

State-injection schemes of quantum computation in Spekkens' toy theory

Lorenzo Catani* and Dan E. Browne

Physics and Astronomy department, University College London, Gower St, London WC1E 6BT, United Kingdom

(Received 26 February 2018; published 7 November 2018)

Spekkens' toy theory is a noncontextual hidden variable model with an epistemic restriction, a constraint on what the observer can know about the reality. In reproducing many features of quantum mechanics in an essentially classical model, it clarified our understanding of what behavior can be truly considered intrinsically quantum. In this work, we show that Spekkens' theory can be also used to help understanding aspects of quantum computation—in particular, an important subroutine in fault-tolerant quantum computation called state injection. State injection promotes fault-tolerant quantum circuits, which are usually limited to the classically efficiently simulatable stabilizer operations, to full universal quantum computation. We show that the limited set of fault-tolerant operations used in standard state-injection circuits can be realized within Spekkens' theory, and that state injection leads to nonclassicality in the form of contextuality. To achieve this, we extend prior work connecting Spekkens' theory and stabilizer quantum mechanics, showing that subtheories of the latter can be represented within Spekkens' theory, in spite of the contextuality in qubit stabilizer quantum mechanics. The work shines light on the relationship between quantum computation and contextuality.

DOI: [10.1103/PhysRevA.98.052108](https://doi.org/10.1103/PhysRevA.98.052108)

I. INTRODUCTION

Spekkens' toy theory is a noncontextual hidden variable model made to advocate the epistemic view of quantum mechanics, where quantum states are seen as states of incomplete knowledge about a deeper underlying reality [1,2]. The idea of the model is to reproduce quantum theory through a phase-space-inspired theory with the addition of a constraint on what an observer can know about the ontic state (identified with a phase-space point) describing the reality of a system. In the case of odd-dimensional systems, the toy theory has been proven to be *operationally equivalent* to qudit stabilizer quantum mechanics [3], where the latter is a subtheory of quantum mechanics restricted to eigenstates of tensors of Pauli operators, Clifford unitaries, and Pauli measurement observables [4]. “Operationally equivalent” means that the two theories predict the same statistics of outcomes, given the same states, transformations, and measurements. The equivalence between Spekkens' toy theory and qudit stabilizer quantum mechanics can be proven by representing qudit stabilizer quantum mechanics using Gross' Wigner functions [5]. These turn out to be exactly equivalent to Spekkens' epistemic states and measurements. The measurement update rules are consistent and positiveness-preserving, while Clifford gates are mapped into consistent symplectic affine transformations [3].

In the case of qubits, the above equivalence does not hold. The toy theory is noncontextual by construction, whereas qubit stabilizer quantum mechanics shows state-independent contextuality, as witnessed by the Peres-Mermin square argument [6–8]. This is reflected in the impossibility of finding a nonnegative Wigner function that maps qubit stabilizer quantum mechanics into Spekkens' toy theory [10,11]. Note

that the nonnegativity is needed to interpret the epistemic states and measurements as well-defined probabilities and thus state the operational equivalence. Even if the toy theory and qubit stabilizer quantum mechanics are not operationally equivalent, some restricted versions of them do show the same statistics. Our aim is to identify the subtheories of Spekkens' toy theory that are operationally equivalent to subtheories of qubit stabilizer quantum mechanics. These will be closed subsets of operations, states and measurements in stabilizer quantum mechanics where states and measurements can be nonnegatively represented by covariant Wigner functions.

In this work we use Spekkens' subtheories for an application in the field of quantum computation. More precisely, we use them to study state-injection schemes of quantum computation [12]. The latter are part of one of the currently leading models of fault-tolerant universal quantum computation (UQC). This model is composed of a “free” part, which consists of quantum circuit that are efficiently simulatable by a classical computer (usually stabilizer circuits), and the injection of so-called “magic” resource states (which are usually distilled from many copies of noisy states through magic state distillation [13]) that enable universal quantum computation. In 2014 Howard *et al.* [14] proved that in a state-injection scheme for qudits of odd prime dimensions, with the free part composed by stabilizer circuits, the contextuality possessed *solely* by the magic resource is a necessary resource for universal quantum computation. In terms of systems of dimensions 2 a similar result due to Delfosse *et al.* [15] was derived for rebits, where the classical noncontextual free part is composed of Calderbank-Steane-Shor (CSS) circuits [16]. However, as already pointed out, an analog version of Howard's result for qubits cannot be found, since qubit stabilizer quantum mechanics is already contextual. Nevertheless, it has been proven [17] that in any state-injection scheme for qubits where we get rid of the state-independent contextuality,

*lorenzo.catani.14@ucl.ac.uk

the contextuality possessed *solely* by the magic resource is necessary for universal quantum computation. A more complete version of this result is also treated in Ref. [18], where a general framework for state-injection schemes of qubits with contextuality as a resource is provided.

More precisely, in Ref. [18], Raussendorf *et al.* develop a framework for building nonnegative and noncontextual subtheories of qubit stabilizer quantum mechanics via the choice of a phase function $\gamma(\lambda)$ on phase-space points, which defines the Weyl operators and consequently the Wigner functions [see Eq. (2)]. They require that the allowed free measurements preserve the nonnegativity of the Wigner function. In principle this requirement constrains the number of allowed observables. For this reason they also require tomographic completeness, i.e., that any state can be fully measured by the observables allowed in the free part of the scheme, which guarantees that the set of free observables is large enough for the state-injection scheme to work. Unlike the case of measurements, they allow gates that introduce negativity in the Wigner functions, i.e., noncovariant gates, the reason being that the gates can always be absorbed in the measurements without altering the outcome distribution of the computation. Furthermore, in Ref. [19], Wallman and Bartlett address the issue of finding the subtheories of qubit quantum mechanics that are nonnegative in certain quasiprobability representation (and so are classically simulatable and correspond to noncontextual ontological models). They construct the so-called 8-state model, which can be seen as a generalization of Spekkens' toy theory with an enlarged ontic space. The nonnegativity for states and measurements is guaranteed by considering both the possible Wigner representations of a qubit [11].

It is important to point out that in the mentioned frameworks of Refs. [17] and [18], the definition of state-injection schemes is broader than the one we consider here and it also includes schemes based on measurement-based quantum computation with cluster states [20]. We here consider only state-injection schemes as developed by Zhou *et al.* in Ref. [12]—defined in Sec. II C—like the ones in Refs. [14] and [15], and we show that Spekkens' subtheories are an intuitive and effective tool to treat these cases. We first use Spekkens' subtheories to represent the noncontextual free part of the known examples of state-injection schemes, both for qubits and qudits, where contextuality arises as a resource [14,15]. These can be unified in the following framework (Fig. 1): *Spekkens' subtheory* + *Magic state(s)* \rightarrow *UQC*. Second, we prove in Theorem 1 that qubit SQM can be obtained from a Spekkens' subtheory via state injection since all its objects that do not belong to the Spekkens' subtheory, namely, noncovariant Clifford gates, can be injected, where the circuit needed for the injection is always made of objects belonging to the Spekkens' subtheory. This means that Spekkens' subtheories contain all the tools for performing state-injection schemes of quantum computation. There is no need to consider bigger noncovariant subtheories in the free part.

The proof of Theorem 1 suggests a state-injection scheme, where contextuality is a resource, based on injection of CCZ states. State-injection schemes with the related Toffoli (CCNOT) gates are already known [21–27], but our scheme

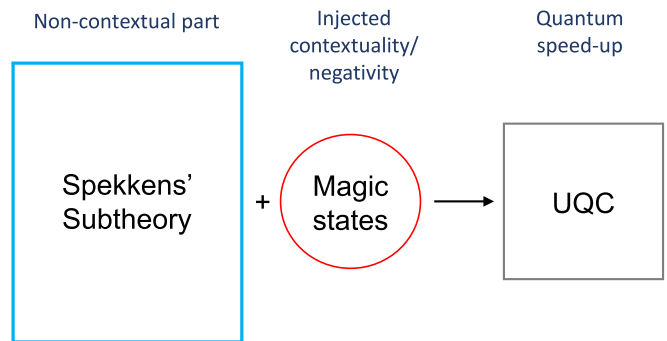


FIG. 1. Computational scheme. Schematic representation of the computational scheme of the paper.

differs from them as our noncontextual free part of the computation—a strict subset of the CSS rebit subtheory considered in Ref. [15]—is such that it is not possible to remove any object from it without denying the possibility of obtaining universal quantum computation via state injection. The price to pay for this minimality is the injection of the control- Z state, $CZ|++\rangle$, too (which also provides the Hadamard gate). By analyzing this example, we can associate different proofs of contextuality to the injection of different states, making a link between different classes of contextuality experiment and different states. More precisely, we show how the Clifford noncovariant CZ gate (as well as the phase gate S) can provide proofs of the Peres-Mermin square argument and the GHZ paradox. Moreover, the injection of the $T|+\rangle$ magic state, where T is the popular $\frac{\pi}{8}$ non-Clifford gate, allows, in addition to the previous proofs of contextuality (as $T^2 = S$), also to obtain the maximum quantum violation of the CHSH inequality [28].

In the remainder of the paper we start by covering some preliminary material on Spekkens' toy theory, Wigner functions and state-injection schemes in Sec. II. We then provide the definition of a Spekkens' subtheory in Sec. III. In Sec. IV we describe Howard's and Delfosse's cases for qudits [14] and rebits [15], respectively, and we prove that they fit in our framework where the free parts of the computation, qudit stabilizer quantum mechanics, and CSS rebits, respectively, are Spekkens' subtheories. We then set the instructions to construct a Spekkens' subtheory from the choice of a nonnegative Wigner function in Sec. V. We do so in line with Ref. [18] and we find that the main difference from Raussendorf *et al.*'s formulation (and also from the 8-state model) consists of demanding for the covariance of the Wigner function with respect to the allowed gates. Moreover, we do not demand for tomographic completeness. By exploiting this comparison we then prove Theorem 1. It basically shows that any state-injection scheme can be obtained from our framework, since any object not present in the considered Spekkens' subtheory can be injected by using an injection scheme made of objects in the Spekkens' subtheory. In Sec. VI we provide an example of state injection for qubits (rebits) based on CCZ magic states. We analyze the presence of different proofs of contextuality in correspondence of different state injected gates in Sec. VII and we recap all the results and the future directions in Sec. VIII.

II. PRELIMINARIES

In this work we focus on subtheories of quantum mechanics that we call Spekkens' subtheories, and their relation with state-injection schemes of quantum computation. We here recall some basic notions and definitions characterizing Spekkens' toy theory, Wigner functions, and state-injection schemes that will be useful for our purposes.

A. Spekkens' toy theory

Spekkens' toy theory is a noncontextual hidden variable theory with an *epistemic restriction*, i.e., a restriction on what can be known about the hidden variables (or *ontic states*) describing the physical system [1–3]. Ontic states are points λ in phase space, which we here assume to be discrete, $\Omega = \mathbb{Z}_d^n$, where n is the number of the d -dimensional subsystems composing the system. An Observable Σ is defined as a linear functional in phase space, i.e., it takes the form $\Sigma = \sum_m (a_m X_m + b_m P_m)$, where X_m, P_m denote fiducial variables, like position and momentum, that label the phase space, $a_m, b_m \in \mathbb{Z}_d$, and $m \in 0, \dots, n-1$. In the following we denote the ontic states and observables when considered in their vectorial representation, and vectors in general, with bold characters. The outcome σ of any observable measurement $\Sigma = (a_0, b_0, \dots, a_{n-1}, b_{n-1})$ given the ontic state $\lambda = (x_0, p_0, \dots, x_{n-1}, p_{n-1})$, where $x_j, p_j, a_j, b_j \in \mathbb{Z}_d$ for every $j \in \{0, \dots, n-1\}$, is given by their inner product: $\sigma = \Sigma^T \lambda = \sum_j (a_j x_j + b_j p_j)$, where all the arithmetic is over \mathbb{Z}_d .

The epistemic restriction is called the *classical complementarity principle* and it states that two observables can be jointly known only when their Poisson bracket is zero. This can be simply recast in terms of the symplectic inner product: $[\Sigma_1, \Sigma_2] \equiv \Sigma_1^T J \Sigma_2 = 0$, where $J = \bigoplus_{j=1}^n \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. A set of observables that can be jointly known by the observer represents a subspace of Ω , known as an *isotropic subspace* and denoted as $V = \text{span}\{\Sigma_1, \dots, \Sigma_n\} \subseteq \Omega$, where Σ_i indicates one of the generators of V .

The observer's best description of the physical system is a probability distribution $p(\lambda)$ over Ω which is called the *epistemic state*. It is defined as

$$P_{(V, \mathbf{w})}(\lambda) = \frac{1}{N} \delta_{V^\perp + \mathbf{w}}(\lambda), \quad (1)$$

where the perpendicular complement of V is, by definition, $V^\perp = \{a \in \Omega \mid \mathbf{a}^T \mathbf{b} = 0 \forall b \in V\}$. The subspace of known variables V specifies the observables Σ_j that are known and the evaluation shift vector $\mathbf{w} \in V$ the values σ_j that they take, $\Sigma_j^T \cdot \mathbf{w} = \sigma_j$. The indicator function $\delta_{V^\perp + \mathbf{w}}(\lambda)$ takes value 1 when λ belongs to the set $V^\perp + \mathbf{w}$ and 0, otherwise; N is a normalization factor.

The allowed transformations in Spekkens' theory are the ones that preserve the epistemic restriction, i.e., the symplectic affine transformations G in phase space (in general, a subset of the permutations), namely, $G(\lambda) = S\lambda + \mathbf{a}$, where S is a symplectic matrix and $\mathbf{a} \in \Omega$ is a translation vector. The elements Π_k of a sharp measurement Π , where the integer k denotes the outcome associated with the measurement, have an epistemic representation analog to the states of the form

of Eq. (1). Here, we are in a dual representation between states and observables, where we denote with V_Π and \mathbf{r}_k the subspace of known observables and the evaluation shift vector associated with the k th element of the sharp measurement, respectively. Figure 2 provides a graphic representation of epistemic states, observables, and evolutions for some particular examples of quantum states, observables, and gates.

B. Wigner functions

Wigner functions are a way of recasting quantum mechanics in the phase-space framework [9–11]. They are called quasiprobability distributions, not proper probability distributions, because they can take also negative values. Nevertheless, their marginals represent probability distributions of measurement outcomes. The feature of negativity is usually associated with a signature of nonclassicality [29,30]. We here define Wigner functions following Ref. [18]. The Wigner function of a quantum state ρ is defined by the function γ ,

$$W_\rho^\gamma(\lambda) = \text{Tr}[A^\gamma(\lambda)\rho], \quad (2)$$

where the phase-point operator is

$$A^\gamma(\lambda) = \frac{1}{N_\Omega} \sum_{\lambda' \in \Omega} \chi([\lambda, \lambda']) T^\gamma(\lambda'), \quad (3)$$

and the Weyl operator is defined by

$$T^\gamma(\lambda) = w^{\gamma(\lambda)} Z(\lambda_Z) X(\lambda_X), \quad (4)$$

where the phase-space point is $\lambda = (\lambda_Z, \lambda_X) \in \Omega$. We will omit the superscript γ in the future to soften the notation. The normalization N_Ω is such that $\text{Tr}[A(\lambda)] = 1$. The functions χ and w will be appropriately characterized in the case of qubits and qudits in Sec. IV, as well as γ . The operators $Z(\lambda_Z), X(\lambda_X)$ represent the (generalized) Pauli operators,

$$X(\lambda_X) = \sum_{\lambda'_X \in \mathbb{Z}_d} |\lambda'_X - \lambda_X\rangle \langle \lambda'_X|, \quad (5)$$

$$Z(\lambda_Z) = \sum_{\lambda_X \in \mathbb{Z}_d} \chi(\lambda_X \lambda_Z) |\lambda_X\rangle \langle \lambda_X|. \quad (6)$$

The most important property of the Wigner functions for this work is the property of covariance, which means that (in accordance with the definition used by Gross in Ref. [5], Theorem 7]), for all allowed states ρ in the theory,

$$W_{U\rho U^\dagger}(\lambda) = W_\rho(S\lambda + \mathbf{a}), \quad (7)$$




where S is a symplectic transformation and \mathbf{a} is a translation vector. This property guarantees that the transformations in quantum mechanics correspond to symplectic affine transformations in phase space.

C. State-injection schemes of quantum computation

In this work we consider state-injection schemes of quantum computation as developed in Ref. [12]. They represent one of the leading models for fault-tolerant universal quantum computation when combined with the magic state distillation procedure due to Bravyi and Kitaev in Ref. [13]. The latter allows to distill nonstabilizer magic states from noisy copies of quantum states with a high threshold for the error rate

Quantum State	Spekkens' epistemic state	Quantum State	Spekkens' epistemic state
$ 0\rangle$	$(0, y)$ (x,P) $(1,1)$ <input type="checkbox"/> $(1,0)$ <input type="checkbox"/> $(0,1)$ <input checked="" type="checkbox"/> $(0,0)$ <input checked="" type="checkbox"/>	$ +\rangle$	$(x, 0)$ (x,P) $(1,1)$ <input type="checkbox"/> $(1,0)$ <input checked="" type="checkbox"/> $(0,1)$ <input checked="" type="checkbox"/> $(0,0)$ <input checked="" type="checkbox"/>
$ 1\rangle$	$(1, y)$ (x,P) $(1,1)$ <input checked="" type="checkbox"/> $(1,0)$ <input checked="" type="checkbox"/> $(0,1)$ <input type="checkbox"/> $(0,0)$ <input type="checkbox"/>	$ -\rangle$	$(x, 1)$ (x,P) $(1,1)$ <input checked="" type="checkbox"/> $(1,0)$ <input type="checkbox"/> $(0,1)$ <input checked="" type="checkbox"/> $(0,0)$ <input type="checkbox"/>

Observable	Spekkens' representation
Z	$\left\{ \begin{array}{l} (x,P) \\ (1,1) \\ (1,0) \\ (0,1) \\ (0,0) \end{array} \right\}, (1, y) \left\{ \begin{array}{l} (x,P) \\ (1,1) \\ (1,0) \\ (0,1) \\ (0,0) \end{array} \right\}$
X	$\left\{ \begin{array}{l} (x,P) \\ (1,1) \\ (1,0) \\ (0,1) \\ (0,0) \end{array} \right\}, (x, 1) \left\{ \begin{array}{l} (x,P) \\ (1,1) \\ (1,0) \\ (0,1) \\ (0,0) \end{array} \right\}$

Gate	Spekkens' representation	Example
X	$(x, y) \rightarrow (x + 1, y)$	$(0, y) \rightarrow (1, y)$ 
Y	$(x, y) \rightarrow (x + 1, y + 1)$	$(0, y) \rightarrow (1, y)$ 
Z	$(x, y) \rightarrow (x, y + 1)$	$(x, 0) \rightarrow (x, 1)$ 

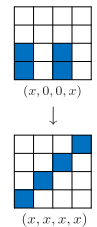
Gate	Spekkens' representation	Example
$CNOT$	(x_1, y_1, x_2, y_2) \downarrow $(x_1, y_1 + y_2, x_1 + x_2, y_2)$	$(x, 0, 0, x)$ \downarrow (x, x, x, x) 

FIG. 2. Representation of a noncontextual subtheory of qubit stabilizer quantum mechanics in Spekkens' toy model. In the figure above, in order, the allowed pure states, observables, and gates of the noncontextual subtheory of qubit stabilizer quantum mechanics considered in the proof of Theorem 1 are represented in Spekkens' toy model, according to the definitions of epistemic states, observables, and evolutions (gates) defined in Sec. II A. We have also indicated the probability distributions associated to the epistemic states, where $x, y \in \mathbb{Z}_d$, and how the gates act on them. In the last two figures we have considered the scenarios corresponding to acting with X, Y on $|0\rangle$, with Z on $|+\rangle$ and with $CNOT$ on $|+\rangle$ (thus obtaining the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$). More detailed examples can be found in Refs. [2] and [3].

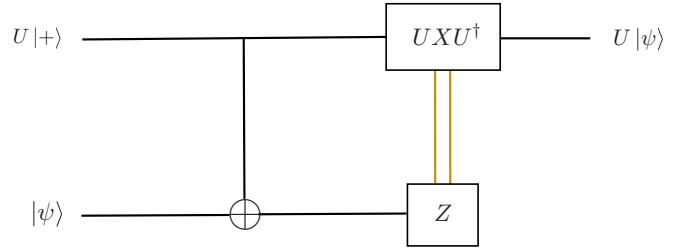


FIG. 3. State-injection schemes of quantum computation. The state-injection schemes that we consider in this work are the ones developed by Zhou, Leung, and Chuang in Ref. [12]. The diagonal gate U can be injected in the circuit by using objects that are allowed in the free part of the computation. The injected state is $U|+\rangle$, which is subjected to a controlled not with the input state $|\psi\rangle$. Conditioned on the outcome of the measurement of the Pauli Z on the state $|\psi\rangle$ after the CNOT, the correction UXU^\dagger is applied to the state $U|+\rangle$. At the end we obtain the gate U applied to the input state $|\psi\rangle$.

(about 14.6%), given a setting where only Clifford gates are fault tolerant. The key idea of state injection is that a non-Clifford gate can be implemented with the combination of the magic state, a Clifford group circuit and Pauli measurements. More precisely, we can define state-injection schemes for implementing any diagonal unitary gate U as follows.

Definition 1 (Zhou-Leung-Chuang state injection [12]): A **state injection** of an n -qubit unitary gate U is a quantum circuit implementing U composed of the following elements (Fig. 3).

- (1) The injected state $U|+\rangle^{\otimes n}$.
- (2) n CNOT gates, applied transversally.
- (3) n Pauli Z measurements, with the output of the j th measurement denoted as $s_j = (-1)^{m_j}$, where $m_j \in \{0, 1\}$.
- (4) The correction gate $UX^m U^\dagger$, where $m = m_1 \dots m_n$ is the bitstring of measurement outcomes and $X^m = X^{m_1} \otimes \dots \otimes X^{m_n}$.

As was proved in Ref. [12], any diagonal gate U can be implemented via a state-injection circuit of this form. However, for the injection of U to succeed deterministically, the unitary correction $UX^m U^\dagger$ must be implementable in the model. Figure 3 depicts the state-injection scheme just defined.

III. CHARACTERIZATION OF SPEKKENS' SUBTHEORIES

A Spekkens' subtheory is defined as a set of quantum states, transformations, and measurements, $(\mathcal{S}, \mathcal{T}, \mathcal{M})$, which satisfies the following conditions.

- (1) *Subtheory*. The set must be *closed*, which means that any allowed gate cannot bring from one allowed state to a nonallowed one:

$$\forall U \in \mathcal{T}, U\rho U^\dagger \in \mathcal{S} \forall \rho \in \mathcal{S}. \quad (8)$$

- (2) *Spekkens representability*. There must be an operational equivalence between the subtheory of quantum mechanics $(\mathcal{S}, \mathcal{T}, \mathcal{M})$, defined by sets of quantum states, transformations, and measurements, and a subtheory of Spekkens' toy theory $(\mathcal{S}_s, \mathcal{T}_s, \mathcal{M}_s)$, defined by sets of epistemic states,

symplectic affine transformations, and measurements as defined in the previous section.

The operational equivalence means that the statistics of the two subtheories $(\mathcal{S}, \mathcal{T}, \mathcal{M})$ and $(\mathcal{S}_s, \mathcal{T}_s, \mathcal{M}_s)$ are the same. We state this equivalence by finding a *nonnegative* Wigner function that maps the states ρ and the measurement elements Π_k in $(\mathcal{S}, \mathcal{M})$ to epistemic states and measurement elements in $(\mathcal{S}_s, \mathcal{M}_s)$, i.e.,

$$W_\rho(\lambda) = \frac{1}{N} \text{Tr}[\rho A(\lambda)] = \frac{1}{N} \delta_{(V^\perp + \mathbf{w})}(\lambda), \quad (9)$$

$$W_{\Pi_k}(\lambda) = \frac{1}{N'} \text{Tr}[\Pi_k A(\lambda)] = \frac{1}{N'} \delta_{(V_{\Pi}^\perp + \mathbf{r}_k)}(\lambda). \quad (10)$$

The N, N' are the normalization factors so that $\sum_{\lambda \in \Omega} W(\lambda) = 1$ for all the above Wigner functions. Notice at this point that the measurement update rules in Ref. [3] guarantee that also a state after a measurement is nonnegatively represented if the measurement and the original state have nonnegative Wigner functions, as they involve only sums and products of Wigner functions. Moreover we are considering subtheories with duality between states and measurement elements, therefore it is enough to check only the properties of the Wigner functions of states (or measurements) to guarantee Spekkens representability.

The operational equivalence in terms of transformations is implied if the Wigner function Eq. (9) satisfies the property of covariance Eq. (7) for the allowed unitaries $U \in \mathcal{T}$, which guarantees that the transformations in quantum mechanics correspond to transformations that preserve the epistemic restriction in Spekkens' theory. Notice that the property of covariance is defined in terms of Wigner functions and not directly in terms of the phase point operators.¹ Therefore, we do not necessarily need to demand for the standard Wigner function of the transformation, defined as $W_U(\lambda|\lambda') = \frac{1}{N'} \text{Tr}(A(\lambda) U A(\lambda') U^\dagger)$, to be nonnegative in all its elements, once the previous requirements, nonnegativity and covariance of W_ρ , are satisfied. The transition matrix corresponding to the allowed permutation of the phase points can be always found, as shown by the following lemma.

Lemma 1: Given nonnegative Wigner function representations, $W_\rho, W_{\rho'}$, of any two allowed states $\rho, \rho' \in \mathcal{S}$ such that $\rho' = U\rho U^\dagger$, where $U \in \mathcal{T}$, and covariance holds, i.e., $W_{\rho'}(\lambda) = W_\rho(S\lambda + \mathbf{a})$, there always exists a (nonnegative) transition matrix $P_U : \Omega \times \Omega \rightarrow [0, 1]$ representing the transformation $U \in \mathcal{T}$,

$$P_U(\lambda|\lambda') = \frac{1}{N''} \delta_{\lambda, S\lambda' + \mathbf{a}}, \quad (11)$$

where N'' is the normalization factor, such that

$$W_{\rho'}(\lambda) = \sum_{\lambda' \in \Omega} P_U(\lambda|\lambda') W_\rho(\lambda'). \quad (12)$$

Proof. A matrix made of nonnegative elements $P_U(\lambda|\lambda')$ proportional to Kronecker δ 's always exists because it corresponds to the transition matrix representing the permutation

that brings W_ρ to $W_{\rho'}$. More precisely, nonnegative solutions $P_U(\lambda|\lambda')$ to the Eq. (12) for every λ , given the nonnegative $W_\rho(\lambda'), W_{\rho'}(\lambda)$ defined in Eq. (2), always exist. For every fixed λ , the $P_U(\lambda|\lambda')$ are vectors with all zero components apart from one, i.e., they are proportional to Kronecker δ 's. The covariance property Eq. (7) guarantees that this permutation corresponds to a symplectic affine transformation on the phase-space points (independent on the state ρ that U is acting on).

The nonnegative functions Eqs. (9), (10), and (11) can be interpreted as probability distributions and guarantee that the theories $(\mathcal{S}, \mathcal{T}, \mathcal{M})$ and $(\mathcal{S}_s, \mathcal{T}_s, \mathcal{M}_s)$ are operationally equivalent, i.e., they provide the same statistics:

$$\begin{aligned} p(k) &= \text{Tr}(\Pi_k U \rho U^\dagger) \\ &= \sum_{\lambda \in \Omega} W_{\Pi_k}(\lambda) \sum_{\lambda' \in \Omega} P_U(\lambda|\lambda') W_\rho(\lambda'). \end{aligned} \quad (13)$$

To sum up, a Spekkens' subtheory is a (closed) subtheory of quantum mechanics whose states (and measurements) are represented by nonnegative and covariant Wigner functions. We say that a Spekkens' subtheory is *maximal* if the set $(\mathcal{S}, \mathcal{T}, \mathcal{M})$ is such that by adding either another state, gate, or observable to the set of allowed states, transformations, and observables contradicts at least one of the conditions above, i.e., it is no longer a subtheory or Spekkens representable. We will also talk about *minimal* noncontextual subtheories of stabilizer quantum mechanics, meaning those subtheories that can no longer be used for state-injection schemes after the removal of just one object from them.

IV. WIGNER FUNCTIONS FOR SPEKKENS' SUBTHEORIES

We now identify the functions γ defining the Wigner functions in Eq. (2) that allow us to show that the known examples of state-injection schemes with contextuality as a resource, Refs. [14] and [15], fit into the framework depicted in Fig. 1, i.e., that the free parts of those schemes are Spekkens' subtheories.

A. Qudit case

In the case of qudits of odd dimensions Gross' theorem [5] guarantees that there is a nonnegative Wigner representation of all pure stabilizer states. This Wigner function is covariant and also Clifford transformations and Pauli measurements are nonnegatively represented. Thus Gross' Wigner function proves the operational equivalence, in odd dimensions, between stabilizer quantum mechanics and the whole Spekkens' toy theory, as shown in Refs. [2] and [3].

Gross' Wigner function for odd dimensional systems (qudits) is defined according to Eq. (2), where $\chi(a) = e^{\frac{2\pi i}{d} a}$, for $a \in \mathbb{Z}_d$, and $w^{\gamma(\lambda)} = \chi(-2^{-1}\gamma(\lambda))$. The function γ is given by $\gamma(\lambda) = \lambda_X \cdot \lambda_Z$.

In the scheme of Howard *et al.* [14] where they prove that contextuality is a resource for universal quantum computation, the free part of the computation is given by stabilizer quantum

¹This will make a difference only in Sec. IV B, where we consider factorizable Wigner functions for the CSS rebit case.

mechanics in odd prime dimensions, which, by Gross’ Wigner functions, is a maximal Spekkens’ subtheory.²

B. Qubit case

In the case of qubits an analog of Gross’ Wigner function for stabilizer quantum mechanics does not exist [10,11], as some negative stabilizer states are present for any possible choice of Wigner functions. This is related to the contextuality shown by qubit stabilizer quantum mechanics (see, for example, the Peres-Mermin square [8]). Nevertheless, it is possible to state a similar result to Howard *et al.*’s by restricting the free part of the computation to a strict noncontextual and positive subtheory of qubit stabilizer quantum mechanics, as shown by the result of Delfosse *et al.* in 2015 [15].

We start by describing the set of allowed states/gates/observables ($\mathcal{S}_r, \mathcal{T}_r, \mathcal{M}_r$) considered by Delfosse *et al.* The set \mathcal{S}_r , a subset of the stabilizer states, is composed by Calderbank-Steane-Shor (CSS) states [16], i.e., stabilizer states $|\psi\rangle$, whose corresponding stabilizer group $S(|\psi\rangle)$ decomposes into an X and a Z part; i.e., $S(|\psi\rangle) = S_X(|\psi\rangle) \times S_Z(|\psi\rangle)$, where all elements of $S_X(|\psi\rangle)$ and $S_Z(|\psi\rangle)$ are of the form $X(\mathbf{q})$ and $Z(\mathbf{p})$, respectively, where $\mathbf{q}, \mathbf{p} \in \mathbb{Z}_2^n$. CSS states are the eigenstates of the allowed observables belonging to the set \mathcal{M}_r ,

$$\mathcal{M}_r = \{X(\mathbf{q}), Z(\mathbf{p}) | \mathbf{q}, \mathbf{p} \in \mathbb{Z}_2^n\}. \tag{14}$$

The set of allowed transformations is composed by the CSS preserving gates, a subset of the Clifford group C_n (which is the group of unitaries that maps Pauli operators to Pauli operators by conjugation),

$$\begin{aligned} \mathcal{T}_r &= \{g \in C_n | g|\psi\rangle \in \mathcal{S}_r, \forall |\psi\rangle \in \mathcal{S}_r\} \\ &= \left\langle \bigotimes_{i=1}^n H_i, \text{CNOT}(i, j), X_i, Z_i \right\rangle, \end{aligned} \tag{15}$$

where $i, j \in \{1, 2, \dots, n\}$ and $i \neq j$. The universal quantum computation is reached by injecting two particular magic states to the free subtheory of CSS rebits just described [15].

The Wigner function used by Delfosse *et al.* to prove their result is given by

$$A_r(\lambda) = \frac{1}{2^n} \sum_{T(\lambda') \in \mathcal{A}} (-1)^{\langle \lambda, \lambda' \rangle} T(\lambda'), \tag{16}$$

where $T(\lambda) = Z(\mathbf{p}) \cdot X(\mathbf{q})$, $\lambda = (\mathbf{q}, \mathbf{p})$, and $\mathcal{A} = \{T(\lambda) | \mathbf{q} \cdot \mathbf{p} = 0 \text{ mod } 2\}$, where $\mathbf{q} \cdot \mathbf{p}$ denotes the inner product. The set \mathcal{A} is the set of inferred observables. ‘‘Inferred’’ means that these observables may not be directly measurable, but they can be inferred by multiple measurements. For example, in the case of two qubits, the set \mathcal{M}_r and \mathcal{A} are $\mathcal{M}_r = \{\mathbb{I}\mathbb{I}, \mathbb{I}X, \mathbb{I}Z, X\mathbb{I}, Z\mathbb{I}, XX, ZZ\}$, and $\mathcal{A} = \{\mathbb{I}\mathbb{I}, \mathbb{I}X, \mathbb{I}Z, X\mathbb{I}, Z\mathbb{I}, XX, ZZ, XZ, ZX, YY\}$, i.e., the set of all rebits observables. Notice that we removed the ‘‘ \otimes ’’ symbol for the tensor product to simplify the notation. This Wigner

function is always nonnegative for CSS states [15] and it is covariant. In terms of the definition provided in Eq. (2), the function γ is $\gamma(\lambda) = 0$, $\chi(a) = (-1)^a$ and $w^{\gamma(\lambda)} = 1$. This choice guarantees that the phase point operators are Hermitian. However, the price to pay for the Hermiticity in this case is the nonfactorizability of the Wigner function, i.e., the Wigner function is composed by phase-point operators of n qubits that are not given by the tensor products of the ones for the single qubit, e.g., $A_r((0, 0), (0, 0)) \neq A_r(0, 0) \otimes A_r(0, 0)$.

Before we proceed, one may wonder whether the nonfactorisability of the Wigner function is necessary to treat the CSS case and preserve the nonnegativity and covariance. Here we show that it is not. We define a Wigner function that, we argue, is more in line with the construction of Spekkens’ model, where the ontic space of n systems is made by the cartesian products of individual systems’ subspaces. The nonnegative, covariant and factorisable Wigner function for the CSS theory is built out from the single-qubit phase-point operators

$$A_f(0, 0) = \mathbb{I} + X + Z + iY. \tag{17}$$

The phase point operators $A_f(0, 1), A_f(1, 0), A_f(1, 1)$ are given by applying the Pauli X, Y, Z , respectively, by conjugation on $A_f(0, 0)$. The phase point operators of many qubits are given by tensor products of the ones for single qubits $A_f(0, 0), A_f(0, 1), A_f(1, 0), A_f(1, 1)$. Notice that the phase point operators are not Hermitian; however, the allowed observables are only present in their Hermitian part (e.g., for the single qubit in $\mathbb{I} + X + Z$). We now need to prove the following lemma.

Lemma 2: The Wigner function of Delfosse *et al.* $W_r(\lambda) = \text{Tr}(\rho A_r(\lambda))$, given by Eq. (16), is equivalent to the factorisable Wigner function $W_f(\lambda) = \text{Tr}(\rho A_f(\lambda))$, given by Eq. (17), for any $\rho \in \mathcal{S}_r$.

Proof. What we need to prove is actually that $A_r(\lambda) = \mathcal{H}[A_f(\lambda)]$, where $\mathcal{H}[A_f(\lambda)]$ indicates the Hermitian part of the phase point operator $A_f(\lambda)$. The non-Hermitian part of $A_f(\lambda)$ has zero contribution to the Wigner function. It is always composed of tensors of mixtures of Pauli operators with an odd number of Y ’s, that never form allowed observables and so are never in the stabilizer group of any $\rho \in \mathcal{S}_r$. This implies that the non-Hermitian part of $A_f(\lambda)$ has no contribution to the Wigner function as Pauli operators (apart from the identity) are traceless. However, the non-Hermitian part of $A_f(\lambda)$ is important since when its operators compose into phase point operators for multiple qubits, they sometimes provide Hermitian operators that contribute to the Wigner function. We know that $A_r(\lambda)$ is defined as the sum of observables $T(\lambda)$, where $\lambda = (\mathbf{q}, \mathbf{p})$ such that $\mathbf{q} \cdot \mathbf{p} = 0 \text{ mod } 2$. We can now see that also $\mathcal{H}[A_f(\lambda)]$ is given by the sum of observables subjected to the same condition of having zero inner product between the components. This condition indeed singles out all the rebits observables, which are the only ones we are interested in. Given an observable $T(\lambda) = Z(\mathbf{p})X(\mathbf{q})$ in $A_f(\lambda)$, with $\lambda = (\mathbf{q}, \mathbf{p})$ and $\mathbf{q}, \mathbf{p} \in \mathbb{Z}_2^n$, it is Hermitian if and only if $T(\lambda) = T(\lambda)^\dagger$. This means that

$$T(\lambda)^\dagger = X(\mathbf{q})Z(\mathbf{p}) = (-1)^{\mathbf{q} \cdot \mathbf{p}} T(\lambda),$$

which holds if and only if $\mathbf{q} \cdot \mathbf{p} = 0 \text{ mod } 2$.

²Stabilizer quantum mechanics in odd dimensions is the unique maximal Spekkens’ subtheory, since it coincides with the whole Spekkens’ theory.

In conclusion, by using one of the above Wigner functions, Eq. (16) or (17), given the duality between states and measurement elements, the covariance and Lemma 1, we can conclude that CSS rebit subtheory is Spekkens-representable. Moreover the definition of CSS-preserving transformations guarantees the closure property and the discrete Hudson's theorem for rebits (i.e., nonnegativity of the Wigner function of a state if and only if it is a CSS state [15]) guarantees that it is maximal. Therefore, the CSS rebit subtheory of quantum mechanics is a maximal Spekkens' subtheory.

V. SPEKKENS' SUBTHEORIES AS TOOLBOXES FOR STATE INJECTION

We now prove that qubit stabilizer quantum mechanics can be obtained from a Spekkens' subtheory, in the sense that within Spekkens' subtheories it is possible to build a state-injection scheme that injects all the objects of qubit stabilizer quantum mechanics that are not in the subtheories. We need to understand which objects we actually need to inject to reach the full qubit stabilizer quantum mechanics from a Spekkens' subtheory. Let us start by stating the list of instructions to construct the *maximal* Spekkens' subtheory that corresponds to a given choice of γ (in analogy with the framework of [18]).³ We recall that the function γ uniquely specifies the function $\beta(\lambda, \lambda')$, defined such that $T(\lambda)T(\lambda') = w^{\beta(\lambda, \lambda')}T(\lambda + \lambda')$. It results that the observable $T(\lambda)$ preserves positivity iff $\beta(\lambda, \lambda') = 0 \forall \lambda' \text{ s.t. } [\lambda, \lambda'] = 0$, as proven in Ref. [18].

(1) The function γ uniquely defines the set of allowed observables, $\mathcal{M} = \{T(\lambda) \mid \beta(\lambda, \lambda') = 0 \forall \lambda' \text{ s.t. } [\lambda, \lambda'] = 0\}$.

(2) The set of allowed states \mathcal{S} is given by the states corresponding to common eigenstates of d^n commuting observables in \mathcal{M} .

(3) The set of allowed gates is $\{U \mid U\rho U^\dagger = \rho' \in \mathcal{S} \forall \rho \in \mathcal{S}, \text{ and } W_{U\rho U^\dagger}(\lambda) = W_\rho(S\lambda + \mathbf{a}) \forall \lambda \in \Omega\}$. This is a subset of the Clifford unitaries.

Let us point out that the above construction differs from Ref. [18] in that it does not require tomographic completeness and it does require covariance of the Wigner functions. With respect to the Wallman-Bartlett 8-state model [19] the difference holds for analogous reasons. The 8-state model consists of a measurement noncontextual ontological model for *one* qubit stabilizer quantum mechanics, where the one-qubit quantum states (and measurement elements) are represented as uniform probability distributions over an ontic space of dimension 8 and the Clifford transformations (generated by the Hadamard H and phase gate S) are represented by permutations over the ontic space. In the definition of the one qubit stabilizer distributions both the possible phase-point operators for a Wigner function are considered, i.e., both the one with an even number of minuses $A_+(0, 0) = 1 + X + Y + Z$, and the one with an odd number $A_-(0, 0) = 1 + X + Y - Z$. See Ref. [11] for a more extensive description of these two possible pairs of single qubit Wigner functions.

³Notice that with the following construction a given γ provides the *maximal* Spekkens' subtheory, but the Wigner function from the same γ can, obviously, be used to represent any smaller subtheory of the maximal Spekkens' subtheory.

In addition to this, the proposed and straightforward generalization of the 8-state model to more than one qubit, consists of considering the distributions built from the tensor products of the phase-point operators of the single qubit [19]. The resulting subtheory of qubit stabilizer quantum mechanics described by the model then becomes the one composed by all the product states of tensors of Pauli X, Y, Z observables and all the *local* Clifford unitary gates (generated by local H and S). No entanglement is present. Nevertheless, it is possible to reach universal quantum computation from this subtheory by performing measurement-based quantum computation [20] with a particular entangled cluster state [17, 18].

We have seen that the presence of noncovariant Clifford gates in the framework of Raussendorf *et al.* and the 8-state model is the main difference with respect to Spekkens' subtheories. Furthermore, the implementation of all the noncovariant Clifford unitaries would boost Spekkens' subtheories, composed by covariant Clifford gates, to the full qubit stabilizer quantum mechanics.

Theorem 1: Qubit stabilizer quantum mechanics can be obtained from a Spekkens' subtheory via state injection: All the possible noncovariant Clifford gates can be state-injected via a circuit made of objects in the Spekkens' subtheory.

Proof. To prove that qubit stabilizer quantum mechanics can be obtained from a Spekkens' subtheory via state injection we need to show that all the objects needed for injecting any noncovariant Clifford gate are present in at least one Spekkens' subtheory. We recall that to generate the whole Clifford group we need, in addition to the CNOT, also the generators of the local single gates, e.g., the usual phase and Hadamard gates, S, H . Let us consider the following subtheory, which corresponds to the CSS rebit subtheory, Eqs. (14) and (15), with no global Hadamard gates:

(1) The allowed observables are, analogous to Eq. (14), nonmixing tensors of X and Z Pauli operators, $\mathcal{M} = \{X(\mathbf{q}), Z(\mathbf{p}) \mid \mathbf{q}, \mathbf{p} \in \mathbb{Z}_2^n\}$.

(2) The allowed gates are the ones generated by the CNOT and the Pauli rotations X, Z , i.e.,

$$\mathcal{T} = \langle \text{CNOT}(i, j), X_i, Z_i \rangle. \quad (18)$$

(3) The allowed states are, as usual, the eigenstates of the allowed observables.

This is a smaller subtheory than CSS rebit (the difference being the absence of the global Hadamard gate). It possesses all the objects needed for state injection of noncovariant gates. The Z observables and the CNOT gate are present. The correction gates are always Pauli gates, as for any injected Clifford unitary U , even when U is noncovariant, $UX^{\otimes n}U^\dagger$, by definition of a Clifford gate, gives back a Pauli gate. All the objects of this subtheory can be nonnegatively represented by the Wigner functions for the CSS rebit theory of the previous section and also in Spekkens' toy model, as shown in Fig. 2. Therefore, this subtheory is closed and Spekkens representable, i.e., a Spekkens' subtheory, and it is possible for it to reach universal quantum computation via state injection, as proven in detail in the next section.

Here, we will first show that we can obtain the whole Clifford group. Once we have it, we can map any of the allowed states and observables to any in qubit stabilizer quantum mechanics. The whole Clifford group can be achieved by first

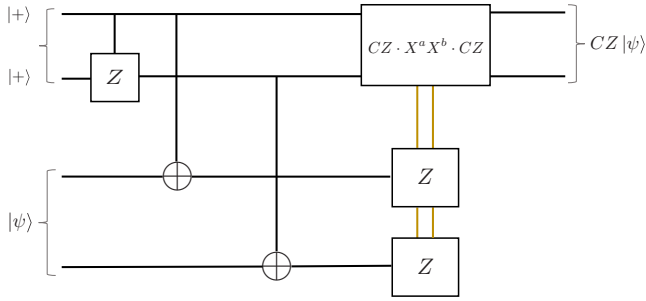


FIG. 4. CZ injection. The first injection of our scheme is the injection of the $CZ|++\rangle$ state, needed to perform the correction in the injection scheme for the CCZ gate and to produce the Hadamard gate. In the figure above the correction is $(CZ)(X^a X^b)(CZ)$ conditioned on obtaining x, y outcomes from the Z measurements, where $(-1)^a = x$ and $(-1)^b = y$. For example, if the outcomes are $x = 1, y = -1$, the correction is $(CZ)(IX)(CZ) = XZ$, which is an allowed gate in our subtheory.

injecting the CZ gate, as shown in Fig. 4, that also provides a construction for the Hadamard gate (Fig. 5) and then the phase gate S . The correction gate for the state-injection scheme of the S gate is given by the Pauli Y gate, which is present, up to a global phase, in our Spekkens’ subtheory as a composition of X and Z Pauli rotations. Notice that, even if state injection, as defined in Sec. II C, allows us to only inject diagonal unitary gates, we can obtain all the nondiagonal gates because we have a full generating set of gates for Clifford unitaries (via the Hadamard gate). The other peculiarity of the Spekkens’ subtheory we are considering is that it is minimal, as we cannot remove any object from it without denying the possibility of achieving universal quantum computation. It contains only the elements needed for the state-injection scheme as defined in Sec. II C. The other schemes that are not minimal, like in Refs. [14,15], have more components than strictly needed for the state-injection scheme defined in Sec. II C. To see that this scheme is minimal, note that if one were to remove the $X(\mathbf{q})$ observables, it would not be possible to obtain the Hadamard gate. Moreover, Spekkens’ subtheories where the observables are tensors of a single Pauli operator and gates that preserve the eigenbasis of that operator, do not allow any state-injection scheme to inject objects outside of them.

The above theorem guarantees that a state-injection scheme can always be recast in the following structure: *Spekkens’ subtheory* + *Magic states* \rightarrow *UQC*.

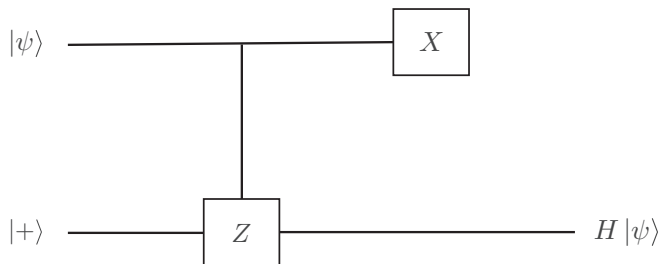


FIG. 5. Hadamard gate via CZ. The Hadamard gate can be obtained once the CZ gate is available. Obtaining H from CZ and X measurements was originally shown in Ref. [31].

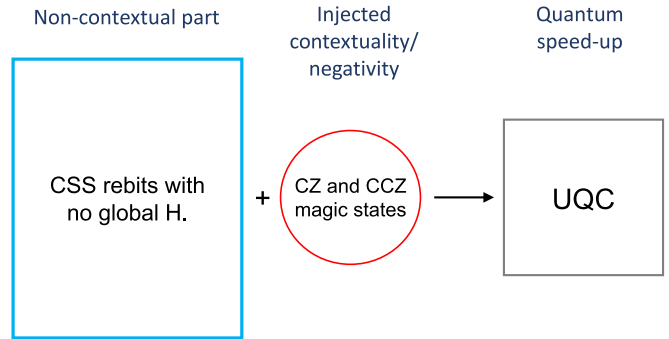


FIG. 6. State-injection scheme based on CCZ injection. By injecting first the CZ state and then the CCZ state we can boost the subtheory of rebit stabilizer quantum mechanics made of observables that are tensors of nonmixing Pauli I, X, Z , and the gates generated by CNOT and the Pauli rotations X, Z to universal quantum computation.

Spekkens’ model contains all the tools for state injection of the noncovariant Clifford gates that appear in qubit stabilizer quantum mechanics. Note that this approach looks at the minimal noncontextual subtheories of stabilizer quantum mechanics where we can still reach universal quantum computation via state injection. We see that each time these minimal subtheories are Spekkens’ subtheories. In the next section we describe how the minimal subtheory of rebit stabilizer quantum mechanics used in the proof of Theorem 1, Eqs. (14) and (18), can reach universal quantum computation through the injection of CCZ magic states.

VI. STATE-INJECTION SCHEMES WITH CCZ STATES

Reaching fault-tolerant universal quantum computation by exploiting Toffoli gates, or CCNOT—control control X , goes back to Peter Shor in 1997 [21]. It is known that the Toffoli gate (enough for universal classical computation) and Hadamard gate allow universal quantum computation [22,23], and, in a sense, this is the most natural universal set of gates, since the Toffoli enables all classical computations, and just by adding the Hadamard gate, which generates superposition, we achieve universal quantum computation. The same result holds if we use the related CCZ, control control Z , gate instead of the Toffoli gate. Other examples of fault-tolerant universal quantum computation involving Toffoli state distillation have been proposed [24–27]. We here propose a scheme of CCZ injection with the fewest possible objects in the free part of the computation. We reach that by also injecting the CZ state before the CCZ. The state-injection scheme is depicted in Fig. 6.

The free part is the one described in the proof of Theorem 1 and defined by Eqs. (14) and (18). This is the subtheory of CSS rebits with no global Hadamard, thus it is a Spekkens’ subtheory. The state-injection scheme uses two state injections: first, the state $CZ|++\rangle$ (Fig. 4), where the correction is given by the $(CZ)(X^a X^b)(CZ)$ conditioned on obtaining x, y outcomes from the measurements of Z ’s, where $(-1)^a = x$ and $(-1)^b = y$. Just to give an example, for outcomes $x = 1, y = -1$ the correction is $(CZ)(IX)(CZ) = XZ$. Second, the injection of the state

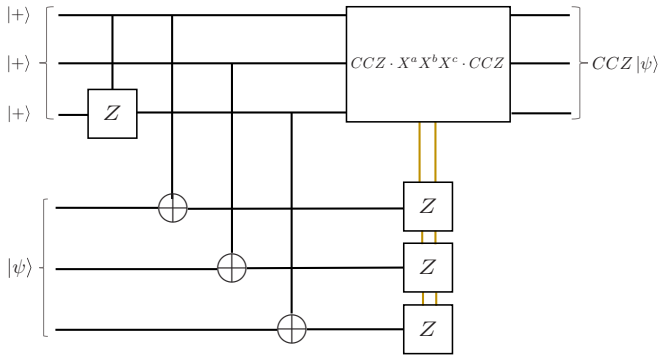


FIG. 7. CCZ injection. The second injection of our scheme is the injection of the $CCZ|+++ \rangle$ state. In the figure above the correction is $(CCZ)(X^a X^b X^c)(CCZ)$ conditioned on obtaining x, y, z outcomes from the Z measurements, where $(-1)^a = x, (-1)^b = y$ and $(-1)^c = z$. For example, if the outcomes are $x = -1, y = 1, z = 1$ the correction is $(CCZ)(XIII)(CCZ) = (X)(CZ)$, which is an allowed gate in our subtheory.

$CCZ|+++ \rangle$ (Fig. 7), where the correction is given by $(CCZ)(X^a X^b X^c)(CCZ)$, with outcomes x, y, z of the measurements of Z 's such that $(-1)^a = x, (-1)^b = y$, and $(-1)^c = z$, e.g., $(CCZ)(XIII)(CCZ) = (X)(CZ)$ if the outcomes are $-1, 1, 1$. Notice that the injection of the CZ also allows us to obtain the Hadamard gate, as shown in Fig. 5. With Hadamard and CCZ gates we then have a universal set for quantum computation. The contextuality, which is not present in the subtheory of CSS rebits, is clearly present after the two injections that lead to universal quantum computation.

A few comments on the free part of the scheme are needed. As already said, it is *minimal*, in the sense that it is not possible to remove any object from the free part of the computation without denying the possibility of obtaining universal quantum computation via state injection. Also it is a strict subtheory of the CSS rebit, where we allow all the same objects apart from the global Hadamard. We argue that this is desirable, since in principle the Hadamard gate is a local gate; we want to keep only the entangling gates to have a global nature.

VII. PROOFS OF CONTEXTUALITY AND STATE INJECTION

The Spekkens' subtheory used for the CCZ state-injection scheme of the previous section allows us to establish a relation between the different resources injected and different proofs of contextuality. It is well known that within qubit stabilizer quantum mechanics we can obtain the Peres-Mermin square argument, which is a proof of state-independent contextuality, and the GHZ paradox, which is a proof of state-dependent contextuality [6–8]. These proofs are not present within the Spekkens' subtheory, which, as we know, always witnesses the absence of any form of contextuality. We now explicitly show how the Peres-Mermin square and GHZ-paradox are obtained after the injection of either the CZ gate or the S gate. We also show that injection of the important non-Clifford $\frac{\pi}{8}$ gate T , in addition to the Peres-Mermin square and GHZ paradox (provided that we can apply the T gate at least two

times, as $T^2 = S$), enables maximum violation of the CHSH inequality. These examples demonstrate that specific states injected to the minimal Spekkens' subtheory here considered, even if they do not provide universality, can be considered resources for specific and distinct manifestations of contextuality.

(1) *Peres-Mermin square.* Let us consider the free Spekkens' subtheory of the CCZ injection scheme supplemented with the injection of the CZ state. This allows us to construct a circuit to perform the Peres-Mermin square argument [7]. Let us first recall that the Peres-Mermin square (shown below) is one of the most intuitive and popular ways to illustrate the notion of Kochen-Specker contextuality.

$X \otimes I$	$I \otimes X$	$X \otimes X$
$I \otimes Z$	$Z \otimes I$	$Z \otimes Z$
$X \otimes Z$	$Z \otimes X$	$Y \otimes Y$

The square is composed of nine Pauli observables on a two-qubit system.⁴ Each row and each column is composed by commuting (simultaneously measurable) observables. With the assumption that the functional relation between commuting observables is preserved in terms of their outcomes (e.g., if an observable C is the product of two observables A, B , also its outcome c is the product of the the outcomes a, b of A, B) and the outcome of each observable does not depend on which other commuting observables are performed with it (noncontextuality), the square shows that it is impossible to assign the outcome of each observable among all the rows and columns without falling into contradiction. For example, if we start by assigning values, say ± 1 , to the observables starting from the first (top left) row on, the contradiction can be easily seen when we arrive at the last column and last row (red circles), that bring different results to the same observable YY , as witnessed by the following simple calculation, $(XZ)(ZX) = YY$, and $(XX)(ZZ) = -(YY)$. Kochen-Specker contextuality refers to the fact that the outcome of a measurement does depend on the other compatible measurements that we perform with it (i.e., on the contexts).

While in our original Spekkens' subtheory we are only allowed to perform the observables in the first two rows of the square, with the presence of the CZ we can obtain the last row too, since $(CZ)(XI)(CZ) = XZ, (CZ)(IX)(CZ) = ZX$ and $(CZ)(XX)(CZ) = YY$. Figure 8 shows a circuit where we can perform all the contexts of the Peres-Mermin square on an arbitrary input state $|\psi \rangle$ by just using objects belonging to the Spekkens' subtheory and CZ injections.

We can obtain the Peres-Mermin square argument also via the injection of the S gate. This time the observables considered in the square are $IX, XII, XX, YI, IY, IY, YX, XY, ZZ$. The ones containing Y can be obtained by applying S to the

⁴Notice that we will not write again the “ \otimes ” symbol for the tensor product to soften the notation.

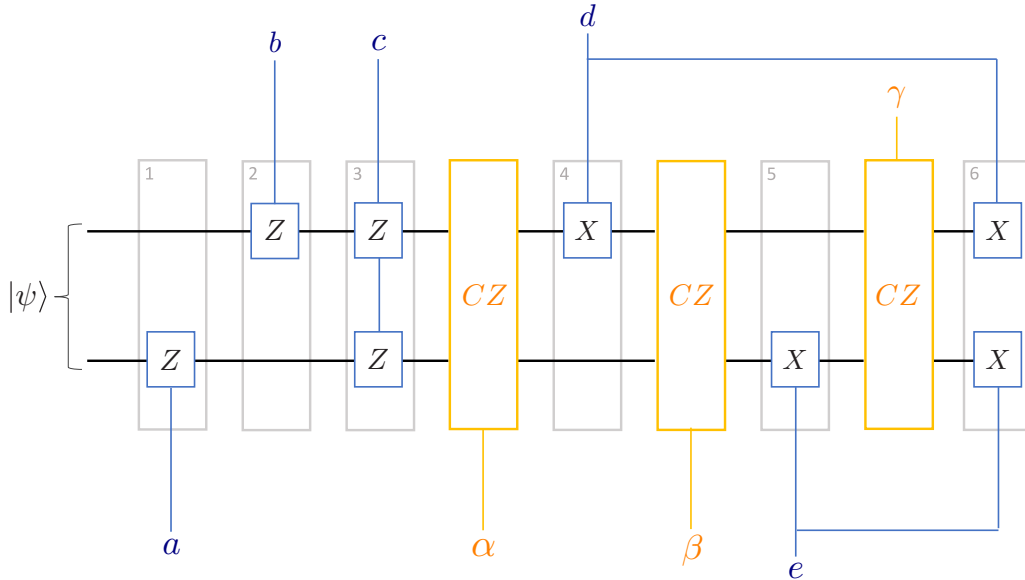


FIG. 8. Peres-Mermin square via Spekkens' subtheories and CZ gates. The above circuit provides a way of implementing all the contexts of the Peres-Mermin square. Each block denoted by CZ corresponds to the injection scheme of Fig. 4 endowed also with a swap gate (which is present in our Spekkens' subtheory as it can be made of a series of three alternated CNOT gates) to set the output state $CZ|\psi\rangle$ as a precise modification of the input state $|\psi\rangle$ (and not of the ancillary resource state $CZ|++\rangle$). Each context can be selected according to some combinations of the classical control bits $a, b, c, d, e, \alpha, \beta, \gamma$ that can take values in $\{0, 1\}$. The value 0 indicates that the corresponding gate is not performed, while the value 1 that it is performed. At the end of every gray block (labeled by numbers) we assume that we can read the output outcome. The three row contexts of the Peres Mermin square are identified by the variables (d, e) , (a, b, c) and $(\alpha, \beta, \gamma, d, e)$ assuming value one, respectively. The three column contexts are identified by (a, d, γ) (b, e, γ) and (c, d, e, γ) . Notice that in the last case where we implement the context XX, ZZ, YY , the measurement of XX is implemented by performing $\mathbb{I}X$ first and then $X\mathbb{I}$, and in this case we consider the outputs related to the blocks labeled by 3,5,6.

X observable, while the others are already present in our Spekkens' subtheory.

(2) *GHZ paradox* [6]. To obtain the GHZ paradox we need to be able to create the GHZ state $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$, already present in our Spekkens' subtheory, and measure the mutually commuting observables XXX, XYY, YXY, YYX . The GHZ state is the common eigenstate of these four operators, with the eigenvalues being $+1, -1, -1, -1$, respectively. While the first observable XXX is already present in our Spekkens' subtheory, the others can be obtained either by local S gate or CZ gate on two of the three single Pauli operators composing each observable. By considering these observables, the quantum predictions are in conflict with any noncontextual hidden variable model that assigns definite pre-existing values, $+1$ and -1 , to the local Pauli observables X, Y . Let us denote these definite values as $\lambda_{x1}, \lambda_{x2}, \lambda_{x3}, \lambda_{y1}, \lambda_{y2}, \lambda_{y3}$ in correspondence of each local Pauli X and Y . The product of the three observables XYY, YXY, YYX , that must yield the outcome -1 , in the hidden variable model means the following expression $\lambda_{x1}\lambda_{x2}\lambda_{x3}\lambda_{y1}^2\lambda_{y2}^2\lambda_{y3}^2 = -1$. However, this is in neat contradiction with the outcome of XXX , which is $+1$, and corresponds to $\lambda_{x1}\lambda_{x2}\lambda_{x3} = +1$.

(3) *CHSH argument* [28]. If we consider our Spekkens' subtheory with the addition of the T gate we can obtain the maximum violation of the CHSH inequality. In the CHSH game a referee asks questions $x, y \in \{0, 1\}$ to Alice and Bob, respectively, who agree on a strategy beforehand to then answer $a, b \in \{0, 1\}$, respectively. They win the game if $xy = a \oplus b$, where the sum is meant to be modulo 2. The

best classical strategy for them consists of always answering $a = b = 0$, which means winning the game with a probability of 75%. By exploiting quantum states and measurements they can do better than that. It results that if they share the Bell state $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$, which is a -1 eigenstate of XX and $+1$ eigenstate of ZZ , and they perform the appropriate observables A_q, B_q (depending on which question $q, 0$ or 1 , the referee asks them) they can win the game with the maximum quantum probability of about 85%. Notice that the Bell state that we consider is present in our Spekkens' subtheory. The observables, which are provided by the presence of the T gate, are $A_0 = Y, A_1 = X, B_0 = TYT^\dagger = \frac{Y-X}{\sqrt{2}}, B_1 = TXT^\dagger = \frac{X+Y}{\sqrt{2}}$. The probability that Alice and Bob win minus the probability that they lose is $\frac{1}{4}(\langle A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \rangle) = \frac{1}{\sqrt{2}}$, as $\langle A_0B_0 \rangle = \langle A_0B_1 \rangle = \langle A_1B_0 \rangle = -\langle A_1B_1 \rangle = \frac{1}{\sqrt{2}}$. Therefore, the probability of winning is $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$.

VIII. CONCLUSIONS

In this work we studied the subtheories of Spekkens' toy theory that are compatible with quantum mechanics, in the sense of making the same operational prediction. We identified these as the closed subtheories within Spekkens' toy theory that have nonnegative and covariant Wigner function representations. Stabilizer quantum mechanics is the maximal Spekkens' subtheory in odd dimensions, as it corresponds to the full Spekkens' theory. This is not true for qubits, as stabilizer quantum mechanics is contextual

and the toy theory does not reproduce its statistics. We used Spekkens' subtheories as a framework to describe the known examples of state-injection schemes for quantum computation on qudits of odd prime dimensions [14] and rebits [15] with contextuality as an injected resource, in the sense that they fit into the scheme of Fig. 1, i.e., *Spekkens' subtheory* + *Magic states* \rightarrow *UQC*, where Spekkens' subtheories embody the noncontextual part of the computational model and the contextuality arises in the injection of the magic states. Furthermore, we showed that Spekkens' subtheories plus state injection allow us to achieve all state-injection schemes where free operations are from the Clifford group (the standard state-injection schemes studied in the fault-tolerance literature). Theorem 1 proves that all of qubit stabilizer quantum mechanics can be obtained from a Spekkens' subtheory via state injection, and thus other state-injection schemes of quantum computation with Clifford group gates as the free operations can be mapped to our framework via a sequence of injections. To prove Theorem 1 we constructed a Spekkens' subtheory which is a strict subtheory of the CSS rebit theory (used in Ref. [15]) and provided a state-injection scheme to reach universal quantum computation by injections of CZ and CCZ states. This subtheory is minimal, meaning that it is not possible to remove any object from it without denying the possibility of reaching universal quantum computation via state injection. By analyzing the different injection processes in the above scheme we also associated different proofs of contextuality to specific state injections of noncovariant gates. In particular we explicitly showed how the CZ and *S* gates are resources for the Peres-Mermin proof of contextuality and the GHZ paradox, and how the *T* gate, used in the most popular state-injection schemes [13], is a resource for maximal violations of the CHSH inequality.

With respect to previous related works, we often referred to Raussendorf *et al.*'s framework [18], since this is very general and includes, for example, also the subtheory of qubit stabilizer quantum mechanics that arises from the 8-state model of Wallman and Bartlett [19]. Raussendorf *et al.*'s framework differs from ours in that it does require tomographic completeness and it does not demand covariant Wigner functions. In our framework, we preferred to use the tools provided by Spekkens' toy theory, which has a less abstract structure, being an intuitive and fully noncontextual hidden variable model. The state-injection schemes we considered are the ones developed in Ref. [12], which means that we are not considering more general ways to use states as a resource such as the cluster state computation, considered in Ref. [18]. An open question is how to extend Theorem 1 to these more general schemes. A suggestion in this direction comes from the example of cluster state computation provided in Refs. [17] and [18]. It consists of a noncontextual free subtheory made of tensors of *X*, *Y*, *Z* Pauli observables, their product eigenstates and all the local Clifford gates, and the resource is a specific entangled cluster state. The free subtheory

in this case is not a Spekkens' subtheory, as the *S* and *H* gates are not covariant if we allow all the product eigenstates of tensors of *X*, *Y*, *Z* Pauli observables. However, if we remove these local gates we can still implement the computational scheme (which never needs to use those gates) and obtain universal quantum computation with the same resource state. In the latter case the free part is now a Spekkens' subtheory. Therefore, this example can be actually recast in our framework of *Spekkens' subtheory* + *Magic state* \rightarrow *UQC*. Finally we point out that all previous works [17–19] look at the biggest noncontextual subtheories of stabilizer quantum mechanics that have state-injection schemes with contextuality as a resource. Here, instead we focus also on the smallest free subtheories from which it is still possible to reach universal quantum computation via state injection.

We believe that the results presented here suggest some future projects. The central role of covariance in our work suggests that its relationship with noncontextuality deserves further study. A recent work on contextuality in the cohomological framework could provide the right tools to address this question [32]. In particular, covariance seems to be strictly related to Spekkens' transformation noncontextuality [33]. As an example of this, the single qubit stabilizer quantum mechanics, already argued to be not covariant, shows transformation contextuality (even if a preparation and measurement noncontextual model for it—e.g., the 8-state model—exists) [34]. One significant question that remains open is to clarify which notion of contextuality is the best one to capture resources for universal quantum computation as, for example, it is known that qubit stabilizer quantum mechanics, despite being contextual, is efficiently classically simulatable [35]. It would be desirable to match the notion of nonclassicality in quantum foundations, namely contextuality, with the notion of nonclassicality in quantum computation, e.g., nonefficient classical simulatability. Finally we think that it would be interesting to extend Spekkens' toy theory to obtain a ψ -epistemic ontological model [36] of *n*-qubit stabilizer quantum mechanics. Possibly some extensions of the 8-state model can achieve this. If so, the epistemic restrictions on which such models were built might be of independent interest. Such work would contribute to further understanding the subtle relationship between contextuality and the computational power of universal quantum computation.

ACKNOWLEDGMENTS

We thank Robert Raussendorf, Juan Bermejo-Vega, Piers Lillystone, Hammam Qassim, Nicolas Delfosse, Cihan Okay, Joel Wallman, and Robert Spekkens for helpful discussions. We also thank Nadish De Silva for useful considerations at the first stage of the project. This work was supported by EPSRC Centre for Doctoral Training in Delivering Quantum Technologies (Grant No. EP/L015242/1).

[1] R. W. Spekkens, Evidence for the epistemic view of quantum states: A toy theory, *Phys. Rev. A* **75**, 032110 (2007).

[2] R. W. Spekkens, *Quasiquantization: Classical Statistical Theories with an Epistemic Restriction*, in *Fund. Theor. of Phys.* (Springer, Dordrecht, 2016), vol. 181.

- [3] L. Catani and D. E. Browne, Spekkens' toy model in all dimensions and its relationship with stabilizer quantum mechanics, *New J. Phys.* **19**, 073035 (2017).
- [4] D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. thesis (1997), [arXiv:quant-ph/9705052](https://arxiv.org/abs/quant-ph/9705052).
- [5] D. Gross, Hudson's theorem for finite-dimensional quantum systems, *J. Math. Phys.* **47**, 122107 (2006).
- [6] D. Greenberger, M. Horne, A. Shimony, and A. Zeilinger, Bell's theorem without inequalities, *Am. J. Phys.* **58**, 1131 (1990).
- [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] E. Wigner, On the quantum correction for thermodynamic equilibrium, *Phys. Rev.* **40**, 749 (1932).
- [10] W. K. Wootters, A Wigner-function formulation of finite-state quantum mechanics, *Ann. Phys.* **176**, 1 (1987).
- [11] C. Cormick, E. F. Galvão, D. Gottesman, J. P. Paz, and A. O. Pittenger, Classicality in discrete Wigner functions, *Phys. Rev. A* **73**, 012301 (2006).
- [12] X. Zhou, D. W. Leung, and I. L. Chuang, Methodology for quantum logic gate construction, *Phys. Rev. A* **62**, 052316 (2000).
- [13] S. Bravij and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, *Phys. Rev. A* **71**, 022316 (2005).
- [14] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Contextuality supplies the magic for quantum computation, *Nat.* **510**, 351 (2014).
- [15] N. Delfosse, P. A. Guerin, J. Bian, and R. Raussendorf, Wigner Function Negativity and Contextuality in Quantum Computation on Rebits, *Phys. Rev. X* **5**, 021003 (2015).
- [16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum Error Correction and Orthogonal Geometry, *Phys. Rev. Lett.* **78**, 405 (1997).
- [17] J. Bermejo-Vega, N. Delfosse, D. E. Browne, C. Okay, and R. Raussendorf, Contextuality as a Resource for Models of Quantum Computation with Qubits, *Phys. Rev. Lett.* **119**, 120505 (2017).
- [18] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega, Contextuality and Wigner function negativity in qubit quantum computation, *Phys. Rev. A* **95**, 052334 (2017).
- [19] J. J. Wallman and S. D. Bartlett, Non-negative subtheories and quasiprobability representations of qubits, *Phys. Rev. A* **85**, 062121 (2012).
- [20] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states, *Phys. Rev. A* **68**, 022312 (2003).
- [21] P. W. Shor, Fault-tolerant quantum computation, [arXiv:quant-ph/9605011](https://arxiv.org/abs/quant-ph/9605011).
- [22] D. Aharonov, A simple proof that Toffoli and Hadamard are quantum universal, [arXiv:quant-ph/0301040](https://arxiv.org/abs/quant-ph/0301040).
- [23] Y. Shi, Both Toffoli and Controlled-NOT need little help to do universal quantum computation, *Quant. Inf. Comput.* **3**, 84 (2003).
- [24] B. Eastin, Distilling one-qubit magic states into Toffoli states, *Phys. Rev. A* **87**, 032321 (2013).
- [25] C. Jones, Novel constructions for the fault-tolerant Toffoli gate, *Phys. Rev. A* **87**, 022328 (2013).
- [26] C. Jones, Composite Toffoli gate with two-round error detection, *Phys. Rev. A* **87**, 052334 (2013).
- [27] A. Paetznick and B. W. Reichardt, Universal Fault-Tolerant Quantum Computation with Only Transversal Gates and Error Correction, *Phys. Rev. Lett.* **111**, 090505 (2013).
- [28] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).
- [29] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasiprobability as a resource for quantum computation, *New J. Phys.* **14**, 113011 (2012).
- [30] R. W. Spekkens, Negativity and Contextuality are Equivalent Notions of Nonclassicality, *Phys. Rev. Lett.* **101**, 020401 (2008).
- [31] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, *Proc. Roy. Soc. A* 0301 (2010).
- [32] C. Okay, S. Roberts, S. D. Bartlett, and R. Raussendorf, Topological proofs of contextuality in quantum mechanics, *Quant. Inf. Comp.* **17**, 1135 (2017).
- [33] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, *Phys. Rev. A* **71**, 052108 (2005).
- [34] P. Lillystone, J. Wallman, and J. Emerson, Contextuality and the single-qubit stabilizer subtheory, [arXiv:1802.06121](https://arxiv.org/abs/1802.06121) (2018).
- [35] D. Gottesman, The Heisenberg representation of quantum computers, [arXiv:quant-ph/9807006](https://arxiv.org/abs/quant-ph/9807006).
- [36] N. Harrigan and R. W. Spekkens, Einstein, incompleteness, and the epistemic view of quantum states, *Found. Phys.* **40**, 125 (2010).