Non-Unitary Probabilistic Quantum Computing

Robert M. Gingrich, and Colin P. Williams

Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Drive, Pasadena, California 91109-8099.

(Dated: September 15, 2003)

We present a method for designing quantum circuits that perform non-unitary quantum computations on n-qubit states probabilistically, and give analytic expressions for the success probability and fidelity. Our scheme works by embedding the desired non-unitary operator within an anti-block-diagonal (n+1)-qubit Hamiltonian, H, which induces a unitary operator $\Omega = \exp(i\varepsilon H)$, with ε a constant. By using Ω acting on the original state augmented with an ancilla prepared in the $|1\rangle$ state, we can obtain the desired non-unitary transformation whenever the ancilla is found to be $|0\rangle$. Our scheme has the advantage that a "failure" result, i.e., finding the ancilla to be $|1\rangle$ rather than $|0\rangle$, perturbs the remaining n-qubit state very little. As a result we can repeatedly re-evolve and measure the sequence of "failed" states until we find the ancilla in the $|0\rangle$ state, i.e., detect the "success" condition. We describe an application of our scheme to probabilistic state synthesis,

I. INTRODUCTION

In the traditional model of quantum computation one prepares an n-qubit state, evolves it under the action of a unitary operator representing the desired computation, and makes a projective measurement on the output state to obtain an answer [1]. In this view, measurement operations are a necessary evil required to extract an answer from the computer, typically at the cost of destroying valuable information encoded in the final superposition state. However, alternative models of quantum computing are possible, which embrace non-unitary operations and elevate them to the status of legitimate gates in the toolbox of the quantum circuit designer [2, 3, 4, 5, 6]. The importance of such non-standard models is that they may inspire new approaches to achieving universal quantum computing hardware that might be easier to implement than the traditional scheme, e.g., by trading quantum circuit complexity for success probability.

Although there has been considerable prior work on designing circuits for performing unitary quantum computations deterministically [7, 8, 9, 10], far less attention has been paid to developing methods for designing circuits that perform *non-unitary* computations *probabilistically*. This is the focus of our paper. Specifically, we present a scheme that allows us to construct a quantum circuit for performing the non-unitary transformation

$$\rho_{\text{in}} \rightarrow \frac{N\,\rho_{\text{in}}\,N^{\dagger}}{\text{tr}(N\,\rho_{\text{in}}\,N^{\dagger})} \tag{1}$$

where N is an arbitrary non-unitary transformation, and ρ_{in} is an arbitrary n-qubit density operator. Note that such a non-unitary transformation is well-defined if and only if $\det(N) \neq 0$. If this condition is not met, we must explicitly exclude input states, ρ_{in}, such that $N\,\rho_{\text{in}}\,N^{\dagger}$ is the zero matrix. Without loss of generality, we may assume the non-unitary matrix N is of dimension $2^n \times 2^n$. If, initially, N has fewer than 2^n rows or columns, we must pad N with zeroes to the right of the columns, and/or beneath the rows, sufficient to make a $2^n \times 2^n$ dimensional matrix. The trace in the denominator guarantees that the output will be properly normalized.

The paper is organized as follows. Section II describes our procedure for embedding an arbitrary non-unitary operator within a larger unitary one, and how to use the result to achieve the desired non-unitary state transformation probabilistically. Section III provides an analysis of the success probability and fidelity of the achieved transformation. Section IV gives some examples of random non-unitary transforms of random input states to illustrate the tradeoff between fidelity and success probability. Section V illustrates how our non-unitary quantum computing procedure can be applied to probabilistic state synthesis.

II. NON-UNITARY EMBEDDING PROCEDURE

Given an arbitrary non-unitary matrix, N, our goal is to devise a quantum circuit sufficient to achieve the transformation $\rho_{\text{in}} \to N \rho_{\text{in}} N^{\dagger} / \operatorname{tr}(N \rho_{\text{in}} N^{\dagger})$. To do so we use N to build a "designer" Hamiltonian that acts on the n original qubits plus one extra ancilla qubit. By reading the output state of the ancilla, we can test whether or not the desired non-unitary transformation has been applied to the n-qubit state.

The first step in our non-unitary embedding procedure is to pad N, if necessary, to make it a square $2^n \times 2^n$ dimensional matrix:

$$N \xrightarrow{pad} \underbrace{\left(\begin{array}{c|c} N & 0 \\ \hline 0 & 0 \end{array}\right)}_{2^n} \tag{2}$$

Next, we define the unitary operator, Ω, via a Hamiltonian built from N. Specifically, let:

$$\Omega = \exp\left(i\varepsilon \begin{pmatrix} 0 & -iN \\ iN^{\dagger} & 0 \end{pmatrix} \right) \tag{3}$$

where ε is a constant. This constant, ε, affects both the fidelity with which we are able to achieve the desired non-unitary transformation as well as its probability of occurrence.

Next, we introduce an ancilla qubit prepared in the state $|1\rangle\langle 1|$, and evolve the ancilla-augmented state under Ω:

$$\rho_{\text{out}} = \Omega\left(|1\rangle\langle 1| \otimes \rho_{\text{in}}\right)\Omega^{\dagger} \tag{4}$$

Finally, we measure the ancilla in the $\{|0\rangle, |1\rangle\}$ basis. Specifically, we define a pair of measurement operators M_0 and M_1 as:

$$\begin{aligned} M_0 &= (|0\rangle\langle 0|) \otimes I \\ M_1 &= (|1\rangle\langle 1|) \otimes I \end{aligned} \tag{5}$$

where I is the $2^n \times 2^n$ dimensional identity matrix. We find the ancilla in the $|0\rangle$ ("success") or $|0\rangle$ ("failure") state with respective probabilities p_0 and p_1 given by:

$$\begin{aligned} p_0 &= \operatorname{tr}(M_0^{\dagger} M_0 \rho_{\text{out}}) \\ p_1 &= \operatorname{tr}(M_1^{\dagger} M_1 \rho_{\text{out}}) \end{aligned} \tag{6}$$

The corresponding density matrices, conditioned on these measurement outcomes, are:

$$\rho_0 = \frac{M_0 \rho_{\text{out}} M_0^\dagger}{p_0} \\ \rho_1 = \frac{M_1 \rho_{\text{out}} M_1^\dagger}{p_1} \tag{7}$$

If the measurement results in "failure" i.e., finding the ancilla to be in the $|1\rangle$ state, we re-introduce the ancilla, and perform the evolution described by equation. 4, but this time using the reduced density matrix ρ_1 rather than ρ_{in}. This process can be repeated indefinitely, using the sequence of reduced density operators generated by successive failures, until the ancilla is found in the "success" condition, i.e., $|0\rangle$. This is possible because, as we will show in §III, upon "failure" the effective operation applied to the n-qubit state is close to the identity. Hence, "failed" attempts at projecting the desired non-unitary computation are not devastating. Indeed, they can be made arbitrarily delicate at the cost of reducing the success probability.

Once measurement of the ancilla yields the "success" condition, the remaining n unmeasured qubits will be in a state that approximates the desired non-unitary transformation. For example, if we happen to succeed on the first measurement, we will have succeeded in transforming our initial state into:

$$\rho_{\text{out}}^{\text{actual}} = \text{tr}_1(\rho_0) \tag{8}$$

This is to be compared against the state transformation we were hoping to obtain, namely:

$$\rho_{\text{out}}^{\text{desired}} = \frac{N \rho_{\text{in}} N^\dagger}{\text{tr}(N \rho_{\text{in}} N^\dagger)} \tag{9}$$

III. SUCCESS PROBABILITY AND FIDELITY

It is natural to ask with what efficiency and fidelity can the desired non-unitary transformation be obtained? To answer these questions, it is helpful to construct the singular value decomposition (SVD) of the desired non-unitary operation.

$$N = U^\dagger \Sigma V \tag{10}$$

Using the SVD, we can write the unitary operator $\Omega = \exp(i\varepsilon H)$ as

$$\begin{aligned} \Omega &= \exp\left(i\varepsilon \begin{pmatrix} 0 & -iN \\ iN^\dagger & 0 \end{pmatrix} \right) \\ &= \begin{pmatrix} U^\dagger \cos(\varepsilon\Sigma) U & 0 \\ 0 & V^\dagger \cos(\varepsilon\Sigma) V \end{pmatrix} + \begin{pmatrix} 0 & U^\dagger \sin(\varepsilon\Sigma) V \\ -V^\dagger \sin(\varepsilon\Sigma) U & 0 \end{pmatrix} \end{aligned} \tag{11}$$

In this form we can see immediately what operations are performed when the ancilla measurement "succeeds" or "fails", i.e., yields $|0\rangle$, or $|1\rangle$ respectively. As Ω acts upon a state of the form $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \rho_{\text{in}}$, upon "failure" the effective transformation is $N_{\text{fail}} = V^\dagger \cos(\varepsilon \Sigma) V$ and upon "success" the effective transformation is $N_{\text{succ}} = U^\dagger \sin(\varepsilon \Sigma) V$, Hence, if the projective measurement fails k times before it first succeeds, the net transformation applied to the input state will be

$N_{\text{net}} = N_{\text{succ}} N_{\text{fail}}^{k}$. Note that this transformation is independent of the state acted upon, ρ_{in}, but does depend upon the scaling parameter in the Hamiltonian, ε. The smaller ε, the closer to performing the identity operation (a "no-op") on each failed attempt. Hence, to ensure high fidelity we need ε to be small. Mathematically, after k failures and one success, the actual state created is:

$$\rho_{\text{out}}^{\text{actual}} = \frac{N_{\text{net}} \rho_{\text{in}} N_{\text{net}}^{\dagger}}{\text{tr}(N_{\text{net}} \rho_{\text{in}} N_{\text{net}}^{\dagger})} \tag{12}$$

Thus to estimate the fidelity (conditioned on success at the $(k+1)$-th trial) we need to compute:

$$F(\rho_{\text{out}}^{\text{actual}}, \rho_{\text{out}}^{\text{desired}}) = \text{tr}\sqrt{\sqrt{\rho_{\text{out}}^{\text{actual}}}\, \rho_{\text{out}}^{\text{desired}} \sqrt{\rho_{\text{out}}^{\text{actual}}}} \tag{13}$$

IV. SOME EXAMPLES

In this section, we give some examples of the fidelity and success probability achievable for four random non-unitary transformations of a random 2-qubit mixed state. The particular details of the non-unitary transformations and state we used are not important. We merely wish to illustrate that for random non-unitary transformations of random states as $\varepsilon \to 0$ the fidelity $\to 1$, the success probability $\to 0$, and the expected fidelity (the product of the two) can have quite complicated behavior. The point is that there is a tradeoff between the probability of achieving the desired non-unitary transformation and its fidelity: the smaller ε, the better we can approximate the desired non-unitary transformation, but the more attempts we will need to make to achieve it.

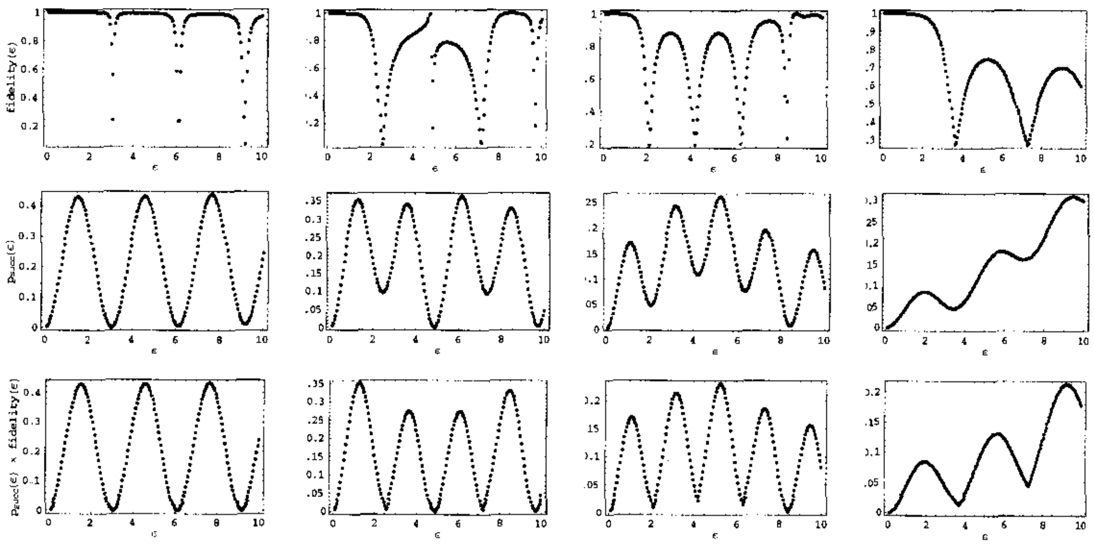

Fig. 1. Four examples (read in columns) of random non-unitary transformations of random input states. The plots are, from top to bottom, the fidelity of the transformation, the success probability, and the product of fidelity times success probability. The results illustrate that there is a tradeoff between the fidelity with which we can approximate the desired non-unitary transformation, and the efficiency with which we can do it.

V. APPLICATION: NON-UNITARY STATE SYNTHESIS

Although schemes for deterministic state synthesis are known, e.g., [11], we will now describe a scheme for *probabilistic* state synthesis using non-unitary quantum computing. Our goal is to find a quantum circuit sufficient to synthesize an arbitrary n-qubit pure state $|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$. To do so, we find a unitary transformation sufficient for synthesizing the desired state probabilistically, and then decompose this unitary transformation into an equivalent quantum circuit. The latter decomposition can be done using, e.g., the generalized singular value decomposition [9], implemented in the QCD quantum circuit design software package [9].

Our non-unitary (probabilistic) state synthesis scheme is depicted in Fig. 2.

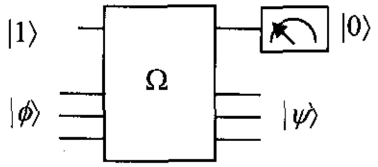

Fig. 2. An equally weighted superposition, $|\phi\rangle = (W \otimes W \ldots \otimes W)|00\ldots0\rangle$ is evolved together with an ancilla under the action of Ω, which is induced from a Hamiltonian containing the non-unitary operator, N. Subsequently, if the ancilla is found to be $|0\rangle$ the remaining qubits will be prepared in the desired superposition state.

We begin by considering the non-unitary transformation defined by:

$$N = \sqrt{2^n} \begin{pmatrix} c_0 & 0 & 0 & 0 \\ 0 & c_1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & c_{2^n-1} \end{pmatrix} \tag{14}$$

Conceptually, if the operation N were available to use, then we could use the equally weighted superposition state, $|\phi\rangle = W^{\otimes n}|00\ldots0\rangle$ (where W is the Walsh-Hadamard gate), to create the desired superposition state $|\psi\rangle$ from the non-unitary operation $N \cdot W^{\otimes n}|00\ldots0\rangle = |\psi\rangle$. However, as N is a non-unitary operation it is not immediately available. Instead, we have to embed N within a larger unitary operation whose outcome is conditioned on the value of an ancilla qubit. Specifically, we define the Hamiltonian $H = \varepsilon \begin{pmatrix} 0 & -iN \\ iN^\dagger & 0 \end{pmatrix}$ and hence, implicitly, the unitary operator $\Omega = \exp(i\varepsilon H)$. Next we introduce an ancilla prepared in the $|1\rangle$ state, perform the evolution $\Omega|1\rangle|\phi\rangle$, and then measure the ancilla. If we find the ancilla to be $|0\rangle$ we are done, as the remaining n-qubits will be in state $|\psi\rangle$. Otherwise, if we find the ancilla to be $|1\rangle$, we evolve the output again under Ω and measure the ancilla. We continue until we find the ancilla to be $|0\rangle$, whereupon the desired state will have been synthesized.

Empirically, we find that the minimum depth of the circuit for *probabilistically* synthesizing $|\psi\rangle$ is typically less than the minimum depth of the circuit for *deterministically* synthesizing $|\psi\rangle$ [9,11], but at the expense of possibly having to repeat the synthesis attempt several times. Nevertheless, this could point to an interesting tradeoff in the design space of quantum computing hardware. If it proves to be experimentally challenging to maintain quantum coherence for several gate operations, but relatively easy to introduce extra qubits, then non-unitary quantum computation might allow certain quantum computations to be achieved non-deterministically that would otherwise be beyond the reach of experimental capability.

VI. CONCLUSIONS

We have presented a systematic technique for achieving non-unitary quantum computations probabilistically by embedding the desired non-unitary operation within a larger unitary one. The latter unitary operator can be decomposed into an equivalent quantum circuit using algebraic, numerical or genetic techniques [7, 8, 9, 10]. Hence, our scheme provides a method for designing a quantum circuit sufficient to implement an arbitrary non-unitary operation probabilistically. Empirically, we find that the resulting circuits can have smaller depth than those used to synthesize the same state deterministically. More work needs to be done on characterizing these bounds.

Acknowledgement: The research described in this paper was performed at the Jet Propulsion Laboratory (JPL), California Institute of Technology, under contract with the National Aeronautics and Space Administration (NASA). We would like to thank the National Security Agency (NSA) and the Advanced Research and Development Activity (ARDA) for funding support.

REFERENCES

[1] M. Nielsen and I. Chuang, "*Quantum Computation and Quantum Information*," Cambridge University Press, ISBN 0-521-63503-9 (2000).
[2] M. A. Nielsen, "Universal Quantum Computation Using Only Projective measurement, Quantum Memory, and Preparation of the $|0\rangle$ State", quant-ph/0108020 (2001).
[3] S. A. Fenner, and Y. Zhang, "Universal Quantum Computation with Two-Qubit and Three-Qubit Projective Measurements", quant-ph/0111077, (2001).
[4] R. Raussendorf and H. J. Briegel, "A One-Way Quantum Computer", Physical Review Letters, Volume 86, Number 22, 28 May (2001), pp.5188-5191.
[5] E. Knill, R. Laflamme, and G. J. Milburn, "A Scheme for Efficient Quantum Computation with Linear Optics," Nature 409, 46 (2001).
[6] J. D. Franson, M. M. Donegan, M. J. Fitch, B. C. Jacobs, and T. B. Pittman, "High-fidelity quantum logic operations using linear optical elements," Phys. Rev. Lett. 89, 137901 (2002).
[7] A. Barenco, Physical Review A, 52, 3457, (1995).
[8] D. P. Di Vincenzo and J. Smolin, "Results on Two-Qubit Gate Design for Quantum Computers," in Proc. Workshop on Physics and Computation, Dallas, TX, IEEE Computer Society Press, (1994) pp.14-23.
[9] L. Song and C. P. Williams, "Quantum Circuit Decomposition of an Arbitrary Unitary Operator," submitted to Physical Review Letters, (2003).
[10] F. Vatan and C. P. Williams, "Optimal Quantum Circuits for General Two-Qubit Gates," submitted to Physical Review Letters. See preprint quant-ph/0308006 (2003).
[11] L. Song, and C. P. Williams, "Computational Synthesis of Any N-Qubit Pure or Mixed State," Quantum Information and Computation, E. Donkor, A. R. Pirich, H. E. Brandt (eds.), in Proc. SPIE Vol. 5105 (2003) pp.195-203.