Degree of quantum correlation required to speed up a computation

Alastair Kay*
Department of Mathematics, Royal Holloway University of London, Egham, Surrey TW20 0EX, United Kingdom
(Received 1 October 2015; published 14 December 2015)

The one-clean-qubit model of quantum computation (DQC1) efficiently implements a computational task that is not known to have a classical alternative. During the computation, there is never more than a small but finite amount of entanglement present, and it is typically vanishingly small in the system size. In this paper, we demonstrate that there is nothing unexpected hidden within the DQC1 model—Grover's search, when acting on a mixed state, *provably* exhibits a speedup over classical, with guarantees as to the presence of only vanishingly small amounts of quantum correlations (entanglement and quantum discord)—while arguing that this is not an artifact of the oracle-based construction. We also present some important refinements in the evaluation of how much entanglement may be present in the DQC1 and how the typical entanglement of the system must be evaluated.

DOI: 10.1103/PhysRevA.92.062329 PACS number(s): 03.67.Ac, 03.65.Ud, 03.67.Mn

I. INTRODUCTION

Any computation whose quantum algorithm has a superior scaling of running time compared to its classical counterpart ought to pass through an intermediate state with nontrivial quantum properties, e.g., entanglement. Indeed, for pure-state computations, it has been shown that entanglement is necessary [1]. However, computation involving mixed states is a far more subtle issue, with no firm resolution, although it is looking increasingly likely that quantum discord must be present in order for there to be an exponential speedup [2,3].

The one-clean-qubit model of quantum computation (DQC1) [4] can provide important insights. Expressed as a decision problem, this is defined as:

Problem 1. Given an efficient classical description of a quantum computation U on n qubits, and a promise that either $\mathrm{Tr}(U) > 1/\mathrm{poly}(n)$ or $\mathrm{Tr}(U) < -1/\mathrm{poly}(n)$, determine which is the case with error probability $\varepsilon < \frac{1}{3}$.

There is no known classical algorithm which can efficiently solve this problem, while there is a quantum circuit that is remarkably simple (Fig. 1). In this circuit, there is one special ("clean") qubit, which is initially prepared in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and a set of n qubits is prepared in the maximally mixed state $\mathbb{1}/2^n$. After applying controlled U between the clean qubit (control) and the mixed qubits (target), we can estimate the probabilities that the clean qubit is in state $|+\rangle$ [to find $\mathrm{Re}(\mathrm{Tr}(U))$] or $(|0\rangle + i|1\rangle)/\sqrt{2}$ [to find $\mathrm{Im}(\mathrm{Tr}(U))$]. There is a very obvious division in the system between the clean qubit and the mixed ones. As such, the authors of [4] examined the entanglement between that bipartition of the system and discovered that it was 0. Entanglement seemed not to be necessary for mixed-state quantum computation, although other measures of nonclassicality such as the quantum discord and measurement-induced disturbance have since been shown to be nonzero across that bipartition [5,6].

Detecting entanglement in a multipartite state using bipartite divisions is, however, quite subtle. A clear demonstration of this is the distribution of entanglement using separable states [7,8]; just because two of the three possible bipartitions of a three-qubit system have no entanglement does not mean that the third bipartition has no entanglement. So it is with the DQC1 model in [9], it was demonstrated that by considering different bipartitions, there is indeed entanglement present. Two additional results are provided in [9]: upper and lower bounds on the maximum amount of entanglement present across any bipartition and a numerical investigation of the entanglement produced by a typical unitary (in the sense of selecting a U uniformly at random from the Haar measure). This investigation suggests that the entanglement is typically exponentially small in n. So, although there is some entanglement present, it is a vanishingly small amount on average.

Even the presence of *almost* no entanglement in the computation might seem surprising. However, in this paper, we draw parallels with a noisy version of Grover's search [10] in which we demonstrate the existence of a quantum speedup in the presence of vanishingly small entanglement (such a result could have been proven from [11] but does not appear to have been) and other nonclassicality measures such as the quantum discord [12,13]. Moreover, unlike the case of the DQC1 model, where the speedup over classical is only *believed*, Grover's search is subject to an oracle-based complexity classification with a proven gap over the classical case. Placed in this context, the power of the DQC1 model seems much less surprising. However, we demand only the existence of a quantum speedup and do not address the important conceptual transition between a polynomial and an exponential speedup. We also improve the results of [9], giving a tight upper bound on the entanglement present in the DQC1 model for any U.

A further criticism of the DQC1 model (or, similarly, the Grover search that we describe here) is that it assumes an implementation of the controlled-U gate. In practice, we have no such implementation and need to decompose the action in terms of elementary gates. Even if the net implementation of controlled U yields little or no entanglement, there is no *a priori* reason why all the intermediate steps should also be almost entanglement-free across all bipartitions. On the other hand, if the controlled U is treated as an oracle, then we can consider other oracle-based problems that are even more trivial in the entanglement sense: the Bernstein-Vazirani problem transforms a product state into a product state [14,15]. The internal workings of the oracle are evidently important and receive further discussion.

*alastair.kay@rhul.ac.uk

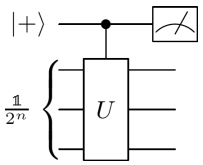

FIG. 1. The DQC1 model. No entanglement is present in the bipartite split between the top (special) qubit and the rest. Estimation of the trace of U proceeds by performing measurements in the bases $(|0\rangle \pm |1\rangle)/\sqrt{2}$ and $(|0\rangle \pm i|1\rangle)/\sqrt{2}$.

Notation

Consider a density matrix of $n+1$ qubits, ρ. Whenever we write ρ in the context of the DQC1 model, we refer specifically to the output of the circuit for estimating the trace of U (Fig. 1), which is a block matrix of the form

$$\rho = \frac{1}{2^{n+1}} \begin{pmatrix} \mathbb{1} & U^\dagger \\ U & \mathbb{1} \end{pmatrix}. \tag{1}$$

We denote by ρ_y, where $y \in \{0,1\}^n$, the partial transpose of ρ taken over the nonclean qubits i, $y_i = 1$, and never the clean qubit, without losing generality. Similarly, U_y denotes the partial transpose of U, such that

$$\rho_y = \frac{1}{2^{n+1}} \begin{pmatrix} \mathbb{1} & U_y^\dagger \\ U_y & \mathbb{1} \end{pmatrix}. \tag{2}$$

The Hamming weight of the string y is denoted w_y.

Throughout this paper, the multiplicative negativity [16,17] is chosen as the entanglement measure in order to maintain consistency with [9]. If $\Lambda_y = \mathrm{spec}(\rho_y)$ is the spectrum of ρ_y, then the multiplicative negativity of ρ with respect to bipartition y is

$$M_y = \sum_{\lambda \in \Lambda_y} |\lambda|. \tag{3}$$

If no entanglement is present, $M_y = 1$ for all $y \in \{0,1\}^n$, while $M_y > 1$ implies the presence of entanglement.

II. MAXIMUM ENTANGLEMENT IN THE DQC1

We start by examining the entanglement properties of the DQC1 model, strengthening the assertions in [9].

Theorem 1. For any unitary U, the output ρ of the DQC1 computation always satisfies

$$M_y \leqslant \frac{5}{4}$$

for all possible bipartitions $y \in \{0,1\}^n$.

Proof. Since it is not immediately clear that U_y is normal, we use the singular value decomposition of U_y,

$$U_y = RDV^\dagger,$$

where R and V are unitary matrices and D is the diagonal, with non-negative diagonal elements d_i. We need to find the eigenvalues of ρ_y, but note that the eigenvalues are invariant under the application of any unitary. We apply the unitary transformation of controlled $R^\dagger$ (controlled off the clean qubit), followed by a Pauli X on the clean qubit, controlled $V^\dagger$, and finished by another Pauli X on the clean qubit. This yields

$$\rho_y \mapsto \frac{1}{2^{n+1}} \begin{pmatrix} \mathbb{1} & D \\ D & \mathbb{1} \end{pmatrix}.$$

The eigenvalues of ρ_y are therefore readily calculated to be $(1 \pm d_i)/2^{n+1}$ for $i = 1 \ldots 2^n$.

How, then, are we to pick $\{d_i\}$ such that the value of

$$M_y = 1 + 2 \sum_{i:d_i>1} \frac{d_i - 1}{2^{n+1}} \tag{4}$$

is maximized? We perform a constrained optimization by noting from [9] that

$$2^n = \mathrm{Tr}(UU^\dagger) = \mathrm{Tr}(U_y U_y^\dagger) = \sum_i d_i^2. \tag{5}$$

Assume that t of the values $d_i > 1$ $(i = 1 \ldots t)$. Hence,

$$M_y = 1 - \frac{t}{2^n} + \frac{1}{2^n} \sum_{i=1}^{t} d_i,$$

subject to $\sum_{i=1}^{2^n} d_i^2 = 2^n$. This is true for all values d_i and t, so we can find the largest possible value by maximizing over all possible values (subject to the constraint):

$$M_y \leqslant \max_{t,\{d_i\}} 1 - \frac{t}{2^n} + \frac{1}{2^n} \sum_{i=1}^{t} d_i. \tag{6}$$

The optimal choice of the d_i is clear: $d_i = 0$ for $i = t+1 \ldots 2^n$ and

$$d_i = \sqrt{\frac{2^n}{t}}$$

otherwise, which gives

$$M_y \leqslant \max_t 1 - \frac{t}{2^n} + \sqrt{\frac{t}{2^n}}.$$

This is maximized by $t = 2^n/4$ (requiring $n \geqslant 2$ such that t is an integer), yielding

$$M_y \leqslant \tfrac{5}{4},$$

compared to the maximum possible value of $\approx 2^{n/2}$.

The limit $M_y = \frac{5}{4}$ is readily saturated. For example, when $n = 2$ we can use

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

since U_{01} has eigenvalues 2, 0, 0, and 0 as required for the optimal construction. For larger n, a construction such as $U \otimes \mathbb{1}^{\otimes(n-2)}$ would provide the requisite eigenvalues. There are then many ways of dressing this operator with unitaries that do not affect the partial transpose to disguise its structure slightly. For example, [9] uses a series of controlled-not gates. Incidentally, this trivial example shows that there are many bipartitions for which $M_y = \frac{5}{4}$: of the $2^n - 1$ possible choices, all 2^{n-1} choices that have $y_1 \oplus y_2 = 1$ exhibit this value.

This section reiterates the conclusion of [9]: there are bipartitions of the DQC1 model in which there is some

entanglement present, and it can be present up to a finite amount. Indeed, there can be many such bipartitions. What we investigate in the rest of this paper is how surprising this result is: Should the fact that we are guaranteed that no more than a small but finite amount of entanglement is present in a bipartition suggest to us that a quantum speedup should be more difficult to realize? What about the fact that for most unitaries it seems that the entanglement is vanishingly small (exponentially small in the system size, N)? To that end, we now make comparisons with a depolarized version of Grover's search, for which we show that even in situations where there is a provable (oracle-based) quantum speedup, this can occur when we are guaranteed that there is never more than an exponentially small amount of entanglement in any bipartition. This is a much stronger statement than has been made for the DQC1 model. As such, using the DQC1 model to make conclusions about the existence of a computational speedup in the presence of little or no entanglement seems obsolete.

III. COMPARISON WITH GROVER'S SEARCH

A standard formulation of Grover's search algorithm [10] starts with an initial state $|+\rangle^{\otimes n}$, trying to evolve to some (unknown) target state $|x_0\rangle$. The evolution is restricted to a subspace spanned by $|x_0\rangle$ and

$$|\psi^{\perp}\rangle = \frac{1}{\sqrt{2^n-1}} \sum_{x\neq x_0} |x\rangle, \tag{7}$$

such that the populated states are of the form

$$|\Psi\rangle = \cos\theta|x_0\rangle + \sin\theta|\psi^{\perp}\rangle, \tag{8}$$

where $\theta \in [0,\pi/2]$. For finite n, only integer multiples of $\sin^{-1}(2^{-n})$ are allowed. If we select a particular bipartition, then $|x_0\rangle = |x_y\rangle|x_{\bar{y}}\rangle$, where, here, the subscript y merely refers to the set of qubits on which the state is defined, and $\bar{y}$ is the complement of y. Similarly, we can define

$$|\psi_y^{\perp}\rangle = \frac{1}{\sqrt{2^{w_y}-1}} \sum_{x\in\{0,1\}^{w_y}: x\neq x_y} |x\rangle,$$

allowing $|\psi^{\perp}\rangle$ to be expressed as

$$|\psi^{\perp}\rangle = \sqrt{\frac{(2^{w_y}-1)(2^{n-w_y}-1)}{2^n-1}}|\psi_y^{\perp}\rangle|\psi_{\bar{y}}^{\perp}\rangle + \sqrt{\frac{2^{n-w_y}-1}{2^n-1}}|x_y\rangle|\psi_{\bar{y}}^{\perp}\rangle + \sqrt{\frac{2^{w_y}-1}{2^n-1}}|\psi_y^{\perp}\rangle|x_{\bar{y}}\rangle.$$

Evidently, the state $|\Psi\rangle$ across this bipartition may be written as a state with no more than two Schmidt coefficients. The maximum entanglement is when the two Schmidt coefficients are $\lambda_1 = \lambda_2 = \frac{1}{2}$ ($w_y = 1$ as $n \to \infty$), yielding a value of $M_y = 2$ for this standard, pure-state, version of Grover's search. There is only ever a finite amount of entanglement between any bipartition, much like the DQC1 model, the only difference being the value.

We now show that there is a variant of this algorithm for which the entanglement can be made vanishingly small [no more than $M_y = 1 + 2^{-n(\frac{1}{2}-\varepsilon)}$ for any $\varepsilon > 0$]. Consider using an initial state of

$$\rho = p|+\rangle\langle+|^{\otimes n} + (1-p)\frac{\mathbb{1}}{2^n} \tag{9}$$

for any $0 < p \leqslant 1$. A single run of the algorithm requires the standard quantum time, $O(2^{n/2})$, and succeeds in finding the search target x_0 with probability $\tilde{p} = p + \frac{1-p}{2^n}$. (The mixture describes that with probability p the pure-state algorithm proceeds, while with probability $1-p$, a maximally mixed state is present. This is unchanged by the application of unitaries and hence is still the maximally mixed state when the measurement outcome is determined and, hence, gives every possible answer with equal probability.) By allowing L repetitions, the algorithm succeeds with probability $1-(1-\tilde{p})^L \approx \tilde{p}L$ for small $\tilde{p}$. Thus, for a given finite ε, we could select p to be as small as $p \sim 2^{-n(\frac{1}{2}-\varepsilon)}$. For sufficiently large n, $\tilde{p} \approx p$, and we need a number of repetitions $L \sim 1/p$. This requires a run time $2^{n/2}L \sim 2^{n(1-\varepsilon)}$, thereby providing an advantage over the classical run time of 2^n, while we anticipate (and prove in the next subsection) that for smaller p, there is less entanglement present.

A. Entanglement

We turn to calculating the entanglement present in the depolarized algorithm. Progress through the algorithm can be specified by a parameter θ, such that the state is

$$\rho(\theta) = p|\Psi(\theta)\rangle\langle\Psi(\theta)| + (1-p)\frac{\mathbb{1}}{2^n}.$$

Assume that the Schmidt coefficients for state $|\Psi\rangle$ are $\cos^2\phi$ and $\sin^2\phi$ with respect to bipartition y. In the large-n limit, ϕ can take on any value $(0,\pi/2]$. $\rho(\theta)$ is unitarily equivalent (where the unitaries are local with respect to the bipartition and, hence, do not change the eigenvalues under the partial transposition) to a state

$$\begin{pmatrix} p\cos^2\phi+\frac{1-p}{2^n} & 0 & 0 & p\cos\phi\sin\phi & \\ 0 & \frac{1-p}{2^n} & 0 & 0 & \\ 0 & 0 & \frac{1-p}{2^n} & 0 & \\ p\cos\phi\sin\phi & 0 & 0 & p\sin^2\phi+\frac{1-p}{2^n} & \\ & & & & \frac{1-p}{2^n}\mathbb{1}_{2^n-4} \end{pmatrix}, \tag{10}$$

where the upper-left 4×4 describes the space spanned by $|x_y\rangle|x_{\bar{y}}\rangle$, $|x_y\rangle|\psi_{\bar{y}}^{\perp}\rangle$, $|\psi_y^{\perp}\rangle|x_{\bar{y}}\rangle$, and $|\psi_y^{\perp}\rangle|\psi_{\bar{y}}^{\perp}\rangle$. We can readily take the partial transpose of this and calculate the eigenvalues: $\frac{1-p}{2^n}$ (repeated 2^n-4 times), $\frac{p}{2}(1\pm\cos(2\phi))+\frac{1-p}{2^n}$, and $\frac{1-p}{2^n}\pm\frac{p}{2}\sin(2\phi)$. Hence,

$$M_y = 1 - \frac{1-p}{2^{n-1}} + p\sin(2\phi).$$

This is maximized at $\phi = \pi/4$, indicating that for all bipartitions, and at all points during the computation,

$$M < 1 + p - \frac{1-p}{2^{n-1}}. \tag{11}$$

When p is exponentially small, the entanglement is always exponentially small and there is still a provable (oracle-based) speedup in searching over the classical case. This compares favorably to the DQC1 model, wherein typical unitaries

have been numerically shown to produce exponentially small amounts of entanglement [9], while having a believed speedup over classical.

B. Quantum discord

Perhaps it is not entanglement that needs to be present in a mixed-state quantum computation. Instead, other measures of nonclassicality, such as the quantum discord, have arisen. If exponentially small entanglement might be considered surprising, perhaps it is the case that there is finite quantum discord? We now show that the discord is also vanishingly small. A precise definition [12,13] of the discord is unnecessary. It suffices to know that it is a non-negative quantity which is always 0 in the classical limit and, for pure states, reduces to the entanglement entropy.

We take $\rho(\theta)$ as for the previous calculation,

$$\begin{pmatrix} p\cos^2\phi+\frac{1-p}{2^n} & 0 & 0 & p\cos\phi\sin\phi & \\ 0 & \frac{1-p}{2^n} & 0 & 0 & \\ 0 & 0 & \frac{1-p}{2^n} & 0 & \\ p\cos\phi\sin\phi & 0 & 0 & p\sin^2\phi+\frac{1-p}{2^n} & \\ & & & & \frac{1-p}{2^n}\mathbb{1}_{2^n-4} \end{pmatrix},$$

and define a second state

$$\sigma = \begin{pmatrix} p\cos^2\phi+\frac{1-p}{2^n} & 0 & 0 & 0 & \\ 0 & \frac{1-p}{2^n} & 0 & 0 & \\ 0 & 0 & \frac{1-p}{2^n} & 0 & \\ 0 & 0 & 0 & p\sin^2\phi+\frac{1-p}{2^n} & \\ & & & & \frac{1-p}{2^n}\mathbb{1}_{2^n-4} \end{pmatrix}.$$

By virtue of being diagonal with respect to a separable basis, the state σ has 0 discord [18] and yet is very close in terms of trace distance to ρ:

$$d = \mathrm{Tr}|\rho-\sigma| = p\sin(2\phi).$$

The quantum discord is continuous [19,20], meaning that we can bound the amount of discord present in $\rho(\theta)$ [19],

$$D(\rho) \leqslant 8d(n-1) + 4h(d), \tag{12}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy. This scales as $O(n2^{-n(\frac{1}{2}-\varepsilon)})$ and is, therefore, also vanishingly small across all bipartitions simultaneously, and for all steps of the algorithm.

C. Decomposing the oracle

An oracle-based problem (whether this is explicit, as for Grover's search, or implicit, requiring the implementation of controlled U in the DQC1 model) is useful for determining the computational complexity of a problem (with respect to that oracle), often enabling lower bounds as well as upper bounds. However, it has the potential to mask a lot of the entanglement properties. If one has to implement an oracle by using a collection of smaller, more manageable, operations, we need to be sure that each of those individual operations does not leave an intermediate state that has large amounts of entanglement. After all, there are many quantum computations that start and end in separable states, and it is only the intermediate products that are entangled. The Bernstein-Vazirani algorithm is one case that hides all the entanglement in such a way [14,15]. Typical DQC1 computations probably also hide their entanglement: imagine decomposing U in terms of one-qubit unitaries and controlled nots and implementing the controlled U by consecutively applying the appropriate controlled-one-qubit and Toffoli gates.[1] The first Toffoli gate is likely to introduce a finite amount of entanglement.

We claim that there need be no corresponding difficulty when using Grover's search. The Grover iterator may be written as

$$H^{\otimes n}P_0H^{\otimes n}P_{x_0},$$

where H is the Hadamard gate, and P_x is an n-qubit controlled-phase gate which adds a phase of π only to state $|x\rangle$, and P_0 is the reflection operator (which works as P_{x_0}, but acting on $|0\rangle^{\otimes n}$ instead of $|x_0\rangle$). Let us take each step in turn. If ρ_{in} is the state before the action of the iterator, and ρ_{out} is the state after the application, then our results so far show that both have exponentially small entanglement and discord. Now, observe that after the action of P_{x_0}, the form of ρ_{in} in Eq. (10) is only changed by adding a negative sign to the off-diagonal elements. Both the entanglement and the discord are unchanged. Application of a set of local unitaries ($H^{\otimes N}$) also cannot change these values. What about the application of P_0? Instead, we observe that after the action by P_0, this is the same as state ρ_{out} with $H^{\otimes n}$ applied to it, which must have the same entanglement properties as ρ_{out}.

Should we decompose the operations any further, perhaps by writing P_{x_0} in terms of a universal set of two-qubit gates? We suggest that this is unnecessary, as it appears that in a wide variety of experimental implementations, the gate P_{x_0} can be implemented directly [21–23]. So, we are justified in our claim that every elementary step of the algorithm leaves us in a state of almost no entanglement and almost no discord.

IV. CONCLUSIONS

One of the aspects of the DQC1 model of computation that originally generated much interest was the suggestion that it achieved its computational speedup without entanglement. In

[1]This is certainly far from the only decomposition that one could make, and this is merely an illustrative argument.

fact, it does use entanglement [9], and that entanglement can be up to a finite amount across many different bipartitions of the system. Even on those bipartitions for which there is no entanglement, it has been shown [5] instead that other measures of nonclassicality are present in finite amounts and could be a resource for the computational speedup that is believed to be present in the DQC1 model.

In this paper, we have contrasted this with Grover's search when acting on an initial state that has a large admixture of the maximally mixed state. The degree of admixture for which a computational speedup is still possible (without any attempt at error correction) was readily derived, and as such, it was shown that over every bipartition both the entanglement and the quantum discord are vanishingly small. Moreover, we know that the computational speedup is present for Grover's search, since we know the minimum running time for the classical algorithm (using a certain oracle). We conclude that the DQC1 is nothing special: Grover's search exhibits stronger properties in every way (guaranteed vs assumed speedup, guaranteed exponentially little entanglement vs little entanglement on average, exponentially little discord vs finite discord), except for one feature: the DQC1 model is believed to have an exponential speedup, while Grover's search is only polynomial.

The presence of quantum discord in the DQC1 model has been taken by a number of authors as "the first real evidence that mixed-state quantum computation can have an advantage over classical computation even when entanglement is absent" [24], choosing to view almost no entanglement as essentially equivalent to no entanglement. However, here, we have almost no entanglement and almost no quantum discord (and, indeed, any measure of quantum resource that is continuous). We are left to conclude that there is a marked difference between "almost no" and "no" entanglement or discord. Exactly what is required for a computation to gain speed over a classical one remains unclear, but it seems that only small amounts of whatever resource suffice. However, this leaves open the possibility that larger amounts of a resource, such as quantum discord, are necessary for an exponential vs polynomial speedup. In this context, it is interesting to contrast with the results of [25], wherein it is shown that any quantum computation (including those with exponential speedups) can be rewritten such that it has an amount of entanglement that vanishes polynomially quickly (for a broad class of entanglement measures), while the current study has demonstrated the case of exponentially little entanglement.

On a final note, we wish to raise an important issue with the calculation of the typical entanglement [9] or discord [5] across a bipartition in the DQC1 computation. The decision problem for the DQC1 model was defined by explicitly bounding the trace away from 0. However, typical unitaries have an expected trace of 0, and the trace is closely centered on the 0 value. As such, the decision problem explicitly asserts that the unitaries involved are not typical, and further studies are required to clarify the impact of this, although the studies of special cases that are performed in the Appendix suggest that the impact is not significant.

ACKNOWLEDGMENT

We thank L. C. Kwek for introductory conversations.

APPENDIX: TYPICAL ENTANGLEMENT

In this Appendix, we illustrate some important features of the calculation of typical entanglement in the DQC1 model. Rather than permitting an arbitrary Haar-random unitary, we concentrate on a subset of unitaries, based on graph states, that facilitate simpler calculations. We define the random unitary, U, in the following way: consider n qubits and select a random diagonal matrix, meaning that each diagonal element is selected at random to be $e^{i\theta_x}$ for all $x \in \{0,1\}^n$. We then conjugate this with Hadamard gates on each qubit (i.e., both before and after the diagonal matrix) before conjugating by controlled phase gates between all pairs of qubits $(i,i+1)$. These conjugations are the unitaries required for preparing the one-dimensional cluster state.

The reason for concentrating on graph states is that there is a well-established formalism for calculating the partial transpose [8,26,27]. If the eigenvalues of U are written as a vector,

$$|\Theta\rangle = \sum_x e^{i\theta_x}|x\rangle,$$

then the eigenvalues of $U_{01010101\ldots01}$ are given by the vector $R|\Theta\rangle$, where

$$R = H^{\otimes n}\left(\sum_{x\in\{0,1\}^n}(-1)^{\sum_{i=1}^{n-1}x_ix_{i+1}}|x\rangle\langle x|\right)H^{\otimes n}.$$

Lemma 1. If n is even, then every matrix element of R has $|\langle y|R|z\rangle| = \frac{1}{2^{n/2}}$. In every row, there are $\frac{1}{2}(2^n + 2^{n/2})$ positive entries and $\frac{1}{2}(2^n - 2^{n/2})$ negative entries.

Proof. The matrix elements have the form

$$\langle y|R|z\rangle = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(z+y)}(-1)^{\sum_{i=1}^{n-1}x_ix_{i+1}}.$$

First, observe that $\langle y|R|z\rangle = \langle 000\ldots0|R|z\oplus y\rangle$, so it suffices to concentrate solely on the first row. The elements in all other rows are just permutations of the first. We denote the elements in this first row R_z.

Note that

$$\sum_{z\in\{0,1\}^n} R_z = 1.$$

This means that if it is true that all 2^n elements have $|R_z| = 1/2^{n/2}$, then since they are all real, it must be that there are $\frac{1}{2}(2^n + 2^{n/2})$ positive entries and $\frac{1}{2}(2^n - 2^{n/2})$ negative entries.

We prove the first half of Lemma 1 by induction, using the base case of $n = 2$:

$$R(00) = \tfrac{1}{2}, \quad R(01) = \tfrac{1}{2}, \quad R(10) = -\tfrac{1}{2}, \quad R(11) = \tfrac{1}{2}.$$

Assume that $|R^{(n-2)}(z)| = \frac{1}{2^{n/2-1}}$. Now consider $R^{(n)}(z\|z_{n-1}z_n)$. For each term x in the sum for $R^{(n-2)}(z)$, there are four terms in $R^{(n)}(z\|z_{n-1}z_n)$: $x\|x_{n-1}x_n$. We can consider each of them separately, and how they affect the additional phases:

$$(-1)^{z_nx_n+z_{n-1}x_{n-1}+x_nx_{n-1}+x_{n-1}x_{n-2}}.$$

One of the phases can be moved into an effective z:

$$R^{(n)}(z\|z_{n-1}z_n) = \frac{1}{4}\sum_{x_n,x_{n-1}} (-1)^{z_n x_n + z_{n-1}x_{n-1} + x_n x_{n-1}} \times R^{(n-2)}(z \oplus (00\ldots0x_{n-1})).$$

Upon performing the sum over x_n, we have either $\frac{1}{2}R^{(n-2)}(z)$ (if $z_n = 0$) or $\frac{1}{2}R^{(n-2)}(z \oplus (00\ldots01))$. By assumption, both have the same absolute value, $1/2^{n/2}$.

Our aim is to evaluate the multiplicative negativity:

$$M_y = 1 + \frac{1}{2^n}\sum_{\lambda\in R|\Theta\rangle:\lambda>1} (\lambda - 1).$$

We assume that each element of $R|\Theta\rangle$ is independent (this may not be strictly true but is a good approximation). This reduces M_y to $M_y = 1 + E$, where E is the expected value of $\max(\lambda - 1, 0)$. To evaluate this, we need the probability distribution for λ. As a consequence of Lemma 1, we have

$$P(\lambda \geqslant 1) = P\left(\left|\sum_{i=1}^{\frac{1}{2}(2^n+2^{n/2})} e^{i\theta_i} - \sum_{i=\frac{1}{2}(2^n+2^{n/2})+1}^{2^n} e^{i\theta_i}\right| \geqslant 2^{n/2}\right).$$

However, if the probability distribution of θ_i is unaffected by a π shift, this is entirely equivalent to

$$P\left(\left|\sum_{i=1}^{2^n} e^{i\theta_i}\right| \geqslant 2^{n/2}\right).$$

We consider two cases. First, each θ_i is a random choice, $\theta_i \in \{0,\pi\}$. In this case, $|\sum_{i=1}^{2^n} e^{i\theta_i}|$ is simply the expected distance of a random walk in one dimension. Second, $\theta_i \in [0,2\pi)$ leads to the interpretation of $|\sum_{i=1}^{2^n} e^{i\theta_i}|$ as a random walk in two dimensions.[2] In either case, Rayleigh's solution for the probability distribution at large n is

$$P\left(x \leqslant \left|\sum_{i=1}^{2^n} e^{i\theta_i}\right| < x+\delta x\right) = \begin{cases} \sqrt{\frac{2}{\pi 2^n}} e^{-x^2/2^{n+1}} dx, & \text{1D}, \\ \frac{2x}{2^n} e^{-x^2/2^n} dx, & \text{2D}, \end{cases}$$

in order to calculate

$$E = \int_{2^{n/2}}^{\infty} P\left(x \leqslant \left|\sum_{i=1}^{2^n} e^{i\theta_i}\right| < x + \delta x\right)\left(\frac{x}{2^{n/2}} - 1\right),$$

which yields

$$E = \begin{cases} \sqrt{\frac{2}{\pi e}} - \operatorname{erfc}\left(\frac{1}{\sqrt{2}}\right), & \text{1D}; \\ \frac{\sqrt{\pi}}{2}\operatorname{erfc}(1), & \text{2D}. \end{cases} \quad \text{(A1)}$$

Figure 2 provides numerical confirmation of this calculation. We conclude that in both cases there is a constant amount of entanglement. This is in contrast with the numerical results in [9] for general random unitaries.

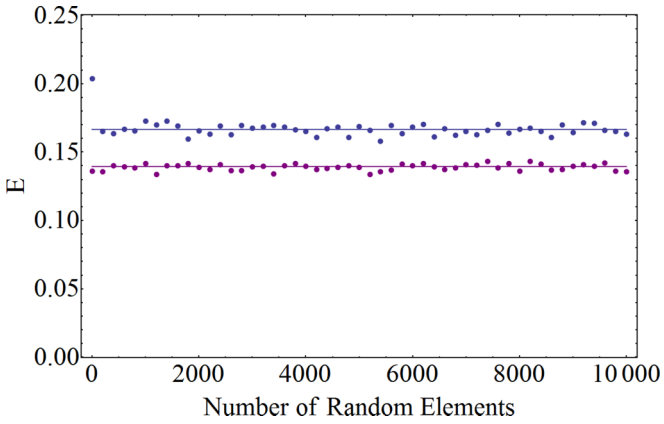

FIG. 2. (Color online) Comparison of theoretical results (lines), Eq. (A1), and average for 10 000 samples (points) for both 1D [upper (blue) line] and 2D [lower (purple) line] random walks.

However, there is one further subtlety that it is important to raise. Recall that for the DQC1 model we are given the promise that the trace of U is bounded away from 0. Meanwhile, the probability distribution for the trace of a typical unitary is strongly centered on the value 0: in effect, we are postselecting on highly atypical unitaries so typicality arguments might not reveal everything. However, it turns out that this only serves to reduce the amount of entanglement present. For a simple argument, consider the case where $\mathrm{Tr}(U) = 2^n$. In this case, we know that $U = \mathbb{1}$ and that $M_y = 1$, less than the above-calculated values. More generally, we have numerically examined the random unitary model described above (restricting the eigenvalues to ± 1), fixing the trace to be different values of $\mathrm{Tr}(U)$ (see Fig. 3). The amount of entanglement present decreases as the value of the trace is increased.

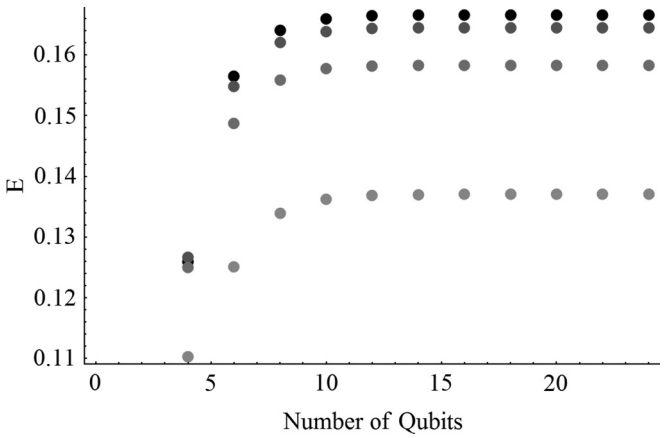

FIG. 3. Typical entanglement for a graph diagonal unitary of fixed trace $\mathrm{Tr}(U)/2^n = \frac{1}{4}, \frac{5}{8}, \frac{3}{4}$, and $\frac{7}{8}$ for shades black through light gray, respectively. The larger the trace, the less entanglement is present.

[2]We define this to be a walk such that at each step, a step length of 1 is taken in a random direction in the plane. Some authors choose to define it as a walk on a square lattice.

[1] R. Jozsa and N. Linden, Proc. R. Soc. Lond. A **459**, 2011 (2003).
[2] B. Eastin, arXiv:1006.4402.
[3] H. Cable and D. E. Browne, New J. Phys. **17**, 113049 (2015).
[4] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[5] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[6] S. Luo, Phys. Rev. A **77**, 022301 (2008).
[7] T. S. Cubitt, F. Verstraete, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **91**, 037902 (2003).
[8] A. Kay, Phys. Rev. Lett. **109**, 080503 (2012).
[9] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
[10] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1996), p. 212.
[11] E. Biham and D. Kenigsberg, Phys. Rev. A **66**, 062301 (2002).
[12] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[13] L. Henderson and V. Vedral, J. Phys. A: Math. Gen. **34**, 6899 (2001).
[14] E. Bernstein and U. Vazirani, in *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1993), p. 11.
[15] D. A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).
[16] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
[17] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
[18] A. Datta, arXiv:1003.5256.
[19] Z. Xi, X.-M. Lu, X. Wang, and Y. Li, J. Phys. A: Math. Theor. **44**, 375301 (2011).
[20] A. Brodutch and K. Modi, Quantum Info. Comput. **12**, 721 (2012).
[21] H. Goto and K. Ichimura, Phys. Rev. A **70**, 012305 (2004).
[22] C.-P. Yang and S. Han, Phys. Rev. A **72**, 032311 (2005).
[23] X.-M. Lin, Z.-W. Zhou, M.-Y. Ye, Y.-F. Xiao, and G.-C. Guo, Phys. Rev. A **73**, 012323 (2006).
[24] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).
[25] M. Van den Nest, Phys. Rev. Lett. **110**, 060504 (2013).
[26] A. Kay, Phys. Rev. A **83**, 020303 (2011).
[27] A. Kay, J. Phys. A: Math. Theor. **43**, 495301 (2010).