Quantum Algorithmic Measurement

Extended Abstract

Dorit Aharonov[1,a], Jordan Cotler[2,3,b], Xiao-Liang Qi[3,c]

[1] *School of Computer Science and Engineering, The Hebrew University of Jerusalem,*
The Edmond J. Safra Campus, 9190416 Jerusalem, Israel

[2] *Society of Fellows, Harvard University, Cambridge, MA 02138 USA*

[3] *Stanford Institute for Theoretical Physics, Stanford University,*
Stanford, CA 94305 USA

[a]doria@cs.huji.ac.il, [b]jcotler@fas.harvard.edu, [c]xlqi@stanford.edu

Abstract

Can quantum computational tools enhance the precision and efficiency of physical experiments? Promising examples are known, but a systematic treatment and comprehensive framework are missing. We introduce Quantum Algorithmic Measurements (QUALMs) to enable the study of quantum measurements and experiments from the perspective of computational complexity and communication complexity. The measurement process is described, in its utmost generality, by a many-round quantum interaction protocol between the experimental system and a full-fledged quantum computer. The QUALM complexity is quantified by the number of elementary operations performed by the quantum computer, including its coupling to the experimental system.

We study how the QUALM complexity depends on the type of allowed access the quantum computer has to the experimental system: local-local, incoherent, coherent, adaptive, etc. We provide the first example of a measurement "task" for which the coherent QUALM complexity is exponentially better than the incoherent one, even if the latter is adaptive; this implies that using entanglement between different systems in experiments may lead to exponential savings in resources. We extend our results to derive a similar exponential advantage for a physically motivated measurement task which determines the symmetry class of the time evolution operator for a quantum many-body system.

Many open questions are raised towards better understanding how quantum computational tools can be applied in experimental physics. A major question is whether an exponential advantage in QUALM complexity can be achieved in the NISQ era; an equally important one is to design new, efficient quantum algorithmic measurements based on our framework, perhaps relying on ideas from quantum algorithms.

QUALMs and Lab Oracles. Since the early days of physics, innovative methods have been invented to interrogate physical systems via *experiments*. Over the past two decades, 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. This body of work constitutes strong evidence that leveraging *quantum computational resources* to manipulate and measure physical systems may dramatically enhance experimental capabilities. But what is the general scope of leveraging quantum computers for experiments? And what are the limitations of such protocols? We will argue that these developments both challenge and clarify the paradigm of experimentation itself, and its relation to computation. Accordingly, we will develop a computational framework for the most general kind of quantum experiment which can be implemented in the physical world. Based on the *quantum Church Turing thesis* [3] we argue

- Quantum measurements should be viewed as a generalization of quantum algorithms. They can be studied and designed abstractly, using gates and circuits.
- In this terminology one can study the *computational complexity* of quantum measurements, as an extension of the way the computational complexity of quantum algorithms is studied.

We thus make use of the language of *computational complexity* and *communication complexity* to define an abstract model of general quantum measurements, which we call *quantum algorithmic measurements* or QUALMs. Using this terminology, we initiate the systematic study of quantum experiments from a complexity-theoretic point of view. Initial seeds for such an approach were given in [1, 4].

For example, consider an X-ray diffraction experiment, performed to determine the crystal structure of a material. It consists of the crystal sample, X-ray photons which exhibit an electromagnetic interaction with the crystal, and a camera and other lab equipment which only interact with the photons (see Figure 1(b)).

This is a very general situation: in a physical experiment, the experimentalist can never fully interact with all degrees of freedom of the physical system she wants to measure. We model our experimental system as consisting of three subsystems (registers): "Nature", denoted by N, which we view as the register that Nature holds secretly, and we have no direct access to it (this is the crystal in the above example). Our apparatus which couples to N is contained in the lab system L (this includes the photons in our example). We additionally have access to a working space system W which we can leverage to perform processing of our quantum data (these are the camera and the data processors in our example). The basic idea is that we can make measurements to read out information from L and W, but not directly from N. In the language of theoretical computer science, an experiment can be viewed as an interactive protocol with Nature (see Figure 1(a)) with interlacing rounds of interactions of two types: one between N and L and the other consisting of a general quantum computation applied on L and W. With this picture in mind, we now introduce the main players in our theory: Lab oracles, QUALMs, and Tasks.

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

Definition 2. *(Roughly) A* $\mathsf{QUALM(N,L,W)}$ *is a specification of a sequence of gates on the subsystems* L, W*, interlaced with applications of the lab oracle superoperator on* N, L*. Some of the qubits in registers* W *are marked as "inputs" and some as "outputs".*

Definition 3. *(Roughly) A task is a tuple* $\mathsf{Task} = (\boldsymbol{S}_{in}, \boldsymbol{S}_{out}, f, \mathcal{G})$*, associated with a given system* $\boldsymbol{N}\otimes\boldsymbol{L}\otimes\boldsymbol{W}$*. Here,* $\boldsymbol{S}_{in}$ *is a p-qubit subsystem of* $\boldsymbol{W}$*,* $\boldsymbol{S}_{out}$ *is a q-qubit subsystem of* $\boldsymbol{W}$*, f is a function*

$$f : \{\mathsf{LO}_0, \mathsf{LO}_1, \mathsf{LO}_2, ...\} \times \{0,1\}^p \longrightarrow \{0,1\}^q\,,$$

and $\mathcal{G}$ *is a set of admissible gates on* $\boldsymbol{L}\otimes\boldsymbol{W}$*. In the domain of f,* $\{\mathsf{LO}_0, \mathsf{LO}_1, \mathsf{LO}_2, ...\}$ *is a set of lab oracles.*

The Task should be viewed as a problem to be solved; a QUALM, as one solution. The computational complexity of the task is that of the most efficient QUALM that achieves it; the QUALM complexity is measured by counting both gates and applications of the lab oracle (queries). A key point is that the physical system is viewed as *input*, though the QUALM is given only *indirect access* to it; the QUALM then computes a function of this physical system.

Exponential separation between coherent and incoherent QUALMs. One basic question is what is the true advantage of allowing our experiments to use full fledged quantum computers. To study this, we can imagine a *hierarchy* of types of accesses to the lab oracle. The most classical access is one in which both state preparation and final measurement are in the computational basis; next in line would be *local-local* QUALMs in which input states and outcome measurement bases must be tensor product vectors; next are single register, non adaptive QUALMs, which allow many parallel independent access to different applications of the lab oracle in a general basis, with postprocessing; allowing adaptive preparations and measurements, we get (roughly) what we call *incoherent* QUALMs which are very general except they prevent coherence both between the lab oracle and the working register, as well as between different applications of the lab oracle (we define them using LOCC protocols). The most quantum (and most general) would be *coherent* QUALMs, which allow unrestricted, entangled usage of a full fledged quantum computers interacting with the lab oracle.

Does coherent access to the physical system buy us an exponential advantage? At first glance, the answer might seem obviously positive, due to famous quantum oracle algorithms such as Simon's [9]. Interestingly, however, Simon's algorithm is achieved without any need for coherent access to the (classical) oracle! Applying the oracle to a product state, measuring in a product (Hadamard) basis, and applying classical post-processing on the result are sufficient. Thus, this algorithm is "local-local", and sits quite *low* in the hierarchy of "quantumness" in accessing the oracle.

Our main result is an example of an experiment which provably provides an *exponential* advantage of coherent over incoherent (even adaptive) access to the lab oracle, suggested by the above question. We prove this first for the following problem, which can be motivated, physically, by the attempt to distinguish a Floquet system from a Brownian circuit (roughly speaking, a fixed Hamiltonian versus a time-dependent, random Hamiltonian):

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 random unitary, remembers it (forever), and then subsequently applies that same unitary to* $\boldsymbol{L}$ *each time the oracle is called. By contrast, the second lab oracle* LO_1 *applies a new random unitary to* $\boldsymbol{L}$ *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. However:

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., L has ℓ qubits), its QUALM complexity is lower bounded by an exponential in ℓ.*

We construct a fairly straightforward proof of the above theorem for non-adaptive protocols; the argument becomes far more complicated in the adaptive case, and this is our main technical contribution. We use Weingarten functions and a substantial dose of combinatorics to arrive at our desired result.

While there are many other known results which can be viewed as suggesting related advantages, to the best of our knowledge all previous results fall short of addressing the above question (see Table 1); they either offer only a quadratic advantage in QUALM complexity, and only under the strong assumption of non-adaptive access [6, 7], or their exponential lower bound is only conjectured (e.g., [5, 8]). The example most closely related to our work is [2], which provides a proven exponential advantage of coherent versus the single register access, for a quantum state distinction problem emerging from the dihedral HSP. 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). Our work is thus the first to demonstrate an exponential advantage in QUALM complexity of coherent over incoherent access QUALMs, when no restriction (including non-adaptiveness) is placed on the incoherent access; moreover, this exponential advantage is achieved using an efficient (and in fact, extremely simple) coherent QUALM, based solely on the swap test. Our work suggests that coherence could be an immense resource in quantum experiments.

We next turn to another physically-motivated task:

Definition 5. (The Symmetry Distinction Problem) *Distinguish with non-negligible success probability between three classes of lab oracles: (i) a lab oracle which applies a fixed Haar-random* **unitary** *to the L system; (ii) a lab oracle which applies a fixed Haar-random* **orthogonal** *matrix to the system; (iii) a lab oracle which applies a fixed Haar-random* **symplectic** *matrix to the system. (Suppose that 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 exponential.

Discussion. Our motivation in this work is Physics. We give the first proof that entanglement is truly *exponentially* advantageous when performing *measurements in the lab.* We note that this exponential advantage is fundamentally new, and is very different from the usual exponential advantage of quantum algorithms, e.g. Simon's algorithm. Looking forward, our framework and methods will be essential to the analysis and development of experimental techniques leveraging quantum computation, and raise many open questions; most importantly, if such exponential advantages can be exhibited in the NISQ era.

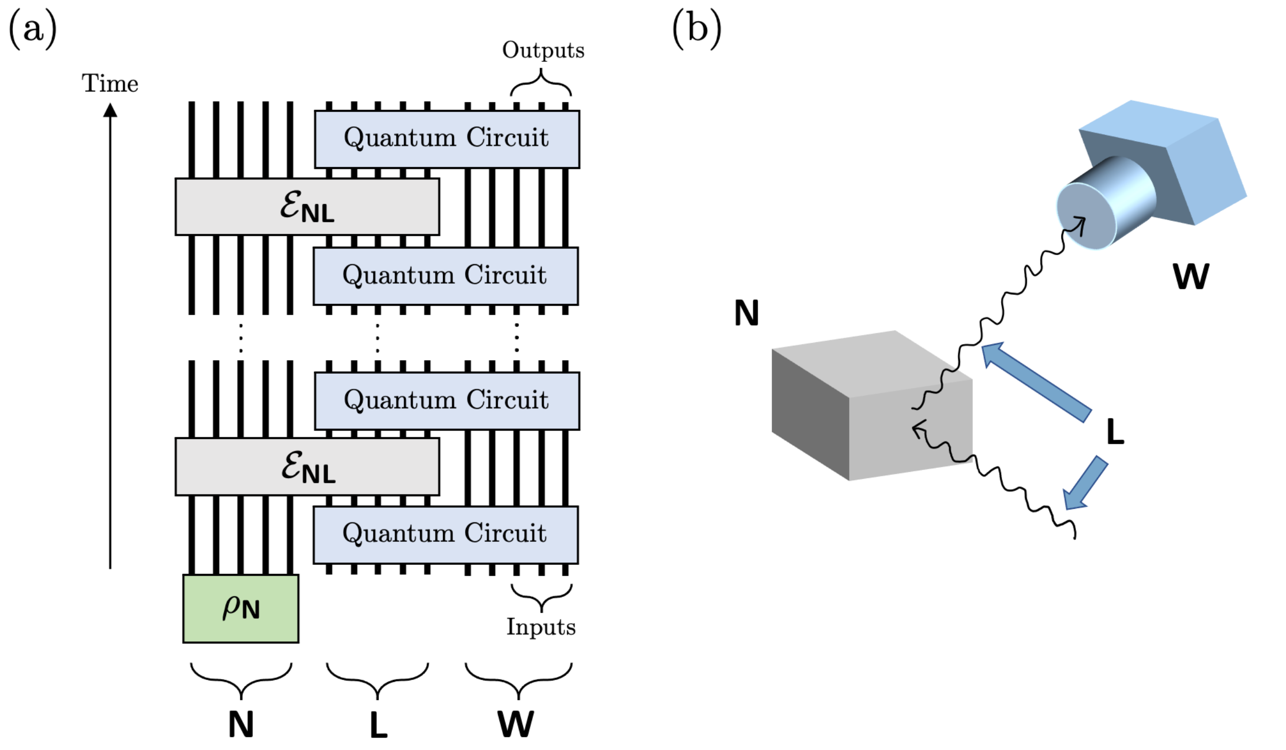

Figure 1: (a) Schematic illustrating the structure of a QUALM as an interaction between Nature and the experimentalist's controlled degrees of freedom. Here N represents the 'Nature' register, L is the 'lab' register, and W is the 'working space' register. The experimentalist does not have direct measurement 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. (b) 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.

Oracle/ access	Binary	Local-local	Single register	Incoherent access	Coherent Access
Classical		Simon's algorithm* [9]	Dihedral, Affine and Heisenberg HSP [8] Conjectured exponential advantage over binary	?	HSP for general groups [5] Conjectured exponential advantage over binary
Quantum		?	?	?	State tomography: quadratic query advantage over single register [6,7] Exponential query advantage in distinguishing coset states for the dihedral group over (*non-adapative*) single register [2] **This work***: Exponential advantage over (*adaptive*) incoherent access

Table 1: Comparison to known results with different access types to the lab oracles. The meaning of the rows and columns is explained in the text. We put an asterisk $(*)$ when *both* the query complexity and gate complexity of the protocol are efficient. All other results are only known to be efficient in terms of query complexity, and not gate complexity. Note that our work is the first to demonstrate a provable exponential advantage separating coherent from incoherent adaptive access; moreover, the coherent QUALM is efficient.

References

[1] Atia, Y., & Aharonov, D. (2017). Fast-forwarding of Hamiltonians and exponentially precise measurements. *Nature Communications*, 8(1), 1-9.

[2] Bacon, D., Childs, A. M., & van Dam, W. (2005). Optimal measurements for the dihedral hidden subgroup problem. *quant-ph/0501044*.

[3] Bernstein, E., & Vazirani, U. (1997). Quantum complexity theory. *SIAM Journal on Computing*, 26(5), 1411-1473.

[4] Cotler, J., Jian, C. M., Qi, X. L., & Wilczek, F. (2018). Superdensity operators for spacetime quantum mechanics. *Journal of High Energy Physics*, 2018(9), 93.

[5] Ettinger, M., Høyer, P., & Knill, E. (2004). The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1), 43-48.

[6] Haah, J., Harrow, A. W., Ji, Z., Wu, X., & Yu, N. (2017). Sample-optimal tomography of quantum states. *IEEE Transactions on Information Theory*, 63(9), 5628-5641.

[7] O'Donnell, R., & Wright, J. (2016, June). Efficient quantum tomography. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing* (pp. 899-912).

[8] Radhakrishnan, J., Rötteler, M., & Sen, P. (2009). Random measurement bases, quantum state distinction and applications to the hidden subgroup problem. *Algorithmica*, 55(3), 490-516.

[9] Simon, D. R. (1997). On the power of quantum computation. *SIAM Journal on Computing*, 26(5), 1474-1483.