A single-shot measurement of the energy of product states in a translation invariant spin chain can replace any quantum computation

Dominik Janzing[1,4], **Pawel Wocjan**[2] **and Shengyu Zhang**[3]

[1] Max Planck Insitute for Biological Cybernetics, Spemannnstrasse 38, 72076 Tübingen, Germany
[2] School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816, USA
[3] Computer Science Department and Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125, USA
E-mail: dominik.janzing@tuebingen.mpg.de, wocjan@cs.ucf.edu and shengyu@caltech.edu

Abstract.   In measurement-based quantum computation, quantum algorithms are implemented via *sequences* of measurements. We describe a translationally invariant finite-range interaction on a one-dimensional qudit chain and prove that a *single-shot* measurement of the *energy* of an appropriate computational basis state with respect to this Hamiltonian provides the output of any quantum circuit. The required measurement accuracy scales inverse polynomially with the size of the simulated quantum circuit. This shows that the implementation of energy measurements on generic qudit chains is as hard as the realization of quantum computation. Here, a 'measurement' is any procedure that samples from the spectral measurement induced by the observable and the state under consideration. As opposed to measurement-based quantum computation, the post-measurement state is irrelevant.

---

[4] Author to whom any correspondence should be addressed.

IOP Institute of Physics 𝚽 DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

Contents

1. Introduction

A characteristic feature of quantum systems is the abundance of mutually incompatible observables. According to the axioms of standard quantum mechanics [1] every self-adjoint operator on the system Hilbert space defines a physical variable that could in principle be measured (the richness of observables even increases if one considers generalized observables, defined by positive operator-valued measures [2]). In particular, for systems that are composed of many components it is by no means obvious how to measure an arbitrary observable given its description as a Hilbert space operator.

In recent years, quantum information processing has shown how one could *in principle* design arbitrarily complex unitary transformations by concatenating elementary operations [3]. Given that a measurement procedure for one non-degenerate observable is available, such unitary transformations would allow us to measure every self-adjoint operator by transforming it into a function of the former. Moreover, it has been recognized that the so-called quantum phase-estimation procedure can be used to measure self-adjoint observables [4]–[6]. Insights of this kind raise the question of which types of observables are *easy* to measure and which ones require *complex* transformations to reduce them to observables for which measurement procedures are known. Even if we specify a set of elementary observables and a set of elementary unitary transformations, it is a difficult task to find lower bounds on the required control operations. The close relation to tasks of quantum information processing suggests addressing this question from a different point of view: instead of trying to find such lower bounds (which are also hard to get for computational problems) one should rather try to place the question of the hardness of certain measurements in the context of complexity theory. This will be done in the present paper by showing that the implementation of certain measurements would already make it possible to solve classically hard computational problems.

The computational power of quantum measurements has extensively been explored in recent years since models for quantum computations have been described that are solely based on measurements [7, 8]. However, these models require either concatenations of measurements or the preparation of an entangled initial state [8]. In contrast, it has been shown that accurate measurements can even solve computational PSPACE-complete

IOP Institute of Physics **Φ** DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

problems[5] when applied to computational basis states [6]. This statement requires a high measurement accuracy allowing one to resolve the exponentially small spectral gaps that are typical for interactions in many-particle systems. Therefore, this result should be understood as exploring complexity-theoretic limitations on the measurement *accuracy* that can be achieved. It should not be interpreted that all (i.e. even less accurate) measurements of these observables are also difficult.

Based on the constructions in [6], it was shown in the unpublished work [9] that one obtains the computational complexity class BQP instead of PSPACE if the required measurement accuracy is only *inverse polynomial* instead of *exponential* in the number of particles. More precisely, it was proved that a measurement instrument is a full BQP-oracle if it is able to measure the so-called *k-local* observables when the system is in an appropriate basis state[6]. Here and in the following, the term 'basis state' always refers to some element of a previously fixed basis that consists of product states in the many-particle system.

Here, we tighten the results of [9] in four different ways[7]. Firstly, we show that *k*-locality can be replaced with finite range interactions in one-dimensional chains. Secondly, we can restrict the attention to translationally invariant operators. Self-adjoint operators of this kind are closer to Hamiltonians of real physical systems. Consequently, both modifications increase the physical relevance of the result: measurements of the observable 'energy', i.e. the Hamiltonian H of a system plays a central role in understanding its physics as the spectrum of the Hamiltonian determines the dynamical and thermodynamical behaviors. Thirdly, we do not need a measurement apparatus for general translationally invariant Hamiltonians. Instead, it suffices in the present setting to measure just one *specific* observable that is universal. Fourthly, we need only a single-shot measurement instead of *repeated* measurements.

The idea of the construction is as follows: first of all we construct a Hamiltonian H that encodes a one-dimensional quantum cellular automaton (QCA). In analogy to the constructions in [10]–[15], the time-evolution $\exp(-iHt)$ leads to superpositions between different time-steps and also between time-steps in a backward-time computation instead of implementing the computation step-by-step. Then we assume that we are given an arbitrary quantum circuit that computes the result (YES, NO) of a computational problem when applied to an appropriate basis state (with respect to an *a priori* chosen product basis). Since the cellular automaton is universal for quantum computing, we can choose an initial basis state such that it simulates the quantum circuit. In other words, the program for the computation and the classical input data are encoded into the basis state. Due to our specific construction of H, the spectrum of its restriction to the smallest H-invariant subspace containing the initial state depends on the result of the simulated quantum circuit. Since we have ensured that the two spectra corresponding to the solutions YES and NO are disjoint, we obtain the answer by measuring only once.

It should be emphasized that we obtain the result of the computation by applying measurements to the *initial* state, which is a basis state encoding program and data. The following argument describes in a metaphoric way why this is possible. We construct H in such

---

[5] The basic idea is that every problem in PSPACE can be solved by an exponential number of applications of the same circuit (which is polynomial both in space and time). After encoding the circuit into a Hamiltonian, a measurement reproduces the result of the computation. The allowed error is an appropriate inverse polynomial function of the total number of time-steps, i.e. layers of the circuit times the number of applications.
[6] Note that the computational power of measurements of 'sparse' observables provided the underlying idea for the BQP-hardness proof of diagonal entry estimation problem in [16].
[7] We emphasize that [9] is included in this paper as a previous development, and is not to be submitted elsewhere.

IOP Institute of Physics 🔶 DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

a way that the computation process stops at the end of the computation whenever the output is negative. Otherwise it continues with performing a large number of idle operations. Whether or not the computation process stops is certainly relevant for the spectrum of the restriction of H to the smallest H-invariant subspace containing the initial state. We choose the number of idle steps in such a way that the spectra become mutually disjoint. Then we can check the result of the computation by a single-shot measurement of the energy applied to the initial state.

2. Defining measurements and their accuracy

Our complexity theoretic results heavily rely on the definition of what it means to measure an observable with a certain accuracy. Following standard definitions in quantum mechanics [1], we define a quantum operation to be a measurement of the observable A if its application to an arbitrary state ρ generates eigenvalues λ_j of A as outcomes such that $\mathrm{tr}(\rho Q_j)$ is the probability of obtaining λ_j, where $A = \sum_j \lambda_j Q_j$ is the spectral decomposition of A. In other words, an A-measurement (applied to the state ρ) allows us to sample from the *spectral measure* induced by the operator A and the state ρ. Since the measurement accuracy is relevant for the implementation complexity (compare [6]), we need a precise definition of the accuracy.

Before formally introducing approximative measurements, we point out that a process generating outcomes whose expected value coincides with $\mathrm{tr}(\rho A)$ is not sufficient for our purposes. To implement measurement of the latter type is certainly a much weaker assumption. Consider, for instance, a Hamiltonian H of the form

$$H := \sum_{j=1}^{n} H_j,$$

where each H_j is an operator acting on k-adjacent particles only. Then we can reproduce the expected value $\mathrm{tr}(\rho H) = \frac{1}{n} \sum_j \mathrm{tr}(\rho(n H_j))$ by choosing a value j randomly (according to the uniform distribution) and implementing a measurement for $n H_j$ (requiring the ability to control only a small subsystem of the quantum system). Moreover, if we restrict the attention to basis states, the expected value can even be computed efficiently.

We now define an approximative measurement:

Definition 1 (measurement accuracy). A measurement of the observable A is said to have *maximal error* δ and *reliability* $1 - \epsilon$ if the following condition holds: the probability of obtaining an outcome λ in the interval $[a - \delta, b + \delta]$ is at least $\mathrm{tr}(\rho Q_{[a,b]})(1 - \epsilon)$ for every interval $[a, b] \subseteq \mathbb{R}$ and every state ρ, where $Q_{[a,b]}$ denotes the spectral projection of A corresponding to the eigenvalues in $[a, b]$.

We emphasize that our definition of approximate measurements focuses only on the measurement outcomes and not on the post-measurement states which are irrelevant.

It is known that the time evolution $\exp(-\mathrm{i}At)$ can efficiently be simulated for all k-local operators[8] A acting on n-qubits in the following sense: a unitary U_t with $\|U_t - \exp(-\mathrm{i}Ht)\| \leqslant \theta$ can be implemented with resources that are only polynomial in $1/\theta$, n and t [17]–[19]. For k-local operators on n-*qudits*, one has to introduce elementary operations on such a system (e.g. those involving only two qudits) in order to define an appropriate notion of complexity.

---

[8] Here a k-local operator is defined as an operator that can be written as a sum of terms that act on k (not necessarily adjacent) qubits only.

It was shown how to realize approximate A-measurements using the quantum-phase estimation procedure using approximations V of $U := \exp(-iA/\|A\|)$ for appropriate t [6, 16]. A measurement with maximal error δ and reliability $1 - \epsilon$ in our sense can be achieved using only resources polynomial in $1/\delta$, $1/\epsilon$ and n. This follows by adapting the arguments of [6, 16, 20, 21] to the above definition of reliability and accuracy.

Roughly speaking, this result means that the realization of quantum computation is at least as hard as the implementation of approximate measurements of k-local observables. The results of [9] can be interpreted as the converse statement stating that the implementation of k-local measurements is at least as hard as the realization of quantum computation. To be more precise, [9] showed that repeated k-local measurements can solve all problems in the complexity class PromiseBQP (i.e. the class of problems that can be solved by the quantum computer in polynomial time by a probabilistic algorithm) and the required measurement accuracy is polynomial in the running time of the simulated circuit. The present work shows that approximate measurements of physically more relevant Hamiltonians (translationally invariant finite-range interactions on qudit chain) can also solve all problems in PromiseBQP. Before proving this, we give the formal definition of PromiseBQP.

3. Quantum computation as approximate energy measurement

The complexity class BQP is usually considered to represent the class of problems that can be solved efficiently on a quantum computer. However, it is often necessary to consider a generalization of this complexity class given by the promise version of BQP (for an introduction into promise problems see [22]). For example, if we want to study complete problems (i.e. problems that fully capture the power of quantum computing), then we have to work with PromiseBQP since BQP is not known to contain a complete problem (just like its classical counterpart BPP and other semantic complexity classes such as MA). For these reasons, we work with PromiseBQP.

BQP is the class of *language-recognition* problems that can be solved efficiently on a quantum computer [13]. A language-recognition problem is to decide whether a given string **x** is an element of a language $L \subseteq \{0, 1\}^*$ or not. The essential point is that a language defines a partition of the set of *all* strings into those that belong to L and those belonging to the complement of L and that the quantum computer must be able to decide whether $x \in L$ and $x \notin L$ for every x. The promise version of a complexity class can also contain decision problems that do not correspond to language-recognition problems. Given a set of *allowed* inputs $\Pi := \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$, the problem is to decide whether $x \in \Pi_{\text{YES}}$ or $x \in \Pi_{\text{NO}}$ given the promise that $x \in \Pi$ (note that language-recognition problems are promise problems, where Π is the set of all strings). We denote this problem by $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$. Observe that the problem of deciding if **x** is in Π could be computationally much harder.

The formal definition of PromiseBQP is:

Definition 2 (PromiseBQP). PromiseBQP is the class of promise problems that can be solved by an uniform[9] family of quantum circuits $(U^{(n)})$. More precisely, it is required that this family of quantum circuits $U^{(n)}$ decides if a string **x** of length n is a YES-instance or NO-instance in

[9] By 'uniform circuit' we mean that there exists a polynomial time classical algorithm that generates a sequence of a polynomial number of quantum gates for every desired input length.

the following sense. The application of $U^{(n)}$ to the computational basis state $|\mathbf{x}, \mathbf{0}\rangle$ produces the state

$$U^{(n)}|\mathbf{x}, \mathbf{0}\rangle = \alpha_{\mathbf{x},0}|0\rangle \otimes |\psi_{\mathbf{x},0}\rangle + \alpha_{\mathbf{x},1}|1\rangle \otimes |\psi_{\mathbf{x},1}\rangle \qquad (1)$$

such that

  (i) $p_{\mathbf{x},1} := |\alpha_{\mathbf{x},1}|^2 \geqslant 2/3$ for all $\mathbf{x} \in \Pi_{\text{YES}}$ and
  (ii) $p_{\mathbf{x},0} := |\alpha_{\mathbf{x},0}|^2 \geqslant 2/3$ for all $\mathbf{x} \in \Pi_{\text{NO}}$ (or equivalently, that $p_{\mathbf{x},1} \leqslant 1/3$).

Equation (1) has to be read as follows: the input string $\mathbf{x}$ determines the first n-qubits. The remaining $a = \text{poly}(n)$ additional ancilla qubits are initialized to $|\mathbf{0}\rangle$. After $U^{(n)}$ has been applied we interpret the first qubit as the relevant output; the remaining $n + a - 1$ output values are irrelevant. The number of the gates of the circuit $U^{(n)}$ is $r = \text{poly}(n)$.

Definition 2 clarifies the notion of an 'efficient quantum algorithm'. The following theorem is the main result of the paper. It states that efficient quantum algorithms can be simulated by energy measurements whose accuracy in the sense of definition 1 is inverse polynomial in the size of the simulated circuit, where the Hamiltonian is a finite-range translationally invariant Hamiltonian on a one-dimensional qudit chain and the initial state is a canonical basis state. The proof of the theorem follows from the construction of the Hamiltonian in section 5 using some general spectral analysis developed in the following section, phrased as lemmas 1 and 2.

Let us first introduce the embedding of two-qubit interactions into a qudit chain. For any operator O on $\mathbb{C}^d \otimes \mathbb{C}^d$ define a family of embedding operators $\mathcal{E}_j^{(m)} : \mathbb{C}^d \otimes \mathbb{C}^d \to (\mathbb{C}^d)^m$ by

$$\mathcal{E}_j^{(m)}(O) := \mathbf{1}^{\otimes j} \otimes O \otimes \mathbf{1}^{m-2-j}.$$

Then we will show:

Theorem 1. *There is an operator V acting on $(\mathbb{C}^{56})^{\otimes 2}$ such that energy measurements with respect to the family of Hamiltonians*

$$H^{(m)} := \sum_{j=0}^{m-2} \mathcal{E}_j^{(m)}(V + V^\dagger) \qquad (2)$$

acting on $(\mathbb{C}^{56})^{\otimes m}$ can probabilistically solve PromiseBQP in the following sense.

Assume we are given a device that is able to implement $H^{(m)}$-measurements with maximal error $\delta = 1/poly(m)$ and reliability $1 - \epsilon$. Let $U^{(n)}$ be a family of quantum circuits that solve a problem in PromiseBQP as in definition 2. Then for all input strings $\mathbf{x}$ of length n, there is a partition $\mathbb{R} = Y_m \dot\cup N_m$, and a computational basis state $|\psi_x\rangle \in (\mathbb{C}^{56})^{\otimes m}$ such that

$$\Pr(\lambda \in Y_m | x \in \Pi_{\text{YES}}) \geqslant p_{\mathbf{x},1}(1 - \epsilon), \qquad (3)$$

$$\Pr(\lambda \in N_m | x \in \Pi_{\text{NO}}) \geqslant p_{\mathbf{x},0}(1 - \epsilon), \qquad (4)$$

where λ is the random variable defined by the energy measurement of $H^{(m)}$ in the state $|\psi_x\rangle$ and $m = poly(n)$. The quantities m, $|\psi_x\rangle$, Y_m and N_m can be efficiently computed from $\mathbf{x}$ and $U^{(n)}$.

Note that V is the same for all m. Later we will construct such an operator V with $\|V\| \leqslant 1$.

4. Spectral requirements on the Hamiltonian

We start with Hamiltonians that are not necessarily of the special form in equation (2). This relaxation allows us to provide a simpler and more intuitive understanding of why accurate energy measurements can solve PromiseBQP-problems at all. We construct a suitable finite-range translationally invariant Hamiltonian on a qudit chain in section 5.

We now briefly review the basic principles of the autonomous Hamiltonian computers proposed by Benioff, Feynman and Margolus [10, 14, 23] since our Hamiltonian can be viewed as a special type of an autonomous Hamiltonian quantum computer. Originally, the construction of computational models in terms of autonomous Hamiltonian dynamics of closed physical systems was motivated, among other things, by the study of thermodynamics of computation. Kitaev observed that these ideas are also useful in quantum complexity theory since they provide a connection between problems of determining spectral properties of Hamiltonians and those of finding solutions of hard computational problems. This link has mainly been used in the context of the proof of the QMA-completeness of the so-called local Hamiltonian problem (estimating the ground state energy for a wide range of Hamiltonians [13], [24]–[27]).

Let $U = U_r U_{r-1} \cdots U_1$ be a quantum circuit consisting of the elementary gates U_t acting on the logical Hilbert space $\mathcal{H}$ for $t = 1, \ldots, r$. We adjoin a Hilbert space $\mathcal{H}_{\text{clock}}$ that represents the clocking device of the autonomous computer and define on $\mathcal{H} \otimes \mathcal{H}_{\text{clock}}$ the 'forward time operator'

$$F := \sum_{t \in \mathbb{Z}} U_t \otimes |t+1\rangle\langle t|, \tag{5}$$

where we have used the convention $U_t = \mathbf{1}$ for $t \notin \{1, \ldots, r\}$. The states $|t\rangle$ label some states in $\mathcal{H}_{\text{clock}}$ and represent the time steps of the quantum circuit U. They do not necessarily span the whole space $\mathcal{H}_{\text{clock}}$. We then define a Hamiltonian by

$$H := F + F^{\dagger}.$$

Applying the time evolution $\exp(-iHt)$ to the state $|\mathbf{x}, \mathbf{0}\rangle \otimes |0\rangle$ leads to superpositions of states of the form

$$F^t|\psi\rangle = \left(\prod_{j=1}^{t} U_j |\mathbf{x}, \mathbf{0}\rangle \right) \otimes |t+1\rangle \qquad \text{with } t > 0$$

and

$$|\mathbf{x}, \mathbf{0}\rangle \otimes |t\rangle \quad \text{with } t \leqslant 0.$$

The idea of Hamiltonian computers is then to initially prepare the clock in a superposition of states with negative t in such a way that the wave packet propagates mainly in forward direction and triggers the implementation of gates.

The reason why such models of autonomous computation can only simulate quantum circuits in such a 'broader sense' (i.e. one has always superpositions of different computational states) is that the Hamiltonians should be k-local for some small constant k. It is not known how to directly implement unitary operations U by time-independent Hamiltonians H of this type where $U = \exp(-iH)$ represents some interesting computation.

An important feature of the forward-time operators in the abovementioned literature is that they act unitarily on the relevant subspace of 'computational states' spanned by $F^t(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$ and $(F^\dagger)^t(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$ with $t \in \mathbb{N}$. This makes a spectral analysis feasible since F and $F^\dagger$ commute on this subspace.

For our construction, we do not want the Hamiltonian really to perform the computation in the above case. However, the above explanation still remains the leading intuition. To prove that approximate energy measurements can solve PromiseBQP-problems, we have to introduce a modification of the above forward-time operator such that it is no longer unitary on the relevant subspace, and analyze its spectral properties. We need the *read-out* gate $R := |1\rangle\langle 1|$ and the *annihilation* gate $A := \mathbf{0}$ (where $\mathbf{0}$ is the zero matrix) for this modification. Let $U = U_r U_{r-1} \cdots U_1$ be a quantum circuit as above and let s be greater than r. We construct a non-unitary quantum circuit

$$\hat{U} = \hat{U}_{s+1}\hat{U}_s\hat{U}_{s-1} \cdots \hat{U}_{r+1}\hat{U}_r\hat{U}_{r-1} \cdots \hat{U}_1\hat{U}_0,$$

where its elementary gates are defined as follows:

$$\hat{U}_0 := A, \tag{6}$$

$$\hat{U}_t := U_t, \quad \text{for } t = 1, \ldots, r, \tag{7}$$

$$\hat{U}_{r+1} := R, \tag{8}$$

$$\hat{U}_t := I, \quad \text{for } t = r+2, \ldots, s, \tag{9}$$

$$\hat{U}_{s+1} := A. \tag{10}$$

The reader may be confused that $\hat{U}_0$ and $\hat{U}_{s+1}$ are trivial since our 'annihilation gate' A is just the zero operator. The reason why we define such an unusual 'quantum circuit' is that this definition allows us to interpret every operation performed by the forward-time operator, including state annihilation, as a (not necessarily unitary) quantum 'gate'. Then we construct a modified forward-time operator (compare equation (5)) by

$$F := \sum_{t=0}^{s+1} \hat{U}_t \otimes |t+1\rangle\langle t|.$$

To intuitively understand why the spectral measure of the Hamiltonian $H := F + F^\dagger$ will then reflect the solution of the computational problem we observe the following. Assume we apply the time evolution $\exp(-iHt)$ to the state $|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle$ and the answer of the problem is 'YES' with probability 1. In this case the orbit

$$\left(\exp(-iH\tau)(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle) \right)_{\tau \in \mathbb{R}_+}$$

consists of superpositions of the states $F^t(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$ for $t = 0, \ldots, s$. This is because $F^\dagger$ and F annihilate the first and the last state in this set, respectively, and on the remaining states (i.e. $t = 1, \ldots, s-1$) they commute since the non-unitary readout gate is irrelevant. The dynamics is then mathematically equivalent to a particle moving on a chain of length $s+1$ (with a dynamics induced by 'hopping terms').

If the answer is 'NO' with probability 1 the dynamics is restricted to the subspace spanned by $F^t(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$ for $t = 0, \ldots, r$, i.e. a dynamics on a chain of length $r+1$.

In the generic case the answer is non-deterministic and we obtain a mixture of both cases such that the probability distribution of the results of a H-measurement depends directly on the outcome probabilities of the simulated circuit. For the mathematical analysis of this case we will use the decomposition

$$|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle = \sqrt{1 - p_1}|\psi_0\rangle \oplus \sqrt{p_1}|\psi_1\rangle,$$

where $|\psi_1\rangle$ is obtained by renormalizing $(F^\dagger)^{r+1} F^{r+1}(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$ and $|\psi_0\rangle$ by renormalizing $|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle - (F^\dagger)^{r+1} F^{r+1}(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$. These components correspond to new initial states for which the answer in the readout step is deterministic. The lemma below specifies precisely the statement and the conditions on F that we require.

Let us briefly introduce some graph theoretic terminology first. The adjacency matrix of the line graph on ℓ nodes is given by

$$\mathcal{L}_\ell := S_\ell + S_\ell^\dagger,$$

where S_ℓ denotes the non-cyclic shift in ℓ dimensions with the canonical basis vectors $|0\rangle, |1\rangle, \ldots, |\ell - 1\rangle$, i.e.

$$S_\ell = \sum_{v=0}^{\ell-2} |v+1\rangle\langle v|.$$

Let λ_v be the vth eigenvalue of $\mathcal{L}_\ell$ and $Q_v^{(\ell)}$ be the corresponding spectral projection. Let $\mathcal{P}_\ell$ be the probability distribution on the eigenvalues induced by the vector corresponding to the first node, i.e.

$$\mathcal{P}_\ell(\lambda_v) := \langle 0 | Q_v^{(\ell)} | 0 \rangle.$$

Then we have

Lemma 1. *Let $U = U_r U_{r-1} \cdots U_1$ be a quantum circuit that accepts the state $|\mathbf{x}, \mathbf{0}\rangle$ with probability $p_{\mathbf{x},1}$ in the sense of definition 2. Let $\hat{U} = \hat{U}_{s+1}\hat{U}_s \cdots \hat{U}_0$ be the corresponding non-unitary quantum circuit as defined in equations (6)–(10). Let F be an operator acting on $\mathcal{H}_d \otimes \mathcal{H}_{\text{clock}}$ where $\mathcal{H}_d$ stands for 'data space' and $\mathcal{H}_{\text{clock}}$ for 'clock space', respectively. Let $|0\rangle, \ldots, |s+1\rangle$ denote some mutually orthogonal states of the clock register. Assume that F and $F^\dagger$ act as*

$$F(|\phi\rangle \otimes |t\rangle) = \hat{U}_t |\phi\rangle \otimes |t+1\rangle, \tag{11}$$

$$F^\dagger(|\phi\rangle \otimes |t+1\rangle) = \hat{U}_t^\dagger |\phi\rangle \otimes |t\rangle, \tag{12}$$

for $t = 0, \ldots, s$ on the smallest F and $F^\dagger$ invariant subspace containing the initial state $|\psi\rangle := |\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle$.

Then the spectral measure induced by $F + F^\dagger$ and the initial state $|\psi\rangle$ is given by the convex combination

$$(1 - p_{\mathbf{x},1})\mathcal{P}_{r+1} + p_{\mathbf{x},1}\mathcal{P}_{s+1}.$$

Proof. Let $|\psi_1\rangle$ be the vector obtained by renormalizing the vector

$$(F^\dagger)^{r+1} F^{r+1} |\psi\rangle = (U_1^\dagger \cdots U_r^\dagger R U_r \cdots U_1 |\mathbf{x}, \mathbf{0}\rangle) \otimes |1\rangle$$

and $|\psi_0\rangle$ by renormalizing $|\psi\rangle - (F^\dagger)^{r+1} F^{r+1} |\psi\rangle$. Let $\mathcal{V}_0$ be the span of $\{F^t |\psi_0\rangle\}_{t=0,\dots,r}$ and $\mathcal{V}_1$ the span of $\{F^t |\psi_1\rangle\}_{j=0,\dots,s}$. The statement $\mathcal{V}_0 \perp \mathcal{V}_1$ follows from the fact that

$$F^t |\psi_0\rangle \perp F^{t'} |\psi_1\rangle \tag{13}$$

holds for all $t \neq t'$, because the states then correspond to different basis vectors in the clock space. For $t = t' = r$ the restrictions of the states $F^t |\psi_1\rangle$ and $F^t |\psi_0\rangle$ to the data register are given by renormalizing

$$R U_r \cdots U_1 |\psi\rangle \quad \text{and} \quad (\mathbf{1} - R) U_r \cdots U_1 |\psi\rangle, \tag{14}$$

respectively. For $0 \leqslant t \leqslant r - 1$ we have to apply the unitary operator $U_{t+1}^\dagger \cdots U_r^\dagger$ to both states in equation (14), which obviously preserves the orthogonality relation.

One can easily check that $\mathcal{V}_0$ and $\mathcal{V}_1$ are invariant under the action of F and $F^\dagger$. This implies that they are also invariant under $F + F^\dagger$.

We first determine the spectral measures induced by $|\psi_0\rangle$ and $|\psi_1\rangle$. On $\mathcal{V}_0$ the operator F is unitarily equivalent to the non-cyclic shift S_{r+1} by identifying the orthonormal basis vectors $F^t |\psi_0\rangle$ with the basis vectors $|t\rangle \in \mathbb{C}^{r+1}$ for $t = 0, \dots, r$. This unitary equivalence is readily verified by checking that F maps the tth basis vector to the $(t+1)$th for $t < r$ and annihilates $F^r |\psi_0\rangle$. Hence the spectral measure induced by $F + F^\dagger$ on $|\psi_0\rangle$ is the same as the spectral measure induced by $\mathcal{L}_r = S_{r+1} + S_{r+1}^\dagger$ on $|0\rangle$, i.e. it is equal to $\mathcal{P}_{r+1}$.

Similarly, $F + F^\dagger$ induces the spectral measure $\mathcal{P}_{s+1}$ on $|\psi_1\rangle$. The spectral measure induced by $|\psi\rangle = \sqrt{1 - p_{\mathbf{x},1}} |\psi_0\rangle \oplus \sqrt{p_{\mathbf{x},1}} |\psi_1\rangle$ is then just the convex sum of the measures induced by $|\psi_0\rangle$ and $|\psi_1\rangle$, respectively. By elementary linear algebra, the corresponding weights are $1 - p_{\mathbf{x},1}$ and $p_{\mathbf{x},1}$. This completes the proof. □

The lemma shows how to construct a Hamiltonian $H = F + F^\dagger$ such that the distribution of the results in an *accurate* measurement is given by the measure $(1 - p_{\mathbf{x},1})\mathcal{P}_{r+1} + p_{\mathbf{x},1}\mathcal{P}_{s+1}$ as in lemma 1. To analyze how to assign measurement outcomes with 'YES' and 'NO' we recall that the spectrum $\mathcal{S}_\ell$ of the line graph $\mathcal{L}_\ell$ contains the values

$$\lambda_v = 2 \cos\left(\frac{\pi(v+1)}{\ell+1}\right),$$

for $v = 0, \dots, \ell - 1$ [28].

If $r + 2$ and $s + 2$ are relatively prime, then $\mathcal{S}_{s+1}$ and $\mathcal{S}_{r+1}$ are disjoint. This assumption is useful since it will allow us to replace the quantum computation with a *single shot* measurement instead of *repeated* sampling. To obtain a lower bound on the distance between these two sets, we apply the function $x \mapsto \arccos(x/2)/\pi$ to the eigenvalues λ_v and μ_w and obtain the values

$$a_v := \frac{v+1}{r+2} \quad \text{and} \quad b_w := \frac{w+1}{s+2}.$$

The minimal distance between any of these values is at least $1/(r+2)(s+2)$. On the interval $[0, \pi]$ the cosine function satisfies the inequality

$$|\cos(x) - \cos(y)| \geqslant \tfrac{1}{4}(x-y)^2,$$

for all x, y with $|x - y| \leqslant 1$. These facts imply that the minimal distance between the spectra $\mathcal{S}_{r+1}$ and $\mathcal{S}_{s+1}$ is at least

$$\Delta := \frac{\pi^2}{2(r+2)^2(s+2)^2}. \tag{15}$$

From an intuitive point of view, this already shows that the ability to implement measurements with inverse polynomial error makes it possible to assign a measurement outcome to either of the two spectra. The following lemma bases this statement on the formal definition of measurement accuracy and analyzes the probability of correctly classifying the input. It follows immediately from the arguments above.

Lemma 2. *Let the distribution of measurement results in an accurate measurement be given by*

$$(1 - q)\mathcal{P}_{r+1} + q\mathcal{P}_{s+1}$$

with $q \in [0, 1]$, where $\mathcal{P}_\ell$ for $\ell = r + 1, s + 1$ denotes the spectral measure of the line graphs of length ℓ as above. Assume we have an approximative measurement procedure with accuracy Δ as in equation (15) and reliability $1 - \epsilon$. For $\delta := \Delta/3$ define

$$Y := \bigcup_{w=0}^{s} [\mu_w - \delta, \mu_w + \delta] \text{ and } N := \mathbb{R} \setminus Y,$$

where μ_w denotes the wth eigenvalue of the line graph of length $s + 1$. Let λ be the measurement outcome.

Then we have the conditional probabilities

$$\Pr(\lambda \in Y \mid \mathbf{x} \in \Pi_{\text{YES}}) \geqslant q\,(1 - \epsilon), \tag{16}$$

$$\Pr(\lambda \in N \mid \mathbf{x} \in \Pi_{\text{NO}}) \geqslant (1 - q)\,(1 - \epsilon). \tag{17}$$

The lemma shows that the error of the measurement-based decision procedure then essentially reproduces the acceptance probabilities of the simulated circuit provided that the probability to have an error greater than Δ is small. The arguments in this section thus establish that energy measurements for local Hamiltonians can be used to solve PromiseBQP-problems. Here 'local' means that the interaction involves only a few, but not necessarily adjacent, qubits (if we represent the clock also by a qubit register). Unfortunately, this does not suffice to prove theorem 1 because we have not described how to construct a *nearest-neighbor translationally invariant interaction H* on a qudit chain having the desired properties. In the next section, we show how to construct such an interaction based on a QCA so that it still satisfies the spectral properties in lemma 1. Large parts of our construction follow the idea of the 'quantum computer on a line' described in [27]. The main difference is that we need a translation invariant Hamiltonian and must therefore encode the gates into the initial state. Moreover, the way we include readout and annihilation gates is due to our specific requirement to obtain disjoint sets of potential measurement results.

Our interaction is not supposed to be the simplest operator satisfying all the above requirements. However, we have chosen an encoding of quantum circuits that seems to be rather concise and quite natural. It is likely that more sophisticated encodings could significantly reduce the size of the unit cell of the QCA.

5. Construction of the Hamiltonian

To construct the QCA, we restrict ourselves to the following universal set of quantum gates. Let S denote the swap gate and W the controlled gate defined by

$$W := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

We require that both gates be only applied to adjacent qubits. Moreover, we require that W be applied only in one direction, i.e. the control-wire will always be the left qubit of the corresponding pair in the data register described later. This set of gates is universal because the W gate is universal if it can be applied to arbitrary qubit pairs [29]. We assume without loss of generality that the quantum circuits U in definition 2 are composed only of S and W acting on adjacent qubits. We also assume that gates acting on disjoint qubit pairs can be performed in parallel. In this way, the quantum circuits are split into *layers*. We refer to these layers as the *time steps* of the quantum circuit.

5.1. Description of our QCA

We now construct a QCA that can simulate any such quantum circuit so that the total number of time-steps required is polynomial in the number of gates and the number of qubits used in the simulated circuit.

We encode the quantum circuit and its input in the initial state of the QCA. It acts on

$$\mathcal{H} := \mathcal{H}_c^{\otimes m},$$

where $\mathcal{H}_c := \mathbb{C}^{56}$ denotes the Hilbert space of a single cell. Our Hamiltonian has the form

$$H = F + F^{\dagger} = \sum_{j=0}^{m-2} \mathcal{E}_j^{(m)}(V + V^{\dagger}), \tag{18}$$

where V acts on two cells, i.e. on $\mathcal{H}_c \otimes \mathcal{H}_c$. Each cell consists of a data and a program cell, i.e. we have

$$\mathcal{H}_c := \mathcal{H}_p \otimes \mathcal{H}_d$$

where $\mathcal{H}_p$ and $\mathcal{H}_d$ denote the Hilbert space of the program and data cell, respectively. We refer to the set of all program cells (i.e. $\mathcal{H}_p^{\otimes m}$) as the *program band* and to that of all data cells (i.e. $\mathcal{H}_d^{\otimes m}$) as the *data band*. The program band initially contains the description of the quantum circuit U to be simulated. We refer to this description as the *program code*. This code is divided into *blocks* where each block corresponds to one time-step of U. The *data register* is a subset of the data band that corresponds to the register on which U acts, i.e. it represents the logical qubits. The remaining part of the data band will only contain formatting symbols.

The Hilbert spaces of the data and program cells are denoted by $\mathcal{H}_d = \mathbb{C}^4$ and $\mathcal{H}_p = \mathbb{C}^{14}$, respectively. The basis vectors of $\mathcal{H}_d$ are identified with the symbols in
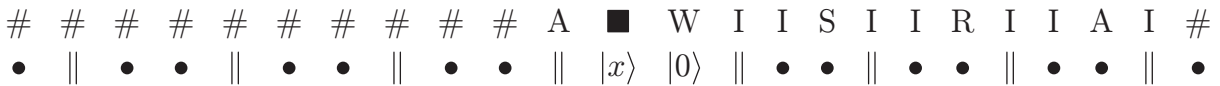
$$\{0, 1\} \cup \{\|, \bullet\},$$

#	#	#	#	#	#	#	#	#	#	A	■	W	I	I	S	I	I	R	I	I	A	I	#
•	‖	•	•	‖	•	•	‖	•	•	‖	$|x\rangle$	$|0\rangle$	‖	•	•	‖	•	•	‖	•	•	‖	•

Figure 1. Initialization of the program and data bands.
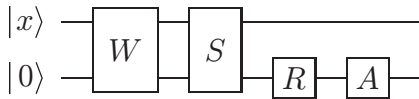

Figure 2. Example of a simple quantum circuit that acts on two qubits and consists of five time-steps. The first qubit that takes the input is x. The second qubit is an ancilla qubit.

those of $\mathcal{H}_p$ with the symbols in

$$\{I, S, W, R, A\} \cup \{\mathbb{I}, \mathbb{S}, \mathbb{W}, \mathbb{R}, \mathbb{A}\} \cup \{\square, ■, \diamondsuit, \#, \}.$$

The program code is composed of the *gate symbols* I, S, W, R and A (see figure 1). These symbols correspond to the identity, S, W, R and A, respectively. The *marked gate symbols* $\mathbb{I}$, $\mathbb{S}$, $\mathbb{W}$, $\mathbb{R}$ and $\mathbb{A}$ are used to control the propagation of the program code. The symbols $\square$, ■, $\diamondsuit$ and # are also used for this purpose. We refer to these symbols as the *hole*, *execution*, *turn-around* and *blank* symbols, respectively. The kets $|0\rangle$ and $|1\rangle$ correspond to the two orthogonal states of a qubit. The symbols ‖ and • are used for formatting purposes; the symbol ‖ makes it possible to determine when the program has been moved by one block. They are contained only in those data cells that do not belong to the *data register*.

During the dynamics the content of the program cells slides over the data cells and triggers the implementation of the gates on the data register. Since we want to construct a nearest-neighbor interaction the sliding of the program can only be realized by moving the content cell-by-cell. Therefore, we need a special control mechanism that ensures that the program is only executed after it has been moved by exactly one block, i.e. the block is again aligned with the corresponding data cells on which the gates are supposed to act (in close analogy to the construction in [27]). The forward time operator F in equation (18) must implement the propagation and the execution of the gates whenever the program is aligned with the data band.

The operator V in equation (18) is thus the product

$$V = T\,X,$$

where X applies gates on $\mathcal{H}_d \otimes \mathcal{H}_d$ conditioned on the state of $\mathcal{H}_p \otimes \mathcal{H}_p$ and T realizes transitions between the basis states of $\mathcal{H}_p \otimes \mathcal{H}_p$.
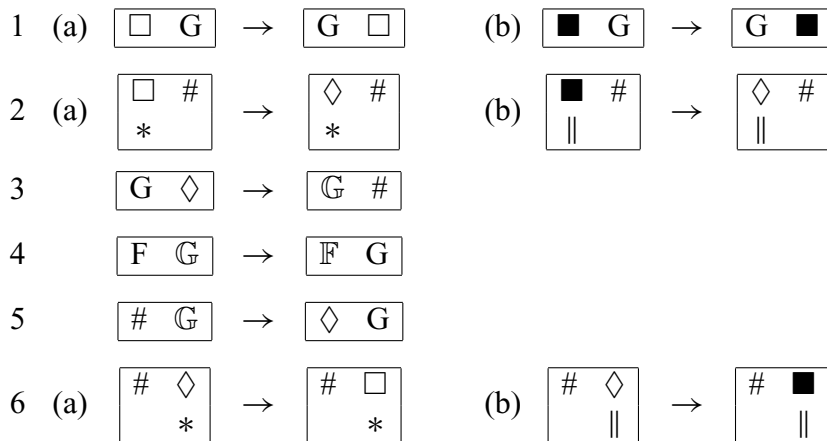
Before we define T and X explicitly, we look at a simple example to see how quantum circuits and inputs are encoded in the initial states. We also explain how the execution of the program code is controlled in a purely local procedure where no global clocking is available.

1. Assume we want to simulate the circuit in figure 2. Then we initialize the program and data bands as shown in figure 1. The program code is A■W IIS IIR IIA I, where the gaps are used to indicate the different time-steps of the quantum circuit U. All other program cells

contain the blank symbol #. Note that the two qubit gates W and S are encoded by symbol pairs IW and IS, respectively, and that the program contains an extra symbol I between the blocks (i.e. the layers of the circuit) and the first command of the program reads A. In the initial state, the first layer of the circuit is aligned with the data register that is initialized in the state $|x, 0\rangle$. The symbols ‖ to the left and right of the data register enclose exactly two ● symbols, corresponding to the number of qubits of U.

2. It is important that the program code starts with the pair A■. One may rather expect the initial configuration ■A, but this would lead to an execution of A in the first step. This is analogous to section 4, where we have to start in the clock state $|1\rangle$ instead of $|0\rangle$ to prevent the execution of the first annihilation gate $\hat{U}_0 := A$. The purpose of this choice of the initial state is to ensure that it is annihilated by the operator $F^\dagger$ because it implements the program in the backward direction. The execution symbol ■ is propagated cell-by-cell to the end of the program code until it arrives at the rightmost cell not containing the blank symbol #. In each step, ■ and the gate symbol G on its right side swap their positions. More precisely, if ■ is in the jth program cell and G in the $(j + 1)$th cell, then G moves to the jth cell and ■ to the $(j + 1)$th cell. While swapping the symbols, the gate corresponding to G is executed. It is applied to data cells j and $j + 1$ if it is a two-qubit gate and to data cell $j + 1$ if it is a single qubit gate. This only happens if data cell j and data $j + 1$ are inside the data register in the case of a two-qubit gate. Similarly, it only happens if the data cell $j + 1$ is inside the data register in the case of a single qubit gate.

3. Once the execution symbol ■ has passed the end of the program code it is converted to the blank symbol # (via the creation of the intermediate turn-around symbol ◊), and a signal is sent to the beginning of the program code. This signal indicates that the execution of the first time-step of the program code has been completed. To avoid the propagation of this signal leading to a backward propagation of the program code, the signal cannot occupy a program cell on its own. It propagates by converting each gate symbol G into a marked version 𝔾 cell by cell. Once the marked gate symbol 𝔾 is at the beginning of the program code, it is converted into the hole symbol □ via the creation of the turn-around symbol ◊.

4. The hole symbol □ propagates cell by cell to the end of the program where it is converted to the blank symbol # and triggers the left propagating marker 𝔾 (via the creation of the intermediate turn-around symbol ◊). The arrival of this marker at the beginning of the program code triggers the conversion of the next copy of # into □. This procedure is repeated until the program code begins and is again aligned with the next copy of the format symbol ‖ in the data band. In this case, the marker 𝔾 triggers the creation of ■ instead of □ and the whole cycle starting in the second step is repeated (again, this is done by the creation of the intermediate turn-around symbol ◊).

The above procedure is implemented by the following nearest-neighbor transition rules. These rules depend only on the contents of two adjacent cells of the QCA. We use $*$ to denote any of the symbols 0, 1 and ●. The symbol represented by $*$ is left unchanged by the corresponding transition rule. In the transition rules 2 and 6, the left-lower and right-lower corners are left empty to indicate that the symbol at that place is not important for the transition rule and that it is left unchanged.

1 (a) $\boxed{\;\square\quad\text{G}\;} \rightarrow \boxed{\;\text{G}\quad\square\;}$ (b) $\boxed{\;\blacksquare\quad\text{G}\;} \rightarrow \boxed{\;\text{G}\quad\blacksquare\;}$

2 (a) $\boxed{\begin{smallmatrix}\square & \# \\ * & \end{smallmatrix}} \rightarrow \boxed{\begin{smallmatrix}\lozenge & \# \\ * & \end{smallmatrix}}$ (b) $\boxed{\begin{smallmatrix}\blacksquare & \# \\ \| & \end{smallmatrix}} \rightarrow \boxed{\begin{smallmatrix}\lozenge & \# \\ \| & \end{smallmatrix}}$

3 $\boxed{\;\text{G}\quad\lozenge\;} \rightarrow \boxed{\;\mathbb{G}\quad\#\;}$

4 $\boxed{\;\text{F}\quad\mathbb{G}\;} \rightarrow \boxed{\;\mathbb{F}\quad\text{G}\;}$

5 $\boxed{\;\#\quad\mathbb{G}\;} \rightarrow \boxed{\;\lozenge\quad\text{G}\;}$

6 (a) $\boxed{\begin{smallmatrix}\# & \lozenge \\ & * \end{smallmatrix}} \rightarrow \boxed{\begin{smallmatrix}\# & \square \\ & * \end{smallmatrix}}$ (b) $\boxed{\begin{smallmatrix}\# & \lozenge \\ & \| \end{smallmatrix}} \rightarrow \boxed{\begin{smallmatrix}\# & \blacksquare \\ & \| \end{smallmatrix}}$

Transitions 1(a) and (b) implement the rightward propagation of the symbols $\square$ and $\blacksquare$, respectively. Transitions 2(a) and (b) take place when $\square$ and $\blacksquare$ have passed the end of the program code, respectively. They create the symbol $\lozenge$ (turn-around). Transition 3 creates a marked gate symbol that initiates the leftward moving signal. Transition 4 implements the propagation of this signal. Once this signal has arrived at the beginning of the program code, transition 5 and transitions 6(a) and (b) create the symbols $\square$ and $\blacksquare$ via the creation of the intermediate turn-around symbol $\lozenge$, respectively. The execution symbol $\blacksquare$ is created only if the turn-around symbol $\lozenge$ is exactly above the formatting symbol $\|$, which happens only if the blocks of the program code are aligned with the data register. Otherwise, the hole symbol $\square$ is created.

Now we are ready to define the transition operator T. It is the annihilation-creation operator on $\mathcal{H}_c \otimes \mathcal{H}_c$ defined by all the above transition rules. It annihilates all configurations that do not appear on the left-hand side of any of the above transitions.

We denote by X the operator that realizes the controlled execution of the gates. It is defined by

$$
\begin{aligned}
X \;:=\; & |\blacksquare\text{S}\rangle\langle\blacksquare\text{S}| \;\otimes\; S_d \;+\; |\blacksquare\text{W}\rangle\langle\blacksquare\text{W}| \;\otimes\; W_d \\
& +|\blacksquare\text{R}\rangle\langle\blacksquare\text{R}| \;\otimes\; (I_d \otimes R_d) \;+\; |\blacksquare\text{A}\rangle\langle\blacksquare\text{A}| \;\otimes\; (I_d \otimes A_d) \\
& +Q \;\otimes\; (I_d \otimes I_d),
\end{aligned}
$$

where

$$
Q := I_p \otimes I_p \;-\; \sum_{G\in\{\text{S,W,R,A}\}} |\blacksquare\text{G}\rangle\langle\blacksquare\text{G}|.
$$

The projectors $|\blacksquare\text{G}\rangle\langle\blacksquare\text{G}|$ for $\text{G} \in \{\text{S, W, R, A}\}$ act on $\mathcal{H}_p \otimes \mathcal{H}_p$. I_p and I_d act as identity on $\mathcal{H}_p$ and $\mathcal{H}_d$, respectively. S_d and W_d act as S and W, respectively, on the subspace of $\mathcal{H}_d \otimes \mathcal{H}_d$ spanned by $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and as identity on the orthogonal complement (spanned by pairs of format symbols $\|$, $\bullet$). Similarly, R_d and A_d act as R and A, respectively, on the subspace of $\mathcal{H}_d$ spanned by $\{|0\rangle, |1\rangle\}$ and as the identity on the complement.

5.2. Spectral properties

We denote the initial state of the QCA by $|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle$, where $|\mathbf{x}, \mathbf{0}\rangle$ is the initial state of the quantum circuit to be simulated and $|1\rangle$ represents the state of the program band and the state of all data cells outside the data register that corresponds to an appropriately chosen initial configuration.

The application of F changes the configuration in the program cells into a new basis state and applies, at the same time, gates to the relevant section in the data cells. This is because the transition rules are designed such that only one transition is possible in each step provided that the initial configuration has been chosen as described in the preceding section. We can thus denote the configurations as the clock states $|1\rangle, |2\rangle, \ldots$. Since our simulation of the original circuit contains not only *execution* steps but also operations where only signals are propagated the circuit is thus extended by polynomial overhead of identity gates on the data cells. Thus we have $\tilde{s} + 1$ steps instead of $s + 1$ until the state is completely annihilated. Likewise, the readout gate causes a conditional annihilation in the step $\tilde{r} + 1$ instead of $r + 1$.

To make sure that F and the initial state $|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle$ satisfy the conditions of lemma 1, we have to check that the application of $F^{\dagger}$ to one of the states in the orbit $F^{t}(|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle)$ with $t = 1, \ldots, \tilde{s}$ indeed leads to the preceding clock state and to an annihilation for $t = 0$. The annihilation property is satisfied since we have started the system in a state where the running of the program in the backward direction would immediately execute the A gate. To see that $F^{\dagger}$ leads in the general case to the preceding states, we have to check our list of transitions in the *backward* direction.

Every configuration that arises from the repeated application of the forward-time operator F always contains exactly one element in the set $\{\square, \blacksquare, \Diamond, \mathbb{I}, \mathbb{S}, \mathbb{W}\}$. If the configuration contains one of the symbols $\square$ and $\blacksquare$ but they are neither preceded nor followed by the blank symbol # (i.e. they are not located at the boundaries of the program code), then only rule 1(a) or (b) can be active in the backward direction. The pattern in rule 2 only occurs when the symbols $\square$ or $\blacksquare$ are located at the right boundary of the program code. In this case, no other rules are active in the backward direction. Similarly, the pattern in rule 6 only occurs when the symbols $\square$ or $\blacksquare$ are located at the left boundary of the program (i.e. only when they are preceded by #). In this case, no other rule is active in the backward direction. The symbol $\Diamond$ only appears in rules 2 and 5 on the right-hand side of the transitions. But there is no configuration where both rules can be applied backwards at the same time. Likewise, the marked gate symbols only occur in rules 3 and 4. Again, there is no configuration where both rules can be applied backwards at the same time.

Hence, we have shown that F meets the requirements of lemma 1 and that the spectral measure induced by $F + F^{\dagger}$ on the initial state $|\mathbf{x}, \mathbf{0}\rangle \otimes |1\rangle$ depends on the acceptance probability $p_{\mathbf{x},1}$. To design a program code such that the supports of the two corresponding spectral measures to be distinguished are disjoint, we may choose the position of the annihilation gate appropriately. In this way, we can always achieve that $\tilde{r} + 2$ and $\tilde{s} + 2$ are relatively prime, ensuring that the minimal distance between the supports of the spectra satisfies equation (15).

6. Conclusions

In contrast to usual measurement-based approaches to quantum computing, we have constructed an observable whose measurements have full quantum computation power when applied to a *basis* state only *once*. The observable is a translation invariant nearest-neighbor interaction

IOP Institute of Physics **Φ** DEUTSCHE PHYSIKALISCHE GESELLSCHAFT

Hamiltonian on a spin chain with a single cell dimension 56. Given an arbitrary quantum circuit of U, an energy measurement applied to the same type of spin chain (but with sufficient length depending on the length of U) indicates the result 'YES' or 'NO' of U since they correspond to mutually disjoint sets of potential measurement results. The gaps between these sets scale inverse polynomially with the number of gates of the simulated quantum circuit. If the measurement device is able to reliably distinguish between these energy values, one can reproduce the outcome probabilities of the circuit exactly. In this sense, one measurement procedure replaces one run of a quantum circuit.

Even though our specific construction is unlikely to be found in real physical systems, our result strongly suggests that energy measurement for real physical systems is a task whose realization is as challenging as the realization of quantum computing. This shows, once more, that quantum information processing in a broader sense is not only required to solve *computational* problems. Instead, it is a task that occurs already in the context of usual quantum control. Since we have shown in a previous paper that more accurate measurements of observables of a similar type solve all problems in the complexity class PSPACE, our result can also be interpreted as showing how the complexity of quantum control procedures depends on the demanded accuracy.

Acknowledgments

References

[1] Jauch J 1968 *Foundations of Quantum Mechanics* (Reading, MA: Addison-Wesley)
[2] Davies E 1976 *Quantum Theory of Open Systems* (London: Academic)
[3] DiVincenzo D 1995 Two-qubit gates are universal for quantum computation *Phys. Rev.* A **51** 1015–22
[4] Janzing D 2006 *Computer Science Approach to Quantum Control* (Karlsruhe: Uni-Verlag)
[5] Travaglione B and Milburn G 2001 Generation of eigenstates using the phase-estimation algorithm *Phys. Rev.* A **63** 032301
[6] Wocjan P, Janzing D and Decker T 2008 Measuring 4-local n-qubit observables could probabilistically solve PSPACE *Quantum Inf. Comput.* **8** 741–55
[7] Childs A, Leung D and Nielsen M 2005 Unified derivations of measurement-based schemes for quantum computation *Phys. Rev.* A **71** 032318
[8] Raussendorf R and Briegel H J 2000 Quantum computing via measurements only *Phys. Rev. Lett.* **86** 5188
[9] Wocjan P and Zhang S 2006 Several natural BQP-complete problems arXiv:quant-ph/0606179
[10] Feynman R 1985 Quantum mechanical computers *Opt. News* **11** 11–46
[11] Janzing D 2007 Spin-1/2 particles moving on a 2D lattice with nearest-neighbor interactions can realize an autonomous quantum computer *Phys. Rev.* A **75** 012307
[12] Janzing D and Wocjan P 2005 Ergodic quantum computing *Quantum Inf. Process.* **4** 129–58
[13] Kitaev A, Shen A and Vyalyi M 2002 *Classical and Quantum Computation* vol 47 (Providence, RI: American Mathematical Society)
[14] Margolus N 1990 Parallel quantum computation ed W Zurek *Complexity, Entropy, and the Physics of Information* (Reading, MA: Addison-Wesley)

[15] Vollbrecht K and Cirac I 2008 Quantum simulators, continuous-time automata, and translationally invariant systems *Phys. Rev. Lett.* **100** 010501

[16] Janzing D and Wocjan P 2007 A simple PromiseBQP matrix problem *Theory Comput.* **3** 61–79

[17] Aharonov D and Ta-Shma A 2003 Adiabatic quantum state generation and statistical zero knowledge *Proc. 35th Annu. ACM Symp. on Theory of Computing* pp 20–9

[18] Berry D, Ahokas G, Cleve R and Sanders B 2007 Efficient quantum algorithms for simulating sparse Hamiltonians *Commun. Math. Phys.* **270** 359–71

[19] Childs A 2004 Quantum information processing in continuous time *PhD Thesis* Massachusetts Institute of Technology

[20] Janzing D and Wocjan P 2006 BQP-complete problems concerning mixing properties of classical random walks on sparse graphs arXiv:quant-ph/0610235

[21] Janzing D and Wocjan P 2007 A PromiseBQP-complete string rewriting problem arXiv:0705.1180

[22] Goldreich O 2006 On promise problems *Essays in Memory of Shimo Even* pp 254–900. Online at http://dx.doi.org/10.1007/11685654_12

[23] Benioff P 1980 The computer as a physical system: a microscopic quantum mechanical model of computers as represented by Turing machines *J. Stat. Phys.* **22** 562–91

[24] Kempe J and Regev O 2003 3-local Hamiltonian is QMA-complete *Quantum Inf. Comput.* **3** 258–64

[25] Kempe J, Kitaev A and Regev O 2004 The complexity of the local Hamiltonian problem *SIAM J. Comput.* **35** 1070–97

[26] Oliveira R and Terhal B 2008 The complexity of quantum spin systems on a two-dimensional square lattice *Quantum Inf. Comput.* at press (arXiv:quant-ph/0504050)

[27] Aharonov D, Gottesman D and Kempe J 2007 The power of quantum systems on a line *Proc. 48th Annu. IEEE Symp. on Foundations of Computer Science* pp 373–83

[28] Cvetkovic D 1997 *Eigenspaces of Graphs* (Cambridge: Cambridge University Press)

[29] Shepherd D, Franz T and Werner R 2006 A universally programmable quantum cellular automaton *Phys. Rev. Lett.* **97** 020502