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 of Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

October 21, 2014

It was proposed in [1] to extend the definition of quantum computers by allowing a quantum system to have control over the order that two blackbox gates would be applied. This control can be shown to be impossible to implement with ordinary quantum circuits.

With this new resource 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 structure at least one of the unitaries must be used twice [2].

It was still unknown whether this resource could provide for a reduction in complexity for solving a computational problem. Using the generalization to n blackboxes proposed in [3], we show a problem that can be solved with $O(n)$ queries to the blackboxes, whereas the best known algorithm with fixed order requires $O(n^2)$ queries.

The quantum control of the order between n unitary gates can be formalized by introducing the n-SWITCH gate. Let $\{U_i\}_0^{n-1}$ be a set of unitaries and

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

for some permutation σ_x, where x is a chosen labelling of permutations. Then the n-SWITCH gate S_n is a controlled quantum gate, defined by

$$S_n|x\rangle|\psi\rangle = |x\rangle\Pi_x|\psi\rangle.$$

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. We say that the set of unitaries satisfies property $\mathbf{P}_y$ if it is true that

$$\forall x \; \Pi_x = \omega^{xy}\Pi_0,$$

where $\omega = e^{i\frac{2\pi}{n!}}$. 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.

The requirement that $d \geq n!$ comes from the fact that it is not possible to satisfy property $\mathbf{P}_y$ for every y if $d < n!$ For example, if $d = 2$ only $\mathbf{P}_0$ and $\mathbf{P}_{n!/2}$ are satisfiable.

The protocol for solving this problem is the following: 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:

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

Then, we apply the n-SWITCH:

$$S_n|C\rangle|\psi\rangle = \frac{1}{\sqrt{n!}}\sum_{x=0}^{n!-1}|x\rangle\Pi_x|\psi\rangle. \tag{2}$$

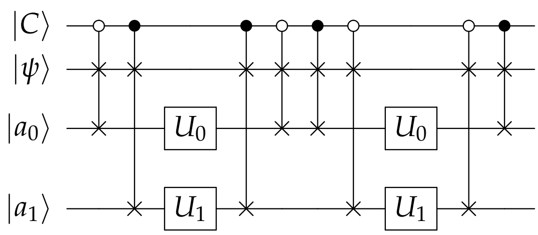
Now we apply the Fourier transform over $\mathbf{Z}_{n!}$ to our control qudit

$$\mathcal{F}_{n!}S_n|C\rangle|\psi\rangle = \frac{1}{n!}\sum_{x,y=0}^{n!-1}|y\rangle\omega^{-xy}\Pi_x|\psi\rangle. \tag{3}$$

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

$$p_y = \frac{1}{n!^2}\left\|\sum_{x=0}^{n!-1}\omega^{-xy}\Pi_x|\psi\rangle\right\|^2. \tag{4}$$

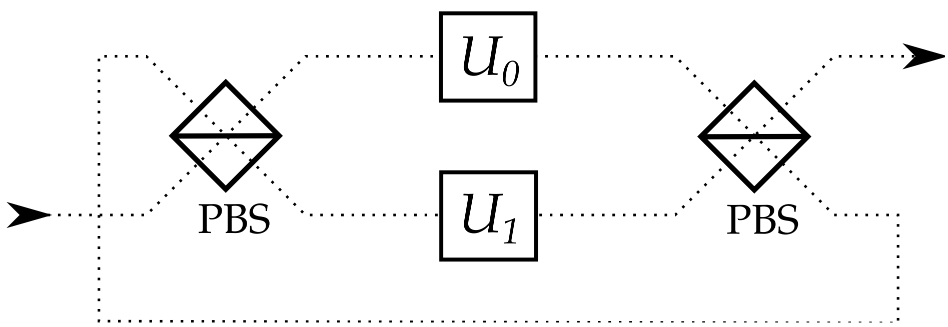
The best way we found of simulating the n-SWITCH gate with a fixed circuit has query complexity $O(n^2)$. The following circuit illustrates the idea for $n = 2$:



For implementations that exploit actual quantum control over the gate ordering it is not so simple to calculate the complexity, since such implementations are explicitly outside the quantum circuit formalism. 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 j-th 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.

Note that this agrees with the number of physical devices implementing U_i that we must build.

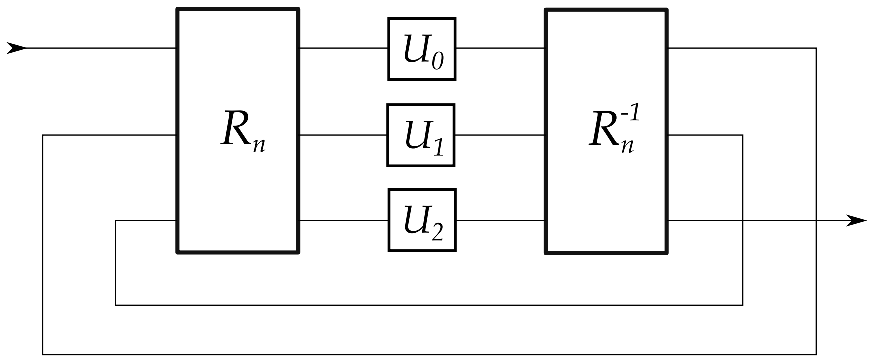
For the case $n = 2$, we propose a simple interferometric implementation, where the control qubit is the polarization of a photon, and the target $|\psi\rangle$ is some internal degree of freedom. This interferometer maps



$(\alpha|H\rangle + \beta|V\rangle)|\psi\rangle$ to

$$\alpha|H\rangle U_1 U_0|\psi\rangle + \beta|V\rangle U_0 U_1|\psi\rangle.$$

The abstract idea can be generalized for larger n as follows: Both control and target are encoded in a single system. When the system enters 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 target in the state $\Pi_x|\psi\rangle$.



References

[1] G. Chiribella et al. "Quantum computations without definite causal structure." *Phys. Rev. A* **88** 022318 (2013). arXiv:0912.0195 [quant-ph].

[2] G. Chiribella. "Perfect discrimination of no-signalling channels via quantum superposition of causal structures." *Phys. Rev. A* **86** 040301 (2012). arXiv:1109.5154 [quant-ph].

[3] T. Colnaghi et al. "Quantum computation with programmable connections between gates." *Phys. Lett. A* **376** 2940–2943 (2012). arXiv:1109.5987 [quant-ph].