Physics Letters A 376 (2012) 2940–2943

Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Quantum computation with programmable connections between gates

Timoteo Colnaghi [a], Giacomo Mauro D'Ariano [a,b], Stefano Facchini [a], Paolo Perinotti [a,b,*]

[a] QUIT group, Dipartimento di Fisica, via Bassi 6, 27100 Pavia, Italy
[b] INFN Gruppo IV, Sezione di Pavia, via Bassi, 6, 27100 Pavia, Italy

ARTICLE INFO

Article history:
Received 17 July 2012
Accepted 20 August 2012
Available online 22 August 2012
Communicated by P.R. Holland

Keywords:
Quantum computation
Quantum algorithms
Quantum switch

ABSTRACT

A new model of quantum computation is considered, in which the connections between gates are programmed by the state of a quantum register. This new model of computation is shown to be more powerful than the usual quantum computation, e.g. in achieving the programmability of permutations of N different unitary channels with 1 use instead of N uses per channel. For this task, a new elemental resource is needed, the *quantum switch*, which can be programmed to switch the order of two channels with a single use of each one.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

Quantum computation [1] has revolutionized computer science, showing that the processing of quantum states can lead to a tremendous speedup in the solution of a class of problems, as compared to traditional algorithms that process classical bits. On the other hand, in classical computation it is customary to design algorithms that treat subroutines in exactly the same way as data—the *program as data* paradigm inspired by the Church's notion of computation [2]—which allows one to compute functions of functions, rather than only functions of bits. Such a programming strategy, however, is not an option in the quantum case. This is due to the fact that in quantum computation data and subroutines are intrinsically different objects—the former being quantum states, the latter unitary transformations—and exact programming of unitary transformations over quantum states is impossible with finite resources [3].

A new kind of computational model is needed for a quantum functional calculus that uses unitary transformations (generally channels) as input and output subroutines. This paradigm has been recently established and developed theoretically, based on the notion of *quantum combs and supermaps* [4,5], which describe circuit-boards in which quantum channels can be plugged. Thus, quantum combs describe any kind of coherent adaptive quantum strategy [6], e.g. any quantum algorithm calling oracles (the oracles are the plugged-in channels). Coherent adaptive strategies are the most general architecture allowed in the quantum circuit model and have been demonstrated to be more powerful than non-adaptive ones for the problem of channel discrimination [7,8]. They are also very useful for quantum computation, as many quantum algorithms consist in the discrimination of classes of oracles.

There exist tasks, however, that even a coherent adaptive quantum strategy cannot accomplish: for example, an algorithm that takes two unknown boxes and, using the boxes a *single time*, connects them in the two possible orders depending on the value of a control qubit. Even more: the algorithm produces a quantum superposition of the two orderings. As shown in Ref. [9], realizing such a "quantum switch" within the standard circuit model would unavoidably need *two uses* of each box. More generally, if we want to achieve the superposition of all possible permutations of the orderings of N boxes, many uses per box will be needed (here it will be shown that the minimum number of uses is N). On the other hand, as already outlined in Ref. [9] for $N = 2$, by using a coherent switching of paths, e.g. in the optical domain, one would need only a single use per oracle.

The number of uses of a box on computational grounds represents the so-called *query complexity*. This is a primary resource to be taken into account, and in some cases it actually corresponds to the number of physical copies of the device that are needed. A coherent switching of input–output connections can have a dramatic impact on the performances of quantum computers, since

* Corresponding author at: QUIT group, Dipartimento di Fisica, via Bassi 6, 27100 Pavia, Italy.
E-mail addresses: timoteo.colnaghi@gmail.com (T. Colnaghi), dariano@unipv.it (G.M. D'Ariano), stefano.facchini@unipv.it (S. Facchini), paolo.perinotti@unipv.it (P. Perinotti).
URLs: http://www.quantummechanics.it (G.M. D'Ariano), http://www.quantummechanics.it (P. Perinotti).

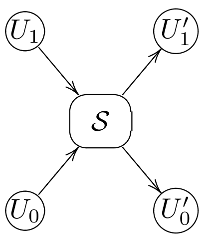
0375-9601/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.physleta.2012.08.028

the use of superpositions of permutations of oracle-calls can be of enormous advantage for oracle discrimination, thus achieving e.g. a fast database search with a low-complexity optical setup.

In this Letter we consider such a new kind of quantum computation, where the connections between gates are themselves programmable on the state of quantum registers. We will show that these dynamical quantum networks are more powerful than the usual quantum computers, in the sense that they reduce the query complexity for some tasks. We will prove this for the case of programming the permutations of N different unitary channels, where the number of uses of each input channel is dramatically reduced from N to 1.

2. The quantum switch

For the permutations of N different unitary channels a new resource is needed, the *quantum switch* (abbreviated as QS), which can programmed to switch the order of two channels with a single use per channel. We will represent the action of the QS with the following graph



(1)

where $\mathcal{S}$ represents the QS having two inputs and two outputs, U_0 and U_1 denote the two input unitary channels, and U_0' and U_1' are the two output ones, which are either $U_0' = U_0$ and $U_1' = U_1$ or $U_0' = U_1$ and $U_1' = U_0$, depending on the state $|0\rangle$ or $|1\rangle$ of a control qubit s (not represented). In formula

$$\mathcal{S}\big(U_1 \otimes U_0 \otimes |i\rangle\big) = U_{1\oplus i} \otimes U_{0\oplus i} \otimes |i\rangle, \tag{2}$$

where the position of U_j, $j = 0, 1$ in the tensor product determines the order in which U_j is applied in the circuit in which the QS is inserted (channel $U_{0\oplus i}$ first). Notice that in principle, other fixed operations can be performed between U_0' and U_1'.

3. Controlled permutations of gates

In order to compare the power of customary quantum computation within the circuit model with that of dynamically programmable quantum networks, we compare their performances in the task of *controlled permutation*, namely the task of programming all possible permutations of N unitary channels $\{U_i\}_{i=0}^{N-1}$ acting in cascade on one target qubit. First we design the most efficient conventional quantum network that achieves controlled permutation, and show that N uses per channel are needed. As we will see the optimal network needs $\mathcal{O}(N^2)$ CNOTs and $\mathcal{O}(N^2)$ control qubits. We then build a network made only of quantum switches that can program all the permutations of the N unitary channels with a single use per channel, and then we prove optimality of this network in minimizing the number of QSs and of control qubits.

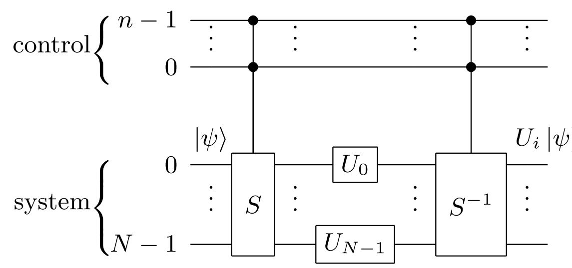
Consider the two following tasks:

Task 1. Let $\mathscr{U} := \{U_i\}_{i=0}^{N-1}$ be a set of N different unitary single-qubit operators. Build an efficient quantum circuit that lets a (unknown) qubit state $|\psi\rangle$ undergo one of the N^N dispositions of the unitaries in $\mathscr{U}$, with the specific disposition programmed on the state of a control register.

Task 2. Build an efficient quantum circuit that outputs the state $U_i|\psi\rangle$ for any $U_i \in \mathscr{U}$, with i programmed on the state of a control register.

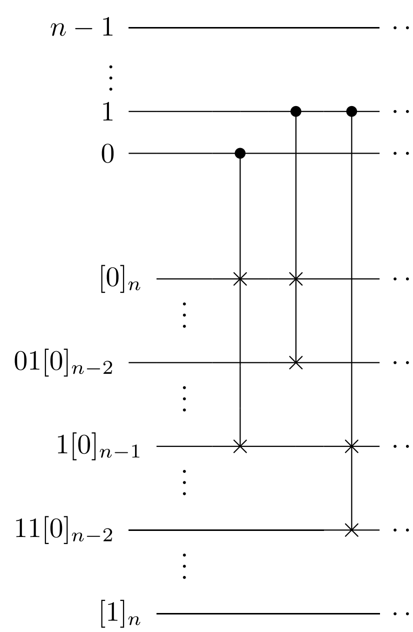
In the following we will show that Task 1 has a straightforward solution in terms of Task 2. For this reason, we first solve Task 2. We restrict to N power of 2, the case of general N following straightforwardly. For $i \in [0, 2^n]$ integer we denote by $[i]_n \in \{0, 1\}^n$ the binary n-string representation of i.

Consider the following circuit composed of two registers, a *system* and a *control*, made of N qubits and $n = \log N$ qubits respectively:



(3)

In the circuit, the system register is prepared in the state $|\psi\rangle \otimes |0\rangle^{N-1}$ and the control in the state $|[i]_n\rangle$. This will output the state $U_i|\psi\rangle$ on the first system qubit. For this purpose one first operates an n-controlled swap S, then each system qubit i undergoes U_i, and finally an inverse n-controlled swap S^{-1} is made. The n-controlled swap is achieved by the following circuit:



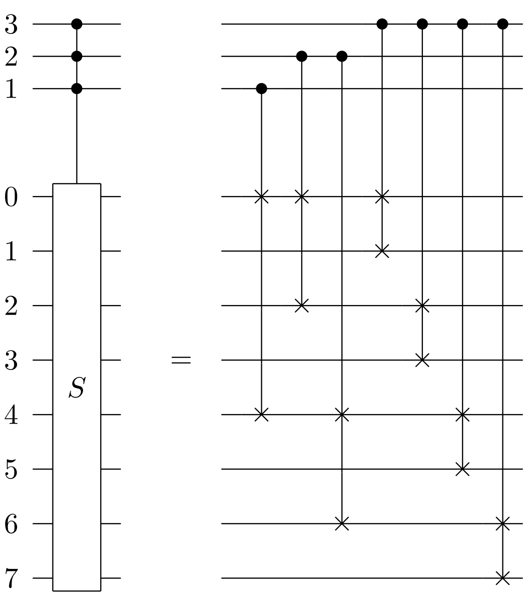
(4)

In words, for $k = 0$ to $n-1$ the circuit does the following: insert 2^k control-swaps controlled by the $(k+1)$th control qubit and swapping system qubit $[s]_k[0]_{n-k}$ with system qubit $[s]_k 1[0]_{n-k-1}$ for every k-bit string $[s]_k$.

Theorem 1. *Circuit (4) achieves Task 2 in the most efficient way.*

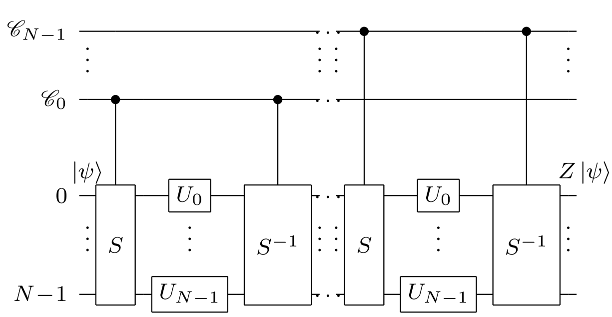
Proof. The minimum number of bits needed to write an integer smaller than N is $n = \log N$, whence the number of controlling qubits is optimal. Then, the best algorithm to single out an element U_i out of the set $\mathscr{U}$ of N unitaries is given by a sequence of bisections of $\mathscr{U}$, seeking at each step to which half U_i belongs, and encoding 0 or 1 accordingly, which is exactly the strategy of Circuit (4), whence also the number of control-swaps is minimal. □

We need 2^k control-swaps to implement the kth steps, whence we need $\sum_{i=0}^{n-1} 2^k = 2^n - 1 = N - 1$ control-swaps in total to perform the n-controlled swap. Knowing that a control-swap can be achieved by the sequence of a CNOT, a Toffoli, and a CNOT, and that the optimal implementation of the Toffoli gate requires 6 CNOTs and 9 single qubit operations [10], we conclude that $8(N-1)$ CNOTs and $9(N-1)$ single-qubit operations are needed to achieve a n-controlled swap, whence $16(N-1)$ CNOTs and $18(N-1)$ single-qubit operations are necessary to achieve Task 2. As an example, for $N = 8$ the 3-controlled swap is achieved with 7 control-swaps as follows



(5)

The result of Theorem 1 allows us to conclude that Task 1 is achievable by an ordinary quantum circuit on $\mathbf{O}(N \log N)$ ancillary qubits plus 1 system qubit, and resorting to $\mathbf{O}(N^2)$ elementary operations, as follows



(6)

where $Z = U_{i_{(N)}} \dots U_{i_{(1)}}$ denotes the programmed disposition of unitaries, and $\mathscr{C}_i$ $(i = 1, \dots, N)$ denote a control register made of n qubits. The circuit is just the juxtaposition of N copies of circuit (3), $\mathscr{C}_i$ being the control system of the $i$the circuit.

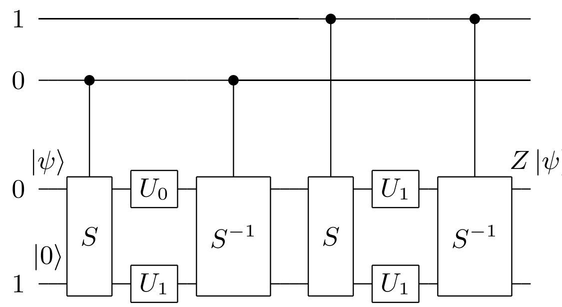
Theorem 2. *Circuit (6) is the most efficient implementation of Task 1.*

Proof. The proof is an immediate consequence of Theorem 1, since the elements of the sequence of unitaries $U_{i_{(N)}} \dots U_{i_{(1)}}$ are all independent, whence the circuit that accomplishes Task 1 in the most efficient way must be a juxtaposition of N optimal circuits achieving Task 2. □

It is easy to see that, by construction, circuit (6) is also the most efficient implementation of Task 1 restricted to just the permutations of the unitaries, namely without repetitions.

In order to implement circuit (6) we need $16N(N-1)$ CNOTs and $18N(N-1)$ single-qubit operations, along with $N \log N$ control qubits plus $N-1$ ancillary qubits (only one system qubit support the transformation). In summary, the resource for Task 1 is $\mathcal{O}(N^2)$ CNOTs and single-qubit operations and $\mathcal{O}(N \log N)$ qubits.

As an example, for $N = 2$, the circuit will be the following



(7)

With the control registers prepared in a superposition state, the system qubit gets entangled with the control register, e.g. for the control register in the state $|\Phi_1\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$ the output joint state of the system qubit supporting the input state $|\psi\rangle$ and the control qubits will be $|\Psi_0\rangle = \frac{1}{\sqrt{2}}[|01\rangle \otimes U_0 U_1 |\psi\rangle + |10\rangle \otimes U_1 U_0 |\psi\rangle]$. Thus, if we program the control qubits in a tensor product of $|+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$ the output joint state will be entangled with all possible dispositions of the unitaries of the set $\mathscr{U}$, a typical manifestation of quantum parallelism.

We now investigate the possibility of programming all the possible permutations of N unitary channels with a single use per channel, using quantum switches. More precisely, the task is the following:

Task 3. Build a computational network with QSs achieving any permutations of the unitaries of the set $\mathscr{U}$ (programmed on the state of a control register) with a single use per unitary.

A solution to Task 3 is provided by the quantum network with QSs built with the following procedure:

(**N**) Build the following input–output box-connections:

1. $U_0 \to \mathcal{S}_1^{(1)} \to \mathcal{S}_1^{(2)} \to \dots \to \mathcal{S}_1^{(N-1)} \to U_0'$
2. for $k = 1$ to $N-2$:

$$\mathcal{S}_1^{(k)} \to \mathcal{S}_2^{(k+1)}, \ \dots, \ \mathcal{S}_k^{(k)} \to \mathcal{S}_{k+1}^{(k+1)},$$

3. for $k = 1$ to $N-1$:

$$U_k \to \mathcal{S}_k^{(k)} \to \mathcal{S}_{k-1}^{(k)} \to \dots \to \mathcal{S}_2^{(k)} \to \mathcal{S}_1^{(k)},$$

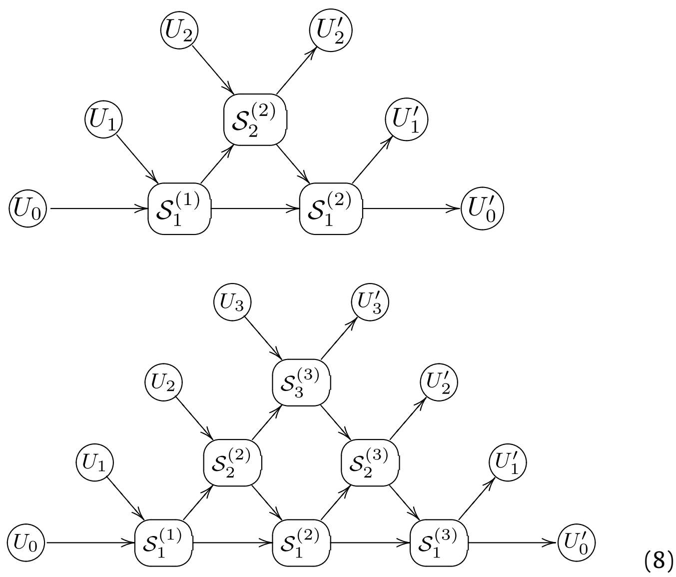
4. $\mathcal{S}_1^{(N-1)} \to U_1', \ \dots, \ \mathcal{S}_{N-1}^{(N-1)} \to U_{N-1}'$.

Finally, to apply the sequence of unitary to the target qubit, one need to connect the output black boxes U_i' each other to obtain their product $U_{N-1}' U_{N-2}' \dots U_0'$.

As an example, the computational networks for $N = 3, 4$ are reported (the control registers omitted).

Table 1
The six possible outputs for the computational circuit (8) for $N = 3$ and corresponding control state(s). The control qubit $s_i^{(j)}$ programs the QS $\mathcal{S}_i^{(j)}$.

$U_2'U_1'U_0'$	State of $s_1^{(1)}\ s_1^{(2)}\ s_2^{(2)}$	$U_2'U_1'U_0'$	State of $s_1^{(1)}\ s_1^{(2)}\ s_2^{(2)}$
$U_2U_1U_0$	$\|0\rangle\|0\rangle\|0\rangle$ $\|1\rangle\|1\rangle\|0\rangle$	$U_2U_0U_1$	$\|1\rangle\|0\rangle\|0\rangle$ $\|0\rangle\|1\rangle\|0\rangle$
$U_0U_2U_1$	$\|1\rangle\|0\rangle\|1\rangle$	$U_1U_2U_0$	$\|0\rangle\|0\rangle\|1\rangle$
$U_1U_0U_2$	$\|0\rangle\|1\rangle\|1\rangle$	$U_0U_1U_2$	$\|1\rangle\|1\rangle\|1\rangle$



(8)

It is easy to see that the circuit uses overall $\sum_{n=1}^{N-1} n = \frac{1}{2}N(N-1)$ QSs, each with a single-qubit control register.

In Table 1 we list the six possible outputs of the circuit for $N = 3$ versus the state of the control qubits $s_i^{(j)}$ (corresponding to the QSs $\mathcal{S}_i^{(j)}$). Notice that the same permutation can be achieved with different states of the control registers.

Theorem 3. *Network (*$\mathbf{N}$*) achieves Task 3 in the most efficient way, minimizing the number of QSs and of ancillary control qubits.*

Proof. The task is to set the ordering of N different unitaries depending on the state of a control register, using a network of QSs. The permutation is defined by the relative ordering of each pair of different unitaries, and there are $\frac{1}{2}N(N-1)$ of such pairs, which also equals the number of QSs and of their respective registers. □

4. Conclusions

We have seen that a quantum computation with programmable connections between gates is more powerful than the usual quantum computation. This has been proved on the specific task of programming all possible permutations of a cascade of unitary channels acting on a qubit, where the number of uses per channels is dramatically reduced from N to 1. For this task the new *quantum switch* resource is needed, which can be programmed to switch the order of two channels, each with a single use. A thorough analysis of the functions on channels that can be physically achievable is in progress, and before its conclusion it is premature to state any conjecture about universal functions for quantum computation with programmable connections. In particular, it is not clear yet whether the QS function is universal or not. As an important example, it can be proved that the W operation considered in Ref. [11] cannot be achieved using only QSs in addition to traditional quantum circuits. However, while QS has a straightforward operational interpretation, W is an admissible mathematical map that presently lacks physical interpretation. On practical grounds, we believe that the ultrafast switch of Ref. [12] is a sufficient optical element for the implementation of the quantum switch, being able to route entangled photons at high speed without disturbing the quantum state. This practical possibility makes the implementation of QS feasible in the near future, opening important new options and perspectives in the design of new quantum algorithms.

Acknowledgements

We acknowledge Scott Aaronson for a stimulating discussion about Ref. [9]. G.M.D. acknowledges interesting discussions with Joe Altepeter and Prem Kumar. This work has been supported by the Italian Ministry of Education through grant PRIN 2008, and by the EU through FP7 STREP project COQUIT. Research at Perimeter Institute for Theoretical Physics is supported in part by Canada through NSERC and by Ontario through MRI.

References

[1] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[2] H. Barendregt, Lambda calculi with types, in: S. Abramski, D.M. Gabbay, T.S.E. Maibaum (Eds.), Handbook of Logic in Computer Science, vol. 2: Computational Structures, Oxford University Press, New York, 1993.
[3] M.A. Nielsen, I.L. Chuang, Phys. Rev. Lett. 79 (1997) 321.
[4] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. Lett. 101 (2008) 060401.
[5] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. A 80 (2009) 022339.
[6] G. Gutoski, J. Watrous, in: Proc. of the 39th Annual ACM Symposium on Theory of Computation, vol. 565, 2007.
[7] G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. Lett. 101 (2008) 180501.
[8] A.W. Harrow, A. Hassidim, D.W. Leung, J. Watrous, Phys. Rev. A 81 (2010) 032339.
[9] G. Chiribella, G.M. D'Ariano, P. Perinotti, B. Valiron, arXiv:0912.0195 [quant-ph], 2009.
[10] V.V. Shende, I.L. Markov, On the CNOT-cost of TOFFOLI gates, arXiv:0803.2316v1 [quant-ph], 2008.
[11] O. Oreshkov, F. Costa, Č. Brukner, arXiv:1105.4464.
[12] M.A. Hall, J.B. Altepeter, P. Kumar, Phys. Rev. Lett. 106 (2011) 053901.