Universal simulation of Hamiltonian dynamics for quantum systems with finite-dimensional state spaces

Michael A. Nielsen,[1,*] Michael J. Bremner,[1,†] Jennifer L. Dodd,[1,‡] Andrew M. Childs,[1,2,§] and Christopher M. Dawson[1,‖]
[1]*Centre for Quantum Computer Technology and Department of Physics, University of Queensland, Brisbane 4072, Queensland, Australia*
[2]*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139*
(Received 14 September 2001; published 30 August 2002)

What interactions are sufficient to simulate arbitrary quantum dynamics in a composite quantum system? Dodd *et al.* [Phys. Rev. A **65**, 040301(R) (2002)] provided a partial solution to this problem in the form of an efficient algorithm to simulate any desired two-body Hamiltonian evolution using any fixed two-body entangling N-qubit Hamiltonian, and local unitaries. We extend this result to the case where the component systems are qudits, that is, have D dimensions. As a consequence we explain how universal quantum computation can be performed with any fixed two-body entangling *N-qudit* Hamiltonian, and local unitaries.

DOI: 10.1103/PhysRevA.66.022317 PACS number(s): 03.67.−a, 03.65.Ta

I. INTRODUCTION

A fundamental problem of physics is to determine if there exist physical systems that are *universal*, in the sense that they can be used to efficiently simulate any other system. A candidate for such a universal system was proposed in Deutsch's 1985 paper [1] in the form of a *universal quantum computer* [1–3]. The purpose of this paper is to investigate what physical systems are universal for quantum computation.

The standard model of a quantum computer consists of N qubits, prepared in the state $|0\rangle^{\otimes N}$, that can be manipulated by a sequence of one- and two-qubit operations, and are subsequently measured in the computational basis. There are many possible physical implementations of this model, and in general it is an interesting problem to determine what critical feature or features of a physical system enable universal quantum computation.

In earlier work by Dodd, Nielsen, Bremner, and Thew [4] it was shown that *entanglement* is a crucial physical ingredient for quantum computation. In particular, [4] showed that the ability to do local unitary operations together with any *fixed* N-qubit two-body entangling Hamiltonian may be used to do universal quantum computation on those N qubits.

In this paper we generalize this result to Hamiltonians defined on *qudits*, that is, D-dimensional quantum systems spanned by the states $|0\rangle, \ldots, |D-1\rangle$. This is of intrinsic interest, and is also noteworthy because of the much richer structure revealed in the general proof than in the $D=2$ case studied in Ref. [4].

To state our main result more precisely, we expand an arbitrary Hamiltonian on N qudits as

$$H = \sum_{j_1 k_1 \cdots j_N k_N} \alpha_{j_1 k_1 \cdots j_N k_N} X^{j_1} Z^{k_1} \otimes \cdots \otimes X^{j_N} Z^{k_N}, \quad (1)$$

where $j_1, k_1, \ldots, j_N, k_N$ each run from 0 through $D-1$, $\alpha_{j_1 k_1 \cdots j_N k_N}$ are complex numbers, and the operators X and Z are D-dimensional generalizations of the familiar Pauli operators, to be defined more precisely later. In our work we restrict attention to the case of Hamiltonians that only include two-body coupling terms, and do not allow three- or more-body coupling terms. A *two-body coupling* between a pair of qudits p and q is a term in Eq. (1) of the form $X^j Z^k \otimes X^l Z^m$, where neither $X^j Z^k$ nor $X^l Z^m$ is equal to the identity, so that the term acts nontrivially on qudits p and q, and acts as the identity on all other qudits. In order to generate arbitrary entanglement in the system it is necessary that each qudit pair (s,t) must be *connected* in the sense that there are coupling terms in Eq. (1) for each adjacent pair in some sequence $(s, \ldots, t)$ of qudits in the system. More explicitly, to any two-body Hamiltonian one can associate a graph whose vertices correspond to the qudits in the system, and whose edges connect vertices representing qudits that are coupled by the Hamiltonian. A Hamiltonian is said to be a *two-body N*-qudit entangling Hamiltonian if the graph is connected, that is, there is a path between any pair of vertices. Our main result is as follows:

> Let H be a given two-body entangling Hamiltonian on N qudits, and let K be a desired two-body Hamiltonian on N qudits. Then we have an efficient algorithm to simulate evolution due to K using only (a) the ability to evolve according to H, and (b) the ability to perform local unitaries (that is, single-qudit unitaries) on the individual qudits.

The algorithm we explain below for performing this simulation is only ''efficient'' in the sense of computer science. That is, it requires resources polynomial in the number of qudits N in the system. Our simulation technique is quite involved, and probably too complicated to be experimentally practical. However, the point of principle demonstrated by our simulation technique is of great importance, namely, that all two-body N-qudit entangling Hamiltonians are qualitatively equivalent, given the ability to perform local unitary

*Electronic address: nielsen@physics.uq.edu.au
†Electronic address: bremner@physics.uq.edu.au
‡Electronic address: jdodd@physics.uq.edu.au
§Electronic address: amchilds@mit.edu
‖Electronic address: dawson@physics.uq.edu.au

operations. Thus, in some sense, the ability to entangle can be regarded as a fundamental physical resource—a type of ''dynamic entanglement'' [37]—that can be utilized to perform interesting processes. We explore this idea and make some concrete suggestions for its development in the concluding section, Sec. V. Furthermore, our work may motivate future research on more practically viable methods for doing universal simulation.

Antecedents to our work may be identified in many different parts of the scientific literature. We now enumerate the different fields in which antecedents may be found, before giving a detailed account of the prior work, and how it relates to our own. The basic techniques we use are generalizations of standard techniques from nuclear magnetic resonance (NMR), especially the techniques known as *refocusing* and *decoupling*. The main motivation for our work is inspired by research into universal gates for quantum computation. More recently there has been substantial interest within the quantum information science literature in the problem of determining when one set of Hamiltonians can be used to simulate another. This interest has arisen largely independently of work in the quantum control literature, where closely related issues are being addressed, albeit using different techniques and language.

The main antecedents of our methods are standard NMR techniques for decoupling and refocusing [5,6] that have been developed and refined over the past half century. These techniques have mostly been applied to manipulate specific Hamiltonians, rather than general classes of Hamiltonians. Ideas from NMR have been applied in the quantum computing context by Jones and Knill [7], and by Leung, Chuang, Yamaguchi, and Yamamoto [8], who considered the problem of efficiently implementing logic gates using a restricted class of Hamiltonians that arises naturally in NMR.

One of the main motivations for our work is the desire to understand what resources are universal for quantum computation. Much prior work has been done on this subject, and many universal sets of gates for quantum computation are known. See, for example, Refs. [2,9]. The work most closely related to ours is independent work of Brylinski and Brylinski [10], who used the representation theory of compact Lie groups and real algebraic geometry to study the problem of which two-qudit gates are universal for computation, given the ability to do single-qudit gates. In particular, they defined the class of *imprimitive* unitary gates on two qudits to be the gates that are not of the form $V \otimes W$ or $(V \otimes W)S$, where V and W are single-qudit unitaries, and S is the swap operation. They showed that any imprimitive gate is universal for quantum computation, given the ability to also do arbitrary local unitary operations. Their results thus imply ours for the case when $N=2$. Our results differ from theirs in several ways. First, even in the case when $N=2$, the techniques used in our proof are radically different. Our techniques are much more elementary, relying only on basic linear algebra, a simple result from the theory of majorization, and some very elementary number theory. Thus, our methods give different insights into the problem of universality than those in Ref. [10]. Second, we consider the case where $N>2$, which is potentially of great interest for applications to quantum computation and quantum control.

Also related to our results is the work on universal gates by Deutsch, Barenco, and Ekert [11] and by Lloyd [12], where it was shown that almost any two-qubit gate is universal for quantum computation. Lloyd sketched a generalization of these results to the case of qudits, and this sketch has recently been made rigorous by Weaver [13]. This work differs from ours in that it focuses on unitary gates rather than continuous-time Hamiltonian evolution, and does not result in an explicit characterization of which sets of unitary gates are universal. Our work explicitly determines which two-body Hamiltonians, together with local unitary operations, are universal. Furthermore, in Refs. [11–13] it was assumed that gates could be independently applied to *any* pair of qudits in the computer, and thus required the ability to turn on and turn off interactions between arbitrary pairs of qudits. By contrast, we assume only a fixed entangling operation.

Interest in universal quantum gates has recently motivated interest in the quantum information science literature in the problem of simulating one Hamiltonian with another. Independently of Dodd, Nielsen, Bremner, and Thew [4], the problem of Hamiltonian simulation for qubits was considered by Dür, Vidal, Cirac, Linden, and Popescu in Ref. [14], where it was shown that all two-qubit entangling Hamiltonians are qualitatively equivalent, in the sense that one can be used to simulate the other, given the ability to do local unitaries. Wocjan, Janzing, and Beth [15] considered a *specific* Hamiltonian acting on a system containing N spin-1/2 particles, and considered the overhead incurred when using this Hamiltonian to simulate other Hamiltonians. Bennett, Cirac, Leifer, Leung, Linden, Popescu, and Vidal [16] have considered the problem of *optimal* simulation of one two-qudit Hamiltonian by another, using general local operations, possibly including ancillas and measurements. Thus they considered a different model than ours, which only involves local unitary operations, and, in particular, does not require the ability to perform interactions with local ancilla. Bennett *et al.* showed that in the two-qubit case the two models are, in fact, equivalent. We also note that the results in Ref. [16] are restricted to the case $N=2$. Vidal and Cirac [17] extended the results of Bennett *et al.* by explicitly obtaining the optimal simulation of one two-qubit Hamiltonian by another in the case where classical communication between parties is allowed, in addition to the ability to do local operations, including the use of ancillas and measurement. They also showed that in the case of two qudits the model where local unitary operations are allowed is *distinct* from the case where local unitary operations and ancilla are allowed, in the sense that the latter may be more efficient than the former. We note that Leung and Vidal [18] have independently obtained results on problems related to those we consider. It is worth noting that while related problems are being addressed in this long list of papers, the methods used are quite varied, and the different methods may provide different insights into quantum dynamics.

Independently of the quantum information science literature there has been much interest in Hamiltonian simulation in the field of *quantum control*. A recent overview of work in

quantum control may be found in Ref. [19]. Of particular interest in this context is a general set of necessary and sufficient conditions for determining whether a given set of Hamiltonians can be used to simulate an arbitrary Hamiltonian (see, for example, Schirmer, Solomon, and Leahy [20]). These conditions can be applied to determine whether, in any specific instance, a collection of Hamiltonians can be used to simulate an arbitrary Hamiltonian, however, they do not directly speak to the question of what class of interactions is universal for quantum computation, given the ability to perform local unitaries.

Finally, we note that the techniques used in this paper are closely related to the interesting problem of using a Hamiltonian H to simulate time-reversed evolution due to the Hamiltonian $-H$. Results on this problem have been obtained by Janzing, Wocjan, and Beth [21], and by Leung [22].

The structure of our paper is as follows. Section II introduces background techniques needed in the main body of the paper, including results on the Pauli group and majorization. Section III explains the $N=2$ case of the general problem, that is, how any two-qudit entangling Hamiltonian can be used to simulate any other two-qudit Hamiltonian, provided local unitaries are allowed. In Sec. IV we explain how this result can be applied to the general problem of quantum computation on N qudits, and prove our central result. Finally, Sec. V concludes the paper with a summary and discussion of our results, and a discussion of open problems.

As the main body of the paper involves a quite extensive construction, some readers may not wish to wade through all the details. We have structured the paper so that such a reader may follow the summaries provided at the beginning of Secs. II and III, all of Sec. IV on universal quantum computation, and all of the discussion in Sec. V.

II. BACKGROUND

We now review the background needed to appreciate the main body of the paper. At a first read it may be useful to skip over the proofs, and pause mainly to appreciate the nomenclature and basic results. Readers who wish to skip the entire section should note the main result: given the ability to evolve according to a Hamiltonian J and perform unitary operations U_k it is possible to simulate evolution according to a Hamiltonian of the form $\Sigma_k \alpha_k U_k J U_k^\dagger$, where the α_k are real numbers. This composition law for Hamiltonians is the basis for all our later simulation results. Note also that throughout the paper we use $=_D$ to indicate equality modulo D. So, for example, $7=_4 3$, since 7 is equal to 3, modulo 4.

The structure of the section is as follows. In Sec. II A we summarize the relations satisfied by operators in the Pauli group. Sec. II B describes the composition laws used later in the paper to build up a library of Hamiltonians we can efficiently simulate given the primitive Hamiltonians initially at our disposal. Finally, Sec. II C reviews the basic elements of the theory of majorization, including a corollary of Uhlmann's theorem crucial to our later analysis.

A. The Pauli group

The D-dimensional Pauli group consists of all D-dimensional operators of the form $\omega^l X^j Z^k$, where $j,k,l = 0,\ldots,D-1$, $\omega = \exp(2\pi i/D)$,

$$X|z\rangle \equiv |z \oplus 1\rangle; \quad Z|z\rangle \equiv \omega^z |z\rangle, \tag{2}$$

and $\oplus$ denotes addition modulo D. The properties of the Pauli group were investigated in detail by Gottesman [23], and the reader is referred to that paper for additional information.

It is worth noting a few simple properties of the Pauli matrices. First, $X^D = Z^D = I$. Thus, when writing the Pauli matrices we can freely interchange expressions such as Z^{D-1} and Z^{-1}, and expressions like $Z^\dagger$ and Z^{-1}. In a similar vein, note that $(X^j Z^k)^\dagger = Z^{-k} X^{-j}$. Through most of the paper we use notation like $Z^{-k}X^{-j}$ in preference to $(X^j Z^k)^\dagger$.

The basic commutation relations for the Pauli group may be written as

$$(X^j Z^k)(X^s Z^t) = \omega^{ks-jt}(X^s Z^t)(X^j Z^k). \tag{3}$$

We will have very frequent occasion to use these commutation relations. In particular, note that $X^j Z^k$ commutes with $X^s Z^t$ if and only if $ks =_D jt$.

Gottesman [23] studied the properties of the Pauli group under conjugation by D-dimensional unitary operators. In particular, he was interested in *normalizer operations*, that is, unitary operations U such that under conjugation by U the Pauli group is taken to itself. In Appendix A we explicitly describe unitary operators performing the following three conjugation operations:

$$X \to Z, \quad Z \to X^{-1}, \tag{4}$$

$$X \to XZ, \quad Z \to Z, \tag{5}$$

$$X \to X^a, \quad Z \to Z^{a^{-1}}, \text{ when } \gcd(a,D) = 1, \tag{6}$$

where $A \to B$ means that $UAU^\dagger = e^{i\theta}B$ for some phase factor $e^{i\theta}$. Note that the phase factors are unimportant for the proof, and will mostly be ignored in the sequel. These equations imply that the following three conjugation operations may also be performed:

$$X \to Z^{-1}, \quad Z \to X, \tag{7}$$

$$X \to X, \quad Z \to XZ, \tag{8}$$

$$X \to X^{a^{-1}}, \quad Z \to Z^a, \text{ when } \gcd(a,D) = 1. \tag{9}$$

We now use the normalizer operations to prove what we term the Pauli-Euclid-Gottesman (PEG) lemma. Aside from its interest as applied in this paper, the PEG lemma is also interesting because it enables us to explicitly calculate the eigenvalues and eigenvectors of all elements of the Pauli group, showing a surprising connection between the Pauli group and Euclid's algorithm ([24], Book 7, Propositions 1 and 2) for finding the greatest common divisor.

Pauli-Euclid-Gottesman Lemma. For any dimension D and for integers j and k such that $1 \leqslant j,k \leqslant D-1$, there exists a unitary operator U such that $X^j Z^k \rightarrow Z^{\gcd(j,k)}$ under conjugation by U.

Note, incidentally, that the PEG lemma implies that the eigenvalues of $X^j Z^k$ are equal to the eigenvalues of $Z^{\gcd(j,k)}$, up to a global phase which may be calculated from the proof, below. The eigenvalues of $Z^{\gcd(j,k)}$ are easily calculable, since Z is already diagonal. The eigenvectors of $X^j Z^k$ may also be extracted from the proof of the PEG lemma, below, where we explain how to construct the conjugating operation, U.

Proof. From Eqs. (4)–(9) we see that it is possible to perform the following operations under conjugation:

$$X^j Z^k \rightarrow X^j Z^{k+\alpha j}, \tag{10}$$

$$X^j Z^k \rightarrow X^{j+\alpha k} Z^k, \tag{11}$$

where α is any integer. The basic idea of the proof is to use these two operations and Euclid's algorithm on the paired exponents of X and Z. We will give an example of how this is done, with the general proof following similar lines. Consider the operator $X^{104} Z^{80}$. Recall how Euclid's algorithm is used to find the greatest common divisor of 104 and 80. We write $104 = 1 \times 80 + 24$, so $\gcd(104,80) = \gcd(80,24)$. Next, we write $80 = 3 \times 24 + 8$, so $\gcd(104,80) = \gcd(24,8)$. Finally, we write $24 = 3 \times 8$, so $\gcd(104,80) = 8$. These steps are easily mimicked with the Pauli operators using Eqs. (10) and (11). We have

$$X^{104} Z^{80} \rightarrow X^{104-1\times 80} Z^{80} = X^{24} Z^{80}, \tag{12}$$

$$X^{24} Z^{80} \rightarrow X^{24} Z^{80-3\times 24} = X^{24} Z^8, \tag{13}$$

$$X^{24} Z^8 \rightarrow X^{24-3\times 8} Z^8 = Z^8. \tag{14}$$

The general proof proceeds analogously, using Euclid's algorithm. ■

A key tool in our analysis is the *operator expansion*. We will explain in detail how this expansion works for the case of two qudits. Any operator J on two qudits may be expanded in the form

$$J = \sum_{jklm} r_{jklm} X^j Z^k \otimes X^l Z^m, \tag{15}$$

where the sum is over the range $j,k,l,m = 0, \ldots, D-1$, and the coefficients r_{jklm} may be calculated using the expression,

$$r_{jklm} = \frac{\mathrm{tr}[(Z^{-k} X^{-j} \otimes Z^{-m} X^{-l}) J]}{D^2}. \tag{16}$$

In general it is useful to introduce the convention that the indices in sums always range over $0, \ldots, D-1$, unless otherwise noted.

Equation (15) applies for any operator, however, Hermitian operators satisfy additional constraints on the form of the coefficients r_{jklm}. For example, if a term of the form $\alpha Z^k \otimes Z^m$ appears in the operator expansion, then its Hermitian conjugate $\alpha^* Z^{-k} \otimes Z^{-m}$ must also appear in the operator expansion. In general, terms in the operator expansion of a Hermitian operator appear in Hermitian conjugate pairs.

The operator expansion may be used to establish a useful identity satisfied by any operator J on a single qudit,

$$\sum_{jk} (X^j Z^k) J (Z^{-k} X^{-j}) = D \mathrm{tr}(J) I. \tag{17}$$

The identity Eq. (17) is well known in quantum information science from the properties of the depolarizing channel for D-dimensional systems. The identity may be verified by direct calculation, or by substituting an operator expansion for J. Equation (17) may also be extended to multiple qudits. For our purposes all that matters is the two-qudit case, which reads

$$\sum_{jklm} (X^j Z^k \otimes X^l Z^m) J (Z^{-k} X^{-j} \otimes Z^{-m} X^{-l}) = D^2 \mathrm{tr}(J) I \otimes I. \tag{18}$$

We conclude this section with a brief digression, noting that an alternate proof of Eq. (17) may be obtained by applying Schur's lemma from group representation theory [25]. Let G_D denote the Pauli group in D dimensions, and note that

$$\sum_{jk} (X^j Z^k) J (Z^{-k} X^{-j}) = \frac{1}{D} \sum_{U \in G_D} U J U^\dagger. \tag{19}$$

The factor $1/D$ on the right-hand side arises because of the phases ω^l in front of a general member of the Pauli group, $\omega^l X^j Z^k$. The right-hand side of this equation commutes with any $U \in G_D$. The result follows from Schur's lemma if we can prove that G_D is irreducible. Suppose G_D is reducible, so that there exists a nontrivial subspace of the qudit state space stable under the operations in G_D. Let P denote the projector onto that subspace. Because the subspace is stable it follows that $ZPZ^{-1} = P$, and thus Z commutes with P. It follows that P can be diagonalized in the basis $|0\rangle, \ldots, |D-1\rangle$, and thus the stable subspace is spanned by a strict subset of $|0\rangle, \ldots, |D-1\rangle$. Suppose $|z\rangle$ is in the stable subspace, but $|z \oplus 1\rangle$ is not. But $X|z\rangle = |z \oplus 1\rangle$, so the subspace is not stable, which is a contradiction. This completes the proof of Eq. (17).

B. Composition laws for Hamiltonian simulation

The basic idea employed in the main part of the paper is to use our primitive set of operations and a small number of *composition laws* to build up a library of Hamiltonian evolutions we can simulate. We now explain the composition laws that we use, adapting from Ref. [4].

(a) Imagine we can evolve according to the Hamiltonian J, and perform unitary operations U and $U^\dagger$. Then it follows from the identity $e^{-itUJU^\dagger} = U e^{-itJ} U^\dagger$ that we can exactly simulate evolution according to the Hamiltonian $UJU^\dagger$.

(b) Imagine we can evolve according to the Hamiltonians J_1 and J_2. Then we can simulate evolution due to $J_1 + J_2$ for

small times Δ, due to the approximate identity

$$e^{-i\Delta(J_1+J_2)} \approx e^{-i\Delta J_1} e^{-i\Delta J_2}. \tag{20}$$

We treat this identity as though it is exact. This is justified, since to simulate a Hamiltonian for a time t it suffices to perform n separate simulations of a time $\Delta \equiv t/n$ each, giving an error of $n \times O(\Delta^2) = O(t\Delta)$. This error can thus be made arbitrarily small by making Δ sufficiently small. Further remarks on the error analysis are made for the qubit case in Ref. [4], and these results carry over directly to the qudit case.

(c) Imagine we can evolve according to the Hamiltonian J. Then, by appropriate timing, we can exactly simulate evolution according to λJ for any $\lambda > 0$.

(d) Imagine we can evolve according to the Hamiltonian J. Then we can evolve according to the Hamiltonian $-J$. We will explicitly prove this only for the case of two-qudit Hamiltonians J, however the proof easily generalizes. Note that we can rewrite Eq. (18),

$$-J = \sum (X^j Z^k \otimes X^l Z^m) J (Z^{-k} X^{-j} \otimes Z^{-m} X^{-l}) - D^2 \mathrm{tr}(J) I \otimes I, \tag{21}$$

where we have extracted the $-J$ by taking the sum on the right-hand side over all terms except $(j,k,l,m) = (0,0,0,0)$. Physically, the term $-D^2 \mathrm{tr}(J) I \otimes I$ is an unimportant rescaling of the energy and can be neglected. The other terms in the expansion for $-J$ are all easily simulated using techniques (a) and (b) above. Note that the complexity of the simulation scales as $O(D^4)$.

The above observations (a)–(d) may be summarized in a single equation as follows. Given the ability to perform evolution according to the Hamiltonian J and the ability to perform unitaries U_k, it is possible to simulate evolution according to a Hamiltonian of the form

$$\sum_k \alpha_k U_k J U_k^\dagger, \tag{22}$$

where the α_k can be arbitrary real numbers.

C. Majorization

The final area of background we shall need is the theory of *majorization*, whose basic elements we now review, following Ref. [26]. More detailed introductions to majorization may be found in Chaps. 2 and 3 of Ref. [27] and in Refs. [28,29]. Suppose $x = (x_1, \ldots, x_D)$ and $y = (y_1, \ldots, y_D)$ are two D-dimensional real vectors. The relation "x is majorized by y" is intended to capture the notion that x is more mixed (i.e., disordered) than y. To make the formal definition we introduce the notation $\downarrow$ to denote the components of a vector rearranged into nonincreasing order, so $x^\downarrow = (x_1^\downarrow, \ldots, x_D^\downarrow)$, where $x_1^\downarrow \geqslant x_2^\downarrow \geqslant \cdots \geqslant x_D^\downarrow$. We say that x is majorized by y, and write $x \prec y$, if

$$\sum_{j=1}^k x_j^\downarrow \leqslant \sum_{j=1}^k y_j^\downarrow, \tag{23}$$

for $k = 1, \ldots, D-1$, and with the inequality holding with equality when $k = D$.

The notion of majorization can be extended in a natural way to Hermitian operators. We say that the Hermitian operator A is majorized by the Hermitian operator B, and write $A \prec B$, if the spectrum $\lambda(A)$ of eigenvalues of A is majorized by the spectrum $\lambda(B)$ of eigenvalues of B, where we regard the spectra $\lambda(A)$ and $\lambda(B)$ as vectors. So, for example,

$$\begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \prec \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \tag{24}$$

since the spectra of the two matrices satisfy the majorization criterion, $(1/2,1/2) \prec (1,0)$.

It is not immediately obvious how this definition of operator majorization connects to any natural notion of comparative disorder. There is a beautiful result due to Uhlmann [30] (see also the reviews [31] and [32]) that provides such a connection. Uhlmann's theorem states that $A \prec B$ if and only if $A = \Sigma_n p_n U_n B U_n^\dagger$, where the U_n are unitary operators, and the p_n form a probability distribution. That is, $A \prec B$ if and only if A can be obtained from B by mixing together operators unitarily equivalent to B. Two important points about the proof of Uhlmann's theorem are that the procedure for finding the p_n and U_n is *constructive*, and, furthermore, there are at most D^2 operators U_n.

We now observe that Uhlmann's theorem has a beautiful corollary when applied to *any* two traceless Hermitian operators A and B [38].

Theorem. Let A and B be any two traceless Hermitian operators, and assume $B \neq 0$. Then $A \prec cB$ for some positive constant c. Uhlmann's theorem then gives an algorithm to find a set of at most D^2 unitary operators U_n, and $c_n > 0$, such that

$$A = \sum_n c_n U_n B U_n^\dagger. \tag{25}$$

As an example of this theorem in action, consider that for any $(j,k) \neq (0,0)$ and $(l,m) \neq (0,0)$ there exist U_n and c_n such that

$$X^j Z^k + Z^{-k} X^{-j} = \sum_n c_n U_n (X^l Z^m + Z^{-m} X^{-l}) U_n^\dagger. \tag{26}$$

Using the techniques of the preceding section, notably Eq. (22), we see that this equation can be interpreted as providing a means of simulating the Hamiltonian $X^j Z^k + Z^{-k} X^{-j}$ given the Hamiltonian $X^l Z^m + Z^{-m} X^{-l}$ and the ability to perform the unitary operations U_n. On its own, this is not an especially useful simulation result! However, similar but more sophisticated variants on this idea will be used in our later construction.

Proof. The case when $A=0$ follows by noting that $0<cB$ for all $c>0$, so we assume $A\neq 0$. We aim to show that $\lambda(A)<c\lambda(B)$, for some $c>0$. Choose

$$c \equiv \max_{k=1,\ldots,D-1} \frac{\sum_{j=1}^{k} \lambda_j^{\downarrow}(A)}{\sum_{j=1}^{k} \lambda_j^{\downarrow}(B)}. \tag{27}$$

Since A and B are traceless and not equal to 0, it follows that $c>0$. For $k=1,\ldots,D-1$ we have

$$\sum_{j=1}^{k} \lambda_j^{\downarrow}(A) = \frac{\sum_{j=1}^{k} \lambda_j^{\downarrow}(A)}{\sum_{j=1}^{k} \lambda_j^{\downarrow}(B)} \sum_{j=1}^{k} \lambda_j^{\downarrow}(B) \tag{28}$$

$$\leqslant c \sum_{j=1}^{k} \lambda_j^{\downarrow}(B). \tag{29}$$

Finally, note that

$$\sum_{j=1}^{D} \lambda_j^{\downarrow}(A) = 0 = \sum_{j=1}^{D} c\lambda_j^{\downarrow}(B), \tag{30}$$

which completes the proof. ■

III. TWO-QUDIT HAMILTONIAN SIMULATION

In this section we study universal simulation with two-qudit Hamiltonians, that is, Hamiltonians of the form

$$H = \sum_{jklm} \alpha_{jklm} X^j Z^k \otimes X^l Z^m. \tag{31}$$

We show that provided this Hamiltonian has a nonzero coupling term, that is, a term not of the form $I\otimes(\cdot)$ or $(\cdot)\otimes I$, then H and local unitary operations can be used to simulate *any* other two-qudit Hamiltonian K.

The basic idea of the proof is to use the composition laws of Sec. II B to increase the library of Hamiltonians that can be simulated. It will be convenient to use the notation $H_1, H_2, \ldots$ to denote the different Hamiltonians that we show how to simulate. The construction is rather complicated, for which reason we break it up into steps. This separation into steps makes it convenient to introduce some global notational conventions. Terms such as j,k,l,m,n,r,s,t are specific to each step, and sometimes to individual lines in the proof, often being used as dummy variables, with the meaning to be determined from context. Terms such as a,b,c,d,f carry over from one step to another. All of these terms ($j,k,\ldots$ and $a,b,\ldots$) are consistently integers in the range $0,\ldots,D-1$.

The general strategy through most of the proof is to gradually eliminate more and more terms from the Hamiltonian, while keeping particular desired couplings. At the end of the proof we are able to simulate a Hamiltonian of an especially simple form, which can then be used to build up arbitrarily complicated Hamiltonians. We now give an outline of the proof. Note that the numbering scheme used in the outline is mirrored in the numbering scheme used in the detailed explanation of the proof given below in Sec. III A.

(1) We show that H and local unitaries can be used to simulate a Hamiltonian H_1 that contains a $Z^a\otimes Z^b$ coupling term. This term is the focus of most of the remaining steps of the proof, as we try to eliminate most of the other coupling terms from the Hamiltonian.

(2) We show that H_1 and local unitaries can be used to eliminate terms in H_1 not of the form $Z^j\otimes Z^k$, and thus to simulate a Hamiltonian H_2 of the form $\Sigma_{jk}\alpha_{jk}Z^j\otimes Z^k$, which still contains the nonzero coupling $\alpha_{ab}Z^a\otimes Z^b$.

(3) We show that H_2 and local unitaries can be used to simulate a Hamiltonian of the form $H_3=\Sigma_n\beta_n(Z^c\otimes Z^d)^n$, with at least one nonzero coupling coefficient β_f.

(4) We show that H_3 and local unitaries can be used to simulate a Hamiltonian of the form $H_6=\kappa Z^a\otimes Z^b+\kappa^* Z^{-a}\otimes Z^{-b}$, for any complex κ.

(5) We show that H_6 and local unitaries can be used to simulate $H_8=(Z^a+Z^{-a})\otimes(Z^b+Z^{-b})$.

(6) Using the corollary to Uhlmann's theorem we show that H_8 can be used to simulate any Hamiltonian of the form $J\otimes J'$, where J and J' are arbitrary traceless Hermitian operators. Any two-qudit Hamiltonian can be expressed as a sum of terms of this form, together with local interactions, so we conclude that any two-qudit Hamiltonian can be simulated using H and local unitaries.

This construction is complex, and a detailed efficiency analysis is not especially enlightening. Nonetheless, from the proof below it follows that the total simulation requires a number of periods of evolution due to H which is *polynomial* in the dimension D. This can be seen by examining each step in the construction and verifying that they involve only a summation $\Sigma_k\alpha_k(U_k\otimes V_k)J(U_k\otimes V_k)^\dagger$ over at most polynomially many terms in D, where the U_k and V_k are local unitaries, J is some entangling Hamiltonian that we are already able to simulate, and the coefficients α_k are also polynomial in D.

It is worth noting that the proof can be substantially simplified if one assumes that D is prime. The reason this simplification occurs is because in prime dimensions all nontrivial elements of the Pauli group are equivalent to one another by unitary conjugation. Thus, given a nonzero coupling term in the Hamiltonian it is easy to simulate a Hamiltonian in which a nonzero coupling of the form $Z\otimes Z$ appears. Given this, steps 1 and 3 can be considerably simplified. We describe in detail how this simplification occurs in Sec. III B.

A. Detailed proof

1. Simulating a Hamiltonian with a nonzero $Z^a\otimes Z^b$ coupling

By assumption, our Hamiltonian includes a coupling term of the form $X^jZ^k\otimes X^lZ^m$ with a nonzero coefficient. If $j\neq 0$ or $l\neq 0$ then the PEG lemma and Eq. (4) imply that by performing local unitary conjugation we can convert this to a coupling term of the form $Z^a\otimes Z^b$ with a nonzero coefficient.

Let H_1 be the Hamiltonian that results when this conjugation is performed. It will be convenient for our later discussion to fix coprime c and d such that $c/d=a/b$, that is, c/d is a/b in lowest common terms. It will also be convenient to define f such that $a=fc$ and $d=fb$.

2. Simulating a Hamiltonian of the form $\Sigma_{jk}\alpha_{jk}Z^j\otimes Z^k$

We have shown that H_1 contains a coupling term of the form $Z^a\otimes Z^b$, however, it could also contain many other coupling terms. We aim to eliminate these other terms, while keeping the coupling $Z^a\otimes Z^b$. In particular, we now explain how to eliminate those terms containing X or a power of X. Note that given the ability to do H_1 we can simulate

$$H_2=\sum_{lm}\ (Z^l\otimes Z^m)H_1(Z^{-l}\otimes Z^{-m}). \tag{32}$$

To evaluate this sum we first use the commutation relations for the generalized Pauli operators and then the observation that $\Sigma_t\omega^{st}=D$ when $s=_D0$, and $\Sigma_t\omega^{st}=0$ otherwise. Using these facts we see that H_2 has the form

$$H_2=\sum_{jk}\ \alpha_{jk}Z^j\otimes Z^k. \tag{33}$$

The term $Z^a\otimes Z^b$ in H_1 was nonzero, so $\alpha_{ab}\neq 0$.

3. Elimination of all terms not of the form $(Z^c\otimes Z^d)^n$

The next step of the proof is to eliminate all the terms in H_2 that are not powers of $(Z^c\otimes Z^d)$. Note that we know there is at least one nonzero term of this form, the term $Z^a\otimes Z^b=(Z^c\otimes Z^d)^f$. The key to this is a simple number-theoretic lemma.

Lemma. Suppose $\gcd(l,m)=1$. Then $jm=_Dkl$ if and only if there exists n such that

$$j=_Dnl, \quad \text{and} \quad k=_Dnm. \tag{34}$$

We will give two proofs of this lemma. The first is a constructive proof that only involves elementary number theory. The second proof is in some sense more elegant in that it invokes the PEG lemma, and makes use of notions of linear algebra. The second proof is given in Appendix B.

Proof. The reverse implication follows by a simple substitution, so we prove only the forward implication. Since $\gcd(l,m)=1$ there exist integers r and s such that $rl+sm=1$. Now choose $n\equiv jr+ks$. Then we have

$$nl=_Djrl+ksl \tag{35}$$

$$=_Djrl+jsm \tag{36}$$

$$=_Dj(rl+sm) \tag{37}$$

$$=_Dj, \tag{38}$$

as required. A similar calculation shows that $nm=_Dk$. ■

Applying our composition laws we see that we can simulate

$$H_3=\sum_{l}\ (X^{-d}\otimes X^c)^lH_2(X^d\otimes X^{-c})^l. \tag{39}$$

Applying the commutation relations for the Pauli matrices this simplifies to

$$H_3=\sum_{jk}\ \alpha_{jk}\left[\sum_{l}\ \omega^{(dj-ck)l}\right]Z^j\otimes Z^k. \tag{40}$$

Note that the sum over l is zero unless $dj=_Dck$. By the lemma, this is the case if and only if $j=_Dnc$ and $k=_Dnd$ for some n, and thus $Z^j\otimes Z^k=(Z^c\otimes Z^d)^n$ for some n. Thus H_3 has the form

$$H_3=\sum_{n}\ \beta_n(Z^c\otimes Z^d)^n, \tag{41}$$

where the β_n are complex numbers. Recall that $a=fc$ and $b=fd$, so $\beta_f\propto\alpha_{ab}$, and there is at least one nonzero coupling term in H_3.

4. Simplifying to a sum of at most two terms

Our next task is to eliminate nearly all the coupling terms in H_3. First, we set up some notation. Since $\gcd(c,d)=1$ we can choose l and m such that $lc+md=1$. It will be convenient to write the coefficients β_n as a D-dimensional vector, that is $\vec{\beta}=(\beta_0,\beta_1,\ldots,\beta_{D-1})$, where we use the convention that expressions like $(x,y,z,\ldots)$ denote column vectors. It will also be convenient to use the notation $\vec{e}_0,\ldots,\vec{e}_{D-1}$ for the unit vectors in this D-dimensional vector space, and to identify $\vec{e}_{-j}$ with $\vec{e}_{D-j}$. So, for example, $\vec{e}_1=(0,1,0,0,\ldots,0)$, and $\vec{e}_{-2}=\vec{e}_{D-2}$. Note that the constraint that H_3 is Hermitian implies that $\vec{\beta}^*=P\vec{\beta}$, where $P\vec{e}_n=\vec{e}_{-n}$ for $n=0,\ldots,D-1$.

Next, suppose $\vec{\gamma}=(\gamma_0,\ldots,\gamma_{D-1})$ is a real vector. Using our composition laws we can simulate the Hamiltonian

$$H_4=\sum_{j}\ \gamma_j(X^{-l}\otimes X^{-m})^jH_3(X^l\otimes X^m)^j. \tag{42}$$

Our strategy will be to choose $\vec{\gamma}$ in such a way that H_4 has an especially simple form. Applying the commutation relations for the Pauli operators gives

$$H_4=\sum_{jn}\ \gamma_j\beta_n\omega^{(lc+md)jn}(Z^c\otimes Z^d)^n \tag{43}$$

$$=\sum_{n}\ \delta_n(Z^c\otimes Z^d)^n, \tag{44}$$

where in the second step we used the fact that $lc+md=1$, and we define

$$\delta_n\equiv\beta_n\sum_{j}\ \omega^{nj}\gamma_j. \tag{45}$$

The sum on the right-hand side is most conveniently written in matrix form as $M\vec{\gamma}$, where M is the matrix with entries $M_{nj} \equiv \omega^{nj}$. Up to a constant M is just the matrix representation of the discrete Fourier transform, which is easily inverted, so we can choose $\vec{\gamma}$ such that $M\vec{\gamma} = \vec{e}_f + \vec{e}_{-f}$.

Recall that the γ_j in Eq. (42) must be real in order for a simulation of H_4 to be possible. We now use a symmetry argument to show that this is the case. Note that $M\vec{\gamma} = \vec{e}_f + \vec{e}_{-f}$, by definition of $\vec{\gamma}$. Since P, $\vec{e}_f$ and $\vec{e}_{-f}$ are real,

$$M\vec{\gamma} = \vec{e}_f + \vec{e}_{-f} = [P(\vec{e}_f + \vec{e}_{-f})]^*. \tag{46}$$

Next, from $M\vec{\gamma} = \vec{e}_f + \vec{e}_{-f}$ and $P^* = P$ we obtain

$$[P(\vec{e}_f + \vec{e}_{-f})]^* = PM^*\vec{\gamma}^*. \tag{47}$$

Combining these results we see that $PM^*\vec{\gamma}^* = M\vec{\gamma}$. Observing that $PM^* = M$ we obtain $M\vec{\gamma}^* = M\vec{\gamma}$, and thus $\vec{\gamma}$ is real.

Summarizing, we have obtained the ability to simulate a Hamiltonian

$$H_4 = \beta Z^a \otimes Z^b + \beta^* Z^{-a} \otimes Z^{-b}, \tag{48}$$

where $\beta \equiv \beta_f$, and the fact that $\beta_{-f} = \beta^*$ follows from the fact that H_4 is Hermitian. Conjugating by $X^{-1} \otimes I$ we also obtain the ability to simulate the Hamiltonian

$$H_5 = \beta\omega^a Z^a \otimes Z^b + (\beta\omega^a)^* Z^{-a} \otimes Z^{-b}. \tag{49}$$

However, note that *any* complex number κ can be formed from real linear combinations of β and $\beta\omega^a$, so by taking appropriate real linear combinations of H_4 and H_5 we see that we can simulate any Hamiltonian of the form

$$H_6 = \kappa Z^a \otimes Z^b + \kappa^* Z^{-a} \otimes Z^{-b}. \tag{50}$$

5. Simulation of a tensor product Hamiltonian

Applying Eq. (6) to the second qudit we see that we can simulate any Hamiltonian of the form

$$H_{7\pm} = \kappa Z^a \otimes Z^{\pm b} + \kappa^* Z^{-a} \otimes Z^{\mp b}, \tag{51}$$

and it follows by taking linear combinations that we can simulate

$$H_8 = (Z^a + Z^{-a}) \otimes (Z^b + Z^{-b}). \tag{52}$$

6. Simulation of any Hamiltonian

Note that $Z^a + Z^{-a}$ and $Z^b + Z^{-b}$ are nonzero, traceless, Hermitian operators, so by the corollary to Uhlmann's theorem we can simulate *any* Hamiltonian of the form $J \otimes J'$, where J and J' are arbitrary traceless, Hermitian operators. The operator expansion implies that an arbitrary two-qudit Hamiltonian can be formed as a real linear combination of such Hamiltonians, together with single-qudit terms of the form $J \otimes I$ or $I \otimes J'$. Thus, with the ability to perform H and local unitary operations we can simulate an arbitrary two-qudit Hamiltonian.

B. The case where D is prime

The proof just given can be substantially simplified in the case where D is prime. We now sketch how the simplified proof goes. The reason for the simplification is that any nontrivial element $X^j Z^k$ of the Pauli group is equivalent under conjugation to Z. To see this, note that if $j \neq 0$ and $k \neq 0$ then, using the PEG lemma it is possible to conjugate $X^j Z^k$ to Z^l, up to a phase factor, for some l such that $1 \leqslant l \leqslant D-1$. Similarly, if $k = 0$ then we can conjugate to some such Z^l using Eq. (4), while if $j = 0$ then the term is already in this form. In turn this may be conjugated to Z using Eq. (6), since l is coprime to D when D is prime. It follows that in step 1 of the above proof we can show that it is possible to simulate a Hamiltonian H_1 that contains a $Z \otimes Z$ coupling term. Step 2 proceeds exactly as before, and results in a Hamiltonian of the form $H_2 = \Sigma_{jk} \alpha_{jk} Z^j \otimes Z^k$, such that $\alpha_{11} \neq 0$.

Step 3 of the preceding proof is substantially simplified. In particular, we note that it is possible to simulate the Hamiltonian

$$H_3 = \sum_l (X^l \otimes X^{-l}) H_2 (X^{-l} \otimes X^l), \tag{53}$$

$$= \sum_{jkl} \alpha_{jk} \omega^{l(k-j)} Z^j \otimes Z^k, \tag{54}$$

$$= D \sum_j \alpha_{jj} (Z \otimes Z)^j. \tag{55}$$

The remainder of the proof can then be completed as before.

IV. APPLICATIONS TO UNIVERSAL QUANTUM COMPUTATION

We have shown that any two-qudit entangling Hamiltonian, together with local unitary operations, may be used to simulate any other two-qudit Hamiltonian. We now extend this result to the problem of universal quantum computation on N qudits. In particular, we show that any two-body N-qudit entangling Hamiltonian, together with local unitaries, can be used to perform universal quantum computation.

The basic strategy follows the method presented in Ref. [4]. The idea is to reduce the problem to the two-qudit case already solved. To do this, we divide the system into a *principal system* P consisting of two qudits coupled by the Hamiltonian H of the entire system, and the *remainder* of the system, denoted S. Our techniques generalize the results in Refs. [7,8], which are themselves generalizations of standard techniques from NMR. The basic idea is to turn off all the interactions between P and S, and within S, leaving only the interactions present in P. We will refer to such a suppression of interactions as *decoupling*. The remaining interactions can then be used, as before, to simulate arbitrary dynamics on the two qudits in P. Thus it is possible to simulate arbitrary dynamics on *any* two qudits coupled by H. Finally, an arbitrary interaction between qudits s and t may be effected by performing a sequence of SWAP gates between the qudits connecting s and t (in the sense defined in Sec. I), applying

the desired interaction, and swapping back. Note that such a sequence of SWAP operations can be performed using the method already described for simulating quantum gates. In this way we can effect any two-qudit Hamiltonian between any pair of qudits in the system, and thus perform universal quantum computation.

The obvious technique for achieving decoupling is to eliminate couplings between P and S, and within S, one at a time, using techniques along the lines of those used to simulate one two-qudit Hamiltonian with another. Unfortunately, this procedure is not efficient, for reasons we now explain. As an example, suppose P consists of two qudits, labeled A and B, and S consists of two qudits, E and F. Then interactions between qudit E and the remainder of the system may be effectively turned off by simulating the Hamiltonian,

$$H' = \frac{\sum_U U_E H U_E^\dagger}{D^2}, \tag{56}$$

where U runs over all Pauli matrices $X^j Z^k$ and the E indicates that U is being applied to the qudit E. While we can, in principle, turn off all interactions in this way, the resulting procedure is not efficient. To see this, notice that turning off all the couplings to the qudit E required a sum over D^2 terms, each a conjugated form of the Hamiltonian H. For an N-qudit system generalizing this procedure in the obvious way would require a sum over D^N terms. The corresponding simulation would therefore have exponential complexity, which is not efficient.

Fortunately, much more efficient techniques for decoupling can be devised. In this section we explain two such techniques. Sec. IV A explains how the decoupling can be performed for a completely *arbitrary* two-qudit Hamiltonian, while Sec. IV B explains how the procedure for decoupling can be substantially simplified and made more efficient when the Hamiltonian has the localized structure found in most physical systems.

A. The case of arbitrary two-qudit interactions

Suppose H is an arbitrary two-qudit entangling Hamiltonian. We now explain how to efficiently eliminate all couplings between a principal system P and the remainder of the system S, and to eliminate all couplings internal to S, while leaving the couplings within P invariant. The method is a straightforward generalization of that described for qubits by Dodd *et al.* [4]. Let U run over all Pauli matrices $X^j Z^k$. Define U_S to be the tensor product of identical operators U acting ditwise on the qudits in S. We form the Hamiltonian

$$H' = \frac{1}{D^2} \sum_U U_S H U_S^\dagger, \tag{57}$$

and observe that H' leaves the Hamiltonian on P invariant, but eliminates all coupling terms between P and S, and all single-qudit terms acting within S.

We now explain a recursive construction to eliminate all remaining couplings in S. First, we break the block S into two blocks S_0 and S_1 of approximately equal size. We decouple S_0 and S_1 by forming the Hamiltonian

$$H'' = \frac{1}{D^2} \sum_U U_{S_0} H' U_{S_0}^\dagger. \tag{58}$$

Next, we break S_0 into two blocks S_{00} and S_{01} of approximately equal size, and break S_1 into two blocks S_{10} and S_{11} of approximately equal size. We can decouple S_{00} from S_{10}, and S_{01} from S_{11} in a single step by forming the Hamiltonian,

$$H''' = \frac{1}{D^2} \sum_U (U_{S_{00}} \otimes U_{S_{10}}) H'' (U_{S_{00}} \otimes U_{S_{10}})^\dagger. \tag{59}$$

By repeating this blocking procedure $\lceil \log_2(n-2) \rceil$ times we can complete the decoupling, leaving a sum over $O(D^{2\log_2 N}) = O(N^{2\log_2 D})$ terms involving the conjugation of H by local unitary operations. Thus we can decouple P from S, leaving only the interaction on system P, using a procedure of complexity $O(N^{2\log_2 D})$. This interaction on system P can then be used to simulate an arbitary two-qudit interaction on P, using the techniques described in the preceding section.

B. The case of localized two-qudit interactions

The method just described assumes a general two-qudit Hamiltonian H. Of course, the Hamiltonians occurring in Nature are usually much more constrained. In particular, it is very common for Hamiltonians to have some sort of localized structure. In this section we explain how localized structure can be exploited to obtain more efficient decoupling schemes than described above for the general case. Note that similar constructions in the context of NMR were reported in Refs. [7,8].

Suppose, for example, that H contains only nearest-neighbor interactions on a one-dimensional lattice. This is obviously a special case, but is a good illustration of the ideas used for more general cases. We number the qudits $1,2,\ldots,N$, and suppose that P contains qudits 1 and 2, while S contains qudits 3 through N. The case of general P and S follows using similar techniques. We can split the decoupling up into three steps. In the first step we eliminate all couplings between P and S, which can be achieved by eliminating all couplings between qudits 2 and 3. We call the resulting Hamiltonian H'. The second step is to eliminate all single-body terms in S. This can be done by simulating the Hamiltonian

$$H'' = \frac{1}{D^2} \sum_U U_S H' U_S^\dagger. \tag{60}$$

We complete the decoupling by simulating

$$H''' = \frac{1}{D^2} \sum_U \; (I \otimes I \otimes U \otimes I \otimes U \otimes I \otimes \cdots) \times H'' (I \otimes I \otimes U \otimes I \otimes U \otimes I \otimes \cdots)^\dagger, \qquad (61)$$

where the conjugation by U is applied to qubits 3,5,7, . . . , which we can easily see turns off all couplings acting between qudits in S.

Thus, we see that for a nearest-neighbor Hamiltonian on a one-dimensional lattice, the decoupling can be performed for *constant* (with respect to N) cost in the simulation, as opposed to the $O(N^{2\log_2 D})$ cost incurred in the case when general interaction terms appear in the Hamiltonian.

This result can easily be generalized. Suppose S can be broken up into a partition $S_1, \ldots, S_m$ with the property that qudits in one member of the partition S_j only couple to qudits outside S_j. To decouple we do the following. For each element of the partition S_j turn off all couplings between S_j and the remainder of the system by simulating the Hamiltonian

$$H_j = \sum_U \; U_{S_j} H_{j-1} U_{S_j}^\dagger, \qquad (62)$$

where $H_0 \equiv H$. It is easy to see that the Hamiltonian H_m contains no single-body terms from S, no couplings between P and S, and all couplings internal to S have been eliminated. The total cost of the simulation scales as $(D^2)^m = D^{2m}$. This cost can be reduced even further by using a recursive procedure like that described for the general two-qudit case, resulting in a scaling of $O(D^{2\log_2 m})$.

Many cases of interest can be described in the framework just introduced. For example, consider an r-dimensional cubic lattice of qudits, with nearest-neighbor interactions. There is a natural partitioning of this lattice into 2^r different sublattices, as follows. First, fix a site in the lattice, and then consider the cubic sublattice S_1 generated by stepping two lattice spacings in every direction. We generate the partition of sublattices $S_1, S_2, \ldots, S_{2^r}$ by translating S_1 one lattice spacing in various directions. (We are ignoring boundary conditions in this discussion; they are easily accommodated, or one can imagine that the lattice has periodic boundary conditions.) Now remove the qudits in P from whichever elements S_p and S_q of the partition they happened to fall into. Notice that qudits in S_j only ever couple *out* of S_j, since the interactions are nearest-neighbor. Thus the procedure described above makes it is possible to decouple P from S using $O(D^{2r})$ operations. More generally, it is not difficult to use such constructions to efficiently decouple P and S for any Hamiltonian containing only localized interactions.

V. DISCUSSION

We have shown that, given any two-qudit entangling Hamiltonian H and local unitaries we can simulate any other two-qudit Hamiltonian. This result was then applied to obtain universal gate constructions for quantum computation. Our results are of interest because they show that such universal simulation is possible, in principle. However, the complexity of our construction limits the practicality of potential implementations, and should encourage the search for more practical methods.

There are two aspects to the analysis of efficiency for our simulations. The first is how they scale with the dimension D of the qudits in the system, and the second is how they scale with the number N of qudits present in the system. The scaling with N is the critical factor, while the scaling with D is not so important, since for most physical systems of interest D is a constant. We have shown that the scaling for simulation of one two-qudit Hamiltonian with another is polynomial in D, and the scaling with N behaves as $O(N^{2\log_2 D})$. Thus the total scaling is $O(\mathrm{poly}(D) N^{2\log_2 D})$, which is polynomial in both N and D.

Our results show that all two-body N-qudit entangling Hamiltonians are qualitatively equivalent, given the ability to perform local unitary operations. Thus, in some sense the ability to entangle can be regarded as a fundamental physical resource—a type of ''dynamic entanglement'' [39]—that can be utilized to perform interesting processes. It would be extremely interesting to develop a detailed quantitative theory of such dynamic entanglement. Following the line of research we have pursued in this paper, some potential questions one might attempt to answer in developing such a theory of dynamic entanglement include

(*a*) What is the optimal procedure for simulating one Hamiltonian with another? See Refs. [15–17] for preliminary results in this direction.

(*b*) Can an entangling Hamiltonian defined on a $D \times D'$ system, where $D \neq D'$, be used to perform universal simulation on those systems? Note that this question has recently been settled in the affirmative [33,34], using methods rather different than that in our paper.

(*c*) Our model assumes that the constituent systems are of finite dimensionality D. It would be interesting to determine whether analogous results hold in infinite dimensions.

(*d*) Are universal simulation results possible for nonunitary processes? For measurement processes? Preliminary results in this direction have been obtained in Refs. [35,36].

(*e*) Can we weaken the condition that arbitrary local unitary operations be allowed during the simulation procedure? It would be interesting, for example, if universal simulation could be performed in a system where local unitaries are applied homogeneously across the entire system.

(*f*) Our model assumes that only a single Hamiltonian is being applied at any given time, namely, either the entangling Hamiltonian H, or a local Hamiltonian on a single qudit. In practice, this is not likely to be exactly the case. What effect do imperfections have?

(*g*) In the theory of entangled state transformation there is a crucial distinction between ''single-shot'' manipulation of entangled states, where just a single copy of the state is available, and manipulations that are performed in the asymptotic limit where a large number of copies of the state are available. The results obtained in the present paper are for single-shot Hamiltonian simulation; it would be interesting to obtain results for the asymptotic case as well.

Note added. Recently we became aware that Wocjan,

Roetteler, Janzing, and Beth have independently obtained some similar results in Ref. [34].

ACKNOWLEDGMENTS

We thank Carl Caves for providing a copy of Horn and Johnson at just the right time. Special thanks to Daniel Gottesman for interesting discussions about the Pauli group, to Ben Schumacher for many encouraging and motivating discussions, and to Markus Grassl for pointing out a significant error in an earlier version of this manuscript. Thanks also to Ivan Deutsch, Tobias Osborne, Damian Pope, and Rob Thew for helpful discussions. A.M.C. thanks the Centre for Quantum Computer Technology at the University of Queensland for its hospitality, and acknowledges the support of the Fannie and John Hertz Foundation. This work was supported in part by the Department of Energy under Cooperative Research Agreement No. DF-FC02-94ER40818.

APPENDIX A: NORMALIZER OPERATIONS FOR THE *D*-DIMENSIONAL PAULI GROUP

In this Appendix we construct the unitary operations U used to perform the conjugation operations Eqs. (4)–(6), which we reproduce here for convenience,

$$X \rightarrow Z, \quad Z \rightarrow X^{-1}, \tag{A1}$$

$$X \rightarrow XZ, \quad Z \rightarrow Z, \tag{A2}$$

$$X \rightarrow X^a, \quad Z \rightarrow Z^{a^{-1}}, \quad \text{provided } \gcd(a,D)=1. \tag{A3}$$

Our constructions are based on those of Gottesman [23], however, Gottesman's interest was mainly in the case of prime D greater than 2, and his constructions only apply for odd values of D. The following constructions apply for D both odd and even.

The conjugation operation for Eq. (A1) is just the D-dimensional discrete Fourier transform, defined by

$$U|j\rangle \equiv \sum_{k=0}^{D-1} \omega^{jk}|k\rangle. \tag{A4}$$

A straightforward calculation shows that $UXU^\dagger = Z$ and $UZU^\dagger = Z^{-1}$, so Eq. (A1) holds.

The definition of the conjugation operation for Eq. (A2) depends on whether D is odd or even. When D is odd we define

$$U|j\rangle \equiv \omega^{j(j-1)/2}|j\rangle. \tag{A5}$$

A straightforward calculation shows that $UXU^\dagger = XZ$ and $UZU^\dagger = Z$, so Eq. (A2) holds for odd D. When D is even we define

$$U|j\rangle \equiv \omega^{j^2/2}|j\rangle, \tag{A6}$$

and then check that $UXU^\dagger = \omega^{1/2}XZ$ and $UZU^\dagger = Z$, so that Eq. (A2) also holds for even D.

Finally, the conjugation operation for Eq. (A3) is defined by

$$U|j\rangle \equiv |aj\rangle, \tag{A7}$$

from which it follows that $UXU^\dagger = X^a$ and $UZU^\dagger = Z^{a^{-1}}$, which completes the constructions needed to verify Eqs. (A1)–(A3).

APPENDIX B: SECOND PROOF OF THE NUMBER THEORY LEMMA

In this Appendix we provide an alternate proof of the number theory lemma used in Sec. III A of the paper. Recall the statement of the lemma:

Lemma. Suppose $\gcd(l,m)=1$. Then $jm =_D kl$ if and only if there exists n such that

$$j =_D nl; \quad k =_D nm. \tag{B1}$$

Proof. By the PEG lemma there exists a normalizer operation U such that $UX^lZ^mU^\dagger = Z^{\gcd(l,m)} = Z$, where the equalities hold up to phase factors. Note that X^lZ^m commutes with X^jZ^k, since $jm =_D kl$, so $UX^jZ^kU^\dagger$ must commute with $Z = UX^lZ^mU^\dagger$. It follows that $UX^jZ^kU^\dagger = Z^n$, up to a phase factor, for some n, and thus

$$X^jZ^k = U^\dagger Z^n U \tag{B2}$$

$$= (U^\dagger Z U)^n \tag{B3}$$

$$= (X^lZ^m)^n \tag{B4}$$

$$= X^{ln}Z^{mn}, \tag{B5}$$

where, again, the equalities hold up to unimportant phase factors. It follows that $j =_D ln$ and $k =_D mn$, as claimed. ■

[1] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[3] J. Preskill, *Physics 229: Advanced Mathematical Methods of Physics—Quantum Computation and Information* (California Institute of Technology, Pasadena, California, 1998), http://www.theory.caltech.edu/people/preskill/ph229/

[4] J.L. Dodd, M.A. Nielsen, M.J. Bremner, and R.T. Thew, Phys. Rev. A **65**, 040301(R) (2002).

[5] C. P. Slichter, *Principles of Magnetic Resonance* (Springer, Berlin, 1996).

[6] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Oxford University Press, Oxford, 1994).

[7] J.A. Jones and E. Knill, J. Magn. Reson. **141**, 322 (1999).

[8] D.W. Leung, I.L. Chuang, F. Yamaguchi, and Y. Yamamoto, Phys. Rev. A **61**, 042310 (2000).
[9] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[10] J.L. Brylinski and R. Brylinski, e-print arXiv: quant-ph/0108062.
[11] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).
[12] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[13] N. Weaver, J. Math. Phys. **41**, 240 (2000).
[14] W. Dür, G. Vidal, J.I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).
[15] P. Wocjan, D. Janzing, and T. Beth, Quantum Inform. Comput. **2**, 117 (2002).
[16] C.H. Bennett, J.I. Cirac, M.S. Leifer, D.W. Leung, N. Linden, S. Popescu, and G. Vidal, e-print arXiv:quant-ph/0107035v1.
[17] G. Vidal and J.I. Cirac, e-print arXiv:quant-ph/0108076.
[18] D. W. Leung and G. Vidal, (Ref. [33]) Appendix C.
[19] H. Rabitz, R. de Vive-Riedle, M. Motzkus, and K. Kompa, Science **288**, 824 (2000).
[20] S.G. Schirmer, A.I. Solomon, and J.V. Leahy, e-print arXiv:quant-ph/0108114v1.
[21] D. Janzing, P. Wocjan, and T. Beth, e-print arXiv:quant-ph/0106085.
[22] D.W. Leung, e-print arXiv:quant-ph/0107041.
[23] D. Gottesman, in *Quantum Computing and Quantum Communications: First NASA International Conference*, edited by C. P. Williams (Springer-Verlag, Berlin, 1999).
[24] Euclid, *Elements* (Cambridge University Press, Cambridge, England, 1908).
[25] J. -P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics Vol. 42 (Springer-Verlag, New York, 1977).
[26] M.A. Nielsen, Phys. Rev. A **63**, 022114 (2001).
[27] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).
[28] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and its Applications* (Academic Press, New York, 1979).
[29] P. M. Alberti and A. Uhlmann, *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing* (Dordrecht, Boston, 1982).
[30] A. Uhlmann, Wiss. Z.-Karl-Marx-Univ. Leipzig, Math.-Naturwiss. Reihe **20**, 633 (1971).
[31] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).
[32] M.A. Nielsen and G. Vidal, Quantum Inform. Comput. **1**, 76 (2001).
[33] C.H. Bennett, J.I. Cirac, M.S. Leifer, D.W. Leung, S. Popescu, and G. Vidal, e-print arXiv:quant-ph/0107035v2, updated version of Ref. [16].
[34] P. Wocjan, M. Roetteler, D. Janzing, and T. Beth, Quantum Inform. Comput. **2**, 133 (2002).
[35] S. Lloyd and L. Viola, Phys. Rev. A **65**, 010101 (2002).
[36] D. Bacon, A.M. Childs, I.L. Chuang, J. Kempe, D.W. Leung, and X. Zhou, Phys. Rev. A **63**, 012306 (2001).
[37] This term was coined in a 1998 conversation between one of us (M.A.N.) and Raymond Laflamme.
[38] Our thanks go to Ben Schumacher, who contributed to the discovery of this theorem.
[39] See Ref. [37].