Computational Advantage from Quantum-Controlled Ordering of Gates

Mateus Araújo,[1,2,*] Fabio Costa,[1,2] and Časlav Brukner[1,2]
[1]Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria
[2]Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

(Received 5 August 2014; revised manuscript received 6 October 2014; published 18 December 2014)

It is usually assumed that a quantum computation is performed by applying gates in a specific order. One can relax this assumption by allowing a control quantum system to switch the order in which the gates are applied. This provides a more general kind of quantum computing that allows transformations on blackbox quantum gates that are impossible in a circuit with fixed order. Here we show that this model of quantum computing is physically realizable, by proposing an interferometric setup that can implement such a quantum control of the order between the gates. We show that this new resource provides a reduction in computational complexity: we propose a problem that can be solved by using $O(n)$ blackbox queries, whereas the best known quantum algorithm with fixed order between the gates requires $O(n^2)$ queries. Furthermore, we conjecture that solving this problem in a classical computer takes exponential time, which may be of independent interest.

DOI: 10.1103/PhysRevLett.113.250402 PACS numbers: 03.67.Ac, 03.65.Ta, 03.67.Lx

A useful tool to calculate the complexity of a quantum algorithm is the blackbox model of quantum computation. In this model, the input to the computation is encoded in a unitary gate—treated as a blackbox—and the complexity of the algorithm is the number of times this gate has to be queried to solve the problem.

Typically, blackbox computation is studied within the quantum circuit formalism [1]. A quantum circuit consists of a collection of wires, representing quantum systems, that connect boxes, representing unitary transformations. In this framework, wires are assumed to connect the various gates in a fixed structure; thus, the order in which the gates are applied is determined in advance and independently of the input states. It was first proposed in Ref. [2] that such a constraint can be relaxed: one can consider situations where the wires, and thus the order between gates, can be controlled by some extra variable. This is natural if one thinks of the circuit's wires as quantum systems that can be in superposition.

Such "superpositions of orders" allow performing information-theoretical tasks that are impossible in the quantum circuit model: it was shown in Ref. [3] that it is possible to decide whether a pair of blackbox unitaries commute or anticommute with a single use of each unitary, whereas in a circuit with a fixed order at least one of the unitaries must be used twice. (The same task was considered in a quantum optics context in Ref. [4], where a less efficient protocol was found.)

It was not known, however, whether this advantage can be translated into more efficient algorithms for quantum computing, i.e., if a quantum computer that can control the order between gates can solve a computational problem with asymptotically less resources than a quantum computer with fixed circuit structure.

Here we present such a problem: given a set of n unitary matrices and the promise that they satisfy one out of $n!$ specific properties, find which property is satisfied. The essential resource to solve this problem is the quantum control over the order of n blackboxes, first introduced in Ref. [5]. We show that, by using this resource, the problem can be solved with $O(n)$ queries to the blackboxes, while the best known algorithm with fixed order requires $O(n^2)$ queries. Furthermore, while both quantum methods of solving the problem run in polynomial time, the best known classical algorithm to solve it runs in exponential time, which may be of independent interest.

We further discuss a possible interferometric implementation of the protocol. For the superposition of the order of just two gates, a realization with current quantum optics techniques is possible. For a higher number of gates, practical implementations become more challenging.

Algorithm.—The quantum control of the order between n unitary gates can be formalized by introducing the n-SWITCH gate. As in Ref. [5], we consider a d-dimensional target system, initialized in some state $|\psi\rangle$, and an $n!$-dimensional control system. Let $\{U_i\}_0^{n-1}$ be a set of unitaries and

$$\Pi_x = U_{\sigma_x(n-1)} \ldots U_{\sigma_x(1)} U_{\sigma_x(0)} \tag{1}$$

for some permutation σ_x, where $x = 0, \ldots, n! - 1$ is a chosen labeling of permutations [6]. Then the n-SWITCH S_n is a controlled quantum gate: its effect is to apply the product of unitaries Π_x to the state $|\psi\rangle$ conditioned on the value of the control register $|x\rangle$. In symbols,

$$S_n|x\rangle|\psi\rangle = |x\rangle\Pi_x|\psi\rangle. \tag{2}$$

Using this gate we can introduce an algorithm that exploits the quantum control of orders to achieve a reduction in query complexity for the solution of a specific problem. The algorithm is based on the standard Hadamard test. The idea is to initiate the control system in a state corresponding to a uniform superposition of all permutations, apply S_n, and then measure the control system in the Fourier basis. With a suitable choice of the unitaries, we can make the result of this measurement deterministic, and, since there are $n!$ different results, this means that we can differentiate between $n!$ different properties of n unitaries.

To be more precise, let $\omega = e^{i(2\pi/n!)}$. We say that the set of unitaries $\{U_i\}_0^{n-1}$ has property $\mathbf{P}_y$ if it is true that

$$\forall x, \qquad \Pi_x = \omega^{xy}\Pi_0, \tag{3}$$

for the given y. For example, property $\mathbf{P}_0$ is the property that $\Pi_x = \Pi_0$ for all x, i.e., that all the matrices commute with each other.

Note that it is not possible to satisfy property $\mathbf{P}_1$ if the dimension of the unitaries d is less than $n!$. To see that, consider $x = y = 1$, and take the determinant on both sides of Eq. (3):

$$\det \Pi_1 = \omega^d \det \Pi_0. \tag{4}$$

Since $\det \Pi_x = \det \Pi_0$, it follows that $\omega^d = 1$, and therefore d must be at least $n!$.

The computational problem is defined as follows: given a set $\{U_i\}_0^{n-1}$ of unitary matrices of dimension $d \geq n!$, decide which of the properties $\mathbf{P}_y$ is satisfied by this set, given the promise that one of these $n!$ properties is satisfied.

The protocol for solving this problem is the following: we initialize the target system in *any* state $|\psi\rangle$ and the control system in the state $|C\rangle$ which corresponds to an equal superposition of all permutations:

$$|C\rangle|\psi\rangle = \frac{1}{\sqrt{n!}}\sum_{x=0}^{n!-1}|x\rangle|\psi\rangle. \tag{5}$$

Then, we apply the n-SWITCH:

$$S_n|C\rangle|\psi\rangle = \frac{1}{\sqrt{n!}}\sum_{x=0}^{n!-1}|x\rangle\Pi_x|\psi\rangle. \tag{6}$$

Now we apply the Fourier transform over $\mathbf{Z}_{n!}$ to our control qudit

$$\mathcal{F}_{n!}S_n|C\rangle|\psi\rangle = \frac{1}{n!}\sum_{x,s=0}^{n!-1}|s\rangle\omega^{-xs}\Pi_x|\psi\rangle \tag{7}$$

and measure the control qudit in the computational basis, with outcome probabilities

$$p_s = \frac{1}{n!^2}\left\|\sum_{x=0}^{n!-1}\omega^{-xs}\Pi_x|\psi\rangle\right\|^2. \tag{8}$$

Using the promise $\Pi_x = \omega^{xy}\Pi_0$, we get that

$$p_s = \frac{1}{n!^2}\left\|\sum_{x=0}^{n!-1}\omega^{x(y-s)}\Pi_0|\psi\rangle\right\|^2 = \delta_{sy}; \tag{9}$$

that is, if property $\mathbf{P}_y$ is true, the result of the measurement is going to be y with probability one, so we can find out which property the unitaries have in a single run of the protocol.

We should notice that the problem is not trivial; i.e., there exist, for every n, infinitely many sets of unitary matrices that satisfy each of the $n!$ properties $\mathbf{P}_y$ (see Sec. 1 of Supplemental Material [7]). The problem, and the corresponding protocol, can be also modified to tolerate possible experimental error. This modification is shown in Sec. 2 of Supplemental Material [7].

Query complexity.—We are interested in determining the number of times that the unitaries U_i must be used to run the algorithm. Clearly, this depends only on the implementation of the n-SWITCH gate, since the unitaries are not used anywhere else. As proposed in [2], the SWITCH can, in principle, be implemented by adding quantum control to the connections between the unitaries. In such an implementation, it is sufficient to use a single copy of each unitary, while the control system determines the order in which the target system passes through the unitaries.

Since the implementation with quantum control of the connections between gates is explicitly outside the quantum circuit formalism, we cannot simply calculate the number of uses of the unitaries by counting the number of times they appear in a circuit. Nevertheless, we can formulate the notion of "gate uses" in a precise, operational, way. Imagine we append, to each gate, an additional "flag" quantum system that counts the number of times that gate is used. This can be done in a reversible way: the jth flag is initialized in the state $|0\rangle_j$ and, whenever the unitary U_j is used, it is updated through the unitary transformation $|f\rangle_j \to |f+1\rangle_j$. It is easy to see that, after applying the n-SWITCH, the state of the flags factorizes, with each flag in the state $|1\rangle_j$. According to this definition, the total number of queries necessary to run the algorithm is n.

In comparison, the optimal simulation of the n-SWITCH gate with a fixed circuit has query complexity $\Omega(n^2)$ [8]. To see this, first note that one can assume without loss of generality that all blackbox unitaries are applied each in a different time step, since, if two blackboxes are applied in parallel, we can always introduce a time delay between them, without changing the action of the circuit. More technically, a circuit defines a partial order for its gates, which can always be completed into a total order. Then, let $\{A_i\}_0^{m-1}$ be the m blackbox unitaries appearing in the

circuit, with $A_j \in \{U_i\}_0^{n-1}$, queried in the order $A_0 \preceq \cdots \preceq A_{m-1}$. From Appendix B of Ref. [2], it follows that it is possible to apply the Π_x to $|\psi\rangle$ only if the unitaries $U_{\sigma_x(0)}, \ldots, U_{\sigma_x(n-1)}$ are present in the circuit in the order defined by σ_x. The lower bound on the query complexity is then the minimal m for which all $n!$ permutations of $\{U_0, \ldots, U_{n-1}\}$ are present as subsequences of the sequence $\{A_0, \ldots, A_{m-1}\}$.

It turns out that this is an open problem in combinatorics [9,10]. However, it is known that the optimal m respects the bounds

$$n^2 - C_\epsilon n^{7/4+\epsilon} \leq m \leq \left\lceil n^2 - \frac{7}{3}n + \frac{19}{3} \right\rceil$$

for any $\epsilon > 0$, where C_ϵ is a constant that depends on ϵ. This concludes the proof.

It is also possible to construct a quantum circuit that simulates the n-SWITCH gate from such a sequence. We shall, however, refrain from doing so. Instead, for completeness, we present a simple circuit that simulates the n-SWITCH gate using $m = n^2$ queries in Sec. 3 of Supplemental Material [7].

Of course, it might not be necessary to use the n-SWITCH gate in order to determine which property $\mathbf{P}_y$ the unitaries satisfy. For example, it is possible to solve the problem by directly measuring the phase obtained when applying the permutation σ_1. Since $\Pi_1 = \omega^y \Pi_0$, this is sufficient to determine y. However, this protocol can work only if the relative phase is measured with an error smaller than $2\pi/n!$, and for blackbox unitaries this can be done only with an exponential amount of queries.

This is the case, for example, for Kitaev's phase estimation algorithm [11]. This algorithm is not usually applied to blackbox unitaries, but this can be done by using the techniques in [12–14]. In this case, to calculate the phase with the required $O(n \log n)$ bits of precision, one would need to implement the matrices controlled-$U_i^{2^k}$, with $k = 1, \ldots, n \log n$, which would require an exponential amount of queries to the blackboxes U_i. Even if one assumes that it is possible to apply controlled-$U_i^{2^k}$ efficiently—a necessary assumption to make Kitaev's algorithm efficient—one would need $O(n \log n)$ queries to each $U_i^{2^k}$ oracle. Since there are n unitaries U_i, the query complexity would be $O(n^2 \log n)$, which is still less efficient than simulating the n-SWITCH with a fixed circuit.

Running time.—Instead of query complexity, we may want to consider the running time of the algorithm. If we assume that this is dominated by applying the unitaries U_i, then there is no difference between the implementation with superposition of orders or the fixed quantum circuit: both run in time $O(n)$ (see Sec. 3 of Supplemental Material [7]).

It is interesting, nevertheless, to compare the time required to solve the problem between quantum and classical computers. If we assume that the unitaries U_i are decomposed in a polynomial amount of elementary gates, they can be given as an input of polynomial size to a classical algorithm, and it makes sense to compare the classical and quantum running times.

As argued above, the problem of determining y reduces to the problem of calculating the relative phase between Π_1 and Π_0, which may differ by the permutation of a single pair of unitaries. However, as discussed before, the dimension of the unitaries must be at least $n!$ for this problem to be nontrivial, and it seems unlikely that one could extract the phase from these exponentially large unitary matrices on a classical computer in polynomial time. On the other hand, the running time of the quantum algorithm is clearly polynomial for unitaries decomposed in a polynomial amount of elementary gates. Therefore, we conjecture that for the problem presented there is an exponential separation between classical and quantum complexity, which may be of independent interest.

Note that our algorithm is based on the quantum Fourier transform, as are several algorithms that show an exponential separation between classical and quantum complexity, but there does not appear to be a more direct connection with specific classes of quantum algorithms, such as those that solve the hidden subgroup problem (see Sec. 4 of Supplemental Material [7]).

Physical implementation.—In Ref. [2], it was proposed to apply the superposition principle to the physical components of a quantum computer that determine the order between gates. Since this requires a quantum control over macroscopic systems, it seems outside of the reach of current technology and could be practically unfeasible. Here we propose an implementation of the n-SWITCH that, although experimentally challenging, might be feasible.

We first consider an optical implementation of a 2-SWITCH for 2×2 unitaries, illustrated in Fig. 1 (this implementation was independently developed in [15]). The control system is the polarization of a photon and the target system some internal degree of freedom of the same photon, such as space bins, time bins, or angular momentum modes. If the photon is prepared in a horizontally

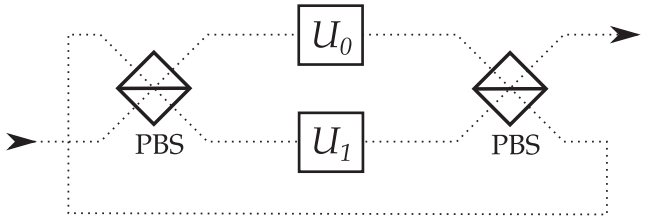

FIG. 1. Linear optical implementation of the 2-SWITCH. The unitaries U_0 and U_1 act on internal degrees of freedom of a single photon, such as space bins, time bins, or angular momentum modes. The polarization state of the photon determines the order in which the unitaries are applied. A photon with polarization $|H\rangle$ is transmitted by the polarizing beam splitters (PBSs), so that U_0 is applied before U_1. For a photon with polarization $|V\rangle$, reflected by the PBSs, U_1 is applied first and U_0 second.

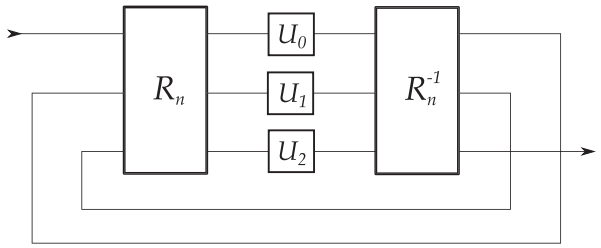

FIG. 2. Implementation of the n-SWITCH (in the figure, $n = 3$). Both the control and target, in state $|x\rangle$ and $|\psi\rangle$, respectively, are encoded in a single (possibly multiparticle) system. When the system enters the n-ROUTERs (R_n) in mode j, it is redirected to mode $\sigma_x(j)$, and the unitary $U_{\sigma_x(j)}$ is applied to $|\psi\rangle$. R_n^{-1} performs the inverse permutation and sends the system to mode $j+1$ of the first router. In this way, a system entering mode 0 of the first router eventually exits mode $n-1$ of the second router with the target in the state $\Pi_x|\psi\rangle$.

polarized state $|H\rangle$, it is transmitted by both PBSs, resulting in the application of the unitary U_0 first and of U_1 second. A photon in a vertically polarized state $|V\rangle$ is reflected by both PBSs; thus, the two unitaries are applied in the reversed order. For an arbitrary polarization state $\alpha|H\rangle + \beta|V\rangle$, the photon exits the interferometer in the state $\alpha|H\rangle U_1 U_0|\psi\rangle + \beta|V\rangle U_0 U_1|\psi\rangle$, which corresponds to the output of the 2-SWITCH.

The extension of this scheme to the general case of an n-SWITCH can be obtained with a generalization of the PBS to an element, which we call the n-ROUTER, with n input modes and n output modes (see Fig. 2). If the control system is in a state $|x\rangle$, the n-ROUTER sends the input mode j to the output mode $\sigma_x(j)$. The unitary $U_{\sigma_x(j)}$ is applied to a system in the mode $\sigma_x(j)$, which then enters a second router that performs the inverse permutation. The output mode j of the second router is then directed to the input mode $j+1$ of the first one. It is straightforward to check that a system entering mode 0 of the first router in the state $|x\rangle|\psi\rangle$ exits mode $n-1$ of the second router in the state $|x\rangle\Pi_x|\psi\rangle$. [In Sec. 5 of Supplemental Material [7], we show how to construct an n-ROUTER with $O(n^2)$ binary routers.]

This higher-dimensional routing can be achieved, for example, with orbital angular momentum of light [16,17]. However, the main limitation of an optical implementation of the n-ROUTER is that it is not scalable in an obvious way, since it requires encoding an exponential number of degrees of freedom in a single photon ($n!$ for the control system and, as argued before, at least $n!$ for the target system). A scalable implementation could be obtained by encoding the degrees of freedom in $O(n \log n)$ particles, each carrying a constant number of degrees of freedom (e.g., one qubit each). The main challenge is then to implement a router that, conditioned on the multiparticle state, coherently directs all the particles in a specific mode. This is, in principle, possible if the particles are bound together, e.g., as atoms in a molecule. Recent progress in matter-wave interferometry suggests that such a quantum control of composite systems could be achievable in the future [18,19].

Other realizations of superposition of orders, based on different models of computation, could also be possible. For example, an implementation of the 2-SWITCH within adiabatic quantum computing was proposed recently [20].

Conclusion.—We have shown that extending the quantum circuit model by allowing quantum control of the order between gates provides a reduction in the number of queries needed to solve a computational problem. Furthermore, we have proposed a physically realizable experimental scheme to implement such a control.

While the reduction is only polynomial, and thus does not create a new complexity class, the result shows that extending the quantum circuit model is possible and can provide a computational advantage. Besides, the computational problem introduced has no known efficient solution by a classical algorithm, which may be of independent interest.

Other extensions of the quantum circuit model of blackbox computation have been proposed [14]: it was shown recently [14,21,22] that a quantum circuit cannot apply blackbox gates conditioned on the state of a control qubit. However, such a control is physically realizable [12,13] and therefore should be allowed by the formalism. It is also intriguing to ask what computational advantages might be achieved once the restrictions imposed by the fixed causal structure of quantum mechanics are relaxed [23].

This work was supported by the Austrian Science Fund (FWF) [Project W1210 Complex Quantum Systems (CoQuS), Special Research Program Foundations and Applications of Quantum Science (FoQuS), and Individual Project No. 24621], the European Commission Project RAQUEL, FQXi, and by the John Templeton Foundation.

*mateus.santos@univie.ac.at

[1] D. Deutsch, Proc. R. Soc. A **425**, 73 (1989).
[2] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Phys. Rev. A **88**, 022318 (2013).
[3] G. Chiribella, Phys. Rev. A **86**, 040301 (2012).
[4] E. Andersson, J. Bergou, and I. Jex, J. Mod. Opt. **52**, 1485 (2005).
[5] T. Colnaghi, G. M. D'Ariano, S. Facchini, and P. Perinotti, Phys. Lett. A **376**, 2940 (2012).
[6] More precisely, $\sigma_x(j)$ is the image of the jth element under the permutation x.
[7] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.250402 for details.
[8] We say that $f(n)$ is $\Omega[g(n)]$ if there exists a constant M such that $f(n) \geq Mg(n)$ for sufficiently large n.
[9] D. Kleitman and D. Kwiatkowski, J. Comb. Theory Ser. A **21**, 129 (1976).
[10] S. Radomirović, Electron. J. Comb. **19**, P31 (2012).
[11] A. Y. Kitaev, arXiv:quant-ph/9511026.

[12] X.-Q. Zhou, T. C. Ralph, P. Kalasuwan, M. Zhang, A. Peruzzo, B. P. Lanyon, and J. L. O'Brien, Nat. Commun. **2**, 413 (2011).
[13] X.-Q. Zhou, P. Kalasuwan, T. C. Ralph, and J. L. O'Brien, Nat. Photonics **7**, 223 (2013).
[14] M. Araújo, A. Feix, F. Costa, and Č. Brukner, New J. Phys. **16**, 093026 (2014).
[15] G. Chiribella, R. Ionicioiu, T. Jennewein, and D. Terno (private communication).
[16] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, Nat. Commun. **4**, 2781 (2013).
[17] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, Phys. Rev. Lett. **105**, 153601 (2010).
[18] M. Arndt, O. Nairz, J. Voss-Andreae, C. Keller, G. van der Zouw, and A. Zeilinger, Nature (London) **401**, 680 (1999).
[19] S. Eibenberger, S. Gerlich, M. Arndt, M. Mayor, and J. Tuxen, Phys. Chem. Chem. Phys. **15**, 14696 (2013).
[20] K. Nakago, M. Hajdušek, S. Nakayama, and M. Murao, arXiv:1310.4061.
[21] A. Soeda (unpublished).
[22] J. Thompson, M. Gu, K. Modi, and V. Vedral, arXiv:1310.2927.
[23] O. Oreshkov, F. Costa, and Č. Brukner, Nat. Commun. **3**, 1092 (2012).