Contextuality as a resource for qubit quantum computation

Juan Bermejo-Vega[1,2], Nicolas Delfosse[3,4], Dan E. Browne[5], Cihan Okay[6], Robert Raussendorf[7]

1: Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Berlin, Germany,

2: Max-Planck Institut für Quantum Optics, Theory Division, Garching, Germany,

3: Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, 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, UK,

6: Department of Mathematics, University of Western Ontario, London, Ontario, Canada,

7: Department of Physics and Astronomy, University of British Columbia, Vancouver, BC, Canada

(Dated: November 18, 2016)

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 wavefunctions.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.

PACS numbers: 03.67.Mn, 03.65.Ud, 03.67.Ac

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 direction, quantum contextuality has recently been established as a necessary resource for QCSI. This was first achieved for qudit 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],assuming that the density matrix is constrained to be real at all times.

In this Letter, we ask whether contextuality can be established as a computational resource for QCSI on *qubits*.

Result. The case of qubits 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 wrt. Pauli measurements, including the completely mixed one [5]. It is thus clear that contextuality of magic states cannot be a computational resource for every QCSI scheme on qubits.

In this Letter, we identify the qubit QCSI schemes for which contextuality of magic states *is* a resource. Specifically, if we (i) restrict the available measurements to exclude state-independent contextuality, but we (ii) retain a set broad enough to still allow for full state tomography, we show that contextuality of magic states is a necessary resource for computational universality. Tomographic completeness is our technical notion for a "true" qubit QCSI scheme and means that any quantum state can be fully measured given sufficiently many copies. The rebit scheme [6], for example, does not satisfy this.

A question that arises at this point is whether conditions (i) and (ii) can be simultaneously satisfied. We demonstrate that this is indeed the case giving an example. 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. When both classes do not coincide, the difference makes it possible to find qubit QCSI schemes with full tomographic power that are free of state-independent contextuality.

The result of this Letter is Theorem 1. It says that if the initial (magic) states of a qubit QCSI scheme are describable by a non-contextual hidden variable model (NCHVM) it becomes fundamentally impossible to implement a universal set of gates. The proof relies on a construction (Lemma 2) of a hidden variable model to simulate such computations.

The role of postulate (ii) is to single out true n-qubit QCSI schemes, which were not previously investigated. We highlight, though, that Theorem 1 applies generally to *any* scheme fulfilling postulate (i) (e.g., that of [6]). This leads us to a final fundamental insight of this work: namely, that for arbitrary two-level quantum systems, if contextuality is a state-dependent feature, then it is a necessary resource for universality in QCSI [7, 8].

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 5 kinds of allowed operations and objects:

1. Measurement of any Pauli observable in a set $\mathcal{O}$.
2. A group $\mathcal{G}$ of "free" Clifford gates that preserve $\mathcal{O}$ via conjugation up to a global phase.
3. Classical processing and feedforward.
4. A set $\mathcal{I}$ of "inferable" Pauli observables, whose value can be inferred via operations 1-3 for any possible quantum state of the system.
5. A set $\mathcal{J}$ of sets of *compatible* Pauli observables whose values can be inferred jointly via 1-3.

Note that $\mathcal{O} \subset \mathcal{I}$ and that, if $A \in \mathcal{I}$, then $\{A\} \in \mathcal{J}$. Further, as illustrated in Fig. 1, not every tuple of commuting Paulis is necessarily in $\mathcal{J}$. In this Letter, we are most interested on those qubit QCSI schemes that fulfill two additional postulates:

(P1) There exists a quantum state that does not exhibit contextuality with respect to measurements in $\mathcal{J}$.

(P2) Tomographic completeness. For any state ρ, the expected value $\langle T_a \rangle_\rho$ of any Pauli observable can be inferred via the allowed operations of the scheme.

Postulate (P2) holds iff $\mathcal{T}_n \subset \mathcal{I}$, i.e., iff the outcome distribution of any Pauli observable can be sampled from via measurements in $\mathcal{O}$ and classical post-processing.

Contextuality. Above, imposing (P1) means that there exists a quantum state ρ whose measurement statistics can be reproduced by *non-contextual hidden variable models* (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 $\lambda_\nu : \mathcal{I} \to \{\pm 1\}$ with two properties:*

(i) For each $\lambda_\nu \in \Lambda$ and $M \in \mathcal{J}$ there exists a quantum state $|\psi\rangle$ such that

$$A|\psi\rangle = \lambda_\nu(A)|\psi\rangle, \quad \forall A \in M. \quad (2)$$

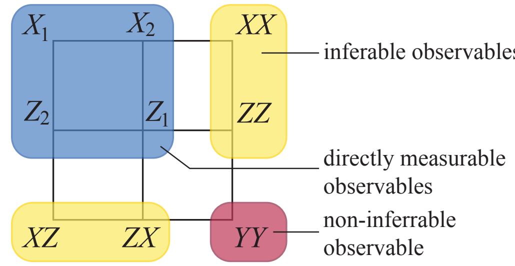

FIG. 1. We consider an example scheme $\mathcal{M}_\mathcal{O}$ on 2-qubits with $\mathcal{O} = \{X_1, X_2, Z_1, Z_2\}$. Here, the correlator X_1X_2 (resp. Z_1Z_2) is not in $\mathcal{O}$ but can be inferred by measuring X_1, X_2 (resp. Z_1, Z_2) and multiplying the outcomes. (This inference scheme is reminiscent of the syndrome measurement of subsystem codes [9].) Yet, X_1X_2 cannot be inferred jointly with Z_1Z_2 because X_1, X_2, Z_1, Z_2 are not all mutually compatible. Similarly, X_1Z_2, Z_1X_2 are not jointly inferable and, more strongly, YY *cannot* be inferred.

(ii) The distribution q_ρ satisfies

$$\langle A \rangle_\rho = \mathrm{tr}(A\rho) = \sum_{\nu \in \mathcal{S}} \lambda_\nu(A) q_\rho(\nu), \quad \forall A \in \mathcal{I} \quad (3)$$

The state ρ is said to be "non-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 (P1). Specifically, in this Letter, $\mathcal{O}$ must be a strict subset of $\mathcal{T}_n$ [7, 8]. *Note:* above, the states $|\psi\rangle$ in (2) are auxiliary. Their purpose is to ensure that value assignments λ_ν correspond to compatible eigenvalues as in quantum mechanics.

Main Result. We now establish contextuality as a resource for all qubit QCSI schemes that fulfill (P1).

Theorem 1. *A qubit QCSI scheme $\mathcal{M}_\mathcal{O}$ on $k \geq 3$ (possibly encoded) qubits satisfying (P1) is universal only if its magic states exhibit contextuality.*

To make this statement precise, we introduce a broad notion of computational universality that is suited to state-injection protocols and allows for encodings.

Definition 2. *A scheme $\mathcal{M}_\mathcal{O}$ is universal if for any $k \geq 1$ there exists an isometrical encoding map $\mathcal{E} : \mathbb{C}^{2^{\otimes k}} \to \mathbb{C}^{2^{\otimes n}}$ of k-logical into n-physical qubits, as well as finite-size circuits of $\mathcal{M}_\mathcal{O}$ operations for the following tasks:*

U1. Prepare any initial state $\mathcal{E}(|x\rangle)$ with $x \in \{0,1\}^k$.

U2. For any quantum gate $V \in SU(2^k)$ and given input state $\mathcal{E}(|\phi\rangle)$, prepare the output state $\mathcal{E}(V|\phi\rangle)$.

U3. Measure any logical qubit in two complementary bases: i.e., $\mathcal{O}$ contains at least two logical Pauli observables $\mathcal{E}(Z_i), \mathcal{E}(X_i)$ for any $i = 1, \ldots, k$.

Above, for any observable A, we define $\mathcal{E}(A)$ so that $\mathcal{E}(A)\mathcal{E}(|\psi\rangle) = \mathcal{E}(A|\psi\rangle)$ for every state $|\psi\rangle \in \mathbb{C}^{2^{\otimes k}}$.

For our result, we require U1-U3 to be accomplished up to an arbitrarily small error ε in the standard trace-operator norms. Further, one may adaptively choose $\mathcal{E}$ along the steps of a computation. Last, allowing for two measurement bases in U3 is a pedagogical assumption that we adopt for simplicity of the argument, by enforcing $\mathcal{M}_{\mathcal{O}}$ to exhibit quantum complementarity. One can, nevertheless, relax U3 to having a single basis while preserving the general structure of our proof [10].

The proof of theorem 1 relies on a characterization of non-contextual hidden variable models for qubit QCSIs. We make three key observations about such models.

First, we note that for any pair $\{A, B\} \in \mathcal{J}$ and $\alpha \in \mathbb{R}$ the observables AB and αA can be inferred by measuring A, B, since the eigenvalues of the latter determine those of the former. Hence, $M := \{A, B, AB, \alpha A\}$ belongs to $\mathcal{J}$. Applying Def. 1.(i) to M, we derive two constraints

$$\lambda_\nu(AB) = \lambda_\nu(A)\lambda_\nu(B), \quad \lambda_\nu(\alpha A) = \alpha\lambda_\nu(A), \tag{4}$$

that any $\lambda_\nu \in \Lambda$ must fulfill.

Second, we prove the following lemma.

Lemma 1. *For any QCSI scheme $\mathcal{M}_{\mathcal{O}}$ fulfilling (P1) the phase $\xi(a)$ in (1) can be chosen w.l.o.g. so that*

$$T_a T_b = T_{a+b} \quad \text{for any triple } \{T_a, T_b, T_a T_b\} \in \mathcal{J}. \tag{5}$$

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 $\mathcal{T}_n' := \{T_a' := \lambda_\nu(T_a)T_a, T_a \in \mathcal{T}_n\}$ 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

$$\begin{aligned} T_{a+b}' &= \lambda_\nu(T_{a+b})T_{a+b} = \lambda((\pm 1)T_a T_b)(\pm 1)T_a T_b \\ &\overset{(4)}{=} (\pm 1)^2 \lambda(T_a T_b) T_a T_b \overset{(4)}{=} \lambda(T_a)T_a \lambda(T_b) T_b = T_a' T_b'. \end{aligned}$$

□

Last, we observe that for any $M \in \mathcal{J}$, $|\psi\rangle$ as in (2) and $T_b \in \mathcal{T}_n$, the state $T_b|\psi\rangle$ is a joint eigenstate of M:

$$(\gamma T_a)T_b|\psi\rangle = \left(\lambda_\nu(\gamma T_a)(-1)^{[a,b]}\right) T_b|\psi\rangle, \ \forall \gamma T_a \in M, \tag{6}$$

where $[a, b] := a_X \cdot b_Z + a_Z \cdot b_X \bmod 2$; combined with (4), this induces a group action of $\mathbb{Z}_2^{2n}$ on value assignments

$$\lambda_\nu \quad \overset{u}{\to} \quad \lambda_{\nu+u}(T_a) := \lambda_\nu(T_a)(-1)^{[u,a]}, \ \forall u \in V. \tag{7}$$

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

Lemma 2. *For any qubit scheme $\mathcal{M}_{\mathcal{O}}$ fulfilling (P1) and quantum circuit $\mathcal{C}$ of $\mathcal{M}_{\mathcal{O}}$ operations, if there exists a* NCHVM $(\mathcal{S}, q_{\rho_{in}}, \Lambda)$ *for an input state ρ_{in}, there then exists a* NCHVM $(\mathcal{S}, q_{\rho_{out}}, \Lambda)$ *for the output $\rho_{out} := \mathcal{C}(\rho_{in})$.*

Proof. We fix a phase convention for T_a so that (5) in Lemma1 holds and introduce a simplified notation

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

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 $s_t \in \{\pm 1\}$, $s_{\prec t} := (s_1, \ldots, s_t)$ 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

$$q_{\rho_{t+1}}(\nu) := \frac{\delta_{s_t, \lambda_\nu(a_t)}}{p(s_t|s_{\prec t})} \frac{q_{\rho_t}(\nu) + q_{\rho_t}(\nu + a_t)}{2}, \tag{8a}$$

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,

$$\begin{aligned} \langle T_a\rangle_{\rho_{t+1}}^{\text{HVM}} &= \sum_{\nu \in \mathcal{S}} q_{\rho_{t+1}}(\nu)\lambda_\nu(a) \qquad (9) \\ &\overset{(8a)}{=} \sum_{\nu \in \mathcal{S}} \tfrac{\delta_{s_t,\lambda_\nu(a_t)} q_{\rho_t}(\nu)}{2p(s_t|s_{\prec t})} \lambda_\nu(a) + \sum_{\nu \in \mathcal{S}} \tfrac{\delta_{s_t,\lambda_\nu(a_t)} q_{\rho_t}(\nu + a_t)}{2p(s_t|s_{\prec t})} \lambda_\nu(a). \\ &\overset{(7)}{=} \sum_{\nu \in \mathcal{S}} \tfrac{\delta_{s_t,\lambda_\nu(a_t)} q_{\rho_t}(\nu)}{2p(s_t|s_{\prec t})} \lambda_\nu(a) + \tfrac{\delta_{s_t,\lambda_\nu(a_t)} q_{\rho_t}(\nu)}{2p(s_t|s_{\prec t})} \lambda_\nu(a)(-1)^{[a,a_t]}, \end{aligned}$$

which we evaluate on two cases:

(A) T_a, T_{a_t} anticommute, hence, $[a, a_t] = 1$. We get $\langle T_a\rangle_{\rho_{t+1}}^{\text{HVM}} = 0$, 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

$$\begin{aligned} \langle T_a\rangle_{\rho_{t+1}}^{\text{HVM}} &= \sum_{\nu \in \mathcal{S}} \frac{1 + s_t\lambda_\nu(a_t)}{2p(s_t|s_{\prec t})} q_{\rho_t}(\nu)\lambda_\nu(a) \\ &\overset{(4)}{=} \frac{\sum_{\nu \in \mathcal{S}} q_{\rho_t}(\nu)\lambda_\nu(a) + s_t \sum_{\nu \in \mathcal{S}} q_{\rho_t}(\nu)\lambda_\nu(a + a_t)}{2p(s_t|s_{\prec t})} \end{aligned}$$

Finally, by induction hypothesis, we arrive at

$$\begin{aligned} \langle T_a\rangle_{\rho_{t+1}}^{\text{HVM}} &= \frac{\langle T_a\rangle_{\rho_t} + s_t\langle T_{a+a_t}\rangle_{\rho_t}}{2p(s_t|s_{\prec t})} \overset{(5)}{=} \frac{\operatorname{tr}\left(\rho_t \frac{I + s_t T_{a_t}}{2} T_a\right)}{p(s_t|s_{\prec t})} \\ &= \operatorname{tr}\left(\frac{\left[\frac{I + s_t T_{a_t}}{2} \rho_t \frac{I + s_t T_{a_t}}{2}\right]}{p(s_t|s_{\prec t})} T_a\right) = \operatorname{tr}(\rho_{t+1} T_a) \end{aligned}$$

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 non-contextual. We begin considering tasks Def. 2.U1-U3 to be error-free and drop this assumption at the end.

First, define $\overline{Z_i} := \mathcal{E}(Z_i), \overline{X_j} := \mathcal{E}(X_j)$. Note that by (A1) and Def. 2.U2, the scheme $\mathcal{M}_{\mathcal{O}}$ can prepare the encoded GHZ state $\overline{|\psi\rangle}$ which is uniquely stabilized by $\overline{X_1X_2X_3}$, $-\overline{X_1Z_2Z_3}$, $-\overline{Z_1X_2Z_3}$, $-\overline{Z_1Z_2X_3}$. By Def. 2.U3, $\mathcal{M}_{\mathcal{O}}$ can also infer the value of any correlator of form $\overline{A_1A_2A_3}$ with $\overline{A_i} \in \{\overline{X_i}, \overline{Z_i}\}$ (by measuring $\overline{A_1}, \overline{A_2}, \overline{A_3}$ individually). In particular, $\overline{|\psi\rangle}$'s stabilizers are inferable. For them, quantum mechanics predicts

$$\left\langle \overline{X_1X_2X_3} - \overline{X_1Z_2Z_3} - \overline{Z_1X_2Z_3} - \overline{Z_1Z_2X_3} \right\rangle_{\psi}^{\mathrm{QM}} = 4.$$

On the other hand, by (A2) and Lemma 2, there exists an NCHVM for $\overline{|\psi\rangle}$ with respect to all triples of form $\{\overline{A_1}, \overline{A_2}, \overline{A_3}, \overline{A_1A_2A_3}, \overline{A_i} \in \overline{X_i}, \overline{Z_i}\}$. Using our constraint (4) for non-contextual value assignments, we get a upper bound for the NCHVM's prediction

$$\left\langle \overline{X_1X_2X_3} - \overline{X_1Z_2Z_3} - \overline{Z_1X_2Z_3} - \overline{Z_1Z_2X_3} \right\rangle_{\psi}^{\mathrm{HVM}} \leq 2,$$

which contradicts quantum mechanics. Hence, either (A1) or (A2) must be false.

Last, our argument holds if tasks U1-U3 can be accomplished up to arbitrarily small errors because the NCHVM's prediction deviates from the quantum mechanical one by a finite amount (larger than 2). □

A qubit QCSI scheme powered by contextuality. Next, we prove the existence of a qubit QCSI scheme $\mathcal{M}_{\mathcal{O}}$, based on local Pauli measurements, that fulfills (P1-P2), which seem a priori at tension (see, e.g., Fig. 1, where the constrains on $\mathcal{O}$ lead to a scheme $\mathcal{M}_{\mathcal{O}}$ where Mermin-Peres' square [7, 8] does not exhibit state-independent contextuality, albeit, at the cost of losing tomographic power). Further, we identify a resource *magic state* $|\psi\rangle$ that renders the scheme universality. This full-fledged example illustrates the utility of our main result (Theorem 1), which says that $|\psi\rangle$ must exhibit contextuality with respect to allowed operations in $\mathcal{M}_{\mathcal{O}}$ (an any other true QCSI scheme).

First, note that the value of any Pauli observable can be inferred by measuring its single-qubit tensor components, hence, local QCSI fulfills (P2). Second, we show (P1) is also met by giving a NCHVM for the mixed state $\rho = I/2^n$ with respect to local operations. The most general operation 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 $\lambda_0(\bigotimes_{i=1}^n \sigma_i^{\alpha_i}) := 1$, which is a joint eigenvalue of

(a) (b)

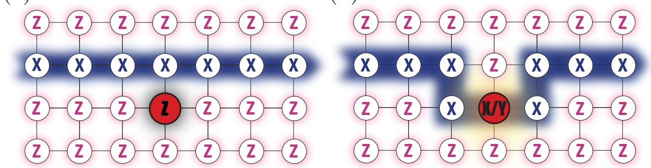

FIG. 2. QCSI with modified cluster state $|\Psi\rangle$ and single-qubit X_i, Y_j, Z_k Pauli measurements: the Z-measurements are used to cut out of the plane a web corresponding to some layout of a quantum circuit; the X-measurements drive the MBQC-simulation of this circuit [11]. By "re-routing" a wire piece, one may choose between implementing and not implementing a non-Clifford gate. (a) Identity operation on the logical state space, (b) Logical $e^{-i\pi/4\,Z}$ gate.

$\{\bigotimes_{i=1}^n \sigma_i^{\alpha_i} : \alpha \in \mathbb{Z}_2^n\}$, 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 (7) with value assignments $\lambda_b(T_a) := (-1)^{[a,b]}, b \in \mathbb{Z}_2^{2n}$ wherein ρ corresponds to a probability distribution $q_\rho(b) := 1/2^{2n}$: 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 $e^{-i\pi/4\,Z}$. 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 [11]. Local Pauli 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 re-route the measuremend-based through a red-site (this can be done with the available X measurements [11]) 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. [12].

Conclusion. In this Letter, we investigated the role of contextuality in qubit QCSI and proved it to be a necessary resource for all such schemes that meet a simple postulate: namely, that the allowed measurements do not exhibit state-independent contextuality. Our result applies if and only if contextuality can be regarded as a physical property possessed by a quantum state. 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 composite dimensions [13] and to generalized QCSI models based on normalizer gates [14–17]. Last, we demonstrated the applicability of our result to a concrete qubit QCSI scheme that does not to exhibit state independent contextuality while retaining tomographic completeness.

Finally, we refer to a companion paper [10] 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.

Acknowledgement. We thank David T. Stephen for comments on the manuscript. JBV acknowledges financial support by AQuS and SIQS. ND is funded by IQIM, the NSF Physics Frontiers Center (PHY-1125565) and the Gordon and Betty Moore Foundation (GBMF-2644). CO is supported by NSERC. RR is funded by NSERC, Cifar. RR is scholar of the Cifar Quantum Information Science program.

[1] S. Bravyi and A. Kitaev, Phys. Rev. A **71** (2005), 10.1103/PhysRevA.71.022316, quant-ph/0403025.
[2] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, California Institute of Technology (1997), quant-ph/9705052v1.
[3] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[4] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New Journal of Physics **14** (2012), arXiv:1201.1256 [quant-ph].
[5] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature **510**, 351 (2014), arXiv:1401.4174 [quant-ph].
[6] N. Delfosse, P. Allard Guerin, J. Bian, and R. Raussendorf, Phys. Rev. X **5**, 021003 (2015), arXiv:1409.5170 [quant-ph].
[7] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[8] A. Peres, Physics Letters A **151**, 107 (1990).
[9] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).
[10] R. Raussendorf, N. Delfosse, D. E. Browne, C. Okay, and J. Bermejo-Vega, arXiv preprint (2015), arXiv:1511.08506 [quant-ph].
[11] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[12] J. Miller and A. Miyake, arXiv preprint (2015), arXiv:1508.02695 [quant-ph].
[13] D. Gottesman, in *Selected papers from the First NASA International Conference on Quantum Computing and Quantum Communications* (Springer, 1998) quant-ph/9802007v1.
[14] M. Van den Nest, Quantum Information and Computation **13** (2013), arXiv:1201.4867v1 [quant-ph].
[15] J. Bermejo-Vega and M. Van Den Nest, Quantum Info. Comput. **14** (2014), arXiv:1210.3637 [quant-ph].
[16] J. Bermejo-Vega, C. Y.-Y. Lin, and M. Van den Nest, Quantum Information and Computation **16** (2016), arXiv:1409.3208 [quant-ph].
[17] J. Bermejo-Vega, C. Yen-Yu Lin, and M. Van den Nest, arXiv preprint (2014), arXiv:1409.4800 [quant-ph].