

This is the accepted manuscript made available via CHORUS. The article has been published as:

Symmetry-protected topological phases with uniform computational power in one dimension

Robert Raussendorf, Dong-Sheng Wang, Abhishodh Prakash, Tzu-Chieh Wei, and David T. Stephen

Phys. Rev. A **96**, 012302 — Published 5 July 2017

DOI: [10.1103/PhysRevA.96.012302](https://doi.org/10.1103/PhysRevA.96.012302)

Symmetry-protected topological phases with uniform computational power in one dimension

Robert Raussendorf¹, Dong-Sheng Wang¹, Abhishodh Prakash², Tzu-Chieh Wei², David T. Stephen¹

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

2: *C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy,
State University of New York at Stony Brook, Stony Brook, NY 11794-3840, USA*

(Dated: April 26, 2017)

We investigate the usefulness of ground states of quantum spin chains with symmetry-protected topological order (SPTO) for measurement-based quantum computation. We show that, in spatial dimension one, if an SPTO phase supports quantum wire, then, subject to an additional symmetry condition that is satisfied in all cases so far investigated, it can also be used for quantum computation.

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

I. INTRODUCTION

The computational power of measurement-based quantum computation (MBQC) [1] critically depends on the resource state used. Families of resource states enabling universal quantum computation exist—cluster states [2] and AKLT-states [3] (see [4], [5]) are examples—but they are very rare in Hilbert space [6], [7].

The latter changes in the presence of symmetry. Here, we are concerned with the scenario of symmetry-protected topological order (SPTO) [8]-[10], in spatial dimension one. In this setting, Hamiltonians are constrained to be invariant under a group G of symmetry transformations, and we consider the ground states of such Hamiltonians as resource states for MBQC. These ground states form physical phases, across which their properties vary smoothly.

It has been conjectured [11], [12] that in the scenario of symmetry-protected topological order, physical phases are identical with “computational phases”. Namely,

Conjecture 1 *The computational power of ground states for measurement-based quantum computation is uniform across each symmetry-protected topologically ordered phase.*

The evidence for this conjecture is the following. In spatial dimension one, for any symmetry-protected phase characterized by a finite abelian symmetry group and a maximally non-commutative cohomology class, all matrix-product states in the phase support quantum wire [12]. That is, quantum information can be shuttled from one end of the spin chain to the other by local measurements, and this process is robust against symmetry-respecting perturbations of the ground state. With regard to quantum computation, it has been shown that for one specific symmetry group, S_4 , there exists a computationally universal SPT ordered phase [13]. Also, there is an extended universal region for a particular A_4 invariant model [14] (for a phase diagram of SPT-ordered phases in one dimension under the symmetry group A_4 see [15]).

There is also support for Conjecture 1 in spatial dimension $\mathcal{D} = 2$. It is known that the two-dimensional

AKLT state [3] is a universal resource for MBQC, on various lattices [4], [5], [16], [17]. Now, the AKLT state can be deformed into a one-parameter family of quantum states such that for a sufficiently strong deformation in one direction, the state transitions from the valence-bond phase into the Néel-ordered phase [18]. It has been numerically demonstrated that along this line of deformed states, the transition of computational power coincides with the physical phase transition [19], [20].

These findings have led to the notion of “computational phases of quantum matter”, which represents an intriguing connection between condensed matter physics and quantum computation.

Here, we further corroborate the above conjecture through the following result. In spatial dimension one, if an SPTO phase supports quantum wire, then, subject to an additional symmetry condition which is satisfied in all cases so far investigated, it can also be used for quantum computation. This result, given as Theorem 2 in Section II, is a strengthening of both [12] and [13]. Namely, it promotes the result [12] from quantum wire to quantum computation. Further, it shows that computational universality in one-dimensional symmetry-protected topologically ordered systems does not only occur for one particular symmetry group [13], but rather is an ubiquitous phenomenon.

The main technical contribution of this paper is a method for carrying out MBQCs suited to resource states in SPT ordered phases, namely the incoherent addition of computational paths. It leads to a number of computational primitives, the first of which is the “oblivious wire” described in Section III C. Oblivious wire is the basis for performing unitary gates (Section IV) and projective measurements (Section V) on the virtual space of the MPS description. It is a counterpart of “buffering” described in [13]. Its main advantage is that it can be applied in every SPTO phase that has a basis for quantum wire.

It should be noted at this point that an MBQC resource state laid out in spatial dimension \mathcal{D} leads to the simulation of a quantum circuit in spatial dimension

$\mathcal{D} - 1$, and hence in $\mathcal{D} = 1$ only a single logical qudit is evolved. The cases of dimension $\mathcal{D} \geq 2$ are therefore of greater practical interest. However, numerous technical aspects are easier to handle in dimension one, and this case can therefore serve as a testing ground for novel computational techniques.

Besides corroborating the notion of “computational phases of matter”, there is a second motivation for the present work. It is the prospect of classifying MBQC schemes by symmetry.

If Conjecture 1 is true, not only are universal resource states easy to come by in the symmetry-protected case, but also, computational power becomes a property of a whole quantum phase as opposed to individual quantum states. Moreover, quantum phases have a succinct mathematical characterization in SPTO, namely, in $\mathcal{D} = 1$, every such phase is uniquely specified by the symmetry group G and an element in the second cohomology group $H^2(G, U(1))$ of G . If Conjecture 1 holds, the computational power of the corresponding MBQC scheme is characterized by the same mathematical objects, giving rise to a classification of MBQC schemes by symmetry.

II. STATEMENT OF THE PROBLEM AND THE RESULT

A. Starting point and problem

We consider symmetry protected topological phases with a unique ground state, in one spatial dimension. Be $|\Phi\rangle$ a ground state in such a phase, given in matrix product form

$$|\Phi\rangle = \kappa(n) \sum_{i_1, \dots, i_n} \langle R | A[i_n] \cdot \dots \cdot A[i_1] | L \rangle |i_1, \dots, i_n\rangle, \quad (1)$$

where $\kappa(n)$ is a normalization constant, and the $A[i]$, $i = 1, \dots, d$ are $D_b \times D_b$ matrices. Therein, d is the Hilbert space dimension of the local physical system, and D_b is the bond dimension, i.e., the dimension of the virtual system.

Uniqueness of the ground state requires that the corresponding MPS tensors $A[i]$ satisfy the injectivity condition [21]. That is, possibly after blocking K consecutive sites, the MPS tensors $A[\mathbf{i}] := \prod_{k=1}^K A[i_k]$ span the space of $D_b \times D_b$ matrices.

Measurement-based quantum computation may be run on the states Eq. (1) as usual; i.e., the simulated gates are chosen by the local measurement bases, taking into account previous measurement outcomes.

Among all the local bases in which the physical degrees of freedom can be measured, there is, for suitable SPTO phases, a special one, namely the so-called wire basis.

Definition 1 *A wire basis is an orthonormal basis (ONB) $\mathcal{B} = \{|0\rangle, \dots, |d-1\rangle\}$ of the physical system such that the matrices $A[i]$ factorize into a logical part C_i and*

a junk part B_i ,

$$A[i] = C_i \otimes B_i, \quad (2)$$

where the C_i are all unitary and constant across the phase.

The significance of the wire basis is that it leads to wire protected by the symmetry throughout the SPTO phase. Specifically, the following result has been established.

Theorem 1 [12]. *Consider a symmetry-protected phase characterized by a finite Abelian group and a maximally non-commutative cohomology class $[\omega]$. Then, for every MPS in this phase there exists a wire basis w.r.t. which the MPS tensor A has the decomposition Eq. (2). The unitary byproduct operators C_i therein are elements of a finite group.*

Measurement of the physical degrees of freedom in the wire basis thus implements wire on the logical part of the virtual system. By virtue of Eq. (2), the tensors $A[i]$ never entangle the logical subsystem with the uncontrolled junk subsystem, and thus preserve the logical information.

Now we turn to the problem: Since the byproduct operators C_i generate a finite group, the above construction does not achieve universal quantum computation on the logical subsystem. There is no immediate fix for this. For example, if the wire basis is perturbed to implement a continuous set of operations, with respect to the new bases $\{|i'\rangle\}$ the tensors A no longer satisfy the factorization property Eq. (2), $A[i'] \neq C_{i'} \otimes B_{i'}$. In result, the logical subsystem becomes entangled with the junk subsystem under measurement in such bases, and quantum information is lost. Thus, the following question arises: “Can quantum wire [12] for the logical subsystem be promoted to universal quantum computation?”.

The present paper gives an affirmative answer to this question. We point out that the desired extension from wire to computation is already known for one specific SPTO phase of one symmetry group, S_4 [13]. The present solution is widely applicable. It only assumes the existence of a wire basis in the considered SPTO phase, and a symmetry condition to be explained below.

B. Result

To state our result, we need to make two more definitions. We first capture the notion of “uniformity of computational power” of a physical phase.

Definition 2 *A given physical phase has uniform computational power X with respect to MBQC if all states in this phase, with the possible exception of a set of measure zero, have computational power X .*

The finite set of logical byproduct operators C_i appearing in the decomposition Eq. (2) will be used to realize

a continuous set of quantum gates in MBQC, acting on the logical part of the virtual space.

Definition 3 \mathcal{O} is the set of Hermitian operators

$$\frac{C_i^{-1}C_j + C_j^{-1}C_i}{2}, \frac{C_i^{-1}C_j - C_j^{-1}C_i}{2i}, \quad (3)$$

for all $0 \leq i < j \leq d-1$. $\mathcal{A}(\mathcal{O})$ the algebra generated by the operators in \mathcal{O} under $[\cdot, \cdot]/i$ and linear combination with real coefficients, and $L(\mathcal{O}) = \exp(i\mathcal{A}(\mathcal{O}))$ is the Lie group generated by $\mathcal{A}(\mathcal{O})$.

Returning to the symmetric MPS state $|\Phi\rangle$ described in Eq. (1), if injectivity holds then the tensor A has the symmetry

$$V(g)^\dagger A[|\psi\rangle] V(g) = A[u(g)|\psi\rangle], \quad \forall g \in G, \quad (4)$$

where $V(g)$ is some projective representation of the symmetry group G acting on the virtual system and $u(g)$ is a unitary representation of G acting on the physical degrees of freedom [8], [10].

With these definitions and observations, we can now state our main result.

Theorem 2 Consider a symmetry-protected phase of a group G with the properties (i) the ground state is unique, (ii) there is a wire basis, and (iii) for all $i = 0, \dots, d-1$ exists a $g \in G$ such that $C_i \otimes I = V(g)$. Then, this SPTO phase has the uniform computational power to execute MBQC simulations of the unitary gates $L(\mathcal{O})$ and the projective measurements of all observables in \mathcal{O} , with arbitrary accuracy.

Remark: The symmetry condition, $C_i \otimes I \in V(G)$, for all $i = 0, \dots, d-1$, ensures that the randomness of measurement can be accounted for in MBQC in the standard fashion [1]. However, there exist other ways of accounting for this randomness in MBQC [22],[23], and the symmetry condition in Theorem 2 may therefore be unnecessarily stringent. On the other hand, it is satisfied in all SPTO phases with a wire basis so far encountered.

In a companion paper [24], we describe how the MBQC-simulable Lie group $L(\mathcal{O})$ of unitary gates is determined by the characteristics of the SPTO phase in which the resource state lives.

III. STRATEGY FOR TURNING WIRE INTO COMPUTATION

A. Computational primitives

The extension from quantum wire to logical gates proceeds in several steps. The key technical ingredient is the “incoherent addition of computational paths”. A computational path is simply the measurement record \mathbf{s} obtained in an individual run of the given MBQC. “Addition of paths” means that, after correcting/ accounting

for the outcome-dependent byproduct operator (which always arises in MBQC), the measurement record is discarded, and multiple computational paths are combined. For interpretation of this procedure, see Section III D.

The first application of adding computational paths is the “oblivious wire” described in Section III C. It provides the capacity to drive any state of the virtual system into a tensor product state $\sigma \otimes \rho_{\text{fix}}$ between the logical and the junk subsystem. In particular, the junk system ends up in the same fixed point state ρ_{fix} every time the oblivious wire is applied. The oblivious wire thus provides a means of conditioning the junk subsystem, which turns out to be of importance for implementing quantum gates. In the present construction, oblivious wire is the counterpart to the buffering technique employed in [13]. In contrast to buffering, oblivious wire requires no trial-until-success.

The oblivious wire leads to three computational primitives, namely (i) the preparation of the virtual system in a tensor product state between the logical and the junk subsystem, (ii) unitary gates on the logical subsystem, and (iii) measurement of the logical subsystem. The latter can also be used for initialization. These three computational primitives are described in Sections III C, IV and V, respectively.

B. Boundary conditions

The oblivious wire, the computational primitives, and the composition of these primitives are intertwined matters. In order to discuss them one after the other rather than everything all at once, we apply a technical trick. Namely, we temporarily change the matrix-product representation of the resource state at the right boundary; See Fig. 1. Specifically, we add a physical degree of freedom at the right boundary, whose dimension equals the dimension of the virtual system. The resulting state $|\tilde{\Phi}\rangle$ has the matrix product representation

$$|\tilde{\Phi}\rangle = \kappa(n) \sum_{i_1, \dots, i_n} A[i_n] \cdot \dots \cdot A[i_1] |L\rangle \otimes |i_1, \dots, i_n\rangle. \quad (5)$$

Physically, this means that MBQC on $|\tilde{\Phi}\rangle$ can be run as a state preparator, in which the output state is mapped from the virtual system to the physical system at the right boundary. From a practical perspective, the need for a physical system of potentially high dimension on the right boundary is unappealing, since it places additional and unnecessary requirements on the experimental setup.

However, we emphasize that the change of boundary conditions from Eq. (1) to Eq. (5) is employed here only as a tool for reasoning, and it is temporary. We revert to the original boundary conditions of the resource state $|\Phi\rangle$ of Eq. (1) in the very last step of the argument; See Section VI. Our main result, Theorem 2, applies to the standard boundary conditions of Eq. (1).

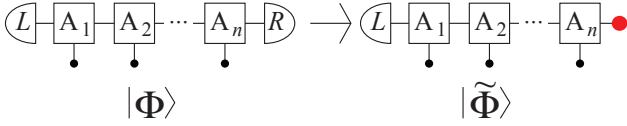


FIG. 1: Boundary conditions of the resource states $|\Phi\rangle$ and $|\tilde{\Phi}\rangle$. $|\tilde{\Phi}\rangle$ has an additional degree of freedom on its right boundary whose number of states is equal to the bond dimension D_b .

C. Oblivious wire

The first computational tool to be established is the “oblivious wire”, which prepares the virtual system in a tensor product state between logical and junk subsystem, and drives the junk system towards a fixed point state. Below, we discuss three procedures of implementing wire, which are minor modifications of another. The first is the MBQC wire proper, and the third is the “oblivious wire”, the procedure of our interest.

Procedure I: All measurement outcomes are fully remembered. All spins are measured in the wire basis, with outcomes s_1, \dots, s_n . The only unmeasured system then is the right boundary, and it is in the state

$$|R\rangle = \Sigma(\mathbf{s}) \otimes \left(\prod_{k=1}^n B_{s_k} \right) |L\rangle.$$

Therein, the first tensor factor is for the logical and the second tensor factor for the junk subsystem. $\Sigma(\mathbf{s})$ is the cumulative byproduct operator on the logical system, depending on the set \mathbf{s} of measurement outcomes,

$$\Sigma(\mathbf{s}) = \prod_{k=1}^n C_{s_k}. \quad (6)$$

So, the action on the logical system is that of the identity modulo a byproduct operator, all across the given physical phase.

Procedure II: The spins 1 to n are measured as before. But then, in addition, the outcome-dependent byproduct operator $\Sigma(\mathbf{s})$ is reversed on the right boundary system by applying its inverse. That is, the total action on the state $|\tilde{\Phi}\rangle$ is $|\mathbf{s}\rangle\langle\mathbf{s}| \otimes \Sigma(\mathbf{s})^{-1}$, where $|\mathbf{s}\rangle := \bigotimes_i |s_i\rangle$. This evolution puts the right boundary system in the state

$$|R\rangle = I \otimes \left(\prod_{k=1}^n B_{s_k} \right) |L\rangle,$$

for all sets \mathbf{s} of measurement outcomes. This is now an exact wire on the logical system.

Procedure III: Procedure II is run, and then outcomes \mathbf{s} are subsequently discarded.

What is being implemented on the state $|\tilde{\Phi}\rangle$ in Procedure III is the quantum channel with Kraus operators

$$P_{\mathbf{s}} = |\mathbf{s}\rangle\langle\mathbf{s}| \otimes \Sigma(\mathbf{s})^{-1}. \quad (7)$$

Here, the first tensor factor is for all the physical spins in the chain, and the second tensor factor is for the additional physical degree of freedom located on the right boundary. It is easily verified that $\sum_{\mathbf{s}} P_{\mathbf{s}}^\dagger P_{\mathbf{s}} = I$, as required for a POVM. The resulting quantum state of the right boundary system is

$$\begin{aligned} \tau_R &= \text{Tr}_{1, \dots, n} \sum_{\mathbf{s}} (|\mathbf{s}\rangle\langle\mathbf{s}| \otimes \Sigma(\mathbf{s})^{-1}) |\tilde{\Phi}\rangle\langle\tilde{\Phi}| (|\mathbf{s}\rangle\langle\mathbf{s}| \otimes \Sigma(\mathbf{s})) \\ &= \sum_{\mathbf{s}} \Sigma(\mathbf{s})^{-1} \langle\mathbf{s}|\tilde{\Phi}\rangle\langle\tilde{\Phi}|\mathbf{s}\rangle \Sigma(\mathbf{s}) \end{aligned} \quad (8)$$

With Eq. (5) we thus have

$$\tau_R = |\kappa(n)|^2 \sum_{\mathbf{s}} I \otimes \left(\prod_{k=1}^n B_{s_k} \right) |L\rangle\langle L| I \otimes \left(\prod_{l=n}^1 B_{s_l}^\dagger \right). \quad (9)$$

We may rewrite this in a simpler form,

$$\tau_R = |\kappa(n)|^2 I \otimes \mathcal{L}^n(|L\rangle\langle L|), \quad (10)$$

where \mathcal{L}^n denotes the n -fold iteration of \mathcal{L} , $\mathcal{L}^n = \underbrace{\mathcal{L} \circ \mathcal{L} \circ \dots \circ \mathcal{L}}_{n \text{ times}}$, and the channel \mathcal{L} is

$$\mathcal{L}(\rho) = \sum_{i=0}^{d-1} B_i \rho B_i^\dagger. \quad (11)$$

By our assumption of uniqueness of the SPTO ground state, the tensors $\{A[i]\}$ satisfy the injectivity condition; See [8],[10]. Then, the matrices $\{B_i\}$ also satisfy injectivity, and the fixed point of the channel \mathcal{L} of Eq. (11) is therefore unique [21].

By adjusting the factor $\kappa(n)$ in Eqs. (1), (5), the normalization for the channel \mathcal{L} may always be chosen such that the largest eigenvalue λ_0 of \mathcal{L} is

$$\lambda_0 = 1. \quad (12)$$

We adopt this convention in the following. The correlation length ξ of the states $|\Phi\rangle, |\tilde{\Phi}\rangle$ is then given by λ_1 , the second-largest eigenvalue of \mathcal{L} , $\xi := -1/\ln \lambda_1$. The unique fixed point of \mathcal{L} is closely approximated after n -fold iteration of the channel \mathcal{L} if $n/\xi \gg 1$,

$$\mathcal{L}^n(\rho) \approx \nu_\rho \rho_{\text{fix}}, \quad (13)$$

with $\nu_\rho \in \mathbb{R}_+$, for all states ρ of the junk system. Therefore, if the virtual system is in a tensor product state $\sigma \otimes \rho$ between the logical and the junk subsystem prior to the action of a channel $I \otimes \mathcal{L}^n$, then the state afterwards is $\sim \sigma \otimes \rho_{\text{fix}}$. Thus, the tensor product structure of the state of the virtual system is preserved, and the junk part is driven towards a unique Hermitian fixed point state ρ_{fix} . This is an important computational ingredient which will be employed in the implementation of unitary gates and measurement.

In addition, even if the joint state between junk and the logical subsystems does not factorize initially, after the application of the oblivious wire it does.

Lemma 1 Consider a channel \mathcal{L} of Eq. (11) derived from an injective resource state $|\Phi\rangle$ of Eq. (1), with left boundary state $|L\rangle$. For any such state it holds that

$$\lim_{n \rightarrow \infty} I \otimes \mathcal{L}^n(|L\rangle\langle L|) = \sigma \otimes \rho_{\text{fix}}, \quad (14)$$

for some Hermitian operator σ depending on $|L\rangle$. Further, $\sigma \otimes \rho_{\text{fix}}$ is positive semidefinite.

Proof of Lemma 1. The channel \mathcal{L} has the following two properties. First, it is a linear map,

$$\mathcal{L}(cA + dB) = c\mathcal{L}(A) + d\mathcal{L}(B), \quad \forall c, d \in \mathbb{C}. \quad (15)$$

Second, under the condition of injectivity it holds that

$$\lim_{n \rightarrow \infty} \mathcal{L}^n(X) = \nu_X \rho_{\text{fix}}, \quad (16)$$

with $\nu_X \in \mathbb{C}$, for all operators X [21] (also see [25]; Sec. 8.2).

We may now write the state $|L\rangle$ of the left boundary in its Schmidt decomposition between the logical and the junk system, $|L\rangle = \sum_j \sqrt{\lambda_j} |\phi_j\rangle \otimes |\psi_j\rangle$, where $\{|\phi_j\rangle\}$, $\{|\psi_j\rangle\}$ are ONBs of the logical and the junk system, respectively, and $\{\lambda_j\}$ are the non-zero eigenvalues of the reduced density matrix. Correspondingly, $|L\rangle\langle L| = \sum_{i,j} \sqrt{\lambda_i \lambda_j^*} |\phi_i\rangle\langle\phi_j| \otimes |\psi_i\rangle\langle\psi_j|$. We thus have

$$\begin{aligned} \lim_{n \rightarrow \infty} I \otimes \mathcal{L}^n(|L\rangle\langle L|) &= \\ &= \sum_{ij} \sqrt{\lambda_i \lambda_j^*} |\phi_i\rangle\langle\phi_j| \lim_{n \rightarrow \infty} \otimes \mathcal{L}^n(|\psi_i\rangle\langle\psi_j|) \\ &= \left[\sum_{ij} \sqrt{\lambda_i \lambda_j^*} \nu(n)_{|\psi_i\rangle\langle\psi_j|} |\phi_i\rangle\langle\phi_j| \right] \otimes \rho_{\text{fix}} \\ &= \sigma \otimes \rho_{\text{fix}} \end{aligned}$$

Therein, we used linearity Eq. (15) in the first line, and Eq. (16) in the second line.

Further, with Eq. (11), $\mathcal{L}(X^\dagger) = (\mathcal{L}(X))^\dagger$, $\forall X$, and thus with Eq. (16) it follows that $\nu_{X^\dagger} = \nu_X^*$. Hence σ is Hermitian. Finally, since \mathcal{L} is completely positive and $|L\rangle\langle L|$ is positive semidefinite, so is $\sigma \otimes \rho_{\text{fix}}$. \square

Thus, we obtain

Computational primitive 1 The virtual system can be prepared in a tensor product state $\tau = \sigma \otimes \rho_{\text{fix}}$, where the junk system is in a defined fixed point state ρ_{fix} .

D. Interpretation of “adding computational paths”

In the oblivious wire construction—Procedure III in Section III C—we have added computational paths corresponding to different measurement records \mathbf{s} by “forgetting” those measurement records (after correction for the byproduct operators $\Sigma(\mathbf{s})$). The purpose of this section

is to clarify that “forgetting” of this classical information is a meaningful operation.

The simplest way to justify the notion of “forgetting information” is to consider a distributed scenario for computation, involving two parties. In this scenario, the primary party, Alice, does not need to forget classical information, but never learns it in the first place.

Suppose, the above Procedure III is outsourced by Alice, the computing party, to some subcontractor Bob. The protocol between Alice and Bob is as follows. (i) Alice sends Bob the state $|\tilde{\Phi}\rangle$, (ii) Bob implements Procedure II, (iii) Bob sends back the right boundary system (which is a physical particle, since $|\tilde{\Phi}\rangle$ has been used instead of $|\Phi\rangle$). Bob does not say which measurement outcomes he obtained, and discards the measured spins (they are being traced over, from Alice’s perspective).

How is Alice supposed to represent the quantum state of the right boundary system that she receives from Bob?—Since Alice has no information about the measurement outcomes obtained by Bob, from her perspective, the operation implemented by Bob is the channel with Kraus operators Eq. (7), leading to the state τ of the right boundary system given in Eq. (10).

However, in the intended computational scenario there is no second party. Rather, a single party is executing the computation in her lab. An interpretation for adding computational paths applicable to the one-party setting is given in Appendix A.

IV. UNITARY GATES

Next we show how to implement a single unitary about an infinitesimal rotation angle $d\alpha$ by measurement of the leftmost qudit in the chain, assuming the junk system is already in its fixed point state ρ_{fix} . For this purpose, we change slightly the computational setting from the previous section. The resource state is now mixed, and its mixedness comes from a mixed state in the left boundary condition. Namely, we consider the resource state of $n+1$ spins plus the right boundary system

$$\tilde{\Phi}_{\text{fix}}(\sigma) = |\kappa(n)|^2 \sum_{\mathbf{i}, \mathbf{j}} (A[\mathbf{i}] (\sigma \otimes \rho_{\text{fix}}) A[\mathbf{j}]^\dagger) \otimes |\mathbf{i}\rangle\langle\mathbf{j}|, \quad (17)$$

where $A[\mathbf{i}] := A[i_{n+1}] \cdots A[i_1]$.

A. Rotations about small angles

To perform a rotation about an infinitesimal angle, we measure the first spin in a basis which slightly deviates from the basis that implements the wire, namely $\mathcal{B}(d\alpha) = \{|0'\rangle, |1'\rangle, |2\rangle, \dots, |m-1\rangle\}$, where

$$\begin{aligned} |0'\rangle &= |0\rangle + d\alpha |1\rangle, \\ |1'\rangle &= |1\rangle - d\alpha |0\rangle, \end{aligned} \quad (18)$$

where $d\alpha \in \mathbb{R}$. The remaining n spins are measured in the wire basis, and the measurement outcomes are forgotten as soon as the accumulated byproduct operator $\Sigma(\mathbf{s})$ are reversed on the right boundary, including the byproduct operator caused by the measurement of the first particle in the basis Eq. (18).

In complete analogy with Eq. (9), the effect of the measurements and byproduct operator reversion can be described on the level of the virtual system,

$$\sigma \otimes \rho_{\text{fix}} \longrightarrow \mathcal{T}_{s_1}(\sigma \otimes \rho_{\text{fix}}), \quad (19)$$

where \mathcal{T}_{s_1} is the channel on the virtual system induced by the measurement of the first spin, with outcome s_1 , followed by an oblivious wire \mathcal{L}^n . We now investigate the channels \mathcal{T}_{s_1} .

First, assume the outcome of the measurement is $0'$. The corresponding matrix $A[0']$ acting on the correlation space is $A[0'] = A[0] + d\alpha A[1] = C_0(I \otimes B_0 + d\alpha C_0^{-1}C_1 \otimes B_1)$. Henceforth, we denote

$$C_0^{-1}C_1 =: C.$$

Given a left boundary state that is factorized between logical system and junk system, $\sigma \otimes \rho_{\text{fix}}$, with the junk system in its fixed point state, the effect of the measurement of the first spin on the correlation system is, up to leading order in $d\alpha$,

$$\begin{aligned} \sigma \otimes \rho_{\text{fix}} &\longrightarrow \sigma \otimes B_0 \rho_{\text{fix}} B_0^\dagger + \\ &+ d\alpha \left(C \sigma \otimes B_1 \rho_{\text{fix}} B_0^\dagger + \sigma C^\dagger \otimes B_0 \rho_{\text{fix}} B_1^\dagger \right). \end{aligned}$$

We now follow up with an oblivious channel \mathcal{L}^n , such that the junk system is back to its fixed point state. To describe the resulting state of the virtual system, it is useful to define the parameters $\nu_{ij} \in \mathbb{C}$ via

$$\lim_{n \rightarrow \infty} \mathcal{L}^n(B_i \rho_{\text{fix}} B_j^\dagger) = \nu_{ij} \rho_{\text{fix}}, \quad (20)$$

for all $i, j = 0, \dots, d-1$. Since ρ_{fix} is Hermitian and $(\mathcal{L}(X))^\dagger = \mathcal{L}(X^\dagger)$ for all X , we have

$$\nu_{ij}^* = \nu_{ji}, \quad \forall i, j. \quad (21)$$

Furthermore, with Eq. (12) it follows that

$$\sum_{i=0}^{d-1} \nu_{ii} = 1. \quad (22)$$

Now, the combined action of the measurement with outcome $0'$ and a subsequent oblivious channel is $\sigma \otimes \rho_{\text{fix}} \longrightarrow \mathcal{T}_0(\sigma \otimes \rho_{\text{fix}})$, with

$$\mathcal{T}_0(\sigma \otimes \rho_{\text{fix}}) = \nu_{00} \sigma \otimes \rho_{\text{fix}} + d\alpha (\nu_{10} C \sigma + \nu_{01} \sigma C^\dagger) \otimes \rho_{\text{fix}}.$$

Thus, we are back to a disentangled logical subsystem, which was the goal.

Let us now examine which transformation was enacted on the logical system. For this purpose, we may split the

term $\sim d\alpha$ in the above expression for the channel \mathcal{T}_0 into a commutator and an anti-commutator part,

$$\begin{aligned} \mathcal{T}_0(\sigma \otimes \rho_{\text{fix}}) &= \nu_{00} \sigma \otimes \rho_{\text{fix}} + \\ &+ \frac{d\alpha}{2} [\nu_{10} C - \nu_{10}^* C^\dagger, \sigma] \otimes \rho_{\text{fix}} + \\ &+ \frac{d\alpha}{2} \{ \nu_{10} C + \nu_{10}^* C^\dagger, \sigma \} \otimes \rho_{\text{fix}}. \end{aligned}$$

The commutator term generates unitary evolution and is thus desirable, while the anti-commutator term generates non-unitary stretching which is undesirable. In general, both parts are present.

We now repeat the above calculation for the outcome $1'$. After reversal of all byproduct operators on the right boundary system, the action on the left boundary condition now is $|L\rangle \longrightarrow (I \otimes B_1 - d\alpha C^\dagger \otimes B_0) |L\rangle$. This holds because $C_1^{-1}C_0 = C^{-1} = C^\dagger$, which is a consequence of the fact that all byproduct operators in the wire basis are unitary, by assumption. We find that $\sigma \otimes \rho_{\text{fix}} \longrightarrow \mathcal{T}_1(\sigma \otimes \rho_{\text{fix}})$, with

$$\mathcal{T}_1(\sigma \otimes \rho_{\text{fix}}) = \nu_{11} \sigma \otimes \rho_{\text{fix}} - d\alpha (\nu_{01} C^\dagger \sigma + \nu_{10} \sigma C) \otimes \rho_{\text{fix}}.$$

Again, the linear order in $d\alpha$ has a unitary commutator part and a non-unitary anti-commutator part. Expanding the above expression,

$$\begin{aligned} \mathcal{T}_1(\sigma \otimes \rho_{\text{fix}}) &= \nu_{11} \sigma \otimes \rho_{\text{fix}} + \\ &+ \frac{d\alpha}{2} [\nu_{10} C - \nu_{10}^* C^\dagger, \sigma] \otimes \rho_{\text{fix}} + \\ &- \frac{d\alpha}{2} \{ \nu_{10} C + \nu_{10}^* C^\dagger, \sigma \} \otimes \rho_{\text{fix}}. \end{aligned}$$

Comparing the expressions for the action of the channels \mathcal{T}_0 and \mathcal{T}_1 , we find that they have the same commutator part, with the same sign, and the same anti-commutator part, with opposite sign. Thus, upon adding the two channels \mathcal{T}_0 and \mathcal{T}_1 , the anti-commutator part vanishes, and the evolution of the logical subsystem becomes purely unitary, up to linear order in $d\alpha$,

$$\begin{aligned} \mathcal{T}_0 + \mathcal{T}_1 : \sigma \otimes \rho_{\text{fix}} &\longrightarrow (\nu_{00} + \nu_{11}) \sigma \otimes \rho_{\text{fix}} + \\ &d\alpha [\nu_{10} C - \nu_{10}^* C^\dagger, \sigma] \otimes \rho_{\text{fix}}. \end{aligned} \quad (23)$$

Up to the norm factor $\nu_{00} + \nu_{11}$ this is now a unitary gate $U(d\alpha)$ with rotation angle $\sim d\alpha$,

$$U(d\alpha) = \exp \left(i d\alpha \frac{\nu_{10} C - \nu_{10}^* C^\dagger}{i(\nu_{00} + \nu_{11})} \right), \quad (24)$$

conditioned upon the measurement outcome 0 or 1 being obtained.

As discussed in Section III D, “adding together” of the two channels \mathcal{T}_0 and \mathcal{T}_1 means that, if the measurement outcome s_1 was either 0 or 1, after the correction of the byproduct operator, the outcome is discarded, i.e. no longer available for any further processing. It is only remembered that one of 0 or 1 occurred.

The reason for conditioning the junk system is now clearly visible. We have a reliable procedure for driving the junk system into a fixed point state ρ_{fix} . The state ρ_{fix} , and even the dimension of the Hilbert space it lives in, are a priori unknown. But that doesn't matter. All that needs to be known about ρ_{fix} are the $d(d-1)/2$ parameters ν_{ij} , $j \geq i$. Those parameters can be measured.

The gate of Eq. (23) is probabilistic but heralded. It simplifies our discussion to convert it into a deterministic gate, at the cost of reducing the rotation angle. This proceeds by adding in the channels \mathcal{T}_i , $i = 2, \dots, d-1$. Individually, any such \mathcal{T}_i acts as $\mathcal{T}_i : \sigma \rightarrow \nu_{ii}\sigma$. And thus the net effect is that in Eq. (23) $\nu_{00} + \nu_{11}$ in the rotation angle is replaced by $\sum_{i=0}^{d-1} \nu_{ii} = 1$, i.e. the rotation angle is reduced.

It may seem counter-intuitive that a probabilistic mixture of two unitaries should be a unitary. Yet, clearly there is no problem with this statement if the two unitaries are the same. Here, one of the two unitaries is the identity, and one is very close to the identity, deviating to linear order in $d\alpha$. The probabilistic mixture of the two is indeed not exactly unitary, but the difference shows up only to quadratic order in $d\alpha$, which we can discard in the present discussion.

We now redo the above calculation for a continuous set of measurement bases $\tilde{\mathcal{B}}(d\alpha, \beta)$, with

$$\begin{aligned} |0(\beta)\rangle &= |0\rangle + d\alpha e^{i\beta} |1\rangle, \\ |1(\beta)\rangle &= |1\rangle - d\alpha e^{-i\beta} |0\rangle, \end{aligned} \quad (25)$$

and $d\alpha, \beta \in \mathbb{R}$. We find that we can now realize the operations

$$U(d\alpha, \beta) = \exp \left(i d\alpha |\nu_{10}\rangle \frac{(e^{-i(\beta+\delta)} C - e^{i(\beta+\delta)} C^\dagger)}{i} \right), \quad (26)$$

where $\nu_{10} = |\nu_{10}| e^{-i\delta}$.

B. Composition

We have so far shown how to implement a single unitary gate with small rotation angle. To accumulate finite rotation angles, MBQC-gate simulations need to be composable. That is, we require that if the gates T and T' can individually be executed by the MBQC, then so can their compositions TT' and $T'T$.

The key, as usual in MBQC, is that the randomness of measurement resulting in the byproduct operators can be counter-acted by the adjustment of measurement bases. If all byproduct operators $C_i \otimes I$ are elements of a projective representation $V(G)$ of the symmetry group G , acting on the logical part of the virtual system only, then byproduct operators can be propagated through the

chain by virtue of the symmetry relation

$$C_i \otimes I - \boxed{\text{A}} - = - \boxed{\text{A}} - C_i \otimes I. \quad (27)$$

u_i

Therein, u_i is in a unitary representation $U(G)$ of G , acting on the physical degrees of freedom. This situation ($C_i \in V(G)$, $\forall i$) applies, for example, to maximally non-commuting factor systems of Abelian groups [12].

Denote by $A(s, \beta)$ the MPS tensor representing the action on the virtual space caused by the measurement of a physical degree of freedom in the basis $\tilde{\mathcal{B}}(d\alpha, \beta)$ of Eq. (25), with outcome s . Further, denote by $A(\mathbf{s}, s, \beta) := (C(\mathbf{s}) \otimes I) A(s, \beta) (C(\mathbf{s})^\dagger \otimes I)$ the MPS tensor obtained from $A(s, \beta)$ by conjugating under a byproduct operator $C(\mathbf{s}) \otimes I$. With Eq. (27), for all \mathbf{s} and all measurement angles β , there is a measurement basis $\mathcal{B}(\beta'(\mathbf{s}))$ such that

$$A(\mathbf{s}, s, \beta) = A(s, \beta'(\mathbf{s})). \quad (28)$$

Hence, $A(\mathbf{s}, s, \beta)$ can be implemented.

Now recall that $\sum_s [A(s, \beta)]$ followed by oblivious wire \mathcal{L}^n implements a channel $T(\beta)$ on states $\sigma_L \otimes \rho_{\text{fix}}$. $\sum_s [A(\mathbf{s}, s, \beta)]$ followed by oblivious wire \mathcal{L}^n thus implements a channel

$$T(\beta'(\mathbf{s})) = C(\mathbf{s}) T(\beta) C(\mathbf{s})^\dagger \quad (29)$$

on this set of states.

Lemma 2 Consider an injective MPS state $|\tilde{\Phi}\rangle$ of Eq. (5) whose MPS tensors factorize w.r.t. a wire basis, $A[i] = B_i \otimes C_i$, and for all $i = 0, \dots, d-1$ exists a $g \in G$ such that $C_i \otimes I = V(g)$. If two transformations $T(\alpha)$, $T'(\beta)$ can be implemented on $|\tilde{\Phi}\rangle$ then so can their composition $T'(\beta)T(\alpha)$.

The proof of Lemma 2 is given in Appendix B.

C. Rotations about finite angles

With Lemma 2, we have so far established that we can execute all unitary gates of form Eq. (26), but with finite rotation angles α replacing the infinitesimal angles $d\alpha$.

Of course, there is nothing special in the choice of the basis elements 0 and 1 in the definition of $C := C_0^{-1} C_1$ leading to Eq. (26). We may replace the labels 0 and 1 by i and j , $0 \leq i, j \neq i \leq d-1$, giving rise to different operators $C = C_i^{-1} C_j$. This observation motivates Definition 3 in Section II.

We have the following result.

Lemma 3 Consider a symmetry-protected phase of a group G with the properties (i) the ground state is unique, (ii) there is a wire basis, and (iii) the byproduct operators C_i are in a projective representation of G , $C_i \otimes I \in V(G)$.

Then, for all resource states $|\tilde{\Phi}\rangle$ of Eq. (5) derived from MPS ground states Eq. (1) in that phase, except a possible subset of measure zero, the unitary gates in $L(\mathcal{O})$ can be arbitrarily closely approximated.

Proof of Lemma 3. Whenever $\nu_{ij} \neq 0$, $\forall i, j = 0, \dots, d-1$, all infinitesimal unitary gates in $L(\mathcal{O})$ can be executed. Then, since the ground state is unique all across the SPTO phase, MPS ground states are injective [8], [10], and Lemma 2 applies. Thus, with $\exp(i d\alpha A) \exp(i d\beta B) \approx \exp(i d\alpha A + i d\beta B)$, for all $A, B \in \mathcal{O}$, all rotations generated by linear combinations of observables in \mathcal{O} can be realized. Furthermore, $\exp(i d\alpha A) \exp(i d\alpha B) \exp(-i d\alpha A) \exp(-i d\alpha B) \approx \exp((d\alpha)^2 [A, B])$, thus rotations generated by any element in $\mathcal{A}(\mathcal{O})$ can be realized, and hence all rotations in $L(\mathcal{O})$.

A value of $\nu_{ij} = 0$, for some $i \neq j$, requires fine-tuning in the phase and thus only occurs for a set of states of measure zero. \square

Thus, whenever wire is protected by symmetry, then a large group of gates and set of measurements can also be carried out all across the SPTO phase. These gates are not protected in the same way as wire is, and they have to be executed in a fashion reminiscent of the Zeno effect. Namely, the measurement bases implementing unitary gates on the virtual system must always remain close to the wire basis, and finite rotation angles are accumulated over a large number of measurements.

We restate Lemma 3, without the conditions and qualifications, as the second computational primitive.

Computational primitive 2 *The logical part of the virtual system can be acted on by all unitary gates in $L(\mathcal{O})$.*

D. Operational cost of unitary evolution

In the above treatment of the unitary transformations, we have discarded terms of order $d\alpha^2$, and indeed, to quadratic order in $d\alpha$ deviations from unitarity arise. When finally composing gates, a rotation about a finite angle α is realized as a sequence of N rotations about an angle $d\alpha = \alpha/N$. The error for each such rotation is thus of order $1/N^2$, and hence the error of the combined procedure is of order $1/N$. Thus, the error of the approximation can be improved by increasing the number N of steps. An error ϵ_{gate} requires order $1/\epsilon_{\text{gate}}$ steps.

Now consider a computation that consists of n unitary gates and allows for a total error ϵ in them. The allowed error per gate then is $\epsilon_{\text{gate}} = \epsilon/n$, and hence the number of steps per gate is $\sim n/\epsilon$. Hence, the total number of steps is $\sim n^2/\epsilon$. This is a quadratic overhead compared to the sequence of n ideal gates, which is still efficient.

V. MEASUREMENT AND INITIALIZATION

We have so far employed measurement only of the right boundary system in the support of $|\tilde{\Phi}\rangle$. This is unsatisfactory, since the presence of the right boundary system is only a transitional feature. It is removed in the final construction, which employs the original resource state $|\Phi\rangle$ of Eq. (1). Here, we describe a procedure of measurement of the virtual system. It is independent of the choice of the right boundary condition.

A. Procedure for measurement

For measurement of the virtual system, computational paths are no longer added, except in the oblivious wire. Furthermore, we choose the measurement bases a finite angle α away from the wire basis, $\mathcal{B}(\alpha) = \{|0'\rangle, |1'\rangle, |m'\rangle = |k\rangle, k \geq 2\}$, with

$$\begin{aligned} |0'\rangle &= \cos \alpha |0\rangle + \sin \alpha |1\rangle, \\ |1'\rangle &= -\sin \alpha |0\rangle + \cos \alpha |1\rangle. \end{aligned} \quad (30)$$

If the measurement outcome is $0'$ the corresponding action on the virtual system is thus $A'[0] = \cos \alpha A[0] + \sin \alpha A[1] = C_0(\cos \alpha I \otimes B_0 + \sin \alpha C \otimes B_1)$. Thus, an initial state $\tau = \sigma \otimes \rho_{\text{fix}}$ transforms into

$$\begin{aligned} \tau \longrightarrow & \cos^2 \alpha C_0 \sigma C_0^\dagger \otimes B_0 \rho_{\text{fix}} B_0^\dagger + \\ & + \sin^2 \alpha C_1 \sigma C_1^\dagger \otimes B_1 \rho_{\text{fix}} B_1^\dagger + \\ & + \sin \alpha \cos \alpha C_0 \sigma C_0^\dagger \otimes B_0 \rho_{\text{fix}} B_1^\dagger + \\ & + \sin \alpha \cos \alpha C_0 C \sigma C_0^\dagger \otimes B_1 \rho_{\text{fix}} B_0^\dagger. \end{aligned}$$

We now follow up the first measurement in the basis $\mathcal{B}(\alpha)$ with an oblivious wire and undoing of the byproduct operator on the right boundary system. The action of this chain of operations on the virtual system is $T_0(\sigma \otimes \rho_{\text{fix}}) = T_0(\sigma) \otimes \rho_{\text{fix}}$, with

$$T_0(\sigma) = \cos^2 \alpha \nu_{00} \sigma + \sin \alpha \cos \alpha (\nu_{10} C \sigma + \nu_{10}^* \sigma C^\dagger) + \sin^2 \alpha \nu_{11} C \sigma C^\dagger. \quad (31)$$

First, for an eigenstate $|\phi_i\rangle$ of C , with $C|\phi_i\rangle = e^{i\phi_i}|\phi_i\rangle$, we find

$$T_0(|\phi_i\rangle\langle\phi_i|) = (\cos^2 \alpha \nu_{00} + \sin^2 \alpha \nu_{11} + |\nu_{10}| \sin 2\alpha \cos(\delta + \phi_i)) |\phi_i\rangle\langle\phi_i|, \quad (32)$$

where we have set $\nu_{10} = e^{i\delta}|\nu_{10}|$.

We now consider the state σ of the logical part of the virtual system in the eigenbasis \mathcal{B}_C of C , $\mathcal{B}_C = \{|\phi_i\rangle | C|\phi_i\rangle = e^{i\phi_i}|\phi_i\rangle\}$,

$$\sigma := \sum_{i,j} \sigma_{ij} |\phi_i\rangle\langle\phi_j|.$$

By the same argument as in Eq. (31) we find that, conditioned upon obtaining the outcome k in the measurement

basis $\mathcal{B}(\alpha)$ of Eq. (30), the expansion coefficients σ_{ij} of σ are updated as

$$\sigma_{ij} \longrightarrow \sigma'_{ij} = f_k(\phi_i, \phi_j) \sigma_{ij}. \quad (33)$$

We call the multipliers $f_k(\phi_i, \phi_j)$ filter functions, since they amplify or diminish some eigenstates over others. It suffices to consider the filter functions $f_k(\phi_i, \phi_i)$ multiplying the diagonal elements of σ . Those filter functions are

$$\begin{aligned} f_0(\phi_i, \phi_i) &= \nu_{00} \cos^2 \alpha + \nu_{11} \sin^2 \alpha + |\nu_{10}| \sin(2\alpha) \cos(\delta + \phi_i), \\ f_1(\phi_i, \phi_i) &= \nu_{00} \sin^2 \alpha + \nu_{11} \cos^2 \alpha - |\nu_{10}| \sin(2\alpha) \cos(\delta + \phi_i), \\ f_k(\phi_i, \phi_i) &= \nu_{kk}, \quad k \geq 2. \end{aligned} \quad (34)$$

Each measurement of a physical spin in the basis $\mathcal{B}(\alpha)$ thus amounts to a weak measurement of the logical part of the virtual system, in which some of the eigenstates of C are relatively boosted while others are diminished. In general no state is completely extinguished in a single measurement. As the filter functions accumulate, they dim out all values of $\cos \phi$ except an increasingly narrow band. In the limit of a large number of repetitions, a projective measurement is achieved. See Fig. 2 for illustration.

If in a sequence of measurements the outcome $0'$ is obtained N_0 times and the outcome $1'$ is obtained N_1 times, the accumulated filter function $F_{N_0, N_1}(\phi) = f_0(\phi, \phi)^{N_0} f_1(\phi, \phi)^{N_1}$ as a function of ϕ reaches its maximum at an angle ϕ_{\max} given by

$$\frac{f_0(\phi_{\max}, \phi_{\max})}{f_1(\phi_{\max}, \phi_{\max})} = \frac{N_0}{N_1}. \quad (35)$$

In the limit of large N_0, N_1 , the eigenvalue $e^{i\phi}$ of C with ϕ closest to ϕ_{\max} is the outcome of the measurement.

With Eq. (34), we obtain an estimate for ϕ from the outcome frequencies N_0, N_1 ,

$$\begin{aligned} \cos(\delta + \phi) &= \frac{\sin^2 \alpha (N_0 \nu_{00} - N_1 \nu_{11})}{\sin 2\alpha (N_0 + N_1) |\nu_{10}|} + \\ &+ \frac{\cos^2 \alpha (N_0 \nu_{11} - N_1 \nu_{00})}{\sin 2\alpha (N_0 + N_1) |\nu_{10}|}. \end{aligned} \quad (36)$$

The outcomes $k \geq 2$ of measurement in the basis $\mathcal{B}(\alpha)$ have no effect on the measurement of the virtual system.

Unitary evolution and measurement of the logical part of the virtual system are illustrated in Fig. 3. In panel (a), the changeover between unitary evolution and measurement is shown. To implement a unitary gate with rotation angle $\mathcal{O}(1)$ on the logical part of the virtual system, a large number of spins in the chain are measured slightly away from the wire basis, and the angle α specifying the measurement basis $\mathcal{B}(\alpha)$ is chosen $\sim 1/(N_0 + N_1)$. Unitarity on the virtual system is beginning to be violated around $\alpha = 1/\sqrt{N_0 + N_1}$. The measurement is

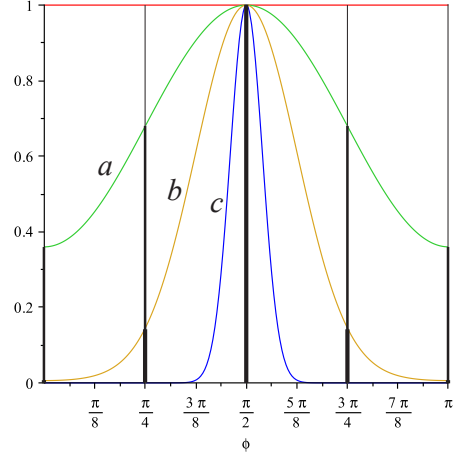


FIG. 2: Accumulated filter functions $f_0^{N_0} f_1^{N_1}$ (normalized). (a) $N_0 = N_1 = 1$, (b) $N_0 = N_1 = 5$, (c) $N_0 = N_1 = 50$. The parameters for this plot are $\nu_{00} = \nu_{11} = 1$, $\nu_{10} = 0.8$, $\alpha = \pi/4$.

optimal for $\alpha = \pi/4$. Panel (b) shows the onset of the large- N limit in measurement. Each dot in the plot is the estimate of $\cos \phi_k$, where $e^{i\phi_k}$ are the eigenvalues of the measured observables C . (In this example, $\phi_k = \pi k/4$, $k \in \mathbb{Z}_8$). The measurement procedure consists of N_M weak measurements in a row, each at an angle $\alpha = 0.5$ away from the wire basis. For small N_M there are fewer points, because most estimates are outside the meaningful region of $|\cos \phi| \leq 1$.

The above weak measurement, estimating $\cos \phi + \delta$, has a degeneracy, since it cannot distinguish between the angles ϕ and $\phi' = -\phi - 2\delta$. This degeneracy can be removed by performing a second sequence of measurements in the basis $\mathcal{B}^*(\alpha) = \{|0'\rangle, |1'\rangle, |2\rangle, \dots\}$, with

$$\begin{aligned} |0'\rangle &= \cos \alpha |0\rangle + i \sin \alpha |1\rangle, \\ |1'\rangle &= i \sin \alpha |0\rangle + \cos \alpha |1\rangle. \end{aligned} \quad (37)$$

In this way, $\sin(\delta + \phi)$ is measured on the virtual system, and in combination with the above one obtains $e^{i(\phi + \delta)}$, hence ϕ . We thus arrive at the following Lemma.

Lemma 4 *Consider a symmetry-protected phase of a group G with the properties (i) the ground state is unique, (ii) there is a wire basis, and (iii) the byproduct operators C_i are in a projective representation of G , $C_i \otimes I \in V(G)$. Then, for all resource states $|\Phi\rangle$ of Eq. (5) derived from MPS ground states Eq. (1) in that phase, except a possible subset of measure zero, projective measurement of the observables in the set \mathcal{O} can be arbitrarily closely approximated.*

We restate this result, without the conditions and qualifications, as our third computational primitive.

Computational primitive 3 *All observables $A \in \mathcal{O}$ can be measured on the logical part of the virtual system.*

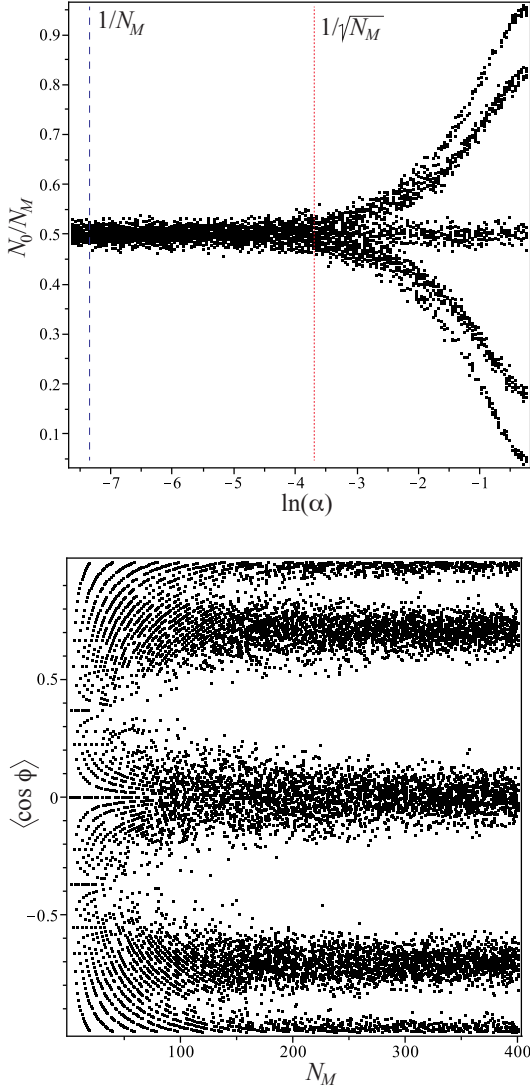


FIG. 3: Measurement of the logical subsystem of the virtual system. (top) Changeover between unitary evolution and measurement. For unitary evolution of the logical subsystem, the angle α in $\mathcal{B}(\alpha)$ is chosen $\sim 1/N_M$, where $N_M := N_0 + N_1$. Unitary evolution turns into measurement at $\alpha \approx 1/\sqrt{N_M}$. The measurement is optimal for $\alpha = \pi/4$. In this plot, $N_M = 1600$. (bottom) Onset of the large- N limit in measurement. Each dot in the plot is the estimate of $\cos \phi_k$, where $e^{i\phi_k}$ are the eigenvalues of the measured observables C . Each such estimate is based on a sequence of N_M individual weak measurements. In this example, $\phi_k = \pi k/4$, $k \in \mathbb{Z}_8$. The parameters for both plots are $\nu_{00} = \nu_{11} = 1$, $\nu_{10} = 0.9$, and the state of the logical subsystem before measurement is completely mixed.

For matters of efficiency of the measurement procedure, it is noted that in addition to measurement in the bases Eq. (30) and (37) for the physical spins, leading to an estimate of $\cos(\phi + \delta)$ and $\sin(\phi + \delta)$ respectively, one

may as well measure in the basis $\mathcal{B}(\alpha, \beta)$ defined by

$$\begin{aligned} |0'\rangle &= \cos \alpha |0\rangle + e^{i\beta} \sin \alpha |1\rangle, \\ |1'\rangle &= \sin \alpha |0\rangle - e^{i\beta} \cos \alpha |1\rangle. \end{aligned} \quad (38)$$

Thereby, an estimate of $\cos(\phi + \delta + \beta)$ is obtained with the same efficiency. One may vary the angle β to perform state tomography, or adjust β to optimize the resolution of the measurement for estimating ϕ (choose β such that $\cos(\phi + \delta + \beta) \approx 0$).

B. Born rule for the logical subsystem

In the above, we have demonstrated that for a measurement of the logical subsystem of the virtual system, the post-measurement state is related to the measurement record in the way described by quantum mechanics, i.e., it is an eigenstate of the measured observable. To complete our discussion of measurement of the logical subsystem, we need relate the measurement record to the state before measurement.

Lemma 5 *In the measurement of an observable C on the state σ of the logical subsystem of the virtual system, the probability $p_C(i)$ of obtaining the post-measurement state $|\phi_i\rangle$ is given by the Born rule,*

$$p_C(i) = \langle \phi_i | \sigma | \phi_i \rangle. \quad (39)$$

Proof of Lemma 5. We consider the channel resulting from combining all computational paths of an individual weak measurement, as described in Eq. (33). With Eqs. (22), (34) we find that

$$\sigma_{ii} \longrightarrow \sum_{k=0}^{d-1} f_k(\phi_i, \phi_i) = \sigma_{ii}, \quad \forall i = 1, \dots, D.$$

Hence, all diagonal elements of σ in the eigenbasis of C are the same before and after the channel. This also holds for any number of iterations of the channel,

$$\sigma_{ii, <} = \sigma_{ii, >}. \quad (40)$$

Now consider a sequence of measurements, with record $\mathbf{k} = (k_1, \dots, k_m)$, that is sufficiently long to project the logical state. Denote by $\mathbf{k} \rightarrow i$ that the measurement record \mathbf{k} is interpreted as outcome i , and by $p_C(\mathbf{k})$ the probability for the outcome \mathbf{k} . The matrix element $\sigma_{ii}(\mathbf{k})$ of the logical state conditioned on the outcome \mathbf{k} is

$$\sigma_{ii}(\mathbf{k}) = \begin{cases} 1, & \text{if } \mathbf{k} \rightarrow i, \\ 0, & \text{if } \mathbf{k} \not\rightarrow i. \end{cases}$$

Then, for the matrix element $\sigma_{ii}(>)$ after measurement it holds that

$$\begin{aligned} \sigma_{ii, >} &= \sum_{\mathbf{k}} \sigma_{ii}(\mathbf{k}) p_C(\mathbf{k}) \\ &= \sum_{\mathbf{k} | \mathbf{k} \rightarrow i} p_C(\mathbf{k}) \\ &= p_C(i). \end{aligned}$$

For the matrix element $\sigma_{ii, <}$ before measurement it holds by definition that $\sigma_{ii, <} = \langle \phi_i | \sigma | \phi_i \rangle$. Hence, with Eq. (40), $\langle \phi_i | \sigma | \phi_i \rangle = p_C(i)$. \square

C. Operational cost of measurement

Measurement is most effective for the choice $\alpha = \pi/4$ in the measurement basis Eq. (30). Then, Eq. (36) for the estimate of $\cos(\phi + \delta)$ simplifies to

$$\cos(\phi + \delta) = \frac{N_0 - N_1}{N_0 + N_1} \frac{\nu_{00} + \nu_{11}}{2|\nu_{01}|}.$$

We first discuss the case where, after a couple of measurement rounds, it is found that $\cos(\phi + \delta) \approx 0$. In this region, the conversion of $\cos(\phi + \delta)$ into ϕ is the most reliable. Assuming that the uncertainty in the constants $\nu_{00}, \nu_{11}, |\nu_{01}|$ and δ is negligible, the experimental uncertainty $\Delta\phi$ of ϕ is $\Delta\phi = 1/\sqrt{N_0 + N_1} \cdot (\nu_{00} + \nu_{11})/4|\nu_{01}|$.

Denote by Δ the smallest distance between two consecutive eigenvalues of the measured observable $C_0^{-1}C_1$ on the unit circle. To reach an accuracy $\Delta\phi = \epsilon\Delta$, with ϵ a small parameter, the number N of measurement steps used for the measurement of the logical subsystem is $(N_0 + N_1)/(\nu_{00} + \nu_{11})$, and thus

$$N = \frac{1}{(4\epsilon\Delta)^2} \frac{(\nu_{00} + \nu_{11})}{|\nu_{01}|^2}. \quad (41)$$

In the remaining case, $\cos(\phi + \delta) \not\approx 0$, the procedure is as follows. First, $\phi + \delta$ is measured with low accuracy, in only a few rounds of measurement. Then, the further measurements proceed in a basis $\mathcal{B}(\pi/4, \beta)$ of Eq. (38) where β is chosen such that $\cos(\phi + \delta + \beta) \approx 0$. This results in a precision measurement of $\cos(\phi + \delta - \beta)$, with the same operational overhead as in Eq. (41).

D. Initialization

Measurement can also be used for initialization of the logical system. To initialize in a fixed reference state, one may measure a suitable byproduct operator C , and subsequently apply a conditional unitary.

VI. REVERTING TO THE BOUNDARY CONDITIONS OF EQ. (1)

In this section we convert to the resource state with the original boundary conditions, and thereby complete the construction. We show that the state $|\tilde{\Phi}\rangle$ of Eq. (5) with the modified boundary condition can be replaced by the original resource state $|\Phi\rangle$ of Eq. (1). The basic reason for why this works is that the computation is completed with a measurement somewhere in the bulk of the chain, sufficiently far from the boundary. Then, because the correlation length is typically finite, the choice of boundary condition does not matter. Below we formalize this intuition.

Lemma 6 *If an MBQC can be performed with a quantum state $|\tilde{\Phi}\rangle$ of Eq. (5) then it can also be performed by*

the quantum state $|\Phi\rangle$ of Eq. (1), which differs from $|\tilde{\Phi}\rangle$ in the choice of the boundary condition at the right end of the chain.

Proof of Lemma 6. The proof splits into two parts. First we show that standard open boundary conditions are fine if the state associated with the right boundary is $I/D \otimes \bar{\rho}_{\text{fix}}$, where $\bar{\rho}_{\text{fix}}$ is the fixed point of the channel $\mathcal{L} := \sum_s [B_s^\dagger]$ with the largest eigenvalue $\bar{\nu}$, and D is the dimension of the logical system. Second, we show how to prepare that state on the right boundary, starting from any boundary state $|R\rangle$.

(i) The main point is that if the logical state of the right boundary system is $\sigma \sim I$, then the forward-propagated byproduct operator $\Sigma(\mathbf{s})$ annihilates on the right boundary, $\Sigma(\mathbf{s}) I \Sigma(\mathbf{s})^\dagger = I$. This is the counterpart to the active correction of the byproduct operator $\Sigma(\mathbf{s})$ in case of the boundary conditions Eq. (5). In case of the boundary conditions Eq. (1) no active intervention is necessary.

For notational simplicity, we consider a sequence $T'_{C,s} \circ T$ of only two operations, where T is a unitary and $T'_{C,s}$ is a measurement of the observable C with outcome s . W.l.o.g. we assume that the input state of the virtual system prior to these gates is $\sigma \otimes \rho_{\text{fix}}$. Any such input state can be prepared, as we have previously shown. We now consider the probabilities $p(s)$ and $p'(s)$ for obtaining the outcome s if the computation is run on an input state $|\tilde{\Phi}\rangle$ and $|\Phi\rangle$, respectively. The probabilities are

$$\begin{aligned} p(s) &= \text{Tr}(T'_{C,s} \circ T(\sigma)) \text{Tr}(\rho_{\text{fix}}) \times c, \\ p'(s) &= \text{Tr}(T'_{C,s} \circ T(\sigma)) \text{Tr}(\rho_{\text{fix}} \bar{\rho}_{\text{fix}}) \times c'/D, \end{aligned}$$

where c, c' are normalization constants independent of s , and thus $p(s) \sim p'(s)$. Since $\sum_s p(s) = \sum_s p'(s) = 1$,

$$p(s) = p'(s), \quad \forall s = 0, \dots, d-1.$$

Thus there is no effect of the right boundary on the measurement statistics, if the right boundary state $I/D \otimes \bar{\rho}_{\text{fix}}$ can be prepared.

(ii) The right boundary state $I/D \otimes \bar{\rho}_{\text{fix}}$ is prepared by running “completely oblivious” wire from the right boundary inwards. Completely oblivious wire is the same as oblivious wire, except that measurement outcomes are discarded without performing any correction anywhere. First, the state $I/D \otimes \bar{\rho}_{\text{fix}}$ is indeed a fixed point of the evolution $\bar{\mathcal{F}} = \sum_s [A(s)]$,

$$\begin{aligned} \sum_{s=0}^{d-1} A(s)^\dagger \left(\frac{I}{D} \otimes \bar{\rho}_{\text{fix}} \right) A(s) &= \sum_{s=0}^{d-1} C_s^\dagger \frac{I}{D} C_s \otimes B_s^\dagger \bar{\rho}_{\text{fix}} B_s \\ &= I/D \otimes \sum_{s=0}^{d-1} B_s^\dagger \bar{\rho}_{\text{fix}} B_s \\ &= \bar{\nu} (I/D \otimes \bar{\rho}_{\text{fix}}). \end{aligned}$$

Second, the state $I/D \otimes \bar{\rho}_{\text{fix}}$ is the eigenstate of $\bar{\mathcal{F}}$ with the largest eigenvalue. Suppose there was an eigenstate τ of $\bar{\mathcal{F}}$ with larger eigenvalue $\bar{\nu}_\tau$, $\bar{\nu}_\tau > \bar{\nu}$. Define $\rho(\tau) := \text{Tr}_L \tau$, where Tr_L is the trace over the logical subsystem. By assumption we have $\bar{\nu}_\tau \tau = \bar{\mathcal{F}}(\tau) = \sum_s C_s^\dagger \otimes B_s^\dagger \tau C_s \otimes$

B_s . Now taking Tr_L on both sides, and using the cyclicity of trace, we find

$$\bar{\nu}_\tau \rho(\tau) = \sum_s B_s^\dagger \rho(\tau) B_s = \bar{\mathcal{L}}(\rho(\tau)).$$

$\bar{\mathcal{L}}$ has a larger eigenvalue than $\bar{\nu}$. Contradiction. Thus, the largest eigenvalue of the channel $\bar{\mathcal{F}}$ is $\bar{\nu}$, the same as of the channel $\bar{\mathcal{L}}$ on the junk system alone.

The largest eigenvalue of $\bar{\mathcal{F}}$ is typically non-degenerate, and $I/D \otimes \bar{\rho}_{\text{fix}}$ is thus the unique stable fixed point. It is closely approximated for a sufficient number of iterations of $\bar{\mathcal{F}}$, starting from any boundary condition $|R\rangle$. \square

Remark: Completely oblivious wire is equivalent to the respective spins being traced out. To implement it, all that needs to be done is to keep a sufficiently long runway of spins between the last spin used for measurement and the right boundary of the chain.

Proof of Theorem 2. Lemma 3 provides the unitary gates in $L(\mathcal{O})$ and Lemma 4 projective measurements of observables in the set \mathcal{O} , given the state $|\tilde{\Phi}\rangle$ of Eq. (5). With Lemma 6, the resource state $|\tilde{\Phi}\rangle$ may be replaced by the resource state $|\Phi\rangle$ of Eq. (1) with standard open boundary conditions on both sides. \square

VII. EXAMPLES

A. $\mathbb{Z}_D \times \mathbb{Z}_D$ symmetry

Here we consider symmetry-protected topological order for the symmetry group $G = \mathbb{Z}_D \times \mathbb{Z}_D$, and are interested in the phase corresponding to the maximally non-commuting factor system. The latter describes a unique projective representation $V(G)$ acting on the virtual system as $V(a \times b) = \tilde{V}(a \times b) \otimes I_{\text{junk}}$, where $a \times b \in \mathbb{Z}_D \times \mathbb{Z}_D$, $\tilde{V}(a \times b) = X^a Z^b$ and X, Z are Heisenberg-Weyl operators in dimension D , defined by $X|z\rangle = |z+1 \bmod D\rangle$, $Z|z\rangle = e^{2\pi i z/D} |z\rangle$. With Theorem 1 of [12] and the proof thereof, the MPS tensor A can be written as

$$A[i] = \tilde{V}(g_i) \otimes B_{\text{junk},i}$$

where $g_i \in \mathbb{Z}_D \times \mathbb{Z}_D$.

The dimension d of the physical spins may now be chosen $d = D^2$, which is compatible with a qudit cluster state. Then, the operators $C_i^{-1} C_j$, for $i, j \neq i \in 0, \dots, D^2 - 1$ are, up to phases, also the Heisenberg-Weyl operators in dimension D minus the identity. There are thus $D^2 - 1$ linearly independent such operators. Therefore the set of Eq. (3), for $d = D^2$, also has $D^2 - 1$ linearly independent elements. Furthermore, all elements of this set are Hermitian and traceless. Hence they span the space of traceless Hermitian $D \times D$ matrices. With Lemma 3, the set of gates realizable in this SPTO phase is thus $SU(D)$. Furthermore, by Lemma 4, all Heisenberg-Weyl operators can be measured in this phase.

B. $(\mathbb{Z}_2 \times \mathbb{Z}_2)^{\times N}$ symmetry

Consider the symmetry group $G = (\mathbb{Z}_2 \times \mathbb{Z}_2)^{\times N}$, and the SPT phase corresponding to the maximally non-commuting factor system. By theorem 1 of [12], there exists a wire basis of 2^{2N} states $|\mathbf{a}\rangle$, with $\mathbf{a} = (\mathbf{a}_X, \mathbf{a}_Z)$ and $\mathbf{a}_X, \mathbf{a}_Z \in \mathbb{Z}_2^N$, such that

$$A[\mathbf{a}] = B_{\text{junk}}[\mathbf{a}] \otimes X(\mathbf{a}_X) Z(\mathbf{a}_Z).$$

The byproduct operators are N -qubit Pauli operators, and the logical qudit is thus equivalent to N qubits.

By Theorem 2, the corresponding MBQC scheme can realize all unitaries in $SU(2^N)$ and measure all N -qubit Pauli observables. It is thus N -qubit universal.

This example illustrates that MBQCs on two- and higher-dimensional spin lattices are implicitly included in our analysis, by treating them as quasi-onedimensional systems. This treatment is, however, not fully satisfactory. First, the symmetry group G grows with the number of logical qubits processed (also see [26]), and universal quantum computation on different numbers of qubits thus happens in distinct physical phases.

Second, the notion of locality in the present example is not what one would expect for MBQC. In all MBQC schemes proposed to date, the size of the support of each individual measurement is fixed and independent of the number of logical qubits processed; and it seems reasonable to impose this property as a necessary requirement. In the present example, however, the support of each measurement is on a 2^{2N} -dimensional physical system, equivalent of $2N$ qubits. It is thus dependent on the number N of logical qubits processed.

VIII. THE MATRIX $[\nu_{ij}]$

A. Measurement

Running of MBQC at any given point in the SPTO phase requires knowledge of the d^2 parameters ν_{ij} characterizing the fixed point state ρ_{fix} of the junk system. These parameters can be estimated as follows. First, a state $\sigma \otimes \rho_{\text{fix}}$ of the virtual system is prepared through oblivious wire (See computational primitive 1). This procedure does not require knowledge of the parameters ν_{ij} . Then follows a sequence of measurements in the wire basis alternating with oblivious wire. The frequencies N_k of obtaining the outcomes k in measurement in the wire basis are, with Eqs. (35) and (34), related via

$$\frac{\nu_{kk}}{\nu_{ll}} = \frac{N_k}{N_l}.$$

In this way, also invoking the normalization condition Eq. (22), all diagonal elements ν_{kk} are measured.

Finally, the off-diagonal elements can be determined by implementing rotations Eq. (26) and measuring the rotation angle, e.g. by change in the population of the various levels of the logical subsystem.

B. Interpretation

The operator $\nu := \sum_{i,j=0}^{d-1} |i\rangle \nu_{ij} \langle j|$ can be given the interpretation of a (mixed) quantum state. With Eq. (21), ν is Hermitian, and with Eq. (22), $\text{Tr } \nu = 1$. Finally, ν is positive semidefinite.

The latter can be seen as follows. Consider a tensor product state $\sum_{ij} B_i \rho_{\text{fix}} B_j^\dagger \otimes |i\rangle \langle j|$ of the junk part of the virtual system and a physical degree of freedom, where $\{|i\rangle\}$ is an ONB of \mathbb{C}^d (the Hilbert space of a physical degree of freedom). For any state $|\psi\rangle$ of the physical system, consider furthermore the expression

$$\begin{aligned} \nu_\psi(n) &:= \langle \psi | \text{Tr}_{\text{junk}} \left(I \otimes \mathcal{L}^n \left(\sum_{ij} |i\rangle \langle j| \otimes B_i \rho_{\text{fix}} B_j^\dagger \right) \right) | \psi \rangle \\ &= \text{Tr}_{\text{junk}} \left(I \otimes \mathcal{L}^n \left(B_\psi \rho_{\text{fix}} B_\psi^\dagger \right) \right), \end{aligned}$$

with $B_\psi = \sum_i \langle \psi | i \rangle B_i$. With Lemma 1, ρ_{fix} is either positive or negative semidefinite, and wlog. may be chosen positive semidefinite (hence, $\text{Tr}(\rho_{\text{fix}}) > 0$). Since $[B_\psi]$ (as a super-operator) is completely positive for all $|\psi\rangle$ and \mathcal{L} is completely positive, it holds that

$$\nu_\psi(n) \geq 0, \quad \forall |\psi\rangle, \forall n.$$

We may now evaluate $\nu_\psi(n)$ in a different way. Using Eq. (20), in the limit of $n \rightarrow \infty$ we have

$$\begin{aligned} \nu_\psi(\infty) &= \langle \psi | \text{Tr}_{\text{junk}} \left(\left(\sum_{ij} |i\rangle \nu_{ij} \langle j| \right) \otimes \rho_{\text{fix}} \right) | \psi \rangle \\ &= \text{Tr}(\rho_{\text{fix}}) \times \langle \psi | \left(\sum_{ij} |i\rangle \nu_{ij} \langle j| \right) | \psi \rangle \\ &= \text{Tr}(\rho_{\text{fix}}) \times \langle \psi | \nu | \psi \rangle. \end{aligned}$$

Comparing the two above expressions for $\nu_\psi(\infty)$, we find that the state ν is positive semidefinite, as claimed.

Now that we know that ν can be regarded as a quantum state, what is its role in the computational scheme? It turns out that each copy of the state ν implements a single quantum gate on the logical subsystem, by interacting with it and subsequently being discarded (traced out). See Fig. 4 for illustration.

This picture arises as follows. First, consider the action on the virtual state $\sigma \otimes \rho_{\text{fix}}$ of a physical degree of freedom being measured in the state $|\psi_0\rangle$ (corresponding to byproduct operator I) followed by oblivious wire \mathcal{L}^n for some sufficiently large n . With Eq. (20),

$$\begin{aligned} \sigma \otimes \rho_{\text{fix}} &\longrightarrow \mathcal{L}^n \left(\left[\sum_i \langle \psi_0 | i \rangle C_i \otimes B_i \right] (\sigma \otimes \rho_{\text{fix}}) \right) \\ &= \sum_{ij} \langle \psi_0 | i \rangle \nu_{ij} \langle j | \psi_0 \rangle C_i \sigma C_j^\dagger \otimes \rho_{\text{fix}}. \end{aligned}$$

Now we consider the following related procedure, which invokes the incoherent addition of computational paths. The physical degree of freedom is measurement in the basis $\mathcal{B}_M = \{|\psi_k\rangle, k = 0, \dots, d-1\}$ which is related to the wire basis \mathcal{B} via a unitary U , $|\psi_k\rangle = U|k\rangle$, for all $|k\rangle \in \mathcal{B}$. For each measurement outcome k , the corresponding byproduct operator C_k is reversed; See Section IV. After that, the measurement outcome k is dis-

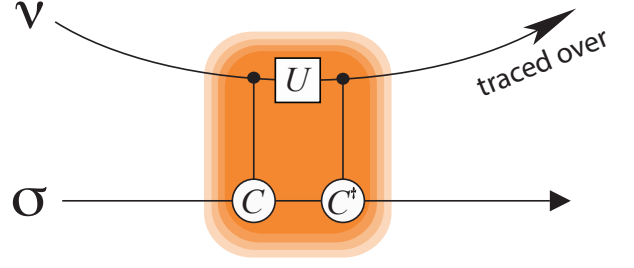


FIG. 4: Computation by interaction of the logical system with the state ν . The state ν represents the “computational essence” of the fixed point state ρ_{fix} of the junk subsystem. U is the unitary that transforms between the wire basis and the measurement basis for the physical degree of freedom. The interaction between the two systems is via the gate Eq. (42).

carded. Combining all computational paths k , this procedure is represented by

$$\sigma \longrightarrow \sum_k \sum_{ij} \langle k | U^\dagger | i \rangle \nu_{ij} \langle j | U | k \rangle C_k^\dagger C_i \sigma C_j^\dagger C_k.$$

Here, we have dropped the tensor factor ρ_{fix} since it remains unaffected by the procedure. We note that a new tensor factor comes into play, namely the physical degree of freedom, with states $\{|i\rangle\}$. We denote by $\Lambda(C)$ the entangling gate

$$\Lambda(C) = \sum_{i=0}^{d-1} |i\rangle \langle i| \otimes C_i, \quad (42)$$

with the physical degree of freedom as control and the logical subsystem as target. With this, the update of the state σ can be rewritten as

$$\sigma \longrightarrow \text{Tr}_{\mathcal{P}} \Lambda(C)^\dagger U \Lambda(C) (\nu \otimes \sigma) \Lambda(C)^\dagger U^\dagger \Lambda(C),$$

where $\text{Tr}_{\mathcal{P}}$ denotes the trace over the physical degree of freedom. This is the state evolution depicted in Fig. 4. We have thus shown that MBQCs in SPTO phases simulate quantum circuits in which each gate be viewed as arising from the interaction between the logical subsystem with a particle prepared in the state ν .

IX. CONCLUSION

We have investigated measurement-based quantum computation on resource states that are ground states in symmetry-protected topologically ordered phases, in spatial dimension one. We have shown that if an SPTO phase supports symmetry-protected quantum wire (and subject to the technical condition that the MBQC byproduct operators are elements of a projective representation of the symmetry group), then this phase also supports quantum computation on one qudit. That is,

any state in the phase is a resource for MBQC in $\mathcal{D} = 1$. For such SPTO phases, Conjecture 1 thus holds.

It is instructive to compare the present construction to the symmetry-protected wire of [12], which it extends to the domain of quantum computation. In [12], symmetry specifies the computational wire completely, and the details of the quantum state in the given SPTO phase play no role at all. This is different in the present scenario for quantum computation. Some information about the resource quantum state does enter the computational scheme, namely a Hermitian $d \times d$ -matrix of coefficients $[\nu_{ij}]$, with d the dimension of the physical spins in the chain. These parameters are not constrained by symmetry, and need to be measured in a self-test prior to the computation.

We conclude with two open questions. The immediate question is whether and how Theorem 2 generalizes to higher spatial dimension $\mathcal{D} \geq 2$.

Even in dimension $\mathcal{D} = 1$, a better understanding of the algebraic side of the presented constructions is desirable. For example, can it happen that a byproduct operator $C_i \otimes I$ is not a symmetry? Furthermore, is the existence of a wire basis necessary for uniform computational power throughout SPTO phases? We have found that the MPS tensors are sometimes very constrained by symmetry, but the constraints are not quite strong enough or not of the right kind to produce a tensor product structure between a logical and a junk system. Can computational schemes that work uniformly across SPTO phases be built on other structures than tensor products?

Acknowledgments

This work is supported by NSERC, Cifar, and the National Science Foundation under Grant No. PHY 1620252. R. Raussendorf is fellow of the Cifar program on Quantum Information Science.

Appendix A: Adding computational paths—the one-party scenario

Here we return to the subject of Section IIID, the interpretation of adding computational paths. We have already provided an interpretation for a distributed computational setting involving two parties. However, in the present situation, the computation is performed by a single party. In this setting, we use “forgetting” of classical information in the following technical sense: Forgetting of information means the commitment to never use that information in any decision-making after the point of “forgetting”. It is thus merely a restriction in the available modes of classical processing, and we do not have to discuss whether the erasure of information is physically possible.

A general quantum computation consists of an initialization, followed by a sequence of unitaries and measure-

ments. Since we have not established all of those computational primitives yet, we consider here the simple case where oblivious wire is implemented on a state $|\tilde{\Phi}\rangle$ with a left boundary state $|L\rangle$, and subsequently an observable A is measured on the logical subsystem of the right boundary state. Furthermore, the left boundary state is of the special tensor product form $|L\rangle = |l\rangle \otimes |j\rangle$, where $|l\rangle$ represents the state of the logical subsystem of the left boundary, and $|j\rangle$ the state of the junk subsystem.

The important quantity in this setting is the probability distribution p_A of measurement outcomes for A given the state $|l\rangle$. The goal is to show that the distribution p_A can be sampled from correctly and efficiently by measurements on $|\tilde{\Phi}\rangle$.

We denote by $q_A(o, \mathbf{s})$ the joint probability for obtaining the measurement record \mathbf{s} on the spins in the chain and the outcome o for the observable A , measured on the right boundary system in the support of $|\tilde{\Phi}\rangle$. By the same argument as in Eqs. (8), (9), but without summation over \mathbf{s} , we find that

$$q_A(\mathbf{s}, o) = q(\mathbf{s}) p_A(o|\mathbf{s}), \quad (\text{A1})$$

where $q(\mathbf{s}) = |\kappa(n)|^2 \|\prod_{k=1}^n B_{s_k} |j\rangle\|^2$ is the probability of obtaining the outcome \mathbf{s} , and

$$p_A(o|\mathbf{s}) = \langle l | P_A(o) | l \rangle$$

is the probability of obtaining the outcome o in the measurement of the right boundary system, given the prior measurement record \mathbf{s} . Therein, $P_A(o)$ is the projector onto the eigenspace of A with eigenvalue o .

We thus find that $p_A(o|\mathbf{s})$ is independent of \mathbf{s} , and, more importantly, that it equals the probability of obtaining the outcome o in the measurement of the observable A on the state $|l\rangle$, $p_A(o|\mathbf{s}) = p_A(o)$ for all \mathbf{s} . Thus, with Eq. (A1),

$$p_A(o) = \sum_{\mathbf{s}} q_A(\mathbf{s}, o). \quad (\text{A2})$$

We now turn to the experimental procedure. In each run of the computation, the computing party obtains one sample (\mathbf{s}, o) from the the probability distribution q_A , and discards the \mathbf{s} -part,

$$(o, \mathbf{s}) \longrightarrow o.$$

This is the step of “forgetting” classical information. The remaining outcomes o are thus sampled from the probability distribution p'_A , with

$$p'_A(o) := \sum_{\mathbf{s}} q_A(\mathbf{s}, o).$$

By comparison with Eq. (A2), $p'_A \equiv p_A$. The procedure thus samples from the correct probability distribution for the measurement outcomes o of A on $|l\rangle$.

Furthermore, every run of the computation generates a sample from the distribution p_A , and the adding of computational paths is thus efficient. Specifically, it does not cause any overhead in the computation.

Appendix B: Proof of Lemma 2

Proof of Lemma 2. The proof is by explicit construction of the procedure of implementing $T'(\beta)T(\alpha)$. This procedure is the following: (i) On the first segment of the spin chain, implement $T(\alpha)$, but retain the measurement outcomes $(s_1, \dots, s_n) = \mathbf{s}$. (ii) On the remaining segment

of the spin chain, implement $T'(\beta'(\mathbf{s}))$. (iii) Sum over all measurement outcomes \mathbf{s} on the first segment and $\mathbf{z} = (z_{n+1}, \dots, z_{n'})$ on the second segment.

We denote by $[a]$ the super operator corresponding to the operator a , and $C(\mathbf{z}, \mathbf{s})$ is the total accumulated byproduct operator. The output state τ_{out} of the combined procedure is

$$\begin{aligned}
 \tau_{\text{out}} &= \sum_{\mathbf{z}} [C(\mathbf{z}, \mathbf{s})]^{-1} \prod_{j=n+2}^{n'} [C_{z_j} \otimes B_{z_j}] [A_{n+1}(z_{n+1}, \beta'(\mathbf{s}))] \sum_{\mathbf{s}} \prod_{i=2}^n [C_{s_i} \otimes B_{s_i}] [A_1(s_1, \alpha)] (\sigma \otimes \rho_{\text{fix}}) \\
 &= \sum_{\mathbf{z}} [C(\mathbf{z}, \mathbf{s})]^{-1} \left[C(\mathbf{z}) \otimes \prod_{j=n+2}^{n'} B_{z_j} \right] [A_{n+1}(z_{n+1}, \beta'(\mathbf{s}))] \sum_{\mathbf{s}} \left[C(\mathbf{s}) \otimes \prod_{i=2}^n B_{s_i} \right] [A_1(s_1, \alpha)] (\sigma \otimes \rho_{\text{fix}}) \\
 &= \sum_{\mathbf{z}, \mathbf{s}} [C(\mathbf{z}, \mathbf{s})]^{-1} \left[C(\mathbf{z}) C(\mathbf{s}) \otimes \prod_{j=n+2}^{n'} B_{z_j} \right] [A_{n+1}(z_{n+1}, \beta)] \left[I \otimes \prod_{i=2}^n B_{s_i} \right] [A_1(s_1, \alpha)] (\sigma \otimes \rho_{\text{fix}}) \\
 &= \sum_{\mathbf{z}, \mathbf{s}} \left[\prod_{j=n+2}^{n'} I \otimes B_{z_j} \right] [A_{n+1}(z_{n+1}, \beta)] \left[\prod_{i=2}^n I \otimes B_{s_i} \right] [A_1(s_1, \alpha)] (\sigma \otimes \rho_{\text{fix}}) \\
 &= \sum_{\mathbf{z}} \left[\prod_{j=n+2}^{n'} I \otimes B_{z_j} \right] [A_{n+1}(z_{n+1}, \beta)] \sum_{\mathbf{s}} \left[\prod_{i=2}^n I \otimes B_{s_i} \right] [A_1(s_1, \alpha)] (\sigma \otimes \rho_{\text{fix}}) \\
 &= \sum_{\mathbf{z}} \left[\prod_{j=n+2}^{n'} I \otimes B_{z_j} \right] [A_{n+1}(z_{n+1}, \beta)] T(\alpha) (\sigma) \otimes \rho_{\text{fix}} \\
 &= T'(\beta) T(\alpha) (\sigma) \otimes \rho_{\text{fix}}
 \end{aligned}$$

Therein, in the third line we have used Eq. (29), and in

the fourth line the relation $C(\mathbf{s}, \mathbf{z}) = C(\mathbf{z})C(\mathbf{s})$. \square

-
- [1] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
 - [2] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
 - [3] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Phys. Rev. Lett. **59**, 799 (1987).
 - [4] A. Miyake, Annals of Physics **326**, 1656 (2011).
 - [5] T.-C. Wei, I. Affleck and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).
 - [6] D. Gross, S.T. Flammia, J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).
 - [7] M.J. Bremner, C. Mora, A Winter, Phys. Rev. Lett. **102**, 190502 (2009).
 - [8] Xie Chen, Zheng Cheng Gu, and Xiao Gang Wen, Phys. Rev. B **83**, 035107 (2011).
 - [9] Xie Chen, Zheng-Cheng Gu, Zheng-Xin Liu, and Xiao-Gang Wen, Phys. Rev. B **87**, 155114 (2013).
 - [10] Norbert Schuch, David Perez-Garcia, and Ignacio Cirac, Phys. Rev. B **84**, 165139 (2011).
 - [11] Akimasa Miyake, Phys. Rev. Lett. **105**, 040501 (2010).
 - [12] D.V. Else, I. Schwarz, S.D. Bartlett and A.C. Doherty, Phys. Rev. Lett. **108**, 240505 (2012).
 - [13] Jacob Miller and Akimasa Miyake, Phys. Rev. Lett. **114**, 120506 (2015).
 - [14] A. Prakash and T.-C. Wei, Phys. Rev. A **92**, 022310 (2015).
 - [15] A. Prakash, C. G. West, and T.-C. Wei, arXiv:1604.00037.
 - [16] Tzu-Chieh Wei, Poya Haghnegahdar, Robert Raussendorf, Phys. Rev. A **90**, 042333 (2014).
 - [17] Tzu-Chieh Wei, Robert Raussendorf, Phys. Rev. A **92**, 012310 (2015).
 - [18] H. Niggemann, A. Klümper, and J. Zittartz, Z. Phys. B **104**, 103 (1997).
 - [19] Andrew S. Darmawan, Gavin K. Brennen, Stephen D. Bartlett, New J. Phys. **14**, 013023 (2012).
 - [20] Ching-Yu Huang, Maximilian Anton Wagner, and Tzu-Chieh Wei, arXiv:1605.08417.
 - [21] D. Perez-Garcia, F. Verstraete, M.M. Wolf, J.I. Cirac, Quantum Inf. Comput. **7**, 401 (2007).
 - [22] Andrew M. Childs, Debbie W. Leung, Michael A. Nielsen, Phys. Rev. A **71**, 032318 (2005).
 - [23] D. Gross, J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).
 - [24] D. Stephen, D.-S. Wang, A. Prakash, T.-C. Wei and R.

- Raussendorf, arXiv:1611.08053.
- [25] Bei Zeng, Xie Chen, Duan-Lu Zhou, Xiao-Gang Wen, arXiv:1508.02595.
- [26] D.V. Else, S.D. Bartlett, A.C. Doherty, New J. Phys. **14**, 113016 (2012).