Degree vs. Approximate Degree and Quantum Implications of Huang's Sensitivity Theorem

Scott Aaronson
University of Texas at Austin

Shalev Ben-David
University of Waterloo

Robin Kothari
Microsoft Quantum

Shravas Rao
Northwestern University

Avishay Tal
University of California at Berkeley

Abstract

Based on the recent breakthrough of Huang (2019), we show that for any total Boolean function f,

1. $\mathsf{deg}(f) = O(\widetilde{\mathsf{deg}}(f)^2)$: The degree of f is at most quadratic in the approximate degree of f. This is optimal as witnessed by the OR function.
2. $\mathsf{D}(f) = O(\mathsf{Q}(f)^4)$: The deterministic query complexity of f is at most quartic in the quantum query complexity of f. This matches the known separation (up to log factors) due to Ambainis, Balodis, Belovs, Lee, Santha, and Smotrovs (2017).

We apply these results to resolve the quantum analogue of the Aanderaa–Karp–Rosenberg conjecture. We show that if f is a nontrivial monotone graph property of an n-vertex graph specified by its adjacency matrix, then $\mathsf{Q}(f) = \Omega(n)$, which is also optimal. We also show that the approximate degree of any read-once formula on n variables is $\Theta(\sqrt{n})$.

Last year, Huang resolved a major open problem in the analysis of Boolean functions called the *sensitivity conjecture* [Hua19], which was open for nearly 30 years [NS94]. Surprisingly, Huang's elegant proof takes less than 2 pages—truly a "proof from the book." Specifically, Huang showed that for any total Boolean function, which is a function $f : \{0,1\}^n \to \{0,1\}$, we have

$$\mathsf{deg}(f) \leq \mathsf{s}(f)^2, \tag{1}$$

where $\mathsf{deg}(f)$ is the real degree of f[1] and $\mathsf{s}(f)$ is the (maximum) sensitivity of f.[2]

In this paper, we describe some implications of Huang's resolution of the sensitivity conjecture to polynomial-based complexity measures of Boolean functions and quantum query complexity. Our first observation is that Huang actually proves a stronger claim than Eq. (1), in which $\mathsf{s}(f)$ can be replaced by $\lambda(f)$, a spectral relaxation of sensitivity.

Theorem 1. *For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$, we have $\mathsf{deg}(f) \leq \lambda(f)^2$.*

In short, while $s(f)$ can be viewed as the maximum number of 1s in any row or column of a certain Boolean matrix, $\lambda(f)$ is the largest eigenvalue of that matrix, which could potentially

[1] The real degree of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is the minimum degree of a real polynomial p over variables $x_1, \ldots, x_n$ such that for all $x \in \{0,1\}^n$, $p(x) = f(x)$.

[2] The sensitivity of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is defined as $\mathsf{s}(f) = \max_{x\in\{0,1\}^n} |\{i : f(x \oplus e_i) \neq f(x)\}|$, where e_i is the n-bit string with the ith bit set to 1 and all other bits set to 0.

be smaller. This observation has several implications because, as we show, $\lambda(f)$ lower bounds many other complexity measures. One of the messages of this work is that $\lambda(f)$ is an interesting complexity measure and can be used to establish relationships between other complexity measures.

We use this observation to prove two main results: Our first result is an optimal relationship between deterministic and quantum query complexity for total functions, and our second result is an optimal relationship between degree and approximate degree for total functions. We then apply the first result to prove the quantum analogue of the Aanderaa–Karp–Rosenberg conjecture and apply the second result to show that the approximate degree of any read-once formula is $\Theta(\sqrt{n})$.

Deterministic vs. quantum query complexity. We know from the seminal results of Nisan [Nis91], Nisan and Szegedy [NS94], and Beals et al. [BBC+01] that for any total Boolean function f, the deterministic query complexity, $\mathsf{D}(f)$, and quantum query complexity, $\mathsf{Q}(f)$, satisfy[3]

$$\mathsf{D}(f) = O(\mathsf{Q}(f)^6). \tag{2}$$

Grover's algorithm [Gro96] shows that for the OR function, a quadratic separation between $\mathsf{D}(f)$ and $\mathsf{Q}(f)$ is possible. This was the best known quantum speedup for total functions until Ambainis et al. [ABB+17] constructed a total function f with

$$\mathsf{D}(f) = \widetilde{\Omega}(\mathsf{Q}(f)^4). \tag{3}$$

We show that the quartic separation (up to log factors) in Eq. (3) is actually the best possible.

Theorem 2. *For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$, we have $\mathsf{D}(f) = O(\mathsf{Q}(f)^4)$.*

We deduce Theorem 2 as a corollary of a new tight relationship between $\mathsf{deg}(f)$ and $\mathsf{Q}(f)$:

Theorem 3. *For all Boolean functions $f : \{0,1\}^n \to \{0,1\}$, we have $\mathsf{deg}(f) = O(\mathsf{Q}(f)^2)$.*

Observe that Theorem 3 is tight for the OR function on n variables, whose degree is n and whose quantum query complexity is $\Theta(\sqrt{n})$ [Gro96, BBBV97]. Prior to this work, the best relation between $\mathsf{deg}(f)$ and $\mathsf{Q}(f)$ was a sixth power relation, $\mathsf{deg}(f) = O(\mathsf{Q}(f)^6)$, which follows from Eq. (2).

Our proof of Theorem 3 relies on the restatement of Huang's result (Theorem 1), showing that $\mathsf{deg}(f) \leq \lambda(f)^2$. We then show that the measure $\lambda(f)$ lower bounds the spectral adversary method in quantum query complexity [BSS03], which is equivalent to the original quantum adversary method of Ambainis [Amb02], which lower bounds $\mathsf{Q}(f)$.

We now show how Theorem 2 straightforwardly follows from Theorem 3 using two previously known connections between complexity measures of Boolean functions.

Proof of Theorem 2 assuming Theorem 3. Midrijanis [Mid04] showed that for all total functions f,

$$\mathsf{D}(f) \leq \mathsf{bs}(f)\,\mathsf{deg}(f), \tag{4}$$

where $\mathsf{bs}(f)$ is the block sensitivity of f.

Theorem 3 shows that $\mathsf{deg}(f) = O(\mathsf{Q}(f)^2)$. Combining the relationship between block sensitivity and approximate degree from [NS94] with the results of [BBC+01], we get that $\mathsf{bs}(f) = O(\mathsf{Q}(f)^2)$. (This can also be proved directly using the lower bound method in [BBBV97].)

Combining these three inequalities yields $\mathsf{D}(f) = O(\mathsf{Q}(f)^4)$ for all total Boolean functions f. ■

[3] This means that for total functions, quantum query algorithms can only outperform classical query algorithms by a polynomial factor. On the other hand, for partial functions, which are defined on a subset of $\{0,1\}^n$, exponential and even larger speedups are possible.

Degree vs. approximate degree. We also know from the works of Nisan and Szegedy [NS94] and Beals et al. [BBC⁺01], that for any total Boolean function f,

$$\mathsf{deg}(f) = O(\widetilde{\mathsf{deg}}(f)^6), \tag{5}$$

where $\widetilde{\mathsf{deg}}(f)$ is the approximate degree of f, the minimum degree of a real polynomial p that for all $x \in \{0,1\}^n$, satisfies $|p(x) - f(x)| \leq 1/3$. We show that this relationship can be also significantly improved.

Theorem 4. *For all Boolean functions* $f : \{0,1\}^n \to \{0,1\}$, *we have* $\mathsf{deg}(f) = O(\widetilde{\mathsf{deg}}(f)^2)$.

This relationship is optimal since it is saturated by the OR function on n bits that has degree n and approximate degree $\Theta(\sqrt{n})$ [NS94].

Theorem 4 follows by combining $\mathsf{deg}(f) \leq \lambda(f)^2$ (Theorem 1) with $\lambda(f) = O(\widetilde{\mathsf{deg}}(f))$. This is the most technically challenging part of this submission, and we provide two proofs of this claim. The first proof is arguably simpler, but it is not self contained and uses Sherstov's composition theorem for approximate degree [She13b], and has a large constant hidden in the big Oh. The second proof does not rely on this result and achieves the optimal constant inside the big Oh.

Observe that because approximate degree lower bounds quantum query complexity, Theorem 4 also implies Theorem 3 (and hence Theorem 2). Although Theorem 3 is a consequence of this, our proof of Theorem 3 is much simpler and additionally proves that $\lambda(f)$ lower bounds the original adversary method [Amb02], which is not implied by the proof of Theorem 4.

Applications. We use Theorem 3 to prove the quantum analogue of the famous *Aanderaa–Karp–Rosenberg conjecture*. Briefly, this conjecture is about the minimum possible query complexity of a nontrivial monotone graph property, for graphs specified by their adjacency matrices.

There are variants of the conjecture for different models of computation. For example, the randomized variant of the Aanderaa–Karp–Rosenberg conjecture, attributed to Karp [SW86, Conjecture 1.2] and Yao [Yao77, Remark (2)], states that for all nontrivial monotone graph properties f, we have $\mathsf{R}(f) = \Omega(n^2)$. Following a long line of work, the current best lower bound is $\mathsf{R}(f) = \Omega(n^{4/3}\log^{1/3} n)$ due to Chakrabarti and Khot [CK01].

The quantum version of the conjecture was raised by Buhrman, Cleve, de Wolf, and Zalka [BCdWZ99], who observed that the best we could hope for is $\mathsf{Q}(f) = \Omega(n)$, because the nontrivial monotone graph property "contains at least one edge" can be decided with $O(n)$ queries using Grover's algorithm. Buhrman et al. [BCdWZ99] also showed that all nontrivial monotone graph properties satisfy $\mathsf{Q}(f) = \Omega(\sqrt{n})$. The current best bound is $\mathsf{Q}(f) = \Omega(n^{2/3}\log^{1/6} n)$, which is credited to Yao in [MSS07]. We resolve this conjecture by showing an optimal $\Omega(n)$ lower bound.

Theorem 5. *Let* $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ *be a nontrivial monotone graph property. Then* $\mathsf{Q}(f) = \Omega(n)$.

Theorem 5 follows by combining Theorem 3 with a known quadratic lower bound on the degree of monotone graph properties.

We then use Theorem 4 to completely characterize the approximate degree of any read-once formula. It is known that the quantum query complexity of any read-once formula on n variables is $\Theta(\sqrt{n})$ [BS04, Rei11]. It has long been conjectured that the approximate degree of any read-once formula is also $\Theta(\sqrt{n})$. It has taken much effort to establish this even for special cases. For example, the conjecture was proved for the simple depth-two read-once formula AND $\circ$ OR in 2013 [BT13, She13a]. This result was later extended to all constant-depth balanced read-once formulas [BT15] and then to constant-depth unbalanced read-once formulas [BBGK18]. We resolve this question for all read-once formulas.

Theorem 6. *For any read-once formula* $f : \{0,1\}^n \to \{0,1\}$, *we have* $\widetilde{\mathsf{deg}}(f) = \Theta(\sqrt{n})$.

References

[ABB+17] Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. Separations in query complexity based on pointer functions. *Journal of the ACM*, 64(5):1–24, September 2017. doi:10.1145/3106234. [p. 2]

[Amb02] Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, jun 2002. doi:10.1006/jcss.2002.1826. [pp. 2, 3]

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, October 1997. doi:10.1137/S0097539796300933. [p. 2]

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. doi:10.1145/502090.502097. [pp. 2, 3]

[BBGK18] Shalev Ben-David, Adam Bouland, Ankit Garg, and Robin Kothari. Classical lower bounds from quantum upper bounds. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 339–349, 2018. doi:10.1109/FOCS.2018.00040. [p. 3]

[BCdWZ99] Harry Buhrman, Richard Cleve, Ronald de Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. In *40th Annual Symposium on Foundations of Computer Science*, pages 358–368, 1999. doi:10.1109/SFFCS.1999.814607. [p. 3]

[BS04] Howard Barnum and Michael Saks. A lower bound on the quantum query complexity of read-once functions. *Journal of Computer and System Sciences*, 69(2):244 – 258, 2004. doi:10.1016/j.jcss.2004.02.002. [p. 3]

[BSS03] Howard Barnum, Michael E. Saks, and Mario Szegedy. Quantum query complexity and semi-definite programming. In *18th Annual IEEE Conference on Computational Complexity (Complexity 2003)*, pages 179–193, 2003. doi:10.1109/CCC.2003.1214419. [p. 2]

[BT13] Mark Bun and Justin Thaler. Dual lower bounds for approximate degree and Markov-Bernstein inequalities. In *Automata, Languages, and Programming: 40th International Colloquium, ICALP 2013*, pages 303–314, 2013. doi:10.1007/978-3-642-39206-1_26. [p. 3]

[BT15] Mark Bun and Justin Thaler. Hardness amplification and the approximate degree of constant-depth circuits. In *Automata, Languages, and Programming: 42nd International Colloquium, ICALP 2015*, pages 268–280, 2015. doi:10.1007/978-3-662-47672-7_22. [p. 3]

[CK01] Amit Chakrabarti and Subhash Khot. Improved lower bounds on the randomized complexity of graph properties. In *Automata, Languages and Programming*, pages 285–296, 2001. doi:10.1007/3-540-48224-5_24. [p. 3]

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, STOC 1996*, pages 212–219, 1996. doi:10.1145/237814.237866. [p. 2]

[Hua19] Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019. doi:10.4007/annals.2019.190.3.6. [p. 1]

[Mid04] Gatis Midrijanis. Exact quantum query complexity for total Boolean functions. *arXiv preprint quant-ph/0403168*, 2004. arXiv:quant-ph/0403168. [p. 2]

[MSS07] Frédéric Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):413–424, 2007. doi:10.1137/050643684. [p. 3]

[Nis91] Noam Nisan. CREW PRAMs and decision trees. *SIAM Journal on Computing*, 20(6):999–1007, 1991. doi:10.1137/0220062. [p. 2]

[NS94] Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, 1994. doi:10.1007/BF01263419. [pp. 1, 2, 3]

[Rei11] Ben W. Reichardt. Reflections for quantum query algorithms. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '11, page 560–569, 2011. doi:10.1137/1.9781611973082.44. [p. 3]

[She13a] Alexander A. Sherstov. Approximating the AND-OR tree. *Theory of Computing*, 9(20):653–663, 2013. doi:10.4086/toc.2013.v009a020. [p. 3]

[She13b] Alexander A. Sherstov. Making polynomials robust to noise. *Theory of Computing*, 9(18):593–615, 2013. doi:10.4086/toc.2013.v009a018. [p. 3]

[SW86] Michael Saks and Avi Wigderson. Probabilistic Boolean decision trees and the complexity of evaluating game trees. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, SFCS '86, page 29–38, 1986. doi:10.1109/SFCS.1986.44. [p. 3]

[Yao77] Andrew Chi-Chih Yao. Probabilistic computations: Toward a unified measure of complexity. In *18th Annual Symposium on Foundations of Computer Science (SFCS 1977)*, pages 222–227, 1977. doi:10.1109/SFCS.1977.24. [p. 3]