Quantum Meets the Minimum Circuit Size Problem

Nai-Hui Chia
Luddy School of Informatics, Computing, and Engineering,
Indiana University, Bloomington, IN, USA

Chi-Ning Chou
School of Engineering and Applied Sciences, Harvard University, Boston, MA, USA

Jiayu Zhang
Department of Computer Science, Boston University, MA, USA
Computing and Mathematical Sciences, California Institute and Technology, Pasadena, CA, USA

Ruizhe Zhang
Department of Computer Science, The University of Texas at Austin, TX, USA

Abstract

In this work, we initiate the study of the Minimum Circuit Size Problem (MCSP) in the quantum setting. MCSP is a problem to compute the circuit complexity of Boolean functions. It is a fascinating problem in complexity theory – its hardness is mysterious, and a better understanding of its hardness can have surprising implications to many fields in computer science.

We first define and investigate the basic complexity-theoretic properties of minimum quantum circuit size problems for three natural objects: Boolean functions, unitaries, and quantum states. We show that these problems are not trivially in NP but in QCMA (or have QCMA protocols). Next, we explore the relations between the three quantum MCSPs and their variants. We discover that some reductions that are not known for classical MCSP exist for quantum MCSPs for unitaries and states, e.g., search-to-decision reductions and self-reductions. Finally, we systematically generalize results known for classical MCSP to the quantum setting (including quantum cryptography, quantum learning theory, quantum circuit lower bounds, and quantum fine-grained complexity) and also find new connections to tomography and quantum gravity. Due to the fundamental differences between classical and quantum circuits, most of our results require extra care and reveal properties and phenomena unique to the quantum setting. Our findings could be of interest for future studies, and we post several open problems for further exploration along this direction.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases Quantum Computation, Quantum Complexity, Minimum Circuit Size Problem

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.47

Related Version *Full Version*: `https://arxiv.org/abs/2108.03171`

Funding *Nai-Hui Chia*: This work was support by the U.S. Department of Defense and NIST through the Hartree Postdoctoral Fellowship at QuICS and by NSF through IUCRC Planning Grant Indiana University: Center for Quantum Technologies (CQT) under award number 2052730.
Chi-Ning Chou: This work was supported by Boaz Barak's NSF awards CCF 1565264 and CNS 1618026.
Jiayu Zhang: This work was supported by Adam Smith's NSF awards 1763786.
Ruizhe Zhang: This work was supported by Dana Moshkovitz's NSF Grant CCF-1648712 and Scott Aaronson's Vannevar Bush Faculty Fellowship from the US Department of Defense.

Acknowledgements We are grateful to Scott Aaronson and Boaz Barak for helpful discussions and valuable comments on our manuscript. We would like to thank Lijie Chen, Kai-Min Chung, Matthew Coudron, Yanyi Liu, and Fang Song for useful discussions.

1 Introduction

The Minimum Circuit Size Problem (MCSP) is one of the central computational problems in complexity theory. Given the truth table of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and a size parameter s (in unary) as inputs, MCSP asks whether there exists a circuit of size at most s for f. While MCSP has been studied as early as the 1950s in the Russian cybernetics program [45], its complexity remains mysterious: we do not know whether it is in P or NP-hard. Meanwhile, besides being a natural computational problem, in recent years, researchers have discovered many surprising connections of MCSP to other areas such as cryptography [42], learning theory [12], circuit complexity [29], average-case complexity [18], and others.

Quantum computing is of growing interest, with applications to cryptography [44], machine learning [8], and complexity theory [28], etc. Inspired by the great success of MCSP in classical computation and the flourishing of quantum computers, we propose a new research program of studying quantum computation through the lens of MCSP. We envision MCSP as a central problem that connects different quantum computation applications and provides deeper insights into the complexity-theoretic foundation of quantum circuits.

1.1 The classical MCSP and its connections to other problems

It is immediate that MCSP $\in$ NP because the input size is 2^n so one can verify if a circuit (given as the certificate/proof) computes the input truth table in time $2^{O(n)}$. However, there is no consensus on the complexity status of this problem – MCSP could be in P, NP-complete, or NP-intermediate. Several works [37, 29] showed negative evidence for proving the NP-hardness of MCSP using standard reduction techniques. We also do not know whether there is an algorithm better than brute force search (see Perebor conjecture for MCSP [45]) or whether there is a search-to-decision reduction or a self-reduction[1] for MCSP[2]. On the other hand, several variants of MCSP are NP-hard under either deterministic reductions [36, 19] or randomized reductions [20, 23].

Researchers have discovered many surprising connections of MCSP to other fields in Theoretical Computer Science including cryptography, learning theory, and circuit lower bounds. To name a few, Razborov and Rudich [42] related natural properties against P/poly with circuit lower bounds and pseudorandomness. Kabanets and Cai [29] showed that MCSP $\in$ P implies new circuit lower bounds, and that MCSP $\in$ BPP implies that any one-way function can be inverted. Allender and Das [5] related the complexity class SZK (Statistical Zero Knowledge) to MCSP. Carmosino, Impagliazzo, Kabanets and Kolokolova [12] showed that MCSP $\in$ BPP gives efficient PAC-learning algorithms. Impagliazzo, Kabanets and Volkovich [25] showed that the existence of indistinguishable obfuscation implies that SAT reduces to MCSP under a randomized reduction. Hirahara [18] showed that if an approximation version of MCSP is NP-hard, then the average-case and worst-case hardness of NP are equivalent. Arunachalam, Grilo, Gur, Oliveira and Sundaram [7] proved that MCSP $\in$ BQP implies new circuit lower bounds. All these results indicate that the MCSP serves as a "hub" that connects many fundamental problems in different fields. Therefore, a deeper understanding of this problem could lead to significant progress in Theoretical Computer Science.

[1] Roughly, a problem is self-reducible if one can solve the problem with size n by algorithms for smaller size.

[2] It is worth noting that every NP-complete problem has search-to-decision reductions and self-reductions.

2 Main results and technical overview

In this work, we consider three different natural objects that a quantum circuit can compute: Boolean functions, unitaries, and quantum states. We start with giving the informal definitions of the minimum circuit size problem for each of them. (See the full version for formal definitions.)

▶ **Definition 1** (MQCSP, informal). *Given the truth table of a Boolean function f and a size parameter s in unary, decide if there exists a quantum circuit C which has size at most s and uses at most s ancilla qubits such that C computes f with high probability.*

▶ **Definition 2** (UMCSP, informal). *Given the full description of a 2^n-dimensional unitary matrix U and a size parameter s in unary, decide if there exists a quantum circuit C which has size at most s and uses at most s ancilla qubits such that C and U are close*[3]*.*

▶ **Definition 3** (SMCSP, informal). *Let $|\psi\rangle$ be an n-qubit state. Given size parameters s and n in unary and access to arbitrarily many copies of $|\psi\rangle$ (or the classical description of $|\psi\rangle$), decide if there exists a quantum circuit C which has size at most s using at most s ancilla qubits such that $C|0^n\rangle$ and $|\psi\rangle$ are close in terms of fidelity.*

In the rest of this section, we first discuss several challenges and difficulties we encountered in the study of MCSP when moving from the classical setting to the quantum setting. Next, we give an overview of all the results and techniques. In particular, we focus on both interpreting the new connections we establish as well as the technical subtleties when quantizing the previous works in the classical setting. For a quick summary of the results, please take a look at Table 1.

2.1 Challenges and difficulties when moving to the quantum setting

In the following, we summarize several fundamental properties of quantum circuits, unitaries, and quantum states that induce problems and difficulties that would not appear in the classical setting.

Quantum computation is generally random and erroneous. It is natural to consider quantum circuits that approximate (rather than exactly computing) the desired unitary. One immediate consequence is that we have to define the quantum MCSPs as promise problems (with respect to the error)[4], which is more challenging to deal with. Moreover, since unitaries and quantum states are specified by complex numbers, we also need to properly tackle the precision issue. These quantum properties make generalizing classical results to the quantum setting non-trivial. For instance, some classical analyses (see [7] for an example) rely on the fact that the classical circuits are deterministic after the random string is made public, while any intermediate computation of a quantum circuit is inherently not deterministic.

Quantum circuits are reversible. This follows from the fact that every quantum gate is reversible. While this seems to be a restriction for quantum circuits, we observe that this enables search-to-decision reductions for UMCSP and SMCSP. Note that the existence of such reduction is a longstanding open question for classical MCSP. This suggests that quantum MCSPs can provide a new angle to leverage the reversibility of quantum circuits.

[3] We say C and U are close if $|(\langle\psi| \otimes I)U^\dagger C(|\psi\rangle|0\rangle)|$ is large for all $|\psi\rangle$.
[4] The definitions above are not promise problems for simplicity. Check the full version for formal definitions.

The introduction of ancilla qubits. As quantum circuits are reversible, every intermediate computation has to happen on the input qubits. Thus, it is very common to introduce *ancilla qubits* which are extra qubits initialized to all zero and can be regarded as additional registers for intermediate computation. Ancilla qubits introduce complications in quantum MCSPs. First, the quantum circuit complexity of an object could be very different when the allowed number of ancilla qubits is different. Second, the classical simulation time of a quantum circuit scales exponentially in the number of input qubits plus the number of ancilla qubits. Namely, when the number of ancilla qubits is super-linear, classical simulations would require super-polynomial time[5]. An immediate consequence is that, unlike classical MCSP, MQCSP is not trivially in NP when allowing a super-linear number of ancilla qubits. In addition, the output of quantum circuits on ancilla qubits can be arbitrary quantum states in general. This property makes certain reductions for quantum MCSPs fail when considering many ancilla qubits.

Various universal quantum gate sets. The choice of the gate set affects the circuit complexity of the given Boolean functions (and unitaries and states). There are various universal quantum gate sets, and transforming from one to the other results in additional polylogarithmic overhead to the circuit complexity by the Solovay-Kitaev Theorem. We note that when considering certain hardness results, the choice of the gate set might matter. Take the approximate self-reduction for SMCSP (in Theorem 12) as an example, we start from constructing such reductions for a particular gate set. We then generalize the result to an arbitrary gate set via the Solovay-Kitaev Theorem; however, it introduces additional overhead to the approximation ratio. Another example is proving NP-hardness for multi-output MQCSP, where we show that the problem is NP-hard when considering particular gate sets, and it is still open whether the problem is NP-hard for all universal gate sets.

2.2 The Hardness of MQCSP and cryptography

We start with stating the hardness results of MQCSP and its implications in cryptography.

▶ **Theorem 4** (Informal)**.**

1. MQCSP *is in* QCMA $\subseteq$ QMA*.*
2. *If* MQCSP *can be solved in quantum polynomial time, then quantum-secure one-way function (*qOWF*) does not exist.*
3. *If one can solve* MQCSP *efficiently, then all problems in* SZK *have efficient algorithms.*
4. *Suppose that quantum-secure indistinguishability obfuscator (i$\mathcal{O}$) for polynomial-size circuits exists. Then,* MQCSP $\in$ BQP *implies* NP $\subseteq$ coRQP[6]*.*
5. *Multiple-output* MQCSP *(under a gate set with some natural properties) is* NP*-hard under randomized reductions.*

We have discussed why MQCSP is not trivially in NP earlier. So, it is natural to wonder what can be a tighter upper bound for MQCSP. Instead of considering classical verifier, we allow the verifier to check the given witness circuit quantumly and thus are able to prove that MQCSP is in QCMA (which is a quantum analogue of MA allowing efficient quantum verifiers but classical witness).

[5] The running time is measured with respect to the size of the truth table or the size of the unitary/quantum state.

[6] coRQP is a complexity class of quantumly solvable problems with perfect soundness and bounded-error completeness.

For item 2 – 5, we study whether some hard problems reduce to MQCSP. Classically, many results use the fact that an MCSP oracle can break certain *pseudorandom generators* to show reductions from hard problems to MCSP. A distinguisher can break a pseudorandom generator by viewing that the string is a truth table of some Boolean function and using the MCSP oracle to decide if the function has small circuit complexity[7]. We generalize this idea to the quantum setting by observing that if the Boolean function has small classical circuit complexity, then its quantum circuit complexity is also small. It is worth noting that the second result implies efficient algorithms for some lattice problems if MQCSP is in BQP.

For item 5, we generalize the recent breakthrough of Ilango, Loff and Oliveira [23] on the NP-hardness of MCSP. We note that the formal theorem statement depends on the gate set choices of MQCSP. To prove this theorem, we follow the proof ideas in [23] and overcome some additional obstacles that appear in the quantum world. The new obstacle comes from (i) the quantum gate set is different from the one in the classical case; (ii) in the quantum world, we need to deal with error terms. We carefully handle these issues and extend the proof to the quantum setting.

2.3 MQCSP and learning theory

A central learning theory setting is (approximately) reconstructing a circuit for an unknown function given a limited number of samples. Learning Boolean functions in the classical setting was extensively studied (see, for example, a survey by Hellerstein and Servedio [17]); however, relatively few explorations have been made under the quantum setting. There are two natural quantum extensions: (i) learning a quantum circuit and (ii) adding quantumness in the learning algorithm. We study both scenarios and provide generic connections between MQCSP and the two settings

PAC learning for quantum circuits. Probabilistic approximately correct (PAC) learning [46] is a standard theoretical framework in learning theory. There are several variants, but for simplicity, we focus on the query model where a classical learning algorithm can query an unknown n-bit Boolean function f on inputs $x_1, \ldots, x_m \in \{0,1\}^n$ and aim to output a circuit approximating f with high probability. To have efficient PAC learning algorithms for polynomial-size quantum circuits, we show that it is necessary and sufficient to have efficient algorithms for MQCSP or its variants.

▶ **Theorem 5** (Informal). *The existence of an efficient PAC learning algorithm for* BQP/poly *is equivalent to the existence of an efficient randomized algorithm for* MQCSP.

Quantum learning. In the past two decades, there has been increased interest in quantum learning (see a survey by Arunachalam and de Wolf [6]) due to the success of machine learning and quantum computing. While there have been interesting quantum speed-ups for specific learning problems such as principal component analysis [34] and quantum recommendation system [30], it is unclear whether the quantumness can provide a generic speed-up in learning theory. A recent result of Arunachalam, Grilo, Gur, Oliveira and Sundaram [7] suggested that this might be difficult by showing that the existence of efficient quantum learning algorithms for a circuit class would imply a breakthrough circuit lower bound. We further generalize their result by showing the equivalence of efficient quantum PAC learning and the non-trivial upper bound for MQCSP.

[7] If the truth table is truly random, it corresponds to a random function and must have large circuit complexity with high probability.

▶ **Theorem 6** (Informal). *The existence of efficient quantum learning algorithms for PAC learning a circuit class* C *is equivalent to the existence of efficient quantum algorithms for* C-MQCSP[8].

The proof idea is to quantize the "learning from a natural property" paradigm of [12]. Briefly speaking, the converse direction "algorithms for MQCSP imply learning algorithms" follows from the idea that one can use the Boolean function (the object to be learned) to construct a PRG with the property that breaking the PRG implies a reconstructing algorithm for f. Then, since an algorithm for MQCSP can break PRG, we obtain an algorithm for f. Another direction follows from the observation that we can still apply the learning algorithm given the truth table of the function. Specifically, for Theorem 5, it turns out that the converse direction is straightforward because $\mathsf{P/poly} \subset \mathsf{BQP/poly}$ while the forward direction requires the number of ancilla bits to be $O(n)$ due to the overhead from a classical simulation for quantum circuits. For Theorem 6, the difficulty lies in the fact that a quantum circuit is *inherently random* and one cannot arbitrarily compose quantum circuits as their wishes. To circumvent these issues, we invoke the techniques in [7] which built up composable tools for *reconstructing* a circuit from a quantum distinguisher.

2.4 MQCSP and quantum circuit lower bounds

The classical MCSP is tightly connected to circuit lower bounds. We generalize the results of Oliveira and Santhanam [38], Arunachalam, Grilo, Gur, Oliveira and Sundaram [7], and Kabanets and Cai [29] to MQCSP.

▶ **Theorem 7** (Informal). *Suppose that* $\mathsf{MQCSP} \in \mathsf{BQP}$. *Then*
1. $\mathsf{BQE} \not\subset \mathsf{BQC}[n^k]$ *for any constant* $k \in \mathbb{N}$[9]*; and*
2. $\mathsf{BQP}^{\mathsf{QCMA}} \not\subset \mathsf{BQC}[n^k]$ *for any constant* $k \in \mathbb{N}$.

For item 1, we use MQCSP to construct a BQP-natural property against quantum circuit classes. Then, with a quantum-secure pseudorandom generator, we can use a "win-win argument" to show that $\mathsf{BQE} \not\subset \mathsf{BQC}[n^k]$ for any $k > 0$. The proof mainly follows from [7, 38]. However, we extend their proofs to the quantum natural properties against *quantum* circuit classes. One technical contribution is a diagonalization lemma for quantum circuits.

For item 2, we follow the idea in [29] to show that the maximum quantum circuit complexity problem[10] can be solved in exponential time with a QCMA oracle. The main difference from the classical case is that we require a QCMA oracle instead of an NP one, which follows from the fact that we assume MQCSP is in BQP[11]. Then, the statement follows from the standard padding argument.

Another aspect of quantum circuit complexity is *hardness amplification*. Kabanets and Cai [29] showed that MCSP can be used as an amplifier to generate many hard Boolean functions. In this part, we show that with an MQCSP oracle, given one quantum extremely hard Boolean function, there is an efficient quantum algorithm that outputs many quantum-hard functions.

---

[8] C-MQCSP is MQCSP with respect to circuit class C.

[9] $\mathsf{BQC}[n^k]$ is the complexity class for problems that can be solved by $O(n^k)$-size quantum circuits with bounded fan-in, and BQE in the set of problems that can be solved in $2^{O(n)}$ time by quantum computers. Previously, Aaronson [1] showed that $\mathsf{P}^{\mathsf{PP}} \not\subset \mathsf{BQC}[n^k]$ unconditionally. However, the relations between P^{PP}, BQE, and $\mathsf{BQP}^{\mathsf{QCMA}}$ are still unclear. We also expect that one can generalize the result of Impagliazzo, Kabanets and Volkovich [25] to show the circuit lower bound for promise-BQP relative to an MQCSP oracle. We will update the result in the full version.

[10] The problem is, given 1^n, ask for a Boolean function $f : \{0,1\}^n \to \{0,1\}$ that has the maximum complexity.

[11] Along this line, the result still holds if we consider $\mathsf{MCSP} \in \mathsf{BQP}$ and maximum classical circuit complexity.

▶ **Theorem 8** (Hardness amplification by MQCSP, informal). *Assume* MQCSP $\in$ BQP. *There exists a* BQP *algorithm that, given the truth table of a Boolean function with quantum circuit complexity* $2^{\Omega(n)}$*, outputs* $2^{\Omega(n)}$ *Boolean functions with* $m = \Omega(n)$ *variables such that each function has quantum circuit complexity greater than* $2^m/(c+1)m$ *for* c *some constant.*

The proof of Theorem 8 closely follows the proof in [29]. The key ingredient is a quantum Impagliazzo-Wigderson generator, which "quantizes" the construction in [26]. The quantum Impagliazzo-Wigderson generator can transform the given quantum extremely hard function to a quantum pseudorandom generator that fools quantum circuits of size $2^{O(n)}$. Since we assume MQCSP $\in$ BQP, it means that we can construct a small quantum distinguishing circuit to accept the truth tables of hard functions. And we can show that our quantum Impagliazzo-Wigderson generator can fool the distinguishing circuit. Hence, most of the outputs of the quantum pseudorandom generator will have high quantum circuit complexity.

To quantize the Impagliazzo-Wigderson generator, we construct a quantum-secure direct-product generator, and also use the quantum Goldreich-Levin Theorem and quantum-secure Nisan-Wigderson generator developed in [7].

Hardness magnification is an interesting phenomenon in classical circuit complexity defined by [41]. It shows that a weak worst-case lower bound can be "magnified" into a strong worst-case lower bound for another problem. (See a recent talk by Oliveira [39].) In this part, we show that MQCSP also has a quantum hardness magnification.

▶ **Theorem 9** (Hardness magnification for MQCSP, informal). *If a gap version of* MQCSP *does not have nearly-linear size quantum circuit, then* QCMA *cannot be computed by polynomial size quantum circuits.*

We note that this is a nontrivial theorem because even if we assume QCMA $\subseteq$ BQC[poly(n)], we can only show MQCSP $\in$ BQC[poly(2^n)], i.e., MQCSP has a polynomial-size quantum circuit by the fact that MQCSP $\in$ QCMA. But the theorem implies that some gap-version of MQCSP has nearly-linear size circuit!

We prove the above theorem via a quantum antichecker lemma, whose classical version was given by [40, 14]. And we observe that the two key ingredients: a delicate design of a Boolean circuit and a counting argument can be quantized.

2.5 MQCSP and quantum fine-grained complexity

Fine-grained complexity theory aims to study the *exact* lower/upper bounds of some problems. For example, most theorists believe 3-SAT is not in P, but we do not know if it can be solved in $2^{o(n)}$ time. Exponential Time Hypothesis (ETH) is a commonly used conjecture in this area which rules out this possibility (see a survey by Williams [47]). Very recently, [22] showed the fine-grained hardness of MCSP for partial function based on ETH. In the quantum setting, [4, 11] proposed quantum fine-grained reductions and quantum strong exponential time hypothesis (QSETH) to study the quantum hardness of problems in BQP. In this part, we follow the works of [22, 4] and prove the quantum hardness of MQCSP for partial functions based on the quantum ETH conjecture,which conjectures that there does not exist a $2^{o(n)}$-time quantum algorithm for solving 3-SAT[12]. The following theorem showed a conditional lower bound for MQCSP for partial functions, i.e., given the truth table of a partial function $f : \{0,1\}^n \to \{0,1,\star\}$, and $s > 0$, decide if f can be computed by a quantum circuit of size at most s.

[12] Existing quantum SAT solvers are not much faster than Grover's search; they need $2^{\Omega(n)}$-time even for 3-SAT.

▶ **Theorem 10** (Fine-grained hardness of MQCSP*, informal)**.** *Assume Quantum ETH. Then, we have* MQCSP *for partial functions cannot be computed in* $N^{o(\log\log N)}$*-quantum time.*

To prove the above theorem, we basically follow the reduction path in [22], which gave a reduction from a fine-grained problem studied by [35] to MQCSP for partial functions. But we need to bypass two subtleties:

- The proof of [22] relies on the structure of the classical read-once formula, but there is no direct correspondence with quantum;
- [35] only proved the classical hardness of the bipartite permutation independent set problem, but we need quantum hardness result.

For the first issue, we prove an unconditional quantum circuit lower bound for that function in the reduction. More specifically, we first show that if a small quantum circuit can compute the partial function γ in the reduction, then that circuit is a quantum read-once formula (defined by [48]); and vice versa. And then, we apply a "dequantization" result by [16] to show that the quantum read-once formula can be converted to a classical read-once formula with the same size. Then, by the structure of the "dequantized" read-once formula, we finally conclude that deciding MQCSP for γ is equivalent to solving the bipartite permutation independent set problem.

For the second issue, we use the quantum fine-grained reduction framework and give a reduction from 3-SAT to the bipartite permutation independent set problem. Therefore, the quantum hardness of MQCSP for partial function follows from the quantum hardness of deciding 3-SAT conjectured by the quantum ETH.

2.6 Quantum circuit complexity for states and unitaries

In this section, we study UMCSP and SMCSP. For SMCSP in Definition 3, we consider two types of inputs: quantum states and the classical description of the state. We consider the inputs as quantum states since we generally cannot have the classical description of the quantum state in the real world, and many related problems (such as shadow tomography [3], quantum gravity [10], and quantum pseudorandom state [27]) have multiple copies of states as inputs. Although this input format makes SMCSP harder, we are able to show that SMCSP has a QCMA protocol[13]. Furthermore, the search-to-decision reduction and the self-reduction in Theorem 12 hold for both versions of SMCSP. We first show hardness upper bounds for UMCSP and SMCSP.

▶ **Theorem 11** (Informal)**.** (1) UMCSP $\in$ QCMA. (2) SMCSP *can be verified by* QCMA *protocols.*

To prove Theorem 11, we use the *swap test* to test whether the witness circuit C outputs the correct states. This suffices to show that SMCSP has a QCMA protocol. To show that UMCSP is in QCMA, checking if the circuit C and U agree on all inputs by using swap test is infeasible since there are infinitely many quantum states in the 2^n-dimensional Hilbert space. If one only checked all the computational basis states (i.e., $\{|x\rangle : x \in \{0,1\}^n\}$), it is possible that the circuit C and the given unitary U are not close on inputs in the form of superposition states. This can come from the following two sources. (a) C can introduce different phases on different computational basis states; (b) using ancilla qubits to implement U results in entanglement between the output qubits and ancilla qubits, which may fail the swap test.

[13] Note that since SMCSP has quantum inputs, the problem is not in QCMA under the standard definition.

To deal with these difficulties, we introduce an additional step in the test called "coherency test". This step tests the circuit output on all the initial states in the form of $|a\rangle + |b\rangle$, where $|a\rangle, |b\rangle$ are different computational basis states. We can prove that it forces the behavior of C to be coherent on all the computational basis states, and forces the phases to be roughly the same.

Reductions for UMCSP and SMCSP that are unknown to the classical MCSP. In addition to the upper bounds, we also show interesting reductions for UMCSP and SMCSP.

▶ **Theorem 12** (Informal).
- ***Search-to-decision reductions:*** *There exist search-to-decision reductions for* UMCSP *and* SMCSP *when no ancilla qubits are allowed.*
- ***Self-reduction:*** SMCSP *is approximately self-reducible.*
- *A gap version of* MQCSP *reduces to* UMCSP*.*

Classically, it is unknown whether MCSP is self-reducible or has search-to-decision reductions. Ilango [21] proved that some variants of MCSP have search-to-decision reductions. Recently, Ren and Santhanam [43] showed that a relativization barrier applies to the deterministic search-to-decision reduction and self-reduction of MCSP. We prove the existence of search-to-decision reductions by using the property that "*quantum circuits are reversible*". In particular, we guess the i-th gate, uncompute the gate from the state or the unitary, and use the decision oracles to check whether the complexity of the new state or the new unitary reduces. By repeating this process for all gates, we can find the desired circuits. This approach suffices for the case where the quantum circuits use no ancilla qubits. On the other hand, when the quantum circuits use ancilla qubits and are not forced to turn ancilla qubits back to the all-zero state, this approach does not work. Consider UMCSP. The quantum circuit may implement a unitary $U \otimes V$. To find the circuit, the approach above needs to start from $U \otimes V$ and do the uncomputation iteratively. However, V is unknown. SMCSP has the similar issues.

For the self-reducibility of SMCSP, we show that one can approximate the circuit complexity of an n-qubit state by computing the circuit complexities of $(n-1)$-qubit states. Roughly, we find a "win-win decomposition" of an n-qubit state such that its circuit complexity is either close to the circuit complexity of an $(n-1)$-qubit state or can be approximated by two $(n-1)$-qubit states.

Finally, we show a reduction related to MQCSP and UMCSP. The proof is by encoding a Boolean function into a particular unitary and showing that the circuit complexity of that unitary gives both upper and lower bounds for the circuit complexity of the Boolean function.

Implications of Hardness of SMCSP and UMCSP. For UMCSP, one application is related to a question Aaronson asked in [2]: does there exist an efficient quantum process that generates a family of unitaries that are indistinguishable from random unitaries given the full description of the unitary? If there is an efficient algorithm for UMCSP, then there is no efficient quantum process that generates unitaries indistinguishable from random unitaries given the full unitary.

Moreover, several implications of MCSP carry to UMCSP by Theorem 12.

▶ **Corollary 13** (Informal). *Suppose* UMCSP $\in$ BQP*. Then,*
- *there is no efficient quantum process that generates a family of unitaries indistinguishable from random unitaries given the full description of the unitary;*
- *there is no* qOWF*;*

- *if we further assume the existence of quantum-secure iO, then* NP ⊆ coRQP*;*
- *there is a* BQP *algorithm for hardness amplification,*
- BQE ⊄ BQC[n^k] *for all* $k \in \mathbb{N}$.

The above results follow from the fact that the gap version of MQCSP suffices to break certain pseudorandom generators.

For SMCSP, we focus on the version where the inputs are copies of quantum states and present its relationships to quantum cryptography, tomography, and quantum gravity.

▶ **Theorem 14** (Informal)**.**

1. *If* SMCSP *has quantum polynomial-time algorithms, then there are no pseudorandom states, and thus no quantum-secure one-way functions.*
2. *Assuming additional conjectures from physics and complexity theory, the existence of an efficient algorithm for* SMCSP *implies the existence of an efficient algorithm for estimating the wormhole's volume.*
3. *If* SMCSP *can be solved efficiently, then one can solve the succinct state tomography problem*[14] *in quantum polynomial time.*

The first result in Theorem 14 follows from the observation that we can use SMCSP algorithms to distinguish whether the given states have large circuit complexities. This results in algorithms for breaking pseudorandom states, and thus algorithms for inverting quantum-secure one-way functions by [27]. It is worth noting that a recent work by Kretschmer [31] showed some relativized results for the problem of breaking pseudorandom states. Since that problem reduces to SMCSP, his results would provide another angle for understanding the hardness of SMCSP. We show the second result under the model and assumptions considered in [10]. Roughly speaking, the volumes of wormholes correspond to circuit complexities of particular quantum states. Thus efficient algorithms for one implies solving the other one efficiently if the correspondence can be computed efficiently. The third result mainly uses the *search-to-decision reduction* in Theorem 12 to find the circuit that computes the state.

3 Discussion and open questions

We lay out the following three-aspect road map for the quantum MCSP program. For each aspect, we present several results and also propose many open directions to explore. We have also summarized all results in this work in Table 1.

First, we define the Minimum Quantum Circuit Size Problem (MQCSP) and study upper bounds and lower bounds for its complexity. Furthermore, we explore the connections between MQCSP and other areas of quantum computing such as quantum cryptography, quantum learning, quantum circuit lower bounds, and quantum fine-grained complexity.

Then, we further extend MQCSP to study the quantum circuit complexities for quantum objects, including unitaries and states.[15] We want to investigate their hardness and connections to other areas in TCS. In this work, we show upper bounds and lower bounds for their complexities, search-to-decision reductions (for UMCSP and SMCSP), a self-reduction (for SMCSP), and reductions from MQCSP to UMCSP. In addition to connections generalized from classical analogues (such as cryptography, learning, and circuit lower bounds), we also find connections that might be unique in the quantum setting, such as tomography and quantum gravity.

[14] The succinct state tomography problem is that given many copies of a state with the promise that its circuit complexity is at most certain s, the problem is to find a circuit that computes the state.

[15] Aaronson has raised questions about quantum circuit complexity for unitaries or states in [2].

For the last part, we want to turn around and ask what could happen when considering quantum algorithms or quantum reductions for MCSP (and also for MQCSP, UMCSP, and SMCSP)? In the previous two parts, we have already observed that efficient quantum algorithms for these problems result in surprising implications to other fields. One can further consider other influences of quantum algorithms to study quantum and classical MCSPs. For example, can SAT reduce to MCSP under quantum reductions?

Following the three-aspect road map for the quantum MCSP program, there are many open directions to explore. In particular, we are interested to understand the hardness of these problems, the relationships between them, and their connections to other fields in computer science.

3.1 Open problems: the complexity of quantum circuits

We start with open problems related to the hardness and relationships between quantum MCSPs. The most basic questions are to understand the complexity of different quantum MCSPs. As we have already seen, it is unclear if quantum MCSPs are in NP. Besides, we do not know if NP- or QCMA-hard problems reduce to them.

▶ **Open Problem 1.** *Are* UMCSP*,* MQCSP*, and* SMCSP *in* NP*? Are these problems* NP*-hard,* QCMA*-hard, or* C*-hard for some complexity class* C *that is between* QCMA *and* SZK*?*

We note that the case that makes these problems not known to be in NP is when there are more than linearly many ancilla qubits. Therefore, if one can show that adding superpolynomially many ancilla qubits does not lead to significant improvement on quantum circuit complexity, then we are likely to put these problems in NP directly. Along this line, we pose the following open question:

▶ **Open Problem 2.** *For every* $n, s, t \in \mathbb{N}$ *with* $t \leq s \leq 2^{O(n)}$*, can we prove that* $\mathsf{BQC}(s,t) \subset \mathsf{BQC}(\mathsf{poly}(s,t), O(n))$*?*

For the hardness of UMCSP and SMCSP, One potential approach for proving NP-hardness of UMCSP is as follows: Prove the NP-hardness of the gap version of certain variants of MQCSP (such as sparse MQCSP or multiMQCSP), and then reduce it to UMCSP via the last reduction in Theorem 12. The hardness of SMCSP seems to be slightly more mysterious than UMCSP. One reason for this is that we do not know any relationship between SMCSP and other quantum MCSPs, and thus the approach of reducing particular variants of quantum MCSP to SMCSP does not directly work. This leads to another important open question:

▶ **Open Problem 3.** *What are the relationships between* UMCSP*,* MQCSP*, and* SMCSP*?*

To answer whether quantum MCSPs are NP-complete, we can also study these problems from another angle, that is, check if quantum MCSPs have particular reductions that all NP-complete problems have. In the previous section, we observed that quantum circuits have some properties leading to search-to-decision reductions for UMCSP and SMCSP without ancilla qubits and an approximate self-reduction for SMCSP. Therefore, we ask whether we can have search-to-decision reductions and self-reductions for these quantum MCSPs.

▶ **Open Problem 4.** *Are there search-to-decision reductions and self-reductions for quantum* MCSP*s?*

It is worth noting that our search-to-decision reductions fail when ancilla qubits are allowed. This mainly follows from the fact that the circuit of the solution can be an non-identity operator on the ancilla qubits in general. This could possibly be addressed by iterating all

possible unitaries or states on an ϵ-net when the number of ancilla qubits are not large (e.g., at most $\log \log n$). However, we need new ideas when considering more ancilla qubits.

Moreover, it would be interesting to investigate the applications of these reductions. For instance, we have seen that the search-to-decision reductions give algorithms with UMCSP or SMCSP oracle additional power to obtain the circuits. This power may lead to interesting applications.

▶ **Open Problem 5.** *Is there any application of search-to-decision reductions or self-reductions for quantum* MCSP*s?*

The hardness of average-case quantum MCSPs (which inputs are given randomly) is another interesting topic to explore. Hirahara [18] showed that there is a worst-case to average-case reduction for the (gap version of) classical MCSP. We wonder if we can prove that quantum MCSPs have worst-case to average-case reductions.

▶ **Open Problem 6.** *Are there worst-case to average-case reductions for quantum* MCSP*s?*

Note that there is negative evidence [9] showing that such classical reductions might not exist for NP-complete problems[16]. The existence of such reduction could result in important applications in cryptography, which we will discuss later.

Finally, we can also try to prove the hardness of quantum MCSPs under stronger assumptions or more powerful reductions.

▶ **Open Problem 7.** *Assuming* QETH *or* QSETH*, is* MQCSP*,* UMCSP*, or* SMCSP *quantumly hard?*

▶ **Open Problem 8.** *Does quantum reduction provide more power to show the hardness of* MCSP*? Specifically, is* $\mathsf{NP} \subseteq \mathsf{BQP}^{\mathsf{MCSP}}$ *or* $\mathsf{NP} \subseteq \mathsf{BQP}^{\mathsf{MQCSP}}$*?*

3.2 Open problems: potential connections to other areas

In this work, in addition to generalizing several known connections for MCSP to quantum MCSPs, we have also discovered several connections which could be unique for quantum MCSPs. There are still many classically existing or unknown connections that we can explore. One fascinating question is whether we can base the security of one-way functions on any of these problems.

▶ **Open Problem 9.** *Can we base the security of cryptographic primitives on* MQCSP*,* UMCSP*,* SMCSP*, or some variants of these problems?*

Note that since quantum MCSPs considered in this work are all worst-case problems, to answer Problem 9, we probably need worst-case to average-case reductions discussed in Problem 6. Moreover, Liu and Pass [32] recently showed that the existence of classical one-way function is equivalent to the average-case hardness of a type of Kolmogorov complexity on uniform distribution. However, the average-case hardness of MCSP on uniform distribution is not known to imply one-wayness even classically, and the quantum version faces a similar obstacle. Very recently, Ilango, Ren, and Santhanam [24] showed that the average-case hardness of Gap-MCSP on a locally samplable distribution is equivalent to the existence of one-way function. Liu and Pass [33] further generalized this result to show equivalence

[16] However, there is no evidence for the existence of quantum worst-case to average-case reductions for NP-complete since the analysis in [9] fails in the quantum setting. See [15] for related discussion.

between the existence of one-way functions and the existence of sparse languages that are hard-on-average (including Kolmogorov complexity, k-SAT, and t-Clique). It is natural to ask whether their results can be generalized to quantum MCSPs. In addition to one-way functions, We are interested in connections between quantum MCSPs and "quantum-only" primitives, e.g., quantum $i\mathcal{O}$, copy protection, quantum process learning, etc.

Along this line, as many quantum problems have quantum inputs, it is natural to consider quantum MCSPs with quantum inputs. We have shown how SMCSP connects to problems in quantum cryptography, quantum gravity, and tomography given quantum states as inputs. This fact gives the possibility that MQCSP, UMCSP, and SMCSP with "succinct" quantum or classical inputs may have surprising connections to other problems in quantum computing. For instance, one can consider inputs which are quantum circuits that encode some objects (e.g., unitaries). Then, the problem is to find another significantly smaller circuit. In [13], Chakrabarti, Chou, Chung and Wu have studied this problem and show applications to quantum supremacy.

Table 1 Summary of our results. A result with no star symbol is a direct extension from its classical analog. A result with one star symbol * requires additional techniques. A result with two star symbols ** is unique in the quantum setting.

	Results	Informal Theorem Index
MQCSP (Def. 1)	$\mathsf{MQCSP} \in \mathsf{QCMA}$	Theorem 4
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow$ No qOWF	Theorem 4
	$\mathsf{SZK} \leq \mathsf{MQCSP}$	Theorem 4
	multiMQCSP is NP-hard under a natural gate set	Theorem 4
	$i\mathcal{O} + \mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow \mathsf{NP} \subseteq \mathsf{coRQP}$	Theorem 4
	PAC learning for $\mathsf{BQP/poly} \Leftrightarrow \mathsf{MQCSP} \in \mathsf{BPP}$	* Theorem 5
	BQP learning $\Leftrightarrow \mathsf{MQCSP} \in \mathsf{BQP}$	* Theorem 6
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow \mathsf{BQE} \not\subset \mathsf{BQC}[n^k],\ \forall k \in \mathbb{N}_+$	* Theorem 7
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow \mathsf{BQP}^{\mathsf{QCMA}} \not\subset \mathsf{BQC}[n^k],\ \forall k \in \mathbb{N}_+$	Theorem 7
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow$ Hardness amplification	* Theorem 8
	Hardness magnification for MQCSP	Theorem 9
	$\mathsf{QETH} \Rightarrow$ quantum hardness of $\mathsf{MQCSP}^\star$	* Theorem 10
UMCSP (Def. 2)	$\mathsf{UMCSP} \in \mathsf{QCMA}$	** Theorem 11
	Search-to-decision reduction for UMCSP	** Theorem 12
	$\mathsf{gap\text{-}MQCSP} \leq \mathsf{UMCSP}$	** Theorem 12
	$\mathsf{UMCSP} \in \mathsf{BQP}$ $\Rightarrow$ No pseudorandom unitaries and no qOWF	Corollary 13
	$i\mathcal{O} + \mathsf{UMCSP} \in \mathsf{BQP} \Rightarrow \mathsf{NP} \subseteq \mathsf{coRQP}$	Corollary 13
	$\mathsf{UMCSP} \in \mathsf{BQP} \Rightarrow$ Hardness amplification in BQP	Corollary 13
	$\mathsf{UMCSP} \in \mathsf{BQP} \Rightarrow \mathsf{BQE} \not\subset \mathsf{BQP}[n^k],\ \forall k \in \mathbb{N}$	Corollary 13
SMCSP (Def. 3)	SMCSP can be verified via QCMA	Theorem 11
	Search-to-decision reduction for SMCSP	** Theorem 12
	Self-reduction for SMCSP	** Theorem 12
	$\mathsf{SMCSP} \in \mathsf{BQP}$ $\Rightarrow$ No pseudorandom states and no qOWF	** Theorem 14
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	** Theorem 14
	Succinct state tomography $\leq$ SMCSP	** Theorem 14

References

1. Scott Aaronson. Oracles are subtle but not malicious. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 15–pp. IEEE, 2006.
2. Scott Aaronson. The complexity of quantum states and transformations: from quantum money to black holes. *arXiv preprint*, 2016. arXiv:1607.05256.
3. Scott Aaronson. Shadow tomography of quantum states. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, pages 325–338, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3188745.3188802.
4. Scott Aaronson, Nai-Hui Chia, Han-Hsuan Lin, Chunhao Wang, and Ruizhe Zhang. On the quantum complexity of closest pair and related problems. In *35th Computational Complexity Conference (CCC 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.
5. Eric Allender and Bireswar Das. Zero knowledge and circuit minimization. In Erzsébet Csuhaj-Varjú, Martin Dietzfelbinger, and Zoltán Ésik, editors, *Mathematical Foundations of Computer Science 2014*, pages 25–32, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.
6. Srinivasan Arunachalam and Ronald de Wolf. Guest column: A survey of quantum learning theory. *ACM SIGACT News*, 48(2):41–67, 2017.
7. Srinivasan Arunachalam, Alex B Grilo, Tom Gur, Igor C Oliveira, and Aarthi Sundaram. Quantum learning algorithms imply circuit lower bounds. *arXiv preprint*, 2020. arXiv:2012.01920.
8. Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.
9. Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for np problems. *SIAM Journal on Computing*, 36(4):1119–1159, 2006.
10. Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract). In Thomas Vidick, editor, *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, volume 151 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 63:1–63:2, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITCS.2020.63.
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.
12. Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. Learning algorithms from natural proofs. In *Proceedings of the 31st Conference on Computational Complexity*, CCC '16, Dagstuhl, DEU, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
13. Shouvanik Chakrabarti, Chi-Ning Chou, Kai-Min Chung, and Xiaodi Wu. Scalable verification of quantum supremacy based on circuit obfuscation. *Manuscript*, 2021.
14. Lijie Chen, Shuichi Hirahara, Igor C Oliveira, Ján Pich, Ninad Rajgopal, and Rahul Santhanam. Beyond natural proofs: Hardness magnification and locality. *Leibniz International Proceedings in Informatics*, 151, 2020.
15. Nai-Hui Chia, Sean Hallgren, and Fang Song. On Basing One-way Permutations on NP-hard Problems under Quantum Reductions. *Quantum*, 4:312, August 2020.
16. Alessandro Cosentino, Robin Kothari, and Adam Paetznick. Dequantizing read-once quantum formulas. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2013.
17. Lisa Hellerstein and Rocco A Servedio. On PAC learning algorithms for rich Boolean function classes. *Theoretical Computer Science*, 384(1):66–76, 2007.

18 Shuichi Hirahara. Non-black-box worst-case to average-case reductions within np. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 247–258. IEEE, 2018.

19 Shuichi Hirahara, Igor C Oliveira, and Rahul Santhanam. Np-hardness of minimum circuit size problem for or-and-mod circuits. In *33rd Computational Complexity Conference (CCC 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

20 R. Ilango. AC0[p] lower bounds and np-hardness for variants of mcsp. *Electron. Colloquium Comput. Complex.*, 26:21, 2019.

21 Rahul Ilango. Connecting Perebor Conjectures: Towards a Search to Decision Reduction for Minimizing Formulas. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:35. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2020.

22 Rahul Ilango. Constant depth formula and partial function versions of mcsp are hard. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 424–433. IEEE, 2020.

23 Rahul Ilango, Bruno Loff, and Igor C. Oliveira. Np-hardness of circuit minimization for multi-output functions. In *35th Computational Complexity Conference (CCC 2020)*, CCC '20, Dagstuhl, DEU, 2020. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. `doi:10.4230/LIPIcs.CCC.2020.22`.

24 Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Hardness on any samplable distribution suffices: New characterizations of one-way functions by meta-complexity. *Electron. Colloquium Comput. Complex.*, 28:82, 2021.

25 Russell Impagliazzo, Valentine Kabanets, and Ilya Volkovich. The power of natural properties as oracles. In *33rd Computational Complexity Conference (CCC 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

26 Russell Impagliazzo and Avi Wigderson. P= BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 220–229, 1997.

27 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 126–152, Cham, 2018. Springer International Publishing.

28 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE. *arXiv preprint*, 2020. `arXiv:2001.04383`.

29 Valentine Kabanets and Jin-Yi Cai. Circuit minimization problem. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 73–79, 2000.

30 Iordanis Kerenidis and Anupam Prakash. Quantum recommendation systems. In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, 2017.

31 William Kretschmer. Quantum Pseudorandomness and Classical Complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:20, 2021.

32 Yanyi Liu and R. Pass. On one-way functions and kolmogorov complexity. *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1243–1254, 2020.

33 Yanyi Liu and Rafael Pass. A note on one-way functions and sparse languages. *Electron. Colloquium Comput. Complex.*, 28:92, 2021.

34 Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature Physics*, 10(9):631–633, 2014.

35 Daniel Lokshtanov, Dániel Marx, and Saket Saurabh. Slightly superexponential parameterized problems. In *Proceedings of the twenty-second annual ACM-SIAM symposium on Discrete Algorithms*, pages 760–776. SIAM, 2011.

36 William J Masek. Some np-complete set covering problems. *Unpublished Manuscript*, 1979.

37 Cody D Murray and R Ryan Williams. On the (non) np-hardness of computing circuit complexity. *Theory of Computing*, 13(1):1–22, 2017.

38 Igor C Oliveira and Rahul Santhanam. Conspiracies between learning algorithms, circuit lower bounds and pseudorandomness. *arXiv preprint*, 2016. arXiv:1611.01190.

39 Igor Carboni Oliveira. Advances in hardness magnification. https://www.dcs.warwick.ac.uk/~igorcarb/documents/papers/magnification-note.pdf, 2019.

40 Igor Carboni Oliveira, Ján Pich, and Rahul Santhanam. Hardness magnification near state-of-the-art lower bounds. In *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

41 Igor Carboni Oliveira and Rahul Santhanam. Hardness magnification for natural problems. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 65–76. IEEE, 2018.

42 Alexander A Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 1(55):24–35, 1997.

43 Hanlin Ren and Rahul Santhanam. A relativization perspective on meta-complexity. *Electron. Colloquium Comput. Complex.*, 28:89, 2021.

44 Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

45 Boris A Trakhtenbrot. A survey of russian approaches to perebor (brute-force searches) algorithms. *Annals of the History of Computing*, 6(4):384–400, 1984.

46 Leslie G Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134–1142, 1984.

47 Virginia Vassilevska Williams. On some fine-grained questions in algorithms and complexity. In *Proceedings of the ICM*, volume 3, pages 3431–3472. World Scientific, 2018.

48 A Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 352–361. IEEE, 1993.