Cohomological framework for contextual quantum computations

Robert Raussendorf
Department of Physics and Astronomy, University of British Columbia, Vancouver, BC, Canada

(Dated: February 15, 2016)

We present a cohomological formulation of measurement-based quantum computation (MBQC), the central object of which is a phase function. The phase function describes symmetries of the resource state of the MBQC, specifies the computational output, and acts as a contextuality witness. It is also a topological object, namely a 1-cocycle in group cohomology. Non-triviality of the cocycles reveals the presence of contextuality, and is a precondition for quantum speedup.

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

An important question in the theory of quantum computation is which key quantum property is responsible for the speedup. This question is often viewed through the lens of resource theories, and a goal of this approach is to show that a candidate quantum property is indispensable for universality or for the hardness of classical simulation. Entanglement [1] and contextuality [2]-[6] have in this way been established as necessary resources [7]-[9], [10]-[13], at least when quantified in specific ways (see [14],[15], however).

Here, we address the initial question from a different, algebraic angle. We ask: "Are there computational structures in Hilbert space, and what do they look like?" We require such structures to satisfy two criteria: (i) They must specify the function computed, and (ii) they must be quantum.

Scanning for examples, one appears in Anders and Browne's contextual measurement-based quantum computation (MBQC) [10] on a 3-qubit Greenberger-Horne-Zeilinger state. It is based on the state-dependent version of Mermin's star [3], which is contextual. Contextuality is an obstruction to describing quantum mechanics in a classical statistical fashion, similar to Bell non-locality [16]. Mermin's star is a genuinely quantum structure. It also computes, if only an OR-gate.

In addition to [10] and its numerous cousins, there exists a contextual MBQC with a real application and a super-polynomial (as far as is known) quantum speedup, namely the MBQC version of the deterministic variant [17] of the 'Discrete Log' quantum algorithm [18].

Next arise the questions of which key structural element is to be gleaned from Mermin's star, and, more generally, how individual examples such as the above fit into a common framework. Here, we provide answers to these questions, for the model of measurement-based quantum computation [19]. The key element in Mermin's star is its non-trivial cohomology (defined below; also see [4]). Further, there is a common framework for contextual quantum computations that has at its center the so-called phase function, a topological object known from crystallography in Fourier space [20]-[22].

The phase function enters MBQC through the description of a group of symmetry transformations on the resource state (See Fig. 1), but it has further computational and physical meaning for MBQC. Namely, it encodes the function computed, up to an additive constant, and it is a witness for contextuality and thus quantumness.

To establish a cohomological framework for MBQC, we combine two links, namely the link between cohomology and contextuality identified by Abramsky and coworkers [4], [23], and the link between contextuality and MBQC [10], [11]. To make those links match, the Čech cohomology used in [23] is replaced by group cohomology [24], and the model of MBQC is moderately generalized.

This paper is organized as follows. First we describe a generalization of MBQC where the possible inputs form a finite group G. Then we present the topological formulation of this generalization in terms of a phase function Φ, leading up to the classification of the equivalence classes of Φ by the first cohomology group of G.

Finally, we investigate the physical and computational manifestations of this classification. We find that non-trivial cohomology of $[\Phi]$ is (a) a precondition for the function computed in the G-MBQC to be non-trivial, and (b) a witness for contextuality in the quantum computation. Furthermore, (c) for any given G-MBQC, we identify a logical contextuality inequality whose maximal violation puts an upper bound on the cost of reproducing the computational output by classical means. Significant speedup thus requires large amounts of contexuality.

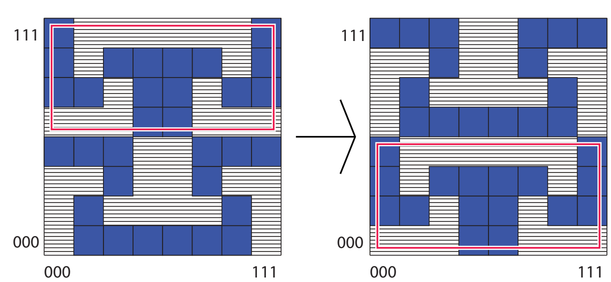

FIG. 1: Similarity transformation on the quasi-probability function $Q_{|GHZ\rangle}$ of a GHZ-state, cf. Eq. (5) [hatched: $Q(..) = -1/64$, solid: $Q(..) = 3/64$]. Q transforms covariantly under the input group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ of the MBQC [10], in such a way that the origin of phase space remains fixed. The effect of the $g \in G$ on $Q_{|GHZ\rangle}$ are translations; i.e., the symmetry transformations of $Q_{|GHZ\rangle}$ are analogous to glide planes.

Generalized notion of MBQC.—To the standard setting [19] of MBQC, we apply a generalization and a specialization. The specialization is to temporally flat MBQCs, i.e., all measurement bases are independent of all measurement outcomes. This is a substantial restriction which needs to be lifted in a subsequent more detailed treatment. We also confine to MBQCs with a single output bit, for notational simplicity.

The generalization concerns the set of possible inputs, which is typically a string of bits. Here we assume the inputs to form a finite group G, Abelian or non-Abelian. The motivation for this generalization is to pinpoint the underlying topological structure. We note that (i) standard MBQC remains a special case, with $G = {\mathbb{Z}_2}^m$, $m \in \mathbb{N}$, and (ii) some structure in the set of inputs is required, for otherwise an unreasonable amount of computational power could be packed into the mapping between inputs and measurement settings; See Appendix A.

We assume that the dimension d of the underlying Hilbert space $\mathcal{H}$ is finite, and that all measurable observables have eigenvalues ± 1 only (they need not be Pauli operators, however). We denote the set of these observables by $\mathcal{O}_+$. We also define the enlarged set $\Omega_+ := \mathcal{O}_+ \cup \{T(g),\, g \in G\} \cup \{I\}$, where the observables $T(g)$ are those for which the measured eigenvalues $(-1)^{o(g)}$ provide the computational outputs $o(g)$. The elements of Ω_+ are labeled by an index set $\mathcal{A}$, $\Omega_+ = \{T_a,\, a \in \mathcal{A}\}$. ($\mathcal{A}$ is the support of a characteristic function, see below.)

For the input value being the identity $e \in G$, the observables in a reference context $C(e)$, with $[T_a, T_{a'}] = 0$, $\forall T_a, T_{a'} \in C(e)$, are simultaneously measured on an MBQC resource state ρ. The corresponding measured eigenvalues $(-1)^{s(a)}$ are post-processed to infer the eigenvalue $(-1)^{o(e)}$ of the observable $T(e) = \prod_{a|\, T_a \in C(e)} T_a$. The outcome $o(e)$ of the MBQC given the input $e \in G$ is thus related to the measurement outcomes via $o(e) = \sum_{a|\, T_a \in C(e)} s(a) \mod 2$.

Regarding all input values, we require of G that it has a projective representation $u(G)$ acting on $\mathcal{H}$. Then, the measurement context for any input $g \in G$ is

$$C(g) = \{u(g) T_a u(g)^\dagger, T_a \in C(e)\}. \qquad (1)$$

The observables $T(g) := \prod_{a|\, T_a \in C(g)} T_a$, with measured eigenvalues $(-1)^{o(g)}$, represent the output of the computation. For all $g \in G$, the computational output $o(g)$ is related to the measurement outcomes via

$$o(g) = \sum_{a|T_a \in C(g)} s(a) \mod 2. \qquad (2)$$

This setting we call G-MBQC.

Above, Eq. (2) relating measurement outcomes to computational output is standard in MBQC [19], but Eq. (1) relating the input of the computation to the measurement settings represents a modification and extension of the original scheme. The latter remains a special case, with $G = {\mathbb{Z}_2}^m$, $m \in \mathbb{N}$; See Appendix B.

To summarize, G-MBQCs take as input an element g of a finite input group G, and are run in three steps. 1) Classical pre-processing. The input $g \in G$ is converted by the CC into the measurement context $C(g)$, cf. Eq. (1). 2) Quantum part. The observables $T_a \in C(g)$ are measured, yielding outcomes $s(a)$. 3) Classical post-processing. The output $o(g)$ is obtained from the measurement outcomes $\{s(a)\}$ via Eq. (2). Comparing with standard MBQC, the CC requires new capability, to accomplish above Step 1.

Let's apply the above definitions to the simplest contextual MBQC, the measurement-based OR-gate [10]. The point about the OR-gate is that it promotes the limited classical control computer in MBQC to classical universality. The resource state is a 3-qubit Greenberger-Horne-Zeilinger state $|\Psi\rangle$, with stabilizer relations $X_1X_2X_3|\Psi\rangle = -X_1Y_2Y_3|\Psi\rangle = -Y_1X_2Y_3|\Psi\rangle = -Y_1Y_2X_3|\Psi\rangle = |\Psi\rangle$, and measurement contexts $C_{00} = \{X_1, X_2, X_3\}$, $C_{01} = \{X_1, Y_2, Y_3\}$, $C_{10} = \{Y_1, X_2, Y_3\}$, $C_{11} = \{Y_1, Y_2, X_3\}$, for the inputs $(0,0), (0,1), (1,0), (1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, respectively. The input group for this MBQC is $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle g_{01}, g_{10}\rangle$, with a representation $\{u(g_{01}) = I_1 \otimes A_2 \otimes A_3,\ u(g_{10}) = A_1 \otimes I_2 \otimes A_3, ..\}$, where $A := (X+Y)/\sqrt{2}$. Thus, $AXA^\dagger = Y$ and $AYA^\dagger = X$, and Eq. (1) reproduces the above four contexts for the corresponding input values.

Back to the general discussion of G-MBQC, there exists a group of equivalence transformations changing the set Ω_+, namely

$$T_a \mapsto T'_a = (-1)^{\mathbf{v}(a)} T_a,\ \forall a \in \mathcal{A},\, \forall \mathbf{v} \in V, \qquad (3)$$

where the phases $\mathbf{v}(a) \in \mathbb{Z}_2$ are such that they preserve all product relations among commuting observables in Ω_+, and V is the maximal set of such transformations. If $\mathbf{u}, \mathbf{v} \in V$ then $\mathbf{u} + \mathbf{v} \in V$; hence $V = {\mathbb{Z}_2}^m$, $m \in \mathbb{N}$.

The motivation for considering these transformations is that basing a G-MBQC on a set Ω_+ of observables vs. a set $\Omega_\mathbf{v} := \{(-1)^{\mathbf{v}(a)} T_a,\, a \in \mathcal{A}\}$ does not change the cost or even the procedure of computation. The G-MBQCs based on the sets $\Omega_\mathbf{v}$, for all $\mathbf{v} \in V$, are therefore equivalent. The transformations induced by V amount to mere consistent relabelings of measurement outcomes, and we regard them as gauge transformations.

However, the transformations V change the computed function $o: G \longrightarrow \mathbb{Z}_2$, such that those functions form equivalence classes. In the previously mentioned GHZ-example [10], the equivalent functions are OR $\cong$ NOR $\cong$ NAND $\cong$ AND. They are all non-linear, and boost the classical control computer (CC), which by itself is capable only of evaluating linear functions, in the same way.

Finally, we impose a consistency condition on Ω_+. By construction, G maps $\mathcal{O}_+$ to itself and Ω_+ to itself under conjugation. The action of G on Ω_+ implies an action of G on $\mathcal{A}$. Namely, for all $a \in \mathcal{A}$ and all $g \in G$, ga is defined through $T_{ga} = u(g) T_a u(g)^\dagger$. Now, we require that, for all $a, b \in \mathcal{A}$,

$$\mathbf{v}(a) = \mathbf{v}(b),\ \forall \mathbf{v} \in V \Longrightarrow a = b. \qquad (4)$$

This implies in particular that if $T_a \in \Omega_+$ then $-T_a \notin \Omega_+$. More generally, for any $a \in \mathcal{A}$, $\chi(a) : V \longrightarrow \{\pm 1\}$ defined by $\mathbf{v} \mapsto \chi_\mathbf{v}(a) := (-1)^{\mathbf{v}(a)}$ is a linear character, $\chi_{\mathbf{u}+\mathbf{v}}(a) = \chi_\mathbf{u}(a)\chi_\mathbf{v}(a)$ for all $a \in \mathcal{A}$; i.e., $\chi(a) \in V^*$. If Eq. (4) holds then all observables $T_a \in \Omega_+$ are uniquely identifiable by the linear character $\chi(a)$ they induce. $\sum_{\mathbf{v}\in V} \overline{\chi}_\mathbf{v}(a)\chi_\mathbf{v}(b) = |V|\delta_{a,b}$ is then implied by character orthogonality. We will use this property shortly.

Formulation in phase space.—To reveal its topological features, we formulate G-MBQC in phase space, equipped with a quasi-probability function Q and a characteristic function Ξ.

The phase space is the module V defined in Eq. (3). The quasi-probability $Q : V \longrightarrow \mathbb{R}$ is defined as $Q_\rho(\mathbf{v}) := \mathrm{Tr}(A_\mathbf{v}\rho)$, with

$$A_\mathbf{v} = \frac{1}{|V|}\sum_{a\in\mathcal{A}} (-1)^{\mathbf{v}(a)} T_a. \tag{5}$$

The characteristic function Ξ is the Fourier transform of Q, $\Xi_\rho(a) := \sum_{\mathbf{v}\in V}(-1)^{\mathbf{v}(a)} W_\rho(\mathbf{v})$. By Eq. (4) and character orthogonality, it follows that

$$\Xi_\rho(a) = \langle T_a\rangle_\rho,\ \forall a \in \mathcal{A}. \tag{6}$$

The phase function Φ. In G-MBQC, the possible resource states ρ are constrained by similarity transformations induced by G. As already discussed, G acts on the set $\mathcal{A}$, and this implies an action on the phase space V, namely $(g(\mathbf{v}))(a) = \mathbf{v}(g^{-1}a)$, for all $a \in \mathcal{A}$; See Lemma 3 in Appendix C. Then, the resource states ρ are such that their quasi-probability functions Q_ρ satisfy $Q_{u^\dagger(g)\rho u(g)}(\mathbf{v}) \equiv Q_\rho(g(\mathbf{v})) = Q_\rho(\mathbf{v} + \mathbf{v}_g)$, $\forall g \in G$, $\forall \mathbf{v} \in V$. That is, the quasi-probability functions Q_ρ of resource states are invariant under combinations of rotations g and matching translations $\mathbf{v}_g$ of the underlying phase space V. Note that the equivalence holds for all states (covariance of Q, see Lemma 2 in Appendix C); the equality only holds for resource states ρ. This situation is analogous to the symmetries of matter density in a crystal. There, the analogue of G is the point group, and the corresponding symmetry transformations can be screw axes and glide planes.

This is illustrated in Fig. 1, for the 3-qubit MBQC [10]. The quasi-probability functions for the states $|GHZ\rangle$ and $g_{11}^\dagger|GHZ\rangle$ are shown, where $g_{11} = A_1A_2$. The resulting translation of $Q_{|GHZ\rangle}$ is by the vector (1,0,0) in the vertical direction, indicated by the rectangles.

In terms of the characteristic function Ξ_ρ, the above symmetry constraint on resource states ρ reads

$$\Xi_\rho(ga) = (-1)^{\Phi_g(a)}\,\Xi_\rho(a), \tag{7}$$

where $\Phi_g \in V$, for all $g \in G$. We have just introduced the phase function $\Phi : G \longrightarrow V$, the central object of the cohomological description of G-MBQC. As a remark, the characteristic function Ξ plays the same role for G-MBQC as the Fourier transform of the matter density plays for crystallography in Fourier space [21], [22].

The phase function Φ has two arguments, $g \in G$ and $a \in \mathcal{A}$, and it satisfies two constraints, linearity on $\mathcal{A}$ and group compatibility on G. First, consider $a, b, c \in \mathcal{A}$ such that $[T_a, T_b] = 0$ and $T_c = \pm T_aT_b$. Then, since $\Phi : G \longrightarrow V$, $\forall g \in G$,

$$\Phi_g(c) = \Phi_g(a) + \Phi_g(b) \mod 2. \tag{8}$$

The group compatibility condition [21] is enforced by associativity, and reads $\Xi_\rho((gh)a) \equiv \Xi_\rho(g(ha))$. With Eq. (7), $\forall g, h \in G$, $\forall a \in \mathcal{A}$, we thus have

$$\Phi_{gh}(a) = \Phi_h(a) + \Phi_g(ha) \mod 2. \tag{9}$$

This compatibility condition can be restated in topological terms. Namely, in group cohomology [24] a k-cochain is a map $\varphi^k : \mathcal{G}^k \longrightarrow M$, where $\mathcal{G}$ is a group and M is a module on which $\mathcal{G}$ acts. Since V is a module, the function $\Phi : G \longrightarrow V$ defined by $g \mapsto \Phi_g$, $\Phi_g : \mathcal{A} \longrightarrow \mathbb{Z}_2$, matches the definition of a 1-cochain. Φ has a coboundary $d\Phi : G \times G \longrightarrow V$, given by $(d\Phi)_{g,h}(a) := \Phi_g(ha) + \Phi_h(a) - \Phi_{gh}(a) \mod 2$. By comparison with Eq. (9), we find that the group compatibility condition has a topological interpretation,

$$d\Phi = 0. \tag{10}$$

The phase function Φ is thus a 1-cocycle, which may be trivial or non-trivial. The coboundary of a 0-cochain is

$$(dA)_g(a) = A(ga) - A(a) \mod 2,\ \forall g \in G, \forall a \in \mathcal{A}. \tag{11}$$

Now considering the equivalence transformations Eq. (3), with Eqs. (6) and (7), we find that

$$\Phi \cong \Phi + d\mathbf{v} \mod 2,\ \forall \mathbf{v} \in V. \tag{12}$$

The phase functions Φ are subject to the restriction Eq. (10) and the identification Eq. (12). For their equivalence classes $[\Phi]$ under the gauge transformations Eq. (3) it therefore holds that

$$[\Phi] \in H^1(G, V).$$

This is the topological characterization of G-MBQC. We now look at its physical and computational ramifications.

(a) Phase function and computation. Up to an additive constant, the phase function contains full information about the computational output, as we now explain. With Eq. (6), for any $a \in \mathcal{A}$, the probability $p_a(s)$ for obtaining the outcome s in the measurement of T_a is $p_a(s) = (1 + (-1)^s\Xi_\rho(a))/2$, and the probability $p_{ga}(s')$ for the outcome s' of T_{ga} is $p_{ga}(s') = (1 + (-1)^{s'}\Xi_\rho(ga))/2$. With the symmetry property Eq. (7) of the resource state ρ, $p_a(s) = p_{ga}(s')$ if the outcomes s and s' are related via $s = s' + \Phi_g(a)$, for all $g \in G$. Now, for any $g \in G$, we define the 'intended' outcome $o(g)$ as the likeliest outcome of the measurement of $T(g)$. With the preceding relation, first, the success probability of computation is uniform over G, and furthermore

$$o(g) = \Phi_g(b_e) + \text{const.} \mod 2, \tag{13}$$

where const. $= o(e)$, and b_e is such that $T_{b_e} = T(e)$. Thus, up to an additive constant, the phase function Φ contains all information about the output function $o : G \longrightarrow \mathbb{Z}_2$ computed in the MBQC.

Furthermore, there exists a connection between cohomological triviality of Φ and computational triviality of the output function o specified by Φ through Eq. (13).

Proposition 1 *Assume that the classical control computer (CC) of G-MBQC has access to a memory of size $|\mathcal{O}_+|$, with binary-valued cells addressable by a, $T_a \in \mathcal{O}_+$. Then, the CC is capable of computing any function o specified through Eq. (13) by a trivial phase function $\Phi = dA$, without any access to quantum resources.*

Remark: If the CC has access to a memory of size $|\Omega_+|$, then it can compute *any* function o without quantum resources. However, Proposition 1 has grip because, typically, $|\mathcal{O}_+| \ll |\Omega_+|$. For example, in standard MBQC, $|\Omega_+ \backslash \mathcal{O}_+| = 2^m$ and $|\mathcal{O}_+| = 2n$, where m is the number of input bits and n the number of qubits in the cluster state. For efficient such computations, $n = \text{Poly}(m)$.

Proof of Proposition 1. With Eq. (13), the computed function is $o(g) = (dA)_g(b_e) + \text{const.}$ Then, with Eqs. (8), (11), $(dA)_g(b_e) = \sum_{a|T_a \in C(e)} (dA)_g(a)$ mod 2 $= \sum_{a|\,T_a \in C(e)} A(ga) - A(a)$ mod 2. To evaluate the $o(g)$, as a pre-computation, load the memory with the values $A(a)$, for all a with $T_a \in \mathcal{O}_+$. Then, at runtime, 1. Call from memory all values $A(a_i)$, with $T_{a_i} \in C(e)$, and add them $\rightarrow v_1$, 2. Compute $a_i' = ga_i$, for all $T_{a_i} \in C(e)$, 3. Call all $A(a_i')$ and add them $\rightarrow v_2$, 4. Add $v_1 + v_2 + \text{const.}$ mod 2 $=: v$, and output v. All required operations are accessible to the CC. □

(b) Phase function and contextuality. By Eq. (13), Φ, when supplemented with a constant, satisfies criterion (i) imposed on computational structures in Hilbert space. But in which sense is it quantum?

Proposition 2 *Consider a G-MBQC $\mathcal{M}$ computing a function $o : G \longrightarrow \mathbb{Z}_2$. If for all phase functions Φ satisfying the output relation Eq. (13) it holds that $[\Phi] \neq 0 \in H^1(G, V)$, then $\mathcal{M}$ is strongly contextual.*

The proof of Proposition 2 is given in Appendix D 1. Prop. 2 provides symmetry-based proofs of contextuality; also see [25]. Namely, in many instances it can be shown that (i) linearity Eq. (8) of Φ, (ii) the output relation Eq. (13), and (iii) $\Phi = dA$ are incompatible. With Prop. 2 contextuality then follows.

This is best illustrated with the example of the measurement-based OR-gate [10] discussed earlier. Recall that the resource state in this MBQC is a 3-qubit GHZ state $|\Psi\rangle$, with stabilizer relations $X_1X_2X_3|\Psi\rangle = -X_1Y_2Y_3|\Psi\rangle = -Y_1X_2Y_3|\Psi\rangle = -Y_1Y_2X_3|\Psi\rangle = |\Psi\rangle$. We consider the input group element $g = g_{11}$ which acts on $\mathcal{O}_+$ as $X_1 \leftrightarrow Y_1$, $X_2 \leftrightarrow Y_3$, $X_3 \circlearrowleft$, $Y_3 \circlearrowleft$. Further, be $a(X_1)$ such that $T_{a(X_1)} = X_1$, etc. With the above eigenvalue equations we then have

$$\Phi_g(a_{XXX}) = 1,\ \Phi_g(a_{YXY}) = 0. \tag{14}$$

By linearity Eq. (8) of Φ_g on commuting observables,

$$\begin{aligned} \Phi_g(a_{XXX}) &= \Phi_g(a_{X_1}) + \Phi_g(a_{X_2}) + \Phi_g(a_{X_3}), \\ \Phi_g(a_{YXY}) &= \Phi_g(a_{Y_1}) + \Phi_g(a_{X_2}) + \Phi_g(a_{Y_3}), \end{aligned} \tag{15}$$

where addition is mod 2. Combining Eqs. (14) and (15), $1 = \Phi_g(a_{X_1}) + \Phi_g(a_{X_3}) + \Phi_g(a_{Y_1}) + \Phi_g(a_{Y_3})$. Now assume that $\Phi = dA$, for some $A \in V$. The previous equation then specializes to

$$\begin{aligned} 1 &= (A(a_{X_1}) - A(a_{Y_1})) + (A(a_{X_3}) - A(a_{Y_3})) + \\ &\quad + (A(a_{Y_1}) - A(a_{X_1})) + (A(a_{Y_3}) - A(a_{X_3}))\ \text{mod } 2 \\ &= 0. \end{aligned}$$

Contradiction. Hence $\Phi \neq dA$ for any A. With Proposition 2, the above MBQC is strongly contextual. □

Note that $1 = \Phi_g(a_{XXX}) \oplus \Phi_g(a_{YXY}) = s(a_{XXX}) \oplus s(a_{YYX}) \oplus s(a_{YXY}) \oplus s(a_{XYY})$. Thus, the obstruction to non-contextuality is the non-linearity of the function computed.

Further note that there is a close relation between the present symmetry based and Mermin's parity based contextuality proofs [3]; See Appendix D.

(c) Contextuality and speedup. In view of the contextual 3-qubit MBQC [10] executing an OR-gate, one may ask "What is contextual about an OR-gate?". A first answer to this question would be that, of course, there is nothing contextual about an OR-gate per se, only one of its physical realizations—the MBQC—is contextual.

But we can say more. There is a non-contextuality inequality whose strength of violation in G-MBQC puts an upper bound on the computational cost of classical function evaluation. Therefore, a significant violation of this inequality is required for quantum speedup.

The quantity $\Delta(o)_\rho := \sum_{g \in G} (1 + (-1)^{o(g)} \langle T(g) \rangle_\rho)/2$ is a contextuality witnesses. The maximum value allowed by quantum mechanics, $\Delta(o)_{\rho,\max} = |G|$, is reached for deterministic G-MBQCs. Be $s : \mathcal{A} \longrightarrow \mathbb{Z}_2$ an internally consistent, non-contextual value assignment, and $\mathcal{S}$ the set of all such assignments. Any s induces a function o_s via $o_s(g) = s(gb)$, for all $g \in G$, where $b \in \mathcal{A}$ is such that $T_b = T(I)$. The value of $\Delta(o)$ for a ncHVM with deterministic value assignments is therefore bounded by

$$\Delta(o)_{HVM} \leq \max_{s \in \mathcal{S}} \big(|G| - \text{wt}(o \oplus o_s)\big), \tag{16}$$

where $\text{wt}(r)$ is the Hamming weight of a function $r : G \longrightarrow \mathbb{Z}_2$. This is a logical non-contextuality inequality [26]. If no consistent non-contextual value assignment reproducing the function o exists, then $\Delta(o)_{HVM} < |G|$.

Proposition 3 *The classical computational cost C_{class} of reducing the evaluation of a function $o : G \rightarrow \mathbb{Z}_2$ to the evaluation of a trivial function o_s, induced by a phase function $\Phi \equiv ds$ via Eq. (13), is bounded by the maximum violation of the logical non-contextuality inequality Eq. (16), $C_{class} \leq |G| - \Delta(o)_{HVM,max}$.*

Taken together with Prop. 1, this result establishes that a large amount of contextuality is necessary for quantum speedup. It is thus a contextuality counterpart to corresponding results [8],[9] for entanglement, and [27] for the negativity of Wigner functions.

Proof of Proposition 3. We establish the upper bound by explicit construction of an algorithm that matches it. Be s a consistent non-contextual value assignment, with $o_s(g) := s(gb_e)$ where b_e is such that $T_{b_e} = T(e)$, that maximizes the r.h.s. of Eq. (16). We assume the set $\tilde{G} := \{g \in G | o_s(g) \neq o(g)\}$ is given in table form. To classically evaluate the function o in question, for any input $g \in G$, check membership in $\tilde{G}$. If $g \in \tilde{G}$, output $o_s(g) \oplus 1$, otherwise output $o_s(g)$. This reduces the evaluation of the function o to the evaluation of o_s, and o_s is indeed of the form Eq. (13), with $\Phi \equiv ds$ and const. $= s(b_e)$. Since $|\tilde{G}| = |G| - \Delta(o)_{HVM,\max}$, the operational cost of sifting through the list $\tilde{G}$ (the memory cost of storing $\tilde{G}$) is bounded by (given by) $|G| - \Delta(o)_{HVM,\max}$. □

Conclusion.—We have described a cohomological framework for measurement-based quantum computation in which the classical inputs form a finite group G. The central object of this framework is the phase function, which constrains the allowed resource states by a symmetry condition, and also specifies the computational output. The possible phase functions group into equivalence classes which are labeled by the first cohomology group of G. We have described computational and physical ramifications of this topological classification. For any given G-MBQC, non-trivial cohomology of the phase function is a witness of quantumness in the form of contextuality, and a precondition for speedup.

The next step suggested by this work is to extend the cohomological framework to G-MBQCs with proper temporal order. Further, group cohomology has also reached the subject of MBQC in a different vein, namely through the description of 'computational phases of matter' [28]-[31] within the paradigm of symmetry-protected topological order. Is there a relation?

From a broad perspective, the search for a quintessential quantum property at the root of the quantum speedup and the search for efficient quantum algorithms are two sides of the same coin. In view of this, the present work raises the following question: "Is there a quantum computational paradigm that relates to contextuality in the same way as 'quantum parallelism' [32] relates to superposition and interference?" In this work we have provided an algebraic framework within which any emerging contender may be examined and utilized.

Acknowledgments. The author thanks Dan Browne and Cihan Okay for discussions. This work has been funded by NSERC and Cifar.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[2] S. Kochen and E.P. Specker, J. Math. Mech. **17**, 59 (1967).
[3] N. D. Mermin, Rev. Mod. Phys. **65**, 803 (1993).
[4] S. Abramsky, A. Brandenburger, New J. Phys. **13**, 113036 (2011).
[5] A. Cabello, S. Severini, A. Winter, Phys. Rev. Lett. **112**, 040401 (2014).
[6] A. Acín, T. Fritz, A. Leverrier, A. Belén Sainz, arXiv:1212.4084.
[7] R. Jozsa and N. Linden, Proc. Roy. Soc. **459**, 2011 (2003).
[8] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[9] M. Van den Nest, W. Dür, G. Vidal, H. J. Briegel, Phys. Rev. A **75**, 012337 (2007).
[10] J. Anders and D.E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).
[11] R. Raussendorf, Phys. Rev. A **88**, 022322 (2013).
[12] M. Howard, J.J. Wallman, V. Veitch, J. Emerson, Nature (London) **510**, 351 (2014).
[13] N. Delfosse, P. Allard Guerin, J. Bian, R. Raussendorf, Phys. Rev. X **5**, 021003 (2015).
[14] D. Gross, S. T. Flammia and J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).
[15] M. Van den Nest, Phys. Rev. Lett. **110**, 060504 (2013).
[16] J.S. Bell, Rev. Mod. Phys. **38**, 447 (1966).
[17] M. Mosca and C. Zalka, arXiv:quant-ph/0301093.
[18] P. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM (IEEE Press, New York, 1994), p. 124.
[19] R. Raussendorf and H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[20] A. Bienenstock and E.P. Ewald, Acta Crystallogr. **15**, 1253 (1962).
[21] N.D. Mermin, Rev. Mod. Phys. **64**, 3 (1992).
[22] D.A. Rabson, J.F. Huesman, and B.N. Fisher, Found. Phys. **33**, 1769 (2003).
[23] S. Abramsky, Shane Mansfield and Rui Soares Barbosa, EPTCS **95**, 1 (2012).
[24] A. Adem and R.J. Milgram, *Cohomology of finite groups*, Springer, Berlin Heidelberg (1994).
[25] J. Lawrence, Phys. Rev. A **89**, 012105 (2014).
[26] L. Hardy, Phys. Lett. A **161**, 21 (1991).
[27] Hakop Pashayan, Joel J. Wallman, Stephen D. Bartlett, Phys. Rev. Lett. **115**, 070501 (2015).
[28] A. Miyake, Phys. Rev. Lett. **105**, 040501 (2010).
[29] D.V. Else, I. Schwarz, S.D. Bartlett, and A.C. Doherty, Phys. Rev. Lett. **108**, 240505 (2012).
[30] J. Miller and A. Miyake, Phys. Rev. Lett. **114**, 120506 (2015).
[31] A. Prakash and T.-C. Wei, Phys. Rev. A **92**, 022310 (2015).
[32] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, quant-ph/9708016 (1997).
[33] Joel J. Wallman, Stephen D. Bartlett, Phys. Rev. A **85**, 062121 (2012).

Appendix A: The need for structure in the input set

If we merely require that the set of input values forms a set with no additional structure, then there is plenty of flexibility in assigning measurement contexts to input values, and this proves to be problematic. Namely, a large amount of computational power can be packed into the relation between inputs and measurement contexts.

The sets $C(\mathbf{i})$ of measured observables are labeled by the input value $\mathbf{i}$. If $\tau : \mathbf{i} \mapsto C(\mathbf{i})$, for all input values $\mathbf{i} \in G$, is a valid assignment of computational inputs to the contexts, then so is $\tau_P : \mathbf{i} \mapsto C(P\mathbf{i})$, where P is an arbitrary permutation of the elements in G. Thus, if a given MBQC can realize a function $o : G \longrightarrow {\mathbb{Z}_2}^m$, with $m \in \mathbb{N}$, it can also realize the function $o_P = o \circ P$.

This is an unsatisfactory state of affairs, as the following example illustrates. Consider first an MBQC with one input and one output bit, $|\Psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $C(0) = \{X_1, X_2\}$, $C(1) = \{Y_1, Y_2\}$, and $o = s_1 \oplus s_2$. The computed function is the identity, $o(i) = i$. Now tensor this computation m times with itself, resulting in an MBQC that evaluates the identity function on m-bitstrings. Nothing is being computed so far. However, by the above freedom in assigning contexts to input values, we can also compute any invertible function P on $G = {\mathbb{Z}_2}^m$. Then we can also compute any Boolean function $o : {\mathbb{Z}_2}^{m-1} \longrightarrow \mathbb{Z}_2$, since for any such function $o(\mathbf{i})$, the m-bit function $\mathbf{y}(\mathbf{i}, j) := (\mathbf{i}, j \oplus o(\mathbf{i}))$ is invertible, and $\mathbf{y}(\mathbf{i}, 0) = (\mathbf{i}, o(\mathbf{i}))$.

Thus, complete freedom in assigning inputs to contexts gives the power of efficiently computing any Boolean function, which is unreasonable. In addition, note that the quantum part of this MBQC is near trivial. The above example illustrates that the freedom in assigning measurement contexts to input values must be constrained.

Appendix B: Standard MBQC is a special case

To demonstrate that standard MBQC [19] is contained in the generalized framework presented here, we have to show that the classical side-processing in standard MBQC is a special case of the classical side processing discussed here. First, the classical post-processing here and in standard MBQC are the same, cf. Eq. (2) and [19]. The difference arises in the preprocessing.

To begin, we note that in both standard MBQC and the present generalization the input specifies the measured observables. In the present setting, this proceeds by the action of an input group on a reference context of measurable observables, see Eq. (1). In the standard setting, no such group action is made explicit. But it is nonetheless there, as we now show.

In the standard setting [19] of MBQC, a measurement context is associated with a bit string $\mathbf{i} \in \mathbb{Z}_2^m$ as follows. For each qubit location k, $k = 1, .., n$, there is a flag $q_k \in \mathbb{Z}_2$ that decides which one of two possible observables,

$$O_k[q_k] = \cos\varphi\, X_k + (-1)^{q_k} \sin\varphi\, Y_k, \tag{B1}$$

is going to be measured. We may assemble the flags q_k in a vector $\mathbf{q} = (q_1, q_2, .., q_n)$. In this notation, for the special case of temporally flat MBQC considered here, the relation between the input $\mathbf{i}$ and the vector $\mathbf{q}$ specifying the measurement setting is linear,

$$\mathbf{q} = Q\mathbf{i} \mod 2,$$

with Q a binary-valued matrix. We now note that for the observables in Eq. (B1) it holds that

$$X_k O_k[0] X_k^\dagger = O_k[1] \;\text{ and }\; X_k O_k[1] X_k^\dagger = O_k[0].$$

There is thus a homomorphism g from $\{\mathbf{i}\} = \mathbb{Z}_2^m$ into the n-qubit Pauli group $\mathcal{P}_n$,

$$\mathbf{i} \mapsto g(\mathbf{i}) := \bigotimes_{l=1}^{n} (X_l)^{[Q\mathbf{i}]_l},$$

with the property that $O_k[q_k(\mathbf{i})] = g(\mathbf{i}) O_k[0] g(\mathbf{i})^\dagger$. The pre-processing in standard MBQC is thus a special case of the generalized setting discussed here. Namely, the input group is $G = \mathbb{Z}_2^m$ and has a unitary representation $u(G) = \{g(\mathbf{i}), \mathbf{i} \in \mathbb{Z}_2^m\}$. The reference context associated with the input $g = I$ is $\{O_k[0],\, k = 1, .., n\}$.

Another question that arises is whether the resource states of MBQC, typically cluster states or, more generally stabilizer states, naturally satisfy the symmetry constraint Eq. (7). This can only hold when the success probability is uniform over all inputs. As for the reverse direction, we have the following Lemma.

Lemma 1 *If the success probability of MBQC with an input group G is uniform over G and the resource state $|\Psi\rangle$ is a stabilizer state with no single qubit disentangled, then $|\Psi\rangle$ satisfies the invariance condition Eq. (7).*

Proof of Lemma 1. We subdivide the set $\mathcal{A}$ into three subsets, namely $\mathcal{A} = \{0\} \cup \mathcal{A}_\text{M} \cup \mathcal{A}_\text{out}$, where $0 \in \mathcal{A}$ is such that $T_0 = I$, $\mathcal{A}_M := \{a \in \mathcal{A} |\, T_a \in \mathcal{O}_+\}$ and $\mathcal{A}_\text{out} = \{a \in \mathcal{A} |\, \exists\, g \in G \text{ s.th. } T_a = T(g)\}$.

Case 1: $\{0\} \subset \mathcal{A}$. With $I = I \cdot I$ and linearity of $\mathbf{v}$, for all $\mathbf{v} \in V$, it holds that $\mathbf{v}(0) = \mathbf{v}(0) + \mathbf{v}(0) \mod 2 = 0$. Since $\Phi_g \in V$ by definition, $\Phi_g(0) = 0$ for all $g \in G$. Further, $\langle T_0 \rangle_\sigma = \langle I \rangle_\sigma = 1$ for all normalized quantum states σ. Eq. (7) is thus satisfied for $0 \in \mathcal{A}$, for all $g \in G$.

Case 2: $\mathcal{A}_\text{out} \subset \mathcal{A}$. Recall that $b_e \in \mathcal{A}_\text{out}$ is such that $T_{b_e} = T(e)$, with e the identity in G. Since for all $g \in G$, $o(g)$ is by definition the outcome with the larger probability, it holds that $(-1)^{o(g)} \langle T_{gb_e} \rangle_\rho \geq 0$. With the assumption of uniform success probability, it further holds that $(-1)^{o(g)} \langle T_{gb_e} \rangle \rho = (-1)^{o(e)} \langle T_{b_e} \rangle_\rho$, $\forall g \in G$. With Eq. (13), we thus find that

$$\langle T_{gb_e} \rangle \rho = (-1)^{\Phi_g(b_e)} \langle T_{b_e} \rangle_\rho,\; \forall g \in G, \tag{B2}$$

which is a special case of the desired relation in which $\mathcal{A}_{\text{out}} \ni a = b_e$. By construction of $\mathcal{A}_{\text{out}}$, for all $a \in \mathcal{A}_{\text{out}}$ there exists a $h \in G$ such that $a = hb_e$. Now, substituting $g \mapsto gh$ in Eq. (B2), we obtain

$$\begin{aligned}\langle T_{ga}\rangle_\rho &= (-1)^{\Phi_{gh}(b_e)}\langle T_{b_e}\rangle_\rho\\ &= (-1)^{\Phi_h(b_e)+\Phi_g(a)}\langle T_{b_e}\rangle_\rho\\ &= (-1)^{\Phi_g(a)}\langle T_a\rangle_\rho.\end{aligned}$$

Therein, we have used the group compatibility condition Eq. (9) in the second line, and Eq. (B2) in the third. With Eq. (6), Eq. (7) is thus satisfied for all $a \in \mathcal{A}_{\text{out}}$.

Case 3: $\mathcal{A}_M \subset \mathcal{A}$. In standard MBQC, all T_a with $a \in \mathcal{A}_M$ are local, and of form Eq. (B1). Since, by assumption, no qubit in the resource stabilizer state $|\Psi\rangle$ is disentangled from the rest, for every qubit $k = 1, .., n$ there is a stabilizer operator S of $|\Psi\rangle$ such that $S|_k = Z_k$, and hence $O_k[q]S = -SO_k[q]$, and $\langle\Psi|O_k[q]|\Psi\rangle = 0$, $\forall k$, $\forall q$. Thus, Eq. (7) holds trivially for all $a \in \mathcal{A}_M$. Hence it holds for all $a \in \mathcal{A}$. $\Box$

Appendix C: The quasi-probability functions Q

Here we discuss properties of the quasi-probability functions $Q_\rho(\mathbf{v}) = \text{Tr}A_\mathbf{v}\rho$, defined through the phase point operators $A_\mathbf{v} = 1/|V| \sum_{a\in\mathcal{A}}(-1)^{\mathbf{v}(a)}T_a$. We begin with an example, to explore how the present definition relates to quasi-probability functions described in the literature.

1. Q for one qubit

We construct the quasi-probability function Q for a single qubit, based on the set

$$\Omega_+ = \{I, X, Y, Z\}.$$

The first step is to construct the phase space V. Since, for consistency, the identity $+I$ always remains $+I$ under all transformations in V, and there are no pairs of commuting observables in $\Omega_+\backslash\{I\}$, hence no corresponding constraints, it holds that $V \cong {\mathbb{Z}_1}^3$. The eight phase point operators are thus

$$A_{\pm,\pm,\pm} = \frac{1}{8}(I \pm X \pm Y \pm Z).$$

This one-qubit quasi-probability distribution has been discussed in [33]. Note for comparison that the phase space for standard one-qubit Wigner functions has four points rather than eight.

2. Basic properties

Every quasi-probability functions Q is a linear mapping sending operators to functions on phase space V, as follows immediately from the definition. Also, probabilities for measurement outcomes of observables $T_a \in \Omega_+$ are given by the sums of $Q_\rho(\mathbf{v})$ over cosets in phase space.

Namely, the probability for obtaining the eigenvalue $(-1)^s$ in the measurement of an observable $T_a \in \Omega_+$ is $p_s(a) = (1 + (-1)^s \langle T_a\rangle)/2$. We may express $p_s(a)$ in terms of the quasi-probability function,

$$\begin{aligned}p_s(a) &= (1 + (-1)^s\langle T_a\rangle)/2 = (1 + (-1)^s\,\Xi_\rho(a))/2\\ &= \tfrac{1}{2}\textstyle\sum_{\mathbf{v}\in V}(1 + (-1)^s\,(-1)^{\mathbf{v}(a)})Q_\rho(\mathbf{v})\\ &= \textstyle\sum_{\mathbf{v}\in V}\delta_{s,\mathbf{v}(a)}Q_\rho(\mathbf{v})\end{aligned}$$

The set of $\mathbf{v} \in V$ for which $\mathbf{v}(a) = s$ is a coset of the subspace $V(a) = \{\mathbf{v} \in V|\ \mathbf{v}(a) = 0\}$, as claimed. In the second line above we have used the fact that $I \in \Omega_+$.

3. Covariance of Q under G

Definition 1 (Covariance) *A quasi-probability function Q is covariant under a group $\mathcal{G}$ of unitary transformations if, for all states σ, all phase space points $a \in V$, and all $h \in H$ it holds that*

$$Q_{u(h)^\dagger\sigma\, u(h)}(\boldsymbol{v}) = Q_\sigma(S_h\boldsymbol{v} + \boldsymbol{v}_h), \tag{C1}$$

with S_h a square invertible matrix and $\boldsymbol{v}_h \in V$.

We then have the following result.

Lemma 2 *The quasi-probability function Q is covariant under the input group G. Furthermore, the origin $\boldsymbol{0} \in V$ remains fixed under all $g \in G$, i.e.,*

$$Q_{u(g)^\dagger\sigma u(g)}(\boldsymbol{v}) = Q_\sigma(S_g\boldsymbol{v}),$$

for all $\boldsymbol{v} \in V$, for all $g \in G$, and all states σ.

We prove Lemma 2 by way of another Lemma. We have already defined the sets $\Omega_\mathbf{v} = \{(-1)^{\mathbf{v}(a)}T_a, a \in \mathcal{A}\}$, for all $\mathbf{v} \in V$. G is acting on all $T_a \in \Omega_+$ by conjugation, $T_a \mapsto u(g)T_a u(g)^\dagger = T_{ga}$, and this induces an action of G on the sets $\Omega_\mathbf{v}$. We define

$$g(\Omega_\mathbf{v}) := \{(-1)^{\mathbf{v}(a)}T_{ga}, a \in \mathcal{A}\},\ \forall \mathbf{v} \in V. \tag{C2}$$

We now show that this action of G permutes the sets $\Omega_\mathbf{v}$.

Lemma 3 *For all $g \in G$, $\forall\boldsymbol{v} \in V$, there exists a $g(\boldsymbol{v}) \in V$ such that*

$$g(\boldsymbol{v})(\cdot) = \boldsymbol{v} \circ g^{-1}(\cdot). \tag{C3}$$

Then, with Eq. (C2) and Lemma 3,

$$g(\Omega_\mathbf{v}) = \{(-1)^{\mathbf{v}(g^{-1}a)}T_a,\, a \in \mathcal{A}\} = \Omega_{g(\mathbf{v})}.$$

Thus, the sets $\Omega_\mathbf{v}$, $\mathbf{v} \in V$, are indeed permuted by the action of G, as claimed.

Proof of Lemma 3. For all triples $a, b, c \in \mathcal{A}$ with $[T_a, T_b] = 0$ and $T_c = (-1)^{\beta(a,b)}T_aT_b$ it holds by definition

Eq. (3) of V that $\mathbf{v}(c) = \mathbf{v}(a) + \mathbf{v}(b) \mod 2$, $\mathbf{v} \in V$. Hence,

$$(-1)^{\mathbf{v}(c)} T_c = (-1)^{\beta(a,b)+\mathbf{v}(a)+\mathbf{v}(b)} T_a T_b, \; \forall \mathbf{v} \in V. \quad \text{(C4)}$$

Conjugating Eq. (C4) by any $u(g)$, $g \in G$, we obtain, after relabeling the elements of $\mathcal{A}$,

$$(-1)^{\mathbf{v}(g^{-1}c)} T_c = (-1)^{\beta(g^{-1}a, g^{-1}b)+\mathbf{v}(g^{-1}a)+\mathbf{v}(g^{-1}b)} T_a T_b, \quad \text{(C5)}$$

for all $\mathbf{v} \in V$ and all $a, b, c \in \mathcal{A}$ with $[T_a, T_b] = 0$ and $T_c = (-1)^{\beta(a,b)} T_a T_b$. Setting $\mathbf{v} \equiv \mathbf{0}$ in Eq. (C5), it follows that, $\forall g \in G$,

$$\beta(a, b) = \beta(g^{-1}a, g^{-1}b), \; \forall a, b \in \mathcal{A}.$$

Therefore, $\forall g \in G$, $\forall \mathbf{v} \in V$ and all $a, b, c \in \mathcal{A}$ with $[T_a, T_b] = 0$ and $T_c \sim T_a T_b$ it holds that

$$\mathbf{v}(g^{-1}c) = \mathbf{v}(g^{-1}a) + \mathbf{v}(g^{-1}b) \mod 2.$$

Thus, $\mathbf{v} \circ g^{-1} \in V$, for all $\mathbf{v} \in V$ and all $g \in G$. $\Box$

Proof of Lemma 2. $Q_{u(g)^\dagger \rho u(g)}(\mathbf{v}) = \operatorname{Tr} u(g) A_\mathbf{v} u(g)^\dagger \rho$, and we are thus interested in how the phase point operators $A_\mathbf{v}$ transform under conjugation by $g \in G$.

$$\begin{aligned} u(g) A_\mathbf{v} u(g)^\dagger &= g \left(\tfrac{1}{|V|} \textstyle\sum_{a \in \mathcal{A}} \chi_\mathbf{v}(a) T_a \right) g^\dagger \\ &= \tfrac{1}{|V|} \textstyle\sum_{a \in \mathcal{A}} \chi_\mathbf{v}(a) T_{ga} \\ &= \tfrac{1}{|V|} \textstyle\sum_{a \in \mathcal{A}} \chi_\mathbf{v}(g^{-1}a) T_a \\ &= \tfrac{1}{|V|} \textstyle\sum_{a \in \mathcal{A}} \chi_{g(\mathbf{v})}(a) T_a \\ &= A_{g(\mathbf{v})}. \end{aligned}$$

Therein, the fourth line follows by Lemma 3. Thus, phase point operators are mapped to phase point operators by conjugation under any $g \in G$.

We now show that G acts linearly on V. For any $g \in G$, for all $a \in \mathcal{A}$ and all $g(\mathbf{u}), g(\mathbf{v}) \in V$,

$$\begin{aligned} \chi_{g(\mathbf{u})+g(\mathbf{v})}(a) &= \chi_{g(\mathbf{u})}(a) \chi_{g(\mathbf{v})}(a) \\ &= \chi_\mathbf{u}(g^{-1}a) \chi_\mathbf{v}(g^{-1}a) \\ &= \chi_{\mathbf{u}+\mathbf{v}}(g^{-1}a) \\ &= \chi_{g(\mathbf{u}+\mathbf{v})}(a). \end{aligned}$$

We may thus write $g(\mathbf{v}) = S_g \mathbf{v}$, for a square matrix S_g, for all $g \in G$ and all $\mathbf{v} \in V$. Since $g^{-1} \in G$, S_g must be invertible. Thus, Eq. (C1) holds, with the special offsets $\mathbf{v}_g = \mathbf{0}$, for all $g \in G$. $\Box$

Appendix D: More on contextuality

1. Proof of Proposition 2

The first step in the proof of Proposition 2 is the following lemma.

Lemma 4 *Be $s : \mathcal{A} \longrightarrow \mathbb{Z}_2$ a consistent non-contextual value assignment. Then, $s' : \mathcal{A} \longrightarrow \mathbb{Z}_2$ is a consistent non-contextual value assignment if and only if there exists a $\mathbf{v} \in V$ such that $s(a) - s'(a) \mod 2 = \mathbf{v}(a)$, $\forall a \in \mathcal{A}$.*

Proof of Lemma 4. "If": With $s(\cdot)$ being a consistent value assignment,

$$(-1)^{s(c)} T_c = (-1)^{s(a)} T_a (-1)^{s(c)} T_b,$$

for all $a, b, c \in \mathcal{A}$ with $[T_a, T_b] = 0$ and $T_c = \pm T_a T_b$. Then, by definition of V,

$$(-1)^{s(c)+\mathbf{v}(c)} T_c = (-1)^{s(a)+\mathbf{v}(a)} T_a (-1)^{s(c)+\mathbf{v}(a)} T_b,$$

for all $\mathbf{v} \in V$. Thus, $s' = s + \mathbf{v} \mod 2$ is a consistent value assignment for all $\mathbf{v} \in V$. In other words, if $s' - s \mod 2 \in V$ then s' is a consistent value assignment.

"Only if": Let $s(\cdot)$ and $s'(\cdot)$ be two consistent non-contextual value assignments. Then, the following two relations simultaneously hold for all $a, b, c \in \mathcal{A}$ with $[T_a, T_b] = 0$ and $T_c = \pm T_a T_b$.

$$\begin{aligned} (-1)^{s(c)} T_c &= (-1)^{s(a)} T_a (-1)^{s(c)} T_b, \\ (-1)^{s'(c)} T_c &= (-1)^{s'(a)} T_a (-1)^{s'(c)} T_b. \end{aligned}$$

Therefore, by multiplying the above equalities,

$$(s \oplus s')(c) = (s \oplus s')(a) \oplus (s \oplus s')(b),$$

for all $a, b, c \in \mathcal{A}$ such that $[T_a, T_b] = 0$ and $T_c = \pm T_a T_b$. Since, by definition, V is the module of all functions satisfying these relations, it follows that $s \oplus s' \in V$. $\Box$

For convenience, we restate Proposition 2.

Proposition *Consider a G-MBQC $\mathcal{M}$ computing a function $o : G \longrightarrow \mathbb{Z}_2$. If for all phase functions Φ satisfying the output relation Eq. (13) it holds that $[\Phi] \neq 0 \in H^1(G, V)$, then $\mathcal{M}$ is strongly contextual.*

Proof of Proposition 2. We establish that if $\mathcal{M}$ is not strongly contextual, i.e., if there exists a consistent value assignment $s : a \in \mathcal{A} \mapsto s(a) \in \mathbb{Z}_2$, then (i) $\Phi = ds$ is a valid phase function, and (ii) $\Phi = ds$ is compatible with Eq. (13). (i) We need to show that $ds : G \longrightarrow V$. Assume that $s(\cdot)$ is a consistent non-contextual value assignment. Then, $T_a(-1)^{s(a)} T_b (-1)^{s(b)} = T_c (-1)^{s(c)}$. Conjugating under any $g \in G$, it follows that $T_{ga}(-1)^{s(a)} T_{gb}(-1)^{s(b)} = T_{gc}(-1)^{s(c)}$. But it also holds that $T_{ga}(-1)^{s(ga)} T_{gb}(-1)^{s(gb)} = T_{gc}(-1)^{s(gc)}$. Therefore, $s(\cdot)$ and $s \circ g^{-1}(\cdot)$ simultaneously are consistent value assignments. By Lemma 4 they must differ by some $\mathbf{v} \in V$. That is, $\exists \mathbf{v} \in V$ such that $s(ga) - s(a) \mod 2 = \mathbf{v}(a)$, $\forall a \in \mathcal{A}$, $\forall g \in G$. By Eq. (11), $s(ga) - s(a) \mod 2 = (ds)_g(a)$. Hence, $(ds)_g \in V$ for all $g \in G$.

(ii) The outputted function given the consistent non-contextual value assignment s is $g \in G \mapsto o(g) = s(gb_e)$, where b_e is such that $T_{b_e} = T(e)$. On the other hand, Eq. (13) states that $o(g) = (ds)_g(b_e) + \text{const.} \mod 2 = s(gb_e) - s(b_e) + \text{const.} \mod 2$. The two expressions for $o : G \longrightarrow \mathbb{Z}_2$ agree for the choice const. $= s(b_e)$. $\Box$

2. The relation between symmetry-based and parity-based contextuality proofs

Our earlier state-dependent contextuality proof for the GHZ-scenario resembles Mermin's original proof [3] insofar as it leads the assumption of context-independent value assignments to an algebraic contradiction. However, the present proof, like [25], is based on a transformation of the observables, whereas Mermin's original proof is based on the observables themselves, without any transformation. Here we explain the relation between those two types of contextuality proofs.

The relation between the present symmetry-based contextuality proofs and the parity proofs of [3] is via the state-independent version of symmetry-based contextuality proofs, which we have not discussed yet. As we will see in Lemma 6 in Appendix D 3, pairs (Ω_+, G) in which G maps Ω_+ onto itself do not lead to state-independent symmetry-based contextuality proofs, and we therefore need to generalize the concept.

To this end, we introduce a symmetry group $\mathcal{G}$ larger than G, $G \subset \mathcal{G}$. It is based on a set of observables $\Omega := \{\pm T_a, T_a \in \Omega_+\}$. Specifically, $\mathcal{G}$ has a projective representation $u(\mathcal{G})$ that maps Ω onto itself under conjugation (but it does not necessarily map Ω_+ to itself). The transformation behaviour under $\mathcal{G}$ is

$$u(h)T_a u(h)^\dagger = (-1)^{\tilde{\Phi}_h(a)} T_{ha},\ \forall h \in \mathcal{G}, \forall a \in \mathcal{A} \qquad \text{(D1)}$$

where the generalized phase function is a map $\tilde{\Phi} : \mathcal{A} \longrightarrow \tilde{V} = \text{span}(\{\tilde{\Phi}_h, h \in \mathcal{G}\})$. Note that the space $\tilde{V}$ into which $\tilde{\Phi}$ maps is constructed in a very different manner from how V was constructed. As a consequence, the $\tilde{\Phi}_h \in \tilde{V}$ do not need to satisfy the linearity requirement Eq. (8) imposed on the original phase function Φ.

Transformation of value assignments s. In a hidden variable model describing the given physical situation, we require the value assignments $s : \mathcal{A} \longrightarrow \mathbb{Z}_2$ to transform under all $h \in \mathcal{G}$ in such a way as to match the transformation of the quantum-mechanical expectation values. With the transformation for observables, since the state ρ doesn't change (Heisenberg picture), the expectation values transform as $\langle T_a \rangle_\rho \mapsto \langle T'_a \rangle_\rho = (-1)^{\tilde{\Phi}_h(a)} \langle T_{ha} \rangle_\rho$. Hence, if a consistent value assignment s exists, it transforms under $h \in \mathcal{G}$ as

$$s(a) \mapsto s'(a) = s(ha) + \tilde{\Phi}(ha) \mod 2. \qquad \text{(D2)}$$

Transformation of constraints. We denote by $\mathcal{C}$ the set of all product constraints among sets of commuting observables in Ω. Be $R = \{\pm \prod_{i\in J} O_i = I\}$. Then, an action of $\mathcal{G}$ on $\mathcal{C}$ is defined via $h \circ R = \{\pm \prod_{i \in J} u(h) O_i u(h)^\dagger = I\}$, for all $h \in \mathcal{G}$. Since $u(h) \left(\prod_{i\in J} O_i\right) u(h)^\dagger = \prod_{i\in J} u(h) O_i u(h)^\dagger$, and $u(h) O_i u(h)^\dagger \in \Omega$ if $O_i \in \Omega$, it holds that $h \circ R \in \mathcal{C}$, for all $h \in \mathcal{G}$ and all $R \in \mathcal{C}$. That is,

$$\mathcal{G} : \mathcal{C} \longrightarrow \mathcal{C}.$$

This has the following consequence.

Lemma 5 *If $s : \mathcal{A} \longrightarrow \mathbb{Z}_2$ is a consistent value assignment, then so is $s' : \mathcal{A} \longrightarrow \mathbb{Z}_2$ as given by Eq. (D2), for every $h \in \mathcal{G}$.*

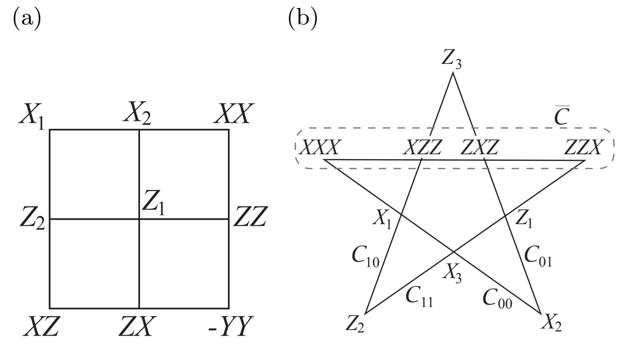

FIG. 2: Mermin's square and star.

Proof of Lemma 5. If s is a consistent non-contextual value assignment satisfying the constraints $\mathcal{C}$, then, $\forall h \in \mathcal{G}$, s' of Eq. (D2) is a consistent value assignment for the constraints $h(\mathcal{C})$. But since $h(\mathcal{C}) = \mathcal{C}$, $\forall h \in \mathcal{G}$, s' is also a consistent non-contextual value assignment for $\mathcal{C}$. □

Structure of the set of consistent value assignments s. If a consistent value assignment s exists, there can be more than one. Denote by $\mathcal{S}$ the set of internal states of the HVM purportedly describing the given physical situation, such that the consistent value assignments are $\{s_\nu |\ \nu \in \mathcal{S}\}$. By Lemma 4, the set of consistent outcome assignments $\{s_\nu | \nu \in \mathcal{S}\}$ form a coset of V,

$$s_\nu \in s_0 + V, \qquad \text{(D3)}$$

assuming that a single solution s_0 exists.

Assuming the existence of an HVM describing the physical situation, the equations (D2) and (D3) must both hold. However, in certain situations those requirements are incompatible. Whenever that happens, the existence of an HVM for the given setting is falsified. Below we first give an example for such a situation, then discuss the general case, and finally explain the connection with state-independent parity proofs of contextuality [3].

Example: Mermin's square. In this example, Ω_+ is the set of all observables appearing in Mermin's square (See Fig. 2a),

$$\Omega_+ = \{I, X_1, X_2, X_1X_2, Z_1, Z_2, Z_1Z_2, X_1Z_2, Z_1X_2, Y_1Y_2\},$$

and $\mathcal{A}$ is the corresponding index set.

Assume that a consistent non-contextual value assignment s exists, $\mathcal{S} \neq \emptyset$, and consider the quantities

$$\eta = \sum_{a\in\mathcal{A}} s(a) \mod 2,\ \ s. \qquad \text{(D4)}$$

Now, for any $h \in \mathcal{G}$, consider the transformed quantity $\eta' = \sum_{a\in\mathcal{A}} s'(a)$. Using Eq. (D2), and $h(\mathcal{A}) = \mathcal{A}$,

$$\eta' = \eta + \sum_{a\in\mathcal{A}} \tilde{\Phi}_h(a) \mod 2. \qquad \text{(D5)}$$

On the other hand, by Lemma 5, s' is also a valid noncontextual value assignment. Thus, applying Eq. (D3)/ Lemma 4 to η', for every $h \in \mathcal{G}$ exists a $\mathbf{v}_h \in V$ such that

$$\eta' = \eta + \sum_{a\in\mathcal{A}} \mathbf{v}_h(a) \mod 2 = \eta \mod 2. \tag{D6}$$

The last equality holds because, by construction of Mermin's square, $\forall \mathbf{v} \in V$ the Hamming weight of $\mathbf{v}$ is even.

Now we choose a specific element of $\mathcal{G}$, namely the Hadamard gate H_1 on the first qubit. Since $H_1\, Y_1 Y_2\, H_1^\dagger = -Y_1 Y_2$, it holds that $\tilde{\Phi}_{H_1}(a_{YY}) = 1$. All other values of $\tilde{\Phi}_{H_1}(a)$, $a \in \mathcal{A}\backslash\{a_{YY}\}$ vanish. Thus, $\sum_{a\in\mathcal{A}} \tilde{\Phi}_{H_1}(a) \mod 2 = 1$. Now comparing Eqs. (D5) and (D6) for the case of $h = H_1$, we find

$$\eta + 1 = \eta \mod 2.$$

Contradiction. Hence, no consistent value assignment s exists. □

Remark: In the above proof, although we dropped the linearity requirement Eq. (8) from $\tilde{\Phi}$, linearity sneaked back in when invoking Lemma 4 to arrive at Eq. (D6).

General method for constructing symmetry-based KS proofs. Suppose there exists an assignment s of values to all observables in Ω_+. We may list these values in a vector $\mathbf{s}$, which, according to Eq. (D2), then transforms under any $h \in \mathcal{G}$ as

$$\mathcal{G} \ni h : \mathbf{s} \mapsto \mathbf{s}' = P_h \mathbf{s} + \mathbf{v}_h \mod 2, \tag{D7}$$

where P_h is a permutation matrix, and $\mathbf{v}_h$ a suitable offset vector. The value assignments $\mathbf{s}$ and $\mathbf{s}'$ need to satisfy the same set of linear constraints,

$$K\mathbf{s} \mod 2 = \mathbf{c} = K\mathbf{s}' \mod 2,$$

where K is the constraint matrix with its rows labeled by constraints and its columns labeled by the elements of $\mathcal{A}$. Combining the two above equations, we find that

$$K(I - P_h)\mathbf{s} = K\mathbf{v}_h \mod 2,\ \forall h \in \mathcal{G}. \tag{D8}$$

If we can find a vector $\mathbf{a}^T$ such that

$$\mathbf{a}^T K (I - P_h) \mod 2 = \mathbf{0}^T, \text{ and} \tag{D9a}$$

$$\mathbf{a}^T K \mathbf{v}_h \mod 2 \neq 0, \tag{D9b}$$

this immediately leads to a contradiction in Eq. (D8).

Connection with Mermin's original parity proofs. The above contextuality proof and Mermin's original parity proof [3] are not the same, because Mermin's proof is about the inconsistency of assignments, and the present proof about the inconsistency of the transformation behaviour of assignments. Nonetheless, both proofs employ the same type of algebraic contradiction.

To see this, we revisit the linear system of equations on which Mermin's proof is built,

$$K\mathbf{s} \mod 2 = \mathbf{u}. \tag{D10}$$

The goal is to find a vector $\mathbf{b}$ such that (i) $\mathbf{b}^T K = \mathbf{0} \mod 2$, and (ii) $\mathbf{b}^T \mathbf{u} \mod 2 \neq 0$. Multiplying Eq. (D10) with any such $\mathbf{b}^T$ immediately leads the contradiction with every noncontextual HVM.

With an eye on the symmetry-based proof displayed in Eq. (D8), we note that the group $\mathcal{G}$, by construction, does not only act on the value assignments, but also on the constraints. Therefore, for each $h \in \mathcal{G}$ there exists a matrix P'_h such that $KP_h = P'_h K$. Now using this in Eq. (D8), we obtain the noncontextual HVM constraint

$$(I - P'_h)K\mathbf{s} = K\mathbf{v}_h \mod 2,\ \forall h \in \mathcal{G}.$$

Therefore, the parity proof based on Eq. (D10) and the symmetry-based proof Eq. (D8) exploit the same algebraic contradiction whenever $\mathbf{b}^T = \mathbf{a}^T(I - P'_h) \mod 2$. This is possible if $\mathbf{b} \in \text{Im}\,(I - P'_h)^T$ for some $h \in \mathcal{G}$. Mermin's parity proof method is thus stronger than the present symmetry based proof: Every symmetry-based proof implies a Mermin-type parity proof, but not the other way around.

3. The roles of covariance and contextuality for G-MBQC

The set Ω_+ was constructed such that it is mapped onto itself under conjugation by G, i.e.,

$$u(g) T_a u(g)^\dagger \in \Omega_+,\ \forall g \in G, , \forall T_a \in \Omega_+. \tag{D11}$$

This property has the following implication with respect to contextuality.

Lemma 6 *If the pair (Ω_+, G) satisfies Eq. (D11), then no symmetry-based state-independent contextuality proof can be based on it.*

Proof of Lemma 6. Eq. (D11) implies that in Eq. (D7) $\mathbf{v}_g = \mathbf{0}$, for all $g \in G$. Thus, the relation Eq. (D9b) needed for a symmetry-based contextuality proof cannot be satisfied for any $\mathbf{a}$. Hence, no symmetry-based contextuality proof exists for the pair (Ω_+, G). □

To summarize, we find that G-MBQC assumes a very particular location with respect to contextuality and covariance of quasi-probability functions. Namely,

(D12)

1. The quasi-probability function Q used to describe the resource state ρ is covariant under the input group G (Lemma 2).
2. There is no state-independent symmetry-based contextuality proof for the pair (Ω_+, G) (Lemma 6).
3. If the G-MBQC in question is non-trivial, then there exists a state-dependent symmetry-based contextuality proof based on the triple (Ω_+, G, ρ) (Prop. 2).

These three properties of G-MBQC crucially depend on the property Eq. (D11) of (Ω_+, G), which is illustrated in the second of the examples below.

Example: State-independent Mermin star. In this example, we consider symmetry transformations in the input group $G = \langle A_1A_2, A_1A_3\rangle$ (recall that $A := (X + Y)/\sqrt{2}$). The purpose is to illustrate that, in attempting a symmetry-based proof, no vector $\mathbf{b}$ which gives a KS contradiction by left-multiplying Eq. (D10) is in $\mathrm{Im}(I - P'_g)^T$, for any $g \in G$.

It suffices to consider A_1A_2, because the identity $I \in G$ cannot produce a KS proof, and the remaining three group elements map onto each other by permutation of particles, under which Mermin's star is invariant.

For the ordering of observables XXX, XZZ, ZXZ, ZZX, X_1, X_2, X_3, Z_1, Z_2, Z_3, and a suitable ordering of constraints where the bottom row corresponds to the "horizontal" context in Mermin's star (see Fig. 2b) , the parity check matrix reads

$$K = \begin{pmatrix} 1&0&0&0&1&1&1&0&0&0\\ 0&1&0&0&1&0&0&0&1&1\\ 0&0&1&0&0&1&0&1&0&1\\ 0&0&0&1&0&0&1&1&1&0\\ 1&1&1&1&0&0&0&0&0&0 \end{pmatrix}.$$

As explained, the right-multiplication of K under AAI, $K \mapsto KP_{AAI}$ may as well be captured by multiplying K from the left by a matrix P'_{AAI}, and

$$P'_{AAI} = \left(\begin{array}{cccc|c} 0&0&0&1&0\\ 0&0&1&0&0\\ 0&1&0&0&0\\ 1&0&0&0&0\\ \hline 0&0&0&0&1 \end{array}\right).$$

Thus, the last column of $I \oplus P'_{AAI}$ is all 0's, and in particular $(1,1,1,1,1)^T \not\in \mathrm{Im}\,(I + P'_{AAI})^T$. Hence, we cannot exploit Mermin's contradiction in this symmetry-based, state-independent argument. We have already seen that the symmetry-based contextuality proof exists in the state-dependent version.

Example: Dressed Mermin star. The purpose of this example is to illustrate the crucial dependence of the first two properties of Eq. (D12) on the property Eq. (D11) of the pair (Ω_+, G). Let's replace the set Ω_+ used in Mermin's star (see Figures 2b and 3) by

$$\Omega_+ \longrightarrow \Omega'_+ = \Omega_+ \cup \{Z_1Z_2, Z_1Z_3, Z_2Z_3\}.$$

The new observables are dependent on the set of observables $\{Y_1Y_2X_3, Y_1X_2Y_3, X_1Y_2Y_3\}$ which are already in Ω_+. However, G does not map Ω'_+ to itself under conjugation. For example,

$$A_1A_2\, Z_1Z_3(A_1A_2)^\dagger = -Z_1Z_3. \tag{D13}$$

We now show that, in consequence, the pair (Ω_+, G) does lead to a state-independent symmetry-based contextuality proof. Following the argument in Appendix D 2, we

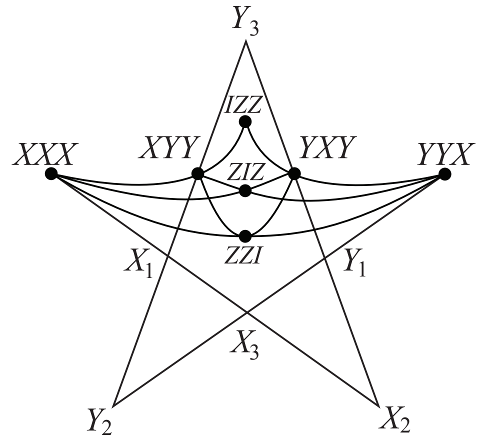

FIG. 3: Dressed Mermin star.

choose a subset Υ of Ω'_+,

$$\Upsilon = \{X_1, X_3, Y_1, Y_3, X_1Y_2Y_3, Y_1X_2Y_3, Z_2Z_3\},$$

and consider the linear combination

$$\eta \;=\; \textstyle\sum_{a|T_a\in\Upsilon} s(a) \mod 2. \tag{D14}$$

Therein, $s(\cdot)$ is a consistent non-contextual value assignment, of which assume that it exists. Since A_1A_2 flips Z_2Z_3 under conjugation, $s(a_{IZZ}) \longrightarrow s(a_{IZZ}) \oplus 1$. The other values s appearing on the r.h.s. of Eq. (D14) are permuted among themselves. Therefore, $A_1A_2 : \eta \mapsto \eta \oplus 1$. On the other hand, η is a sum of constraints (add $2s(a_{XXX}) + 2s(a_{X_2})$ on the r.h.s.), hence must remain constant under all symmetry transformations. Contradiction. Hence, no consistent non-contextual value assignment exists.

By a very similar argument, it can be shown that the quasi-probability function Q' defined by the phase point operators

$$A'_{\mathbf{v}} := \frac{1}{|V|}\sum_{T_a\in\Omega'_+} \chi_{\mathbf{v}}(a)T_a$$

is not covariant under G. In this regard, we ask whether for any $g \in G$ there exists an $\mathbf{u} \in V$ such that $gA'_{\mathbf{0}}g^\dagger = A'_{\mathbf{u}}$. In other words, is there a $\mathbf{u} \in V$ such that $(-1)^{\tilde{\Phi}(\cdot)} = \chi_{\mathbf{u}}(\cdot)$? This is a necessary condition for the covariance of Q' under G. For $G \ni g_0 = A_1A_2$, define

$$\nu := \sum_{a|T_a\in\Upsilon} \tilde{\Phi}_{g_0}(a) \mod 2.$$

By explicit computation, $(-1)^\nu = -1$. However,

$$\begin{aligned}\textstyle\prod_{a|T_a\in\Upsilon}\chi_{\mathbf{u}}(a) \;&=\; \chi_{\mathbf{u}}(a_{X_1})\chi_{\mathbf{u}}(a_{X_2})\chi_{\mathbf{u}}(a_{X_3})\chi_{\mathbf{u}}(a_{XXX})\times\\ &\quad\;\chi_{\mathbf{u}}(a_{Y_1})\chi_{\mathbf{u}}(a_{X_2})\chi_{\mathbf{u}}(a_{Y_3})\chi_{\mathbf{u}}(a_{YXY})\times\\ &\quad\;\chi_{\mathbf{u}}(a_{XXX})\chi_{\mathbf{u}}(a_{XYY})\chi_{\mathbf{u}}(a_{IZZ})\\ &=\; 1\times 1\times 1 = +1.\end{aligned}$$

Note that, on the r.h.s. of the first equality, the observables $X_2, X_1X_2X_3 \notin \Upsilon$, but the corresponding characters $\chi_{\mathbf{u}}(a_{XXX})$ and $\chi_{\mathbf{u}}(a_{X_2})$ appear twice in the product, such that their values do not matter. In the last line, we have used the linearity of $\chi_{\mathbf{u}}(\cdot) = (-1)^{\mathbf{u}(\cdot)}$, cf. Eq. (3). We thus find that $(-1)^{\tilde{\Phi}(\cdot)} \neq \chi_{\mathbf{u}}(\cdot)$, for any $\mathbf{u} \in V$. Therefore, $g_0 A'_{\mathbf{0}} g_0^\dagger \neq A'_{\mathbf{u}}$, for any $\mathbf{u} \in V$, and Q' is not covariant under G, as claimed.