ELSEVIER

Systems & Control Letters 47 (2002) 87–90

SYSTEMS & CONTROL LETTERS

www.elsevier.com/locate/sysconle

Uniform finite generation of compact Lie groups

Domenico D'Alessandro *

Department of Mathematics, Iowa State University, Ames, IA 50011, USA

Received 15 February 2001; received in revised form 11 April 2002; accepted 15 April 2002

Abstract

Consider a compact connected Lie group G and the corresponding Lie algebra $\mathscr{L}$. Let $\{X_1,\dots,X_m\}$ be a set of generators for the Lie algebra $\mathscr{L}$. We prove that G is uniformly finitely generated by $\{X_1,\dots,X_m\}$. This means that every element $K\in G$ can be expressed as $K=e^{Xt_1}e^{Xt_2}\cdots e^{Xt_l}$, where the indeterminates X are in the set $\{X_1,\dots,X_m\}$, $t_i\in\mathbb{R}$, $i=1,\dots,l$, and the number l is uniformly bounded. This extends a previous result by F. Lowenthal in that we do not require the connected one dimensional Lie subgroups corresponding to the X_i, $i=1,\dots,m$, to be compact. We link the results to the existence of universal logic gates in quantum computing and discuss the impact on bang bang control algorithms for quantum mechanical systems. © 2002 Elsevier Science B.V. All rights reserved.

Keywords: Lie groups; Uniform generation; Universal quantum logic gates

1. Introduction

Let G be a connected Lie group and $\mathscr{L}$ the corresponding Lie algebra and let $\{X_1,\dots,X_m\}$ be a set of generators for $\mathscr{L}$. In their classical paper on controllability of systems on Lie groups [4], Jurdjevic and Sussmann proved that any element K in G can be written as

$$K=e^{Xt_1}e^{Xt_2}\cdots e^{Xt_l}, \qquad (1)$$

where the indeterminates X's are in the set $\{X_1,\dots,X_m\}$ and $t_1,\dots,t_l\in\mathbb{R}$ (see Lemma 6.2 in [4]). The number l called *order of generation* depends on K. Lowenthal called the Lie group G *uniformly finitely generated* by $\{X_1,\dots,X_m\}$ if every element $K\in G$ can be written in the form (1) with l *uniformly bounded* and described a number of Lie groups that are uniformly finitely generated by every set of generators of the corresponding Lie algebra (see [6–8] and references therein). Lowenthal also showed in [10] that, if G is compact and the one dimensional connected Lie subgroups of G corresponding to $\{X_1,X_2,\dots,X_m\}$ are also compact, then the Lie group G is uniformly finitely generated by $\{X_1,X_2,\dots,X_m\}$. The aim of this note is to extend this result by relaxing the assumption of compactness of the one dimensional connected Lie groups corresponding to $\{X_1,\dots,X_m\}$. We also discuss in Section 4 the implications of the uniform finite generation result in the problem of characterizing universal quantum logic gates and in algorithms for quantum control. We refer to [1,13,14] for more discussion and results on the uniform generation problem.

2. Uniform finite generation of compact Lie groups

Consider the set of linearly independent generators of $\mathscr{L}$, $\mathscr{S}:=\{X_1,\dots,X_m\}$, we have the following lemma.

* Tel.: +1-515-294-8130.
E-mail address: daless@iastate.edu (D. D'Alessandro).

PII: S0167-6911(02)00178-0

Lemma 1. *There exists a neighborhood N of the identity in G such that every element K in N can be written as*

$$K := e^{Xt_1} e^{Xt_2} \cdots e^{Xt_l}. \tag{2}$$

The indeterminates X are in the set $\mathscr{S}$, $t_j \in \mathbb{R}$, $j = 1,\dots,l$, and

$$l \leqslant n + 2\sum_{k=1}^{n-m} r_k. \tag{3}$$

The sequence r_k, $k = 1,\dots,n-m$, is defined by the recursive rule

$$r_1 = 1, \quad r_2 = 2, \quad r_k = 2r_{k-2} + r_{k-1} + 1. \tag{4}$$

Proof. First notice that, if $\{X_1,X_2,\dots,X_n\}$ is a basis for $\mathscr{L}$, a neighborhood of the identity in G can be obtained by varying $t_1,\dots,t_n$ in a neighborhood of the origin in $\mathbb{R}^n$ in the expression

$$K := e^{X_1t_1} e^{X_2t_2} \cdots e^{X_nt_n}. \tag{5}$$

This follows from the Inverse Function Theorem (see e.g. [15, Lemma 3.1, Chapter 5] for a statement of this result)

We now show how to generate a basis of $\mathscr{L}$ by using similarity transformations involving only the elements in the set $\mathscr{S}$.

There exist two elements X_k,X_i and a (arbitrarily small) time $\tilde{t}$ such that $e^{X_k\tilde{t}}X_ie^{-X_k\tilde{t}}$ is linearly independent from $X_1,....,X_m$. If this was not the case, we would have

$$e^{X_kt}X_ie^{-X_kt} = \sum_{s=1}^{m} a_s(t)X_s \tag{6}$$

for some functions $a_s(t)$ and for every t. Differentiating (6) at $t = 0$, we obtain

$$[X_k,X_i] = \sum_{s=1}^{m} \dot{a}_s(0)X_s \tag{7}$$

for every $k,i = 1,2,\dots,m$ which (if $\dim(\mathscr{L}) > m$) contradicts the fact that $X_1,\dots,X_m$ are generators of $\mathscr{L}$. Set

$$X_{m+1} := e^{X_k\tilde{t}}X_ie^{-X_k\tilde{t}}. \tag{8}$$

Of course, $X_1,\dots,X_{m+1}$ are still a set of linearly independent generators and therefore, as above, there exist two elements $X_k,\bar{X}_i$ in the set $\{X_1,\dots,X_m,X_{m+1}\}$ and a (arbitrarily small) time $\tilde{t}$ such that $e^{X_k\tilde{t}}X_ie^{-X_k\tilde{t}}$ is linearly independent from $X_1,\dots,X_{m+1}$. As in (8), we obtain a new element of $\mathscr{L}$ that we call X_{m+2}, such that $\{X_1,X_2,\dots,X_{m+2}\}$ is an $(m+2)$-dimensional subspace of $\mathscr{L}$. Proceeding this way we obtain a basis $X_1,\dots,X_m,X_{m+1},\dots,X_n$ of the Lie algebra $\mathscr{L}$ where the first m elements are the generators we started with and the elements $X_{m+1},\dots,X_n$ are obtained via similarity transformations with the iterative procedure we have described. Every element X_i, $i = 1,\dots,n$ can be written in the form

$$X_i = e^{\bar{X}_rt_r}e^{\bar{X}_{r-1}t_{r-1}} \cdots e^{\bar{X}_1t_1} \\ \times X_ke^{-\bar{X}_1t_1} \cdots e^{-\bar{X}_{r-1}t_{r-1}}e^{-\bar{X}_rt_r}, \tag{9}$$

where the indeterminates $\bar{X}_1,\dots,\bar{X}_r$ belong to $\mathscr{S}$ and the (worst case) number of factors r depends on the step we are considering. At the first step $r = 1$. At the second step the worst situation is when the linearly independent element X_{m+2} is obtained as $e^{X_i\tilde{t}}X_{m+1}e^{-X_i\tilde{t}}$, with $X_i \in \mathscr{S}$, in which case $r = 2$. From this point on the worst situation happens when the element X_{m+k} is obtained as $e^{X_{m+k-2}\tilde{t}}X_{m+k-1}e^{-X_{m+k-2}\tilde{t}}$. The number r for the kth step, r_k, can be obtained by setting $r_1 = 1$, $r_2 = 2$, $r_k = 2r_{k-2} + 1 + r_{k-1}$.[1]

Replacing now in (5) the expressions of e^{X_jt}, $j = 1,\dots,n$ in terms of the matrices in $\mathscr{S}$ we obtain an expression of the form (2). The exponentials of $X_1,....,X_m$ contribute a single factor. The exponential of the element X_{m+k}, $k=1,\dots,n-m$ contributes $2r_k+1$ factors. which explains the bound in (3). □

A simple argument borrowed from the proof in [10] (see also Theorem 1.1 in [14] for the case $m > 2$) is now sufficient to complete the proof of the result.

Theorem 2. *Every connected compact Lie group G is uniformly finitely generated by any set of linearly independent $\{X_1,\dots,X_m\}$ generators of the corresponding Lie algebra.*

Proof. From Lemma 1, every element K in a neighborhood N of the identity in G can be expressed as

[1] This is the worst case number of factors as far as the choice of elements used at each step is concerned. At the $k(>2)$th step the worst situation happens when we consider $e^{X_{m+k-1}\tilde{t}}X_{m+k-2}e^{-X_{m+k-1}\tilde{t}}$ or $e^{X_{m+k-2}\tilde{t}}X_{m+k-1}e^{-X_{m+k-2}\tilde{t}}$. We consider always the second alternative which will give a lesser number of factors.

the product of form (1) with indeterminates $X \in \mathscr{S}$, and l uniformly bounded. Now

$$G = \bigcup_{K \in G} KN. \tag{10}$$

This is an open cover of G and by compactness of G contains a finite subcover. Therefore, we can write

$$G = \bigcup_{i=1}^{r} K_i N. \tag{11}$$

Since from Lemma 6.2 in [4] every K_i is the finite product of elements of the form $e^{X_i t}$, the theorem follows. □

3. Extension to the case of nonnegative parameters $t_1, \ldots, t_l$

From a practical point of view, it is natural to ask whether or not every element can be expressed in the form (1) with l uniformly bounded and $t_i \geqslant 0$, $i = 1, \ldots, l$. In terms of controllability of right invariant vector fields on G, this means that we can reach every point in G from the identity by alternately 'turning on and off' the different vector fields with a uniformly bounded number of switches. If we do not require the number of factors in (1) to be uniformly bounded the answer to this question is already contained in [4] (see the remark after Theorem 6.5). We have:

Theorem 3 (Jurdjevic and Sussmann [4]). *Every element $K \in G$ can be written as in* (1) *with $t_i \geqslant 0$, $i = 1, 2, \ldots, l$.*

Proof. The elements of the form (1), with $t_i \geqslant 0$, form a semigroup $S \subseteq G$ with nonempty interior in G (Lemma 6.1 in [4,16]) which is dense in G. To prove denseness, recall that every element K in G can be written in the form (1) $t_i \in \mathbb{R}$ and for each element $e^{-X|t|}$, there exists a sequence of positive values $t_k \geqslant 0$ such that

$$\lim_{k \to \infty} e^{Xt_k} = e^{-X|t|}. \tag{12}$$

In fact, pick the sequence $e^{nX|t|}$, which by compactness has a converging subsequence $e^{n(k)X|t|}$. By setting $e^{Xt_k} := e^{(n(k+1)-n(k)-1)X|t|}$ we obtain (12). Since S is a semigroup, with nonempty interior and dense in G, it follows from Lemma 6.3 in [4] that $S = G$. □

A simple addition to the argument in the previous section is needed in order to extend Theorem 2 to the case of nonnegative parameters $t_i \geqslant 0$. First notice that from the inverse function theorem and the proof of Lemma 1, there exist $n + 1$ elements in G, $K_1, \ldots, K_{n+1}$, such that the image of the map F from some open set in $\mathbb{R}^n_+$ to G, defined by

$$F(t_1, t_2, \ldots, t_n) := K_1 e^{Xt_1} K_2 e^{Xt_2} \cdots K_n e^{Xt_n} K_{n+1}, \tag{13}$$

is an open set in G. The indeterminates X are in $\mathscr{S}$. Using Theorem 3, we can express $K_1, \ldots, K_{n+1}$ in the form (1) with $t_i \geqslant 0$, and therefore there exists an open set $U \subseteq G$ such that all the elements $K \in U$ can be expressed as in (1) with $t_i \geqslant 0$, $i = 1, 2, \ldots, l$, with a given l. Therefore, using the same argument as in the proof of Theorem 2, we obtain the following result.

Theorem 4. *Every element K of a connected compact Lie group can be written in the form* (1) *where the indeterminates X are in a arbitrary set $\{X_1, \ldots, X_m\}$ of linearly independent generators of the corresponding Lie algebra, $t_i \geqslant 0$, and the number of factors l is uniformly bounded.*

4. Concluding remarks and applications to quantum computing and control

There has recently been a renewed interest in Lie group decompositions of form (1) in view of their application to specify control laws for quantum mechanical systems. Results along this line have appeared for example in [2,3,5,11,12]. In these applications, the relevant compact Lie group is the Lie group of special unitary matrices $SU(n)$ and each of the generators $\{X_1, \ldots, X_m\}$ represents a value of the control variable. The result of Jurdjevic and Sussmann implies that it is possible to drive the state of the system from the identity to any value X_f in $SU(n)$ with a finite number of switches. The proof shown here implies that the number of switches required is uniformly bounded over $X_f \in SU(n)$. The applications have most often concerned control of spin systems. In some cases, it is possible to derive explicit formulas for the values of $t_1, \ldots, t_l$ in the factorization (1) and, from these, control algorithms.

The original result of Jurdjevic and Sussmann has also been interpreted as a universality result for quantum logic gates in quantum computing [9,17]. By looking at the decomposition (1) as a sequence of operations on elementary pieces of information, one can say that every operation can be obtained by a sequence of elementary operations. In fact, as we have shown here, the number of required operations is uniformly bounded. In this case too the relevant Lie group is the set of unitary matrices of appropriate dimensions.

The paper [17] also contains an alternative proof that every unitary matrix can be written in form (1) where the indeterminates X belong to a (generic) pair of Hermitian matrices. Although not explicitly mentioned by the author, this proof also works to prove the uniform finite generation result in this special case. The proof presented here for the general case shares some important ideas with the one in [17].

References

[1] P.E. Crouch, F. Silva Leite, On the uniform finite generation of $SO(n,\mathbb{R})$, Systems Control Lett. 2 (1983) 341–347.

[2] D. D'Alessandro, Constructive controllability of one and two spin $\frac{1}{2}$ particles, Proceedings of the 2001 American Control Conference, Arlington, VA, June 2001.

[3] D. D'Alessandro, Control of one and two homonuclear spins, ArXiv:quant-ph/0106127, June 2001.

[4] V. Jurdjevic, H. Sussmann, Control systems on Lie groups, J. Differential Equations 12 (1972) 313–329.

[5] N. Khaneja, R. Brockett, S.J. Glaser, Time optimal control of spin systems, Phys. Rev. A 63 (2001) 032308.

[6] R. Kock, F. Lowenthal, Uniform finite generation of three-dimensional linear Lie groups, Canad. J. Math. 27 (1975) 396–417.

[7] R. Kock, F. Lowenthal, Uniform finite generation of Lie groups locally isomorphic to $SL(2,\mathbb{R})$, Rocky Mountain J. Math. 7 (4) (1977) 707–724.

[8] R. Kock, F. Lowenthal, Uniform finite generation of complex Lie groups of dimension two and three, Rocky Mountain J. Math. 10 (2) (1980) 319–331.

[9] S. Lloyd, Almost any quantum logic gate is universal, Phys. Rev. Lett. 75 (2) (1995) 346.

[10] F. Lowenthal, Uniform finite generation of the rotation group, Rocky Mountain J. Math. 1 (1971) 575–586.

[11] V. Ramakrishna, K. Flores, H. Rabitz, R. Ober, Quantum control by decompositions of $SU(2)$, Phys. Rev. A 62 (2000) 053409-1–5.

[12] S. Schirmer, Quantum control using Lie group decompositions, in: Proceedings of the 40th Conference on Decision and Control, Orlando, FL, December 2001.

[13] F. Silva Leite, Uniform controllable sets of left-invariant vector fields on compact Lie groups, Systems Control Lett. 6 (1986) 329–335.

[14] F. Silva Leite, Bounds on the order of generation of $SO(n,\mathbb{R})$ by one-parameter subgroups, Rocky Mountain J. Math. 21 (2) (1991) 879–911.

[15] S. Sternberg, Lectures on Differential Geometry, Prentice-Hall, Englewood Cliffs, NJ, 1964.

[16] H.J. Sussmann, V. Jurdjevic, Controllability of nonlinear systems, J. Differential Equations 12 (1972) 95–116.

[17] N. Weaver, On the universality of almost every quantum logic gate, J. Math. Phys. 41 (1) (2000) 240–243.