Optimal creation of entanglement using a two-qubit gate

B. Kraus and J. I. Cirac
Institute for Theoretical Physics, University of Innsbruck, A-6020 Innsbruck, Austria
(Received 20 November 2000; published 17 May 2001)

We consider a general unitary operator acting on two qubits in a product state. We find the conditions such that the state of the qubits after the action is as entangled as possible. We also consider the possibility of using ancilla qubits to increase the entanglement.

DOI: 10.1103/PhysRevA.63.062309 PACS number(s): 03.67.Hk, 03.65.Ta, 03.65.Ca

I. INTRODUCTION

Entanglement [1,2] is a quantum-mechanical feature that can be employed for computational and communication purposes. During the past few years, a big effort has been made in order to create entanglement in several laboratories [3]. This entanglement can then be used for many fascinating things, such as teleportation [4], quantum cryptography [5], and quantum computation [6]. In some of these experiments, the entanglement is produced by starting out from a product state of two systems (typically qubits) and using some physical process that gives rise to an interaction between them. Such an interaction will be called nonlocal. Thus, one of the relevant problems in this context is to find ways of generating ‘‘as much entanglement as possible’’ for a given experimental setup, i.e., a nonlocal interaction.

The first steps to answer this problem have been given in Refs. [7–9]. In particular, given a nonlocal Hamiltonian, Dür *et al.* have found the optimal way of generating entanglement. It consists of applying some fast local operations *during* the interaction processes in such a way that the rate at which entanglement increases is always maximal. In some situations, however, one cannot apply fast local operations during the process, but rather a fixed quantum gate is given. In this work, we find the states $|\phi\rangle_A$ and $|\psi\rangle_B$ for which the entanglement of $U_{AB}|\phi\rangle_A|\psi\rangle_B$ is maximal, where U_{AB} is an arbitrary unitary operator. Thus, our results give a characterization of two-qubit gates in terms of the entanglement that they can produce. For example, we will determine which are the operators U_{AB} that can create maximally entangled states. While most of our results are concerned with two qubits, we will also show that if we allow them to be initially (locally) entangled with some ancillas, one can obtain more entanglement, at least for certain measures of entanglement.

In general, an arbitrary unitary operator acting on two qubits can be parametrized in terms of 15 coefficients (plus a global phase). Thus, to study the maximum entanglement that can be produced in terms of all these parameters seems a formidable task. However, we will show that one can always decompose $U_{AB}=(U_A\otimes U_B)U_d(V_A\otimes V_B)$, where U_d has a special form that only depends on three parameters and the rest are local unitary operators. This implies that we can restrict ourselves to characterize operators in the form U_d. The use of the magic basis introduced in Ref. [10] will also considerably simplify our derivations.

This paper is divided into five sections. In Sec. II, we introduce our notation and recall some measures of entanglement and their properties. In Sec. III, we show that there exists a decomposition of any two-qubit gate, which allows us to simplify the problem. In Sec. IV, we consider the problem of two qubits. We determine how much entanglement can be produced by a general two-qubit gate acting on a product state. We also find which of those states gives rise to that amount of entanglement. In Sec. V, we discuss the case in which we allow the qubits to be initially entangled with ancillas. We will show that the solution to the problem depends on the measure of entanglement we use to quantify it. We will also give two examples in which this problem can be solved analytically for a particular measure of entanglement.

II. DEFINITIONS AND PROPERTIES OF ENTANGLEMENT MEASURES

The purpose of this section is twofold. On the one hand, we give the definitions and notations that will be used throughout the whole paper. On the other hand, we review some measures of entanglement (for pure states) and some of their properties.

A. Definitions

We consider two partners, Alice and Bob, who possess two quantum systems, *A* and *B*, respectively. These systems will be composed of one or two qubits each. We will express the states of these qubits in terms of the computational basis, $\{|0\rangle,|1\rangle\}$. The Hilbert space of system *A* (*B*) will be denoted by $\mathcal{H}_A$ ($\mathcal{H}_B$), respectively.

Throughout this paper, we use capital Greek letters for joint states of systems *A* and *B* and small letters for states describing either system *A* or system *B*. We denote by $|\Psi^\perp\rangle$ a state that is orthogonal to $|\Psi\rangle$, whereas $|\Psi^*\rangle$ denotes the complex conjugate of $|\Psi\rangle$ in the computational basis. We will denote the Pauli operators by $\sigma_x,\sigma_y,\sigma_z$ and by $\vec{\sigma}=(\sigma_x,\sigma_y,\sigma_z)$. If it is not clear on which system an operator is acting, we specify it with either a subscript or superscript, e.g., $\vec{\sigma}_A$ or σ_x^A.

For two qubits, the Bell basis is defined as follows:

$$|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),\quad |\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle). \tag{1}$$

We also make use of the so-called magic basis [10], which is defined in the same way as the Bell basis except for some global phases. We will denote the elements of this basis by

$$|\Phi_1\rangle=|\Phi^+\rangle, \quad |\Phi_2\rangle=-i|\Phi^-\rangle, \tag{2a}$$

$$|\Phi_3\rangle=|\Psi^-\rangle, \quad |\Phi_4\rangle=-i|\Psi^+\rangle. \tag{2b}$$

The coefficients of a general state in that basis will be typically denoted by μ_k; that is, we write $|\Psi\rangle=\Sigma_k\mu_k|\Phi_k\rangle$. In what follows, $|\Phi\rangle$ denotes a maximally entangled state.

B. Measures of entanglement

We review here some measures of entanglement for pure states. In the first part of the paper, we are going to use the so-called *concurrence* [11], C. It is defined as

$$C(|\Psi\rangle)=|\langle\Psi|\sigma_y\otimes\sigma_y|\Psi^*\rangle|. \tag{3}$$

Writing $|\Psi\rangle$ in the magic basis, we get

$$C(|\Psi\rangle)=\left|\sum_k \mu_k^2\right|. \tag{4}$$

In the second part of the paper, we will use other measures of entanglement, which are better expressed in terms of the Schmidt coefficients. A pure state $|\Psi\rangle$, describing the state of two particles, A and B, each of dimension m, always has a Schmidt decomposition in the form

$$|\Psi\rangle=\sum_{k=1}^{m} c_k|\phi_k\rangle_A|\psi_k\rangle_B, \tag{5}$$

where $\langle\phi_k|\phi_l\rangle=\langle\psi_k|\psi_l\rangle=\delta_{kl}\ \forall\ k,\ l=1,\ldots,m$. The real and positive coefficients c_k, which are the square roots of the eigenvalues of the reduced density operator, $\rho_A=\mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$ [or $\rho_B=\mathrm{tr}_A(|\Psi\rangle\langle\Psi|)$], are called Schmidt coefficients. We will choose them in decreasing order, i.e., $c_1\geqslant c_2\geqslant\cdots\geqslant c_m$.

The *entropy of entanglement* is defined as follows:

$$E_E(|\Psi\rangle)\equiv S(\rho_A)=-\mathrm{tr}[\rho_A\log_2(\rho_A)]=-\sum_{k=1}^{m} c_k^2\log_2(c_k^2). \tag{6}$$

This measure has a well-defined meaning: given n copies of a state $|\Psi\rangle$, one can then produce, using only local operations and classical communication, $nE_E(|\Psi\rangle)$ maximally entangled states and vice versa (in the limit $n\to\infty$).

Another useful measure is the *Schmidt number* [12], which we will denote by E_S. It is the number of Schmidt coefficients that are different than zero, minus one.

There is another set of measures, the so-called *entanglement monotones*, which arises in the context of allowed modification of entangled states under local operations [13]. They are defined as

$$E_n(|\Psi\rangle)=\sum_{k=n}^{m} c_k^2 \tag{7}$$

for $n=1,\ldots,m-1$.

We will also use the so-called 2-entropy (related to the 2-Rènyi entropy) of the reduced density operator [14]. It is defined as

$$E_R(|\Psi\rangle)\equiv S_R(\rho_A)=1-\mathrm{tr}(\rho_A^2)=1-\sum_{k=1}^{m} c_k^4, \tag{8}$$

where again ρ_A denotes the reduced density operator of $|\Psi\rangle\langle\Psi|$, and c_k denotes the Schmidt coefficients of $|\Psi\rangle$. In the following, we will call this measure the *Rènyi entanglement*.

C. Properties

A state describing two qubits contains two Schmidt coefficients at most, c_1,c_2, where $c_2=\sqrt{1-c_1^2}$. Thus, its entanglement is completely determined by one parameter, c_1. All the measures of entanglement are monotonic functions of each other and, therefore, equivalent. In higher dimensions (m-level systems), though, this is no longer true. Let us denote now by $|\Psi\rangle$ and $|\Psi'\rangle$ two states describing two m-level systems. Then it might happen that for some measure $|\Psi\rangle$ is more entangled than $|\Psi'\rangle$, whereas for some other measure it is the other way around.

Let us briefly recall some of the properties that have to be satisfied by any measure of entanglement, E [15].

(a) Monotonicity under local operations: Suppose that Alice makes a measurement on her qubit and she obtains with probability p_k the state σ_k. Then the entanglement cannot increase on average, i.e.,

$$E(\rho)\geqslant\sum_k p_kE(\sigma_k). \tag{9}$$

(b) Convexity: The entanglement decreases if we discard some information, i.e.,

$$E\left[\sum_k p_k\rho_k\right]\leqslant\sum_k p_kE(\rho_k). \tag{10}$$

Now we briefly summarize some useful properties of the particular measures of entanglement mentioned in the preceding subsection. Let us start with the properties of the concurrence, C, assuming that we have the following two qubits.

(i) $C(|\Psi\rangle)=1$ iff $\mu_k^2=e^{i\delta}|\mu_k|^2$ $(k=1,\ldots,4)$. This means that a state, written in the magic basis, is maximally entangled iff its coefficients are real, except for a global phase.

(ii) $C(|\Psi\rangle)=0$ iff $|\Psi\rangle$ is a product state iff $\Sigma_k\mu_k^2=0$.

These two properties imply that if $|\Phi\rangle$ and $|\Phi^\perp\rangle$ are real in the magic basis (and therefore they are maximally entangled), then the state $|\Phi\rangle\pm i|\Phi^\perp\rangle$ is a product state.

Let us also review some properties of the entropy of entanglement, E_E, the Schmidt number, E_S, the entanglement monotones, E_n, and the Rènyi entanglement, E_R, for arbitrary states of two m-level systems.

(1) A maximally entangled state, $|\Psi\rangle$, of two m-level systems has m Schmidt coefficients, which are all $1/\sqrt{m}$. Thus $E_E(|\Psi\rangle)=\log_2(m)$, $E_S(|\Psi\rangle)=m-1$, $E_n(|\Psi\rangle)=(m-n)/m$ $(n=1,\ldots,m-1)$ and $E_R(|\Psi\rangle)=1-1/m$.

(2) A product state can be written as $|\Psi\rangle=|\phi\rangle_A|\psi\rangle_B$, thus it has only one Schmidt coefficient, which is equal to 1. And so $E_E(|\Psi\rangle)=E_S(|\Psi\rangle)=E_n(|\Psi\rangle)=E_R(|\Psi\rangle)=0$ $(n=1,\ldots,m-1)$.

III. UNITARY OPERATIONS

In the next sections, we will calculate the maximum attainable entanglement produced by two-qubit gates. In this section, we consider an arbitrary unitary operator U_{AB} acting on two qubits and derive some properties that will simplify the problem.

In Appendix A, we show that for any unitary operator U_{AB} there exist local unitary operators U_A, U_B, V_A, V_B and a unitary operator U_d such that

$$U_{AB}=U_A\otimes U_B U_d V_A\otimes V_B, \tag{11}$$

where

$$U_d=e^{-i\vec{\sigma_A}^T d\vec{\sigma_B}} \tag{12}$$

and d is a diagonal matrix. Here, $\vec{\sigma_A}^T$ denotes the transpose of $\vec{\sigma_A}$ expressed in the computational basis. We will denote the diagonal elements of d by $\alpha_x, \alpha_y, \alpha_z$. Note that any measure of entanglement is not changed by local unitary operators. Thus the entanglement created by U_{AB} is the same as the one created by $U_d V_A\otimes V_B$. And so the maximal amount of entanglement that can be produced by applying a general unitary, U_{AB}, is the same as the one created by U_d. This means that we have to deal with unitaries that are determined by only three parameters $(\alpha_x,\alpha_y,\alpha_z)$ instead of 15 parameters, which are used in order to describe a general unitary operator acting on two qubits.

Furthermore, in Appendix B we show that when studying the maximum amount of entanglement created by a two-qubit gate, we can restrict ourselves to the case in which

$$\pi/4\geqslant\alpha_x\geqslant\alpha_y\geqslant\alpha_z\geqslant 0. \tag{13}$$

This is due to the fact that the maximal amount of entanglement created by U_d is symmetric around $\pi/4$, and $\pi/2$-periodic in α_x, α_y, and α_z.

It can be easily shown that the operator U_d is diagonal in the magic basis, and therefore we can write

$$U_d=\sum_{k=1}^{4} e^{-i\lambda_k}|\Phi_k\rangle\langle\Phi_k|. \tag{14}$$

The phases λ_k are

$$\begin{aligned}\lambda_1&=\alpha_x-\alpha_y+\alpha_z,\\ \lambda_2&=-\alpha_x+\alpha_y+\alpha_z,\\ \lambda_3&=-\alpha_x-\alpha_y-\alpha_z,\\ \lambda_4&=\alpha_x+\alpha_y-\alpha_z.\end{aligned} \tag{15}$$

IV. TWO QUBITS

In this section, we consider the following scenario. Alice and Bob have one qubit each. They want to entangle them by applying a given unitary operation U_{AB}. Their main goal is to find the best separable (pure [16]) input state that gives as much entanglement as possible. According to our previous discussions, we just have to find which states $|\phi\rangle_A, |\psi\rangle_B$ maximize the concurrence of the output state $U_d|\phi\rangle_A, |\psi\rangle_B$, where U_d is given in Eq. (12) with restrictions (13). We will call these states best input states.

Writing the input and output state in the magic basis with the coefficients w_k and μ_k, respectively, we apply the unitary operator U_d and obtain

$$\sum_k \mu_k|\Phi_k\rangle=U_d(|\phi\rangle_A|\psi\rangle_B)=\sum_k w_k e^{-i\lambda_k}|\Phi_k\rangle. \tag{16}$$

We want to maximize the concurrence of the output state, $C=|\Sigma_k\mu_k^2|$, where we have to make sure that the following conditions are satisfied.

(c1) $\Sigma_k|\mu_k|^2=1$, which is that the output state is normalized. Note that since U_d is unitary, this implies that the input state is normalized.

(c2) $\Sigma_k\mu_k^2 e^{2i\lambda_k}=0$. This condition is due to the fact that the input state is a product state, which can be seen as follows. From Eq. (16), we see that $w_k=\mu_k e^{i\lambda_k}$, and according to Sec. II C (ii) this last one is a product state iff the sum of the coefficients in the magic basis squared vanishes, which implies the above equation.

We can determine the maximum of the concurrence of the output state under the conditions (c1) and (c2) by maximizing C^2 and imposing the above conditions in terms of Lagrange multipliers, i.e., we maximize

$$f(\mu_1\cdots\mu_4)=\sum_{k,l}\mu_k^2(\mu_l^*)^2-2\eta_1\left(\sum_k|\mu_k|^2-1\right)-\eta_2\sum_k\mu_k^2 e^{2i\lambda_k}-\eta_2^*\sum_k(\mu_k^*)^2e^{-2i\lambda_k}, \tag{17}$$

where η_1 is real. We find it convenient to denote $\Sigma_l(\mu_l^*)^2=Ce^{i\gamma}$, $\eta_2=|\eta_2|e^{i\epsilon}$, and $\mu_k=|\mu_k|e^{i\xi_k}$. We obtain

$$\mu_k\sum_l(\mu_l^*)^2=\eta_1\mu_k^*+\eta_2\mu_k e^{2i\lambda_k}\quad\forall\ k. \tag{18}$$

Multiplying Eq. (18) by μ_k, summing over k, and using conditions (c1) and (c2), we find that $\eta_1=C^2$. And so we have, assuming that $C\neq 0$,

$$\mu_k(Ce^{i\gamma}-\eta_2 e^{2i\lambda_k})/C^2=\mu_k^*. \tag{19}$$

One of the solutions to this equation is $\mu_k=0$. To find the others, we write Eq. (19) as

$$\left|1-\frac{|\eta_2|}{C}e^{i(2\lambda_k-\gamma+\epsilon)}\right|=C. \tag{20}$$

Let us distinguish now two cases, namely when η_2 is zero or not.

(i) $\eta_2=0$: From Eq. (20), it follows that $C=1$. Using then Eq. (19), it is easy to see that $e^{2i\xi_k}=e^{-i\gamma}\ \forall\ k$. Thus all the coefficients have the same phase (except for the sign) and therefore the output state is, according to the discussions of Sec. II C, a maximally entangled state. In order to obtain this state by applying U_d to a product state, the conditions (c1) and (c2) still have to be imposed. In Appendix C, we show that those conditions can be fulfilled iff $\alpha_x+\alpha_y\geqslant\pi/4$ and at the same time $\alpha_y+\alpha_z\leqslant\pi/4$. There, we also determine the best input state.

(ii) $\eta_2\neq 0$: In this case, Eq. (20) can have at most two solutions for a fixed value of $|\eta_2|/C$. Thus, in order to fulfill Eq. (18) $\forall\ k$, at least two of the coefficients have to vanish [17]. Let us call the other two μ_k and μ_l. Then, in order to fulfill conditions (c1) and (c2), we have to satisfy $|\mu_k|^2+|\mu_l|^2e^{2i[\lambda_l+\xi_l-(\lambda_k+\xi_k)]}=0$ and the normalization condition. Thus $|\mu_k|=|\mu_l|=1/\sqrt{2}$ and the difference between the two phases ξ_k and ξ_l is $\lambda_l-\lambda_k-\pi/2$. With all that, it is now simple to determine that the largest reachable concurrence is

$$C=\max_{k,l}|\sin(\lambda_k-\lambda_l)|. \tag{21}$$

Except for global phases, the corresponding output state is $1/\sqrt{2}(|\Phi_k\rangle+i|\Phi_l\rangle e^{\lambda_k-\lambda_l})$ and the separable input state, which leads to this maximum, is

$$\frac{1}{\sqrt{2}}(|\Phi_k\rangle+i|\Phi_l\rangle). \tag{22}$$

Note that the input state $(1/\sqrt{2})(|\Phi_k\rangle-i|\Phi_l\rangle)$ [the corresponding output state would then be $(1/\sqrt{2})(|\Phi_k\rangle-i|\Phi_l\rangle e^{\lambda_k-\lambda_l})$] leads to the same amount of entanglement.

Note that in the case $\alpha_x\leqslant\pi/8$, we obtain that $C=\sin(\alpha_x+\alpha_y)$, which is directly related to the entanglement capability of the Hamiltonian of the form $\sigma_A^T d\sigma_B$ [8]. For higher values of α_x, the result may not be directly related to that quantity.

In summary, in this subsection we have shown that if we apply U_d to a separable input state and calculate the maximum of the concurrence of the output state, then we find the following: If $\alpha_x+\alpha_y\geqslant\pi/4$ and $\alpha_y+\alpha_z\leqslant\pi/4$, then this maximum is equal to 1. Otherwise it is given by Eq. (21). In addition, we determined the best input state in each of those two cases. Note that, since we were dealing with two-qubit states, we could have taken, according to the discussions in Sec. II C, any other measure of entanglement to obtain the same result.

V. USING ANCILLAS

We analyze now whether and how it would be possible to increase the amount of entanglement of the output state with the help of auxiliary systems. So, we consider the situation in which Alice and Bob have two qubits each [18]. Let us denote the auxiliary qubits by A' and B'. We allow input states in which Alice and Bob's qubits are locally entangled, i.e., of the form $|\phi\rangle_{AA'}|\psi\rangle_{BB'}$. Then they apply a nonlocal unitary transformation, U_{AB}, to the qubits A and B. The question is, then, for which $|\phi\rangle_{AA'}$ and $|\psi\rangle_{BB'}$ they are able to reach $\max_{|\phi\rangle_{AA'},|\psi\rangle_{BB'}}E(U_{AB}\otimes\mathbb{1}_{A'B'}|\phi\rangle_{AA'},|\psi\rangle_{BB'})$, where E denotes some measure of entanglement between Alice's two qubits and Bob's two qubits. In what follows, we write again simply $|\phi\rangle$ ($|\psi\rangle$) instead of $|\phi\rangle_{AA'}$ ($|\psi\rangle_{BB'}$). On the other hand, according to Sec. III, we can restrict ourselves to operators U_d of the form (12). For convenience, we will denote the input state in which $|\phi\rangle$ and $|\psi\rangle$ are both maximally entangled as *local maximally entangled*, and the one in which both are product states as a *local product state*.

The main difference from the preceding section is that now the best input states depend on the measure of entanglement. To illustrate this fact, we show in the first subsection that for some measures of entanglement the best input states are the ones in which $|\phi\rangle$ and $|\psi\rangle$ are entangled. On the other hand, there are measures of entanglement for which a local product state is the best input state.

In the second subsection, we show that for some special class of U_d (where d has only one nonvanishing element), the solution to our problem is independent of the measure of entanglement. In particular, we show how much entanglement can be created in this case and what is the best input state. Furthermore, for the class of U_d in which all the diagonal elements of d are the same, we will determine the maximum Rènyi entanglement as well as the best input state according to this measure of entanglement.

A. Dependence on the measure of entanglement

Let us compare the answer to our problem for some of the measures of entanglement that we recalled in Sec. II. According to some numerical examples, we have the following.

(i) Schmidt number: The best local maximally entangled states are always better than the best local product states. This can be easily understood since in the first case the maximum value that E_S can take is 3, whereas in the latter one it can be at most 1. Thus using this measure of entanglement, the ancillas will in general increase the entanglement of the output state.

(ii) Rènyi entanglement: We have checked that for this measure, the best input states are always either local product states or local maximally entangled states. In particular, in the next subsection we will provide analytical results for some particular cases.

(iii) Entanglement monotones: We have verified that there are unitary operators U_d for which local product states are the best input states, whereas for some other values the local maximally entangled states lead to the most entangled output state. But there also exists some U_d for which neither the local product states nor the local maximally entangled states are the best input states.

From these examples, it becomes clear that it does not make much sense to ask for the best input state if one does not specify according to which measure of entanglement.

B. Examples

Before we start with the examples, let us make some general statement about the input state. It can always be written in the Schmidt decomposition as

$$|\phi\rangle_{AA'} = c_a|\phi_0\rangle_A|0\rangle_{A'} + s_a|\phi_0^\perp\rangle_A|1\rangle_{A'}, \tag{23a}$$

$$|\psi\rangle_{BB'} = s_b|\psi_0\rangle_B|0\rangle_{B'} + c_b|\psi_0^\perp\rangle_B|1\rangle_{B'}, \tag{23b}$$

where $c_a^2+s_a^2=c_b^2+s_b^2=1$. This is due to the fact that local unitaries applied to A' and B' do not change the entanglement (and commute with U_d). Let us now treat two cases in which it is possible to determine the best input state for some measures of entanglement. The first one should be viewed as a very simple illustration, whereas the second one is much more involved.

1. Example 1

Let us consider the following simple unitary operator:

$$U_d = e^{-i\alpha S_x} = \cos(\alpha)\mathbb{1} - i\sin(\alpha)\sigma_x\otimes\sigma_x, \tag{24}$$

where $S_x=\sigma_x\otimes\sigma_x$. In this case, it is fairly simple to determine the output state. It has at most two Schmidt coefficients and therefore the state can be viewed as a state describing two qubits. This implies, as discussed in Sec. II C, that all the measures of entanglement are equivalent when calculating the optimal states. We take E_E.

Let us define ρ_1 as the density operator whose off-diagonal elements are zero, whereas the diagonal elements are the same as that of the state ρ. Using the fact that the von Neumann entropy is convex, we have that $S(\rho_1)\geqslant S(\rho)$. Apart from that, since the problem is symmetric under exchanging system (AA') with (BB'), it is easy to verify that the states with $\sigma_x|\phi\rangle\propto|\phi^\perp\rangle$ and $\sigma_x|\psi\rangle\propto|\psi^\perp\rangle$ lead to the most entangled output state. Now, since the states $|\phi\rangle=|1\rangle, |\psi\rangle=|1\rangle$, as well as the states $|\phi\rangle=|\Phi^+\rangle, |\psi\rangle=|\Phi^+\rangle$ fulfill this condition, both a local product state and a local maximally entangled state are the best input states. The maximal entropy of entanglement that can be obtained is then

$$\max E_E = -\cos(\alpha)^2\log_2[\cos(\alpha)^2] - \sin(\alpha)^2\log_2[\sin(\alpha)^2]. \tag{25}$$

2. Example 2

Here we determine the best input state, according to the Rènyi entanglement, corresponding to a unitary of the form

$$U_d = e^{-i\alpha(S_x+S_y+S_z)} = [\cos(\alpha)^3 - i\sin(\alpha)^3]\mathbb{1} - i\sin(\alpha)\cos(\alpha)e^{i\alpha}(S_x+S_y+S_z), \tag{26}$$

where $S_\beta\equiv\sigma_\beta\otimes\sigma_\beta$ $(\beta=x,y,z)$. Here we have used $[S_x,S_y]=[S_x,S_z]=[S_y,S_z]=0$. In Appendix D we show that, according to any measure of entanglement, the best input state can always be written as

$$|\phi\rangle_{AA'} = c_a|0\rangle_A|0\rangle_{A'} + s_a|1\rangle_A|1\rangle_{A'}, \tag{27a}$$

$$|\psi\rangle_{BB'} = s_b|0\rangle_B|0\rangle_{B'} + c_b|1\rangle_B|1\rangle_{B'}, \tag{27b}$$

where $s_a^2+c_a^2=s_b^2+c_b^2=1$.

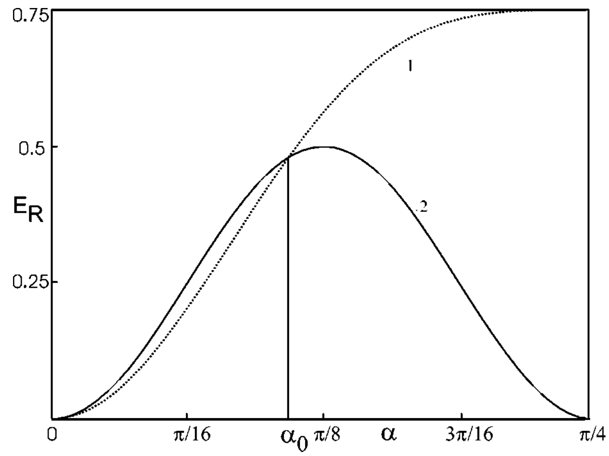

FIG. 1. Rènyi entanglement for the local maximally entangled input state (1) and for the product state $|01\rangle$ (2).

Let us start by proving that the best input state is either a local product state or a local maximally entangled state. Calculating the reduced density operator, one finds that $\rho_A=\rho_1\oplus\rho_2$ [$\mathrm{tr}(\rho_1\rho_2)=0$], where ρ_1,ρ_2 are 2×2 matrices that depend on s_a, s_b, and α. It is straightforward to calculate $E_R(U_d|\phi\rangle|\psi\rangle)=S_R(\rho_A)=S_R(\rho_1)+S_R(\rho_2)$ and determine its maxima. One finds that either the local product states $(s_a^2, s_b^2=0,1)$ or the local maximally entangled states $(s_a^2=s_b^2=\frac{1}{2})$ always lead to a maximum of the Rènyi entanglement. In the case of a local product state, it is easy to check that the best one is $|01\rangle$ (or equivalently $|10\rangle$ [19]). Let us denote by E_R^{me} (E_R^{ps}) the Rènyi entanglement for a local maximally entangled input state (product state $|01\rangle$). We obtain

$$E_R^{\mathrm{me}}(\alpha) = \frac{3}{16}[3 - 2\cos(4\alpha) - \cos(4\alpha)^2], \tag{28a}$$

$$E_R^{\mathrm{ps}}(\alpha) = \frac{1}{2}[1 - \cos(4\alpha)^2]. \tag{28b}$$

Comparing those two expressions, we find that $\forall\ \alpha<\alpha_0$, where $\alpha_0=\arccos(1/5)/4\approx0.109\pi$, the local product state is the best input state, and otherwise the local maximally entangled state leads to the output state with the largest Rènyi entanglement. In Fig. 1, we illustrate this result.

VI. CONCLUSIONS

We have shown which separable pure two-qubit states have to be used in order to create as much entanglement as possible by applying a general two-qubit gate. We have shown which unitary operators are able to create a maximally entangled state. For all the other unitary operators, we have given the maximal amount of entanglement that can be created by them [Eq. (21)]. Furthermore, we have shown that by using ancillas one has to specify which is the measure of entanglement to be maximized. We have given two examples of unitary operations for which it is possible to determine the maximal amount of some particular measure of entanglement.

Note added in proof. Recently, J. Pachos informed us that the result of Appendix A has been independently derived by N. Khaneja and S. J. Glaser (Ref. [20]).

ACKNOWLEDGMENTS

We would like to thank Wolfgang Dür, Guifre Vidal, and, especially, Maciek Lewenstein for fruitful discussions. This work has been supported by the Austrian Science Foundation (SFB ''control and measurement of coherent quantum systems''), the ESF PESC Programm on Quantum Information, TMR network ERB-FMRX-CT96-0087, the IST Program EQUIP, and the Institute for Quantum Information GmbH.

APPENDIX A: DECOMPOSITION OF UNITARY OPERATORS

In this appendix, we show that for any unitary operator U_{AB} acting on two qubits, there exist local unitary operators U_A, U_B, V_A, V_B and a nonlocal unitary $U_d = e^{-i\sigma_A^T d \sigma_B}$ (d diagonal) such that

$$U_{AB} = U_A \otimes U_B U_d V_A \otimes V_B. \tag{A1}$$

Our proof will be constructive. Let us call a basis consisting of maximally entangled orthonormal states a maximally entangled basis. In what follows, the use of the subscript k implies that the definition or statement is true for $k = 1, \ldots, 4$ if not stated differently.

Lemma 1. For any maximally entangled basis $\{|\Psi_k\rangle\}$, there exist phases ζ_k and local unitaries U_A, U_B such that

$$U_A \otimes U_B e^{i\zeta_k} |\Psi_k\rangle = |\Phi_k\rangle. \tag{A2}$$

Proof. According to the discussion in Sec. II C (i), we can always write $|\Psi_k\rangle = e^{\gamma_k} |\overline{\Psi}_k\rangle$, where $|\overline{\Psi}_k\rangle$ is real in the magic basis. Let us consider two different states $|\overline{\Psi}_k\rangle$ and $|\overline{\Psi}_l\rangle$. Then $1/\sqrt{2}(|\overline{\Psi}_k\rangle - i|\overline{\Psi}_l\rangle) = |e,f\rangle$ and $1/\sqrt{2}(|\overline{\Psi}_k\rangle + i|\overline{\Psi}_l\rangle) = |\tilde{e},\tilde{f}\rangle$, where $|e\rangle, |\tilde{e}\rangle \in \mathcal{H}_A$ and $|f\rangle, |\tilde{f}\rangle \in \mathcal{H}_B$. Note that $|e,f\rangle$ must be orthogonal to $|\tilde{e},\tilde{f}\rangle$. This immediately implies that these vectors must give the Schmidt decomposition of both $|\overline{\Psi}_{k,l}\rangle$. Thus we can write

$$|\overline{\Psi}_1\rangle = \frac{1}{\sqrt{2}}(|e,f\rangle + |e^\perp, f^\perp\rangle), \tag{A3a}$$

$$|\overline{\Psi}_2\rangle = \frac{-i}{\sqrt{2}}(|e,f\rangle - |e^\perp, f^\perp\rangle). \tag{A3b}$$

Using the same arguments for $|\overline{\Psi}_{3,4}\rangle$, it is easy to determine that they can be written as

$$|\overline{\Psi}_3\rangle = \frac{-i}{\sqrt{2}}(e^{i\delta}|e, f^\perp\rangle + e^{-i\delta}|e^\perp, f\rangle), \tag{A4a}$$

$$|\overline{\Psi}_4\rangle = \pm\frac{1}{\sqrt{2}}(e^{i\delta}|e, f^\perp\rangle - e^{-i\delta}|e^\perp, f\rangle) \tag{A4b}$$

for some δ. In this case, choosing

$$U_A = |0\rangle\langle e| + |1\rangle\langle e^\perp| e^{i\delta}, \tag{A5a}$$

$$U_B = |0\rangle\langle f| + |1\rangle\langle f^\perp| e^{-i\delta}, \tag{A5b}$$

and the phases ζ_k appropriately, we have Eq. (A2).

Note that this first lemma implies that one can go from one maximally entangled basis to any other using only local unitaries, if one chooses the global phases appropriately.

Lemma 2. Given a general unitary operator, U, there always exist phases ϵ_k and two maximally entangled bases $\{|\Psi_k\rangle\}$ and $\{|\tilde{\Psi}_k\rangle\}$ such that

$$U|\Psi_k\rangle = e^{i\epsilon_k}|\tilde{\Psi}_k\rangle. \tag{A6}$$

Proof. We give a constructive proof. Let us denote by $\{|\Psi_k\rangle\}$ the eigenstates of $U^T U$, where U^T denotes the transpose of U in the magic basis and $e^{2i\epsilon_k}$ are the corresponding eigenvalues. Note that the eigenvectors of the symmetric operator $U^T U$ are orthonormal and real, except for global phases. Thus, since we are working in the magic basis, they build a maximally entangled basis. Now we define $|\tilde{\Psi}_k\rangle$ as

$$|\tilde{\Psi}_k\rangle \equiv e^{-i\epsilon_k} U |\Psi_k\rangle. \tag{A7}$$

Since the set $\{|\tilde{\Psi}_k\rangle\}$ also forms an orthonormal basis, it remains to prove that its elements are real. In order to show that, let us consider the eigenvalue equation $(U^T U - e^{2i\epsilon_k}\mathbb{1})|\Psi_k\rangle = 0$. Multiplying it by $U^* e^{-i\epsilon_k}$, we get that $(e^{-i\epsilon_k}U - e^{i\epsilon_k}U^*)|\Psi_k\rangle = 0$, which is true iff $e^{-i\epsilon_k}U|\Psi_k\rangle$ is real.

With all that, we are now in the position to show that any unitary operator can be decomposed into local operators and U_d as in Eq. (A1). So let us now give the procedure to determine the unitary operators that appear there.

(i) Calculate the eigensystem of the unitary, symmetric operator $U^T U$. Let us denote the eigenvalues by $e^{2i\epsilon_k}$ and the eigenstates by $|\Psi_k\rangle$. As proven in lemma 2, the set of those states is a maximally entangled basis.

(ii) Choose V_A, V_B and the phases ξ_k, as explained in lemma 1, such that

$$V_A \otimes V_B e^{i\xi_k}|\Psi_k\rangle = |\Phi_k\rangle. \tag{A8}$$

(iii) Calculate

$$|\tilde{\Psi}_k\rangle = e^{-i\epsilon_k} U |\Psi_k\rangle. \tag{A9}$$

Note that according to lemma 2, the set of those states is also a maximally entangled basis.

(iv) Choose the eigenvalues of U_d, $e^{i\lambda_k}$ (note that this is equivalent to choosing the diagonal elements of d) and the unitary operators U_A, U_B such that

$$U_A^\dagger \otimes U_B^\dagger e^{i(\lambda_k+\xi_k+\epsilon_k)}|\tilde{\Psi}_k\rangle = |\Phi_k\rangle, \tag{A10}$$

which, according to lemma 1, is always possible. It is simple to check that with these definitions we obtain the decomposition (A1).

APPENDIX B: PERIODICITY AND SYMMETRY OF THE MAXIMAL AMOUNT OF ENTANGLEMENT

Let us start out by proving the periodicity of the entanglement created by U_d. We define d (d') as a matrix whose diagonal elements are $\alpha_x, \alpha_y, \alpha_z$ ($\alpha_x+\pi/2, \alpha_y, \alpha_z$), respectively. It is simple to verify that $U_d = -iS_x U_{d'}$. Since S_x is a tensor product of two local unitary operators, the entanglement created by U_d is the same as the one created by $U_{d'}$. The same argumentation holds for α_y and α_z, and therefore the amount of entanglement created by U_d is $\pi/2$ periodic in α_x, α_y, and α_z.

To prove the symmetry around $\pi/4$ in $\alpha_x, \alpha_y, \alpha_z$ of the maximal amount of entanglement, we use the following definition: d (d') is a matrix whose diagonal elements are $\pi/4 + \alpha_x, \alpha_y, \alpha_z$ ($\pi/4 - \alpha_x, \alpha_y, \alpha_z$). It is straightforward to show that $U_d = -i\sigma_x^A U_{d'}^* \sigma_x^B$, where $U_{d'}^*$ denotes the complex conjugate of $U_{d'}$ in the standard basis. And so we have that $E(U_d|\Psi\rangle) = E(U_{d'}^* \sigma_x^B|\Psi\rangle)$, where we used the fact that local unitary operators do not change the entanglement. Now, we use the fact that for any measure of entanglement, E, $E(|\Psi\rangle) = E(|\Psi^*\rangle)$. This is obvious, since all the measures are determined by the Schmidt coefficients and they are real. Thus, we have that $E(U_d|\Psi\rangle) = E(U_{d'}(\sigma_x^B|\Psi\rangle)^*)$. It is clear that the maximal amount of entanglement created by U_d is the same as the one created by $U_{d'}$. Again the same argumentation holds for the other angles, which proves the statement.

APPENDIX C: TWO-QUBIT GATES THAT CREATE MAXIMALLY ENTANGLED STATES

We are going to prove here that there exists a normalized product state $|\phi\rangle|\psi\rangle$ such that $|\Phi\rangle = U_d|\phi\rangle|\psi\rangle$ is a maximally entangled state iff $\alpha_x+\alpha_y \geqslant \pi/4$ and $\alpha_y+\alpha_z \leqslant \pi/4$. According to our discussions in Sec. II C and Sec. IV, this is equivalent to fulfilling the conditions (c1) and (c2), where $\mu_k^2 = |\mu_k|^2 e^{-i\gamma}$. Multiplying condition (c2) by $e^{-i(\gamma+2\lambda_3)}$, we obtain

$$|\mu_3|^2 + |\mu_1|^2 e^{i\alpha_2} + |\mu_2|^2 e^{i\alpha_3} + |\mu_4|^2 e^{i\alpha_1} = 0, \tag{C1}$$

where we have defined $\alpha_1 = 4(\alpha_x+\alpha_y)$, $\alpha_2 = 4(\alpha_x+\alpha_z)$, and $\alpha_3 = 4(\alpha_y+\alpha_z)$. Note that since $\pi/4 \geqslant \alpha_x \geqslant \alpha_y \geqslant \alpha_z \geqslant 0$, we have that $2\pi \geqslant \alpha_1 \geqslant \alpha_2 \geqslant \alpha_3 \geqslant 0$.

Let us distinguish the following two cases now.

(i) $\alpha_1 < \pi$ (or $\alpha_3 > \pi$). In this case, all the imaginary parts appearing in Eq. (C1) are positive (negative) and therefore the sum can never vanish.

(ii) $\alpha_1 \geqslant \pi$ and $\alpha_3 \leqslant \pi$. Here the imaginary part of $|\mu_4|^2 e^{i\alpha_1}$ is negative, whereas that of $|\mu_2|^2 e^{i\alpha_3}$ is positive, and therefore it is always possible to find a solution to Eq. (C1). In particular, we can choose $\mu_1 = 0$. Then writing the real and imaginary part of Eq. (C1) and the normalization condition (c1), we simply have to solve

$$\sin(\alpha_3)|\mu_2|^2 + \sin(\alpha_1)|\mu_4|^2 = 0, \tag{C2}$$

$$|\mu_3|^2 + \cos(\alpha_3)|\mu_2|^2 + \cos(\alpha_1)|\mu_4|^2 = 0, \tag{C3}$$

$$|\mu_2|^2 + |\mu_3|^2 + |\mu_4|^2 = 1. \tag{C4}$$

Note that since we have found the solution for the μ_k's, it is easy to determine the input state by using the formula $w_k = \mu_k e^{i\lambda_k}$.

APPENDIX D: BEST INPUT STATE FOR EXAMPLE 2

Here we prove that the input state that leads to the most entangled output state can be written as

$$|\phi\rangle = c_a|00\rangle + s_a|11\rangle, \tag{D1a}$$

$$|\psi\rangle = s_b|00\rangle + c_b|11\rangle, \tag{D1b}$$

where $s_a^2 + c_a^2 = s_b^2 + c_b^2 = 1$. We will use that $[\sigma_{\vec{n}}^A \otimes \sigma_{\vec{n}}^B, U_d] = 0$, where $\sigma_{\vec{n}} = \vec{\sigma}\cdot\vec{n}$. This can be easily verified using the commutation relations of the Pauli operators.

Let us now recall that the input state in system AA' can be written as $|\phi\rangle = c_a|\phi_0\rangle_A|0\rangle_{A'} + s_a|\phi_0^\perp\rangle_A|1\rangle_{A'}$, where $c_a^2 + s_a^2 = 1$. It is clear that there exists a vector $\vec{n}$ such that $\sigma_{\vec{n}}|\phi_0\rangle = |\phi_0\rangle$ and $\sigma_{\vec{n}}|\phi_0^\perp\rangle = -|\phi_0^\perp\rangle$. Note that $|\phi\rangle$ is invariant under $\sigma_{\vec{n}}^A \otimes \sigma_z^{A'}$, i.e.,

$$\sigma_{\vec{n}}^A \otimes \sigma_z^{A'}|\phi\rangle = |\phi\rangle. \tag{D2}$$

Using the fact that U_d commutes with $\sigma_{\vec{n}}^A \otimes \sigma_{\vec{n}}^B$ and with local operators acting on the auxiliary systems together with Eq. (D2), we have that $\sigma_{\vec{n}}^A \otimes \sigma_z^{A'} \otimes \sigma_{\vec{n}}^B \otimes V_{B'} U_d|\phi\rangle|\psi\rangle = U_d|\phi\rangle \sigma_{\vec{n}}^B \otimes V_{B'}|\psi\rangle$ for any unitary operator $V_{B'}$.

Let us now introduce a new auxiliary system, which we denote by C. Then, using the property (a) of any measure of entanglement, E, we have that

$$E(U_{AB}|\phi\rangle_{AA'}|\tilde{\psi}\rangle_{BB'C}) \geqslant E(U_{AB}|\phi\rangle_{AA'}|\psi\rangle_{BB'}), \tag{D3}$$

where

$$|\tilde{\psi}\rangle_{BB'C} = (1/\sqrt{2})(|\psi\rangle_{BB'}|0\rangle_C + \sigma_{\vec{n}}^B \otimes V_{B'}|\psi\rangle_{BB'}|1\rangle_C). \tag{D4}$$

Now choosing $V_{B'} = \sigma_z^{B'}$ and requiring that $\sigma_{\vec{n}}^B \otimes V_{B'}|\psi\rangle_{BB'} = |\psi\rangle_{BB'}$, which implies that $|\psi\rangle = s_b|\phi_0 0\rangle + c_b|\phi_0^\perp 1\rangle$, we get that $E(U_{AB}|\phi\rangle_{AA'}|\psi\rangle_{BB'}) \geqslant E(U_{AB}|\tilde{\phi}\rangle_{AA'}|\tilde{\psi}\rangle_{BB'})$, $\forall |\tilde{\phi}\rangle, |\tilde{\psi}\rangle$, where both $|\phi\rangle$ and $|\psi\rangle$ are invariant under the operation $\sigma_{\vec{n}} \otimes \sigma_z$. Using the same argumentation as before, we can apply the local operator $\sigma_{\vec{n}'} \otimes \sigma_{\vec{n}'}$, where $\vec{n}'$ is defined as $\sigma_{\vec{n}'}|\phi_0\rangle = |0\rangle$ and $\sigma_{\vec{n}'}|\phi_0^{\perp}\rangle = -|1\rangle$. Combining all that, we have that

$$E(U_{AB}|\phi\rangle|\psi\rangle) \leq E\{U_{AB}[(c_a|00\rangle + s_a|11\rangle)(s_b|00\rangle + c_b|11\rangle)]\}, \quad \text{(D5)}$$

$\forall\ |\phi\rangle, |\psi\rangle$.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935).

[3] See, for example, the special issue of Fortsch. Phys. **48**, 767 (2000), and references therein; see also C. A. Sackett *et al.*, Nature (London) **404**, 256 (2000); A. Rauschenbeutel *et al.*, Science **288**, 2024 (2000).

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

[5] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] See A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996); A. Steane, Rep. Prog. Phys. **61**, 117 (1998); A. Barenco, Contemp. Phys. **37**, 375 (1996); A. Ekert, P. Hayden, and Hitoshi Inamori, e-print quant-ph/0011013.

[7] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (2000); P. Zanardi, e-print quant-ph/0010074.

[8] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, e-print quant-ph/0006034.

[9] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).

[10] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[11] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[12] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1993).

[13] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999); M. A. Nielsen, *ibid.* **83**, 436 (1999).

[14] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996), and references therein.

[15] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).

[16] Note that the maximum entanglement reached for pure states is always larger than the one reached by a mixed state. This can be seen as follows: let us write an arbitrary mixed state ρ in its eigenbasis, i.e., $\rho = \Sigma_k p_k |\Psi_k\rangle\langle\Psi_k|$. Using the convexity of any measure of entanglement, E, [Eq. (10)], we have that $E(\rho) \leq \max_{|\Psi_k\rangle} E(|\Psi_k\rangle)$. Thus it suffices to consider only pure states.

[17] Note that if two or more λ's are equal, this does not need to be necessary. However, we can discard this case since it has zero measure in the set of unitary operators, and obtain this result by imposing continuity.

[18] Note that since one of Alice's and Bob's subsystems (the one on which they apply the unitary operator) is a qubit, the state describing such a subsystem and an ancilla of arbitrary dimension can always be viewed as a state describing two qubits (it has at most two Schmidt coefficients).

[19] Note that, due to the symmetry of the problem, the entanglement produced by the input state $|01\rangle$ has to be the same as the one produced by $|10\rangle$.

[20] N. Khaneja and S. J. Glaser, e-print quant-ph/0010100.