Geometric theory of nonlocal two-qubit operations

Jun Zhang,[1] Jiri Vala,[2,3] Shankar Sastry,[1] and K. Birgitta Whaley[2,3]
[1]*Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, California 94720*
[2]*Department of Chemistry and Pitzer Center for Theoretical Chemistry, University of California, Berkeley, California 94720*
[3]*Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, California 94720*
(Received 21 September 2002; published 18 April 2003)

We study nonlocal two-qubit operations from a geometric perspective. By applying a Cartan decomposition to su(4), we find that the geometric structure of nonlocal gates is a 3-torus. We derive the invariants for local transformations, and connect these local invariants to the coordinates of the 3-torus. Since different points on the 3-torus may correspond to the same local equivalence class, we use the Weyl group theory to reduce the symmetry. We show that the local equivalence classes of two-qubit gates are in one-to-one correspondence with the points in a tetrahedron except on the base. We then study the properties of perfect entanglers, that is, the two-qubit operations that can generate maximally entangled states from some initially separable states. We provide criteria to determine whether a given two-qubit gate is a perfect entangler and establish a geometric description of perfect entanglers by making use of the tetrahedral representation of nonlocal gates. We find that exactly half the nonlocal gates are perfect entanglers. We also investigate the nonlocal operations generated by a given Hamiltonian. We first study the gates that can be directly generated by a Hamiltonian. Then we explicitly construct a quantum circuit that contains at most three nonlocal gates generated by a two-body interaction Hamiltonian, together with at most four local gates generated by single-qubit terms. We prove that such a quantum circuit can simulate any arbitrary two-qubit gate exactly, and hence it provides an efficient implementation of universal quantum computation and simulation.

DOI: 10.1103/PhysRevA.67.042313 PACS number(s): 03.67.Lx, 03.65.Fd, 03.65.Ta, 89.70.+c

I. INTRODUCTION

Considerable effort has been made on the characterization of nonlocal properties of quantum states and operations. Grassl *et al.* [1] have computed locally invariant polynomial functions of density matrix elements. Makhlin [2] has recently analyzed nonlocal properties of two-qubit gates and presented local invariants for an operation $M \in \mathrm{U}(4)$. Makhlin also studied some basic properties of perfect entanglers, which are defined as the unitary operations that can generate maximal entangled states from some initially separable states. Also shown were entangling properties of gates generated by several different Hamiltonian operators. All these results are crucial for physical implementations of quantum computation schemes.

Determining the entangling capabilities of operations generated by a given physical system is another intriguing and complementary issue. Zanardi [3,4] has explored the entangling power of quantum evolutions. The most extensive recent effort to characterize entangling operations is due to Cirac and co-workers [5–12]. Kraus and Cirac [8] focused on finding the best separable two-qubit input states such that some given unitary transformation can create maximal entanglement. Vidal, Hammerer, and Cirac [9] developed the interaction cost for a nonlocal operation as the optimal time to generate it from a given Hamiltonian. The same group, Hammerer, Vidal, and Cirac [12] then extended these considerations to characterize nonlocal gates. These works are closely related to time optimal control as addressed recently by Khaneja, Brockett, and Glaser [13], who studied systems described by a Hamiltonian that contains both a nonlocal internal or drift term, and a local control term. All these studies assume that any single-qubit operation can be achieved almost instantaneously. This is a good approximation for the situation when the control terms in the Hamiltonian can be made large compared to the internal couplings.

Universality and controllability are issues of crucial importance in physical implementations of quantum information processing [14,15]. A series of important results have been obtained since questions of universality were first addressed by Deutsch in his seminal papers on quantum computing [16,17]. Deutsch [17] proved that any unitary operation can be constructed from generalized Toffoli gate operating on three qubits. DiVincenzo [18] proved universality for two-qubit gates by reconstructing three-qubit operations using these gates and a local NOT gate. Similarly, Barenco [19,20] and Sleator and Weinfurter [21] identified the controlled unitary operation as a universal two-qubit gate. Barenco [22] showed the universality of the controlled-NOT (CNOT) gate supplemented with any single-qubit unitaries, and pointed out advantages of CNOT in the context of quantum information processing. Lloyd [23] showed that almost any quantum gate for two or more qubits is universal. Deutsch *et al.* [24] proved that almost any two-qubit gate is universal by showing that the set of nonuniversal operations in U(4) is of lower dimension than the U(4) group. Universal properties of quantum gates acting on an $n \geqslant 2$ dimensional Hilbert space have been studied by Brylinski [25]. Dodd *et al.* [26] have pointed out that universal quantum computation can be achieved by any entangling gate supplemented with local operations. Bremner *et al.* [27] recently demonstrated this by extending the results of Brylinski, giving a constructive proof that any two-qubit entangling gate can generate CNOT if arbitrary single-qubit operations are also available. Universal sets of quantum gates for *n*-qubit sys-

tems have been explored by Vlasov [28,29] in connection with Clifford algebras.

General results on efficient simulation of any unitary operation in $SU(2^n)$ by a discrete set of gates are embodied in the Solovay-Kitaev theorem [15,30] and in recent work due to Harrow, Recht, and Chuang [31]. The Solovay-Kitaev theorem implies the equivalence of different designs of universal quantum computers based on suitable discrete sets of single-qubit and two-qubit operations in a quantum circuit. An example is the standard universal set of gates including CNOT and three discrete single-qubit gates, namely, Hadamard, phase, and $\pi/2$ gates [15]. Other universal sets have also been proposed. According to the Solovay-Kitaev theorem, every such design can represent a circuit that is formulated using the standard set of gates. Consequently, all quantum computation constructions—including algorithms, error correction, and fault tolerance—can be efficiently simulated by physical systems that can provide a suitable set of operations, and do not necessarily need to be implemented by the standard gates. This moves the focus from the study of gates to study of the Hamiltonians whose time evolution gives rise to the gates. In this context, Burkard *et al.* [32] studied the quantum computation potential of the isotropic exchange Hamiltonian. This interaction can generate $\sqrt{\text{SWAP}}$ gate directly. However, CNOT cannot be obtained directly from the exchange interaction. Burkard *et al.* showed that it can be generated via a circuit of two $\sqrt{\text{SWAP}}$ gates and a single-qubit phase rotation. Bennett *et al.* [33] discussed the optimal simulation of one two-qubit Hamiltonian by using another Hamiltonian and general local operations. More recently, Whaley and co-workers have shown that the two-particle exchange interaction is universal when physical qubits are encoded into logical qubits, allowing a universal gate set to be constructed from this interaction alone [34–39]. This has given rise to the notion of ''encoded universality,'' in which a convenient physical interaction is made universal by encoding into a subspace [36,37]. Isotropic, anisotropic, and generalized forms of the exchange interaction have recently been shown to possess considerable power for efficient construction of universal gate sets, allowing explicit universal gate constructions that require only a small number of physical operations [35,38–40].

In this paper, we analyze nonlocal two-qubit operations from a geometric perspective and show that considerable insight can be achieved with this approach. We are concerned with three main questions here. First, achieving a geometric representation of two-qubit gates. Second, characterizing or quantifying all operations that can generate maximal entanglement. Third, exact simulation of any arbitrary two-qubit gates from a given two-body physical interaction together with single-qubit gates. The fundamental mathematical techniques in this paper are Cartan decomposition and Weyl group in the Lie group representation theory. The application of these theories to the Lie algebra su(4) provides us with a natural and intuitive geometric approach to investigate the properties of nonlocal two-qubit operations. This geometric approach reveals the nature of the problems intrinsically and allows a general formulation of solutions to the three issues of interest here.

Because it is the nonlocal properties that generate entanglement in quantum systems, we first study the invariants and geometric representation of nonlocal two-qubit operations. A pair of two-qubit operations are called locally equivalent if they differ only by local operations. We apply the Cartan decomposition theorem to su(4), the Lie algebra of the special unitary group SU(4). We find that the geometric structure of nonlocal gates is a 3-torus. On the other hand, the Cartan decomposition of su(4) derived from the complexification of sl(4) yields an easy way to derive the invariants for local transformations. These invariants can be used to determine whether two gates are locally equivalent. Moreover, we establish the relation of these local invariants to the coordinates of the 3-torus. This provides with a way to compute the corresponding points on the 3-torus for a given gate. It turns out that a single nonlocal gate may correspond to finitely many different points on the 3-torus. If we represent these points in a cube with side length π, there is an obvious symmetry between these points. We then use the Weyl group theory to reduce this symmetry. We know that in this case the Weyl group is generated by a set of reflections in $\mathbb{R}^3$. It is these reflections that create the kaleidoscopic symmetry of points that correspond to the same nonlocal gate in the cube. We can explicitly compute these reflections, and thereby show that the local equivalence classes of two-qubit gates are in one-to-one correspondence with the points in a tetrahedron except on the base. This provides a complete geometric representation of nonlocal two-qubit operations.

The second objective of this paper is to explore the properties of perfect entanglers, that is, the quantum gates that can generate maximally entangled states from some initially separable states. We start with criteria to determine whether a given two-qubit gate is a perfect entangler. A condition for such a gate has been stated in Ref. [2]. We provide here a proof of this condition and show that the condition can be employed within our geometric analysis to determine which fraction of all nonlocal two-qubit gates are perfect entanglers. We show that the entangling property of a quantum gate is only determined by its geometric representation on the 3-torus. Using the result that every point on the tetrahedron corresponds to a local equivalence class, we then show that the set of all perfect entanglers is a polyhedron with seven faces and possessing a volume equal to exactly half that of the tetrahedron. This implies that amongst all the nonlocal two-qubit operations, exactly half of them are capable of generating maximal entanglement.

Finally, we explore universality and controllability aspects of nonlocal properties of given physical interactions and the potential of such specified Hamiltonians to generate perfect entanglers. Our motivation is related to that of encoded universality, namely, determining the potential for universal quantum computation and simulation of a given physical Hamiltonian. However, whereas encoded universality sought to construct encodings to achieve universality of quantum logic, here we focus on the simulation of any arbitrary two-qubit gate. Achievement of this, together with our second result above, allows generation of maximal entanglement as well as providing universality. To realize this, we consider

here the conventional scenario of a Hamiltonian acting on a physical set of qubits such that any arbitrary single-qubit operation and certain specific two-qubit operations may be turned on for selected time durations in series. Generally speaking, two-qubit interactions include both local and nonlocal terms. The nonlocal terms can give rise to not only well-known entangling gates such as CNOT, but also to many other classes of gates that may or may not lie in the perfect entangling sector. We therefore, seek a systematic way to construct quantum circuits from a given physical Hamiltonian that can simulate *any* arbitrary two-qubit gate exactly. As in the study of encoded universality we start with the gates that can be directly generated by a given Hamiltonian. Generally, these gates form a one-dimensional subset on the 3-torus. To construct an exact simulation of any arbitrary two-qubit gate, we make use of the quantum circuit model. We explicitly construct a quantum circuit that contains three nonlocal gates generated by a given two-body interaction Hamiltonian for corresponding finite time durations, together with at most four local gates. We prove that such a quantum circuit can simulate *any* arbitrary two-qubit operation exactly and is therefore universal. In particular, it can therefore *efficiently* provide maximal entanglement from any arbitrary Hamiltonian of this form. Such efficient construction from any given Hamiltonian is extremely useful for design and experimental implementation of quantum information processing schemes.

II. PRELIMINARIES

In this section, we briefly review some basic facts about Cartan decomposition and the Weyl group within the Lie group representation theory [42–45], and then apply these results to su(4), the Lie algebra of the special unitary group SU(4). Applications of Cartan decomposition to quantum system control can also be found in Ref. [13].

We concentrate on SU(4) when studying two-qubit gates. It is well-known that an arbitrary two-qubit gate $U_0 \in \mathrm{U}(4)$ can be decomposed as the product of a gate $U_1 \in \mathrm{SU}(4)$ and a global phase shift $e^{i\alpha}$, where $\alpha \in \mathbb{R}$. Because the global phase has no significance in quantum mechanics, we can thereby reduce the study of the group U(4) of two-qubit quantum evolution operators to SU(4). Extensions of results from the group SU(4) back to U(4) are made when appropriate.

We heuristically introduce a partition of the set of two-qubit operations represented by the group SU(4). This set splits into two subsets, one of local gates $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ and the other of nonlocal gates $\mathrm{SU}(4)\backslash\mathrm{SU}(2)\otimes\mathrm{SU}(2)$. The latter splits further into a set of perfect entanglers, i.e., those that can generate maximally entangled states, an example of which is CNOT, and the complementary set of those nonlocal gates that are not perfect entanglers. This schematic partition is illustrated in Fig. 1. A rigorous definition of perfect entanglers is presented in Sec. IV.

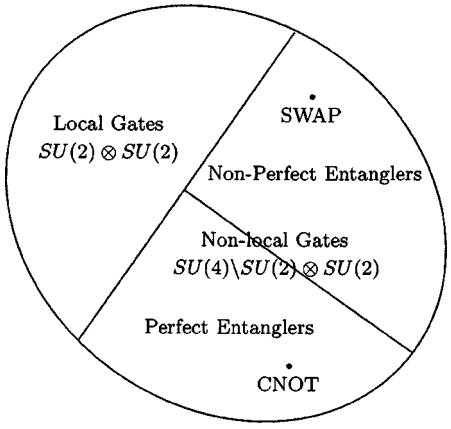


FIG. 1. Partition of all the gates in SU(4).

A. The Cartan decomposition and the Weyl group

Our first goal is to establish fundamentals for a geometric picture of nonlocal unitary operations with emphasis on their generators, which are represented by the Hamiltonian operators in physical context. We start with a summary of some basic definitions [42–45]. Consider a Lie group G and its corresponding Lie algebra $\mathfrak{g}$. The adjoint representation Ad_g is a map from the Lie algebra $\mathfrak{g}$ to $\mathfrak{g}$ which is the differential of the conjugation map a_g from the Lie group G to G given by $a_g(h)=ghg^{-1}$. For matrix Lie algebras, $\mathrm{Ad}_g(Y)=gYg^{-1}$, where g, Y are both represented as matrices of compatible dimensions. The differential of the adjoint representation is denoted by ad, and ad_X is a map from the Lie algebra $\mathfrak{g}$ to $\mathfrak{g}$ given by the Lie bracket with X, that is, $\mathrm{ad}_X(Y)=[X,Y]$.

We now define an inner product on $\mathfrak{g}$ by the Killing form $B(X,Y)=\mathrm{tr}(\mathrm{ad}_X\mathrm{ad}_Y)$. Let $\{X_1,\ldots,X_n\}$ be a basis for $\mathfrak{g}$. The numbers $C^i_{jk}\in\mathbb{C}$ such that

$$[X_j,X_k]=\sum_{i=1}^{n} C^i_{jk}X_i \tag{1}$$

are the *structure constants* of the Lie algebra $\mathfrak{g}$ with respect to the basis, where j, k run from 1 to n. Since

$$\begin{aligned}\mathrm{ad}_{X_j}[X_1,\ldots,X_n]&=\left[\sum_{i=1}^{n} C^i_{j1}X_i,\ldots,\sum_{i=1}^{n} C^i_{jn}X_i\right]\\&=[X_1,\cdots,X_n]\begin{bmatrix} C^1_{j1} & \cdots & C^1_{jn}\\ \vdots & & \vdots\\ C^n_{j1} & \cdots & C^n_{jn}\end{bmatrix},\end{aligned} \tag{2}$$

the matrix representation of ad_{X_j} with respect to the basis is

$$\begin{bmatrix} C^1_{j1} & \cdots & C^1_{jn}\\ \vdots & & \vdots\\ C^n_{j1} & \cdots & C^n_{jn}\end{bmatrix}. \tag{3}$$

Thus, the trace of $\mathrm{ad}_{X_j}\mathrm{ad}_{X_k}$, which is $B(X_j,X_k)$, is $\Sigma_{a,b=1}^{n} C_{jb}^{a}C_{ka}^{b}$, which is also the jkth entry of the matrix of the quadratic form $B(,)$. The Lie algebra $\mathfrak{g}$ is semisimple if and only if the Killing form is nondegenerate, i.e., the determinant of its matrix is nonzero.

Let K be a compact subgroup of G, and $\mathfrak{k}$ be the Lie algebra of K. Assume that $\mathfrak{g}$ admits a direct sum decomposition $\mathfrak{g}=\mathfrak{p}\oplus\mathfrak{k}$, such that $\mathfrak{p}=\mathfrak{k}^{\perp}$ with respect to the metric induced by the inner product.

Definition 1 (Cartan decomposition of the Lie algebra $\mathfrak{g}$*).* Let $\mathfrak{g}$ be a semisimple Lie algebra and let the decomposition $\mathfrak{g}=\mathfrak{p}\oplus\mathfrak{k}$, $\mathfrak{p}=\mathfrak{k}^{\perp}$ satisfy the commutation relations

$$[\mathfrak{k},\mathfrak{k}]\subset\mathfrak{k},\quad [\mathfrak{p},\mathfrak{k}]\subset\mathfrak{p},\quad [\mathfrak{p},\mathfrak{p}]\subset\mathfrak{k}. \tag{4}$$

This decomposition is called a Cartan decomposition of $\mathfrak{g}$, and the pair $(\mathfrak{g},\mathfrak{k})$ is called an orthogonal symmetric Lie algebra pair.

A maximal Abelian subalgebra $\mathfrak{a}$ contained in $\mathfrak{p}$ is called a *Cartan subalgebra* of the pair $(\mathfrak{g},\mathfrak{k})$. If $\mathfrak{a}'$ is another Cartan subalgebra of $(\mathfrak{g},\mathfrak{k})$, then there exists an element $k\in K$ such that $\mathrm{Ad}_k(\mathfrak{a})=\mathfrak{a}'$. Moreover, we have $\mathfrak{p}=\cup_{k\in K}\mathrm{Ad}_k(\mathfrak{a})$.

Proposition 1 (decomposition of the Lie group G*).* Given a semisimple Lie algebra $\mathfrak{g}$ and its Cartan decomposition $\mathfrak{g}=\mathfrak{p}\oplus\mathfrak{k}$, let $\mathfrak{a}$ be a Cartan subalgebra of the pair $(\mathfrak{g},\mathfrak{k})$, then $G=K\exp(\mathfrak{a})K$.

For $X\in\mathfrak{a}$, let $W\in\mathfrak{g}$ be an eigenvector of ad_X and $\alpha(X)$ the corresponding eigenvalue, i.e.,

$$[X,W]=\alpha(X)W. \tag{5}$$

The linear function α is called a *root* of $\mathfrak{g}$ with respect to $\mathfrak{a}$. Let Δ denote the set of nonzero roots, and $\Delta_{\mathfrak{p}}$ denote the set of roots in Δ which do not vanish identically on $\mathfrak{a}$. Note that if $\alpha\in\Delta$, it is also true that $-\alpha\in\Delta$.

Let M and M' denote the centralizer and normalizer of $\mathfrak{a}$ in K, respectively. In other words,

$$M=\{k\in K\,|\,\mathrm{Ad}_k(X)=X \ \text{ for each } X\in\mathfrak{a}\},$$

$$M'=\{k\in K\,|\,\mathrm{Ad}_k(\mathfrak{a})\subset\mathfrak{a}\}. \tag{6}$$

Definition 2 (Weyl group). The quotient group M'/M is called the Weyl group of the pair (G,K). It is denoted by $W(G,K)$.

One can prove that $W(G,K)$ is a finite group. Each $\alpha\in\Delta_{\mathfrak{p}}$ defines a hyperplane $\alpha(X)=0$ in the vector space $\mathfrak{a}$. These hyperplanes divide the space $\mathfrak{a}$ into finitely many connected components, called the *Weyl chambers*. For each $\alpha\in\Delta_{\mathfrak{p}}$, let s_α denote the reflection with respect to the hyperplane $\alpha(X)=0$ in $\mathfrak{a}$.

Proposition 2 (generation of the Weyl group). The Weyl group is generated by the reflections s_α, $\alpha\in\Delta_{\mathfrak{p}}$.

This proposition is proved in Corollary 2.13, Chap. VII in Ref. [42].

B. Application to su(4)

Now we apply the above results to su(4), the Lie algebra of the special unitary group SU(4). The Lie algebra $\mathfrak{g}=\mathrm{su}(4)$ has a direct sum decomposition $\mathfrak{g}=\mathfrak{p}\oplus\mathfrak{k}$, where

$$\mathfrak{k}=\mathrm{span}\,\frac{i}{2}\{\sigma_x^1,\sigma_y^1,\sigma_z^1,\sigma_x^2,\sigma_y^2,\sigma_z^2\},$$

$$\mathfrak{p}=\mathrm{span}\frac{i}{2}\{\sigma_x^1\sigma_x^2,\sigma_x^1\sigma_y^2,\sigma_x^1\sigma_z^2,\sigma_y^1\sigma_x^2,\sigma_y^1\sigma_y^2,\ \sigma_y^1\sigma_z^2,\sigma_z^1\sigma_x^2,\sigma_z^1\sigma_y^2,\sigma_z^1\sigma_z^2\}. \tag{7}$$

Here σ_x, σ_y, and σ_z are the Pauli matrices, and $\sigma_\alpha^1\sigma_\beta^2=\sigma_\alpha\otimes\sigma_\beta$. If we use X_j to denote the matrices in Eq. (7), where j runs from left to right in Eq. (7), we can derive the Lie brackets of X_j and X_k. These are summarized in the following:

$[X_j,\,X_k]$	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}
X_1	0	$-X_3$	X_2	0	0	0	0	0	0	$-X_{13}$	$-X_{14}$	$-X_{15}$	X_{10}	X_{11}	X_{12}
X_2	X_3	0	$-X_1$	0	0	0	X_{13}	X_{14}	X_{15}	0	0	0	$-X_7$	$-X_8$	$-X_9$
X_3	$-X_2$	X_1	0	0	0	0	$-X_{10}$	$-X_{11}$	$-X_{12}$	X_7	X_8	X_9	0	0	0
X_4	0	0	0	0	$-X_6$	X_5	0	$-X_9$	X_8	0	$-X_{12}$	X_{11}	0	$-X_{15}$	X_{14}
X_5	0	0	0	X_6	0	$-X_4$	X_9	0	$-X_7$	X_{12}	0	$-X_{10}$	X_{15}	0	$-X_{13}$
X_6	0	0	0	$-X_5$	X_4	0	$-X_8$	X_7	0	$-X_{11}$	X_{10}	0	$-X_{14}$	X_{13}	0
X_7	0	$-X_{13}$	X_{10}	0	$-X_9$	X_8	0	$-X_6$	X_5	$-X_3$	0	0	X_2	0	0
X_8	0	$-X_{14}$	X_{11}	X_9	0	$-X_7$	X_6	0	$-X_4$	0	$-X_3$	0	0	X_2	0
X_9	0	$-X_{15}$	X_{12}	$-X_8$	X_7	0	$-X_5$	X_4	0	0	0	$-X_3$	0	0	X_2
X_{10}	X_{13}	0	$-X_7$	0	$-X_{12}$	X_{11}	X_3	0	0	0	$-X_6$	X_5	$-X_1$	0	0
X_{11}	X_{14}	0	$-X_8$	X_{12}	0	$-X_{10}$	0	X_3	0	X_6	0	$-X_4$	0	$-X_1$	0
X_{12}	X_{15}	0	$-X_9$	$-X_{11}$	X_{10}	0	0	0	X_3	$-X_5$	X_4	0	0	0	$-X_1$
X_{13}	$-X_{10}$	X_7	0	0	$-X_{15}$	X_{14}	$-X_2$	0	0	X_1	0	0	0	$-X_6$	X_5
X_{14}	$-X_{11}$	X_8	0	X_{15}	0	$-X_{13}$	0	$-X_2$	0	0	X_1	0	X_6	0	$-X_4$
X_{15}	$-X_{12}$	X_9	0	$-X_{14}$	X_{13}	0	0	0	$-X_2$	0	0	X_1	$-X_5$	X_4	0

Now the structure constants C_{jk}^{i} can be found from the above table [see Eq. (1)] so that we can evaluate

$$B(X_j,X_k)=\sum_{a=1}^{15}\sum_{b=1}^{15}C_{jb}^{a}C_{ka}^{b}=-8\,\delta_{jk}. \tag{8}$$

It is easy to verify that $\mathrm{tr}(X_jX_k)=-\delta_{jk}$, and thus the Killing form of su(4) is $B(X,Y)=8\,\mathrm{tr}(XY)$. Since $\mathfrak{k}=\mathrm{span}\{X_1,\ldots,X_6\}$ and $\mathfrak{p}=\mathrm{span}\{X_7,\ldots,X_{15}\}$, from the Lie bracket computation table above, it is clear that

$$[\mathfrak{k},\mathfrak{k}]\subset\mathfrak{k},\quad[\mathfrak{p},\mathfrak{k}]\subset\mathfrak{p},\quad[\mathfrak{p},\mathfrak{p}]\subset\mathfrak{k}. \tag{9}$$

Therefore the decomposition $\mathfrak{g}=\mathfrak{k}\oplus\mathfrak{p}$ is a Cartan decomposition of su(4). Note that the Abelian subalgebra

$$\mathfrak{a}=\mathrm{span}\,\frac{i}{2}\{\sigma_x^1\sigma_x^2,\sigma_y^1\sigma_y^2,\sigma_z^1\sigma_z^2\} \tag{10}$$

is contained in $\mathfrak{p}$ and is a maximal Abelian subalgebra, i.e., we cannot find any other Abelian subalgebra of $\mathfrak{p}$ that contains $\mathfrak{a}$. Hence it is a Cartan subalgebra of the pair $(\mathfrak{g},\mathfrak{k})$. Further, since the set of all the local gates K is a connected Lie subgroup $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ of SU(4), and there is a one-to-one correspondence between connected Lie subgroups of a Lie group and subalgebras of its Lie algebra [45], it is clear that $\mathfrak{k}$ in Eq. (7) is just the Lie subalgebra corresponding to K. From Proposition 1, any $U\in\mathrm{SU}(4)$ can be decomposed as

$$U=k_1Ak_2=k_1\exp\left\{\frac{i}{2}(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)\right\}k_2, \tag{11}$$

where $k_1,\ k_2\in\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, and $c_1,\ c_2,\ c_3\in\mathbb{R}$.

Another more intuitive Cartan decomposition of su(4) can be obtained via the complexification of sl(4). Consider $G=\mathrm{SL}(4)$, the real special linear group, and $K=\mathrm{SO}(4)$, the special orthogonal group. The Lie algebra sl(4) is the set of 4×4 real matrices of trace zero, and so(4) is the set of 4×4 real skew symmetric matrices. Then sl(4) can be decomposed as $\mathrm{sl}(4)=\mathrm{so}(4)\oplus\mathfrak{p}$, where $\mathfrak{p}$ is the set of 4×4 real symmetric matrices. This is nothing but the decomposition of a matrix into symmetric and skew symmetric parts, and it is indeed a Cartan decomposition of sl(4). Consider the following subset of the complexification of sl(4):

$$\mathfrak{g}_\mu=\mathrm{so}(4)+i\mathfrak{p}. \tag{12}$$

It can be verified that $\mathfrak{g}_\mu$ is exactly su(4), and thus $(\mathfrak{g}_\mu,\mathrm{so}(4))$ is an orthogonal symmetric Lie algebra pair. The isomorphism carrying $\mathfrak{k}$ in Eq. (7) into so(4) is just the transformation from the standard computational basis of states to the Bell basis in Refs. [2,12]. This procedure is of crucial importance in computing the invariants for two-qubit gates under local transformations. See Sec. III for more details.

Now let us compute the Weyl group $W(G,K)$. Let $X=i/2(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)\in\mathfrak{a}$. Identify $\mathfrak{a}$ with $\mathbb{R}^3$, then $X=[c_1,c_2,c_3]$. The roots of $\mathfrak{g}$ with respect to $\mathfrak{a}$ are eigenvalues of the matrix of ad_X:

$$\begin{aligned}\Delta_{\mathfrak{p}}=i\{&c_1-c_2,-c_1-c_2,-c_1-c_3,c_1-c_3,c_2-c_3,c_2+c_3,\\&-c_1+c_2,c_1+c_2,c_1+c_3,-c_1+c_3,\\&-c_2+c_3,-c_2-c_3\}.\end{aligned} \tag{13}$$

For $\alpha=i(c_1-c_3)\in\Delta_{\mathfrak{p}}$, the plane $\alpha(X)=0$ in $\mathfrak{a}$ is the set $\{X\in\mathbb{R}^3|u^TX=0\}$, where $u=[1,0,-1]^T$. The reflection of $X=[c_1,c_2,c_3]$ with respect to the plane $\alpha(X)=0$ is

$$s_\alpha(X)=X-\frac{2uu^T}{\|u\|^2}X=[c_3,c_2,c_1]. \tag{14}$$

Similarly, we can compute all the reflections s_α as follows:

$$\begin{aligned}&s_{i(c_3-c_2)}(X)=[c_1,c_3,c_2],\quad s_{i(c_2+c_3)}(X)=[c_1,-c_3,-c_2],\\&s_{i(c_2-c_1)}(X)=[c_2,c_1,c_3],\quad s_{i(c_1+c_2)}(X)=[-c_2,-c_1,c_3],\\&s_{i(c_1-c_3)}(X)=[c_3,c_2,c_1],\quad s_{i(c_1+c_3)}(X)=[-c_3,c_2,-c_1].\end{aligned} \tag{15}$$

From Proposition 2, the Weyl group $W(G,K)$ is generated by s_α given in Eq. (15). Therefore, the reflections s_α are equivalent to either permutations of the elements of $[c_1,c_2,c_3]$, or permutations with sign flips of two elements.

III. NONLOCAL OPERATIONS

We now study nonlocal two-qubit operations within the group theoretical framework of the preceding section. The Cartan decomposition of su(4) provides us with a good starting point to explore the invariants under local gate operations. It also reveals that the geometric structure of the local equivalence classes is none other than a 3-torus. Every point on this 3-torus corresponds to a local equivalence class of two-qubit gates. Different points may also correspond to the same equivalence class. To reduce this symmetry, we apply the Weyl group theory. We show that the local equivalence classes of two-qubit gates are in one-to-one correspondence with the points in a tetrahedron, except on the base where there are two equivalent areas. This tetrahedral representation of nonlocal operations plays a central role in our subsequent discussion of perfect entanglers and the design of universal quantum circuits.

A. Local invariants and local equivalence classes

Two unitary transformations $U,\ U_1\in\mathrm{SU}(4)$ are called *locally equivalent* if they differ only by local operations: $U=k_1U_1k_2$, where $k_1,\ k_2\in\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ are local gates. This clearly defines an equivalence relation on the Lie group SU(4). We denote the equivalence class of a unitary transfor-

mation U as $[U]$. From the Cartan decomposition of su(4) in Sec. II B, any two-qubit gate $U \in \mathrm{SU}(4)$ can be written in the following form:

$$U = k_1 A k_2 = k_1 \exp\left\{\frac{i}{2}(c_1\sigma_x^1\sigma_x^2 + c_2\sigma_y^1\sigma_y^2 + c_3\sigma_z^1\sigma_z^2)\right\} k_2, \tag{16}$$

where $k_1,\ k_2 \in \mathrm{SU}(2)\otimes\mathrm{SU}(2)$. Because the two-qubit gate U is periodic in c_k, the geometric structure of $[c_1,c_2,c_3]$ is a 3-torus, $T^3 = S^1\times S^1\times S^1$.

In Ref. [2], local invariants were given for two-qubit gates. Here we will connect these invariants of Makhlin to the coordinates $[c_1,c_2,c_3]$ on the 3-torus. We first consider the case of the two-qubit gates in SU(4), and then extend the results to the general case of U(4).

1. SU(4) Operations

Consider the transformation from the standard basis of states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ to the Bell basis $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, $|\Phi^-\rangle = i/\sqrt{2}(|01\rangle + |10\rangle)$, $|\Psi^+\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$, $|\Psi^-\rangle = i/\sqrt{2}(|00\rangle - |11\rangle)$. In this basis, the two-qubit gate U in Eq. (16) can be written as

$$U_B = Q^\dagger U Q = Q^\dagger k_1 A k_2 Q, \tag{17}$$

where

$$Q = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}. \tag{18}$$

Recalling that $i/2\{\sigma_x^1,\sigma_y^1,\sigma_z^1,\sigma_x^2,\sigma_y^2,\sigma_z^2\}$ is a basis for $\mathfrak{k}$, it is not hard to verify that $i/2Q^\dagger\{\sigma_x^1,\sigma_y^1,\sigma_z^1,\sigma_x^2,\sigma_y^2,\sigma_z^2\}Q$ forms a basis for so(4), the Lie algebra of the special orthogonal group SO(4). Hence U_B can be written as

$$U_B = O_1 Q^\dagger A Q O_2, \tag{19}$$

where

$$O_1 = Q^\dagger k_1 Q \in \mathrm{SO}(4),$$
$$O_2 = Q^\dagger k_2 Q \in \mathrm{SO}(4). \tag{20}$$

Equation (19) can also be obtained from the Cartan decomposition of su(4) derived from the complexification of sl(4), as discussed in Sec. II B. An Abelian subalgebra $\mathfrak{a}$ is generated by $i/2\{\sigma_x^1\sigma_x^2,\sigma_y^1\sigma_y^2,\sigma_z^1\sigma_z^2\}$, and the transformation to the Bell basis takes these operators to $i/2\{\sigma_z^1,-\sigma_z^2,\sigma_z^1\sigma_z^2\}$. Therefore, we have $U_B = O_1 F O_2$, where

$$F = Q^\dagger A Q = \exp\left\{\frac{i}{2}(c_1\sigma_z^1 - c_2\sigma_z^2 + c_3\sigma_z^1\sigma_z^2)\right\}$$
$$= \mathrm{diag}\left\{e^{i\frac{c_1-c_2+c_3}{2}}, e^{i\frac{c_1+c_2-c_3}{2}}, e^{-i\frac{c_1+c_2+c_3}{2}}, e^{i\frac{-c_1+c_2+c_3}{2}}\right\}. \tag{21}$$

Let

$$m = U_B^T U_B = O_2^T F^2 O_2, \tag{22}$$

where O_2 is defined by Eq. (20). The complete set of local invariants of a two-qubit gate $U \in \mathrm{SU}(4)$ is given by the spectrum of the matrix m [2], and hence by the eigenvalues of F^2,

$$\{e^{i(c_1-c_2+c_3)},\ e^{i(c_1+c_2-c_3)},\ e^{-i(c_1+c_2+c_3)},\ e^{i(-c_1+c_2+c_3)}\}. \tag{23}$$

Since m is unitary and $\det m = 1$, the characteristic polynomial of m is then

$$|sI - m| = s^4 - \mathrm{tr}(m)s^3 + \frac{1}{2}[\mathrm{tr}^2(m) - \mathrm{tr}(m^2)]s^2 - \overline{\mathrm{tr}(m)}s + 1. \tag{24}$$

Therefore the spectrum of m is completely determined by only the two quantities $\mathrm{tr}(m)$ and $\mathrm{tr}^2(m) - \mathrm{tr}(m^2)$. For a two-qubit gate U given in Eq. (16), its local invariants can be derived from Eq. (23) as

$$\mathrm{tr}(m) = 4\cos c_1\cos c_2\cos c_3 + 4i\sin c_1\sin c_2\sin c_3,$$
$$\mathrm{tr}^2(m) - \mathrm{tr}(m^2) = 16\cos^2 c_1\cos^2 c_2\cos^2 c_3 - 16\sin^2 c_1\sin^2 c_2\sin^2 c_3 - 4\cos 2c_1\cos 2c_2\cos 2c_3. \tag{25}$$

2. Generalization to U(4)

Now let us consider the local invariants for the general case of U(4) [2]. An arbitrary two-qubit gate $U \in \mathrm{U}(4)$ can be decomposed as the product of a gate $U_1 \in \mathrm{SU}(4)$ and a global phase shift $e^{i\alpha}$, where $\det U = e^{i4\alpha}$. It follows that $m(U_1) = e^{-i2\alpha}m(U)$, where

$$m(U) = (Q^\dagger U Q)^T Q^\dagger U Q \tag{26}$$

and

$$\mathrm{tr}[m(U_1)] = e^{-i2\alpha}\mathrm{tr}[m(U)],$$
$$\mathrm{tr}^2[m(U_1)] - \mathrm{tr}[m^2(U_1)] = e^{-i4\alpha}\{\mathrm{tr}^2[m(U)] - \mathrm{tr}[m^2(U)]\}. \tag{27}$$

It is clear that the global phase factor just rotates the eigenvalues of $m(U)$ along the unit circle in the complex plane, while keeping their relative phase invariant. Therefore, it does not affect the entangling properties and we can consequently divide by $\det(U)$. The local invariants of a two-qubit gate U are thus given by

$$G_1 = \frac{\mathrm{tr}^2[m(U)]}{16\det U},$$
$$G_2 = \frac{\mathrm{tr}^2[m(U)] - \mathrm{tr}[m^2(U)]}{4\det U}, \tag{28}$$

where the numerical factors are incorporated into the denominators to provide convenient normalization. If U is now written in the following form:

$$U = e^{i\alpha} k_1 A k_2 = e^{i\alpha} k_1 \exp\left\{ \frac{i}{2} (c_1 \sigma_x^1 \sigma_x^2 + c_2 \sigma_y^1 \sigma_y^2 + c_3 \sigma_z^1 \sigma_z^2) \right\} k_2, \tag{29}$$

we can compute its local invariants as

$$G_1 = \cos^2 c_1 \cos^2 c_2 \cos^2 c_3 - \sin^2 c_1 \sin^2 c_2 \sin^2 c_3 + \frac{i}{4} \sin 2c_1 \sin 2c_2 \sin 2c_3,$$

$$G_2 = 4\cos^2 c_1 \cos^2 c_2 \cos^2 c_3 - 4\sin^2 c_1 \sin^2 c_2 \sin^2 c_3 - \cos 2c_1 \cos 2c_2 \cos 2c_3. \tag{30}$$

Because the local invariants G_1 and G_2 characterize the nonlocal properties of unitary operations, we can use these two invariants to check whether a pair of two-qubit gates are locally equivalent. The invariants G_1 and G_2 are evaluated by taking the matrix representation of a gate in the Bell basis and then using Eqs. (26) and (28). For example, CNOT and controlled-Z [referred as C(Z)] possess identical values of the local invariants, given by $G_1 = 0$ and $G_2 = 1$. Therefore, they belong to the same local equivalence class. We refer to this class as [CNOT]. On the other hand, the local invariants for $\sqrt{\text{SWAP}}$ are $G_1 = i/4$ and $G_2 = 0$. Hence this gate belongs to a different local equivalence class that we refer to as $[\sqrt{\text{SWAP}}]$. Note that from Eq. (28), since the local invariants are functions of eigenvalues of the matrix m, the local equivalence class can alternatively be defined simply via the set of eigenvalues of the matrix m.

B. Geometric representation of two-qubit gates

Equation (30) reveals the relation between the local invariants G_1 and G_2 and the coordinates $[c_1, c_2, c_3]$ of the 3-torus structure of nonlocal two-qubit gates. From this relation, given a set of coordinates $[c_1, c_2, c_3]$, we can easily compute the local invariants for a local equivalence class. Vice versa, from a given pair of values of the local invariants G_1 and G_2, we can also find the points on the 3-torus that correspond to a given two-qubit operation. In general, we expect to find multiple points on the 3-torus for a given pair G_1 and G_2. We now show how this multiple-valued nature can be removed by using the Weyl group to construct a geometric representation that allows the symmetry to be reduced.

To visualize the geometric structure of the two-qubit gates, we first consider a cube with side length π in the vector space $\mathfrak{a}$. This provides an equivalent representation of the points on the 3-torus, since $T^3 \cong \mathbb{R}^3/\mathbb{Z}^3$. Clearly, every point in this cube corresponds a local equivalence class. However, different points in the cube may belong to the same local equivalence class. For example, both the points $[\pi/4, \pi/4, \pi/4]$ and $[\pi/4, 3\pi/4, 3\pi/4]$ correspond to the gate $\sqrt{\text{SWAP}}$.

We use the theory of the Weyl group to reduce this symmetry in the cube. From the Lie group representation theory, the orbits of local gates K acting on $\text{SU}(4)/\text{SU}(2) \otimes \text{SU}(2)$ are in one-to-one correspondence with the orbits of the Weyl group $W(G,K)$ on $\mathfrak{a}$ [41]. From Proposition 2, the Weyl group $W(G,K)$ is generated by the reflections s_α as given in Eq. (15). Note that in Eq. (15), the reflections s_α are either permutations or permutations with sign flips of two entries in $[c_1, c_2, c_3]$. Therefore, if $[c_1, c_2, c_3]$ is an element in a local equivalence class $[U]$, then $[c_i, c_j, c_k]$, $[\pi - c_i, \pi - c_j, c_k]$, $[c_i, \pi - c_j, \pi - c_k]$, and $[\pi - c_i, c_j, \pi - c_k]$ are also in $[U]$, where (i,j,k) is a permutation of $(1,2,3)$. With the meaning clear from the context of the discussion, in the remainder of this paper we shall use the triplet $[c_1, c_2, c_3]$ to denote either the corresponding local equivalence class of a two-qubit gate, or simply to refer to a specific point on the 3-torus or cube.

Since each orbit of the Weyl group $W(G,K)$ on $\mathfrak{a}$ contains precisely one point in a Weyl chamber, the local equivalence classes of two-qubit gates are in one-to-one correspondence with the points of a Weyl chamber. Hence, each Weyl chamber contains all the local equivalence classes. Recall that the Weyl chambers are obtained by dividing the vector space $\mathfrak{a}$ by the hyperplanes $\alpha(X) = 0$, where $\alpha \in \Delta_\mathfrak{p}$ as given in Eq. (13). Therefore, we can obtain the Weyl chambers by dividing the cube by the planes

$$\{X \in \mathfrak{a} : c_1 - c_2 = 0\}, \quad \{X \in \mathfrak{a} : c_1 + c_2 = \pi\},$$
$$\{X \in \mathfrak{a} : c_1 - c_3 = 0\}, \quad \{X \in \mathfrak{a} : c_1 + c_3 = \pi\}, \tag{31}$$
$$\{X \in \mathfrak{a} : c_2 - c_3 = 0\}, \quad \{X \in \mathfrak{a} : c_2 + c_3 = \pi\}.$$

Figure 2(a) shows that after dividing the cube by the planes $c_1 - c_3 = 0$, $c_1 + c_3 = \pi$, $c_2 - c_3 = 0$, and $c_2 + c_3 = \pi$, we obtain six square pyramids. One of these pyramids is shown in Fig. 2(b). Further dividing this pyramid by the planes $c_1 - c_2 = 0$ and $c_1 + c_2 = \pi$, we get a tetrahedron $OA_1A_2A_3$ such as that shown in Fig. 2(c). Notice that for any point $[c_1, c_2, 0]$ on the base of this tetrahedron, its mirror image with respect to the line LA_2, which is $[\pi - c_1, c_2, 0]$, corresponds to the same local equivalence class. Therefore, with the caveat that the basal areas LA_2A_1 and LA_2O are identified as equivalent, we finally arrive at the identification of the tetrahedron $OA_1A_2A_3$ as a Weyl chamber, and we denote this by $\mathfrak{a}^+$. There are 24 such Weyl chambers in total, and each of them has the volume $\pi^3/24$. Note that every point in $\mathfrak{a}^+$ corresponds to a different local equivalence class. Consequently, the Weyl chamber $\mathfrak{a}^+$ provides a geometric representation of all the possible two-qubit gates.

For a given two-qubit gate, it is important to find its coordinates $[c_1, c_2, c_3]$ on the 3-torus, and hence in the Weyl chamber $\mathfrak{a}^+$. With this representation in the tetrahedron $\mathfrak{a}^+$ we have removed the multiple-valued nature of the coordinates on the 3-torus and cube and therefore can now take the coordinates $[c_1, c_2, c_3]$ as an alternative set of local invariants. They provide a useful geometric representation of local

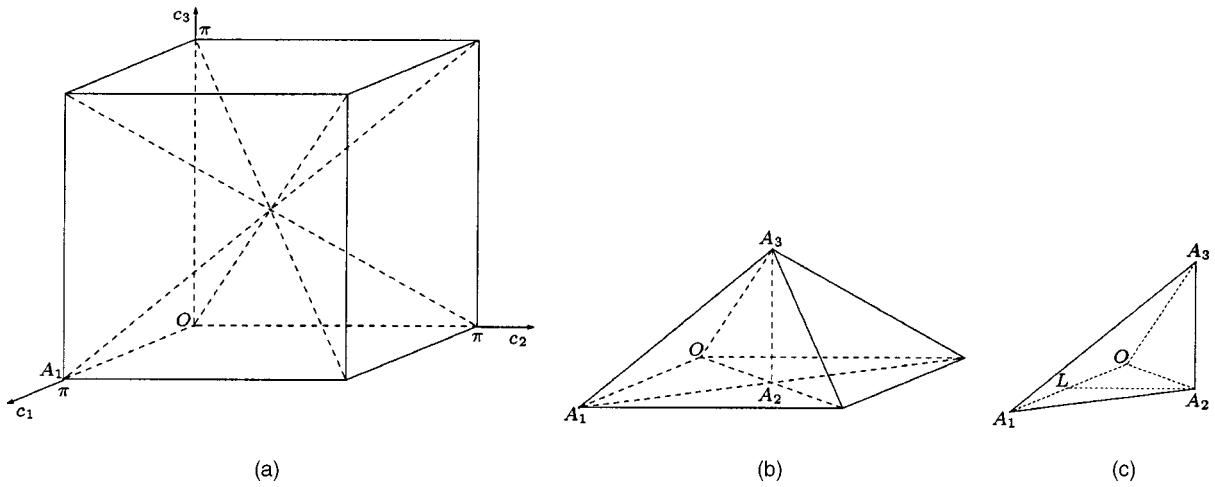


FIG. 2. Illustration of the tetrahedral representation of nonlocal two-qubit operations. (a) Divide the cube by the planes $c_1-c_3=0$, $c_1+c_3=\pi$, $c_2-c_3=0$, and $c_2+c_3=\pi$. (b) One of the six equivalent square pyramids produced from (a). Further dividing this pyramid by the planes $c_1-c_2=0$ and $c_1+c_2=\pi$ gives (c), the tetrahedron $OA_1A_2A_3$, with $A_1=[\pi,0,0]$, $A_2=[\pi/2,\pi/2,0]$, and $A_3=[\pi/2,\pi/2,\pi/2]$. $OA_1A_2A_3$ is a Weyl chamber, denoted a^+, with the exception of points on its base where we have an equivalence of LA_2A_1 with LA_2O, where L is the point $[\pi/2,0,0]$. Every point in a^+ corresponds to a local equivalence class of two-qubit operations.

invariants that is easy to visualize and is entirely equivalent to G_1 and G_2. They can be used directly to implement the local equivalence class of particularly prescribed two-qubit gates for a given Hamiltonian. More generally, this alternative set of local invariants helps us to gain a better understanding of the local invariants and geometric representation of two-qubit gates.

It is clear that the local gates K correspond to the points O and A_1 in Figs. 2(a)–2(c). We now study several nontrivial examples of nonlocal gates to determine the corresponding coordinates $[c_1,c_2,c_3]$ in $\mathfrak{a}^+$. All the other points of a particular local equivalence class in the cube can be obtained by applying the Weyl group $W(G,K)$ to the corresponding point in $\mathfrak{a}^+$. Note that for a gate $[c_1,c_2,c_3]$ in $\mathfrak{a}^+$, its inverse is just $[\pi/2-c_1,c_2,c_3]$.

(1) CNOT: Following the procedure to compute the local invariants described above [see Eqs. (26) and (28)], we obtain $G_1=0$ and $G_2=1$ for the two-qubit gate CNOT. Solving Eq. (30):

$$\cos^2c_1\cos^2c_2\cos^2c_3-\sin^2c_1\sin^2c_2\sin^2c_3=0,$$
$$\sin 2c_1\sin 2c_2\sin 2c_3=0, \tag{32}$$
$$-\cos 2c_1\cos 2c_2\cos 2c_3=1,$$

we find that $[\pi/2,0,0]$ is the corresponding point for CNOT in the Weyl chamber $\mathfrak{a}^+$. This is the point L in Fig. 2(c).

(2) SWAP: For the gate SWAP, we have $G_1=-1$ and $G_2=-3$. Solving Eq. (30), we obtain that the corresponding point for SWAP is $[\pi/2,\frac{\pi}{2},\frac{\pi}{2}]$, i.e., the point A_3 in Fig. 2(c).

(3) $\sqrt{\text{SWAP}}$: The local invariants for the gate $\sqrt{\text{SWAP}}$ are $G_1=i/4$ and $G_2=0$. Solving Eq. (30) for this case, we derive that $[\pi/4,\pi/4,\pi/4]$ is the corresponding point in $\mathfrak{a}^+$. This is the midpoint of OA_3 in Fig. 2(c).

(4) Controlled-U gate: Suppose U is an arbitrary single-qubit unitary operation,

$$U=\exp(\gamma_1 i\sigma_x+\gamma_2 i\sigma_y+\gamma_3 i\sigma_z). \tag{33}$$

For the controlled-U gate, the local invariants are $G_1=\cos^2\gamma$ and $G_2=2\cos^2\gamma+1$, where $\gamma=\sqrt{\gamma_1^2+\gamma_2^2+\gamma_3^2}$. By solving Eq. (30), we find that $[\gamma,0,0]$ is the corresponding point in $\mathfrak{a}^+$. Hence, all the controlled-U gates correspond to the line OL in $\mathfrak{a}^+$, where L is [CNOT].

IV. CHARACTERIZATION OF PERFECT ENTANGLERS

Entanglement is one of the most striking quantum-mechanical features that plays a key role in quantum computation and quantum information. It is used in many applications such as teleportation and quantum cryptography [15]. In many applications, it is often desired to generate maximal entanglement from some unentangled initial states. The nonlocal two-qubit operations that can generate maximal entanglement are called perfect entanglers. In this section, we study the perfect entanglers using the geometric approach established in the previous sections. We will prove a theorem that provides a sufficient and necessary condition for a two-qubit gate to be a perfect entangler. It turns out that whether a two-qubit gate can generate maximal entanglement is only determined by its location on the 3-torus, or more specifically, in the Weyl chamber $\mathfrak{a}^+$. We show that in the tetrahedral representation of nonlocal gates summarized in Fig. 2(c), all the perfect entanglers constitute a polyhedron with seven faces, whose volume is exactly half that of the tetrahedron. This implies that the among all the nonlocal two-qubit operations, precisely half of them are capable of generating maximal entanglement from some initially separable states.

For a two-qubit state ψ, define a quadratic function $E(\psi)=\psi^TP\psi$, where $P=-\frac{1}{2}\sigma_y^1\sigma_y^2$ [2]. It can be shown that $\max_\psi|E(\psi)|=\frac{1}{2}$, and $E(\psi)=0$ if and only if ψ is an unentangled state. This function thus defines a measure of entanglement for a pure state. If $|E(\psi)|=\frac{1}{2}$, we call ψ a maxi-

mally entangled state. It can be proved that the function E is invariant under the local operations.

Definition 3 (perfect entangler). A two-qubit gate U is called a perfect entangler if it can produce a maximally entangled state from an unentangled one.

Definition 4 (convex hull). The convex hull C of N points $p_1, \ldots, p_N$ in $\mathbb{R}^n$ is given by

$$C=\left\{ \sum_{j=1}^{N} \theta_j p_j \middle| \quad \theta_j \geqslant 0 \quad \text{for all} \quad j \quad \text{and} \quad \sum_{j=1}^{N} \theta_j = 1 \right\}. \tag{34}$$

Theorem 1 (condition for perfect entangler). A two-qubit gate U is a perfect entangler if and only if the convex hull of the eigenvalues of $m(U)$ contains zero.

This result was first mentioned by Makhlin [2] but no proof was given. We provide here a proof and then go on to develop a geometrical analysis that provides a quantification of the relative volume of perfect entanglers in SU(4).

Proof: From the Cartan decomposition of su(4) in Sec. II B, any two-qubit gate $U \in \mathrm{U}(4)$ can be written in the following form,

$$\begin{aligned} U &= e^{i\alpha} k_1 A k_2 \\ &= e^{i\alpha} k_1 \exp\left\{ \frac{i}{2} (c_1 \sigma_x^1 \sigma_x^2 + c_2 \sigma_y^1 \sigma_y^2 + c_3 \sigma_z^1 \sigma_z^2) \right\} k_2, \end{aligned} \tag{35}$$

where $k_1,\ k_2 \in \mathrm{SU}(2) \otimes \mathrm{SU}(2)$. For any arbitrary unentangled state ψ_0, we have

$$E(U\psi_0) = E(e^{i\alpha} k_1 A k_2 \psi_0) = e^{i2\alpha} E(A\psi), \tag{36}$$

where $\psi = k_2 \psi_0$ is again an unentangled state. From Eq. (36), it is clear that $|E(U\psi_0)| = |E(A\psi)|$. Therefore, U is a perfect entangler if and only if A is a perfect entangler. Furthermore, we have

$$\begin{aligned} E(A\psi) &= \psi^T A^T P A \psi \\ &= (Q^\dagger \psi)^T (Q^\dagger A Q)^T (Q^T P Q) (Q^\dagger A Q) (Q^\dagger \psi) \\ &= \frac{1}{2} (Q^\dagger \psi)^T F^2 (Q^\dagger \psi), \end{aligned} \tag{37}$$

where Q and F are defined as in Eqs. (18) and (21), respectively. The last equality in Eq. (37) holds since $Q^T P Q = \frac{1}{2} I$. Let $\phi = Q^\dagger \psi$. Since ψ is an unentangled state, we get $E(\psi) = 0$. Hence,

$$\begin{aligned} E(\psi) &= \psi^T P \psi \\ &= \phi^T Q^T P Q \phi = \frac{1}{2} \phi^T \phi \\ &= \frac{1}{2} (\phi_1^2 + \phi_2^2 + \phi_3^2 + \phi_4^2) = 0. \end{aligned} \tag{38}$$

Since $\psi^\dagger \psi = 1$, we have $\phi^\dagger \phi = 1$, that is,

$$|\phi_1|^2 + |\phi_2|^2 + |\phi_3|^2 + |\phi_4|^2 = 1. \tag{39}$$

Recall the definition of F from Eq. (21),

$$F = \mathrm{diag}\{ e^{i(c_1 - c_2 + c_3)/2}, e^{i(c_1 + c_2 - c_3)/2}, e^{-i(c_1 + c_2 + c_3)/2}, e^{i(-c_1 + c_2 + c_3)/2} \}. \tag{40}$$

For simplicity, we denote the eigenvalues of F as $\{\lambda_k\}_{k=1}^4$. Then the eigenvalues of $m(U)$ are just $\{\lambda_k^2\}_{k=1}^4$. We have

$$E(A\psi) = \frac{1}{2} (Q^\dagger \psi)^T F^2 (Q^\dagger \psi) = \frac{1}{2} \phi^T F^2 \phi = \frac{1}{2} \sum_{k=1}^{4} \phi_k^2 \lambda_k^2. \tag{41}$$

If A is a perfect entangler, we have

$$\begin{aligned} \frac{1}{2} = |E(A\psi)| &= \frac{1}{2} |\phi_1^2 \lambda_1^2 + \phi_2^2 \lambda_2^2 + \phi_3^2 \lambda_3^2 + \phi_4^2 \lambda_4^2| \\ &\leqslant \frac{1}{2} (|\phi_1^2 \lambda_1^2| + |\phi_2^2 \lambda_2^2| + |\phi_3^2 \lambda_3^2| + |\phi_4^2 \lambda_4^2|) \\ &= \frac{1}{2} (|\phi_1^2| + |\phi_2^2| + |\phi_3^2| + |\phi_4^2|) = \frac{1}{2}. \end{aligned} \tag{42}$$

The equality in Eq. (42) holds if and only if there exists a real number $\theta \in [0, 2\pi]$ such that

$$\begin{aligned} &\phi_1^2 \lambda_1^2 = |\phi_1|^2 e^{i2\theta}, \quad \phi_2^2 \lambda_1^2 = |\phi_2|^2 e^{i2\theta}, \\ &\phi_3^2 \lambda_1^2 = |\phi_3|^2 e^{i2\theta}, \quad \phi_4^2 \lambda_1^2 = |\phi_4|^2 e^{i2\theta}. \end{aligned} \tag{43}$$

From Eq. (38), we obtain

$$\begin{aligned} \phi_1^2 + \phi_2^2 + \phi_3^2 + \phi_4^2 &= e^{i2\theta} \left(\frac{|\phi_1|^2}{\lambda_1^2} + \frac{|\phi_2|^2}{\lambda_2^2} + \frac{|\phi_3|^2}{\lambda_3^2} + \frac{|\phi_4|^2}{\lambda_4^2} \right) \\ &= 0. \end{aligned} \tag{44}$$

Since $1/\lambda_k = \overline{\lambda_k}$, it follows that

$$|\phi_1|^2 \lambda_1^2 + |\phi_2|^2 \lambda_2^2 + |\phi_3|^2 \lambda_3^2 + |\phi_4|^2 \lambda_4^2 = 0. \tag{45}$$

From the relation in Eq. (39), we conclude that if U is a perfect entangler, the convex hull of the eigenvalues of $m(U)$ contains zero.

Conversely, suppose the convex hull of the eigenvalues of $m(U)$ contains zero, that is, there exist $\{\alpha_k\}_{k=1}^4 \subset [0,1]$ such that

$$\alpha_1^2\lambda_1^2+\alpha_2^2\lambda_2^2+\alpha_3^2\lambda_3^2+\alpha_4^2\lambda_4^2=0,$$

$$\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2=1. \tag{46}$$

Let

$$\phi=\left(\frac{\alpha_1}{\lambda_1},\frac{\alpha_2}{\lambda_2},\frac{\alpha_3}{\lambda_3},\frac{\alpha_4}{\lambda_4}\right)^T, \tag{47}$$

and $\psi=Q\phi$. From Eq. (38), we have

$$E(\psi)=\frac{1}{2}\phi^T\phi=\frac{1}{2}\left(\frac{\alpha_1^2}{\lambda_1^2}+\frac{\alpha_2^2}{\lambda_2^2}+\frac{\alpha_3^2}{\lambda_3^2}+\frac{\alpha_4^2}{\lambda_4^2}\right)=0. \tag{48}$$

Hence ψ is an unentangled state. From Eq. (41), we derive

$$E(A\psi)=\frac{1}{2}\phi^TF^2\phi=\frac{1}{2}(\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2)=\frac{1}{2}. \tag{49}$$

Therefore, U is a perfect entangler. ■

We now derive the conditions under which points $[c_1,c_2,c_3]$ in the Weyl chamber $\mathfrak{a}^+$ are perfect entanglers. We begin with two corollaries to Theorem 1.

Corollary 1. If $[c_1,c_2,c_3]$ is a perfect entangler, then $[\pi-c_1,c_2,c_3]$ and $[\pi/2-c_1,\pi/2-c_2,\pi/2-c_3]$ are both perfect entanglers.

Proof: We know that $[c_1,c_2,c_3]$ and $[c_1,-c_2,-c_3]$ correspond to the same two-qubit gate. Since the 3-torus has the minimum positive period π, $[-\pi+c_1,-c_2,-c_3]$ also belongs to the same local equivalence class. From Eqs. (44) and (45), if $[c_1,c_2,c_3]$ is a perfect entangler, so is $[-c_1,-c_2,-c_3]$. Therefore, $[\pi-c_1,c_2,c_3]$ is a perfect entangler.

From Theorem 1, U is a perfect entangler if and only if the convex hull of the eigenvalues of $m(U)$ contains zero, that is, there exist $\{\alpha_k\}_{k=1}^4\subset[0,1]$ such that

$$\alpha_1^2e^{i(c_1-c_2+c_3)}+\alpha_2^2e^{i(c_1+c_2-c_3)}+\alpha_3^2e^{-i(c_1+c_2+c_3)}+\alpha_4^2e^{i(-c_1+c_2+c_3)}=0, \tag{50}$$

$$\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2=1. \tag{51}$$

Substitute the coordinates of the point $[\pi/2-c_1,\pi/2-c_2,\pi/2-c_3]$ into Eq. (50):

$$i\{\alpha_1^2e^{-i(c_1-c_2+c_3)}+\alpha_2^2e^{-i(c_1+c_2-c_3)}+\alpha_3^2e^{i(c_1+c_2+c_3)}+\alpha_4^2e^{-i(-c_1+c_2+c_3)}\}=0. \tag{52}$$

Together with Eq. (51), it is clear that $[\pi/2-c_1,\pi/2-c_2,\pi/2-c_3]$ is a perfect entangler. ■

Corollary 2. For a two-qubit gate U, if its corresponding point in the Weyl chamber $\mathfrak{a}^+$ *is* $[c_1,\pi/2-c_1,c_3]$, $[c_1,c_1-\pi/2,c_3]$, *or* $[c_1,c_2,\pi/2-c_2]$, U is a perfect entangler.

Proof: For the gate $[c_1,\pi/2-c_1,c_3]$, the eigenvalues of $m(U)$ are

$$\{e^{i(c_1-c_2+c_3)},e^{i(c_1+c_2-c_3)},e^{-i(c_1+c_2+c_3)},e^{i(-c_1+c_2+c_3)}\}=e^{-i(c_1+c_2+c_3)}\{e^{i2(c_1+c_3)},e^{i2(c_1+c_2)},1,e^{i2(c_2+c_3)}\}. \tag{53}$$

The convex hull of the eigenvalues of $m(U)$ always contains the origin, and thus $[c_1,\pi/2-c_1,c_3]$ is a perfect entangler. The other cases can be proved similarly. ■

Note that for $[c_1,\pi/2-c_1,c_3]$, picking $c_1=\pi/2$ and $c_3=0$, we obtain the perfect entangler [CNOT]; picking $c_1=\pi/4$ and $c_3=\pi/4$, we get the perfect entangler $[\sqrt{\text{SWAP}}]$.

With these corollaries in hand, we can proceed to derive the conditions under which a general point $[c_1,c_2,c_3]$ on the 3-torus is a perfect entangler.

Theorem 2 (perfect entangler on 3-torus). Consider a two-qubit gate U and its corresponding representation $[c_1,c_2,c_3]$ on the 3-torus. U is a perfect entangler if and only if one of the following two conditions is satisfied:

$$\frac{\pi}{2}\leqslant c_i+c_k\leqslant c_i+c_j+\frac{\pi}{2}\leqslant\pi,$$

$$\frac{3\pi}{2}\leqslant c_i+c_k\leqslant c_i+c_j+\frac{\pi}{2}\leqslant 2\pi, \tag{54}$$

where (i,j,k) is a permutation of $(1,2,3)$.

Proof. Given the eigenvalues of $m(U)$ in Eq. (53), it suffices to study whether the convex hull of $\{1,e^{i2(c_1+c_2)},e^{i2(c_1+c_3)}e^{i2(c_2+c_3)}\}$ contains the origin or not. Suppose that one of the conditions in Eq. (54) is satisfied. In this case, the points $\{e^{i2(c_1+c_2)},e^{i2(c_1+c_3)},e^{i2(c_2+c_3)}\}$ have to be on the unit circle as shown in Figs. 3(a) or 3(b). It is clear that the convex hull of these three points contains the origin. From Theorem 1, U is therefore a perfect entangler.

Conversely, suppose that U is a perfect entangler. Then the convex hull of the eigenvalues of $m(U)$ contains the origin. If all the three points $\{e^{i2(c_1+c_2)},e^{i2(c_1+c_3)},e^{i2(c_2+c_3)}\}$ are on the upper or lower semicircle, the convex hull of $\{1,e^{i2(c_1+c_2)},e^{i2(c_1+c_3)},e^{i2(c_2+c_3)}\}$ does not contain the origin. Therefore, we can always pick one point on the upper semicircle and one point on the lower semicircle such that one of the two conditions in Eq. (54) is satisfied. ■

The above analysis shows that whether a two-qubit gate is a perfect entangler or not is only determined by its geometric representation $[c_1,c_2,c_3]$ on the 3-torus. Recall that in Sec. III B, we show that the local equivalence classes of two-qubit gates are in one-to-one correspondence with the points of the Weyl chamber $\mathfrak{a}^+$, which can be represented by a tetrahedron as shown in Fig. 2(c). We are now ready for the final stage of the procedure, namely to identify those points in the *tetrahedron* that correspond to perfect entanglers.

Consider a two-qubit gate $[c_1,c_2,c_3]$. As shown in Fig. 4, in the tetrahedron $OA_1A_2A_3$, we have $c_1\geqslant c_2\geqslant c_3\geqslant 0$. Hence $2(c_1+c_2)\geqslant 2(c_1+c_3)\geqslant 2(c_2+c_3)\geqslant 0$. As in the proof of Theorem 2, consider the convex hull of $\{1,e^{i2(c_1+c_2)},e^{i2(c_1+c_3)}e^{i2(c_2+c_3)}\}$. We can identify the following three cases of the gates that do not provide maximal entanglement, and are thus not perfect entanglers:

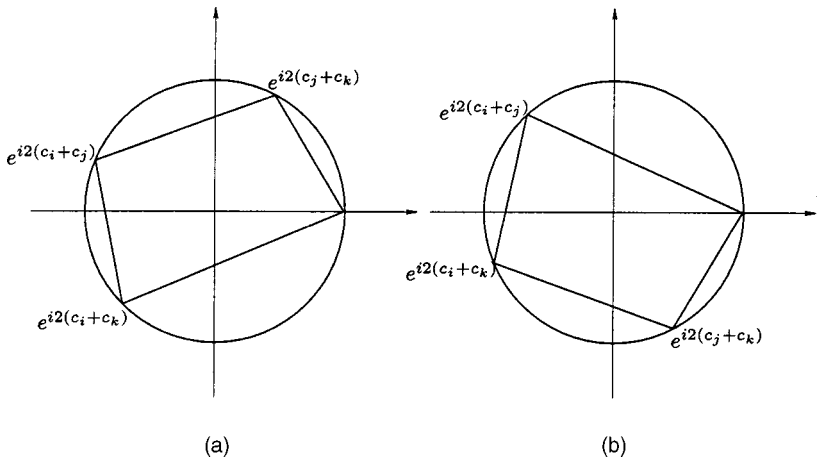


FIG. 3. Illustration of the proof of Theorem 2.

(1) If $c_1+c_2\leqslant\pi/2$, that is, all the $e^{i2(c_j+c_k)}$ are on the upper semicircle, the gate is not a perfect entangler. In the tetrahedron $OA_1A_2A_3$, $c_1+c_2\leqslant\pi/2$ corresponds to the tetrahedron $LQPO$.

(2) If $c_2+c_3\geqslant\pi/2$, that is, all the $e^{i2(c_j+c_k)}$ are on the lower semicircle, the gate is not a perfect entangler either. This case corresponds to the tetrahedron NPA_2A_3.

(3) From Theorem 2, we obtain that the gates represented by points in the set $\{X\in\alpha^+|\,2(c_1+c_3)\geqslant 2(c_2+c_3)+\pi\}$ are not perfect entanglers. This set is the tetrahedron $LMNA_1$.

The set of perfect entanglers can thus be obtained by removing these three tetrahedra from $OA_1A_2A_3$. This is done in Fig. 4 where it is thereby evident that the polyhedron $\mathrm{LMNPQA_2}$ is the residual set of perfect entanglers. Here the point P corresponds to the gate $\sqrt{\mathrm{SWAP}}$, N corresponds to its inverse, and L corresponds to the CNOT gate. Computing the volume of the Weyl chamber $OA_1A_2A_3$ and of these three polyhedra, we have

$$V(OA_1A_2A_3)=\frac{\pi^3}{24},$$

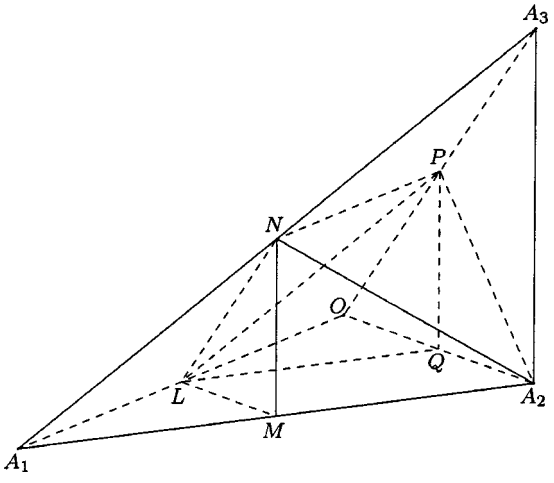


FIG. 4. Polyhedron $\mathrm{LMNPQA_2}$ corresponds to perfect entanglers in the Weyl chamber α^+ [see Fig. 2(c)], where L, M, N, P, and Q are the midpoints of the line segments A_1Q, A_1A_2, A_1A_3, A_3Q, and A_2Q, respectively. P corresponds to the gate $\sqrt{\mathrm{SWAP}}$, N to its inverse, and L to the CNOT gate.

$$V(LQPO)=\frac{\pi^3}{192},\quad V(NPA_2A_3)=\frac{\pi^3}{96},$$

$$V(LMNA_1)=\frac{\pi^3}{192}. \tag{55}$$

Therefore, the volume of the polyhedron $\mathrm{LMNPQA_2}$ is $\pi^3/48$, which is half of the volume of $OA_1A_2A_3$. This implies that among all the nonlocal two-qubit gates, half of them are perfect entanglers. Note that the polyhedron $LMNPQA_2$ is symmetric with respect to the plane $c_1=\pi/2$, which provides a geometric explanation of Corollary 1. The points in Corollary 2 correspond to the triangles LMN, LPQ, and NPA_2, which are three faces of the set of perfect entanglers. Also recall that the line OL represents all the controlled-U gates. Hence CNOT, located at L, is the only controlled-U gate that is a perfect entangler. Thus we see that the geometric representation provides an intuitive visual picture to understand the nonlocal properties of two-qubit gates, as well as allowing quantification of the weight of perfect entanglers.

V. PHYSICAL GENERATION OF NONLOCAL GATES

We now investigate the universal quantum computation and simulation potential of a given physical Hamiltonian. We first study the gates that can be generated by a Hamiltonian directly. Generally speaking, these gates form a one-dimensional subset on the 3-torus geometric representation of nonlocal gates. For any arbitrary two-qubit gate, we will explicitly construct a quantum circuit that can simulate it exactly with a guaranteed small number of operations. Construction of efficient circuits is especially important in the theoretical design and experimental implementations of quantum information processing. We assume only that we can turn on local operations individually. Our starting point is thus any arbitrary single-qubit operation and a two-body interaction Hamiltonian. The single- and two-qubit operations may be, for example, a sequence of pulses of an optical field that are suitably tuned and focused on each individual qubit. The qubits may be represented by either a solid-state system such as a quantum dot in a cavity [45], or by a gas-phase system such as an optical lattice [46].

A. Nonlocal operations generated by a given Hamiltonian

In this subsection we investigate the nonlocal gates that can be generated by a given Hamiltonian H for a time duration t, that is, $U(t)=\exp(iHt)$. Recall that $\mathfrak{k}$ in Eq. (7) is the Lie subalgebra corresponding to K, the Lie subgroup of all the local gates. Therefore, $\mathfrak{k}$ can be viewed as the local part in su(4), and $\mathfrak{p}$ as the nonlocal part. If the Hamiltonian H contains the nonlocal part, that is, $iH\cap\mathfrak{p}\neq\varnothing$, then H can generate nonlocal gates.

We first consider a Hamiltonian H for which iH is in the Cartan subalgebra $\mathfrak{a}$, and then extend to the general case. Assume $H=\frac{1}{2}(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)$. The local equivalence classes of $U(t)$ form a continuous flow on the 3-torus as time evolves. This provides us a geometric picture to study the properties of the gates generated by a given Hamiltonian. To illustrate the ideas, we consider the following examples.

Example 1 (exchange Hamiltonians). (1) Isotropic (Heisenberg) exchange: $H_1=\frac{1}{4}(\sigma_x^1\sigma_x^2+\sigma_y^1\sigma_y^2+\sigma_z^1\sigma_z^2)$—In this case, the two-qubit gate $U(t)$ generated by the Hamiltonian H_1 is

$$U(t)=\exp(iH_1t)=\exp i\frac{t}{4}(\sigma_x^1\sigma_x^2+\sigma_y^1\sigma_y^2+\sigma_z^1\sigma_z^2). \tag{56}$$

Hence the Hamiltonian H_1 generates the flow $[t/2,t/2,t/2]$ on the 3-torus. The local invariants can thus be computed from Eq. (30):

$$G_1(t)=\frac{\mathrm{tr}^2(m)}{16\det U}=\left(\cos^3\frac{t}{2}-i\sin^3\frac{t}{2}\right)^2=\frac{e^{it}}{16}(3+e^{-2it})^2,$$

$$G_2(t)=\frac{\mathrm{tr}^2(m)-\mathrm{tr}(m^2)}{4\det U}=4\left(\cos^6\frac{t}{2}-\sin^6\frac{t}{2}\right)-\cos^3t=3\cos t. \tag{57}$$

We reduce the symmetry of the flow to the Weyl chamber $\mathfrak{a}^+$, as shown in Fig. 4. We obtain that for $t\in[2k\pi,2k\pi+\pi]$, the trajectory is $[t/2,t/2,t/2]$; and for $t\in[2k\pi+\pi,2(k+1)\pi]$, the trajectory is $[t/2,\pi-t/2,\pi-t/2]$. Therefore, the flow generated by the isotropic Hamiltonian H_1 evolves along OA_3A_1, which corresponds to all the local equivalence classes that can be generated by H_1. Moreover, it can easily be seen that $\sqrt{\mathrm{SWAP}}$ and its inverse are the only two perfect entanglers that can be achieved by this Hamiltonian.

(2) Two-dimensional exchange, i.e., XY Hamiltonian: $H_2=\frac{1}{4}(\sigma_x^1\sigma_x^2+\sigma_y^1\sigma_y^2)$—The Hamiltonian H_2 generates the flow $[t/2,t/2,0]$ for $t\in[2k\pi,2k\pi+\pi]$, and $[\frac{t}{2},\pi-\frac{t}{2},0]$ for $t\in[2k\pi+\pi,2(k+1)\pi]$. Hence the trajectory evolves along OA_2A_1. It is evident that H_2 can generate a set of perfect entanglers that corresponds to the line segments QA_2 and A_2M in $\mathfrak{a}^+$. Note that A_2M represents exactly the same local equivalence classes as QA_2. The local invariants of $U(t)$ are $G_1(t)=\cos^4(t/2)$ and $G_2(t)=1+2\cos t$.

(3) One-dimensional exchange, i.e., Ising Hamiltonian: $H_3=\frac{1}{4}\sigma_y^1\sigma_y^2$—The trajectory generated by the Hamiltonian H_3 in $\mathfrak{a}^+$ is $[t/2,0,0]$, which evolves along the line OA_1. Hence the gates generated by the Hamiltonian H_3 are all the controlled-U gates. As noted above, CNOT, located at L, is the only perfect entangler that can be generated by this Hamiltonian. The local invariants of $U(t)$ are $G_1(t)=\cos^2(t/2)$ and $G_2(t)=2+\cos t$.

For any arbitrary $H=\frac{1}{2}(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)$, the trajectory on the 3-torus is $[c_1t,c_2t,c_3t]$. If both c_1/c_2 and c_1/c_3 are rational, the trajectory generated by the Hamiltonian H forms a loop on the 3-torus. If either c_1/c_2 or c_1/c_3 is irrational, the trajectory forms a proper dense subset of 3-torus.

Next let us consider the case when $iH\in\mathfrak{p}$. Recall that we have $\mathfrak{p}=\cup_{k\in K}\mathrm{Ad}_k(\mathfrak{a})$. Hence for any arbitrary $iH\in\mathfrak{p}$, there exists a local gate $k\in\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ such that

$$\mathrm{Ad}_k(iH)=iH_a, \tag{58}$$

where $H_a=\frac{1}{2}(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)$. It follows that

$$U(t)=\exp(iHt)=\exp(k^\dagger iH_akt)=k^\dagger\exp\left(\frac{i}{2}(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)t\right)k. \tag{59}$$

Therefore, the trajectory of $U(t)$ in the Weyl chamber $\mathfrak{a}^+$ is $[c_1t,c_2t,c_3t]$. Equation (58) also implies that H and H_a have the same set of eigenvalues. We can thus use this property to derive the triplet $[c_1,c_2,c_3]$ explicitly. The following example shows how to find the flow in the Weyl chamber $\mathfrak{a}^+$ for a given Hamiltonian H with $iH\in\mathfrak{p}$.

Example 2 (generalized exchange with cross-terms). Consider the generalized anisotropic exchange Hamiltonian $H=\frac{1}{2}(J_{xx}\sigma_x^1\sigma_x^2+J_{yy}\sigma_y^1\sigma_y^2+J_{xy}\sigma_x^1\sigma_y^2+J_{yx}\sigma_y^1\sigma_x^2)$ discussed in Ref. [39]. The eigenvalues of H are

$$\frac{1}{2}\{\sqrt{(J_{xx}+J_{yy})^2+(J_{xy}-J_{yx})^2},-\sqrt{(J_{xx}+J_{yy})^2+(J_{xy}-J_{yx})^2},\sqrt{(J_{xx}-J_{yy})^2+(J_{xy}+J_{yx})^2},-\sqrt{(J_{xx}-J_{yy})^2+(J_{xy}+J_{yx})^2}\}, \tag{60}$$

whereas the eigenvalues of H_a are

$$\frac{1}{2}\{-c_1+c_3+c_2,-c_1-c_3-c_2,c_1+c_3-c_2,c_1-c_3+c_2\}. \tag{61}$$

Since H and H_a have the same set of eigenvalues, by comparing Eqs. (60) and (61) and recalling that $c_1\geqslant c_2\geqslant c_3\geqslant 0$, we find

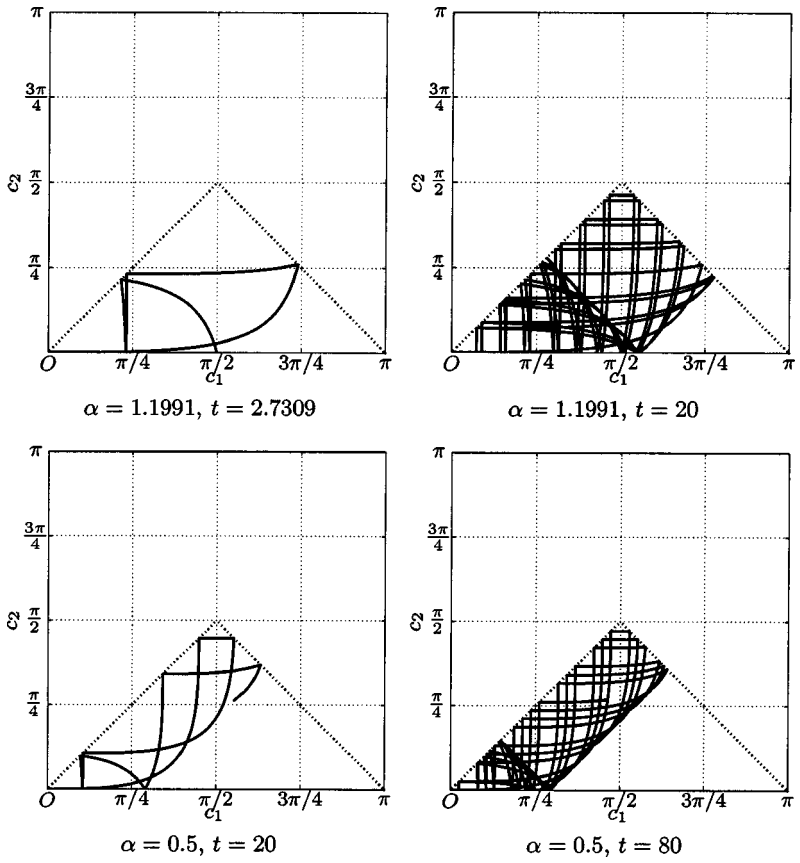


FIG. 5. The flow generated by H_J in the Weyl chamber $\mathfrak{a}^+$.

$$c_1=\frac{1}{2}(\sqrt{(J_{xx}+J_{yy})^2+(J_{xy}-J_{yx})^2}+\sqrt{(J_{xx}-J_{yy})^2+(J_{xy}+J_{yx})^2}),$$

$$c_2=\frac{1}{2}|\sqrt{(J_{xx}+J_{yy})^2+(J_{xy}-J_{yx})^2}-\sqrt{(J_{xx}-J_{yy})^2+(J_{xy}+J_{yx})^2}|, \tag{62}$$

$$c_3=0.$$

Therefore, the flow generated by this Hamiltonian in the Weyl chamber $\mathfrak{a}^+$ is $[c_1t,c_2t,0]$, which evolves in the plane OA_1A_2.

Now we consider the general case when $iH\in \mathrm{su}(4)$ and H contains both the local and nonlocal part. To derive the trajectory of $U(t)=\exp(iHt)$ on the 3-torus, we first compute the local invariants of $U(t)$ as in Eqs. (26) and (28):

$$G_1(t)=\frac{\mathrm{tr}^2(m(U(t)))}{16},$$

$$G_2(t)=\frac{\mathrm{tr}^2(m(U(t)))-\mathrm{tr}(m^2(U(t)))}{4}. \tag{63}$$

Then from the relation of the local invariants and c_i, we can obtain the flow $[c_1(t),c_2(t),c_3(t)]$ on the 3-torus by solving Eq. (30):

$$G_1=\cos^2c_1\cos^2c_2\cos^2c_3-\sin^2c_1\sin^2c_2\sin^2c_3+\frac{i}{4}\sin 2c_1\sin 2c_2\sin 2c_3,$$

$$G_2=4\cos^2c_1\cos^2c_2\cos^2c_3-4\sin^2c_1\sin^2c_2\sin^2c_3-\cos 2c_1\cos 2c_2\cos 2c_3. \tag{64}$$

Example 3 (Josephson junction charge-coupled qubits). For Josephson (charged-coupled) qubits [47], elementary two-qubit gates are generated by the Hamiltonian $H_J=-\frac{1}{2}E_J(\sigma_x^1+\sigma_x^2)+(E_J^2/E_L)\sigma_y^1\sigma_y^2$. If E_J is tuned to αE_L, $\alpha\in\mathbb{R}$, the local invariants can be obtained,

$$G_1=\frac{1}{(1+\alpha^2)^2}(\alpha^2(x^2+y^2-1)+x^2)^2,$$

$$G_2=\frac{1}{1+\alpha^2}(3\alpha^2-1-4y^2\alpha^2+8\alpha^2x^2y^2+4x^2-4x^2\alpha^2), \tag{65}$$

where

$$x=\cos\alpha^2E_Lt,\quad y=\cos\sqrt{(\alpha^2+1)}\alpha E_Lt. \tag{66}$$

By solving Eq. (64), we find that the flow generated by this Hamiltonian on the 3-torus is

$$c_1(t)=\alpha^2E_Lt-\omega(t),$$

$$c_2(t)=\alpha^2 E_L t+\omega(t), \tag{67}$$

$$c_3(t)=0,$$

where $\omega(t)=\tan^{-1}\sqrt{(1+\alpha^2y^2)/(\alpha^2-\alpha^2y^2)}$. Since $c_3=0$, the Hamiltonian H_J can reach only those local equivalence classes on the base OA_1A_2, as shown in Fig. 4. Therefore, the Hamiltonian H_J is not able to generate the perfect entangler [$\sqrt{\text{SWAP}}$]. The trajectory generated by H_J in the Weyl chamber $\mathfrak{a}^+$ is shown in Fig. 5.

For the Hamiltonian H_J to achieve [CNOT], we need to solve Eq. (65) for $G_1=0$ and $G_2=1$. After some algebraic derivations, we find

$$x^2=\frac{1}{2},\quad y^2=\frac{\alpha^2-1}{2\alpha^2}. \tag{68}$$

It follows that

$$t=\frac{(2k+1)\pi}{4\alpha^2E_L},$$

$$2\alpha^2\cos\sqrt{1+\alpha^{-2}}\,\frac{2k+1}{4}\pi=\alpha^2-1, \tag{69}$$

where $k\in\mathbb{Z}$. When $E_L=1$, numerical solution of these expressions shows that the minimum time solution for the Hamiltonian H_J to achieve [CNOT] is obtained for $\alpha=1.1991$, and the minimum time is 2.7309.

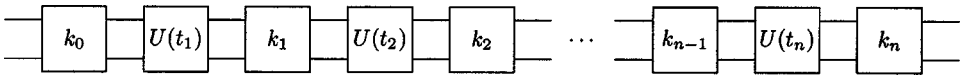
Note that when the Hamiltonian H contains only the nonlocal part, that is, $iH\in\mathfrak{p}$, the flow generated by the Hamiltonian on the 3-torus has constant velocity. However, when the Hamiltonian H contains both the local and nonlocal part, the velocity of the flow on the 3-torus is usually time dependent as shown in the above example.

B. Design of universal quantum circuits

Now let us consider how to generate *any* arbitrary two-qubit operation from a given two-body Hamiltonian together with local gates. The local gates form the Lie subgroup $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, which also contains all the single-qubit operations. We will show that by applying the Hamiltonian at most three times, together with four appropriate local gates, we can exactly simulate any arbitrary two-qubit gate, i.e., we can implement any SU(4) operation. Consequently, if the accessibility of any local gate is assumed, this results in satisfying the universality condition needed for quantum computation or simulation in a very efficient manner.

From the discussion in the preceding subsection, we know that a given Hamiltonian is not able to generate any arbitrary two-qubit operation simply by turning it on for a certain time period. Generally, the set of the gates that can be generated by a Hamiltonian directly is a one-dimensional subset of the 3-torus. For example, we know that [$\sqrt{\text{SWAP}}$] can be directly generated from the isotropic exchange interaction between two physical qubits, whereas [CNOT] cannot be obtained in this way [2] (unless encoding into multiple qubits is employed [35]). [CNOT] can however be achieved by a circuit consisting of two $\sqrt{\text{SWAP}}$ and a local gate [32]. We shall adopt the approach of constructing a quantum circuit that contain both nonlocal gates generated by a given Hamiltonian and local gates, and show that this quantum circuit can simulate any arbitrary nonlocal two-qubit operation exactly with only a small number of operations.

Consider a Hamiltonian H with $iH\in\mathfrak{p}$. The gate generated by this Hamiltonian for a time duration t is $U(t)=\exp(iHt)$. Consider the following prototype quantum circuit:



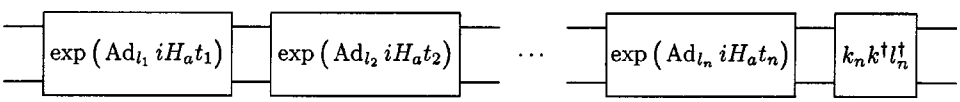
where k_j are local gates, and n a given integer. Note that the circuit is to be read from left to right. The matrix representation of the above quantum circuit is

$$k_nU(t_n)k_{n-1}\cdots k_2U(t_2)k_1U(t_1)k_0. \tag{70}$$

We will investigate the nonlocal gates that can be simulated by this quantum circuit. Recall that for this Hamiltonian H, there exists a local gate $k\in\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ such that $\mathrm{Ad}_k(iH)=iH_a$, where $H_a=\frac{1}{2}(c_1\sigma_x^1\sigma_x^2+c_2\sigma_y^1\sigma_y^2+c_3\sigma_z^1\sigma_z^2)$. Hence

$$U(t)=\exp(iHt)=\exp(\mathrm{Ad}_{k^\dagger}iH_at). \tag{71}$$

Let $l_j=(kk_{j-1}\cdots k_0)^\dagger$, quantum circuit (70) can now be described as



and its matrix representation is

$$k_n k^{\dagger} l_n^{\dagger} \exp(\mathrm{Ad}_{l_n} iH_a t_n) \cdots \exp(\mathrm{Ad}_{l_2} iH_a t_2) \exp(\mathrm{Ad}_{l_1} iH_a t_1). \tag{72}$$

We can then pick k_j such that l_j are in the Weyl group $W(G,K)$. In that case, we have $\mathrm{Ad}_{l_j} iH_a t_j \in \mathfrak{a}$. Since $\mathfrak{a}$ is a maximal Abelian subalgebra, the quantum circuit in Eq. (72) is locally equivalent to

$$\exp(\mathrm{Ad}_{l_n} iH_a t_n + \mathrm{Ad}_{l_2} iH_a t_2 + \cdots + \mathrm{Ad}_{l_1} iH_a t_1). \tag{73}$$

Proposition 2 tells us that the Weyl group $W(G,K)$ is generated by the reflections s_α given in Eq. (15). Hence for a given s_α, where $\alpha \in \Delta_{\mathfrak{p}}$, there exists a local gate k_α such that for any $X \in \mathfrak{a}$, $\mathrm{Ad}_{k_\alpha}(X) = s_\alpha(X)$. Following the procedure in Lemma 2.4, Chap. VII in Ref. [42], we obtain k_α as in the following:

α	$s_\alpha([c_1,c_2,c_3])$	k_α
$i(c_3-c_2)$	$[c_1,c_3,c_2]$	$\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_x^1+\frac{i}{2}\sigma_x^2\right)$
$i(c_2-c_1)$	$[c_2,c_1,c_3]$	$\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_z^1+\frac{i}{2}\sigma_z^2\right)$
$i(c_1-c_3)$	$[c_3,c_2,c_1]$	$\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_y^1+\frac{i}{2}\sigma_y^2\right)$
$i(c_2+c_3)$	$[c_1,-c_3,-c_2]$	$\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_x^1-\frac{i}{2}\sigma_x^2\right)$
$i(c_1+c_2)$	$[-c_2,-c_1,c_3]$	$\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_z^1-\frac{i}{2}\sigma_z^2\right)$
$i(c_1+c_3)$	$[-c_3,c_2,-c_1]$	$\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_y^1-\frac{i}{2}\sigma_y^2\right)$

Recall that the flow generated by $\exp(iH_a t)$ on the 3-torus is $[c_1 t, c_2 t, c_3 t]$. By choosing some appropriate l_j from the Weyl group $W(G,K)$, we can steer the flow generated by the Hamiltonian. For example, if we want to change the flow from $[c_1 t, c_2 t, c_3 t]$ into $[c_1 t, -c_3 t, -c_2 t]$, we can simply apply the reflection $k_{i(c_2+c_3)}$,

$$\begin{aligned}\mathrm{Ad}_{k_{i(c_2+c_3)}}(iH_a t) &= \exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_x^1-\frac{i}{2}\sigma_x^2\right)(iH_a t)\\ &\quad\times\exp\frac{\pi}{2}\left(-\frac{i}{2}\sigma_x^1+\frac{i}{2}\sigma_x^2\right)\\ &= \frac{i}{2}(c_1\sigma_x^1\sigma_x^2 - c_3\sigma_y^1\sigma_y^2 - c_2\sigma_z^1\sigma_z^2)t.\end{aligned} \tag{74}$$

The following example exemplifies this idea.

Example 4 (construction of CNOT from isotropic exchange Hamiltonian). Consider the isotropic Hamiltonian $H_1 = \frac{1}{4}(\sigma_x^1\sigma_x^2 + \sigma_y^1\sigma_y^2 + \sigma_z^1\sigma_z^2)$. Our goal is to simulate [CNOT] by a quantum circuit containing local gates and two-qubit gates generated by H_1. As shown in Fig. 6, the flow generated by $U(t) = \exp(iH_1 t)$ in the Weyl chamber $\mathfrak{a}^+$ is $[t/2,t/2,t/2]$, which evolves along OA_3 for $t \in [0,\pi]$. In the Weyl chamber $\mathfrak{a}^+$, the point L ($[\pi/2,0,0]$) corresponds to [CNOT]. We then want to switch the flow from $[t/2,t/2,t/2]$ to $[t/2,-t/2,-t/2]$ at a certain time instant so that the flow can reach the point L. In order to do that, we can simply apply the reflections $s_{i(c_2+c_3)}$ and $s_{i(c_3-c_2)}$ in series. The corresponding local gate is thus

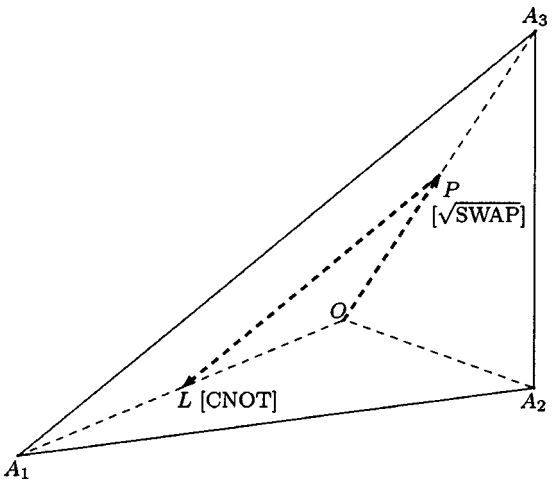


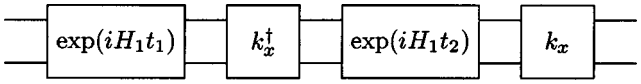
FIG. 6. The flow generated by the quantum circuit $k_x \exp(iH_1 t_2) k_x^{\dagger} \exp(iH_1 t_1)$ in the Weyl chamber $\mathfrak{a}^+$.

$$\begin{aligned}k_x &= k_{i(c_3-c_2)} k_{i(c_2+c_3)}\\ &= \exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_x^1+\frac{i}{2}\sigma_x^2\right)\exp\frac{\pi}{2}\left(\frac{i}{2}\sigma_x^1-\frac{i}{2}\sigma_x^2\right)\\ &= \exp\frac{i\pi}{2}\sigma_x^1,\end{aligned} \tag{75}$$

and we have

$$\begin{aligned}k_x \exp(iH_1 t) k_x^{\dagger} &= \exp(\mathrm{Ad}_{k_x} iH_1 t)\\ &= \exp\frac{i}{4}(\sigma_x^1\sigma_x^2 - \sigma_y^1\sigma_y^2 - \sigma_z^1\sigma_z^2)t.\end{aligned} \tag{76}$$

Now consider the following quantum circuit:



The flow generated by this quantum circuit evolves along the line OA_3 for $t \in [0,t_1]$, and then switches into a direction parallel to the line PL in the plane OA_3A_1 for $t \geqslant t_1$. The matrix representation of this quantum circuit is

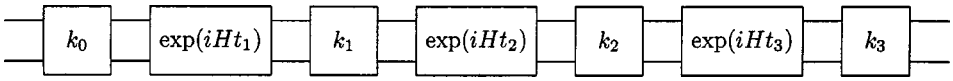
$$\begin{aligned}&k_x \exp(iH_1 t_2) k_x^{\dagger} \exp(iH_1 t_1)\\ &= \exp\frac{i}{4}(\sigma_x^1\sigma_x^2 - \sigma_y^1\sigma_y^2 - \sigma_z^1\sigma_z^2)t_2\\ &\quad\times\exp\frac{i}{4}(\sigma_x^1\sigma_x^2 + \sigma_y^1\sigma_y^2 + \sigma_z^1\sigma_z^2)t_1\end{aligned}$$

$$= \exp\left(\frac{t_1+t_2}{2} \frac{i}{2} \sigma_x^1 \sigma_x^2 + \frac{t_1-t_2}{2} \frac{i}{2} \sigma_y^1 \sigma_y^2 + \frac{t_1-t_2}{2} \frac{i}{2} \sigma_z^1 \sigma_z^2 \right). \quad (77)$$

Hence the terminal point of the flow is $[(t_1+t_2)/2,(t_1-t_2)/2,(t_1-t_2)/2]$. If we choose $t_1=\pi/2$ and $t_2=\pi/2$, the terminal point is none other than $[\pi/2,0,0]$, and thus the quantum circuit simulates [CNOT]. As shown in Fig. 6, the flow generated by this quantum circuit is OPL, which goes along the line OP first, and after hitting the point P, it turns to the point L along the line PL. Since P is nothing but $\sqrt{\text{SWAP}}$, and $t_2=t_1=\pi/2$, we arrive at the known result that [CNOT] can be simulated by a circuit consisting of two $\sqrt{\text{SWAP}}$ and a local gate [32].

We now derive the following theorem which asserts that when $n=3$ quantum circuit (70) can simulate *any* arbitrary nonlocal two-qubit gate. This theorem provides a geometric approach to construct a quantum circuit to simulate any arbitrary two-qubit gate from a two-body interaction Hamiltonian.

Theorem 3 (universal quantum circuit). Given a Hamiltonian H with $iH \in \mathfrak{p}$, any arbitrary two-qubit gate $U \in \mathrm{SU}(4)$ can be simulated by the following quantum circuit:



where k_j are local gates.

Proof. From Cartan decomposition of su(4) in Sec. II B, any arbitrary two-qubit gate $U \in \mathrm{SU}(4)$ can be written in the following form:

$$U = k_l \exp\left\{ \frac{i}{2} (\gamma_1 \sigma_x^1 \sigma_x^2 + \gamma_2 \sigma_y^1 \sigma_y^2 + \gamma_3 \sigma_z^1 \sigma_z^2) \right\} k_r, \quad (78)$$

where k_l and k_r are local gates, and γ_1, γ_2, $\gamma_3 \in \mathbb{R}$. We also know that for any given $iH \in \mathfrak{p}$, there exists a local gate k such that $\mathrm{Ad}_k(iH) = iH_a$, where $H_a = \frac{1}{2}(c_1 \sigma_x^1 \sigma_x^2 + c_2 \sigma_y^1 \sigma_y^2 + c_3 \sigma_z^1 \sigma_z^2)$ and $c_1 \geqslant c_2 \geqslant c_3 \geqslant 0$. Therefore, the flow generated by iH on the 3-torus is $[c_1 t, c_2 t, c_3 t]$. The matrix representation of the above quantum circuit is

$$k_3 \exp(iHt_3) k_2 \exp(iHt_2) k_1 \exp(iHt_1) k_0. \quad (79)$$

Let

$$l_1 = (k k_0 k_r^\dagger)^\dagger,$$
$$l_2 = (k k_1 k_0 k_r^\dagger)^\dagger, \quad (80)$$
$$l_3 = (k k_2 k_1 k_0 k_r^\dagger)^\dagger;$$

the quantum circuit (79) can be written as

$$k_3 k^\dagger l_3^\dagger \exp(\mathrm{Ad}_{l_3} iH_a t_3) \exp(\mathrm{Ad}_{l_2} iH_a t_2) \exp(\mathrm{Ad}_{l_1} iH_a t_1) k_r. \quad (81)$$

Choose some appropriate local gates k_0, k_1, and k_2 such that

$$l_1 = I,$$
$$l_2 = k_{i(c_3-c_2)} k_{i(c_1+c_3)}, \quad (82)$$
$$l_3 = k_{i(c_2-c_1)} k_{i(c_3-c_2)} k_{i(c_1+c_2)},$$

and let $k_3 = k_l l_3 k$. It follows that the quantum circuit (79) is now

$$\begin{aligned} & k_l \exp(\mathrm{Ad}_{l_3} iH_a t_3) \exp(\mathrm{Ad}_{l_2} iH_a t_2) \exp(\mathrm{Ad}_{l_1} iH_a t_1) k_r \\ &= k_l \exp\left(\frac{i}{2} (c_3 \sigma_x^1 \sigma_x^2 - c_2 \sigma_y^1 \sigma_y^2 - c_1 \sigma_z^1 \sigma_z^2) t_3 \right) \\ &\quad \times \exp\left(\frac{i}{2} (-c_3 \sigma_x^1 \sigma_x^2 - c_1 \sigma_y^1 \sigma_y^2 + c_2 \sigma_z^1 \sigma_z^2) t_2 \right) \\ &\quad \times \exp\left(\frac{i}{2} (c_1 \sigma_x^1 \sigma_x^2 + c_2 \sigma_y^1 \sigma_y^2 + c_3 \sigma_z^1 \sigma_z^2) t_1 \right) k_r \\ &= k_l \exp\Big[(c_1 t_1 - c_3 t_2 + c_3 t_3) \frac{i}{2} \sigma_x^1 \sigma_x^2 + (c_2 t_1 - c_1 t_2 \\ &\quad - c_2 t_3) \frac{i}{2} \sigma_y^1 \sigma_y^2 + (c_3 t_1 + c_2 t_2 - c_1 t_3) \frac{i}{2} \sigma_z^1 \sigma_z^2 \Big) k_r. \end{aligned} \quad (83)$$

To simulate the two-qubit gate U in Eq. (78), we only need to solve the following equation:

$$\begin{pmatrix} c_1 & -c_3 & c_3 \\ c_2 & -c_1 & -c_2 \\ c_3 & c_2 & -c_1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \gamma_3 \end{pmatrix}. \quad (84)$$

Since

$$\det \begin{pmatrix} c_1 & -c_3 & c_3 \\ c_2 & -c_1 & -c_2 \\ c_3 & c_2 & -c_1 \end{pmatrix} = c_1(c_1^2 - c_2 c_3) + (c_1+c_2)c_3^2 + (c_1+c_3)c_2^2 > 0, \quad (85)$$

we can always find a solution for Eq. (84). Therefore, quantum circuit (79) can simulate any arbitrary two-qubit gate. ■

From the above constructive proof, it is clear that together with four appropriate local gates, we can simulate any arbitrary two-qubit gate by turning on a two-body interaction Hamiltonian for at most three times. Also note that in the proof, the way to choose the local gates k_0, k_1, and k_2 is not unique. There are many different ways to choose the local gates and time parameters so as to construct the quantum circuit that achieves the same two-qubit operation. We therefore can pick the one that is optimal in terms of some cost index such as time.

VI. CONCLUSION

In this paper we have derived a geometric approach to study the properties of nonlocal two-qubit operations, starting from the Cartan decomposition of su(4) and making use of the Weyl group. We first showed that the geometric structure of nonlocal gates is a 3-torus. By further reducing the symmetry, the geometric representation of nonlocal gates was seen to be conveniently visualized as a tetrahedron. Each point inside this tetrahedron corresponds to a different equivalent class of nonlocal gates. We then investigated the properties of those two-qubit operations that can generate maximal entanglement. We provided a proof of the condition of Makhlin for perfect entanglers [2] and then derived the corresponding geometric description of these gates within the tetrahedral representation. It was found that exactly half of the nonlocal two-qubit operations result in maximal entanglement, corresponding to a seven-faced polyhedron with volume equal to one half of the tetrahedron. Lastly, we investigated the nonlocal operations that can be generated by a given Hamiltonian. We proved that given a two-body interaction Hamiltonian, it is always possible to explicitly construct a quantum circuit for exact simulation of any arbitrary nonlocal two-qubit gate by turning on the two-body interaction for at most three times, together with four local gates. This guarantees that a highly *efficient* simulation of nonlocal gates can be made with any Hamiltonian consisting of arbitrary two-qubit interactions and allowing control of single-qubit operations.

ACKNOWLEDGMENTS

We acknowledge helpful discussions with Dr. Markus Grassel. We thank the NSF for financial support under ITR Grant No. EIA-0205641 (S.S. and K.B.W.). J.V. and K.B.W.'s effort was also sponsored by the Defense Advanced Research Projects Agency (DARPA), the Air Force Laboratory, Air Force Materiel Command, USAF, under Contract No. F30602-01-2-0524, and the Office of Naval Research under Grant No. FDN 00014-01-1-0826.

[1] M. Grassl, M. Rötteler, and T. Beth, Phys. Rev. A **58**, 1833 (1998).
[2] Y. Makhlin, e-print quant-ph/0002045.
[3] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (2000).
[4] P. Zanardi, Phys. Rev. A **63**, 040304 (2001).
[5] W. Dür, G. Vidal, J.I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).
[6] J.I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[7] W. Dür and J.I. Cirac, Phys. Rev. A **64**, 012317 (2001).
[8] B. Kraus and J.I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[9] G. Vidal, K. Hammerer, and J.I. Cirac, e-print quant-ph/0112168 version 2.
[10] G. Vidal, L. Masanes, and J.I. Cirac, Phys. Rev. Lett. **88**, 047905 (2002).
[11] G. Vidal and J.I. Cirac, Phys. Rev. Lett. **88**, 167903 (2002).
[12] K. Hammerer, G. Vidal, and J.I. Cirac, e-print quant-ph/0205100.
[13] N. Khaneja, R. Brockett, and S.J. Glaser, Phys. Rev. A **63**, 032308 (2001).
[14] J. Gruska, *Quantum Computing* (McGraw-Hill, London, 1999).
[15] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[16] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).
[17] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[18] D.P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[19] A. Barenco, Proc. R. Soc. London, Ser. A **449**, 679 (1995).
[20] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[21] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[22] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).
[23] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[24] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).
[25] J.-L. Brylinski and R. Brylinski, e-print quant-ph/0108062.
[26] J.L. Dodd, M.A. Nielsen, M.J. Bremner, and R.T. Thew, e-print quant-ph/0106064.
[27] M.J. Bremner, C.M. Dawson, J.L. Dodd, A. Gilchrist, A.W. Harrow, D. Mortimer, M.A. Nielsen, and T.J. Osborne, e-print quant-ph/0207072.
[28] A.Y. Vlasov, Phys. Rev. A **63**, 054302 (2001).
[29] A.Y. Vlasov, J. Math. Phys. **43**, 2959 (2002).
[30] A. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).
[31] A.W. Harrow, B. Recht, and I.L. Chuang, e-print quant-ph/011031.
[32] G. Burkard, D. Loss, D.P. DiVincenzo, and J.A. Smolin, Phys. Rev. B **60**, 11 404 (1999).
[33] C.H. Bennett, J.I. Cirac, M.S. Leifer, D.W. Leung, N. Linden, S. Popescu, and G. Vidal, Phys. Rev. A **66**, 012305 (2002).
[34] D. Bacon, J. Kempe, D.A. Lidar, and K.B. Whaley, Phys. Rev. Lett. **85**, 1758 (2000).
[35] D.P. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K.B. Whaley, Nature (London) **408**, 337 (2000).

[36] J. Kempe, D. Bacon, D. Lidar, and K. Whaley, Phys. Rev. A **63**, 042307 (2001).
[37] J. Kempe, D. Bacon, D.P. DiVincenzo, and K.B. Whaley, Quantum Inf. Comput. **1**, 241 (2001); e-print quant-ph/0112013.
[38] J. Kempe and K.B. Whaley, Phys. Rev. A **65**, 052330 (2002).
[39] J. Vala and K.B. Whaley, Phys. Rev. A **66**, 022304 (2002).
[40] D. Lidar and L.-A. Wu, Phys. Rev. Lett. **88**, 017905 (2001).
[41] S. Helgason, *Differential Geometry, Lie Groups, and Symmetric Spaces* (Academic, New York, 1978).
[42] R.N. Cahn, *Semi-Simple Lie Algebras and Their Representations* (Benjamin/Cummings, Menlo Park, CA, 1984), available at http://www-physics.lbl.gov/~rncahn/cahn.html
[43] W.Y. Hsiang, *Lectures on Lie Groups* (World Scientific, Singapore, 1998).
[44] F.W. Warner, *Foundations of Differentiable Manifolds and Lie Groups* (Springer-Verlag, New York, 1983).
[45] A. Imamoglu, D.D. Awschalom, G. Burkard, D.P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, Phys. Rev. Lett. **83**, 4204 (1999).
[46] I.H. Deutsch and P.S. Jessen, Phys. Rev. A **57**, 1972 (1998).
[47] Y. Makhlin, G. Schön, and A. Shnirman, Nature (London) **395**, 305 (1999).