| Annales Henri Poincaré

Universality of Single-Qudit Gates

Adam Sawicki and Katarzyna Karnas

Abstract. We consider the problem of deciding if a set of quantum one-qudit gates $\mathcal{S} = \{g_1, \ldots, g_n\} \subset G$ is universal, i.e. if $<\mathcal{S}>$ is dense in G, where G is either the special unitary or the special orthogonal group. To every gate g in $\mathcal{S}$ we assign the orthogonal matrix Ad_g that is image of g under the adjoint representation $\mathrm{Ad}: G \to SO(\mathfrak{g})$ and $\mathfrak{g}$ is the Lie algebra of G. The necessary condition for the universality of $\mathcal{S}$ is that the only matrices that commute with all Ad_{g_i}'s are proportional to the identity. If in addition there is an element in $<\mathcal{S}>$ whose Hilbert–Schmidt distance from the centre of G belongs to $]0, \frac{1}{\sqrt{2}}[$, then $\mathcal{S}$ is universal. Using these we provide a simple algorithm that allows deciding the universality of any set of d-dimensional gates in a finite number of steps and formulate a general classification theorem.

1. Introduction

Quantum computer is a device that operates on a finite-dimensional quantum system $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ consisting of n *qudits* [4,19,28] that are described by d-dimensional Hilbert spaces, $\mathcal{H}_i \simeq \mathbb{C}^d$ [29]. When $d = 2$ qudits are typically called qubits. The ability to effectively manufacture optical gates operating on many modes, using, for example, optical networks that couple modes of light [9,33,34], is a natural motivation to consider not only qubits but also higher-dimensional systems in the quantum computation setting (see also [30,31] for the case of fermionic linear optics and quantum metrology). One of the necessary ingredients for a quantum computer to work properly is the ability to perform arbitrary unitary operation on the system $\mathcal{H}$. We distinguish two types of operations. The first are one-qudit operations (one-qudit gates) that belong to $SU(\mathcal{H}_i) \simeq SU(d)$ and act on a single qudit. The second are k-qudit operations (k-qudit gates), $k \geq 2$, that belong to $SU(\mathcal{H}_{i_1} \otimes \cdots \otimes \mathcal{H}_{i_k}) \simeq SU(d^k)$ and act on the chosen k qudits. A k-qudit gate is non-trivial if it is not a tensor product of k single-qudit gates. We say that one-qudit gates $\mathcal{S} = \{g_1, \ldots, g_n\}$

are *universal* if any gate from $SU(d)$ can be built, with an arbitrary precision, using gates from $\mathcal{S}$. Mathematically, this means that the set $<\mathcal{S}>$ generated by elements from $\mathcal{S}$ is dense in $SU(d)$ and its closure is the whole $SU(d)$, i.e. $\overline{<\mathcal{S}>} = SU(d)$. It is known that once we have access to a universal set of one-qudit gates together with one additional two-qudit gate that does not map separable states onto separable states, we can build within a given precision, an arbitrary unitary gate belonging to $SU(\mathcal{H})$ [12] (see [32] for the similar criteria for fermionic and bosonic quantum computing). Thus, in order to characterise universal sets of gates for quantum computing with qudits, one needs to characterise sets that are universal for one qudit.

Although there are some qualitative characterisations of universal one-qudit gates, the full understanding is far from complete. It is known, for example, that almost all sets of qudit gates are universal, i.e. universal sets $\mathcal{S}$ of the given cardinality c form a Zariski open set in $SU(d)^{\times c}$. By the definition of a Zariski open set we can therefore deduce that non-universal gates can be characterised by vanishing of a finite number of polynomials in the gates entries and their conjugates [21,27]. These polynomials are, however, not known, and it is hard to find operationally simple criteria that decide one-qudit gates universality. Some special cases of two- and three-dimensional gates have been studied in [8,35]. The main obstruction in these approaches is the lack of classification of finite and infinite disconnected subgroups of $SU(d)$ for $d > 4$. Recently, there were also approaches providing algorithms for deciding universality of a given set of quantum gates that can be implemented on quantum automatas [17].

The goal of this paper is to provide some simple criteria for universality of one-qudit gates that can be applied even if one does not know classification of finite/infinite disconnected subgroups of $SU(d)$. To achieve this we divide the problem into two. First, using the fact that considered gates $\mathcal{S} = \{g_1, \ldots, g_n\}$ belong to groups that are compact simple Lie groups G, we provide a criterion which allows to decide if an infinite subgroup is the whole group G. It is formulated in terms of the adjoint representation matrices Ad_g, $g \in \mathcal{S}$ and boils down to finding the dimension of the commutant of all Ad_{g_i}'s. The necessary condition for universality is that the commutant is one-dimensional. Checking this reduces to calculating the dimension of the kernel of a matrix constructed from Ad_{g_i}'s, whose coefficients are polynomial in the entries of gates and their complex conjugates. Next, we give sufficient conditions for a set generated by $\mathcal{S}$ to be infinite. They stem from inequalities that relate the distances of two group elements and their commutators from the identity [7,15]. In particular, we show that for a pair of gates g_1 and g_2, for which the Hilbert–Schmidt distances from the centre $Z(G)$ of G are less than $\frac{1}{\sqrt{2}}$ and such that $[g_1, g_2]_\bullet := g_1 g_2 g_1^{-1} g_2^{-1} \notin Z(G)$, deciding universality boils down to checking if the corresponding Lie algebra elements generate the whole Lie algebra. Next we show that for a gate whose distance from $Z(G)$ is larger than $\frac{1}{\sqrt{2}}$, $\mathrm{dist}(g, Z(G)) \geq \frac{1}{\sqrt{2}}$, there is always $n \in \mathbb{N}$ such that $\mathrm{dist}(g^n, Z(G)) < \frac{1}{\sqrt{2}}$. Moreover, using Dirichlet approximation theorems (and their modifications)

we give an upper bound for the maximal N_G such that for every $g \in G$ we have $\text{dist}(g^n, Z(G)) < \frac{1}{\sqrt{2}}$ for some $1 \le n \le N_G$. For the gates that satisfy the necessary condition for universality, we show that the group generated by $\mathcal{S}$ is either 1) finite iff the distance of all its elements (besides those belonging to $Z(G)$) from $Z(G)$ is longer than $\frac{1}{\sqrt{2}}$ or 2) otherwise equal to G. This key observation gives rise to a simple algorithm that allows to decide universality of any given set of gates. Moreover, it leads to a general classification theorem. In order to formulate it we introduce the notion of the *exceptional spectrum*. For example, the spectrum of $g \in SU(d)$ is exceptional iff it is a collection of nth roots of $\alpha \in \mathbb{C}$, where $1 \le n \le N_{SU(d)}$ and $\alpha^d = 1$. Notably, there are only finitely many exceptional spectra and their number can be easily calculated. Our classification theorem states that $\mathcal{S}$ which satisfies the necessary universality condition and contains at least one matrix with a non-exceptional spectrum is universal. Our approach to checking if the generated group is infinite is somehow related to [22, 25]; however, the conceptual differences in both approaches are significant and the methods should be treated as independent. The problem of deciding if a finitely generated group is infinite has been also studied, and there are some algorithms that allow checking this property (see, for example, [2, 3, 17, 18]). In contrast to these approaches, our reasoning is based on the set of basic properties of compact connected simple Lie groups. The advantage for us of this approach is that it is explicit and direct. Moreover, the resulting algorithm is simple and can be easily implemented.

It is worth stressing here that universality criteria on the level of Lie groups require some additional conditions comparing to the level of Lie algebras. As an example, it was shown in [37] that for the system of n qubits, the set $\mathcal{S}$ consisting of all 1-qubit gates and the SWAP gates between all pairs of qubits is not universal, whereas an analogous set of gates with the square roots of SWAP is universal. It is, however, evident that in both cases the corresponding Hamiltonians generate $\mathfrak{su}(2^n)$. The interesting universal and non-universal extensions of local unitary gates in the setting for fermionic and bosonic quantum computing can be also found in [32].

In our paper we also demonstrate that the adjoint representation, this time for Lie algebras, can be useful in deciding if a finite subset $\mathcal{X}$ of a real compact semisimple Lie algebra generates the whole algebra (Sect. 3.1). This problem has been studied intensively in control theory [1, 11, 26] and in connection to universality of Hamiltonians, symmetries and controllability of quantum systems [14, 36, 40, 41]. There are numerous criteria known, and admittedly some are very general. Nevertheless, in Sect. 3.1 we provide criteria for the universality of $\mathcal{X}$ using our approach with the adjoint representation. As the considered groups are compact and connected, any gate $g \in G$ can be written as $g = e^X$, where X is an element of the Lie algebra of the group. In Theorem 4.6 we show that when all elements $g \in \mathcal{S}$ satisfy $\text{dist}(g, Z(G)) < \frac{1}{\sqrt{2}}$ the necessary and sufficient condition for universality of $\mathcal{S}$ is completely determined by generation of the Lie algebra by the logarithms of the gates from $\mathcal{S}$ (see Sect. 4.1 for the definition of the logarithm).

The last part of the paper concerns applications of the above ideas to $SU(2)$, $SO(3)$ and $SU(3)$. In particular, we give a full characterisation of the universal pairs of single-qubit gates and show that for any pair of $SU(2)$ gates our algorithm terminates for a word of the length $l \leq 13$. Moreover, if the universality algorithm does not terminate in Step 2 with $1 \leq l \leq 4$ the set $\mathcal{S}$ cannot be universal. We also show that for $SU(2)$ the exceptional spectra are in direct correspondence with the characters of the finite subgroups of $SU(2)$. We also characterise real and complex 2-mode beamsplitters that are universal when acting on $d \geq 3$ modes. Our approach allows to reproof the results of [8,35] without the knowledge of disconnected infinite or finite subgroups of $SO(3)$ and $SU(3)$.

2. Preliminaries

2.1. Compact Semisimple Lie Algebras

A real Lie algebra is a finite-dimensional vector space $\mathfrak{g}$ over $\mathbb{R}$ together with a commutator $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ that: (1) is bilinear, (2) is antisymmetric and (3) satisfies Jacobi identity $[[X, Y], Z] + [[Z, X], Y] + [[Y, Z], X] = 0$. In this paper we will often skip 'real' as we will consider only real Lie algebras. A Lie algebra $\mathfrak{g}$ is non-abelian if there is a pair $X, Y \in \mathfrak{g}$ such that $[X, Y] \neq 0$. A subspace $\mathfrak{h} \subset \mathfrak{g}$ is a subalgebra of $\mathfrak{g}$ if and only if for any $X, Y \in \mathfrak{h}$ we have $[X, Y] \in \mathfrak{h}$, i.e. $\mathfrak{h}$ is closed under taking commutators. An important class of subalgebras are *ideals*. A subalgebra $\mathfrak{h} \subset \mathfrak{g}$ is an ideal of $\mathfrak{g}$ if for any $X \in \mathfrak{g}$ and any $Y \in \mathfrak{h}$ we have $[X, Y] \in \mathfrak{h}$. One easily checks that an intersection of ideals is an ideal.

Definition 2.1. A non-abelian Lie algebra $\mathfrak{g}$ is simple if $\mathfrak{g}$ has no ideals other than 0 and $\mathfrak{g}$.

We say that a Lie algebra $\mathfrak{g}$ is a direct sum of Lie algebras, $\mathfrak{g} = \oplus_{i=1}^{n} \mathfrak{g}_i$, if and only if it is a direct sum of vector spaces $\{\mathfrak{g}_i\}_{i=1}^{n}$ and $[\mathfrak{g}_i, \mathfrak{g}_j] = 0$ for all $i \neq j$. In this case $\mathfrak{g}_i$'s are ideals of $\mathfrak{g}$. The algebras we are interested in belong to a special class of either simple Lie algebras or their direct sums. In the following we briefly discuss their properties.

A representation of a real Lie algebra on a real vector space is a linear map $\phi : \mathfrak{g} \to \mathrm{End}_{\mathbb{R}}(V)$ that satisfies $\phi([X, Y]) = [\phi(X), \phi(Y)]$. A representation is called *irreducible* if V has no $\phi(\mathfrak{g})$-invariant subspace $W \subset V$, i.e. a subspace for which $\phi(X)W \subset W$, for all $X \in \mathfrak{g}$.

As $\mathfrak{g}$ is a real vector space itself, one can consider representation of $\mathfrak{g}$ on $\mathfrak{g}$. In fact, there exists a canonical representation of this type that is called the *adjoint representation*:

$$\mathrm{ad} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g}), \quad \mathrm{ad}_X(Y) := [X, Y]. \tag{2.1}$$

Note that invariant spaces of the adjoint representation are ideals and therefore the adjoint representation of a simple Lie algebra is irreducible. Using the

adjoint representation we define a bilinear form on $\mathfrak{g}$, called the *Killing form* given by $B(X,Y) = \mathrm{tr}\,(\mathrm{ad}_X \circ \mathrm{ad}_Y)$.[1] The Killing form satisfies

$$B\left(\mathrm{ad}_X\left(Y\right), Z\right) + B\left(\mathrm{ad}_X\left(Z\right), Y\right) = 0. \tag{2.2}$$

Definition 2.2. A real Lie algebra $\mathfrak{g}$ is a <u>compact semisimple Lie algebra</u> if its Killing form is negative definite.

Assume now that $\mathfrak{g}$ is a compact semisimple Lie algebra, and let $\mathfrak{a} \subset \mathfrak{g}$ be an ideal. Let $\mathfrak{a}^\perp$ be the orthogonal complement of $\mathfrak{a}$ with respect to the Killing form. For any $X \in \mathfrak{g}$, $Y \in \mathfrak{a}^\perp$, and $Z \in \mathfrak{a}$ we have

$$B\left([X,Y], Z\right) = -B\left(Y, [X,Z]\right) = 0. \tag{2.3}$$

Hence, $[X,Y] \in \mathfrak{a}^\perp$. Therefore, $\mathfrak{a}^\perp$ is also an ideal. Note next that $[\mathfrak{a}, \mathfrak{a}^\perp] \subset \mathfrak{a} \cap \mathfrak{a}^\perp$. The restriction of B to the ideal $\mathfrak{a} \cap \mathfrak{a}^\perp$ is obviously zero. But B is negative definite; hence, $\mathfrak{a} \cap \mathfrak{a}^\perp = 0$. As a result, $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^\perp$ is a direct sum of ideals. We can repeat this procedure for $\mathfrak{a}$ and $\mathfrak{a}^\perp$, and after a finite number of steps finally we get:

Fact 2.3. *A real compact semisimple Lie algebra is a direct sum of real compact simple Lie algebras.*

Let us next choose a basis $\{X_i\}_{i=1}^{\dim\mathfrak{g}}$ in $\mathfrak{g}$ that satisfies $B(X_i, X_j) = -\delta_{ij}$. On this basis ad_X is an antisymmetric trace zero real matrix, hence an element of the special orthogonal Lie algebra $\mathfrak{so}(\dim\mathfrak{g})$. Finally, we remark that the subalgebra of a simple or a semisimple Lie algebra need not to be simple/semisimple.

2.2. Compact Semisimple Lie Groups

A Lie group G is a group that has a structure of a differential manifold, and the group operations are smooth. We say that G is compact if it is a compact manifold, i.e. any open covering of G has a finite subcovering. It is well known that a closed subgroup of a Lie group is a Lie group [13,38]. In this section we will always consider closed subgroups. An important class of subgroups are normal subgroups. $H \subset G$ is a normal subgroup if for each $g \in G$ we have $gHg^{-1} \subset H$. We denote it by $H \triangleleft G$. In this case the quotient G/H is a group. A disconnected G consists of connected components. Connected components of a Lie group are open, and their number is finite if G is compact, as otherwise they would constitute an open covering of G that does not possess finite subcovering. The identity component G_e, i.e. the component that contains the neutral element e, is a normal subgroup of G. This can be easily seen as the maps $\phi_g : G \to G$, $\phi_g(h) = ghg^{-1}$ are continuous for every $g \in G$; hence, they map components into components. But $e \in \phi_g(G_e)$ for all $g \in G$; hence, $\phi_g(G_e) = G_e$. The quotient G/G_e is a group (because G_e is normal) which for a compact G is a finite group called the *components group*.

The connection between Lie groups and Lie algebras is established in the following way. Left invariant vector fields on G together with vector fields

---

[1] Upon a choice of basis in $\mathfrak{g}$ endomorphisms ad_X and ad_Y are matrices and hence we can compute the trace.

commutators form the Lie algebra $\mathfrak{g}$ of a Lie group G. Note that these fields are determined by their value at e and therefore $\mathfrak{g}$ can be identified with the tangent space to G at e, i.e. $\mathfrak{g} = T_eG$. For every $X \in \mathfrak{g}$ there is a unique one-parameter subgroup $\gamma(t)$ whose tangent vector at e is X. We define the exponential map $\exp : \mathfrak{g} \to G$ to be: $\exp(X) := \gamma(1)$. For any Lie group the image of the exponential map, $\exp(\mathfrak{g})$, is contained in the identity component G_e and when G is compact $\exp(\mathfrak{g}) = G_e$. Therefore, for a compact and connected group every element $g \in G$ is of the form $\exp(X)$ for some $X \in \mathfrak{g}$. For matrix Lie groups $G \subset \mathrm{GL}(n, \mathbb{C})$ these definitions simplify as the exponential map is the matrix exponential that is defined by $e^X = \sum_{i=0}^{\infty} \frac{X^n}{n!}$ and the Lie algebra is defined as $\mathfrak{g} = \{X : e^{tX} \in G, \ \forall t \in \mathbb{R}\}$.

Definition 2.4. A compact connected Lie group is simple/semisimple if its Lie algebra is a compact simple/a compact semisimple Lie algebra.

Recall that the Lie algebra $\mathfrak{h}$ of the identity component of $H \lhd G$ is an ideal of the Lie algebra $\mathfrak{g}$. We can also use an equivalent definition that says a compact connected group G is simple if it has no connected normal subgroups. Similarly, as for Lie algebras, compact semisimple Lie groups have a particularly nice structure.

Fact 2.5. *Let G be a compact connected semisimple group. Then*

$$G = (G_1 \times \cdots \times G_k) / Z,$$

where each G_i is a simple compact group and Z is contained in the centre of $G_1 \times \cdots \times G_k$.

A representation of a Lie group on a real vector space is a homomorphism $\Phi : G \to \mathrm{GL}_{\mathbb{R}}(V)$, i.e. Φ satisfies $\Phi(g_1g_2) = \Phi(g_1)\Phi(g_2)$. A particularly important example is the adjoint representation of G on $\mathfrak{g}$.

$$\mathrm{Ad} : G \to \mathrm{Aut}(\mathfrak{g}), \quad \mathrm{Ad}_g(X) := gXg^{-1}. \tag{2.4}$$

The image of Ad_G is $\mathrm{Ad}_G = G/Z(G)$, where $Z(G)$ is the centre of G. For a semisimple compact Lie group $Z(G)$ is finite by definition and therefore Ad is a finite covering homomorphism onto $G/Z(G)$. For a compact connected simple Lie groups the adjoint representation is irreducible.

The relation between the adjoint representations of a compact connected semisimple Lie group and its Lie algebra, Ad and ad, follows from the fact that Ad is a smooth homomorphism. For any $X \in \mathfrak{g}$ and all $t \in \mathbb{R}$ elements $\mathrm{Ad}_{e^{tX}}$ form a one-parameter subgroup in $\mathrm{Aut}(\mathfrak{g})$ whose tangent vector at $t = 0$ is ad_X. As this group is uniquely determined by its tangent vector we have $\mathrm{Ad}_{e^{tX}} = e^{\mathrm{ad}_{tX}}$. Using this relation we easily see that the Killing form on $\mathfrak{g}$ is invariant with respect to the adjoint action, i.e. $B(\mathrm{Ad}_gX, \mathrm{Ad}_gY) = B(X, Y)$. Recall that for a compact semisimple G the Killing form is an inner product (negative definite) and therefore Ad_g is an orthogonal matrix belonging to $SO(\mathfrak{g})$. After the choice of an orthonormal basis in $\mathfrak{g}$, using (2.4) we can calculate entries of the matrix Ad_g. It is easy to see that this matrix belongs to $SO(\dim \mathfrak{g})$.

2.3. Subgroups of a Compact Semisimple Lie Group

Let G be a Lie group. We say that $H \subset G$ is a discrete subgroup of G if there is an open cover of H such that every open set in this cover contains exactly one element from H—we will call it a *discrete open cover* of H. If G is compact every discrete subgroup is finite. To see this, assume that there is an infinite discrete subgroup H in a compact G and take the open cover of G that is a union of the discrete open cover of H and the open set which consists of elements not in this discrete cover. Then this cover is infinite and has no finite subcover; hence, we get contradiction. By the similar argument any closed disconnected subgroup H of a compact G has finitely many connected components. The Lie algebra $\mathfrak{h}$ of the identity component H_e is a subalgebra of $\mathfrak{g}$, and the exponential map is surjective onto H_e; however, $\mathfrak{h}$ needs not to be semisimple. We distinguish three possible types of closed subgroups of the compact Lie group G: (1) finite discreet subgroups, (2) disconnected subgroups with a finite number of connected components and (3) connected subgroups.

In this paper we consider groups that are generated by a finite number of elements from some compact semisimple Lie group G. More precisely for $\mathcal{S} = \{g_1, \ldots, g_k\} \subset G$ we consider the closure of

$$< \mathcal{S} > := \left\{ g_{i_1}^{k_1} \ldots g_{i_m}^{k_m} : g_{i_j} \in \mathcal{S}, k_j \in \mathbb{N}, i_j \in \{1, \ldots, n\} \right\},$$

which is a Lie subgroup of G (see Fact 2.6 for the proof). In particular, we want to know when $\overline{< \mathcal{S} >} = G$. It is known that almost any two elements of G generate a compact semisimple G. Moreover, as shown by Kuranishi [27] elements that are in a sufficiently small neighbourhood of e generate G if and only if their corresponding Lie algebra elements generate $\mathfrak{g}$. The proof is, however, not constructive. The author of [21] shows that pairs generating G form a Zariski open subset of $G \times G$. In our work we adopt and develop some of the ideas contained in [21] and [27] and this way obtain characterisation of sets $\mathcal{S}$ that generate groups $SU(d)$ or $SO(d)$. Moreover, our approach results in a simple algorithm that enables deciding the universality of any given set of gates. For the completeness we prove the following.

Fact 2.6. *The closure of $<\mathcal{S}>$ is a Lie group.*

Proof. By the theorem of Cartan [13,38] we know that a closed subgroup of a Lie group is a Lie group. The set $\overline{<S>}$ is obviously closed, and hence we are left with showing that it is has a group structure. By the construction $\mathcal{S}$ is invariant under multiplication and therefore $\overline{< \mathcal{S} >}$ has this property too. As a direct implication of Dirichlet approximation theorem (see Theorem 5.2), for every element $g \in \mathcal{S}$ there is a sequence $\{g^{n_k}\}$, such that $g^{n_k} \to I$ when $k \to \infty$. Thus, $I \in \overline{< \mathcal{S} >}$. Note, however, that by the same argument the sequence $\{g^{n_k - 1}\} \subset \mathcal{S}$ converges to g^{-1}. Thus, $\overline{< \mathcal{S} >}$ has a group structure. The result follows. $\qquad \square$

In order to clarify the terminology, whenever we say the group generated by $\mathcal{S}$ we mean the compact Lie group $\overline{< \mathcal{S} >}$.

3. Generating Sets for Compact Semisimple Lie Algebras and Lie Groups

We begin with some remarks concerning irreducible representations on real vector spaces that we will call irreducible real representations. The well-known version of the Schur lemma states that a representation of a Lie group or a Lie algebra on a complex vector space (complex representation) is irreducible iff the only matrices that commute with all representation matrices are $\{\lambda I : \lambda \in \mathbb{C}\}$. In our paper the considered representations are irreducible real representations. A real irreducible representation can be of (1) real type, (2) complex type or (3) quaternion type. The type of representation determines the structure of endomorphisms commuting with the representation matrices (see chapter II.6 of [10] for full discussion). The following theorem holds (theorem II.6.7 of [10])

Fact 3.1 (Schur Lemma). *For a real irreducible representation, the algebra of endomorphisms commuting with the representation matrices is isomorphic to:* (1) $\mathbb{R}$ *when the representation is of the real type,* (2) $\mathbb{C}$ *when the representation is of the complex type,* (3) $\mathbb{H}$ *when the representation is of the quaternion type;* $\mathbb{H}$ *stands for Hamilton quaternions.*

Next we show that the adjoint representation for a compact simple Lie group/algebra is of the real type. Using Table II.6.2 and Propositions II.6.3 of [10] it suffices to show that its complexification is of the real type. On the other hand, by Proposition II.6.4 it reduces to showing that the complexfication $\mathfrak{g}^{\mathbb{C}}$ of a compact simple Lie algebra $\mathfrak{g}$ possesses a symmetric, non-degenerate and Ad_G-invariant form. To this end we define the Killing form on $\mathfrak{g}^{\mathbb{C}}$ in the analogues way as in $\mathfrak{g}$, i.e. $B_{\mathfrak{g}^{\mathbb{C}}}(X_1, X_2) = \mathrm{tr}(\mathrm{ad}_X \circ \mathrm{ad}_Y)$, $X, Y \in \mathfrak{g}^{\mathbb{C}}$. Note that a basis of $\mathfrak{g}$ over $\mathbb{R}$ is a basis of $\mathfrak{g}^{\mathbb{C}}$ over $\mathbb{C}$. Thus, $B_{\mathfrak{g}^{\mathbb{C}}}$ is a non-degenerate symmetric Ad_G-invariant form as the Killing form for $\mathfrak{g}$ is such. Hence,

$$\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \{\lambda I : \lambda \in \mathbb{R}\} = \mathcal{C}(\mathrm{Ad}_G).$$

3.1. Generating Sets for Compact Semisimple Lie Algebras

In this section $\mathfrak{g}$ will denote a compact semisimple Lie algebra. Let $\mathcal{X} = \{X_1, \ldots, X_n\} \subset \mathfrak{g}$. We say that $\mathcal{X}$ generates $\mathfrak{g}$ if any element of $\mathfrak{g}$ can be written as a finite linear combination of X_i's and finitely nested commutators of X_i's:

$$\sum_i \alpha_i X_i + \sum_{i,j} \alpha_{i,j}[X_i, X_j] + \cdots.$$

Our aim is to provide a general criterion that uses the adjoint representation of compact semisimple Lie algebras to verify when $\mathcal{X} \subset \mathfrak{g}$ generates $\mathfrak{g}$. This problem has been studied over the years, and there are many other approaches that do not use the adjoint representation. It is also an important question in control theory as it plays a central role in controllability of certain dynamical systems [1,11,26]. The corresponding conditions are known as the so-called *Lie algebra rank condition* [11,26]. The more recent conditions that are in the spirit of what we will present in Lemma 3.2 include [39,40] and in particular

[41] where the problem for compact Lie algebras is studied. As we will see in the next section conditions for generation of Lie algebras are too weak when one considers generation of Lie groups. Thus, this section plays a marginal role for the rest of the paper (excluding Theorem 4.6). The main purpose of this section is to give evidence that the adjoint representation can be useful in deciding both Lie algebras and Lie groups generation problem.

Let $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall X \in \mathfrak{g} \; [\mathrm{ad}_X, L] = 0\}$ denote the space of endomorphisms of $\mathfrak{g}$ that commute with all ad_X, $X \in \mathfrak{g}$. By the Jacobi identity $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}})$ is a Lie subalgebra of $\mathrm{End}(\mathfrak{g})$. Moreover, also by Jacobi identity, if $L \in \mathrm{End}(\mathfrak{g})$ commutes with ad_X and ad_Y then it also commutes with $\mathrm{ad}_{\alpha X + \beta Y}$ and $\mathrm{ad}_{[X,Y]}$. Let us denote by $\mathcal{C}(\mathrm{ad}_{\mathcal{X}})$ the solution set of

$$[\mathrm{ad}_{X_1}, \cdot] = 0, \dots, [\mathrm{ad}_{X_n}, \cdot] = 0.$$

It is clear that if $\mathcal{X}$ generates $\mathfrak{g}$, then $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$. It happens that the converse is true for semisimple Lie algebras. Let next $\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_k$ be a decomposition of a semisimple $\mathfrak{g}$ into simple ideals. Let $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$. Every $X_i \in \mathcal{X}$ has a unique decomposition:

$$X_i = X_{i,1} + \cdots + X_{i,k}, \quad \text{where } X_{i,j} \in \mathfrak{g}_j.$$

Therefore, $\mathcal{X}$ generates $\mathfrak{g}$ if every set $\mathcal{X}_i = \{X_{1,i}, \dots, X_{n,i}\}$ generates $\mathfrak{g}_i$, $i \in \{1, \dots, k\}$. Note that if the projection of $\mathcal{X}$ onto some simple component of $\mathfrak{g}$ is zero then $\mathcal{X}$ cannot generate and $\mathfrak{g}$ and $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) \neq \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$. Thus, the equality $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$ implies that $\mathcal{X}$ has nonzero intersection with every simple component of $\mathfrak{g}$.

Lemma 3.2. *Let $\mathfrak{g}$ be a compact semisimple Lie algebra and $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$ its finite subset. $\mathcal{X}$ generates $\mathfrak{g}$* **if and only if** *$\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$.*

Proof. Let n be the number of components of $\mathfrak{g}$, and let us denote by $\mathfrak{h} \subset \mathfrak{g}$ the Lie algebra generated by $\mathcal{X}$. Assume that $\mathfrak{h} \neq \mathfrak{g}$, but $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$. The equality of commutants implies that $\mathfrak{h}$ has nonzero intersection with every simple component of $\mathfrak{g}$. Using the Killing form we can decompose $\mathfrak{g}$ into a direct product of vector spaces (not necessarily Lie algebras), $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^{\perp}$. For any $X \in \mathfrak{h}$, $Y \in \mathfrak{h}$ and $Z \in \mathfrak{h}^{\perp}$ we have $\mathrm{ad}_X Y \in \mathfrak{h}$ and $\mathrm{ad}_X Z \in \mathrm{h}^{\perp}$. The latter is true as $B(\mathrm{ad}_X Z, Y) = -B(Z, \mathrm{ad}_X Y) = 0$, for any $Y \in \mathfrak{h}$. Therefore, for $X \in \mathfrak{h}$ operators ad_X respect the decomposition $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^{\perp}$ and have a block diagonal structure:

$$\mathrm{ad}_X = \begin{pmatrix} \mathrm{ad}_X\big|_{\mathfrak{h}} & 0 \\ 0 & \mathrm{ad}_X\big|_{\mathfrak{h}^{\perp}} \end{pmatrix}. \tag{3.1}$$

Let $P : \mathfrak{g} \to \mathfrak{h}$ be the orthogonal, with respect to the Killing form, projection operator onto $\mathfrak{h}$. Then obviously $[P, \mathrm{ad}_X] = 0$ for any $X \in \mathfrak{h}$. Note, however, that if P belonged to $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}})$ then $\mathfrak{h}$ would be an ideal of $\mathfrak{g}$. But the only ideals of $\mathfrak{g}$ are direct sums of its simple components. Thus, $\mathfrak{h}$ is either $\mathfrak{g}$ which is a contradiction or $\mathfrak{h}$ is a direct sum of $k < n$ simple components of $\mathfrak{g}$ which is again a contradiction. $\qquad\square$

Using the Schur lemma we obtain:

Corollary 3.3. *Let $\mathfrak{g}$ be a compact simple Lie algebra and $\mathcal{X} = \{X_1, \ldots, X_n\} \subset \mathfrak{g}$ be its finite subset. $\mathcal{X}$ generates $\mathfrak{g}$ if and only if $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \{\lambda I : \lambda \in \mathbb{R}\}$.*

Finally, let us remark that it is very important to consider not a defining but the adjoint representation. To see this let X_1, X_2 be two matrices that generate $\mathfrak{su}(2)$ and consider the set $\mathcal{X} = \{X_1 \otimes I, X_2 \otimes I, I \otimes X_1, I \otimes X_2\} \subset \mathfrak{su}(4)$. Note that the Lie algebra generated by $\mathcal{X}$ is $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \subset \mathfrak{su}(4)$. One checks by direct calculations that the only 4×4 matrix commuting with $\mathcal{X}$ is proportional to the identity. This is, however, not the case for matrices ad_X, $X \in \mathcal{X}$. Hence, changing the adjoint representation in Corollary 3.3 into the defining one would obtain the equality between $\mathfrak{su}(2) \oplus \mathfrak{su}(2)$ and $\mathfrak{su}(4)$ which is of course not true.

3.2. Generating Sets for Compact Semisimple Lie Groups

We are interested in the following problem. Let G be a compact connected semisimple Lie group, and let $\mathcal{S} = \{g_1, \ldots, g_n\} \subset G$. We want to know when $\overline{< \mathcal{S} >} = G$. To this end we use adjoint representation.

Let $\mathcal{C}(\mathrm{Ad}_G) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall g \in G \ [\mathrm{Ad}_g, L] = 0\}$ denote the space of endomorphisms of $\mathfrak{g}$ that commute with all Ad_g, $g \in G$. By the Jacobi identity $\mathcal{C}(\mathrm{Ad}_G)$ is a Lie subalgebra of $\mathrm{End}(\mathfrak{g})$. Moreover, if $L \in \mathrm{End}(\mathfrak{g})$ commutes with Ad_g and Ad_h then it also commutes with Ad_{gh}. Let us denote by $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$ the solution set of

$$[\mathrm{Ad}_{g_1}, \cdot] = 0, \ldots, [\mathrm{Ad}_{g_n}, \cdot] = 0.$$

It is clear that if $\mathcal{S}$ generates G then $\mathcal{C}(\mathrm{Ad}_G) = \mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$. It happens that with some additional assumptions the converse is true for semisimple Lie groups.

Lemma 3.4. *Let G be a compact connected semisimple Lie group and $\mathcal{S} = \{g_1, \ldots, g_n\} \subset G$ its finite subset such that $<\mathcal{S}>$ is infinite and the projection of $<\mathcal{S}>$ onto every simple component of G is also infinite. $\mathcal{S}$ generates G if and only if $\mathcal{C}(\mathrm{Ad}_G) = \mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$.*

Proof. Let us denote by H the closure of the group generated by $\mathcal{S}$, i.e. $H = \overline{< \mathcal{S} >}$. H is a compact Lie group that contains infinite number of elements. Let H_e be the identity component of H. As we know H_e is a normal subgroup of H. Let $\mathfrak{h} \subset \mathfrak{g}$ be the Lie algebra of H_e, and let n be the number of simple components of $\mathfrak{g} = Lie(G)$. Under our assumption $\mathfrak{h}$ has nonzero intersection with every simple component of $\mathfrak{g}$. Assume that $\mathfrak{h} \neq \mathfrak{g}$, but $\mathcal{C}(\mathrm{Ad}_G) = \mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$. Using the Killing form we can decompose $\mathfrak{g}$ into a direct product of vector spaces (not necessarily Lie algebras), $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^{\perp}$. For any $g \in H$, $X \in \mathfrak{h}$ and $Y \in \mathfrak{h}^{\perp}$ we have $\mathrm{Ad}_g Y \in \mathfrak{h}$ and $\mathrm{Ad}_g Y \in \mathrm{h}^{\perp}$. The latter is true as $B(\mathrm{Ad}_g Y, X) = B(Y, \mathrm{Ad}_{g^{-1}} X) = 0$, for any $X \in \mathfrak{h}$. Therefore, for $h \in H$ the operators Ad_h respect the decomposition $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^{\perp}$ and have a block diagonal structure:

$$\mathrm{Ad}_h = \begin{pmatrix} \mathrm{Ad}_h\big|_{\mathfrak{h}} & 0 \\ 0 & \mathrm{Ad}_h\big|_{\mathfrak{h}^{\perp}} \end{pmatrix}. \tag{3.2}$$

Let $P : \mathfrak{g} \to \mathfrak{h}$ be the orthogonal projection with respect to the Killing form onto $\mathfrak{h}$. Then obviously $[P, \mathrm{Ad}_h] = 0$ for any $h \in H$. Note, however, that if

P belonged to $\mathcal{C}(\mathrm{Ad}_G)$ then $\mathfrak{h}$ would be Ad_G-invariant subspace of $\mathfrak{g}$. But the only Ad-invariant subspaces of $\mathfrak{g}$ are simple components of $\mathfrak{g}$. Hence, either $\mathfrak{h} = \mathfrak{g}$ which is a contradiction or $\mathfrak{h}$ is a direct sum of $k < n$ simple components of $\mathfrak{g}$ which again is a contradiction as $\mathfrak{h}$ has nonzero intersection with all n simple components. $\qquad\square$

Using the Schur lemma we obtain:

Corollary 3.5. *Let G be a compact connected simple Lie group and $\mathcal{S} = \{g_1, \ldots, g_n\}$ its finite subset. Assume $<\mathcal{S}>$ is infinite. The set $\mathcal{S}$ generates G if and only if $\mathcal{C}(\mathrm{Ad}_G) = \{\lambda I : \lambda \in \mathbb{R}\}$.*

Finally, note that $\overline{<\mathcal{S}>}$ is infinite in particular when at least one of g_i's is of infinite order. Hence,

Corollary 3.6. *Let G be a compact connected simple Lie group and $\mathcal{S} = \{g_1, \ldots, g_n\} \subset G$ its finite subset such that at least one of g_i's is of infinite order. $\mathcal{S}$ generates G if and only if $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}}) = \{\lambda I : \lambda \in \mathbb{R}\}$.*

In the next section we characterise when $<\mathcal{S}>$ is infinite and when $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$ can be different from $\mathcal{C}(\mathrm{ad}_{\mathcal{X}})$ for semisimple groups of our interest, i.e. for $G = SU(d)$ and $G = SO(d)$.

4. Groups $SU(d)$ and $SO(d)$

In this section we focus on two groups G that are particularly important from the perspective of quantum computation and linear quantum optics, i.e. $G = SO(d)$ or $G = SU(d)$.

$$SO(d) = \{O \in \mathrm{Gl}_d(\mathbb{R}) : O^t O = I, \det O = 1\}, \tag{4.1}$$

$$SU(d) = \{U \in \mathrm{Gl}_d(\mathbb{C}) : U^\dagger U = I, \det X = 1\}. \tag{4.2}$$

Their Lie algebras $\mathfrak{g}$ are:

$$\mathfrak{so}(d) = \{X \in \mathrm{Mat}_d(\mathbb{R}) : X^t = -X, \mathrm{tr}X = 0\}, \tag{4.3}$$

$$\mathfrak{su}(d) = \{X \in \mathrm{Mat}_d(\mathbb{C}) : X^\dagger = -X, \mathrm{tr}X = 0\}. \tag{4.4}$$

The centres of G are finite and given by $Z(SU(d)) = \{\alpha I : \alpha \in \mathbb{C}, \alpha^d = 1\}$, $Z(SO(2d)) = \{\pm I\}$ and $Z(SO(2d+1)) = I$. Groups $SU(d)$ for $d \geq 2$ and groups $SO(d)$ for $d \geq 3$ and $d \neq 4$ are compact connected simple Lie groups. On the other hand, $SO(4)$ is still compact and connected, but it is not simple as its Lie algebra is a direct sum of Lie algebras $\mathfrak{so}(4) = \mathfrak{so}(3) \oplus \mathfrak{so}(3)$; hence, $SO(4)$ is semisimple. The Killing form on both $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$, up to a constant positive factor, is given by $B(X, Y) = \mathrm{tr}XY$. We next introduce an orthonormal basis in $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$. Let $E_{kl} = |k\rangle\langle l|$ be a $d \times d$ matrix whose only nonzero (and equal to 1) entry is (k, l). The commutation relations are $[E_{ij}, E_{kl}] = \delta_{jk}E_{il} - \delta_{li}E_{k,j}$. Let

$$X_{ij} = E_{ij} - E_{ji}, \; Y_{ij} = i(E_{ij} + E_{ji}), \; Z_{ij} = i(E_{ii} - E_{jj}). \tag{4.5}$$

One easily checks that for $i, j \in \{1, \ldots, d\}$, $i < j$ matrices $\{X_{ij}, Y_{ij}, Z_{i,i+1}\}$ form an orthogonal basis of $\mathfrak{su}(d)$ and matrices $\{X_{ij}\}$ of $\mathfrak{so}(d)$. We will call these two bases the standard bases of $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$, respectively.

4.1. Gates and Their Lie Algebra Elements

In this section we explain how to any set of gates $\mathcal{S}$ we assign the set of Lie algebra elements $\mathcal{X}$.

Let us recall that for a unitary matrix $U \in SU(d)$ there is a unitary matrix $V \in SU(d)$ such that $D = V^\dagger U V = \mathrm{diag}\{e^{i\phi_1}, \ldots, e^{i\phi_d}\}$. The nonzero entries of D constitute the spectrum of U. In order to find $X \in \mathfrak{su}(d)$ such that $U = e^X$ one should calculate a logarithm of U. This can be done using the decomposition $U = V D V^\dagger$, and it boils down to calculating logarithms of diagonal matrix D. Since the logarithm of $z \in \mathbb{C}$ is not uniquely defined we will use the convention that $\log z = \arg(z)$, where $\arg(z)$ is the argument of z, and we assume $\arg(z) \in [0, 2\pi)$. Thus, we choose $X \in \mathfrak{su}(d)$ that satisfies $U = e^X$ as $X = V \tilde{D} V^\dagger$, where $\tilde{D} = \mathrm{diag}\{i\phi_1, \ldots, i\phi_d\}$, every $\phi_i \in [0, 2\pi)$. This way to any set of gates $\mathcal{S} = \{U_1, \ldots, U_n\} \subset SU(d)$ we assign the set of Lie algebra elements $\mathcal{X} = \{X_1, \ldots, X_n\} \subset \mathfrak{su}(d)$.

Matrices in $SO(d)$ typically cannot be diagonalised by the orthogonal group. Nevertheless, for a matrix $O \in SO(d)$ there is an orthogonal matrix V such that $R = V^t O V$ is block diagonal with two types of blocks: (1) one identity matrix I_k of dimension $0 \le k \le d$ and (2) 2×2 rotations by angles $\phi_i \in (0, 2\pi)$, i.e. matrices $O(\phi_i)$ from $SO(2)$. We again want to find $X \in \mathfrak{so}(d)$ such that $O = e^X$. In our paper we choose $X = V \tilde{R} V^t$, where $\tilde{R}$ has the same block diagonal structure as R and (1) the block of $\tilde{R}$ corresponding to the identity block of R is the zero matrix 0_k of dimension $0 \le k \le d$, (2) the blocks corresponding to 2×2 ϕ_i-rotation blocks of R are matrices $\begin{pmatrix} 0 & \phi_i \\ -\phi_i & 0 \end{pmatrix} \in \mathfrak{so}(2)$, where every $\phi_i \in (0, 2\pi)$. We will call R and $\tilde{R}$ normal forms of $O \in SO(d)$ and $X \in \mathfrak{so}(d)$, respectively, and angles ϕ_i's the spectral angles. Summing up, using the above procedure, to any set of gates $\mathcal{S} = \{O_1, \ldots, O_n\} \subset SO(d)$ we assign the set of Lie algebra elements $\mathcal{X} = \{X_1, \ldots, X_n\} \subset \mathfrak{so}(d)$.

Throughout the paper, whenever we speak about the Lie algebra elements associated with gates (or the logarithms of the gates) we mean matrices constructed according to the above two procedures.

4.2. The Difference Between $\mathcal{C}(\mathrm{Ad}_\mathcal{S})$ and $\mathcal{C}(\mathrm{ad}_\mathcal{X})$

4.2.1. The Case of $SU(d)$. Let $\mathcal{S} = \{U_1, \ldots, U_n\} \subset SU(d)$, and let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be the corresponding set of Lie algebra elements (constructed as described in Sect. 4.1). In this section we study when the spaces $\mathcal{C}(\mathrm{Ad}_\mathcal{S})$ and $\mathcal{C}(\mathrm{ad}_\mathcal{X})$ are different. Note first that using $\mathrm{Ad}_{e^{X_i}} = e^{\mathrm{ad}_{X_i}}$ we have $\mathcal{C}(\mathrm{ad}_\mathcal{X}) \subseteq \mathcal{C}(\mathrm{Ad}_\mathcal{S})$. Hence, we are particularly interested in the situation when $\mathcal{C}(\mathrm{Ad}_\mathcal{S})$ is strictly larger then $\mathcal{C}(\mathrm{ad}_\mathcal{X})$. Matrices U_i can be put into diagonal form $U_i = V_i D_i V_i^\dagger$, where $V_i \in SU(d)$ and $D_i = \{e^{\phi_1^i}, \ldots, e^{\phi_d^i}\}$, $\phi_j^i \in [0, 2\pi)$. Note now that $\mathrm{Ad}_{U_i} = \mathrm{Ad}_{V_i D_i V_i^\dagger} = O_i \mathrm{Ad}_{D_i} O_i^t$, where $O = \mathrm{Ad}_{V_i} \in SO(d^2 - 1)$. Let us order the standard basis of $\mathfrak{su}(d)$ as follows

$\{X_{12}, Y_{12}, \ldots, X_{d-1,d}, Y_{d-1,d}, Z_{1,2}, \ldots Z_{d-1,d}\}$. The matrix Ad_{D_i} in this basis has a block diagonal form:

$$\mathrm{Ad}_{D_i} = \begin{pmatrix} O(\phi_{1,2}^i) & & & & & & \\ & \ddots & & & & & \\ & & O(\phi_{1,d}^i) & & & & \\ & & & \ddots & & & \\ & & & & O(\phi_{2,d}^i) & & \\ & & & & & \ddots & \\ & & & & & & O(\phi_{d-1,d}^i) \\ & & & & & & & I_{d-1} \end{pmatrix}, \qquad (4.6)$$

where

$$O\left(\phi_{k,l}^i\right) = \begin{pmatrix} \cos\left(\phi_{k,l}^i\right) & \sin\left(\phi_{k,l}^i\right) \\ -\sin\left(\phi_{k,l}^i\right) & \cos\left(\phi_{k,l}^i\right) \end{pmatrix}, \qquad \text{where, } \phi_{k,l}^i := \phi_k^i - \phi_l^i, \quad (4.7)$$

and I_{d-1} is $(d-1)\times(d-1)$ identity matrix. Matrices from $\mathcal{X}$ are given by $X_i = V_i \tilde{D}_i V_i^\dagger$ and $\tilde{D}_i = i\left\{\phi_1^i, \phi_2^i, \ldots, \phi_d^i\right\}$. Hence, $\mathrm{ad}_{X_i} = \mathrm{ad}_{V_i \tilde{D}_i V_i^\dagger} = O \mathrm{ad}_{\tilde{D}_i} O^t$, and we have (in the standard basis of $\mathfrak{su}(d)$ ordered as previously):

$$\mathrm{ad}_{\tilde{D}_i} = \begin{pmatrix} X(\phi_{1,2}^i) & & & & & & \\ & \ddots & & & & & \\ & & X(\phi_{1,d}^i) & & & & \\ & & & \ddots & & & \\ & & & & X(\phi_{2,d}^i) & & \\ & & & & & \ddots & \\ & & & & & & X(\phi_{d-1,d}^i) \\ & & & & & & & 0_{d-1} \end{pmatrix}, \qquad (4.8)$$

where

$$X\left(\phi_{k,l}^i\right) = \begin{pmatrix} 0 & \phi_{k,l}^i \\ -\phi_{k,l}^i & 0 \end{pmatrix}, \text{ where, } \phi_{k,l}^i = \phi_k^i - \phi_l^i, \qquad (4.9)$$

and 0_{d-1} is $(d-1)\times(d-1)$ zero matrix. Note that $\phi_{k,l}^i \in (-2\pi, 2\pi)$. Comparing structures of matrices Ad_{D_i} and $\mathrm{ad}_{\tilde{D}_i}$ we deduce that if all $\phi_{i,j}^i \neq \pm\pi$ then $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}}) = \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$. The situation is different when $\phi_{k,l}^i = \pm\pi$. In this case Ad_{D_i} has additional degeneracies compared to $\mathrm{ad}_{\tilde{D}_i}$ as $O(\phi_{k,l}^i) = O(\pm\pi) = -I_2$. Let P be the rotation plane corresponding to the angle $\phi_{k,l}^i = \pm\pi$. One can then construct a rotation $O' \in SO(d^2-1)$ whose elementary rotation planes are exactly as in $\mathrm{ad}_{\tilde{D}_i}$ except P which is replaced by a plane P', $P \perp P'$. This can be achieved using available $d-1$ directions corresponding to I_{d-1}. If the rotation angle along P' is also π then $[\mathrm{Ad}_{U_i}, O'] = 0$ and $[\mathrm{ad}_{X_i}, O'] \neq 0$. Hence, the space $\mathcal{C}(\mathrm{Ad}_{U_i})$ is larger than $\mathcal{C}(\mathrm{ad}_{X_i})$ and there is possibility that it might be true also for sets $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$ and $\mathcal{C}(\mathrm{ad}_{\mathcal{X}})$. As a conclusion we get

Fact 4.1. *Let $S = \{U_1, \ldots, U_n\} \subset SU(d)$ and $\mathcal{X} = \{X_1, \ldots, X_n\}$ be the corresponding set of Lie algebra elements (constructed as described in Sect. 4.1). The space $\mathcal{C}(\mathrm{Ad}_S)$ can be larger than $\mathcal{C}(\mathrm{ad}_\mathcal{X})$ if and only if the difference between spectral angles for at least one of the matrices $U_i \in \mathcal{S}$ is equal to $\pm\pi$.*

4.2.2. The Case of $SO(d)$. We consider $\mathcal{S} = \{O_1, \ldots, O_n\} \subset SO(d)$ and $\mathcal{X} = \{X_1, \ldots, X_n\}$ be the corresponding Lie algebra elements (constructed as described in Sect. 4.1). We have $\mathcal{C}(\mathrm{ad}_\mathcal{X}) \subseteq \mathcal{C}(\mathrm{Ad}_S)$, and our goal is to characterise the cases when the space $\mathcal{C}(\mathrm{Ad}_S)$ can be strictly larger than $\mathcal{C}(\mathrm{ad}_\mathcal{X})$. Matrices O_i can be put into a standard form $O_i = V_i R_i V_i^\dagger$, where $V_i \in SO(d)$ and R_i is a block diagonal matrix consisting of $k \leq \lfloor \frac{d}{2} \rfloor$ two-dimensional blocks representing rotations by angles $\{\phi_1^i, \ldots, \phi_k^i\}$, $\phi_j^i \in (0, 2\pi)$ and one $(d-2k)$-dimensional block that is the identity matrix. Note next that $\mathrm{Ad}_{O_i} = \mathrm{Ad}_{V_i R_i V_i^\dagger} = \mathrm{Ad}_{V_i} \mathrm{Ad}_{R_i} \mathrm{Ad}_{V_i}^t$. Each matrix Ad_{R_i} can be brought to the standard block diagonal form containing the following blocks

1. $O(\phi_{a,b}^i)$ and $O(\psi_{a,b}^i)$, where $\phi_{a,b}^i = \phi_a^i - \phi_b^i$, $\psi_{a,b}^i = \phi_a^i + \phi_b^i$, $a < b$. The number of these blocks is $k(k-1)$.
2. The identity block of dimension $k + \frac{(d-2k)(d-2k-1)}{2}$.
3. Blocks $O(\phi_j^i)$, where $j \in \{1, \ldots, k\}$. Each block $O(\phi_j^i)$ appears $(d-2k)$ times. Hence, we have $k(d-2k)$ blocks like this.

Matrices ad_{X_i} have the same structure as matrices Ad_{O_i} albeit the identity block is replaced by the 0-block of the same dimension, and the rotational blocks $O(\phi_{a,b}^i)$, $O(\psi_{a,b}^i)$ and $O(\phi_j^i)$ are replaced by $\begin{pmatrix} 0 & \phi_j^i \\ -\phi_j^i & 0 \end{pmatrix} \in \mathfrak{so}(2)$, where every $\phi_j^i \in (0, 2\pi)$. Repeating the reasoning for $SU(d)$ we get:

Fact 4.2. *Let $S = \{U_1, \ldots, U_n\} \subset SO(d)$ and $\mathcal{X} = \{X_1, \ldots, X_n\} \subset \mathfrak{so}(d)$ be the corresponding set of Lie algebra elements (constructed as described in Sect. 4.1). The space $\mathcal{C}(\mathrm{Ad}_S)$ can be bigger than $\mathcal{C}(\mathrm{ad}_\mathcal{X})$ if and only if the difference or the sum of spectral angles ϕ_a^i and ϕ_b^i for at least one of the matrices $O_i \in \mathcal{S}$ is an odd multiple of π.*

4.3. Pairs Generating Infinite Subgroups of G

In this section we show that elements that are close enough to $Z(G)$ generate G if the corresponding Lie algebra elements generate $\mathfrak{g}$ (see Theorem 4.6). We begin with recalling the elementary properties of the matrix exponential and the matrix logarithm. To this end we define the norm of $A \in \mathrm{Mat}_d(\mathbb{C})$ by $\|A\| = \sqrt{\mathrm{tr}(AA^\dagger)}$.

Next we recall that the group commutator of two invertible matrices (with respect to matrix multiplication) is defined as $[A, B]_\bullet = ABA^{-1}B^{-1}$. Naturally, if matrices commute in a usual sense then $[A, B]_\bullet = I$. The following lemma relates the distance between $[A, B]_\bullet$ and I to the distances of A and B from the identity.

Lemma 4.3. *Let $A, B \in G$ where $G = SU(d)$ or $G = SO(d)$, and let $C = [A, B]_\bullet$. We have the following:*

$$\|C - I\| \leq \sqrt{2}\|A - I\|\|B - I\|, \tag{4.10}$$

$$\text{If } [A, C]_\bullet = I \text{ and } \|B - I\| < 2, \text{ then } [A, B]_\bullet = I. \tag{4.11}$$

Proof. Can be found in Lemmas 36.15 and 36.16 of [15]. $\qquad \square$

We next define open balls in $G = SO(d)$ or $SU(d)$ centred around elements from $Z(G)$ and of radius $1/\sqrt{2}$, $B_\alpha = \{g \in G : \|g - \alpha I\| < 1/\sqrt{2}\}$. Let $\mathcal{B} = \bigcup_{\alpha I \in Z(G)} B_\alpha$.

Lemma 4.4. *Let $g, h \in B_1$, and assume $[g, h]_\bullet \neq I$. The group $<g, h>$ generated by g, h is infinite.*

Proof. Define the sequence $g_0 = g$, $g_1 = [g_0, h]_\bullet$, $g_n = [g_{n-1}, h]_\bullet$. By our assumptions $\|h - I\| = d \le 1/\sqrt{2}$. Therefore, using Lemma 4.3

$$\|g_n - I\| \le \sqrt{2}d\|g_{n-1} - I\|.$$

Thus, $\|g_n - I\| \le (\sqrt{2}d)^n\|g - I\|$ and $g_n \to I$, when $n \to \infty$. Assume that the sequence is finite, i.e. for some N we have $g_N = I$. That means $[g_{N-1}, h]_\bullet = I$. But $g_{N-1} = [g_{N-2}, h]_\bullet$ and clearly $\|g_k - I\| < 2$ and by Lemma 4.3, $[g_{N-2}, h]_\bullet = I$. Repeating this argument we get $[g, h]_\bullet = I$ which is a contradiction. Therefore, $<g, h>$ is infinite. $\qquad \square$

Corollary 4.5. *Let $g \in B_{\alpha_1}$ and $h \in B_{\alpha_2}$, where α_1 and α_2 are such that $\alpha_1 I, \alpha_2 I \in Z(G)$ and assume $[g, h]_\bullet \notin Z(G)$. Then the group $<g, h>$ is infinite.*

Proof. If $\alpha_1 = \alpha_2 = 1$ the result follows from Lemma 4.4. For all other α_i's let $g' = \alpha_1^{-1}g$ and $h' = \alpha_2^{-1}h$. Then $h', g' \in B_1$ and $[g', h']_\bullet \neq I$. Thus, by Lemma 4.4, $<g', h'>$ is infinite. Note that $<g, h>$ is up to the finite covering equal to $<g', h'>$ and therefore is infinite too. $\qquad \square$

We next provide explicit conditions for elements of G to belong to balls B_α. To this end let $\alpha_m I$ be the elements of $Z(G)$. We have the following

$$\|g - \alpha_m I\|^2 = \text{tr}(g - \alpha_m I)(g^* - \alpha_m^* I) = 2\text{tr}I - \alpha_m^*\text{tr}g - \alpha_m\text{tr}g^*. \tag{4.12}$$

For $SU(d)$ we have $\alpha_m^d = 1$ and hence $\alpha_m = \cos\theta_m + i\sin\theta_m$, where $\theta_m = \frac{2m\pi}{d}$ and $m \in \{1, \ldots, d\}$. Let $\{e^{i\phi_1}, e^{i\phi_2}, \ldots, e^{i\phi_d}\}$ be the spectrum of $U_d \in SU(d)$. The conditions for $U_d \in SU(d)$ to belong to the ball B_{α_m} read:

$$U_d \in B_{\alpha_m} \Leftrightarrow \sum_{i=1}^d \sin^2\frac{\phi_i - \theta_m}{2} < \frac{1}{8}, \quad \sum_{i=1}^d \phi_i = 0 \bmod 2\pi. \tag{4.13}$$

For $SO(2k + 1)$ the centre is trivial and we have only one ball B_1. Let $\{1, e^{i\phi_1}, e^{-i\phi_1}, \ldots, e^{i\phi_k}, e^{-i\phi_k}\}$ be the spectrum of $O_{2k+1} \in SO(2k + 1)$. We have

$$O_{2k+1} \in B_1 \Leftrightarrow \sum_{i=1}^k \sin^2\frac{\phi_i}{2} < \frac{1}{16}. \tag{4.14}$$

Finally, $Z(SO(2k)) = \{I, -I\}$ and we have two balls B_1, B_{-1}. Let

$$\{e^{i\phi_1}, e^{-i\phi_1}, \ldots, e^{i\phi_k}, e^{-i\phi_k}\},$$

be the spectrum of O_{2k}. The conditions for the spectral angles are as follows

$$O_{2k} \in B_1 \Leftrightarrow \sum_{i=1}^{k} \sin^2 \frac{\phi_i}{2} < \frac{1}{16}, \tag{4.15}$$

$$O_{2k} \in B_{-1} \Leftrightarrow \sum_{i=1}^{k} \sin^2 \frac{\phi_i - \pi}{2} < \frac{1}{16}. \tag{4.16}$$

Theorem 4.6. *Let $G = SO(d)$ or $G = SU(d)$. Let $\mathcal{S} = \{g_1, \ldots, g_n\} \subset G$ be such that $g_i \in B_\alpha$, where $\alpha I \in Z(G)$, and let $\mathcal{X} = \{X_1, \ldots, X_n\} \subset \mathfrak{g}$ be the Lie algebra elements assigned to $\mathcal{S}$ (constructed as described in Sect. 4.1). $\mathcal{S}$ generates G if and only if $\mathcal{X}$ generates $\mathfrak{g}$.*

Proof. By Lemma 3.4, matrices $\mathcal{S}$ generate G if they generate an infinite subgroup and $\mathcal{C}(\mathrm{Ad}_\mathcal{S}) = \mathcal{C}(\mathrm{Ad}_G)$. The cases when spaces $\mathcal{C}(\mathrm{Ad}_\mathcal{S})$ and $\mathcal{C}(\mathrm{ad}_\mathcal{X})$ can differ are characterised by Facts 4.1 and 4.2. Assume that $\mathcal{S} \subset SU(d)$. The spaces $\mathcal{C}(\mathrm{Ad}_\mathcal{S})$ and $\mathcal{C}(\mathrm{ad}_\mathcal{X})$ can differ if and only if for one of the matrices $g_i \in \mathcal{S}$ we have $\phi^i_{a,b} = k\pi$, where k is odd. But then $\phi^i_a = \phi^i_b \pm \pi$ and for some $\theta_m = \frac{2\pi m}{d}$

$$\sin^2 \frac{\phi^i_b \pm \pi - \theta_m}{2} + \sin^2 \frac{\phi^i_b - \theta_m}{2} = 1,$$

which means g_i does not satisfy (4.13). Assume next that $\mathcal{S} \subset SO(d)$. The spaces $\mathcal{C}(\mathrm{Ad}_\mathcal{S})$ and $\mathcal{C}(\mathrm{ad}_\mathcal{X})$ can differ iff the difference or the sum of spectral angles ϕ^i_a and ϕ^i_b is equal to an odd multiple of π. For odd d we arrive at

$$\sin^2 \frac{\pm\phi^i_b \pm \pi}{2} + \sin^2 \frac{\phi^i_b}{2} = 1,$$

and for even d we additionally have

$$\sin^2 \frac{\pm\phi^i_b \pm \pi - \pi}{2} + \sin^2 \frac{\phi^i_b - \pi}{2} = 1,$$

which means g_i does not satisfy (4.14), (4.15) or (4.16). $\qquad\square$

4.4. Universal Sets for G

In this section we consider situation when not all the matrices belonging to $\mathcal{S}$ are contained in $\mathcal{B}$. We already know that if there are two elements $g, h \in \overline{< S >} \cap \mathcal{B}$ such that $[g, h]_\bullet \notin Z(G)$ then the group $\overline{< S >}$ is infinite. It turns out that for $\mathcal{S}$ that satisfies the necessary universality condition, i.e. $\mathcal{C}(\mathrm{Ad}_{g_1}, \ldots, \mathrm{Ad}_{g_k}) = \{\lambda I\}$, this is actually an equivalence relation.

Lemma 4.7. *Let $\mathcal{S} = \{g_1, \ldots, g_k\} \subset G$ be such that $\mathcal{C}(\mathrm{Ad}_{g_1}, \ldots, \mathrm{Ad}_{g_k}) = \{\lambda I\}$. The group $\overline{< S >}$ is infinite **if and only if** there are at least two elements $g, h \in \overline{< S >} \cap \mathcal{B}$ satisfying $[g, h]_\bullet \notin Z(G)$.*

Proof. Assume $\overline{< S >}$ is infinite. Then under the assumption $\mathcal{C}(\mathrm{Ad}_\mathcal{S}) = \{\lambda I\}$ we have $\overline{< S >} = G$. Thus, balls B_α must contain elements of $<S>$ commuting to a non-central elements and the result follows. On the other hand, if there are at least two elements $g, h \in \overline{< S >}$ such that they belong to some balls

B_α, where $\alpha I \in Z(G)$, and $[g,h]_\bullet \notin Z(G)$ then by Corollary 4.5 $\overline{<S>}$ is infinite. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

We already know that the necessary universality condition places significant constraints on the structure of the infinite $\overline{<S>}$. It turns out that this is the case also when $\overline{<S>}$ is finite. The constrains regard the structure of $<S> \cap \mathcal{B}$.

Lemma 4.8. *Let $S = \{g_1,\ldots,g_k\} \subset G$ be such that $\mathcal{C}(\mathrm{Ad}_{g_1},\ldots,\mathrm{Ad}_{g_k}) = \{\lambda I\}$. Then either the intersection of $<S>$ with $\mathcal{B}$ is dense in $\mathcal{B}$ or is a subgroup of $Z(G)$. In the first case $\overline{<S>} = G$, and in the second one $\overline{<S>}$ is finite.*

Proof. The group $\overline{<S>}$ can be either infinite or finite. When it is infinite, then by the necessary universality condition, i.e. $\mathcal{C}(\mathrm{Ad}_{g_1},\ldots,\mathrm{Ad}_{g_k}) = \{\lambda I\}$, we have $\overline{<S>} = G$, and it is obvious that $\mathcal{B} \cap <S>$ is dense in $\mathcal{B}$. Assume next that $<S>$ is finite. By Corollary 4.5 the group commutators of elements from $\mathcal{B} \cap <S>$ belong to $Z(G)$. We first show that in fact they are equal to the identity, i.e. elements from $\mathcal{B} \cap <S>$ commute. To see this let $h_1 \in B_{\alpha_1}$ and $h_2 \in B_{\alpha_2}$. Assume $[h_1,h_2]_\bullet \in Z(G)$. One can always find $\tilde{h}_1, \tilde{h}_2 \in B_1$ such that $h_1 = \alpha_1 \tilde{h}_1$ and $h_2 = \alpha_2 \tilde{h}_2$. We have:

$$[h_1,h_2]_\bullet = [\alpha_1\tilde{h}_1, \alpha_2\tilde{h}_2]_\bullet = \alpha_1\tilde{h}_1\alpha_2\tilde{h}_2\alpha_1^{-1}\tilde{h}_1^{-1}\alpha_2^{-1}\tilde{h}_2 = [\tilde{h}_1,\tilde{h}_2]_\bullet. \qquad (4.17)$$

But by inequality (4.10) we have $[\tilde{h}_1,\tilde{h}_2]_\bullet \in B_1$, and it is also easy to see that B_{α_i}'s are disjoint. Thus, $[h_1,h_2]_\bullet = I$. Next we note that each $B_\alpha \cap <S>$ is invariant under the conjugation by elements from G. Let $\{h_1,\ldots,h_m\}$ be all elements from $B_\alpha \cap <S>$. Once again we can find elements $\{\tilde{h}_1,\ldots,\tilde{h}_m\} \subset B_1$ satisfying $h_i = \alpha\tilde{h}_i$. Let $\mathfrak{g} \ni X_i = \log\tilde{h}_i$ (constructed as described in Sect. 4.1). Thus, elements of $B_\alpha \cap <S>$ are of the form $\{\alpha e^{X_1},\ldots,\alpha e^{X_m}\}$. We also know that $B_\alpha \cap <S>$ is Ad_S-invariant, i.e.

$$g_i\alpha e^{X_j}g_i^{-1} = \alpha\mathrm{Ad}_{g_i}e^{X_j} = \alpha e^{X_r}, \quad g_i \in S, \qquad (4.18)$$

where $i \in \{1,\ldots,k\}$ and $j,r \in \{1,\ldots,m\}$. Thus, we have $\mathrm{Ad}_{g_i}e^{X_j} = e^{X_r}$. As the distance from the identity of the left and right sides is smaller than 1 we have $\log\mathrm{Ad}_{g_i}e^{X_j} = \log e^{X_r}$. By the construction, $\log e^{X_r} = X_r$ and from our definition of logarithm: $\log\mathrm{Ad}_{g_i}e^{X_j} = \mathrm{Ad}_{g_i}\log e^{X_j} = \mathrm{Ad}_{g_i}X_j$. Hence, $\mathrm{Ad}_{g_i}X_j = X_r$ and the subspace $\{X_1,\ldots,X_m\} \subset \mathfrak{g}$ is an invariant subspace for all matrices $\{\mathrm{Ad}_{g_1},\ldots\mathrm{Ad}_{g_k}\}$. By the condition $\mathcal{C}(\mathrm{Ad}_{g_1},\ldots,\mathrm{Ad}_{g_k}) = \{\lambda I\}$ this subspace must be either 0 or $\mathfrak{g}$. Assume it is $\mathfrak{g}$. Recall that we have:

$$[\alpha e^{X_j}, \alpha e^{X_j}] = 0, \ i,j \in \{1,\ldots,k\}.$$

Thus, there is U such that $\alpha e^{X_i} = \alpha e^{UD_iU^{-1}}$, where D_i is diagonal. Hence, $X_i = UD_iU^{-1}$. Thus, matrices $\{X_1,\ldots,X_m\}$ commute and we get a contradiction. Hence, $<S> \cap B_\alpha$ is either empty or αI. The result follows. $\qquad \square$

Lemma 4.8 leads to the following conclusion:

Corollary 4.9. *Let $S = \{g_1,\ldots,g_k\} \subset G$ be such that $\mathcal{C}(\mathrm{Ad}_{g_1},\ldots,\mathrm{Ad}_{g_k}) = \{\lambda I\}$. Then $<S>$ is infinite **if and only if** there is an element in $<S>$ that belongs to $\mathcal{B}$ and does not belong to $Z(G)$.*
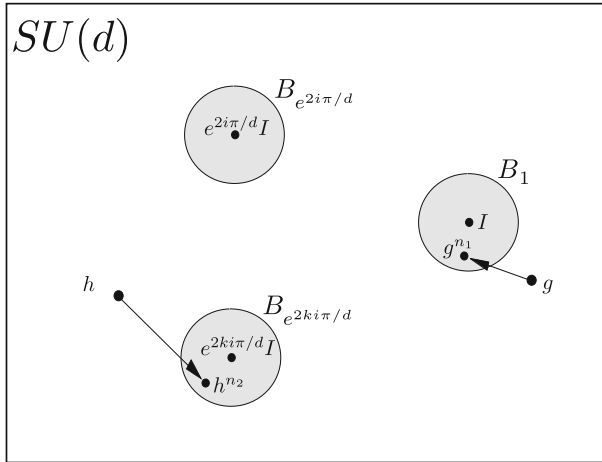
FIGURE 1. Group $SU(d)$ with the exemplary open balls B_α centred at elements form $Z(SU(d))$

Of course, $\mathcal{S}$ can be such that its elements do not belong to $\mathcal{B}$. In the following we show that by taking powers we can move every element of G into B_α for some $\alpha I \in Z(G)$. Moreover, there is a global upper bound for the required power.

Fact 4.10. *For groups $G = SU(d)$ and $G = SO(d)$ there is $N_G \in \mathbb{N}$ such that for every $g \in G$, $g^n \in B_{\alpha_m}$ for some $\alpha_m I \in Z(G)$ and $1 \leq n \leq N_G$.*

Proof. Let us first recall that by the Dirichlet theorem (see Theorem 201 in [23]), for given real numbers $x_1, x_2, \ldots, x_k$ we can find $n \in \mathbb{N}$ so that $nx_1, \ldots, nx_k$ all differ from integers by as little as we want. Let $\{\phi_1, \ldots, \phi_k\}$ be the spectral angles of $g \in G$, and let $\phi_i = 2\pi x_i$, where $x_i \in [0, 1)$. By Dirichlet theorem we can always find n such that nx_i's are close enough to integers to make g^n to belong to B_1. For $g \in G$ let n_g be the smallest positive integer such that $g^{n_g} \in B_\alpha$ for some $\alpha I \in Z(G)$ (by Dirichlet theorem we know that $n_g < \infty$). Let $\mathcal{O}_g^{n_g}$ be an open neighbourhood[2] of g such that for any $h \in \mathcal{O}_g^{n_g}$ we have $h^{n_g} \in B_\alpha$. Note that there might be some $h \in \mathcal{O}_g^{n_g}$ for which n_g is not optimal, but this will not play any role. Let $\left\{\mathcal{O}_g^{n_g}\right\}_{g \in G}$ be the resulting open cover of G. As G is compact there is a finite subcover $\left\{\mathcal{O}_{g_i}^{n_{g_i}}\right\}$ and hence $N_G = \sup_i n_{g_i}$ is well defined and finite. $\square$

For $g \in G$ let $1 \leq n_g \leq N_G$ denote the smallest integer such that $g^{n_g} \in \mathcal{B}$ (see Fig. 1). Using Corollary 4.9 we deduce that $<\mathcal{S}>$ is finite if and only if for every $g \in< S >$ we have $g^{n_g} \in Z(G)$. This in turn places certain constrains on the spectra of elements belonging to $<\mathcal{S}>$.

---

[2] This kind of a neighbourhood exists as taking powers is a continuous operation.

Definition 4.11. Assume $g \notin \mathcal{B}$. The spectrum of g is exceptional if for some $1 \leq n \leq N_G$ we have $g^n \in Z(G)$.

In other words the spectrum of g is exceptional iff (1) $g \in SU(d)$ and all spectral elements of g are n^{th} roots of $\alpha \in \mathbb{C}$, where $\alpha^d = 1$, for some fixed $1 \leq n \leq N_{SU(d)}$, (2) $g \in SO(2k+1)$ and all spectral elements of g are n^{th} roots of unity for some fixed $1 \leq n \leq N_{SO(2k+1)}$, (3) $g \in SO(2k)$ and all spectral elements of g are n^{th} roots of α, where $\alpha^2 = 1$, for some fixed $1 \leq n \leq N_{SO(2k+1)}$. Note that the set of exceptional spectra is a finite set. As a direct consequence we get the following result:

Theorem 4.12. *Let $\mathcal{S} = \{g_1, g_2, \ldots, g_k\} \subset G$, where $G = SO(d)$ and $d \neq 4$ or $G = SU(d)$. Assume $\mathcal{C}(\text{Ad}_{g_1}, \ldots, \text{Ad}_{g_k}) = \{\lambda I\}$ and that there is at least one element in $\mathcal{S}$ for which the spectrum is not exceptional. Then $\overline{< \mathcal{S} >} = G$.*

4.5. The Algorithm for Checking Universality

In this section we present a simple algorithm that allows to decide universality of any given set of gates $\mathcal{S} \subset G$ in a finite number of steps. It works for $G = SU(d)$ and $G = SO(k)$, besides $k = 4$.

The Algorithm for checking universality of $\mathcal{S} = \{g_1, \ldots, g_n\}$

Step 1. Check if $\mathcal{C}(\text{Ad}_{\mathcal{S}}) = \{\lambda I\}$. If the answer is NO stop as the set $\mathcal{S}$ is not universal. If YES, set $l = 1$ and go to Step 2.

Step 2. Check if there is a matrix $g \in \mathcal{S}$ for which g^{n_g} belongs to $\mathcal{B}$ but not to $Z(G)$, where $1 \leq n_g \leq N_G$. If so $\mathcal{S}$ is universal. If NO, set $l = l+1$.

Step 3. Define the new set $\mathcal{S}$ by adding to $\mathcal{S}$ words of length l, i.e. products of elements from $\mathcal{S}$ of length l. If the new $\mathcal{S}$ is equal to the old, the group $<\mathcal{S}>$ is finite. Otherwise, go to Step 2.

If the group generated by $\mathcal{S}$ is finite the algorithm terminates in Step 3 for some $l < \infty$. Otherwise, it terminates in Step 2 for $l < \infty$. In the following we discuss the bounds for l. In case when the group generated by $\mathcal{S}$ is finite the upper bound for l is the order of largest finite subgroup of $SU(d)$. When the set $\mathcal{S}$ is symmetric, i.e. $\mathcal{S} = \{U_1, \ldots, U_k, U_1^{-1}, \ldots, U_k^{-1}\}$ and the group generated by $\mathcal{S}$ is infinite, the bound for l can be determined by looking at the averaging operator $T_{\mathcal{S}} : L^2(SU(d)) \to L^2(SU(d))$:

$$(T_{\mathcal{S}}f)(g) = \frac{1}{2k} \sum_{i=1}^{k} \left(f(U_i g) + f\left(U_i^{-1}g\right) \right). \tag{4.19}$$

Let $\|T\|_{\text{op}} := \sup_{f \in L^2(SU(d))} \frac{\|Tf\|_2}{\|f\|_2}$, where $\|\cdot\|_2$ is the usual L^2 norm. One easily checks that shifting operators $(\tilde{U}f)(g) = f(U^{-1}g)$ are unitary and hence their operator norm is 1. Thus, using triangle inequality, we see that $\|T_{\mathcal{S}}\|_{\text{op}} \leq 1$. In fact, the constant function $f = 1$ is the eigenvector of $T_{\mathcal{S}}$ with the eigenvalue 1 and $\|T_{\mathcal{S}}\|_{\text{op}} = 1$. Let $L_0^2(SU(d))$ be the subspace of $L^2(SU(d))$ containing functions with the vanishing mean. Consider operator $T_{\mathcal{S}}|_{L_0^2(SU(d))}$. The norm of this operator is 1 if and only if 1 is an accumulation point of the spectrum of $T_{\mathcal{S}}$. Otherwise, it is strictly less than 1 and we will denote it by λ_1. If this is the case we say that $T_{\mathcal{S}}$ has a spectral gap. The recent results [5,6] ensure

that $T_{\mathcal{S}}$ has a gap at least when matrices from $\mathcal{S}$ have algebraic entries. For transcendental entries the problem of the spectral gap existence is open. In fact, Sarnak conjectures the spectral gap is present for any universal set. The existence of spectral gap has interesting implications. As shown in [24] (our formulas are slightly different than in [24] as we use Hilbert–Schmidt norm):

Fact 4.13. *Let $\mathcal{S}$ be a universal, symmetric set of gates and assume $T_{\mathcal{S}}$ has a spectral gap. Let $\lambda_1 = \|T_{\mathcal{S}}|_{L_0^2(SU(d))}\|_{\mathrm{op}}$. For every $U \in SU(d)$, $\epsilon > 0$ and*

$$n > A \log\left(\frac{1}{\epsilon}\right) + B$$

there is $U_n \in W_n(\mathcal{S})$ such that $\|U - U_n\| < \epsilon$, where

$$A = \frac{d^2 - 1}{\log(1/\lambda_1)}, \quad B = \frac{\log\left(2^{d^2-1}/a_1\right) + \frac{1}{2}(d^2 - 1)\log(d^2 - 1)}{\log(1/\lambda_1)}$$

and a_1 is such that for any ball of radius ϵ in $SU(d)$ its volume (with respect to normalised Haar measure) V_{B_ϵ} satisfies

$$V(B_\epsilon) \geq a_1 \epsilon^{d^2-1}.$$

The upper bound for l in our algorithm in case when $<\mathcal{S}>$ is infinite is given by the minimal number of gates that are needed to approximate an element whose distance from $\mathcal{B}$ is equal to $\frac{1}{2\sqrt{2}}$ with the precision $\epsilon = \frac{1}{2\sqrt{2}+\delta}$, where δ is arbitrarily small positive number. Using Fact 4.13 this number is bounded by:

$$l \leq \frac{d^2 - 1}{\log(1/\lambda_1)} \log(2\sqrt{2} + \delta) + \frac{\log\left(2^{d^2-1}/a_1\right) + \frac{1}{2}(d^2 - 1)\log(d^2 - 1)}{\log(1/\lambda_1)} \quad (4.20)$$

Moreover, by explicit calculation the volume

$$V(B_\epsilon) = \frac{1}{\pi}\left(2\arcsin\frac{\epsilon}{2\sqrt{2}} - \frac{1}{2}\sin 4\arcsin\frac{\epsilon}{2\sqrt{2}}\right).$$

One easily checks that $a_1 \epsilon^3$, where

$$a_1 = \frac{16\sqrt{2}}{\pi}\left(2\arcsin\frac{1}{8} - \frac{1}{2}\sin\left(4\arcsin\frac{1}{8}\right)\right),$$

satisfies $V(B_\epsilon) \geq a_1 \epsilon^3$ for $\epsilon \in [0, \frac{1}{2\sqrt{2}}]$.

Finally, we note that when spectral gap is small, i.e. λ_1 is close to 1 the upper bound given by 4.20 can be in fact very big. This is the case, for example, when matrices $\mathcal{S}$ are very close to some matrix $U \in SU(d)$. But then they can be simultaneously introduced to a ball B_α and deciding their universality requires actually $l = 1$. Thus, it seems that the bound given in 4.20 is useful only if λ_1 is well separated from 1.

5. Computing N_G

In this section we find upper bounds for $N_{SU(d)}$ and $N_{SO(d)}$ using Dirichlet's approximation theorem [16,23]. These bounds are used in the algorithm presented in Sect. 4.5.

Theorem 5.1. *For a given real number a and a positive integer N there exist integers $1 \leq n \leq N$ and p such that $n\phi$ differs from p by at most $\frac{1}{N+1}$, i.e.*

$$|na - p| \leq \frac{1}{N+1}. \tag{5.1}$$

We will use Theorem 5.1 in calculation of N_G for $G = SO(3)$ and $G = SU(2)$—these two cases when $g \in G$ has a one spectral angle. The simultaneous version of Dirichlet's theorem gives a similar approximation for a collection of real numbers $\phi_1, \ldots, \phi_k$. We will use it for $SO(2k+1)$.

Theorem 5.2. *For given real numbers $a_1, \ldots, a_d$ and a positive integer N there exist integer $1 \leq n \leq N$ and integers $p_1, \ldots, p_k$ such that*

$$|na_i - p_i| \leq \frac{1}{(N+1)^{1/d}}. \tag{5.2}$$

For groups $SO(2k)$ and $SU(d)$ we need to prove a modified version of Dirichlet's theorem. To this end for any $x \in \mathbb{R}$ and $d \in \mathbb{Z}_+$ we define $\{x\}_k$ to be the difference between x and the largest $p + \frac{k}{d}$ that is smaller or equal to x, where $p \in \mathbb{Z}$, $k \in \{0, 1, \ldots, d-1\}$. Clearly, $\{x\}_k \in [0, 1)$. For $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$ we define $\{x\}_k = (\{x_1\}_k, \ldots, \{x_m\}_k)$. Let $\mathcal{L}_{m,d}$ be the lattice in $\mathbb{R}^m$ given by points

$$(q_1, \ldots, q_m), \left(q_1 + \frac{1}{d}, \ldots, q_m + \frac{1}{d}\right), \ldots, \left(q_1 + \frac{d-1}{d}, \ldots, q_m + \frac{d-1}{d}\right),$$

where $q_1, \ldots q_m \in \mathbb{Z}$. An important property of the lattice $\mathcal{L}_{m,d}$ is that for any $p, q \in \mathcal{L}_{m,d}$ we have $p \pm q \in \mathcal{L}_{m,d}$. As a direct consequence of this property we get the following theorem.

Theorem 5.3. *For $a = (a_1, \ldots, a_m)$ and positive $\epsilon < \frac{1}{2d}$ there exist integer $1 \leq n \leq \left\lceil \frac{1}{d\epsilon^m} \right\rceil$ and a point $p = (p_1, \ldots, p_m) \in \mathcal{L}_{m,d}$ such that $\forall i \in \{1, \ldots, m\}$:*

$$|na_i - p_i| < \epsilon. \tag{5.3}$$

Proof. For a given point $a = (a_1, \ldots, a_m) \in \mathbb{R}^m$ consider $dQ^m + 1$ points:

$$\{na\}_0, \{na\}_1, \ldots, \{na\}_{d-1}, \ n \in \{0, \ldots, Q^m\} \tag{5.4}$$

Next take an m-dimensional cube $[0, 1)^m$ and divide it into dQ^m boxes by drawing planes parallel to its faces at distances $\frac{1}{\sqrt[m]{dQ}}$. By Dirichlet's pigeon hole principle, at least two points from (5.4) fall to the same box. Let these points be $\{q_1 a\}_i$ and $\{q_2 a\}_j$, where $i, j \in \{1, \ldots, d-1\}$ and $q_1 < q_2$. Note that q_1 cannot be equal to q_2 as in this case $\epsilon > \frac{1}{2d}$. As the lattice $\mathcal{L}_{m,d}$ is invariant with respect to addition and subtraction of its points we have $\max_l |\{(q_2 - q_1)a_l\}_k| < \frac{1}{\sqrt[m]{dQ}}$, where $k = j - i$ if $i < j$ or $k = d + j - i$ when $i > j$. The result follows. $\qquad\square$

We begin with finding the exact values of $N_{SU(2)}$ and $N_{SO(3)}$.

Fact 5.4. $N_{SO(3)} = 12$ *and* $N_{SU(2)} = 6$.

Proof. Let $O \in SO(3)$, and let $[0, 2\pi) \ni \phi = 2a\pi$ be its spectral angle. By Theorem 5.1 for a given N there are integers p and $1 \le n \le N$ such that $|na - p| \le \frac{1}{N+1}$. Multiplying this inequality by π yields $|n\frac{\phi}{2} - p\pi| \le \frac{\pi}{N+1}$. Note that (4.14) simplifies to $|\sin\frac{\psi}{2}| < \frac{1}{4}$, i.e. for a given ϕ we look for n such that $|n\frac{\phi}{2} - p\pi| < \arcsin\frac{1}{4}$. Combining these two observations we need to find the smallest N such that $\frac{\pi}{N+1} < \arcsin\frac{1}{4}$. It is

$$N = \left\lceil \frac{\pi - \arcsin\frac{1}{4}}{\arcsin\frac{1}{4}} \right\rceil = 12. \tag{5.5}$$

Formula (5.5) gives an upper bound for $N_{SO(3)}$. Note, however, that for $\frac{\phi}{2} = \arcsin\frac{1}{4}$ the smallest n such that $|n\arcsin\frac{1}{4} - \pi| < \arcsin\frac{1}{4}$ is exactly 12 (see Fig. 2a); hence, $N_{SO(3)} = 12$.

Assume next $U \in SU(2)$ and $[0, 2\pi) \ni \phi = a\pi$ be its spectral angle. By Theorem 5.1 for a given N there are integers p and $1 \le n \le N$ such that $|na - p| \le \frac{1}{N+1}$. Multiplying this inequality by $\frac{\pi}{2}$ yields $\left|n\frac{\phi}{2} - p\frac{\pi}{2}\right| \le \frac{\pi}{2(N+1)}$. Note that (4.14) simplifies to $\left|\sin\frac{\psi}{2}\right| < \frac{1}{4}$ or $\left|\sin\frac{\psi-\pi}{2}\right| < \frac{1}{4}$, i.e. for a given ϕ we look for n such that $\left|n\frac{\phi}{2} - p\frac{\pi}{2}\right| < \arcsin\frac{1}{4}$. Combining these two observations we need to find the smallest N such that $\frac{\pi}{2(N+1)} < \arcsin\frac{1}{4}$. This is

$$N = \left\lceil \frac{\frac{\pi}{2} - \arcsin\frac{1}{4}}{\arcsin\frac{1}{4}} \right\rceil = 6. \tag{5.6}$$

Formula (5.6) gives an upper bound for $N_{SU(2)}$. Note, however, that for $\frac{\phi}{2} = \arcsin\frac{1}{4}$ the smallest n such that $\left|n\arcsin\frac{1}{4} - \frac{\pi}{2}\right| < \arcsin\frac{1}{4}$ is exactly 6 (see Fig. 2b). Hence, $N_{SU(2)} = 6$. □

Fact 5.5. *The values of $N_{SO(2k+1)}$ and $N_{SO(2k)}$ are bounded from the above by:*

$$N_{SO(2k+1)} < \left\lceil \left(\frac{\pi}{\arcsin\frac{1}{4\sqrt{k}}}\right)^k \right\rceil, \tag{5.7}$$

$$N_{SO(2k)} < \left\lceil \frac{1}{2}\left(\frac{\pi}{\arcsin\frac{1}{4\sqrt{k}}}\right)^k \right\rceil. \tag{5.8}$$

Proof. The spectral angles of $O \in SO(d)$ are $\{\phi_1, -\phi_1, \ldots, \phi_k, -\phi_k\}$ if $d = 2k$ or $\{\phi_1, -\phi_1, \ldots, \phi_k, -\phi_k, 0\}$ if $d = 2k+1$. We first address the case of $SO(2k)$. Assume that $\phi_i = a_i\pi$ for all $i \in \{1, \ldots, k\}$. The lattice $\pi \cdot \mathcal{L}_{k,2}$ corresponds exactly to points $\left\{\frac{\phi_1}{2}, \ldots, \frac{\phi_k}{2}\right\}$ at which balls B_1 and B_{-1} given by conditions (4.15) and (4.16) are centred. Let us next find the smallest hypercube
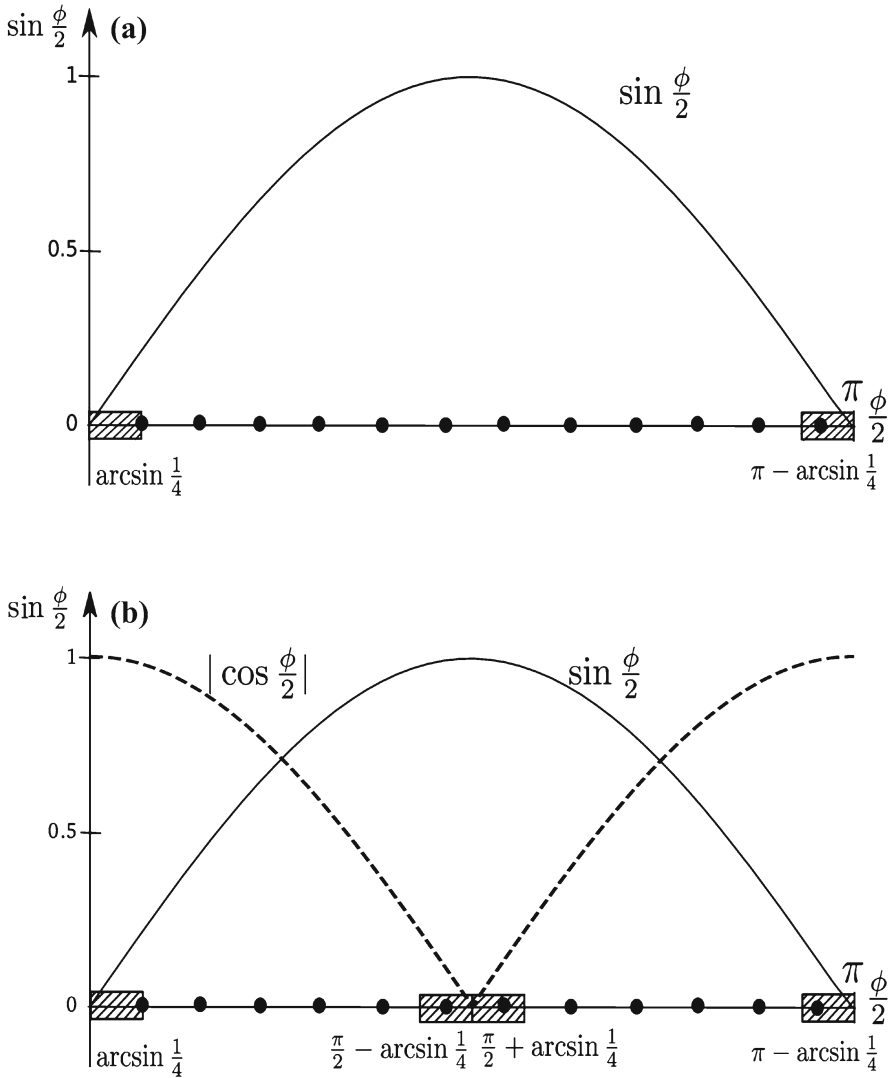
FIGURE 2. **a** Condition (4.14) for $SO(3)$. *Black dots* correspond to $n \arcsin \frac{1}{4}$, and *dashed* segments are determined by $\left| \sin \frac{\phi}{2} \right| < \frac{1}{4}$. **b** Conditions (4.13) for $U \in SU(2)$. *Black dots* correspond to $n \arcsin \frac{1}{4}$, and *dashed* segments are determined by $\left| \sin \frac{\phi}{2} \right| < \frac{1}{4}$ or $\left| \sin \frac{\phi - \pi}{2} \right| < \frac{1}{4}$

$\left[-\frac{\beta_k}{2}, \frac{\beta_k}{2} \right]^{\times k}$ contained in the ball B_1. By symmetry, its edge length will be the same for B_{-1}. To this end one needs to minimise $\sum_i \phi_i^2$ under the condition $\sum_i \sin^2 \phi_i = \frac{1}{16}$. Calculations with the use of the Lagrange multipliers

show that the coordinates of the minimising point are all equal and hence $k \sin^2 \frac{\beta_k}{2} = \arcsin \frac{1}{16}$. That means $\frac{\beta_k}{2} = \arcsin \frac{1}{4\sqrt{k}}$ is the half of the edge length of the largest hypercube contained in a ball $B_{\pm 1}$. We next apply Theorem 5.3 to the lattice $\mathcal{L}_{k,2}$ and the point $a = (a_1, \ldots, a_k)$ with $\epsilon = \frac{\arcsin \frac{1}{4\sqrt{k}}}{\pi} < \frac{1}{4}$. As a result we obtain point $p \in \mathcal{L}_{k,2}$ such that:

$$|na_i - p_i| < \frac{\arcsin \frac{1}{4\sqrt{k}}}{\pi}, \tag{5.9}$$

where

$$n < \left\lceil \frac{\pi^k}{2 \left(\arcsin \frac{1}{4\sqrt{k}} \right)^k} \right\rceil.$$

For $SO(2k+1)$ we can directly apply Theorem 5.2. Looking at the hypercube that is contained in one of the balls given by conditions (4.15) and (4.16) we get the desired result. $\qquad\square$

Fact 5.6. *For $d \geq 3$ the value of $N_{SU(d)}$ is bounded from the above by:*

$$N_{SU(d)} < \left\lceil \frac{1}{d} \left(\frac{2\pi}{\beta_d} \right)^{d-1} \right\rceil,$$

where β_d is such that $(d-1) \sin^2 \frac{\beta_d}{2} + \sin^2 \frac{(d-1)\beta_d}{2} = \frac{1}{8}$.

Proof. For $U \in SU(d)$ let $\{\phi_1, \ldots, \phi_d\}$ be the spectral angles of U. Assume that for every $i \in \{1 \ldots, d-1\}$ we have $[0, 2\pi) \ni \phi_i = a_i\pi$. As $\sum_i \phi_i = 0 \bmod 2\pi$ we can always put $\phi_d = -\sum_{i=1}^{d-1} \phi_i$. We need to first find the edge length of the largest hypercube $\left[-\frac{\beta_d}{2}, \frac{\beta_d}{2} \right]^{\times(d-1)}$ contained in the ball B_1. By symmetry of condition (4.14), this length will be the same for other balls. We need to minimise $\sum_i \phi_i^2$ under the condition $\sum_{i=1}^{d-1} \sin^2 \phi_i + \sin^2 \left(\sum_{i=1}^{d-1} \phi_i \right) = \frac{1}{8}$. Calculations with the use of the Lagrange multipliers show that the coordinates of the minimising point are all equal and hence β_d satisfies:

$$(d-1) \sin^2 \frac{\beta_d}{2} + \sin^2 \frac{(d-1)\beta_d}{2} = \frac{1}{8}. \tag{5.10}$$

In order to apply Theorem 5.3 we need to check if $\frac{\beta_d}{2\pi} < \frac{1}{2d}$. By Eq. (5.10) β_d is clearly close to zero and therefore we can assume that $\sin \frac{\beta_d}{2}$ approximately equals $\frac{\beta_d}{2}$. Then it follows that $\frac{\beta_d}{2\pi} = \frac{1}{2\pi\sqrt{2d(d-1)}}$ which is clearly smaller than $\frac{1}{2d}$. Thus, we can apply Theorem 5.3 to the lattice $\mathcal{L}_{d-1,d}$ and the point $a = (a_1, \ldots, a_{d-1})$ with $\epsilon = \frac{\beta_d}{2\pi} < \frac{1}{2d}$. As a result, we obtain point $p \in \mathcal{L}_{d-1,d}$ such that:

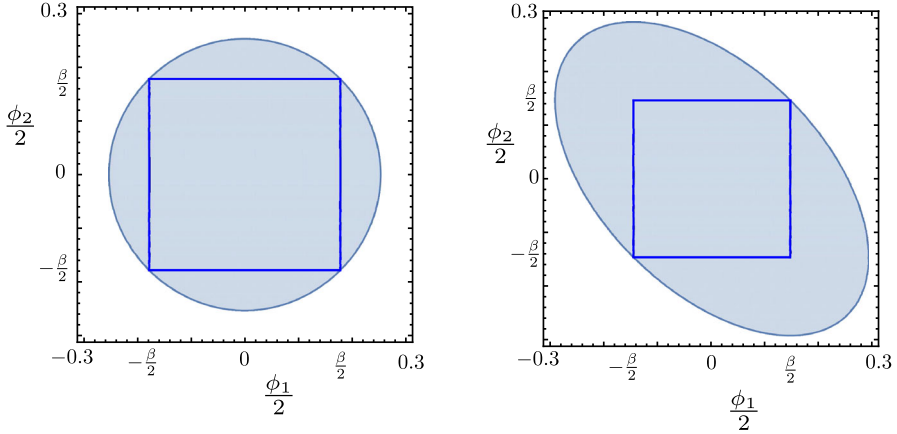$$|na_i - p_i| < \frac{\beta_d}{2\pi}, \tag{5.11}$$

FIGURE 3. Smallest hypercubes contained in the balls B_1 for $SO(4)$ and $SU(3)$, respectively

where

$$n < \left\lceil \frac{1}{d} \left(\frac{2\pi}{\beta_d} \right)^{d-1} \right\rceil.$$

The result follows.   □

For $d = 3$ we obtain $\frac{\beta_3}{2} = \arctan \sqrt{\frac{6-\sqrt{34}}{2+\sqrt{34}}}$ and $N_{SU(3)} < 154$. On the other hand, numerical calculations yield $N_{SU(3)} = 49$. For orthogonal groups we have that numerical calculations yield $N_{SO(5)} = 172$ and $N_{SO(4)} = 86$, where the bounds given by (5.7) and (5.8) are $N_{SO(5)} < 312$ and $N_{SO(4)} < 151$, respectively. The difference between the bounds and values calculated numerically reflects the obvious fact that the considered hypercubes are rather brutal approximations of the balls B_α (see Fig. 3). However, we stress that the choice of hypercubes we made is the most optimal from the perspective of Dirichlet's theorems. Let us also note that the upper bound for N_G seems to be more accurate for $SO(4)$ than for $SU(3)$. We believe this stems from the fact that the 'square-ball' area ratio is smaller for $SU(3)$ than for $SO(4)$ (see Fig. 3). The way how these ratios should be incorporated into formulas for the upper bound on N_G is left as an open problem. We suppose this should be done by introducing some additional factor that depends on the square-ball ratio.

6. Universality for $SU(2)$ and $SO(3)$

In the following we discuss universality of gates in case when $G = SU(2)$ or $G = SO(3)$. In particular, we formulate explicit conditions (Fact 6.1) for $\mathcal{C}(\mathrm{Ad}_\mathcal{S}) = \{\lambda I\}$, where $\mathcal{S}$ is a finite subset of G. For both $SU(2)$ and $SO(3)$ exceptional spectra are determined by one spectral angle, and if at least one matrix from

$\mathcal{S}$ has non-exceptional spectrum the algorithm in Sect. 4.5 terminates in Step 2 with $l = 1$. In Sect. 6.3.1 we show that for $\mathcal{S}$ consisting of two matrices that have exceptional spectra one can decide their universality in at most $l = 4$ steps. Moreover, our algorithm always terminates for $l \leq 13$.

6.1. $SU(2)$ and $SO(3)$: Review of Useful Properties

In the following we recall useful facts about groups $SO(3)$ and $SU(2)$. In particular, we introduce their parameterisations and briefly discuss the covering homomorphism given by the adjoint representation.

Commutation relations for the Lie algebras of the considered groups are as follows:

$$\mathfrak{su}(2): \quad [X, Y] = 2Z, \quad [X, Z] = -2Y, \quad [Y, Z] = 2X. \tag{6.1}$$

where X, Y, Z are defined as

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \, Y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \, Z = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

and

$$\mathfrak{so}(3): \quad [X_{23}, X_{13}] = -X_{12}, \quad [X_{23}, X_{12}] = X_{13}, \quad [X_{13}, X_{12}] = X_{23}, \tag{6.2}$$

where X_{ij} are defined as in (4.5). The Lie algebras $\mathfrak{su}(2)$ and $\mathfrak{so}(3)$ are isomorphic through the adjoint representation ad : $\mathfrak{su}(2) \to \mathfrak{so}(3)$. The isomorphism is established by $X \mapsto \mathrm{ad}_X = -2X_{23}$, $Y \mapsto \mathrm{ad}_Y = 2X_{13}$, $Z \mapsto \mathrm{ad}_Z = -2X_{12}$.

Elements of groups $SU(2)$ and $SO(3)$ can be expressed using exponential map. By Cayley–Hamilton theorem we have:

$$SU(2): \; U(\phi, \vec{k}) = e^{\phi \cdot u(\vec{k})} = e^{\phi(k_x X + k_y Y + k_z Z)} = \cos \phi I + \sin \phi u(\vec{k}), \tag{6.3}$$

$$SO(3): \; O(\phi, \vec{k}) = e^{\phi \cdot o(\vec{k})} = e^{\phi(-k_x X_{23} + k_y X_{13} - k_z X_{12})}$$

$$= I + \sin \phi o(\vec{k}) - 2 \sin^2 \frac{\phi}{2} o(\vec{k})^2, \tag{6.4}$$

where $\vec{k} = [k_x, k_y, k_z] \in \mathbb{R}^3$ is a rotation axis, $k_x^2 + k_y^2 + k_z^2 = 1$, and $\phi \in [0, 2\phi)$. Groups $SU(2)$ and $SO(3)$ are related by the covering homomorphism Ad : $SU(2) \to SO(3)$ given by $\mathrm{Ad}_{e^A} = e^{\mathrm{ad}_A}$, where $A \in \mathfrak{su}(2)$ and Ad : $U(\phi, \vec{k}) \mapsto O(2\phi, \vec{k})$. Ad is in this case double covering. Using (6.3) we can easily calculate the product $U(\gamma, \vec{k}_{12}) = U(\phi_1, \vec{k}_1)U(\phi_2, \vec{k}_2)$, where

$$\cos \gamma = \cos \phi_1 \cos \phi_2 - \sin \phi_1 \sin \phi_2 \vec{k}_1 \cdot \vec{k}_2, \tag{6.5}$$

$$\vec{k}_{12} = \frac{1}{\sin \gamma} \left(\vec{k}_1 \sin \phi_1 \cos \phi_2 + \vec{k}_2 \sin \phi_2 \cos \phi_1 + \vec{k}_1 \times \vec{k}_2 \sin \phi_1 \sin \phi_2 \right). \tag{6.6}$$

Making use of (6.5) one checks that two $SU(2)$ matrices $U(\phi_1, \vec{k}_1)$, $U(\phi_2, \vec{k}_2)$ that do not belong to $\{I, -I\}$ commute iff the axes $\vec{k}_1$ and $\vec{k}_2$ are parallel, that is $[u(\vec{k}_1), u(\vec{k}_2)] = 0$. Similarly, they anticommute iff the axes $\vec{k}_1$ and $\vec{k}_2$ are orthogonal and rotation angles are $\phi_1, \phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$. As for matrices from $SO(3)$, recall that they cannot anticommute. In order to check when

they commute we note that commuting and anticommuting $SU(2)$ matrices satisfy the identity $U_1 U_2 U_1^{-1} U_2^{-1} = \pm I$. But $\text{Ad}_{\pm I} = I$ and therefore $O(\phi_1, \vec{k}_1)$ commutes with $O(\phi_2, \vec{k}_2)$ iff either axes $\vec{k}_1$ and $\vec{k}_2$ are parallel or $\vec{k}_1 \perp \vec{k}_2$ and $\phi_1, \phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$.

   Finally, it is known that all automorphisms of $SU(2)$ are inner automorphisms; thus, they are in one-to-one correspondence with elements of $SO(3)$. Using our notation $O \in SO(3)$ determines the automorphism $\Phi_O : SU(2) \to SU(2)$ given by

$$\Phi_O(U(\phi, \vec{k})) = U(\phi, O\vec{k}). \qquad (6.7)$$

6.2. Exceptional Spectra and Spaces $\mathcal{C}(\text{Ad}_S)$ for $SU(2)$ and $SO(3)$

For any matrix $U(\phi, \vec{k}) \in SU(2)$ the spectrum is given by $\{e^{i\phi}, e^{-i\phi}\}$, $\phi \in [0, 2\pi)$. By Definition 4.11 the spectrum of $U(\phi, \vec{k})$ is exceptional iff $e^{i\phi}$ is a root of 1 or -1 of order $n = \{1, \ldots, N_{SU(2)}\}$. The corresponding $\phi \in [0, 2\pi)$ will be called exceptional angle. Similarly, for $O(\phi, \vec{k}) \in SO(3)$ the spectrum is given by $\{e^{i\phi}, e^{-i\phi}, 1\}$ and thus is exceptional iff $e^{i\phi}$ is a root of unity of order $1 \leq n \leq N_{SO(3)}$. The corresponding $\phi \in [0, 2\pi)$ will be called an exceptional angle. We can easily compute the number of exceptional spectra for $SU(2)$ and $SO(3)$ using the Euler's totient function $\varphi(n)$ by noting that the roots of -1 of order n are the roots of unity of order $2n$.

   Let us denote the sets of exceptional angles for $SU(2)$ and $SO(3)$ by $\mathcal{L}_{SU(2)}$ and $\mathcal{L}_{SO(3)}$, respectively. We have:

$$|\mathcal{L}_{SU(2)}| = \sum_{n=1}^{6} \varphi(n) + \sum_{n=4}^{6} \varphi(2n) = 24, \qquad (6.8)$$

$$|\mathcal{L}_{SO(3)}| = \sum_{n=1}^{12} \varphi(n) = 46. \qquad (6.9)$$

The elements of sets $\mathcal{L}_G$ are of the form $\mathcal{L}_G = \{a\pi : a \in \mathcal{L}'_G\}$, where

$$\mathcal{L}'_{SU(2)} = \left\{0, \frac{1}{2}, 1, \frac{3}{2}, \frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{5}{3}, \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{6}{5}, \frac{7}{5}, \frac{8}{5}, \frac{9}{5}, \frac{1}{6}, \frac{5}{6}, \frac{7}{6}, \frac{11}{6}\right\},$$

$$\mathcal{L}'_{SO(3)} = \mathcal{L}'_{SU(2)} \cup \left\{\frac{2}{7}, \frac{4}{7}, \frac{6}{7}, \frac{8}{7}, \frac{10}{7}, \frac{12}{7}, \frac{2}{9}, \frac{4}{9}, \frac{8}{9}, \frac{10}{9}, \frac{14}{9}, \frac{16}{9}, \frac{2}{11}, \frac{4}{11}, \frac{6}{11}, \frac{8}{11}, \right.$$
$$\left. \frac{10}{11}, \frac{12}{11}, \frac{14}{11}, \frac{16}{11}, \frac{18}{11}, \frac{20}{11}\right\}, \qquad (6.10)$$

We next discuss the conditions when the space $\mathcal{C}\left(\text{Ad}_{U(\phi_1, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)}\right)$ is different than $\mathcal{C}\left(\text{ad}_{u(\vec{k}_1)}, \text{ad}_{u(\vec{k}_2)}\right)$. First, we note that elements $u(\vec{k}_1)$, $u(\vec{k}_2)$ generate Lie algebra $\mathfrak{su}(2)$ iff $[u(\vec{k}_1), u(\vec{k}_2)] \neq 0$. In this case by Lemma 3.3, the solution set $\mathcal{C}(\text{ad}_{u(\vec{k}_1)}, \text{ad}_{u(\vec{k}_2)}) = \{\lambda I\}$. Using Fact 4.2 we note that the space $\mathcal{C}\left(\text{Ad}_{U(\phi_1, \vec{k}_1)}, \text{Ad}_{U(\phi_1, \vec{k}_2)}\right)$ can be different than $\mathcal{C}\left(\text{ad}_{u(\vec{k}_1)}, \text{ad}_{u(\vec{k}_2)}\right)$ if

at least one ϕ_i is equal to $\frac{k\pi}{2}$. In the following we give exact conditions when it happens.

Fact 6.1. *Assume that $[u(\vec{k}_1), u(\vec{k}_2)] \neq 0$. The space $\mathcal{C}\left(\mathrm{Ad}_{U(\phi_1,\vec{k}_1)}, \mathrm{Ad}_{U(\phi_2,\vec{k}_2)}\right)$ is larger than $\{\lambda I : \lambda \in \mathbb{R}\}$ if and only if: (1) $\phi_1, \phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ and (2) one of $\phi_i \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ and $\vec{k}_1 \perp \vec{k}_2$.*

Proof. By Fact 4.2 $\mathcal{C}\left(\mathrm{Ad}_{U(\phi_1,\vec{k}_1)}, \mathrm{Ad}_{U(\phi_2,\vec{k}_2)}\right)$ can be larger than $\{\lambda I : \lambda \in \mathbb{R}\}$ if at least one of the spectral angles of $\mathrm{Ad}_{U(\phi_1,\vec{k}_1)}$, $\mathrm{Ad}_{U(\phi_2,\vec{k}_2)}$ is $k\pi$. Therefore, we have to consider situation when either two angles ϕ_1 and ϕ_2 are equal to $\frac{k\pi}{2}$ or exactly one of ϕ_i's is $\frac{k\pi}{2}$, $k \in \{1,3\}$. For the case (1) generators are of the form $U\left(\frac{k\pi}{2}, \vec{k}_1\right)$ and $U\left(\frac{k\pi}{2}, \vec{k}_2\right)$, where $\vec{k}_1 \cdot \vec{k}_2$ is arbitrary. Note that $\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_1\right)} = O(k\pi, \vec{k}_1)$ and $\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_2\right)} = O(k\pi, \vec{k}_2)$ are rotation matrices by angles $2\phi_1 = 2\phi_2 = k\pi$. A rotation $O(\phi_3, \vec{k}_3)$ by an arbitrary angle ϕ_3 and about the axis $\vec{k}_3 = \vec{k}_1 \times \vec{k}_2$ commutes with the rotations $O(k\pi, \vec{k}_1)$ and $O(k\pi, \vec{k}_2)$ and is different than λI.

Let us consider the case when exactly one of ϕ_i's is $\frac{k\pi}{2}$. We are given the generators $U\left(\frac{k\pi}{2}, \vec{k}_1\right)$ and $U\left(\phi_2, \vec{k}_2\right)$. Note that the rotation $O(\pi, \vec{k})$, where $\vec{k} \parallel \vec{k}_2$, commutes with both $\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_1\right)} = O(k\pi, \vec{k}_1)$ and $\mathrm{Ad}_{U(\phi_2,\vec{k}_2)} = O(2\phi_2, \vec{k}_2)$ provided $\vec{k}_1 \perp \vec{k}_2$. Therefore, in this case $\mathcal{C}(\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_1\right)}, \mathrm{Ad}_{U(\phi_2,\vec{k}_2)})$ is larger than $\{\lambda I : \lambda \in \mathbb{R}\}$. We are left with showing that if $\vec{k}_1 \not\perp \vec{k}_2$ and exactly one ϕ_i's is an odd multiple of π, the space $\mathcal{C}(\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_1\right)}, \mathrm{Ad}_{U(\phi_2,\vec{k}_2)})$ is equal to $\{\lambda I : \lambda \in \mathbb{R}\}$.

By formula (6.3) if $\vec{k}_1 \not\perp \vec{k}_2$, $\phi_1 = \frac{k\pi}{2}$ and $\phi_2 \neq \frac{k\pi}{2}$, then the only orthogonal matrix commuting with $\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_1\right)} = O(k\pi, \vec{k}_1)$ and $\mathrm{Ad}_{U(\phi_2,\vec{k}_2)}$ is the identity matrix. In the following we show that relaxing orthogonality to an arbitrary endomorphism gives only λI. To see this, note that endomorphisms commuting with $\mathrm{Ad}_{U(\phi_2,\vec{k}_2)}$ are of the form

$$A = \alpha_2 O(\theta_2, \vec{k}_2) + \beta_2 |\vec{k}_2\rangle\langle\vec{k}_2|,$$

where $\alpha_2, \beta_2 \in \mathbb{R}$ and $\theta_2 \in [0, 2\pi)$. On the other hand, matrices commuting with $\mathrm{Ad}_{U\left(\frac{k\pi}{2},\vec{k}_1\right)}$ are of the form

$$B = E\left(\vec{k}_1^\perp\right) + \beta_1 |\vec{k}_1\rangle\langle\vec{k}_1|,$$

where $E\left(\vec{k}_1^\perp\right)$ is an arbitrary matrix acting on the two-dimensional space perpendicular to $\vec{k}_1$ such that $E\left(\vec{k}_1^\perp\right)\vec{k}_1 = 0$ and $\beta_1 \in \mathbb{R}$. Let $\{\vec{k}_1, \vec{k}_2, \vec{k}_{12}\}$, where $\vec{k}_{12} = \vec{k}_1 \times \vec{k}_2$ be a basis of $\mathbb{R}^3$. Matrices A and B must agree on the basis vectors. This way we obtain the following equations:

$$\beta_1 \vec{k}_1 = \alpha_2 O(\theta_2, \vec{k}_2)\vec{k}_1 + \beta_2 \langle\vec{k}_1|\vec{k}_2\rangle\vec{k}_2, \tag{6.11}$$

$$(\alpha_2 + \beta_2)\vec{k}_2 = E\left(\vec{k}_1^{\perp}\right)\vec{k}_2 + \beta_1\langle\vec{k}_1|\vec{k}_2\rangle\vec{k}_1, \tag{6.12}$$

$$E\left(\vec{k}_1^{\perp}\right)\vec{k}_{12} = \alpha_2 O(\theta_2, \vec{k}_2)\vec{k}_{12}. \tag{6.13}$$

The left-hand side of (6.10) is a vector perpendicular to $\vec{k}_1$, and the right-hand side of (6.10) is a vector perpendicular to $\vec{k}_2$. The only vector satisfying both of these conditions is proportional to $\vec{k}_{12}$ and therefore $\theta_2 = n\pi$. Hence, $O(\theta_2, \vec{k}_2) = \pm I$. From Eq. (6.10) we get

$$\beta_1\vec{k}_1 = \pm\alpha_2\vec{k}_1 + \beta_2\langle\vec{k}_1|\vec{k}_2\rangle\vec{k}_2,$$

which means $\beta_1 = \pm\alpha_2$ and either $\beta_2 = 0$ or $\vec{k}_1 \perp \vec{k}_2$. If $\beta_2 = 0$ then $A = \pm\alpha_2 I$ and hence the equality between A and B implies

$$\mathcal{C}\left(\mathrm{Ad}_{U\left(\frac{k\pi}{2}, \vec{k}_1\right)}, \mathrm{Ad}_{U(\phi_2, \vec{k}_2)}\right) = \{\lambda I : \lambda \in \mathbb{R}\}.$$

Therefore, the only solution that yields a bigger space $\mathcal{C}(\mathrm{Ad}_{U\left(\frac{k\pi}{2}, \vec{k}_1\right)}, \mathrm{Ad}_{U(\phi_2, \vec{k}_2)})$ corresponds to $\vec{k}_1 \perp \vec{k}_2$. $\qquad\square$

6.3. Universal $SU(2)$ Gates

In this section we consider the set $\mathcal{S}$ of two non-commuting matrices $U(\phi_1, \vec{k}_1)$, $U(\phi_2, \vec{k}_2)$ and ask when they generate $SU(2)$. We treat separately three cases:

1. When $\mathcal{C}(\mathrm{Ad}_{U(\phi_1, \vec{k}_1)}, \mathrm{Ad}_{U(\phi_2, \vec{k}_2)}) = \{\lambda I\}$ and at least one of ϕ_i's is non-exceptional—by Theorem 4.12, $\overline{<\mathcal{S}>} = SU(2)$,
2. When $\mathcal{C}(\mathrm{Ad}_{U(\phi_1, \vec{k}_1)}, \mathrm{Ad}_{U(\phi_2, \vec{k}_2)}) = \{\lambda I\}$ and both angles are exceptional. This determines the maximal running time of the algorithm shown in Sect. 4.5 to be $l = 13$.
3. When $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}}) \neq \{\lambda I\}$ we identify what is the structure of $<\mathcal{S}>$.

We start from studying the last case. We already know that when $\vec{k}_1 \perp \vec{k}_2$ and $\phi_2 = \frac{m\pi}{2}$, where $m \in \{1, 3\}$ the group generated by $U(\phi_1, \vec{k}_1)$, $U(\phi_2, \vec{k}_2)$ is not $SU(2)$ as $\mathcal{C}\left(\mathrm{Ad}_{U(\phi_1, \vec{k}_1)}, \mathrm{Ad}_{U(\phi_2, \vec{k}_2)}\right) \neq \{\lambda I\}$. We will now show that in this case this group is either finite or infinite *dicyclic group*. To this end let $b := U(\phi_1, \vec{k}_1)$ and $x := U(\frac{\pi}{2}, \vec{k}_2)$ and assume b is of finite order. The group generated by b and x has the following presentation:

$$H = \left\langle b, x \,|\, x^4 = I, b^n = I, xbx^{-1} = b^{-1}\right\rangle. \tag{6.14}$$

As H contains $-I$ we have $(-b)^n = -I$ for n odd. Let $a = -b$ then

$$H = \left\langle a, x \,|\, x^4 = I, a^{2n} = I, xax^{-1} = a^{-1}\right\rangle, \tag{6.15}$$

which is the definition of the dicyclic group of order $4n$ (it is the central extension of the dihedral group of order $2n$ by $-I$). In case when a is of the infinite order, after closure, we obtain a group consisting of two connected components. The first one is a one-parameter group $\{U(t, \vec{k}_1) : t \in \mathbb{R}\}$ generated by $U(\phi_1, \vec{k}_1)$, and the second one is its normaliser $\{U\left(\frac{\pi}{2}, \vec{k}_2\right)U(t, \vec{k}_1) : t \in \mathbb{R}\}$. The only other case when $\mathcal{C}\left(\mathrm{Ad}_{U(\phi_1, \vec{k}_1)}, \mathrm{Ad}_{U(\phi_2, \vec{k}_2)}\right) \neq \{\lambda I\}$ corresponds to

the situation when both ϕ_1 and ϕ_2 are odd multiples of $\frac{\pi}{2}$. In this case the group generated by $U(\phi_1, \vec{k}_1)$, $U(\phi_2, \vec{k}_2)$ is the same as the group generated by $U(\gamma, \vec{k}_{12}) = U(\phi_1, \vec{k}_1)U(\phi_2, \vec{k}_2)$ and $U(\phi_2, \vec{k}_2)$. One can easily calculate that $\cos\gamma = \vec{k}_1 \cdot \vec{k}_2$ and $\vec{k}_{12} \perp \vec{k}_2$. Thus, the group is once again the dicyclic group of the order $4n$ where n is the order of $U(\gamma, \vec{k}_{12})$.

Lemma 6.2. *Assume that $U(\phi_1, \vec{k}_1)$ and $U(\phi_2, \vec{k}_2)$ do not commute and $\vec{k}_1 \cdot \vec{k}_2 = 0$ and $\phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$. Then the group generated by $U(\phi_1, \vec{k}_1)$ and $U(\phi_2, \vec{k}_2)$ is either 1) the dicyclic group of order $4n$*

$$n = \max(\operatorname{order}U(\phi_1, \vec{k}_1), \operatorname{order}U(\phi_1 + \pi, \vec{k}_1)), \quad (6.16)$$

when $\operatorname{order}U(\phi_1, \vec{k}_1) < \infty$, or 2) the infinite dicyclic group if $\operatorname{order}U(\phi_1, \vec{k}_1) = \infty$. When both ϕ_i's belong to $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ the group generated by $U(\phi_1, \vec{k}_1)$ and $U(\phi_2, \vec{k}_2)$ is also the dicyclic group of the order $4n$ where n is the order of $U(\gamma, \vec{k}_{12}) = U(\phi_1, \vec{k}_1)U(\phi_2, \vec{k}_2)$.

In other words, the group generated by two non-commuting matrices from $SU(2)$ that do not satisfy the necessary condition for universality is either a finite or an infinite dicyclic group.

6.3.1. Two Exceptional Angles. Let $\phi_1 \in \mathcal{L}_{SU(2)} \setminus \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$[3] and $\phi_2 \in \mathcal{L}_{SU(2)} \setminus \{0, \pi\}$, and let $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\}$ be a two-element subset of $SU(2)$. Using automorphism (6.7), for any $O \in SO(3)$ the group generated by $\mathcal{S}$ is isomorphic with the group generated by $U(\phi_1, O\vec{k}_1)$ and $U(\phi_2, O\vec{k}_2)$. This freedom allows us to choose $O \in SO(3)$ such that $\vec{k}'_1 = O\vec{k}_1 = [0, 0, 1]$ and $\vec{k}'_2 = O\vec{k}_2 = [\sin\alpha, 0, \cos\alpha]$, for some $\alpha \in [0, 2\pi)$. Thus, in the following we will work with matrices $\mathcal{S}' = \{U(\phi_1, \vec{k}'_1), U(\phi_2, \vec{k}'_2)\}$. Our aim is to determine how long does it take for the algorithm shown in Sect. 4.5 to decide the universality of $\mathcal{S}'$. If the algorithm does not terminate with $l = 1$ this means that the product of matrices from $\mathcal{S}$ have exceptional spectral angles. Thus, using formula (6.5)

$$\cos\alpha = \vec{k}'_1 \cdot \vec{k}'_2 = \frac{\cos\phi_1 \cos\phi_2 - \cos\gamma}{\sin\phi_1 \sin\phi_2}, \quad (6.17)$$

for some $\gamma \in \mathcal{L}_{SU(2)}$. In order to determine all such cases we need to exclude all triplets ϕ_1, ϕ_2, γ that lead to $|\cos\alpha| \geq 1$. For all remaining cases we run our algorithm with matrices $\mathcal{S}$. The termination results are as follows:

1. The algorithm terminates in Step 2 for $l \leq 4$, and the resulting group is $SU(2)$.
2. The algorithm terminates in Step 3 with $5 \leq l \leq 6$, and the resulting group has 24 elements and is isomorphic to the binary tetrahedral group $<2, 3, 3> := \{a, b, c | a^2 = b^3 = c^3 = abc\}$.

---

[3] The case when both ϕ_i's are odd multiples of $\frac{\pi}{2}$ was treated in Lemma 6.2.

TABLE 1. Number of exceptional triplets ϕ_1, ϕ_2, γ terminating the universality algorithm for different l's

l	Step	Number of triplets ϕ_1, ϕ_2, γ	Generated group
$-$	1	80	Dicyclic group
3	2	3232	$SU(2)$
4	2	160	$SU(2)$
5	3	56	$<2,3,3>$
6	3	40	$<2,3,3>$
7	3	144	$<2,3,4>$
8	3	80	$<2,3,4>$
8	3	240	$<2,3,5>$
9	3	352	$<2,3,5>$
10	3	288	$<2,3,5>$
11	3	32	$<2,3,5>$
12	3	80	$<2,3,5>$
13	3	32	$<2,3,5>$

3. The algorithm terminates in Step 3 with $7 \leq l \leq 8$, and the resulting group has 48 elements and is isomorphic to the binary octahedral group $<2,3,4> := \{a, b, c | a^2 = b^3 = c^4 = abc\}$.
4. The algorithm terminates in Step 3 with $8 \leq l \leq 13$, and the resulting group has 120 elements and is isomorphic to the binary icosahedral group $<2,3,5> := \{a, b, c | a^2 = b^3 = c^5 = abc\}$.

To be more precise among all 10,560 exceptional triplets ϕ_1, ϕ_2, γ there are 4816 satisfying $|\cos \alpha| < 1$. The number of triplets ϕ_1, ϕ_2, γ that give termination of the algorithm for the length of the word equal to l and the resulting groups are presented in Table 1.

As a direct consequence we get the following theorem:

Theorem 6.3. *Assume $\mathcal{S} = \left\{ U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2) \right\} \subset SU(2)$. In order to verify universality of $\mathcal{S}$ it is enough to consider words of the length $l \leq 4$. Moreover, the algorithm terminates for $l \leq 13$. If it terminates in Step 1 the resulting group is either infinite or finite dicyclic group. If it terminates with $1 \leq l \leq 4$ the resulting group is $SU(2)$. For $l \geq 5$ it is binary tetrahedral or binary octahedral or binary icosahedral group.*

7. Universality of 2-mode Beamsplitters

In this section we address the universality problem of a single gate that belong to $SO(2)$ or $SU(2)$ and act on a d-dimensional space, where $d > 2$. More precisely, we consider the Hilbert space $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_d$, where $\mathcal{H}_k \simeq \mathbb{C}$, $d > 2$. Next we take a matrix $B \in SU(2)$ or $B \in SO(2)$. This matrix will be referred to as a 2-mode beamsplitter. We assume that we can permute *modes* and therefore we have access to matrices B and $B^\sigma = \sigma^t B \sigma$, where σ is the permutation matrix. Next, we define matrices B_{ij} or B_{ij}^σ to be the matrices that act on a two-dimensional subspace $\mathcal{H}_i \oplus \mathcal{H}_j \subset \mathcal{H}$ as B or B^σ, respectively,

and on the other components of $\mathcal{H}$ as the identity. This way we obtain the set of $2\binom{d}{2} = d(d-1)$ matrices $\mathcal{S}_d = \{B_{ij}, B^\sigma_{ij} : i < j, \ i, j \in \{1, \ldots, d\}\}$ in $SU(d)$ or $SO(d)$, respectively. Let us denote by $\mathcal{X}_d = \{b_{ij}, b^\sigma_{ij} : i < j, \ i, j \in \{1, \ldots, d\}\}$ the set of corresponding Lie algebra elements $B_{ij} = e^{b_{ij}}$, $B^\sigma_{ij} = e^{b^\sigma_{ij}}$ (constructed as in Sect. 4.1). Our goal is to find out when $\mathcal{S}_d$ is universal, i.e. when $\overline{< \mathcal{S}_d >} = SO(d)$ or $\overline{< \mathcal{S}_d >} = SU(d)$. In particular, we focus on showing, for which B the set $\mathcal{S}_3$ is universal. It is known that for such B also any set $\mathcal{S}_d$ with $d > 3$ will be universal (see [34,35] for two alternative proofs).

7.1. Spaces $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$ and $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3})$

In this section we characterise when $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ for both orthogonal and unitary beamsplitters. Our strategy is to first check when $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$. This can be done relatively easy. Then we use Facts 4.1 and 4.2 to find $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$.

7.1.1. The Case of Orthogonal Group. Let $B \in SO(2)$ be a rotation matrix by an angle $\phi \in (0, 2\pi)$. Making use of the notation introduced in Sect. 6 we have

$$\mathcal{S}_3 = \{B_{23}(\pm\phi), B_{13}(\pm\phi), B_{12}(\pm\phi)\}, \tag{7.1}$$

$$\mathcal{X}_3 = \{\pm\phi X_{23}, \pm\phi X_{13}, \pm\phi X_{12}\}, \tag{7.2}$$

where $B_{ij}(\pm\phi)$ correspond to the rotation matrices in three dimensions, i.e. $B_{12}(\phi) = O(\pm\phi, \vec{k}_z)$, $B_{13}(\phi) = O(\pm\phi, \vec{k}_y)$, and $B_{23}(\phi) = O(\pm\phi, \vec{k}_x)$, where $\vec{k}_x = [1, 0, 0]$, $\vec{k}_y = [0, 1, 0]$, $\vec{k}_z = [0, 0, 1]$ and matrices $X_{i,j}$ are defined by (4.5). Note that matrices belonging to $\mathcal{X}$ form a basis of the Lie algebra $\mathfrak{so}(3)$ iff $\phi \neq 0$. Therefore, by Corollary 3.3 we know that $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$. The adjoint matrices $\mathrm{Ad}_{O(\pm\phi, \vec{k}_i)}$ are again rotation matrices by angles $\pm\phi$ along axes $\vec{k}_i$. On the other hand, by Fact 4.2 we know that $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$ can be different than $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3})$ only if $\phi = \pm\pi$. Indeed, in this case the adjoint matrices $\mathrm{Ad}_{O(\pm\phi, \vec{k}_i)}$ commute. Summing up we have

Fact 7.1. *For a 2-mode orthogonal beamsplitter. If $\phi \neq 0$ then $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$. On the other hand, $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ iff $\phi \notin \{0, \pi\}$.*

7.1.2. The Case of Unitary Group. Let $B \in SU(2)$. Making use of the notation introduced in Sect. 6 we assume $B = U(\phi, \vec{k})$, $\phi \neq 0 \bmod \pi$, $\vec{k} = [k_x, k_y, k_z]$ and $k_x^2 + k_y^2 + k_z^2 = 1$. Therefore, we have:

$$\begin{aligned} \mathcal{X}_3 &= \{b_{ij}, b^\sigma_{ij} : 1 \le i < j \le 3\} = \phi \cdot \{k_x X_{ij} + k_y Y_{ij} + k_z Z_{ij}, \\ &\quad -k_x X_{ij} + k_y Y_{ij} - k_z Z_{ij} : 1 \le i < j \le 3\}, \end{aligned} \tag{7.3}$$

$$\begin{aligned} \mathcal{S}_3 &= \{B_{ij}, B^\sigma_{ij} : 1 \le i < j \le 3\} = \{I_{ij}(\phi) + \sin\phi(k_x X_{ij} + k_y Y_{ij} + k_z Z_{ij}), \\ &\quad I_{ij}(\phi) + \sin\phi(-k_x X_{ij} + k_y Y_{ij} - k_z Z_{ij}) : 1 \le i < j \le 3\}, \end{aligned} \tag{7.4}$$

where $I_{ij}(\phi) = \cos\phi(E_{ii} + E_{jj}) + E_{ll}$, $l \in \{1, 2, 3\}\backslash\{i, j\}$ and matrices $\{X_{ij}, Y_{ij}, Z_{ij}\}$ are defined as in (4.5). We start from finding $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3})$. To this end note that $[b_{ij}, b^\sigma_{ij}] = 4k_y(k_x Z_{ij} - k_z X_{ij})$. If $[b_{ij}, b^\sigma_{ij}] \neq 0$ then b_{ij} and b^σ_{ij} generate $\mathfrak{su}(2)_{ij}$. Thus, we have access to all elements X_{ij}, Y_{ij} and Z_{ij} $1 \le i < j \le 3$. Hence, $\mathcal{X}_3$ generates $\mathfrak{su}(3)$ and $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$. If in turn

$[b_{ij}, b_{ij}^{\sigma}] = 0$ then we need to consider four cases: (1) $k_y \neq 0$ and $k_x = 0 = k_z$, (2) $k_y = 0$ and $k_x \neq 0$ and $k_z \neq 0$, (3) $k_y = 0 = k_z$ and $k_x \neq 0$, (4) $k_y = 0 = k_x$ and $k_z \neq 0$.

1. In this case $b_{ij} = k_y Y_{ij} = b_{ij}^{\sigma}$; therefore, we have access to all $\{Y_{ij}\}_{i<j}$, $i, j \in \{1, 2, 3\}$. But by the commutation relations $[Y_{ij}, Y_{ik}] = -X_{jk}$, $[Y_{ij}, Y_{jk}] = -X_{ik}$, $[Y_{ij}, Y_{kj}] = -X_{ik}$ and $[X_{ij}, Y_{ij}] = 2Z_{ij}$. Thus, we can generate all basis elements of $\mathfrak{su}(3)$ starting from Y_{ij}'s. This means $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$.

2. In this case $b_{ij} = -b_{ij}^{\sigma}$. Direct calculations show that elements:

$$[b_{12}, [b_{12}, b_{13}]], \ [b_{12}, [b_{12}, b_{23}]], \ [b_{13}, [b_{13}, b_{12}]],$$
$$[b_{13}, [b_{13}, b_{23}]], \ [b_{23}, [b_{23}, b_{12}]], \ [b_{12}, [b_{12}, [b_{13}, b_{23}]]],$$
$$[b_{23}, [b_{13}, [b_{23}, b_{12}]]], \ [b_{13}, [b_{13}, [b_{23}, b_{12}]]],$$

form a basis of $\mathfrak{su}(3)$. Thus, $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$.

3. In this case the algebra generated by $\mathcal{X}_3$ is clearly $\mathfrak{so}(3)$. Hence, $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) \neq \{\lambda I\}$.

4. In this case the algebra generated by $\mathcal{X}_3$ is abelian. Hence, $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) \neq \{\lambda I\}$.

We have just shown:

Fact 7.2. *For a 2-mode unitary beamsplitter $B = I \cos\phi + \sin\phi(k_x X + k_y Y + k_z Z)$, where $k_x^2 + k_y^2 + k_z^2 = 1$ we have $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) = \{\lambda I\}$ unless (a) $k_y = 0 = k_z$ and $k_x = 1$, (b) $k_y = 0 = k_x$ and $k_z = 1$.*

Next we characterise $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$. The adjoint matrices $\mathrm{Ad}_{B_{ij}}$ and $\mathrm{Ad}_{B_{ij}^{\sigma}}$ are elements of $SO(\mathfrak{su}(3)) \simeq SO(8)$. The rotation angles of both $\mathrm{Ad}_{B_{ij}}$ and $\mathrm{Ad}_{B_{ij}^{\sigma}}$ are $\pm\phi$, 2ϕ and 0. On the other hand, by Fact 4.1 we know that $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$ can be different than $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3})$ only if the rotation angle is $\pm\pi$. This corresponds to situations when either $\phi = \pm\pi$ or $\phi = \pm\frac{\pi}{2}$. In the first case $B = -I$; thus, obviously $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) \neq \{\lambda I\}$. The case $\phi = \pm\frac{\pi}{2}$ corresponds to $\frac{\pi}{2} \cdot \mathcal{S}_3 = \mathcal{X}_3$.

Fact 7.3. *For a 2-mode unitary beamsplitter $B = I \cos\phi + \sin\phi(k_x X + k_y Y + k_z Z)$ we have $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ unless (a) $k_y = 0 = k_z$ and $k_x = 1$, (b) $k_y = 0 = k_x$ and $k_z = 1$, (c) $\phi = \pm\frac{\pi}{2}$ and $k_z = 0$.*

Proof. Recall that $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) \subseteq \mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$. Cases (a) and (b) correspond to situations when $\mathcal{C}(\mathrm{ad}_{\mathcal{X}_3}) \neq \{\lambda I\}$. Case (c) follows from direct calculations for six Ad_g matrices with $\phi = \pm\frac{\pi}{2}$ and $g \in \mathcal{S}_3$. They were done with the help of a symbolic calculation software. We only verify that when $\phi = \pm\frac{\pi}{2}$ and $k_z = 0$ indeed $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) \neq \{\lambda I\}$. Therefore, we define $\mathfrak{h} = \mathrm{Span}_{\mathbb{R}}\{Z_{12}, Z_{23}\}$, $\dim_{\mathbb{R}}\mathfrak{h} = 2$ and show that for $\phi = \pm\frac{\pi}{2}$ and $k_z = 0$ the space $\mathfrak{h}$ is an invariant subspace for matrices $\mathrm{Ad}_{B_{ij}}$ and $\mathrm{Ad}_{B_{ij}^{\sigma}}$, i.e. of $\mathcal{S}_3$. To this end we calculate

$$\mathrm{Ad}_{B_{12}} Z_{12} = -Z_{12}, \quad \mathrm{Ad}_{B_{13}} Z_{12} = -Z_{23}, \quad \mathrm{Ad}_{B_{23}} Z_{12} = Z_{12} + Z_{23}, \quad (7.5)$$

$$\mathrm{Ad}_{B_{12}} Z_{23} = Z_{23} + Z_{12}, \quad \mathrm{Ad}_{B_{13}} Z_{23} = -Z_{12}, \quad \mathrm{Ad}_{B_{23}} Z_{23} = -Z_{23}. \quad (7.6)$$

and $\mathrm{Ad}_{B_{ij}^{\sigma}} Z_{kl} = \mathrm{Ad}_{B_{ij}} Z_{kl}$. Therefore, the projection operator $P : \mathfrak{su}(3) \to \mathfrak{h}$ commutes with matrices from $\mathcal{S}_3$, and thus it belongs to $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$. $\square$

It is interesting to look at the structure of the group $\overline{<\mathcal{S}_3>}$ when $k_z = 0$ and $\phi = \frac{\pi}{2}$. Matrices are of the form $B_{ij} = e^{i\psi} E_{ij} - e^{-i\psi} E_{ji} + E_{kk}$ and $B_{ij}^{\sigma} = -e^{-i\psi} E_{ij} + e^{i\psi} E_{ji} + E_{kk}$, where $1 \leq i < j \leq 3$, $k \neq i, j$ and $\psi \in [0, 2\pi)$. If ψ is a rational multiple of π, then it is easy to see that $<\mathcal{S}_3>$ is a finite group and when ψ is an irrational multiple of π the group $\overline{<\mathcal{S}_3>}$ is infinite and disconnected. In fact, these are groups isomorphic to $\Delta(6n^2)$ and $\Delta(6\infty^2)$ given in [20].

7.2. When $\mathcal{S}_3$ is Universal?

Having characterised when $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ we check in this section when the group $<\mathcal{S}_3>$ is infinite and this way we get the full classification of universal 2-mode beamsplitters.

7.2.1. The Case of the Orthogonal Group.
Combining Theorem 4.12 with Fact 7.1 for $\phi \notin \mathcal{L}_{SO(3)}$ we obtain that the group generated by $\mathcal{S}_3$ is exactly $SO(3)$. When $\phi \in \mathcal{L}_{SO(3)}$ we consider the matrix: $O(\gamma, \vec{k}_{xz}) = O(\phi, \vec{k}_x) O(\phi, \vec{k}_z)$. The trace yields the following equation that relates γ and ϕ:

$$\cos \gamma = \frac{\cos^2 \phi + 2 \cos \phi - 1}{2}. \tag{7.7}$$

If $\phi = \frac{(2k+1)\pi}{2}$, where $k \in \mathbb{Z}$, then matrices $O(\phi, \vec{k}_x)$, $O(\phi, \vec{k}_y)$ and $O(\phi, \vec{k}_z)$ are permutation matrices and they form three-dimensional representation of S_3. For all remaining $\phi \in \mathcal{L}_{SO(3)}$ we calculate $\cos \gamma$ using (7.7) and compare it with the values of $\cos \alpha$ for all $\alpha \in \mathcal{L}_{SO(3)}$. We find out they never agree. Therefore, $\gamma \notin \mathcal{L}_{SO(3)}$, and we can apply Theorem 4.12 and Fact 7.1 to $U(\gamma, \vec{k}_{xz})$. Summing up:

Theorem 7.4. *Any 2-mode orthogonal beamsplitter with $\phi \notin \left\{ \frac{\pi}{2}, \frac{3\pi}{2} \right\}$ is universal on 3 and hence $n > 3$ modes.*

7.2.2. The Case of the Unitary Group.
Recall that by Fact 7.3 the space $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ if and only if all the entries of a matrix $B \in SU(2)$ are nonzero and at least one of them belongs to $\mathbb{C}$. So we are left with checking if under these assumptions $<\mathcal{S}_3>$ is infinite. Let $\{e^{i\phi}, e^{-i\phi}\}$ be the spectrum of B. Matrices B_{ij} and B_{ij}^{σ} have the same spectra $\{e^{i\phi}, e^{-i\phi}, 1\}$. Looking at the definitions of the open balls B_{α}, $\alpha^3 = 1$ we see that a matrix from $SU(3)$ with one spectral element equal to one can be introduced (by taking powers) only to the ball with $\alpha = 1$. Moreover, the maximal n that is needed is exactly the same as for $SO(3)$ and the exceptional angles belong to the set $\mathcal{L}_{SO(3)}$. Therefore, by Theorem 4.12, $\phi \notin \mathcal{L}_{SO(3)}$ implies that the group generated by, for example, B_{12} and B_{23} is infinite. In the following we show that $<\mathcal{S}_3>$ is infinite also for $\phi \in \mathcal{L}_{SO(3)}$ (providing ϕ is such that $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$).

Let us consider $<\mathcal{R}> = <B_{12}(\phi), B_{23}(\phi)>$ with $\phi \in \mathcal{L}_{SO(3)}$. Our goal is to show that $\mathcal{R} \subset \mathcal{S}_3$ generates an infinite group. To this end we use the following procedure:

1. We calculate trace of the product $B_{12}(\phi)B_{23}(\phi)$ and note that it belongs to $\mathbb{R}$. Therefore, spectrum of $B_{12}(\phi)B_{23}(\phi)$ is of the form $\{e^{i\gamma}, e^{-i\gamma}, 1\}$, where the relation between ϕ and γ is given by

$$\operatorname{tr} B_{12}(\phi)B_{23}(\phi) = 2\cos\phi + \cos^2\phi + k_z^2 \sin^2\phi = 2\cos\gamma + 1. \qquad (7.8)$$

2. Using (7.8), for each $\gamma \in \mathcal{L}_{SO(3)}$ we compute

$$k_z^2 = \frac{2\cos\gamma + 1 - 2\cos\phi - \cos^2\phi}{\sin^2\phi}, \qquad (7.9)$$

and check whether $0 < k_z^2 < 1$. The pairs (ϕ, γ) that fail this test are excluded from the further considerations. We note that $k_z^2 = 1$ corresponds to diagonal matrices $B_{12}(\phi), B_{23}(\phi)$ and $k_z^2 = 0$ corresponds the situation when $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3}) \neq \{\lambda I\}$.

3. For the pairs (ϕ, γ) that give $0 < k_z^2 < 1$ we consider the matrix $U(\gamma') = B_{12}(2\phi)B_{23}(2\phi)$. Its trace is again real, and we get

$$\operatorname{tr} B_{12}(2\phi)B_{23}(2\phi) = \frac{1}{2}\left(2 + 4\cos(2\phi) + \left(1 - k_z^2\right)(\cos(4\phi) - 1)\right) = 2\cos\gamma' + 1, \qquad (7.10)$$

where k_z^2 is determined by ϕ and γ. Direct computations show that $\gamma' \notin \mathcal{L}_{SO(3)}$ if $\phi \notin \left\{\pm\frac{\pi}{2}, \pm\frac{2\pi}{3}\right\}$. We treat both of these cases separately.

4. For $\phi = \pm\frac{2\pi}{3}$ and the fixed k_z^2 we consider yet another product of matrices $U(\gamma'') = B_{23}^2(\phi)B_{12}^2(\phi)B_{23}(\phi)B_{12}(\phi)$ with a real trace:

$$\operatorname{tr} B_{23}^2(\phi)B_{12}^2(\phi)B_{23}(\phi)B_{12}(\phi)$$
$$= \frac{1}{8}\left(\cos\phi + 3\cos(2\phi) + 4\cos(3\phi) + 6\cos(4\phi) + 4\cos(5\phi) + \cos(6\phi) - 2\right)$$
$$+32k_z^4 \sin^4\phi\cos^2\phi + 8k_z^2 \sin^2\phi\left(-2\cos\phi + 4\cos(2\phi) + 2\cos(3\phi) + \cos(4\phi) + 4\right)$$
$$= 2\cos\gamma''. \qquad (7.11)$$

Direct computations show that $\gamma'' \notin \mathcal{L}_{SO(3)}$; thus, we are done for $\phi \in \mathcal{L}_{SO(3)} \setminus \left\{\frac{\pi}{2}, -\frac{\pi}{2}\right\}$. The same composition for $U_{23}\left(\frac{\pi}{2}\right), U_{12}\left(\frac{\pi}{2}\right)$ may give a matrix of the spectral angle $\gamma = \pm\frac{2\pi}{3}$.

For $\phi = \pm\frac{\pi}{2}$ an additional treatment is needed. It consists of three steps:

1. Assume $B_{ij}\left(\frac{\pi}{2}\right)$ does not commute with its permutations $B_{ij}^\sigma(\frac{\pi}{2})$ for $1 \leq i < j \leq 3$. In this case we can use $B_{ij}(\gamma) = B_{ij}\left(\frac{\pi}{2}\right)B_{ij}^\sigma\left(\frac{\pi}{2}\right), 1 \leq i < j \leq 3$ as the new set of generators. Note that the angle γ depends on the trace of $B_{ij}\left(\frac{\pi}{2}\right)B_{ij}^\sigma\left(\frac{\pi}{2}\right)$ as $\cos\gamma = 1 - 2k_y^2$. Thus, $\gamma \neq \pm\frac{\pi}{2}$ if $k_y^2 \neq \frac{1}{2}$ and then we can apply the previous procedure to show that $<B_{12}(\gamma), B_{23}(\gamma)>$ is infinite.

2. For $\phi = \pm\frac{\pi}{2}$ and $k_y^2 = \frac{1}{2}$, $k_x^2 + k_z^2 = \frac{1}{2}$ we consider yet another product

$$\operatorname{tr} B_{12}^2\left(\frac{\pi}{2}\right)B_{13}\left(\frac{\pi}{2}\right)B_{23}\left(\frac{\pi}{2}\right)B_{13}^2\left(\frac{\pi}{2}\right) = k_z^2 = 2\cos\gamma'''$$

We find out that the only $\gamma \in \mathcal{L}_{SO(3)}$ satisfying $2\cos\gamma = k_z^2 - 1$ for $0 \leq k_z^2 \leq \frac{1}{2}$ are $\gamma = \pm\frac{2\pi}{3}$. But then $k_z^2 = 0$. Thus, by Fact 7.3 the space $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}_3})$ is larger than $\{\lambda I\}$.

3. Finally, we assume that matrices $B_{ij}\left(\frac{\pi}{2}\right)$ commute with their permutations. Recall that it happens if either $k_y = \pm 1$ and $k_x = k_z = 0$ or $k_y = 0$ and $k_x, k_z \neq 0$. The group generated for $k_y = \pm 1$ is, of course, finite. Therefore, we need to consider only the case when $k_y = 0$ and $k_x, k_z \neq 0$. But in this case Step 2 of the previous procedure is never satisfied (from Eq. (7.9) one can only obtain $k_z^2 = 0$ for $\gamma = \pm\frac{2\pi}{3}$).

Summing up:

Theorem 7.5. *Any 2-mode unitary gate such that all its entries are nonzero and at least one of them is a complex number is universal on 3 and hence $n > 3$ modes.*

Acknowledgements

References

[1] Albertini, F., D'Alessandro, D.: Notions of controllability for bilinear multilevel quantum systems. IEEE Trans. Automat. Contr. **48**, 1399–1403 (2003)

[2] Babai, L.: Deciding finiteness of matrix groups in Las Vegas polynomial time. In: Proceedings of the Third Annual ACM SIAM Symposium on Discrete Algorithms (Orlando, FL, 1992), pp. 33–40. ACM, New York (1992)

[3] Babai, L., Beals, R., Rockmore, D.N.: Deciding finiteness of matrix groups in deterministic polynomial time. In: Proceedings of International Symposium on Symbolic and Algebraic Computation, ISSAC-93, pp. 117–126. ACM Press (1993)

[4] Barenco, A., et al.: Elementary gates for quantum computation. Phys. Rev. A **52**, 3457–3467 (1995)

[5] Bourgain, J., Gamburd, A.: A spectral gap theorem in SU(d). J. Eur. Math. Soc. **014**(5), 1455–1511 (2012)

[6] Bourgain, J., Gamburd, A.: On the spectral gap for finitely-generated subgroups of SU(2). Invent. Math. **171**(1), 83–121 (2008)

[7] Böttcher, A., Wenzel, D.: The Frobenius norm and the commutator. Linear Algebra Appl. **429**, 1864–1885 (2008)

[8] Bouland, A., Aaronson, S.: Generation of universal linear optics by any beam splitter. Phys. Rev. A **89**, 062316 (2014)

[9] Bromberg, Y., et al.: Quantum and classical correlations in waveguide lattices. Phys. Rev. Lett. **102**, 253904 (2009)

[10] Bröcker, T., tom Dieck, T.: Representations of Compact Lie Groups. Springer, New York (1985)

[11] Brockett, R.W.: System theory on group manifolds and coset spaces. SIAM J. Control **10**(2), 265–284 (1972)

[12] Bryliński, R., Chen, G.: Mathematics of Quantum Computation. Chapman and Hall/CRC Press, Boca Raton, FL (2002)

[13] Cartan, E.: La théorie des groupes finis et continus et l'Analysis Situs. Mémorial Sci. Math. **XLII**, 1–6 (1930)

[14] Childs, A.M., et al.: Characterization of universal two-qubit Hamiltonians. Quantum Inf. Comput. **11**, 19–39 (2011)

[15] Curtis, W., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Interscience Publishers, John Wiley and Sons, New York (1962)

[16] Cusick, T.W.: Dirichlet's diophantine approximation theorem. Bull. Aust. Math. Soc. **16**, 219–224 (1977)

[17] Derksen, H., Jeandel, E., Koiran, P.: Quantum automata and algebraic groups. J. Symb. Comput. **39**, 357–371 (2005)

[18] Detinko, A.S., Flannery, D.L.: On deciding finiteness of matrix groups. J. Symb. Comput. **44**, 1037–1043 (2009)

[19] Deutsch, D., Barenco, A., Ekert, A.: Universality in quantum computation. Proc. R. Soc. Lond. A **425**, 73–90 (1989)

[20] Fairbarn, W.M., Fulton, T., Klink, W.H.: Finite and disconnected subgroups of $SU(3)$ and their application to the elementary-particle spectrum. J. Math. Phys. **5**, 1038–1051 (1964)

[21] Field, M.: Generating sets for compact semisimple Lie groups. Proc. Am. Math. Soc. **127**, 3361–3365 (1999)

[22] Freedman, M.H., Kitaev, A., Lurie, J.: Diameters of homogeneous spaces. Math. Res. Lett. **10**, 11 (2003)

[23] Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Clarendon Press, Oxford (1960)

[24] Harrow, A.W., Recht, B., Chuang, I.L.: Efficient discrete approximations of quantum gates. J. Math. Phys. **43**(9), 4445–4451 (2002)

[25] Jeandel, E.: Universality in quantum computation. In: Díaz, J., Karhumäki, J., Lepistö, A., Sannella, D. (eds) Automata, Languages and Programming, ICALP 2004, Lecture Notes in Computer Science, vol. 3142. Springer (2004)

[26] Jurdjevic, V., Sussmann, H.: Control systems on Lie groups. J. Differ. Equ. **12**, 313–329 (1972)

[27] Kuranishi, M.: On everywhere dense imbedding of free groups in Lie groups. Nagoya Math. J. **2**, 63–71 (1951)

[28] Lloyd, S.: Almost any quantum logic gate is universal. Phys. Rev. Lett. **75**, 2 (1995)

[29] Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

[30] Oszmaniec, M., Gutt, J.A., Kuś, M.: Classical simulation of fermionic linear optics augmented with noisy ancillas. Phys. Rev. A **90**, 020302 (2014)

[31] Oszmaniec, M., et al.: Random bosonic states for robust quantum metrology. Phys. Rev. X **6**, 041044 (2016)

[32] Oszmaniec, M., Zimobrás, Z.: Universal extensions of restricted classes of quantum operations. arXiv:1705.11188 (2017)

[33] Politi, A., et al.: Silica-on-silicon waveguide quantum circuits. Science **320**, 646–649 (2008)

[34] Reck, M., et al.: Experimental realization of any discrete unitary operator. Phys. Rev. Lett. **73**, 58–61 (1994)

[35] Sawicki, A.: Universality of beamsplitters. Quantum Inf. Comput. **16**, 291–312 (2016)

[36] Schirmer, S.G., Fu, H., Solomon, A.I.: Complete controllability of quantum systems. Phys. Rev. A **63**, 063410 (2001)

[37] Schuch, N., Siewert, J.: Natural two-qubit gate for quantum computation using the XY interaction. Phys. Rev. A **67**, 032301 (2003)

[38] Sugiura, M.: Unitary representations and harmonic analysis, 2nd edn. North-Holland Mathematical Library, Amsterdam (1990)

[39] Zeier, R., Schulte-Herbrüggen, T.: Symmetry principles in quantum systems theory. J. Math. Phys. **52**, 113510 (2011)

[40] Zeier, R., Zimborás, Z.: On squares of representations of compact Lie algebras. J. Math. Phys. **56**, 081702 (2015)

[41] Zimborás, Z., et al.: Symmetry criteria for quantum simulability of effective interactions. Phys. Rev. A **92**, 042309 (2015)

Adam Sawicki and Katarzyna Karnas
Center for Theoretical Physics PAS
Al. Lotników 32/46
02-668 Warsaw
Poland
e-mail:a.sawicki@cft.edu.pl

Katarzyna Karnas
e-mail:karnas@cft.edu.pl