Contextuality as a Resource for Models of Quantum Computation with Qubits

Juan Bermejo-Vega,[1,2] Nicolas Delfosse,[3,4] Dan E. Browne,[5] Cihan Okay,[6] and Robert Raussendorf[7]
[1]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany
[2]Max-Planck Institut für Quantum Optics, Theory Division, 85748 Garching, Germany
[3]Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA
[4]Department of Physics and Astronomy, University of California, Riverside, California 92521, USA
[5]Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom
[6]Department of Mathematics, University of Western Ontario, London, Ontario N6A 5B7, Canada
[7]Department 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 $\mathcal{M}_\mathcal{O}$ 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 $\mathcal{M}_\mathcal{O}$. (C2) Tomographic completeness. For any state ρ, 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 $\mathcal{M}_\mathcal{O}$ 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 magic states is a resource for QCSI *if* condition (C1) holds. Therefore, condition (C1) is the structural element that unifies the previously discussed quopit [5] and rebit [6] case, and the qubit scenarios discussed here. Together, condition (C1) and Theorem 1 characterize the contextuality types that are needed in quantum computation via state injection, showing that state-dependent contextuality with respect to Pauli observables is a universality resource.

As a final remark, we note that the measurements available in QCSI schemes satisfying (C1) preserve positivity of suitable Wigner functions [9].

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

$$T_a := \xi(a) Z(a_Z) X(a_X) := \xi(a) \bigotimes_{i=1}^{n} Z_i^{a_{Z_i}} \bigotimes_{j=1}^{n} X_j^{a_{X_j}}, \quad (1)$$

where $a := (a_Z, a_X)$ is a $2n$-bit string and $\xi(a)$ is a phase. Pauli observables define an operator basis that we call $\mathcal{T}_n$.

A qubit scheme $\mathcal{M}_\mathcal{O}$ of quantum computation via state injection (QCSI) consists of a resource $\mathcal{M}$ of initial "magic" states and 3 kinds of allowed operations: (1) Measurement of any Pauli observable in a set $\mathcal{O}$. (2) A group G of "free" Clifford gates that preserve $\mathcal{O}$ 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 $\mathcal{O}$ (cf. Fig. 1). We name the latter

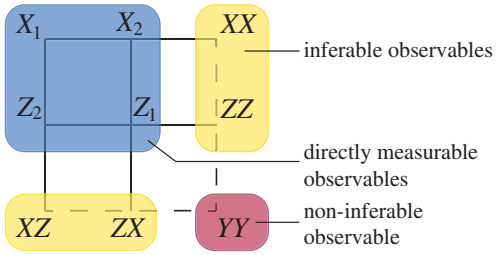

FIG. 1. We consider an example scheme $\mathcal{M}_\mathcal{O}$ on two qubits with $\mathcal{O} = \{X_1, X_2, Z_1, Z_2\}$. Straight lines connect maximal sets of jointly inferable observables. Here, the correlator X_1X_2 (Z_1Z_2) is not in $\mathcal{O}$ but can be inferred by measuring X_1, X_2 (Z_1, Z_2) and multiplying their outcomes. (This scheme is reminiscent of the syndrome measurement of subsystem codes [10].) Yet, X_1X_2 cannot be inferred jointly with Z_1Z_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_1Z_2 the outcome statistics of X_1X_2 become uniformly random. Similarly, X_1Z_2 and Z_1X_2 can be separately inferred but not jointly. Further, YY *cannot* be inferred (observables in $\mathcal{O}$ cannot distinguish its eigenstates).

"*inferable*" and let $\mathcal{I}$ be the superset of $\mathcal{O}$ defined by them. Analogously, we let $\mathcal{J}$ 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 $\mathcal{J}$. Yet, $A \in \mathcal{I}$ implies that $\{A\} \in \mathcal{J}$. Furthermore, for any pair of observables $\{A, B\} \in \mathcal{J}$ and $\alpha \in \mathbb{R}$, the observables $AB, \alpha A$ can be inferred jointly by measuring A, B, since the eigenvalues of the latter determine those of the former. Hence,

$$\{A, B\} \in \mathcal{J} \Rightarrow \{A, B, AB, \alpha A\} \in \mathcal{J}, \quad \forall\ \alpha \in \mathbb{R}. \quad (2)$$

Constraint (C2) holds if and only if $\mathcal{T}_n \subset \mathcal{I}$, i.e., if and only if the outcome distribution of any Pauli observable can be sampled via measurements in $\mathcal{O}$ and classical postprocessing.

Contextuality.—Above, imposing (C1) means that there exists a quantum state ρ whose measurement statistics can be reproduced by a noncontextual hidden variable model (NCHVM), which we introduce next.

Definition 1.—A NCHVM $(\mathcal{S}, q_\rho, \Lambda)$ for the state ρ with respect to a scheme $\mathcal{M}_\mathcal{O}$ consists of a probability distribution q_ρ over a set $\mathcal{S}$ of internal states and a set $\Lambda = \{\lambda_\nu\}_{\nu \in \mathcal{S}}$ of value assignment functions $\lambda_\nu : \mathcal{I} \to \{\pm 1\}$ that fulfill (i) For any $\lambda_\nu \in \Lambda$ and $M \in \mathcal{J}$ the real numbers $\{\lambda_\nu(A)\}_{A \in M}$ are compatible eigenvalues: i.e., there exists a quantum state $|\psi\rangle$ such that

$$A|\psi\rangle = \lambda_\nu(A)|\psi\rangle, \quad \forall\ A \in M. \quad (3)$$

(ii) The distribution q_ρ satisfies

$$\langle A \rangle_\rho = \mathrm{tr}(A\rho) = \sum_{\nu \in \mathcal{S}} \lambda_\nu(A) q_\rho(\nu), \quad \forall\ A \in \mathcal{I}. \quad (4)$$

The state ρ is said to be "contextual" or to "exhibit contextuality" if no NCHVM with respect to $\mathcal{M}_\mathcal{O}$ exists.

Qubit QCSI for which *all* possible inputs exhibit contextuality are forbidden by (C1). Specifically, in this Letter, $\mathcal{O}$ must be a strict subset of $\mathcal{T}_n$.

Main result.—We now establish contextuality as a resource for quantum computational universality for all qubit QCSI schemes that fulfill (C1). Below, we call a scheme $\mathcal{M}_\mathcal{O}$ *universal* if for any integer $n \geq 1$ and $V \in U(2^n)$ there exists a finite-size circuit of $\mathcal{M}_\mathcal{O}$ operations that prepares the n-qubit state $V|0\rangle$ up to any positive trace-norm error.

Theorem: A qubit QCSI scheme $\mathcal{M}_\mathcal{O}$ 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 ($\star$), that every qubit must be measurable in at least two complementary Pauli bases. This requirement enforces $\mathcal{M}_\mathcal{O}$ 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 $M \coloneqq \{A, B, AB, \alpha A\} \in \mathcal{J}$ as in Eq. (2), we derive two constraints

$$\lambda_\nu(AB) = \lambda_\nu(A)\lambda_\nu(B), \qquad \lambda_\nu(\alpha A) = \alpha\lambda_\nu(A), \quad (5)$$

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 $\mathcal{M}_\mathcal{O}$ fulfilling (C1) the phase $\xi(a)$ in Eq. (1) can be chosen w.l.o.g. so that

$$T_a T_b = T_{a+b} \quad \text{for any triple } \{T_a, T_b, T_a T_b\} \in \mathcal{J}. \quad (6)$$

Proof.—Let ξ be given and let λ_ν be a consistent value assignment for the scheme $\mathcal{M}_\mathcal{O}$. W.l.o.g., we can redefine $\mathcal{T}'_n \coloneqq \{T'_a \coloneqq \lambda_\nu(T_a)T_a, T_a \in \mathcal{T}_n\}$ and $\mathcal{O}' = \{T'_a, T_a \in \mathcal{O}\}$ 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

$$\begin{aligned} T'_{a+b} &= \lambda_\nu(T_{a+b})T_{a+b} = \lambda((\pm 1)T_a T_b)(\pm 1)T_a T_b \\ &\overset{(5)}{=} (\pm 1)^2 \lambda(T_a T_b)T_a T_b \overset{(5)}{=} \lambda(T_a)T_a\lambda(T_b)T_b = T'_a T'_b. \end{aligned}$$

□

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

$$(\gamma T_a)T_b|\psi\rangle = (\lambda_\nu(\gamma T_a)(-1)^{[a,b]})T_b|\psi\rangle, \quad \forall\, \gamma T_a \in M, \quad (7)$$

where $[a, b] \coloneqq a_X b_Z + a_Z b_X \bmod 2$; combined with Eq. (5), this induces a group action of $\mathbb{Z}_2^{2n}$ on value assignments

$$\lambda_\nu^{\pi}\lambda_{\nu+u}(T_a) \coloneqq \lambda_\nu(T_a)(-1)^{[u,a]}, \quad \forall\ u \in V. \quad (8)$$

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 $\mathcal{M}_\mathcal{O}$ fulfilling (C1) and any quantum circuit $\mathcal{C}$ of $\mathcal{M}_\mathcal{O}$ operations, if there exists a NCHVM $(\mathcal{S}, q_{\rho_{\text{in}}}, \Lambda)$ for some given input state ρ_{in}, there then exists a NCHVM $(\mathcal{S}, q_{\rho_{\text{out}}}, \Lambda)$ for the output $\rho_{\text{out}} \coloneqq \mathcal{C}(\rho_{\text{in}})$.

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 further efficient if oracles for sampling from $q_{\rho_{\text{in}}}$ and computing any $\lambda_\nu \in \Lambda$ are given. The random walk first samples a state $\nu_0 \in \mathcal{S}$ from $q_{\rho_{\text{in}}}$ and, upon measurement of $T_{a_t} \in \mathcal{O}$ at time t, outputs $\lambda_{\nu_t}(T_{a_t})$ given ν_t and updates $\nu_t \to \nu_t + a$ with $1/2$ probability. The correctness of this algorithm follows from Eq. (9) below and is analyzed in detailed 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

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

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 $t = 1$, $\rho_1 = \rho_{\text{in}}$ has an NCHVM by assumption. At any other time $t + 1$, given an NCHVM $(\mathcal{S}, q_{\rho_t}, \Lambda)$ for the state ρ_t, we construct an NCHVM $(\mathcal{S}, q_{\rho_{t+1}}, \Lambda)$ for ρ_{t+1}. Specifically, let $T_{a_t} \in \mathcal{O}$ be the observable measured at time t with corresponding outcome $s_t \in \{\pm 1\}$, $s_{\prec t} \coloneqq (s_1, \ldots, s_t)$ be the string of prior measurement records, and $p(s_t|s_{\prec t})$ the conditional probability of measuring s_t; we will now show that ρ_{t+1} admits the hidden-variable representation

$$q_{\rho_{t+1}}(\nu) \coloneqq \frac{\delta_{s_t,\lambda_\nu(a_t)}}{p(s_t|s_{\prec t})}\frac{q_{\rho_t}(\nu) + q_{\rho_t}(\nu + a_t)}{2}, \quad (9)$$

where $p(s_t|s_{\prec t})$ can be predicted by the HVM, since $2p(s_t|s_{\prec t}) = \langle I + s_t T_{a_t}\rangle_{\rho_t} = \langle I\rangle_{\rho_t} + s_t\langle T_{a_t}\rangle_{\rho_t}$—which are known by the induction promise. Our goal is to show that $(\mathcal{S}, q_{\rho_{t+1}}, \Lambda)$ predicts the expected value of any $T_a \in \mathcal{I}$ measured at time $t + 1$. For this, we derive a useful expression,

$$\begin{aligned} \langle T_a\rangle^{\text{HVM}}_{\rho_{t+1}} &= \sum_{\nu\in\mathcal{S}} q_{\rho_{t+1}}(\nu)\lambda_\nu(a) \\ &\overset{(9)}{=} \sum_{\nu\in\mathcal{S}} \frac{\delta_{s_t,\lambda_\nu(a_t)}q_{\rho_t}(\nu)}{2p(s_t|s_{\prec t})}\lambda_\nu(a) + \sum_{\nu\in\mathcal{S}} \frac{\delta_{s_t,\lambda_\nu(a_t)}q_{\rho_t}(\nu + a_t)}{2p(s_t|s_{\prec t})}\lambda_\nu(a). \\ &\overset{(8)}{=} \sum_{\nu\in\mathcal{S}} \frac{\delta_{s_t,\lambda_\nu(a_t)}q_{\rho_t}(\nu)}{2p(s_t|s_{\prec t})}\lambda_\nu(a) + \frac{\delta_{s_t,\lambda_\nu(a_t)}q_{\rho_t}(\nu)}{2p(s_t|s_{\prec t})}\lambda_\nu(a)(-1)^{[a,a_t]}, \end{aligned} \quad (10)$$

which we evaluate on two cases: *(A)* T_a, T_{a_t} anticommute, hence, $[a, a_t] = 1$. We get $\langle T_a \rangle^{\mathrm{HVM}}_{\rho_{t+1}} = 0$, in agreement with quantum mechanics. *(B)* T_a, T_{a_t} commute. In this case $[a, a_t] = 0$. Using the identity $\delta_{s,\lambda} = (1 + s\lambda)/2, s, \lambda \in \{\pm 1\}$, we obtain

$$\langle T_a \rangle^{\mathrm{HVM}}_{\rho_{t+1}} = \sum_{\nu \in \mathcal{S}} \frac{1 + s_t \lambda_\nu(a_t)}{2p(s_t|s_{\prec t})} q_{\rho_t}(\nu)\lambda_\nu(a) \overset{(5)}{=} \frac{\sum_{\nu \in \mathcal{S}} q_{\rho_t}(\nu)\lambda_\nu(a) + s_t \sum_{\nu \in \mathcal{S}} q_{\rho_t}(\nu)\lambda_\nu(a + a_t)}{2p(s_t|s_{\prec t})}.$$

Finally, by induction hypothesis, we arrive at

$$\langle T_a \rangle^{\mathrm{HVM}}_{\rho_{t+1}} = \frac{\langle T_a \rangle_{\rho_t} + s_t \langle T_{a+a_t} \rangle_{\rho_t}}{2p(s_t|s_{\prec t})} \overset{(6)}{=} \frac{\mathrm{tr}(\rho_t \frac{I + s_t T_{a_t}}{2} T_a)}{p(s_t|s_{\prec t})} = \mathrm{tr}\left(\frac{\left[\frac{I + s_t T_{a_t}}{2}\right] \rho_t \frac{I + s_t T_{a_t}}{2}}{p(s_t|s_{\prec t})} T_a \right) = \mathrm{tr}(\rho_{t+1} T_a),$$

which is again the quantum mechanical prediction. □

Finally, we prove our main result.

Proof of theorem 1.—We derive a contradiction by assuming (A1) that $\mathcal{M}_\mathcal{O}$ is universal and (A2) that all magic states in $\mathcal{M}$ are noncontextual. We first consider the computation to be error-free and drop this assumption at the end.

Recall that, by assumption ($\star$), two complementary Pauli observables, denoted Z_i, $X_i \in \mathcal{O}$ w.l.o.g., can be measured on any qubit. By (A1), the scheme $\mathcal{M}_\mathcal{O}$ can prepare the encoded GHZ state $|\psi\rangle$ that is uniquely stabilized by $X_1X_2X_3$, $-X_1Z_2Z_3$, $-Z_1X_2Z_3$, $-Z_1Z_2X_3$. Furthermore, $\mathcal{M}_\mathcal{O}$ can also infer the value of any correlator of form $A_1A_2A_3$ with $A_i \in \{X_i, Z_i\}$ (in particular, $|\psi\rangle$'s stabilizers) by measuring A_1, A_2, A_3 individually. Quantum mechanics predicts

$$\langle X_1X_2X_3 - X_1Z_2Z_3 - Z_1X_2Z_3 - Z_1Z_2X_3 \rangle^{\mathrm{QM}}_{\psi} = 4.$$

On the other hand, by (A2) and Lemma 2, there exists an NCHVM for $|\psi\rangle$ with respect to all quadruples of form $\{A_1, A_2, A_3, A_1A_2A_3, A_i \in X_i, Z_i\}$. Using constraint (5) for noncontextual value assignments, we derive an inequality for the NCHVM's prediction

$$\langle X_1X_2X_3 - X_1Z_2Z_3 - Z_1X_2Z_3 - Z_1Z_2X_3 \rangle^{\mathrm{HVM}}_{\psi} \leq 2,$$

originally due to Mermin [12], which contradicts quantum mechanics. Hence, either (A1) or (A2) must be false.

Last, our argument holds if arbitrarily small errors are present because the HVM's prediction deviates from the quantum mechanical one by a finite amount (larger than 2). □

A qubit QCSI scheme powered by contextuality.— Here we prove that for any number n of qubits there exists a universal qubit QCSI scheme $\mathcal{M}_\mathcal{O}$ that fulfills the conditions (C1) and (C2). The $\mathcal{O}$ measurements available in this scheme are all single-qubit Pauli measurements, the group $\mathcal{G}$ contains all single-qubit Clifford gates, and the magic state is locally unitarily equivalent to a 2D cluster state. This family of examples demonstrates that the classification provided by our main result (Theorem 1) is not empty.

We now show that single-qubit Pauli measurents satisfy (C1) and (C2). First, note that the value of any Pauli observable can be inferred by measuring its single-qubit tensor components; hence, local QCSI fulfills (C2). Second, we show (C1) is also met by giving a NCHVM for the mixed state $\rho = I/2^n$ with respect to single-qubit operations. The most general joint measurement in $\mathcal{J}$ that we can implement with the latter is to measure n single-qubit Paulis $\sigma_1, \ldots, \sigma_n$ on distinct qubits, which lets us infer the value of any observable $\gamma \bigotimes_{i=1}^n \sigma_i^{\alpha_i}$ with $\alpha \in \mathbb{Z}_2^n, \gamma \in \mathbb{R}$. Hence, the function $\lambda_0(\bigotimes_{i=1}^n \sigma_i^{\alpha_i}) \coloneqq 1$, which is a joint eigenvalue of $\{\bigotimes_{i=1}^n \sigma_i^{\alpha_i} : \alpha \in \mathbb{Z}_2^n\}$, extends linearly to a value assignment fulfilling Def. 1(i). Picking $\mathcal{T}_n = \{I, X, Y, Z\}^{\otimes n}$, we obtain an NCHVM via (8) with value assignments $\lambda_b(T_a) \coloneqq (-1)^{[a,b]}, b \in \mathbb{Z}_2^{2n}$ wherein ρ corresponds to a probability distribution $q_\rho(b) \coloneqq 1/2^{2n}$: indeed, our HVM predicts $\langle \gamma T_a \rangle_\rho = \gamma$ for $T_a = T_0 = I$ and 0 otherwise, matching the quantum mechanical prediction —this can be checked by computing the average of $\lambda_b(T_a)$ over b in each case.

Last, we present a family of magic states that promote our local QCSI scheme to universality. Unlike in standard magic state distillation [1], which relies on product magic states, our scheme has no entangling operations and requires entanglement to be present in the input to be universal. We show that a possibility is to use a modified cluster state $|\Psi\rangle$ that contains cells as in Fig. 2 with "red-site" qubits that are locally rotated by a T gate $e^{-i\pi/8Z}$. Our approach is to use such state to simulate a universal scheme of measurement based quantum computation based on adaptive local measurements $\{Z, X, Y, X \pm Y/\sqrt{2}\}$ on a regular 2D cluster state [13]. Local Pauli

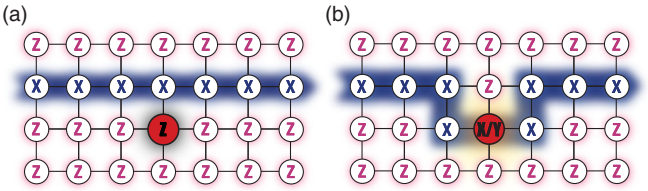

FIG. 2. QCSI with modified cluster state $|\Psi\rangle$ and single-qubit X_i, Y_j, Z_k Pauli measurements: the Z measurements are used to cut out of the plane a web corresponding to some layout of a quantum circuit, while the X measurements drive the MBQC simulation of this circuit [13]. By "rerouting" a wire piece, one may choose between implementing and not implementing a non-Clifford gate. (a) Identity operation on the logical state space. (b) X or Y is measured adaptively to implement a logical $e^{-i\pi/8Z}$ gate in MBQC [13].

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.

[1] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).
[2] D. Gottesman, Ph. D. thesis, California Institute of Technology, 1997, arXiv:quant-ph/9705052v1.
[3] D. Gottesman, Theory of fault-tolerant quantum computation, Phys. Rev. A **57**, 127 (1998).
[4] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, New J. Phys. **14**, 113011 (2012).
[5] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Contextuality supplies the 'magic' for quantum computation, Nature **510**, 351 (2014).
[6] N. Delfosse, P. Allard Guerin, J. Bian, and R. Raussendorf, Wigner Function Negativity and Contextuality in Quantum Computation on Rebits, Phys. Rev. X **5**, 021003 (2015).
[7] N. D. Mermin, Simple Unified Form for the Major No-Hidden-Variables Theorems, Phys. Rev. Lett. **65**, 3373 (1990).
[8] A. Peres, Incompatible results of quantum measurements, Phys. Lett. A **151**, 107 (1990).
[9] R. Raussendorf, N. Delfosse, D. E. Browne, C. Okay, and J. Bermejo-Vega, Contextuality and Wigner-function negativity in qubit quantum computation, Phys. Rev. A **95**, 052334 (2017).
[10] D. Poulin, Stabilizer Formalism for Operator Quantum Error Correction, Phys. Rev. Lett. **95**, 230504 (2005).
[11] J. Bermejo-Vega and M. Van Den Nest, Classical simulations of Abelian-group normalizer circuits with intermediate measurements, Quantum Inf. Comput. **14**, 181 (2014).
[12] N. D. Mermin, Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States, Phys. Rev. Lett. **65**, 1838 (1990).
[13] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).
[14] J. Miller and A. Miyake, Hierarchy of universal entanglement in 2D measurement-based quantum computation, npj Quantum Information **2**, 16036 (2016).
[15] D. Gottesman, Fault-tolerant quantum computation with higher-dimensional systems, in *Selected papers from the First NASA International Conference on Quantum Computing and Quantum Communications* (Springer, New York, 1998).
[16] N. Delfosse, C. Okay, J. Bermejo-Vega, D. E. Browne, and R. Raussendorf, Equivalence between contextuality and negativity of the Wigner function for qudits, arXiv: 1610.07093.
[17] M. Van den Nest, Efficient classical simulations of quantum Fourier transforms and normalizer circuits over Abelian groups, Quantum Inf. Comput. **13** (2013).
[18] J. Bermejo-Vega, C. Y.-Y. Lin, and M. Van den Nest, Normalizer circuits and a Gottesman-Knill theorem for infinite-dimensional systems, Quantum Inf. Comput. **16** (2016).
[19] J. Bermejo-Vega, C. Yen-Yu Lin, and M. Van den Nest, The computational power of normalizer circuits over black-box groups, arXiv:1409.4800.
[20] J. Bermejo-Vega and K. C. Zatloukal, Abelian hypergroups and quantum computation, arXiv:1509.05806.