by Ambainis in [1].
Theorem 4. Let $f$ be a Boolean function with $s_1(f) = 2$ and $s_0(f) \geq 3$. Then

$$C_0(f) \leq 2s_0(f) - 2. \quad (35)$$

Proof. Let $G$ be a graph induced on a vertex set $\{x \mid f(x) = 1\}$. Suppose $z$ is 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 $S_1, S_2, \ldots, S_m$. Since $S_0$ is a minimum certificate for $z$, we have that $S_i \cap G \neq \emptyset$ for $i \in [m]$. Let the dimension of $S_0$ be $n'$.

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 $N_{i,j}$.

As $S_0$ is a 0-certificate, each vertex of $G$ in any $S_i$ is sensitive to its neighbour in $S_0$. Thus 1-sensitivity in each $S_i$ is at most 1. By Theorem 2, it follows that either $R(G, S_i) = \frac{1}{2}$ and $G \cap S_i$ is a $(n' - 1)$-dimensional subcube or $R(G, S_i) \geq \frac{3}{4}$. We call such subcubes light or heavy respectively. Let the number of light cubes be $l$, then the number of heavy cubes is $m - l$. Assume the light cubes are $S_1, S_2, \ldots, S_l$.

Each vertex of $G$ in any $S_i$ gives sensitivity 1 to its neighbour in $S_0$, thus

$$\sum_{i=1}^{m} R(G, S_i) \leq s_0(f). \quad (36)$$

Hence

$$l \frac{1}{2} + (m - l) \frac{3}{4} \leq s_0(f), \quad (37)$$

$$3m - 4s_0(f) \leq l. \quad (38)$$

Assume on the contrary that $C_0(f) > 2s_0(f) - 2$ or equivalently $m \geq 2s_0(f) - 1$. In that case $l \geq 3(2s_0(f) - 1) - 4s_0(f) = 2s_0(f) - 3$.

Let $s_0(f) = 3$, then $l \geq 3$. First assume $l = 3$. Then $S_1, S_2, S_3$ are light and $S_4, S_5$ are heavy. This implies

$$3 = s_0(f) \geq \sum_{i=1}^{m} R(G, S_i) \geq 3 \cdot \frac{1}{2} + 2 \cdot \frac{3}{4} = 3. \quad (39)$$

Thus for each $j \in \{4, 5\}$ we have $R(G, S_j) = \frac{3}{4}$, which means that $R(S_j \setminus G, S_j) = \frac{1}{4}$. By Theorem 2 0-sensitivity in $S_j$ is at least 2. Let $v_j \not\in G$ be a vertex with sensitivity 2 in $S_j$. Assume $v_j \in G$ for some $i \in [3]$. As $v_i$ has full sensitivity, its neighbour $v_{i,j} \in G$. Hence there is at most one such $i \in [3]$ that $v_i \in G$. But then $v \in S_0$ can only have neighbours in $G$ in one light and one heavy cube. Hence $v$ does not have full sensitivity: a contradiction, since $\sum_{i=1}^{m} R(G, S_i) = 3$.

Thus we have $l \geq 4$ for $s_0(f) = 3$.

Now let $s_0(f) \geq 3$. Assume there is a vertex $v \in S_0$ that has $s_0(f)$ neighbours in $G$ among light cubes. Let $S_i$ be a light cube with $v_i \in G$. If $s_0(f) \geq 4$, then $l \geq 2s_0(f) - 3 > s_0(f)$, if $s_0(f) = 3$, then $l \geq 4 > 3$. Thus $l > s_0(f)$. Hence there
is a light cube $S_j$ such that $v_j \notin G$. Since $v_i$ has full sensitivity, $v_{i,j} \in G$, and there are $s_0(f)$ such $i$. But $v_j$ is also sensitive to one neighbour in $S_j$; hence $v_j$ has sensitivity $s_0(f) + 1$, a contradiction.

Thus any vertex $v \in S_0$ has at most $s_0(f) - 1$ neighbours in $G$ in light cubes. Then $l \leq 2(s_0(f) - 1)$, otherwise we would have a contradiction by the pigeonhole principle. If there are no heavy cubes, then $m = l \leq 2s_0(f) - 2$ and we are done. Otherwise there is a heavy cube $S_h$. Let $S'$ be the subset of vertices in $S_0$ that each has exactly $s_0(f) - 1$ neighbours in $G$ in light cubes. Since $l \geq 2s_0(f) - 3$, we have $R(S', S_0) \geq \frac{1}{2}$.

Pick a vertex $v \in S'$. Let $S_i, S_j$ be light cubes with $v_i \in G$ and $v_j \notin G$. If $s_0(f) \geq 4$, then by $l \geq 2s_0(f) - 3$ we have that the number of choices for $j$ is at least $(2s_0(f) - 3) - (s_0(f) - 1) = 2$; if $s_0(f) = 3$, then since $l \geq 4$, this number is also at least 2. Since $v_j$ has full sensitivity, $v_{i,j} \in G$, and there are $s_0(f) - 1$ choices for $i$. On the other hand, as $S_j$ is a light cube, $v_j$ is sensitive to a neighbour in $S_j$. Hence $v_j$ has full sensitivity, so its neighbour $v_{j,h} \notin G$. But then $v_h$ has at least 3 neighbours not in $G$, and, as $s_1(f) = 2$, we have $v_h \notin G$.

This shows that for a vertex $v \in S'$, its neighbour in $S_h$ does not belong to $G$. Let $S'_0$ be the set of $S'$ neighbours in $S_h$. Then $R(S_h \setminus G, S_h) \geq R(S'_h, S_h) = R(S', S_0) \geq \frac{1}{2}$; a contradiction, since $S_h$ is a heavy cube.

This result together with Theorem 1 proves that (30) is the optimal separation for $s_1(f) = 2$, $s_0(f) \leq 4$. It is possible to show by a more detailed analysis that it is also optimal for $s_1(f) = 2$, $s_0(f) = 5$. Thus we conjecture that this separation is optimal in the general case.

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

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

(40)

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 tight relations between $C_0(f)$ and $s_0(f), s_1(f)$.

### 5.2 Case $s_1(f) = 3$

In this case, taking a $C_0(f) = (\frac{3}{4} + o(1)) s_0(f) s_1(f)$ separation for $s_1(f) = 3$ gives a $C_0(f) = [2s_0(f)]$ separation for arbitrary $s_0(f)$. For $s_0(f) = 1$ this is optimal by Theorem 1. It can also be proved that it is optimal for $s_0(f) = 2$:

**Theorem 5.** For a Boolean function $f$ with $s_1(f) = 3$, $s_0(f) = 2$, $C_0(f) \leq 4$.

The full proof contains extensive case analysis, hence we omit it. We present the main lemma we have used for the proof.

In the previous proofs we looked at the neighbour cubes $S_1, S_2, \ldots, S_{C_0(f)}$ of a minimal certificate $S_0$ with length $C_0(f)$. Here we use Lemma 2 which allows us to limit the structure of $G \cap S_i$ for $s_1(f) = 3$, $s_0(f) = 2$. Note that $s_0$ and $s_1$ are both at most 2 in each $S_i$, because $S_0$ is a 0-certificate.
The lemma heavily relies on Theorem 2 and the related notion of irreducible subgraphs of the hypercube, both introduced in [4].

**Definition 9.** Let $G$ be a subgraph of $Q_n$. We call $G$ irreducible, if for all $i \in [n], b \in \{0, 1\}$ there exists a vertex $x \in G$ such that $x_i = b$.

**Lemma 2.** Let $G$ be a non-empty subgraph of $Q_n$ induced on the vertex set $\{x \mid f(x) = 1\}$ of a function $f$ with $s_0(f) \leq 2, s_1(f) \leq 2$. Then $G$ is either a union of two $(n-2)$-dimensional subcubes or an irreducible subgraph of $Q_n$ with $R(G, Q_n) \geq \frac{1}{2}$.

As both $s_0$ and $s_1$ are at most 2 in each of $S_i$, it is either the case that $R(G \cap S_i, Q_n) \geq \frac{1}{2}$ or $G \cap S_i$ is isomorphic to only a few types of graphs, which are simple to analyse individually.

**References**

1. A. Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220 – 238, 2006.
2. A. Ambainis, M. Bavarian, Y. Gao, J. Mao, X. Sun, and S. Zuo. Tighter relations between sensitivity and other complexity measures. In J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, editors, *International Colloquium on Automata, Languages, and Programming*, volume 8572 of *Lecture Notes in Computer Science*, pages 101–113. Springer Berlin Heidelberg, 2014.
3. A. Ambainis and X. Sun. New separation between $s(f)$ and $bs(f)$. *CoRR*, abs/1108.3494, 2011.
4. A. Ambainis and J. Vihrovs. Size of sets with small sensitivity: a generalization of Simon’s lemma. *TAMC 2015, to appear*, 2015.
5. R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001.
6. H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21 – 43, 2002.
7. S. Cook, C. Dwork, and R. Reischuk. Upper and lower time bounds for parallel random access machines without simultaneous writes. *SIAM Journal on Computing*, 15:87–97, 1986.
8. P. Hatami, R. Kulkarni, and D. Pankratov. Variations on the Sensitivity Conjecture. Number 4 in Graduate Surveys, Theory of Computing Library, 2011.
9. C. Kenyon and S. Kutin. Sensitivity, block sensitivity, and $\ell$-block sensitivity of Boolean functions. *Information and Computation*, 189(1):43 – 53, 2004.
10. N. Nisan. CREW PRAMS and decision trees. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC ’89, pages 327–335, New York, NY, USA, 1989. ACM.
11. D. Rubinstein. Sensitivity vs. block sensitivity of Boolean functions. *Combinatorica*, 15(2):297–299, 1995.
12. H.-U. Simon. A tight $\Omega(\log \log N)$-bound on the time for parallel RAM’s to compute nondegenerated Boolean functions. In *Proceedings of the 1983 International FCT-Conference on Fundamentals of Computation Theory*, pages 439–444, London, UK, 1983. Springer-Verlag.
13. M. Virza. Sensitivity versus block sensitivity of Boolean functions. *Information Processing Letters*, 111(9):433 – 435, 2011.