Quantum Information Processing, Vol. 1, No. 4, August 2002 (© 2003)

Nonlocal Properties of Two-Qubit Gates and Mixed States, and the Optimization of Quantum Computations

Yuriy Makhlin[1]

Received April 30, 2002; accepted July 6, 2002

Entanglement of two parts of a quantum system is a nonlocal property unaffected by local manipulations of these parts. It can be described by quantities invariant under local unitary transformations. Here we present, for a system of two qubits, a set of invariants which provides a complete *description of nonlocal properties. The set contains 18 real polynomials of the entries of the density matrix. We prove that one of two* ***mixed states*** *can be transformed into the other by single-qubit operations if and only if these states have equal values of all 18 invariants. Corresponding local operations can be found efficiently. Without any of these 18 invariants the set is incomplete. Similarly, nonlocal, entangling properties of two-qubit* ***unitary gates*** *are invariant under single-qubit operations. We present a* complete *set of 3 real polynomial invariants of unitary gates. Our results are useful for optimization of quantum computations since they provide an effective tool to verify if and how a given two-qubit operation can be performed using exactly one elementary two-qubit gate, implemented by a basic physical manipulation (and arbitrarily many single-qubit gates).*

KEY WORDS: quantum information; entanglement; invariants; nonlocality.

PACS: 03.67-a; 03.67.Lx.

1. INTRODUCTION

Nonlocality is an important ingredient in quantum information processing, e.g., in quantum computation and quantum communication. Nonlocal correlations in quantum systems reflect entanglement between its parts. Genuine nonlocal properties should be described in a form invariant under

---

[1] Institut für Theoretische Festkörperphysik, Universität Karlsruhe, D-76128 Karlsruhe, Germany and Landau Institute for Theoretical Physics, Kosygin st. 2, 117940 Moscow, Russia. E-mail: makhlin@tfp.physik.uni-karlsruhe.de

local unitary operations. In this paper we discuss such locally invariant properties of (i) unitary transformations and (ii) mixed states of a two-qubit system.

Two 2-qubit unitary transformations (logic gates), M and $L \in SU(4)$, are called locally equivalent if they differ only by local operations: $L = U_1 M U_2$, where $U_1, U_2 \in SU(2)^{\times 2}$ are combinations of single-qubit gates on two qubits.(1) A property of a two-qubit operation can be considered nonlocal only if it has the same value for locally equivalent gates. We present a complete set of local invariants of a two-qubit gate: two gates are equivalent if and only if they have equal values of all these invariants. The set contains three real polynomials of the entries of the gate's matrix ($\mathrm{Re}\, G_1$, $\mathrm{Im}\, G_1$, and G_2 from Table 2, cf. Eq. (2)). This set is minimal: the group $SU(4)$ of two-qubit gates is 15-dimensional and local operations eliminate at most $2 \dim[SU(2)^{\times 2}] = 12$ degrees of freedom; hence any set should contain at least $15 - 12 = 3$ invariants.

This result can be used to optimize quantum computations. Quantum algorithms are built out of elementary quantum logic gates. Any many-qubit quantum logic circuit can be constructed out of single-qubit and two-qubit operations.(2–5) The ability to perform 1-qubit and 2-qubit operations is a requirement to any physical realization of quantum computers. Barenco *et al.*(5) showed that the controlled-not (CNOT) gate together with single-qubit gates is sufficient for quantum computations. Furthermore, it is easy to prove that *any* two-qubit gate M forms a universal set with single-qubit gates, if M itself is not a combination of single-qubit operations and the SWAP-gate, which interchanges the states of two qubits. The efficiency of such a universal set, that is the number of operations from the set needed to build a certain quantum algorithm, depends on M.

For a particular realization of quantum computers, a certain two-qubit operation M (or a set $\exp[i\mathcal{H}t]$ of operations generated by a certain Hamiltonian) is usually considered elementary. It can be performed by a basic physical manipulation (switching of one parameter or application of a pulse). Then the question of optimization arises: what is the most economical way to perform a particular computation, i.e., what is the minimal number of elementary steps? In many situations two-qubit gates are more costly than single-qubit gates (e.g., they can take a longer time, involve complicated manipulations or stronger additional decoherence), and then only the number of two-qubit gates counts.

The simplest and important version of this question is how a given two-qubit gate L can be performed using the minimal number of elementary two-qubit gates M. In particular, when is it sufficient to employ M only once?(6) This is the case when the two gates are locally equivalent, and computation of invariants gives an effective tool to verify this. Moreover, if M and L are equivalent, a procedure presented below allows to find efficiently single-qubit gates U_1, U_2, which in combination with M produce L. If one elementary two-qubit step is not sufficient, one can ask how many are needed. Counting of dimensions suggests that two steps always suffice: indeed, for single-qubit gates U_i the combination $U_1MU_2MU_3$ has $3 \times 6 = 18$ free parameters and, in principle, may span the whole 15-dimensional group $SU(4)$ of 2-qubit gates. Still, often it does not: if M is a bad entangler, e.g., is close to $\hat{1}$ (or *any* single-qubit gate), then $U_1MU_2MU_3$ is also close to a single-qubit gate for any U_i's and cannot represent a good entangler, e.g., CNOT, which is distant from single-qubit operations.

A related problem is that of local invariants of quantum states. A mixed state is described by a density matrix $\hat{\rho}$. Two states are called locally equivalent if one can be transformed into the other by local operations: $\hat{\rho} \to U^\dagger \hat{\rho} U$, where U is a local gate. Apparently, the coefficients of the characteristic polynomials of $\hat{\rho}$ and of the reduced density matrices of two qubits are locally invariant. The method developed in Refs. 7 and 8, in principle, allows to compute all invariants.

Clearly, each invariant has equal values for equivalent states. A useful tool for verification of local equivalence of two states is a *complete* set of invariants that distinguishes all inequivalent states: if each invariant from the set has equal values on two states ρ_1, ρ_2, their local equivalence is guaranteed. Further, the smaller this set is, the easier it is to verify equivalence. For a two-qubit system there are nine functionally independent invariants which suffice to find out if two *generic* states are locally equivalent or not, but additional invariants may be needed to resolve a remaining finite number of states, and a set of 10 invariants was suggested for this purpose.(9) In Ref. 8, a set of 20 invariants was presented. However it was not clear if this set was complete.

Here we present a *complete* set of 18 polynomial invariants, which extends the aforementioned set of 10 invariants(11) (see Table 1 and Eq. (3)). We prove that two states are locally equivalent if and only if all 18 invariants have equal values in these states. Hence, any nonlocal characteristic of entanglement is a function of these invariants.(10) We also show that no subset of this set is complete.

To demonstrate applications of our results, we discuss in the last section which 2-qubit operations can be constructed out of only one elementary 2-qubit gate for Josephson charge qubits(12,13) or for qubits based on spin degrees of freedom in quantum dots.(14)

2. SINGLE-QUBIT GATES AS ORTHOGONAL MATRICES

The following result is used below to classify two-qubit gates.

Theorem 1. Single-qubit gates with unit determinant are represented by real orthogonal matrices in the Bell basis $1/\sqrt{2}(|00\rangle + |11\rangle)$, $i/\sqrt{2}(|01\rangle + |10\rangle)$, $1/\sqrt{2}(|01\rangle - |10\rangle)$, $i/\sqrt{2}(|00\rangle - |11\rangle)$.

The transformation of a matrix M from the standard basis of states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ into the Bell basis is described as $M \to M_B = Q^\dagger M Q$, where

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix} \tag{1}$$

Proof. We introduce a measure of entanglement in a pure 2-qubit state $\psi_{\alpha\beta}$, a quadratic form Ent ψ, which in the standard basis is defined as $\operatorname{Ent}\psi = \det\hat{\psi} = \psi_{00}\psi_{11} - \psi_{01}\psi_{10}$. This quantity is locally invariant. Indeed, a single-qubit gate $W_1 \otimes W_2$ transforms $\hat{\psi}$ into $W_1\hat{\psi}W_2^T$, preserving the determinant.

Under a unitary operation V the matrix of this form transforms as $\widehat{\mathrm{Ent}} \to V^T \widehat{\mathrm{Ent}}\, V$. In the Bell basis it is proportional to the identity matrix. Since local gates preserve this form, they are given by orthogonal matrices in this basis. As unitary and orthogonal they are also real. Thus local operations form a subgroup of the group $SO(4, \mathbf{R})$ of real orthogonal matrices. This subgroup is 6-dimensional, and hence coincides with the group. □

3. CLASSIFICATION OF TWO-QUBIT GATES

Our result for unitary gates is expressed in terms of M_B.

Theorem 2. The complete set of local invariants of a two-qubit gate M, with $\det M = 1$, is given by the set of eigenvalues of the matrix $M_B^T M_B$.

In other words, two 2-qubit gates with unit determinants, M and L, are equivalent up to single-qubit operations iff the spectra of $M_B^T M_B$ and $L_B^T L_B$ coincide. Since $m \equiv M_B^T M_B$ is unitary, its eigenvalues have absolute value 1 and are bound by $\det m = 1$. For such matrices the spectrum is completely described by a complex number $\operatorname{tr} m$ and a real number $\operatorname{tr}^2 m - \operatorname{tr} m^2$.

The matrix m is unitary and symmetric. The following statement is used in the proof of Theorem 2:

Lemma. Any unitary symmetric matrix m has a real orthogonal eigenbasis.

Proof. Any eigenbasis of m can be converted into a real orthogonal one, as seen from the following observation: If $\mathbf{v}$ is an eigenvector of m with eigenvalue λ then $\mathbf{v}^*$ is also an eigenvector with the same eigenvalue (conjugation of $m^*\mathbf{v} = m^{-1}\mathbf{v} = \lambda^{-1}\mathbf{v} = \lambda^*\mathbf{v}$ gives this result). Hence, $\mathrm{Re}\,\mathbf{v}$ and $\mathrm{Im}\,\mathbf{v}$ are also eigenvectors. □

Proof of Theorem 2. In the Bell basis local operations transform a unitary gate M_B into $O_1 M_B O_2$, where $O_1, O_2 \in SO(4, \mathbf{R})$ are orthogonal matrices. Therefore $m = M_B^T M_B$ is transformed to $O_2^T m O_2$. Obviously, the spectrum of m is invariant under this transformation.

To prove completeness of the set of invariants, we notice that the lemma above implies that m can be diagonalized by an orthogonal rotation O_M, i.e., $m = O_M^T d_M O_M$ where d_M is a diagonal matrix. Suppose that another gate L is given, and $l \equiv L_B^T L_B$ has the same spectrum as m. Then the entries of d_M and d_L are related by a permutation. Hence $d_M = P^T d_L P$, where P is an orthogonal matrix, which permutes the basis vectors. Using the relation of m to d_M and of l to d_L, we conclude that $l = O^T m O$ where $O \in SO(4, \mathbf{R})$.

Single-qubit operations O and $O' \equiv L_B O^T M_B^{-1}$ transform one gate into the other: $L_B = O' M_B O$. The gate O' is a single-qubit operation since it is real and orthogonal. Indeed, $O'^T O' = (M_B^{-1})^T O L_B^T L_B O^T M_B^{-1} = (M_B^{-1})^T O l O^T M_B^{-1} = (M_B^{-1})^T m M_B^{-1} = \hat{1}$. On the other hand, O' is unitary as a product of unitary matrices. This implicates its reality. □

So far we have discussed equivalence up to single-qubit transformations *with unit determinant*. However, physically unitary gates are defined only up to an overall phase factor. The condition $\det M = 1$ fixes this phase factor but not completely: multiplication by $\pm i$ preserves the determinant. With this in mind, we describe a procedure to verify if two 2-qubit unitary gates with arbitrary determinants are equivalent up to local transformations and an overall phase factor: For each of them we calculate

$$m = M_B^T M_B = Q^T M^T Q^* Q^\dagger M Q \tag{2}$$

and compare the pairs $[\mathrm{tr}^2 m \det M^\dagger;\ \mathrm{tr}\, m^2 \det M^\dagger]$. If they coincide, the gates are equivalent and the proof of Theorem 2 allows to express explicitly one gate via the other and single-qubit gates, O and O'. Clearly, due to the cyclic property of the trace, one can use the matrix $m' \equiv M^T Q^* Q^\dagger M Q Q^T = M^T \widehat{\mathrm{Ent}}\, M\, \widehat{\mathrm{Ent}}^{-1}$ instead of m.

4. CLASSIFICATION OF TWO-QUBIT STATES

In this section we discuss equivalence and invariants of two-qubit states up to local operations. Let us express a 2-qubit density matrix in terms of Pauli matrices acting on the first and the second qubit:

$$\hat{\rho} = \tfrac{1}{4}\hat{1} + \tfrac{1}{2}\mathbf{s}\vec{\sigma}^1 + \tfrac{1}{2}\mathbf{p}\vec{\sigma}^2 + \beta_{ij}\sigma_i^1\sigma_j^2 \tag{3}$$

If the qubits are considered as spin-1/2 particles, then $\mathbf{s}$ and $\mathbf{p}$ are their average spins in the state $\hat{\rho}$, while $\hat{\beta}$ is the spin-spin correlator: $\beta_{ij} = \langle S_i^1 S_j^2 \rangle$. Any single-qubit operation is represented by two corresponding 3×3 orthogonal real matrices of "spin rotations", $O, P \in SO(3, \mathbf{R})$. Such an operation, $O \otimes P$, transforms $\hat{\rho}$ according to the rules: $\mathbf{s} \to O\mathbf{s}$, $\mathbf{p} \to P\mathbf{p}$, and $\hat{\beta} \to O\hat{\beta}P^T$. We find a set of invariants which completely characterize $\hat{\rho}$ up to local gates.

The density matrix is specified by 15 real parameters, while local gates form a 6-dimensional group. Thus we expect $15 - 6 = 9$ functionally independent invariants (I_1–I_9 in Table I). However, these invariants fix a state only up to a finite symmetry group, and additional invariants are needed.(8) In Table I we present a set of 18 polynomial invariants and prove that the set is complete.

Theorem 3. Two states are locally equivalent exactly when the invariants I_1–I_{18} have equal values for these states. (Only signs of I_{10}, I_{11}, I_{15-18} are needed.)

None of the invariants can be removed from the set without affecting completeness, as demonstrated by examples in the table.

The proof below gives an explicit procedure to find single-qubit gates which transform one of two equivalent states into the other.

Proof. It is clear that all I_i in the table are invariant under independent orthogonal rotations O, P, i.e., under single-qubit gates. To prove that they form a complete set, we show that for given values of the invariants one can by local operations transform any density matrix with these invariants to a specific form. In the course of the proof we fix more and more details of the density matrix by applying local gates (this preserves the invariants).

The first step is to diagonalize the matrix $\hat{\beta}$, which can be achieved by proper rotations O, P (singular value decomposition). The invariants I_1–I_3 determine the diagonal entries of $\hat{\beta}$ up to a simultaneous sign change for any two of them. Using single-qubit operations $R^i \otimes \hat{1}$ (where R^i is the π-rotation about the axis $i = 1, 2, 3$) we can fix these signs: all three eigenvalues, b_1, b_2, b_3, can be made nonnegative, if $I_1 = \det \hat{\beta} \geq 0$, or negative, if $\det \hat{\beta} < 0$. Further transformations, with $O = P$ representing permutations of basis vectors, place them in any needed order. From now on we consider only states with a fixed diagonal $\hat{\beta}$. Hence, only such single-qubit gates, $O \otimes P$, are allowed which preserve $\hat{\beta}$. The group of such operations depends

Table I. The Complete Set of Invariants of a Two-Qubit State[a]

$I_{1,2,3}$	$\det\hat{\beta},\ \mathrm{tr}(\hat{\beta}^T\hat{\beta}),\ \mathrm{tr}(\hat{\beta}^T\hat{\beta})^2$	0	0
$I_{4,5,6}$	$\mathbf{s}^2,\ [\mathbf{s}\hat{\beta}]^2,\ [\mathbf{s}\hat{\beta}\hat{\beta}^T]^2$	$\mathbf{s}$	0
$I_{7,8,9}$	$\mathbf{p}^2,\ [\hat{\beta}\mathbf{p}]^2,\ \hat{\beta}^T\hat{\beta}\mathbf{p}]^2$	0	$\mathbf{p}$
I_{10}	$(\mathbf{s},\ \mathbf{s}\hat{\beta}\hat{\beta}^T,\ \mathbf{s}[\hat{\beta}\hat{\beta}^T]^2)$	$(1;1;\pm 1)$	0
I_{11}	$(\mathbf{p},\ \hat{\beta}^T\hat{\beta}\mathbf{p},\ [\hat{\beta}^T\hat{\beta}]^2\mathbf{p})$	0	$(1;1;\pm 1)$
I_{12}	$\mathbf{s}\hat{\beta}\mathbf{p}$	$(1;\pm b_1^3;0)$	$(\mp b_2^3;1;0)$
I_{13}	$\mathbf{s}\hat{\beta}\hat{\beta}^T\hat{\beta}\mathbf{p}$	$(1;\pm b_1;0)$	$(\mp b_2;1;0)$
I_{14}	$e_{ijk}e_{lmn}s_ip_l\beta_{jm}\beta_{kn}$	$(0;0;1)$	$(0;0;\pm 1)$
I_{15}	$(\mathbf{s},\ \mathbf{s}\hat{\beta}\hat{\beta}^T,\ \hat{\beta}\mathbf{p})$	$(0;1;1)$	$(\pm 1;0;0)$
I_{16}	$(\mathbf{s}\hat{\beta},\ \mathbf{p},\ \hat{\beta}^T\hat{\beta}\mathbf{p})$	$(\pm 1;0;0)$	$(0;1;1)$
I_{17}	$(\mathbf{s}\hat{\beta},\ \mathbf{s}\hat{\beta}\hat{\beta}^T\hat{\beta},\ \mathbf{p})$	$(1;1;0)$	$(0;0;\pm 1)$
I_{18}	$(\mathbf{s},\ \hat{\beta}\mathbf{p},\ \hat{\beta}\hat{\beta}^T\hat{\beta}\mathbf{p})$	$(0;0;\pm 1)$	$(1;1;0)$

[a] Here $(\mathbf{a},\mathbf{b},\mathbf{c})$ stands for the triple scalar product $\mathbf{a}\cdot(\mathbf{b}\times\mathbf{c})$, and e_{ijk} is the Levi–Cevita symbol; $\mathbf{s}\hat{\beta}$ is a 3-vector with components $s_j\beta_{ji}$, etc. The last two columns present, for each invariant, $\mathbf{s},\mathbf{p}$ in a situation when only this invariant distinguishes between two nonequivalent states. In these examples we assume a nondegenerate $\hat{\beta}$, with $b_3 = 0$ for I_{12-18}.

on b_1, b_2, b_3. We examine all possibilities below, showing that the invariants I_{4-18} fix the state completely.

(A) $\hat{\beta}$ is nondegenerate: all b_i are different. Then the only $\hat{\beta}$-preserving local gates are $r^i \equiv R^i \otimes R^i$.

The invariants I_{4-6} and I_{7-9} set absolute values of six components s_i, p_i, but not their signs. The signs are bound by other invariants. In particular, I_{10} and I_{11} fix the values of $s_1s_2s_3$ and $p_1p_2p_3$. Furthermore, I_{12-14} give three linear constraints on three quantities s_ip_i. When $\hat{\beta}$ is not degenerate, one can solve them for s_ip_i. Let us consider several cases:

(i) $\mathbf{s}$ has at least two nonzero components, say s_1, s_2. These two can be made positive by single-qubit gates r^1, r^2. After that, the signs of $p_{i=1,2}$ are fixed by values of s_ip_i, while I_{10} fixes the sign of s_3. The sign of p_3 can be determined from s_3p_3, if $s_3 \neq 0$; if $s_3 = 0$ then p_3 is fixed by $I_{15} = p_3s_1s_2b_3(b_2^2 - b_1^2)$ or $I_{17} = p_3s_1s_2b_1b_2(b_2^2 - b_1^2)$.

If $\mathbf{p}$ has at least two nonzero components, a similar argument applies, with $I_{11,16,18}$ instead of $I_{10,15,17}$. If both $\mathbf{s}$ and $\mathbf{p}$ have at most one nonzero component, s_i and p_j, then either (ii) $i = j$, and the signs are specified by s_ip_i up to $\hat{\beta}$-preserving gates r^k; or (iii) $i \neq j$, and one can use r^i, r^j to make both components nonnegative.

(B) $\hat{\beta}$ has two equal nonzero eigenvalues: $b_3 \neq b_1 = b_2 \neq 0$. We define horizontal components $\mathbf{s}_\perp = (s_1, s_2, 0)$, $\mathbf{p}_\perp = (p_1, p_2, 0)$. Then $\hat{\beta}$-preserving operations are generated by simultaneous, coinciding rotations of $\mathbf{s}_\perp$ and $\mathbf{p}_\perp$ [i.e., $\mathbf{s}_\perp \to O\mathbf{s}_\perp$, $\mathbf{p}_\perp \to O\mathbf{p}_\perp$, where $O \in SO_{1,2}(2)$ is a 2D-rotation], as well as r^i.

The invariants I_{4-9} fix $\mathbf{s}_\perp^2$, s_3^2, $\mathbf{p}_\perp^2$ and p_3^2. To specify $\mathbf{s}$ and $\mathbf{p}$ completely the angle between $\mathbf{s}_\perp$ and $\mathbf{p}_\perp$, as well as the signs of s_3 and p_3 should be determined. These are bound by the remaining invariants. In particular, I_{12-14} fix s_3p_3 and $\mathbf{s}_\perp\mathbf{p}_\perp$. The latter sets the angle between $\mathbf{s}_\perp$ and $\mathbf{p}_\perp$ up to a sign.

There are two possibilities: (i) $s_3 = p_3 = 0$. The states with opposite angles are related by r^1 and hence equivalent. (ii) $s_3 \neq 0$ (the case $p_3 \neq 0$ is analogous). Applying r^1, if needed, we can assume that s_3 is positive. Then, p_3 is specified by the value of s_3p_3. Apart from that, I_{15} sets $(\mathbf{s}_\perp \times \mathbf{p}_\perp)_3 s_3$, and hence the sign of the cross product $\mathbf{s}_\perp \times \mathbf{p}_\perp$. This fixes the density matrix completely.

(C) $b_1 = b_2 = 0$, $b_3 \neq 0$. In this case $\hat{\beta}$-preserving operations are independent rotations of $\mathbf{s}_\perp$ and $\mathbf{p}_\perp$ [which form $SO_{1,2}(2)^{\times 2}$] and r^i. The invariants I_{4-9} fix $\mathbf{s}_\perp^2$, s_3^2, $\mathbf{p}_\perp^2$, and p_3^2, while I_{12} (or I_{13}) sets s_3p_3. It is easy to see that they specify the state completely.

(D) $b_1 = b_2 = b_3 \neq 0$. All transformations $O \otimes O$, where $O \in SO(3)$, preserve $\hat{\beta}$. The invariants I_4, I_7, and I_{12} fix $\mathbf{s}^2$, $\mathbf{p}^2$, and $\mathbf{sp}$, and this information is sufficient to determine $\mathbf{s}$ and $\mathbf{p}$ up to a rotation.

(E) $\hat{\beta} = 0$. In this case all local transformations preserve $\hat{\beta}$; hence, $\mathbf{s}$ and $\mathbf{p}$ can rotate independently. The only nonzero invariants, I_4 and I_7, fix $\mathbf{s}^2$ and $\mathbf{p}^2$. □

5. DISCUSSION

In this section we demonstrate applications of our results. We calculate the invariants for several two-qubit gates to find out which of them are locally equivalent. These gates include CNOT, SWAP and its square root, as well as several gates $\exp(i\mathcal{H}t)$ generated by Hamiltonians $\frac{1}{4}\vec{\sigma}^1\vec{\sigma}^2$, $\frac{1}{4}\vec{\sigma}^1_\perp\vec{\sigma}^2_\perp$ [here $\vec{\sigma}_\perp = (\sigma_x; \sigma_y)$] and $\frac{1}{4}\sigma^1_y\sigma^2_y$ (cf. Refs. 6, 13 and 14) after evolution during time t. Analyzing the invariants we see that to achieve CNOT one needs to perform a two-qubit gate at least twice if the latter is triggered by the Heisenberg Hamiltonian $\vec{\sigma}\vec{\sigma}$. At the same time SWAP and $\sqrt{\mathrm{SWAP}}$ can be performed with one elementary two-qubit gate.(6) The Ising coupling $\sigma_y\sigma_y$ allows to perform CNOT in one step, while the XY interaction $\vec{\sigma}_\perp\vec{\sigma}_\perp$ requires at least two steps for all three gates. The results are summarized in Table II.

In Josephson qubits(13) elementary two-qubit gates are generated by the interaction $\mathcal{H} = -\frac{1}{2}E_J(\hat{\sigma}^1_x + \hat{\sigma}^2_x) + (E_J^2/E_L)\hat{\sigma}^1_y\hat{\sigma}^2_y$. Investigation of the

Table II. Invariants of Two-Qubit Gates, $G_1 = \mathrm{tr}^2\, m \det M^\dagger/16$ and $G_2 = (\mathrm{tr}^2\, m - \mathrm{tr}\, m^2)\det M^\dagger/4$. The Latter Is Always a Real Number. Numerical Prefactors Are Chosen to Simplify Expressions in the Table

	Identity	CNOT	SWAP	$\sqrt{\mathrm{SWAP}}$
G_1	1	0	-1	$i/4$
G_2	3	1	-3	0
$\mathcal{H}$	$\vec{\sigma}^1\vec{\sigma}^2$	$\vec{\sigma}^1_\perp\vec{\sigma}^2_\perp$	$\sigma^1_y\sigma^2_y$	
G_1	$\frac{1}{16}e^{it}(3+e^{-2it})^2$	$\cos^4(t/2)$	$\cos^2(t/2)$	
G_2	$3\cos t$	$1+2\cos t$	$2+\cos t$	

invariants shows that CNOT can be performed if E_J is tuned to αE_L for a finite time $t = \alpha\pi(2n+1)/4E_L$, where n is an integer and α satisfies $\alpha^2\cos[\pi(n+\frac{1}{2})\sqrt{1+\alpha^{-2}}] = -1$.

For creation of entanglement between qubits a useful property of a two-qubit gate is its ability to produce a maximally entangled state (with $|\,\mathrm{Ent}\,\psi| = 1/2$) from an unentangled one.(6) This property is locally invariant and one can show that a gate M is a perfect entangler exactly when the convex hull of the eigenvalues of the corresponding matrix m contains zero. In terms of the invariants, introduced in Table 2, this condition reads: $\sin^2\gamma \le 4|G_1| \le 1$ and $\cos\gamma(\cos\gamma - G_2) \ge 0$, where $G_1 = |G_1|e^{i\gamma}$. Among the gates in the table CNOT and $\sqrt{\mathrm{SWAP}}$ are perfect entanglers. The Heisenberg Hamiltonian can produce only two perfect entanglers ($\sqrt{\mathrm{SWAP}}$ or its inverse), while $\sigma_y\sigma_y$—only CNOT. At the same time, the XY coupling $\vec{\sigma}_\perp\vec{\sigma}_\perp$ produces a set of perfect entanglers if the system evolves for time t with $\cos t \le 0$.

To conclude, we have presented complete sets of local polynomial invariants of two-qubit gates (3 real invariants) and two-qubit mixed states (18 invariants) and demonstrated how these results can be used to optimize quantum logic circuits and to study entangling properties of unitary operations.

ACKNOWLEDGMENTS

I am grateful to G. Burkard, D. P. DiVincenzo, M. Grassl, G. Schön, and A. Shnirman for fruitful discussions and to the Humboldt Foundation, the BMBF and the German Government for financial support.

REFERENCES

1. The subgroup $SU(2)^{\times 2}$ of single-qubit operations in $SU(4)$ consists of operators $u \otimes v$, where u acts only on the first and v on the second qubit.
2. D. P. DiVincenzo, *Phys. Rev. A* **51**, 1015 (1995).
3. S. Lloyd, *Phys. Rev. Lett.* **75**, 346 (1995).
4. D. Deutsch, A. Barenco, and A. Ekert, *Proc. R. Soc. Lond. A* **449**, 669 (1995).
5. A. Barenco *et al.*, *Phys. Rev. A* **52**, 3457 (1995).
6. G. Burkard, D. Loss, D. P. DiVincenzo, and J. A. Smolin, *Phys. Rev. B* **60**, 11404 (1999).
7. E. M. Rains, preprint, (1997), quant-ph/9704042.
8. M. Grassl, M. Rötteler, and T. Beth, *Phys. Rev. A* **58**, 1833 (1998).
9. N. Linden, S. Popescu, and A. Sudbery, *Phys. Rev. Lett.* **83**, 243 (1999); see also N. Linden and S. Popescu, *Fortsch. Phys.* **46**, 567 (1998).
10. This function can be non-polynomial. For instance, the values of the invariants $I_{19} = (\mathbf{s}, \mathbf{s}\hat{\beta}\hat{\beta}^T, \hat{\beta}\hat{\beta}^T\hat{\beta}\mathbf{p})$ and $I_{20} = (\mathbf{p}, \hat{\beta}^T\hat{\beta}\mathbf{p}, \mathbf{s}\hat{\beta}\hat{\beta}^T\hat{\beta})$ are completely determined by I_{1-18} but are not polynomial functions of them. As shown by M. Grassl (private communication), I_{1-20} generate the same polynomial ring as invariants from Ref. 8.
11. Ten invariants from Ref. 9 are I_{1-6}, I_{12}, I_{13} and a polynomial of these and I_{14}. Hence this set is incomplete (cf. examples in Table 1).
12. A. Shnirman, G. Schön, and Z. Hermon, *Phys. Rev. Lett.* **79**, 2371 (1997).
13. Yu. Makhlin, G. Schön, and A. Shnirman, *Nature* **386**, 305 (1999).
14. D. Loss and D. P. DiVincenzo, *Phys. Rev. A* **57**, 120 (1998).