Generating sets for $SO(d)$, $SU(d)$

Katarzyna Karnas
Joint work with Adam Sawicki

Center for Theoretical Physics PAS

September 30, 2016

Outline

1. Introduction
2. Problem formulation and possible applications
3. Conditions for generating infinite groups
4. Maximal power N_G
5. Conditions for being dense in a Lie group G
6. Results for $SU(2)$, $SU(3)$, $SO(3)$
7. Summmary

Lie groups, Lie algebras and representation theory

- Lie algebra $\mathfrak{g}$ is simple if it has no nontrivial ideals and semisimple if it is a direct sum of simple ideals.

$$\mathfrak{g} = \mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_k.$$

- G is simple if its Lie algebra is simple. The groups $G = SU(d)$, $G = SO(d)$ are simple except $G = SO(4)$.
- Adjoint representation of G and $\mathfrak{g}$:

$$\mathrm{Ad} : G \to SO(\mathfrak{g}),\ \mathrm{Ad}_g X = gXg^{-1},\ X \in \mathfrak{g},$$
$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{so}(\mathfrak{g}),\ \mathrm{ad}_X(Y) = [X, Y],\ X, Y \in \mathfrak{g}$$

- Adjoint representations of simple Lie algebras and simple Lie groups are irreducible. By Schur lemma:

$$\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall X \in \mathfrak{g}\ [\mathrm{ad}_X, L] = 0\} = \{\lambda I\}$$
$$\mathcal{C}(\mathrm{Ad}_G) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall g \in G\ [\mathrm{Ad}_g, L] = 0\} = \{\lambda I\}$$

- When G compact and connected, then $\exp : \mathfrak{g} \to G$ is onto. For every $g \in G$ there is $X \in \mathfrak{g}$ such that $g = \exp(X)$.

Problem formulation

$\mathcal{S} = \{g_1, \ldots, g_n\} \subset G$, where $G = SU(d)$ or $G = SO(d)$.

$< \mathcal{S} >= G$ if every $g \in G$ can be represented as $g = \prod^{N<\infty} g_{i_j}^{n_{i_j}}$, $g_{i_j} \in \mathcal{S}$

- $< \mathcal{S} >$ is infinite
- $\overline{< \mathcal{S} >}$ is dense in G

Theorems (Kuranishi, da Silva-Leite) [5]

(1) Let $\mathfrak{g}$ be a semisimple Lie algebra over $\mathbb{C}$. Then there exist $x, y \in \mathfrak{g}$ s.t. the minimal subalgebra containing x and y is $\mathfrak{g}$.
(2) Let $\mathfrak{t}'$ be a compact real form of a semisimple Lie algebra over $\mathbb{C}$. Then there exist $x, y \in \mathfrak{t}$ s.t. the minimal subalgebra containing x and y is $\mathfrak{t}$.

Theorem 3 (Kuranishi, Field) [5, 4]

Let G be a connected semisimple Lie group. Then there exist the set of pairs $(g, h) \in G$ s.t. the minimal closed subgroup containing g and h is Zariski dense in $G \times G$.

Possible applications in physics

- Lie algebras: control systems

$$\dot{X}(t) = \left(H + \sum_i u_i(t) H_i \right) X(t)$$

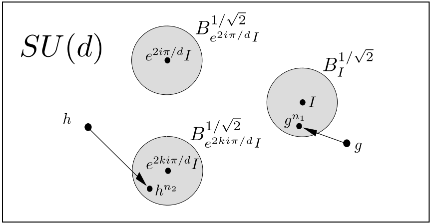
$X(t) \in \mathbb{C}^n$ -state, $H, H_i \in \mathfrak{g}$ - Hamiltonians, $u_i(t) \in \mathbb{R}$ - control amplitudes.

- Lie groups: quantum optics
  - $g \in SU(2)$ - quantum gate acting on a single qubit
  - $g \in \underbrace{SU(2) \otimes \ldots \otimes SU(2)}_{k}$ - gate acting on a system of k qubits separately
  - $g \in SU(2^k)$ - gate acting on a system of k qubits, entangling allowed
  - $g \in SU(d)$ - quantum gate acting on a single qudit (d-state system)

Generating infinite groups

Let $[g,h]_\bullet = ghg^{-1}h^{-1}$ and $\|g\| = \sqrt{\mathrm{tr}(gg^*)}$. Then [2]

$$\|[g,h]_\bullet - I\| \leq \sqrt{2}\|g - I\|\|h - I\|,$$
$$\text{If } [g,[g,h]_\bullet]_\bullet = I \text{ and } \|h - I\| < 2, \text{ then } [g,h]_\bullet = I.$$



Lemma (Sawicki, K.)

Let $g \in B^{1/\sqrt{2}}_{e^{i\theta_m}I}$ and $h \in B^{1/\sqrt{2}}_{e^{i\theta_n}I}$ and assume $[g,h] \notin Z(G)$. The group $< g, h >$ generated by g, h is infinite.

Explicit conditions for $g \in B^{1/\sqrt{2}}_{e^{i\theta_m} I}$

The condition $\|g - e^{i\theta_m} I\| < \frac{1}{\sqrt{2}}$ can be transformed to the form
$\|g - e^{i\theta_m} I\|^2 < \frac{1}{2} \Rightarrow \mathrm{tr}(g - e^{i\theta_m} I)(g^* - e^{-i\theta_m} I) = 2\mathrm{tr} I - e^{-i\theta_m}\mathrm{tr} g - e^{i\theta_m}\mathrm{tr} g^* < \frac{1}{2}$.

- Let $\{e^{i\phi_1}, e^{i\phi_2}, \ldots, e^{i\phi_d}\}$ be the spectrum of $g \in SU(d)$.

$$g \in B_{e^{i\theta_m} I} \Leftrightarrow \sum_{i=1}^{d} \sin^2 \frac{\phi_i - \theta_m}{2} < \frac{1}{8}, \quad \sum_{i=1}^{d} \phi_i = 0 \bmod 2\pi.$$

- Let $\{1, e^{i\phi_1}, e^{-i\phi_1}, \ldots, e^{i\phi_k}, e^{-i\phi_k}\}$, $k = \lfloor \frac{d}{2} \rfloor$ be the spectrum of $g \in SO(d)$.

$$g \in B^{1/\sqrt{2}}_{I} \Leftrightarrow \sum_{i=1}^{k} \sin^2 \frac{\phi_i}{2} < \frac{1}{16},$$

$$g \in B^{1/\sqrt{2}}_{-I} \Leftrightarrow \sum_{i=1}^{k} \sin^2 \frac{\phi_i - \pi}{2} < \frac{1}{16} \ - \text{ only if } d \ - \text{ even}.$$

Maximal power N_G

Maximal power

For groups $G = SU(d)$ and $G = SO(d)$ there is $N_G \in \mathbb{N}$ such that for every $g \in G$, $g^n \in B^{1/\sqrt{2}}_{\alpha_m I}$ for some $e^{i\theta_m} I \in Z(G)$ and $1 \leq n \leq N_G$.

Proof: By Dirichlet approximation theorem and its modification

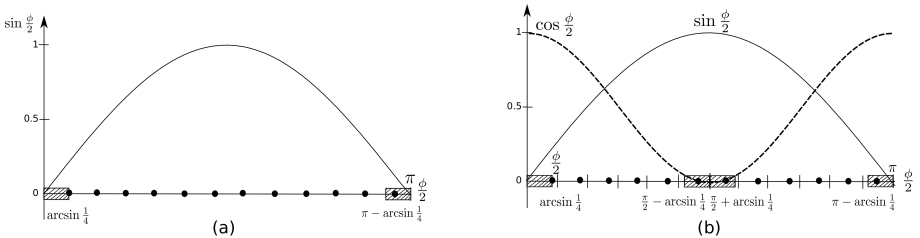
Dirichlet approximation theorem 1

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

Dirichlet approximation theorem 2 (modification required [1])

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

Example: $SO(3)$ and $SU(2)$



$$N_{SO(3)} = \lceil \frac{\pi - \arcsin \frac{1}{4}}{\arcsin \frac{1}{4}} \rceil = 12, \quad N_{SU(2)} = \lceil \frac{\pi/2 - \arcsin \frac{1}{4}}{\arcsin \frac{1}{4}} \rceil = 12$$

General case:

$$N_{SO(d)} < \lceil \left(\frac{1}{2}\right)_{d-even} \left(\frac{\pi}{\arcsin \frac{1}{4\sqrt{k}}}\right)^k \rceil, \qquad N_{SU(d)} < \lceil \frac{1}{d} \left(\frac{2\pi}{\beta_d}\right)^{d-1} \rceil$$

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

Exceptional spectra of Ad_g

Definition

Assume $g \notin B_{\alpha I}^{1/\sqrt{2}}$ for any $\alpha I \in Z(G)$. A spectral angle ϕ of Ad_g is called an **exceptional angle** iff

1. $\phi \neq 0 \, mod \, \pi$ and there is $n \in \{2, \ldots, N_G\}$ such that $n\phi = 0 \, mod \, \pi$ and $g^n \in B_{\alpha I}^{1/\sqrt{2}}$, or
2. $\phi = (2k+1)\pi$ and there is $n \in \{2, \ldots, N_G\}$ such that $n\phi = 0 \, mod \, 2\pi$ and $g^n \in B_{\alpha I}^{1/\sqrt{2}}$

An exceptional matrix g satisfies $[g^n, h^m]_{\bullet} \in Z(G)$ for some $n, m \in \mathbb{N}$.

- There is $1:1$ correspondence between spectra of Ad_g and g, $g \in SO(d)$
- There is $d-1:1$ correspondence between spectra of Ad_g and g, $g \in SU(d)$

When does infinite $\overline{< \mathcal{S} >}$ is equal to G?

For $\mathfrak{g} = \mathfrak{su}(d), \mathfrak{so}(d)$, $\mathrm{ad}_{\mathfrak{g}}$ is an irreducible representation. By **Schur lemma**

$$\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall x \in \mathfrak{g}\ [\mathrm{ad}_x, L] = 0\} = \{\lambda I\}$$

Let $\mathcal{X} = \{x_1, \ldots, x_k\}$ and $\mathcal{S} = \{g_1, \ldots, g_k\}$, where $g_i = e^{x_i}$. We define

$$\mathcal{C}(\mathrm{ad}_{\mathcal{X}}) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall x_i \in \mathcal{X}\ [\mathrm{ad}_{x_i}, L] = 0\} = \{\lambda I\}$$
$$\mathcal{C}(\mathrm{Ad}_{\mathcal{S}}) = \{L \in \mathrm{End}(\mathfrak{g}) : \forall g_i \in \mathcal{S}\ [\mathrm{Ad}_{g_i}, L] = 0\} = \{\lambda I\}$$

$\mathcal{C}(\mathrm{ad}_{\mathcal{X}}) \subset \mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$. They can differ iff some spectral angles of elements in $\mathrm{Ad}_{\mathcal{S}}$ are $\pm\pi$.

Theorem 1

$\mathcal{X}$ - finite subset of a compact semisimple Lie algebra such that the projection of $\mathcal{X}$ onto every simple component of $\mathfrak{g}$ is nonzero. $< \mathcal{X} >= \mathfrak{g}$ iff $\mathcal{C}(\mathrm{ad}_{\mathfrak{g}}) = \mathcal{C}(\mathrm{ad}_{\mathcal{X}})$.

Theorem 2

$\mathcal{S}$ - finite subset of a compact connected semisimple Lie group G such that $< \mathcal{S} >$ is infinite and the projection of $\mathcal{S}$ onto every simple component of G is also infinite. $< \mathcal{S} >= G$ if and only if $\mathcal{C}(\mathrm{Ad}_G) = \mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$.

Results for $G = SU(2)$

- List of exceptional angles $\mathcal{L}_{SU(2)} = \{0, \pi, \pm\frac{\pi}{2}, \frac{k\pi}{3}, \frac{k\pi}{4}, \frac{k\pi}{5}, \frac{k\pi}{6}\}$
- Let $\mathcal{X} = \{x_1, x_2\}$ where $x_1 = k_x X + k_y Y + k_z Z$ and $x_2 = -k_x X + k_y Y - k_z Z$
- Let $\mathcal{S} = \{g(\phi_1, \vec{k}_1), g(\phi_2, \vec{k}_2)\}$ where $g(\phi_1, \vec{k}_1) = e^{\phi_1 x_1}$ and $g(\phi_2, \vec{k}_2) = e^{\phi_2 x_2}$. By Cayley-Hamilton theorem

$$g(\phi_1, \vec{k}_1) = I \cos\phi_1 + (k_x X + k_y Y + k_z Z)\sin\phi_1,$$
$$g(\phi_2, \vec{k}_2) = I \cos\phi_2 + (-k_x X + k_y Y - k_z Z)\sin\phi_2$$

- $< \mathcal{S} >$ not infinite if $\phi_1, \phi_2 \in \mathcal{L}_{SU(2)}$ and $\vec{k}_1, \vec{k}_2$ are symmetry axes of Platonic polyhedrons
- $\mathcal{C}(\mathrm{Ad}_{\mathcal{S}})$ is larger than $\{\lambda I\}$ if $g(\phi_1, \vec{k}_1), g(\phi_2, \vec{k}_2)$ either commute or anticommute

Universal sets for $SU(d)$, $d > 2$

$\mathcal{S}_{SU(2)} = \{g(\phi, \vec{k}),\ \sigma^t g(\phi, \vec{k})\sigma\}$, where σ - permutation matrix
We embed $g(\phi, \vec{k})$ and $\sigma^t g(\phi, \vec{k})\sigma$ into matrices from $SU(d)$, e.g.

$$g_{12}(\phi) = \begin{pmatrix} I\cos\phi + ik_z\sin\phi & (k_x + ik_y)\sin\phi & 0 \\ (-k_x + ik_y)\sin\phi & I\cos\phi - ik_z\sin\phi & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ etc.}$$

For which $\phi, \vec{k}$ the set $< \mathcal{S} >$ is a generating set?

1. $\phi \notin \{0, \pm\pi, \pm\frac{\pi}{2}\}$ and $\vec{k} \neq \vec{k}_z$ nor $\vec{k} \neq \vec{k}_x$
2. **Any 2-mode orthogonal beamsplitter with $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$ is universal on 3 and hence $n > 3$ modes.**
3. **Any 2-mode unitary gate whose all entries are nonzero and at least one of them is a complex number is universal on 3 and hence $n > 3$ modes.**

Summary

- Upper bound of N_G
- Definition of exceptional spectra
- Criterion using adjoint representation for deciding if $< g, h >$ is dense in G
- Explicit conditions for 2-element generating sets $\mathcal{S} \subset SU(2), SO(3), SU(3)$ to be generating (universal) sets
- *All* the pairs of generators of finite $SU(2)$ subgroups listed
- Non-generating sets in $SU(2)$ and $S0(2)$ become generating in almost all cases after embedding into $SU(d)$ and $SO(d)$ respectively, $d \geq 3$

References

- A. Sawicki, K. Karnas *Universality of single qudit gates*, arXiv:1609.05780
- W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras* (Interscience Publishers, John Wiley and sons, 1962)
- T. W. Cusick, *Dirichlet's diophantine approximation theorem*, B. Aust. Math. Soc. 16 (1977), 219 - 224
- M. Field, *Generating Sets for compact semisimple Lie Groups*, Proc. Amer. Math. Soc. 127 (1999), 3361-3365
- M. Kuranishi, *On everywhere dense imbedding of free groups in Lie groups*, Nagoya Mathematical J. 2, (1951), 63-71
- M.Reck *et al.*, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. 73 (1994), 58-61