Experimental Quantum Computing without Entanglement

B. P. Lanyon,* M. Barbieri,† M. P. Almeida, and A. G. White

Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, Australia

(Received 15 August 2008; published 13 November 2008)

Deterministic quantum computation with one pure qubit (DQC1) is an efficient model of computation that uses highly mixed states. Unlike pure-state models, its power is not derived from the generation of a large amount of entanglement. Instead it has been proposed that other nonclassical correlations are responsible for the computational speedup, and that these can be captured by the quantum discord. In this Letter we implement DQC1 in an all-optical architecture, and experimentally observe the generated correlations. We find no entanglement, but large amounts of quantum discord—except in three cases where an efficient classical simulation is always possible. Our results show that even fully separable, highly mixed, states can contain intrinsically quantum mechanical correlations and that these could offer a valuable resource for quantum information technologies.

DOI: 10.1103/PhysRevLett.101.200501 PACS numbers: 03.67.Lx, 03.67.Ac

While a great deal of work has been done on the conventional pure-state models of quantum computing [1,2], relatively little is known about computing with mixed states. Deterministic quantum computation with one pure qubit (DQC1) is a model of computation that employs only a single qubit in a pure state, alongside a register of qubits in the fully mixed state [3]. While this model is not universal—it cannot implement any arbitrary algorithm—it can still efficiently solve important problems that are thought to be classically intractable. One of the original applications identified was the simulation of quantum systems [3]. Since then exponential speedups have been identified in estimating the average fidelity decay under quantum maps [4], quadratically signed weight enumerators [5], and the Jones Polynomial in knot theory [6]. DQC1 also affords efficient parameter estimation at the quantum metrology limit [7]. That such a useful tool could be built with only a single pure quantum bit is particularly appealing given the current state of experimental quantum computing, where decoherence is a significant obstacle in the path to large-scale implementations.

Besides its practical applications, DQC1 is also fascinating from a fundamental perspective. Its power is thought to lie somewhere between universal classical and quantum computing—it is strictly less powerful than a universal quantum computer [3] and no efficient classical simulation has been found or thought likely to exist [8,9]. Furthermore its power is thought not to come from the generation of entanglement, which is at most marginally present in DQC1 [9]. This is surprising, as entanglement is widely believed to lie at the heart of the advantages offered by a quantum computer—a belief supported by the discovery that a universal pure-state quantum computer must generate a large amount of entanglement in order to offer any speedup over a classical computer [10,11]. However, no such proof exists for mixed-state models. Instead it has been proposed that DQC1 generates other types of nonclassical correlations and that these are responsible for the computational advantage [8,12–14].

In this Letter we present a small-scale implementation of DQC1 in a linear-optic architecture [15]. We observe and fully characterize the predicted nonclassical correlations. Our results show that while there is no entanglement, other intrinsically quantum mechanical correlations are generated, except in the cases where an efficient classical simulation is always possible. Furthermore, we demonstrate that a small fraction of a single pure quantum bit is enough to implement DQC1 efficiently [9]. This represents the first implementation of DQC1 outside of a liquid-state NMR architecture, in which the question of nonclassical correlations was not addressed [16]. Unlike liquid-state NMR, there are several known paths to scalable linear-optic quantum computing [2,17,18], and there is active development of the necessary technology [19–21].

We perform a first-order implementation of the DQC1 algorithm for estimating the normalized-trace of a unitary matrix [3,8,9,12]. This achieves an exponential speedup over the best known classical approach; i.e., it requires exponentially fewer resources as the size of the unitary increases. It is thought highly unlikely that an efficient, but as yet unknown, classical approach can exist [9]. That DQC1 can perform this task efficiently underpins its ability to solve the range of practical problems listed above.

Figure 1 shows the normalized-trace estimation algorithm. The required input state is separable and consists of a single pure qubit c (control) in the logical state $|0\rangle\langle 0|$, and a register of n qubits in the completely mixed state $I_n/2^n$, where I_n is the n-qubit identity. The circuit consists of the standard Hadamard gate [1] applied to the control qubit, and a unitary (U_n) on the register controlled by qubit c. The state of all $n + 1$ qubits at the output of the circuit is

$$\rho_{\rm cr} = \frac{1}{2N}\begin{bmatrix} I_n & U_n^\dagger \\ U_n & I_n \end{bmatrix}, \qquad (1)$$

where $N = 2^n$. The reduced state of qubit c—achieved by

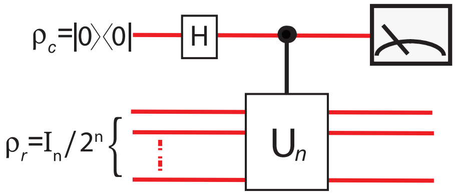

FIG. 1 (color online). Algorithm for estimating the normalized trace of the unitary operator U_n, using deterministic quantum computing with 1-qubit (DQC1). I_n is the n-qubit identity. Repeated running of the circuit and measurement of qubit c in the Pauli X (Y) basis yields an estimate of the corresponding expectation value, from which one can derive the real (imaginary) part of the normalized trace ($\mathrm{Tr}[U_n]/2^n$).

performing a partial trace over the register—is given by

$$\rho_c = \frac{1}{2}\begin{bmatrix} 1 & \mathrm{Tr}[U_n]^\dagger/N \\ \mathrm{Tr}[U_n]/N & 1 \end{bmatrix}. \tag{2}$$

Thus the normalized trace of U_n is encoded in the coherences of qubit c, and can be retrieved by measuring the expectation values of the standard Pauli operators X and Y, since $\langle X\rangle = \mathrm{Re}[\mathrm{Tr}(U_n)/N]$ and $\langle Y\rangle = -\mathrm{Im}[\mathrm{Tr}(U_n)/N]$.

An expectation value is estimated by repeatedly running the circuit. One can achieve a fixed accuracy ϵ in this estimate with a number of runs $L \sim \ln(P_e^{-1})/\epsilon^2$, where P_e is the probability that the estimate is farther from the true value than ϵ [9]. That the accuracy does *not* scale with the size of the unitary, and scales logarithmically with the error probability, means that this is an efficient algorithm for estimating the normalized-trace. In contrast, classical approaches suffer an exponential increase in the required number of resources with the size of the unitary [9]. Note that the algorithm does not efficiently return the full trace $\mathrm{Tr}[U_n]$. This would require multiplying the estimate of the normalized trace by 2^n, thereby amplifying the uncertainty by an amount that is exponential in the size of the unitary.

We implement the first-order ($n = 1$) case for

$$U_1 = Z_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}. \tag{3}$$

In this case $\langle X\rangle = (1 + \cos\theta)/2$ and $\langle Y\rangle = (\sin\theta)/2$. Our implementation is shown in Fig. 2. We encode quantum information in the polarization of single photons. Single qubit gates are realized deterministically using birefringent wave plates. The two-qubit controlled-Z_θ gate is realized nondeterministically using a recently developed technique requiring only one cnot [15]. Measurement of single photons in the two output modes signals a successful run of the algorithm and occurs with probability 1/12.

Each photonic qubit is passed through a polarization interferometer, allowing the preparation of noisy (mixed) states by introducing a path difference between the two arms, Fig. 2. A path difference greater than the photon coherence length results in a fully decohered—that is, a fully mixed—photonic qubit. By tuning the path difference

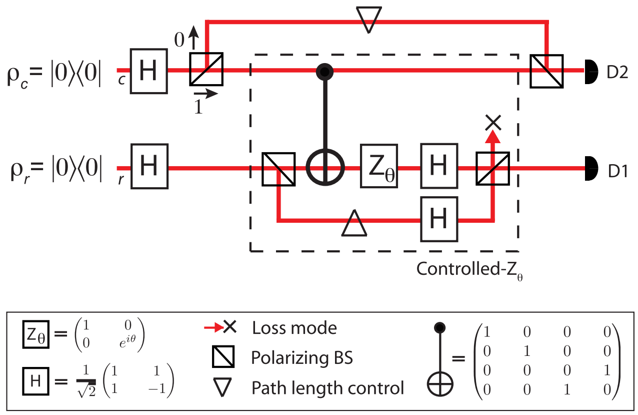

FIG. 2 (color online). Experimental schematic. Qubits at the input and output are encoded in the polarization of single photons ($|0\rangle = |H\rangle$, $|1\rangle = |V\rangle$, horizontal and vertical). Coincident measurement of single photons at fiber-coupled counting modules (D1, D2) signals a successful run of the algorithm. Photons are generated via spontaneous parametric down conversion of a frequency-doubled mode-locked Ti:sapphire laser (820 nm → 410 nm, $\Delta\tau = 80$ fs at 82 MHz) pumping a type-I 2 mm $\mathrm{BiB_3O_6}$ crystal; filtered to 820 ± 1.5 nm; collected into two single-mode optical fibers; then injected into free-space modes c and r. With 100 mW at 410 nm, we measure a twofold coincidence rate at the output of the optical circuit of $\approx 100\ \mathrm{s}^{-1}$. Interferometers are realized using calcite beam displacer pairs, rotating one displacer of a pair about an axis perpendicular to the plane defined by the two paths enables relative path length control. The two-qubit gate is realized nondeterministically as described in Ref. [29].

between zero and the photon coherence length we can accurately control the level of mixture in the qubit between zero and maximum, respectively.

We implement the algorithm over the range $-\pi \le \theta \le \pi$ Eq. (3). Figure 3(a) compares the experimentally observed results with the theoretical prediction (calculated assuming perfect circuit operation and measured input states). We observe high correlation between experiment and theory quantified by a reduced χ^2 of 0.7 (real curve) and 1.2 (imaginary curve) [22]. Deviations are due to imperfect circuit operation caused by optical beam steering as θ is varied, interferometric instability and nonclassical interference instability. These effects could be reduced by moving to micro-optic systems [21].

Interestingly, the exponential speedup offered by this algorithm is not compromised by reducing the purity of qubit c [9]. Consider replacing the initial state of this qubit with the mixed state $\frac{1}{2}\{I_1 + \alpha Z\}$, where α now reflects the purity ($p = [1 + \alpha^2]/2$, $0 \le \alpha \le 1$). At the output of the circuit the state is now given by

$$\rho_c = \frac{1}{2}\begin{bmatrix} 1 & \alpha\mathrm{Tr}[U_n]^\dagger/N \\ \alpha\mathrm{Tr}[U_n]/N & 1 \end{bmatrix}. \tag{4}$$

The effect of mixture in qubit c is to reduce $\langle X\rangle$ and $\langle Y\rangle$ by α [Eq. (2)], thereby making it harder to estimate the normalized-trace. To achieve the same fixed accuracy as

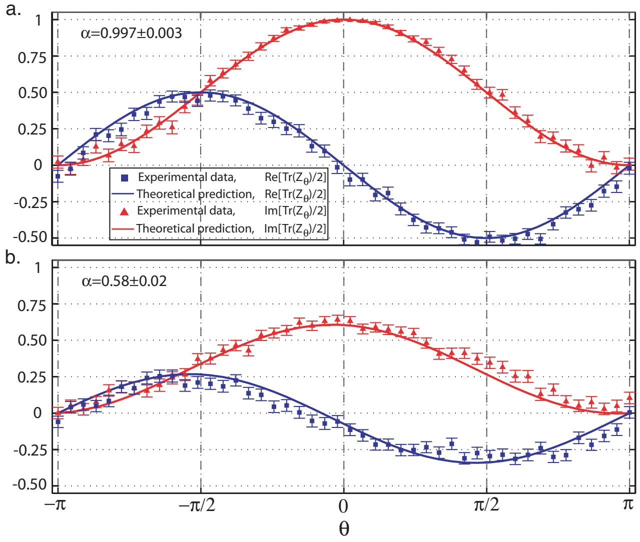

FIG. 3 (color online). Algorithm output. Real (blue or dark gray) and imaginary (red or gray) parts of the normalized-trace measured for two values of α, over a range of θ, Eq. (4). α is the degree of purity of the control qubit as described in the text. $\langle X\rangle$ is estimated by counting the number of coincident photon pairs $(N_\pm)$ when projecting qubit c into the states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, over 10 sec. Then $\langle X\rangle = (N_+ - N_-)/(N_+ + N_-)$. The same technique is used to estimate $\langle Y\rangle$, but in this case we project into the states $|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. All error bars are calculated assuming Poissonian uncertainties in the counting statistics. We use the standard definition for a reduced-χ^2 calculation [22], allowing for 3 degrees of freedom [the real and imaginary parts of the trace are simple trigonometric functions defined by an amplitude, frequency and phase, Eq. (3)]. Note that the goal of the algorithm is to return the normalized trace. The full trace is not required for the DQC1 applications mentioned in the introduction.

before requires an increased number of runs $L' \sim L/\alpha^2$. While this clearly adds an additional overhead, as long as α is nonzero, the algorithm still provides an efficient evaluation of the trace. Even access to the tiniest fraction of a single pure qubit is sufficient to achieve an exponential speedup over the best known classical approach.

Figure 3(b) compares the experimentally observed algorithm results with the theoretical predictions (calculated assuming perfect circuit operation and measured input states), for the measured value of $\alpha = 0.58 \pm 0.02$. We observe a high degree of correlation between experiment and theory quantified by a reduced χ^2 of 1.8 (real curve) and 2.0 (imaginary curve). The increased χ^2 in this case [compared to Fig. 3(a)] is due to a less favorable optical alignment, not an intrinsic error associated with initializing c into a mixed state. The additional resource overhead is reflected in the amplitude reduction by a factor of α compared with the results shown in Fig. 3(a). Note that in the limit where the control qubit is completely incoherent, $\alpha = 1$, the entire input state is fully mixed and any unitary evolution leaves the state unchanged—the algorithm does not work. The ability to prepare the control qubit in a superposition state that is at least partially coherent is a necessary condition for a computational speedup. However, as we show later, it is not sufficient.

We analyze the correlations generated by the algorithm by performing tomography of the two-qubit output state, Eq. (1), using 36 (overcomplete) measurement bases. This allows a reconstruction of the density matrix, from which the correlations can be derived. Figure 4 shows two measures of nonclassical correlations—the well-known *tangle* [24,25] and the lesser-known *discord* [12–14]. The tangle is a complete measure of entanglement in two-qubit states, and represents perhaps the most striking divergence from classical behavior. However, entanglement is not the only kind of nonclassical correlation. A far stronger measure, which encompasses entanglement and more, is given by the discord.

The discord is concerned with a fundamental characteristic of classical systems—that their information content is locally accessible and can be obtained without perturbing the state for independent observers [14]. If the discord is zero there exists a local measurement protocol under which all the state information can be revealed, without perturbing the state for observers who do not have access to the measurement results. If the discord is nonzero then no such protocol exists. For pure states, discord is a measure of entanglement—no other nonclassical correlations can be distinguished. However, for mixed states the discord captures more nonclassical correlations than entanglement [12].

The results show that, to within experimental error, our implementation does not give rise to any entanglement. However, in general it does generate quantum discord. We observe a high degree of correlation between the theoretical and measured discord values, quantified by a reduced χ^2 of 1.6. These results are consistent with recent theoretical work [12] which predicts that, although the entanglement is generally zero for arbitrary instances of this algorithm, discord is consistently present.

In our implementation the discord is zero in two distinct cases, $\theta = \{0, \pm\pi\}$, corresponding, respectively, to the controlled-Z_θ gate implementing the identity I and the controlled-sign gate $CZ_{\pm\pi}$. Both of these gates are members of the Clifford group, as is the Hadamard [1]. Thus in these cases the entire state evolution is implemented only by gates from the Clifford group. Further, the algorithm involves preparing the input in a mixture of logical basis states, and measurement of observables in the Pauli group [1]. Under these conditions the Gottesman-Knill theorem states that the entire algorithm can *always*—i.e., for an arbitrary-size implementation—be efficiently simulated on a classical computer [1,26]. In contrast, for all other values of θ the action of the controlled-Z_θ gate is responsible for a non-Clifford-group evolution. There is no known classical method to efficiently simulate an arbitrary-size algorithm that evolves in this way—thereby allowing for a quantum speedup. It is also straightforward to show that an implementation of the algorithm composed entirely of gates from the Clifford group produces a state with zero discord

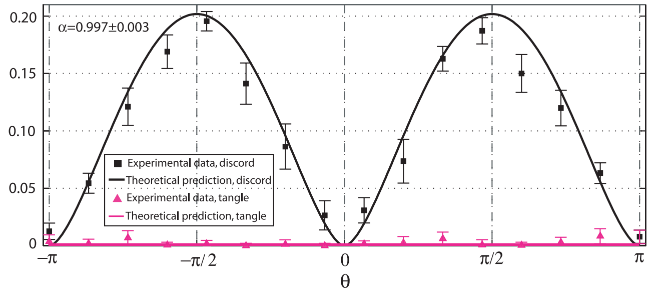

FIG. 4 (color online). Nonclassical correlations generated by our DQC1 algorithm. Discord and tangle are derived from the reconstructed density matrices measured at the algorithm output for $\alpha = 0.997 \pm 0.003$ [Fig. 3(a)]. Discord is calculated by optimizing over all 1-qubit projective measurements on qubit c, Fig. 1 [26]. Theoretical predictions are calculated using measured input states and assuming perfect circuit operation.

(this is true to any order [26]). These results suggest a link between discord and the potential for computational speedup. An important path for further research is to determine whether all DQC1 circuits that do not generate discord can be efficiently simulated on a classical computer. Such a result would provide strong evidence that the discord is a more accurate measure than entanglement of the resources required for a quantum speedup.

Our circuit does not generate entanglement: it takes a mixture of separable states at the input to a different mixture of separable states at the output [26]. Indeed, this is true for an arbitrary-size DQC1 implementation, with respect to the partition between the register and the control [4,9]. In general both the input and output consist of a mixture of 2^n separable states. The key to the computational power is that the mapping between the input and output terms is highly nontrivial: any classical simulation would need to keep track of the evolution of all 2^n state amplitudes. In the case of a Clifford group evolution the mapping is trivial, and a classical simulation is efficient.

We have demonstrated a quantum algorithm that achieves an exponential speedup over the best known classical approach, and yet does not employ entanglement. Instead we observed that the model generates other nonclassical correlations that can exist even in fully separable highly mixed states. Besides the fundamental interest, this could have implications in the many burgeoning quantum computing architectures where environmental decoherence presents a significant obstacle to universal pure-state quantum computing. It is of interest to explore quantum discord in other contexts, such as ‘‘nonlocality without entanglement’’ [27,28]—while the two-qubit states of interest in these works are not entangled they have nonzero discord, signifying the presence of quantum correlations.

The authors wish to thank C. Caves, A. Datta, A, Shaji, and G. Vidal for discussions. We acknowledge financial support from the Australian Research Council and the IARPA-funded Army Research Office Contract No. W911NF-05-0397.

*Corresponding author.
lanyon@physics.uq.edu.au
†Present address: Laboratoire C. Fabry, Institut d'Optique, France.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[3] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[4] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier, Phys. Rev. Lett. **92**, 177906 (2004).
[5] E. Knill and R. Laflamme, Inf. Proc. Lett. **79**, 173 (2001).
[6] P. W. Shor and S. P. Jordan, Quantum Inf. Comput. **8**, 681 (2008).
[7] S. Boixo and R. D. Somma, Phys. Rev. A **77**, 052320 (2008).
[8] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).
[9] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
[10] R. Jozsa and N. Linden, Proc. R. Soc. A **459**, 2011 (2003).
[11] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[12] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[13] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[14] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[15] B. Lanyon *et al.*, arXiv:0804.0272v1 [Nature Phys. (to be published)].
[16] C. A. Ryan, J. Emerson, D. Poulin, C. Negrevergne, and R. Laflamme, Phys. Rev. Lett. **95**, 250502 (2005).
[17] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[18] J. L. O'Brien, Science **318**, 1567 (2007).
[19] Special Issue on Single photons on demand [New J. Phys. **6**, 85 (2004)].
[20] Special Issue on Single-photon: detectors, applications, and measurement [J. Mod. Opt. **51**, 1265 (2004)].
[21] A. Politi *et al.*, Science **320**, 646 (2008).
[22] $\chi^2 = (N - M)^{-1} \sum_1^N (a_i - b_i)^2/\sigma_i^2$ where: N is the number of sample points, $M = 3$ is the number of fitting parameters in our functions; a_i is the ith data point; b_i is the ith theoretical point; and σ_i is the uncertainty in a_i [23].
[23] J. R. Taylor, *An Introduction to Error Analysis* (University Science Books, Sausalito, CA, 1997).
[24] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[25] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, Phys. Rev. A **65**, 012301 (2001).
[26] See EPAPS Document No. E-PRLTAO-101-019847 for mathematical details of the proofs cited in the text. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[27] C. H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999).
[28] G. J. Pryde, J. L. O'Brien, A. G. White, and S. D. Bartlett, Phys. Rev. Lett. **94**, 220406 (2005).
[29] N. K. Langford *et al.*, Phys. Rev. Lett. **95**, 210504 (2005).