

ARTICLE




<https://doi.org/10.1038/s41467-021-27922-0>

OPEN

Quantum algorithmic measurement

Dorit Aharonov¹, Jordan Cotler^{2,3}   & Xiao-Liang Qi³

There has been recent promising experimental and theoretical evidence that quantum computational tools might enhance the precision and efficiency of physical experiments. However, a systematic treatment and comprehensive framework are missing. Here we initiate the systematic study of experimental quantum physics from the perspective of computational complexity. To this end, we define the framework of quantum algorithmic measurements (QUALMs), a hybrid of black box quantum algorithms and interactive protocols. We use the QUALM framework to study two important experimental problems in quantum many-body physics: determining whether a system's Hamiltonian is time-independent or time-dependent, and determining the symmetry class of the dynamics of the system. We study abstractions of these problems and show for both cases that if the experimentalist can use her experimental samples coherently (in both space and time), a provable exponential speedup is achieved compared to the standard situation in which each experimental sample is accessed separately. Our work suggests that quantum computers can provide a new type of exponential advantage: exponential savings in resources in quantum experiments.

¹School of Computer Science and Engineering, The Hebrew University of Jerusalem, The Edmond J. Safra Campus, 9190416 Jerusalem, Israel. ²Society of Fellows, Harvard University, Cambridge, MA 02138, USA. ³Stanford Institute for Theoretical Physics, Stanford University, Stanford, CA 94305, USA.
email: jcotler@fas.harvard.edu

Since the early days of physics, innovative methods have been invented to interrogate physical systems via *experiments*. By example, some experiments measure constants of nature, such as the speed of light or the charge the electron; others quantify dynamical properties of systems, such as rates of chemical reactions; yet others infer structural properties, like the symmetry group of a crystal. Often experiments seek to learn more abstract information, such as the chain of chemical reactions that comprise photosynthesis, or whether Yang–Mills theory describes the strong force. We can ask: what exactly is an experiment, in its full scope of generality?

Over the past two decades, we have witnessed a new era in this respect, in which ingredients, ideas and concepts originating from the world of quantum computation are being incorporated into the experimental physics toolbox^{1–25}. This body of work constitutes strong evidence that leveraging quantum computational resources to manipulate and measure physical systems may dramatically enhance experimental capabilities. However, what is the extent of these improvements? And what is the right model in which one can study the possibilities and limitations of these more general quantum experiments? A theoretical framework for the systematic study of general quantum experiments, and the resources they require, does not exist yet. The *quantum Church Turing thesis*²⁶ suggests that any physical process can be efficiently (i.e., with only polynomial overhead) simulated by a *quantum* algorithm applying local quantum gates. This observation not only constitutes the pillar on which the entire theory of quantum algorithms and quantum computational complexity stands, but it has also had a profound impact on our understanding of quantum physics in the past two decades (see, e.g. ref. 27). We take this insight one step further to the setting of quantum experiments.

In this work we provide a computational complexity framework for quantum experiments. We argue that (i) Experiments should be viewed as generalizations of quantum algorithms. They can be studied and designed abstractly, using quantum gates and circuits. (ii) One can study the *computational complexity* of quantum experiments, as an extension of the way the computational complexity of quantum algorithms is studied. We thus use the language of *computational complexity* to define an abstract model of general experiments, which we call *quantum algorithmic measurements*, or *QUALMs*, which we hypothesize is universal for quantum experiments. Initial seeds for our approach were given in^{24,28}.

Results

The quantum algorithmic measurement framework. Our starting point is the postulate that the goal of any physical experiment is to compute a function from an input physical system to a classical outcome. The value of the function holds the information that the experimentalist wishes to extract about that physical system. In contrast to standard (quantum or classical) algorithms, the input for a physical experiment is a physical system; the experimentalist is not given a full classical description of it. Instead, access to the physical input system is mediated by quantum operations and measurements, which in general provide only limited information.

A first natural attempt is to model experiments as “black box” quantum algorithms: queries to the physical system (namely applications of the unknown superoperator describing the system) are interlaced with controlled quantum computations applied by the experimentalist. However, it turns out that this model is not general enough to describe all quantum experiments;

in particular, it does not allow the physical system being studied to maintain its own inaccessible (or private) quantum memory.

Towards defining a universal model of experiments, consider the concrete example of an X-ray diffraction experiment, performed to determine the crystal structure of a material. The experiment involves a crystal sample; X-ray photons, which exhibit an electromagnetic interaction with the crystal; and a camera as well as other lab equipment, which only interact with the photons (see Fig. 1(a)). This is a very general situation: in a physical experiment, the experimentalist usually cannot fully interact with all degrees of freedom of the physical system she desires to measure. We thus model a general experimental system as consisting of three subsystems (registers). The first is called “Nature”, denoted by N , which we view as the system that Nature holds secretly, and to which the experimentalist has no direct access in the experiment (this is the crystal in the above example). Our apparatus in the lab is denoted by W for “work space” (e.g. the camera and data processors in the X-ray example). The degrees of freedom that the experimentalist does have access to, but which couple to the hidden degrees of freedom of N , comprise the “lab” register L (e.g., the X-ray photons).

In the X-ray example, the *input physical system*, which the experimentalist would like to measure or learn about, can be described by the combination of the (unknown) state and structure of the crystal, together with the (unknown) interaction between the crystal and the photons (it is unknown since it is a function of the unknown properties of the crystal). More generally, we model an input physical system by a *lab oracle*. The description of the lab oracle contains the initial state of the hidden degrees of freedom N , its dynamics, and the interaction between N and L .

Definition 1 (Roughly) A lab oracle is described by a pair $LO(N, L) = (\mathcal{E}_{NL}, \rho_N)$, where \mathcal{E}_{NL} is a superoperator acting jointly on N and L , and ρ_N is the initial state of the N system.

Our general model of a physical experiment is described in Fig. 1(b). We model a physical experiment as an interactive protocol applied between the work space W and Nature N ; these two registers communicate using the lab register L , which serves as a “message” register. The superoperator \mathcal{E}_{NL} describing the interaction between L and N , given by the physical system to be measured or probed, is unknown and is viewed as a *black box*, which can be “queried”; namely, it can be applied at will by the experimentalist. The addition of the Nature register N allows us to arrive at a rather simple hybrid model, which combines two basic models in computer science: interactive protocols, and black box algorithms.

We next introduce a notion paralleling that of a *computational problem* in the algorithmic world. It is called a *Task*, and it encapsulates the experimental goal that the experimentalist wishes to achieve. The *Task* consists of the information that the experimentalist wishes to extract, expressed as a function from lab oracles (capturing physical systems) to classical outputs. It also includes the constraints on the experiment due to various limitations in the lab, specified by the *admissible gate set*. These gates are constrained to not act on N , and they can also express additional constraints in the laboratory such as geometric restrictions on the interactions.

Definition 2 (Roughly) A task is a tuple $\text{Task} = (S_{\text{in}}, S_{\text{out}}, f, \mathcal{G})$, associated with a given system $N \otimes L \otimes W$. Here, $S_{\text{in}}, S_{\text{out}} \subseteq W$ consist of p and q qubits respectively; f is a function

$$f: \{LO_0, LO_1, LO_2, \dots\} \times \{0, 1\}^p \longrightarrow \{0, 1\}^q, \quad (1)$$

and \mathcal{G} is a set of admissible gates on $L \otimes W$. In the domain of f , $\{LO_0, LO_1, LO_2, \dots\}$ is a set of lab oracles.

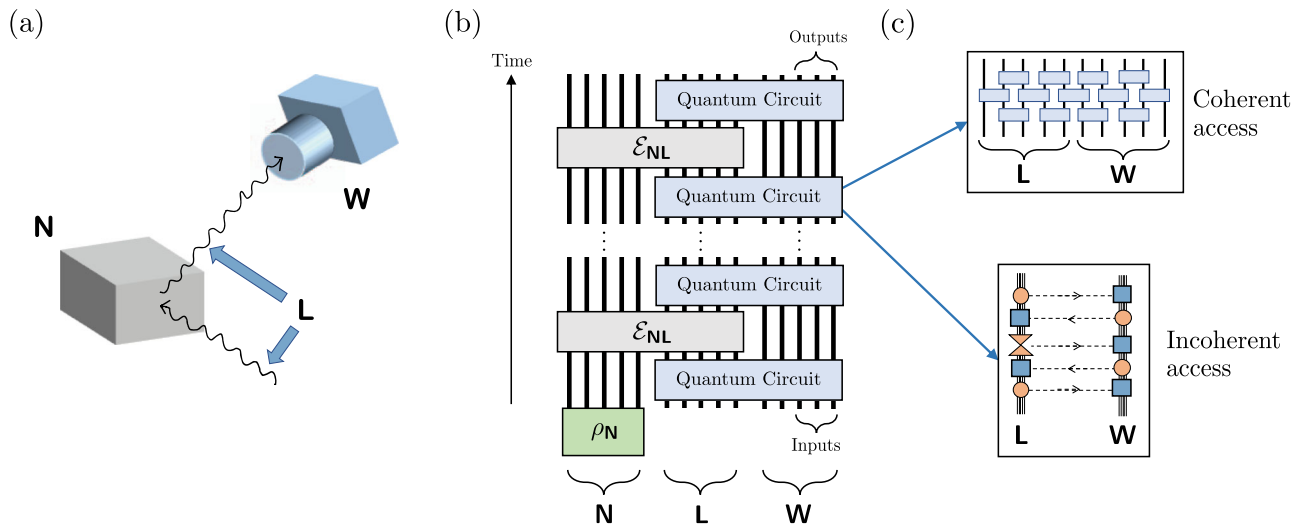


Fig. 1 Schematic of a quantum algorithmic measurement. **a** Illustration of a QUALM for X-ray diffraction, where **N** is the crystal sample, **L** consists of the X-ray photons (including the incoming and outgoing ones), and **W** contains the camera and other lab equipment for taking and processing the image. **b** Schematic illustrating the structure of a QUALM as an interaction between Nature and the experimentalist’s controlled degrees of freedom. Here **N** represents the ‘Nature’ register, **L** is the ‘lab’ register, and **W** is the ‘working space’ register. The experimentalist does not have direct measurement access to the **N** register, which should be thought of as the “hidden” degrees of freedom of the physical system on which the experiment is conducted. The initial state on **N** is ρ_N and the input and output subsets of **W** are specified. **c** Illustration of the coherent and incoherent access QUALMs. Coherent access QUALMs allow for general unitary dynamics on the lab and working spaces. Incoherent access QUALMs only permit classical communication between the lab and working spaces; each orange solid circle is a completely positive (CP) map and each blue box is a completely positive trace-preserving (CPTP) map. At least one of the CP maps between each application of the lab oracle is a complete measurement, indicated by a double triangle. The direction of the arrows in the horizontal dashed lines indicates the direction of classical information flow.

Note that the function f in the above definition has as its inputs not only the lab oracle, but also a classical bit string. The latter should be thought of as additional parameters that describe the desired data, e.g. the specification of the temperature at which the experimentalist may want to perform a certain experiment. While in the above definition the output of f is deterministic, a very natural generalization is for the output to be a *probability distribution* over classical output strings; this allows expressing approximated tasks or taking into account finiteness of precision (see discussion in Example 1 in the Supplementary Information).

Finally we can define a QUALM; this specifies an experimental protocol, i.e., a way to implement the experiment such that it achieves the desired task.

Definition 3 (Roughly) A $\text{QUALM}(\mathbf{N}, \mathbf{L}, \mathbf{W})$ is a specification of a sequence of admissible gates from a set \mathcal{G} on the subsystems **L**, **W**, interlaced with applications of a black box operator \square acting on **N**, **L**; some of the qubits (i.e., those in S_{in}) in the register **W** are marked as inputs and some (i.e., those in S_{out}) as outputs.

We note that this definition is tightly related to the definitions of quantum strategies²⁹ and quantum combs³⁰ introduced in the context of quantum interactive protocols or games. A QUALM is designed in order to achieve a specific experimental Task. To see which Task is achieved by the QUALM, we can view the QUALM naturally as a map from the input lab oracle $(\mathcal{E}_{\text{NL}}, \rho_N)$ to a standard quantum circuit, acting on $\mathbf{N} \otimes \mathbf{L} \otimes \mathbf{W}$, whose input bits are in S_{in} and output bits are in S_{out} . **N** is initialized to ρ_N , all qubits in **W** and **L** except for S_{in} are initialized to 0, and the input to the circuit is given in S_{in} . The circuit applies to this initial state the gate sequence of the QUALM, where whenever \square appears, \mathcal{E}_{NL} is applied. The output of the circuit is given by measuring S_{out} in the computational basis. We say that a QUALM achieves a given Task if (i) the sets $\mathcal{G}, S_{\text{in}}, S_{\text{out}}$ are the same for the QUALM and the Task, and (ii) for every lab oracle LO and input string x to S_{in} , the result of the measurement of the output qubits S_{out}

(after the application of the corresponding circuit) is equal (or close, in cases of approximations) to $f(\text{LO}, x)$, with f being the Task function.

The computational complexity of a QUALM is the number of gates plus the number of lab oracle applications; the QUALM complexity of the Task is that of the most efficient QUALM that achieves it. We propose that QUALM complexity is a standardized way to quantify and study the (asymptotic behavior of the) cost of achieving an experimental task in the laboratory.

In the Supplementary Information, we provide a versatile set of examples for how different experimental tasks can be viewed as Tasks and be realized by QUALMs. We hypothesize that the QUALM framework is a *universal* model for quantum experiments, in the sense that any physical process realizing an experimental task can be simulated efficiently (i.e., with at most polynomial overhead in all resources) by a QUALM; in other words, we speculate that the quantum Church Turing thesis can be extended from computational problems to experiments, by generalizing quantum algorithms to QUALMs. We stress that all the ingredients included in the QUALM framework seem to be necessary for its universality; in particular, the register **N** is necessary in order to describe some of the more sophisticated physical experiments (see, e.g., the verification example in Supplementary Note B in the Supplementary Information). We thus arrive at a framework that allows us to initiate a rigorous study of the resources required in order to perform physical experimental tasks.

Exponential advantage of coherent QUALMs. An overwhelming majority of quantum experiments performed in contemporary laboratories are of a much more restricted type than general QUALMs. In those more restricted experiments, which we call *incoherent* QUALMs, the physical system is usually probed by preparing it in some state, possibly letting it evolve, applying a measurement, and then post-processing the measurement’s

outcome classically. This may be repeated many times, and the initial state and the basis of measurement may even depend adaptively on previous outcomes. The key point is that these experiments do not utilize coherence between different accesses of the lab oracle, or between the lab space and the working space. We formally define incoherent QUALMs using the notion of LOCC (local operations and classical communication) protocols; see Fig. 1(c).

The first question we choose to address in the QUALM framework is whether generalizing quantum experiments beyond incoherent QUALMs, could lead to significant savings in resources in physics experiments. To this end, we compare incoherent QUALMs to the most general possible QUALMs, which are allowed to leverage a full-fledged quantum computer, apply quantum gates on the lab register during the experiment, and so on. We refer to these general, unrestricted experiments as *coherent QUALMs*.

We study this question in the context of two basic experimental tasks. The first is the task of distinguishing a Floquet system from a random quantum evolution. Roughly speaking, we want to design an experiment that distinguishes a fixed Hamiltonian from a time-dependent, random Hamiltonian. We consider the following toy version of this problem:

Definition 4 (The fixed unitary problem) (Roughly) Consider two lab oracles LO_0 and LO_1 , corresponding to two physical systems. The first lab oracle LO_0 picks a Haar-random unitary, remembers it (forever), and then subsequently applies that *same* unitary to \mathbf{L} each time the oracle is called. By contrast, the second lab oracle LO_1 applies a new Haar-random unitary to \mathbf{L} each time the oracle is called. The goal is to distinguish between LO_0 and LO_1 with non-negligible success probability.

There is a very simple coherent QUALM that distinguishes between LO_0 and LO_1 : just call the lab oracle twice and perform a SWAP test on the two output states. Indeed, variants of the fixed unitary problem and the SWAP protocol have been previously studied (see e.g.^{31,32}). However, it turns out that an incoherent QUALM would require exponential resources. Here we provide such an exponential complexity separation. This is implied by the following lower bound:

Theorem 1 (Exponential lower bound for incoherent adaptive QUALMs for the fixed unitary problem) (Roughly) For any incoherent QUALM for the “fixed unitary problem” on ℓ qubits (i.e., \mathbf{L} has ℓ qubits), its QUALM complexity is lower bounded by an exponential in ℓ , namely $\Omega(2^{2\ell/7})$.

The proof is not too difficult if the incoherent QUALM is non-adaptive, however the argument becomes far more complicated in the adaptive setting. We sketch here the two key points of the proof (See the Methods section and the Supplementary Information for more details).

The first is to reduce incoherent QUALMs to simple measurement QUALMs. In a generic incoherent QUALM, there can be multiple rounds of classical communications between \mathbf{L} and \mathbf{W} , before and after each application of the lab oracle (see Fig. 1(c)). However, we show that a generic incoherent QUALM is equivalent to a probabilistic average over a family of “simple measurement QUALMs”, which refers to special incoherent QUALMs that simply (i) prepare a state, (ii) apply the lab oracle to that state, (iii) measure the result, and then repeat (i), (ii), (iii) with different settings. The state preparations and measurement bases can depend adaptively on the measurement results of previous steps.

The other key part of the proof is our lower bound for the simple measurement QUALMs required to perform the task. Let P_k be the probability distribution of the k measurement results in the case of the lab oracle applying a newly-chosen random unitary each time. P_k is uniformly random. Q_k is the distribution

over all k intermediate measurement results for the fixed unitary oracle, and we show it is exponentially close to P_k . This is achieved using the Weingarten functions $W(\tau, D)$; we write:

$$Q_k(s) = \sum_{\sigma, \tau \in S^k} \text{tr}(A_s \sigma) \text{tr}(B_s \tau^{-1}) W(\tau \sigma^{-1}, D) \quad (2)$$

with A_s and B_s operators corresponding to the adaptive choice of preparation state and basis of measurement for each of the oracle calls. σ, τ are elements of the permutation group. The difficulty here is that in computing the 1-norm distance between P_k and Q_k , the sum over s cannot be carried over straightforwardly, due to the dependence of the input states and bases of measurement on previous measurement results. A key ingredient in the proof is to show that in the above sum, the term corresponding to each permutation τ on the k oracle calls can be partitioned to two, such that the sum associated with each part is done one by one over parameters, which are independent from the remaining parameters in the sum.

Our second physically motivated task is to determine the symmetry class of the dynamics of a quantum many-body system. The symmetries of a many-body system are essential to its physical properties, and are the core of all analytic treatments. It is generally difficult to ascertain the symmetries of an uncharacterized quantum system; however, we might intuit that a quantum computer could aid in this endeavor. We study the following toy version of the problem:

Definition 5 (The Symmetry Distinction Problem) Distinguish, with non-negligible success probability, between three classes of lab oracles: (i) a lab oracle LO_U , which applies a fixed Haar-random unitary to the \mathbf{L} system; (ii) a lab oracle LO_O , which applies a fixed Haar-random orthogonal matrix to the system; (iii) a lab oracle LO_{Sp} , which applies a fixed Haar-random symplectic matrix to the system. (Suppose that \mathbf{L} contains an even number of qubits).

If one is allowed coherent access, then one can use a generalization of the SWAP test (this time on a maximally entangled state and with a little more sophistication) to determine the symmetry type of the lab oracle. However, extending the techniques used in the proof of Theorem 1, we can prove our second main theorem, stating that any incoherent (even adaptive) QUALM for the symmetry distinction problem will have QUALM complexity at least of order $\Omega(2^{2\ell/7})$. The idea of the proof is that LO_U , LO_O and LO_{Sp} are each indistinguishable from the lab oracle LO_1 that generates a new Haar-random unitary each time it is queried, and so are indistinguishable from one another.

Discussion

Our motivation in this work is Physics. We argued that recent developments involving computational elements in quantum experiments, suggest a general model for quantum experiments, which clarifies the paradigm of experimentation itself. We have demonstrated an exponential advantage in QUALM complexity of coherent over incoherent access QUALMs (even when the latter are adaptive), for two physically motivated problems. Moreover, this exponential advantage is achieved using an very simple coherent QUALM, based solely on the SWAP test.

At first glance, it might seem that early quantum black box algorithms such as Simon’s algorithm³³ already provide an exponential advantage of coherent over incoherent QUALMs, even if not for physically motivated tasks. However, when viewed as a QUALM, Simon’s algorithm in fact falls within the incoherent QUALM framework. Indeed, Simon’s algorithm accesses each sample separately, uses product state preparations, and only utilizes measurements in a tensor product basis. However, recently, Simon’s algorithm was upgraded to a recursive

version³⁴, which was used to provide an example of an exponential separation between the computational power of quantum circuits (with access to a black box) of different depths. Another example of such a separation of the depth hierarchy was given in³⁵. Interestingly, these results can be interpreted (with a little bit of translation work) into two other examples of exponential separations between coherent and incoherent QUALMs, albeit for tasks, which are quite contrived from a physics perspective.

It is also interesting to view related and previous works in the language of QUALMs, and compare to our work. Some previous results imply a quadratic advantage in QUALM complexity, and only under the strong assumption of non-adaptive access in the incoherent setting^{36,37}. For other results an exponential lower bound is only conjectured (e.g., refs. 38,39). An example more closely related to our work is ref. 40, which provides a proven exponential advantage of coherent QUALMs over what we call “single register access” (which is a restricted case of incoherent QUALMs) for a quantum state distinction problem emerging from the dihedral hidden subgroup problem. However, importantly, the coherent protocol suggested has exponential gate complexity, and so the related experiment is not known to be efficient even in the coherent access setting (also, once again, the lower bound holds only under the strong non-adaptive assumption). The recent independent work of ref. 41 studied a closely related setting, and provided an exponential query complexity separation between incoherent and coherent QUALMs for a state tomography task, using quantum machine learning; however, as in ref. 40, the focus of ref. 41 is on query complexity; both their coherent and incoherent experiments have exponential gate complexity.

We gave the first evidence that entanglement and coherence could be truly exponentially advantageous (in terms of physical resources) when performing experiments in the lab, for physically motivated tasks. Our work suggests that coherence could be an immense resource in quantum experiments, and highlights the fact that quantum computers have a huge potential not only in speeding up the solution for computational problems, but also in providing dramatic savings in performing experimental tasks. In particular, important savings in resources may be achievable by using more sophisticated quantum algorithmic ideas, much beyond the SWAP test, which is used here.

Looking forward, we hope that the QUALM framework will be helpful in the study and development of new experimental techniques leveraging quantum computational components and ideas. Numerous interesting open questions are raised; for example, does adaptiveness help in the incoherent setting (see refs. 42,43)? How can more sophisticated quantum input states and measurement bases help in various experiments? How much does a larger work space buy us? Importantly, the examples we provided here lose their exponential advantage in the presence of noise. Can exponential advantages in QUALM complexity be exhibited in the NISQ era? More generally, can the advantages be achieved in settings closer to reality, e.g., where the lab oracles are efficient? It would be very interesting to experimentally demonstrate advantages of coherent quantum experiments.

Methods

Notations. We consider a total Hilbert space $H = N \otimes L \otimes W$ (we use the same notation to denote the subsystems and their associated Hilbert spaces). N stands for the “Nature” Hilbert space of n qubits, to which the experimentalist has no direct access; The “lab” Hilbert space is denoted L and consists of ℓ qubits, corresponding to the degrees of freedom of the physical system, which the experimentalist can access, and W , a subsystem of w qubits, can be thought of as the “working space” of the experimentalist. The set of states (density matrices) on each subsystem will be denoted by $\mathcal{D}(N), \mathcal{D}(L), \mathcal{D}(W), \dots$; we similarly denote classical probability distributions on $\{0, 1\}^k$ by $\mathcal{D}(\{0, 1\}^k)$. We denote the Hilbert space of the union of two subsystems L, W (as well as the set of qubits) by LW , or $L \otimes W$. Operators,

superoperators, as well as sets thereof, will be denoted using a calligraphic font: $\mathcal{E}, \mathcal{Q}, \mathcal{O}$ etc. We will often abuse notation, and refer to an ordered sequence of superoperators $\mathcal{Q} = (\mathcal{Q}_1, \mathcal{Q}_2, \dots, \mathcal{Q}_k)$ as equal to the operator $\mathcal{Q} = \mathcal{Q}_k \circ \dots \circ \mathcal{Q}_2 \circ \mathcal{Q}_1$, which is the result of applying the superoperators in the sequence in the given order.

The QUALM framework. We now provide the definitions required for the QUALM framework; The setup is summarized in Fig. 1. Our first definition is that of the *lab oracle*; it models the input physical system on which the experiment is performed.

Definition 6 (Lab Oracle). A lab oracle is specified by a pair $LO = (\mathcal{E}_{NL}, \rho_N)$ where \mathcal{E}_{NL} is a quantum superoperator (i.e. a completely positive trace-preserving map) on $N \otimes L$ and ρ_N is state on N . The set of lab oracles is denoted by $\mathcal{L}(\mathcal{O}(N, L))$.

Now we define the notion of a *task*, which corresponds to the “experimental problem” to be solved: it describes what it is that the experimentalist wants to measure. The experimentalist must achieve the task only by using the lab oracle superoperator, together with the operations at her disposal in her laboratory (i.e., the admissible gates on $L \otimes W$).

Definition 7 (Admissible gates). We denote by \mathcal{G} a set of “admissible gates”, namely a set of quantum superoperators acting on $L \otimes W$. (Note that superoperators include measurements).

Definition 8 (Task). A ‘task’ is a tuple $\text{Task} = (S_{\text{in}}, S_{\text{out}}, f, \mathcal{G})$, associated with a given system $N \otimes L \otimes W$ (which is usually implicit). Here, S_{in} is a p -qubit subsystem of W , S_{out} is a q -qubit subsystem of W , f is a function

$$f: \{LO_0, LO_1, LO_2, \dots\} \times \{0, 1\}^p \rightarrow \{0, 1\}^q, \tag{3}$$

and \mathcal{G} is a set of admissible gates on $L \otimes W$. In the domain of f , $\{LO_0, LO_1, LO_2, \dots\}$ is a set of lab oracles (here we denoted this set as discrete, but of course one can also consider a continuous set of lab oracles as input), i.e. a subset of $\mathcal{L}(\mathcal{O}(N, L))$.

This definition can be thought of as follows. Given a set of lab oracles that represent possible input physical systems, the task is to compute the function f , which takes as input a lab oracle, some classical lab settings (i.e., bit strings in $\{0, 1\}^p$), and outputs a classical ‘experimental result’ (i.e., bit strings $\{0, 1\}^q$). The task is to be achieved by constructing a circuit from admissible gates in \mathcal{G} , in conjunction with interspersed calls to the lab oracle superoperator. In many situations it is more natural to consider output *probability distributions* and define f to be

$$f: \{LO_0, LO_1, LO_2, \dots\} \times \{0, 1\}^p \rightarrow \mathcal{D}(\{0, 1\}^q). \tag{4}$$

Such is the case for classical sampling tasks, for continuous sets of input lab oracles (see example 2 in subsection 2.5 in Supplementary Information), as well as in the context of the task of distinguishing between lab oracles, which is the main focus of this paper; in this case, this generalized notion of a task in fact reduces to Definition 8.

We can now define a QUALM, which can be viewed as a specific choice of protocol for the execution of a Task.

Definition 9 (QUALM) A QUALM over the set of admissible gates \mathcal{G} acting on registers L, W , is an ordered sequence of symbols $\mathcal{Q} = (\mathcal{Q}_1, \mathcal{Q}_2, \dots, \mathcal{Q}_{\text{final}})$ from the alphabet $\mathcal{G} \cup \{\square\}$, together with a specification of input and output subsystems $S_{\text{in}}, S_{\text{out}} \subseteq W$. Here, we are treating \mathcal{G} as a set of symbols (i.e., each gate labels a distinct symbol) and likewise \square is a symbol. Each QUALM has an associated map

$$\text{QUALM} : \mathcal{L}(\mathcal{O}(N, L)) \rightarrow \text{QuantumCircuits}(N \otimes L \otimes W). \tag{5}$$

This function takes in a lab oracle LO , and outputs a quantum circuit on $N \otimes L \otimes W$. Specifically, $\text{QUALM}(LO)$ ‘compiles’ a quantum circuit $\mathcal{Q} = (\mathcal{Q}_1, \mathcal{Q}_2, \dots, \mathcal{Q}_{\text{final}})$ where each symbol in \mathcal{G} is replaced by its corresponding gate, and each \square is replaced by the superoperator \mathcal{E}_{NL} corresponding to LO . $S_{\text{in}}, S_{\text{out}}$ correspond to the input and output subsystems of the resulting circuit, respectively.

In less formal terms, a QUALM is a quantum circuit built out of an admissible gate set, where the circuit has designated spots for a lab oracle superoperator to be inserted, and specified input and output qubits.

Now we explain what it means for a QUALM to achieve a particular Task. We first define the output density matrix of a QUALM for a given lab oracle LO . The idea is to compile the quantum circuit $\text{QUALM}(LO)$ for the lab oracle LO , and then to use it to evaluate $f(LO, x)$. To do so, we construct the initial state of the circuit to be (i) ρ_N^{LO} (i.e. the state corresponding to the lab oracle LO) on N , (ii) $|x\rangle\langle x|$ on S_{in} , and (iii) the zero state elsewhere. The full initial state will be denoted as $\rho_N^{\text{LO}} \otimes |x\rangle\langle x|_{S_{\text{in}}} \otimes |\mathbf{0}\rangle\langle \mathbf{0}|$. We will run the initial state through the circuit $\text{QUALM}(LO)$, and then trace out everything not in S_{out} :

$$\rho_{S_{\text{out}}}(\text{QUALM}(LO, x)) = \text{tr}_{S_{\text{out}}} \left\{ \text{QUALM}(LO) \left[\rho_N^{\text{LO}} \otimes |x\rangle\langle x|_{S_{\text{in}}} \otimes |\mathbf{0}\rangle\langle \mathbf{0}| \right] \right\}. \tag{6}$$

We note that a Task specifies a function $f: \{LO_0, LO_1, LO_2, \dots\} \times \{0, 1\}^p \rightarrow \{0, 1\}^q$. We say that the QUALM implements the Task with error at most ϵ if for each

input (LO_B, x) , we have

$$\left\| \rho_{S_{\text{out}}}(\text{QUALM}(\text{LO}_I, x)) - |f(\text{LO}_I, x)\rangle\langle f(\text{LO}_I, x)| \right\|_1 \leq \epsilon. \quad (7)$$

Note that this definition reduces to standard quantum algorithms, by letting the set of lab oracles in the domain be the empty set.

Remark 1 (*Subroutines, Error reduction by repetition, Approximation*). We remark that standard manipulations from the theory of algorithms carry over to the QUALM setting in a natural way. In particular, a QUALM can be used as a subroutine by another QUALM, as long as they both act on the same lab register **L** (like in standard subroutines, we can decide which qubit “wires” to glue from the original QUALM to the input qubits of the subroutine QUALM, and similarly for the outputs).

Using such subroutine QUALMs, one can achieve error reduction (also known as amplification); this is a standard primitive in probabilistic algorithms⁴⁴, which is also needed in this work. This is done by a straightforward generalization of the way it is done for algorithms. For example, suppose we want to reduce the error probability of a given QUALM, which achieves a certain deterministic task with error $1/3$; and further suppose that the image of the function f has a single output bit, measured at the end of the QUALM in the computational basis. One can construct a new QUALM', which first copies the p -bit input string xm times (for some desired amplification parameter m). It then applies QUALM as a subroutine m times, each time with a new set of qubits initialized to 0 (which together with the p qubits containing the appropriate copy of x , constituting the working register **W** of the particular subroutine). QUALM' then applies a majority calculation on all outputs of the m subroutines; this majority is the output bit of the QUALM'.

In the same manner, we can consider amplifications for QUALMs, which compute probabilistic functions. If for two different lab oracles the output distributions are δ apart in total variation distance, one can amplify the distance by repetition and classical postprocessing.

QUALM complexity. Having defined tasks and QUALMs, we now turn to defining QUALM complexity.

Definition 10 (*Gate complexity, query complexity, and QUALM complexity*). The gate complexity of a given QUALM over the admissible set of gates \mathcal{G} is the length (i.e. the number of symbols from $\mathcal{G} \cup \{\square\}$) of the sequence \mathcal{Q} , minus the number of \square symbols. We denote this by $\text{GateComplexity}[\text{QUALM}]$, and call this the QUALM gate complexity. Similarly, the query complexity is the number of \square 's appearing in \mathcal{Q} , and this is denoted by $\text{QueryComplexity}[\text{QUALM}]$. This is called the QUALM query complexity. We call the sum

$$\text{GateComplexity}[\text{QUALM}] + \text{QueryComplexity}[\text{QUALM}] = |\mathcal{Q}| \quad (8)$$

the QUALM complexity.

The exact (respectively, approximate) QUALM complexity of a task is given by the QUALM with least QUALM complexity, which achieves the task exactly (respectively, approximately).

We also note that it might be relevant, in various situations, to weight gates versus query calls differently, namely to consider the QUALM complexity to be

$$\text{GateComplexity}[\text{QUALM}] + \lambda \text{QueryComplexity}[\text{QUALM}] \quad (9)$$

for some suitable penalty factor λ .

As usual in computational complexity⁴⁵, one is interested in *families* of tasks and QUALMs, where some parameter dictating the *size* of the problem grows to infinity, and we ask how the complexity grows as a function of that parameter.

Different types of access to a lab oracle. Towards clarifying the power of different QUALMs in terms of their computational abilities, we consider different types of *accesses* of QUALMs to a lab oracle. The most natural (though presently least realistic) one is the access of a full quantum computer. By this we mean a general QUALM, without the restrictions to be specified shortly. In particular, the set of admissible gates \mathcal{G} can be a universal set, and there is no restriction on which gates can be applied at any given time.

Definition 11 (*Coherent access*). We will refer to a general QUALM (i.e., with a universal gate set) defined in Definition 9 as a QUALM with *coherent access* to the lab oracle.

In realistic physics experiments, access is often far more limited. The experimental setup may not be able to introduce quantum entanglement between the physical system $\mathbf{N} \otimes \mathbf{L}$ and the rest of the lab **W**. Measurements to the system may destroy the quantum coherence in the physical system or even completely destroy the quantum state. In the QUALM framework this is captured by restrictions on the admissible gate sets and the allowed sequences of gates. To make concrete progress we consider a model of many contemporary experiments, which we call *incoherent access*. To this end, we need to recall the definition of a one-round LOCC protocol between two parties (see, e.g., ⁴⁶). First, we recall that a map $\mathcal{N}^{\mathbf{R}}$ on density matrices on the register **R** is completely positive (CP for short) if it can be associated with a set of Kraus operators $\{\mathcal{A}_\alpha\}_\alpha$ such that for all ρ on **R**

$$\mathcal{N}^{\mathbf{R}}(\rho) = \sum_\alpha \mathcal{A}_\alpha \rho \mathcal{A}_\alpha^\dagger. \quad (10)$$

Furthermore, $\mathcal{N}^{\mathbf{R}}$ is trace-preserving if

$$\sum_\alpha \mathcal{A}_\alpha^\dagger \mathcal{A}_\alpha = \mathbb{1}. \quad (11)$$

A completely positive trace-preserving (CPTP) map is often called, simply, a quantum channel.

Now we specify a quantum channel that implements a certain kind of communication between subsystems **A** and **B** called a “one-round LOCC” (see⁴⁶).

Definition 12 (*One-round LOCC*). A one-round LOCC operator from subsystems **A** to **B** is a quantum channel (i.e. a CPTP map) $\mathcal{E}^{\mathbf{AB}}$ acting on $\mathcal{D}(\mathbf{A} \otimes \mathbf{B})$, which is of the form

$$\mathcal{E}^{\mathbf{AB}}(\cdot) = \sum_\alpha \mathcal{M}_\alpha^{\mathbf{A}}(\cdot) \otimes \mathcal{N}_\alpha^{\mathbf{B}}(\cdot) \quad (12)$$

with $\mathcal{M}_\alpha^{\mathbf{A}}$ a completely positive (CP) map acting on the **A** subsystem, and $\mathcal{N}_\alpha^{\mathbf{B}}$ a completely positive and trace-preserving (CPTP) map acting on the **B** subsystem.

It should be noted that this definition in fact requires $\mathcal{E}^{\mathbf{A}} \equiv \sum_\alpha \mathcal{M}_\alpha^{\mathbf{A}}$ to be a CPTP map (instead of merely a CP map), since $\mathcal{E}^{\mathbf{A}}$ is the reduced channel obtained by tracing over **B** in $\mathcal{E}^{\mathbf{AB}}$.

With the above definition in mind, we can now define incoherent access QUALMs:

Definition 13 (*Incoherent access*). We say a QUALM uses *incoherent access* to the lab oracle if the following holds for the sequence of symbols \mathcal{Q} . Let k be the number of times the symbol \square appears in $\mathcal{Q} = (\mathcal{Q}_1, \mathcal{Q}_2, \dots, \mathcal{Q}_{\text{final}})$. As usual, we associate \mathcal{Q} with the channel $\mathcal{Q} = \mathcal{Q}_{\text{final}} \circ \dots \circ \mathcal{Q}_2 \circ \mathcal{Q}_1$, and regroup terms as

$$\mathcal{Q} = \mathcal{C}_k \circ \square \circ \mathcal{C}_{k-1} \circ \square \circ \dots \circ \square \circ \mathcal{C}_0 \quad (13)$$

where \mathcal{C}_i is a sequence of gates applied after the i th call to the lab oracle, and before the $(i+1)$ st one. We require that

- For each $i \in \{0, \dots, k\}$, the sequence of admissible gates \mathcal{C}_i can be written as an r_i -round LOCC protocol, for some finite number of rounds r_i . In other words, \mathcal{C}_i can be written as a composition $\mathcal{C}_i = \mathcal{C}_{i,r_1} \circ \dots \circ \mathcal{C}_{i,r_{r_i}} \circ \mathcal{C}_{i,1}$ such that for every j , $\mathcal{C}_{i,j}$ is a one-round LOCC channel. Without losing generality, we can assume $\mathcal{C}_{i,j}$ alternates between **L**-to-**W** and **W**-to-**L** one-round LOCC channels, since the composition of two **L**-to-**W** one-round LOCC's is still a one-round LOCC.
- Moreover we also require that for each i there exists at least one index $j \in \{1, \dots, r_i\}$ such that $\mathcal{C}_{i,j}$ is a complete measurement, which is a special one-round LOCC operator from **L** to **W**, as follows:

$$\mathcal{C}_{i,j}(\cdot) = \sum_{\alpha \in \{0,1\}^f} \mathcal{M}_\alpha^{\mathbf{L}}(\cdot) \otimes \mathcal{N}_\alpha^{\mathbf{W}}(\cdot), \quad (14)$$

such that $\mathcal{M}_\alpha^{\mathbf{L}}$ is a rank one projection for each α , i.e., $\mathcal{M}_\alpha^{\mathbf{L}}(\rho) = |\psi_\alpha\rangle\langle\psi_\alpha| \langle\psi_\alpha|\rho|\psi_\alpha\rangle$ for some pure state $|\psi_\alpha\rangle$, and $\{|\psi_\alpha\rangle\}_{\alpha \in \{0,1\}^f}$ is an orthonormal basis for **L**.

The above definition roughly means that the interaction between the **L** and **W** registers is an LOCC throughout the QUALM protocol; moreover, between any two applications of the lab oracle, the lab register **L** is measured using a complete measurement. No coherence can be generated between the state generated by a given single call to the lab oracle, and any other register used by the QUALM – this is the source for the term “incoherent access QUALM”.

We note that the above definition allows *adaptive access* to the lab oracle; namely, the state of the register **L** before an application of the lab oracle may depend on previous measurement results both of **L** and of **W**, and those in turn may depend on the lab oracle.

Sketch of the proof of Theorem 1. The proof of Theorem 1 consists of two steps. The first step is to study a special case, which we call a ‘simple measurement’ (SM) QUALM, and show that it cannot distinguish the two lab oracles $\text{LO}_1(\ell)$, $\text{LO}_0(\ell)$. The second step is to show that the output of a general incoherent access QUALM can be related to a probabilistic average of those SM QUALMs, so that a general incoherent access QUALM cannot do better than a SM QUALM. In the following we will first define the SM QUALM and sketch the proof for this special case, and then discuss how the general incoherent QUALM is reduced to SM QUALM.

Definition 14 (Roughly) *Single measurement QUALM*. The SM QUALM is illustrated in Fig. 2. It describes a QUALM where there is only one measurement carried out after each application of lab oracle. The measurements are of a particular form: each is a POVM in which each element is of rank one. In the i th round, the measurement output s_i is recorded in a new tensor factor of **W**, denoted by \mathbf{W}_i . The i th POVM is thus described by

$$|\lambda_{s_0 s_1 \dots s_i}^i\rangle\langle\lambda_{s_0 s_1 \dots s_i}^i|_{\mathbf{W}_i}, \text{ where } \sum_{s_i} \lambda_{s_0 s_1 \dots s_i}^i |\lambda_{s_0 s_1 \dots s_i}^i\rangle\langle\lambda_{s_0 s_1 \dots s_i}^i| = \mathbb{1}, \quad 0 < \lambda_{s_0 s_1 \dots s_i}^i \leq 1. \quad (15)$$

We note that both $|\lambda_{s_0 s_1 \dots s_i}^i\rangle$ and $\lambda_{s_0 s_1 \dots s_i}^i$ depend not only on s_i but also on all previous measurement results s_0, \dots, s_{i-1} or in short, $s_{<i}$. After the measurement, **L** is prepared into a mixed state $\sigma_{s_0 s_1 \dots s_i}^i$, which again can depend on the previous measurement results s_1, \dots, s_{i-1} . After the last measurement, a readout channel \mathcal{C}_{out} is applied to **W**, which maps the diagonal density operator of **W** to a single qubit output state.

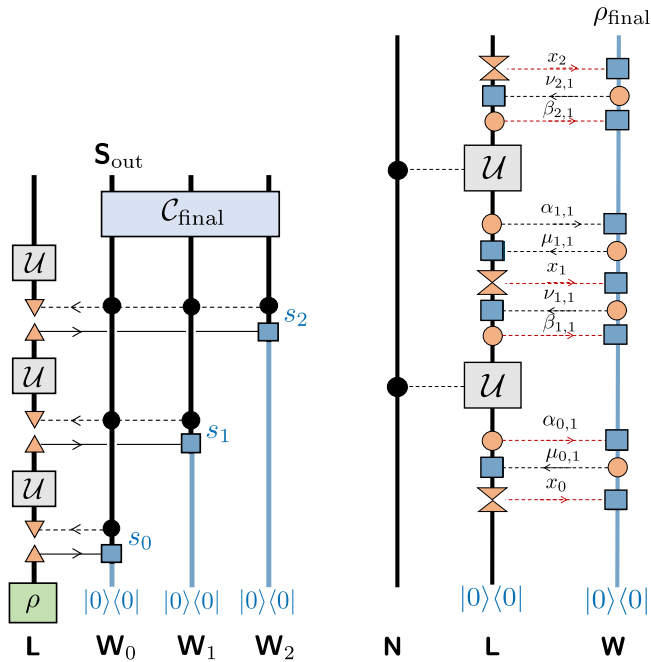


Fig. 2 Circuit for a simple measurement QUALM. (Left) Illustration of the simple measurement QUALM defined in Definition 14. The upward pointing triangles indicate the weighted projection $\rho_L \rightarrow \langle y_{s_0, \dots, s_i} | \rho_L | y_{s_0, \dots, s_i} \rangle \lambda_{s_0, \dots, s_i}^i$. The horizontal solid lines indicate the recording of POVM measurement results in W_i . The horizontal dashed lines connected to downward pointing triangles indicate the preparation of initial state σ_{s_0, \dots, s_i} controlled by previous measurement results s_0, \dots, s_i . (Right) Illustration of the incoherent access QUALM defined in Definition 13. Each orange solid circle is a CP map and each blue box is a CPTP map. At least one of the CP maps between each application of the lab oracle is a complete measurement, indicated by the double triangle. The direction of the arrow in each horizontal dashed line indicates the direction of classical information flow. Only the LOCC's corresponding to $\beta_{i,j}$ and x_i lead to conditional probabilities that depend on the lab oracle, which are indicated by red dashed lines.

For the SM QUALM, the output density operator is determined by applying the readout channel $\mathcal{C}_{\text{final}}$ to the diagonal density operator of W , which encodes the probability distribution of the measurement results s_0, s_1, \dots, s_k . For the fixed random unitary lab oracle $\text{LO}_\ell(\ell)$ (Definition 4), the probability distribution is

$$Q_k(s_0, s_1, \dots, s_k) = \Pr(s_0) \cdot \left(\int_{\text{Haar}} dU \prod_{i=1}^k \langle y_{s_0, s_1, \dots, s_i}^i | U \sigma_{s_0, s_1, \dots, s_{i-1}}^{i-1} U^\dagger | y_{s_0, s_1, \dots, s_i}^i \rangle \lambda_{s_0, s_1, \dots, s_i}^i \right) \quad (16)$$

with $\Pr(s_0) = |\langle y_{s_0}^0 | 0^L \rangle|^2 \lambda_{s_0}^0$. The probability distribution for the other lab oracle $\text{LO}_1(\ell)$ (Definition 4) is

$$\begin{aligned} P_k(s_0, s_1, \dots, s_k) &= \Pr(s_0) \left(\prod_{i=1}^k \int_{\text{Haar}} dU_i \langle y_{s_0, s_1, \dots, s_i}^i | U_i \sigma_{s_0, s_1, \dots, s_{i-1}}^{i-1} U_i^\dagger | y_{s_0, s_1, \dots, s_i}^i \rangle \lambda_{s_0, s_1, \dots, s_i}^i \right) \\ &= \Pr(s_0) D^{-k} \prod_{i=1}^k \lambda_{s_i}^i. \end{aligned} \quad (17)$$

In the following we will often denote the ordered sequence s_0, s_1, \dots, s_k by s for simplicity.

Our conclusion is that these two probability distributions Q_k and P_k are difficult to distinguish. More precisely, for $k < (2^\ell / \sqrt{6})^{4/7}$, we will prove

$$\| P_k - Q_k \|_1 = \sum_s |P_k(s) - Q_k(s)| \leq \mathcal{O}\left(\frac{k^3}{2^\ell}\right). \quad (18)$$

The key mathematical tool we use is the Weingarten functions of the unitary group:

$$\int_{\text{Haar}} dU [U^{\otimes k}]_{IJ} [U^{*\otimes k}]_{KL} = \sum_{\sigma, \tau \in S^k} \tau_{KI} \sigma_{LJ} W(\tau \sigma^{-1}, D). \quad (19)$$

Here I, J, K, L label an orthonormal basis in the k -copied Hilbert space. The action of the permutation group elements σ and τ corresponds to the permutation of different Hilbert space copies. Using Eqn. (19), Q_k in Eq. (16) can be rewritten as

$$Q_k(s) = \sum_{\sigma, \tau \in S^k} \text{tr}(A_s \sigma) \text{tr}(B_s \tau^{-1}) W(\tau \sigma^{-1}, D). \quad (20)$$

with $A_s = \otimes_{i=1}^k \sigma_{s_0, s_1, \dots, s_{i-1}}^{i-1}$, $B_s = \otimes_{i=1}^k |y_{s_0, s_1, \dots, s_i}^i\rangle \langle y_{s_0, s_1, \dots, s_i}^i| \lambda_{s_0, s_1, \dots, s_i}^i$. The sum in Eqn. (20) consists of three kinds of terms: (i) $\tau = \sigma = \mathbb{1}$; (ii) $\tau = \mathbb{1}, \sigma \neq \mathbb{1}$; (iii) $\tau \neq \mathbb{1}$. This leads to the following inequality:

$$\begin{aligned} |Q_k(s) - P_k(s)| &\leq |W(\mathbb{1}, D) - D^{-k}| \text{tr}(B_s) + \sum_{\sigma \neq \mathbb{1}} |W(\sigma^{-1}, D)| |\text{tr}(A_s \sigma)| \text{tr}(B_s) \\ &\quad + \sum_{\tau \neq \mathbb{1}} \sum_{\sigma} |W(\tau \sigma^{-1}, D)| |\text{tr}(A_s \sigma)| |\text{tr}(B_s \tau^{-1})| \end{aligned} \quad (21)$$

$$\leq \left[|W(\mathbb{1}, D) - D^{-k}| + \sum_{\nu \neq \mathbb{1}} |W(\nu, D)| \right] \text{tr}(B_s) + \sum_{\nu} |W(\nu, D)| \sum_{\tau \neq \mathbb{1}} |\text{tr}(B_s \tau^{-1})|. \quad (22)$$

In the second step we have used $|\text{tr}(A_s \sigma)| \leq 1$. Carrying the sum over s and using known properties of the Weingarten function⁴⁷, for $k < (2^\ell / \sqrt{6})^{4/7}$ we obtain

$$\delta(P_k, Q_k) \equiv \sum_s |Q_k(s) - P_k(s)| \leq c_1 + c_2 T \quad (23)$$

with

$$T = \frac{1}{D^k} \sum_{\tau \neq \mathbb{1}} \sum_s |\text{tr}(B_s \tau^{-1})| \quad (24)$$

and coefficients $c_1 = \mathcal{O}\left(\frac{k^{7/2}}{D^2}\right)$, $c_2 = 1 + \mathcal{O}\left(\frac{k^2}{D}\right)$. The remaining task is to bound T . T contains a product of matrix elements of the form

$$M_{ji} = \langle y_{s_0, s_1, \dots, s_i}^i | y_{s_0, s_1, \dots, s_j}^j \rangle \quad (25)$$

For example, for $k = 8$, $\tau = (175462)(3)(8)$ which maps 175462 cyclically to 754621 and preserves 3, 8), we have $|\text{tr}(B_s \tau^{-1})| = |M_{71} M_{57} M_{45} M_{64} M_{26} M_{12}| \prod_{i=1}^8 \lambda_{s_0, s_1, \dots, s_i}^i$. Because of the absolute value, we cannot directly carry the summation over s . However, we can decompose this string into two segments and use the simple inequality $2|ab| \leq |a|^2 + |b|^2$. By carefully choosing the segments, we prove that the sum over s can now be carried using the completeness condition, and the adaptiveness does not cause a problem because one can always start the sum from the latest index s_k . Using this method we obtain

$$T \leq \frac{k^3}{D} + \frac{k^2}{D} + \mathcal{O}\left(\frac{k^5}{D^2}\right). \quad (26)$$

Using Eq. (23) this proves the bound (18) with $c_2 T$ the dominant term.

The remaining task is to prove that a general incoherent QUALM (Fig. 2(b)) cannot do better than SM QUALM. Here we will only provide an intuitive explanation of the idea, leaving more details in the Supplementary Information. In a general incoherent QUALM, multiple rounds of classical communication occur between L and W between two applications of the lab oracle. If we consider a case when the communication is only one way from L to W , then it is equivalent to a sequence of weak measurements, followed by a projective measurement in a complete basis. One can always consolidate all these measurements into a single POVM that is in the form of the one we have in SM QUALM. The problem becomes more nontrivial because there are communication from W to L , which measures the state of W , and tells L to apply a quantum channel determined by the measurement output. More precisely, the measurement corresponds to a family of CP maps \mathcal{M}_ν^W . For a state ρ_W , the measurement output ν has probability $p_\nu = \text{tr}(\mathcal{M}_\nu^W(\rho_W))$. When the measurement output is ν , a quantum channel \mathcal{N}_ν^L is applied to L . The key idea is that this procedure can always be replaced by a deterministic (i.e., classical) computation based on previous measurement results and some random numbers. In other words, even if W is a quantum computer, since it is only allowed to send classical information to L , it can be simulated by a classical computer with random number generators. Consequently, we can replace all W to L one-way LOCC by deterministic instructions with random number inputs. Then for fixed values of these random numbers, what happens to L is just some quantum channels applied between weak measurements. In this case the consolidation can be done to reduce the QUALM to an SM QUALM. This establishes that a general incoherent QUALM is equivalent to a classical probabilistic average over SM QUALMs. Since the probabilistic average cannot perform better than the best SM QUALM, we have proved Theorem 1.

Data availability

No data was collected for this work.

Received: 12 May 2021; Accepted: 14 December 2021;

Published online: 16 February 2022

References

- D'Ariano, G. M., Paris, M. G. & Sacchi, M. F. Quantum tomography. *Adv. Imaging Electron Phys.* **128**, 206–309 (2003).
- Bae, J. & Kwak, L. C. Quantum state discrimination and its applications. *J. Phys. A: Math. Theor.* **48**, 083001 (2015).
- Jacobs, K. Quantum measurement theory and its applications. (Cambridge University Press, 2014).
- Gross, D., Liu, Y. K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105**, 150401 (2010).
- Flammia, S. T., Gross, D., Liu, Y. K. & Eisert, J. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators. *N. J. Phys.* **14**, 095022 (2012).
- Kueng, R., Rauhut, H. & Terstiege, U. Low rank matrix recovery from rank one measurements. *Appl. Comput. Harmonic Anal.* **42**, 88–116 (2017).
- Riofrio, C. A. et al. Experimental quantum compressed sensing for a seven-qubit system. *Nat. Commun.* **8**, 1–8 (2017).
- Aaronson, S. Shadow tomography of quantum states. *SIAM J. Comput.* **49**, STOC18–368 (2019).
- Cotler, J. & Wilczek, F. Quantum overlapping tomography. *Phys. Rev. Lett.* **124**, 100401 (2020).
- Evans, T. J., Harper, R. & Flammia, S. T. Scalable Bayesian Hamiltonian learning. Preprint at <https://arxiv.org/abs/1912.07636> (2019).
- Huang, H.-Y., Kueng, R. & Preskill, J. Predicting many properties of a quantum system from very few measurements. *Nat. Phys.* **16**, 1050–1057 (2020).
- Yu, N. Sample efficient tomography via Pauli Measurements. Preprint at <https://arxiv.org/abs/2009.04610> (2020).
- Kok, P., Braunstein, S. L. & Dowling, J. P. Quantum lithography, entanglement and Heisenberg-limited parameter estimation. *J. Opt. B: Quantum Semiclass. Opt.* **6**, S811 (2004).
- Schmitt, S. et al. Submillihertz magnetic spectroscopy performed with a nanoscale quantum sensor. *Science* **356**, 832–837 (2017).
- Arrad, G., Vinkler, Y., Aharonov, D. & Retzker, A. Increasing sensing resolution with error correction. *Phys. Rev. Lett.* **112**, 150801 (2014).
- Dür, W., Skotiniotis, M., Froewis, F. & Kraus, B. Improved quantum metrology using quantum error correction. *Phys. Rev. Lett.* **112**, 080801 (2014).
- Ozeri, R. Heisenberg limited metrology using quantum error-correction codes. Preprint at <https://arxiv.org/abs/1310.3432> (2013).
- Kessler, E. M., Lovchinsky, I., Sushkov, A. O. & Lukin, M. D. Quantum error correction for metrology. *Phys. Rev. Lett.* **112**, 150802 (2014).
- Zhou, S., Zhang, M., Preskill, J. & Jiang, L. Achieving the Heisenberg limit in quantum metrology using quantum error correction. *Nat. Commun.* **9**, 1–11 (2018).
- Aharonov, D., Ben-Or, M., Eban, E. & Mahadev, U. Interactive proofs for quantum computations. Preprint at <https://arxiv.org/abs/1704.04487> (2017).
- Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. 517–526 (IEEE, 2009).
- Gheorghiu, A., Kapourniotis, T. & Kashefi, E. Verification of quantum computation: An overview of existing approaches. *Theor. Comput. Syst.* **63**, 715–808 (2019).
- Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456–460 (2013).
- Atia, Y. & Aharonov, D. Fast-forwarding of Hamiltonians and exponentially precise measurements. *Nat. Commun.* **8**, 1–9 (2017).
- Hayden, P. & Preskill, J. Black holes as mirrors: quantum information in random subsystems. *J. High Energy Phys.* **2007**, 120 (2007).
- Bernstein, E. & Vazirani, U. Quantum complexity theory. *SIAM J. Comput.* **26**, 1411–1473 (1997).
- Gharibian, S., Huang, Y., Landau, Z. & Shin, S. W. Quantum Hamiltonian complexity. *Foundations and Trends in Theoretical Computer Science* **10.3**, 159–282 (2015).
- Cotler, J., Jian, C. M., Qi, X. L. & Wilczek, F. Superdensity operators for spacetime quantum mechanics. *J. High Energy Phys.* **2018**, 93 (2018).
- Gutoski, G. & Watrous, J. Toward a general theory of quantum games. In *Proceedings of the Thirty-ninth annual ACM symposium on Theory of Computing*. 565–574 (2007).
- Chiribella, G., D'Ariano, G. M. & Perinotti, P. Quantum circuit architecture. *Phys. Rev. Lett.* **101**, 060401 (Association for Computing Machinery, 2008).
- Childs, A. M., Harrow, A. W. & Wocjan, P. Weak Fourier-Schur sampling, the hidden subgroup problem, and the quantum collision problem. In *Annual Symposium on Theoretical Aspects of Computer Science*. 598–609 (Springer, Berlin, Heidelberg, 2007).
- Bubeck, S., Chen, S. & Li, J. Entanglement is necessary for optimal quantum property testing. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*. 692–703 (IEEE, 2020).
- Simon, D. R. On the power of quantum computation. *SIAM J. Comput.* **26**, 1474–1483 (1997).
- Chia, N. H., Chung, K. M. & Lai, C. Y. On the need for large quantum depth. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. 902–915 (Association for Computing Machinery, 2020).
- Coudron, M. & Menda, S. Computations with greater quantum depth are strictly more powerful (relative to an oracle). In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. 889–901 (Association for Computing Machinery, 2020).
- Haah, J., Harrow, A. W., Ji, Z., Wu, X. & Yu, N. Sample-optimal tomography of quantum states. *IEEE Trans. Inf. Theor.* **63**, 5628–5641 (2017).
- O'Donnell, R. & Wright, J. Efficient quantum tomography. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 899–912 (Association for Computing Machinery, 2006).
- Radhakrishnan, J., Rötteler, M. & Sen, P. Random measurement bases, quantum state distinction and applications to the hidden subgroup problem. *Algorithmica* **55**, 490–516 (2009).
- Ettinger, M., Hoyer, P. & Knill, E. The quantum query complexity of the hidden subgroup problem is polynomial. *Inf. Process. Lett.* **91**, 43–48 (2004).
- Bacon, D., Childs, A. M. & van Dam, W. Optimal measurements for the dihedral hidden subgroup problem. Preprint at <https://arxiv.org/abs/0501044> (2005).
- Huang, H.-Y., Kueng, R. & Preskill, J. Information-theoretic bounds on quantum advantage in machine learning. *Physical Review Letters* **126**, 190505 (2021).
- Harrow, A. W., Hassidim, A., Leung, D. W. & Watrous, J. Adaptive versus nonadaptive strategies for quantum channel discrimination. *Phys. Rev. A* **81**, 032339 (2010).
- Gharibian, S., Piddock, S. & Yirka, J. Oracle complexity classes and local measurements on physical Hamiltonians. *Proceedings of the 37th Symposium on Theoretical Aspects of Computer Science (STACS)*, 2020.
- Arora, S. & Barak, B. *Computational complexity: a modern approach* (Cambridge University Press, 2009).
- Papadimitriou, C. *Computational Complexity* (Addison-Wesley, 1994).
- Chitambar, E., Leung, D., Mančinska, L., Ozols, M. & Winter, A. Everything you always wanted to know about LOCC (but were afraid to ask). *Commun. Math. Phys.* **328**, 303–326 (2014).
- Collins, B. & Matsumoto, S. Weingarten calculus via orthogonality relations: new applications. Preprint at <https://arxiv.org/abs/1701.04493> (2017).

Acknowledgements

We would like to thank I. Cirac, P. Hayden, F. Hernandez, N. Hunter-Jones, A. Kitaev, H.-H. Lin, D. Ranard, S. Sachdev, and R. de Wolf, for valuable discussions. D.A. is supported by ISF grant number 0399494-1721/17, by Simons grant number 385590, and by Quantum ISF grant number 2137/19. J.C. is supported by a Junior Fellowship from the Harvard Society of Fellows and the U.S. Department of Energy under grant Contract Number DE-SC0012567; part of this work was completed with support from the Fannie and John Hertz Foundation and the Stanford Graduate Fellowship program. X.L.Q. is supported by the Simons Foundation, and in part by the DOE Office of Science, Office of High Energy Physics, the grant de-sc0019380. D.A., J.C., and X.L.Q. all developed the theoretical results and co-wrote the paper.

Author contributions

D.A., J.C., and X.L.Q. participated equally in developing the QUALM framework, proving the key theorems, and writing the paper.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41467-021-27922-0>.

Correspondence and requests for materials should be addressed to Jordan Cotler.

Peer review information *Nature Communications* thanks the anonymous reviewer(s) for their contribution to the peer review of this work.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2022