Ancilla-driven universal quantum computation

Citation for published version:
Anders, J, Oi, DKL, Kashefi, E, Browne, DE & Andersson, E 2010, 'Ancilla-driven universal quantum computation', *Physical Review A*, vol. 82, no. 2, 020301. https://doi.org/10.1103/PhysRevA.82.020301

Digital Object Identifier (DOI):
10.1103/PhysRevA.82.020301

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Physical Review A

PHYSICAL REVIEW A **82**, 020301(R) (2010)

Ancilla-driven universal quantum computation

Janet Anders,[1,*] Daniel K. L. Oi,[2] Elham Kashefi,[3] Dan E. Browne,[1] and Erika Andersson[4]

[1] *Department of Physics & Astronomy, University College London, London WC1E 6BT, United Kingdom*
[2] *SUPA, Department of Physics, University of Strathclyde, Glasgow G4 0NG, United Kingdom*
[3] *School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, United Kingdom*
[4] *SUPA, Department of Physics, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

(Received 19 November 2009; revised manuscript received 25 March 2010; published 10 August 2010)

We introduce a model of quantum computation intermediate between the gate-based and measurement-based models. A quantum register is manipulated remotely with the help of a single ancilla that "drives" the evolution of the register. The fully controlled ancilla qubit is coupled to the computational register only via a *fixed* unitary two-qubit interaction and then measured in suitable bases, driving both single- and two-qubit operations on the register. Arbitrary single-qubit operations directly on register qubits are not needed. We characterize all interactions E that induce a unitary, stepwise deterministic measurement back-action on the register sufficient to implement any quantum channel. Our scheme offers experimental advantages for computation, state preparation, and generalized measurements, since no tunable control of the register is required.

DOI: 10.1103/PhysRevA.82.020301 PACS number(s): 03.67.Lx, 03.67.Ac

The two best-known strategies for quantum computation are the gate-based and measurement-based (MBQC) models. In the former, a computation is performed by actively manipulating individual register qubits by a network of logical gates. The required control of the register is very challenging to realize experimentally. MBQC is an alternative strategy that relies on the effect of measurements on entangled quantum systems [1,2]. A computation is implemented *passively*, as a sequence of adaptive single-qubit measurements on an entangled multipartite resource state and realized in experiments [3] were single qubit measurements are "cheap."

In this Rapid Communication we introduce a hybrid model that fits many experimental settings. The scheme uses a single fully controlled ancilla qubit, which is coupled sequentially to one or at most two qubits of a register via a *fixed* entangling operation, E. After each coupling the ancilla is measured in a suitable basis, providing a back-action onto the register. This implements both single- and two-qubit operations on the register qubits. No other operations on the register qubits are necessary, in particular, arbitrary single-qubit operations directly on the register qubits are not required. Moreover, using a single additional qubit appended to a state in the register, any positive operator valued measurement (POVM), and thus any quantum channel, can be realized. The computation requires no direct control of the register nor the preparation of a large entangled state. The processing of information is driven by active manipulation of the ancilla alone and we shall call the model ancilla-driven quantum computation (ADQC).

Implementing operations on a static register is similar to gate-based quantum computing. The fixed ancilla-register interaction and measurement driven computation resembles MBQC. For MBCQ, no characterization currently exists of exactly what classes of entangled states lead to universal computation. For ADQC, we are able to characterize the necessary and sufficient entangling interactions.

Previous attempts to construct *programmable*, deterministic and universal quantum operations have concluded this to be impossible [4,5]. These schemes also use "program qubits," i.e., ancillas, that are coupled to a register with a fixed interaction. The difficulty lies not in the entangling operation but in implementing an *arbitrary* (single-qubit) operation using a fixed interaction. Our results bypass existing no-go theorems as we allow *feedback* within the programmable part and a final *local* redefinition of the computational basis of the register.

Many existing schemes use "flying" qubits for mediating interactions between register qubits, e.g., Refs. [6,7]. The key difference of ADQC is that register qubits are addressed only with a fixed coupling operation; no other register operation, neither unitary nor measurements, is required. This is advantageous in many experimental situations as the computational register not only can be separated from state preparation and measurement but also does not require bespoke control. Long-lived but static qubits are addressed by mobile ancilla qubits using a fixed entangling interaction. Realizations of interest include neutral atoms in optical lattices [8], micro ion trap arrays [9], nuclear-electron spin systems [10], and cavity QED superconducting qubits [7]. In cavity QED, for example, it is desirable to be able to *fix* the interaction time as done in Ref. [11]. ADQC is also useful in systems where measurements are destructive, i.e., experiments with photons,

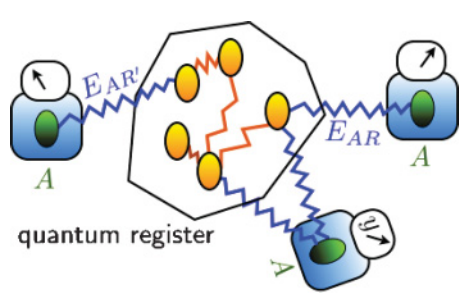

FIG. 1. (Color online) Illustration of an ancilla-driven computation on a register consisting of several qubits. A single ancilla, A, is sequentially coupled to one, or at most two, register qubits, R and R', etc., and measured. The coupling, E_{AR}, is fixed throughout the computation while the measurements on the ancilla, indicated by the arrows, can differ.

*j.anders@ucl.ac.uk

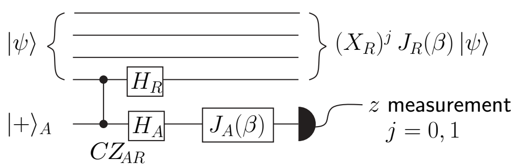

FIG. 2. Ancilla-driven implementation of a single qubit rotation, $J_R(\beta)$, on a register qubit R. The initial state of the register can be a pure state, $|\psi\rangle$, or a mixed state. The ancilla and register qubits are first coupled with $E_{AR} = H_A\, H_R\, \mathrm{CZ}_{AR}$. The rotation $J(\beta)$ is then implemented on the ancilla and transferred to the register qubit by measuring the ancilla in the z basis. The result of the measurement, $j = 0,1$, determines if an X correction appears on the register qubit.

as the measurement never acts directly on the register but leaves it intact for further manipulation.

The idea behind ADQC is simple yet surprisingly powerful; see Fig. 1. The ancilla, A, is prepared, then entangled with a register qubit R using a fixed interaction E_{AR} and then measured. The induced back-action onto the register is what "steers" the register to the desired state [12]. An example of a universal interaction between register and ancilla is the controlled-Z (CZ) interaction followed by local Hadamards, $H = (X + Z)/\sqrt{2}$ with X, Y, Z the Pauli matrices,

$$E_{AR} = H_A\, H_R\, \mathrm{CZ}_{AR}, \tag{1}$$

where $\mathrm{CZ} = \mathbb{1} - 2\,|11\rangle\langle 11|$. This is reminiscent of MBQC where resource states are constructed using the CZ operation [1,2]. For ADQC, however, local Hadamards are necessary, since otherwise one cannot implement arbitrary single-qubit operations on register qubits.

An arbitrary single qubit unitary can be decomposed, using $J(\beta) = H\, e^{i\frac{\beta}{2} Z}$, as $U = e^{i\alpha}\, J(0)\, J(\beta)\, J(\gamma)\, J(\delta)$ with parameters β, γ, δ (Euler angles), and α (global phase) in $\mathbb{R}$ [13]. To implement $J_R(\beta)$ on the register in the ancilla-driven model, the ancilla is first prepared in the state $|+\rangle_A = (|0\rangle + |1\rangle)/\sqrt{2}$ and then coupled to the qubit R via E_{AR}; see Fig. 2. Instead of acting on the register qubit the rotation $J_A(\beta)$ is applied to the ancilla and transferred to the register qubit by measuring the ancilla in the computational z basis $|j\rangle$ with $j = 0,1$. Alternatively, the ancilla can be measured immediately in the rotated basis $|\beta_+\rangle_A = \cos\frac{\beta}{2}|0\rangle_A + i\,\sin\frac{\beta}{2}|1\rangle_A$ and $|\beta_-\rangle_A = \cos\frac{\beta}{2}|1\rangle_A + i\,\sin\frac{\beta}{2}|0\rangle_A$. The implemented operation on the register qubit is

$${}_A\langle j|\, J_A(\beta)\, E_{AR}\, |+\rangle_A = U_R(j)\, J_R(\beta), \tag{2}$$

with (fixed) Pauli correction $U_R(j) = (X_R)^j$ that depends on the measurement outcome j of the ancilla. (We neglect global phases.) The correction can be removed by changing the ancilla measurement bases of future computational operations, cf. Refs. [1,2,14].

Arbitrary single qubit unitaries together with an entangling operation, such as the CZ gate, form a universal set of gates. To entangle two register qubits R and R', they each interact with the ancilla via the same operation E; see Fig. 3. A y measurement of the ancilla then mediates the entangling operation between R and R',

$${}_A\langle y_j|\, E_{AR}\, E_{AR'}\, |+\rangle_A = U_R(j) \otimes U_{R'}(j)\; \mathrm{CZ}_{RR'}. \tag{3}$$

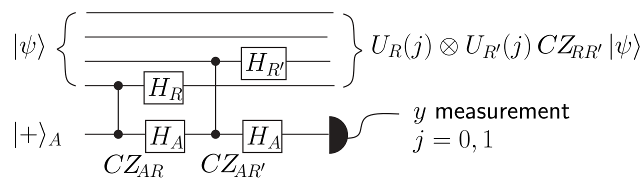

FIG. 3. Ancilla-driven implementation of a controlled-Z gate, $\mathrm{CZ}_{RR'}$, on two register qubits R and R'. Both register qubits are coupled with $E_{AR(AR')} = H_A\, H_{R(R')}\, \mathrm{CZ}_{AR(AR')}$ to the ancilla which is then measured in the y basis. The corrections $U_R(j)$ and $U_{R'}(j)$ are local and can be applied through ancilla-driven single-qubit rotations.

This is a CZ operation up to local corrections $U_R(j) = H_R[(\mathbb{1}_R + i\,Z_R)/\sqrt{2}]\,(Z_R)^j$, and similarly for R', that again depend on the outcome j of the ancilla measurement. $U_R(j)$ and $U_{R'}(j)$ can be applied as single-qubit operations as described above. Thus ADQC with a fixed interaction $E_{AR} = H_A\, H_R\, \mathrm{CZ}_{AR}$ allows implementation of any computation or *universal state preparation* [15].

A fundamental question in the context of new models for quantum computation is to specify *all* entangling operations, E, that lead to universality [16,17]. To add structure to this question one can restrict to computations with a number of desirable properties. An important requirement for ADQC is that no operation, including any corrections, ever needs direct implementation on the register. We therefore consider unitary, stepwise deterministic, "tensor-commuting" (as defined below) computations; i.e., by adapting ancilla measurement bases alone, corrections on the register can be absorbed and the computation remains deterministic at every step [18,19].

While in cluster state MBQC only standard X, Y, and Z corrections occur, here we allow a broader class which we entitle *generalized Pauli corrections* (other generalizations of the Pauli group have been studied in Ref. [20]). We consider all single-qubit Hermitian unitaries P which satisfy $\mathrm{tr}(P) = 0$, parametrized as $P(a,b,c) = aX + bY + cZ$ with $a,b,c \in \mathbb{R}$ and $a^2 + b^2 + c^2 = 1$. The canonical decomposition [21,22] for two-qubit unitaries, $E_{AR} = (W_A' \otimes W_R)\, D_{AR}\, (V_A' \otimes V_R)$, separates the nonlocal part

$$D_{AR}(\alpha_x,\alpha_y,\alpha_z) = e^{-i(\alpha_x X_A \otimes X_R + \alpha_y Y_A \otimes Y_R + \alpha_z Z_A \otimes Z_R)} \tag{4}$$

with $0 \leqslant \alpha_{x,y,z} \leqslant \pi/4$ from local single-qubit unitaries on the register, V_R, W_R, and the ancilla, V_A', W_A'. To allow composition of operations to arbitrarily large computations, all corrections on register qubits need to interchange with future entangling operations, D_{AR}, in such a way that they remain localized, i.e., the resulting correction is a tensor product between the register and ancilla. This allows the corrections on each register qubit to shift through the computational pattern and accumulate at the final step where they can be removed by a *local* redefinition of the computational basis [23]. If there exist such corrections, we say that the entangling operation, D_{AR}, *tensor-commutes* with the corrections [24], i.e., $D_{AR}\, P_R(a,b,c)\, D_{AR}^\dagger = P_A(\tilde{a},\tilde{b},\tilde{c}) \otimes P_R(a',b',c')$, where $\tilde{P}_A$ and P_R' are also generalized Pauli transformations (or the identity, see Ref. [25]). A key result of this article is that only two classes of couplings are universal.

Theorem. The interactions E_{AR} between any register qubit R and the ancilla A that result in a (i) unitary, stepwise deterministic evolution of the register, that (ii) tensor-commute with corrections, and that (iii) admit universal state preparation of the register using ADQC, are locally equivalent to (i.e., D_{AR} is of the form of) the *Ising model* or the *Heisenberg XX model* with maximal coupling strength $\alpha = \pi/4$ or $\alpha_x = \alpha_y = \pi/4$.

The theorem states not only what interactions are sufficient but also which are *necessary*. Interactions must be locally equivalent either to the CZ gate, as shown constructively in the example above, or the CZ + SWAP gate, where CZ + SWAP $= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| - |11\rangle\langle 11|$. Both of these are maximally entangling [22,26] and Clifford operations [27]. It is, however, important to note that the local operations play a crucial role. The CZ gate on its own is not enough but needs to be accompanied by Hadamard operations as in Eq. (1).

Moreover, any generalized measurement, or POVM, on the register can be performed with the (repeated) help of an additional register qubit which introduces extra degrees of freedom to form a Neumark extension of the system's state [28,29]. This is of interest especially when measurements on the system would remove the physical qubit, such as photon measurements. In ADQC, any destructive measurement is instead made on the ancilla and the register qubits remain for future operations.

The proof of the theorem is involved and technical details can be found in Ref. [25]. An outline is given here. When the ancilla with initial state $|+\rangle_A$ and a single register qubit are coupled, and the ancilla is subsequently measured in $|\pm\rangle_A$ then the state $|\psi\rangle$ of the register (and similarly for mixed states) becomes

$$|\psi\rangle \mapsto K_R^{\pm}/\sqrt{p^{\pm}}\,|\psi\rangle, \tag{5}$$

where the Kraus operators $K_R^{\pm}$ are given by

$$K_R^{\pm} = {}_A\langle\pm|\,E_{AR}\,|+\rangle_A = {}_A\langle\pm_{\theta,\phi}|\,W_R\,D_{AR}\,V_R\,|+_{\gamma,\delta}\rangle_A, \tag{6}$$

and $p^{\pm} = \mathrm{tr}(K_R^{\pm\dagger}K_R^{\pm})$ are the probabilities of measurement outcome + or −. Also, $|+_{\gamma,\delta}\rangle_A = \cos\frac{\gamma}{2}|0\rangle_A + e^{i\delta}\sin\frac{\gamma}{2}|1\rangle_A = V_A'|+\rangle_A$ and $|\pm_{\theta,\phi}\rangle_A = W_A'^{\dagger}|\pm\rangle_A$, where γ, δ, θ, and ϕ denote ancilla parameters in V_A' and W_A'.

In a stepwise deterministic computation the Kraus operators must be proportional to unitaries. This implies that one of the α's, say α_z, must vanish. Additionally, the two Kraus operations shall relate to another via a generalized Pauli operation, $K_R^-/\sqrt{p^-} = e^{i\Delta}\,P_R\,K_R^+/\sqrt{p^+}$, where Δ is a global phase. Moreover, the nonlocal part of the interaction, D_{AR}, must tensor-commute with this correction P_R. These requirements restrict the interaction to four classes, $D_{AR}(\pi/4,\pi/4,0)$, $D_{AR}(0 < \alpha_x < \pi/4,\pi/4,0)$, $D_{AR}(\pi/4,0,0)$, and $D_{AR}(0 < \alpha < \pi/4,0,0)$, each with their individual sets of acceptable ancilla parameters γ, θ, δ, ϕ, and sets $P(a,b,c)$ with a,b,c of tensor-commuting corrections.

Two of these classes, however, are not sufficient for universal state preparation. Ising interactions with nonmaximal interaction strength, $D_{AR}(0 < \alpha < \pi/4,0,0)$, can be used to steer unitary, stepwise deterministic evolutions of a register qubit. Yet all the implementable single qubit unitaries lie in a plane of the Bloch sphere; $D_{AR}(0 < \alpha < \pi/4,0,0)$ (plus fixed local unitaries) is *not universal*. For Heisenberg models with nonmaximal coupling strength, $D_{AR}(0 < \alpha_x < \pi/4,\pi/4,0)$, it is impossible to *compose* several single-qubit operations while preserving stepwise determinism, see Ref. [25] for details. This leaves only two universal classes, $D_{AR}(\pi/4,0,0)$ and $D_{AR}(\pi/4,\pi/4,0)$. These are locally equivalent to CZ_{AR} and $\mathrm{CZ}_{AR} + \mathrm{SWAP}_{AR}$, leading to the theorem.

We note that the choice of *local unitaries* in E_{AR} is not trivial—CZ alone cannot steer all register evolution as no basis change can be achieved at the register qubit. However, the example above shows that together with local Hadamards enabling basis changes, the CZ interaction is universal. For the CZ + SWAP interaction it is easy to verify that ADQC is identical to the one-way model [1] and hence allows universal state preparation, as the role of ancilla and register qubits are simply swapped.

ADQC is suited to many physical realizations, e.g., a register of atoms trapped in an optical lattice addressed by ancilla marker atoms [6], which interact via cold collisions to generate CZ gates [8], or an array of ions in microtraps and an ancilla read-write ion that interacts by laser-induced state-dependent pushing forces [9]. Using optimized control pulses [30] it may be possible to generate the E_{AR} operation efficiently and robustly in a single step. We can also consider different systems for register and ancilla, e.g., a cavity QED [11] register, and Rydberg atoms traversing them as ancillas [31]. While "static" qubit field states are hard to manipulate directly, "flying" Rydberg atoms are easily controlled by lasers and measured by field ionization. We note that Ref. [31] suggests entangling two cavity qubits by sequential interaction with an ancilla Rydberg atom which is then measured [cf. Eq. (3)]. Different cavity qubit rotations are achieved by varying the register-ancilla control pulse. In contrast, ADQC requires only a single fixed register-ancilla operation.

Another hetero qubit scheme uses nuclear and electron spins, e.g., an array of long-lived phosphorus donor nuclear spins in silicon as the register [10], and electron ancillas move around the array by charge transport by adiabatic passage (CTAP) [32]. Control and characterization of the nuclear-electron interaction is reduced to optimization of a single two-qubit unitary, simplifying the task considerably, especially for qubits subject to manufacturing variation and tolerances [33]. We can exploit spin-orbit effects to introduce anisotropies into the Heisenberg interaction [34,35] which allow Ising-type entangling unitaries to be generated [36]. Finally, superconducting qubits coupled with an effective Hamiltonian of the $XX + YY$ type via a superconducting microwave stripline [7] are also good candidates for ADQC.

Imperfections could arise in a number of ways, for example, in decoherence or in the timing and finite duration of the measurements. Future work will investigate how quantum error correction techniques can be employed to deliver fault tolerance in the ADQC model and allow implementation in a yet broader class of physical systems.

In summary, ADQC is a method of implementing any quantum channel on a quantum register driven by operations on an ancilla using only a fixed entangling operation E_{AR}. ADQC is a valuable model that shifts the question of universal resources away from MBQC resource states and their structure and focuses instead on basic building blocks of such states. These can be characterized systematically by requiring properties necessary and sufficient for universal computation. This approach can be adapted to investigate computations with relaxed properties, e.g., we might not require the computation to be stepwise deterministic, similar to computation using computational tensor network states [17]. We expect that these correspond to unitary Kraus operators, i.e., one of the α's must vanish; however, the branching relation could be non-Pauli but instead any finite root of $\mathbb{1}$. This would lead to schemes based on Ising or Heisenberg interactions with smaller coupling strength, $\alpha < \pi/4$.

We thank Mark Hillery for insightful discussions. J.A. is funded by the Royal Society and supported by the EPSRC's QIPIRC network. D.E.B. thanks the National Science Foundation of Singapore. J.A. and D.E.B. acknowledge support by QNET. We all thank SUPA and QUISCO. D.E.B. and E.K. acknowledge support by the QICS network.

[1] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[2] H. J. Briegel *et al.*, Nat. Phys. **5**, 19 (2009); D. E. Browne and H. J. Briegel, in *Lectures on Quantum Information* (Wiley, New York, 2007), chap. 20, p. 359.
[3] P. Walther *et al.*, Nature (London) **434**, 169 (2005).
[4] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[5] S. F. Huelga, J. A. Vaccaro, A. Chefles, and M. B. Plenio, Phys. Rev. A **63**, 042303 (2001); S. F. Huelga, M. B. Plenio, and J. A. Vaccaro, *ibid.* **65**, 042316 (2002).
[6] T. Calarco, U. Dorner, P. Julienne, C. Williams, and P. Zoller, Phys. Rev. A **70**, 012306 (2004).
[7] J. Majer *et al.*, Nature (London) **449**, 443 (2007).
[8] D. Jaksch, H. J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller, Phys. Rev. Lett. **82**, 1975 (1999).
[9] J. I. Cirac and P. Zoller, Nature (London) **404**, 579 (2000).
[10] B. E. Kane, Nature (London) **393**, 133 (1998).
[11] M. Brune *et al.*, Phys. Rev. Lett. **101**, 240402 (2008).
[12] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[13] V. Danos, E. Kashefi, and P. Panangaden, Phys. Rev. A **72**, 064301 (2005).
[14] E. Kashefi *et al.*, Electron Notes Theor. Comp. Sci. **249**, 307 (2009).
[15] The computational patterns for ADQC, generated with the *noncommuting* operators E_{AR}, and MBQC can be translated into each other using a novel type of open graph states, the twisted graph states [14]. This allows us to find ADQC patterns with the smallest possible depth.
[16] M. Van den Nest, A. Miyake, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).
[17] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).
[18] V. Danos and E. Kashefi, Phys. Rev. A **74**, 052310 (2006).
[19] D. E. Browne *et al.*, New J. Phys. **9**, 250 (2007).
[20] S. Clark *et al.*, Quantum Inf. Comput. **8**, 0106 (2008).
[21] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. A **67**, 042313 (2003).
[22] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[23] The final correction can also be implemented explicitly in the ancilla-driven manner; the only nondeterministic case where repeated application may be necessary.
[24] These requirements also permit a standardization procedure as defined for the MBQC model [37].
[25] E. Kashefi *et al.*, Theor. Comput. Sci. (to be published).
[26] M. S. Leifer, L. Henderson, and N. Linden, Phys. Rev. A **67**, 012306 (2003).
[27] D. Gottesman, Ph.D. thesis, CalTech, 1997; S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[28] E. Andersson and D. K. L. Oi, Phys. Rev. A **77**, 052104 (2008).
[29] B. Reznik, Int. J. Quantum Inf. **4**(1), 181 (2006).
[30] U. V. Poulsen *et al.*, e-print arXiv:0910.4495; R. Nigmatulli and S. G. Schirmer, New J. Phys. **11**, 105032 (2009).
[31] V. Giovannetti, D. Vitali, P. Tombesi, and A. Ekert, Phys. Rev. A **62**, 032306 (2000).
[32] A. D. Greentree, J. H. Cole, A. R. Hamilton, and L. C. L. Hollenberg, Phys. Rev. B **70**, 235317 (2004).
[33] S. G. Schirmer and D. K. L. Oi, Phys. Rev. A **80**, 022333 (2009).
[34] K. V. Kavokin, Phys. Rev. B **64**, 075305 (2001).
[35] L-A. Wu and D. A. Lidar, Phys. Rev. A **66**, 062314 (2002).
[36] M. Borhani and D. Loss, Phys. Rev. A **71**, 034308 (2005).
[37] V. Danos *et al.*, J. ACM **54**(2), 8 (2007).