Storing Quantum Dynamics in Quantum States: A Stochastic Programmable Gate

G. Vidal,[1] L. Masanes,[1,2] and J.I. Cirac[1]

[1]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*

[2]*Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, E-08028 Barcelona, Spain*

(Received 31 January 2001; published 11 January 2002)

We show how to encode quantum dynamics in the state of a quantum system, in such a way that the system can be used to stochastically perform, at a later time, the stored transformation on some other quantum system. The probability of failure decreases exponentially with the number of qubits that store the transformation. We discuss optimality of this scheme, whose applications include viability of a (stochastic) programmable quantum gate and the teleportation of quantum transformations using entanglement and unidirectional classical communication.

DOI: 10.1103/PhysRevLett.88.047905 PACS numbers: 03.67.Lx, 05.40.–a

Quantum information science investigates the potential of quantum mechanics to process and transmit information in novel ways. Quantum systems are usually conceived as containers for data, which are processed by means of a unitary evolution. Here we will explore to what extent quantum mechanics allow for the processing itself—i.e., instead of the data—to be stored in a quantum system. In particular, we will present a scheme to encode unitary transformations in, and to stochastically retrieve them from, quantum states. The practical importance of this result relies on the fact that, once the operation has been captured in a quantum state, it can be processed by means of any standard state manipulation technique. And thus, for instance, the operation can be simply kept for later use, but it can also be transmitted to a remote party (e.g., using teleportation) or can be estimated by means of a proper measurement.

The storage of operations is, as explained below, necessarily imperfect. The present scheme will fail with a probability ϵ that exponentially decreases with the number of qubits in which the operation has been encoded. More specifically, we shall discuss how to store, using N qubits and with probability $\epsilon = 2^{-N}$ of failure in its later retrieval, an arbitrary rotation of a qubit around the $\hat{z}$ axis. For $N = 1$ we will prove that the scheme is optimal; i.e., it has the minimal error probability ever possible, whereas for $N > 1$ some evidence in the same direction will be presented.

Let us start by considering two quantum systems that we will call *program* and *data registers,* with corresponding Hilbert spaces $\mathcal{H}_P$ and $\mathcal{H}_D$. A *program state* $|U\rangle \in \mathcal{H}_P$ will be said to store the transformation U, if some "fixed" protocol employing $|U\rangle$ is able to perform U on an arbitrary *data state* $|d\rangle \in \mathcal{H}_D$. Here a fixed protocol means that the manipulation of the joint state $|d\rangle \otimes |U\rangle$ does not require knowing the operation U nor the data $|d\rangle$. A device able to transform the previous state into $U|d\rangle \otimes |\mathcal{R}_{d,U}\rangle$, where $|\mathcal{R}_{d,U}\rangle$ is just some residual state, is known as a *programmable quantum gate* [1]. Thus, in a similar fashion as most "classical" computers take both program and data as input bit strings, a programmable or universal quantum gate is a device whose action U on an arbitrary data state $|d\rangle$ is completely determined by the program state $|U\rangle$.

Nielsen and Chuang analyzed in Ref. [1] the possibility of constructing one such gate. Its total dynamics are described in terms of a fixed unitary operator G,

$$G[|d\rangle \otimes |U\rangle] = (U|d\rangle) \otimes |\mathcal{R}_U\rangle, \tag{1}$$

where the residual state $|\mathcal{R}_U\rangle$ was showed to be independent of $|d\rangle$. Also the following important result was proved: any two inequivalent operations U and V require orthogonal program states, that is, $\langle U \mid V\rangle = 0$, if the same transformation G is to implement them according to Eq. (1). This means that in order to perfectly store one operation U_i, chosen from a finite set $\{U_i\}_{i\in I}$, a vector state $|U_i\rangle$ belonging to an orthonormal basis $\{|U_i\rangle \in \mathcal{H}_P\}_{i\in I}$ has to be used. In other words, different operations of the gate necessarily correspond to mutually *distinguishable* programs. This has two direct implications. First, a classical binary string could have been used in the first place as a program (there is no gain in using quantum states for this purpose). The second consequence concerns the feasibility of such gates: even for the simplest data register, a qubit (i.e., $\mathcal{H}_D = C^2$), the set of unitary transformations, SU(2), is infinite. Therefore no universal gate implementing an arbitrary (say) one-qubit operation can be constructed using a program register whose Hilbert space $\mathcal{H}_P$ has finite dimension.

Here we will assume, nevertheless, that only N qubits are available as a program register, and thus $\mathcal{H}_P = C^{2\otimes N}$ is finite dimensional. For simplicity, we will restrict our attention to one-qubit operations of the form

$$U_\alpha \equiv \exp\left(i\alpha\,\frac{\sigma_z}{2}\right), \tag{2}$$

for an arbitrary angle $\alpha \in [0, 2\pi)$, which correspond to arbitrary rotations around the $\hat{z}$ axis of a spin 1/2 particle [2]. We would then like to answer the following question: To what extent can N qubits store an arbitrary operation U_α?

The quality of the storage is determined by how well the operation can be retrieved, that is, by how well it can be finally performed on the unknown data state $|d\rangle$. One possibility would be to consider *approximate* transformations, with the output state of the gate being an approximation to $U_\alpha|d\rangle$. But this can already be achieved by classically encoding a truncated binary expansion of the angle α [3]. Alternatively, as we will next discuss, *stochastic* transformations may be considered. In this case the programmable gate does not always succeed at performing U after processing the program $|U\rangle$, but when it does succeed, then the output state is exactly $U_\alpha|d\rangle$. Of course, we also want to be able to know whether the gate achieved its goal or not. Reasonably, the *a priori* probability of success is a good merit for this kind of programmable gates. Since in principle such probability p_α^d may depend both on the data $|d\rangle$ and on the operation U_α under consideration, we will use its average

$$\langle p\rangle \equiv \int_{C^2} d(|d\rangle) \int \frac{d\alpha}{2\pi}\, p_\alpha^d \tag{3}$$

to quantify the performance of the gate.

Let us suppose, first, that only one qubit, i.e., $N = 1$, is available to encode any of the transformations U_α. In this case the *equatorial state*

$$|\alpha\rangle \equiv \frac{1}{\sqrt{2}}(e^{i\alpha/2}|0\rangle + e^{-i\alpha/2}|1\rangle) \tag{4}$$

can be used to store U_α, in the sense that a CNOT gate, $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x$—taking the data and program register as control and target qubits, respectively—will be able to transform the data state $|d\rangle$ according to U_α, with probability 1/2, for all $|d\rangle$ and all U_α (see Fig. 1). Indeed, it is straightforward to check that

$$|d\rangle \otimes |\alpha\rangle \overset{\text{CNOT}}{\rightarrow} \frac{1}{\sqrt{2}}(U_\alpha|d\rangle \otimes |0\rangle + U_\alpha^\dagger|d\rangle \otimes |1\rangle), \tag{5}$$

and therefore a projective measurement in the $\{|0\rangle, |1\rangle\}$ basis of the program register will make the data qubit collapse either into the desired state $U_\alpha|d\rangle$ or into the wrong state $U_\alpha^\dagger|d\rangle$, with the announced probabilities.

In order to see that no scheme exists better than the one above, let us consider the most general stochastic programmable gate using a single qubit as a program register.

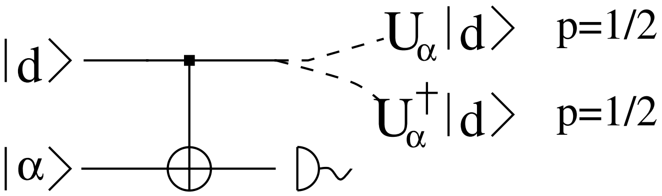

FIG. 1. Optimal stochastic quantum programmable gate with a single-qubit program register. Data and program states $|d\rangle$ and $|\alpha\rangle$ are transformed, depending on the result of a measurement on the program register, either into $U_\alpha|d\rangle$ or $U_\alpha^\dagger|d\rangle$, with error probability $\epsilon = 1/2$.

It can always be represented by a unitary transformation G_s given by

$$G_s[|d\rangle \otimes |U_\alpha\rangle \otimes |0\rangle] \equiv \sqrt{p_\alpha^d}\,(U_\alpha|d\rangle) \otimes |\tau_\alpha^d\rangle + \sqrt{1 - p_\alpha^d}\,|\chi_\alpha^d\rangle, \tag{6}$$

taking the data and program states, together with a fixed state $|0\rangle$ of a third (ancillary) system $\mathcal{H}_A$, into $U_\alpha|d\rangle$ with probability p_α^d. Note that all kets appearing in Eq. (6) are normalized vectors. We demand that for all possible d, d', α, α', the state $\langle\tau_\alpha^d \,|\, \chi_{\alpha'}^{d'}\rangle \in \mathcal{H}_D$ vanishes. This is equivalent to requiring that by means of a measurement—onto the support $\Pi_\tau \subseteq \mathcal{H}_P \otimes \mathcal{H}_A$ of the vectors $|\tau_\alpha^d\rangle$ and its complementary subspace $\Pi_\tau^\perp$—we are able to know whether the gate succeeded or not.

Since G_s is a linear transformation, by decomposing $|d\rangle$ as $a|\overline{0}\rangle + b|\overline{\pi}\rangle$, where a, b are complex coefficients $(|a|^2 + |b|^2 = 1)$ and $|\overline{0}\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, $|\overline{\pi}\rangle \equiv i(|0\rangle - |1\rangle)/\sqrt{2}$, we obtain that the right-hand side of Eq. (6) must be equal to

$$\begin{aligned} &a[\sqrt{p_\alpha^{\overline{0}}}\,(U_\alpha|\overline{0}\rangle) \otimes |\tau_\alpha^{\overline{0}}\rangle + \sqrt{1 - p_\alpha^{\overline{0}}}\,|\chi_\alpha^{\overline{0}}\rangle], \\ &+b[\sqrt{p_\alpha^{\overline{\pi}}}\,(U_\alpha|\overline{\pi}\rangle) \otimes |\tau_\alpha^{\overline{\pi}}\rangle + \sqrt{1 - p_\alpha^{\overline{\pi}}}\,|\chi_\alpha^{\overline{\pi}}\rangle]. \end{aligned} \tag{7}$$

This implies that the probability of success p_α^d and the vector $|\tau_\alpha^d\rangle$, from now on p_α and $|\tau_\alpha\rangle$, do not depend on the data $|d\rangle$. On the other hand, the most general codification scheme of U_α on a qubit, $[0, 2\pi) \rightarrow C^2$, can be parametrized as $|U_\alpha\rangle \equiv A(\alpha)\,|\underline{0}\rangle + B(\alpha)\,|\underline{\pi}\rangle$, where $A(\alpha)$ and $B(\alpha)$ are complex functions $(\langle U_\alpha \,|\, U_\alpha\rangle = |A(\alpha)|^2 + |B(\alpha)|^2 + 2\,\mathrm{Re}[A(\alpha)B^*(\alpha)\,\langle\underline{0}\,|\,\underline{\pi}\rangle] = 1)$ and the states $|\underline{0}\rangle$ and $|\underline{\pi}\rangle$ correspond to the (not necessarily orthonormal) programs $|U_0\rangle$ and $|U_\pi\rangle$. Expanding now $|U_\alpha\rangle$ in Eq. (6) we find that its right-hand side must read

$$\begin{aligned} &A(\alpha)[\sqrt{p_0}\,U_0|d\rangle \otimes |\tau_0\rangle + \sqrt{1 - p_0}\,|\chi_0^d\rangle], \\ &+B(\alpha)[\sqrt{p_\pi}\,U_\pi|d\rangle \otimes |\tau_\pi\rangle + \sqrt{1 - p_\pi}\,|\chi_\pi^d\rangle] \end{aligned} \tag{8}$$

for any $|d\rangle$, which readily implies that the states $|\tau_\alpha\rangle(\equiv |\tau\rangle)$ do not depend on α and that $\sqrt{p_\alpha}\,U_\alpha = A(\alpha)\sqrt{p_0}\,U_0 + B(\alpha)\sqrt{p_\pi}\,U_\pi$. This last equation leads to $A(\alpha) = \sqrt{p_\alpha/p_0}\cos(\alpha/2)$ and $B(\alpha) = \sqrt{p_\alpha/p_\pi}\sin(\alpha/2)$. If we now substitute these in state $|U_\alpha\rangle$, from its normalization we obtain

$$p_\alpha = \left(\frac{\cos^2\frac{\alpha}{2}}{p_0} + \frac{\sin^2\frac{\alpha}{2}}{p_\pi} + 2\,\frac{\cos\frac{\alpha}{2}\sin\frac{\alpha}{2}\,\mathrm{Re}[\langle\underline{0}\,|\,\underline{\pi}\rangle]}{\sqrt{p_0 p_\pi}}\right)^{-1}. \tag{9}$$

Recall that our goal is to maximize the average probability of success (3). Without loss of generality we can require that $p_0 \geq p_\alpha$ [4], which corresponds to choosing $\mathrm{Re}[\langle\underline{0}\,|\,\underline{\pi}\rangle] = 0$. It is now easy to compute $\langle p\rangle$, which reads $\sqrt{p_0 p_\pi}$. Substituting all the previous findings in Eq. (6), and computing the scalar product of $G_s[|\overline{0}\rangle \otimes |\underline{0}\rangle \otimes |0\rangle]$ and $G_s[|\overline{\pi}\rangle \otimes |\underline{\pi}\rangle \otimes |0\rangle]$ we obtain

$$0 = -\sqrt{p_0 p_\pi} + \sqrt{1 - p_0}\sqrt{1 - p_\pi}\,\langle\chi_0^{\overline{0}}\,|\,\chi_\pi^{\overline{\pi}}\rangle. \tag{10}$$

That is, $\sqrt{p_0 p_\pi}$ is at most $\sqrt{1-p_0}\sqrt{1-p_\pi}$. The most favorable case corresponds to $p_0 = 1 - p_\pi$, and therefore the maximal $\langle p\rangle = \sqrt{p_0 p_\pi}$ is 1/2, achieved when $p_\alpha = 1/2$ is constant. This ends the proof that Eqs. (4) and (5) constitute the optimal protocol for storing and stochastically retrieving an operation U_α in a single qubit, with the associated error $\epsilon \equiv 1 - \langle p\rangle$ being 1/2.

We now move to consider the storage of U_α using more qubits, $N > 1$. When the previous scheme fails, not only has the data $|d\rangle$ not yet been processed properly, but in addition it has been modified in an unwished manner (which is unknown to the user of the gate) into $U_\alpha^\dagger|d\rangle$. However, a single second go of the previous gate may correct $U_\alpha^\dagger|d\rangle$ into $U_\alpha|d\rangle$ at once. This is achieved by just inserting $U_\alpha^\dagger|d\rangle$ in the gate of Eq. (5), together with a new program state, namely $|2\alpha\rangle$ (see Fig. 2). That is, the two-qubit program $|\alpha\rangle \otimes |2\alpha\rangle$ stores U_α with a probability of failure $\epsilon = 1/4$ in the retrieval stage.

In case of a new failure, the state of the system becomes $U_\alpha^{\dagger 3}|d\rangle$. We can insert again this state, together with state $|4\alpha\rangle$, into the elementary gate. If we keep on obtaining failures, we can try to correct the state as many times as wished, provided that the state $|2^{l-1}\alpha\rangle$ is available at the lth attempt. Therefore, for any N, the N-qubit state

$$|U_\alpha^N\rangle \equiv \bigotimes_{l=1}^{N} |2^{l-1}\alpha\rangle \tag{11}$$

can be used to implement the transformation U_α with probability $1 - (1/2)^N$ [5]. The corresponding stochastic programmable gate (see Fig. 3) consists of the unitary transformation of $|d\rangle \otimes |U_\alpha^N\rangle$ into

$$\frac{1}{2^{N/2}}\left(\sqrt{2^N - 1}\, U_\alpha|d\rangle \otimes |\tau\rangle + U_\alpha^{(2^N-1)\dagger}|d\rangle \otimes |\chi\rangle\right) \tag{12}$$

and of a posterior measurement of the program register (either in state $|\tau\rangle$ or $|\chi\rangle \equiv |1\rangle^{\otimes N}$, $\langle\tau\,|\,\chi\rangle = 0$). Its failure probability, $\epsilon = (1/2)^N$, decreases exponentially with the size N of the program register.

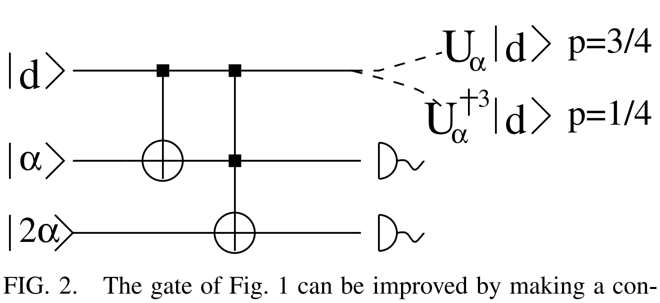
|d⟩
|α⟩
|2α⟩
$U_\alpha|d\rangle$ p=3/4
$U_\alpha^{\dagger 3}|d\rangle$ p=1/4

FIG. 2. The gate of Fig. 1 can be improved by making a conditional correction of the output after its CNOT gate. This is achieved by means of a Toffoli gate, which acts as a CNOT between the first and third lines of the circuit only when the second line carries a $|1\rangle$, corresponding to a failure in Fig. 1. A measurement on the program qubits in the $\{|0\rangle, |1\rangle\}$ basis will reveal whether the gate failed (this happens when outcome 1 is obtained from both registers, i.e., $\epsilon = 1/4$) or succeeded.

We are tempted to conjecture that, for any N, Eqs. (11) and (12) define again an optimal protocol to store and stochastically retrieve U_α. Notice, on the one hand, that the N-qubit program register in the unknown state $|U_\alpha^N\rangle$ has maximal entropy, since $\int d\alpha/(2\pi)\,|U_\alpha^N\rangle\langle U_\alpha^N| = (I/2)^{\otimes N}$, where I is the identity operator in C^2. That is, the program state carries as much information as possible, with N bits of information about α being extractable from it for large N [6]. On the other hand, we will now prove that our scheme is the optimal way of retrieving U_α from the program $|U_\alpha^N\rangle$ as given in Eq. (11).

Indeed, let G_s^N be a unitary transformation producing $U_\alpha|d\rangle$ from $|d\rangle \otimes |U_\alpha^N\rangle$, with probability p_α (we already learned, from the single-qubit case, that the probability of success is independent of the data state $|d\rangle$). From G_s^N we can construct another gate $G_{s'}^N$ with constant probability of success $p'_\alpha = \langle p\rangle_{G_s^N}$, where $\langle p\rangle_{G_s^N} \equiv \int d\alpha/(2\pi)p_\alpha$ is the average probability of success of G_s^N, precisely the quantity to be maximized. The construction goes as follows. Given a program state $|U_\alpha^N\rangle$, we will randomly choose an angle $\alpha_0 \in [0, 2\pi)$ and will transform the program into $|U_{\alpha+\alpha_0}^N\rangle$. This can be achieved by performing $U_{\alpha_0} \otimes U_{\alpha_0}^2 \otimes \cdots \otimes U_{\alpha_0}^{2^{N-1}}$ on $|U_\alpha^N\rangle$. Then we will run G_s^N on $|d\rangle$ using the new program, to obtain $U_{\alpha+\alpha_0}|d\rangle$ with probability $p_{\alpha+\alpha_0}$. Finally, we will perform $U_{\alpha_0}^\dagger$ on $U_{\alpha+\alpha_0}|d\rangle$. The overall effect is the promised gate $G_{s'}^N$, and therefore we need only to optimize over programmable gates with constant success probability p,

$$|d\rangle \otimes |U_\alpha^N\rangle \otimes |0\rangle \to \sqrt{p}\, U_\alpha|d\rangle \otimes |\tau_\alpha\rangle + \sqrt{1-p}\,|\chi_\alpha^d\rangle. \tag{13}$$

Let us choose the data $|d\rangle$ to be an equatorial state $|\beta\rangle$ of angle β, so that $U_\alpha|\beta\rangle = |\alpha + \beta\rangle$. Unitarity of the whole transformation G'_s implies, if $\beta' \equiv \pi + \beta + \alpha - \alpha'$, that

$$\langle\beta'\,|\,\beta\rangle\langle U_{\alpha'}^N\,|\,U_\alpha^N\rangle = (1-p)\langle\chi_{\alpha'}^{\beta'}\,|\,\chi_\alpha^\beta\rangle \tag{14}$$

(notice that $\langle\beta'|U_{\alpha'}^\dagger U_\alpha|\beta\rangle = 0$). The absolute value of the left-hand side of Eq. (14) is now at most $1 - p$. But we can easily compute the above scalar products using Eq. (4), to get the bound $[\sin 2^{N-1}(\alpha - \alpha')]/2^N \le 1 - p$.

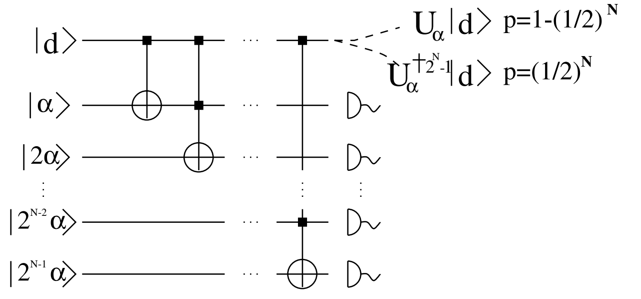
|d⟩
|α⟩
|2α⟩
$|2^{N-2}\alpha\rangle$
$|2^{N-1}\alpha\rangle$
$U_\alpha|d\rangle$ p=1-(1/2)^N
$U_\alpha^{\dagger 2^N-1}|d\rangle$ p=(1/2)^N

FIG. 3. Stochastic programmable quantum gate with a N-qubit program register and success probability $p = 1 - (1/2)^N$, i.e., $\epsilon = (1/2)^N$. The gate fails only when all the outcomes of a $\{|0\rangle, |1\rangle\}$-basis measurement on the N register qubits are 1.

Finally, taking $\alpha - \alpha' = \pi(1/2)^N$ we get that $p \leq 1 - (1/2)^N$, as we wanted to prove. Thus, once the operation U_α has been encoded in N qubits as $|U_\alpha^N\rangle$, the optimal extraction protocol necessarily fails with probability $\epsilon = (1/2)^N$. However, whether the encoding is also optimal remains an open question for $N > 1$.

Notice that if we want to warrant *a priori* a successful implementation of U_α, infinitely many qubits are required for the program register, as originally stated in [1]. Interestingly enough, the average length of the program required to perform U_α with certainty is, in contrast, very small. Indeed, since with probability $p_1 = 1/2$ the gate of Eq. (5) achieves the goal after using a single-qubit program; with probability $p_2 = 1/4$ a two-qubit program is sufficient; the average length $\langle N\rangle$ of the required program is

$$\langle N\rangle \equiv \sum_{N=1}^{\infty} p_N N = \sum_{N=1}^{\infty} \frac{N}{2^N} = 2. \qquad (15)$$

That is, *on average,* a two-qubit program is sufficient to store and retrieve with certainty any operation U_α.

Let us finally comment on how the storage of operations can be applied in the context of quantum remote control, as introduced by Huelga *et al.* in [7]. Suppose two distant parties, Alice and Bob, try to process some data state $|d\rangle$ of, say, a qubit, according to some unitary operation U. Alice possesses a device able to perform U, whereas Bob has the qubit in state $|d\rangle$. Their goal is that Bob ends up with the processed state $U|d\rangle$. If the internal state of Alice's device cannot be teleported, then the optimal protocol [7] is to use standard teleportation [8] to send the data from Bob to Alice, who will use the device to process it and will teleport it back to Bob. This scheme requires two-way classical communication, and the coexistence in time and space of the data $|d\rangle$ and the device that performs U.

If, alternatively, Alice codifies the operation U in a quantum state using the scheme we have discussed, and then teleports the state to Bob, classical communication only from Alice to Bob is required to achieve quantum remote control. In addition, Bob can receive the codified operation even when the data state $|d\rangle$ is not yet available. The price to be paid, however, is that the scheme succeeds only with some probability. Taking into account that a general SU(2) operation decomposes into three rotations U_α [2], each of these requiring, on average, a two-qubit program, and that teleportation of an equatorial state uses 1 bit of communication and 1 ebit of entanglement [9], we conclude that on average 6 ebits of entanglement and 6 bits of communication from Alice to Bob suffice in order to remotely perform a general $U \in$ SU(2). Whether the same task can be accomplished with less resources remains an open question.

To summarize, we have presented a scheme for storing any unitary operation in a finite number of qubits, in a way that it can be stochastically retrieved at a later time. It would be interesting to know which are the minimal resources needed, per operation, in order to store and retrieve a large amount of them with asymptotic perfection. The results of Dür *et al.* [10] represent a promising first step in this direction.

We thank W. Dür for useful comments. This work was supported by the Austrian Science Foundation (SFB Project No. 11), the Spanish newspaper "La Vanguardia," the Institute for Quantum Information GmbH, and the European Community (HPMF-CT-1999-00200 and EQUIP Project No. IST-1999-11053).

Note added.—After completion of this paper we have learned of Preskill's work [11] on quantum error correction, where essentially the same scheme, but without proof of optimality, was originally discussed.

[1] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[2] Recall that any unitary transformation on a qubit can be obtained by composing three of such rotations and, for instance, two fixed $\pi/2$ rotations along the $\hat{y}$ axis, as in the Euler angles' construction.

[3] Suppose that only $N = 4$ qubits are available to store U_α, and that $\alpha/2\pi = 0.011\,010\,1\ldots$. Then we can store the first four digits, 0110, classically. The gate will read them and perform $U_{\tilde{\alpha}}$, where $\tilde{\alpha}/2\pi = 0.0110$. The error in the fidelity of the resulting output tends to 0 exponentially fast in N.

[4] Given any stochastic programmable gate G_s with success probability p_α for U_α, we can construct another one, G_s', from it with associated probability $p_{\alpha+\alpha_0}$ (and thus with the same average probability) as follows. G_s' consists in first performing $U_{-\alpha_0}$ to the data $|d\rangle$ and then performing G_s with the program $|U_{\alpha+\alpha_0}\rangle$, the probability of success being $p_{\alpha+\alpha_0}$. This program corresponds, therefore, to the program $|U_\alpha'\rangle$ of G_s', with the modified success probability. Therefore we can always choose $p_0 \geq p_\alpha$.

[5] The several-step correction character of our scheme for implementing U_α is inspired in the one used by J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001), to implement a nonlocal unitary operation (see also [11]). In the present context all intermediate measurements and conditional actions can be substituted by a single unitary operation, as described in Figs. 2 and 3. In the text we have presented the several-measurement version for pedagogical reasons.

[6] L. Masanes *et al.* (to be published).

[7] S. F. Huelga, J. A. Vaccaro, A. Chefles, and M. B. Plenio, quant-ph/0005061.

[8] C. Bennett, G. Brassard, C. Crepeau, R. Josza, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[9] See, e.g., H.-K. Lo, Phys. Rev. A **62**, 012313 (2000).

[10] W. Dür and J. I. Cirac, Phys. Rev. A **64**, 012317 (2001).

[11] J. Preskill, quant-ph/9705031, Sect. 7.