Contextuality supplies the ‘magic’ for quantum computation

Mark Howard1,2, Joel Wallman2, Victor Veitch2,3 & Joseph Emerson2

Quantum computers promise dramatic advantages over their classical counterparts, but the source of the power in quantum computing has remained elusive. Here we prove a remarkable equivalence between the onset of contextuality and the possibility of universal quantum computation via ‘magic state’ distillation, which is the leading model for experimentally realizing a fault-tolerant quantum computer. This is a conceptually satisfying link, because contextuality, which precludes a simple ‘hidden variable’ model of quantum mechanics, provides one of the fundamental characterizations of uniquely quantum phenomena. Furthermore, this connection suggests a unifying paradigm for the resources of quantum information: the non-locality of quantum theory is a particular kind of contextuality, and non-locality is already known to be a critical resource for achieving advantages with quantum communication. In addition to clarifying these fundamental issues, this work advances the resource framework for quantum computation, which has a number of practical applications, such as characterizing the efficiency and trade-offs between distinct theoretical and experimental schemes for achieving robust quantum computation, and putting bounds on the overhead cost for the classical simulation of quantum algorithms.

Quantum information provides unique new capabilities for computation such as Shor’s factoring algorithm1 and quantum simulation algorithms2. This naturally raises the fundamental question: what unique resources of the quantum world enable the advantages of quantum information? There have been many attempts to answer this question, with proposals including the hypothetical ‘quantum parallelism’3 some associate with quantum superposition, the necessity of large amounts of entanglement4, and much ado about quantum discord5. Unfortunately none of these proposals have proven satisfactory6–9, and, in particular, none have helped resolve outstanding challenges confronting the field. For example, on the theoretical side, the most general classes of problems for which quantum algorithms might offer an exponential speed-up over classical algorithms are poorly understood. On the experimental side, there remain significant challenges to the design of robust, large-scale quantum computers, and an important open problem is to determine the minimal physical requirements of a useful quantum computer10,11. A framework identifying relevant resources for quantum computation should help clarify these issues—for example, by identifying new simulation schemes for classes of quantum algorithms and by clarifying the trade-offs between the distinct physical requirements for achieving robust quantum computation. Here we establish that quantum contextuality, a generalization of non-locality identified12,13 almost 50 years ago, is a critical resource for quantum speed-up within the leading model for fault-tolerant quantum computation, known as magic state distillation (MSD)14–16. A framework identifying relevant resources for quantum computation should help clarify these issues—for example, by identifying new simulation schemes for classes of quantum algorithms and by clarifying the trade-offs between the distinct physical requirements for achieving robust quantum computation. Here we establish that quantum contextuality, a generalization of non-locality identified12,13 almost 50 years ago, is a critical resource for quantum speed-up within the leading model for fault-tolerant quantum computation, known as magic state distillation (MSD)14–16.

Contextuality was first recognized as an intrinsic feature of quantum theory via the Bell–Kochen–Specker ‘no-go’ theorem. This theorem implies the impossibility of explaining the statistical predictions of quantum theory in a natural way. In particular, the actual outcome observed under a quantum measurement cannot be understood as simply revealing a pre-existing value of some underlying ‘hidden variable’17. A key observation is that the non-locality of quantum theory is a special case of contextuality. Under the locality restrictions motivating quantum communication, non-locality is a quantifiable cost for classical simulation complexity18 and a fundamental resource for practical applications such as device-independent quantum key distribution19–21. Locality restrictions can make relevant measurement-based quantum computation13, for which non-locality quantifies the resources required to evaluate non-linear functions22,23. However, locality restrictions are not relevant in the standard quantum circuit model for quantum computation, and, in this context, a large amount of entanglement has been shown to be neither necessary nor sufficient for an exponential computational speed-up9.

Here we consider the framework of fault-tolerant stabilizer quantum computation24 which provides the most promising route to achieving robust universal quantum computation thanks to the discovery of high-threshold codes in two-dimensional geometries25–29. In this framework, only a subset of quantum operations—namely, stabilizer operations—can be achieved via a fault-tolerant encoding. These operations define a closed subtheory of quantum theory, the stabilizer subtheory, which is not universal and in fact admits an efficient classical simulation30. The stabilizer subtheory can be promoted to universal quantum computation through MSD31–33 which relies on a large number of ancillary resource states. Here we show that quantum contextuality plays a critical role in characterizing the suitability of quantum states for MSD. Our approach builds on recent work31,32 that has established a remarkable connection between contextuality and graph-theory. We use the framework of refs 31 and 32 to identify non-contextuality inequalities such that the onset of state-dependent contextuality, using stabilizer measurements, coincides exactly with the possibility of universal quantum computing via MSD. The scope of our results differs depending on whether we consider a model of computation using qubits (systems of even prime dimension) or qudits (systems of odd prime dimension). We note that some authors use the term qudit to describe a system with an arbitrary number of levels. Whereas in both cases we can prove that violating a non-contextuality inequality is necessary for quantum-computational speed-up via MSD, in the qudit case we are able to prove that a state violates a non-contextuality inequality if and only if it lies outside the known boundary for MSD.

1Department of Mathematical Physics, National University of Ireland, Maynooth, Ireland. 2Institute for Quantum Computing and Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada. 3Department of Statistics, University of Toronto, 100 St George Street, Toronto, Ontario M5S 3G3, Canada.
Graph–based contextuality

Interpreting measurements on a quantum state as merely revealing a pre-existing property of the system leads to disagreement with the predictions of quantum theory. In quantum mechanics, a projective measurement can be decomposed as a set of binary tests. Contradictions with models using pre-existing value assignments can arise when these tests appear in multiple measurement scenarios—that is, in multiple contexts. In other words, we cannot always assign a definite value to tests appearing in multiple contexts and consequently quantum mechanics cannot be described by a non-contextual hidden variable (NCHV) theory. The earliest demonstrations of quantum contextuality used sets of tests such that no NCHV model could reproduce the quantum predictions, regardless of what quantum state was actually measured. Recently, a more general framework has been derived in which a given set of tests can be considered to have non-contextual value assignments only if the measured state satisfies a non-contextuality inequality33. We briefly review this framework below.

Consider a set of $n$ binary tests, which can be represented in quantum mechanics by a set of $n$ rank-1 projectors $\{P_1, \ldots, P_n\}$. Two such tests are compatible, and so can be simultaneously performed on a quantum system, if and only if the projectors are orthogonal. We define the witness operator $\Sigma$ for a set of tests to be

$$\Sigma = \sum_{i=1}^{n} P_i$$

(1)

and the associated exclusivity graph $\Gamma$ to be a graph wherein each vertex corresponds to a projector and two vertices are adjacent (connected) if the corresponding projectors are compatible. Only one outcome can occur when a measurement of a set of orthogonal projectors is performed, so we require that a value of 1 will be assigned to at most one projector in each measurement. Since two vertices of $\Gamma$ are adjacent if and only if the corresponding projectors are compatible, the maximum value of $\Sigma$ in an NCHV model, $\langle \Sigma \rangle_{\text{NCHV}}$, is the independence number $\alpha(\Gamma)$, that is, the size of the largest set of vertices of $\Gamma$ such that no two elements of the set are adjacent.

The maximum quantum mechanical (QM) value of $\Sigma$ can be obtained by varying over projectors satisfying the appropriate compatibility relations and over quantum states. This quantity is bound above by the Lovasz number, $\vartheta$, of the exclusivity graph, that is,

$$\langle \Sigma \rangle_{\text{QM}} \leq \vartheta(\Gamma)$$

(2)

where $\vartheta$ can be calculated as the solution to a semidefinite program. Graphs for which $\vartheta(\Gamma) = \alpha(\Gamma)$ indicate that appropriately chosen projectors $\{P_i\}$ and states $\rho$ may reveal quantum contextuality by violating the non-contextuality inequality:

$$\text{Tr}(\Sigma \rho) \leq \vartheta(\Gamma)$$

(3)

For generalized probabilistic theories, an important class of ‘post-quantum’ theories, the maximum value of $\Sigma$ is given by the fractional packing number of the exclusivity graph $\lambda^*(\Gamma)$, that is:

$$\langle \Sigma \rangle_{\text{GPT}} = \lambda^*(\Gamma)$$

(4)

Note that if $\vartheta(\Gamma) < \langle \Sigma \rangle_{\text{QM}} = \vartheta(\Gamma)$, then the optimal choice of quantum state and projectors is maximally contextual, in that no greater violation of the non-contextuality inequality can be obtained in any generalized probabilistic theory.

The stabilizer formalism

Quantum information theory relies heavily on a family of finite groups usually called the (generalized) Pauli groups. The most promising and well understood quantum error correcting codes—stabilizer codes—are built using the elements of these groups, that is, Pauli operators. Qubits are the most commonly used building blocks for quantum computing, but a circuit using qudits has the same computational power. While qudits with larger dimensionality may pose new experimental challenges, these may be offset by a lower overhead for fault-tolerant computation16. In this section we outline the mathematical structure associated with the generalized Pauli group and the geometrical characterization of probabilistic mixtures of stabilizer states.

The stabilizer formalism for $p$-dimensional systems (where $p$ is a prime number) is defined using the generalized $X$ and $Z$ operators

$$X[j] = |j+1\rangle, \quad Z[j] = \omega^j |j\rangle$$

(5)

where $\omega = \exp\left(\frac{2\pi i}{p}\right)$. The set of Weyl–Heisenberg displacement operators is defined as

$$D_p = \{D_{xz} = \omega^{-1}x^z : x, z \in \mathbb{Z}_p^\times\}$$

(6)

where $2^{-1}$ is the multiplicative inverse of 2 in the finite field $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. For $p = 2$, one can replace $\omega^{-1}$ with $i$ in equation (6) to recover the familiar qubit Pauli operators. The Clifford group $C_{p,n}$ is defined to be the normalizer of the group $\langle D_p^\otimes n \rangle$ (that is, the group generated by the set of displacement operators), that is,

$$C_{p,n} = \{U \in \text{Aut}(d^n) : U \langle D_p^\otimes n \rangle U^\dagger = \langle D_p^\otimes n \rangle\}$$

(7)

and the set of stabilizer states is the image of the computational basis under the Clifford group $C_{p,n}$.

The stabilizer polytope is the convex hull of the set of stabilizer states. For a single system, the stabilizer polytope $\mathcal{P}$ is defined by the following set of simultaneous inequalities

$$\mathcal{P}_{\text{STAB}} = \left\{ \rho : \text{Tr}(\rho A^\otimes) \geq 0, \forall \mathbf{q} \in \mathbb{Z}_p^{n+1} \right\}$$

(8)

where $A^\otimes = -I_p + \sum_{j=1}^{p-1} P_j^\otimes$ and $P_j^\otimes$ is the projector onto the eigenspace of $q^j$ for the $j$th operator in the list $\{D_{xz}, D_{xz}, D_{xy}, D_{xy}, \ldots, D_{x}^{p-1}\}$ (the eigenbases of these operators form a complete set of mutually unbiased bases). In the preceding expression $I_p$ is the $p \times p$ identity matrix and $\mathbf{q}$ is a vector of length $p + 1$ with entries from $\{0, 1, \ldots, p-1\}$.

Magic state distillation

The stabilizer formalism of the previous section was developed in the search for quantum error-correcting codes, that is, codes allowing the robust, fault-tolerant storage and manipulation of quantum information stored across many subsystems15–24. Surface codes25–29, in particular, admit a comparatively high fault-tolerance threshold within an experimentally realistic planar physical layout. Codes such as these have a finite non-universal set of transversal (that is, manifestly fault-tolerant) operations that must be supplemented with an additional resource—a supply of so-called magic states—in order to attain universality. MSD refers to the subroutine, described below, wherein almost pure resource states are constructed using large numbers of impure resource states14–16.

An MSD protocol consists of the following steps: (1) prepare $n$ copies of a suitable (see below) input state, that is, $\rho^\otimes_m$; (2) perform a Clifford operation on $\rho^\otimes_m$; (3) perform a stabilizer measurement on all but the first $m$ registers, postselecting on a desired outcome. With appropriate choices of stabilizer operations, the resulting output state in the first $m$ registers, $\rho^\otimes_{\text{out}}$, is purified in the direction of a magic state $|\psi\rangle$, so that $\langle \psi| \rho^\otimes_{\text{out}} |\psi\rangle > \langle \psi| \rho^\otimes_{\text{in}} |\psi\rangle$. This process can be reiterated until $\rho^\otimes_{\text{out}}$ is sufficiently pure, at which point the resource $\rho^\otimes_{\text{out}}$ is used up to approximate a non-Clifford operation (via ‘state injection’) —for example, the π/8 gate or its qudit generalizations16,14. Supplementing stabilizer operations with the ability to perform such gates enables fault-tolerant and universal quantum computation.

For which states $\rho_m$ does there exist an MSD routine purifying $\rho^\otimes_{\text{out}}$ towards a non-stabilizer state? A large subset of quantum states have been ruled out by virtue of the fact that efficient classical simulation schemes are known for noiseless stabilizer circuits supplemented by access to an arbitrary number of states from the polytope $\rho^\otimes_m \in \mathcal{P}_{\text{Sim}}$ (refs 30, 35, 36). This polytope $\mathcal{P}_{\text{Sim}}$ of the known simulable states is described by13,37.
Figure 1 | A two-dimensional slice through qutrit state space. Three distinct regions in the space of 3 × 3 matrix operators: the region shaded in pale green describes quantum state space (valid density operators); region $P_{\text{SIM}}$, with hatched shading, corresponds to ancillas known to be efficiently simulable (and hence useless for quantum computation via MSD); and the dark red region $P_{\text{STAB}}$ describes mixtures of stabilizer states. The strict inclusion $P_{\text{STAB}} \subset P_{\text{SIM}}$ identifies a large class of bound magic states.35

We will prove that all states $\rho$ in the set $P_{\text{SIM}}$ are non-contextual with respect to stabilizer measurements. Our definition of stabilizer contextuality as a computational resource

Figure 2. The maximal violation of our non-contextuality inequality is achieved by the state $\rho_{\text{SIM}}$ as contextual, so that the conditions for contextuality and the possibility of quantum speed-up via MSD coincide exactly.

Proof. For $p = 2$, a software package41 can be used to obtain:

$\rho^{(2)} = \text{Clique cover number}$, which is the minimum number of cliques needed to cover every vertex of $\Gamma$. (A clique is a subset of a graph’s vertices wherein every pair of vertices is connected.) The clique cover number cannot be greater than the number of distinct bases in $|\Pi|^r$, which contains $p + 1$ separable bases and $p^2 - p$ entangled bases. Therefore $\delta(\Gamma) \leq \chi(\Gamma) \leq p^3 + 1$. Then, since there exist $p^n$ quantum

...
proving that any state includes the maximally mixed state) can violate a non-contextuality in-
states have been previously conjectured to be sufficient to promote quantum computation via MSD.
results establish that contextuality is a necessary resource for universal computation.

Significance and outlook
For qubits, the mere presence of contextuality cannot be sufficient to promote stabilizer circuits to universality since any state $\rho \notin P_{\text{SIM}}$ which includes the maximally mixed state) can violate a non-contextuality inequality constructed from stabilizer measurements. For example, converting the Peres–Mermin magic square to a 24-ray (projector) proof of contextuality and applying the formalism of refs 31 and 32 gives a non-contextuality inequality that is violated by all two-qubit states, including states of the form $\rho \otimes \sigma = I/4$.

The crucial difference between qubits and qudits is that state-independent contextuality (like that of the Peres–Mermin square) is never manifested within the qudit stabilizer formalism. Consequently, for qubits, any contextuality is necessarily state-dependent and our results show that this contextuality has an operational meaning as a necessary and possibly sufficient resource for the ‘magic’ that makes quantum computers work. In the case of qubits, it is a pressing open question whether a suitable operationally motivated refinement or quantification of contextual-ity can align more precisely with the potential to provide a quantum speed-up.

METHODS SUMMARY
Here we outline the argument that we use to prove that, for odd-prime $p$, the inde-
pendence number of $I^p$ is $p^3$. Recall that the independence number of a graph $I$ is the size of the largest independent set of $I$, where an independent set is a set of mutually non-commuting projectors in $[I]$. Because the elements of $[I]$ are all rank one, two elements are non-commuting if and only if they are non-orthogonal.

We prove $\alpha(I^p) = p^3$ by proving $\alpha(I^p) \geq p^3$ and $\alpha(I^p) < p^3 + 1$. This completes the proof since $\alpha(I^p)$ is an integer. In Theorem 2 we show that $\alpha(I^p) \geq p^3$ by showing that there exists a set of $p^3$ mutually non-orthogonal elements of $[I]$, for any $A \in P_{\text{SIM}}$ and $\rho \notin P_{\text{SIM}}$. In Lemmas 3–5 we parametrize the set of stabilizer projectors using the symplectic representation of the Clifford group in order to transform a condition of mutual non-orthogonality of projectors into a set of algebraic constraints on parameters. In Theorem 6 we then show that $\alpha(I^p) < p^3 + 1$ by showing that no subset of $p^3 + 1$ elements of $[I]$ can satisfy the constraints established in Lemmas 3–5, that is, there cannot exist a subset of $p^3 + 1$ mutually non-orthogonal elements of $[I]$.
29. Fowler, A. G., Mariantoni, M., Martinis, J. M. & Cleland, A. N. Surface codes: towards practical large-scale quantum computation. Phys. Rev. A 86, 032324 (2012).
30. Aaronson, S. & Gottesman, D. Improved simulation of stabilizer circuits. Phys. Rev. A 70, 052328 (2004).
31. Cabello, A., Severini, S. & Winter, A. (Non-)Contextuality of physical theories as an axiom. Preprint at http://arxiv.org/abs/1010.2163 (2010).
32. Cabello, A., Severini, S. & Winter, A. Graph-theoretic approach to quantum correlations. Phys. Rev. Lett. 112, 040401 (2014).
33. Cormick, C., Galvão, E. F., Gottesman, D., Pablo Paz, J. & Pittenger, A. O. Classicality in discrete Wigner functions. Phys. Rev. A 73, 012301 (2006).
34. Howard, M. & Vala, J. Qudit versions of the qubit \( \pi/8 \) gate. Phys. Rev. A 86, 022316 (2012).
35. Veitch, V., Ferrie, C., Gross, D. & Emerson, J. Negative quasi-probability as a resource for quantum computation. N. J. Phys. 14, 113011 (2012).
36. Mari, A. & Eisert, J. Positive Wigner functions render classical simulation of quantum computation efficient. Phys. Rev. Lett. 109, 230503 (2012).
37. van Dam, W. & Howard, M. Noise thresholds for higher-dimensional systems using the discrete Wigner function. Phys. Rev. A 83, 032310 (2011).
38. Appleby, D. M., Bengtsson, I. & Chaturvedi, S. Spectra of phase point operators in odd prime dimensions and the extended Clifford group. J. Math. Phys. 49, 012102 (2008).
39. Wallman, J. J. & Bartlett, S. D. Non-negative subtheories and quasiprobability representations of qudits. Phys. Rev. A 85, 062121 (2012).
40. Gross, D. Hudson’s theorem for finite-dimensional quantum systems. J. Math. Phys. 47, 122107 (2006).
41. Wootters, W. K. The discrete Wigner function. Ann. NY Acad. Sci. 480, 275–282 (1986).
42. Gibbons, K. S., Hoffman, M. J. & Wootters, W. K. Discrete phase space based on finite fields. Phys. Rev. A 70, 062101 (2004).
43. Östergård, P. R. J. A fast algorithm for the maximum clique problem. Discrete Appl. Math. 120, 197–207 (2002).
44. Veitch, V., Mousavian, S. A. H., Gottesman, D. & Emerson, J. The resource theory of stabilizer computation. N. J. Phys. 16, 013009 (2014).
45. Howard, M., Brennan, E. & Vala, J. Quantum contextuality with stabilizer states. Entropy 15, 2340–2362 (2013).
46. Peres, A. Two simple proofs of the Kochen-Specker theorem. J. Phys. A 24, L175–L178 (1991).
47. Spekkens, R. W. Contextuality for preparations, transformations, and unsharp measurements. Phys. Rev. A 71, 052108 (2005).
48. Acín, A., Fritz, T., Leverrier, A. & Szehr, O. A combinatorial approach to nonlocality and contextuality. Preprint at http://arxiv.org/abs/1212.4084 (2012).

Supplementary Information is available in the online version of the paper.

Acknowledgements M.H. was supported by the Irish Research Council (IRC) as part of the Empower Fellowship programme, and all authors acknowledge support from CIFAR and the Government of Canada through NSERC.

Author Contributions All authors made significant contributions to the results, interpretation and presentation of this Article.

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of the paper. Correspondence and requests for materials should be addressed to J.E. (jemerson@math.uwaterloo.ca)