CS294-92: Analysis of Boolean Functions Spring 2025

Lecture 24: The Sensitivity Conjecture

Instructor: Avishay Tal Scribe: Matthew Ding

In the previous lecture, we introduced the query, or black-box model, along with various measures of complexity within this model. For example, we introduced deterministic query complexity, which is the minimum depth of any decision tree computing f. In this lecture we introduce the Sensitivity Conjecture proposed by Nisan and Szegedy in 1994, as well as the recent breakthrough by Huang in 2019 which proves the conjecture.

24.1 Certificate complexity and block sensitivity

An additional query complexity measure is non-deterministic query complexity, also known as *certificate complexity*.

Definition 24.1 (Certificate complexity)**.** *The certificate complexity of a function f on x (denoted $C_f(x)$) is the minimum number of coordinates a prover needs to reveal in x to convince a deterministic verifier of the value of $f(x)$.*

We can also give an equivalent definition through the notion of restrictions:

Definition 24.2 (Restriction)**.** *A **restriction** ρ is a partial assignment $\rho : [n] \to \{-1, *, 1\}$. A string $x \in \{-1,1\}^n$ is called consistent with ρ if for all $i \in [n]$, either $\rho_i = *$ or $\rho_i = x_i$.*

Thus the certificate complexity can also be written as

$$C_f(x) = \min_{\substack{\rho \\ x \text{ consistent with } \rho \\ f|_\rho \text{ is constant}}} |\rho^{-1}(1)| + |\rho^{-1}(-1)| \tag{24.1}$$

Recall from Lecture 4 the definition of *sensitivity*:

Definition 24.3 (Sensitivity)**.** *The sensitivity of a Boolean function $f : \{-1,1\}^n \to \{-1,1\}$ on input $x : \{-1,1\}^n$ is number of coordinates which are pivotal on x.*

$$\mathbf{Sens}_f(x) \triangleq |\{i \in [n] : f(x) \neq f(x^{\oplus i})\}| \tag{24.2}$$

A generalized notion of sensitivity, called *block sensitivity*, allows for not just single coordinates to be flipped, but sets of coordinates.

Definition 24.4 (Block sensitivity [Nis89])**.** *The block sensitivity of a Boolean function $f : \{-1,1\}^n \to \{-1,1\}$ on input $x \in \{-1,1\}^n$ (denoted $\mathbf{BlockSens}_f(x)$) is the maximum number of disjoint blocks of coordinates $B_1, \ldots, B_m \subseteq [n]$ which are pivotal on x.*

We can additionally define certificate complexity, sensitivity, and block sensitivity on the entire function f, which is the maximum value on any input x.

Definition 24.5.

$$C(f) \triangleq \max_{x \in \{-1,1\}^n} C_f(x)$$
$$\mathbf{Sens}(f) \triangleq \max_{x \in \{-1,1\}^n} \mathbf{Sens}_f(x)$$
$$\mathbf{BlockSens}(f) \triangleq \max_{x \in \{-1,1\}^n} \mathbf{BlockSens}_f(x)$$

Claim 24.6. *For all functions $f : \{-1,1\}^n \to \{-1,1\}$ and inputs $x \in \{-1,1\}^n$,*

$$\mathbf{Sens}_f(x) \leq \mathbf{BlockSens}_f(x) \leq C_f(x) \leq D(f) \tag{24.3}$$

Proof. The first and third inequality are due to definition. To prove the second inequality, we fix x, and let $B_1, \ldots, B_m$ be any disjoint set of blocks such that $f(x) \neq f(x^{\oplus B_i})$. If a certificate for function f on x does not reveal at least one coordinate in each block, a verifier cannot distinguish between $f(x)$ and $f(x^{\oplus B_i})$, which are both consistent with the certificate but have different values. Therefore the number of bits must be at least the number of blocks. □

The following lemma is given without proof:

Lemma 24.7. *For all functions $f : \{-1,1\}^n \to \{-1,1\}$,*

$$D(f) \leq C(f)^2 \tag{24.4}$$

Theorem 24.8. *For all functions $f : \{-1,1\}^n \to \{-1,1\}$,*

$$C(f) \leq \mathbf{BlockSens}(f) \cdot \mathbf{Sens}(f) \tag{24.5}$$

Proof. Let x be an input maximizing the value of $C_f(x)$. Let $m = \mathbf{BlockSens}_f(x)$ and let $B_1, \ldots, B_m$ be a set of m disjoint blocks such that $f(x) \neq f(x^{\oplus B_i})$ for all $i \in [m]$. Without loss of generality we can assume that each of these blocks is minimal, i.e., there exists no subset of any block $C_i \subseteq B_i$ such that $f(x) \neq f(x^{\oplus C_i})$ (otherwise we just replace B_i with C_i). Thus $\forall B' \subset B_i$, $f(x) = f(x^{\oplus B'})$, and $\mathbf{Sens}_f(x^{\oplus B_i}) \geq |B_i|$. Therefore we have $\mathbf{Sens}(f) \geq |B_i|$ for all $i \in [m]$.

Let ρ be the restriction which fixes $\rho(j) = x_j$ for all $j \in \bigcup_{i \in [m]} B_i$. By construction x is consistent with ρ. We show that $f|_\rho$ is constant through the following claim:

Claim 24.9. *If y is consistent with ρ, then $f(x) = f(y)$.*

Proof. Assume for contradiction $f(x) \neq f(y)$. We can define a new block $B_{m+1} = \{j \in [n] : x_j \neq y_j\}$. Since y is consistent with ρ, B_{m+1} is nonempty and disjoint from $B_1, \ldots, B_m$. If $f(x) \neq f(y)$, then $\mathbf{BlockSens}_f(x) \geq m + 1$, which is a contradiction. □

From the restriction definition of certificate complexity in Equation 24.1, we have

$$C(f) = C_f(x) \leq |\rho^{-1}(1)| + |\rho^{-1}(-1)| = \sum_{i \in [m]} B_i \leq m \cdot \mathbf{Sens}(f) = \mathbf{BlockSens}(f) \cdot \mathbf{Sens}(f) \tag{24.6}$$

□

Notation	Query complexity measure
$D(f)$	Deterministic query complexity
$R(f)$	Randomized query complexity
$Q(f)$	Quantum query complexity
$C(f)$	Certificate query complexity
$\mathbf{BlockSens}(f)$	Block sensitivity
$\deg(f)$	Degree
$\widetilde{deg}(f)$	Approximate degree

Table 24.1: List of query complexity measures [Nis89, NS94, BBC+98]. All measures are known to be related by a polynomial (specifically quartic) factor, but before [Hua19] it was unclear how sensitivity related to these measures.

24.2 The Sensitivity Conjecture

The Sensitivity Conjecture, also known as the Sensitivity vs. Block Sensitivity Conjecture, states that sensitivity and block sensitivity are related by a polynomial factor.

Conjecture 24.10 (Sensitivity Conjecture [NS94])**.** *For all Boolean functions* $f : \{-1,1\}^n \to \{-1,1\}$*,*

$$\mathbf{BlockSens}(f) \leq \mathbf{Sens}(f)^{O(1)} \tag{24.7}$$

Equivalently,

$$\deg(f) \leq \mathbf{Sens}(f)^{O(1)} \tag{24.8}$$

24.2.1 Previous progress

For upper-bounds on sensitivity, [Rub95] showed a function f such that $\mathbf{BlockSens}(f) \geq \frac{1}{2}\mathbf{Sens}(f)^2$. Additionally, it was well-known that there exists a function f such that $\deg(f) \geq \mathbf{Sens}(f)^2$, as witnessed by $f = \mathsf{OR}_{\sqrt{n}} \circ \mathsf{AND}_{\sqrt{n}}$.

For lower-bounds, a line of work [Sim83, KK04, ABG+14, APV16] showed increasingly stronger bounds in relation to block sensitivity, up to $\mathbf{BlockSens}(f) \leq 2^{\mathbf{Sens}(f)-1}(\mathbf{Sens}(f) - 1/3)$. However, the best known results before Huang were an exponential relationship between sensitivity and block sensitivity.

24.2.2 Proof of conjecture

Huang proved the Sensitivity Conjecture by showing the following theorem:

Theorem 24.11 ([Hua19])**.** *For all Boolean functions $f : \{-1,1\}^n \to \{-1,1\}$,*

$$\deg(f) \leq \mathbf{Sens}(f)^2 \tag{24.9}$$

For $x, y \in \{-1,1\}^n$, let $x \sim y$ denote x and y being adjacent vertices in the Boolean hypercube, i.e., the Hamming distance between x and y is exactly 1. Consider the following graph related to the Boolean function f:

Definition 24.12 (Sensitivity graph)**.** *The sensitivity graph of a Boolean function f is defined as the graph $G_f = (V, E)$, where $V = \{-1,1\}^n$, and $E = \{(x,y) : x \sim y, f(x) \neq f(y)\}$, i.e. the subset of sensitive edges on the Boolean hypercube.*

The sensitivity is thus given as the maximum degree in the sensitivity graph: $\mathbf{Sens}(f) \triangleq \max_{v \in V} \deg(v)$. Additionally, denote A_f as the adjacency matrix of graph G_f and $\lambda(f)$ as the maximum eigenvalue A_f.

Remark 24.13. Note that we slightly overload the notation $\deg(\cdot)$. $\deg(f)$ refers to the degree of the function f as a multilinear polynomial, while $\deg(v)$ refers the the degree of vertex v in the sensitivity graph G_f.

We can assume without loss of generality that $\deg(f) = n$. If f has degree $d < n$, we can restrict f to the d coordinates of any degree-d monomial in the Fourier representation of f. This gives a degree-d Boolean function f' on d variables whose sensitivity is at most the sensitivity of the original function. Thus proving $\deg(f') \leq \mathbf{Sens}(f')^2$ implies $\deg(f) \leq \mathbf{Sens}(f)^2$.

We prove the following lemma, which was the main contribution in the work of Huang:

Lemma 24.14 ([Hua19])**.**

$$\forall f : \deg(f) \leq \lambda(f)^2 \tag{24.10}$$

It is well-known that $\forall f : \lambda(f) \leq \mathbf{Sens}(f)$, as the maximum eigenvalue of the adjacency matrix lower bounds the maximum degree in any graph (see, for example, Theorem 5 in Chapter VIII of [Bol98]). Thus Lemma 24.14 directly implies the Sensitivity conjecture, as we have

$$\forall f : \deg(f) \leq \lambda(f)^2 \leq (\max_{v \in V} \deg(v))^2 \leq \mathbf{Sens}(f)^2 \tag{24.11}$$

For the remainder of the section, we give an overview of the proof to Lemma 24.14.

Proof Sketch. Note that any $m \times m$ real symmetric matrix has real eigenvalues $\lambda_m \leq \lambda_{m-1}, \ldots, \leq \lambda_1$. Therefore we can write $\lambda(f) = \max_{v \neq \vec{0}} \frac{\|A_f v\|_2}{\|v\|_2}$.

We prove that there exists some vector $v' \neq \vec{0}$ such that $\frac{\|A_f v\|_2}{\|v\|_2} \geq \sqrt{n}$.

Claim 24.15. *For all n, there exists an assignment of $\{-1, 1\}$ on the edges of the n-dimensional hypercube such that $B^2 = n\mathbb{I}$.*

Proof Sketch. 1. Base case: Let $B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. We can show that $B_1^2 = \mathbb{I}$.

2. Inductive step: Let $B_n = \begin{bmatrix} B_{n-1} & \mathbb{I} \\ \mathbb{I} & -B_{n-1} \end{bmatrix}$. We can show that

$$\begin{bmatrix} B_{n-1} & \mathbb{I} \\ \mathbb{I} & -B_{n-1} \end{bmatrix} \begin{bmatrix} B_{n-1} & \mathbb{I} \\ \mathbb{I} & -B_{n-1} \end{bmatrix} = \begin{bmatrix} B_{n-1}^2 + \mathbb{I} & 0 \\ 0 & B_{n-1}^2 + \mathbb{I} \end{bmatrix} = \begin{bmatrix} n\mathbb{I} & 0 \\ 0 & n\mathbb{I} \end{bmatrix} \tag{24.12}$$

□

Corollary 24.16. *B_n has 2^{n-1} eigenvalues of $\sqrt{n}$ and 2^{n-1} eigenvalues of $-\sqrt{n}$.*

Proof Sketch. Since $B_n^2 = n\mathbb{I}$, which has all eigenvalues n, B_i has eigenvalues $\pm\sqrt{n}$. Additionally since $\mathrm{Tr}(B_n) = 0$ as the diagonal of B_n is all zeroes, we must have equal number of eigenvalues $\sqrt{n}$ and $-\sqrt{n}$. □

We partition the set of strings $\{-1, 1\}^n$ into subsets $V_0 = \{x \in \{-1, 1\}^n : f(x) = \mathsf{PARITY}(x)\}$ and $V_1 = \{x \in \{-1, 1\}^n : f(x) \neq \mathsf{PARITY}(x)\}$. We can also map these strings to the set $[2^n]$ using their binary representation, which represent indices of vectors in $\mathbb{R}^{2^n}$. Thus we can also consider V_0 and V_1 as defining subspaces of $\mathbb{R}^{2^n}$ of dimension $|V_0|$ and $|V_1|$ respectively. Since we can assume $\deg(f) = n$ without loss of generality,

$$\widehat{f}([n]) = \frac{|V_0| - |V_1|}{2^n} \neq 0 \tag{24.13}$$

so $|V_0| \neq |V_1|$. Without loss of generality we can assume $|V_0| > |V_1|$, i.e. $|V_0| \geq 2^{n-1} + 1$, and the vectors supported on the indices in V_0 form a $\geq 2^{n+1} + 1$ subspace. Since B_n has 2^{n-1} eigenvalues of $\sqrt{n}$, the eigenspace of eigenvalue $\sqrt{n}$ has dimension 2^{n-1}. Therefore the intersection of V_0 subspace and the $\sqrt{n}$ eigenspace has dimension ≥ 1, and there exists a $\sqrt{n}$ eigenvector in $\mathbb{R}^{2^n}$ only supported on the indices in V_0. Call this vector v, and define $v' \in \mathbb{R}^{2^n}$ such that $v'_x = |v_x|$. Since v is an eigenvector, $v' \neq \vec{0}$.

Claim 24.17. *For all indices $x \in [2^n]$, $(A_f v')_x \geq \sqrt{n} \cdot v'_x$*

Proof Sketch. For all $x \in V_1$, since v' has no support on the indices in V_1, $(A_f v')_x = \sqrt{n} \cdot v'_x = 0$.

For all $x \in V_0$,

$$\sqrt{n} \cdot v'_x \triangleq \sqrt{n} \cdot |v_x| = |(B_n v)_x| = \left| \sum_{y \sim x} B_{x,y} v_y \right| \tag{24.14}$$

Additionally,

$$(A_f v')_x = \sum_{\substack{y \sim x \\ f(x) \neq f(y)}} v'_y = \sum_{\substack{y \sim x \\ y \in V_0}} v'_y = \sum_{y \sim x} v'_y \triangleq \sum_{y \sim x} |v_y| \tag{24.15}$$

By the triangle inequality,

$$\left|\sum_{y\sim x} B_{x,y} v_y\right| \leq \sum_{y\sim x} |v_y| \tag{24.16}$$

proving the claim. □

Claim 24.17 implies that $\lambda(f) \geq \frac{\|A_f v'\|_2}{\|v'\|_2} \geq \sqrt{n} \geq \sqrt{\deg(f)}$, completing the proof of Theorem 24.11. □

24.3 Current status and open problems

We summarize the relationship between the query complexity measures in Table 24.1, ignoring constant factors.

Currently, it is known that for all total functions f,

$$\left.\begin{matrix} Q(f) \leq R(f) \\ \mathbf{BlockSens}(f) \leq C(f) \end{matrix}\right\} \leq D(f) \leq \deg(f)^3 \leq \lambda(f)^6 \leq \mathbf{Sens}(f)^6 \tag{24.17}$$

The exact relation between deterministic and quantum query complexity is known up to log factors. There exists a function f such that $D(f) \leq Q(f)^4$ [ABDK+20], and a function f such that $D(f) \geq \widetilde{O}(Q(f)^4)$ [ABB+15].

The exact relation between randomized query complexity and quantum query complexity remains an open question. On one side, it was shown that there exist functions f such that $R(f) \geq Q(f)^3$ [BS20, SSW23]. On the other side, $R(f) \leq Q(f)^4$ is only known due to the deterministic query case [ABDK+20]. In that work they additionally conjecture the following two relations:

Conjecture 24.18 ([ABDK+20])**.** *There exist functions $f : \{-1,1\}^n \to \{-1,1\}$ such that*

$$R(f) \leq Q(f)^3 \tag{24.18}$$

$$D(f) \leq \mathbf{BlockSens}(f)^2 \tag{24.19}$$

References

[ABB+15] Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. Separations in Query Complexity Based on Pointer Functions, 2015.

[ABDK+20] Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. Degree vs. Approximate Degree and Quantum Implications of Huang's Sensitivity Theorem, 2020.

[ABG+14] Andris Ambainis, Mohammad Bavarian, Yihan Gao, Jieming Mao, Xiaoming Sun, and Song Zuo. Tighter Relations Between Sensitivity and Other Complexity Measures, 2014.

[APV16] Andris Ambainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs. Sensitivity versus certificate complexity of boolean functions. In *International Computer Science Symposium in Russia*, pages 16–28. Springer, 2016.

[BBC+98] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum Lower Bounds by Polynomials, 1998.

[Bol98] Béla Bollobás. *Modern Graph Theory*, volume 184. Springer Science & Business Media, 1998.

[BS20] Nikhil Bansal and Makrand Sinha. k-forrelation optimally separates quantum and classical query complexity, 2020.

[Hua19] Hao Huang. Induced subgraphs of hypercubes and a proof of the Sensitivity Conjecture, 2019.

[KK04] Claire Kenyon and Samuel Kutin. Sensitivity, block sensitivity, and ℓ-block sensitivity of Boolean functions. *Information and Computation*, 189(1):43–53, 2004.

[Nis89] 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. Association for Computing Machinery.

[NS94] Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational complexity*, 4:301–313, 1994.

[Rub95] David Rubinstein. Sensitivity vs. block sensitivity of Boolean functions. *Combinatorica*, 15(2):297–299, 1995.

[Sim83] Hans-Ulrich Simon. A tight Ω (loglog n)-bound on the time for parallel Ram's to compute nondegenerated boolean functions. In *International Conference on Fundamentals of Computation Theory*, pages 439–444. Springer, 1983.

[SSW23] Alexander A. Sherstov, Andrey A. Storozhenko, and Pei Wu. An optimal separation of randomized and quantum query complexity, 2023.