SUPPLEMENTARY MATERIAL

A hidden variable model for universal quantum computation with magic states on qubits

Michael Zurel,[1,2] Cihan Okay,[1,2] and Robert Raussendorf[1,2]

[1]*Department of Physics and Astronomy, University of British Columbia, Vancouver, BC, Canada*
[2]*Stewart Blusson Quantum Matter Institute, University of British Columbia, Vancouver, BC, Canada*

(Dated: November 3, 2020)

A comment regarding notation: Equation and Theorem references to the main text carry a suffix "[m]" below, to distinguish them from the equation numbering in this supplement. For example, Eq. (8) from the main text is here referred to as Eq. (8) [m].

I. STRATONOVICH-WEYL CORRESPONDENCE

In the field of quantum optics, the Stratonovich-Weyl (SW) correspondence is a set of criteria that well-behaved quasi-probability distributions over phase space have to satisfy. Denote by $F_A^{(s)} : X \longrightarrow \mathbb{C}$ the quasiprobability distribution corresponding to the (not necessarily Hermitian) operator A, with X the phase space and s a real parameter in the interval $[-1, 1]$. In the standard formalism for infinite-dimensional Hilbert spaces, $s = -1, 0, 1$ correspond to the Glauber-Sudarshan P, Wigner, and Husimi Q function, respectively. Then, the following set of criteria is imposed on the $F_A^{(s)}$ [1]; also see [2],

(0) Linearity: $A \longrightarrow F_A^{(s)}$ is a one-to-one linear map.

(1) Reality:

$$F_{A^\dagger}^{(s)}(u) = \left(F_A^{(s)}(u)\right)^*, \forall u \in X.$$

(2) Standardization:

$$\int_X d\mu(u) F_A^{(s)}(u) = \operatorname{Tr} A.$$

(3) Covariance:

$$F_{g\cdot A}^{(s)}(u) = F_A^{(s)}(g^{-1}u),\ g \in G,$$

with G the dynamical symmetry group.

(4) Traciality:

$$\int_X d\mu(u) F_A^{(s)}(u) F_B^{(-s)}(u) = \operatorname{Tr} AB.$$

To investigate the SW criteria in the present setting, we first extend the probability distributions p_ρ defined in Eq. (2) [m] for proper density matrices to a quasiprobability function W defined for all operators A, via

$$A = \sum_\alpha W_A(\alpha) A_\alpha. \tag{1}$$

We note that W does not come with a parameter s; there is only a single quasiprobability function W. This will affect the formulation of traciality.

Further, the mapping $A \longrightarrow W_A$ is linear, $A + B$ can be represented as $W_A + W_B$. However, the mapping is one-to-many, and the Stratonovich-Weyl criterion (0) is thus not satisfied. In fact, this is a general consequence of Kochen-Specker contextuality, as has been demonstrated in [3].

The remaining SW conditions apply.

(1) Reality. All phase point operators A_α are Hermitian by definition, cf. Eq. (1) [m]. Therefore $A^\dagger$ can be represented by the quasiprobability distribution $\alpha \mapsto W_A(\alpha)^*$.

(2) Standardization. By their definition Eq. (1) [m], the phase point operators satisfy $\operatorname{Tr} A_\alpha = 1$, for all $\alpha \in \mathcal{V}_n$. Standardization,

$$\operatorname{Tr} A = \sum_\alpha W_A(\alpha), \tag{2}$$

follows by taking the trace of Eq. (1).

(3) Covariance. Let Cl_n denote the n-qubit Clifford group. We have the following result.

Lemma 1 *For any operator A it holds that*

$$W_{gAg^\dagger}(\alpha) = W_A(g^{-1}\alpha),\ \ \forall g \in Cl_n. \tag{3}$$

Proof of Lemma 1. First we show that Λ_n is mapped into itself under the action of the Clifford group. Namely, for all stabilizer sates $|\sigma\rangle \in \mathcal{S}$,

$$\begin{aligned} \operatorname{Tr}(gA_\alpha g^\dagger |\sigma\rangle\langle\sigma|) &= \operatorname{Tr}(A_\alpha\, g^\dagger|\sigma\rangle\langle\sigma|g) \\ &= \operatorname{Tr}(A_\alpha\, |\sigma'\rangle\langle\sigma'|) \\ &\geq 0. \end{aligned}$$

Furthermore, $\operatorname{Tr}(gA_\alpha g^\dagger) = \operatorname{Tr} A_\alpha = 1$. Hence, with the definition Eq. (1) [m] of Λ_n, it holds that $gA_\alpha g^\dagger \in \Lambda_n$, for all $\alpha \in \mathcal{V}_n$ and all $g \in \mathrm{Cl}_n$.

Now we show that for every $\alpha \in \mathcal{V}_n$ and every $g \in \mathrm{Cl}_n$ there is a unique $\beta \in \mathcal{V}_n$ such that

$$gA_\alpha g^\dagger = A_\beta. \tag{4}$$

Let $\mathcal{S}_\alpha$ be the subset of stabilizer states that specifies A_α, i.e. A_α is the unique solution in Λ_n to the set of constraints $\mathrm{Tr}(X|\sigma\rangle\langle\sigma|) = 0$ for all $|\sigma\rangle \in \mathcal{S}_\alpha$. In fact, we can choose the size of $\mathcal{S}_\alpha$ to be equal to $2^{2n} - 1$ [4, Theorem 18.1]. Let $g \cdot S_\alpha$ denote the set of stabilizers $g|\sigma\rangle\langle\sigma|g^\dagger$ where $|\sigma\rangle \in \mathcal{S}_\alpha$. Then the action of g gives a one-to-one correspondence between the set of solutions to the constraints specified by $\mathcal{S}_\alpha$ and $g^\dagger \cdot \mathcal{S}_\alpha$ since if X is a solution to the former then $gXg^\dagger$ is a solution to the latter and vice versa. Moreover, $gXg^\dagger$ belongs to the polytope Λ_n. Therefore $gA_\alpha g^\dagger$ specifies a vertex. In other words, given $\alpha \in \mathcal{V}_n$ and $g \in \mathrm{Cl}_n$, Eq. (4) holds for a suitable $\beta \in \mathcal{V}_n$. We thus define $g\alpha := \beta$, and Eq. (4) becomes

$$gA_\alpha g^\dagger = A_{g\alpha}. \tag{5}$$

Therefore,

$$\begin{aligned}
\textstyle\sum_\alpha W_{gAg^\dagger}(\alpha)A_\alpha &= gAg^\dagger \\
&= \textstyle\sum_\alpha W_A(\alpha)\, gA_\alpha g^\dagger \\
&= \textstyle\sum_\alpha W_A(\alpha)A_{g\alpha} \\
&= \textstyle\sum_\alpha W_A(g^{-1}\alpha)A_\alpha.
\end{aligned}$$

Thus, $W_{gAg^\dagger}(\alpha) = W_A(g^{-1}\alpha)A_\alpha$. $\Box$

We remark that, for qubits, only non-unique quasiprobability functions can be Clifford covariant. Namely, if the phase point operators form an operator basis, i.e., are linearly independent, then the resulting quasiprobability function cannot be Clifford covariant [5].

The covariance property can be used to efficiently simulate the effect of Clifford unitaries in QCM, as an alternative to the method of treating Clifford unitaries discussed in the main text.

(4) Traciality. In the absence of a continuously varying parameter s, we introduce a dual quasiprobability function $\tilde{W}$ in addition to W, to stand in for $F^{(-s)}$. Namely, for all projectors $\Pi_{a,s}$, corresponding to measurements of Pauli observables T_a with outcome s, we define

$$\tilde{W}_{\Pi_{a,s}}(\alpha) := Q_a(s|\alpha).$$

By linearity, this implies expressions for all $\tilde{W}_{T_a}(\alpha)$. Since the Pauli operators form an operator basis, again by linearity one obtains $\tilde{W}_A$ for any operator A. Then,

$$\mathrm{Tr}AB = \sum_\alpha \tilde{W}_A(\alpha)W_B(\alpha)$$

follows from Eq. (4) [m].

We thus satisfy the SW criteria (1) - (4).

To conclude, we emphasize that for the present purpose of classically simulating QCM, a crucial property of W is positivity preservation under Pauli measurement. This property has no counterpart in the Stratonovich-Weyl correspondence.

II. SOME BACKGROUND ON QCM

Quantum computation with magic states (QCM) is a scheme for universal quantum computation, closely related to the circuit model. From a practical point of view, QCM is very advantageous for fault-tolerant quantum computation [13], but that does not concern us here.

A. Operations in QCM

There are two types of operations in QCM, the "free" operations and the resources. They free operations are (i) Preparation of all stabilizer states, (ii) All Clifford unitaries, and (iii) Measurement of all Pauli observables.

The resource are arbitrarily many copies of the state

$$|\mathcal{T}\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}. \tag{6}$$

The state $|\mathcal{T}\rangle$ is called a "magic state".

A stabilizer state is a pure n-qubit quantum state which is the joint eigenstate of a maximal set of commuting Pauli operators [14–16]. The n-qubit Clifford group Cl_n is the largest subgroup of $SU(2^n)$ with the property that for any $g \in Cl_n$ and all Pauli operators T_a there exists a Pauli operator T_b such that

$$gT_a g^\dagger = \pm T_b.$$

That is, the Clifford group is the normalizer of the Pauli group.

The distinction between free operations and resources in QCM is motivated by the Gottesman-Knill theorem. Namely, the free operations alone are not universal for quantum computation, and, in fact, can be efficiently classically simulated. The magic states restore computational universality (see below), hence the name.

A further motivation for subdividing the computational primitives into free operations and resources stems from quantum error correction. Fault-tolerant versions of the free operations are comparatively easy to produce, but the creation of fault-tolerant magic states is very operationally costly.

B. Computational universality

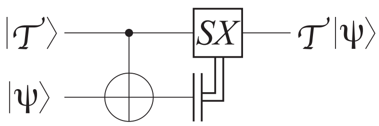
It is well known [17] that the gates

$$\{\mathrm{CNOT}_{ij}, H_i, \mathcal{T}_i,\ 1 \le i \neq j \le n\}$$

form a universal set, i.e., enable universal quantum computation. Therein, the controlled NOT gates CNOT_{ij} between qubits i and j and the Hadamard gates H_i are in the Clifford group. The only non-Clifford element in the above universal set is

$$\mathcal{T}_i = \exp\left(-i\frac{\pi}{8}Z_i\right).$$

This gate can be simulated by the use of a single magic state $|\mathcal{T}\rangle$ in a circuit of Clifford gates and Pauli measurements (circuit reproduced from Fig. 10.25 of [16]),



.

Therein, the lower qubit is measured in the Z-basis, and the binary measurement outcome classically controls the SX-gate. S is a Clifford gate,

$$S_i = \exp\left(-i\frac{\pi}{4}Z_i\right).$$

Thus, the magic states Eq. (6) boost the free operations to quantum computational universality.

III. COMPLEXITY PARAMETER OF THE STATE POLYTOPE Λ_n

A question that arises with Theorem 2 [m] is what determines the value of n labelling the state polytope Λ_n, and hence the complexity of the simulation. In this regard, we make the following observation.

Lemma 2 *Any quantum computation in the magic state model that operates on an initial state $|\mu\rangle_A \otimes |\sigma\rangle_B$, where $|\mu\rangle$ is an n-qubit magic state and $|\sigma\rangle$ is an m-qubit stabilizer state, can with the same efficiency be run on the magic state $|\mu\rangle$ alone.*

Supplementing the non-stabilizer magic state $|\mu\rangle$ with stabilizer states is thus redundant. For example, if the magic states used in a given QCM are all of T-type, then n can be taken to be the number of those states.

Proof of Lemma 2. Wlog. we discuss the version of QCM where the quantum computation consists of a sequence of only Pauli measurements. We give an explicit procedure to replace the sequence τ on $A\otimes B$ by an equivalent sequence $\tilde{\tau}^{(A)}$ of measured observables that act only on the subsystem A. The proof is by induction, and the induction hypothesis is that, at time t, the sequence $\tau_{\leq t}$ of measurements has been replaced by a computationally equivalent sequence $\tilde{\tau}^{(A)}_{\leq t}$ of Pauli measurements on the register A only. This statement is true for $t = 0$, i.e., the empty measurement sequence. We now show that the above statement for time t implies the analogous statement for time $t + 1$.

At time t, the state of the quantum register evolved under the computationally equivalent measurement sequence $\tilde{\tau}^{(A)}_{\leq t}$ is $|\Psi(t)\rangle = |\psi(t)\rangle_A \otimes |\sigma\rangle_B$. We now consider the Pauli observable $T(t + 1) \in \tau$ to be measured next, and write $T(t + 1) = S_A(t + 1) \otimes R_B(t + 1)$. There are two cases.

Case I: $T(t+1)$ *commutes with the entire stabilizer* $\mathcal{S}$ *of* $|\sigma\rangle$. Hence, also $R_B(t + 1)$ commutes with $\mathcal{S}$. But then, either $R_B(t + 1)$ or $-R_B(t + 1)$ is in $\mathcal{S}$, and $R_B(t + 1)$ may be replaced by its eigenvalue ±1 in the measurement. Hence, the measurement of $T(t + 1)$ is equivalent to the measurement of $\pm S_A(t + 1)$.

Case II: $T(t + 1)$ *does not commute with the entire stabilizer* $\mathcal{S}$ *of* $|\sigma\rangle$. Then, the measurement outcome s_{t+1} is completely random. Further, there exists a Clifford unitary U such that

$$\begin{aligned} U\mathcal{S}U^\dagger &= \langle X_{B:1}, X_{B:2}, .., X_{B:m}\rangle, \\ UT(t + 1)U^\dagger &= Z_{B:1}. \end{aligned}$$

Therefore, the state resulting from the measurement of $T(t+1)$, with outcome s_{t+1} on the state $|\Psi(t)\rangle$ is the same state as the one resulting from the following procedure:

1. Apply the Clifford unitary U to $|\Psi(t)\rangle = |\psi(t)\rangle_A \otimes |\sigma(t)\rangle_B$, leading to
$$U\,|\Psi(t)\rangle = |\tilde{\psi}(t)\rangle \otimes |\overline{+}\rangle_B,$$
where $|\overline{+}\rangle_B := \bigotimes_{i\in B} |+\rangle_{B:i}$.
2. Measure $Z_{B:1}$ on $|\tilde{\psi}(t)\rangle \otimes |\overline{+}\rangle_B$, with outcome s_{t+1}.
3. Apply $U^\dagger$.

Now, note that the measurement in Step 2, of the Pauli observable $Z_{B:1}$ is applied to the stabilizer state $|\overline{+}\rangle_B$. The result is $|\tilde{\sigma}(t + 1)\rangle = |s_{t+1}\rangle_{B:1} \bigotimes_{j=2}^m |+\rangle_{B:j}$. Therefore, after normalization, the effect of the measurement can be replaced by the unitary $(X_{B:1})^{s_{t+1}}\, H_{B:1}$.

Thus, the whole procedure may be replaced by the Clifford unitary $U^\dagger\, (X_{B:1})^{s_{t+1}}\, H_{B:1}\, U$. But Clifford unitaries don't need to be implemented. They are just propagated past the last measurement, thereby affecting the measured observables by conjugation whereby their Pauli-ness is preserved. In result, in Case II, the measurement of $T(t + 1)$ doesn't need to be performed at all. It is replaced by classical post-processing of the subsequent measurement sequence.

We conclude that in both the cases I and II, given the induction assumption, the original measurement sequence $\tau_{\leq t+1}$ can be replaced by a computationally equivalent measurement sequence $\tilde{\tau}^{(A)}_{\leq t+1}$ acting on register A only. By induction, the complete measurement sequence τ can be replaced by a computationally equivalent sequence $\tilde{\tau}^{(A)}$ acting on A only.

Since the measurements $\tilde{\tau}^{(A)}$ are applied to an unentangled initial state $|\mu\rangle_A \otimes |\sigma\rangle_B$, the register B can be dropped. Finally, the measurement sequence $\tilde{\tau}^{(A)}$ is of the same length or shorter than τ, and can be efficiently computed from the latter. Hence its implementation is at least as efficient. □

IV. MULTI-QUBIT PHASE POINTS FROM [10] ARE EXTREMAL

The present work, there is no negativity anywhere in the classical simulation of QCM. The shifting of the cause for computational hardness away from negativity to other potential sources is a major disruption with the prior works [6–10].

But underneath this discontinuity lies an element of continuity. Namely, the direct precursor to the present work is Ref. [10]; and the phase point operators of the multi-qubit quasiproability function defined therein are also extremal vertices of the present state polytope Λ_n. This is the content of Lemma 4 below, the main result of this section. It shows that the multi-qubit phase space defined in [10] is a subset of the phase space of the present model, describing a sector of it in which the update rules under Clifford unitaries and Pauli measurements are guaranteed to be computationally efficient.

Recall from [10] a couple of definitions. We call a set $\Omega \subset E_n$ closed under inference if for all $a, b \in \Omega$ with the property that $[a, b] = 0$ it holds that $a + b \in \Omega$. (Here $[a, b] := a_X b_Z + a_Z b_X \mod 2$.) We call a set $\Omega \subset E_n$ non-contextual if it supports a non-contextual value assignment. Sets Ω which are both closed under inference and non-contextual are called "cnc" [10] (also see [12]). Of particular interest in are maximal cnc sets, which are cnc sets that are not strictly contained in any other cnc set. They give rise to the following multi-qubit phase point operators

$$A_\Omega^\gamma = \frac{1}{2^n} \sum_{a \in \Omega} (-1)^{\gamma(a)} T_a, \tag{7}$$

where Ω is a maximal cnc set, and $\gamma : \Omega \longrightarrow \mathbb{Z}_2$ is a non-contextual value assignment.

Theorem 1 in [10] classifies the maximal cnc sets. For the present purpose it may be rephrased as

Lemma 3 *If a subset of E_n is closed under inference and does not contain a Mermin square then it is non-contextual.*

Proof sketch for Lemma 3. Theorem 1 of [10] classifies the subsets of E_n that are closed under inference and do not contain a Mermin square. They all turn out to be non-contextual. □

We now have the following result (also see [11] for an independent proof).

Lemma 4 *For any number n of qubits, the phase point operators A_Ω^γ of Eq. (7) are vertices of Λ_n.*

An independent proof of this result is given in [11].

Proof of Lemma 4. Pick an n, any pair (Ω, γ). A_Ω^γ has unit trace, and, as shown in [10], satisfies $\text{Tr}(|\sigma\rangle\langle\sigma| A_\Omega^\gamma) \geq 0$. Therefore, $A_\Omega^\gamma \in \Lambda_n$, and A_Ω^γ has an expansion

$$A_\Omega^\gamma = \sum_{\beta \in \mathcal{V}_n} p_{\Omega,\gamma}(\beta) A_\beta, \tag{8}$$

where $p_{\Omega,\gamma}(\beta) \geq 0$, $\forall \beta$, and $\sum_\beta p_{\Omega,\gamma}(\beta) = 1$. Thus, $p_{\Omega,\beta}$ is a probability distribution. Henceforth, we consider any A_β for which $p_{\Omega,\gamma}(\beta) > 0$.

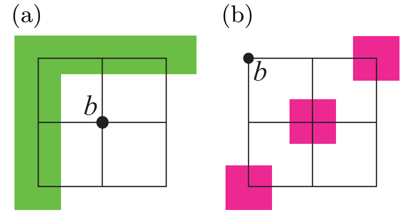


FIG. 1. Two possibilities for the set $\Omega \cap M$, shown in color.

Now pick an $a \in \Omega$ and consider $\text{Tr}\,(T_a A_\Omega^\gamma)$. With Eq. (7), it holds that $(-1)^{\gamma(a)} = \sum_\beta p_{\Omega,\gamma}(\beta) \langle T_a \rangle_\beta$. Since $p_{\Omega,\beta}$ is a probability distribution and $|\langle T_a \rangle_\beta| \leq 1$ for all β, it follows that

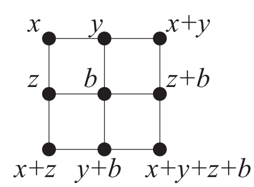
$$\langle T_a \rangle_\beta = (-1)^{\gamma(a)}, \ \forall\, \beta \text{ with } p_{\Omega,\gamma}(\beta) > 0.$$

That is, every phase point operator that appears on the rhs. of Eq. (8) with non-zero coefficient agrees with A_Ω^γ on the expectation values $\langle T_a \rangle$ for all $a \in \Omega$.

Now we turn to the expectation values for $b \notin \Omega$. Any set $\tilde{\Omega} \subset E_n$ that is closed under inference and contains both Ω and b is contextual, by the maximality of Ω. By Lemma 3, any such $\tilde{\Omega}$ contains a Mermin square M, and furthermore $b \in M$.

Since M is closed under inference, so is $\Omega \cap M$. Also, since Ω is maximal, $\Omega \cap M$ is maximal in M. Up to permutations of rows and columns, there are two possibilities for $\Omega \cap M$, which are displayed in Fig. 1.

Case (a). For any b there exists a triple $\{x, y, z\} \subset M \backslash b$ such that $[x, y] = [x, z] = [b, y] = [b, z] = 0$, $[x, b] = [y, z] \neq 0$. We have the following Mermin square:



Therein, Mermin's contradiction to the existence of a non-contextual HVM is encapsulated in the operator relation $(T_x T_y)(T_z T_b) = -(T_x T_z)(T_y T_b)$.

We chose the following phase conventions.

$$\begin{array}{l} T_{x+y} = T_x T_y,\ T_{z+b} = T_z T_b, \\ T_{x+z} = T_x T_z,\ T_{y+b} = T_y T_b, \end{array} \tag{9}$$

and

$$\begin{array}{rcl} T_{x+y+z+b} &=& T_{x+z} T_{y+b}, \\ T_{x+y+z+b} &=& -T_{x+y} T_{z+b}. \end{array} \tag{10}$$

Recall that with the first part of the proof $\langle T_j \rangle_\beta = (-1)^{\gamma(j)}$, for $j = x, y, z$. Now assume that $\langle T_b \rangle_\beta = \nu$, with $-1 \leq \nu \leq 1$. Now, with Eq. (9)

$$\begin{array}{rcl} \langle T_{x+y} \rangle_\beta &=& (-1)^{\gamma(x)+\gamma(y)},\ \langle T_{x+z} \rangle_\beta = (-1)^{\gamma(x)+\gamma(z)}, \\ \langle T_{y+b} \rangle_\beta &=& \nu(-1)^{\gamma(y)},\ \langle T_{z+b} \rangle_\beta = \nu(-1)^{\gamma(z)}. \end{array}$$

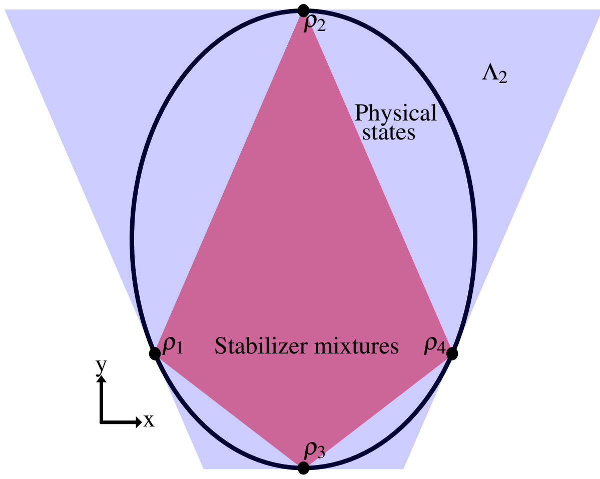


FIG. 2. Cross section of the space $\mathrm{Herm}_1(4)$ parameterized by Eq. 11. The two-qubit stabilizer polytope is inscribed in the set of physical states and the set of physical states is inscribed in the polytope Λ_2. The states labelled by ρ_1–ρ_4 are given in Eq. (12).

Therefore, with Eq. (10),

$$\begin{aligned} \langle T_{x+y+z+b}\rangle_\beta &= \nu(-1)^{\gamma(x)+\gamma(y)+\gamma(z)} \\ &= -\nu(-1)^{\gamma(x)+\gamma(y)+\gamma(z)}. \end{aligned}$$

This is satisfiable only if $\nu = 0$, and hence $\langle T_b\rangle_\beta = 0$.

Case (b). The argument is analogous to case (a), and we do not repeat it here.

By the above case distinction, for any $b \in E_n\backslash\Omega$ either case (a) or (b) applies, and each way the consequence is that $\langle T_b\rangle_\beta = 0$. Therefore, any phase point operator A_β that appears on the rhs of Eq. (8) with nonzero $p_{\Omega,\gamma}(\beta)$ agrees with A_Ω^γ on *all* expectation values of Pauli observables; hence $A_\Omega^\gamma = A_\beta$ for all such β.

Now assume there exists no such A_β. Taking the trace of Eq. (8) yields $1 = 0$; contradiction. Hence, there must exist a β such that $A_\Omega^\gamma = A_\beta$, for all (Ω, γ). □

V. THE TWO-QUBIT POLYTOPE Λ_2

Fig. 1 in the main text shows what the polytope Λ_n looks like for a single qubit, $n = 1$. The polytope Λ_1 is a cube inscribing the Bloch ball—the set of physical quantum states. The situation is similar for multiple qubits. In general, Λ_n is not a hypercube, it is a more general polytope, but it still inscribes the set of physical states.

Fig. 2 shows a cross section of the space $\mathrm{Herm}_1(4)$, indicating the states which are contained in the two-qubit stabilizer polytope—the set of mixtures of pure two-qubit stabilizer states, the set of physical states, and the polytope Λ_2. The cross section is parameterized by

$$\rho(x,y) = \frac{1}{4}I_{12} + x(Z_1+Z_2) + y(X_1X_2 + Z_1Z_2 - Y_1Y_2). \tag{11}$$

The four states labelled in the figure are

$$\begin{aligned} \rho_1 &= \frac{1}{4}I_{12} - \frac{1}{8}(Z_1+Z_2), \\ \rho_2 &= \frac{1}{4}I_{12} + \frac{1}{4}(X_1X_2 + Z_1Z_2 - Y_1Y_2), \\ \rho_3 &= \frac{1}{4}I_{12} - \frac{1}{12}(X_1X_2 + Z_1Z_2 - Y_1Y_2), \\ \rho_4 &= \frac{1}{4}I_{12} + \frac{1}{8}(Z_1+Z_2). \end{aligned} \tag{12}$$

VI. Λ_n IS BOUNDED

The set E_n has the structure of a vector space over $\mathbb{Z}_2$. The commutator $T_aT_bT_aT_b$ is given by $(-1)^{[a,b]}$ where $[a,b] = a_Z^Tb_X + b_Z^Ta_X \mod 2$. A subspace of E_n on which the symplectic form $[\cdot,\cdot]$ vanishes is called an isotropic subspace. For an isotropic subspace $I \subset E_n$ and a value assignment $\lambda : I \to \mathbb{Z}_2$ we define a projector

$$\Pi_{I,\lambda} = \frac{1}{|I|}\sum_{a\in I}(-1)^{\lambda(a)}T_a.$$

Summing over all value assignments gives a resolution of the identity: $\sum_\lambda \Pi_{I,\lambda} = \mathbb{1}$. For each stabilizer state $|\sigma\rangle$ there is a unique pair (I,λ) consisting of a maximal isotropic subspace and a value assignment defined on it such that $\Pi_{I,\lambda} = |\sigma\rangle\langle\sigma|$. Then for $X \in \Lambda_n$ we have

$$\begin{aligned} \mathrm{Tr}(X\Pi_{a,s}) &= \mathrm{Tr}(X\Pi_{a,s}\mathbb{1}) \\ &= \mathrm{Tr}(X\Pi_{a,s}\textstyle\sum_{\lambda'}\Pi_{I',\lambda'}) \\ &= \textstyle\sum_{\lambda'}\mathrm{Tr}(X\Pi_{a,s}\Pi_{I',\lambda'}) \\ &= \textstyle\sum_{\lambda|\ \lambda(a)=s}\mathrm{Tr}(X\Pi_{I,\lambda}) \geq 0. \end{aligned}$$

Therefore Λ_n is contained in the hypercube defined by

$$\{X \in \mathrm{Herm}_1(2^n)|\ \mathrm{Tr}(\Pi_{a,s}X) \geq 0,\ \forall a \in E_n - \{0\},\ s = 0,1\}$$

and thus it is bounded.

[1] R.L. Stratonovich, Zh. Eksp. Theor. Fiz. **31**, 1012 (1956) [Sov. Phys. JETP **4**, 891 (1957)].
[2] C. Brif, A. Mann, J. Phys. A **31**, 9 (1998).
[3] M.S. Leifer and O.J.E. Maroney, Phys. Rev. Lett. **110**, 120401 (2013).
[4] V. Chvatal, Linear programming, W. H. Freeman and Company, New York, (1983).
[5] H. Zhu, Phys. Rev. Lett. **116**, 040501 (2016).
[6] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New J. Phys. **14**, 113011 (2012).

[7] N. Delfosse, P. Allard Guerin, J. Bian and R. Raussendorf, Phys. Rev. X **5**, 021003 (2015).
[8] N. Delfosse, C. Okay, J. Bermejo-Vega, D. E. Browne, and R. Raussendorf, New J. Phys. **19**, 123024 (2017).
[9] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega, Phys. Rev. A **95**, 052334 (2017).
[10] R. Raussendorf, J. Bermejo-Vega, E. Tyhurst, C. Okay, M. Zurel, Phys. Rev. A **101**, 012350 (2020).
[11] A. Heimendahl, MSc Thesis, University of Cologne, 2019.
[12] William M. Kirby, Peter J. Love, Phys. Rev. Lett. 123, 200501 (2019).
[13] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[14] D. Gottesman, Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, p. 32-43 (Cambridge, MA, International Press, 1999)
[15] S. Aaronson, D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[16] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
[17] A. Yao, Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, 352–361 (1993).