

Fine-Grained Complexity via Quantum Natural Proofs

Yanlin Chen ✉

University of Maryland (QuICS), College Park, MD, USA

Yilei Chen ✉

Shanghai Qi Zhi Institute, Tsinghua University, Beijing, China

Rajendra Kumar ✉

Indian Institute of Technology Delhi, New Delhi, India

Subhasree Patro ✉

Eindhoven University of Technology, The Netherlands

Florian Speelman ✉

University of Amsterdam and QuSoft, The Netherlands

Abstract

Buhrman, Patro, and Speelman [11] presented a framework of conjectures that together form a quantum analogue of the strong exponential-time hypothesis and its variants. They called it the QSETH framework. In this paper, using a notion of quantum natural proofs (built from natural proofs introduced by Razborov and Rudich), we show how part of the QSETH conjecture that requires properties to be “compression oblivious” can in many cases be replaced by assuming the existence of quantum-secure pseudorandom functions, a standard hardness assumption. Combined with techniques from Fourier analysis of Boolean functions, we show that properties such as PARITY and MAJORITY are compression oblivious for certain circuit class Λ if subexponentially secure quantum pseudorandom functions exist in Λ , answering an open question in [11].

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases Fine-grained complexity, Quantum natural proofs, QSETH, Pseudorandom functions

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2026.60

Category RANDOM

Related Version *Full Version:* <https://arxiv.org/pdf/2504.10363> [13]

Funding *Yanlin Chen:* Acknowledges the support from a QuICS Hartree Postdoctoral Fellowship. *Yilei Chen:* Supported by Tsinghua University startup funding, and Shanghai Qi Zhi Institute Innovation Program SQZ202405.

Rajendra Kumar: Supported by the Chandrukha New Faculty Fellowship from IIT Delhi and the Prime Minister Early Career Research Grant from the Anusandhan National Research Foundation (ANRF).

Subhasree Patro: Acknowledges the support from the Dutch Ministry of Education, Culture, and Science through Gravitation project “Challenges in Cyber Security - 024.006.037” for this work.

Florian Speelman: Supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL program, and the project Divide and Quantum “D&Q” NWA.1389.20.241 of the program “NWA-ORC”, which is partly funded by the Dutch Research Council (NWO).



© Yanlin Chen, Yilei Chen, Rajendra Kumar, Subhasree Patro, and Florian Speelman;
licensed under Creative Commons License CC-BY 4.0
Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques
(APPROX/RANDOM 2026).

Editors: Mohit Singh and Tom Gur; Article No. 60; pp. 60:1–60:23



Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

A well-studied problem in complexity theory is CNFSAT, the problem of whether a formula, input in conjunctive normal form, has a satisfying assignment. Not only is there no polynomial time known for CNFSAT, there is also no known algorithm that significantly improves over the brute-force method of checking all 2^n assignments. Impagliazzo, Paturi and Zane in [23, 24] conjectured that determining whether an input CNF formula is satisfiable or not cannot be done in time $O(2^{n(1-\varepsilon)})$ for any constant $\varepsilon > 0$. They called it *Strong Exponential-Time Hypothesis* (SETH). As a consequence, SETH-based lower bounds were shown for many computational problems; for example, see [31, 8, 21].

Variants of classical SETH

Subsequent works also explored alternate directions in which the strong exponential-time hypothesis can be weakened and thereby made more plausible. For, e.g.,

1. The *satisfiability* problem is studied for other (more general) succinct representations of Boolean functions such as BPSAT or **CircuitSAT** - the problem of whether a polynomial-size branching program or a polynomial-size circuit has a satisfying assignment. Furthermore, respective hardness conjectures for these satisfiability problems, namely NCSETH and **CircuitSETH** (under the name “**CircuitSAT** form of SETH”) have also been discussed together with their implications [2, 30].
2. Another direction of study that has made SETH more plausible is by computing more complicated properties of the formula. For example, counting the number of satisfying assignments and computing whether the number of satisfying assignments is even or odd is captured by $\#$ SETH and $\oplus$ SETH, respectively; see [17] for example.

Unfortunately, neither SETH nor NCSETH or **CircuitSETH**, hold relative to *quantum* computation, as using Grover’s algorithm for unstructured search [19] it is possible to solve the respective satisfiability problems in $O(2^{n/2})$ time - leading to conjectured lower bounds of complexity $\Omega(2^{n/2})$. While these lower bounds have interesting consequences (as shown by [1, 11]), in the quantum case, generalizing the properties to be computed (as suggested in Item 2) is a way to come up with variants of the hypothesis that enable stronger bounds: for many of such tasks it is likely that the quadratic quantum speedup, as given by Grover’s algorithm, no longer exists. In fact, motivated by this exact observation, Buhrman, Patro, and Speelman [11] introduced a framework of Quantum Strong Exponential-Time Hypotheses (QSETH) as quantum analogues to SETH, with a striking feature that allows one to technically unify quantum analogues of SETH, $\oplus$ SETH, $\#$ SETH, NCSETH, $\oplus$ NCSETH, etc., all under one umbrella conjecture.

The QSETH framework

Buhrman *et al.* consider the problem in which one is given a formula or a circuit representation of a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and is asked whether a property $P : \{0, 1\}^{2^n} \rightarrow \{0, 1\}$ on its truth table¹ evaluates to 1. They conjectured that when the circuit representation is *obfuscated* enough (that is, the description of the circuit provides no advantages over treating the circuit as a black-box with query access to its truth table), then for *most*

¹ Truth table of a formula/circuit ϕ on n variables, denoted by $\text{tt}(\phi)$, is a 2^n bit string derived in the following way $\text{tt}(\phi) = \bigcirc_{a \in \{0, 1\}^n} \phi(a)$; the symbol $\circ$ denotes concatenation.

properties P (that are “compression oblivious” with respect to the representation), the time taken to compute P on the truth table of $\text{poly}(n)$ -sized circuits is lower bounded by $Q(P)$, i.e., the $1/3$ -bounded error quantum query complexity of P , on all bit strings of length 2^n .

Note that there are two requirements to using the QSETH framework. Firstly, the input formula or circuit must be “obfuscated enough” - as we already saw this translates to saying that knowing the description of the input must not help towards computing P any more than just having query access to the truth table of the input. The second requirement (which is the main topic of discussion of this paper) is that the property P itself must be “compression oblivious” - a notion introduced in [11] that we discuss next.

Compression-oblivious properties

Buhrman *et al.* defined this notion to capture properties whose *query complexity* on all strings is a lower bound for the *time complexity* to compute the property even for inputs that are “compressible” as a truth table of small formulas (or circuits). This notion is useful (to their framework) because if the formula (or circuit) is obfuscated enough then one can use the quantum query lower bound of such a property to conjecture a time lower bound of computing that property on a small formula (or circuit).² Therefore, before using their framework, one has to be convinced that the property is indeed compression-oblivious with respect to the circuit representation considered. They give various results to initiate the study of the set of compression-oblivious languages; see Section 2.3 in [11]. For example, they show the following.

- For simple properties, such as OR, AND, they were able to prove that these are compression-oblivious for polynomial-size AC_2^0 circuits.
- They gave an example of a property that is *not* compression oblivious for polynomial-sized circuits (or any smaller class of representations).³
- For more complicated properties, such as PARITY or MAJORITY, they show that proving compression-obliviousness would separate P from $PSPACE$; see Theorem 9 in [11]. Their result indicates that *unconditionally* proving compression-obliviousness for a complicated property is hard. One way around this would be to directly *conjecture* the compression-obliviousness of such properties, which was the choice of [11]. However, it would be desirable to put this on more solid ground.

² Here is an example to illustrate why obfuscation is important. Consider the OR property. The quantum query complexity of OR when restricted to truth tables of small CNF or DNF formulas defined on n input variables is $\Omega(\sqrt{N})$ where $N = 2^n$ - let us denote this statement by $(\star)$. Furthermore, the structure of CNF formulas are not known to help in computing OR more efficiently than $O(\sqrt{N})$. Therefore, we can use the same lower bound from $(\star)$ to conjecture the lower bound of $\Omega(\sqrt{N})$ for CNFSAT in the quantum setting. However, DNF formulas are not obfuscated enough for OR as we can compute OR in $\text{poly}(n)$ time when input formulas are DNFs. This means we cannot use the query lower bound of $\sqrt{N}$ from $(\star)$ for the DNFs as we do in the case of CNF formulas.

³ Consider the following property (Example 7 in [11]), defined on some string $z \in \{0, 1\}^{2^n}$, which we view as the truth table of a formula or circuit:

$$P_{\text{large-c}}(z) = \text{PARITY}(z) \wedge [\text{there exists no circuit } C \text{ of size less than } 2^{n/100} \text{ s.t. } z = \text{tt}(C)].$$

We use $\text{tt}(C)$ to denote the truth table of C . Because most strings are not a truth table of a small circuit, the query complexity of this property is close to the query complexity of PARITY, i.e., $Q(P_{\text{large-c}}) = \Omega(2^n)$. Nevertheless, the property is always 0 when restricted to truth tables of small circuits, and therefore trivial to compute. Therefore, $P_{\text{large-c}}$ is not compression oblivious for polynomial-sized circuits (or any smaller class of representations).

One might ask – *why is the notion of compression-oblivious properties useful for the QSETH framework when it is hard to prove results about this notion for many properties?*

Towards answering this question, consider the $\oplus$ QSETH hypothesis - implicitly stated and discussed in [11] and explicitly stated in [14, 12]. It says,

► **Conjecture 1** (Conjecture 8.9 in [12]). *For each constant $\delta > 0$, there exists $c > 0$ such that there is no bounded-error quantum algorithm that solves $\oplus$ CNFSAT (even restricted to formulas with at most $c \cdot n^2$ clauses) in $O(2^{n(1-\delta)})$ time.*

One can go about refuting this conjecture in two (immediate) ways.

1. Either one could use the description of the input formulas to help deduce PARITY of the truth table corresponding to this formula (which would mean that the CNF formula is not obfuscated enough and one could use the structure of the formula towards computing PARITY more efficiently), or
2. One could use the fact that the set of truth tables on which PARITY is to be computed is “not too big” (as the number of polynomial length formulas are not too many) and potentially use this information to speed up the computation quantumly.

While both approaches seem like good starting points, the likelihood of Item 1 not working out is probably for the same reason why $\oplus$ SETH is not refuted yet. Which brings us to Item 2. There is a stark contrast between the possible speedups that quantum can offer over classical computation. For example, there exists a quantum *query* algorithm that can compute *any* property in $\tilde{O}(\sqrt{N})$ many queries, when the input is promised to be the N -length truth table of a small formula [4, 5, 25]; such an algorithm is impossible in the classical setting. Although efficient in the number of queries, the algorithm itself is not *time* efficient. But the existence of this algorithm (in contrast to the lack of one in the classical setting) does alert us that query complexity cannot naively be used to lower bound time complexity in our setting, without taking care. (The results of the current work will indicate that such a fast algorithm is unlikely to refute $\oplus$ QSETH via Item 2.)

As pointed out by Buhrman *et al.* [11], the proof barrier does not allow one to (easily) prove compression-obliviousness of properties such as PARITY or MAJORITY. It is therefore natural to ask if there are other reasons why certain properties, say PARITY for example, should be compression oblivious. The authors leave the following open question:

“What complexity-theoretic assumptions are needed to show that, e.g., the PARITY property, is compression oblivious?”

It is precisely this question we answer in this paper. While our answer doesn’t give us a way around *conjecturing* the compression obliviousness of these properties, it gives strong evidence supporting the conjecture and the use of the QSETH framework.

1.1 Main idea: arguing compression obliviousness via quantum natural proofs

Following is the answer to the question asked earlier.

► **Theorem 2** (Informal restatement of Theorem 34). *The properties PARITY and MAJORITY are compression oblivious for a circuit class $\mathcal{M}$ unless there are no quantum-secure $\mathcal{M}$ -constructible PRFs (of a particular type).⁴*

In fact, we conclude the same for a larger class of properties (which includes PARITY and MAJORITY). The details are mentioned in the statement of Theorem 34.

⁴ For us, the logical statements “ A implies B ”, “if A then B ” and “ $\neg A$ unless B ” are all equivalent.

1.1.1 Natural proofs by Razborov and Rudich

To prove our results, we use the notion of *natural proofs* introduced by Razborov and Rudich [28]. Consider a Boolean function defined on other Boolean functions, or equivalently defined on their truth tables. Razborov and Rudich called a property (of Boolean functions) *natural* if it satisfies certain “constructivity” and “largeness” conditions. Roughly speaking, for their proof, the constructivity condition requires that the property is decidable in $\text{poly}(n)$ time when the 2^n -sized truth table of an n -input Boolean function is given as input. The largeness condition requires that the property holds for a sufficiently large fraction of the set of all Boolean functions. Moreover, they say a property is useful against a complexity class Λ if every sequence of Boolean functions having the property (infinitely often) defines a language outside of Λ . A *natural proof* is a proof that establishes that a certain language lies outside of Λ . This can be formally defined as (following the notation of Chow [16]),

► **Definition 3** (Υ -natural property with density δ , Definition 3 in [16]). *Let Υ be a complexity class and let $\delta := (\delta_n)_{n \in \mathbb{N}}$ denote a sequence of positive real numbers. A property $D := (D_n)_{n \in \mathbb{N}}$ is Υ -natural with density $\delta := (\delta_n)_{n \in \mathbb{N}}$ if the following statements hold:*

1. *largeness: $\exists n', \forall n > n', |D_n| \geq 2^{2^n} \cdot \delta_n$, and*
2. *constructivity: the problem of determining whether a Boolean function $f_n \in D_n$, when given as input the truth table of f_n on n variables, is decidable in Υ .*

Note that the largeness is captured by the density function $(\delta_n)_{n \in \mathbb{N}}$ and constructivity is captured by the complexity class Υ . Additionally, this Υ -natural property is useful against a complexity class Λ if the following statement is satisfied.

► **Definition 4** (Useful property, Definition 4 in [16]). *Let Λ denote a complexity class. A property $D := (D_n)$ is useful against complexity class Λ if $\forall (f_n)$, we have $(f_n) \notin \Lambda$ whenever (f_n) is a sequence of Boolean functions satisfying $f_n \in D_n$ for infinitely many n .*

Using these definitions, Razborov and Rudich prove the following.

► **Theorem 5** (Main theorem of Razborov and Rudich as stated in [16]). *If there exists a 2^{k^ε} -hard pseudorandom generator in $\text{SIZE}(k^c)$, then there is no P/poly-constructible natural property with density $1/2^{n^d}$ that is useful against the complexity class $\text{SIZE}(n^e)$ whenever $e > 1 + cd/\varepsilon$.*

Broadly speaking, their proof idea is to use the *algorithm* that computes the P/poly-natural property of density $(\delta_n = \frac{1}{2^{n^d}})$ that is useful against $\text{SIZE}(n^e)$ (if such a property exists) as a *distinguisher* to distinguish truth tables of functions with $\text{poly}(n)$ -size circuits from truth tables of truly random functions. As this algorithm computes a natural property of density (δ_n) , this means the distinguisher (which is the algorithm itself) can now distinguish a δ_n fraction of truly random functions. As δ_n here is quite large (for all n), this translates to a statistical test with a significant advantage to distinguish pseudorandom functions from truly random (n -input) functions. This in turn breaks the assumption about the existence of pseudorandom generators.

1.1.2 Technical overview

We use techniques similar to those of Razborov and Rudich to relate compression obliviousness of PARITY (and MAJORITY) with the existence of quantum-secure pseudorandom functions. We divide our contributions into two broad categories: a part that uses natural proofs, and a part that uses techniques from Fourier analysis of Boolean functions.

Part 1: quantum natural proofs

We use the term *quantum natural proofs* to mean that the proof relies on natural properties computable within a complexity class that captures quantum computation; equivalently, Υ in Definition 3 is a quantum complexity class. In our case, it is sufficient to consider Υ to be $\text{BQTIME}(\text{linear})$. Let $P = (P_n)_{n \in \mathbb{N}}$ be the property whose compression obliviousness, with respect to M , we want to study. Additionally, suppose that P satisfies the following two conditions.

- The property P is computable in $\text{DTIME}(N)$; where N is the length of the input.
- For all $S \subseteq \{0, 1\}^N$ of size $|S| \geq 2^N (1 - \frac{1}{N^2})$, the $Q(P_n|_S)$, i.e., the quantum query complexity to compute P on strings in set S , is $\Omega(N)$.

We can show that P has to be compression oblivious with respect to M unless a type of quantum secure pseudorandom functions doesn't exist.

Towards contradiction, let us assume that P is *not* compression oblivious for M . This means there exists a quantum algorithm that computes P on truth tables of functions corresponding to M in $N^{1-\alpha}$ time for some constant $\alpha > 0$. Let $\mathcal{A}$ denote this algorithm. Without loss of generality, let us assume $\mathcal{A}$ is a $1/10$ -bounded-error quantum algorithm. Let $\mathcal{B}$ denote the algorithm that computes P in $\text{DTIME}(N)$ as promised earlier. Using $\mathcal{A}$ and $\mathcal{B}$, we now construct an algorithm $\mathcal{D}$ that, on all inputs z , does the following:

1. Run $\mathcal{A}$ on z for $M = O(1)$ many times and note the outputs.
2. Run $\mathcal{B}$ on z once.
3. ACCEPT if over M runs of $\mathcal{A}$ on input z the number of times $\mathcal{A}(z) = \mathcal{B}(z)$ is *at most* $\frac{8}{10} \cdot M$, otherwise REJECT. (We need the success probability of $\mathcal{D}$ to be at least $2/3$ therefore choosing $M = O(1)$ suffices.)

Let z be a Boolean string of length $N = 2^n$. Let D_n denote the set of N -bit strings that $\mathcal{D}$ accepts with at least $2/3$ success probability. It is easy to see that $\mathcal{D}$ rejects strings for which $\mathcal{A}$ correctly computes P (i.e., with success probability $9/10$). Recall that, correctness of $\mathcal{A}$ is only promised for strings that are truth tables of functions having $\text{poly}(n)$ -size circuits. There is no guarantee on how $\mathcal{A}$ behaves outside of this promise. But, we do know that P has a quantum query complexity of $\Omega(N)$ on all sets of size at least $2^N (1 - \frac{1}{N^2})$. As $\mathcal{A}$ is a strictly-sublinear time algorithm (hence, also a strictly-sublinear query algorithm), it can at best correctly compute P on at most $2^N (1 - \frac{1}{N^2})$ many strings outside of its promise. This, by construction, means $\mathcal{D}$ accepts at least $\frac{2^N}{N^2}$ many strings of length N and therefore D_n will contain these strings (or alternatively these functions). Now it is easy to see that $\mathcal{D}$ computes a natural property $(D_n)_{n \in \mathbb{N}}$, of density $(\delta_n = \frac{1}{2^{2n}})_{n \in \mathbb{N}}$, in $2 \cdot 2^n$ quantum time. Moreover, this property $(D_n)_{n \in \mathbb{N}}$ is useful against complexity class M .

Once we have the natural property which is useful against M , we run a similar argument as done by Razborov and Rudich. As the algorithm $\mathcal{D}$ computes (D_n) , it can distinguish truth tables of functions with small circuits (i.e., circuits of $\text{polylog}(n)$ -depth and $\text{poly}(n)$ -size or simply $\text{poly}(n)$ -size) from truth tables of truly random functions with $\frac{1}{2^{2n}}$ advantage. But many believe that it is not possible to have quantum adversaries that are bounded by $2 \cdot 2^n$ time and distinguish pseudorandom functions constructible in M with $\frac{1}{2^{2n}}$ advantage. Then it must be the case that P is compression oblivious for M .

Part 2: Fourier analysis of Boolean functions

As discussed above, our impossibility results hold for properties that are computable in $\text{DTIME}(\text{linear})$ and that have high quantum query complexity even when the computation is restricted to strings from sets of size $2^N (1 - \frac{1}{N^2})$. Both PARITY and MAJORITY can be

computed in $\text{DTIME}(\text{linear})$. Moreover, using techniques from Fourier analysis, we are able to show that PARITY and MAJORITY also require $\Omega(N)$ many quantum queries on sets of size $2^N(1 - \frac{1}{N^2})$. Therefore, proving Theorem 2.

1.2 Related work

- Chen *et al.* in [14] use the QSETH framework to conjecture quantum time lower bounds for variants of CNFSAT such as $\oplus\text{CNFSAT}$ and $\#\text{CNFSAT}$, etc and show lower bounds for several computational problems, such as variants of lattice problems, set-cover, hitting-set, etc., as implications.
- Arunachalam *et al.* in [7] also discuss the notion of quantum natural properties but they do so to relate learning algorithms and circuit lower bounds. As one of the results, they show that containment of the Minimum Circuit Size Problem (MCSP) in BQP implies new circuit lower bounds. This type of result was later extended by [15] to show that a few (more) quantum complexity classes can be separated if the Minimum Quantum Circuit Size Problem (MQCSP) is in BQP. Despite the overlap in topic, both of these works turn out to be complementary to the current work. We use the notion of quantum natural properties to strengthen Buhrman *et al.*'s QSETH framework by grounding assumptions in cryptography.
- Contrary to Razborov and Rudich's impossibility result, Chow [16] proves the existence of a natural proof useful to imply circuit lower bounds as a consequence of the Exponential-Time Hypothesis (ETH).

1.3 Discussion and open questions

In agreement with [11], we also believe that the notion of *compression-oblivious* properties is of independent interest. (See the blog post by Aviad Rubinfeld also expressing interest [29].)

- There may be other connections with topics in meta-complexity theory (as the one we witness in this paper) or say, connections with obfuscation as suspected by Aviad Rubinfeld [29] or connections with Kolmogorov complexity (as suggested by Harry Buhrman).
- Note that our results cannot be extended to show PARITY and MAJORITY are compression oblivious for AC^0 circuits. This is because AC^0 -constructible pseudorandom functions are not secure against $2^{\text{polylog}(n)}$ -time adversaries [26]. Therefore, extending this result to PARITY or MAJORITY for AC_2^0 -QSETH, i.e. CNF or DNF input, would be another step towards grounding the (necessary) assumption that such properties are compression oblivious.
- It is also worthwhile to study compression obliviousness of properties that don't meet the criteria discussed in our paper. There might be properties for which one may be able to construct natural proofs of slightly worse densities potentially implying some other complexity theoretic results as shown in [16].

On the other front, our proof technique also allows us to, in a rather black-box way, check if a particular property is likely to be compression-oblivious. One could plausibly extend our results to a larger set of functions that have a similar structure, e.g., a natural candidate would be to show an equivalent statement for symmetric functions with non-negligible mass on high-degree Fourier coefficients. It is very likely that there are in fact many properties of the type we discuss in this paper; one could use techniques similar to ones used in [3] to formally estimate the number of such properties.

1.4 Structure of the paper

In Section 2, we present useful definitions and notations. In Section 3, we formally define the QSETH framework. Our definitions omit an ambiguity from its original version presented in [11]. In Section 4, we prove our main result - the complexity-theoretic evidence for compression obliviousness of PARITY and MAJORITY. A few proofs useful for this section are moved to Appendix A. Additionally, in [13, Appendix A] in the full version of this paper, we reprove some of the earlier results about compression-oblivious properties that were given in [11]; we do this to convince the readers of the correctness of our proposed definition of the QSETH framework.

2 Preliminaries

Most of the definitions and notions presented in this section are taken from [6], and we restate them here for completeness and ease of reading.

2.1 Uniform models of computation

► **Definition 6** (Function and language recognition). *Let $f : \{0, 1\}^* \rightarrow \{0, 1\}$ be a Boolean function. The language corresponding to f is the set of strings L_f on which f evaluates to 1, i.e., $\forall x \in \{0, 1\}^*$,*

$$x \in L_f \iff f(x) = 1.$$

Additionally, we say a Turing machine M decides a language L_f if for all $x \in \{0, 1\}^$, whenever M is initialized to the start configuration on input x , the machine M halts with $f(x)$ written on its output tape.*

► **Definition 7** (DTIME, Definition 1.12 in [6]). *Let $T : \mathbb{N} \rightarrow \mathbb{N}$ be a function. A language L is in $\text{DTIME}(T(n))$ if there exists a Turing machine M , and there exists a constant c , such that $\forall n, \forall x \in \{0, 1\}^n$, M on input x runs in $c \cdot T(n)$ steps and decides L .*

► **Definition 8** (BQTIME, adapting Definition 10.9 in [6]). *Let $f : \{0, 1\}^* \rightarrow \{0, 1\}$ and $T : \mathbb{N} \rightarrow \mathbb{N}$ be a function. We say f is computable in quantum $T(n)$ -time, or (equivalently) say $L_f \in \text{BQTIME}(T(n))$, if there is a classical polynomial-time Turing machine that, for every $n \in \mathbb{N}$, on input $(1^n, 1^{T(n)})$ outputs the descriptions of a $T(n)$ -size quantum circuit,⁵ let us denote it by $F := (F_1, \dots, F_{T(n)})$, such that for every $x \in \{0, 1\}^n$, the output of the following process is $f(x)$ with probability at least $2/3$:*

1. Initialize an m -qubit quantum state $|x\rangle |0^{m-n}\rangle$, where $m \leq T(n)$.
2. Apply one after the other $T(n)$ elementary quantum operations $F_1, \dots, F_{T(n)}$ to the state.⁶
3. Measure the last qubit in the computational basis and output the measurement outcome.

A language L_f corresponding to a Boolean function $f : \{0, 1\}^* \rightarrow \{0, 1\}$ is in BQP if there exists a polynomial p such that f is computable in quantum $p(n)$ -time, or equivalently, $L_f \in \text{BQTIME}(p(n))$.

⁵ A few clarifications.

- A description of a T -size quantum circuit $F := (F_1, \dots, F_T)$ is an ordered sequence of T elements, where $\forall i \in [T]$ each element $F_i = (G_i, w_i)$ specifies a quantum elementary gate $G_i \in \{\text{CNOT}\} \cup \{\text{set of all 1-qubit operations}\}$ and the label(s) of the wire(s) w_i on which gate G_i will be applied.
- The action “applying an elementary quantum operation $F_i = (G_i, w_i)$ ” means applying the elementary gate G_i on wire specified by location(s) w_i .
- The size of the quantum circuit, on the other hand, is the number of elements in its description.

⁶ See Footnote 5.

2.2 Non-uniform model of computation - Boolean circuits and circuit families

► **Definition 9** (Boolean circuits, Definition 6.1 in [6]). *For every $n \in \mathbb{N}$, an n -input, single-output Boolean circuit is a directed acyclic graph with n sources (i.e., vertices with no incoming edges but could have an unbounded number of outgoing edges) and one sink (i.e., vertex with no outgoing edges); let us denote the sink vertex by s . All non-source vertices are called gates and are labeled with one of $\wedge$, $\vee$ or $\neg$ (the logical operations AND, OR and NOT, respectively). The vertices labeled with $\wedge$ and $\vee$ have fan-in equal to 2 and those labeled with $\neg$ gate have fan-in 1. The source vertices are labeled with indices $i \in [n]$. We use $\text{label}(v)$ to denote the label of a vertex v . The circuit-size of C , denoted by $|C|$, is the total number of vertices in it.*

If C is a Boolean circuit and $x \in \{0,1\}^n$ is some input, then the output of C on x , denoted by $C(x)$, is defined in the natural way. More formally, for every vertex v of C we define a $\text{val}(v)$ as follows: if $\text{label}(v) = i$ then $\text{val}(v) = x_i$ and otherwise $\text{val}(v)$ is defined recursively by applying the logical operation of v labeled by $\text{label}(v)$ on the values of vertices connected to v . The output $C(x)$ is the value of the sink vertex $\text{val}(s)$.

In any situation, if we require that the Boolean circuits are only allowed to have $\wedge$ and $\vee$ gates with fan-in 2, as opposed to these gates having unbounded fan-in, then we explicitly mention it.

► **Definition 10** (Circuit family and language recognition, Definition 6.2 in [6]). *Let $T : \mathbb{N} \rightarrow \mathbb{N}$ be a function. A $T(n)$ -size circuit family is a sequence $\{C_n\}_{n \in \mathbb{N}}$ of Boolean circuits where for every n , C_n has n inputs and a single output and its circuit size $|C_n| \leq T(n)$.*

► **Definition 11** (SIZE). *Let $T : \mathbb{N} \rightarrow \mathbb{N}$ be a function. We say a language $L \in \text{SIZE}(T)$ if there exists a $T(n)$ -size circuit family $\{C_n\}_{n \in \mathbb{N}}$ such that $\forall n$, C_n consists of $\wedge$ and $\vee$ gates with fan-in 2 and $\neg$ gates of fan-in 1 and, moreover, $\forall x \in \{0,1\}^n, x \in L \iff C_n(x) = 1$.*

► **Definition 12** (Complexity class). *A complexity class is a set of languages.*

► **Definition 13** (Circuit family corresponding to a language). *Let L be a language (as in Definition 6). We say a family of circuits $\{C_n\}_{n \in \mathbb{N}}$ corresponds to language L , if $\forall n$, $\forall x \in \{0,1\}^n$, we have $x \in L \iff C_n(x) = 1$.*

► **Definition 14** (P/poly, Definition 6.5 in [6]). *P/poly is the class of languages that are decidable by polynomial-sized circuit families, or equivalently, $\text{P/poly} = \cup_{c,d} \text{SIZE}(c \cdot n^d) = \cup_{c,d} \text{SIZE}_{c,d}$.*

► **Definition 15** (AC_2^0 , Adapting Definition 6.25 in [6]). *A language L is in AC_2^0 if there exists a polynomial $p : \mathbb{N} \rightarrow \mathbb{N}$ and there exists a $p(n)$ -size circuit family $\{C_n\}_{n \in \mathbb{N}}$ corresponding to L where $\forall n$, circuit C_n uses $\neg$, $\wedge$ and $\vee$ gates, with latter two allowed to have unbounded fan-in, and has depth at most 2.*

► **Definition 16** (Type-O complexity class). *We say a complexity class is of Type-O if it is any of the following complexity classes:*

1. *For every $d \in \mathbb{N}$ and $k \in \mathbb{N}$, we include the class $\text{AC}_{d,k}^0$; we say a language $L \in \text{AC}_{d,k}^0$ if there exists a family of Boolean circuits $\{C_n\}_{n \in \mathbb{N}}$ corresponding to L such that $\forall n$, C_n uses $\neg$, $\wedge$ and $\vee$ gates, with latter two allowed to have unbounded fan-in, and has depth at most d and circuit size $|C_n| \leq n^k$.*

2. For every $d \in \mathbb{N}$ and $k \in \mathbb{N}$, we include the class $\text{NC}_{d,k}$; we say a language $L \in \text{NC}_{d,k}$ if there exists a family of Boolean circuits $\{C_n\}_{n \in \mathbb{N}}$ corresponding to L such that $\forall n$, C_n has depth at most $\log^d n$ and circuit size $|C_n| \leq n^k$.
3. For every $d \in \mathbb{N}$ and $k \in \mathbb{N}$, we include the class $\text{SIZE}_{d,k}$; we say a language $L \in \text{SIZE}_{d,k}$ if there exists a family of Boolean circuits $\{C_n\}_{n \in \mathbb{N}}$ corresponding to L such that $\forall n$, C_n has circuit size $|C_n| \leq d \cdot n^k$.

2.3 Truth tables of circuits, languages and a few other useful notations

A truth table is binary string capturing the outputs of a Boolean function. If a function is defined on n binary inputs then its corresponding truth table is a Boolean string in $\{0, 1\}^{2^n}$. The notion of a truth table can also be extended to capture the membership of strings in a language by fixing the length of the strings. We formally define these notions as follows.

► **Definition 17 (Truth tables).** For any $n \in \mathbb{N}$, let $f_n : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. Then the truth table of f_n , denoted by $\text{tt}(f_n)$, is a 2^n -length binary string constructed in the following way:

$$\text{tt}(f_n) = \bigcirc_{a \in \{0, 1\}^n} f_n(a).$$

Here $f_n(a)$ denotes the output f_n on input a . And for the concatenation, the strings $a \in \{0, 1\}^n$ are taken in lexicographic order.

For a language $L \subseteq \{0, 1\}^*$ the notion of truth table is as follows: for any $n \in \mathbb{N}$, the truth table of L at n , denoted by $\text{tt}(L, n)$, is a 2^n -length binary vector that can be obtained by concatenating the outputs $b_a := [a \in L]$ for all $a \in \{0, 1\}^n$ taken in lexicographic order.

Other useful notations

Let n be an integer. Let $f_n : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function on n input variables.

- We use F_n to denote the set of *all* Boolean functions defined on n input variables; We represent $F_n = \{\text{tt}(f_n) \mid f_n \text{ is a Boolean function on } n \text{ variables}\}$ as the set of truth tables of all functions $f_n : \{0, 1\}^n \rightarrow \{0, 1\}$, implying $F_n = \{0, 1\}^{2^n}$ and $|F_n| = 2^{2^n}$. We also use $N = 2^n$.
- We overload the notation of $\text{tt}(\cdot)$ on sets of Boolean functions to denote the following: if S is a set of Boolean functions on n variables then $\text{tt}(S) = \{\text{tt}(f_n) \mid f_n \in S\}$.
- Let Λ be a complexity class. Let $L \in \Lambda$. Furthermore, let $f_n : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function such that $\text{tt}(f_n) = \text{tt}(L, n)$ then we say f_n is a *sub-element* of Λ .
- We sometimes also overload the notation of $\text{tt}(\cdot)$ on complexity classes to denote the following: if Λ is a complexity class then $\text{tt}(\Lambda, n) = \{\text{tt}(f_n) \mid f_n \text{ sub-element in } \Lambda\}$ or equivalently $\text{tt}(\Lambda, n) = \{\text{tt}(L, n) \mid L \in \Lambda\}$. Furthermore, we use $\text{tt}(\Lambda) = \bigcup_{n \in \mathbb{N}} \text{tt}(\Lambda, n)$.

3 The QSETH framework

3.1 Definitions

► **Definition 18 (Property).** A Boolean property (or just property) is a sequence $P := (P_n)_{n \in \mathbb{N}}$ where each P_n is a set of Boolean functions defined on n variables.

Alternatively, one can view P_n as a set of 2^n -length Boolean strings that are truth tables of functions $f_n \in P_n$, or equivalently view it as a function $P_n : \{0, 1\}^{2^n} \rightarrow \{0, 1\}$ such that $P_n(\text{tt}(f_n)) = 1$ if and only if $f_n \in P_n$; see Definition 17 for the definition of a truth table. Also note that it is possible for a property P to be *partial*. In such a case, for every n , there could be some functions f_n for which we don't care whether or not they belong to P_n .⁷

⁷ For example, both the properties PP_{edit} and PP_{ics} considered in [11] are partial.

Quantum query complexity of P

The (bounded-error) quantum query complexity is defined only in a non-uniform setting; therefore, we define this notion for P_n for every $n \in \mathbb{N}$. A quantum query algorithm $\mathcal{B}$ for $P_n : \{0, 1\}^{2^n} \rightarrow \{0, 1\}$, on an input $x \in \{0, 1\}^{2^n}$ begins in a fixed initial state $|\psi_0\rangle$, applies a sequence of unitaries $U_0, O_x, U_1, O_x, \dots, U_T$, and performs a measurement whose outcome is denoted by z . Here, the initial state $|\psi_0\rangle$ and the unitaries $U_0, U_1, \dots, U_T$ are independent of the input x . The unitary O_x represents the “query” operation, and maps $|i\rangle |b\rangle$ to $|i\rangle |b + x_i \bmod 2\rangle$ for all $i \in [2^n] - 1$. We say that $\mathcal{B}$ is a $1/3$ -bounded-error algorithm computing P_n if for all x in the domain of P_n , the success probability of outputting $z = P_n(x)$ is at least $2/3$. Let $\text{cost}(\mathcal{B})$ denote the number of queries $\mathcal{B}$ makes to O_x throughout the algorithm. The $1/3$ -bounded-error quantum query complexity of P_n , denoted by $Q_{1/3}(P_n)$, is defined as $Q_{1/3}(P_n) = \min\{\text{cost}(\mathcal{B}) : \mathcal{B} \text{ computes } P_n \text{ with error probability } \leq 1/3\}$.⁸

Algorithms computing a property P in black-/white-box setting

We say a (bounded-error quantum) algorithm $\mathcal{A}$ computes a property P (as in Definition 18) in the *black-box* setting if for all $n \in \mathbb{N}$, for all f_n given its truth table as input, i.e., a 2^n -length Boolean string, $\mathcal{A}$ makes (quantum) queries to this input and (with success probability at least $2/3$) determines whether or not $f_n \in P_n$. An algorithm computing P in the *white-box* setting gets a circuit description of f_n , which is possibly a more succinct description of f_n ’s truth table, and the algorithm has to determine whether or not $f_n \in P_n$. We emphasize that, in both the black-/white-box setting, we care about the *time* that algorithm $\mathcal{A}$ takes when deciding whether or not $f_n \in P_n$.

We now present the definition of compression-oblivious properties. In simple terms, these are the properties whose quantum query complexity is a lower bound for the time complexity to compute the property even for inputs that are “compressible” as a truth table of small formulas (or circuits). Formally,

► **Definition 19** ($\Gamma_{d,k}$ -compression-oblivious properties). *Let $d, k \in \mathbb{N}$. Let $\Gamma_{d,k}$ denote a Type-O complexity class as stated in Definition 16 parameterized by d and k . We say a property P is $\Gamma_{d,k}$ -compression-oblivious, denoted by $P \in \mathcal{CO}(\Gamma_{d,k})$, if for every constant $\delta > 0$, for every quantum algorithm $\mathcal{A}$ that computes P in the **black-box** setting, $\forall n' \in \mathbb{N}, \exists n \geq n'$ and $\exists$ a set $L = \{L^1, L^2, \dots\} \subseteq \Gamma_{d,k}$ of “hard languages”, such that $\forall$ circuit families $\{C_{n''}^1\}_{n'' \in \mathbb{N}}$ corresponding to L^1 , $\forall$ circuit families $\{C_{n''}^2\}_{n'' \in \mathbb{N}}$ corresponding to L^2 , $\dots$, the algorithm $\mathcal{A}$ uses at least $Q_{1/3}(P_n)^{1-\delta}$ quantum time on at least one of the inputs in $\{C_n^i\}_{i \in [|L|]}$.⁹*

► **Definition 20** (compression-oblivious properties w.r.t. AC_2^0 , NC, P/poly). *We say a property $P : \{0, 1\}^* \rightarrow \{0, 1\}$ is*

1. $P \in \mathcal{CO}(\text{AC}_2^0)$ if $d = 2$ and $\exists k \in \mathbb{N}$ such that $P \in \mathcal{CO}(\text{AC}_{d,k}^0)$,
2. $P \in \mathcal{CO}(\text{AC}^0)$ if $\exists d \in \mathbb{N}, \exists k \in \mathbb{N}$ such that $P \in \mathcal{CO}(\text{AC}_{d,k}^0)$,
3. $P \in \mathcal{CO}(\text{NC})$ if $\exists d \in \mathbb{N}, \exists k \in \mathbb{N}$ such that $P \in \mathcal{CO}(\text{NC}_{d,k})$, and
4. $P \in \mathcal{CO}(\text{P/poly})$ if $\exists d \in \mathbb{N}, \exists k \in \mathbb{N}$ such that $P \in \mathcal{CO}(\text{SIZE}_{d,k})$.

⁸ Note that if $\text{PARITY} := (\text{PARITY}_n)_{n \in \mathbb{N}}$ is the property we are considering, under our definition of PARITY_n the value of $Q(\text{PARITY}_n)$ is equal to $\Omega(2^n)$ and not $\Omega(n)$. For the property $\text{OR} := (\text{OR}_n)_{n \in \mathbb{N}}$ then $Q(\text{OR}_n) = \Omega(2^{\frac{n}{2}})$.

⁹ While the idea of compression-oblivious properties can be easily expressed informally, describing the notion formally requires discussing intricate details to bridge the connections between uniform (e.g., algorithm $\mathcal{A}$ computing P) and non-uniform models of computations (e.g., query complexity $Q(P_n)$).

The original definition of compression-oblivious properties, as presented in Section 2.2 of [11], does not clearly enforce a unique ordering of the quantifiers, which can potentially lead to undesirable consequences. Hence, we make the effort of presenting a more formal definition of Γ -compression-oblivious properties in Definitions 19 and 20 (with the approval of the authors [11]).

Having formally defined Γ -compression-oblivious properties for all $\Gamma \in \{\text{AC}_2^0, \text{AC}^0, \text{NC}, \text{P/poly}\}$ we now state the Γ -QSETH conjecture. Earlier in this section, we discussed the difference between computing a Boolean property in a black-box setting versus computing the same property in a white-box setting. The compression-oblivious properties are those properties for which its corresponding quantum query complexity lower bounds the time complexity in the *black-box* setting. For such properties, Buhrman *et al.* conjectured that the time complexity of computing these properties in the *white-box* setting is as bad as it is in the black-box setting. This assumes that the succinct description of the Boolean functions doesn't help in computing the properties more efficiently. (This is similar to the *Black-Box Hypothesis (BBH)* stated in [22].) More formally,

► **Conjecture 21** (Γ -QSETH, a more formal presentation of Conjecture 5 in [11]). *Let $\Gamma \in \{\text{AC}_2^0, \text{AC}^0, \text{NC}, \text{P/poly}\}$ be a complexity class (as in Definition 12). Let P be a Γ -compression-oblivious property. The Γ -QSETH conjecture states that $\exists d, \exists k \in \mathbb{N}$, such that for every constant $\delta > 0$, for every quantum algorithm $\mathcal{A}$ that computes P in the **white-box** setting, $\forall n' \in \mathbb{N}, \exists n \geq n', \exists$ a set $L = \{L^1, L^2, \dots\} \subseteq \Gamma_{d,k}, \forall$ circuit families $\{C_{n''}^1\}_{n'' \in \mathbb{N}}$ corresponding to $L^1, \forall$ circuit families $\{C_{n''}^2\}_{n'' \in \mathbb{N}}$ corresponding to $L^2, \dots$, the algorithm $\mathcal{A}$ uses at least $Q_{1/3}(P_n)^{1-\delta}$ quantum time on at least one of the inputs in $\{C_n^i\}_{i \in [|L|]}$. Note that $\Gamma_{d,k}$ is a Type-O complexity class corresponding to Γ .*

3.2 Relevance

Note that a basic version of the QSETH conjecture and its implications has already been discussed in complementary works [1, 11], and other variants of QSETH are discussed more recently in [14] and in Chen's PhD thesis [12]. For example,

► **Conjecture 22** (Basic-QSETH, Conjecture 8.3 in [12]). *For each constant $\delta > 0$, there exists $c > 0$ such that there is no bounded-error quantum algorithm that solves CNFSAT (even restricted to formulas with at most cn^2 many clauses) in $O(2^{\frac{n(1-\delta)}{2}})$ time.*

► **Conjecture 23** ($\oplus$ QSETH, Conjecture 8.9 in [12]). *For each constant $\delta > 0$, there exists $c > 0$ such that there is no bounded-error quantum algorithm that solves $\oplus$ CNFSAT (even restricted to formulas with at most cn^2 many clauses) in $O(2^{n(1-\delta)})$ time.*

► **Conjecture 24** ($\#$ QSETH, Conjecture 8.8 in [12]). *For each constant $\delta > 0$, there exists $c > 0$ such that there is no bounded-error quantum algorithm that solves $\#$ CNFSAT (even restricted to formulas with at most cn^2 many clauses) in $O(2^{n(1-\delta)})$ time.*

We are able to get these conjectures as a corollary to our QSETH framework. More precisely,

► **Corollary 25.** *The AC_2^0 -QSETH implies Conjecture 22. Additionally, if we assume that $\text{PARITY} \in \text{CO}(\text{AC}_2^0)$ then AC_2^0 -QSETH implies Conjectures 23 and 24.*

Proof. The proof of $\text{OR} \in \text{CO}(\text{AC}_2^0)$ was first given in [11] (we also present the proof in the full version of this paper). Thereafter, setting $d = 2$ and $k = 3$ for AC_2^0 -QSETH conjecture implies Conjectures 22–24. ◀

Therefore, all the QSETH-based lower bounds presented in Chen's PhD thesis [12] immediately follow from our QSETH framework.

4 When certain properties are not P/poly-compression-oblivious

In this section, we show that it is reasonable to conjecture that there exist $d', k' \in \mathbb{N}$ and $d'', k'' \in \mathbb{N}$ for which properties such as PARITY and MAJORITY are $\text{SIZE}_{d', k'}$ -compression-oblivious and $\text{SIZE}_{d'', k''}$ -compression-oblivious, respectively. We do so by relating this conjecture to topics in circuit complexity and pseudorandomness. In fact, we are able to show similar consequences for properties that satisfy certain constraints. PARITY and MAJORITY happen to be such properties.

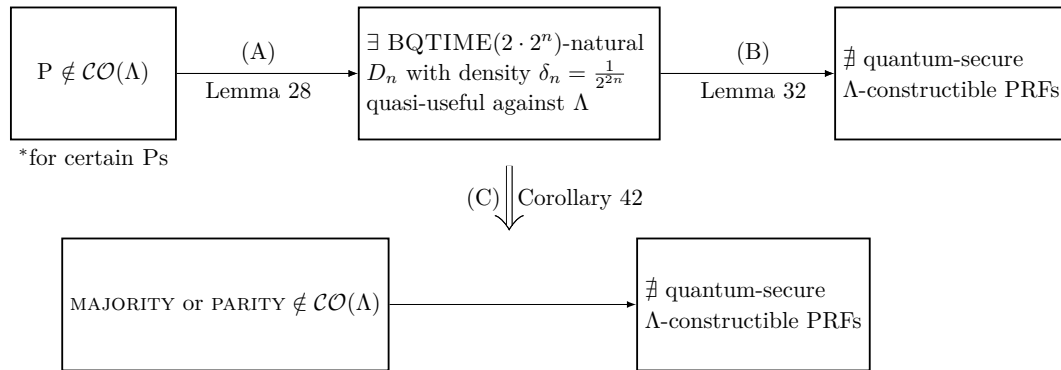
Following the notation about natural proofs from [28] and [16], we now define the following.

► **Definition 26** (Υ -natural property with density δ). *Let Υ be a complexity class (as in Definition 12) and let $\delta := (\delta_n)_{n \in \mathbb{N}}$ denote a sequence of positive real numbers. A property $D := (D_n)_{n \in \mathbb{N}}$ (as in Definition 18) is Υ -natural with density $\delta := (\delta_n)_{n \in \mathbb{N}}$ if the following statements hold:*

1. *largeness: $\exists n', \forall n > n', |D_n| \geq 2^{2^n} \cdot \delta_n$, and*
2. *constructivity: the problem of determining whether a Boolean function $f_n \in D_n$, when given as input the truth table of f_n on n variables, is decidable in Υ , which in more formal terms translates to saying $L_D \in \Upsilon$ where $L_D := \bigcup_{n \in \mathbb{N}} \{\text{tt}(f_n) \mid f_n \in D_n\}$.*

► **Definition 27** (Quasi-useful property, Definition 5 in [16]).¹⁰ *Let Λ denotes a complexity class. A property $D := (D_n)$, or equivalently the corresponding language $L_D := \bigcup_{n \in \mathbb{N}} \{\text{tt}(g_n) \mid g_n \in D_n\}$, is quasi-useful against complexity class Λ if $\forall (f_n)$, we have $(f_n) \notin \Lambda$ whenever (f_n) is sequence of Boolean functions satisfying $f_n \in D_n$ for all sufficiently large n .*

Our goal is to realize the chain of arguments as illustrated in Figure 1.



► **Figure 1** Chain of arguments presented in this section. We discuss the implications when a certain class of properties P are not Λ -compression-oblivious in links (A) and (B). In link (C) we show that MAJORITY and PARITY belong to this class of properties.

¹⁰ Note that Razborov and Rudich use the notion of *useful* property which is defined for infinitely many n . However, for our results the notion of *quasi-useful* property (defined for all sufficiently large n) makes more sense so we use this instead.

Realising link (A)

The proof idea is as follows. Let $\Lambda = \text{SIZE}_{d,k}$. Our choice of d, k will be clear later. If $\text{PARITY} \notin \mathcal{CO}(\Lambda)$ (or say $\text{MAJORITY} \notin \mathcal{CO}(\Lambda)$ may be for another choice of d, k) then (from the definition of compression-oblivious properties) there exists a quantum algorithm that computes the PARITY (or MAJORITY) of truth tables of circuits C that are sub-elements of Λ in time sublinear in the size of the input $\text{tt}(C)$. Using this algorithm and the linear time deterministic algorithm to compute PARITY (or MAJORITY) on all strings of length $|\text{tt}(C)|$, we will construct a $\text{BQTIME}(\text{linear})$ -natural property that is quasi-useful against complexity class Λ . Interestingly enough, the idea also generalizes to other simple properties that satisfy certain requirements; we formalize that in the statement of Lemma 28.

► **Lemma 28.** *Let $d, k \in \mathbb{N}$ and $\Lambda = \text{SIZE}_{d,k}$. If a property $P : \{0,1\}^* \rightarrow \{0,1\}$, or alternatively denoted as $(P_n)_{n \in \mathbb{N}}$ (as in Definition 18), satisfies the following conditions:*

1. $P \notin \mathcal{CO}(\Lambda)$,
 2. P on inputs of length N is computable in $\text{DTIME}(N)$, which more formally means $L_P := \bigcup_{n \in \mathbb{N}} \{\text{tt}(f_n) \mid f_n \in P_n\} \in \text{DTIME}(N)$, and
 3. $\forall S \subseteq \{0,1\}^N$ of size $|S| \geq 2^N(1 - \frac{1}{N^2})$, any $1/3$ -bounded-error quantum query algorithm that computes $P_{\log N}$ on each $x \in S$ requires $\Omega(N)$ queries,
- then there exists a $\text{BQTIME}(2 \cdot N)$ -natural property (D_n) with density $\delta_n = \frac{1}{N^2}$ and this natural property is quasi-useful against complexity class Λ .

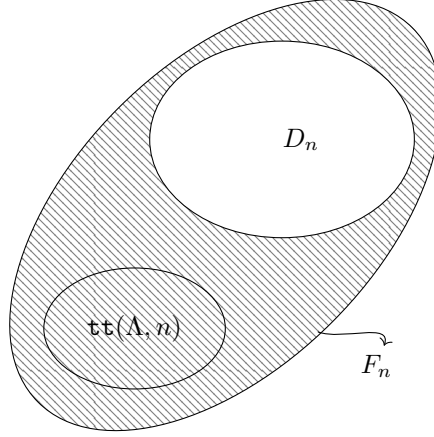
Proof. Let $d, k \in \mathbb{N}$ and let $\Lambda = \text{SIZE}_{d,k}$. From Definition 19 we say, $P \notin \mathcal{CO}(\Lambda)$ if and only if $\exists \delta > 0$, $\exists$ algorithm $\mathcal{A}$ computing property P such that $\exists n' \in \mathbb{N}$ and $\forall n \geq n'$, $\forall L = \{L^1, L^2, \dots\} \subseteq \Lambda$, $\mathcal{A}$ uses at most $Q_{1/3}(P_n)^{1-\delta}$ quantum time on all inputs in $\{\text{tt}(L^i, n)\}_{i \in [|L|]}$.

Then, let $n \geq n'$, let $N = 2^n$ and let L be the largest subset of Λ , i.e., the set Λ itself, $\mathcal{A}$ computes the property in at most $Q_{1/3}(P_n)^{1-\delta}$ time for all binary strings in $\text{tt}(\Lambda) = \{\text{tt}(L^i, n)\}_{i \in [|L|]}$. Furthermore, we have $|\text{tt}(\Lambda)| \leq 2^{d' \cdot n^k}$ for some $d' > d$; this is because all the languages $L^i \in \Lambda$ which means for every L^i there must exist a circuit family $\{C_n^i\}_{n \in \mathbb{N}}$ with $|C_n^i| \leq d \cdot n^k$ and the number of such circuits is at most $2^{d' \cdot n^k}$ which means the number of *unique* 2^n -length truth tables that Λ can hold is at most $2^{d' \cdot n^k}$. W.l.o.g., let us assume that $\mathcal{A}$ computes P with success probability at least $9/10$ (as we can boost the probability of success by running the $1/3$ -bounded-error algorithm $\mathcal{A}$ and then take majority voting). For all $n > n'$, for all $x \in \text{tt}(\Lambda, n)$, the algorithm $\mathcal{A}$ computes $P(x)$ in $Q_{1/10}(P_{\log |x|})^{1-\delta} \leq |x|^{1-\delta}$ time for some constant $\delta > 0$.

In addition, let $\mathcal{B}$ denote a deterministic (quantum or classical) algorithm that computes P on all $y \in \{0,1\}^*$ in $\Theta(|y|)$ time – upper and lower bound follow from Item 2 and Item 3 of the theorem statement, respectively. Using $\mathcal{A}$ and $\mathcal{B}$ we now construct Algorithm $\mathcal{D}$ that on an input $z \in \{0,1\}^N$ does the following:

1. Run $\mathcal{A}$ on z for $M = O(1)$ times and note the outputs.
2. Run $\mathcal{B}$ on z once.
3. **Accept** if over M runs of $\mathcal{A}$ on input z the number of times $\mathcal{A}(z) = \mathcal{B}(z)$ is at most $\frac{8}{10} \cdot M$, otherwise **reject**. We need the success probability of $\mathcal{D}$ to be at least $2/3$ therefore choosing $M = O(1)$ suffices.

Notice that Algorithm $\mathcal{D}$ (with high probability) computes a property that is quasi-useful (Definition 27) against complexity class Λ . This is true because $\mathcal{B}(z) = P(z)$ for all z and whenever $z \in \text{tt}(\Lambda)$ the $\Pr[\mathcal{A}(z) = P(z)] \geq 0.9$, which means the outputs $\mathcal{A}(z)$ and $\mathcal{B}(z)$ are equal more than $9/10$ of the M times. Therefore, if $z \in \text{tt}(\Lambda)$ then $\mathcal{D}$ rejects z .



■ **Figure 2** A pictorial representation of the fraction of 2^n -length strings that the algorithm $\mathcal{D}$ accepts. Recall that F_n denotes the full set $\{0, 1\}^{2^n}$; hence, $|F_n| = 2^{2^n}$. The set $\text{tt}(\Lambda, n)$ denotes the set of strings $\{\text{tt}(L, n) \mid L \in \Lambda\}$. Algorithm $\mathcal{A}$ is guaranteed to accept all strings from $\text{tt}(\Lambda, n)$ with success probability at least $9/10$ and no guarantee whatsoever on strings in $F_n \setminus \text{tt}(\Lambda, n)$. The set D_n denotes the set of 2^n -length strings that Algorithm $\mathcal{D}$ accepts.

What is left is to argue that Algorithm $\mathcal{D}$ computes a $\text{BQTIME}(2 \cdot N)$ -natural property that satisfies both the *largeness* and *constructivity* conditions as mentioned in Definition 26. Let $z \in F_n$ and let $D_n = \{z \mid |z| = 2^n \text{ and Algorithm } \mathcal{D} \text{ accepts } z\}$.

- Algorithm $\mathcal{D}$ on any z of size $N = 2^n$ can in at most $2 \cdot N$ quantum time decide whether or not $z \in D_n$; hence satisfying the *constructivity* condition.
- We argue about the largeness condition of $|D_n| \geq 2^N \cdot \delta_n$ for $\delta_n = \frac{1}{N^2}$ in the following way. Consider the set F_n , i.e., the set of truth tables of all Boolean functions defined on n input variables. For a string $z \in F_n$, the algorithm $\mathcal{D}$ rejects z only if $\Pr[\mathcal{A}(z) = P(z)] > 8/10$. In other words, $\mathcal{D}$ rejects z whenever $z \in F_n \setminus D_n$; see Figure 2. The runtime of Algorithm $\mathcal{A}$ on N -length inputs is $O(N^{1-\beta})$ time (for a constant $\beta > 0$), and we know from Item 3 in the statement of the theorem that $\mathcal{A}$ cannot compute P correctly (with success probability greater than $2/3$) on sets bigger than $2^N(1 - \frac{1}{N^2})$. Hence, $|F_n \setminus D_n| \leq 2^N \cdot (1 - \frac{1}{N^2})$, which means $|D_n| \geq \frac{2^N}{N^2}$.

This concludes the proof of Lemma 28. ◀

Realising link (B)

We will now show the cryptographic implications when properties like PARITY and MAJORITY are not compression-oblivious. In link (A) we showed that, if either of these properties is not compression-oblivious with respect to complexity class $\Lambda = \text{SIZE}_{d,k}$ for some constants $d, k \in \mathbb{N}$, then we can construct a $\text{BQTIME}(2 \cdot 2^n)$ -natural property useful against Λ . Any quantum algorithm computing this natural property can now be used to distinguish pseudorandom functions constructible in $\Lambda = \text{SIZE}_{d,k}$ from truly random functions. However, such linear-time (linear in the length of the truth table of the functions) quantum distinguishers are not believed to exist. Therefore, it is plausible that a quantum algorithm computing this natural property in the specified time does not exist.

Let us recall the standard definition of pseudorandom functions [18].

► **Definition 29** (Keyspace). Let $K : \mathbb{N} \rightarrow \mathbb{N}$ be a function. A key space $\mathcal{K}$ generated by the function K is a set of sets defined as $\mathcal{K} = \{\{0, 1\}^{K(n)}\}_{n \in \mathbb{N}}$ and we use $\mathcal{K}(n)$ to denote the set $\{0, 1\}^{K(n)}$.

Note that, for our results, the function K is always chosen to be a polynomial.

► **Definition 30** (Pseudorandom functions (PRFs)).

A set $F = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}\}_{n \in \mathbb{N}, k \in \mathcal{K}(n)}$, is called a family of pseudorandom functions with key space $\mathcal{K}$ generated by function K if for all probabilistic polynomial time (p.p.t.) adversary A , there is a negligible function ε such that for all $n \in \mathbb{N}$,

$$|\Pr_k[A^{f_k(\cdot)}(1^n) = 1] - \Pr_{\text{TR}}[A^{\text{TR}(\cdot)}(1^n) = 1]| < \eta(n),$$

where the probability is also over the random string used by A , TR denotes a truly random function from $\{0, 1\}^n$ to $\{0, 1\}$.

Sometimes we may strengthen or weaken the definition by letting the adversary's running time be $T(n)$ -bounded, and letting the distinguishing probability to be less than some specific function $\eta(n)$. In this case, we call it a (K, T, η) -PRF. Additionally, if the family F , which can be interpreted as a families of circuits, corresponds to languages in Λ , then we call it as Λ -constructible (K, T, η) -PRFs.

Pseudorandom functions can also be defined against quantum adversaries making (classical or) quantum queries; see [32] for example. Formally stated as follows.

► **Definition 31** (Quantum-secure PRFs). A set $F = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}\}_{k \in \mathcal{K}(n), n \in \mathbb{N}}$ is called a family of quantum-secure pseudorandom functions with key space $\mathcal{K}$ generated by a function K if for all polynomial time (polynomial in the length of its input) quantum adversary A making quantum queries, there is a negligible function ε such that for all $n \in \mathbb{N}$,

$$|\Pr_k[A^{f_k(\cdot)}(1^n) = 1] - \Pr_{\text{TR}}[A^{\text{TR}(\cdot)}(1^n) = 1]| < \eta(n),$$

where the probability is also over the random string used by A , TR denotes a truly random function from $\{0, 1\}^n$ to $\{0, 1\}$.

Sometimes (just as we do for PRFs) we may strengthen or weaken the definition by letting the adversary's running time be $T(n)$ -bounded, and letting the distinguishing probability governed by some other function $\eta(n)$. In this case, we denote them by (K, T, η) -quantum-secure-PRFs. Additionally, if the family F , which can be interpreted as a families of circuits, correspond to languages in Λ , then we call it as Λ -constructible (K, T, η) -quantum-secure-PRFs.

Using this notion of quantum-secure pseudorandom functions, we are able to prove the following.

► **Lemma 32.** Let $d, k \in \mathbb{N}$. If there exists a $\text{BQTIME}(2 \cdot 2^n)$ -natural property of density $\delta_n \geq \frac{1}{2^{2n}}$ that is quasi-useful against the complexity class $\Lambda = \text{SIZE}_{d,k}$ then there doesn't exist any Λ -constructible $(d \cdot n^k, 2 \cdot 2^n, \frac{1}{2^{2n}})$ -quantum-secure-PRF; the size of the truth table of function f_n is 2^n .

Proof. Let $N = 2^n$ be the length of the truth table of functions on n variables. Let P be a $\text{BQTIME}(2 \cdot N)$ -natural property of density $\delta_n \geq \frac{1}{2^{2n}}$ that is quasi-useful against the complexity class $\text{SIZE}_{d,k}$. Let $\mathcal{C}$ be the algorithm that computes this property P . Because $\mathcal{C}$ computes P , for any (sufficiently large) value of n the following statements hold.

- Algorithm $\mathcal{C}$ rejects z whenever z is a string from $\text{tt}(\text{SIZE}_{d,k}, n)$; this is because P is quasi-useful against $\text{SIZE}_{d,k}$.
- There are at least $\frac{1}{2^{2n}} \cdot 2^{2^n}$ number of functions in F_n that $\mathcal{C}$ accepts; this is because the P has density $\delta_n \geq \frac{1}{2^{2n}}$.
- Furthermore, $\mathcal{C}$ runs in $\text{BQTIME}(2 \cdot 2^n)$.

Combining these observations we can see that

$$|\Pr[\mathcal{C}(x) = 1] - \Pr[\mathcal{C}(y) = 1]| \geq \frac{1}{2^{2n}}$$

when x is chosen at random from $\text{tt}(\text{SIZE}_{d,k}, n)$ and y is chosen at random from F_n . This means $\mathcal{C}$, despite being an algorithm running in $\text{BQTIME}(2 \cdot N)$ time, can distinguish $\text{SIZE}_{d,k}$ -constructible pseudorandom functions from the set of all random functions. Hence, showing that $\text{SIZE}_{d,k}$ -constructible $(d \cdot n^k, 2 \cdot 2^n, \frac{1}{2^{2n}})$ -quantum-secure-PRFs do not exist. ◀

We could also state our assumption about the existence of quantum-secure PRFs as a conjecture.

► **Conjecture 33.** *There exists $d, k \in \mathbb{N}$ for which $\text{SIZE}_{d,k}$ -constructible $(d \cdot n^k, 2 \cdot 2^n, \frac{1}{2^{2n}})$ -quantum-secure-PRFs exist.*

Using Lemma 28 and Lemma 32 we can now claim the following statement.

► **Theorem 34.** *Let $P : \{0, 1\}^* \rightarrow \{0, 1\}$ be the Boolean property satisfying Items 2 and 3 stated in Lemma 28. Then property $P \in \mathcal{CO}(P/\text{poly})$ unless Conjecture 33 is false.*

Proof. If $P \notin \mathcal{CO}(P/\text{poly})$ then $\forall d, \forall k \in \mathbb{N}$ we have $P \notin \mathcal{CO}(\text{SIZE}_{d,k})$; see Definition 20. For every value of d, k we will then be able to construct a $\text{BQTIME}(2 \cdot 2^n)$ -natural property that will be quasi-useful against $\text{SIZE}_{d,k}$. This means for all values of d, k we will no longer have $\text{SIZE}_{d,k}$ -constructible $(d \cdot n^k, 2 \cdot 2^n, \frac{1}{2^{2n}})$ -quantum-secure-PRFs. Hence, falsifying Conjecture 33. ◀

► **Remark 35.** Although not explicitly used in this paper, we would also like to mention that under the assumption that the learning with errors (LWE) conjecture holds against quantum algorithms, there exist quantum-secure PRFs evaluatable by NC^2 circuits (NC^1 if we assume the quantum hardness of RingLWE) [9]. This suggests that under the quantum hardness of LWE (resp. RingLWE), PARITY and MAJORITY are compression obliviousness with respect to the complexity class NC^2 (resp. NC^1).

► **Remark 36** (Strengthening Conjecture 33 with OWFs). First, recall the definition of one-way functions.

► **Definition 37** (One-way functions (OWFs)). *A function $g : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is called a (T, η) -one-way function if there is a polynomial p such that for all adversary A running in time T , for all $n \in \mathbb{N}$,*

$$\Pr_{x \leftarrow \{0, 1\}^{p(n)}} [A(1^n, g(x)) = x' \text{ such that } g(x') = g(x)] < \eta(n).$$

For example, when $T = 2^n$, we can set the length of the domain and range to be $p(n) = n^2$, therefore a $T = 2^n$ adversary will not trivially break such an OWF.

It is known [20, 18] that (K, T, η) -PRF exists if $(\text{poly}(T), \text{poly}(\eta))$ -one-way function exists. Furthermore, the same result holds against quantum adversaries even if the adversary for the PRF is allowed to make superposition queries [32]. Therefore, we can say that

$(2^n, 2^{-\omega(n)})$ -PRF against quantum adversaries exists as long as $(\text{poly}(2^n), \text{poly}(2^{-\omega(n)}))$ -one-way function against quantum adversaries exists. Therefore, the following conjecture implies Conjecture 33.

► **Conjecture 38.** *Quantum secure $(\text{poly}(2^n), \text{poly}(2^{-\omega(n)}))$ -one-way functions exist.*

Realising implication (C)

Earlier in this section we discussed that the arguments presented work for properties that satisfy Items 1–3 in the statement of Lemma 28. For properties like PARITY or MAJORITY it is trivial to see that they admit a linear time (quantum and classical) deterministic algorithm. However, it is not immediately clear if the query complexity of computing these properties is “high” on sets $S \subset F_n$ that are not the full set F_n but still are relatively “large”. Using techniques from Fourier analysis of Boolean properties, we can show that this is indeed the case with PARITY and MAJORITY. In fact, we are able to say something more. More precisely, we show that the following statement holds.

► **Lemma 39.** *Let N be an integer and let $S \subseteq \{0, 1\}^N$ be a subset of size $s \geq 2^N (1 - \frac{1}{N^2})$. Let $P : \{0, 1\}^N \rightarrow \{-1, 1\}$ be a Boolean property with $Q(P) = \Omega(N)$ and the N -degree Fourier coefficient $|\hat{P}([N])| \geq \sqrt{\frac{1}{2N}}$.¹¹ Then every quantum algorithm that, with error probability $\varepsilon \leq \frac{1}{2N^2}$, computes P on each $x \in S$ uses $\Omega(N)$ queries.*

Proof. Suppose there exists a T -query algorithm, let us denote by $\mathcal{A}_S$, to compute property P on all $x \in S$ with worst-case error probability $\varepsilon \leq \frac{1}{2N^2}$. W.l.o.g, we can assume that the output of $\mathcal{A}_S$ is in $\{-1, 1\}$. Let $R(x)$ denote the probability that $\mathcal{A}_S$ outputs -1 ; then we can immediately see that $\forall x \in S$,

$$(1 - 2R(x)) \cdot P(x) \geq (1 - 2\varepsilon).^{12} \quad (1)$$

We will now estimate the degree of the polynomial $R(x)$. Observe that $\deg(R(x)) = \deg(1 - 2R(x))$. Let $Q(x) = (1 - 2R(x))$ and let $\varepsilon' = (1 - 2\varepsilon)$. Let the Fourier expansions of $Q(x) = \sum_{B \subseteq [N]} \hat{Q}(B) \chi_B(x)$ and $P(x) = \sum_{B \subseteq [N]} \hat{P}(B) \chi_B(x)$, respectively.

Towards a contradiction, suppose that $\deg(Q(x)) < N$ then $\hat{Q}([N]) = 0$, which implies

$$\begin{aligned} \left(\sum_{B \subseteq 2^{[N]}} \hat{Q}(B) \cdot \hat{P}(B) \right)^2 &\stackrel{(1)}{=} \left(\sum_{B \subseteq 2^{[N]} \setminus [N]} \hat{Q}(B) \cdot \hat{P}(B) \right)^2 \\ &\stackrel{(2)}{\leq} \left(\sum_{B \subseteq 2^{[N]} \setminus [N]} \hat{Q}(B)^2 \right) \cdot \left(\sum_{B \subseteq 2^{[N]} \setminus [N]} \hat{P}(B)^2 \right) \\ &\stackrel{(3)}{\leq} 1 - \frac{1}{2N}; \end{aligned}$$

¹¹Note that we use these constants so that Lemma 39 can be almost directly used for PARITY and MAJORITY. However, one can modify these constants to accommodate other properties as well.

¹²Since $R(x)$ is the probability that $\mathcal{A}_S$ outputs -1 and since the error probability of the algorithm is at most ε , we know that (a) if $x \in P^{-1}(-1)$, then $R(x) \geq 1 - \varepsilon$, and (b) if $x \in P^{-1}(1)$, then $R(x) \leq \varepsilon$. If this is the case (a), we obtain $(1 - 2R(x)) \cdot P(x) = (1 - 2R(x)) \cdot (-1) \geq 1 - 2\varepsilon$. Moreover, even in case (b), we obtain $(1 - 2R(x)) \cdot P(x) = (1 - 2R(x)) \cdot (+1) \geq (1 - 2\varepsilon)$. Hence Equation 1 holds.

(1) using the assumption that $\hat{Q}([N]) = 0$, (2) is argued using Cauchy-Schwarz inequality and (3) comes by using Parseval's theorem (on Boolean output and bounded functions). However, from Equation 1 we have that $\forall x \in S, Q(x) \cdot P(x) \geq \varepsilon'$ which means

$$\begin{aligned}
 \left(\sum_{B \in 2^{[N]}} \hat{Q}(B) \cdot \hat{P}(B) \right)^2 &= \left(\frac{1}{2^N} \sum_{x \in \{0,1\}^N} Q(x) \cdot P(x) \right)^2 \\
 &= \frac{1}{2^N} \left(\sum_{x \in S} Q(x) \cdot P(x) + \sum_{x \in \{0,1\}^N \setminus S} Q(x) \cdot P(x) \right)^2 \\
 &\geq \left(\varepsilon' \cdot \frac{|S|}{2^N} + \frac{1}{2^N} \sum_{x \in \{0,1\}^N \setminus S} Q(x) \cdot P(x) \right)^2 \\
 &\geq \left(\varepsilon' \cdot \frac{|S|}{2^N} - \frac{2^N - |S|}{2^N} \right)^2 \\
 &\geq \left(\left(1 - \frac{1}{N^2}\right) \cdot \frac{|S|}{2^N} - \frac{2^N - |S|}{2^N} \right)^2 \\
 &\geq \left(1 - \frac{3}{N^2} \right)^2 \\
 &> 1 - \frac{6}{N^2},
 \end{aligned}$$

leading to a contradiction; therefore, $\deg(Q(x)) = \deg(R(x)) = N$; using polynomial method [10] this implies $T = \Omega(N)$. $\blacktriangleleft$

Having stated Lemma 39 we can now immediately prove similar query lower bounds for PARITY and a *variant* of MAJORITY as their N -degree Fourier coefficients are 1 and at least $\sqrt{\frac{2}{\pi N}}$, respectively [27]. Moreover, this kind of result can be extended to show similar lower bounds for all Boolean properties P that have a non-negligible Fourier-mass of high degree coefficients. In fact, for PARITY we can show that similar lower bounds hold even on smaller sets as well. Also, we can prove such query lower bounds for MAJORITY and *st*-MAJORITY. More precisely,

▷ **Claim 40** (see Lemma 43 in Appendix A for proof). Let $S \in \{0,1\}^N$ be a subset of size $s \geq 0.8 \cdot 2^N$. Every quantum algorithm that, with success probability at least $\geq 2/3$, computes PARITY on each $x \in S$ uses $\Omega(N)$ queries.

and,

▷ **Claim 41** (see Lemma 48 in Appendix A for proof). Let $S \in \{0,1\}^N$ be a subset of size $s \geq 2^N \left(1 - \frac{1}{2 \cdot N^2}\right)$. Every quantum algorithm that, with success probability $(1 - \varepsilon) \geq \left(1 - \frac{1}{2 \cdot N^2}\right)$, computes MAJORITY (*st*-MAJORITY) on each $x \in S$ uses $\Omega(N)$ queries.

The result proved in Lemma 28 when combined with the results stated in Claims 40 and 41 along with Theorem 34 lead us to the following result.

► **Corollary 42.** Let $\Lambda = P/\text{poly}$ be the complexity class. The properties $\text{PARITY} \in \mathcal{CO}(\Lambda)$, $\text{MAJORITY} \in \mathcal{CO}(\Lambda)$ and *st*-MAJORITY $\in \mathcal{CO}(\Lambda)$ unless Conjecture 33 is false.

References

- 1 Scott Aaronson, Nai-Hui Chia, Han-Hsuan Lin, Chunhao Wang, and Ruizhe Zhang. On the quantum complexity of closest pair and related problems. In *Proceedings of the 35th Computational Complexity Conference, CCC '20*, Dagstuhl, DEU, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2020.16.
- 2 Amir Abboud, Thomas Dueholm Hansen, Virginia Vassilevska Williams, and Ryan Williams. Simulating branching programs with edit distance and friends: or: a polylog shaved is a lower bound made. In Daniel Wicks and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 375–388. ACM, 2016. doi:10.1145/2897518.2897653.
- 3 Andris Ambainis. A note on quantum black-box complexity of almost all boolean functions. *Inf. Process. Lett.*, 71(1):5–7, 1999. doi:10.1016/S0020-0190(99)00079-4.
- 4 Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H. Putra, and Shigeru Yamashita. Quantum identification of boolean oracles. In Volker Diekert and Michel Habib, editors, *STACS 2004, 21st Annual Symposium on Theoretical Aspects of Computer Science, Montpellier, France, March 25-27, 2004, Proceedings*, volume 2996 of *Lecture Notes in Computer Science*, pages 105–116. Springer, 2004. doi:10.1007/978-3-540-24749-4_10.
- 5 Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita. Improved algorithms for quantum identification of boolean oracles. *Theor. Comput. Sci.*, 378(1):41–53, 2007. doi:10.1016/J.TCS.2006.12.013.
- 6 Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009. URL: <http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521424264>.
- 7 Srinivasan Arunachalam, Alex B. Grilo, Tom Gur, Igor C. Oliveira, and Aarthi Sundaram. Quantum learning algorithms imply circuit lower bounds. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 562–573. IEEE, 2021. doi:10.1109/FOCS52979.2021.00062.
- 8 Arturs Backurs and Piotr Indyk. Edit distance cannot be computed in strongly subquadratic time (unless SETH is false). In Rocco A. Servedio and Ronitt Rubinfeld, editors, *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 51–58. ACM, 2015. doi:10.1145/2746539.2746612.
- 9 Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 719–737. Springer, 2012. doi:10.1007/978-3-642-29011-4_42.
- 10 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. doi:10.1145/502090.502097.
- 11 Harry Buhrman, Subhasree Patro, and Florian Speelman. A Framework of Quantum Strong Exponential-Time Hypotheses. In Markus Bläser and Benjamin Monmege, editors, *38th International Symposium on Theoretical Aspects of Computer Science (STACS 2021)*, volume 187 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 19:1–19:19, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.STACS.2021.19.
- 12 Yanlin Chen. *On Quantum Algorithms and Limitations for Convex Optimization and Lattice Problems*. PhD thesis, University of Amsterdam, 2024.
- 13 Yanlin Chen, Yilei Chen, Rajendra Kumar, Subhasree Patro, and Florian Speelman. Fine-grained complexity via quantum natural proofs. arXiv:2504.10363, 2025. doi:10.48550/arXiv.2504.10363.
- 14 Yanlin Chen, Yilei Chen, Rajendra Kumar, Subhasree Patro, and Florian Speelman. QSETH Strikes Again: Finer Quantum Lower Bounds for Lattice Problem, Strong Simulation, Hitting Set Problem, and More. In Alina Ene and Eshan Chattopadhyay, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2025)*, volume 353 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:24, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.APPROX/RANDOM.2025.6.

- 15 Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang. Quantum Meets the Minimum Circuit Size Problem. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.47.
- 16 Timothy Y. Chow. Almost-natural proofs. *Journal of Computer and System Sciences*, 77(4):728–737, 2011. doi:10.1016/J.JCSS.2010.06.017.
- 17 Marek Cygan, Holger Dell, Daniel Lokshtanov, Dániel Marx, Jesper Nederlof, Yoshio Okamoto, Ramamohan Paturi, Saket Saurabh, and Magnus Wahlström. On problems as hard as cnf-sat. *ACM Transactions on Algorithms (TALG)*, 12(3):1–24, 2016. doi:10.1145/2925416.
- 18 Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, 1986. doi:10.1145/6490.6503.
- 19 Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996. doi:10.1145/237814.237866.
- 20 Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999. doi:10.1137/S0097539793244708.
- 21 Cupjin Huang, Michael Newman, and Mario Szegedy. Explicit lower bounds on strong quantum simulation. *IEEE Transactions on Information Theory*, 66(9):5585–5600, 2020. doi:10.1109/TIT.2020.3004427.
- 22 Russell Impagliazzo, Valentine Kabanets, Antonina Kolokolova, Pierre McKenzie, and Shadab Romani. Does looking inside a circuit help? In *42nd International Symposium on Mathematical Foundations of Computer Science*, volume 83 of *LIPIcs*, pages 1:1–1:13, 2017. doi:10.4230/LIPIcs.MFCS.2017.1.
- 23 Russell Impagliazzo and Ramamohan Paturi. On the complexity of k-sat. *Journal of Computer and System Sciences*, 62(2):367–375, 2001. doi:10.1006/jcss.2000.1727.
- 24 Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences*, 63(4):512–530, 2001. doi:10.1006/jcss.2001.1774.
- 25 Robin Kothari. An optimal quantum algorithm for the oracle identification problem. In Ernst W. Mayr and Natacha Portier, editors, *31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014)*, *STACS 2014, March 5-8, 2014, Lyon, France*, volume 25 of *LIPIcs*, pages 482–493. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2014. doi:10.4230/LIPIcs.STACS.2014.482.
- 26 Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, fourier transform, and learnability. *Journal of ACM*, 40(3):607–620, 1993. doi:10.1145/174130.174138.
- 27 Ryan O’Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2021. arXiv:2105.10386. arXiv:2105.10386.
- 28 Alexander A. Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997. doi:10.1006/JCSS.1997.1494.
- 29 Aviad Rubinfeld. Quantum DNA sequencing & the ultimate hardness hypothesis. Blog post, 2019. URL: <https://theorydish.blog/2019/12/09/quantum-dna-sequencing-the-ultimate-hardness-hypothesis/>.
- 30 R. Ryan Williams. Self-improvement for circuit-analysis problems. In Bojan Mohar, Igor Shinkar, and Ryan O’Donnell, editors, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 1374–1385. ACM, 2024. doi:10.1145/3618260.3649723.
- 31 Ryan Williams. A new algorithm for optimal 2-constraint satisfaction and its implications. *Theoretical Computer Science*, 348(2-3):357–365, 2005. doi:10.1016/J.TCS.2005.09.023.
- 32 Mark Zhandry. How to construct quantum random functions. In *FOCS*, pages 679–687. IEEE Computer Society, 2012. doi:10.1109/FOCS.2012.37.

A

 Proofs of Claim 40 and Claim 41

► **Lemma 43.** *Let $S \in \{0, 1\}^N$ be a subset of size $s \geq 0.8 \cdot 2^N$. Every quantum algorithm that, with success probability at least $\geq 2/3$, computes PARITY on each $x \in S$ uses $\Omega(N)$ queries.*

Proof. Suppose there exists a T -query bounded-error quantum algorithm $\mathcal{A}_S$ to compute parity on each $x \in S$ with worst-case error probability $\leq 1/3$. Here, without loss of generality, we assume the output of $\mathcal{A}_S$ is in $\{-1, 1\}$, where 1 means odd parity and -1 means even parity. Let $P(x)$ be the polynomial that represents $\mathcal{A}_S$'s probability of outputting -1 on input x . Since $\mathcal{A}_S$ has worst-case error probability at most $1/3$ on each $x \in S$, we can immediately see $(1 - 2P(x)) \cdot (-1)^{|x|} \geq 1/3$ for every $x \in S$, where $|x|$ denotes the Hamming weight of x .

Observe that $\deg(P(x)) = \deg(1 - 2P(x))$ and $\mathbb{E}_{x \in \{0, 1\}^N}[(1 - 2P(x))(-1)^{|x|}]$ is the Fourier coefficient of the degree- N term of $(1 - 2P(x))$. We obtain

$$\begin{aligned} \mathbb{E}_{x \in \{0, 1\}^N}[(1 - 2P(x))(-1)^{|x|}] &= \frac{1}{2^N} \left(\sum_{x \in S} [(1 - 2P(x))(-1)^{|x|}] + \sum_{x \in \{0, 1\}^N \setminus S} [(1 - 2P(x))(-1)^{|x|}] \right) \\ &\geq \frac{1}{2^N} \cdot (s/3 - (2^N - s)) > 0, \end{aligned}$$

implying that $\deg(P(x)) \geq N$. Then by polynomial method [10],¹³ we immediately obtain $T \geq N/2$. ◀

► **Lemma 44** (Theorem 5.19 in [27]). *Let N be an odd integer and let $\text{odd-MAJORITY} : \{0, 1\}^N \rightarrow \{0, 1\}$ be defined as*

$$\text{odd-MAJORITY}(x) = \begin{cases} 1, & \text{if } |x| > \frac{N}{2}, \\ 0, & \text{otherwise,} \end{cases}$$

where $|x| = |\{i \mid i \in [N] \text{ and } x_i = 1\}|$. If the Fourier expansion of odd-MAJORITY is

$$\text{odd-MAJORITY}(x) = \sum_{B \subseteq \{0, 1\}^N} \text{ODD-MAJ}(B) \chi_B(x),$$

where $\chi_B(x) = (-1)^{x \cdot B}$, then $\text{ODD-MAJ}(B) = 0$ whenever $|B| \equiv 0 \pmod{2}$ and for $|B| = N$ we have

$$\text{ODD-MAJ}(B)^2 = \frac{4}{4^N} \binom{N-1}{\frac{N-1}{2}}^2 \geq \frac{6}{\pi(3N-1)} > \frac{2}{\pi N}.$$

► **Lemma 45.** *Let N be an odd integer and let $S \in \{0, 1\}^N$ be a subset of size $s \geq 2^N \left(1 - \frac{1}{N^2}\right)$. Every quantum algorithm that, with error probability $\varepsilon \leq \frac{1}{2 \cdot N^2}$, computes odd-MAJORITY on each $x \in S$ uses $\Omega(N)$ queries.*

Proof. The absolute value of the N -degree Fourier coefficient for odd-MAJORITY is at least $\sqrt{\frac{2}{\pi N}}$ using Lemma 39 gives us the required proof. ◀

¹³By the polynomial method we know if the amplitudes of the final state are degree- N polynomials of x then we need to make at least $T \geq N/2$ queries.

► **Lemma 46.** *Let N be an even integer and let $S \in \{0,1\}^N$ be a subset of size $s \geq 2^N(1 - \frac{1}{2 \cdot N^2})$. Every quantum algorithm that, with error probability $\varepsilon \leq \frac{1}{2 \cdot N^2}$, computes MAJORITY on each $x \in S$ uses $\Omega(N)$ queries.*

We embed the *odd*-MAJORITY into the MAJORITY and then argue lower bound for MAJORITY for sets of size at least $2^N(1 - \frac{1}{2 \cdot N^2})$ using the result obtained in Lemma 45.

Proof. Towards contradiction, let us assume that there is a set $B \subseteq \{0,1\}^N$ of size $b \geq 2^N(1 - \frac{1}{2 \cdot N^2})$ that uses at most $N^{0.999}$ queries to compute MAJORITY on all strings $y \in B$. The set $B = \{B_0 \circ 0\} \sqcup \{B_1 \circ 1\}$ can be viewed as two disjoint sets of strings ending with 0 and 1, respectively. Clearly $|B_1| \leq 2^{N-1}$ and by our assumption we have $|B| \geq 2^N(1 - \frac{1}{2 \cdot N^2})$, therefore, $|B_0| = |B| - |B_1| \geq 2^N(\frac{1}{2} - \frac{1}{2 \cdot N^2})$. Set $S' = B_0$. The set S' is a subset of strings of N' -length strings where $N' = N - 1$ and moreover N' is odd. Therefore, in terms of N' we have $|B_0| \geq 2^{N'+1}(\frac{1}{2} - \frac{1}{2 \cdot (N'+1)^2}) = 2^{N'} - \frac{2^{N'}}{2 \cdot (N'+1)^2} > 2^{N'}(1 - \frac{1}{N'^2})$. As $S' = B_0$, computing MAJORITY on strings in $B_0 \circ 0$ (or equivalently $S' \circ 0$) would be equivalent to computing *odd*-MAJORITY on N' -length strings in S' of size $|S'| \geq 2^{N'}(1 - \frac{1}{N'^2})$. But we know from Lemma 45 a sublinear query algorithm is not possible for these set sizes. Hence, proved. ◀

We can give query lower bound for *st*-MAJORITY by just setting $S' = B_1$ and running the same arguments mentioned in the proof of Lemma 46. Giving the following result for *st*-MAJORITY.

► **Lemma 47.** *Let N be an even integer and let $S \in \{0,1\}^N$ be a subset of size $s \geq 2^N(1 - \frac{1}{2 \cdot N^2})$. Every quantum algorithm that, with error probability $\varepsilon \leq \frac{1}{2 \cdot N^2}$, computes *st*-MAJORITY on each $x \in S$ uses $\Omega(N)$ queries.*

When N is odd, all the three definitions of MAJORITY, *st*-MAJORITY and *odd*-MAJORITY are equivalent. Therefore, combining Lemmas 45–47 we get the following.

► **Lemma 48.** *Let $S \in \{0,1\}^N$ be a subset of size $s \geq 2^N(1 - \frac{1}{2 \cdot N^2})$. Every quantum algorithm that, with success probability $(1 - \varepsilon) \geq (1 - \frac{1}{2 \cdot N^2})$, computes MAJORITY (*st*-MAJORITY) on each $x \in S$ uses $\Omega(N)$ queries.*