

Solovay-Kitaev Decomposition Strategy for Single-Qubit Channels

Dong-Sheng Wang,¹ Dominic W. Berry,² Marcos C. de Oliveira,^{1,3} and Barry C. Sanders¹

¹*Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*

²*Department of Physics and Astronomy, Macquarie University, Sydney, New South Wales 2109, Australia*

³*Instituto de Física Gleb Wataghin, Universidade Estadual de Campinas, 13083-859 Campinas, São Paulo, Brazil*

(Received 17 May 2013; published 25 September 2013)

Inspired by the Solovay-Kitaev decomposition for approximating unitary operations as a sequence of operations selected from a universal quantum computing gate set, we introduce a method for approximating any single-qubit channel using single-qubit gates and the controlled-NOT (CNOT). Our approach uses the decomposition of the single-qubit channel into a convex combination of “quasiextreme” channels. Previous techniques for simulating general single-qubit channels would require as many as 20 CNOT gates, whereas ours only needs one, bringing it within the range of current experiments.

DOI: [10.1103/PhysRevLett.111.130504](https://doi.org/10.1103/PhysRevLett.111.130504)

PACS numbers: 03.67.Ac, 03.65.Yz, 89.70.Eg

Quantum computing requires the capability to efficiently approximate arbitrary quantum operations as a sequence of a finite set of operations. The celebrated Solovay-Kitaev theorem [1,2] addresses this problem by providing a strategy for approximating any unitary operation U within error tolerance ϵ as a sequence of $O(\text{polylog}(1/\epsilon))$ gates chosen from the finite set. Dawson and Nielsen [3] introduced an algorithm for the Solovay-Kitaev decomposition, and many improvements have appeared recently [4–10]. These algorithms are central to quantum simulation efforts, which is especially important because quantum simulation is regarded as the most promising direction for a nontrivial quantum computation [11].

Closed-system (i.e., Hamiltonian-generated) quantum simulation is well established [12–16], but open-system quantum simulation is still at an early stage with attention focused on simulating memoryless (Markovian) dynamics based on a Lindblad master equation [17–22]. Open-system quantum simulation is important to cool to the ground state [23], prepare thermal states [24,25] and entangled states [26,27], and study nonequilibrium quantum phase transitions [28]. Conversely, dissipative dynamics can be a resource for universal quantum computing [29].

Given the importance of open-system quantum simulation, efficiently approximating channels rather than just approximating unitary evolution is critical. Here, we solve single-qubit channel simulation, developing methods that could ultimately be adapted for multiqubit channels. Our channel simulator could be regarded as a primitive for simulating open-system dynamics, in the same way as single-qubit unitary gates are a primitive for closed-system dynamics.

An obvious direction for implementing a channel is applying Stinespring dilation to implement a channel as a unitary operator on an expanded Hilbert space. This resultant unitary transformation can then be implemented by standard techniques [4–10]. The problem with this approach is that it requires implementing a general unitary

operator on a space with dimension given by the cube of the Hilbert space dimension for the original system. In the case of a single-qubit channel, a unitary operation on three qubits would be required. The best known technique to implement a general unitary on three qubits requires a complicated circuit with 20 controlled-NOT (CNOT) gates [30]. An alternative technique [18] uses one ancilla qubit but uses a sequence of a large number of interactions, which would require a large number of CNOTs.

It is possible to achieve channels far more easily in special cases, or probabilistically, and to date, experimental realizations have had these limitations [31–35]. In particular, a *unital* qubit channel, such as the phase damping channel, can be achieved relatively easily by applying a random unitary operation. Alternatively, if one is willing to accept a significant probability of failure, then it is straightforward to provide a method to generate arbitrary channels [36]. In contrast, our technique for qubit channels is general, deterministic, and only requires one CNOT and ancilla together with local operations. As it is already possible to demonstrate a single CNOT in several physical systems [37], our technique is implementable with current technology.

We quantify the error tolerance ϵ by the Schatten one-norm distance between the simulated channel and the correct channel [21,38]. The classical and quantum algorithms we derive for single-qubit channel simulation are efficient in that their time and space costs are no worse than $\text{polylog}(1/\epsilon)$. Our algorithms and complexity results for channel simulation rely on decomposing the channel into a convex combination of simpler channels, dilating each of these channels to unitary mappings on two qubits [18], and making use of the Solovay-Kitaev Dawson-Nielsen (SKDN) algorithm [3].

A succinct statement of the problem we solve follows.

Problem.—Construct an efficient autonomous algorithm for designing an efficient quantum circuit, implemented from a small single-qubit universal gate set, that accurately simulates any completely positive trace-preserving

single-qubit mapping for any input state within prespecified error tolerance ϵ quantifying the distance between true and approximated states.

Our solution has the following components: (i) the decomposition of arbitrary single-qubit channels as a convex combination of quasiextreme single-qubit channels [39], (ii) a cost reduction of single-qubit channel simulation from requiring a unitary operation on three qubits to a circuit with one ancillary qubit and one CNOT, (iii) a geometric lookup database for implementing the SKDN algorithm [3] to decompose unitary operators, and (iv) a proof of efficient simulation by showing that the costs for both the classical algorithm for designing the circuit and the quantum circuit itself are at most $\text{polylog}(1/\epsilon)$.

Now, we proceed to the technical aspects. The system is a single qubit whose state is a positive semidefinite operator $\rho \in \mathcal{T}(\mathcal{H}^S)$ with \mathcal{H}^S the two-dimensional Hilbert space for the system and $\mathcal{T}(\mathcal{H})$ denoting the set of operators on Hilbert space \mathcal{H} . The channel is

$$\mathcal{E}: \mathcal{T}(\mathcal{H}^S) \rightarrow \mathcal{T}(\mathcal{H}^S): \rho \mapsto \sum_i K_i \rho K_i^\dagger, \quad (1)$$

with the summation at the end showing the operator-sum representation [40,41]. The operators $\{K_i\}$ are called Kraus operators and satisfy $\sum_i K_i^\dagger K_i = \mathbb{1}$.

The channel can be dilated to a unitary operator on the joint Hilbert space $\mathcal{H}^{SE} = \mathcal{H}^S \otimes \mathcal{H}^E$, with E denoting the environment (or ancillary space) being introduced to purify the dynamics. Conversion of channel \mathcal{E} to a Hamiltonian-generated unitary evolution can be achieved by performing a Stinespring dilation with unitary operator $U: \mathcal{H}^{SE} \rightarrow \mathcal{H}^{SE}$, and

$$U: \mathcal{T}(\mathcal{H}^{SE}) \rightarrow \mathcal{T}(\mathcal{H}^{SE}): \rho^{SE} \mapsto \rho'^{SE} = U \rho^{SE} U^\dagger, \quad (2)$$

such that $\text{tr}_E \rho'^{SE} = \rho^S$, $\text{tr}_E \rho'^{SE} = \rho'^S$, and $\mathcal{E}: \rho^S \mapsto \rho'^S$. Specifically, the Kraus operators (1) have representation $K_i = {}^E \langle i|U|0\rangle^E$ for $|i\rangle^E$ (including $|0\rangle^E$) an orthonormal basis state of the environment [41].

The unitary operator U is a minimal dilation of \mathcal{E} if U is a dilation such that $\dim \mathcal{H}^E = (\dim \mathcal{H}^S)^2$. For the case of a single qubit, $\dim \mathcal{H}^E = 4$ for minimal dilation. Although \mathcal{H}^E should have a dimension that is the square of the dimension of \mathcal{H}^S , and hence four dimensional, we will show that we only require a single resettable ancillary qubit, so $\dim \mathcal{H}^E = 2$.

We develop the algorithm for a general single-qubit completely positive trace-preserving (CPTP) map using the geometrical state representation $\rho = (1/2)[\mathbb{1} + \mathbf{b} \cdot \boldsymbol{\sigma}]$, where \mathbf{b} is a three-dimensional vector and $\boldsymbol{\sigma} := (X, Y, Z)$. The CPTP map can then be represented by a 4×4 matrix [39,42]

$$\mathcal{E} \mapsto \mathbb{T} = \begin{pmatrix} 1 & 0 \\ \mathbf{t} & \mathbf{T} \end{pmatrix}, \quad \mathbb{T}_{ij} = \frac{1}{2} \text{tr}[\sigma_i \mathcal{E}(\sigma_j)], \quad \sigma_0 := \mathbb{1}, \quad (3)$$

with \mathbb{T} having 12 independent parameters. In this representation, the channel is an affine map [43]

$$\mathcal{E}: \rho \mapsto \frac{1}{2}(\mathbb{1} + \mathbf{b}' \cdot \boldsymbol{\sigma}), \quad \mathbf{b}' = \mathbf{T}\mathbf{b} + \mathbf{t}. \quad (4)$$

Geometrically, \mathcal{E} maps the state ball into an ellipsoid, with \mathbf{t} the shift from the ball's origin and \mathbf{T} a distortion matrix for the ball.

In our approach, the channel is constructed from two simpler channels, each of which can be simulated using only one ancillary qubit. Any single-qubit channel can be decomposed into a convex combination of two channels belonging to the closure of the set of extreme points of the set of single-qubit channels [39]. It turns out that these quasiextreme channels, denoted as \mathcal{E}^{qe} , can be simulated using only one ancillary qubit. In addition, the convex combination is easy to implement, simply by probabilistically implementing one or the other of the quantum channels.

For any CPTP map, the distortion matrix can be transferred into a diagonal form via a singular-value decomposition, so $\mathcal{E} = U(\boldsymbol{\varphi})\mathcal{E}'U(\boldsymbol{\delta})$ for some \mathcal{E}' with a diagonal \mathbf{T}' [43]. In the case of the quasiextreme channel, the shift vector and distortion matrix are of the form [39]

$$\mathbf{t}'_{\text{qe}} = (0, 0, \sin\mu \sin\nu)^T, \quad (5)$$

$$\mathbf{T}'_{\text{qe}} = \text{diag}(\cos\nu, \cos\mu, \cos\mu \cos\nu) \quad (6)$$

for some μ and ν . This map can be obtained via two Kraus operators

$$K_0 = \begin{pmatrix} \cos\beta & 0 \\ 0 & \cos\alpha \end{pmatrix}, \quad K_1 = \begin{pmatrix} 0 & \sin\alpha \\ \sin\beta & 0 \end{pmatrix}, \quad (7)$$

where $\alpha = (\mu + \nu)/2$ and $\beta = (\mu - \nu)/2$. The channel \mathcal{E}^{qe} is a generalization of the amplitude damping channel.

The circuit to implement the channel \mathcal{E}^{qe} is depicted in Fig. 1. The rotation takes the form $R_y(2\gamma) = \exp(-iY\gamma) = 1 \cos\gamma - iY \sin\gamma$; the two angles in the rotations are $2\gamma_1 = \beta - \alpha + \pi/2$ and $2\gamma_2 = \beta + \alpha - \pi/2$. The measurement in the computational basis with the outcome $|0\rangle$ ($|1\rangle$) corresponds to the realization of the Kraus operator K_0 (K_1). There is only one CNOT required because the final operation is just a classically controlled X operation.

To explain the action of this circuit, note first that the unitary operations $U(\boldsymbol{\delta})$ and $U(\boldsymbol{\varphi})$ are just the unitaries to diagonalize the distortion matrix. If the system qubit were in the state $|0\rangle$, then the CNOT would have no action on the ancilla, and the two rotations combine to give $R_y(2\beta)$, which yields the state $\cos\beta|0\rangle + \sin\beta|1\rangle$. If the system is

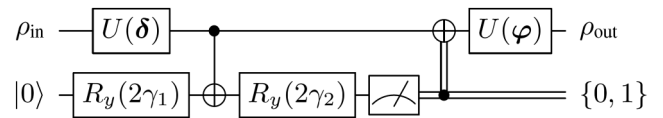


FIG. 1. The circuit to implement the quasiextreme channel \mathcal{E}^{qe} . The unitary operators $U(\boldsymbol{\delta})$ and $U(\boldsymbol{\varphi})$ serve to diagonalize the channel.

in the state $|1\rangle$, then an X operation flips the ancilla, and then the two rotations give $\cos\alpha|0\rangle + \sin\alpha|1\rangle$. Measuring the ancilla in the state $|0\rangle$ then multiplies state $|0\rangle$ for the system by $\cos\beta$ and state $|1\rangle$ by $\cos\alpha$; this is the action of K_0 . Similarly, measuring the ancilla in the state $|1\rangle$ multiplies state $|0\rangle$ for the system by $\sin\beta$, and state $|1\rangle$ by $\sin\alpha$; this is the action of the operator

$$K'_1 = \begin{pmatrix} \sin\beta & 0 \\ 0 & \sin\alpha \end{pmatrix}. \quad (8)$$

In that case, we can simply apply X , which gives the required Kraus operator K_1 .

In contrast, the direct approach to simulate a single-qubit channel is to use Stinespring dilation to construct a unitary acting on the system qubit and two ancillary qubits. This approach is somewhat inefficient, as a large number of gates is needed to implement a three-qubit unitary. The best known technique to achieve a three-qubit unitary uses 20 CNOTs [30], although the proven lower bound is 14 [44]. In contrast, our technique succeeds with only one such gate. Our result is now summarized in Proposition 1.

Proposition 1.—Any single-qubit CPTP channel \mathcal{E} can be simulated with one ancillary qubit, one CNOT, and four single-qubit operations.

Proof: From Theorem 14 in Ref. [39], any single-qubit channel \mathcal{E} can be decomposed into the convex combination $\mathcal{E} = p\mathcal{E}_1^{\text{qe}} + (1-p)\mathcal{E}_2^{\text{qe}}$, with $0 \leq p \leq 1$. Note that channels $\mathcal{E}_1^{\text{qe}}$ and $\mathcal{E}_2^{\text{qe}}$ can be diagonalized, but the unitary operators to do so may be different in the two cases. The quasiextreme channels $\mathcal{E}_i^{\text{qe}}$ can be realized by using the appropriate initial unitary operator, then applying the circuit above with corresponding angles α_i and β_i , and then applying the final unitary operator. Then, the channel \mathcal{E} can be simulated by randomly implementing the two quasiextreme channels according to a classical random number generator with probabilities p and $1-p$. The above circuit uses one CNOT, two rotations, a classically controlled X gate, and two additional unitary operators to diagonalize $\mathcal{E}_i^{\text{qe}}$. The final diagonalizing unitary $U(\varphi)$ may be combined with the X gate, so only four single-qubit unitary operators are needed. ■

In order to complete the decomposition of the channel into a universal gate set, it is necessary to decompose the single-qubit unitary operators in Proposition 1 into the gate set. In the case that the gate set includes Clifford and T ($T = Z^{1/4}$) operations, then any of the techniques given in Refs. [3–8] can be used. Here, we are concerned with the more general problem of what can be achieved with CNOTs and a universal single-qubit gate set S . This problem is relevant to experimental situations where not all single-qubit gates can be applied. The motivation for considering Clifford and T operations in other work is that they are important for encoded logical qubits with error correction, but such an experiment would be beyond current technology.

We therefore consider a variation of the SKDN approach [3] with the CNOT and gates from S . Figure 2(a) depicts the SKDN strategy by which any single-qubit unitary operator $U(\boldsymbol{\theta}) = e^{i\theta_0} \exp(-i\boldsymbol{\theta} \cdot \boldsymbol{\sigma})$ can be approximately (within ϵ) decomposed into a unitary operator $\tilde{U} = \cdots U_2 U_1 U_0$ comprising a $\text{polylog}(1/\epsilon)$ sequence of gates from S [1,2].

The SKDN algorithm provides an explicit construction that requires at most $O(\log^{2.71}(1/\epsilon))$ time and $O(\log^{3.97}(1/\epsilon))$ gates [3] but requires a database of single-qubit gates $\{G_n\}$ depicted schematically in Fig. 2(b). This database gives each G_n as a sequence of gates from S . However, Dawson and Nielsen do not discuss how to search this database [3]; we explicitly provide an efficient geometric search technique, depicted in Fig. 2(c) and described below.

Ignoring the global phase, each U can be identified with coordinate $\boldsymbol{\theta} \in \mathbb{R}^3$. As $U(\boldsymbol{\theta}) = U[\boldsymbol{\theta}(1 - \pi/|\boldsymbol{\theta}|)]$, the space \mathbb{R}^3 can be reduced to a radius $\pi/2$ ball, as depicted in Fig. 2(c). We therefore embed a cubic lattice into \mathbb{R}^3 to use as a lookup table. That is, we construct a database such that, for each cube, there is a sequence of gates that produces a unitary operation within that cube. Then, if we require a sequence of operators to approximate a given unitary operator, we identify which cube in the lattice this unitary operator occupies and then select the corresponding sequence of operators from the database. Each cube has side length $1/32\sqrt{3}$, thereby ensuring a maximum separation of $1/32$ between the unitary and the approximating sequence, which is sufficient for the SKDN algorithm. For the example of T and H (Hadamard) gates, we find that no more than 36 are required. (An alternative database lookup procedure is given in Ref. [6].)

Using this database construction with the SKDN algorithm and Proposition 1, we have an explicit algorithm to decompose a single-qubit channel into CNOTs and gates

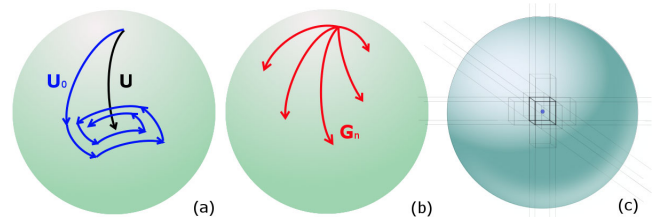


FIG. 2 (color online). Schematic diagram for the SKDN algorithm. (a) Representation of the algorithm on the Bloch ball. The SKDN algorithm finds a polynomial-length gate sequence to approximate an arbitrary single-qubit unitary operator U by starting with an initial approximation U_0 with initial error bound $\epsilon_0 < 1/32$ followed by iteratively constructing operators to produce decreasing errors. (b) Action of gates G_n in the lookup database represented as rotations of the sphere. (c) The radius $\pi/2$ ball of single-qubit unitary operations (note that this is different than the Bloch ball). Each lookup database gate element G_n is located within one cube of a period $1/32\sqrt{3}$ cubic lattice. At the boundary, a cube's center can lie outside the ball but still must be a legitimate domain for the search algorithm.

from S . This classical design algorithm accepts as input the error tolerance ϵ for the single-qubit channel and the channel parameters \mathcal{E} . As output, the algorithm delivers the description of the quantum algorithm implemented as a sequence of gates from the instruction set.

The procedure to be followed will depend on what single-qubit gates are available experimentally and the desired accuracy. For experiments in the near future, the best approach is likely to be to simply use a lookup database directly, as it will be challenging to produce single-qubit sequences longer than 36. Alternatively, if the full set of single-qubit unitaries is available, then one may use the circuit in Fig. 1 directly. The procedure outlined above should be used if there is a restricted single-qubit gate set and high precision is required. In the special case that the single-qubit gate set is $\{H, T\}$, then one can use new techniques, such as those in Ref. [10].

For completeness, we need to bound the error in the channel in terms of the error in the unitary. For the unitary, the error is simply the worst-case two-norm distance between the true and approximate pure states in the system Hilbert space

$$\|U - \tilde{U}\| := \max_{|\psi\rangle} \|(U - \tilde{U})|\psi\rangle\|. \quad (9)$$

The appropriate measure of error for the channel is the Schatten one-norm [21,38]

$$\|\mathcal{E} - \tilde{\mathcal{E}}\|_{1 \rightarrow 1} := \max_{\rho} \|\mathcal{E}(\rho) - \tilde{\mathcal{E}}(\rho)\|_1, \quad \|\bullet\|_1 := \text{tr}\sqrt{\bullet^\dagger \bullet}. \quad (10)$$

The following proposition establishes that the channel-simulation error condition is satisfied if the error bound for the dilated unitary operator U is $\epsilon/2$.

Proposition 2.—For CPTP maps $\mathcal{E}, \tilde{\mathcal{E}}: \mathcal{T}(\mathcal{H}) \rightarrow \mathcal{T}(\mathcal{H})$ with respective minimal dilations $U, \tilde{U}: \mathcal{H} \otimes \mathcal{H}' \rightarrow \mathcal{H} \otimes \mathcal{H}'$, then $\|\mathcal{E} - \tilde{\mathcal{E}}\|_{1 \rightarrow 1} \leq 2\|U - \tilde{U}\|$.

Proof: Using Eq. (17) of Ref. [45] and the convexity of trace distance,

$$\begin{aligned} 2\max_{|\psi\rangle} \|(U - \tilde{U})|\psi\rangle\| &\geq \max_{|\psi\rangle} \|U|\psi\rangle\langle\psi|U^\dagger - \tilde{U}|\psi\rangle\langle\psi|\tilde{U}^\dagger\|_1 \\ &\geq \max_{\rho} \|\mathcal{E}(\rho) - \tilde{\mathcal{E}}(\rho)\|_1. \end{aligned} \quad (11)$$

Using the definitions, this immediately gives the required inequality. ■

We now articulate our complete result for the decomposition of the channel into the universal gate set.

Proposition 3.—Any single-qubit channel \mathcal{E} can be approximated within one-norm distance ϵ using $O(\log^{3.97}(1/\epsilon))$ computer time and gates from the set S , and using one CNOT, one ancillary qubit and one classical bit.

Proof: First, via Proposition 1, the channel can be decomposed into a convex combination of channels and thereby simulated using one ancilla qubit, one CNOT

operation, and four single-qubit unitary operators. Provided each of the channels in the convex combination is simulated within distance ϵ , the overall channel is simulated within distance ϵ by the convexity of the one-norm distance.

Via Proposition 2, the error bound for the channel is satisfied if the two-qubit unitary operators are approximated within distance $\epsilon/2$. There are four single-qubit unitary operators used within the circuit. The error bound will be satisfied, provided each of these unitary operators is approximated within distance $\epsilon/8$. These unitary operators can be approximated via the SKDN algorithm with $O(\log^{3.97}(1/\epsilon))$ gates from S . Using our lookup database, the SKDN algorithm may be implemented efficiently, in that the classical complexity to determine the gate sequence does not exceed $O(\log^{2.71}(1/\epsilon))$. ■

We now have the full algorithm for open-system single-qubit channel quantum simulation. For a given input channel, the channel will be decomposed into the form in Proposition 1, and then the single-qubit rotations which contain continuous variables therein will further be decomposed into sequences of universal gates satisfying the error condition. This simulator accepts the initial state ρ and yields the approximate output state $\tilde{\mathcal{E}}(\rho)$ while satisfying the error condition of Proposition 2.

This scheme could be implemented in a number of quantum computing architectures. For example, it could be implemented with linear optics, although in that case, the CNOT is nondeterministic, and other methods are available to perform nondeterministic channels [35,36]. A promising architecture to deterministically demonstrate this scheme is trapped ions. CNOT gates have been demonstrated with error below 0.01 [46], and single-qubit gates have been demonstrated with error below 10^{-4} [47]. In the case of trapped ions, it is possible to perform general single-qubit gates, so it is not necessary to use gate sequences. Nevertheless, the ability to perform large numbers of sequential single-qubit operations (nearly 1000 in Ref. [47]) means that gate sequences could easily be demonstrated.

In summary, we have shown how to implement a single-qubit channel using the CNOT and a universal set of single-qubit gates S . This can be regarded as a quantum simulation, except it differs from other quantum simulation methods in that we directly simulate the mapping rather than continuous-time evolution. Our quantum circuit is appealing for experimental implementation because only two qubits are necessary, rather than three as the Stinespring dilation theorem suggests. As a result, only one CNOT operation is needed, as compared to 20 for a straightforward application of Stinespring dilation. When decomposing the single-qubit unitary operators into gates from S , the number of gates and classical complexity follow from the Solovay-Kitaev Dawson-Nielsen algorithm. This work raises a number of questions for future

research. Most importantly, is it possible to achieve similar simplifications for *qudit* channels? Another question is whether it is possible to obtain further simplifications for the simulation of qubit channels.

We thank J. Eisert, C. Horsman, P. Høyer, and N. Wiebe for valuable discussions. D. S. W. acknowledges financial support from USARO. Subsequent to the appearance of our work on the arXiv, S. D. Bartlett sent us his related unpublished work, which showed that the quasiextreme channel in Fig. 1 required only one CNOT gate and not two [48], and we modified accordingly. We thank an anonymous referee for the simplified proof of Proposition 2. M. C. O. acknowledges support from AITF and the Brazilian agencies CNPq and FAPESP through the Instituto Nacional de Ciência e Tecnologia—Informação Quântica (INCT-IQ). D. W. B. is funded by an ARC Future Fellowship (FT100100761). B. C. S. acknowledges AITF, CIFAR, NSERC, and USARO for financial support. This project was supported in part by the National Science Foundation under Grant No. NSF PHY11-25915.

-
- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
- [2] A. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics Vol. 47 (American Mathematical Society, Providence, 2002).
- [3] C. M. Dawson and M. A. Nielsen, *Quantum Inf. Comput.* **6**, 81 (2006).
- [4] V. Kliuchnikov, D. Maslov, and M. Mosca, *Quantum Inf. Comput.* **13**, 0607 (2013).
- [5] V. Kliuchnikov, D. Maslov, and M. Mosca, *Phys. Rev. Lett.* **110**, 190502 (2013).
- [6] T. T. Pham, R. Van Meter, and C. Horsman, *Phys. Rev. A* **87**, 052332 (2013).
- [7] G. Duclos-Cianci and K. M. Svore, [arXiv:1210.1980v1](https://arxiv.org/abs/1210.1980v1).
- [8] P. Selinger, [arXiv:1212.6253v1](https://arxiv.org/abs/1212.6253v1).
- [9] B. Giles and P. Selinger, *Phys. Rev. A* **87**, 032332 (2013).
- [10] V. Kliuchnikov, [arXiv:1306.3200](https://arxiv.org/abs/1306.3200).
- [11] D. S. Abrams and S. Lloyd, *Phys. Rev. Lett.* **79**, 2586 (1997).
- [12] S. Lloyd, *Science* **273**, 1073 (1996).
- [13] D. Aharonov and A. Ta-Shma, in *Proceedings of the 35th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2003), Vol. 35.
- [14] D. W. Berry, G. Ahokas, R. Cleve, and B. C. Sanders, *Commun. Math. Phys.* **270**, 359 (2007).
- [15] A. M. Childs, *Commun. Math. Phys.* **294**, 581 (2010).
- [16] N. Wiebe, D. W. Berry, P. Høyer, and B. C. Sanders, *J. Phys. A* **44**, 445308 (2011).
- [17] D. Bacon, A. M. Childs, I. L. Chuang, J. Kempe, D. Leung, and X. Zhou, *Phys. Rev. A* **64**, 062302 (2001).
- [18] S. Lloyd and L. Viola, *Phys. Rev. A* **65**, 010101(R) (2001).
- [19] H. Weimer, M. Müller, I. Lesanovsky, P. Zoller, and H.-P. Bühler, *Nat. Phys.* **6**, 382 (2010).
- [20] H. Wang, S. Ashhab, and F. Nori, *Phys. Rev. A* **83**, 062317 (2011).
- [21] M. Kliesch, T. Barthel, C. Gogolin, M. Kastoryano, and J. Eisert, *Phys. Rev. Lett.* **107**, 120501 (2011).
- [22] T. Barthel and M. Kliesch, *Phys. Rev. Lett.* **108**, 230504 (2012).
- [23] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon, *Science* **309**, 1704 (2005).
- [24] B. M. Terhal and D. P. DiVincenzo, *Phys. Rev. A* **61**, 022301 (2000).
- [25] D. Poulin and P. Wocjan, *Phys. Rev. Lett.* **103**, 220502 (2009).
- [26] J. T. Barreiro, M. Müller, P. Schindler, D. Nigg, T. Monz, M. Chwalla, M. Hennrich, C. F. Roos, P. Zoller, and R. Blatt, *Nature (London)* **470**, 486 (2011).
- [27] M. Müller, S. Diehl, G. Pupillo, and P. Zoller, *Adv. At. Mol. Opt. Phys.* **61**, 1 (2012).
- [28] T. Prosen and E. Ilievski, *Phys. Rev. Lett.* **107**, 060403 (2011).
- [29] F. Verstraete, M. M. Wolf, and J. I. Cirac, *Nat. Phys.* **5**, 633 (2009).
- [30] M. Mottonen and J. J. Vartiainen, *Trends in Quantum Computing Research* (Nova, New York, 2006), Chap. 7.
- [31] M. P. Almeida, F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, P. H. S. Ribeiro, and L. Davidovich, *Science* **316**, 579 (2007).
- [32] L. Qing, L. Jian, and G. Guang-Can, *Chin. Phys. Lett.* **24**, 1809 (2007).
- [33] T. Hannemann, C. Wunderlich, M. Plesch, M. Ziman, and V. Buzek, [arXiv:0904.0923](https://arxiv.org/abs/0904.0923).
- [34] J.-C. Lee, Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, *Opt. Express* **19**, 16309 (2011).
- [35] K. A. G. Fisher, R. Prevedel, R. Kaltenbaek, and K. J. Resch, *New J. Phys.* **14**, 033016 (2012).
- [36] M. Piani, D. Pitkanen, R. Kaltenbaek, and N. Lütkenhaus, *Phys. Rev. A* **84**, 032304 (2011).
- [37] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, *Nature (London)* **464**, 45 (2010).
- [38] J. Watrous, *Quantum Inf. Comput.* **5**, 058 (2005).
- [39] M. B. Ruskai, S. Szarek, and E. Werner, *Linear Algebra Appl.* **347**, 159 (2002).
- [40] R. Bhatia, *Positive Definite Matrices* (Princeton University Press, Princeton, NJ, 2007).
- [41] K. Kraus, *States, Effects and Operations* (Springer-Verlag, Berlin, 1983).
- [42] M. M. Wolf and J. I. Cirac, *Commun. Math. Phys.* **279**, 147 (2008).
- [43] C. King and M. Ruskai, *IEEE Trans. Inf. Theory* **47**, 192 (2001).
- [44] V. V. Shende, I. L. Markov, and S. S. Bullock, *Phys. Rev. A* **69**, 062321 (2004).
- [45] P. Hayden, D. Leung, P. W. Shor, and A. Winter, *Commun. Math. Phys.* **250**, 371 (2004).
- [46] J. Benhelm, G. Kirchmair, C. F. Roos, and R. Blatt, *Nat. Phys.* **4**, 463 (2008).
- [47] K. R. Brown, A. C. Wilson, Y. Colombe, C. Ospelkaus, A. M. Meier, E. Knill, D. Leibfried, and D. J. Wineland, *Phys. Rev. A* **84**, 030303 (2011).
- [48] S. D. Bartlett, R. Blume-Kohout, and R. W. Spekkens (private communication).