

# Quantum Complexity: Theory and Application

Edited by

Bill Fefferman<sup>1</sup>, Sevag Gharibian<sup>2</sup>, Norbert Schuch<sup>3</sup>, and  
Barbara Terhal<sup>4</sup>

1 University of Chicago, US, bfefferman@gmail.com

2 Universität Paderborn, DE, sevag.gharibian@gmail.com

3 Universität Wien, AT, norbert.schuch@gmail.com

4 TU Delft, NL, b.m.terhal@tudelft.nl

---

## Abstract

This report documents the program and outcomes of Dagstuhl Seminar 21261 “Quantum Complexity: Theory and Application”. The seminar ran from June 27 to July 2, 2021, and was held in a hybrid format (due to COVID travel restrictions). Of the 55 total participants from 14 countries, 17 participants were on-site, and 38 were remote. Recent advances in both theoretic and experimental aspects of quantum complexity theory were presented and discussed, ranging from new theoretical developments via a “Quantum Strong Exponential Time Hypothesis”, to more experimentally oriented talks involving benchmarking of random circuits in quantum supremacy experiments. In addition, an open problem session and a discussion session regarding the current state of the field were included.

**Seminar** June 27 – July 2, 2021 – <http://www.dagstuhl.de/21261>

**2012 ACM Subject Classification** Theory of computation → Quantum complexity theory

**Keywords and phrases** complexity theory, many-body systems, proof and verification systems, quantum computation, quantum supremacy

**Digital Object Identifier** 10.4230/DagRep.11.5.76

## 1 Executive Summary

*Bill Fefferman (University of Chicago, US)*

*Sevag Gharibian (Universität Paderborn, DE)*

*Norbert Schuch (Universität Wien, AT)*

*Barbara Terhal (TU Delft, NL)*

**License** © Creative Commons BY 4.0 International license

© Bill Fefferman, Sevag Gharibian, Norbert Schuch, and Barbara Terhal

**Background and motivation.** Since the seminal discovery of an efficient quantum integer factorization algorithm by Peter Shor in 1994, the field of Quantum Computation has blossomed into a large-scale international effort to build, test, and study the possibilities that information processing using quantum particles may provide. A central role in these developments has been played by Quantum Complexity Theory, a traditionally theoretical realm of research focusing on such questions as: Which physical properties of Nature can be efficiently computed? Can the behavior of an untrusted or noisy quantum computer be verified? What might constitute convincing evidence of “quantum supremacy” over classical computers?



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 4.0 International license

Quantum Complexity: Theory and Application, *Dagstuhl Reports*, Vol. 11, Issue 05, pp. 76–88

Editors: Bill Fefferman, Sevag Gharibian, Norbert Schuch, and Barbara Terhal



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

With the first generation of completed “Noisy Intermediate Scale Quantum (NISQ)” experiments already staking quantum supremacy claims, however, the answers to such “traditionally theoretical” questions have taken on an urgent and practical relevance. For example, a complexity theoretic understanding of which realistic physical problems are “just hard enough” for classical computers and “easy enough” for quantum computers is the natural starting point for “quantum supremacy” testbeds. With functioning experimental devices in place, one must next convincingly confirm the device is performing as designed, particularly in the presence of noise. Finally, if the aim of such experiments is to cast doubt on the Extended Church-Turing Thesis, then a strong standard of evidence is required; such a standard must be rigorously stated and developed.

**Seminar Topics.** This seminar covered a range of topics under the broad umbrella of Quantum Complexity Theory, ranging from highly theoretical to experimentally driven. We briefly overview some of these here; further examples and details are in the included talk abstracts.

*Theoretical directions.* The field of Quantum Complexity Theory is concerned, broadly speaking, with a rigorous mathematical study of the resources required to perform certain computational tasks. To first order, this involves dividing the “computational world” into two buckets: Easy versus hard problems. However, in reality, the complexity landscape is much finer than this. For example, one might ask – given that problem  $X$  has a known efficient quantum algorithm, does there nevertheless exist a *faster* quantum algorithm for  $X$ ? This typically falls under the classical area of “fine-grained complexity”, which has only recently begun to emerge as having a quantum analogue. Conversely, one may ask – is problem  $X$  hard only when one wishes to have a high precision answer, becoming easy when a larger margin of error is allowed? Classically, this falls under the umbrella of “hardness of approximation”, and which has seen intense study in the guise of the “quantum PCP conjecture”. Finally, given that quantum computers are believed more powerful than classical ones, a natural question is: *Do there exist computational problems whose difficulty lies strictly between classical and quantum?* Here, a natural object of study has been so-called “stoquastic” quantum systems, whose time evolution can often be simulated in practice via randomized (i.e. Monte Carlo) techniques, but which nevertheless appear difficult to classically simulate in the *worst case* in a rigorous fashion. Recent advances and the state of the art in all of these topics, as well as a number of others, were discussed at the seminar.

*Experimentally motivated directions.* The recent explosion of the so-called Noisy Intermediate-Scale Quantum (NISQ) computation era has brought many new questions to the forefront of Quantum Complexity Theory. For example, to date, two of the leading frameworks for experimental demonstration of “quantum supremacy” have been *random circuit sampling* and *Boson sampling*. On the one hand, much progress has been made closing the remaining gaps in the theoretical hardness proofs for these tasks on classical computers. On the other hand, for experiments that *have* been conducted, important practical topics such as how to benchmark such experimental random circuit setups have very recently been studied. Moreover, beyond the quest for quantum supremacy lies the next question: *What practical applications might NISQ devices already prove useful for?* These and related topics were presented and discussed at the seminar.

**Participants and program overview.** Due to the on-going COVID situation, the seminar was held in hybrid format. This meant that of the 55 total participants joining from 14 countries around the world (from North America to Europe to Asia), 17 were on-site, and

38 were remote. To allow all audience members to participate, a few measures were taken, which arguably worked quite well given the circumstances:

- During each of the seminar’s on-site sessions, a Zoom session was projected onto a whiteboard, to which all remote participants were invited. The Zoom participants could see and hear on-site whiteboard and slide presentations, as well as interrupt to ask questions (via the room’s loudspeaker system). This made for a reasonably efficient setup in which both on-site and hybrid participants could discuss in real-time. A Slack channel was also set up to ease communication, and by popular request, after talks a virtual Zoom chat room was set up so that the remote participants could also chat amongst themselves.
- To accommodate both types of audience members, a mix of on-site and remote talks were scheduled. On-site talks were typically held in the morning (CEST), allowing remote audience members in Europe Asia to attend. These were held at “standard” times, starting at 9:00 CEST. Remote talks were largely scheduled in the late afternoon and evening (17:00 and 20:00 CEST), this time accessible to North American and European participants.
- Seminar participants Marcel Hinsche (on-site) and James Watson (off-site) graciously offered to act as “technical help volunteers” for local and remote participants, ensuring the hybrid setup ran smoothly for both local and remote attendees.

Regarding the remaining program structure, a strong emphasis was placed on plentiful open time for ad-hoc discussion – typically 14:00 to 17:00 was left open expressly for this purpose. A social outing (hike) was organized by participant Dominik Hangleiter on Wednesday afternoon, and a traditional social night in the music room took place on Wednesday evening.

**Acknowledgements.** The seminar’s participants and organizing committee wholeheartedly thank the Schloss Dagstuhl administrative and technical staff, who before, during, and after the seminar were incredibly supportive, professional, and patient with us quantum computer scientists. Many of the seminars participants, both online and off-line, commented very positively of the experience, citing it as a very welcome break to the stress of the on-going COVID pandemic.

## 2 Table of Contents

### Executive Summary

*Bill Fefferman, Sevag Gharibian, Norbert Schuch, and Barbara Terhal* . . . . . 76

### Overview of Talks

An area law for 2D frustration-free spin systems

*Anurag Anshu* . . . . . 80

Quantum fine-grained complexity

*Harry Buhrman* . . . . . 80

Gaussian Boson sampling and its complexity

*Abhinav Deshpande* . . . . . 81

Linear growth of quantum circuit complexity

*Jens Eisert* . . . . . 81

Quantum Hardness of Approximation

*Lior Eldar* . . . . . 82

The power of random quantum circuits

*Bill Fefferman* . . . . . 82

(Sub)Exponential advantage of adiabatic quantum computation with no sign problem

*András Gilyén* . . . . . 83

Verifying BQP Computations on Noisy Devices with Minimal Overhead

*Elham Kashefi* . . . . . 84

Compact Fermion to Qubit Mappings

*Joel David Klassen* . . . . . 84

Provably efficient machine learning for quantum many-body problems

*Richard Küng* . . . . . 85

On QMA Queries with Tree-like Dependencies

*Dorian Rudolph* . . . . . 85

Classical proofs of quantum knowledge

*Thomas Vidick* . . . . . 86

**Participants** . . . . . 87

**Remote Participants** . . . . . 87

### 3 Overview of Talks

#### 3.1 An area law for 2D frustration-free spin systems

Anurag Anshu (*University of California – Berkeley, US*)

**License** © Creative Commons BY 4.0 International license  
© Anurag Anshu

**Joint work of** Anurag Anshu, Itai Arad, David Gosset

**Main reference** Anurag Anshu, Itai Arad, David Gosset: “An area law for 2D frustration-free spin systems”, CoRR, Vol. abs/2103.02492, 2021.

**URL** <https://arxiv.org/abs/2103.02492>

We prove that the entanglement entropy of the ground state of a locally gapped frustration-free 2D lattice spin system satisfies an area law with respect to a vertical bipartition of the lattice into left and right regions. We first establish that the ground state projector of any locally gapped frustration-free 1D spin system can be approximated to within error  $\epsilon$  by a degree  $O(\sqrt{\log 1/\epsilon})$  multivariate polynomial in the interaction terms of the Hamiltonian. This generalizes the optimal bound on the approximate degree of the boolean AND function, which corresponds to the special case of commuting Hamiltonian terms. For 2D spin systems we then construct an approximate ground state projector (AGSP) that employs the optimal 1D approximation in the vicinity of the boundary of the bipartition of interest. This AGSP has sufficiently low entanglement and error to establish the area law using a known technique.

#### 3.2 Quantum fine-grained complexity

Harry Buhrman (*CWI – Amsterdam, NL*)

**License** © Creative Commons BY 4.0 International license  
© Harry Buhrman

**Joint work of** Harry Buhrman, Bruno Loff, Florian Speelman, and Subhasree Patro

**Main reference** Harry Buhrman, Bruno Loff, Subhasree Patro, Florian Speelman: “Limits of quantum speed-ups for computational geometry and other problems: Fine-grained complexity via quantum walks”, CoRR, Vol. abs/2106.02005, 2021.

**URL** <https://arxiv.org/abs/2106.02005>

One of the major challenges in computer science is to establish lower bounds on the resources, usually time, that are needed to solve computational problems. This holds in particular for computational problems that appear in practice. One way towards dealing with this situation is the study of fine-grained complexity where we use special reductions to prove time lower bounds for many diverse problems based on the conjectured hardness of some key problems. For example, computing the edit distance between two strings, a problem that has a practical interest when determining the genetic distance between species based on their DNA, has an algorithm that takes  $O(n^2)$  time. Using a fine-grained reduction it can be shown that faster algorithms for edit distance also imply a faster algorithm for the Boolean Satisfiability (SAT) problem (that is believed to not exist). This is evidence that the current edit distance algorithms are optimal. Another problem, besides SAT, that is used as a basis for these reductions is the 3SUM problem. The situation in the quantum regime is no better; almost all known lower bounds for quantum algorithms are defined in terms of query complexity, which doesn't help much for problems for which the best-known algorithms take super-linear time. Therefore, employing fine-grained reductions in the quantum setting seems a natural way forward. However, translating the classical fine-grained reductions directly into the quantum regime is not always possible for various reasons. In this talk, I will present

some recent results in which we circumvent these challenges and prove quantum time lower bounds for some problems in BQP conditioned on the conjectured quantum hardness of SAT (and its variants) and the 3SUM problem. This is based on joint work with Bruno Loff, Florian Speelman, and Subhasree Patro.

### 3.3 Gaussian Boson sampling and its complexity

*Abhinav Deshpande (University of Maryland – College Park, US)*

**License** © Creative Commons BY 4.0 International license  
 © Abhinav Deshpande  
**Joint work of** Abhinav Deshpande, Arthur Mehta, Trevor Vincent, Nicolas Quesada, Marcel Hinsche, Marios Ioannou, Lars Madsen, Jonathan Lavoie, Haoyu Qi, Jens Eisert, Dominik Hangleiter, Bill Fefferman, Ish Dhand  
**Main reference** Abhinav Deshpande, Arthur Mehta, Trevor Vincent, Nicolas Quesada, Marcel Hinsche, Marios Ioannou, Lars Madsen, Jonathan Lavoie, Haoyu Qi, Jens Eisert, Dominik Hangleiter, Bill Fefferman, Ish Dhand: “Quantum Computational Supremacy via High-Dimensional Gaussian Boson Sampling”, CoRR, Vol. abs/2102.12474, 2021.  
**URL** <https://arxiv.org/abs/2102.12474>

Recent demonstrations of a quantum speedup with Gaussian boson sampling have been challenged by new algorithms claiming the absence of this speedup. In this talk, I will discuss the computational hardness of Gaussian boson sampling in an idealized setting of parameters. I will also discuss how, outside of the idealized setting, certain algorithms can simulate some instances of Gaussian boson sampling.

### 3.4 Linear growth of quantum circuit complexity

*Jens Eisert (FU Berlin, DE)*

**License** © Creative Commons BY 4.0 International license  
 © Jens Eisert  
**Joint work of** Jens Eisert, Jonas Haferkamp, Naga B. T. Kothakonda, Nicole Yunger Halpern, and Philippe Faist  
**Main reference** Jonas Haferkamp, Philippe Faist, Naga B. T. Kothakonda, Jens Eisert, Nicole Yunger Halpern: “Linear growth of quantum circuit complexity”, CoRR, Vol. abs/2106.05305, 2021.  
**URL** <https://arxiv.org/abs/2106.05305>

Quantifying quantum states’ complexity is a key problem in various subfields of science, from quantum computing to black-hole physics. We prove a prominent conjecture by Brown and Susskind about how random quantum circuits’ complexity increases. Consider constructing a unitary from Haar-random two-qubit quantum gates. Implementing the unitary exactly requires a circuit of some minimal number of gates - the unitary’s exact circuit complexity. We prove that this complexity grows linearly in the number of random gates, with unit probability, until saturating after exponentially many random gates. Our proof is surprisingly short, given the established difficulty of lower-bounding the exact circuit complexity. Our strategy combines differential topology and elementary algebraic geometry with an inductive construction of Clifford circuits.

Joint work with Jonas Haferkamp, Philippe Faist, Naga B. T. Kothakonda, and Nicole Yunger Halpern

### 3.5 Quantum Hardness of Approximation

*Lior Eldar (IL)*

**License**  Creative Commons BY 4.0 International license  
© Lior Eldar

**Main reference** Lior Eldar: “Robust Quantum Entanglement at (Nearly) Room Temperature”, in Proc. of the 12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference, LIPIcs, Vol. 185, pp. 49:1–49:20, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

**URL** <http://dx.doi.org/10.4230/LIPIcs.ITCS.2021.49>

Quantum entanglement is notoriously hard to maintain and its fragility is arguably the main obstacle preventing us from building a quantum computer. In terms of local Hamiltonians this means that while we know that ground-state of “feasible” quantum systems are highly entangled, we physically can only access the Gibbs states of these quantum systems, and these alas cannot sustain global-scale entanglement.

In this talk we consider the problem of designing systems that exhibit robust quantum entanglement: formally we would like to design a local Hamiltonian for which not only the ground-state is highly entangled but one can also demonstrate that its Gibbs state at non-zero temperature (independent of system size) can only be approximated by deep quantum circuits. Such systems are not known to date.

In [Eldar ’21] we show that one can approach such a “holy grail” system and construct a Hamiltonian on  $n$  qubits with log-local terms for which the Gibbs state even at nearly-constant temperatures, decaying only at a rate of  $1/\log\log(n)$  cannot be approximated by shallow quantum circuits – i.e. of depth less than  $\log(n)$ . The construction involves using state of the art quantum locally testable codes (qLTC), appended with shallow classical decoders for expander codes, together with an analysis of the evolution of thermal errors under qLTCs. The analysis uses the Metropolis Hastings algorithm to show that the errors in the thermal state evolving under a qLTC Hamiltonian tend to form only very sparse errors that are locally correctable – which may be useful elsewhere.

Many open questions remain – among which are improving (reducing) the locality of the construction, and increasing the temperature for which circuit lower bounds can be demonstrated to a constant.

### 3.6 The power of random quantum circuits

*Bill Fefferman (University of Chicago, US)*

**License**  Creative Commons BY 4.0 International license  
© Bill Fefferman

**Joint work of** Adam Bouland, Bill Fefferman, Zeph Landau, Yunchao Liu, Umesh Vazirani

**Main reference** Adam Bouland, Bill Fefferman, Zeph Landau, Yunchao Liu: “Noise and the frontier of quantum supremacy”, CoRR, Vol. abs/2102.01738, 2021.

**URL** <https://arxiv.org/abs/2102.01738>

**Main reference** Adam Bouland, Bill Fefferman, Chinmay Nirkhe, Umesh V. Vazirani: “Quantum Supremacy” and the Complexity of Random Circuit Sampling”, in Proc. of the 10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA, LIPIcs, Vol. 124, pp. 15:1–15:2, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019.

**URL** <http://dx.doi.org/10.4230/LIPIcs.ITCS.2019.15>

In this talk we will discuss recent results on the power of random quantum circuits, inspired by the “quantum supremacy” experiments of Google and USTC. We will discuss two new results: first we consider the “low noise” scenario in which the goal is to prove the hardness of approximate sampling from the output distribution of a random quantum circuit. The

main obstacle faced in prior work on this subject is that the average-case hardness results for computing output probabilities of random circuits are not robust enough to imprecision to connect with the Stockmeyer argument for hardness of sampling. In this work we exponentially improve this robustness to imprecision. In the case of BosonSampling, we bring the proven hardness to within a constant factor in the exponent of the robustness required for hardness of sampling.

Second, we consider the realistic “high noise” scenario. We show that it remains hard to compute the output probabilities of noisy random quantum circuits without error correction, providing the noise rate of the device is below the error detection threshold. This hardness persists despite the fact that these probabilities are exponentially close to uniform. Consequently, the small deviations away from uniformity are hard to compute, formalizing an important intuition behind Google’s supremacy claim.

Interestingly, we then argue that these two results are connected, in that any further progress on proving hardness in the “low noise scenario” would require techniques which \*do not\* work to improve the hardness results in the “high noise scenario”.

### 3.7 (Sub)Exponential advantage of adiabatic quantum computation with no sign problem

*András Gilyén (Caltech – Pasadena, US)*

**License** © Creative Commons BY 4.0 International license  
© András Gilyén

**Joint work of** Hastings, Matthew B.; Gilyén, András; Vazirani, Umesh

**Main reference** András Gilyén, Matthew B. Hastings, Umesh Vazirani, “(Sub)Exponential advantage of adiabatic quantum computation with no sign problem”, Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, June 2021, Pages 1357–1369

**URL** <https://doi.org/10.1145/3406325.3451060>

**Main reference** András Gilyén, Matthew B. Hastings, Umesh V. Vazirani: “(Sub)Exponential advantage of adiabatic Quantum computation with no sign problem”, in Proc. of the STOC ’21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21–25, 2021, pp. 1357–1369, ACM, 2021.

**URL** <http://dx.doi.org/10.1145/3406325.3451060>

We demonstrate the possibility of (sub)exponential quantum speedup via a quantum algorithm that follows an adiabatic path of a gapped Hamiltonian with no sign problem. This strengthens the superpolynomial separation recently proved by Hastings. The Hamiltonian that exhibits this speed-up comes from the adjacency matrix of an undirected graph, and we can view the adiabatic evolution as an efficient  $O(\text{poly}(n))$ -time quantum algorithm for finding a specific “EXIT” vertex in the graph given the “ENTRANCE” vertex. On the other hand we show that if the graph is given via an adjacency-list oracle, there is no classical algorithm that finds the “EXIT” with probability greater than  $\exp(-n^\delta)$  using at most  $\exp(n^\delta)$  queries for  $\delta = 1/5 - o(1)$ . Our construction of the graph is somewhat similar to the “welded-trees” construction of Childs et al., but uses additional ideas of Hastings for achieving a spectral gap and a short adiabatic path.

### 3.8 Verifying BQP Computations on Noisy Devices with Minimal Overhead

*Elham Kashefi (University of Edinburgh, GB)*

**License** © Creative Commons BY 4.0 International license

© Elham Kashefi

**Joint work of** Elham Kashefi, Dominik Leichtle, Luka Music, Harold Ollivier

**Main reference** Elham Kashefi, Dominik Leichtle, Luka Music, Harold Ollivier: “Securing Quantum Computations in the NISQ Era”, CoRR, Vol. abs/2011.10005, 2021.

**Main reference** <https://arxiv.org/abs/2011.10005>

With the development of delegated quantum computation, clients will want to ensure confidentiality of their data and algorithms, and the integrity of their computations. While protocols for blind and verifiable quantum computation exist, they suffer from high overheads and from oversensitivity: When running on noisy devices, imperfections trigger the same detection mechanisms as malicious attacks, resulting in perpetually aborted computations. We introduce the first blind and verifiable protocol for delegating BQP computations to a powerful server with repetition as the only overhead. It is composable and statistically secure with exponentially-low bounds and can tolerate a constant amount of global noise.

### 3.9 Compact Fermion to Qubit Mappings

*Joel David Klassen (Phasecraft – London, GB)*

**License** © Creative Commons BY 4.0 International license

© Joel David Klassen

**Joint work of** Joel Klassen and Charles Derby

**Main reference** Charles Derby, Joel Klassen, Johannes Bausch, Toby Cubitt: “Compact fermion to qubit mappings”, Phys. Rev. B, Vol. 104, p. 035118, American Physical Society, 2021.

**URL** <http://dx.doi.org/10.1103/PhysRevB.104.035118>

**Main reference** Charles Derby, Joel Klassen: “A Compact Fermion to Qubit Mapping Part 2: Alternative Lattice Geometries”, CoRR, Vol. abs/2101.10735, 2021.

**URL** <https://arxiv.org/abs/2101.10735>

Mappings between fermions and qubits are valuable constructions in physics. To date only a handful exist. In addition to revealing dualities between fermionic and spin systems, such mappings are indispensable in any quantum simulation of fermionic physics on quantum computers. The number of qubits required per fermionic mode, and the locality of mapped fermionic operators strongly impact the cost of such simulations. We present a fermion to qubit mapping that outperforms all previous local mappings in both the qubit to mode ratio and the locality of mapped operators. In addition to these practically useful features, the mapping bears an elegant relationship to the toric code, which we discuss. We additionally discuss the general algebraic framework employed to construct this mapping.

### 3.10 Provably efficient machine learning for quantum many-body problems

*Richard Küng (Johannes Kepler Universität Linz, AT)*

**License** © Creative Commons BY 4.0 International license

© Richard Küng

**Joint work of** Richard Küng, Hsin-Yuan Huang, Giacomo Torlai, Victor Albert, John Preskill

**Main reference** Hsin-Yuan Huang, Richard Kueng, Giacomo Torlai, Victor V. Albert, John Preskill: “Provably efficient machine learning for quantum many-body problems”, CoRR, Vol. abs/2106.12627, 2021.

**URL** <https://arxiv.org/abs/2106.12627>

Classical machine learning (ML) provides a potentially powerful approach to solving challenging problems in quantum physics and chemistry. However, the advantages of ML over more traditional methods have not been firmly established. We prove that classical ML algorithms can efficiently predict ground state properties of a physical system, after learning from data obtained by measuring related systems. We also prove that classical ML algorithms can efficiently classify a wide range of quantum phases of matter. Our arguments are based on the concept of a classical shadow, a succinct classical description of a quantum state that can be constructed in feasible quantum experiments and be used to predict many properties of the state.

### 3.11 On QMA Queries with Tree-like Dependencies

*Dorian Rudolph (Universität Paderborn, DE)*

**License** © Creative Commons BY 4.0 International license

© Dorian Rudolph

**Joint work of** Sevag Gharibian, Dorian Rudolph

The quantum analogue of NP, called QMA (Quantum Merlin Arthur) has the physically motivated complete problem of estimating the ground state energy of a local Hamiltonian. A related problem is simulating the measurement of a local Hamiltonian’s ground state. Ambainis (CCC 2014) showed that this problem, denoted APX-SIM (Approximate Simulation), is  $P^{QMA[\log]}$ -complete.  $P^{QMA[\log]}$  is the class of problems that can be solved by a deterministic polynomial-time Turing machine that may ask a QMA-oracle  $O(\log(n))$  adaptive queries. Gharibian, Piddock, and Yirka (STACS 2020) show that a polynomial number of parallel queries can be simulated using a logarithmic number of adaptive queries and therefore  $P^{QMA[\log]} = P^{||QMA}$ , which also holds for StocQMA.

In the classical setting, an even stronger result is given by Gottlob (JACM 1995): A polynomial number of NP queries with a tree-like dependency graph can be simulated using a logarithmic number of adaptive queries (i.e.,  $P^{NP[\log]} = \text{Trees}(\text{NP})$ ). More generally, dependent queries can be modeled as a query graph, in which each node contains a query to an oracle for some class C, that is constructed by a uniform circuit taking results from incoming edges as inputs. Within this model, we strengthen Gottlob’s result to query graphs with a bounded separator number (this includes bounded treewidth) and apply it to the quantum setting by proving  $P^{C[\log]} = \text{BSN}(C)$  for C in NP, MA, QCMA, QMA, QMA(2), where  $\text{BSN}(C)$  denotes the class of problems poly-time reducible to query graph with queries to a C-oracle and a bounded separator number. We further show that query graphs with a logarithmic separator number can be solved by  $QP^{C[\log^2]}$ . We also improve the state of the art for StocQMA by showing that query graphs of constant depth can be solved using a logarithmic number of queries.

### 3.12 Classical proofs of quantum knowledge

*Thomas Vidick (Caltech – Pasadena, US)*

**License**  Creative Commons BY 4.0 International license  
© Thomas Vidick

**Joint work of** Thomas Vidick, Tina Zhang

**Main reference** Thomas Vidick, Tina Zhang: “Classical Proofs of Quantum Knowledge”, in Proc. of the Advances in Cryptology – EUROCRYPT 2021, pp. 630–660, Springer International Publishing, 2021.

**URL** [https://doi.org/10.1007/978-3-030-77886-6\\_22](https://doi.org/10.1007/978-3-030-77886-6_22)

We define the notion of a proof of knowledge in the setting where the verifier is classical, but the prover is quantum, and where the witness that the prover holds is in general a quantum state. We establish simple properties of our definition, including that, if a nondestructive classical proof of quantum knowledge exists for some state, then that state can be cloned by an unbounded adversary, and that, under certain conditions on the parameters in our definition, a proof of knowledge protocol for a hard-to-clone state can be used as a (destructive) quantum money verification protocol. In addition, we provide two examples of protocols (both inspired by private-key classical verification protocols for quantum money schemes) which we can show to be proofs of quantum knowledge under our definition. Finally, we show that, under our definition, the verification protocol introduced by Mahadev (FOCS 2018) is a classical argument of quantum knowledge for QMA relations.

## Participants

- Simon Apers  
Free University of Brussels, BE
- Sergio Boixo  
Google – Venice, US
- Harry Buhrman  
CWI – Amsterdam, NL
- Libor Caha  
IBM Research-Zurich, CH
- Jens Eisert  
FU Berlin, DE
- Lior Eldar  
IL

- Sevag Gharibian  
Universität Paderborn, DE
- Dominik Hangleiter  
University of Maryland –  
College Park, US
- Marcel Hinsche  
FU Berlin, DE
- Marios Ioannou  
FU Berlin, DE
- Robert König  
TU München, DE

- Maris Ozols  
University of Amsterdam, NL
- Dorian Rudolph  
Universität Paderborn, DE
- Norbert Schuch  
Universität Wien, AT
- Barbara Terhal  
TU Delft, NL
- Frank Verstraete  
Ghent University, BE
- Petra Wolf  
Universität Trier, DE

## Remote Participants

- Scott Aaronson  
University of Texas – Austin, US
- Dorit Aharonov  
The Hebrew University of  
Jerusalem, IL
- Anurag Anshu  
University of California –  
Berkeley, US
- Itai Arad  
Technion – Haifa, IL
- Johannes Bausch  
University of Cambridge, GB
- Adam Boulund  
Stanford University, US
- Sergey Bravyi  
IBM TJ Watson Research Center  
– Yorktown Heights, US
- Michael Bremner  
University of Technology –  
Sydney, AU
- Andrew Childs  
University of Maryland –  
College Park, US
- Toby Cubitt  
University College London, GB
- Abhinav Deshpande  
University of Maryland –  
College Park, US
- Bill Fefferman  
University of Chicago, US
- András Gilyén  
Caltech – Pasadena, US

- David Gosset  
University of Waterloo, CA
- Alex Grilo  
Sorbonne University – Paris, FR
- Sandy Irani  
University of California –  
Irvine, US
- Stacey Jeffery  
CWI – Amsterdam, NL
- Elham Kashefi  
University of Edinburgh, GB
- Joel David Klassen  
Phasecraft – London, GB
- Robert König  
TU München, DE
- Robin Kothari  
Microsoft Corporation –  
Redmond, US
- Richard Küng  
Johannes Kepler Universität  
Linz, AT
- Urmila Mahadev  
California Institute of Technology  
– Pasadena, US
- Milad Marvian  
University of New Mexico, US
- Rewad Mezher  
University of Edinburgh, GB
- Tomoyuki Morimae  
Kyoto University, JP

- Ramis Movassagh  
IBM Research – Boston, US
- Daniel Nagaž  
Slovak Academy of Sciences –  
Bratislava, SK
- Harumichi Nishimura  
Nagoya University, JP
- David Pérez García  
Complutense University of  
Madrid, ES
- Stephen Piddock  
University of Bristol, GB
- Jamie Sikora  
Virginia Polytechnic Institute –  
Falls Church, US
- Maarten Stroeks  
University of Cambridge, GB
- Aarthi Sundaram  
Microsoft/Microsoft Quantum –  
Redmond, US
- Yuki Takeuchi  
NTT – Kyoto, JP
- Ewin Tang  
University of Washington –  
Seattle, US
- Thomas Vidick  
Caltech – Pasadena, US
- James Watson  
University College London, GB
- Justin Yirka  
University of Texas – Austin, US

