Nonunitary quantum computation in the ground space of local Hamiltonians

Naïri Usher,[1,*] Matty J. Hoban,[2,3] and Dan E. Browne[1]

[1]*Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom*

[2]*Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom*

[3]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*

(Received 1 April 2017; published 12 September 2017)

A central result in the study of quantum Hamiltonian complexity is that the k-local Hamiltonian problem is quantum-Merlin-Arthur–complete. In that problem, we must decide if the lowest eigenvalue of a Hamiltonian is bounded below some value, or above another, promised one of these is true. Given the ground state of the Hamiltonian, a quantum computer can determine this question, even if the ground state itself may not be efficiently quantum preparable. Kitaev's proof of QMA-completeness encodes a unitary quantum circuit in QMA into the ground space of a Hamiltonian. However, we now have quantum computing models based on measurement instead of unitary evolution; furthermore, we can use postselected measurement as an additional computational tool. In this work, we generalize Kitaev's construction to allow for nonunitary evolution including postselection. Furthermore, we consider a type of postselection under which the construction is consistent, which we call tame postselection. We consider the computational complexity consequences of this construction and then consider how the probability of an event upon which we are postselecting affects the gap between the ground-state energy and the energy of the first excited state of its corresponding Hamiltonian. We provide numerical evidence that the two are not immediately related by giving a family of circuits where the probability of an event upon which we postselect is exponentially small, but the gap in the energy levels of the Hamiltonian decreases as a polynomial.

DOI: 10.1103/PhysRevA.96.032321

I. INTRODUCTION

The advent of quantum information has brought the fields of theoretical computer science and physics closer together in new and exciting ways. In particular, it has been shown that key problems in condensed-matter theory, such as finding the ground state of a class of Hamiltonians, can be studied through the lens of quantum computational complexity [1].

Kitaev, building upon ideas originally developed by Feynman [2], was the first to connect the two together. He showed that determining whether a system has ground-state energy E_0 that is less than a or greater than b is a hard problem for a quantum computer. However, once given a candidate ground state, a quantum computer can efficiently check its energy. More formally, Kitaev thus defined the k-local Hamiltonian problem which he subsequently proved is quantum-Merlin-Arthur–complete, the quantum computing analog of the class NP [3,4]. Intuitively, NP-complete problems are hard to solve on a classical computer, even though candidate solutions—or proofs—can be efficiently checked, and thus, similarly, QMA-complete problems will be hard for a quantum computer to solve. Since then, building on Kitaev's seminal work, the field of quantum Hamiltonian complexity has flourished [5–10].

At the heart of the proof of QMA-completeness of the k-local Hamiltonian lies the circuit-to-Hamiltonian construction, which maps the unitary evolution of quantum states described by a quantum circuit to the ground states of a Hamiltonian operator. This procedure thus effectively encodes the computation within the Hamiltonian's ground space, or kernel when thought of as a linear operator. The key idea is that accepting computations will have low-energy eigenstates (below a), whereas rejecting ones will not (above b). The gap $a - b$ in energies is taken to be lower bounded by an inverse polynomial in the size of the problem input. The associated QMA-hard problem is thus to approximate the ground-state energy to polynomial accuracy.

Since Kitaev's work, the framework and models of quantum computation have evolved beyond the unitary quantum circuit model, with many of these models being motivated by ideas in physics. Such examples include the Knill-Laflamme-Milburn (KLM) [11] scheme for universal quantum computation with linear optics, and measurement-based quantum computing (MBQC) [12,13], whereby universal quantum computation is achieved by a sequence of (single-qubit) measurements made on an entangled resource state. Crucially, the circuit model and MBQC can simulate one another, and are of equivalent computational power.

The tool of postselection was introduced by Aaronson [14], who showed that given the ability to postselect, quantum circuits could solve PP-complete problems. PP is a powerful complexity class, containing both NP and QMA [14–16]. Postselection similarly boosts the power of classical computation, although it is interesting to note that quantum computing taken in conjunction with postselection is more powerful than with just classical computation.

The probability of the event upon which we postselect can be exponentially small in the input size. Indeed, otherwise the postselected computation could be simulated by running the computation a polynomial number of times. Yet, at the same time, postselection is a useful tool in quantum computational complexity. For example, there is now a growing body of evidence showing that sampling from the distributions produced by restricted, nonuniversal, quantum circuits is hard for a classical computer. By adding postselection to our computational toolbox, sampling problems such as boson sampling [17] and IQP sampling [18,19] can be shown to be hard to efficiently classically simulate.

*ucapnus@ucl.ac.uk

In the following, we investigate the construction of natural versions of the k-local Hamiltonian problem from nonunitary quantum computation, which will bring in considerations connected to postselection and which we shall study via computational complexity.

Result 1. Proposition 1 provides a generalization of the Feynman-Kitaev construction encoding unitary evolution to the case of nonunitary evolution. This is achieved by considering evolution via measurements, as seen in MBQC, which is implemented by renormalized projectors.

Result 2. Motivated by this construction, we introduce tame postselection; we then show that this kind of postselection limits the computational complexity of the computations encoded in the ground space of our Hamiltonians constructed from nonunitary evolution.

Result 3. We numerically investigate the scaling of the smallest nonzero eigenvalue in postselected quantum circuits. This is achieved by considering tame postselection gadgets, such as the Hadamard gadget from IQP sampling [18], and study its associated Hamiltonian, where we find two radically different behaviors. In one case, the gap scales as an inverse exponential while, in the other, it scales as an inverse polynomial. This suggests that the probability of the postselected event succeeding is not immediately connected to the gap in the Hamiltonian, which makes the connection between the k-local Hamiltonian problem and nonunitary computation very subtle.

The paper proceeds as follows. In Sec. II, we review the k-local Hamiltonian problem and its associated computational complexity class QMA. In particular, we highlight the role of the circuit-to-Hamiltonian construction in Kitaev's original proof that k-local Hamiltonian is QMA-complete. In Sec. III we introduce the formalism for constructing versions of the k-local Hamiltonian problem from quantum circuits with postselection. Given this construction, we then consider what we call tame postselection as motivated by the study of MBQC in Sec. IV and show that the computational complexity of a version of QMA where the circuits include tame postselection is only as powerful postselected quantum computing alone. We then discuss the connection between these forms of computations and forms of the k-local Hamiltonian problem with an exponentially small gap $a-b$. We then go on to give numerical evidence that certain postselected circuits (where we postselect on exponentially unlikely events) can still give rise to Hamiltonians with gaps that are inverse polynomially bounded. Finally, in Sec. V we end with some discussion about future directions of research.

II. k-LOCAL HAMILTONIAN PROBLEM

The dynamics of many-body quantum systems are described by a Hamiltonian operator. Typical Hamiltonians studied within condensed-matter physics are described as a sum of Hermitian operators that act on a number k of subsystems, which are then said to be k local. Despite this simplicity, the matrix representation of a Hamiltonian operator acting on n qubits is of dimension exponential in n. Therefore, computing its properties, such as the ground state or ground-state energy by brute force diagonalization can be hard. Although it may seem natural to use quantum computers to compute such properties of Hamiltonians, quantum Hamiltonian complexity tells us that this would still be a hard task. In order to further understand this we must formalize the problem of interest and its associated complexity class.

Definition 1. The k-local Hamiltonian problem: given a k-local Hermitian operator $H=\sum_{i=1}^{r(n)} H_i$, $||H_i|| \leqslant t(n)$ and two real numbers $0 \leqslant a \leqslant b$ such that $b-a > \frac{1}{s(n)}$, and $r(n)$, $s(n)$, and $t(n)$ are polynomials, determine if $\lambda_{\min}(H) < a$ or $\lambda_{\min}(H) > b$, given the promise that one of these is the case and where $\lambda_{\min}(H)$ denotes the smallest eigenvalue of the operator H.

This problem is QMA-complete. That is, it is in the complexity class QMA and every problem in QMA may be reduced to it. For the sake of completeness, we present the definition of this complexity class. A computation begins with a classical input x of size n encoded in binary representation and ends with a single bit as output. In general, we wish to determine whether the input is a *yes* instance (output bit is 1) or a *no* instance (output bit is zero). That is, whether it belongs to the set of strings $\mathcal{L}_{yes}$ whose output is accepting or to the set of rejecting outputs $\mathcal{L}_{no}$, promised that it does indeed belong to one of these two sets.

The class QMA stands for quantum Merlin Arthur, where we imagine that Arthur, who has limited computational power, wishes to determine whether a given input x belongs to a language. To do so, he not only has access to a quantum computer, but also to a quantum state, the alleged proof $|\psi\rangle$. This proof state is given to him by Merlin, a computationally unbounded agent. Effectively, this is the quantum probabilistic analog of the class NP, whose *yes* instances have polynomial size proofs.

We need to be more precise about the quantum computation that Arthur does on the quantum state $|\psi\rangle$. First, there are $v(n)$ qubits in the quantum state $|\psi\rangle$ and the quantum computer is a quantum circuit with $w(n)$ quantum gates acting on $y(n)+v(n)$ qubits, where $v(n)$, $w(n)$, and $y(n)$ are polynomial functions in n. The description of the quantum gates and the specification of their sequence is efficiently generated by a classical computer in time at most polynomial in n, thus giving a so-called uniform family of quantum circuits $\{V_x\}$ that have a description which depends on the input x. The circuits take $|\psi\rangle|00\ldots0\rangle$ as an input quantum state, where $|00\ldots0\rangle$ is the state of $y(n)$ qubits initialized in the state $|0\rangle$. Then, after all of the $w(n)$ gates have been applied, there is a measurement in the computational basis $\{|0\rangle,|1\rangle\}$ made on the first qubit to decide the classical output of the computation: the outcome of this measurement is represented by a bit $q_{out} \in \{0,1\}$. This is typically a probabilistic process, and so we allow an error probability ϵ for Arthur's computer to output the wrong answer. We now have the ingredients for defining QMA.

Definition 2. A promise problem $\mathcal{L}=(\mathcal{L}_{yes},\mathcal{L}_{no})$ is in QMA if for an input $x \in \{0,1\}^n$, there exists a uniform family of quantum circuits $\{V_x\}$ taking $|\psi\rangle|00\ldots0\rangle$ as input, and with bit value $q_{\text{out}} \in \{0,1\}$ as an outcome of a measurement on the first qubit in the basis $\{|q_{\text{out}}\rangle\}$, such that

$$\begin{aligned} x \in \mathcal{L}_{yes} \quad &\text{if} \quad \exists|\psi\rangle, \quad \text{such that} \quad \mathrm{P}[q_{\text{out}}=1] \geqslant \alpha, \\ x \in \mathcal{L}_{no} \quad &\text{if} \quad \forall|\psi\rangle, \quad \mathrm{P}[q_{\text{out}}=1] \leqslant \beta, \end{aligned}$$

such that $\alpha-\beta \geqslant 1/poly(n)$, where $poly$ is a polynomial.

It should be noted that NP is contained in QMA. In the next subsection we will give an overview of the proof that k-local Hamiltonian is QMA-complete. The central idea is to build a Hamiltonian whose ground state encodes the computation performed in a QMA computation such that the energy of the Hamiltonian is bounded below a if and only if $x \in \mathcal{L}_{yes}$, and above b if and only if $x \in \mathcal{L}_{no}$.

QMA-completeness of the k-local Hamiltonian problem

The proof that the k-local Hamiltonian problem is QMA-complete proceeds in two parts: first, it is shown to be in QMA and then it is shown to be QMA-hard. The first part relies on effectively sampling the Hamiltonians energy given copies of the ground state. If there exist states with energy below a, then a quantum computer will be able to check this is correct, provided it is given an efficient description of the ground state as a proof state. On the other hand, if no low-energy state exists, then Merlin cannot send any state to convince us that the ground-state energy is near zero. Here, we shall focus on the hardness proof which relies on the circuit-to-Hamiltonian construction, whereby Arthur's quantum computation is translated into a Hamiltonian such that its lowest-eigenvalue eigenstate describes the evolution of a quantum state during that computation.

Feynman had the original insight that the discrete time evolution of a quantum system can be encoded in a Hamiltonian by constructing an operator whose kernel contains each evolution state [2]. The system is assumed to be in an initial state $|\psi_0\rangle$ at time step zero and evolves, via a sequence of intermediate states $|\psi_i\rangle$, to a final state $|\psi_L\rangle$ at time step L.

Now, in order to track the discrete time evolution of the system, a clock register is appended. For example, this could be a pointer particle moving to the left or to the right of a one-dimensional lattice. Here, a hop to a site to the right corresponds to a clock transition from time step t to $t+1$. As in quantum computation operations are reversible, the particle is also allowed to move to the left. Thus L time steps require $L+1$ qubits, although we note that there exist more efficient clock constructions [5].

The history state $|\eta\rangle$ corresponds to the equal superposition over all correct evolution states:

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{i=0}^{L} |\psi_i\rangle_{\text{sys}} \otimes |i\rangle_{\text{clock}},$$

where it suffices to indicate the quantum system and clock register. The state $|\eta\rangle$ should be contained within the kernel of the constructed Hamiltonian, which consists of operators acting on the Hilbert spaces associated with both the system and the clock as indicated by the above history state. Thus the ground state describes the history of the computation acting on the input state $|\psi_0\rangle_{\text{sys}}$.

First, the unitary V_x enacted by Arthur in a QMA computation is decomposed into a polynomial sequence of single- and two-qubit gates $V_x = U_L \dots U_1$, which are picked from a universal gate set. Thus we may generically consider the gates to be applied sequentially, one after the other, the gate U_j being applied after j time steps, resulting in the input state $|\psi\rangle|00\dots0\rangle$ having evolved to $U_j \dots U_1|\psi\rangle|00\dots0\rangle$. The history state of the computation can thus be expressed as

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{j=1}^{L} U_j \dots U_1|\psi\rangle|00\dots0\rangle \otimes |j\rangle.$$

The next step is to construct a Hamiltonian operator H such that the history state lies within its kernel. This will be made up of three Hamiltonians: an input, a propagation, and an output Hamiltonian. The role of the input Hamiltonian H_{in} is to verify that the ancillary qubits Arthur has access to are correctly initialized to the state $|00\dots0\rangle$. This is attained by having an operator that projects onto the subspace orthogonal to $|00\dots0\rangle$ but projects onto the clock state being $|0\rangle$. Next, the propagation Hamiltonian ensures the correct unitary operators are applied at each time step. It is defined as the sum of the individual propagation Hamiltonian terms $H_{\text{prop}} = \sum_{j=1}^{L} H_j$, where H_j contains the evolution from time step $j-1$ to j. In this time step, a state $|\psi\rangle$ evolves to a new state as the result of a unitary operator U_j being applied, giving a component of the history state proportional to

$$|\psi\rangle \otimes |j-1\rangle + U_j|\psi\rangle \otimes |j\rangle,$$

which can easily be verified to lie within the kernel of

$$H_j = \tfrac{1}{2}(-U_j \otimes |j\rangle\langle j-1| - U_j^\dagger \otimes |j-1\rangle\langle j| + \mathbb{I} \otimes |j\rangle\langle j| + \mathbb{I} \otimes |j-1\rangle\langle j-1|).$$

Finally, at time step L, the output qubit q_{out} is measured in the computational basis, which in the case of an accepting computation yields the outcome $|1\rangle$. In this case, the resulting output state resides in the null space of $H_{\text{out}} = |0\rangle\langle 0|_{q_{\text{out}}} \otimes |L\rangle\langle L|$, which acts on the output qubit and clock system and applies identity to all other systems.

The task at hand is to now compute the smallest eigenvalue of the Hamiltonian $H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$. By defining the change of basis operator $W = \sum_{j=1}^{L} U_j \dots U_1 \otimes |j\rangle\langle j|$ and the state $|\phi\rangle = \frac{1}{\sqrt{L+1}} \sum_{i=1}^{L} |i\rangle$, the history state can be expressed as $|\eta\rangle = W(|\psi\rangle|00\dots0\rangle \otimes |\phi\rangle)$. Thus we can now consider $|\psi\rangle|00\dots0\rangle \otimes |\phi\rangle$ to be in the kernel of the operator $W^\dagger H W$, a simpler operator which nonetheless conserves the spectrum.

From here, the task is to show that if $x \in \mathcal{L}_{yes}$, then the minimum eigenvalue of H is less than a, whereas if $x \in \mathcal{L}_{no}$, then it is greater than b, where $b - a \geqslant \frac{1}{\text{poly}(n)}$; see [3]. This ends our summary of some of the key ideas used in the proof of QMA-completeness of the k-local Hamiltonian problem. The core idea was to see how the construction of the Hamiltonian H relates directly to deciding a problem in QMA. In the next section we will generalize this construction, in particular by building a propagation Hamiltonian that allows for nonunitary evolutions, leaving the other terms in the Hamiltonian essentially unchanged.

III. LOCAL HAMILTONIANS FROM POSTSELECTED QUANTUM CIRCUITS

Measurements are a key component in quantum computation, and even more so in MBQC whereby they drive the computation. As both the circuit model and MBQC are equivalent in terms of computational power, the complexity class QMA

could equally be defined as an MBQC, where part of the resource state is prepared by Merlin. However, in the proof of the k-local Hamiltonian being QMA-complete, the Hamiltonian construction is made with respect to the quantum circuit model, with a single measurement performed at the end of the computation. Thus we now consider how nonunitary evolution due to projective measurements can be encoded into Hamiltonians.

A. Evolution via renormalized projection

We now consider the process whereby a projective measurement is applied to a pure state, yielding an outcome m. We thus now imagine the evolution of a state $|\psi\rangle$ at time t to a new state $|\psi'\rangle = L|\psi\rangle$ at time $t+1$, where the operator L is proportional to a projector, that is $L = \Pi/\sqrt{\langle\psi|\Pi|\psi\rangle}$ and where Π is a projector.

Previously, we considered the unitary time evolution of a system from t to $t+1$ and constructed the associated history state of the system and the clock register. We now follow the same approach in order to obtain a new history state, this time corresponding to an evolution obtained via measurement:

$$|\eta\rangle = |\psi\rangle \otimes |t\rangle + L|\psi\rangle \otimes |t+1\rangle. \tag{1}$$

In the next result, we now spell out a Hamiltonian H_t in which this history state $|\eta\rangle$ lives.

Proposition 1. Given a projective measurement $\{\Pi, \mathbb{I}-\Pi\}$ at time step t, for the measurement outcome on state $|\psi\rangle$ corresponding to projector Π occurring with probability $p = \langle\psi|\Pi|\psi\rangle$ independent of input state $|\psi\rangle$, the un-normalized history state $|\eta\rangle = |\psi\rangle \otimes |t\rangle + L|\psi\rangle \otimes |t+1\rangle$ lies in the kernel of

$$H_t = \frac{p}{p+1}\left[L \otimes \left(\frac{1}{\sqrt{p}}|t\rangle\langle t| - |t\rangle\langle t+1| - |t+1\rangle\langle t| + \sqrt{p}|t+1\rangle\langle t+1|\right)\right] + (\mathbb{I}-\Pi) \otimes |t+1\rangle\langle t+1|, \tag{2}$$

for $L = p^{-\frac{1}{2}}\Pi$.

Proof. Since the span of the clock states $\{|t\rangle, |t+1\rangle\}$ is a two-dimensional Hilbert space, the operator H_t can be decomposed as

$$H_t = N\big(H_{11} \otimes |t\rangle\langle t| + H_{12} \otimes |t\rangle\langle t+1| + H_{21} \otimes |t+1\rangle\langle t| + H_{22} \otimes |t+1\rangle\langle t+1|\big), \tag{3}$$

where N is a normalization constant and H_{ij} is an operator acting on the system with initial state $|\psi\rangle$. The requirement for the history state $|\eta\rangle$ to satisfy $H|\eta\rangle = 0$ leads to

$$N(H_{11}|\psi\rangle + H_{12}L|\psi\rangle \otimes |t\rangle + H_{21}|\psi\rangle \otimes |t+1\rangle + H_{22}L|\psi\rangle \otimes |t+1\rangle) = 0.$$

As the operator H_t is constrained to be Hermitian, we have that $H_{21} = H_{12}^\dagger$. This produces the following system of equations:

$$H_{11}|\psi\rangle + H_{12}L|\psi\rangle = 0,$$
$$H_{12}^\dagger|\psi\rangle + H_{22}L|\psi\rangle = 0.$$

A natural solution to the above set of equations is given by $H_{11} = \frac{1}{p}\Pi$, $H_{12} = -\frac{1}{\sqrt{p}}\Pi$, and $H_{22} = \Pi$, thus yielding the operator

$$H_t = N\Pi \otimes \left(\frac{1}{p}|t\rangle\langle t| - \frac{1}{\sqrt{p}}|t\rangle\langle t+1| - \frac{1}{\sqrt{p}}|t+1\rangle\langle t| + |t+1\rangle\langle t+1|\right). \tag{4}$$

We now, without loss of generality, constrain the operator H_t to be a projector, i.e., $H_t^2 = H_t$. But, we note that we now have that $H^2 = cH$, where

$$H_t^2 = N^2\left(1+\frac{1}{p}\right)\Pi \otimes \left(\frac{1}{p}|t\rangle\langle t| - \frac{1}{\sqrt{p}}|t\rangle\langle t+1| - \frac{1}{\sqrt{p}}|t+1\rangle\langle t| + |t+1\rangle\langle t+1|\right), \tag{5}$$

and where $c = N(1+p^{-1})$. This thus leads to a normalization constant N which depends on the outcome probability p, i.e., $N(p) = p/(p+1)$.

By construction, the Hamiltonian H_t contains the history state $|\eta\rangle$ in its kernel. But, the question is now whether the kernel contains any other states. And indeed, due to the orthogonality of the projectors in the measurement, there will be states lying in an orthogonal subspace of the projector Π, that is of the form $(\mathbb{I}-\Pi)|\psi\rangle \otimes |t'\rangle$, in particular for $t' = t$ and $t' = t+1$. In order to exclude these states from the kernel, we add the following term to the Hamiltonian H_t $(\mathbb{I}-\Pi)^\perp \otimes |t+1\rangle\langle t+1|$ to H_t, and we thus finally obtain

$$H_t = N(p)\left[\frac{1}{\sqrt{p}}\Pi \otimes \left(\frac{1}{\sqrt{p}}|t\rangle\langle t| - |t\rangle\langle t+1| - |t+1\rangle\langle t| + \sqrt{p}|t+1\rangle\langle t+1|\right)\right] + (\mathbb{I}-\Pi) \otimes |t+1\rangle\langle t+1|, \tag{6}$$

for $N(p) = p/(p+1)$. This concludes the proof. ■

We can now consider a circuit of T time steps where at each time step either a unitary or a renormalized projector is sequentially applied to the input state $|\psi\rangle|00\ldots0\rangle$. That is, the computation evolves in layers of unitary evolution and measurements. For example, after T time steps of a

circuit in which a unitary U_i is alternated with a renormalized projector L_j, the state of the system would be $|\psi_T\rangle = U_T L_{T-1} \dots L_2 U_1 |\psi\rangle$. The history state $|\eta\rangle$ is then

$$|\eta\rangle = \frac{1}{T+1} \times (|\psi\rangle \otimes |0\rangle + \dots + U_T L_{T-1} \dots L_2 U_1 |\psi\rangle \otimes |T\rangle),$$

which is in the kernel of the Hamiltonian $H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$ with H_{in} and H_{out} as defined before and now

$$H_{\text{prop}} = \sum_{i=0}^{T/2} H_{2i}^{\text{unitary}} + \sum_{j=1}^{T/2} H_{2j-1}^{\text{post}}, \tag{7}$$

with H_i^{unitary} and H_j^{post} being operators of the form in Eq. (1) and in Proposition 1, respectively. Therefore, evolution involving measurements can be encoded into a Hamiltonian in a natural extension of the Kitaev-Feynman approach.

Of course the above evolution corresponds to conditioning on a particular outcome occurring, i.e., postselection. Here, postselection is modeled by the renormalized projector, but crucially relies on the quantum state to dictate the norm of this renormalized projector. Indeed this is one of the major modifications to the k-local Hamiltonian problem when we consider postselection. Here, the operator norm of the individual evolution terms H_j^{post} in the Hamiltonian may not be bounded by a polynomial in the input size to the problem. For indeed, if the probability p of a particular event happening is exponentially small, then the operator norm will be upper bounded by an exponential.

B. Tame postselection

Clearly given evolution involving general postselection, to construct the above Hamiltonian with the history state in its kernel we will need to know the initial quantum state $|\psi\rangle$ to calculate the renormalized projectors. However, a crucial aspect of the k-local Hamiltonian problem is that it is defined independent of its ground state. Therefore, to get around these issues we study the concept of tame postselection. Here, the initial state $|\psi\rangle|00\dots0\rangle$ evolves to $U|\psi\rangle|00\dots0\rangle$ via unitary evolution, before a projective measurement $\{\Pi, \mathbb{I} - \Pi\}$ is applied to the system. We then postselect on the outcome associated with Π occurring, and have that the probability of obtaining this outcome is independent of the initial state $|\psi\rangle$. Note that the probability of obtaining the outcome could be exponentially small in the size of $|\psi\rangle$. We emphasize that we only demand that the probability be independent of only $|\psi\rangle$; it could vary if we replace the state $|00\dots0\rangle$ with another (known) quantum state.

Definition 3. Given a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{anc}}$ consisting of a system with space $\mathcal{H}_{\text{sys}}$, and an ancillary system with space $\mathcal{H}_{\text{anc}}$ (both with the same dimension), in an initial quantum state $|\phi\rangle = |\psi\rangle|0\rangle$ such that $|\psi\rangle \in \mathcal{H}_{\text{sys}}$ and $|0\rangle \in \mathcal{H}_{\text{anc}}$, if a unitary U is applied to $|\phi\rangle$ followed by a projective measurement $\{\Pi_k := |k\rangle\langle k|\}_k$ with outcomes $\{k\}$ applied to the system $\mathcal{H}_{\text{sys}}$, then postselection on a particular outcome k' is tame postselection if $p(k') := \langle\psi|\langle 0|U^\dagger(\Pi_{k'} \otimes \mathbb{I}_{\text{anc}})U|\psi\rangle|0\rangle$ is the same for all $|\psi\rangle \in \mathcal{H}_{\text{sys}}$.

An example of tame postselection would be the Hadamard gadget, which was used in Ref. [18] to show the classical hardness of IQP sampling. This is a method of implementing a Hadamard gate via measurement and postselection, as illustrated in Fig. 1. Here, a qubit in an arbitrary state $|\psi\rangle$ is entangled with an ancilla (initialized in the fixed $|+\rangle$ state) via a controlled-Z operator $|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes Z$, with Z being the Pauli-Z operator. Then, the first qubit is measured in the Pauli-X basis $\{|+\rangle, |-\rangle\}$ and we postselect upon obtaining the outcome associated with state $|+\rangle$. This results in the state on the second qubit being $H|\psi\rangle$. Here, the probability of obtaining the measurement outcome is $1/2$ for both outcomes, and thus is independent of the state $|\psi\rangle$. On the other hand, if we were to alter the ancilla to have a state other than $|+\rangle$, this probability could change. This helps us emphasize that tame postselection is tame with respect to a particular "input" subsystem.

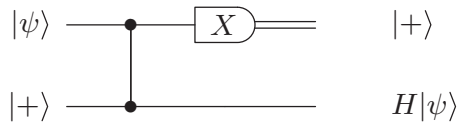

FIG. 1. Hadamard gadget. A measurement of the Pauli-X observable is performed on the first qubit. By postselecting on obtaining the outcome $+1$ corresponding to eigenvector $|+\rangle$, a Hadamard gate is applied to the unmeasured qubit.

This postselection results in a unitary operator being applied to the unmeasured system, a concept which is at the core of MBQC wherein unitary evolution is simulated by measurements. We generalize this kind of postselection "gadget" in the following result.

Proposition 2. Let $|\psi\rangle|E\rangle$ be a quantum state in a Hilbert space $\mathcal{H} = \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{env}}$, where $|\psi\rangle \in \mathcal{H}_{\text{sys}}$ and $|E\rangle \in \mathcal{H}_{\text{env}}$, and the two Hilbert spaces have the same dimension. Suppose a unitary operator U is applied to the joint system, followed by a projective measurement on $\mathcal{H}_{\text{sys}}$ in the orthonormal basis $\{|e_k\rangle\}$, as illustrated in Fig. 2. Let $p_m = \langle E|\langle\psi|(|e_m\rangle\langle e_m| \otimes \mathbb{I})|\psi\rangle|E\rangle$ denote the probability of outcome m occurring. Then, if p_m is independent of the state $|\psi\rangle \in \mathcal{H}_{\text{sys}}$, the action of this process on the system is equivalent to applying $\sqrt{p_m}V_m$ to $|\psi\rangle$, where V_m is a unitary operator.

Proof. The system is prepared in the state $|\psi\rangle \in \mathcal{H}_{\text{sys}}$ and is initially uncorrelated with the environment $|E\rangle \in \mathcal{H}_{\text{env}}$. A unitary operator U acting on the joint state space $\mathcal{H} = \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{env}}$ is applied, followed by a projective measurement of an orthonormal basis $\{|e_k\rangle\}$ of the system, as shown in Fig. 1. The resulting evolution (up to normalization factors) is given by

$$\rho \otimes |e_0\rangle\langle e_0| \to \Pi_m U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \Pi_m, \tag{8}$$

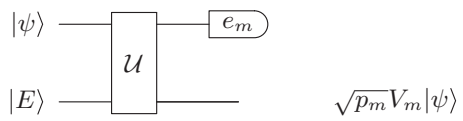

FIG. 2. Unitary operator is applied to an unknown state $|\psi\rangle$ and an ancilla, before the system is measured. This results in subnormalized unitary being applied to the ancilla.

where m denotes the obtained measurement outcome associated with projector $\Pi_m = |e_m\rangle\langle e_m| \otimes \mathbb{I}$ and $\rho = |\psi\rangle\langle\psi|$. We can consider the state ρ'_{env} of the environment system with Hilbert space $\mathcal{H}_{\text{env}}$ after the application of U and measurement Π_m, which is then the effective image of a map $\mathcal{K}_m$ on input state ρ, i.e., $\rho' = \mathcal{K}_m(\rho) = \text{tr}_{\text{sys}}(K_m|\psi\rangle\langle\psi|K_m^\dagger)$, where the K_m associated with outcome m is defined as

$$K_m = ((\Pi_m \otimes \mathbb{I})U(\mathbb{I} \otimes |E\rangle\langle E|)).$$

Therefore, upon tracing out the system in $\mathcal{H}_{\text{sys}}$, we have an effective map on the state ρ of $L_m \rho L_m^\dagger$ with $L_m = \langle e_m|U(\mathbb{I} \otimes |E\rangle\langle E|)$. Here, we demand that the outcome probability p_m be independent of the input state, i.e., $p_m = \langle\psi|L_m^\dagger L_m|\psi\rangle, \forall\ |\psi\rangle$. The only way this is satisfiable for all input states is if $L_m^\dagger L_m = p_m\mathbb{I}$. This, in turn, means that L_m must be proportional to a unitary operator V_m, such that $L_m = \sqrt{p_m}V_m$. ■

Clearly, the Hadamard gadget is one such example of a process as outlined in this result. It shows that the tame postselection we consider corresponds to applying a unitary in the input state $|\psi\rangle$ after renormalizing by the probability of getting that outcome. Thus if we wish to encode a tame postselection into a Hamiltonian as previously outlined, then a renormalized unitary evolution will be encoded, which is a subtle alteration of the Kitaev-Feynman construction. However, as we will discuss next, this postselection can also be used to solve very powerful computations.

C. Computational complexity of postselected quantum circuits

We consider quantum circuits in which postselection is given "for free," i.e., we can decide the property of an input conditioned on the outcome of some measurement. Aaronson was the first to define the complexity class PostBQP as the class of decision problems which can be decided by a quantum circuit that is of size polynomial in the input size that utilizes postselection [14]. To be more formal, for an input x of size n, a classical machine generates a description of a quantum circuit C_x in time at most polynomial in n; hence it is a uniform circuit. This quantum circuit takes as input the state $|00\ldots0\rangle$, and has a set of postselection qubits, and an output qubit. A measurement in the computational basis $\{|0\rangle,|1\rangle\}$ is made on both the postselection and output qubits, with the classical bit strings q_{post} and q_{out} as the outcomes, respectively. The circuit then postselects on getting $q_{\text{post}} = (0,0\ldots0) := 0$, and then conditioned on these outcomes, the circuit decides whether to accept an input (if $q_{\text{out}} = 1$) or not. We allow this decision process to fail with some nonzero probability, thus giving us the following complexity class.

Definition 4. A promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ is in PostBQP if for an input $x \in \{0,1\}^n$, there exists a uniform quantum circuit family $\{C_x\}$ with each C_x taking $|00\ldots0\rangle$ as input, and with postselection and output qubits, which are all measured in the computational basis and giving outcomes as bit strings q_{post} and q_{out} such that

$$\text{if } x \in \mathcal{L}_{yes}, \quad \text{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] \geqslant 2/3,$$
$$\text{if } x \in \mathcal{L}_{no}, \quad \text{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] \leqslant 1/3,$$

where $\text{P}[q_{\text{post}} = 0] \geqslant 2^{-poly(n)}$ and $poly$ is some polynomial function.

We need the constraint that $\text{P}[q_{\text{post}} = 0] \geqslant 2^{-poly(n)}$ so that we have a consistent definition of PostBQP: for any choice of universal gate set for the circuit C_x we get exactly the same complexity class. This subtlety has been discussed and addressed by Kuperberg [20]. It should also be noted that the number of qubits being postselected does not make any difference to the class as long as it is polynomial in the size of the input: for example, a circuit with only one postselection qubit can be simulated by a circuit with $m > 1$ postselection qubits by having $m-1$ of the postselection qubits be prepared in the state $|0\rangle$ and not have any unitary act on them. Also, any circuit containing intermediate postselected measurements can be simulated by one with only postselection at the end on the registry by using the technique of deferring measurements at the cost of introducing a new ancilla [14]. Aaronson first proved that PP $\subseteq$ PostBQP, and claimed to prove that PostBQP $\subseteq$ PP, but without putting a bound on the probability $\text{P}[q_{\text{post}} = 0]$. Here PP is the set of languages that are decided by probabilistic Turing machine with unbounded error, i.e., the error can be arbitrarily close to $1/2$. As mentioned earlier this is a relatively large complexity class in that it contains both NP and QMA (and thus BQP). As mentioned, Kuperberg pointed out this oversight, and if one bounds the probability as we have done, the containment PostBQP $\subseteq$ PP is indeed true, as pointed out in the following theorem.

Theorem 1 (Aaronson and Kuperberg [14,20]). PostBQP = PP.

Therefore, if we consider quantum computations with postselection we have access to great computational power. Equally, if we encode these computations in the ground state of a Hamiltonian through the Kitaev-Feynman construction, then given access to this state we have access to this computational power. In this section we want to formalize the computational complexity of the computations that are being translated into Hamiltonians through this construction. In particular, if this computation involves postselection, what is the computational complexity of a circuit that takes an arbitrary state (a proof state) with some fixed ancilla qubits, and subjects it to unitary evolution and postselection as well as a final measurement?

Just as QMA contains BQP, but is distinct since it allows for access to quantum proof states, we now consider the analog of QMA that allows for postselection in Arthur's computation and thus contains PostBQP; naturally, we call this analog PostQMA, where we have that PostBQP $\subseteq$ PostQMA. The main difference between PostBQP and PostQMA is that, in the latter, a proof state $|\psi\rangle$ is an input into a quantum circuit, and without loss of generality we will fix it such that the size of the postselection register is the same size as the state $|\psi\rangle$. We will argue that we can do this after presenting the definition as follows.

Definition 5. A promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ is in PostQMA if for an input $x \in \{0,1\}^n$, there exists a uniform quantum circuit family $\{V_x\}$ with each V_x taking $|\psi\rangle|00\ldots0\rangle$ as input and $|\psi\rangle$ consisting of a number of qubits w at most polynomial in n, and with postselection and output qubits, which are all measured in the computational basis and giving outcomes as bit strings $q_{\text{post}} \in \{0,1\}^w$ and $q_{\text{out}} \in \{0,1\}$ such

that

$$\text{if } x \in \mathcal{L}_{yes}, \quad \exists|\psi\rangle \ \mathrm{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] \geqslant 2/3,$$
$$\text{if } x \in \mathcal{L}_{no}, \quad \forall|\psi\rangle \ \mathrm{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] \leqslant 1/3,$$

where $\mathrm{P}[q_{\text{post}} = 0] \geqslant 2^{-poly(n)}$, and $poly$ is some polynomial function.

The first thing to observe about this class is that, as expected, PostBQP is contained in PostQMA, since the circuit could just "ignore" the input $|\psi\rangle$ and replace it with the all-zeros input $|00\ldots0\rangle$, and we recover those computations in PostBQP. Also, as mentioned, it is not a restriction to have the postselection register have w qubits (i.e., the same size at the proof state $|\psi\rangle$). Given a circuit where postselection is on fewer than w qubits, we can pad out the size of the register with ancillas prepared in the state $|0\rangle$. If a circuit has more than w qubits in the postselection register, then we can just take the NOR of measurement outcomes to reduce to the register being of size w. Also, again intermediate postselected measurements do not affect the computational complexity for the same reasons they do not alter PostBQP. Finally, we note that since developing our results, independent work by Morimae and Nishimura showed that PostQMA = PSPACE [21], thus showing that tame postselection is a genuine limitation from a complexity theoretic point of view.

In our work we are concerned with tame postselection as defined earlier in Definition 3. In the definition, we can map every element to a postselected quantum circuit. The ancillary system $\mathcal{H}_{\text{anc}}$ is the input to the quantum circuit initiated to the state $|00\ldots0\rangle$, the system $\mathcal{H}_{\text{sys}}$ is associated with the proof given from Merlin in state $|\psi\rangle$, the unitary U acting on $\mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{anc}}$ is the unitary in the quantum circuit, and the postselection register is the set of qubits of $\mathcal{H}_{\text{sys}}$ with the projector Π_k being $|00\ldots0\rangle\langle00\ldots0|$. Therefore, tame postselection is the condition that the probability of $q_{\text{post}} = 0$ is the same for all states $|\psi\rangle$.

Given all of the above elements we can consider the complexity class PostQMA* associated with postselected circuits such that they satisfy tame postselection. We also see the convenience of having the postselection register being the size of the proof state since the first w qubits of the circuit can be the proof system, and without loss of generality, the postselection register is again the first w qubits of the circuit. This circuit is then an example of tame postselection as in Definition 3. The following definition of PostQMA* can now be presented.

Definition 6. A promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ is in PostQMA* if for an input $x \in \{0,1\}^n$, there exists a uniform quantum circuit family $\{V_x\}$ with each V_x taking $|\psi\rangle|00\ldots0\rangle$ as input and $|\psi\rangle$ consisting of a number of qubits w at most polynomial in n, and with postselection and output qubits, which are all measured in the computational basis and giving outcomes as bit strings $q_{\text{post}} \in \{0,1\}^w$ and $q_{\text{out}} \in \{0,1\}$ such that

$$\text{if } x \in \mathcal{L}_{yes}, \quad \exists|\psi\rangle \ \mathrm{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] \geqslant 2/3,$$
$$\text{if } x \in \mathcal{L}_{no}, \quad \forall|\psi\rangle \ \mathrm{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] \leqslant 1/3,$$

where $\mathrm{P}[q_{\text{post}} = 0] \geqslant 2^{-poly(n)}$ and is the same for all $|\psi\rangle$ and $poly$ is some polynomial function.

At first sight, given Proposition 2, it might not seem obvious that PostQMA* is a class more powerful than QMA since tame postselection results in unitary evolution of $|\psi\rangle$ up to renormalization. However, following similar arguments as outlined earlier with regard to ⊆PostQMA, we have that PostBQP ⊆ PostQMA* ⊆ PostQMA; therefore, PP ⊆ PostQMA*. In particular, to show that PostBQP ⊆ PostQMA*, Arthur can just "replace" the state $|\psi\rangle$ with the all-zeros state, $|00\ldots0\rangle$, and this is permitted by the definition of PostQMA*. That is, take a circuit that is used to decide a problem in PostBQP, which consists of preparing the input state $|00\ldots0\rangle$ of r qubits, feeding it into a quantum circuit with unitary U, and then postselecting on the first qubit giving outcome zero for a computational basis measurement, and accepting if the second qubit gives 1 for a computational basis measurement. This can readily be turned into a PostQMA* algorithm for an arbitrary proof state $|\psi\rangle$ of, say, $w = r$ qubits provided by Merlin (if $w \neq r$ then either the input or proof state can be padded with extra ancillas by Arthur). First, Arthur prepares $w - 1$ qubits in state $|00\ldots0\rangle := |0_{w-1}\rangle$ and the r qubits in the state $|00\ldots0\rangle := |0_r\rangle$ from the PostBQP computation. Arthur's initial quantum state is then $|\psi\rangle|0_{w-1}\rangle|0_r\rangle$; he then applies U to $|0_r\rangle$ and identity operators to all the other qubits. After the application of these unitaries, he will measure the state the $w - 1$ qubits in the state $|0_{w-1}\rangle$ and the first qubit of the system in state $U|0_r\rangle$ in the computational basis, and postselect on getting the outcome 0. This probability is independent of the state $|\psi\rangle$ since there is no interaction between Arthur's qubits prepared in the state $|0_{w-1}\rangle|0_r\rangle$ and $|\psi\rangle$. Finally, Arthur uses a measurement of the second qubit of the state $U|0_r\rangle$ to accept or reject. This construction also is compatible with the definition of PostQMA*, since the postselection register was of size w.

So far the only complexity theoretic upper bound on PostQMA* is PostQMA ⊆ NEXP, but can we do better? The next result gives a strong bound on the class PostQMA*.

Theorem 2. PostQMA* = PostBQP = PP.

Proof. As discussed earlier, we have the inclusion that PP ⊆ PostQMA*, so it remains to prove that PostQMA* ⊆ PP. We prove this using GapP functions, which is the difference between the number of accepting and rejecting paths of a nondeterministic Turing machine. More formally, given a nondeterministic Turing machine $\mathcal{N}$ and input x, then $N_{\text{acc}}(x)$ and $N_{\text{rej}}(x)$ are the number of accepting and rejecting paths of $\mathcal{N}$, respectively, given x; then a GapP function is $f(x) = N_{\text{acc}}(x) - N_{\text{rej}}(x)$ [22]. The complexity class PP is defined as those languages $\mathcal{L}$ where f and g are GapP functions such that if input x is in $\mathcal{L}$, then $2/3 \leqslant f(x)/g(x) \leqslant 1$, and if $x \notin \mathcal{L}$, then $0 \leqslant f(x)/g(x) \leqslant 1/3$.

Returning to the circuits in the class PostQMA*, the probability of accepting conditioned on a particular outcome happening is $\mathrm{P}[q_{\text{out}} = 1|q_{\text{post}} = 0] = \mathrm{P}[q_{\text{out}} = 1, q_{\text{post}} = 0]/\mathrm{P}[q_{\text{post}} = 0]$. We will show that this conditional probability is the quotient of two GapP functions and thus PostQMA* ⊆ PP. Without loss of generality we will take the universal gate set of the quantum circuits to be the Hadamard and Toffoli gates.

First, since the definition of tame postselection means that $\mathrm{P}[q_{\text{post}} = 0]$ is the same for all possible states $|\psi\rangle$, then we can evaluate this probability for the case where $|\psi\rangle = |00\ldots0\rangle$,

the all-zeros input. That is, we have a quantum circuit and wish to calculate $\mathrm{P}[q_{\mathrm{post}} = 0]$ for this circuit. Using a result of Fortnow and Rogers, this probability will be equal to $g(x)/2^{h(x)}$ for some g being a GapP function and $h(x)$ being an efficiently computable function dependent on the number of Hadamard gates in the circuit for input x [23]. However, $\mathrm{P}[q_{\mathrm{out}} = 1, q_{\mathrm{post}} = 0]$ may not be the same for $|\psi\rangle$ as it is for the all-zeros input, so we need to address this issue separately.

The complicating factor for evaluating $\mathrm{P}[q_{\mathrm{out}} = 1, q_{\mathrm{post}} = 0]$ is that it is a probability for an input state $|\psi\rangle$, so we can calculate the maximal value of this probability (for all states $|\psi\rangle$) to decide whether the input is accepted. First, we divide the qubits into the proof qubits and ancillae qubits, denoted sys and anc, respectively. Following Vyalyi [16], we can see this maximal probability as the largest eigenvalue $\lambda_{\max}$ of the operator

$$A = \mathrm{tr}_{\mathrm{anc}}((|00\ldots0\rangle\langle 00\ldots0|_{q_{\mathrm{post}}} \otimes |1\rangle\langle 1|_{q_{\mathrm{out}}}) \times V_x(\mathbb{I}_{\mathrm{sys}} \otimes |00\ldots0\rangle\langle 00\ldots0|_{\mathrm{anc}})V_x^\dagger).$$

Since $\lambda_{\max}^d \leqslant \mathrm{tr}(A^d) \leqslant 2^w \lambda_{\max}^d$, and the operator A is a $2^w - \mathrm{by} - 2^w$ operator, if we choose $d = w + 1$, then we have the following useful relationships:

$$\begin{aligned}
&\text{if } \max \mathrm{P}[q_{\mathrm{out}} = 1, q_{\mathrm{post}} = 0] \\
&= (\lambda_{\max} 2^{h(x)})/g(x) \leqslant 1/3 \\
&\Rightarrow (3/2)^{d-1}(2^{h(x)})\mathrm{tr}(A^d))/g(x) \leqslant 1/3, \\
&\text{if } \max \mathrm{P}[q_{\mathrm{out}} = 1, q_{\mathrm{post}} = 0] \\
&= (\lambda_{\max} 2^{h(x)})/g(x) \geqslant 2/3 \\
&\Rightarrow (3/2)^{d-1}(2^{h(x)})\mathrm{tr}(A^d))/g(x) \geqslant 2/3.
\end{aligned}$$

It was proven by Vyalyi that $\mathrm{tr}(A^d) = k(x)2^{-dh'(x)}$, where k is a GapP function, and $h'(x)$ is another efficiently computable function dependent on the number of Hadamards in the circuit [16]. Since $(3/2)^{d-1}2^{h(x)-dh'(x)}$ is an efficiently computable function and an efficiently computable function multiplied by a GapP function is another GapP function [22], we can define $f(x) = (3/2)^{d-1}2^{h(x)-dh'(x)}k(x)$ to obtain

$$\begin{aligned}
x \in \mathcal{L}_{yes} \quad &\text{if } f(x)/g(x) \geqslant 2/3, \\
x \in \mathcal{L}_{no} \quad &\text{if } f(x)/g(x) \leqslant 1/3,
\end{aligned}$$

if the promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ is in PostQMA* and thus PostQMA$^* \subseteq$ PP. ■

Therefore, tame postselection restricts the computational power at hand to just be that which is found in standard postselected quantum circuits without proof states. As a result, if we use the Kitaev-Feynman construction to build a Hamiltonian encoding a tame postselected quantum circuit into its null space, a state in the null space just encodes problems in PP, and nothing more powerful. This might sound very powerful since QMA $\subseteq$ PP, with equality thought unlikely to hold [16]. On the other hand, we now contrast PostQMA* with another generalization of QMA.

Lin and Fefferman described the class $\mathrm{QMA}_{\mathrm{exp}}$ in Ref. [24]. This class $\mathrm{QMA}_{\mathrm{exp}}$ is defined in the same way as QMA, except the gap between α and β now satisfies $\alpha - \beta \geqslant 2^{-poly(n)}$ for $poly$ being some polynomial in the input size n. It was proven by Lin and Fefferman that $\mathrm{QMA}_{\mathrm{exp}} = \mathrm{PSPACE}$, the class of problems decided by a deterministic classical computer using an amount of space at most polynomial in the size of the input. In addition, they also described another natural generalization of the k-local Hamiltonian problem, where the promise gap $b - a$ is permitted to be separated by only an inverse exponential, i.e., $b - a \geqslant 2^{-poly(n)}$ for some polynomial function $poly$. This problem is called the precise k-local Hamiltonian problem and was shown to be complete for $\mathrm{QMA}_{\mathrm{exp}}$.

How does $\mathrm{QMA}_{\mathrm{exp}}$ relate to PostQMA*? It is known that PP $\subseteq$ PSPACE, with good evidence that equality does not hold [25]. Therefore, with this computational complexity evidence at hand we could argue that the k-local Hamiltonian problem constructed from tame postselected quantum circuits will not be as hard to solve as an arbitrary precise k-local Hamiltonian problem. It seems that the Hamiltonians resulting from tame postselected quantum circuits could live in an intermediate regime between QMA and $\mathrm{QMA}_{\mathrm{exp}}$.

In this section we have given some evidence from computational complexity that the Kitaev-Feynman circuit-to-Hamiltonian circuit when applied to tame postselected quantum circuits can result in encoding hard computations in the ground space. However, this computation is still bounded in a sensible way, thus reinforcing the notion of it being tame. In particular, tame postselected quantum circuits will probably not have the power of $\mathrm{QMA}_{\mathrm{exp}}$ even though we are permitted to postselect on events which occur with an exponentially small probability. In the next section we will look at families of tame postselected circuits and their corresponding Hamiltonians, and in particular numerically study the gap between the ground state and the next highest energy state.

IV. POSTIQP AND HADAMARD GADGETS

It is known that the k-local Hamiltonian problem, where the promise gap scales as an inverse polynomial with system size, is QMA-complete. On the other hand, the problem where the promise gap scales as an inverse exponential is PSPACE complete. Here, we note that the problem statements are circuit independent, and that the circuit-to-Hamiltonian construction is only used in the proofs of hardness.

Thus we can ask whether, in the case of circuit families encoding evolution via renormalized projectors, the probabilities of acceptance and rejection can be mapped to that of a given complexity class. In other words, are these circuit families hard for a specified class? In order to investigate this question, we shall consider two similar though distinct circuit families and probe the behavior of the scaling of the smallest nonzero eigenvalue, as this determines the promise gap. We shall find that one circuit family has a gap scaling as an inverse exponential, whereas the other has a gap scaling as an inverse polynomial with system size.

A. Tame postselected circuits

One surprising aspect of postselection is that it can limit the kinds of circuits we need to consider to get the complexity class PostBQP. In particular, the circuit can be an instantaneous quantum polytime (IQP) circuit [18], which consists of preparing a set of qubits in the state $|0\rangle$, applying a set of

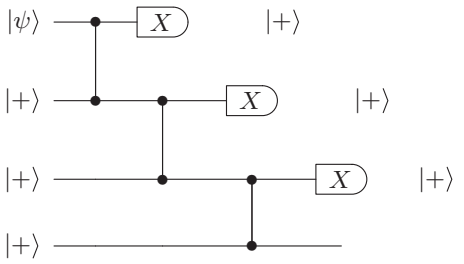

FIG. 3. Three Hadamard gadgets are implemented using three additional qubits.

unitary gates that are diagonal in the local Pauli-X basis, and then measuring in the computational basis. Since all of the unitary gates are diagonal in the same basis, they all commute with each other and can be considered to be implemented "simultaneously," in some sense. Equivalently, an IQP circuit consists of preparing a set of qubits in the state $|+\rangle$, applying a set of unitary gates that are diagonal in the local Pauli-Z basis, then Hadamard gates to all of the qubits, and finally measuring qubits in the computational basis. To be a uniform IQP circuit, given a classical input $x \in \{0,1\}^n$, the description of the gates which are diagonal in the Pauli-Z basis must be generated by a classical computer in time at most polynomial in n. By considering postselection, the complexity class PostIQP is obtained, for which Bremner, Jozsa, and Shepherd proved that PostIQP = PostBQP, the proof of which is based on the Hadamard gadget as outlined earlier. Thus postselection drastically simplifies the kinds of circuits we need to consider.

The result of all of this is that we can define PostQMA such that Arthur's circuit is an IQP circuit, and by virtue of PostQMA* = PostBQP we have exactly the same computational power. Therefore, we can restrict to considering Hamiltonians constructed from IQP circuits without loss of generality. Taking these circuits as inspiration we will consider how the gap $b-a$ of the Hamiltonian scales in the size of the postselected circuit with which we start.

We will consider two classes of postselected circuit based on the Hadamard gadget, and numerically analyze the corresponding gaps $b-a$ between the ground-state energy and the energy of the first excited state. The Hadamard gadget satisfies the notion of tame postselection and so is an ideal candidate for which we can build circuits. It should be noted that in both families of circuit the total probability of success of the postselected event decreases exponentially in the size of the circuit. However, in terms of the gap $b-a$, in one family denoted as $\mathcal{F}_1$ this appears to decrease exponentially in the size of the postselected circuit, but in the other family, denoted by $\mathcal{F}_2$, it seems to decrease polynomially in the size of the circuit. Thus the intuition that the probability of success

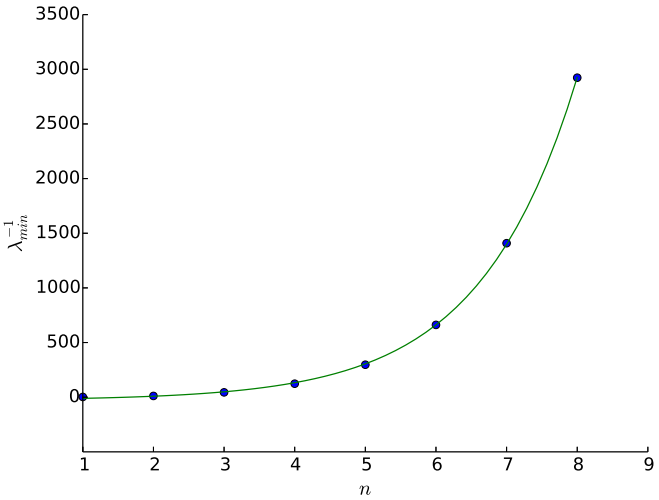

FIG. 4. Scaling of the eigenvalues of the Hamiltonian as a function of Hadamard gadgets, with Hamiltonian in Eq. (9). Here, we fit the data to an exponential function $y = A\,e^{bc} + c$, yielding $A = 8.802$, $b = 0.727$, and $c = -28.767$.

dictates the gap $b-a$ of the corresponding Hamiltonian is not immediately obvious. To emphasize this point, in both families of circuits the corresponding Hamiltonians all have terms that have operator norms that are bounded by some polynomial in the circuit size. Therefore, the circuit family $\mathcal{F}_2$ seems to encode a Hamiltonian problem contained in QMA, while family $\mathcal{F}_1$ does not.

B. Circuit family $\mathcal{F}_1$

First, we consider an arbitrary quantum state and n postselection qubits initialized in the $|+\rangle$ state. Neighboring qubits are entangled with a controlled-Z (CZ) gate and are then measured one after the other in the Pauli-X basis and postselecting upon receiving outcome $|+\rangle$. An example of such a circuit for three gates is shown in Fig. 3. Effectively, the state of the first qubit is teleported on the second and acted upon by a Hadamard gate. This is then the input to a new Hadamard gadget, implementing a new Hadamard gate. The effect of this circuit is to sequentially teleport the state $|\psi\rangle$ from qubit to qubit, each time applying a Hadamard gate to it, thus causing it to oscillate between the state $|\psi\rangle$ and $H|\psi\rangle$.

If n Hadamard gates are applied, then we need to implement n Hadamard gadgets, which requires n ancillary postselection qubits and n measurements. The space of our qubits will be 2^{n+1}, and the clock will be qudit of dimension $2n+1$. The propagation Hamiltonian will be made of $2n$ terms, where odd terms correspond to Kitaev's unitary Hamiltonians and even terms to a projection Hamiltonian. Explicitly, we can write the propagation Hamiltonian as

$$
\begin{aligned}
H_{\text{prop}} = \sum_{j=0}^{n-1} \frac{1}{2}[-CZ^{(j+1,j+2)} \otimes (|2j\rangle\langle 2j+1| + |2j+1\rangle\langle 2j|) + \mathbb{I} \otimes (|2j\rangle\langle 2j| + |2j+1\rangle\langle 2j+1|)] \\
+ \frac{1}{3}\Pi^{(j+1)} \otimes \left[2|2j+1\rangle\langle 2j+1| - \frac{1}{\sqrt{2}}|2j+1\rangle\langle 2j+2| - \frac{1}{\sqrt{2}}|2j+2\rangle\langle 2j+1| + |2j+2\rangle\langle 2j+2|\right] \\
+ (\mathbb{I} - \Pi)^{(j+1)} \otimes |2j+2\rangle\langle 2j+2|, \qquad (9)
\end{aligned}
$$

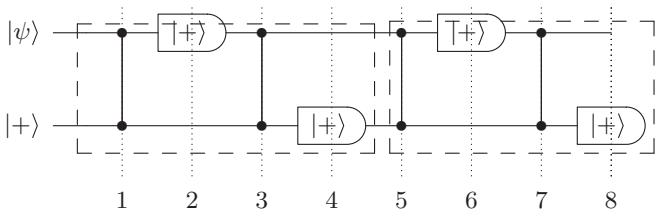

FIG. 5. Each box is a postselected circuit implementing the identity on the input qubit $|\psi\rangle$ and recycling qubits, since the ancillas will always be in the state $|+\rangle$.

where $CZ^{(i,j)}$ denotes the control-Z operator acting on qubits i and j with identity on all others, and where $\Pi^{(i)}$ corresponds to the projector $|+\rangle\langle+|$ acting on qubit i, with identity on all other qubits.

We constructed the propagation Hamiltonian of the circuit, computed its smallest nonzero eigenvalue, and illustrate its reciprocal $\lambda_{\text{min}}^{-1}$ in Fig. 4, with an exponential function fitted to the data. Therefore, the intuition that as the probability of success decreases exponentially, the gap closes as an inverse exponential seems to be correct.

C. Circuit family $\mathcal{F}_2$

In this circuit family, again the input to the circuit is $|\psi\rangle$ with an ancillary qubit initialized as $|+\rangle$. One round of the circuit will correspond to the application of the controlled-Z gate, a measurement of the first qubit in the Pauli-X basis with postselection on outcome $|+\rangle$, followed by another controlled-Z gate and a final measurement on the second qubit in the Pauli-X basis with postselection on outcome $|+\rangle$. With postselection, this initial circuit effectively implements the identity, as the output is given by $|\psi\rangle \otimes |+\rangle$. By repeating this process, we obtain a circuit such as that in Fig. 5, where each box corresponds to this initial circuit involving two postselections.

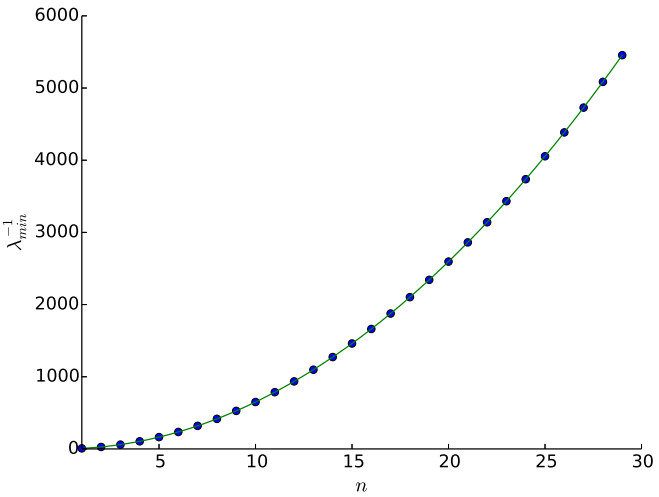

FIG. 6. Scaling of the reciprocal of the smallest eigenvalue of the Hamiltonian corresponding to circuit family $\mathcal{F}_2$, as shown in Eq. (10). Here, we fit the data to a quadratic function $y = ax^2 + bx + c$, and obtain $a = 6.5$, $b = 0.04$, and $c = 1.4$.

The propagation Hamiltonian H_{prop} in the Kitaev-Feynman construction corresponding to this circuit is now constructed according to the number of rounds n of each gadget in the box of Fig. 5. One box corresponds to a unitary operator being applied, a renormalized projector, a unitary operator, and a final renormalized projector $H_{\text{prop}} = \sum_{j=0}^{n-1} H_j$, where

$$
\begin{aligned}
H_j = {} & \frac{1}{2}(-CZ \otimes (|j\rangle\langle j+1| + |j+1\rangle\langle j|) + \mathbb{I} \otimes (|j\rangle\langle j| + |j+1\rangle\langle j+1|) + \frac{1}{3}(|+\rangle\langle+| \otimes \mathbb{I}) \\
& \otimes \left[2|j+1\rangle\langle j+1| - \frac{1}{\sqrt{2}}|j+1\rangle\langle j+2| - \frac{1}{\sqrt{2}}|j+2\rangle\langle j+1| + |j+2\rangle\langle j+2|\right] + (|-\rangle\langle-| \otimes \mathbb{I}) \otimes |j+2\rangle\langle j+2| \\
& + \frac{1}{2}(-CZ \otimes (|j+2\rangle\langle j+3| + |j+3\rangle\langle j+2|) + \mathbb{I} \otimes (|j+2\rangle\langle j+2| + |j+3\rangle\langle j+3|) \\
& + \frac{1}{3}(\mathbb{I} \otimes |+\rangle\langle+|) \otimes \left[2|j+3\rangle\langle j+3| - \frac{1}{\sqrt{2}}|j+3\rangle\langle j+4| - \frac{1}{\sqrt{2}}|j+4\rangle\langle j+3| + |j+4\rangle\langle j+4|\right] \\
& + (\mathbb{I} \otimes |-\rangle\langle-|) \otimes |j+4\rangle\langle j+4|. \qquad (10)
\end{aligned}
$$

The dimension of the auxiliary clock depends on the number of rounds we implement and is given by $4n + 1$. We numerically find the smallest nonzero eigenvalue and depict its reciprocal $\lambda_{\text{min}}^{-1}$ as it scales in n in Fig. 6, with a quadratic function fitted to the data. The smallest nonzero eigenvalue of the propagation Hamiltonian thus seems to scale as an inverse polynomial function.

Thus we have two quantum circuits effectively implementing the same trivial operation, but which nonetheless exhibit a starkly different behavior. In each case, the Hamiltonian encoding the circuit is built, and its smallest nonzero eigenvalue plotted as a function of system size. Two starkly distinct cases are observed. In the first, the eigenvalues scale exponentially with system size, whereas, in the second, a polynomial—quadratic—scaling is observed, even though both circuits are effectively implementing the same unitary operator. Yet, the spectrum of their respective Hamiltonians are radically different.

V. DISCUSSION

In this work, we introduced the idea of tame postselection, which allowed us to generalize the k-local Hamiltonian prob-

lem to nonunitary evolutions and to consider its computational complexity.

Our first result, Proposition 1, generalized Hamiltonians encoding unitary evolution within their kernel to nonunitary evolution. This was achieved by extending the circuit-to-Hamiltonian construction to evolutions via renormalized projectors, which map pure states to pure states. As quantum computing can be expressed in two different yet equivalent frameworks, a question for future research is to understand how the Hamiltonians encoding these different computations are related.

Our second result is the introduction of tame postselection, which allows for these Hamiltonians to not depend on the input state, where we have that the probability of an event occurring is input independent. We then show that tame postselection limits the computational power of the class QMA when given access to a postselection register. We then considered the computational complexity of the computations that are being encoded in this extended construction, and showed that they are exactly the quantum computations with postselection as defined by Aaronson. Therefore, given certain assumptions about computational complexity, solving the k-local Hamiltonian problem given Hamiltonians constructed from circuits with postselection is harder than the standard problem that is QMA-complete, but not as hard as the so-called precise k-local Hamiltonian problem which allows for gap that is exponentially small between energy eigenstates.

Our third and final result shows the radically different behavior of two circuits implementing the same operations via a Hadamard gadget, but of which the corresponding Hamiltonians present starkly different behavior. Here, the question is to understand the origin of this difference. This suggests that the probability of the postselected event succeeding is not immediately connected to the gap in the Hamiltonian, which makes the connection between the k-local Hamiltonian problem and nonunitary computation very subtle.

Thus the main direction for future research is to get a better characterization of Hamiltonians resulting from postselected quantum circuits. We numerically explored a couple of examples of postselected circuit families that exhibited similar behavior from the point-of-view of state transformation and the probability of success of all postselected events exponentially decreased in the size of the circuits; however, their corresponding Hamiltonians exhibited very different behavior. It seems that one of the Hamiltonians can be solved within QMA since there was a polynomially small gap between the ground-state and first excited-state energies; the other family of Hamiltonians seemed to have an exponentially small gap. Therefore, this gap might not be determined by the probability of success for the postselected events nor the effective unitary implemented by the tame postselection as indicated by Proposition 1. The natural question is then what determines this gap?

One major hope for this work is that it is useful in demonstrating that the simulation of certain Hamiltonians is hard, such as in the work of Ref. [26]. Since postselection is a useful tool in proving such hardness results, it seems natural to build postselection into the Hamiltonians and then make arguments based on the k-local Hamiltonian problem. By bringing all of these elements together we may get a better understanding of what kinds of quantum systems are hard to classically simulate and why.

ACKNOWLEDGMENTS

This work was supported by EPSRC, partly through the Centre for Doctoral Training in Delivering Quantum Technologies (Grant No. EP/L015242/1) and the Networked Quantum Information Technologies (NQIT) Hub (Grant No. EP/M013243/1).

[1] S. Arora and B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, Cambridge, UK, 2009).

[2] R. P. Feynman, Quantum mechanical computers, Opt. News **11**, 11 (1985).

[3] A. H. Shen, A. Yu. Kitaev, and M. N. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, Providence, RI, 2002).

[4] J. Kempe, A. Kitaev, and O. Regev, The complexity of the local Hamiltonian problem, SIAM J. Comput. **35**, 1070 (2006).

[5] J. Kempe and O. Regev, 3-local Hamiltonian is QMA-complete, Quantum Inf. Comp. **3**, 258 (2003).

[6] S. Bravyi and M. Vyalyi, Commutative version of the k-local Hamiltonian problem and common eigenspace problem, Quantum Inf. Comp. **5**, 187 (2005).

[7] S. Bravyi, D. P. Divincenzo, R. I. Oliveira, and B. M. Terhal, The complexity of stochastic local Hamiltonian problems, Quantum Inf. Comp. **8**, 0361 (2008).

[8] T. Cubitt and A. Montanaro, Complexity classification of local Hamiltonian problems, in *Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS'14)* (IEEE, New York, 2014), pp. 120–129.

[9] N. P. Breuckmann and B. M. Terhal, Space-time circuit-to-Hamiltonian construction and its applications, J. Phys. A: Math. Theor. **47**, 195304 (2014).

[10] D. Gottesman and S. Irani, The quantum and classical complexity of translationally invariant tiling and Hamiltonian problems, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS'09)* (IEEE, New York, 2009), pp. 95–104.

[11] E. Knill, R. Laflamme, and G. J. Milburn, A scheme for efficient quantum computation with linear optics, Nature (London) **409**, 46 (2001).

[12] R. Raussendorf and H. J. Briegel, A One-Way of Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).

[13] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Measurement-based quantum computation, Nat. Phys. **5**, 19 (2009).

[14] S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time, Proc. R. Soc. A **461**, 3473 (2005).

[15] C. Marriott and J. Watrous, Quantum Arthur–Merlin games, Comput. Complex. **14**, 122 (2005).

[16] M. Vyalyi, Qma= pp implies that pp contains ph, ECCCTR: Electronic Colloquium on Computational Complexity, Technical Report No. 21 (2003).

[17] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing* (ACM Press, Materials Park, OH, 2011), pp. 333–342.

[18] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, Proc. R. Soc. A **467**, 459 (2011).

[19] M. J. Hoban, J. J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D. E. Browne, Measurement-Based Classical Computation, Phys. Rev. Lett. **112**, 140505 (2014).

[20] G. Kuperberg, How hard is it to approximate the Jones polynomial? arXiv:0908.0512 [quant-ph].

[21] T. Morimae and H. Nishimura, Merlinization of complexity classes above BQP, arXiv:1704.01514 [quant-ph].

[22] S. Fenner, PP-lowness and simple definition of AWPP, Theory Comput. Syst. **36**, 199 (2003).

[23] L. Fortnow and J. D. Rogers, Complexity limitations on quantum computation, arXiv:cs/9811023 [cs.CC].

[24] B. Fefferman and C. Lin, Quantum Merlin Arthur with exponentially small gap, arXiv:1601.01975.

[25] J. Aspnes, R. Beigel, M. L. Furst, and S. Rudich, The expressive power of voting polynomials, Combinatorica **14**, 135 (1994).

[26] A. Bouland, L. Mančinska, and X. Zhang, Complexity classification of two-qubit commuting Hamiltonians, arXiv:1602.04145 [quant-ph].