

Entanglement and deterministic quantum computing with one qubit

Michel Boyer,^{1,*} Aharon Brodutch,^{2,3,†} and Tal Mor^{4,‡}

¹*DIRO, Université de Montréal, Montréal, Québec, Canada*

²*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

³*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

⁴*Computer Science Department, Technion, Haifa, Israel*

(Received 27 July 2016; published 21 February 2017)

The role of entanglement and quantum correlations in complex physical systems and quantum information processing devices has become a topic of intense study in the past two decades. In this work we present tools for learning about entanglement and quantum correlations in dynamical systems where the quantum states are mixed and the eigenvalue spectrum is highly degenerate. We apply these results to the deterministic quantum computing with one qubit (DQC1) computation model and show that the states generated in a DQC1 circuit have an eigenvalue structure that makes them difficult to entangle, even when they are relatively far from the completely mixed state. Our results strengthen the conjecture that it may be possible to find quantum algorithms that do not generate entanglement and yet still have an exponential advantage over their classical counterparts.

DOI: [10.1103/PhysRevA.95.022330](https://doi.org/10.1103/PhysRevA.95.022330)

I. INTRODUCTION

Quantum computing is a promising theoretical field that mainly deals with problems that are hard for regular computers and are easy for a quantum computer [1–3]. Experiments in quantum computing devices do not yet employ many qubits, and the most successful approaches can deal with only 7–14 qubits [4–7]. While many experimental and theoretical efforts are geared towards the implementation of universal quantum machines with more qubits, there could be considerable advantages with other less powerful models which we call *semiquantum computer* (SQC) models.

SQCs outperform classical computers for some tasks while being less powerful and potentially less technologically demanding than universal quantum computers. For more than a decade, there have been various descriptions of SQCs that could demonstrate a quantum advantage (sometimes called *quantum supremacy* [8]). In some cases these models do not even require or produce entanglement [9–12].

Among the candidate SQC models are those such as quantum annealers [13], which may be able to beat classical computers in a benchmarking experiment but do not seem to offer an exponential advantage (in the input size). Other candidate models, which we call subuniversal quantum computers (SuQCs), probably do offer an exponential advantage for a few specific tasks but remain subuniversal. Three prominent examples of SuQCs are the linear optics model [14], instantaneous quantum computing [15], and deterministic quantum computing with one qubit (DQC1) [16].

For each (candidate) SuQC model there are three important questions we can ask:

(1) What hard problems can it solve efficiently, and are these problems interesting (e.g., for science or industry)?

(2) Is it indeed much more feasible experimentally, and if so, why?

(3) What are the conceptual properties that make it (exponentially) more powerful than a classical computer?

Briefly, let us mention the status of DQC1 in connection to the first two questions: A generic problem for the DQC1 model is the trace estimation problem, i.e., estimating the normalized trace of an efficiently implementable unitary operation. For some subsets of n -qubit unitaries this problem is believed to be hard for a classical computer [17,18]; that is, there is good evidence that it is impossible to find a classical polynomial time (in n) algorithm for estimating the normalized trace. For example, it is possible to use the DQC1 model to estimate the Jones polynomial at a fifth root of unity for the trace closure of a braid. This special case is complete for DQC1 and was implemented experimentally on four qubits [19]. The model is, however, an idealization as it assumes no errors in the implementation. It is currently unknown if DQC1 is a viable model that can be scaled up in the presence of imperfections.

Here we deal with the third question with regards to DQC1. Our approach is to study the space of quantum states that can be generated during the computational process and, in particular, study the correlations within these states. This approach follows earlier works on the circuit model [20,21], DQC1 [22–27], measurement-based quantum computing [28], and other models [10]. As in these works, we do not take error correction into account.

For pure-state quantum circuits, Vidal [21] showed that a circuit can be efficiently simulated on a classical computer when the amount of entanglement is not large [i.e., the maximal Schmidt rank over all bipartition grows slower than $\log(n)$] at all times. Jozsa and Linden [20] showed that there is an efficient classical simulation of a quantum circuit if the register has a p -block structure for constant p at all times. An n -qubit state ρ has a p -block structure if $\rho = \bigotimes_j \rho_j$ and ρ_j are $m_j \leq p$ qubit states. This structure implies that the blocks are not correlated. When ρ is pure, the lack of correlations means that there is no entanglement between blocks of qubits. Preliminary results on the DQC1 model [23,29] have given some reason to suspect that discord, a more general measure of quantum correlations,

*boyer@iro.umontreal.ca

†Present address: Center for Quantum Information and Quantum Control, University of Toronto, Toronto, Ontario, Canada; brodutch@physics.utoronto.ca

‡talmo@cs.technion.ac.il

may play a role similar to pure state entanglement in this context.

For any measure of quantum correlations (e.g., entanglement or discord) and any specific way of quantifying these correlations \mathcal{C} , we may ask if one of the following is a necessary condition for computational speedup:

(1) At some point in the algorithm the register must have large amounts of quantum correlations \mathcal{C} for at least one bipartition.

(2) At some point in the algorithm the register must have some quantum correlations for exponentially many bipartitions.

By large amounts we mean that \mathcal{C} scales in a way similar to its upper bound [for example, if \mathcal{C} is the entanglement monotone *negativity* [30], it should scale faster than $\text{polylog}(n)$].

There is already strong evidence that statement 1 is not valid for entanglement [17]; that is, it is known that entanglement quantified by multiplicative negativity at any point in a DQC1 circuit is bounded from above by a constant. Moreover, for universal quantum computing, it is known that statement 1 can be true only for particular choices of entanglement measures [31]. There is some evidence to support statement 1 for other types of quantum correlations [29]; that is, in DQC1 the correlations as measured by the operator Schmidt rank grow quickly with the system size [22], and there is discord between the first qubit and the rest of the system [23]. However, the latter statement does not imply that there are large amounts of discord for a bipartition that can support a lot of discord; moreover, it is known that the results on discord are not symmetric; that is, there is no discord if the measurements are made on the last n qubits [29].

Our results below are related to statement 2. We present tools to study entanglement in degenerate quantum systems undergoing unitary evolution and show that while general DQC1 circuits can generate a state which is entangled over many bipartitions, this entanglement is always more sensitive to depolarizing noise than a generic quantum state. We also show that specific DQC1 complete circuits have less entangling power than generic circuits. As a conclusion of our results, we conjecture that statement 2 is probably violated for entanglement [i.e., for DQC1 with large α ; see Eq. (1)]. The evidence in support of statement 2 for discord is significantly stronger since discord is more robust to depolarizing noise.

II. DEFINITIONS

A. Entanglement and discord

A state ρ on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be separable with respect to the bipartition $\{A; B\}$ if and only if it can be decomposed as $\rho = \sum_i \rho_i^A \otimes \rho_i^B$, where ρ_i^A are states on \mathcal{H}_A and ρ_i^B are states on \mathcal{H}_B . If ρ is not separable, it is entangled. A sufficient condition for entanglement is that the partial transpose of ρ denoted $(T \otimes \mathbb{1})(\rho)$ has a negative eigenvalue. Such a state is said to be a nonpositive partial transpose (non-PPT) state; non-PPT states are entangled. If there are two pure states $|\psi\rangle, |\phi\rangle$ such that $\langle\phi|(T \otimes \mathbb{1})(\rho)|\phi\rangle = 0$ while $\langle\psi|(T \otimes \mathbb{1})(\rho)|\psi\rangle \neq 0$, then ρ is non-PPT [32].

While most quantum states on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ are entangled when the Hilbert space dimensions are large, there is

always a ball of separable states around the completely mixed state; that is, for an n -qubit system and a given bipartition there is a finite ϵ such that all τ with $\|\tau - \frac{1}{2^n} \mathbb{1}\|_1 < \epsilon$ are separable [33]. One implication is that for small n , a room-temperature liquid-state NMR processor is never entangled for any bipartition [34].

States on the boundary of separable states are called *boundary separable* [32]. Here we define a new subset of boundary separable states (see Appendix B for proof that this is a subset).

Definition 1. A separable state ρ is *boundary separable in its unitary orbits* if for all $\epsilon > 0$ there is a unitary U^ϵ with $\|U^\epsilon - \mathbb{1}\| < \epsilon$ such that $U^\epsilon \rho U^{\epsilon\dagger}$ is entangled.

This subset is particularly relevant to systems undergoing unitary dynamics. Some states cannot be entangled by any unitary operation on the system [35].

Definition 2. A state ρ is called *separable from spectrum* if for all unitaries U the state $U\rho U^\dagger$ is separable. Similarly, it is *PPT from spectrum* if for all unitaries U the state $U\rho U^\dagger$ is PPT.

Discord is an asymmetric measure of quantum correlations. A bipartite quantum state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is zero discord with respect to a measurement on subsystem A if and only if [29,36,37] there is a basis of states $\{|l\rangle\}$ for \mathcal{H}_A such that $\rho = \sum_l a_l |l\rangle\langle l|^A \otimes \rho_l^B$, with ρ_l^B states on \mathcal{H}_B . If ρ is not zero discord, it is discordant. For pure states, discord is symmetric and coincides with entanglement; moreover, any entangled state is always discordant for measurements on either subsystem [29]. Unlike separable states, the set of zero-discord states is nowhere dense [38]; that is, there is no ball of zero discord states.

B. DQC1

The input to an $n + 1$ qubit DQC1 circuit is a $\text{poly}(n)$ description of a unitary quantum circuit U that can be implemented efficiently as a $\text{poly}(n)$ sequence of one- and two-qubit gates chosen from a universal gate set. The circuit is applied to the initial $(n + 1)$ -qubit state

$$\rho_n^\alpha = \frac{1 - \alpha}{2^n} |0\rangle\langle 0| \otimes \mathbb{1}_n + \frac{\alpha}{2^{n+1}} \mathbb{1}_{n+1}. \quad (1)$$

After the evolution, the first qubit is measured, and the expectation values of an operator $\sigma_\mu \in \{\sigma_y, \sigma_x\}$ on the first qubit are recorded;¹ that is, the output of the computation is

$$\text{tr}[U\rho_n^\alpha U^\dagger \sigma_\mu] = \frac{1 - \alpha}{2^n} \text{tr}[U(|0\rangle\langle 0| \otimes \mathbb{1}_n)U^\dagger (\sigma_\mu \otimes \mathbb{1}_n)]. \quad (2)$$

Note that we define DQC1 as an estimation problem and use the term *complete* below in that context.

We define cDQC1 to be the subset of DQC1 circuits with the restriction $U = [|0\rangle\langle 0| \otimes \mathbb{1}_n + |1\rangle\langle 1| \otimes V] H_1$, where V is a unitary that can be efficiently decomposed into a polynomial

¹Our results concern the intermediate states, so they also apply to more general algorithms where the readout is not restricted. Such versions of DQC1 have been considered in the past, although it is not clear how far one can relax this restriction before making DQC1 universal.

number of one- or two-qubit gates and H_1 is a Hadamard gate on the first qubit. This family of controlled unitaries is vanishingly small in the set of all $(n + 1)$ -qubit unitaries. Nevertheless, it is sufficient for solving problems that are DQC1 complete [18], and most of the results regarding correlations in DQC1 were restricted to this model. To falsify statements about necessary conditions for computational speedup, it is sufficient to show that they do not hold for a single *complete* problem for DQC1,² so the restriction to cDQC1 is well motivated.³

We will use the notation n_{\perp} to denote the subsystem consisting of the n qubits that are initially in the maximally mixed state. In cDQC1 the first qubit in the bipartition $\{1; n_{\perp}\}$ plays a special role since it is the only qubit to have any coherence at any time. Note that $\{1; n_{\perp}\}$ is a special case of $\{1; n\}$, the set of all bipartitions that have one qubit for one party and n for the rest (there are $n + 1$ elements in the set). In general for any k we define the set of bipartitions $\{k, n + 1 - k\}$ where one party has k qubits and the other has the rest. There are overall $2^n - 1$ nontrivial bipartitions.

III. ENTANGLEMENT IN DQC1

A. The pure $\alpha = 0$ case

Knill and Laflamme [16] introduced DQC1 as an algorithm for liquid-state NMR where it is possible to efficiently initialize ρ^α with α close to 1. It is, however, instructive to consider entanglement in the idealized $\alpha = 0$ case before continuing to general α .

Lemma 1. The state ρ_n^0 is boundary separable in its unitary orbit for all $2^n - 1$ bipartitions $\{k; n + 1 - k\}$ where $0 < k \leq n$.

Proof. To find U^ϵ we start with $n = 1$. Let R_θ be the unitary that acts trivially on the subspace $\text{span}(|01\rangle, |10\rangle)^\perp$ such that $R_\theta |01\rangle = \cos \theta |01\rangle + \sin \theta |10\rangle$ and $R_\theta |10\rangle = -\sin \theta |01\rangle + \cos \theta |10\rangle$; then, for all $0 < \theta < \frac{\pi}{2}$, $R_\theta \rho_1^0 R_\theta^\dagger$ is entangled since it is non-PPT. That can be seen by noting that $\langle 11 | (T \otimes \mathbb{1})(R_\theta \rho_1^0 R_\theta^\dagger) | 11 \rangle = 0$, whereas $\langle 00 | (T \otimes \mathbb{1})(R_\theta \rho_1^0 R_\theta^\dagger) | 11 \rangle = \frac{1}{2} \cos \theta \sin \theta \neq 0$. Then, since $R_\theta = \mathbb{1}$ for $\theta = 0$, for any $\epsilon > 0$ there is $0 < \theta < \frac{\pi}{2}$ such that $\|R_\theta - \mathbb{1}\| < \epsilon$ due to the continuity of R_θ in θ , and we can take $U^\epsilon = R_\theta$. This is also true for the more general n and any bipartition; for example, if the first qubit is in part A and the l_{th} qubit is in part B , it is possible to have R_θ act on those two qubits and entangle them; the rest of the system will remain in a factorized maximally mixed state. ■

What is rather surprising is that the subclass of unitaries used in cDQC1 are precisely those that do not produce entanglement in the $\{1; n_{\perp}\}$ bipartition [29].

So, on the one hand, entanglement in the $\{1; n_{\perp}\}$ bipartition is easy in a generic DQC1 circuit (at $\alpha = 0$); on the other hand, there is a subclass, cDQC1, which is known to contain DQC1 complete problems and cannot generate entanglement in this cut. Our main result from the analysis of $\alpha = 0$ is that the existence of entanglement in the general case does not

indicate that entanglement should exist in subsets of circuits that can encode DQC1 complete problems.

B. The $\{1; n\}$ bipartition ($\alpha > 0$)

We continue with entanglement at $1 > \alpha > 0$ and a general one-qubit- n -qubit bipartition $\{1; n\}$ (of which $\{1; n_{\perp}\}$ is a special case).

Lemma 2. A DQC1 circuit cannot generate entanglement at any $\{1; n\}$ bipartition if and only if $\alpha \geq \frac{1}{2}$.

Proof. In [39], Johnston showed that given an $(n + 1)$ -qubit state with eigenvalue spectrum $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{2^{n+1}}$, the following is a necessary and sufficient condition for separability from spectrum in any $\{1; n\}$ bipartition:

$$\lambda_1 \leq \lambda_{2^{n+1}-1} + 2\sqrt{\lambda_{2^{n+1}-2}\lambda_{2^{n+1}}}. \tag{3}$$

The DQC1 state has a degenerate spectrum with two eigenvalues, $\frac{2-\alpha}{2^{n+1}}$ and $\frac{\alpha}{2^{n+1}}$, each with degeneracy 2^n . So condition (3) is violated for $\alpha \geq \frac{1}{2}$. ■

Lemma 2 is surprising since $\|U\rho_n^\alpha U^\dagger - \frac{1}{2^{n+1}}\mathbb{1}\|_1 = 1 - \alpha$ so $U\rho_n^\alpha U^\dagger$ is separable, but far outside the ball of separable states at large n . To see this, take the state $\tau = \sum_{i=2}^{2^{n+1}-1} \frac{1}{2^{n+1}-2} |i\rangle\langle i|$ with $\|\tau - \frac{1}{2^{n+1}}\mathbb{1}\| = \frac{2}{2^n}$. Since τ has eigenvalues $\lambda_{2^{n+1}} = \lambda_{2^{n+1}-1} = 0$, then, by Eq. (3), for any $\{1; n\}$ bipartition there is some U such that $U\tau U^\dagger$ is entangled and therefore outside the ball of separable states. This result shows that entanglement in the set $U\rho_n^\alpha U^\dagger$ is particularly sensitive to noise in the initial state.

The result above complements the result of Datta, Flammia, and Caves [17], who found an explicit family of unitaries such that for $\alpha < \frac{1}{2}$ the state $U\rho_n^\alpha U^\dagger$ is entangled for any bipartition. Furthermore, these states are not PPT, which is consistent with evidence that PPT from spectrum is the same as separable from spectrum [40].

C. General bipartitions ($\alpha \geq 0$)

Moving to the more general case, we build on the results of Hildebrand [35], who provided a necessary and sufficient condition for a state to be PPT from spectrum. Hildebrand's general condition (see Theorem 1) is generally difficult to apply to states with a generic eigenvalue spectrum. In Sec. A 2 we show how to apply this result to the highly degenerate states in the set $S_{m,n}^{\lambda_+, \lambda_-}$ defined in Definition 7. The DQC1 states are in this set, and the following is a special case of Lemma 5:

Lemma 3. Let ρ be a state on $\mathcal{H}_k \otimes \mathcal{H}_{n-k+1}$ with $k < \frac{n+1}{2}$. If ρ has two eigenvalues $\lambda_1 > \lambda_2$, each with degeneracy 2^k , then ρ is PPT from spectrum if and only if $\frac{1}{2}(\lambda_1 + \lambda_2) - 2^{k-1}(\lambda_1 - \lambda_2) \geq 0$.

Proof. Using the notation defined in Appendix A, we have $p = 2^k$, $p_+ = 2^{k-1}(2^k - 1) \leq 2^n$, and of course $p_- \leq 2^n$, so that $\rho \in S_{k,n-k+1}^{\lambda_2, \lambda_1}$ and Lemma 5 applies. ■

Lemma 4. A necessary condition and a sufficient condition for ρ_n^α to be PPT from spectrum for all bipartitions of the $n + 1$ qubits ($n \geq 2$) are, respectively,

$$\alpha \geq 1 - \frac{1}{2^{\lfloor \frac{n}{2} \rfloor}}, \quad \alpha \geq 1 - \frac{1}{2^{\lfloor \frac{n+1}{2} \rfloor}}, \tag{4}$$

where $\lfloor x \rfloor$ is the floor of x (i.e., x rounded down to the nearest integer).

²Assuming DQC1 is a SuQC.

³However, one should be careful since the reduction may require additional qubits.

Proof. The two eigenvalues of ρ_n^α are $\lambda_1 = \frac{2-\alpha}{2^{n+1}}$ and $\lambda_2 = \frac{\alpha}{2^{n+1}}$. By Lemma 3, ρ_n^α is PPT from spectrum for any $\{k; (n+1-k)\}$ cut with $1 \leq k < \frac{n+1}{2}$ if and only if

$$\alpha \geq 1 - \frac{1}{2^k}. \quad (5)$$

If $n = 2m$, $k < \frac{n+1}{2}$ if and only if $k \leq m = \lfloor \frac{n}{2} \rfloor = \lfloor \frac{n+1}{2} \rfloor$ and the conditions coincide, giving a necessary and sufficient condition.

If $n = 2m + 1$, $\{m+1; m+1\}$ bipartitions are to be handled separately. If $U\rho_n^\alpha U^\dagger$ is not PPT for a $\{m+1; m+1\}$ bipartition, then $(U \otimes \mathbb{1})\rho_{n+1}^\alpha(U \otimes \mathbb{1})^\dagger$ is not PPT for a $\{m+1; m+2\}$ bipartition; consequently, if $\alpha \geq 1 - \frac{1}{2^{\lfloor \frac{n+1}{2} \rfloor}} = 1 - \frac{1}{2^m}$ for $k = m+1$, then by (5), ρ_{n+1}^α is PPT from spectrum for $\{m+1; m+2\}$ bipartition, and thus ρ_n^α is PPT from spectrum also for $\{m+1; m+1\}$ bipartitions. That proves the sufficiency condition.

If $n = 2m + 1$ and if $U\rho_{n-1}^\alpha U^\dagger$ is not PPT for a $\{m; m+1\}$ bipartition, then $(U \otimes \mathbb{1})\rho_n^\alpha(U \otimes \mathbb{1})^\dagger$ is not PPT for a $\{m+1; m+1\}$ bipartition; thus, if ρ_n^α is PPT from spectrum for $\{m+1; m+1\}$ bipartitions, then ρ_{n-1}^α is PPT from spectrum for $\{m; m+1\}$ bipartitions, implying by Eq. (5) with $k = m = \lfloor \frac{n}{2} \rfloor$ that $\alpha \geq 1 - \frac{1}{2^{\lfloor \frac{n}{2} \rfloor}}$. ■

The scaling of this condition means that for any fixed α or even for $\alpha < 1 - \frac{1}{\text{Poly}(n)}$ there will always be states that are entangled for some U and large enough n . Moreover, the number of bipartitions for which this statement holds grows exponentially with the size of n . In a follow-up paper [41] we show how to construct an explicit family of U such that $U\rho_n^\alpha U^\dagger$ is not PPT when condition (5) is violated.

D. Discord

The lack of entanglement for low n in liquid-state NMR experiments and DQC1 led to various conjectures about discord as a more appropriate signature of the quantum advantage [10,25,26]. Datta *et al.* [23] provided evidence for this conjecture by showing that the separable $\{1; n_\perp\}$ bipartite cut in cDQC1 was usually discordant with respect to a measurement on the first qubit. This state is, however, never discordant with respect to a measurement on n_\perp [29]. Moreover, there are also (seemingly DQC1 complete) subsets of cDQC1 where the final state is not discordant for a measurement on the first qubit [42]; however, even in these circuits the state may be discordant at some intermediate time [29].

For a qualitative study of the role of discord in DQC1 it is enough to study the “clean” case $\alpha = 0$. This follows from the fact that an $(n+1)$ -qubit state of the form $(1-\alpha)\rho + \alpha\frac{\mathbb{1}}{2^{n+1}}$ is discordant if and only if ρ is discordant [43]. This fact, together with the fact that entanglement implies discord, means that for any bipartition and any α there are unitaries U such that $U\rho_n^\alpha U^\dagger$ is discordant with respect to a measurement on either subsystem and any other bipartition.

IV. CONCLUSIONS

Questions regarding the role of entanglement in quantum computing algorithms have been studied since the first quan-

tum algorithms were tested in liquid-state NMR. The DQC1 algorithm was designed as a test bed for answering these questions, but even with this simplified model the results are inconclusive. Here we studied the ability of DQC1 to generate entanglement under various constraints.

Noise in the initial state [i.e., α in Eq. (1)] determines the ability of a generic circuit to generate entanglement. We showed that in any $\{1; n\}$ bipartition, a circuit cannot generate entanglement when $\alpha \geq \frac{1}{2}$ (Lemma 2). We also provided a necessary and sufficient condition for the DQC1 circuit to generate non-PPT states [Eq. (5)].

We defined a property called boundary separable in unitary orbits (Definition 1) and showed that the initial states of DQC1 at $\alpha = 0$ are easy to entangle in any bipartition (Lemma 1). On the other hand, the DQC1-complete subset, cDQC1, cannot generate entanglement in the $\{1; n_\perp\}$ cut, despite the fact that the first qubit is the only one with any coherence at any time. We conclude that there is no reason to suspect that families of DQC1-complete circuits are those that generate more entanglement than other nontrivial families of circuits.

Our most surprising result is that the entanglement in the set all of states generated in a DQC1 circuit is more fragile to depolarizing noise than a generic mixed state. Based on this and the conclusion above, we are optimistic about the possibility of finding DQC1-complete circuits where entanglement is never generated at any point for the vast majority of bipartite cuts (and possibly all bipartite cuts) at all n . Such circuits would provide extremely strong evidence that quantum computational speedup can be achieved without entanglement.

We pointed out that, at the qualitative level, the study of discord can be restricted to $\alpha = 0$. Based on that, we conclude that a subset of circuits that do not generate discord on the one hand and are DQC1 complete on the other is unlikely to exist.

We believe that the next challenge will be to find a family of DQC1 circuits which encode classically hard computational problems and, at the same time, do not generate any entanglement for most bipartitions at some $\alpha < 1 - \frac{1}{\text{Poly}(n)}$ or, conversely, give strong evidence that such a family is unlikely to exist, for example, by finding an algorithm that can simulate any separable instance of DQC1.

Our results were presented in the context of DQC1. The approaches developed here will be useful for further study of entanglement and quantum correlations in other candidate SuQCs. More generally, our methods can be applied to the study of entanglement and quantum correlation in other complex systems involving mixed quantum states.

ACKNOWLEDGMENTS

We would like to thank N. Johnston, R. Laflamme, and R. Liss for useful discussions and comments. A.B. was partly funded through NSERC, Industry Canada, and CIFAR. M.B. was partly support by NSERC and FQRNT through INTRIQ. T.M. was funded by the Wolfson Foundation and the Israeli MOD Research and Technology Unit. A.B. and T.M. were partly supported the Gerald Schwartz and Heather Reisman Foundation.

APPENDIX A: PPT FROM SPECTRUM FOR DQC1 STATES

In this Appendix we provide some general results regarding the possibility that the state $U\rho_n^\alpha U^\dagger$ is not PPT. We begin with a review of the results by Hildebrand [35] and continue to explicitly calculate the necessary and sufficient conditions for PPT from spectrum for a particular set of states where the largest and smallest eigenvalues are highly degenerate.

1. Recap of definitions and main theorem from Hildebrand [35]

a. Notations and definitions

In the following, $[n]$ denotes the set $\{1, \dots, n\}$ of n elements; $H(n)$ denotes the space of $n \times n$ Hermitian matrices or Hermitian operators on \mathcal{H}_n , and $H_+(nm)$ denotes the set of positive semidefinite $nm \times nm$ matrices or positive-semidefinite (PSD) operators on $\mathcal{H}_n \otimes \mathcal{H}_m$.

Definition 3. Let $p_+ = \frac{p(p+1)}{2}$ and $p_- = \frac{p(p-1)}{2}$ for $p \in \mathbb{N}$; also let $S_+^p = \{(i, j) \mid 1 \leq i \leq j \leq p\}$ and $S_-^p = \{(i, j) \mid 1 \leq i < j \leq p\}$. A *linear ordering* of the pairs $(i, j) \in S_+^p$ (respectively in S_-^p) is a bijective map $\sigma_+ : S_+^p \rightarrow [p_+]$ (respectively $\sigma_- : S_-^p \rightarrow [p_-]$).

Definition 4. The linear ordering $\sigma_- : S_- \rightarrow [p_-]$ is said to be *consistent* with $\sigma_+ : S_+^p \rightarrow [p_+]$ if for all $(k_1, l_1), (k_2, l_2) \in S_-^p$, $\sigma_+(k_1, l_1) < \sigma_+(k_2, l_2)$ implies $\sigma_-(k_1, l_1) < \sigma_-(k_2, l_2)$.

Remark 1. For each $\sigma_+ : S_+^p \rightarrow [p_+]$ there is exactly one $\sigma_- : S_-^p \rightarrow [p_-]$ that is consistent with σ_+ .

Definition 5. Let $x \in \mathbb{R}^p$ be a vector with non-negative entries. A *linear ordering* (σ_+, σ_-) is said to be *compatible* with x if $\sigma_+(k_1, l_1) < \sigma_+(k_2, l_2)$ implies $x_{k_1} x_{l_1} \geq x_{k_2} x_{l_2}$.

The linear ordering above is a simple way to put the products $x_k x_l$ in decreasing order for $1 \leq k \leq l \leq p$. If the products are all distinct, there is just one way. In the case of identical elements the order is not relevant.

$$\Sigma_\pm = \{(\sigma_+, \sigma_-) \mid \exists x \in \mathbb{R}^p \mid x_1 > x_2 > \dots > x_p > 0 : (\sigma_+, \sigma_-) \text{ compatible with } x\}.$$

Definition 6. If $\lambda = (\lambda_i)_{1 \leq i \leq nm}$ is a sorted list of mn real numbers in decreasing order, $p = \min(m, n)$, and (σ_+, σ_-) is a consistent pair of orderings of S_+^p and S_-^p , then $\Lambda(\lambda; \sigma_+, \sigma_-)$ is the $p \times p$ matrix defined by

$$\Lambda(\lambda; \sigma_+, \sigma_-) = \begin{cases} \lambda_{nm+1-\sigma_+(k,l)} & k \leq l, \\ -\lambda_{\sigma_-(l,k)} & k > l. \end{cases}$$

b. Main result

Theorem 1. If $A \in H_+(nm)$ has $\lambda = (\lambda_i)_{1 \leq i \leq nm}$ as eigenvalues in decreasing order, then A has a positive-semidefinite partial transpose (PPT) for all decompositions of \mathcal{H}_{nm} as a tensor product space $\mathcal{H}_n \otimes \mathcal{H}_m$ if and only if for all $(\sigma_+, \sigma_-) \in \Sigma_\pm$ the following holds:

$$\Lambda(\sigma_+, \sigma_-) + \Lambda(\sigma_+, \sigma_-)^T \geq 0.$$

Proof. See Theorem 1 of [35]. ■

2. Application to special states with a highly degenerate eigenvalue spectrum

Definition 7. For $m < n$, we define $\mathcal{S}_{m,n}^{\lambda_+, \lambda_-}$ as the set of states $\tau \in H_+(2^m 2^n)$ that have λ_+ as their largest eigenvalue with degeneracy at least $p_- = 2^{2m-1} - 2^{m-1}$ and λ_- as the smallest eigenvalue with degeneracy at least $p_+ = 2^{2m-1} + 2^{m-1}$ (note that there are $2^{m+n} - 2^{2m}$ free eigenvalues).

Lemma 5. All states $\tau \in \mathcal{S}_{m,n}^{\lambda_+, \lambda_-}$ are separable from spectrum if and only if $\frac{1}{2}(\lambda_+ + \lambda_-) - 2^{m-1}(\lambda_+ - \lambda_-) \geq 0$.

Proof. Let λ be the list of eigenvalues of $\tau \in \mathcal{S}_{m,n}^{\lambda_+, \lambda_-}$ sorted in decreasing order and $p = 2^m$; all the matrices $\Lambda(\lambda; \sigma_+, \sigma_-)$ are then equal and have the following form:

$$\Lambda_{k,l} = \begin{cases} \lambda_- & 1 \leq k \leq l \leq p, \\ -\lambda_+ & p \geq k > l \geq 1. \end{cases}$$

It follows that the off-diagonal entries of $\Lambda + \Lambda^T$ are equal to $\lambda_- - \lambda_+$ and the diagonal entries are $2\lambda_-$, and thus

$$\Lambda + \Lambda^T = (\lambda_- + \lambda_+) \mathbb{1} + (\lambda_- - \lambda_+) K,$$

where $K_{i,j} = 1$ for all $1 \leq i, j \leq p$. For any $x \in \mathbb{R}^p$

$$x^T (\Lambda + \Lambda^T) x = (\lambda_+ + \lambda_-) \|x\|^2 - (\lambda_+ - \lambda_-) \left(\sum_i x_i \right)^2,$$

and the minimum value for $\|x\| = 1$ is obtained if all x_i are equal, i.e., $x_i = \frac{1}{\sqrt{p}}$ for $1 \leq i \leq p$, giving a minimum of $(\lambda_+ + \lambda_-) - p(\lambda_+ - \lambda_-)$. By Theorem 1, τ is separable from spectrum if and only if $(\lambda_+ + \lambda_-) - p(\lambda_+ - \lambda_-) \geq 0$. ■

APPENDIX B: BOUNDARY-SEPARABLE STATES

In the main text we stated that the set of states that are boundary separable in their unitary orbits is a subset of the set of boundary-separable states. Below is proof of that statement.

Lemma 6. If ρ is boundary separable in its unitary orbits, then ρ is boundary separable.

Proof. The following inequalities apply whether $\|\cdot\|$ is the trace norm, the operator norm, or the Hilbert-Schmidt norm. Here we assume it is the trace norm. Let U be such that $\|U - \mathbb{1}\| < \epsilon/2$ and $U\rho U^\dagger$ is entangled. Using the fact that $\|\cdot\|$ is a norm (i.e., the triangle inequality holds) and that $\|A^\dagger\| = \|A\|$, $\|AB\| \leq \|A\| \|B\|$, and $\|AB\| \leq \|A\|_\infty \|B\|$,

$$\begin{aligned} \|U\rho U^\dagger - \rho\| &= \|U\rho(U^\dagger - \mathbb{1}) + (U - \mathbb{1})\rho\| \\ &\leq \|U\|_\infty \|\rho\| \|U^\dagger - \mathbb{1}\| + \|U - \mathbb{1}\| \|\rho\| \\ &< \epsilon. \end{aligned}$$

- [1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).
- [2] A. Steane, *Rep. Prog. Phys.* **61**, 117 (1998).
- [3] E. Bernstein, C. H. Bennett, G. Brassard, and U. V. Vazirani, *SIAM J. Comput.* **26**, 1411 (1997).
- [4] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P. J. J. O'Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A. N. Cleland, and J. M. Martinis, *Nature (London)* **519**, 66 (2015).
- [5] C. Negrevergne, T. S. Mahesh, C. A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D. G. Cory, and R. Laflamme, *Phys. Rev. Lett.* **96**, 170501 (2006).
- [6] D. Lu, H. Li, D.-A. Trottier, J. Li, A. Brodutch, A. P. Krismanich, A. Ghavami, G. I. Dmitrienko, G. Long, J. Baugh, and R. Laflamme, *Phys. Rev. Lett.* **114**, 140505 (2015).
- [7] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, *Phys. Rev. Lett.* **106**, 130506 (2011).
- [8] J. Preskill, [arXiv:1203.5813](https://arxiv.org/abs/1203.5813).
- [9] D. Kenigsberg, T. Mor, and G. Ratsaby, *Quantum Inf. Comput.* **6**, 606 (2006).
- [10] V. Vedral, *Found. Phys.* **40**, 1141 (2010).
- [11] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor, *Theor. Comput. Sci.* **320**, 15 (2004).
- [12] A. Kay, *Phys. Rev. A* **92**, 062329 (2015).
- [13] S. Boixo, T. F. Ronnow, S. V. Isakov, Z. Wang, D. Wecker, D. A. Lidar, J. M. Martinis, and M. Troyer, *Nat. Phys.* **10**, 218 (2014).
- [14] S. Aaronson and A. Arkhipov, in *Proceedings of the STOC '11 Forty-Third Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2011), pp. 333–342.
- [15] D. Shepherd and M. J. Bremner, *Proc. R. Soc. A* **465**, 1413 (2008).
- [16] E. Knill and R. Laflamme, *Phys. Rev. Lett.* **81**, 5672 (1998).
- [17] A. Datta, S. T. Flammia, and C. M. Caves, *Phys. Rev. A* **72**, 042316 (2005).
- [18] P. W. Shor and S. P. Jordan, *Quantum Inf. Comput.* **8**, 681 (2008).
- [19] G. Passante, O. Moussa, C. A. Ryan, and R. Laflamme, *Phys. Rev. Lett.* **103**, 250501 (2009).
- [20] R. Jozsa and N. Linden, *Proc. R. Soc. London, Ser. A* **459**, 2011 (2003).
- [21] G. Vidal, *Phys. Rev. Lett.* **91**, 147902 (2003).
- [22] A. Datta and G. Vidal, *Phys. Rev. A* **75**, 042310 (2007).
- [23] A. Datta, A. Shaji, and C. Caves, *Phys. Rev. Lett.* **100**, 050502 (2008).
- [24] A. Datta, Ph.D. thesis, University of New Mexico, 2008.
- [25] A. Datta and A. Shaji, *Int. J. Quantum Inf.* **09**, 1787 (2011).
- [26] R. Laflamme, D. G. Cory, C. Negrevergne, and L. Viola, *Quantum Inf. Comput.* **2**, 166 (2002).
- [27] F. F. Fanchini, M. F. Cornelio, M. C. de Oliveira, and A. O. Caldeira, *Phys. Rev. A* **84**, 012313 (2011).
- [28] E. G. Rieffel and H. M. Wiseman, *Phys. Rev. A* **89**, 032323 (2014).
- [29] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, *Rev. Mod. Phys.* **84**, 1655 (2012).
- [30] G. Vidal and R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).
- [31] M. V. den Nest, *Phys. Rev. Lett.* **110**, 060504 (2013).
- [32] M. Boyer and T. Mor, in *Theory and Practice of Natural Computing: TPNC 2014* (Springer, Cham, 2014), pp. 107–118; M. Boyer, A. Brodutch, and T. Mor, *Soft Comput.* (2017), doi:[10.1007/s00500-017-2518-6](https://doi.org/10.1007/s00500-017-2518-6)
- [33] L. Gurvits and H. Barnum, *Phys. Rev. A* **66**, 062311 (2002).
- [34] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, *Phys. Rev. Lett.* **83**, 1054 (1999).
- [35] R. Hildebrand, *Phys. Rev. A* **76**, 052325 (2007).
- [36] H. Ollivier and W. H. Zurek, *Phys. Rev. Lett.* **88**, 017901 (2001).
- [37] M. Boyer, [arXiv:1608.08136](https://arxiv.org/abs/1608.08136).
- [38] A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti, and A. Acín, *Phys. Rev. A* **81**, 052318 (2010).
- [39] N. Johnston, *Phys. Rev. A* **88**, 062330 (2013).
- [40] S. Arunachalam, N. Johnston, and V. Russo, *Quantum Inf. Comput.* **15**, 0694 (2015).
- [41] M. Boyer, A. Brodutch, and T. Mor (unpublished).
- [42] B. Dakić, V. Vedral, and Č. Brukner, *Phys. Rev. Lett.* **105**, 190502 (2010).
- [43] B. Groisman, D. Kenigsberg, and T. Mor, [arXiv:quant-ph/0703103](https://arxiv.org/abs/quant-ph/0703103).