Contextuality as a Resource for Models of Quantum Computation with Qubits

Juan Bermejo-Vega, Nicolas Delfosse, Dan E. Browne, Cihan Okay, and Robert Raussendorf
1Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
2Max-Planck Institut für Optik, Theory Division, 85748 Garching, Germany
3Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA
4Department of Physics and Astronomy, University of California, Riverside, California 92521, USA
5Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom
6Department of Mathematics, University of Western Ontario, London, Ontario N6A 5B7, Canada
7Department of Physics and Astronomy, University of British Columbia, Vancouver, British Columbia V6T 1Z1, Canada

(Received 16 November 2016; published 21 September 2017)

A central question in quantum computation is to identify the resources that are responsible for quantum speed-up. Quantum contextuality has been recently shown to be a resource for quantum computation with magic states for odd-prime dimensional qudits and two-dimensional systems with real wave functions. The phenomenon of state-independent contextuality poses a priori an obstruction to characterizing the case of regular qubits, the fundamental building block of quantum computation. Here, we establish contextuality of magic states as a necessary resource for a large class of quantum computation schemes on qubits. We illustrate our result with a concrete scheme related to measurement-based quantum computation.

DOI: 10.1103/PhysRevLett.119.120505

The model of quantum computation by state injection (QCSI) [1] is a leading paradigm of fault-tolerance quantum computation. Therein, quantum gates are restricted to belong to a small set of classically simulable gates, called Clifford gates [2], that admit simple fault-tolerant implementations [3]. Universal quantum computation is achieved via injection of magic states [1], which are the source of quantum computational power of the model.

A central question in QCSI is to characterize the physical properties that magic states need to exhibit in order to serve as universal resources. In this regard, quantum contextuality has recently been established as a necessary resource for QCSI. This was first achieved for quopit systems [4,5], where the local Hilbert space dimension is an odd prime power, and subsequently for local dimension two with the case of rebits [6]. In the latter, the density matrix is constrained to be real at all times.

In this Letter we ask “Can contextuality be established as a computational resource for QCSI on qubits?” This is not a straightforward extension of the quopit case because the multiqubit setting is complicated by the presence of state-independent contextuality among Pauli observables [7,8]. Consequently, every quantum state of \( n \geq 2 \) qubits is contextual with respect to Pauli measurements, including the completely mixed one [5]. It is thus clear that contextuality of magic states alone cannot be a computational resource for every QCSI scheme on qubits.

Yet, there exist qubit QCSI schemes for which contextuality of magic states is a resource, and we identify them in this Letter. Specifically, we consider qubit QCSI schemes \( \mathcal{M}_O \) that satisfy the following two constraints: (C1) Resource character. There exists a quantum state that does not exhibit contextuality with respect to measurements available in \( \mathcal{M}_O \). (C2) Tomographic completeness. For any state \( \rho \), the expectation value of any Pauli observable can be inferred via the allowed operations of the scheme.

The motivation for these constraints is the following. Condition (C1) constitutes a minimal principle that unifies, simplifies and extends the quopit [5] and rebit [6] settings. While seemingly a weak constraint, it excludes the possibility of Mermin-type state-independent contextuality [7,8] among the available measurements (see Lemma 1 below). A priori, the absence of state-independent contextuality comes at a price. Namely, for any QCSI scheme \( \mathcal{M}_O \) on \( n \geq 2 \) qubits, not all \( n \)-qubit Pauli observables can be measured. Thus, the question arises of whether this limits access to all \( n \) qubits for measurement. As we show in this Letter, this does not have to be the case.

Addressing this question, we impose tomographic completeness as our technical condition for a true \( n \)-qubit QCSI scheme, cf. (C2). It means that any quantum state can be fully measured given sufficiently many copies. The rebit scheme [6], for example, does not satisfy this.

One of our results is that for any number \( n \) of qubits there exists a QCSI scheme that satisfies both conditions (C1) and (C2). The reason why both conditions can simultaneously hold lies in a fundamental distinction between observables that can be measured directly in a given qubit QCSI scheme from those that can only be inferred by measurement of other observables. The resulting qubit QCSI schemes resemble their quopit counterparts [4,5] in the absence of state-independent contextuality, yet have full tomographic power for the multiqubit setting.

The main result of this Letter is Theorem 1. It says that if the initial (magic) states of a qubit QCSI scheme are describable by a noncontextual hidden variable model
(NCHVM) it becomes fundamentally impossible to implement a universal set of gates. We highlight that Theorem 1 applies generally to any scheme fulfilling the condition (C1), including that of Ref. [6].

The condition (C1) plays a pivotal role in our analysis. It is clear that contextuality of the magic states can be a resource only if condition (C1) holds. In this Letter we establish the converse, namely, that contextuality of the resource only if condition (C1) holds. Therefore, condition (C1) is the structural element that unifies the previously discussed quopit [5] and rebit [6] magic states is a resource for QCSI.

Setting.— An n-qubit Pauli observable $T_a$ is a Hermitian operator with $\pm 1$ eigenvalues of form

$$T_a := \xi(a) Z(a_2) X(a_1) := \xi(a) \otimes \bigotimes_{i=1}^{n} Z^{a_{2i}} \bigotimes_{j=1}^{n} X^{a_{2j}},$$

where $a := (a_2, a_1)$ is a 2n-bit string and $\xi(a)$ is a phase. Pauli observables define an operator basis that we call the injection (QCSI) consists of a resource $M$ of initial “magic” states and 3 kinds of allowed operations: (1) Measurement of any Pauli observable in a set $O$. (2) A group $G$ of “free” Clifford gates that preserve $O$ via conjugation up to a global phase. (3) Classical processing and feedforward. Adaptive circuits of operations 1–3 may be combined with classical postprocessing in order to simulate measurements of Pauli observables that are not in $O$ (cf. Fig. 1). We name the latter “inferable” and let $I$ be the superset of $O$ defined by them. Analogously, we let $J$ be the set of sets of compatible Pauli observables that can be inferred jointly, which define the “contexts” of our computational model. As shown in Fig. 1, not every set of compatible Pauli observables is necessarily in $J$.

FIG. 1. We consider an example scheme $\mathcal{M}_O$ on two qubits with $O = \{X_1, X_2, Z_1, Z_2\}$. Straight lines connect maximal sets of jointly inferable observables. Here, the correlator $X_1 X_2 (Z_1 Z_2)$ is not in $O$ but can be inferred by measuring $X_1, X_2 (Z_1, Z_2)$ and multiplying their outcomes. (This scheme is reminiscent of the syndrome measurement of subsystem codes [10].) Yet, $X_1 Z_1$ cannot be inferred jointly with $Z_1 Z_2$ because a forbidden measurement of $X_1, X_2, Z_1, Z_2$ would be required to reproduce all quantum correlations, but after measuring, e.g., $Z_1$ and $Z_2$ to infer $Z_1 Z_2$ the outcome statistics of $X_1 X_2$ become uniformly random. Similarly, $X_1 Z_1$ and $Z_1 X_2$ can be separately inferred but not jointly. Further, $YY$ cannot be inferred (observables in $O$ cannot distinguish its eigenstates).

Theorem: A qubit QCSI scheme $\mathcal{M}_O$ satisfying (C1) is universal for $n \geq 3$ qubits only if its magic states exhibit contextuality.

Theorem 1 applies even in the setting where the computation happens in an encoded subspace, reproducing the rebit results of Ref. [6]. We provide a general proof of this fact in a companion paper [9] and show it here in the encoding-free scenario under an additional assumption, denoted (●), that every qubit must be measurable in at least two complementary Pauli bases. This requirement enforces $\mathcal{M}_O$ to exhibit the phenomenon of quantum
complementarity and simplifies our main argument while preserving its core structure.

The proof of Theorem 1 relies on a characterization of noncontextual hidden variable models for qubit QCSIs. We make three key observations about such models.

First, by applying Def. 1.(i) to $M := \{A, B, AB, \alpha A\} \in \mathcal{J}$ as in Eq. (2), we derive two constraints

$$
\lambda_\nu(AB) = \lambda_\nu(A)\lambda_\nu(B), \quad \lambda_\nu(\alpha A) = \alpha \lambda_\nu(A),
$$

(5)

that any $\lambda_\nu \in \Lambda$ must fulfill for any pair $\{A, B\} \in \mathcal{J}$, $\alpha \in \mathbb{R}$.

Second, we prove the following lemma.

**Lemma 1:** For any QCSI scheme $\mathcal{M}_\nu$ fulfilling (C1) the phase $\xi(a)$ in Eq. (1) can be chosen w.l.o.g. so that $T_a T_b = T_{a+b}$ for any triple $\{T_a, T_b, T_{a+b}\} \in \mathcal{J}$. (6)

**Proof.—** Let $\xi$ be given and let $\lambda_\nu$ be a consistent value assignment for the scheme $\mathcal{M}_\nu$. W.l.o.g., we can redefine $T'_\nu := \{T'_\nu := \lambda_\nu(T_a) T_a, T_a \in T_\nu\}$ and $\mathcal{O}_\nu = \{T'_\nu, T_a \in \mathcal{O}\}$ introducing a classical relabeling of measurement outcomes, without changing any quantum feature of the scheme. Using $T_{a+b} = \pm T_a T_b$, we obtain

$$
T_{a+b} = \lambda_\nu(T_{a+b}) T_{a+b} = \lambda((\pm 1)T_a T_b)(\pm 1)T_a T_b
$$

$$
= (\pm 1)^2 \lambda(T_a T_b) T_a T_b = \lambda(T_a) \lambda(T_b) T_a T_b = T_a T_b.
$$

(5)

Last, we observe that for any $M \in \mathcal{J}$, $|\psi\rangle$ as in Eq. (3) and $T_b \in T_\nu$, the state $T_b |\psi\rangle$ is a joint eigenstate of $M$:

$$
\langle \gamma T_a T_b |\psi\rangle = (\lambda_\nu(\gamma T_a)(-1)^{[a,b]} |\psi\rangle, \quad \forall \gamma T_a \in M,
$$

(7)

where $[a, b] := a_1 b_2 + a_2 b_1$ mod 2; combined with Eq. (5), this induces a group action of $\mathbb{Z}_2^{2n}$ on value assignments

$$
\lambda_\nu^{\pi} \lambda_\nu^{u+a}(T_a) := \lambda_\nu(T_a)(-1)^{[u,a]}, \quad \forall u \in V.
$$

(8)

With these tools, we arrive at a powerful intermediate result, namely, a method to construct NCHVMs that can simulate qubit QCSIs on noncontextual inputs.

**Lemma 2:** For any qubit scheme $\mathcal{M}_\nu$ fulfilling (C1) and any quantum circuit $\mathcal{C}$ of $\mathcal{O}_\nu$ operations, if there exists a NCHVM $(\mathcal{S}, q_{\rho_{in}}, \Lambda)$ for some given input state $\rho_{in}$, then there exists a NCHVM $(\mathcal{S}, q_{\rho_{out}}, \Lambda)$ for the output $\rho_{out} := C(\rho_{in})$.

Lemma 2 establishes that contextuality cannot be freely generated in qubit QCSI. A surprising aspect of this fact is that it holds for circuits that contain intermediate measurements. Intuitively, unitary gates in $\mathcal{G}$ must induce an action on the set of noncontextual states since they preserve the set $\mathcal{O}$. However, the evolution of noncontextual states under measurement is far from intuitive since the latter can often prepare states that are inaccessible to gates [11].

Lemma 2 leads to a simple classical random-walk algorithm for sampling from the output distribution of all measurements in $\mathcal{C}$, which is more efficient if oracles for sampling from $q_{\rho_{in}}$ and computing any $\lambda_\nu \in \Lambda$ are given. The random walk first samples a state $\nu_0 \in \mathcal{S}$ from $q_{\rho_{in}}$ and, upon measurement of $T_{a_i} \in \mathcal{O}$ at time $t$, outputs $\lambda_\nu(T_{a_i})$ given $\nu_t$ and updates $\nu_t \rightarrow \nu_t + \alpha$ with 1/2 probability. The correctness of this algorithm follows from Eq. (9) below and is analyzed in detail in Ref. [9].

**Proof.—** We fix a phase convention for $T_a$ so that Eq. (6) in Lemma 1 holds and introduce a simplified notation

$$
\lambda_\nu(a) := \lambda_\nu(T_a), \quad \text{where } T_a \in \mathcal{I}, \quad a \in \mathbb{Z}_2^{2n}.
$$

Because free unitaries preserve $\mathcal{O}$ they can be propagated out of $\mathcal{C}$ via conjugation. Hence, we can w.l.o.g. assume that $\mathcal{C}$ consists only of measurements. Our proof is by induction. At time $t = 1$, $\rho_1 = \rho_{in}$ has an NCHVM by assumption. At any other time $t + 1$, given an NCHVM $(\mathcal{S}, q_{\rho_{in}}, \Lambda)$ for the state $\rho_{in}$, we construct an NCHVM $(\mathcal{S}, q_{\rho_{out}}, \Lambda)$ for $\rho_{out}$. Specifically, let $T_{a_i} \in \mathcal{O}$ be the observable measured at time $t$ with corresponding outcome $s_t \in \{\pm 1\}$, $s_{-t} := (s_1, \ldots, s_t)$ be the string of prior measurement records, and $p(s_t | s_{-t})$ the conditional probability of measuring $s_t$; we will now show that $\rho_{out}$ admits the hidden-variable representation

$$
q_{\rho_{out}}(\nu) = \frac{\delta_{s_t, s_{-t}} q_{\rho_{in}}(\nu) + q_{\rho_{in}}(\nu + a_t)}{p(s_t | s_{-t})},
$$

(9)

where $p(s_t | s_{-t})$ can be predicted by the HVM, since $2p(s_t | s_{-t}) = \langle I + s_t T_{a_i} | \rho_i \rangle = \langle I | \rho_i + s_t(T_{a_i}) | \rho_i \rangle$—which are known by the induction promise. Our goal is to show that $(\mathcal{S}, q_{\rho_{out}}, \Lambda)$ predicts the expected value of any $T_a \in \mathcal{I}$ measured at time $t + 1$. For this, we derive a useful expression,
which we evaluate on two cases: (A) $T_{a_{i}}$, $T_{a_{i}}$ anticommute, hence, $[a_{i}, a_{j}] = 1$. We get $\langle T_{a_{i}} \rangle^{\text{HVM}} = 0$, in agreement with quantum mechanics. (B) $T_{a_{i}}$, $T_{a_{j}}$ commute. In this case $[a_{i}, a_{j}] = 0$. Using the identity $\delta_{\lambda, \lambda'} = (1 + s\lambda)/2, s, \lambda \in \{\pm 1\}$, we obtain

$$\langle T_{a_{i}} \rangle^{\text{HVM}} = \sum_{i \in S} s_{i} \alpha_{\lambda_{i}}(a_{i}) \frac{1}{p(s_i | s_{-i})} q_{\lambda_{i}}(\nu) \alpha_{\lambda_{i}}(a)$$

$$\leq \sum_{i \in S} s_{i} e^{\lambda_{i}}(a_{i}) + s_{i} \sum_{i \in S} q_{\lambda_{i}}(\nu) \lambda_{i}(a + a_{i}) \frac{1}{2p(s_i | s_{-i})}.$$

Finally, by induction hypothesis, we arrive at

$$\langle T_{a_{i}} \rangle^{\text{HVM}} = \langle T_{a_{i}} \rangle_{\rho} + \frac{s_{i} \langle T_{a_{i}+a_{i}} \rangle_{\rho}}{p(s_i | s_{-i})} = \text{tr} \left( \frac{I + s_{i} T_{a_{i}+a_{i}}}{2} \rho \right) = \text{tr} \left( \frac{I_{+} + s_{i} T_{a_{i}}}{2} \rho \right) = \langle T_{a_{i}} \rangle_{\rho} + \frac{s_{i} \langle T_{a_{i}+a_{i}} \rangle_{\rho}}{p(s_i | s_{-i})}.$$
measurements are available by assumption. Now, an on-site measurement of $X$ or $Y$ on one of the red qubits of $|\Psi\rangle$ has the same effect as measuring $(X \pm Y)/\sqrt{2}$ on a cluster state. To complete the simulation, it is enough to reroute the measurement-based computation through a red site (this can be done with the available $X$ measurements [13]) whenever a measurement of $(X \pm Y)/\sqrt{2}$ is needed. (See Fig. 2 for illustration.) Note that an alternative resource state for one-qubit Pauli measurements is the so-called “union-jack” hypergraph state of Ref. [14].

Conclusion.—In this Letter we investigated the role of contextuality in qubit QCSI and proved that it is a necessary resource for all such schemes that meet a simple minimal condition: namely, that the allowed measurements do not exhibit state-independent contextuality. Our result applies if and only if contextuality emerges as a physical property possessed by quantum states (with respect to the measurements available in the computational model). We extended earlier results on odd-prime dimensional qudits [4,5] and rebits [6], and thereby completed establishing contextuality as a resource in QCSI in arbitrary prime dimensions. We conjecture that this result generalizes to all composite dimensions [15] (the composite odd case was recently covered after completion of this work [16]) and to algebraic extensions of QCSI models based on normalizer gates [11,17–20]. Further, we demonstrated the applicability of our result to a concrete qubit QCSI scheme that does not exhibit state independent contextuality while retaining tomographic completeness.

Finally, we refer to a companion paper [9] where we investigate the role of Wigner functions in qubit QCSI. There, we use Wigner functions to motivate the near-classical sector of the free operations in qubit QCSI, and relate their Wigner-function negativity to contextuality and hardness of classical simulation. In comparison, in this Letter, constraint (C1) completely removes the need to introduce Wigner functions, and leads us to the simplest and most general proof that contextuality can be a resource in qubit QCSI that we are aware of. For this reason, we regard the establishing of condition (C1) as a fundamental structural insight of our Letter.

We thank David T. Stephen and the anonymous reviewers for comments on the manuscript. J. B. V. acknowledges financial support by Horizon 2020 (640800–AQuS–H2020-FETPROACT–2014) and SIQS. N. D. is funded by Institute for Quantum Information and Matter (IQIM), the National Science Foundation Physics Frontiers Center (PHY-1125565) and the Gordon and Betty Moore Foundation (GBMF-2644). C. O. is supported by Natural Sciences and Engineering Research Council of Canada (NSERC). R. R. is funded by NSERC, Cifar. R. R. is scholar of the Cifar Quantum Information Science program.