Parsimonious and robust realizations of unitary maps in the one-way model

Vincent Danos
Université Paris 7 & CNRS, 175 Rue du Chevaleret, 75013 Paris, France

Elham Kashefi
Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Prakash Panangaden
School of Computer Science, McGill University, Montreal, Quebec, Canada H3A 2A7
(Received 3 January 2005; published 6 December 2005)

We present a new set of generators for unitary maps over $\mathbb{C}^2$ which differs from the traditional rotation-based generating set in that it uses a single-parameter family of unitaries $J(\alpha)$. These generators are implementable in the one-way model [Raussendorf and Briegel, Phys. Rev. Lett. **86**, 5188 (2001)] using only two qubits, and lead to both parsimonious and robust implementations of general unitaries. As an illustration, we give an implementation of the controlled-U family which uses only 14 qubits, and has a 2-colorable underlying entanglement graph (known to yield robust entangled states).

DOI: 10.1103/PhysRevA.72.064301 PACS number(s): 03.67.Lx, 03.65.Ta

I. INTRODUCTION

In this paper we introduce a simple parameterized family $J(\alpha)$ that generates all unitaries over $\mathbb{C}^2$. By adding the unitary operator controlled-Z ($\wedge Z$) defined over $\mathbb{C}^2 \otimes \mathbb{C}^2$, one then obtains a set of generators for all unitary maps over $\otimes^n \mathbb{C}^2$. Not only are these generators remarkably simple, but they also integrate neatly with measurement-based quantum computing models. Such models [1–9], and notably the *one-way* model [1–3], have been recently brought to the fore, because they allow for easier and scalable physical implementations [10–15].

Both $J(\alpha)$ and controlled-Z , have simple realizations in the one-way model, using only two qubits. As a consequence, one obtains an implementation of the controlled-U ($\wedge U$) family of unitaries, using only 14 qubits. Combining these as building blocks, any general unitary can be obtained by using relatively few auxiliary qubits.

Comparable realizations were already obtained by using a specific subclass of entangled states, known as cluster states, which need far more auxiliary qubits to implement the controlled-U family. Special instances of this were known before [3], for example, with the controlled phase gate, but, as far as we know, this is the best realization for the *general* controlled unitary gate. Furthermore, cluster states do have another interesting property, namely that their underlying entanglement graphs have no odd-length cycles, and such states have been shown to be robust against decoherence [16]. Fortunately, our building blocks also belong to this larger class, so that by using them nothing is lost in terms of robustness, while, as noted above, fewer qubits are needed.

II. A UNIVERSAL SET FOR UNITARIES

Let us prove first that the following one-parameter family $J(\alpha)$ generates all unitary operators on $\mathbb{C}^2$:

$$J(\alpha) := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

We can see already that the Pauli spin matrices, phase and Hadamard operators can be described using only $J(\alpha)$:

$$X = J(\pi)J(0), \quad P(\alpha) = J(0)J(\alpha),$$

$$Z = J(0)J(\pi), \quad H = J(0).$$

We will also use the following equations:

$$J(0)^2 = I,$$

$$J(\alpha)J(0)J(\beta) = J(\alpha + \beta),$$

$$J(\alpha)J(\pi)J(\beta) = e^{i\alpha} Z J(\beta - \alpha).$$

The second and third equations are referred to as the *additivity* and *subtractivity* relations. Additivity gives another useful pair of equations:

$$XJ(\alpha) = J(\alpha + \pi) = J(\alpha)Z. \tag{1}$$

Any unitary operator U on $\mathbb{C}^2$ can be written:

$$U = e^{i\alpha} J(0)J(\beta)J(\gamma)J(\delta)$$

for some α, β, γ and δ in $\mathbb{R}$. We will refer to this as a *J-decomposition* of U.

To prove this note that all three Pauli rotations are expressible in terms of $J(\alpha)$:

$$R_x(\alpha) = e^{-i(\alpha/2)} J(\alpha)J(0), \tag{2}$$

$$R_y(\alpha) = e^{-i(\alpha/2)} J(0)J\left(\frac{\pi}{2}\right)J(\alpha)J\left(-\frac{\pi}{2}\right), \tag{3}$$

$$R_z(\alpha) = e^{-i(\alpha/2)} J(0)J(\alpha). \tag{4}$$

From the Z-X decomposition, we know that every 1-qubit unitary operator U can be written as

$$U = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta)$$

and using Eqs. (4) and (2) we get

$$U = e^{i\alpha} e^{-i[(\beta+\gamma+\delta)/2]} J(0) J(\beta) J(\gamma) J(\delta).$$

We conclude in particular, that $J(\alpha)$ generates all 1-qubit unitary operators. It should be noted that an implicit form of the J-decomposition was considered in a recent paper [7] concerned with the unification of various measurement based models. However the authors do not define explicitly the operators $J(\alpha)$, nor do they infer their universality.

Next, we turn to the decomposition of controlled-U in terms of $J(\alpha)$ and controlled-Z. Subscripts to operators indicate the qubit to which they apply, and we sometimes abbreviate $J_i(\alpha)$ as J_i^α.

Suppose U has J-decomposition $e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$, then controlled-$U$ can also be decomposed as follows:

$$\wedge U_{12} = J_1^0 J_1^{\alpha'} J_2^0 J_2^{\beta+\pi} J_2^{-\gamma/2} J_2^{-\pi/2} J_2^0 \wedge Z_{12} J_2^{\pi/2} J_2^{\gamma/2} J_2^{(-\pi-\delta-\beta)/2} \times J_2^0 \wedge Z_{12} J_2^{(-\beta+\delta-\pi)/2}$$

with $\alpha' = \alpha + (\beta+\gamma+\delta)/2$.

To prove the above decomposition, we first define auxiliary unitary operators:

$$A = J(0) J(\beta+\pi) J\left(-\frac{\gamma}{2}\right) J\left(-\frac{\pi}{2}\right),$$

$$B = J(0) J\left(\frac{\pi}{2}\right) J\left(\frac{\gamma}{2}\right) J\left(\frac{-\pi-\delta-\beta}{2}\right),$$

$$C = J(0) J\left(\frac{-\beta+\delta-\pi}{2}\right).$$

Then, using the additivity relation we obtain $ABC = I$. On the other hand, using both the subtractivity relation and Eqs. (1), we get

$$\begin{aligned} AXBXC &= J(0) J(\beta+\pi) J\left(-\frac{\gamma}{2}\right) J\left(-\frac{\pi}{2}\right) J(\pi) J\left(\frac{\pi}{2}\right) J\left(\frac{\gamma}{2}\right) \\ &\quad \times J\left(\frac{-\pi-\delta-\beta}{2}\right) J(\pi) J\left(\frac{-\beta+\delta-\pi}{2}\right) \\ &= e^{-i[(\delta+\beta+\gamma)/2]} J(0) J(\beta) J(\gamma) J(\delta). \end{aligned}$$

Therefore one also has $e^{i[(2\alpha+\beta+\gamma+\delta)/2]} AXBXC = U$.

Combining our two equations in A, B, C, we obtain controlled-$U_{12} = P_1(\alpha') A_2 \wedge X_{12} B_2 \wedge X_{12} C_2$ with $\alpha' = \alpha + (\beta + \gamma + \delta)/2$; a decomposition which we can rewrite using our generating set:

$$P(\alpha)_1 = J_1^0 J_1^\alpha,$$

$$\wedge X_{12} = H_2 \wedge Z_{12} H_2 = J_2^0 \wedge Z_{12} J_2^0$$

to obtain the above decomposition of controlled-U.

As we will see, this decomposition leads to an implementation for the controlled-U operator using only 14 qubits. Using Y or Z in place of X in the argument above, one finds costlier decompositions using 15 and 16 qubits. No comparable decomposition was given previously.

Having all unitaries U over $\mathbb{C}^2$ and all unitaries of the form controlled-U over $\mathbb{C}^2 \otimes \mathbb{C}^2$ we can conclude that:

Theorem 1 (Universality). The set $\{J(\alpha)$, *controlled-Z*$\}$ *generates all unitaries*.

The following unitaries $H = J(0)$, $P(\pi/4) = J(0) J(\pi/4)$, and controlled-$X = J(0) \wedge Z J(0)$, are known to be *approximately universal*, in the sense that any unitary can be approximated within any precision by combining these [17]. Therefore the set $J(0)$, $J(\pi/4)$ and controlled-Z is also approximately universal.

III. ONE-WAY IMPLEMENTATIONS

So far we have obtained a generating set for unitaries that compares well with the usual one based on controlled-X and general rotations $R(\alpha, \beta, \gamma)$, in that our 1-qubit family of unitaries has only one parameter. Now we turn to the main advantage of our generating set which is that $J(\alpha)$ and controlled-Z have realizations in the one-way model using few qubits.

We begin with a quick recapitulation of the one-way model. Computations involve combinations of 2-qubit entanglement operators controlled-Z_{ij}, 1-qubit measurements M_i^α, and 1-qubit Pauli corrections X_i, Z_i, where i, j represent the qubits on which each of these operations apply, and α is a parameter in $[0, 2\pi]$. Such combinations, together with two distinguished sets of qubits (possibly overlapping) corresponding to inputs and outputs, will be called *measurement patterns*, or simply patterns. One can associate an *entanglement graph* to any pattern, where the vertices are the pattern qubits, and the (undirected) edges are given by the controlled-Z_{ij} operators [18].

Importantly, in a pattern, corrections are allowed to depend on previous measurement outcomes. There is also a parallel notion of dependent measurements, but we will not use it here.

To be more specific, M_i^α is an xy measurement, defined by a pair of complementary orthogonal projections, applied at qubit i, on the following vectors:

$$|+_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$

$$|-_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle)$$

Conventionally, we take measurement outcomes to range in $\mathbb{Z}_2 = \{0, 1\}$, 0 corresponding to a collapse to $|+_\alpha\rangle$, and 1 to a collapse to $|-_\alpha\rangle$.

Since qubits are measured at most once, we may represent unambiguously the outcome of the measurement done at qubit i by s_i. Dependent corrections will be written X_i^s and Z_i^s with $s = \Sigma_{i \in I} s_i$. Their meaning is that $X_i^0 = Z_i^0 = I$ (no correction is applied), while $X_i^1 = X_i$ and $Z_i^1 = Z_i$.

Now that we have a notation, we may describe the two patterns implementing our generators:

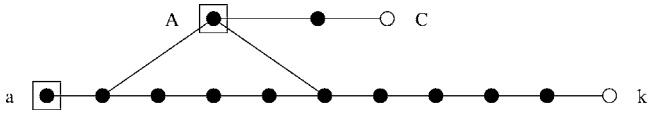

FIG. 1. Graph state for the controlled-U pattern: input qubits A and a are boxed, output qubits are C and k, measured qubits are solid circles.

$$\mathfrak{J}(\alpha) \coloneqq X_2^{s_1} M_1^{-\alpha} \wedge Z_{12}$$

$$\wedge\mathfrak{Z} \coloneqq \wedge Z_{12}$$

In the first pattern, 1 is the only input and 2 is the only output, while in the second both 1 and 2 are inputs and outputs (note that we are allowing patterns to have overlapping inputs and outputs).

These patterns are indeed among the simplest possible. Remarkably, there is only one single dependency overall, which occurs in the correction phase of $\mathfrak{J}(\alpha)$. No set of patterns without any measurement could be a generating set, since those can only implement unitaries in the Clifford group [9].

It is easy to verify that $\mathfrak{J}(\alpha)$ and controlled-$\mathfrak{Z}$ respectively implement $J(\alpha)$ and controlled-Z. Combining these two patterns, by composition and tensoring, will therefore generate patterns realizing all unitaries over $\otimes^n\mathbb{C}^2$.

Let us now examine the implementation of controlled-U, based on the decomposition which we recall:

$$\begin{aligned}\wedge U_{12} = {} & J_1^0 J_1^{\alpha'} J_2^0 J_2^{\beta+\pi} J_2^{-\gamma/2} J_2^{-\pi/2} J_2^0 \wedge Z_{12} \\ & \times J_2^{\pi/2} J_2^{\gamma/2} J_2^{(-\pi-\delta-\beta)/2} J_2^0 \wedge Z_{12} J_2^{(-\beta+\delta-\pi)/2}\end{aligned}$$

with $\alpha' = \alpha + (\beta+\gamma+\delta)/2$. Replacing each of the generators in the above expression by the corresponding pattern, we get

$$\begin{aligned}& X_C^{s_B} M_B^0 \wedge Z_{BC} X_B^{s_A} M_A^{-\alpha'} \wedge Z_{AB} X_k^{s_j} M_j^0 \wedge Z_{jk} X_j^{s_i} M_i^{-\beta-\pi} \wedge Z_{ij} X_i^{s_h} \\ & \quad \times M_h^{\gamma/2} \wedge Z_{hi} X_h^{s_g} M_g^{\pi/2} \wedge Z_{gh} X_g^{s_f} M_f^0 \wedge Z_{fg} \wedge Z_{Af} X_f^{s_e} \\ & \quad \times M_e^{-\pi/2} \wedge Z_{ef} X_e^{s_d} M_d^{-\gamma/2} \wedge Z_{de} X_d^{s_c} M_c^{(\pi+\delta+\beta)/2} \wedge Z_{cd} X_c^{s_b} \\ & \quad \times M_b^0 \wedge Z_{bc} \wedge Z_{Ab} X_b^{s_a} M_a^{(\beta-\delta+\pi)/2} \wedge Z_{ab}\end{aligned}$$

with input qubits $\{A,a\}$ and output qubits $\{C,k\}$. We have reserved uppercase (lowercase) letters for qubits used in implementing the J operators on control qubit A (target qubit a), and have indeed used a total number of 14 qubits.

Figure 1 shows the corresponding entanglement graph, where vertices represent qubits and edges connect the qubits of an entangled pair. This graph has only one cycle of length 6.

This graph also has a further interesting property, namely that all possible paths linking boundary vertices (inputs and outputs) are of even length (2, 6, 10 as it happens) as we can see in Fig. 2.

Say that a path is *extreme* in a graph with inputs and outputs, if it goes from the boundary to itself; say that a graph with inputs and outputs is *even* if all its extreme paths are of even length; say that a pattern is even if its entanglement graph is even. We may then rephrase the last observation by saying that the pattern for controlled-U is even.

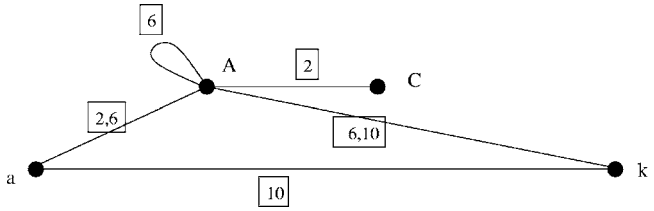

FIG. 2. Extreme paths in controlled-U pattern: numbers represent the length of paths; solid circles represent the pattern input and output qubits.

Patterns with an empty command sequence—among which one finds those implementing permutations over $\otimes^n\mathbb{C}^2$—are even. Indeed, all their paths, therefore all their extreme paths, are of length zero, and zero is even.

Furthermore, even patterns are closed under tensor product and composition. Indeed, the graph associated to the tensor product of two patterns is the juxtaposition of the components graphs, and therefore has a path space which is the disjoint sum of the path spaces of its components. On the other hand any extreme path in a composite pattern is a product of extreme paths of the components, and therefore has even length. This has a nice consequence:

Theorem 2. Any unitary can be realized by a pattern with a 2-colorable underlying graph.

Any unitary can be realized by a pattern obtained from the J-decomposition pattern, the controlled-U pattern, and the permutation patterns, combined by tensor and composition. Any cycle in such a pattern is either a cycle internal to some basic pattern (which rules out J-decomposition and permutation patterns which have a linear entanglement graph), so living inside a controlled-U pattern, therefore of length 6 and hence even, or the cycle is a product of extreme paths, therefore even, because all basic patterns are even, and by the above discussion, so is any combination of them. This completes the proof of the theorem. □

As said, 2-colorable entanglement graphs are interesting since purification protocols exist for their associated graph states, making them physically implementable in a way that is robust against decoherence [16]. So it is good news that such robust implementations can be obtained in the one-way model for all unitary operators.

It is important to note a similar result was known for a particular graph states so called cluster states [3]. The underlying graph of the cluster states are rectangular grids and hence 2-colorable. However to realize an arbitrary unitary operator one needs to consume many qubits and perform many Pauli measurements to respect the underlying structure, whereas in our proposed implementation all the unnecessary measurements have been removed and yet a 2-colorable graph is obtained.

IV. CONCLUSION

To conclude, we have exhibited a simple set of generators for the group of unitary maps over $\otimes^n\mathbb{C}^2$ which has not been considered before, as far as we know. Our primary interest

was to use it as a way to understand the measurement-based quantum computing model known as the one-way model [1]. Indeed, this set yields parsimonious implementations of unitaries in the one-way model. Moreover, we were able to show that the entanglement graphs underlying these implementations can always be chosen to be 2-colorable. Such graphs lead to entangled states belonging to the family of graph states for which physical implementations are well underway [12,13]. Purification protocols exist for the particular subclass of 2-colorable graph states, which make them physically implementable in a way that is robust against decoherence [16]. In making this comparison we note that the cluster-state implementations (where the underlying graph is a grid) are designed to work with "off the shelf" components of a particularly simple and physically realizable type whereas, of course, we have designed a special graph state to be as efficient as possible. However, we can use our controlled-unitary as a basic building block and have both efficiency and robustness. Note that any arbitrary combinations of our controlled-unitaries are also robust in this sense, which makes this an attractive building block. In order to appreciate this point better consider the situation with cluster states. In this case one can translate any circuit into a cluster state implementation; however, such implementations will typically contain several Pauli measurements. If one were to remove these Pauli measurements—for example, using the techniques of [18]—there is no guarantee that the result would have the two-colorability property that leads to robustness.

The grid-based graph states are known to fit well with proposed implementations based on optical lattices but there exist other proposals for implementations of arbitrary graphs [13] and these could be used for our graphs. Finally, from a complexity-theoretic point of view it is potentially interesting to use our graphs as a way of establishing lower bounds on the depth complexity of computations. In related work [19] we have already used the results of the present paper to establish properties of information flow in graph-state based computations.

ACKNOWLEDGMENTS

E.K. was partially supported by the PREA, MITACS, ORDCF and CFI projects. P.P. was supported by EPSRC (U.K.) and NSERC (Canada).

[1] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[2] R. Raussendorf and H. Briegel, Quantum Inf. Comput. **2**, 6 (2002).
[3] R. Raussendorf, D. E. Browne, and H.-J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[4] D. W. Leung, Int. J. Quantum Inf. **2**, 1 (2004).
[5] P. Aliferis and D. W. Leung, Phys. Rev. A **70**, 062314 (2004).
[6] A. M. Childs, D. W. Leung, and M. A. Nielsen, "Unified derivations of measurement-based schemes for quantum computation," quant-ph/0404132.
[7] P. Jorrand and S. Perdrix, "Unifying quantum computation with projective measurements only and one-way quantum computation," quant-ph/0404125.
[8] S. Perdrix, and P. Jorrand, "Measurement-based quantum turing machines and their universality," quant-ph/0404146.
[9] V. Danos, E. Kashefi, and P. Panangaden, "The measurement calculus," quant-ph/0412135.
[10] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[11] M. A. Nielsen and C. M. Dawson, "Fault-tolerant quantum computation with cluster states," quant-ph/0405134.
[12] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[13] S. R. Clark, C. Moura Alves, and D. Jaksch, New J. Phys. **7**, 124 (2005).
[14] S. D. Barrett and P. Kok, Phys. Rev. A **71**, 060310 (2005).
[15] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature (London) **434**, 169 (2005).
[16] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[18] M. Hein, J. Eisert, and H.-J. Briegel, Phys. Rev. A **69**, 062311 (2004).
[19] V. Danos and E. Kashefi, "Determinism in the one-way model," quant-ph/0506062.