Gate simulation and lower bounds on the simulation time

Robert Zeier,* Markus Grassl,[†] and Thomas Beth[‡]

Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 76128 Karlsruhe, Germany

Unitary operations are the building blocks of quantum programs. Our task is to design efficient or optimal implementations of these unitary operations by employing the intrinsic physical resources of a given n-qubit system. The most common versions of this task are known as Hamiltonian simulation and gate simulation, where Hamiltonian simulation can be seen as an infinitesimal version of the general task of gate simulation. We present a Lie-theoretic approach to Hamiltonian simulation and gate simulation. From this, we derive lower bounds on the time complexity in the n-qubit case, generalizing known results to both even and odd n. To achieve this we develop a generalization of the so-called magic basis for two-qubits. As a corollary, we note a connection to entanglement measures of concurrence-type.

PACS number(s): 03.67.Lx, 03.67.Mn

I. INTRODUCTION

As a starting point for the emerging field of quantum computation (for a review see, e.g., Refs. [1,2]) Feynman [3] established in 1982 a connection between simulation of quantum systems by computers on the one hand and computation using quantum systems on the other hand. Since this time many different models for computation using quantum systems have been proposed.

In all these models the common target is to constructively implement unitary operations by employing the intrinsic physical resources. Forming the counterpart of operations on a classical computer, these unitary operations build the components of quantum programs. Whichever (reasonable) system is provided to us by an experimentalist, we exploit the resources immanent to the system.

In this paper we confine ourselves to n-qubit systems where the resources are given by local unitary operations and by the natural time evolution specified by the Hamilton operator. This allows us to implement a given unitary operation by interrupting the natural time evolution with local unitary operations. Referring to such implementations as programs, our objective is to study efficient or optimal programs. To achieve this, usually two different versions of this problem are considered. Hamiltonian simulation is the one version and denotes an infinitesimal implementation of unitary operations, i.e., the unitary operation is in a neighborhood of the identity. The second version is called gate simulation and describes an implementation of unitary operations not restricted to a neighborhood of the identity. We give an exact definition of both versions in Sec. II.

In this paper we address two major topics. First we consider two-qubit systems. Combining the manifold results known for two-qubit systems, we can close gaps and simplify the line of reasoning. In addition, by using Lie-theoretic methods we derive a unified approach to the methodology. The motivation for this extensive reconsideration is twofold:

First, we show that understanding simple cases in detail helps to generalize them to higher-dimensional systems. Second, we obtain generally applicable (Lie-theoretic) methods that provide tools in the analysis of higher-dimensional systems.

Beyond this, the two-qubit case is interesting in its own. We can characterize the minimal time for Hamiltonian simulation directly using arguments from Lie theory. With the help of this characterization we explain and reprove a majorizationlike condition [4] for the minimal simulation time. By employing the Weyl group of the corresponding Lie algebra, we are able to simplify and clarify the known approach of Ref. [4], especially with respect to Ref. [5]. In the case of two-qubit systems we consider gate simulation as well. We present a refined analysis of the majorizationlike condition of Refs. [6,7], which will be built explicitly on the results of Ref. [5].

The second major topic deals with the case of general n-qubit systems. We first discuss a generalization of the so-called magic basis [8,9] to higher-dimensional systems. With this information on the structure of unitary operations we develop lower bounds on the minimal time for gate simulations. Our method applies to all n-qubit systems and generalizes a result of Ref. [10] for even n. We also discuss the used techniques in connection to entanglement measures, in particular, the concurrence [9,11].

The whole text is written in a Lie-theoretic flavor. For further reference, the Lie-theoretic concepts needed in the text will be introduced briefly in Sec. III. Using this theory puts us in the position to formulate strong arguments in a coherent language.

In Sec. II we introduce our model and in Sec. III we state the Lie-theoretic concepts needed in the main body of the text. The Hamiltonian simulation for two-qubits will be discussed in Sec. IV, followed by the analysis of gate simulation for two-qubits in Sec. V. The generalization of the magic basis for two-qubits is considered together with lower bounds on the time complexity for general n-qubit systems in Sec. VI. In Sec. VII we give a brief outline to related work, in Sec. VIII we continue with a discussion of connections of our approach to concurrence-type entanglement measures, and in Sec. IX we close with the conclusion. In the appendix

---

*Electronic address: zeier@ira.uka.de

†Electronic address: grassl@ira.uka.de

‡Electronic address: EISS_Office@ira.uka.de

we recall a spectral approach to infinitesimal Hamiltonian simulation.

II. THE MODEL

We consider a system of n qubits, where $n \in \mathbb{N}$ is finite. This system can be modeled within an n-fold tensor product $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ of n 2D complex vector spaces $\mathbb{C}^2$, i.e., a tensor product of single qubits. The time evolution of the system is governed by the Schrödinger equation for the time-evolution operator (see, e.g., [12], p. 72),

$$\frac{d}{dt}U(t) = (-iH)U(t),$$

where t denotes the time, $U(t)$ the time evolution operator, and H the Hamilton operator, which is supposed to be time-independent ($\hbar = 1$). Because of the irrelevance of a global phase in quantum mechanics, we restrict ourselves to evolution operators from the special unitary group $SU(2^n)$.

In addition to the possibility to let the system evolve according to the evolution operator $U(t) = \exp(-iHt)$, in our model we allow the application of local unitary operators. A unitary operator is considered as local when it does not induce any interaction between different qubits, i.e., when it has the form of an n-fold tensor product $U_1 \otimes \cdots \otimes U_n$ of unitary operators $U_i \in SU(2)$ with $i \in \{1, \ldots, n\}$. The time for the application of local unitary operations is negligible and assumed to be zero. Thereby we have specified the available resources that constitute the possibilities to control the system.

We emphasize that, for mathematical reasons, we restrict our model to consider only systems for which the system Hamilton operators can be represented without use of local terms. As a consequence, in the case of infinitesimal Hamiltonian simulation we can simulate Hamilton operators exactly only if the Hamilton operator can be represented without use of local terms. To remove the local terms of a system Hamilton operator, one usually employs some approximations (see, e.g., [4], p. 3 or [13], p. 288). But we refrain from considering such approximations. In addition, avoiding local terms in Hamilton operators seems to release us from some problems with infinite programs, i.e., an infinite number $m = \infty$ of steps (see below). In Ref. [14] it is analyzed under which conditions we need infinite programs for time optimal control in the more general setting, which includes local terms in the system Hamilton operator. Nevertheless, we consider for technical reasons all types of programs, even infinite ones. The available resources will be utilized below in three ways.

First, we consider the simulation of a unitary gate, i.e., a unitary operator. This notion of simulation means that the system is able to implement a given unitary gate by interrupting the natural time evolution with local unitary operations. Definition 1 states this in a more formal way. The term "gate simulation" was introduced in Ref. [4] on p. 3.

Definition 1 (gate simulation). An n-qubit system with Hamilton operator H and local unitary operators available simulates a unitary gate U in time t if there exists local

unitary operators U_0 and U_j as well as times $t_j \geq 0$ with $t = \sum_{j=1}^m t_j$, $j \in \mathbb{N}$, $1 \leq j \leq m$, and $m \in \mathbb{N} \cup \{0, \infty\}$, so that

$$U = \left[\prod_{j=1}^m U_j \exp(-iHt_j) \right] U_0.$$

Remark. Due to the noncommutativity of the unitary group we restrict the symbol Π for elements V_j from the unitary group to the following meaning:

$$\prod_{j=e}^f V_j := \begin{cases} \left(\prod_{j=e+1}^f V_j \right) V_e & \text{for } f \geq e, \\ \text{id} & \text{for } f < e, \end{cases}$$

where $e, f \in \mathbb{Z}$, and the identity element of the unitary group is denoted by id. In the case of f infinite, the symbol Π represents an element from the closure of convergent sequences.

Second, we introduce a particular concept of infinitesimal simulation of a unitary gate. A given unitary gate U is treated as a point of a one-parameter group $\exp(-iH't')$. The infinitesimal simulation of the Hamilton operator H' denotes that the system simulates the corresponding one-parameter group for infinitesimal times t', i.e., the derivatives of the one-parameter group and of the simulation coincide for infinitesimal times. We emphasize that in Definition 2 the notion of infinitesimal Hamiltonian simulation is defined independently of the unitary gate U.

Definition 2 (infinitesimal Hamiltonian simulation). An n-qubit system with Hamilton operator H and local unitary operators available simulates an Hamilton operator H' infinitesimally in time t if there exists local unitary operators U_0 and U_j as well as times $t_j \geq 0$ where $t = \sum_{j=1}^m t_j$, $j \in \mathbb{N}$, $1 \leq j \leq m$, and $m \in \mathbb{N} \cup \{0, \infty\}$ so that $\Pi_{j=0}^m U_j$ is equal to the identity of the unitary group and the following equation holds:

$$\lim_{\substack{t' \to 0 \\ t' > 0}} \left[\frac{d}{dt'} \exp(-it'H') \right]$$

$$= \lim_{\substack{t' \to 0 \\ t' > 0}} \left(\frac{d}{dt'} \left\{ \left[\prod_{j=1}^m U^j \exp(-it'Ht_j) \right] U_0 \right\} \right). \quad (1)$$

Remark. The condition $\Pi_{j=0}^m U_j = \text{id}$ ensures that our program specified by U_0, the U_js, and the t_js operates nearby the identity for $t' \to 0$.

We note that in Refs. [15–18] the notion of infinitesimal Hamiltonian simulation was extended by the so-called first-order approximation to unitary operators. Similar ideas were used in Ref. [4] where it was proposed to follow the evolution of the system exactly by the Hamiltonian simulation. Concurrently, it was remarked in Ref. [4] that to follow the evolution of the system exactly is only possible infinitesimally, as the control is not continuous. In this text we do not consider such approximations.

Though Definition 2 presents the essential meaning of infinitesimal Hamiltonian simulation, it appears to be very unpractical. Thus we present an equivalent condition, which is usually formulated as definition [15–19].

Lemma 1. An n-qubit system with Hamilton operator H and local unitary operators available simulates the Hamilton operator H' infinitesimally in time t if and only if there exists local unitary operators V_j as well as times $t_j \geq 0$ with $t = \Sigma_{j=1}^m t_j$, $j \in \mathbb{N}$, $1 \leq j \leq m$, and $m \in \mathbb{N} \cup \{0, \infty\}$ so that the following equation holds:

$$H' = \sum_{j=1}^m t_j (V_j^{-1} H V_j). \qquad (2)$$

Proof. The "only-if" case: The left-hand side of Eq. (1) equals $-iH'$ and the right-hand side of Eq. (1) equals

$$\lim_{\substack{t' \to 0 \\ t' > 0}} \left[\frac{d}{dt'} \left(\left\{ \prod_{j=1}^m \exp[-it'(W_j H W_j^{-1})t_j] \right\} W_0 \right) \right], \qquad (3)$$

where

$$W_j = \begin{cases} U_m & \text{for } j = m, \\ W_{j+1} U_j & \text{for } 0 \leq j < m. \end{cases}$$

We differentiate, compute the limit, and equate the result of Eq. (3) with $-iH'$. After this we use $V_j := W_j^{-1}$ and $W_0 = \Pi_{j=0}^m U_j = \text{id}$ to obtain Eq. (2).

The "if" case: After insertion of Eq. (2) in Eq. (1) we obtain the "if" case. ∎

Third, we introduce in Definition 3 the notion of infinitesimal gate simulation, which depends explicitly on the given unitary gate U.

Definition 3 (infinitesimal gate simulation). An n-qubit system with Hamilton operator H and local unitary operators available simulates a unitary gate U infinitesimally in time t if there exists an Hamilton operator H' and local unitary gates U_1 and U_2 such that the equation $U = U_1 \exp(-iH')U_2$ holds and the system simulates the Hamilton operator H' infinitesimally in time t.

Remark. Actually, we do not use Definition 3 later in the text. But we state this definition to highlight that Definition 2 is independent of some unitary operator U and does not incorporate different decompositions of U which could lead to different Hamilton operators H'. The existence of different Hamilton operators H' will be employed in Sec. V.

Before we proceed, we discuss our model. Entanglement describes important nonlocal properties of states and gates. Because entanglement is invariant under local unitary operations [2], it seems reasonable to neglect the time needed to implement local unitary gates for the implementation of general unitary gates. This is supported by the fact that two-qubit gates are considered as significantly more difficult to implement than one-qubit gates [20]. Additionally, in nuclear magnetic resonance (NMR) the application of local unitary operations in zero time is expressed by the notion of the "fast control limit," which is conventionally considered as a good approximation. This is reasonable because local and nonlocal gates operate on different time scales [5,21,22].

III. LIE-THEORETIC PREPARATIONS

In this section we recall Lie-theoretic notions and methods that will be employed throughout the paper. This reflects the intimate connection of the considered problems to Lie theory, and it makes the text more readable and self-contained. For convenience, this section can also be regarded as a reference section. We remark that our presentation in this section was partly inspired by Refs. [5,23,24].

A. Basic concepts

For our purposes we can consider Lie groups as linear matrix groups, i.e., as closed subgroups of the general linear group. The tangent space to the Lie group G at the identity is isomorphic to the Lie algebra $\mathfrak{g}$ corresponding to G. A Lie algebra, which is in particular a vector space, comes with a bilinear and skew-symmetric multiplication operation called the Lie bracket [,]. The Lie algebra $\mathfrak{g}$ is closed under the Lie bracket and the Jacobi identity

$$[[g_1, g_2], g_3] + [[g_3, g_1], g_2] + [[g_2, g_3], g_1] = 0$$

holds for all elements $g_1, g_2, g_3 \in \mathfrak{g}$. We emphasize that we use only real or complex Lie algebras that are finite dimensional. For general reference on Lie groups and Lie algebras, please consult Refs. [25–35]. In the following let G denote a Lie group and $\mathfrak{g}$ its associated Lie algebra.

The map $\text{ad}_\mathfrak{g}(g)$ from the Lie algebra $\mathfrak{g}$ to itself is defined by $h \mapsto [g, h]$, where $h, g \in \mathfrak{g}$. With this notation, the adjoint representation of the Lie algebra $\mathfrak{g}$ in itself is given by $g \mapsto \text{ad}_\mathfrak{g}(g)$. Let $\text{ad}_\mathfrak{g}(\mathfrak{h})$ denote the set $\{\text{ad}_\mathfrak{g}(h) | h \in \mathfrak{h}\}$ for some subspace $\mathfrak{h}$ of the Lie algebra $\mathfrak{g}$. Now, we can introduce a symmetric bilinear form on the Lie algebra $\mathfrak{g}$: the Killing form $B_\mathfrak{g}(g, h) := \text{Tr}_\mathfrak{g}[\text{ad}_\mathfrak{g}(g) \circ \text{ad}_\mathfrak{g}(h)]$. If the Killing form is nondegenerate it can be thought as an inner product on the Lie algebra, although it does in general not fulfill the axiom of positivity.

Definition 4 (orthogonal symmetric Lie algebra) (see [25], p. 213 and [30], pp. 225–226 and 246). A pair $(\mathfrak{g}, \theta)$ is an orthogonal symmetric Lie algebra if (i) $\mathfrak{g}$ is a real Lie algebra, (ii) θ is an involutive automorphism of $\mathfrak{g}$, and (iii) the connected Lie group of linear transformations of $\mathfrak{g}$ generated by $\text{ad}_\mathfrak{g}(\mathfrak{k})$ is compact, where $\mathfrak{k}$ is the set of fixed points of θ in $\mathfrak{g}$.

Remark. An automorphism of a Lie algebra $\mathfrak{g}$ respects the Lie bracket, i.e., for all g and h in $\mathfrak{g}$ we have $\theta([g, h]) = [\theta(g), \theta(h)]$. An involutive automorphism is in addition self-inverse. Let $\mathfrak{k}$ and $\mathfrak{p}$ be the eigenspaces of θ in $\mathfrak{g}$ for the $+1$ and -1 eigenvalue, respectively. Consider the canonical decomposition $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$. Condition (ii) of Definition 4 is equivalent to (see [30], pp. 226-227)

$$[\mathfrak{k}, \mathfrak{k}] \subset \mathfrak{k}, [\mathfrak{k}, \mathfrak{p}] \subset \mathfrak{p}, [\mathfrak{p}, \mathfrak{p}] \subset \mathfrak{k}. \qquad (4)$$

In Ref. [5] this decomposition was called the Cartan decomposition. If Eq. (4) holds we can define θ by

$$\theta(k) = k \text{ for all } k \in \mathfrak{p} \text{ and } \theta(p) = -p \text{ for all } p \in \mathfrak{p}. \qquad (5)$$

In addition, when $\mathfrak{g}$ is the Lie algebra of a compact group G then Condition (iii) of Definition 4 is always true.

For further reference, we assume that $\mathfrak{g}$ is semisimple, i.e., that the Killing form of $\mathfrak{g}$ is nondegenerate, and that $(\mathfrak{g}, \theta)$ is an orthogonal symmetric Lie algebra. As an example, the Lie algebra $\mathfrak{su}(2^n)$, which corresponds to the Lie group $SU(2^n)$, is semisimple. We fix a canonical decomposition $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ satisfying Eq. (4) and a maximal Abelian subalgebra $\mathfrak{a}$ contained in $\mathfrak{p}$. Let $K = \exp(\mathfrak{k})$ and $A = \exp(\mathfrak{a})$ denote the subgroups of G generated by $\mathfrak{k}$ and $\mathfrak{a}$, respectively. After this preparation we obtain a decomposition $G = K \, A \, K$ of the Lie group G.

Fact 1 (K A K decomposition of the Lie group G*) ([25], Chap. V, Theorem 6.7).* With the notation as given above, the Lie group G corresponding to $\mathfrak{g}$ can be decomposed as

$$G = K \, A \, K.$$

Similar to the adjoint representation $\mathrm{ad}_{\mathfrak{g}}$ of a Lie algebra $\mathfrak{g}$ in itself, we can define the adjoint representation $\mathrm{Ad}_{\mathfrak{g}}$ of a Lie group G in its Lie algebra $\mathfrak{g}$. For an element $G \in G$ we introduce $\phi_G(G)$ as the map $H \mapsto G^{-1} H G$ with the signature $G \to G$. The map $\mathrm{Ad}_{\mathfrak{g}}(G)$ has the signature $\mathfrak{g} \to \mathfrak{g}$ and is defined as the differential of $\phi_G(G)$. For matrix representations we can write $\mathrm{Ad}_{\mathfrak{g}}(G)$ as the map $g \mapsto G^{-1} g G$. We use the shortcut $\mathrm{Ad}_{\mathfrak{g}}(K) := \cup_{K \in K} \mathrm{Ad}_{\mathfrak{g}}(K)$ and get the relation between the subspace $\mathfrak{p}$ and its Abelian subalgebra $\mathfrak{a}$:

Fact 2 ([25] Chap. V, Lemma 6.3 (iii)). The following equation holds:

$$\mathfrak{p} = [\mathrm{Ad}_{\mathfrak{g}}(K)](\mathfrak{a}).$$

B. The Weyl group and infinitesimal convexity

We use the notation

$$C_K(\mathfrak{a}) := \{K \in K | [\mathrm{Ad}_{\mathfrak{g}}(K)](a) = a \text{ for all } a \in \mathfrak{a}\}$$

and

$$N_K(\mathfrak{a}) := \{K \in K | [\mathrm{Ad}_{\mathfrak{g}}(K)](\mathfrak{a}) \subset \mathfrak{a}\},$$

respectively, for the centralizer $C_K(\mathfrak{a})$ and the normalizer $N_K(\mathfrak{a})$ of $\mathfrak{a}$ in K.

Definition 5 (Weyl group) (see [25], p. 284 or [27], p. 381). The Weyl group corresponding to $\mathfrak{a}$ is the factor group $N_K(\mathfrak{a})/C_K(\mathfrak{a})$. We denote this group by $\mathcal{W}(G, A)$, where $A = \exp(\mathfrak{a})$.

The Weyl group $\mathcal{W}(G, A)$ is finite (see Fact 3 below). In order to compute the Weyl group, we introduce the concept of restricted roots.

Definition 6 (restricted root) (cf. [27], p. 370). Let λ be a linear function on $\mathfrak{a}$. The linear subspace $\mathfrak{g}^\lambda$ is given by

$$\mathfrak{g}^\lambda = \{g \in \mathfrak{g} | [a, g] = \lambda(a) g \text{ for all } a \in \mathfrak{a}\}.$$

The linear function λ is called a restricted root of $\mathfrak{g}$ with respect to $\mathfrak{a}$ if $\mathfrak{g}^\lambda \neq \{0\}$ and λ is not identically zero on $\mathfrak{a}$. Let $\Delta_{\mathfrak{a}}$ denote the set of restricted roots of $\mathfrak{g}$ with respect to $\mathfrak{a}$.

Remark. In Ref. [27] on p. 370, the restricted roots are defined with respect to $i\mathfrak{a}$. But the concept of restricted roots can also be defined with respect to $\mathfrak{a}$.

Due to the fact that $\mathfrak{g}$ is semisimple, we deduce that the Killing form $B_{\mathfrak{g}}$ restricted to $\mathfrak{a} \times \mathfrak{a}$ is nondegenerate. With this in mind, a restricted root λ is equal to the map $a \mapsto B_{\mathfrak{g}}(a_\lambda, a)$, where $a_\lambda \in \mathfrak{a}$ is uniquely determined. We extend the Killing form to restricted roots by $B_{\mathfrak{g}}(\lambda, \mu) := B_{\mathfrak{g}}(a_\lambda, a_\mu)$. For every $\lambda \in \Delta_{\mathfrak{a}}$ the reflection $s_\lambda(\mu)$ of a restricted root $\mu \in \Delta_{\mathfrak{a}}$ with respect to the hyperplane $\{a \in \mathfrak{a} | \lambda(a) = 0\}$ is given by

$$s_\lambda(\mu) := \mu - 2\frac{B_{\mathfrak{g}}(\mu, \lambda)}{B_{\mathfrak{g}}(\lambda, \lambda)}\lambda.$$

Following Ref. [25] on p. 286, the reflection s_λ can be extended to elements of $\mathfrak{a}$. For $a \in \mathfrak{a}$ the reflection $s_\lambda(a)$ of $a \in \mathfrak{a}$ in the hyperplane $\{a \in \mathfrak{a} | \lambda(a) = 0\}$ is given by

$$s_\lambda(a) = a - 2\frac{B_{\mathfrak{g}}(a, a_\lambda)}{B_{\mathfrak{g}}(a_\lambda, a_\lambda)}a_\lambda. \tag{6}$$

With this preparation we get a possibility to compute the Weyl group corresponding to $\mathfrak{a}$.

Fact 3 ([27], p. 383). The Weyl group corresponding to $\mathfrak{a}$ is finite and is generated by the reflections s_λ, where $\lambda \in \Delta_{\mathfrak{a}}$.

Recall that $\mathcal{W}(G, A)$ is a subset of K and operates on $\mathfrak{a}$ by $\mathrm{Ad}_{\mathfrak{g}}(K)$, where $K \in K$.

Definition 7 (Weyl orbit) (see, e.g., [36], p. 422). The Weyl orbit $\mathcal{W}(a)$ of an element $a \in \mathfrak{a}$ is defined as the set $\{[\mathrm{Ad}_{\mathfrak{g}}(W)](a) | W \in \mathcal{W}(G, A)\}$. By appealing to Fact 2 the Weyl orbit $\mathcal{W}(p)$, for $p \in \mathfrak{p}$, is defined as $\mathcal{W}(p) := \mathcal{W}(a)$, where $a \in [\mathrm{Ad}_{\mathfrak{g}}(K)](p) \cap \mathfrak{a}$.

To understand that the definition of $\mathcal{W}(p)$ for $p \in \mathfrak{p}$ is independent of a and thus well defined, we now characterize the Weyl orbits in more detail.

Fact 4 ([27], Lemma 7.38). Let $[\mathrm{Ad}_{\mathfrak{g}}(K)](a) = a'$, where $a, a' \in \mathfrak{a}$ and $K \in K$. Then there exists an element $K' \in N_K(\mathfrak{a})$ such that $[\mathrm{Ad}_{\mathfrak{g}}(K')](a) = a'$.

By Fact 4 two elements a and a' from the Weyl orbit $\mathcal{W}(p)$ of $p \in \mathfrak{p}$ are conjugated by an element of the Weyl group, which proves that the definition (Def. 7) of $\mathcal{W}(p)$ is independent of a. This shows in addition that the Weyl orbit $\mathcal{W}(p)$ is equal to $\mathfrak{a} \cap [\mathrm{Ad}_{\mathfrak{g}}(K)](p)$. Let us denote the convex hull of the Weyl orbit $\mathcal{W}(p)$ by $\mathfrak{c}(p)$. We state now the infinitesimal version of Kostant's convexity theorem.

Fact 5 (Kostant's convexity theorem, infinitesimal version) (see [36], Theorem 8.2 or [37], Theorem 1). Let Γ be the orthogonal projection of $\mathfrak{p}$ on $\mathfrak{a}$ with respect to the Killing form. For every $p \in \mathfrak{p}$ one obtains

$$\Gamma([Ad_g(K)](p)) = \mathfrak{c}(p).$$

Remark. The essential meaning of the infinitesimal version of Kostant's convexity theorem (Fact 5) is that the projection of $[\mathrm{Ad}_{\mathfrak{g}}(K)](p)$ to $\mathfrak{a}$ with respect to the Killing form is a convex set and its extreme points are given by the Weyl orbit $\mathcal{W}(p)$.

In order to characterize the Weyl orbits in more detail we introduce additional concepts. The subspace $\mathfrak{a}$ can be divided into connected components called Weyl chambers.

Definition 8 (Weyl chamber) ([25], p. 287). Let λ be any restricted root of $\mathfrak{g}$ with respect to $\mathfrak{a}$. The hyperplanes $\{a \in \mathfrak{a} | \lambda(a) = 0\}$ divide $\mathfrak{a}$ into finitely many connected components excluding their boundary hyperplanes. Such a con-

nected component is called Weyl chamber. The closure of a Weyl chamber including their boundary hyperplanes is called closed Weyl chamber.

Fact 6 ([25], Theorem 2.12, Chap. VII). The Weyl group permutes the Weyl chambers.

We choose some arbitrary, but fixed, order on the restricted roots of $\mathfrak{g}$ with respect to $\mathfrak{a}$. Therefore, the restricted roots can be divided into positive and negative (restricted) roots, where positive and negative is defined regarding to the chosen order. A restricted root is called fundamental if it is positive and not a sum of two positive (restricted) roots ([26], p. 59). Let $\{\alpha_k\} \subset \Delta_\mathfrak{a}$ be the set of fundamental (restricted) roots. Since the Killing form restricted to $\mathfrak{a} \times \mathfrak{a}$ is nondegenerate we can define as before for every (restricted) root λ the element $a_\lambda \in \mathfrak{a}$ so that $B_\mathfrak{g}(a_\lambda, a) = \lambda(a)$ for all $a \in \mathfrak{a}$. The set $\{a \in \mathfrak{a} \,|\, B_\mathfrak{g}(a_{\alpha_k}, a) > 0 \text{ for all } \alpha_k\}$ is a Weyl chamber and it is called the fundamental Weyl chamber ([26] p. 61).

Fact 7 (adapted from [26], Proposition I, Sec. 2.11). Let λ and μ be restricted roots corresponding to elements a_λ and a_μ of the closed fundamental Weyl chamber, respectively. The element a_μ lies in the convex hull of the Weyl orbit $\mathcal{W}(a_\lambda)$ of a_λ if and only if $\lambda(a) \geq \mu(a)$ for all elements a of the fundamental Weyl chamber. The condition $\lambda(a) \geq \mu(a)$ is equivalent to $B_\mathfrak{g}(a_\lambda, a) \geq B_\mathfrak{g}(a_\mu, a)$.

C. The two-qubit case

We now treat the case G=SU(4). To be more concrete we introduce a matrix representation for the real semisimple Lie algebra $\mathfrak{su}(4)$, which corresponds to G. Let

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

be the the Pauli matrices and set

$$\sigma_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

to be the identity matrix. We identify $\sigma_x = \sigma_1$, $\sigma_y = \sigma_2$, and $\sigma_z = \sigma_3$ and use the following definitions:

$$X_1 := \frac{i}{2}\sigma_0 \otimes \sigma_1, \quad X_2 := \frac{i}{2}\sigma_0 \otimes \sigma_2, \quad X_3 := \frac{i}{2}\sigma_0 \otimes \sigma_3,$$

$$X_4 := \frac{i}{2}\sigma_1 \otimes \sigma_0, \quad X_5 := \frac{i}{2}\sigma_2 \otimes \sigma_0, \quad X_6 := \frac{i}{2}\sigma_3 \otimes \sigma_0,$$

$$X_7 := \frac{i}{2}\sigma_1 \otimes \sigma_1, \quad X_8 := \frac{i}{2}\sigma_2 \otimes \sigma_2, \quad X_9 := \frac{i}{2}\sigma_3 \otimes \sigma_3,$$

$$X_{10} := \frac{i}{2}\sigma_1 \otimes \sigma_2, \quad X_{11} := \frac{i}{2}\sigma_1 \otimes \sigma_3, \quad X_{12} := \frac{i}{2}\sigma_2 \otimes \sigma_1,$$

$$X_{13} := \frac{i}{2}\sigma_2 \otimes \sigma_3, \quad X_{14} := \frac{i}{2}\sigma_3 \otimes \sigma_1, \quad X_{15} := \frac{i}{2}\sigma_3 \otimes \sigma_2.$$

The standard (or defining) representation of $\mathfrak{su}(4)$ is

$$\mathfrak{g} := \mathfrak{su}(4) = \mathrm{span}_\mathbb{R}\{X_1, \ldots, X_{15}\},$$

where $\mathrm{span}_\mathbb{R}$ denotes the real span. Let

$$\mathfrak{k} := \mathrm{span}_\mathbb{R}\{X_1, \ldots, X_6\},$$

$$\mathfrak{p} := \mathrm{span}_\mathbb{R}\{X_7, \ldots, X_{15}\},$$

$$\text{and} \quad \mathfrak{a} := \mathrm{span}_\mathbb{R}\{X_7, \ldots, X_9\}.$$

With this notation one can easily check that $\mathfrak{k}$ and $\mathfrak{p}$ fulfill the commutator relations in Eq. (4). Since the group SU(4) is compact, the pair $(\mathfrak{g}, \theta)$ defines an orthogonal symmetric Lie algebra, where θ is given by Eq. (5). The subspace $\mathfrak{a}$ forms a maximal Abelian subalgebra in $\mathfrak{p}$. The set of restricted roots with respect to $\mathfrak{a}$ can be computed as the eigenvalues of $\mathrm{ad}_\mathfrak{g}(c_1 X_7 + c_2 X_8 + c_3 X_9)$, where $c_i \in \mathbb{R}$:

$$[\pm i(c_2 - c_3), \, \pm i(c_2 + c_3), \, \pm i(c_1 - c_3), \, \pm i(c_1 + c_3),$$
$$\pm i(c_1 + c_2), \, \pm i(c_1 - c_2)]. \tag{7}$$

We use Eq. (6) to obtain a generating set for the Weyl group (corresponding to $\mathfrak{a}$) as a set of matrices

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \tag{8}$$

which operate on the vectors

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \triangleq X_7, \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \triangleq X_8, \quad \text{and} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \triangleq X_9. \tag{9}$$

With the notation of Eq. (9) the Killing form restricted to $\mathfrak{a} \times \mathfrak{a}$ is given by

$$B_\mathfrak{g}(a,b)|_{\mathfrak{a} \times \mathfrak{a}} := a^T \begin{pmatrix} -8 & 0 & 0 \\ 0 & -8 & 0 \\ 0 & 0 & -8 \end{pmatrix} b.$$

Now we give the elements $a_\lambda \in \mathfrak{a}$ corresponding to the restricted roots λ in Eq. (7), i.e., elements $a_\lambda \in \mathfrak{a}$ such that $B_\mathfrak{g}(a_\lambda, a) = \lambda(a)$ for all $a \in \mathfrak{a}$:

$$\left\{ \frac{\pm i}{-8}\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \frac{\pm i}{-8}\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \frac{\pm i}{-8}\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \right.$$
$$\left. \frac{\pm i}{-8}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \frac{\pm i}{-8}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{\pm i}{-8}\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right\}.$$

We have used the basis of Eq. (9) to represent the elements a_λ. In order to present our results in the context of Ref. [4], we choose an order on the (restricted) roots such that the roots of Eq. (7), which have a plus sign, constitute the posi-

tive ones. With this convention for an element $d = d_1 X_7 + d_2 X_8 + d_3 X_9$ of the fundamental Weyl chamber we get the following set of equations ($d_i \in \mathbb{R}$):

$$\{d_2 - d_3 > 0, \ d_2 + d_3 > 0, \ d_1 - d_3 > 0, \ d_1 + d_3 > 0,$$
$$d_1 + d_2 > 0, \ d_1 - d_2 > 0\}, \tag{10}$$

where we have identified $(\mathbb{R}, >)$ with $(i\mathbb{R}, >)$ by defining $ir_1 > ir_2 \Leftrightarrow r_1 > r_2$ for all $r_1, r_2 \in \mathbb{R}$.

IV. INFINITESIMAL HAMILTONIAN SIMULATION FOR TWO QUBITS

A. Lie-theoretic explanation

Following Definition 2 we consider now infinitesimal Hamiltonian simulation for two qubits. We emphasize that in the two-qubit case local unitary operations correspond to elements of $K = \exp(\mathfrak{k})$. We use the notation of Sec. III, especially that of Sec. III C. Since we restrict ourselves to Hamilton operators without local terms (see Sec. II), we have for all nonlocal Hamilton operators H and H' that $iH \in \mathfrak{p}$ and $iH' \in \mathfrak{p}$, where $\mathfrak{p}$ is the subvector space of the Lie algebra $\mathfrak{g}$ introduced in Sec. III. Thus, we can use Fact 2 to write every nonlocal Hamilton operator H' as $H' = [\mathrm{Ad}_\mathfrak{g}((L')^{-1})](a')$, where a' is an element of $\mathfrak{a}$ and L' is a local unitary operator.

Theorem 1. Assume that H and H' are nonlocal Hamilton operators acting on a two-qubit system. Let a' be an element of $\mathfrak{a}$, where $a' = [\mathrm{Ad}_\mathfrak{g}(L')](H')$ for some local unitary operator L'. A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the Hamilton operator H' in time t if and only if the Hamilton operator (a'/t) lies in the convex closure of the Weyl orbit $\mathcal{W}(H)$ of H. The condition is independent of the choice of a'.

Remark. Actually, Theorem 1 is the infinitesimal version of Fact 8 (see below and Ref. [5]). In order to clarify the connection of Theorem 2 to the work of Ref. [5], we give here a proof of this infinitesimal version using arguments of Refs. [4,5].

Proof. Assume that

$$t \sum_{i=1}^{m_3} q_i'' [\mathrm{Ad}_\mathfrak{g}(K_i'')](H) \tag{11}$$

is a simulation of H' in time t, where K_i'' are local unitary operators, $H, H' \in \mathfrak{p}$, $q_i'' \geq 0$, and $\sum_{i=1}^{m_3} q_i'' = 1$.

Due to Fact 2 there exists a and a' in $\mathfrak{a}$, where $a = [\mathrm{Ad}_\mathfrak{g}(L)](H)$ and $a' = [\mathrm{Ad}_\mathfrak{g}(L')](H')$ for some local unitary operators L and L'. We remark that local unitary operations cost no time. Thus, the existence of the simulation in Eq. (11) is equivalent to the existence of a simulation $t \sum_{i=1}^{m_2} q_i' [\mathrm{Ad}_\mathfrak{g}(K_i')](a)$ of a' by a in time t, where K_i' are some local unitary operators, $q_i' \geq 0$, and $\sum_{i=1}^{m_2} q_i' = 1$. Let Γ and Γ' denote the orthogonal projections (with respect to the Killing form) of $\mathfrak{p}$ on $\mathfrak{a}$ and $\mathfrak{a}^\perp$, respectively. We can write the simulation as

$$t \sum_{i=1}^{m_2} q_i' (\Gamma\{[\mathrm{Ad}_\mathfrak{g}(K_i')](a)\} + \Gamma'\{[\mathrm{Ad}_\mathfrak{g}(K_i')](a)\}) = a'.$$

This is equivalent to

$$t \sum_{i=1}^{m} q_i \Gamma\{[\mathrm{Ad}_\mathfrak{g}(K_i)](a)\} = a', \tag{12}$$

where K_i are some local unitary operators, $q_i \geq 0$, and $\sum_{i=1}^m q_i = 1$. The last equivalence follows in the backward direction by employing Fact 5 to rewrite the projection Γ as a convex combination and in the forward direction by the fact that the term $\sum_{i=1}^{m_2} q_i' \Gamma'\{[\mathrm{Ad}_\mathfrak{g}(K_i')](a)\}$ has to be zero.

By the remark following Fact 5 we know that the projection of $[\mathrm{Ad}_\mathfrak{g}(K)](p)$ to $\mathfrak{a}$ with respect to the Killing form is a convex set. Thus, we can write Eq. (12) as

$$\Gamma\{[\mathrm{Ad}_\mathfrak{g}(K')](a)\} = (a'/t)$$

for some local unitary operator K'. With Fact 5 we get that (a'/t) lies in the convex closure of the Weyl orbit $\mathcal{W}(a)$ of a. Since $a = [\mathrm{Ad}_\mathfrak{g}(L)](H)$, we can replace a by H in the preceding sentence. This proves the theorem except for the independence of the choice of a'.

Assume that we replace a' by $a'' \in \mathfrak{a}$, where $a'' = [\mathrm{Ad}_\mathfrak{g}(L'')](H')$ for some local unitary operator L''. Due to Fact 4, there exist an element $W \in \mathcal{W}(\mathrm{G}, \mathrm{A})$ so that $a'' = [\mathrm{Ad}_\mathfrak{g}(W^{-1})](a')$. Since operating with an element of the Weyl group leaves the Weyl orbit $\mathcal{W}(H)$ unchanged, the Weyl orbit is equal to $[\mathrm{Ad}_\mathfrak{g}(W)][\mathcal{W}(H)]$. It is obvious that the convex closure of the Weyl orbit $\mathcal{W}(H)$ is left unchanged as well. Hence, the element a' is in the convex closure of the Weyl orbit $\mathcal{W}(H)$ if and only if a'' is. ∎

For $a' \in \mathfrak{a}$ it was also proven in Ref. [4] that the set of Hamilton operators (a'/t), which can be simulated in time one, is convex. We emphasize that the extreme points of this set are given by the Weyl orbit $\mathcal{W}(H)$, which can be computed by means of Eq. (8). In Ref. [4] the extreme points were given and their extremality was proven by another method. As in Ref. [4], we state now a version of Theorem 1 that gives a condition for infinitesimal Hamiltonian simulation in the two-qubit case that is easier to check.

Theorem 2 ([4], p. 11). Assume that H and H' are nonlocal Hamilton operators acting on a two-qubit system. Let a and a' be elements of the closed fundamental Weyl chamber, where $a = a_1 X_7 + a_2 X_8 + a_3 X_9 = [\mathrm{Ad}_\mathfrak{g}(L)](H)$ and $a' = a_1' X_7 + a_2' X_8 + a_3' X_9 = [\mathrm{Ad}_\mathfrak{g}(L')](H')$ for some local unitary operators L and L' ($a_i, a_i' \in \mathbb{R}$). A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the Hamilton operator H' in time t iff the following equations hold:

$$a_1 \geq a_1'/t, \tag{13a}$$

$$a_1 + a_2 + a_3 \geq (a_1' + a_2' + a_3')/t, \tag{13b}$$

$$a_1 + a_2 - a_3 \geq (a_1' + a_2' - a_3')/t. \tag{13c}$$

Remark. We force a and a' to be (almost) unique elements of $\mathfrak{a}$ by choosing them to be elements of the closed fundamental Weyl chamber. If a or a' lies on the boundary of the fundamental Weyl chamber, they are elements of the closed fundamental Weyl chamber, but not elements of the fundamental Weyl chamber. Only in this case there remains a

nonuniqueness, and the considered element can possibly be chosen to lie on different boundary hyperplanes of the closed fundamental Weyl chamber.

Proof. As the Weyl group permutes the Weyl chambers (see Fact 6) we can choose a and a' to be elements of the closed fundamental Weyl chamber. We recall from Eq. (10) that an element $d = d_1 X_7 + d_2 X_8 + d_3 X_9$ lies in the fundamental Weyl chamber iff $d_2 - d_3 > 0$, $d_2 + d_3 > 0$, $d_1 - d_3 > 0$, $d_1 + d_3 > 0$, $d_1 + d_2 > 0$, and $d_1 - d_2 > 0$ holds. Applying Theorem 1 and Fact 7 we get that $a_1 d_1 + a_2 d_2 + a_3 d_3 \geqslant (a_1' d_1 + a_2' d_2 + a_3' d_3)/t$ holds for all elements $d = d_1 X_7 + d_2 X_8 + d_3 X_9$ of the fundamental Weyl chamber. Eliminating the quantifiers in the previous condition, e.g., using the computer algebra system QEPCAD [38,39], we obtain the conditions of Eq. (13). ∎

B. Majorization

In this section we introduce some concepts from the theory of majorization that will be employed later. Our presentation is succinct and we refer to Refs. [40–45] for a more detailed treatment of this topic.

For an element $x = (x_1, \ldots, x_k)^T$ of $\mathbb{R}^k$ we denote by $x^\downarrow = (x_1^\downarrow, \ldots, x_k^\downarrow)^T$ a permutation of x so that $x_i^\downarrow \geqslant x_j^\downarrow$ if $i < j$, where $1 \leqslant i, j \leqslant k$.

Definition 9 (majorization) ([45], p. 28). A vector $x \in \mathbb{R}^k$ is majorized by a vector $y \in \mathbb{R}^k$ if

$$\sum_{i=1}^{l} x_i^\downarrow \leqslant \sum_{i=1}^{l} y_i^\downarrow \quad \text{for all } 1 \leqslant l \leqslant k$$

and

$$\sum_{i=1}^{k} x_i^\downarrow = \sum_{i=1}^{k} y_i^\downarrow.$$

The notation $x \prec y$ means that x is majorized by y.

We recall the notion of s-majorization introduced in Ref. [4]. For an element $x = (x_1, x_2, x_3)^T$ of $\mathbb{R}^3$ we introduce the vector $\hat{x} = (|x_1|, |x_2|, |x_3|)^T$, and we define the s-ordered version $x^{\downarrow s}$ of x by setting $x_1^{\downarrow s} := \hat{x}_1^\downarrow$, $x_2^{\downarrow s} := \hat{x}_2^\downarrow$, and $x_3^{\downarrow s} := \mathrm{sgn}(x_1 x_2 x_3) \hat{x}_3^\downarrow$. The signum of $x_1 x_2 x_3$ is denoted by $\mathrm{sgn}(x_1 x_2 x_3)$.

Definition 10 ([4], p. 11). The vector $x \in \mathbb{R}^3$ is s-majorized by $y \in \mathbb{R}^3$ if

$$x_1^{\downarrow s} \leqslant y_1^{\downarrow s},$$

$$x_1^{\downarrow s} + x_2^{\downarrow s} + x_3^{\downarrow s} \leqslant y_1^{\downarrow s} + y_2^{\downarrow s} + y_3^{\downarrow s},$$

$$x_1^{\downarrow s} + x_2^{\downarrow s} - x_3^{\downarrow s} \leqslant y_1^{\downarrow s} + y_2^{\downarrow s} - y_3^{\downarrow s}.$$

The notation $x \prec_s y$ means that x is s-majorized by y.

We emphasize that a vector representing an element from the Lie subalgebra $\mathfrak{a}$ is s-ordered if and only if it lies in the closed fundamental Weyl chamber, as given in Eq. (10), except that for the closure the relation $<$ has to be replaced by the relation $\leqslant$. This gives a geometric motivation for the s-ordered vectors. In addition, the necessary and sufficient conditions for Hamiltonian simulation in Eq. (13) are equivalent to the definition of s-majorization.

Corollary 1 ([4], p. 11). Assume that H and H' are nonlocal Hamilton operators acting on a two-qubit system. Let a and a' be elements of $\mathfrak{a}$, where $a = a_1 X_7 + a_2 X_8 + a_3 X_9 = [\mathrm{Ad}_\mathfrak{g}(L)](H)$ and $a' = a_1' X_7 + a_2' X_8 + a_3' X_9 = [\mathrm{Ad}_\mathfrak{g}(L')](H')$ for some local unitary operators L and L'. We use the notation $\vec{a} = (a_1, a_2, a_3)^T \in \mathbb{R}^3$ and $\vec{a}' = (a_1', a_2', a_3')^T \in \mathbb{R}^3$. A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the Hamilton operator H' in time t if and only if the following equation holds:

$$\vec{a}' \prec_s t\vec{a}.$$

There is a similar condition on infinitesimal Hamiltonian simulation that is given in terms of a majorization condition on the spectra of the considered Hamilton operators. This result (see the Appendix and Ref. [46], pp. 9–10) should be compared to the s-majorization condition in Corollary 1.

V. GATE SIMULATION FOR TWO QUBITS

As in Definition 1 we consider now gate simulation, which is a global version of infinitesimal Hamiltonian simulation. We recall a theorem of Khaneja *et al.* [5].

Fact 8 ([5], Theorem 10). Assume that H is a nonlocal Hamilton operator acting on a two-qubit system. A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the unitary gate U in time t if and only if the unitary gate U can be decomposed as

$$U = L_1 \exp(tW) L_2, \tag{14}$$

where L_1 and L_2 are local unitary operators and W is an element that lies in the convex hull of the Weyl orbit $\mathcal{W}(H)$ of H.

Remark. An equivalent version of Eq. (14) is

$$L_1^{-1} U L_2^{-1} = \exp(tW). \tag{15}$$

This means that U can be simulated in time t if and only if there exists a unitary gate U', which is locally equivalent to U and can be expressed as $U' = \exp(tW)$. But there exists a restriction on the elements L_1 and L_2. As $\exp(tW)$ is an element of $\mathrm{A} = \exp(\mathfrak{a})$, we have that $L_1^{-1} U L_2^{-1}$ has to be an element of A, too. There exists different unitary operations U' that satisfy this restriction. The appearance of different unitary operations U' is a consequence of the nonuniqueness of the KAK decomposition of Fact 1, which will be analyzed in detail below. We emphasize that it may be impossible to express U as $U = \exp(tW)$ with the same (or shorter) time t as in Eq. (15).

We present now the results on gate simulation in similar fashion as done in Sec. IV B for Hamiltonian simulation. Due to the remark following Fact 8, a local unitary operation U can be simulated in time t if and only if a local unitary operation U', which is locally equivalent to U can be expressed as $U' = \exp(tW)$, where W denotes an element of the Weyl orbit of the system Hamiltonian. In the sequel, let K_i, for $i \in \{1, \ldots, 8\}$, be suitable elements from the set of local unitary gates $\mathrm{K} = \exp(\mathfrak{k})$. In addition we denote by A and A'

some appropriate elements of $A = \exp(\mathfrak{a})$. In view of Fact 1 we can decompose the unitary gate U and locally equivalent gates U' as $U = K_1 A K_2$ and $U' = K_3 A' K_4$, respectively. To characterize all unitary gates U', which are locally equivalent to U, it is necessary and sufficient to characterize all A' satisfying $K_5 A' K_6 = A$. Thus we have to identify all A', which can be written as $A' = (K_7^{-1} A K_7) K_8$. This is done in the following lemma.

Lemma 2. For a fixed $A \in A$ and an arbitrary element of the form $A' = (K^{-1} A K) K' \in A$ with $K, K' \in K$, we can choose K from the Weyl group and K' from the set $K \cap A$.

Related to θ from the definition (Definition 4) of an orthogonal symmetric Lie algebra $(\mathfrak{g}, \theta)$, there exists a global version Θ operating on the Lie group G (see, e.g., Ref. [32], Theorem 2.3 of Chap. IV or Ref. [27], Theorem 6.31). We define Θ by $\Theta(K'') = K''$ for $K'' \in K$ and $\Theta(P) = P^{-1}$ for $P \in P = \exp(\mathfrak{p})$. We employ the mapping $(\,)^\star : G \to G$ given by $G \mapsto G^\star := \Theta(G^{-1})$. We use here the symbol $(\,)^\star$ in order to avoid confusion with the symbol $(\,)^*$, which denotes complex conjugation. We have that $(G_1 G_2)^\star = G_2^\star G_1^\star$ for $G_1, G_2 \in G$, $P^\star = P$ for $P \in P$, and $(K'')^\star = (K'')^{-1}$ for $K'' \in K$ (see Ref. [34], p. 81). We introduce the map $\phi : G/K \to P$, which is defined as $GK \mapsto \phi(GK) := (GK)(GK)^\star = GG^\star$. This map ϕ was studied in Ref. [34] on pp. 81–82 and in Ref. [27] in the Proof of Theorem 6.31. Reference [34] proves that ϕ induces an isomorphism of G/K onto P.

Proof of Lemma 2. We employ the map ϕ and obtain the equations $\phi[(K^{-1} A K) K'] = K^{-1} A^2 K$ and $\phi(A') = (A')^2$. Since $A' = (K^{-1} A K) K'$ is given in the condition of Lemma 2, we obtain $K^{-1} A^2 K = (A')^2$. And due to Fact 4, we can choose K as an element of the Weyl group. Thus, $K^{-1} A K \in A$ which proves that $K' \in K \cap A$. ∎

We still need to characterize the elements of $K \cap A$. This will be done now.

Lemma 3. The elements of set $K \cap A$ are given by $\exp(z_1 \pi X_7 + z_2 \pi X_8 + z_3 \pi X_9)$, where $z_j \in \mathbb{Z}$ for $j \in \{1, 2, 3\}$ and X_7, X_8, X_9 as defined on p. 12.

Proof. First, we show that the elements $\exp(z_1 \pi X_7 + z_2 \pi X_8 + z_3 \pi X_9)$ constitute a subset of $K \cap A$. As $\exp(z_1 \pi X_7 + z_2 \pi X_8 + z_3 \pi X_9)$ for $z_j \in \mathbb{Z}$ are by definition elements of A and A is an Abelian group, we obtain that

$$\exp(z_1 \pi X_7 + z_2 \pi X_8 + z_3 \pi X_9)$$
$$= \exp(z_1 \pi X_7) \exp(z_2 \pi X_8) \exp(z_3 \pi X_9)$$
$$= (i\sigma_1 \otimes \sigma_1)^{z_1} (i\sigma_2 \otimes \sigma_2)^{z_2} (i\sigma_3 \otimes \sigma_3)^{z_3}.$$

This proves that the elements constitute a subset of $K \cap A$. Second, we show that $K \cap A$ is a subset of the set given by the elements $\exp(z_1 \pi X_7 + z_2 \pi X_8 + z_3 \pi X_9)$. We make the ansatz $\exp(a_7 X_7 + a_8 X_8 + a_9 X_9) = \exp(a_1 X_1 + a_2 X_2 + a_3 X_3 + a_4 X_4 + a_5 X_5 + a_6 X_6)$, where $a_i \in \mathbb{R}$, X_i were given on p. 12, and $i \in \{1, \ldots, 9\}$. By direct computations one gets for a_7, a_8, and a_9 the conditions

$$(a_7 - a_8 - a_9)/\pi \in \mathbb{Z},$$

$$(a_7 + a_8 - a_9)/\pi \in \mathbb{Z},$$

$$(a_7 + a_8 + a_9)/\pi \in \mathbb{Z},$$

$$(a_7 - a_8 + a_9)/\pi \in \mathbb{Z}.$$

This implies $a_i/\pi \in \mathbb{Z}$ for $i \in \{7, 8, 9\}$. ∎

Now, we state the majorizationlike equivalent of Fact 8.

Corollary 2 (see Ref. [6], Lemma or Ref. [7], Result 1). Assume that H is a nonlocal Hamilton operator acting on a two-qubit system and that we intend to simulate the unitary operation U. Let a and a' be elements of $\mathfrak{a}$, where $a = a_1 X_7 + a_2 X_8 + a_3 X_9 = [\mathrm{Ad}_{\mathfrak{g}}(K_1)](H)$, $a' = a_1' X_7 + a_2' X_8 + a_3' X_9$, and $U = K_2 \exp(a') K_3$ for some local unitary operations $K_1, K_2, K_3 \in K$. We use the notation $\vec{a} = (a_1, a_2, a_3)^T \in \mathbb{R}^3$ and $\vec{a'} = (a_1', a_2', a_3')^T \in \mathbb{R}^3$. A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the unitary operation U in time t if and only if the following equation holds for at least one choice of $\vec{z} = (z_1, z_2, z_3)^T \in \mathbb{Z}^3$:

$$\vec{a'} + \pi \vec{z} <_s t\vec{a}.$$

Proof. By Fact 2 and Fact 1 we can choose a and a', respectively, as given. Applying the remark following Fact 8 it is necessary and sufficient to consider some unitary gates U', which are locally equivalent to U. By use of Fact 1 these locally equivalent gates U' can be represented as $U' = K_1' A' K_2'$, where A' is an element of A and K_1', K_2' are local unitary gates. The different possibilities for A' in this decomposition are given by Lemma 2 as $A' = \exp\{[\mathrm{Ad}_{\mathfrak{g}}(K)](a')\} K'$, where K is an element of the Weyl group, $K' \in K \cap A$, and $K' = \exp(k')$. With the characterization of $K \cap A$ from Lemma 3 we deduce that $K \cap A$ is left invariant by operations of the Weyl group. Since A is Abelian and $K \cap A$ is left invariant by operations of the Weyl group, we can write A' as $A' = \exp\{[\mathrm{Ad}_{\mathfrak{g}}(K)](a') + k'\} = \exp\{[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'')\}$, where $K'' = \exp(k'')$ for some element $K'' \in K \cap A$. By Fact 8 we obtain that $A' = \exp\{[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'')\} = \exp(tW)$, where W lies in the convex hull of the Weyl orbit $\mathcal{W}(a)$ of a. When we consider the equation $\exp\{[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'')\} = \exp(tW)$ in a basis where both $[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'')$ and tW are diagonal, then we obtain by the periodicity of the exponential function that $[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'') + M = tW$, where $M = \mathrm{diag}(2\pi i \lambda_1, 2\pi i \lambda_2, 2\pi i \lambda_3, 2\pi i \lambda_4)$ and $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{Z}$. As $[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'')$ and tW are elements of $\mathfrak{a}$, it follows that $M \in \mathfrak{a}$. We can write M as $M = 2\pi z_1 X_7 + 2\pi z_2 X_8 + 2\pi z_3 X_9 = 2k_1$ where $z_1 = (\lambda_1 + \lambda_2) \in \mathbb{Z}$, $z_2 = (\lambda_1 + \lambda_3) \in \mathbb{Z}$, $z_3 = (\lambda_2 + \lambda_3) \in \mathbb{Z}$, $K_1 = \exp(k_1)$, and $K_1 \in K \cap A$. Thus, we obtain $[\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'') + 2k_1 = [\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k'' + 2k_2) = [\mathrm{Ad}_{\mathfrak{g}}(K)](a' + k_3) = tW$, where $K_i = \exp(k_i)$, $K_i \in K \cap A$, and $i \in \{1, 2, 3\}$. Corollary 1 completes the proof. ∎

Searching for a refinement of Corollary 2, we state bounds on the coefficients of a_1, a_2, and a_3 of an element $a_1 X_7 + a_2 X_8 + a_3 X_9$ of $\mathfrak{a}$. It follows from Lemma 2 and Lemma 3 that the coefficients a_i, $i \in \{1, 2, 3\}$, are periodic with period π. (Concerning this periodicity, we refer also to Appendix B of Ref. [47] and p. 7 of Ref. [24].) Bearing the π-periodicity in mind, we can restrict the coefficients a_i to the interval $[-\pi/2, \pi/2]$. This choice is compatible with our

conventions in Sec. III C. To reduce the symmetry induced by the Weyl group, we restrict ourselves to elements of the closed fundamental Weyl chamber. From Eq. (10) or from the s-order of Sec. IV B, we get that $a_1 \geq 0$, $a_2 \geq 0$, $a_1 \geq a_2$, and $a_2 \geq a_3$. These considerations lead to the following corollary.

Corollary 3 (see Ref. [6], Theorem 1 or Ref. [7], Result 2). Assume that H is a nonlocal Hamilton operator acting on a two-qubit system and that we intend to simulate the unitary gate U. Let a and a' be elements of $\mathfrak{a}$, where $a = a_1 X_7 + a_2 X_8 + a_3 X_9 = [\mathrm{Ad}_\mathfrak{g}(K_1)](H)$, $a' = a'_1 X_7 + a'_2 X_8 + a'_3 X_9$, and $U = K_2 \exp(a') K_3$ for some local unitary operations $K_1, K_2, K_3 \in K$. In addition, we force $a_1, a_2, a_3, a'_1, a'_2$, and a'_3 to be elements from the interval $[-\pi/2, \pi/2]$. We use the notation $\vec{a} = (a_1, a_2, a_3)^T \in \mathbb{R}^3$ and $\vec{a}' = (a'_1, a'_2, a'_3)^T \in \mathbb{R}^3$. A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the unitary gate U in time t if and only if the following equation holds for at least one choice of $\vec{z} = (z_1, z_2, z_3)^T \in \{(0,0,0)^T, (-1,0,0)^T\}$:

$$\vec{a}' + \pi \vec{z} <_s t \vec{a}.$$

Remark. In the proof we follow Refs. [6,7].

Proof. Due to Corollary 2, it is sufficient to prove that for every $\vec{z} \in \mathbb{Z}^3$ one of the following conditions holds:

$$\vec{a}' + \pi(0,0,0)^T <_s \vec{a}' + \pi \vec{z},$$

$$\vec{a}' + \pi(-1,0,0)^T <_s \vec{a}' + \pi \vec{z}.$$

We first consider the case that $|z_i| > 1$, for some $i \in \{1,2,3\}$. Because $a'_i \leq \pi/2$, the maximal component $(\vec{a}' + \pi \vec{z})_1^{\downarrow s}$ of the s-ordered version of $\vec{a}' + \pi \vec{z}$ is greater than or equal to $2\pi - \pi/2 = 3\pi/2$. We check the conditions of Definition 10 and obtain that $\vec{a}' + \pi(0,0,0)^T <_s \vec{a}' + \pi \vec{z}$.

Second, we consider the case that $|z_i| \leq 1$ for all $i \in \{1,2,3\}$. By easy, but tedious, computations one can check that $\vec{a}' + \pi(0,0,0)^T <_s \vec{a}' + \pi \vec{z}$ for

$$\vec{z} \in \{(-1,-1,0)^T, \ (-1,0,-1)^T, \ (0,-1,-1)^T,$$
$$(0,-1,1)^T, \ (0,0,0)^T, \ (-1,0,1)^T\}$$

and that $\vec{a}' + \pi(-1,0,0)^T <_s \vec{a}' + \pi \vec{z}$ for

$$\vec{z} \in \{(-1,-1,-1)^T, \ (-1,-1,1)^T, \ (-1,0,0)^T, \ (0,-1,0)^T,$$
$$(0,0,-1)^T, \ (0,0,1)^T\}.$$

For all other $\vec{z} \in \{-1,0,1\}^3$ we have that both $\vec{a}' + \pi(0,0,0)^T <_s \vec{a}' + \pi \vec{z}$ and $\vec{a}' + \pi(-1,0,0)^T <_s \vec{a}' + \pi \vec{z}$ hold. ∎

VI. LOWER BOUNDS FOR n-QUBIT SYSTEMS

In the two-qubit case we used a particular decomposition $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ of the Lie algebra that leads to a decomposition G $= KAK$ of the Lie group where $K = \exp(\mathfrak{k})$ is the set of local unitary operations. By this approach, e.g., the optimal simulation result of Fact 8 can be obtained. In the more general n-qubit case we can use decompositions $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ of the corresponding Lie group where $K = \exp(\mathfrak{k})$ contains all local uni-

tary operations. Although K is, in general, not equal to the set of local unitary operations, we can generalize the approach from the two-qubit case in order to prove lower bounds on the time complexity for gate simulation. Lower bounds were considered in Ref. [10], and we refine and generalize the approach of Ref. [10] in this section. In doing so, we put this approach in a broader context.

A. Magic basis (for two qubits)

We begin by recalling the Bell basis and the magic basis. The Bell basis (see Refs. [48,49]) is a vector space basis for two-qubit pure states:

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

We employ the ket-vector notation, see, e.g., Ref. [2]. If we include some relative phases in the Bell basis we get the magic basis which was introduced in Ref. [8] and coined by Hill and Wootters [9]:

$$|e_1\rangle := |\Phi^+\rangle,$$

$$|e_2\rangle := i|\Phi^-\rangle,$$

$$|e_3\rangle := i|\Psi^+\rangle,$$

$$|e_4\rangle := |\Psi^-\rangle.$$

The magic basis is connected to the entanglement of formation (see Ref. [8] and related work in Refs. [50,51]). We neglect here this connection, but refer to Sec. VIII.

The magic basis has two important properties. First, the local unitary operations on two qubits are real and orthogonal in the magic basis (see Ref. [9], p. 5023 and Theorem 1 of Ref. [52]). Second, the elements of the $A = \exp(\mathfrak{a})$ (for notations see, e.g., Sec. III C) are diagonal in the magic basis, as remarked in Ref. [47] on p. 3 and Ref. [7] on p. 2. The basis change from the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ to the magic basis is given by Q^{-1}, where

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

For elements $U \in \mathrm{SU}(4)$ the map $U \mapsto Q^{-1}UQ$ (see Ref. [52]) reflects the isomorphism between $\mathrm{SU}(2) \otimes \mathrm{SU}(2)$ and $\mathrm{SO}(4)$ (see, e.g., Ref. [35], p. 52).

B. Representation theory

It is not obvious how the magic basis generalizes to higher number of qubits and which properties remain. Motivated by the properties of the magic basis for two qubits, we seek for basis changes of the local unitary operations $[\text{SU}(2)]^{\otimes n}$ into the orthogonal group (if possible). To analyze this we need some representation theory.

Definition 11 (Lie group representation) (see, e.g., Ref. [53], p. 210). A complex representation of the Lie group G in the finite-dimensional and complex vector space $V_{\mathbb{C}}$ is a continuous homomorphism $\tau:\text{G}\rightarrow\text{GL}(V_{\mathbb{C}})$ from the group G into the group $\text{GL}(V_{\mathbb{C}})$ of invertible and linear transformations which operate on $V_{\mathbb{C}}$.

A representation τ in a finite-dimensional and complex vector space $V_{\mathbb{C}}$ is called irreducible if there exists no subspace $U_{\mathbb{C}}$ other than $U_{\mathbb{C}}=0$ or $U_{\mathbb{C}}=V_{\mathbb{C}}$ such that the subspace is $\tau(\text{G})$-invariant, i.e., the equation $\tau(\text{G})U_{\mathbb{C}}\subset U_{\mathbb{C}}$ holds (see, e.g., Ref. [53], p. 210). We state an important fact on tensor products of irreducible representations.

Fact 9 ([54], Prop. 4.14 of Chap. II). If τ_1 is an irreducible complex representation of G_1 in the complex vector space $V_{\mathbb{C}}$ and τ_2 is an irreducible complex representation of G_2 in the complex vector space $W_{\mathbb{C}}$, then $\tau_1\otimes\tau_2$ is an irreducible complex representation of $G_1\times G_2$ in the complex vector space $V_{\mathbb{C}}\otimes W_{\mathbb{C}}$. Furthermore, any irreducible representation of $G_1\times G_2$ is a tensor product of this form.

Below we use bilinear forms $\mathcal{B}:V_{\mathbb{C}}\times V_{\mathbb{C}}\rightarrow\mathbb{C}$, which are $\mathbb{C}$-linear in both arguments, to characterize irreducible complex representations. Let v_1 and v_2 be some arbitrary elements of $V_{\mathbb{C}}$. A bilinear form is called symmetric if $\mathcal{B}(v_1,v_2)=\mathcal{B}(v_2,v_1)$ and skew symmetric if $\mathcal{B}(v_1,v_2)=-\mathcal{B}(v_2,v_1)$. A bilinear form is $\tau(\text{G})$-invariant if $\mathcal{B}(v_1,v_2)=\mathcal{B}(\tau(G)v_1,\tau(G)v_2)$ for all $G\in\text{G}$.

Definition 12 (cf., Refs. [53,54]). Consider an irreducible complex representation τ of G in $V_{\mathbb{C}}$. The representation τ is said to be of real type if $V_{\mathbb{C}}$ admits a bilinear form that is nonzero, nondegenerate, $\tau(\text{G})$-invariant, and symmetric; complex type if $V_{\mathbb{C}}$ admits no bilinear form that is nonzero, nondegenerate, and $\tau(\text{G})$-invariant; and quaternionic type if $V_{\mathbb{C}}$ admits a bilinear form that is nonzero, nondegenerate, $\tau(\text{G})$-invariant, and skew symmetric.

We introduce the map $\chi_\tau:\text{G}\rightarrow\mathbb{C},G\mapsto\text{Tr}[\tau(G)]$, which is the character χ_τ of the representation τ. We use the character to characterize the type (real, complex, or quaternionic) of irreducible complex representations.

Fact 10 (Ref. [53], Theorem 4.8.1). Let τ denote an irreducible complex representation of G in $V_{\mathbb{C}}$. The character χ_τ is real valued if and only if there exists a $\tau(\text{G})$-invariant, nonzero, complex bilinear form $\mathcal{B}$ on $V_{\mathbb{C}}$ that is automatically nondegenerate and uniquely determined, up to a nonzero scalar factor. This bilinear form $\mathcal{B}$ is either symmetric or skew symmetric.

By means of Fact 10 we can decide if the type of a representation is complex. To complete the classification of the type (real, complex, or quaternionic) of irreducible complex representations, we state another fact that allows us to determine the type of a representation by computing an normalized integral over the compact Lie group G.

Fact 11 (see Ref. [53], Prop. 4.8.7 and Ref. [54], Prop. 6.8 of Chap. II). Let τ be an irreducible complex representation of the compact Lie group G in $V_{\mathbb{C}}$ with character χ_τ. Then we have

$$\int\chi_\tau(G^2)dG=\begin{cases}1 & \Leftrightarrow\tau\text{ is of real type,}\\0 & \Leftrightarrow\tau\text{ is of complex type,}\\-1 & \Leftrightarrow\tau\text{ is of quaternionic type.}\end{cases}$$

Representations can be identified with subgroups of $\text{GL}(V_{\mathbb{C}})$, so we can extend Definition 12 to subgroups of $\text{GL}(V_{\mathbb{C}})$. We denote the general linear group on a complex vector space of dimension k by $\text{GL}(k,\mathbb{C})$. Next we characterize the subgroups of $\text{GL}(k,\mathbb{C})$ that are conjugated to subgroups of the orthogonal group (motivated by Sec. VI A) or the symplectic group.

Fact 12 (adapted from Ref. [26], Theorem H of Chap. 3). A compact subgroup of the general linear group $\text{GL}(k,\mathbb{C})$ is conjugated in $\text{GL}(k,\mathbb{C})$ to a subgroup of the orthogonal group $\text{O}(k)$ if and only if it is of real type. Accordingly, a subgroup of $\text{GL}(2k,\mathbb{C})$ is conjugated in $\text{GL}(2k,\mathbb{C})$ to a subgroup of the (unitary) symplectic group $\text{Sp}(k)$ if and only if it is of quaternionic type.

Remark. Actually, Ref. [26] gives an algorithm to compute the basis change from the bilinear form mentioned in Definition 12. For the notation $\text{Sp}(k)$ see Sec. VI D and Ref. [55].

After this preparation we consider the case of local unitary operations $[\text{SU}(2)]^{\otimes n}$. We employ the standard representation of SU(2):

$$G=\begin{pmatrix}a+ib & c+id\\-c+id & a-ib\end{pmatrix},$$

where $a,b,c,d\in\mathbb{R}$ and $a^2+b^2+c^2+d^2=1$. To compute the integral of Fact 11, we introduce the real parameters $0\leq\phi<2\pi$, $0\leq\psi_1\leq\pi$, and $0\leq\psi_2\leq\pi$ as follows:

$$a=\cos(\phi)\sin(\psi_1)\sin(\psi_2),$$

$$b=\sin(\phi)\sin(\psi_1)\sin(\psi_2),$$

$$c=\cos(\psi_1)\sin(\psi_2),$$

$$d=\cos(\psi_2).$$

We obtain

$$\int\chi_\tau(G^2)d[\text{SU}(2)]^{\otimes n}=\left(\int\chi_\tau(G^2)d\text{SU}(2)\right)^n$$

$$=\left(\int_0^{2\pi}\int_0^\pi\int_0^\pi\Xi(\phi,\psi_1,\psi_2)d\psi_2d\psi_1d\phi\right)^n$$

$$=(-1)^n,$$

where

$$\Xi(\phi,\psi_1,\psi_2) = \{4\cos(\phi)^2[1 - \cos(\psi_1)^2 - \cos(\psi_2)^2$$
$$+ \cos(\psi_1)^2\cos(\psi_2)^2] - 2\}\sin(\psi_1)\sin(\psi_2)^2.$$

This proves the following theorem.

Theorem 3. The local unitary operations on an even number of qubits are conjugated to a subgroup of an orthogonal group. The local unitary operations on an odd number of qubits are conjugated to a subgroup of a (unitary) symplectic group.

Remark. Similar results are obtained in Ref. [56] using a different approach.

C. Thompson's theorem and majorization

Following Ref. [10], we present in this subsection a theorem due to Thompson [57] and a majorization condition for the spectra of the sum of two Hermitian matrices. Both results will be employed below.

Fact 13 (Ref. [57]). Let A and B be Hermitian matrices. Then there exist unitary matrices U_1 and U_2 such that

$$\exp(iA)\exp(iB) = \exp(iU_1^{-1}AU_1 + iU_2^{-1}BU_2).$$

This result of Thompson relies partly on a conjecture of Horn [58]. This conjecture was recently proven [59–64]. By induction, we get Corollary 4.

Corollary 4. Let A_j denote Hermitian matrices. Then there exist unitary matrices U_j such that

$$\prod_{j=1}^{m}\exp(iA_j) = \exp\left(i\sum_{j=1}^{m}U_j^{-1}A_jU_j\right).$$

We state now a result which gives us bounds for the the spectra of the sum of two Hermitian matrices. Reference [41] attributes this result to Ky Fan [65]. We denote the vector of eigenvalues of the $k \times k$-dimensional matrix A, including multiplicities, by $\mathrm{spec}(A) = [\mathrm{spec}(A)_1, \ldots, \mathrm{spec}(A)_k]^T$. In addition, we assume that $\mathrm{spec}(A)_i \geq \mathrm{spec}(A)_j$ if $i < j$ ($1 \leq i, j \leq k$).

Fact 14 (Ref. [41], Theorem 9.G.1). Let A and B denote Hermitian matrices. Then the following equation holds:

$$\mathrm{spec}(A + B) \prec \mathrm{spec}(A) + \mathrm{spec}(B).$$

D. Lower bounds

In this section we derive lower bounds on the minimal time to simulate unitary operations (see Definition 1). We begin by discussing the (unitary) symplectic group. Following Ref. [55] on p. 22, we introduce the bilinear form

$$\mathcal{B}_{\mathrm{Sp}}(\vec{x},\vec{y}) := \sum_{j=1}^{k}(x_iy_{i+k} - x_{i+k}y_i), \tag{16}$$

where $\vec{x} = (x_1,\ldots,x_{2k})^T \in \mathbb{C}^{2k}$ and $\vec{y} = (y_1,\ldots,y_{2k})^T \in \mathbb{C}^{2k}$. Let J_k denote the matrix

$$J_k = \begin{pmatrix} 0_k & I_k \\ -I_k & 0_k \end{pmatrix},$$

where is the I_k is the $k \times k$-dimensional identity matrix and 0_k the $k \times k$-dimensional zero matrix.

Definition 13 (see, e.g., Ref. [55], Prop. 1 on p. 22). The subgroup of the unitary group U($2k$) of degree $2k$ composed of the matrices M which leave the bilinear form in Eq. (16) invariant, i.e., which satisfy the condition

$$M^TJ_kM = J_k, \tag{17}$$

is called the (unitary) symplectic group and is denoted by Sp(k).

The group Sp(k) can be considered as operating on a k-dimensional module over the quaternions $\mathbb{H}$ leaving a symplectic (scalar) product invariant (Ref. [55], pp. 16–24). All elements of Sp(k) have determinant one (see, e.g., Ref. [55], p. 203). When we regard Sp(k) as a manifold its real dimension is $2k^2 + k$ (Ref. [55], p. 23).

We recall from Theorem 3 that the local unitary operations on an odd number of qubits are conjugated to a subgroup of a (unitary) symplectic group. Using that $(J_k)^{-1} = -J_k$, the condition in Eq. (17) can be proved to be equivalent to

$$M^{-1} = J_kM^T(J_k)^{-1}. \tag{18}$$

We know that the local unitary operations on an odd number of qubits meet the condition in Eq. (18) in some appropriate chosen basis. But we can state the condition also in the standard representation of $[\mathrm{SU}(2)]^{\otimes n}$ with n odd. We use the identification $2k = 2^n$. Let J'_n denote the matrix

$$J'_n := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{\otimes n} = (i\sigma_y)^{\otimes n}$$

and recall the standard representation of SU(2):

$$G = \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix},$$

where $a,b,c,d \in \mathbb{R}$. We use the notation

$$G_j = \begin{pmatrix} a_j+ib_j & c_j+id_j \\ -c_j+id_j & a_j-ib_j \end{pmatrix},$$

where $a_j,b_j,c_j,d_j \in \mathbb{R}$. It can be checked that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}G^T\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = G^{-1}$$

and we obtain that

$$J'_n\left(\mathop{\otimes}_{j=1}^{n}G_j\right)^T(J'_n)^{-1} = \left(\mathop{\otimes}_{j=1}^{n}G_j\right)^{-1}, \tag{19}$$

which holds obviously for odd and even. From now on, n is no longer restricted to be odd. We emphasize that $(J'_n)^{-1} = (J'_n)^T = (-1)^n J'_n$. It follows that

$$\left(\mathop{\otimes}_{j=1}^{n}G_j\right)^T J'_n\left(\mathop{\otimes}_{j=1}^{n}G_j\right) = J'_n. \tag{20}$$

Let $\mathcal{H}$ denote the 2^n-dimensional complex vector space on which the group SU(2^n) operates. We introduce the bilinear form $\mathcal{B}_{\mathcal{H}}(x,y) := x^T J'_n y$ on the Hilbert space $\mathcal{H}$. We have that

$$\mathcal{B}_{\mathcal{H}}(y,x) = y^T J'_n x = (-1)^n x^T J'_n y = (-1)^n \mathcal{B}_{\mathcal{H}}(x,y),$$

which proves that $\mathcal{B}_{\mathcal{H}}(x,y)$ is symmetric for n even and skew-symmetric for n odd. From Eq. (20) we get that $\mathcal{B}_{\mathcal{H}}(x,y)$ is left invariant by $[\mathrm{SU}(2)]^{\otimes n}$. Hence, we have identified $\mathcal{B}_{\mathcal{H}}(x,y)$ as the bilinear form of Definition 12 operating on $V_{\mathbb{C}} = \mathcal{H}$.

This motivates the following definition of the tilde mapping, which operates on the local unitary operations as the inverse operation.

Definition 14. We introduce the tilde mapping

$$\Psi : \begin{cases} \mathrm{SU}(2^n) \to \mathrm{SU}(2^n) \\ U \mapsto \widetilde{U} := \Psi(U) = J'_n U^T (J'_n)^{-1}. \end{cases}$$

It is apparent from $[J'_n U^T (J'_n)^{-1}][J'_n U^T (J'_n)^{-1}]^\dagger = I_{2^n}$ and $\det[(J'_n)^{-1} U^T J'_n] = \det(U)$ that the tilde mapping preserves the group $\mathrm{SU}(2^n)$.

Remark. The tilde mapping is a generalization of the map $U \mapsto (\sigma_y)^{\otimes n} U^T (\sigma_y)^{\otimes n}$ for even n from Ref. [10] on p. 5. It can be easily checked that the two maps coincide in the case of even n. See also the discussion in Sec. VIII.

We state now an important lemma characterizing the tilde mapping.

Lemma 4. Let V and W denote some local unitary operations and let U denote some arbitrary unitary operation. The following three equations hold:

$$\widetilde{V} = V^{-1},$$

$$\widetilde{W} = W^{-1},$$

$$VUW\Psi(VUW) = VU\widetilde{U}V^{-1}.$$

Proof. The first and second claim follows from Eq. (19). We prove now the third claim: $VUW\Psi(VUW) = VUW\widetilde{W}\widetilde{U}\widetilde{V} = VUWW^{-1}\widetilde{U}V^{-1} = VU\widetilde{U}V^{-1}.$ ∎

This proves that local unitary operations preserve the spectrum of $U\widetilde{U}$. We now state the theorem that gives us lower bounds for the minimal time to simulate a unitary gate. We use the notation arg where $\arg[\exp(im)] = m$ and $\arg[(x_1, \ldots, x_l)^T] = (\arg[x_1], \ldots, \arg[x_l])^T.$

Theorem 4. Assume that H is a nonlocal Hamilton operator acting on an n-qubit system and that we intend to simulate the unitary gate U. An n-qubit system with Hamilton operator H and local unitary operators available is able to simulate the unitary gate U in time t only if the following equation holds for at least one choice of $\vec{z} \in \mathbb{Z}^{2n}$:

$$\arg[\mathrm{spec}(U\widetilde{U})] + 2\pi\vec{z} < 2t \ \mathrm{spec}(H).$$

Remark. This theorem generalizes the work in Theorem 5 and Corollary 7 of Ref. [10]. In the proof we use ideas from Ref. [10].

Proof. Assume that $U = [\prod_{j=1}^m W_j \exp(-it_j H)] W_0$ is a simulation of U, where W_j denotes some local unitary operations, $t_j \geq 0$, and $\sum_{j=1}^m t_j = t.$ Let

$$V_j = \begin{cases} W_m & \text{for } j = m, \\ V_{j+1} W_j & \text{for } 0 \leq j < m. \end{cases}$$

and $H_j = V_j H V_j^{-1} (1 \leq j \leq m).$ Thus, the simulation of U can written as $U = [\prod_{j=1}^m \exp(-it_j H_j)] V_0$ where $\mathrm{spec}(H_j) = \mathrm{spec}(H)$ for all $1 \leq j \leq m.$

We use Corollary 4 to find some suitable Hermitian operators H'_j and H''_j with $\mathrm{spec}(H'_j) = \mathrm{spec}(H''_j) = \mathrm{spec}(H)$ and $j \in \{1, \ldots, m\}$ such that

$$\left[\prod_{j=1}^m \exp(-it_j H_j) \right] \Psi \left[\prod_{j=1}^m \exp(-it_j H_j) \right]$$
$$= \exp\left[\prod_{j=1}^m -it_j(H'_j + H''_j) \right]. \tag{21}$$

When we combine $\widetilde{V}_0 = V_0^{-1}$ with Eq. (21) we obtain that

$$\mathrm{spec}(U\widetilde{U}) = \mathrm{spec}\left\{ \exp\left[i\prod_{j=1}^m t_j(H'_j + H''_j) \right] \right\}.$$

We employ Fact 14 to complete the proof:

$$\arg[\mathrm{spec}(U\widetilde{U})] + 2\pi\vec{z} = \mathrm{spec}\left(\sum_{j=1}^m t_j(H'_j + H''_j) \right) < 2t \ \mathrm{spec}(H).$$

∎

E. Involutive automorphisms

We end this section by highlighting connections between the tilde mapping of Def. 14 and involutive automorphisms of the Lie algebra $\mathfrak{su}(2^n)$.

The tilde mapping is similar to the $(\ )^\star$-map used in the proof of Lemma 2 in Sec. V. For n odd, K must be equivalent to $\mathrm{Sp}(2^{n-1})$ and, respectively, for n even, K must be equivalent to $\mathrm{SO}(2^n)$. In both cases, the map $U \to U\widetilde{U}$ plays a similar rôle as the map ϕ in Sec. V.

Following Ref. [25] on pp. 451–452, we state all Riemannian symmetric spaces $\mathrm{SU}(2^n)/K$ induced by involutive automorphisms of the Lie algebra $\mathfrak{su}(2^n).$ We have to consider three cases that correspond to the types AI, AII, and AIII of involutive automorphisms. In the case of type AI, we have to treat the Lie algebra $\mathfrak{g} = \mathfrak{su}(k)$ and the involutive automorphism $\theta_{\mathrm{AI}}(g) = g^*.$ The involutive automorphism θ_{AI} gives rise to the Riemannian symmetric space $\mathrm{SU}(k)/\mathrm{SO}(k).$

The Lie algebra $\mathfrak{g} = \mathfrak{su}(2k)$ and the involutive automorphism $\theta_{\mathrm{AII}}(g) = J_k g^* (J_k)^{-1}$ belong to type AII. We obtain the Riemannian symmetric space $\mathrm{SU}(2k)/\mathrm{Sp}(k).$

For completeness we mention the type AIII even though we do not use the corresponding Riemannian symmetric space in this paper. The Lie algebra is $\mathfrak{g} = \mathfrak{su}(p+q)$ and the corresponding involutive automorphism is given by $\theta_{\mathrm{AII}}(g) = I_{p,q} g I_{p,q}.$ We have used the notation

$$I_{p,q} = \begin{pmatrix} -I_p & 0_{p,q} \\ 0_{q,p} & I_q \end{pmatrix},$$

where I_p denotes the $p \times p$-dimensional identity matrix and $0_{p,q}$ denotes the $p \times q$-dimensional zero matrix. This gives us

the Riemannian symmetric space $\mathrm{SU}(p+q)/\mathrm{S}(\mathrm{U}(p)\times\mathrm{U}(q))$. The group $\mathrm{S}(\mathrm{U}(p)\times\mathrm{U}(q))$ can be represented by the matrices

$$\begin{pmatrix} g_1 & 0_{p,q} \\ 0_{q,p} & g_2 \end{pmatrix},$$

where $g_1\in\mathrm{U}(p)$, $g_2\in\mathrm{U}(q)$, and $\det(g_1)\det(g_2)=1$.

VII. RELATED WORK

To recognize the considerable amount of related work we give a short outline of the connections to our work. Various aspects of (infinitesimal) Hamiltonian simulation as considered in Sec. IV were studied in Refs. [4,13–19,46,66–75]. Some references consider models where—in contrast to our model—additional resources were used: prior entanglement [73], additional classical communication [46], measurements [4], or ancillas [4,46].

For two qubits, gate simulation (see Sec. V) was analyzed in Refs. [5–7,14,24,76]. In Ref. [23] Lie group decompositions were used to obtain a theory of n-qubit gate simulation. In general these decompositions do not lead to optimal simulations. In the case of three qubits some progress on the time optimality problem for gate simulation was reported in Ref. [77], see also Ref. [78]. Concerning lower bounds, we have generalized (see Sec. VI) the approach of Ref. [10].

VIII. DISCUSSION

In this section we address a peculiar similarity between our approach to lower bounds on the time complexity for gate simulation and the concurrence [9,11,79,80], as well as some of its generalizations [56,81–94]. The concurrence C of a pure two-qubit state $|\psi\rangle\in\mathbb{C}^4$ was defined in Ref. [11] as

$$C(|\psi\rangle)=|\langle\psi|\widetilde{\psi}\rangle|,$$

where $|\psi\rangle:=(\sigma_y\otimes\sigma_y)(|\psi\rangle)^*$. Let λ_1, λ_2, λ_3, and λ_4 denote the (positive) square roots of the eigenvalues of the matrix $\rho\widetilde{\rho}$, where $\widetilde{\rho}:=(\sigma_y\otimes\sigma_y)\rho^*(\sigma_y\otimes\sigma_y)$. We assume that $\lambda_1\geqslant\lambda_2\geqslant\lambda_3\geqslant\lambda_4$. References [9,11] show that the concurrence C of a two-qubit density matrix ρ is given by

$$C(\rho)=\max\{0,\lambda_1-\lambda_2-\lambda_3-\lambda_4\}. \tag{22}$$

Uhlmann [82] considered generalizations of the concurrence. Following this approach we introduce some notations. Let us call a map ϑ that operates on a complex vector space $V_{\mathbb{C}}$ antilinear if the equation $\vartheta(b_1|\psi_1\rangle+b_2|\psi_2\rangle)=(b_1)^*\vartheta(|\psi_1\rangle)+(b_2)^*\vartheta(|\psi_2\rangle)$ holds for all b_1, $b_2\in\mathbb{C}$ and all $|\psi_1\rangle,|\psi_2\rangle\in V_{\mathbb{C}}$. For an antilinear operator ϑ the (Hermitian) adjoint $\vartheta^\dagger$ is defined by the condition that $\langle\psi_1|\vartheta^\dagger\psi_2\rangle=\langle\psi_2|\vartheta\psi_1\rangle$ holds for all $|\psi_1\rangle,|\psi_2\rangle\in V_{\mathbb{C}}$. If an antilinear operator ϑ satisfies the condition $\vartheta^\dagger=\vartheta^{-1}$ we call this operator antiunitary. When the map ϑ is antiunitary and $\vartheta^{-1}=\vartheta$ holds, then we have that ϑ^2 equals the identity map and we define ϑ to be a conjugation. A skew conjugation is an antiunitary operator ϑ fulfilling $\vartheta^{-1}=-\vartheta$. Assume in the following that ϑ is a conjugation. Now, Uhlmann defined a generalized

tilde mapping by its operation on pure states $|\widetilde{\psi}\rangle:=\vartheta(|\psi\rangle)$ and its operation on density matrices $\widetilde{\rho}:=\vartheta\rho\vartheta^{-1}=\vartheta\rho\vartheta$. In addition he generalizes the concept of concurrence to more than two qubits for pure states

$$C_\vartheta(|\psi\rangle):=|\langle\psi|\widetilde{\psi}\rangle|$$

and for mixed states

$$C_\vartheta(\rho):=\min\sum_j|\langle\phi_j|\widetilde{\phi}_j\rangle|,$$

where the minimum is taken over all decompositions $\rho=\Sigma_j|\phi_j\rangle\langle\phi_j|$ of ρ into nonnormalized pure states $|\phi_j\rangle$. Uhlmann [82] proved that in strong analogy to Eq. (22) the generalized concurrence is given by

$$C_\vartheta(\rho)=\max\left\{0,\lambda_1-\sum_{j>1}\lambda_j\right\},$$

where the λ_is are the square roots of the eigenvalues of the matrix $\rho\widetilde{\rho}$ and $\lambda_i\geqslant\lambda_j$ for $i<j$.

References [88,91,94] consider the map on density matrices given by

$$\rho\mapsto\widetilde{\rho}:=(\sigma_y)^{\otimes n}\rho^*(\sigma_y)^{\otimes n}. \tag{23}$$

In addition, the map

$$iH\mapsto i\widetilde{H}:=(-i\sigma_y)^{\otimes n}(iH)^*[(-i\sigma_y)^{\otimes n}]^{-1} \tag{24}$$

is introduced in Ref. [56] for elements iH of the Lie algebra $\mathfrak{su}(2^n)$. The map in Eq. (24) can be applied to a Hamilton operator H:

$$\widetilde{H}=(-i\sigma_y)^{\otimes n}(H)^*[(-i\sigma_y)^{\otimes n}]^{-1}=(\sigma_y)^{\otimes n}(H)^*(\sigma_y)^{\otimes n}.$$

This shows that both Eq. (23) and (24) are induced by the conjugation ϑ_1 given by

$$\vartheta_1(|\psi\rangle)=\sigma_y^{\otimes n}(|\psi\rangle)^*.$$

In this case we get the concurrence C_{ϑ_1}. The corresponding tilde mapping is given by its action on pure states $|\widetilde{\psi}\rangle=\vartheta_1|\psi\rangle$ and its action on density matrices $\widetilde{\rho}=\vartheta_1\rho\vartheta_1^{-1}=\vartheta_1\rho\vartheta_1$. Proposition 8 of Ref. [95] (for related remarks see Ref. [85]) states that the conjugation ϑ_1 is the (up to a phase) unique antilinear operator acting on the complex vector space $(\mathbb{C}^2)^{\otimes n}$ which is invariant under basis changes by local unitary operations U except for an factor equal to $\det(U)$. Further on, Ref. [95] states that such an antilinear mapping exists only for n-qubit systems and not for general n-qudit systems.

After this short excursion into entanglement measures of concurrence-type, we can state a connection between this type of entanglement measures and lower bounds on the time complexity for gate simulation. The tilde mapping of Def. 14, which was used in the main body of the text, can be interpreted in the context of concurrence-type entanglement measures. Since $H^T=H^*$ holds for all Hermitian operators we obtain

$$\Psi(U) = J'_n[\exp(iH)]^T (J'_n)^{-1} = \exp[iJ'_n H^* (J'_n)^{-1}],$$

where $iJ'_n H^* (J'_n)^{-1}$ is up to a minus sign equal to the rhs of Eq. (24). This highlights that if we consider the lower bounds introduced in Sec. VI we are essential in setting of Ref. [82] with $\vartheta = \vartheta_1$.

In both constructions, for the lower bounds on the time complexity to simulate unitary operators and for the computation of the concurrence, the essential point is that the spectrum of both $U\tilde{U}$ and $\rho\tilde{\rho}$ is invariant under local unitary operations. This highlights that there is a connection between entanglement measures and lower bounds on the time complexity for gate simulation. We are looking forward to generalizing some of these ideas.

IX. CONCLUSION

Starting with an extensive reconsideration of infinitesimal Hamiltonian simulation and gate simulation in the two-qubit case, we streamlined the different approaches by using Lie-theoretic methods. As the success of this approach suggests, this seems to be the appropriate level of description for such a theory.

Going beyond two-qubits, we derived lower bounds on the time complexity for gate simulation. For this aim, we developed an analog of the magic basis for general multipartite qubit systems. This gives us a first idea of the structure of unitary operations with respect to the set of local unitary operations. In addition, we related our approach to entanglement measures of concurrence-type.

Note added in proof. Recently we realized that Theorem 3 can be derived from Theorem 5 of Ref. [96]. In the proof of that theorem, a basis change similar to our basis change in Sec. VI D for odd n is given.

ACKNOWLEDGMENTS

APPENDIX: SPECTRAL THEORY FOR INFINITESIMAL HAMILTONIAN SIMULATION

In this appendix we prove a similar version of Theorem 2. Relying on Sec. IV B, we use arguments from the theory of majorization applied to the spectrum of Hamilton operators. We denote the vector of eigenvalues of the $k \times k$-dimensional matrix A, including multiplicities, by $\mathrm{spec}(A) = (\mathrm{spec}(A)_1, \ldots, \mathrm{spec}(A)_k)^T$. In addition, we assume that $\mathrm{spec}(A)_i \geq \mathrm{spec}(A)_j$ if $i < j$ $(1 \leq i, j \leq k)$. The majorization of the spectra of two matrices is, by a theorem of Uhlmann [97], related to the convex combination of unitary orbits.

Fact 15 (Uhlmann) (see, e.g., [97], Satz 3 or [42], Theorem 2-2). For Hermitian matrices A and B the condition $\mathrm{spec}(A) \prec \mathrm{spec}(B)$ is equivalent to

$$A = \sum_i q_i U_i^{-1} B U_i,$$

where U_i are unitary matrices, $q_i \geq 0$, and $\Sigma_i q_i = 1$.

We need another theorem connecting the notion of majorization with the convex hull of all permuted versions of a vector.

Fact 16 (Rado) (see, e.g., Ref. [98] or [41], Prop. 4.C.1). The vector x is majorized by the vector y if and only if x lies in the convex hull of all permutations of y.

The spectral version of Theorem 2 reads as follows:

Theorem 5 ([46], pp. 9–10). Assume that H and H' are nonlocal Hamilton operators acting on a two-qubit system. Let a and a' be elements of $\mathfrak{a}$, where $a = a_1 X_7 + a_2 X_8 + a_3 X_9 = [\mathrm{Ad}_\mathfrak{g}(L)](H)$ and $a' = a'_1 X_7 + a'_2 X_8 + a'_3 X_9 = [\mathrm{Ad}_\mathfrak{g}(L')](H')$ for some local unitary operators L and L' $(a_i, a'_i \in \mathbb{R})$. A two-qubit system with Hamilton operator H and local unitary operators available is able to simulate the Hamilton operator H' in time t if and only if

$$\mathrm{spec}(a') \prec t\,\mathrm{spec}(a).$$

Remark. The necessity of this condition was proven in Ref. [15]. In the proof, we follow Ref. [46].

Proof. Due to Fact 2 we can choose a and a' as given. The "only-if" case follows by Fact 15. We consider now the "if" case. By invoking Fact 16, we get that

$$\mathrm{spec}(a'/t) = \sum_k q_k P_k\, \mathrm{spec}(a),$$

where P_k is a permutation, $q_k \geq 0$, and $\Sigma_k q_k = 1$. Since a and a' are elements of $\mathfrak{a}$, they commute. It follows that there exists a basis where a and a' are simultaneously diagonal. In that basis the permutations P_k correspond to permutations of the diagonal elements of a. For that reason we have that

$$(a'/t) = \sum_k q_k U_k^{-1} a U_k$$

for some unitary operators U_k, which permute the spectrum of a. We emphasize that the U_k are not necessarily local. But we prove now that we can find local unitary operators implementing any permutation of the spectrum of a. Conjugation by the local unitary operators $[(\sigma_0 - i\sigma_1)/\sqrt{2}] \otimes [(\sigma_0 - i\sigma_1)/\sqrt{2}]$, $[(\sigma_0 + i\sigma_3)/\sqrt{2}] \otimes [(\sigma_0 + i\sigma_3)/\sqrt{2}]$, and $[(\sigma_0 + i\sigma_1)/\sqrt{2}] \otimes [(\sigma_0 - i\sigma_1)/\sqrt{2}]$ permutes the eigenvalues as respectively follows: $(1,2,3,4) \mapsto (2,1,3,4)$, $(1,2,3,4) \mapsto (1,3,2,4)$, and $(1,2,3,4) \mapsto (1,2,4,3)$. As all permutations on four-vectors are generated by this permutations, the "if" case follows. ∎

We note that the local unitary operators that permute the spectrum of elements of $\mathfrak{a}$ are given in Ref. [46], but there the second local unitary operator is misprinted.

[1] G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments* (Springer, Berlin, 2001).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[3] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[4] 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).

[5] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001).

[6] G. Vidal, K. Hammerer, and J. I. Cirac, Phys. Rev. Lett. **88**, 237902 (2002).

[7] K. Hammerer, G. Vidal, and J. I. Cirac, Phys. Rev. A **66**, 062321 (2002).

[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

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

[10] A. M. Childs, H. L. Haselgrove, and M. A. Nielsen, Phys. Rev. A **68**, 052311 (2003).

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

[12] J. J. Sakurai, *Modern Quantum Mechanics* (Addison-Wesley, Reading, MA, 1994), rev. ed.

[13] L. Masanes, G. Vidal, and J. I. Latorre, Quantum Inf. Comput. **2**, 285 (2002).

[14] H. L. Haselgrove, M. A. Nielsen, and T. J. Osborne, Phys. Rev. A **68**, 042303 (2003).

[15] P. Wocjan, D. Janzing, and T. Beth, Quantum Inf. Comput. **2**, 117 (2002).

[16] D. Janzing, P. Wocjan, and T. Beth, Phys. Rev. A **66**, 042311 (2002).

[17] P. Wocjan, M. Rötteler, D. Janzing, and T. Beth, Quantum Inf. Comput. **2**, 133 (2002).

[18] P. Wocjan, M. Rötteler, D. Janzing, and T. Beth, Phys. Rev. A **65**, 042309 (2002).

[19] H. Chen, Quantum Inf. Comput. **3**, 249 (2003).

[20] A quantum information science and technology roadmap, Tech. Report LA-UR-02-6900, URL http://qist.lanl.gov (2002) (unpublished).

[21] U. Heberlen and J. S. Waugh, Phys. Rev. **175**, 453 (1968).

[22] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1997); reprinted with corrections.

[23] N. Khaneja and S. J. Glaser, Chem. Phys. **267**, 11 (2001).

[24] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. A **67**, 042313 (2003).

[25] S. Helgason, *Differential Geometry, Lie Groups, and Symmetric Spaces* (American Mathematical Society, Providence, 2001), reprinted with corrections.

[26] H. Samelson, *Notes on Lie Algebras*, 2nd ed. (Springer, New York, 1999).

[27] A. W. Knapp, *Lie Groups Beyond an Introduction*, 2nd ed. (Birkhäuser, Boston, 2002).

[28] V. S. Varadarajan, *Lie Groups, Lie Algebras, and Their Representations* (Springer, New York, 1984).

[29] S. Kobayashi and K. Nomizu, *Foundations of Differential Geometry* (Wiley, New York, 1991), Vol. 1.

[30] S. Kobayashi and K. Nomizu, *Foundations of Differential Geometry* (Wiley, New York, 1996), Vol. 2.

[31] J. A. Wolf, *Spaces of Constant Curvature*, 5th ed. (Publish or Perish, Wilmington, 1984).

[32] O. Loos, *Symmetric Spaces I: General Theory* (W. A. Benjamin, New York, 1969).

[33] O. Loos, *Symmetric Spaces II: Compact Spaces and Classification* (W. A. Benjamin, New York, 1969).

[34] A. Borel, *Semisimple Groups and Riemannian Symmetric Spaces* (Hindustan Book Agency, 1998).

[35] R. Gilmore, *Lie Groups, Lie Algebras, and Some of Their Applications* (Krieger Publishing, Malabar, 1994), reprint.

[36] B. Kostant, Ann. Sci. Ec. Normale Super. **4**, 413 (1973).

[37] G. J. Heckman, PhD thesis, Leiden (1980).

[38] G. E. Collins and H. Hong, J. Symb. Comput. **12**, 299 (1991).

[39] QEPCAD Version B 1.21 (2003), URL http://www.cs.usna.edu/~qepcad/B/QEPCAD.html

[40] M. A. Nielsen and G. Vidal, Quantum Inf. Comput. **1**, 76 (2001).

[41] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications* (Academic, New York, 1979).

[42] P. M. Alberti and A. Uhlmann, *Stochasticity and Partial Order* (VEB Deutscher Verlag der Wissenschaften, Berlin, 1982).

[43] T. Ando, Linear Algebr. Appl. **118**, 163 (1989).

[44] T. Ando, Linear Algebr. Appl. **199**, 17 (1989).

[45] R. Bhatia, *Matrix Analysis* (Springer, New York, 1997).

[46] G. Vidal and J. I. Cirac, Phys. Rev. A **66**, 022315 (2002).

[47] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).

[48] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

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

[50] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[51] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, (R)3319 (1997).

[52] Y. Makhlin, Quantum Inf. Process. **1**, 243 (2003).

[53] J. J. Duistermaat and J. A. C. Kolk, *Lie Groups* (Springer, Berlin, 2000).

[54] T. Bröcker and T. tom Dieck, *Representations of Compact Lie Groups* (Springer, New York, 1985).

[55] C. Chevalley, *Theory of Lie Groups I* (Princeton University Press, Princeton, 1999), reprint.

[56] S. S. Bullock and G. K. Brennen, J. Math. Phys. **45**, 2447 (2004).

[57] R. C. Thompson, Linear and Multilinear Algebra **19**, 187 (1986).

[58] A. Horn, Pac. J. Math. **12**, 225 (1962).

[59] B. V. Lidskii, Funct. Anal. Appl. **16**, 139 (1982).

[60] J. Day, W. So, and R. C. Thompson, Linear Algebr. Appl. **280**, 289 (1998).

[61] A. A. Klyachko, Selecta Math., New Ser. **4**, 419 (1998).

[62] A. Knutson and T. Tao, J. Am. Math. Soc. **12**, 1055 (1999).

[63] A. Knutson, Linear Algebr. Appl. **319**, 61 (2000).

[64] W. Fulton, Bull., New Ser., Am. Math. Soc. **37**, 209 (2000).

[65] K. Fan, Proc. Natl. Acad. Sci. U.S.A. **35**, 652 (1949).

[66] L. Viola, S. Lloyd, and E. Knill, Phys. Rev. Lett. **83**, 4888 (1999).

[67] J. A. Jones and E. Knill, J. Magn. Reson. **141**, 322 (1999).

[68] D. W. Leung, I. L. Chuang, F. Yamaguchi, and Y. Yamamoto, Phys. Rev. A **61**, 042310 (2000).

[69] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys.

Rev. Lett. **87**, 137901 (2001).

[70] M. Stollsteimer and G. Mahler, Phys. Rev. A **64**, 052301 (2001).

[71] J. L. Dodd, M. A. Nielsen, M. J. Bremner, and R. T. Thew, Phys. Rev. A **65**, 040301(R) (2002).

[72] D. W. Leung, J. Mod. Opt. **49**, 1199 (2002).

[73] G. Vidal and J. I. Cirac, Phys. Rev. Lett. **88**, 167903 (2002).

[74] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A **66**, 022317 (2002).

[75] A. M. Childs, D. W. Leung, and G. Vidal, IEEE Trans. Inf. Theory **50**, 1189 (2004).

[76] M. J. Bremner, C. M. Dawson, J. L. Dodd, A. Gilchrist, A. W. Harrow, D. Mortimer, M. A. Nielsen, and T. J. Osborne, Phys. Rev. Lett. **89**, 247902 (2002).

[77] N. Khaneja, S. J. Glaser, and R. Brockett, Phys. Rev. A **65**, 032301 (2002).

[78] N. Khaneja, S. J. Glaser, and R. Brockett, Phys. Rev. A **68**, 049903(E) (2003).

[79] W. K. Wootters, Philos. Trans. R. Soc. London, Ser. A **356**, 1717 (1998).

[80] W. K. Wootters, Quantum Inf. Comput. **1**, 27 (2001).

[81] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[82] A. Uhlmann, Phys. Rev. A **62**, 032307 (2000).

[83] A. Wong and N. Christensen, Phys. Rev. A **63**, 044301 (2001).

[84] S. Albeverio and S.-M. Fei, J. Opt. B: Quantum Semiclassical Opt. **3**, 223 (2001).

[85] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).

[86] K. Audenaert, F. Verstraete, and B. DeMoor, Phys. Rev. A **64**, 052304 (2001).

[87] P. Badziag, P. Deuar, M. Horodecki, P. Horodecki, and R. Horodecki, J. Mod. Opt. **49**, 1289 (2002).

[88] G. Jaeger, M. Teodorescu-Frumosu, A. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **67**, 032307 (2003).

[89] H. Fan, K. Matsumoto, and H. Imai, J. Phys. A **36**, 4151 (2003).

[90] A. Loziński, A. Buchleitner, K. Życzkowski, and T. Wellens, Europhys. Lett. **62**, 168 (2003).

[91] M. Teodorescu-Frumosu and G. Jaeger, Phys. Rev. A **67**, 052305 (2003).

[92] E. Gerjuoy, Phys. Rev. A **67**, 052308 (2003).

[93] F. Verstraete, J. Dehaene, and B. DeMoor, Phys. Rev. A **68**, 012103 (2003).

[94] G. Jaeger, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **68**, 022318 (2003).

[95] K. G. H. Vollbrecht and R. F. Werner, J. Math. Phys. **41**, 6772 (2000).

[96] M. J. Bremner, J. L. Dodd, M. A. Nielsen, and D. Bacon, Phys. Rev. A **69**, 012313 (2004).

[97] A. Uhlmann, Wiss. Z.-Karl-Marx-Univ. Leipzig, Math.-Naturwiss. Reihe **20**, 633 (1971).

[98] R. Rado, J. Lond. Math. Soc. **27**, 1 (1952).