ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 21, Number 2, Spring 1991

# BOUNDS ON THE ORDER OF GENERATION OF $\mathbf{SO(n, R)}$ BY ONE-PARAMETER SUBGROUPS

F. SILVA LEITE

ABSTRACT. A Lie group $G$ is said to be uniformly finitely generated by one-parameter subgroups $\exp(tX_i)$, $i = 1, \ldots, n$, if there exists a positive integer $k$ such that every element of $G$ may be expressed as a product of at most $k$ elements chosen alternatively from these one-parameter subgroups.

In this paper we construct sets of left invariant vector fields on $SO(n)$, in particular, pairs $\{A, B\}$, whose one-parameter subgroups uniformly finitely generate $SO(n)$ and find an upper bound on the order of generation of $SO(n, \mathbf{R})$ by these subgroups. We give special attention to the case $n = 3$.

**0. Introduction.** If the Lie algebra of a connected Lie group $G$ is generated by the elements $X_1, \ldots, X_n$, then every element of $G$ may be expressed as a finite product of elements of the form $\exp(tX_i)$, where $t$ is real and $i = 1, \ldots, n$ (Jurdjevic and Sussmann [**6**]). However, the number of elements required for $g \in G$ may not be uniformly bounded as $g$ ranges through $G$. If, in addition, $G$ is compact and $\exp(tX_i)$, $i = 1, \ldots, n$ are also compact, then it follows from Theorem 1.1 that there exists a positive integer $k$ such that every element of $G$ may be expressed as a product of at most $k$ elements from $\exp(tX_i)$, $i = 1, \ldots, n$. That is, $G$ is uniformly finitely generated by these one-parameter subgroups with order of generation $k$.

For two and three-dimensional Lie groups, the problem has been completely solved by Koch and Lowenthal. In [**1**], Crouch and the present author take the initial steps in the problem of uniform finite generation of $SO(n, \mathbf{R})$ (the real $n(n-1)/2$-dimensional special orthogonal group with Lie algebra $so(n)$) and concentrate on finding pairs of generators for $so(n)$, orthogonal with respect to the killing form $\langle \cdot, \cdot \rangle$ and whose one-parameter subgroups uniformly finitely generate $SO(n)$.

This paper is still devoted to the uniform generation problem of $SO(n)$. Section 1 is introductory. Sections 2 and 3 are concerned with

Work supported in part by Centro de Matemática da Universidade de Coimbra-INIC and by JNICT under project 87.62.
Received by the editors on May 22, 1984 and in revised form on May 27, 1988.

Copyright ©1991 Rocky Mountain Mathematics Consortium

the main problem. The basic idea is to use a decomposition theory for semisimple Lie groups based on the theory of symmetric spaces and briefly discussed in Section 2. The resultant decomposition of $SO(n)$ into a product of a finite number of one-parameter subgroups involves a certain set $\{X_1, \ldots, X_r\}$ of elements of $so(n)$, the corresponding generating set of $so(n)$. An upper bound is found for the uniform finite generation of $SO(n)$ by $\exp(tX_i)$, $i = 1, \ldots, r$, $t \in \mathbf{R}$.

Special attention is, however, given to pairs $\{A, B\}$ of generators of $so(n)$ which are known to exist for every semisimple Lie algebra [**10**]. In Section 3, pairs $\{A, B\}$ of generators of $so(n)$ nonorthogonal with respect to $\langle \cdot, \cdot \rangle$ are constructed. Each of these pairs is such that every element belonging to $\exp(tX_i)$, $i = 1, \ldots, r$, $t \in \mathbf{R}$ ($\{X_1, \ldots, X_r\}$ is a generating set obtained in Section 2) may be expressed as a finite product involving only elements from the one-parameter subgroups generated by $A$ and $B$. This result is combined with one obtained in Section 2 to find an upper bound on the order of generation of $SO(n)$ by $\exp(tA)$ and $\exp(tB)$. The results obtained from Sections 1, 2 and 3 can be improved if $n = 3$. We treat this special case in the Appendix.

## 1. Uniform finite generation of Lie groups and its order of generation.

**Definition 1.1.** A connected Lie Group $G$ is said to be uniformly finitely generated by one-parameter subgroups $\exp(tX_1), \ldots, \exp(tX_n)$ if there is a positive integer $k$ such that every element of $G$ can be written as a product of at most $k$ elements chosen from these subgroups. The least such $k$ is called the *order of generation* of $G$.

Although the order of generation of $G$ depends on the one-parameter subgroups, it must be greater than or equal to the dimension of $G$ (Sard's theorem [**18**]).

The following theorem, whose proof is included here just for the sake of completeness, was proved by Lowenthal [**13**] for a pair of generators, and it gives a sufficient condition for the uniform finite generation of a connected and compact Lie group.

**Theorem 1.1.** *Let $G$ be a connected and compact Lie Group, $X_1, \ldots, X_n$ generators of the Lie algebra $\mathcal{L}(G)$ and $\exp(tX_i)$, $i = 1, \ldots, n$, compact. Then $G$ is uniformly finitely generated by $\exp(tX_i)$, $i = 1, \ldots, n$.*

*Proof.* Let $G_m$ be the set of all products of $m$ elements $\exp(tX_i)$, $i = 1, \ldots, n$. As $\exp(tX_i)$ is compact for every $i$, then $G_m$ is also compact. $G$ is connected and $\{X_1, \ldots, X_n\}_{\mathrm{L.A.}} = \mathcal{L}(G)$, that is, $\mathcal{L}(G)$ is the smallest Lie algebra that contains $X_1, \ldots, X_n$. Hence, there is an integer $l$ such that $g$ is a product of $l$ elements of the form $\exp(tX_i)$, $i = 1, \ldots, n$, $t \in \mathbf{R}$ (Jurdjevic and Sussmann [**5**]). Then $\forall g \in G$, $g \in G_l$ and $G = \cup_{l=1}^{\infty} G_l$. $G$ is complete since, being connected and compact, it is metrizable (Riemannian metric); so, by the Baire category theorem, $G$ is of second category and $G_l$, for some $l$, contains an open set $U$. Hence $G = \cup_{g \in G} gU$; since $\forall g \in G$, $gU$ is open, this is an open cover for $G$ and clearly it contains a finite subcover, i.e., there are $g_1, \ldots, g_r$ such that $G = \cup_{i=1}^{r} g_i U$. But each $g_i$, $i = 1, \ldots, r$, is a finite product of elements of $\exp(tX_i)$, $i = 1, \ldots, n$, and $U \subset G_l$ so the proof is complete. $\square$

The uniform finite generation problem has been completely solved by Lowenthal and Koch for two and three-dimensional Lie groups; [**7**—**9**, **12**—**15**]. In particular, in [**13**] Lowenthal calculates the order of generation of $SO(3)$ by any two one-parameter subgroups $\exp(tA)$, $\exp(tB)$, ($[A, B] \neq 0$) and shows that it is a function of the angle between the axes of the two generators. (Note that $so(3)$ is generated by any two noncommutative elements and that the corresponding one-parameter subgroups are compact.)

Now a canonical basis of $so(n)$ is defined, namely the skew symmetric matrices $A_{ij}$, $1 \leq i < j \leq n$, where

$$[A_{ij}]_{kl} = \begin{cases} \delta_{ik}\delta_{jl}, & 1 \leq k \leq l \leq n, \\ -\delta_{il}\delta_{jk}, & 1 \leq l \leq k \leq n, \end{cases}$$

($[A]_{kl}$ stands for the $kl$-th component of a matrix $A$) with commutation relations ($[A, B] = AB - BA$)

$$[A_{ij}, A_{kl}] = \delta_{jk}A_{il} + \delta_{il}A_{jk} - \delta_{ik}A_{jl} - \delta_{jl}A_{ik}.$$

Although there are Lie groups that can be uniformly finitely generated by one-parameter subgroups that are not compact (for instance $T = SO(2)\times SO(2)$ is generated by $\exp(tA_{12})$ and $\exp(t(A_{12}+\sqrt{2}A_{34}))$ and the order of generation is 2), only compact one-parameter subgroups of $SO(n)$ will be considered in order to be able to use Theorem 1.1.

**2. Decomposition of Lie groups based on symmetric spaces and corresponding generating sets of $SO(n)$.** The first part of this section contains general ideas concerning Riemannian symmetric manifolds (R.S. manifolds). We have decided to include here these ideas for the sake of completeness.

A Riemannian manifold $M$ is called symmetric if each point $p \in M$ is an isolated fixed point of an involutive isometry $s_p$ of $M$.

Let $M$ be an R.S. manifold. The set $I(M)$ of all the isometries of $M$ acts transitively on $M$. This action gives $M$ the structure of a homogeneous space $G/K$ where $G = I_0(M)$ and $K$ is the (compact) isotropy subgroup of $G$ at a point $x_0$. The mapping $\sigma : G \to G$ defined by $\sigma(x) = s_{x_0} x s_{x_0}$ is an involutive automorphism of $G$ and $K = \{x \in G : \sigma(x) = x\}$. If $\mathcal{G}$ and $\mathcal{T}$ denote the Lie algebras of $G$ and $K$, respectively, $(d\sigma)_e$ is an involutive automorphism of $\mathcal{G}$ and $\mathcal{G}$ admits a direct sum decomposition $\mathcal{G} = \mathcal{T} \oplus \mathcal{P}$ with $\mathcal{T} = \{X \in \mathcal{G} : (d\sigma)_e X = X\}$ and $\mathcal{P} = \{X \in \mathcal{G} : (d\sigma)_e X = -X\}$. Since $(d\sigma)_e$ is an automorphism, it follows that

$$[\mathcal{T},\mathcal{T}] \subset \mathcal{T},\ [\mathcal{T},\mathcal{P}] \subset \mathcal{P} \quad \text{and} \quad [\mathcal{P},\mathcal{P}] \subset \mathcal{T}. \tag{2.1}$$

$\mathcal{T}$ is a subalgebra of $\mathcal{G}$, and $\mathcal{P}$ is a vector space.

If $\pi$ denotes the natural mapping of $G$ into $M$ defined by $x \mapsto x \cdot x_0$, $(d\pi)_e$ is a linear mapping of $\mathcal{G}$ onto $T_{x_0}M$ (the tangent space of $M$ at $x_0$) with kernel $\mathcal{T}$ that maps $\mathcal{P}$ isomorphically onto $T_{x_0}M$. Now if $P = \exp \mathcal{P}$, $\pi$ maps one-parameter subgroups contained in $P$ into the geodesics emanating from $x_0$, $\exp(tX) \mapsto \exp tX \cdot x_0$.

A Lie algebra $\mathcal{G}$ which admits a direct sum decomposition, $\mathcal{G} = \mathcal{T} \oplus \mathcal{P}$, into the $\pm 1$ eigenspaces of an involutive automorphism $s$ satisfying (2.1) and such that the group of inner automorphisms of $\mathcal{G}$ generated by $\mathcal{T}$ is compact, is said to be an orthogonal symmetric Lie algebra $(\mathcal{G}, s)$. A pair $(G, K)$, where $G$ is a connected Lie group with Lie algebra $\mathcal{G}$

and $K$ is a Lie subgroup of $G$ with Lie algebra $\mathcal{T}$, is said to be the pair associated with the orthogonal symmetric Lie algebra $(\mathcal{G}, s)$, and $K$ is called the symmetric subgroup.

A Cartan subalgebra of $(\mathcal{G}, s)$ is a maximal abelian subalgebra of $\mathcal{G}$ contained in $\mathcal{P}$. All Cartan subalgebras of $(\mathcal{G}, s)$ are conjugate under $\mathrm{Ad}_G K$, the adjoint representation of $K$.

**Lemma 2.1.** *If $M$ is an R.S. manifold $G/K$, then $G = KAK$ where $A = \exp \mathcal{A}$ for any Cartan subalgebra $\mathcal{A}$ of the orthogonal symmetric Lie algebra associated with $(G, K)$.*

The proof can be found in Crouch and Silva Leite [**1**].

To decompose a Lie group one simply identifies an involutive automorphism of $G$ and corresponding symmetric subgroup $K_1$ and forms the decomposition $G = K_1 A_1 K_1$. Since each involutive isometry of $M = G/K_1$ gives rise to an involutive automorphism of $G$, to decompose a Lie group one must find first an R.S. manifold of the form $G/K_1$. It is clear that R.S. manifolds play an important part in decompositions of Lie groups.

After having decomposed $G = K_1 A_1 K_1$, $K_1$ can be decomposed similarly to obtain $G = K_2 A_2 K_2 A_1 K_2 A_2 K_2$. If this procedure is continued until an abelian group $K_i$ is encountered, $G$ becomes a product of abelian subgroups $K_i, A_i, A_{i-1}, \ldots, A_1$, namely,

$$\begin{aligned} G = K_i A_i K_i A_{i-1} K_i A_i K_i A_{i-2} \cdots K_i A_i K_i A_1 K_i A_i K_i \cdots \\ \cdots A_{i-2} K_i A_i K_i A_{i-1} K_i A_i K_i. \end{aligned} \tag{2.2}$$

At each stage, different choices of involutive automorphisms may exist, each of which gives a different decomposition of the symmetric subgroup $K_j$, and consequently of $G$.

After decomposing $G$ as a product of abelian subgroups, the decomposition of $G$ as a product of one-parameter subgroups is a trivial matter.

Involutive automorphisms $\sigma$ for the classical matrix groups always exist. Full details can be found in Helgason [**3**].

Throughout this paper we only consider R.S. manifolds $M = SO(n)/K$ and associated orthogonal symmetric Lie algebras $(so(n), \sigma)$

given by

$$\begin{array}{c}\mathcal{G} = so(p+q) = \\ p \geq q \geq 1\end{array} \left\{ \begin{pmatrix} X_1 X_2 \\ -X_2^t X_3 \end{pmatrix};\ \begin{array}{l} X_1 \in so(p),\ X_3 \in so(q) \\ X_2 \text{ arbitrary} \end{array} \right\}$$

$$(*) \qquad \sigma(X) = I_{p,q} X I_{p,q}, \qquad I_{p,q} = \begin{pmatrix} -I_p & 0 \\ 0 & I_q \end{pmatrix}$$

$$\mathcal{T} = \left\{ \begin{pmatrix} X_1 & 0 \\ 0 & X_3 \end{pmatrix}; X_1 \in so(p),\ X_3 \in so(q) \right\},$$

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 & X_2 \\ -X_2^t & 0 \end{pmatrix},\ X_2 \text{ arbitrary} \right\}$$

$$K = SO(p) \times SO(q).$$

A Cartan subalgebra of $(\mathcal{G}, \sigma)$ is $\mathcal{A} = \sum_{i=1}^{q} \mathbf{R} A_{i,p+i}$ with dimension $q$.

When $p+q$ is even there are other choices for $\sigma$ and $K$ (see Chapter X of Helgason [**3**]). However, only the symmetric space structure $(*)$ (which is unique up to conjugacy when $p+q$ is odd) will be considered in this article.

As a consequence of the decompositions of $SO(n)$ outlined in the beginning of this section and in $(*)$ above, into $r$ one-parameter subgroups of the form $\exp(tA_{ij})$, one can associate with each such decomposition a generating set of $SO(n)$, the *corresponding generating set* and a number, the number $r$ of one-parameter subgroups that such a decomposition yields. Although in some cases this number coincides with the order of generation of $SO(n)$ by the one-parameter subgroups belonging to the corresponding generating set, in general it only is an upper bound on the order of generation. We shall refer to this as the *number of generation* relative to the given decomposition.

Whereas the order of generation only depends on the generating set, the number of generation is also a function of the decomposition chosen and the relation to each other.

**Lemma 2.2.** *The number of generation of $SO(n)$ corresponding to a decomposition of $SO(n)$ by one-parameter subgroups of the form* $\exp(tA_{ij})$ *increases with $p$ being minimal* (*equal to the* dim *of* $SO(n)$) *when $SO(m)$, $\forall m \in [3,n] \cap \mathbf{Z}$, is decomposed according to the symmetric space structure in $(*)$, with $p = q$ or $p = q+1$ $(p+q = m)$.*

The proof can be found in [**1**, Section 3].

**Lemma 2.3.** *The cardinality of the generating set of* $SO(n)$ (*or* $so(n)$) *corresponding to a decomposition of* $SO(n)$ *decreases when* $p$ *increases, being minimal* (*equal to* $n-1$) *when* $SO(m)$, $\forall m \in [3,n] \cap \mathbf{Z}$, *is decomposed according to the symmetric space structure in* $(*)$, *with* $p = m-1$, $q = 1$.

*Proof.* If, $\forall i = 0, 1, \ldots, n-3$, $SO(n-i)$ is decomposed according to the symmetric space structure $(*)$ with $p = n-i-1$, $q = 1$, the result is the decomposition

$$\begin{aligned} SO(n) = {} & K_{n-2}A_{n-2}K_{n-2}A_{n-1}K_{n-2}A_{n-2}K_{n-2}\cdots K_{n-2}A_{n-2}K_{n-2}A_1 \\ & K_{n-2}A_{n-2}K_{n-2}\cdots K_{n-2}A_{n-2}K_{n-2}A_{n-1}K_{n-2}A_{n-2}K_{n-2}, \end{aligned}$$

where $K_{n-2}, A_{n-2}, \ldots, A_2, A_1$ are distinct one-parameter subgroups of the form $\exp(tA_{ij})$. So, the generating set of $so(n)$ contains $n-1$ elements and is clearly a minimal generating set.

To prove that # (generating set) increases when $p$ decreases, it is sufficient to show that if, for a certain $i$, $SO(n-i)$ is decomposed as in $(*)$ with $p < n-i-1$ then #(generating set) is greater than $n-1$. Without loss of generality $i$ can be taken equal to zero. Now $SO(n) = KAK$ where $K = SO(p) \times SO(n-p)$, $p < n-1$ and $A$ is $n-p$ dimensional. Then, #(generating set) $\geq (p-1) + (n-p-1) + n - p = 2n-2-p > n-1$ ($p-1$ and $n-p-1$ being the cardinal number of minimal generating sets of $SO(p)$ and $SO(n-p-1)$, respectively). Clearly $2n-2-p$ increases when $p$ decreases and the lemma follows. $\square$

*Remark* . It is clear from Lemma 2.2 that when $SO(m)$, $\forall m \in [3,n] \cap \mathbf{Z}$, is decomposed as in $(*)$ with $p = q$ or $p = q+1$ ($p+q = m$), $SO(n)$ is uniformly finitely generated by the one-parameter subgroups belonging to the corresponding generating set with order of generation equal to $n(n-1)/2$. However, this generating set contains more elements than the generating set corresponding to any other decomposition based on $(*)$ (Lemma 2.3).

In the next section only generating sets of $SO(n)$ with $n$ elements will be considered. The reason for that choice will become clear later.

**Lemma 2.4.** *The generating set corresponding to a decomposition of $SO(n)$ by one-parameter subgroups resulting from decompositions of $SO(n)$ and subsequent symmetric subgroups as in $(*)$ contains $n$ elements if and only if for some $m_1 \in [4, n] \cap \mathbf{Z}$, $SO(m_1)$ is decomposed with $p = m_1 - 2$, $q = 2$ and $SO(m)$, $\forall m \in [3, n] \cap (\mathbf{Z} \backslash \{m_1\})$ is decomposed with $p = m - 1$, $q = 1$.*

*Proof.* Without loss of generality, we can take $m_1 = n$. Then, $SO(n) = KAK$ with $K = SO(n-2) \times SO(2)$ and $A$ two-dimensional. Now if, $\forall i \in [2, n-3] \cap \mathbf{Z}$, $SO(n-i)$ is decomposed as $SO(n-i) = K_i A_i K_i$ with $K_i = SO(n-(i+1))$ and $A_i$ one-dimensional, by Lemma 2.3 the corresponding generating set of $SO(n-2)$ contains $n-3$ elements. Therefore, the generating set of $SO(n)$ corresponding to the decomposition above contains $(n-3)+1+2 = n$ elements. Now the lemma follows as a consequence of Lemma 2.3. $\square$

**Theorem 2.1.** *$SO(n)$ is uniformly finitely generated by the $n$ one-parameter subgroups corresponding to the decomposition outlined in Lemma 2.4 with $m_1 = n$, and the number of generation is $2^{n-2} + 2$.*

*Proof.* The first part is a consequence of the last lemma. Now, if the decomposition mentioned in Lemma 2.4 is applied to $SO(n)$, we have $SO(n) = SO(n-2) \times SO(2) A SO(n-2) \times SO(2)$, with $A$ a two-dimensional abelian subgroup and hence $SO(n-2) = K_i A_i K_i A_{i-1} \cdots K_i A_i K_i A_1 K_i A_i K_i \cdots A_{i-1} K_i A_i K_i$ with $i = n-4$, $K_i, A_i, A_{i-1}, \ldots, A_1$ one-parameter subgroups. In this decomposition of $SO(n-2)$, $K_i$ occurs $2^i$ times and $A_j$, $1 \le j \le i$ occurs $2^{j-1}$ times. Thus $SO(n-2)$ is a product of $2^{n-4} + \sum_{j=1}^{n-4} 2^{j-1} = \sum_{j=0}^{n-4} 2^j = 2^{n-3} - 1$ one-parameter subgroups. Therefore, $SO(n)$ can be decomposed as a product of $2(2^{n-3} - 1 + 1) + 2 = 2^{n-2} + 2$ one-parameter subgroups. $\square$

*Remark* . It is easy to conclude that in particular $\{\exp(tA_{i,i+1}); i = 1, \ldots, n-1; t \in \mathbf{R}\} \cup \{\exp(tA_{1n})\}$ is a generating set of $SO(n)$ satisfying Theorem 2.1.

**3. The use of permutation matrices in constructing nonorthogonal pairs $\{\mathbf{A}, \mathbf{B}\}$ of vector fields that generate $\mathbf{so(n)}$ and the uniform generation of $\mathbf{so(n)}$ by $\exp(\mathbf{tA})$ and $\exp(\tau\mathbf{B})$.** In this section, pairs of generators of $so(n)$, nonorthogonal with respect to the killing form, will be constructed and the uniform generation problem of $SO(n)$ partially solved for these pairs. As in the method used by Crouch and Silva Leite [**1**] to construct orthogonal pairs, permutation matrices play an important role here.

The diagram below, showing the canonical basis elements of $so(n)$, provides a good visualization of some of the results obtained here and will be often referred to throughout this section.

$$\begin{array}{cccccccc}
A_{12} & A_{13} & A_{14} & A_{15} & \ldots & A_{1,n-1} & A_{1n} \\
 & A_{23} & A_{24} & A_{25} & \ldots & A_{2,n-1} & A_{2n} \\
 & & A_{34} & A_{35} & \ldots & A_{3,n-1} & A_{3n} \\
 & & & A_{45} & \ldots & A_{4,n-1} & A_{4n} \\
 & & & & \ddots & \vdots & \vdots \\
 & & & & & A_{n-2,n-1} & A_{n-2,n} \\
 & & & & & & A_{n-1,n}
\end{array}$$

DIAGRAM 3.1.

**Lemma 3.1.** *If $P_\Pi^\alpha$ is a real permutation matrix defined by $P_\Pi^\alpha e_i = \alpha_i e_{\Pi(i)}$, $i = 1, \ldots, n$, $\alpha_i^2 = 1$, $\Pi$ a permutation on $n$ letters, then $\forall i, j \in \{1, \ldots, n\}$,*

$$P_\Pi^\alpha A_{ij} (P_\Pi^\alpha)^{-1} = \alpha_i \alpha_j A_{\Pi(i),\Pi(j)}.$$

The proof only involves a few calculations.

Given a permutation matrix $P_\Pi^\alpha \in SO(n)$, the existence of $A_\Pi^\alpha \in so(n)$ such that $\exp(A_\Pi^\alpha) = P_\Pi^\alpha$ is a consequence of the exponential map being surjective (see Helgason [**3**, p. 135]). Conditions on the entries of $A_\Pi^\alpha$ may be found using the fact that if $P_\Pi^\alpha$ has the eigenvector $x$ corresponding to the eigenvalue $\lambda$ then $A$ has the same eigenvector corresponding to the eigenvalue $\mathfrak{H}_\lambda = \log_\theta \lambda$, for some $\theta$.

Let $P$ be the permutation matrix defined by $Pe_i = e_{i+1}$, $i = 1, \ldots, n-1$, $Pe_n = (-1)^{n+1} e_1$, and let $A \in so(n)$ be such that $\exp(A) = P$. If $n$ is odd, $A$ has the following form:

$$
\left(\begin{array}{ccccc|cccc}
0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-1}{2}} & -\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 \\
-\alpha_1 & 0 & \alpha_1 & \ddots & \vdots & \alpha_{\frac{n-1}{2}} & \ddots & & -\alpha_2 \\
-\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 & \vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \alpha_1 & \alpha_2 & & \ddots & -\alpha_{\frac{n-1}{2}} \\
-\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-1}{2}} \\
\hline
\alpha_{\frac{n-1}{2}} & -\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \alpha_2 & \vdots \\
\vdots & \ddots & \ddots & & -\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 \\
\alpha_2 & & \ddots & & & -\alpha_2 & \ddots & 0 & \alpha_1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-1}{2}} & -\alpha_{\frac{n-1}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0
\end{array}\right)
$$

where $\alpha_1, \ldots, \alpha_{(n-1)/2}$ satisfy the system of $(n-1)/2$ equations,

$$
\begin{cases}
-\displaystyle\sum_{l=1}^{(n-1)/2} 2\alpha_l \sin(l\theta_1) = \theta_1 + 2\pi k_1 \\
-\displaystyle\sum_{l=1}^{(n-1)/2} 2\alpha_l \sin(2l\theta_1) = 2\theta_1 + 2\pi k_2 \\
\quad\vdots \\
-\displaystyle\sum_{l=1}^{(n-1)/2} 2\alpha_l \sin(\tfrac{(n-1)}{2} l\theta_1) = (n-1)\theta_1/2 + 2\pi k_{(n-1)/2}
\end{cases}
$$

for some $k_1, \ldots, k_{(n-1)/2} \in \mathbf{Z}$, $\theta_1 = 2\pi/n$. And if $n$ is even, $A$ has the form

$$\left(\begin{array}{ccccc|ccccc}
0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-2}{2}} & \alpha_{\frac{n}{2}} & \alpha_{\frac{n-2}{2}} & \cdots & \alpha_2 & \alpha_1 \\
-\alpha_1 & 0 & \alpha_1 & \ddots & & \alpha_{\frac{n-2}{2}} & \ddots & \ddots & & \alpha_2 \\
-\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \alpha_1 & \alpha_2 & \ddots & \ddots & \ddots & \alpha_{\frac{n-2}{2}} \\
\alpha_{\frac{n-2}{2}} & & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \ddots & \ddots & \ddots & \alpha_{\frac{n}{2}} \\
\hline
-\alpha_{\frac{n}{2}} & -\alpha_{\frac{n-2}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{\frac{n-2}{2}} \\
-\alpha_{\frac{n-2}{2}} & \ddots & \ddots & \ddots & & -\alpha_1 & 0 & \alpha_1 & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & & -\alpha_2 & -\alpha_1 & 0 & \ddots & \alpha_2 \\
-\alpha_2 & \ddots & \ddots & \ddots & & \vdots & \ddots & \ddots & \ddots & \alpha_1 \\
-\alpha_1 & -\alpha_2 & \cdots & -\alpha_{\frac{n-2}{2}} & -\alpha_{\frac{n}{2}} & -\alpha_{\frac{n-2}{2}} & \cdots & -\alpha_2 & -\alpha_1 & 0
\end{array}\right)$$

with $\alpha_1, \ldots, \alpha_{n/2}$ satisfying the following set of $n/2$ equations,

$$\begin{cases}
-\sum_{l=1}^{(n-2)/2} 2\alpha_l \sin(l\theta_1) - \alpha_{n/2} = \theta_1 + 2\pi k_1 \\
-\sum_{l=1}^{(n-2)/2} 2\alpha_l \sin(3l\theta_1) + \alpha_{n/2} = 3\theta_1 + 2\pi k_2 \\
\qquad \vdots \\
-\sum_{l=1}^{(n-2)/2} 2\alpha_l \sin((n-1)l\theta_1) + (-1)^{1+n/2}\alpha_{n/2} = (n-1)\theta_1 + 2\pi k_{n/2}
\end{cases}$$

for some $k_1, k_2, \ldots, k_{n/2} \in \mathbf{Z}$, $\theta_1 = \pi/n$.

As a consequence of the definition of $P$ together with Lemma 3.1, the canonical basis $\mathcal{B} = \{A_{ij}; i, j = 1, \ldots, n,\ i < j\}$ of $so(n)$ can be divided into $[n/2]$ equivalence classes. The equivalence class of a certain element $A_{ij}$ is the set of canonical basis elements that belong to the orbit of $\exp(t \operatorname{Ad} A)$, $t \in \mathbf{R}$, that passes through $A_{ij}$.

Let $[\alpha_i]$, $i = 1, \ldots, [n/2]$ denote the equivalence classes. (This notation is used to agree with the structure of $A$.) Note that for a certain $i$, $[\alpha_i]$ is the set of canonical basis elements with coefficients $\pm\alpha_i$ in the expression of $A$. Clearly,

$$[\alpha_i] = \{A_{kl} \in \mathcal{B} : l - k = i\} \cup \{A_{kl} \in \mathcal{B} : l - k = n - i\}$$

$\forall i = 1, \dots, [n/2]$. If $\beta_i$ and $\beta_{n-i}$ denote $\{A_{kl} \in \mathcal{B} : l - k = i\}$ and $\{A_{kl} \in \mathcal{B} : l-k = n-i\}$, respectively, $[\alpha_i] = \beta_i \cup \beta_{n-i}$, $i = 1, \dots, [n/2]$. Hence, $\forall j = 1, \dots, n-1$, $\#\beta_j = n - j$ and $\beta_j$ can be seen as the set of elements along the $j$-th diagonal (counted from left to right) in Diagram 3.1.

$\beta_1$ is a generating set of $so(n)$ and it is minimal in the sense that no subset of $\beta_1$ generates $so(n)$. In fact, if $SO(m)$, $m = 3, \dots, n$, is decomposed according to the symmetric space structure $(*)$ in Section 2, with $p = m - 1$, $q = 1$, the corresponding canonical decomposition of $so(n)$ is as follows:

$$so(n) = \mathcal{T}_{n-2} \oplus \left(\bigoplus_{i=1}^{n-2} \mathcal{P}_i\right),$$

$$\mathcal{P}_i = \operatorname{span}\{A_{ij}, j = i+1, \dots, n\}, \qquad \mathcal{T}_{n-2} = \mathbf{R}A_{n-1,n}\,.$$

Since $A_{i,i+1} \in \mathcal{P}_i$, $\forall i = 1, \dots, n-2$ $A_{i,i+1}$ can be chosen to generate $A_i = \exp(\mathcal{A}_i)$ and it follows that $\{A_{i,i+1}; i = 1, \dots, n-1\} = \beta_1$ is a generating set of $so(n)$. That it is minimal is due to the fact that any minimal generating set of $so(n)$ whose elements belong to the canonical basis $\mathcal{B}$ has cardinality $n-1$. In fact, if $X = \{X_1, \dots, X_{n-2}\} \subset \mathcal{B}$ is a minimal generating set of $so(n)$, there exists $i \in \{1, \dots, n-1\}$ such that $A_{ij} \notin X$, $j = 2, \dots, n$, $j > i$. We can assume, without any loss of generality, that $i = 1$. Then, using the commutation relations in Section 1 we see that $A_{1j} \notin \{X_1, \dots, X_{n-2}\}_{\text{L.A.}}$, that is, $\{X_1, \dots, X_{n-2}\}$ does not generate $so(n)$. Clearly, $[\alpha_1]$ is a generating set since it contains $\beta_1$, and $\beta_i$, $i \neq 1$ is not a generating set.

**Theorem 3.1.** *For $n > 3$, let $A \in so(n)$ satisfy $\exp(A) = P_\Pi$, $P_\Pi$ the permutation matrix defined by $P_\Pi e_i = e_{\Pi(i)}$, $i = 1, \dots, n-1$, $P_\Pi e_n = (-1)^{n+1} e_{\Pi(n)}$, $\Pi$ the cyclic permutation on $n$ letters and $B \in \{\exp(t \operatorname{ad} A) \cdot A_{n-1,n}, t \in \mathbf{R}\} \subset so(n)$. Then $SO(n)$ is uniformly generated by $\exp(tA)$ and $\exp(sB)$ with number of generation $2^{n-1} + 5$*

*and* $\{A,B\}_{\text{L.A.}} = so(n)$. *If* $B$ *also belongs to* $\mathcal{B}$, *then the number of generation is* $2^{n-1}+3$ *and* $\langle A,B\rangle$ *is not zero in general.*

*Proof.* Let $SO(n)$ be decomposed as in Lemma 2.4 with $m_1 = n$ and $so(n)$ decomposed according to the corresponding canonical decomposition, i.e., $so(n) = \mathcal{T}_1 \oplus \mathcal{P}_1$, $\mathcal{T}_1 = so(n-2) \oplus so(2) = so(n-2) \oplus \mathbf{R}A_{12}$, $\mathcal{P}_1 = \operatorname{span}(\{A_{1j}, j = 3,\dots,n\} \cup \{A_{2j}, j=3,\dots,n\})$ and $\mathcal{T}_2 = so(n-2) = \mathcal{T}_{n-2} \oplus \big(\oplus_{i=3}^{n-2} \mathcal{P}_i\big)$, $\mathcal{P}_i = \operatorname{span}\{A_{ij}, j = i+1,\dots,n\}$. Since $\mathcal{A}_1$ is a two-dimensional abelian subalgebra contained in $\mathcal{P}_1$, and $\mathcal{A}_i$ is a one-dimensional abelian subalgebra of $\mathcal{P}_i$ $\forall i = 3,\dots,n-2$, take $\mathcal{A}_1 = \mathbf{R}A_{1n} + \mathbf{R}A_{23}$, $\mathcal{A}_i = \mathbf{R}A_{i,i+1}$, $i = 3,\dots,n-2$ and $\mathcal{T}_{n-2} = \mathbf{R}A_{n-1,n}$. Then $SO(n)$ is uniformly generated by the $n$ one-parameter subgroups generated by $[\alpha_1]$ with number of generation $2^{n-2}+2$ (Theorem 2.1). That is,

$$SO(n) = \underbrace{K_{n-2}A_{n-2}K_{n-2}A_{n-3}\cdots K_{n-2}A_{n-2}K_{n-2}A_{n-3}K_{n-2}A_{n-2} K_{n-2}\cdots A_{n-3}K_{n-2}A_{n-2}K_{n-2}}_{*} \exp(tA_{12})A_1\exp(sA_{12}) \underbrace{K_{n-2}A_{n-2} K_{n-2}A_{n-3}\cdots K_{n-2}A_{n-2}K_{n-2}A_3K_{n-2}A_{n-2}K_{n-2}\cdots A_{n-3}K_{n-2} A_{n-2}K_{n-3}}_{*}$$

$$t,s\in\mathbf{R},\quad K_{n-2} = \exp tA_{n-1,n},\quad A_i = \mathcal{L}(\mathcal{A}_i),\quad i = 3,\dots,n-2.$$

By construction of $A$ and $B$ there exist real numbers $t_1,\dots,t_n$ such that $\exp(t_i \operatorname{ad} A)\cdot B = A_{i,i+1}$, $i = 1,\dots,n-1$, $\exp(t_n \operatorname{ad} A)\cdot B = A_{1n}$. The use of the Baker–Campbell–Hausdorff formula allows every one of the $2^{n-2}+2$ one-parameter subgroups that appear in (3.1) to be expressed as a product of three one-parameter subgroups generated by $A$ and $B$. Hence, taking into account the composition of terms with the same generator a total number of $3(2^{n-2}+2) - (2^{n-2}+1) = 2^{n-1}+5$ subgroups generated by $A$ and $B$ is obtained.

If $B = A_{n-1,n}$, then the product $*$ in (3.1) contains $2^{n-2}-3$ elements, the first and the last of which is $\exp(tB)$ and, after reducing the terms with the same generator in $\exp(tA_{12})A_1\exp(sA_{12})$, a total number of $2(2^{n-2}-3)+9 = 2^{n-1}+3$ one-parameter subgroups is obtained. The result when $B$ is another element of $[\alpha_1]$ is a consequence of taking a decomposition of $SO(n)$ that is conjugate to the one considered above. (For instance, if $B = A_{n-2,n-1}$, the automorphism of $so(n)$ defined by $X \mapsto e^{-A}Xe^{A}$ maps $A_{n-1,n}$ into $A_{n-2,n-1}$. Under this automorphism the direct sum decomposition of $so(n)$ above,

$$so(n) = \mathcal{T}_{n-2} \oplus \left(\bigoplus_{i=3}^{n-2} \mathcal{P}_i\right) \oplus \mathbf{R}A_{12} \oplus \mathcal{P}_1,$$

gives rise to a direct sum decomposition

$$so(n) = \mathcal{T}^1_{n-2} \oplus \left(\bigoplus_{i=3}^{n-2} \mathcal{P}^1_i\right) \oplus \mathbf{R}A_{1n} \oplus \mathcal{P}^1_1,$$

where $\mathcal{T}^1_{n-2} = \mathbf{R}A_{n-2,n-1}$, $\mathcal{P}^1_i = \operatorname{span}\{e^{-A}A_{ij}e^{A}, j = i+1,\dots,n\}$, $i = 3,\dots,n-2$ and $\mathcal{P}^1_1 = \operatorname{span}(e^{-A}A_{1j}e^{A}, j = 3,\dots,n\} \cup \operatorname{span}\{e^{-A}A_{2j}e^{A}, j = 2,\dots,n\}$. Thus, taking $A_1 = \exp(tA_{n-1,n})\exp(sA_{12})$, $A_i = \exp(tA_{i-1,i})$, $i = 3,\dots,n-2$ and $K_{n-2} = \exp(tA_{n-2,n-1})$ the result follows.) Now, to each vector $x = (x_1,\dots,x_m)$, $m = n(n-1)/2$ of $\mathbf{R}^m$ we associate an element $X \in so(n)$ defined by

$$X = \left(\begin{array}{ccc|ccc}
0 & x_1 & x_2 & x_4 & \cdots & x_{m-n+1} \\
-x_1 & 0 & x_3 & x_5 & & \vdots \\
-x_2 & -x_3 & 0 & x_6 & & \vdots \\
\hline
-x_4 & -x_5 & -x_6 & 0 & & \\
\vdots & & & & \ddots & x_m \\
-x_{m-n+1} & \cdots & & & -x_m & 0
\end{array}\right).$$

A simple calculation shows that $\forall X, Y \in so(n)$, $\operatorname{trace}(XY) = -2(x,y)$ ($(\cdot,\cdot)$ is the inner product). Then, since $\langle A, B\rangle = \operatorname{trace}(\operatorname{ad} A \cdot \operatorname{ad} B) = (n-2)\operatorname{trace}(AB)$ (Helgason [**3**, p. 189]), $\langle A, B\rangle = -2(n-2)(a,b)$ and by construction $A$ and $B$ can be chosen nonorthogonal. □

Clearly, $A$ and $B$ can be replaced by $UAU^{-1}$ and $UBU^{-1}$ for some permutation matrix $U$ without changing the result.

It is not clear whether or not canonical basis elements other than those already considered (belonging to $[\alpha_1]$) may satisfy our requirements; that is, maybe candidates for an element $B$ such that $\exp(tB)$

and $\exp(tA)$ ($A$ defined as in the theorem above) uniformly finitely generate $SO(n)$. From earlier results it is known that if $B$ belongs to the orbit of $\exp(t\ \mathrm{ad}\ A)$ that passes through $[\alpha_k]$ for some $k$, then $\forall A_{ij} \in [\alpha_k]$, $\exists\, t_{ij} \in \mathbf{R}$ such that $\exp(t_{ij}\mathrm{ad}\, A) \cdot B = A_{ij}$. Thus, if $[\alpha_k]$ is a generating set of $so(n)$, $\exp(tA)$ and $\exp(tB)$ uniformly generate $SO(n)$. The next step is to prove that $[\alpha_k]$ generates $so(n)$ if and only if $n$ and $k$ are coprime numbers.

Let $\beta_j$, $j = 1, \dots, n-1$ be defined as before. We use the notation

$$-[\beta_i, \beta_j] = \{A_{sr} \in \mathcal{B} : A_{rs} \in [\beta_i, \beta_j]\}.$$

The next lemma can be easily proved by using the structure formulas of $so(n)$ with respect to the canonical basis

**Lemma 3.2.** (1) *$\forall i \neq 1$, $\cup_{m\in\mathbf{N}}\beta_{mi}$ belongs to a proper subalgebra of $so(n)$.*

(2) *$\forall i < j$, $i + j \leq n$, $\beta_{j-1} \subset -[\beta_i, \beta_j]$.*

(3) *$\forall i, j$, $\beta_{j+i} \subset [\beta_i, \beta_j]$.*

**Lemma 3.3.** *If both $n$ and $k$ have a common divisor $m \neq 1$, $[\alpha_k]$ is not a generating set of $so(n)$.*

*Proof.* This is an immediate consequence of Lemma 3.2 (1) since if both $n$ and $k$ have a common divisor $m$, both $n$ and $n-k$ also have the same divisor $m$ and both $\beta_k$ and $\beta_{n-k}$ belong to a proper subalgebra of $so(n)$. $\beta_m$ is a generating set of this subalgebra. $\square$

Next we prove that if $n$ and $k$ are coprime numbers, then $[\alpha_k]$ is a generating set of $so(n)$. If every element of $\beta_1$ can be obtained by Lie brackets of elements of $\beta_k$ and $\beta_{n-k}$, obviously $[\alpha_k]_{\mathrm{L.A.}} = so(n)$.

Assume that $n$ and $k$ are coprime numbers. Then $n \equiv k_1 \bmod k$, i.e., $n = j_0 k + k_1$ for some $k_1 \in \{1, \dots, k-1\}$, $j_0 \in \mathbf{N}$. Consider the class $C_{j_0} = \{\beta_{n-k}, \beta_{n-2k}, \ldots, \beta_{n-j_0k} = \beta_{k_1}\}$ whose elements satisfy the following $j_0 - 1$ relations.

$$(3.2)\qquad \begin{array}{cc} (1) & \beta_{n-2k} \subset -[\beta_k, \beta_{n-k}] \\ (2) & \beta_{n-3k} \subset -[\beta_k, \beta_{n-2k}] \\ \vdots & \vdots \\ (j_0-1) & \beta_{k_1} = \beta_{n-j_0k} \subset -[\beta_k, \beta_{n-(j_0-1)k}]. \end{array}$$

(See Lemma 3.2(2).) From (1), $\forall Z_2 \in \beta_{n-2k}$ there exist $X_2 \in \beta_k$ and $X_1 \in \beta_{n-k}$ such that $Z_2 = -[X_2, X_1]$. From (2), $\forall Z_3 \in \beta_{n-3k}$ there exist $X_3 \in \beta_k$ and $Y_1 \in \mathcal{B}_{n-2k}$ such that $Z_3 = -[X_3, Y_1]$. But $Y_1 \in \beta_{n-2k}$; thus, $Y_1 = -[X_2, X_1]$ for some $X_2 \in \beta_k$, $X_1 \in \beta_{n-k}$. So $Z_3 = [X_3, [X_2, X_1]]$, for some $X_1, X_2$ and $X_3$ belonging to $[\alpha_k]$. The same argument used throughout the relations $(3), \ldots, (j_0 - 1)$ clearly leads to the following. $\forall Z_{j_0} \in \beta_{n-j_0k} = \beta_{k_1}$, there exist $X_1, X_2, \ldots, X_{j_0} \in [\alpha_k]$ such that

$$(3.3)\qquad Z_{j_0} = (-1)^{j_0+1}[X_{j_0}, [X_{j_0-1}, [\ldots [X_3, [X_2, X_1]] \ldots]]].$$

Note that $n - j_0k = k_1 < k$ and $n - (j_0 - i)k = k_1 + ik > k$, $\forall i \geq 1$. Therefore, if $\beta_j$ is viewed as the $j$-th diagonal in Diagram 3.1 (rigorously the set of elements along the $j$-th diagonal), $\mathbf{C}_{j_0}$ is a set of diagonals, $\beta_{k_1}$ being the only diagonal in this set situated below $\beta_k$.

If $k_1 = 1$, then every element of $\beta_1$ can be obtained by Lie brackets of elements of $[\alpha_k]$ and $[\alpha_k]$ is a generating set of $so(n)$. If $k_1 \neq 1$, then $k \equiv k_2 \bmod k_1$, i.e., $k = j_1k_1 + k_2$ for some $k_2 \in \{1, \ldots, k_1 - 1\}$, $j_1 \in \mathbf{N}$. $\mathbf{C}_{j_1} = \{\beta_k, \beta_{k-k_1}, \ldots, \beta_{k-j_1k_1} = \beta_{k_2}\}$ and its elements satisfy the $j_1$ relations,

$$(3.4)\qquad \begin{array}{cc} (1') & \beta_{k-k_1} \subset -[\beta_{k_1}, \beta_k] \\ (2') & \beta_{k-2k_1} \subset -[\beta_{k_1}, \beta_{k-k_1}] \\ \vdots & \vdots \\ (j_1') & \beta_{k_2} = \beta_{k-j_1k_1} \subset -[\beta_{k_1}, \beta_{k-(j_1-1)k_1}]. \end{array}$$

It is easy to conclude, just using the same arguments as above, that $\forall Z'_{j_1} \in \beta_{k-j_1k_1} = \beta_{k_2}$, there exist $X'_1 \in \beta_k$ and $X'_2, X'_3, \ldots, X'_{j_1+1} \in \beta_{k_1}$

such that $Z'_{j_1} = (-1)^{j_1}[X'_{j_1+1}, [X'_{j_1}, [\dots[X'_3, [X'_2, X'_1]]\dots]]]$. Hence, (3.3) can be applied to every element of $\beta_{k_1}$ and the result is that every element of $\beta_{k_2}$ can be obtained by Lie brackets of elements of $[\alpha_k]$:

$$k - j_1 k_1 = k_2 < k_1, \qquad k - (j_1 - i)k_1 = k_2 + ik_1 > k_1, \qquad \forall i \geq 1.$$

So, $\beta_{k_2}$ is the only diagonal of $\mathbf{C}_{j_1}$ situated below $\beta_{k_1}$ (in Diagram 3.1) and also no elements of $\mathbf{C}_{j_1}$ are situated above $\beta_k$.

If $k_1 = 1$, the process ends here and $[\alpha_k]$ is a generating set of $so(n)$. If $k_1 \neq 1$, then $k_1 \equiv k_3 \bmod k_2$, i.e., $k_1 = j_2 k_2 + k_3$ for some $k_3 \in \{1, \dots, k_2 - 1\}$, $j_3 \in \mathbf{N}$. Once again one proceeds as previously. The system of equations

$$\begin{array}{cl} n = j_0 k + k_1 & (0 < k_1 < k) \\ k = j_1 k_1 + k_2 & (0 < k_2 < k_1) \\ k_1 = j_2 k_2 + k_3 & (0 < k_3 < k_2) \\ \vdots & \\ k_{N-2} = j_{N-1} k_{N-1} + k_N & (0 < k_N < k_{N-1}) \\ k_{N-1} = j_N k_N, & \end{array}$$

known as Euclid's algorithm is used in elementary arithmetic to determine the greatest common divisor $k_N$ of $n$ and $k$. Since it has been assumed that $n$ and $k$ are coprime, this process will end up with the equation $k_{N-2} = j_{N-1} k_{N-1} + k_N$, with $k_N = 1$, and some integer $N$. $\mathbf{C}_{j_{N-1}} = \{\beta_{k_{N-2}}, \beta_{k_{N-2}-k_{N-1}}, \dots, \beta_{k_{N-2}-j_{N-1}k_{N-1}} = \beta_1\}$ with elements satisfying the $j_{N-1}$ relations,

$$\begin{array}{c} \beta_{k_{N-2}-k_{N-1}} \subset -[\beta_{k_{N-1}}, \beta_{k_{N-2}}] \\ \beta_{k_{N-2}-2k_{N-1}} \subset -[\beta_{k_{N-1}}, \beta_{k_{N-2}-k_{N-1}}] \\ \vdots \\ \beta_1 = \beta_{k_N} \subset -[\beta_{k_{N-1}}, \beta_{k_{N-2}-(j_{N-1}-1)k_{N-1}}]. \end{array} \tag{3.5}$$

Clearly, every element of $\beta_1$ may be written as brackets of elements from $[\alpha_k]$.

Therefore, one can formulate the lemma that has just been proved.

**Lemma 3.4.** *If $n$ and $k$ are coprime numbers, then $[\alpha_k]_{\mathrm{L.A.}} = so(n)$.*

Lemmas 3.3 and 3.4 can be put together in the following theorem.

**Theorem 3.2.** *Let $g = so(n, \mathbf{R})$, $[\alpha_k]$ as defined in the beginning of this section. Then, $[\alpha_k]_{\mathrm{L.A.}} = g$ if and only if $n$ and $k$ are coprime numbers.*

Now, if we use the fact that any two noncommutative elements of $\mathcal{B}$ generate a subalgebra of $so(n)$ that is isomorphic to $so(3)$, the procedure used above to show that $[\alpha_k]_{\mathrm{L.A.}} = so(n)$ when $n$ and $k$ are coprime numbers also shows that $\forall X$ belonging to any of the following sets: $\beta_{n-ik}$, $i = 2, \dots, j_0$, $\beta_{k-ik_1}$, $i = 1, \dots, j_1, \dots, \beta_{k_{N-2}-ik_{N-1}}$, $i = 1, \dots, j_{N-1}$, satisfying the relations (3.2), (3.4)... and (3.5), respectively, $\exp(tX)$, $t \in \mathbf{R}$ may be written as a product of one-parameter subgroups $\exp(\theta A)$ and $\exp(\tau B)$ where $A$ is defined as in the beginning of the section and $B$ belongs to the orbit of $\exp(t \operatorname{ad} A)$ that passes through $[\alpha_k]$. That is, if we consider the set

$$\begin{aligned} \{\beta_k\} \cup \{\beta_{n-ik}, i = 1, \dots, j_0\} \cup \{\beta_{k-ik_1}, i = 1, \dots, j_1\} \\ \cup \{\beta_{k_1-ik_2}, i = 1, \dots, j_2\} \cup \dots \cup \{\beta_1\} \end{aligned} \tag{3.6}$$

whose elements are clearly identified with those diagonals in Diagram 3.1 which are obtained by successive use of Lie brackets of the elements in $[\alpha_k]$ then, to each element $\beta_i$ in (3.6) a number $N_i$ (the number of generation of $\exp(t\beta_i)$ by $\exp(tA)$ and $\exp(tB)$) is associated. Clearly,

$$\begin{aligned} & N_k \le N_{n-ik} < N_{k_1} < N_{k-jk_1} < N_{k_2} < N_{k_1-sk_2} < N_{k_3} < \cdots, \\ & \forall i = 1, 2, \dots, j_0 - 1, \ j = 1, \dots, j_1 - 1, \ s = 1, \dots, j_2 - 1, \dots . \end{aligned} \tag{3.7}$$

The set (3.6) is totally ordered by means of a relation $\preccurlyeq$ defined as follows: $\beta_i \preccurlyeq \beta_j$ if and only if $\beta_i = \beta_j$ or $\beta_i$ is situated below $\beta_j$ in Diagram 3.1. From comments made during the proof of Lemma 3.4 it is easily seen that

$$\begin{gathered} \beta_1 \prec, \dots, \prec \beta_{k_2} \prec \beta_{k_1-sk_2} \prec \beta_{k_1} \prec \beta_{k-jk_1} \prec \beta_k \prec \beta_{n-ik} \prec \beta_{n-k}, \\ \forall i = 2, \dots, j_0 - 1, \ j = 1, \dots, j_1 - 1, \ s = 1, \dots, j_2 - 1. \end{gathered} \tag{3.8}$$

FIGURE 3.1.

Now, if $SO(m)$, $3 \leq m \leq n$, is decomposed as in $(*)$ Section 2 with $p = m - 1$, $q = 1$, the result is a decomposition of $SO(n)$ by one-parameter subgroups $A_i$, $i = 1, \ldots, n-2$ and $K_{n-2}$ that can be chosen to be generated by $n-1$ canonical basis elements $A_{ij_i}$, $i = 1, \ldots, n-1$. As a consequence of (3.7) and (3.8) it is clear that, if these elements

$A_{ij_i}$ are selected by

$$\begin{gathered}\{A_{i,i+k}, i=1,\dots,n-k\} \subset \beta_k,\\ \{A_{i,i+k_1}, i=n-k+1,\dots,n-k_1\} \subset \beta_{k_1},\\ \{A_{i,i+k_2}, i=n-k_1+1,\dots,n-k_2\} \subset \beta_{k_2},\dots,\\ \{A_{i,i+1}, i=n-k_{N-1}+1,\dots,n-2\} \subset \beta_{k_N}=\beta_1,\\ \{A_{n-1,n}\} \subset \beta_1,\end{gathered} \tag{3.9}$$

we obtain far better results (in the sense that the number of generation of $SO(n)$ by $\exp(tA)$ and $\exp(tB)$ is as small as possible) than if they belong to any other diagonal of the set (3.6). Figure 3.1 shows the position of the elements (3.9) in Diagram 3.1. Hence, in order to improve the final result, a decomposition of $SO(n)$ (isomorphic to the one above) should be chosen in such a way that the greater the word length in terms of $\exp(tA)$ and $\exp(tB)$ a subgroup of $SO(n)$ is, the fewer times it appears in the decomposition of $SO(n)$.

Many things would then have to be taken into consideration and the final answer does not appear to be very easy. However, all the difficulties in trying to solve this problem are overcome as a consequence of the next result.

It will be proved that if $[\alpha_k]$ generates $so(n)$ there exists a decomposition of $SO(n)$ such that the corresponding generating set of $so(n)$ is $[\alpha_k]$ itself. This has been seen to be true when $k=1$ (see the proof of Theorem 3.1).

**Theorem 3.3.** *For $n>3$, let $A \in so(n)$ satisfy $\exp(A)=P_\Pi, P_\Pi$ the permutation matrix defined by $P_\Pi e_i = e_{\Pi(i)}$, $i=1,\dots,n-1$, $P_\Pi e_n = (-1)^{n+1} e_{\Pi(n)}$, $\Pi$ the cyclic permutation on $n$ letters and $B \in \{\exp(t \text{ ad } A)\cdot X,\ X \in [\alpha_k],\ t \in \mathbf{R}\} \subset so(n)$, $n$ and $k$ coprime numbers. Then $SO(n)$ is uniformly generated by $\exp(tA)$ and $\exp(tB)$ with number of generation $2^{n-1}+5$ and $\{A,B\}_{\text{L.A.}} = so(n)$. If $B$ also belongs to $[\alpha_k]$, then the number of generation is $2^{n-1}+3$.*

*Proof.* Let

$$\Pi_1 = \begin{pmatrix} 1 & 2 & \dots & n-k & n-k+1 & \dots & n \\ k+1 & k_2 & \dots & n & 1 & \dots & k \end{pmatrix}$$

be a permutation on $n$ letters. $\Pi_1 = \Pi^k$ where $\Pi$ is defined above. A standard result is that, since $n$ and $k$ are coprime, $\Pi^k$ is conjugate to $\Pi$, that is, there exists a permutation $\Pi_C$ s.t. $\Pi_C \Pi \Pi_C^{-1} = \Pi^k . \Pi_C$ is defined by $\Pi_C(i) = (i-1)k+1$ if $(i-1)k+1 \leq n$, $\Pi_C(i) = j$ if $(i-1)k+1 \equiv j \bmod n$. Clearly, if $P_{\Pi_C}$ is a permutation matrix satisfying $P_{\Pi_C} e_i = \alpha_i e_{\Pi_C(i)}$, $\prod_{i=1}^n \alpha_i = 1$ (respectively, $-1$), if $n$ is odd (respectively, even), the automorphism of $so(n)$ defined by $X \mapsto P_{\Pi_C} X P_{\Pi_C}^{-1}$ also defines a one-to-one map from $[\alpha_1]$ into a subset $S$ of $\pm[\alpha_k]$ where $S$ is such that, if $A_{ij} \in S$, then $A_{ji} \notin S$. Now, instead of the decomposition of $SO(n)$ as in the proof of Theorem 3.1, one takes

$$\begin{aligned}
\mathcal{A}_1 &= \mathbf{R}(P_{\Pi_C} A_{1n} P_{\Pi_C}^{-1}) + \mathbf{R}(P_{\Pi_C} A_{23} P_{\Pi_C}^{-1}),\\
\mathcal{A}_i &= \mathbf{R}(P_{\Pi_C} A_{i,i+1} P_{\Pi_C}^{-1}), \qquad i = 3, \ldots, n,\\
\mathcal{T}_{n-2} &= \mathbf{R}(P_{\Pi_C} A_{n-1,n} P_{\Pi_C}^{-1}),\\
\mathcal{T}_2 &= so(2) = \mathbf{R}(P_{\Pi_C} A_{12} P_{\Pi_C}^{-1}),
\end{aligned}$$

and so $SO(n)$ becomes written as a product of $2^{n-2}+2$ one-parameter subgroups generated by the elements of $[\alpha_k]$. The result follows in a similar way to the proof of Theorem 3.1. $\square$

**Example 3.1.** $g = so(5)$, $k = 2$.

$[\alpha_2] = \{A_{13}, A_{24}, A_{35}\} \cup \{A_{14}, A_{25}\}$ generates $so(5)$.

$\Pi_C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$,

$so(5) = \underbrace{so(3) \oplus so(2)}_{\mathcal{T}_1} \oplus \mathcal{P}_1,$

$$\begin{array}{cccc}
 & & [\alpha_2] & \\
A_{12} & A_{13} & A_{14} & A_{15} \\
 & A_{23} & A_{24} & A_{25} \\
 & & A_{34} & A_{35} \\
 & & & A_{45}
\end{array}$$

$\mathcal{P}_1 = \operatorname{span}\{A_{12}, A_{14}, A_{15}, A_{23}, A_{34}, A_{35}\}$,

$\mathcal{A}_1 = \mathbf{R}A_{14} + \mathbf{R}A_{35}$,

$\mathcal{T}_1 = \operatorname{span}\{A_{13}, A_{24}, A_{25}, A_{45}\}$, $so(2) = \mathbf{R}A_{13}$,

$so(3) = \text{span}\{A_{24}, A_{25}, A_{45}\} = \mathcal{T}_3 \oplus \mathcal{P}_3$, $\mathcal{P}_3 = \text{span}\{A_{24}, A_{45}\}$,

$\mathcal{T}_3 = \mathbf{R}A_{25}, \mathcal{A}_3 = \mathbf{R}A_{24}$,

$SO(5) = K_3 A_3 K_3 SO(2) A_1 SO(2) K_3 A_3 K_3$, $K_3 = \exp(\mathcal{T}_3)$,

$A_3 = \exp(\mathcal{A}_3)$, $A_1 = \exp(\mathcal{A}_1)$, $SO(2) = \exp(tA_{13})$, i.e.,

$SO(5) = \exp(t_1 A_{25}) \exp(t_2 A_{24}) \exp(t_3 A_{25}) \exp(t_4 A_{13}) \exp(t_5 A_{14})$

$\exp(t_6 A_{35}) \exp(t_7 A_{13}) \exp(t_8 A_{25}) \exp(t_9 A_{24}) \exp(t_{10} A_{25})$.

If $A, B$ are defined as in Theorem 3.3, $SO(5)$ becomes generated by $\exp(tA)$ and $\exp(tB)$ with order of generation 21 (19 if $B \in [\alpha_k]$).

The present work has been devoted to reducing the upper bound on the order of generation of $SO(n, \mathbf{R})$ (by one-parameter subgroups) to its minimum.

The following example shows that for $SO(7)$ the upper bound given by the Theorem 3.3 is not the minimum achievable.

**Example.** Let $G = SO(7)$, $\{A, B\}$ a pair of generators of $so(7)$ defined by $\exp(A) = P$, $P$ a permutation matrix satisfying $Pe_i = e_{i+1}$, $i = 1, \ldots, 6$, $Pe_7 = e_1$ and $B = A_{34}$. Since $B \in [\alpha_1]$, $X \in \{\exp(t \text{ ad} A) \cdot B, t \in \mathbf{R}\}$, $\forall X \in [\alpha_1]$. Only two decompositions of $SO(7)$ as in $(*)$, Section 2 having corresponding generating sets contained in $[\alpha_1]$ and giving different numbers of generation exist. By choosing the decomposition that gives the least number of generation and taking into account that $\forall X \in [\alpha_1]$ and $\forall t \in \mathbf{R}$, $\exp(tX) = \exp(\theta A) \exp(tB) \exp(-\theta A)$, for some $\theta$ depending on $X$, it follows from Theorem 3.1 and Theorem 4.2 that $\{A, B\}$ is uniformly completely controllable in at most $2^6 + 2 = 66$ switches. (See the Appendix for terminology.) However, if $SO(7)$ is decomposed as a product of one-parameter subgroups as in Lemma 2.2, although the corresponding generating set is not contained in $[\alpha_1]$, its elements can be obtained by brackets of elements in $[\alpha_1]$. Using Lemma 3.2 one can reduce the number of switches found previously. The diagram below illustrates the decomposition of $so(7)$ corresponding to the chosen symmetric space decomposition of $SO(7)$ and also shows which canonical basis elements have been selected as a generating set. ndbrace.tex

$$\begin{array}{cccccc}
uA_{12} & A_{13} & A_{14} & A_{15} & A_{16} & uA_{17} \\
 & uA_{23} & uA_{24} & A_{25} & A_{26} & A_{27} \\
 & & A_{34} & uA_{35} & A_{36} & A_{37} \\
 & & & uA_{45} & uA_{46} & A_{47} \\
 & & & & A_{56} & uA_{57} \\
 & & & & & uA_{67}
\end{array}$$

For the Lie group, one has $SO(7) = K_1 A_1 K_1$, $K_1 = SO(4) \times SO(3)$ $(= K_1^1 \times K_1^2)$ is the Lie group of

$$\mathcal{T}_1 = \operatorname{span}\{A_{12}, A_{13}, A_{23}\} \cup \operatorname{span}\{A_{ij}; i < j; i, j = 4, 5, 6, 7\},$$
$$A_1 = \exp(\mathcal{A}_1), \qquad \mathcal{A}_1 = \operatorname{span}\{A_{24}, A_{35}, A_{17}\}.$$

$K_1^1 = SO(4) = K_2 A_2 K_2$, $K_2 = SO(2) \times SO(2)$ is the Lie group of

$$\mathcal{T}_2 = \operatorname{span}\{A_{45}, A_{67}\}, \qquad A_2 = \exp(\mathcal{A}_2),$$
$$\mathcal{A}_2 = \operatorname{span}\{A_{46}, A_{57}\} \cdot K_1^2 = SO(3) = K_3 A_3 K_3,$$
$$K_3 = SO(2) = \exp(\tau A_{12}), \qquad A_3 = \exp(tA_{23}).$$

So, in the decomposition

$$SO(7) = K_2 A_2 K_2 K_3 A_3 K_3 A_1 K_3 A_3 K_3 K_2 A_2 K_2,$$

since $K_2, K_3, A_1, A_2$ and $A_3$ are all abelian subgroups, $SO(7)$ may be decomposed as a product of one-parameter subgroups generated by the elements selected from the diagram above. Hence, $\exp(tX)$ appears once, twice or four times in the decomposition depending on whether $X$ belongs to $\{A_{24}, A_{35}, A_{17}\}$, $\{A_{46}, A_{57}\}$ or $\{A_{12}, A_{23}, A_{45}, A_{67}\}$, respectively. Now, $[A_{34}, A_{23}] = -A_{24}$ and $[A_{34}, A_{45}] = A_{35}$, so $\forall t \in \mathbf{R}$, $\exp(tA_{24})$ and $\exp(tA_{35})$ may be written as a product of five elements from $\exp(\tau A)$ and $\exp(\theta B)$ ($\{A, B\}$ as above) and $[A_{45}, A_{56}] = A_{46}$, $[A_{56}, A_{67}] = A_{57}$. So, seven elements from $\exp(\tau A)$ and $\exp(\theta B)$ are required for $\exp(tA_{46})$ and $\exp(tA_{57})$. All the other one-parameter subgroups in the decomposition may be written as $\exp(tA)\exp(\theta B)\exp(-tA)$, and the final result after composition of terms with the same generator is that $SO(7)$ is uniformly finitely generated by $\exp(tA)$ and $\exp(\tau B)$ with number of generations 65. So $\{A, B\}$ is uniformly controllable with at most 64 switches.

To determine the order of generation of $SO(n)$ with respect to a set of one-parameter subgroups that generate $SO(n)$, one has to find out how generators and decompositions relate to each other.

The first task to solve the uniform finite generation problem of $G$ is to characterize all the generators of the Lie algebra $\mathcal{L}(G)$ of a given Lie Group $G$. Although several important results have already been obtained (see Jurdjevic and Kupka [**4**], Jurdjevic and Sussmann [**5**], Kuranishi [**10**] and also Theorem 3.2, Chapter I in Silva Leite [**17**]), a complete characterization is far from being accomplished even when $G$ is a semisimple Lie group of matrices and the generators are restricted to pairs $\{A, B\}$, which are known to exist. When $G$ is noncompact and its Lie algebra is generated by a set of compact elements ($X \in \mathcal{L}(G)$ is called compact if the one-parameter subgroup it generates, $\exp(tX)$, $t \in \mathbf{R}$ is compact), the order of generation of $G$ corresponding to these generators is infinite.

Decompositions of $G$ based on symmetric spaces may be used to determine the order of generation of $G$ by one-parameter subgroups generated by elements of $\mathcal{L}(G)$. For the classical matrix Lie groups, involutive automorphisms always exist and such decompositions are always possible. When $G$ is connected and compact, the exponential map is onto and a prior knowledge of a set of generators of the Lie algebra $\mathcal{L}(G)$ is not necessary since the decomposition itself provides a corresponding generating set $\{\exp(tX_i), i = 1, \dots, k, t \in \mathbf{R}\}$ of $G$ and consequently a set $\{X_i, i = 1, \dots, k\}$ of generators of $\mathcal{L}(G)$.

For the noncompact case decompositions other than the Cartan decomposition may be used with success. For instance, the Iwasawa and the Bruhat decompositions can both be considered for noncompact Lie groups.

The $SO(n)$ case appears to be the easiest one among all the classical groups of matrices due to the compactness of $SO(n)$, the very simple structure of the canonical basis of $so(n)$ and the existence of permutation matrices in $SO(n)$, which have been an important tool in the present work. As a consequence, a complete solution for $SO(n)$ may yield solutions to the same problem for other groups such as $SO_0(p,q)$ or $SL(n,\mathbf{R})$ (note that $SO(p)\times SO(q)$ and $SO(n)$ are the maximal compact subgroups of $SO_0(p,q)$ and $SL(n,\mathbf{R})$, respectively). This and the important role that generators of $so(n)$ play in constructing uniformly completely controllable vector fields on any paracompact and connected $C^k$-manifold (see Levitt and Sussmann [**11**]) are, in the author's opinion, good reasons for looking primarily to the order of generation problem of the special orthogonal group.

## Appendix
## On the Uniform Generation of $SO(3,R)$

In 1971, F. Lowenthal [**13**] proved that the order of generation of $SO(3)$ by two one-parameter rotations is a function of the angle $\psi$ between the axes of the two rotations, being three if $\psi=\pi/2$ and $k+2$ if $\psi\in[\pi/(k+1),\pi/k)$. The proof of this result is rather long. Instead of working with $SO(3)$, Lowenthal works with the induced subgroup of the Möbius group, and Tchebychev polynomials play an important role in the proof.

When $\psi\in[\pi/2k,\pi/(2k-1))$, $k\geq 2$, a much shorter proof was found to determine the order of generation of $SO(3)$. Although, when $\psi\in[\pi/(2k-1),\pi/(2k-2))$, our result is not as good as Lowenthal's, the complete proof, in both cases, is included here. Unlike the previous methods for $SO(n)$, we do not use decompositions of $SO(3)$ based on symmetric spaces.

**Theorem 4.1.** *$SO(3)$ is uniformly finitely generated by any two one-parameter subgroups $\exp(tA_1)$ and $\exp(tA_2)$ unless $[A_1,A_2]=0$.*

*Proof.* Since $so(3)$ (the set of all $3\times 3$ skew symmetric real matrices) is isomorphic to $\mathbf{R}^3$ with the Lie bracket corresponding to the vector product, it is clear that, if $A_1$ and $A_2$ are any two elements of $so(3)$ that do not commute, then $\{A_1,A_2,[A_1,A_2]\}$ is a basis of $so(3)$ and $\{A_1,A_2\}_{\text{L.A.}}=so(3)$. Every rotation of $SO(3)$ is a plane rotation and, as a consequence, $\exp(tA_1)$ and $\exp(tA_2)$ are compact. Now, Theorem 1.1 applies since $SO(3)$ is connected and compact and the result follows.

□

**The Main Theorem.** *The order of generation of $SO(3)$ by the two one-parameter rotations $\exp(tA_1)$ and $\exp(tA_2)$ is three if $\psi = \pi/2$ and if $\psi \in [\pi/2(k-1), \pi/2(k-2))$, $k \geq 3$, the order of generation is $2k-1$. ($\psi$ is the angle between the axes of the two rotations).*

The term "order of generation" is not correctly used here when $\psi \in [\pi/(2k-1), \pi/(2k-2))$; instead, "the number of generation" should be used. However, for the sake of simplicity, the former is preferred to the latter.

Several lemmas are needed to prove this theorem.

For every vector $x = (x_1, x_2, x_3) \in \mathbf{R}^3$, a skew symmetric matrix

$$X = \begin{pmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{pmatrix},$$

formed with the components of $x$, is defined. It is easy to prove that $\exp(tX)x = x$, $\forall t \in \mathbf{R}$, that is, $x$ is the axis of the rotation $\exp(tX)$. In fact, $\exp(tX)x = x + tXx + (t^2/2!)X^2x + \cdots$, and since $Xx = 0$, the result follows. The one-parameter subgroup $\exp(tX)$ is called the isotropy group at $x$.

**Lemma 4.1.** *$\forall R \in SO(3)$ and $\forall x, y \in \mathbf{R}^3$ with $||x|| = ||y||$, $Rx = y$ if and only if $R\exp(tX)R^{-1} = \exp(tY)$.*

*Proof.* Without loss of generality, we can assume $||x|| = ||y|| = 1$. $SO(3)$ acting on $S^2$ sets up an equivalence relation on $S^2$. The equivalence class containing a point $x$ is the range of the function $\Phi_x : SO(3) \to S^2$ defined by $\Phi_x(R) = Rx$, and we call it the orbit of $x$. Since $Rx = y$, $x$ and $y$ are equivalent. Now, the result is a consequence of the fact that isotropy groups at equivalent points of $S^2$ are conjugate subgroups.

**Lemma 4.2.** *Every rotation $R \in SO(3)$ is representable as a product $R = \exp(t_1X)\exp(t_2Y)\exp(t_3Z)$, $t_i \in \mathbf{R}$, $i = 1, 2, 3$ if and only if $y$ is perpendicular to $x$ and $z$.*

FIGURE 4.1.

The proof of this lemma can be found in Davenport [**2**]. It is assumed that $x$ and $z$ may be equal. If that is the case, then Lemma 4.2 states the same thing as the first part of the main theorem. If not only $x$ and $z$ are equal but also $x$ and $y$ are two orthogonal unit vectors in $\mathbf{R}^3$, the representation of $R$ in Lemma 4.2 is the Euler representation of a rotation by three angular parameters, the Euler angles.

Now, let $a_1$ and $a_2$ be two linearly independent vectors of $\mathbf{R}^3$ and $\psi = \measuredangle(a_1, a_2)$ the angle between them. $a_1$ and $a_2$ generate a plane $\Pi$. Without loss of generality, $a_1$ and $a_2$ can be assumed to be unit vectors. Let $\{a_1, a_2, a_3, \dots\}$ be a sequence of vectors on $\Pi$, where $\forall i \geq 3$, $a_i = \exp(\pi A_{i-1})a_{i-2}$. ($A_j$ is the skew symmetric matrix corresponding to $a_j$, $\forall j$.) $\measuredangle(a_i, a_{i+1}) = \psi$, $\forall i \geq 1$, and $\measuredangle(a_1, a_i) = (i-1)\psi$, $\forall i \geq 1$. Let $a_k$ be the first element in the sequence satisfying $\measuredangle(a_1, a_k) \geq \pi/2$, i.e., $(k-1)\psi \geq \pi/2$ or $\psi \geq \pi/2(k-1)$. (See Figure 4.1.) Clearly, there exists a vector $x \in \Pi_1$ ($\Pi_1$ is the plane perpendicular to $a_1$) such that $x = \exp(tA_{k-1})a_{k-2}$ for some $t \in (0, 2\pi]$. Since $a_1$ and $x$ are perpendicular, Lemma 4.2 can be applied and $\forall R \in SO(3)$,

$$R = \exp(t_1 A_1) \exp(t_2 X) \exp(t_3 A_1), \qquad t_i \in \mathbf{R}. \tag{4.1}$$

At this stage the aim is to write $\exp(t_2 X)$ as a product of elements from the one-parameter subgroups $\exp(tA_1)$ and $\exp(tA_2)$.

Since $a_i = \exp(\pi A_{i-1})a_{i-2}$, $i \geq 3$, and $x = \exp(tA_{k-1})a_{k-2}$, for some $t$, using Lemma 4.1 it follows that, $\forall i \geq 3$ and $\theta \in \mathbf{R}$,

$$\exp(\theta A_i) = \exp(\pi A_{i-1}) \exp(\theta A_{i-2}) \exp(-\pi A_{i-1}), \tag{4.2}$$

and

$$\exp(\theta X) = \exp(tA_{k-1}) \exp(\theta A_{k-2}) \exp(-tA_{k-1}). \tag{4.3}$$

Notation. In the next two lemmas, $e^{tX}$ stands for $\exp(tX)$.

**Lemma 4.3.** *Let $A_i$, $i = 1, 2, \ldots$, be defined as before. Then, $\forall \theta \in \mathbf{R}$,*

$$e^{\theta A_i} = \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2} e^{\pi A_1}}_{i-2} e^{\theta A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{i-2}, \tag{4.4}$$

*if $i = 2n$, and*

$$e^{\theta A_i} = \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2} e^{\pi A_1} e^{\pi A_2}}_{i-2} e^{\theta A_1} \underbrace{e^{-\pi A_2} e^{-\pi A_1} \cdots e^{-\pi A_2}}_{i-2}, \tag{4.5}$$

*if $i = 2n + 1$.*

*Proof* (by induction). It will be proved first that the lemma is true for $i = 2$ and $i = 3$. Then, assuming that it is true for $i = 2m - 2$ and $i = 2m - 1$ it will be proved to be true also for $i = 2m$ and $i = 2m + 1$, $m \in \mathbf{N}$.

The relation (4.4) is trivial when $i = 2$. When $i = 3$, both (4.5) and (4.2) are the same relation, so (4.5) is true when $i = 3$.

Now, from (4.2) with $i = 2m$,

$$e^{\theta A_{2m}} = e^{\pi A_{2m-1}} e^{\theta A_{2m-2}} e^{-\pi A_{2m-1}},$$

and since (4.4) and (4.5) are assumed to be satisfied when $i = 2m - 2$ and $i = 2m - 1$, respectively, it follows that

$$\begin{aligned} e^{\theta A_{2m}} &= \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2}}_{2m-3} e^{\pi A_1} \underbrace{e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-3} \underbrace{e^{\pi A_2} \cdots e^{\pi A_1}}_{2m-4} e^{\theta A_2} \\ &\quad \underbrace{e^{-\pi A_1} e^{-\pi A_2} \cdots e^{-\pi A_2}}_{2m-4} \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2}}_{2m-3} e^{-\pi A_1} \\ &\quad \underbrace{e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-3} \\ &= \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2}}_{2m-3} e^{\pi A_1} e^{-\pi A_2} e^{\theta A_2} e^{\pi A_2} e^{-\pi A_1} \\ &\quad \underbrace{e^{-\pi A_2} \ldots e^{-\pi A_1} e^{-\pi A_2}}_{2m-3} \\ &= \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2} e^{\pi A_1}}_{2m-2} e^{\theta A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2}. \end{aligned}$$

Similarly, from (4.2) with $i = 2m + 1$

$$e^{\theta A_{2m+1}} = e^{\pi A_{2m}} e^{\theta A_{2m-1}} e^{-\pi A_{2m}},$$

and since (4.4) and (4.5) are assumed to be satisfied when $i = 2m$ and $i = 2m - 1$, respectively, it follows that

$$\begin{aligned} e^{\theta A_{2m+1}} &= \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2} e^{\pi A_1}}_{2m-2} e^{\pi A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2} \\ &\quad \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2}}_{2m-3} e^{\theta A_1} \underbrace{e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-3} \\ &\quad \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2} e^{\pi A_1}}_{2m-2} e^{-\pi A_2} \underbrace{e^{-\pi A_1} e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2} \\ &= \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\theta A_2} e^{\pi A_1}}_{2m-2} e^{\pi A_2} e^{-\pi A_1} e^{\theta A_1} e^{\pi A_1} \\ &\quad \underbrace{e^{-\pi A_2} e^{-\pi A_1} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-2} \\ &= \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2}}_{2m-1} e^{\theta A_1} \underbrace{e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{2m-1}, \end{aligned}$$

and the lemma is proved. ◻

**Lemma 4.4.** *If the angle* $\psi = \measuredangle(a_1, a_2) \in [\pi/2(k-1), \pi/2(k-2))$, $k \geq 3$, *then, for some* $t \in (0, 2\pi]$ *and* $\theta \in \mathbf{R}$,

$$e^{\theta X} = \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_2}}_{k-3} e^{tA_1} e^{\theta A_2} e^{-tA_1} \underbrace{e^{-\pi A_2} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{k-3}, \tag{4.6}$$

*if* $k$ *is even, and*

$$e^{\theta X} = \underbrace{e^{\pi A_2} e^{\pi A_1} \cdots e^{\pi A_1}}_{k-3} e^{tA_2} e^{\theta A_1} e^{-tA_2} \underbrace{e^{-\pi A_1} \cdots e^{-\pi A_1} e^{-\pi A_2}}_{k-3}, \tag{4.7}$$

*if* $k$ *is odd.*

*Proof.* $e^{tA_{k-1}}$ and $e^{\theta A_{k-2}}$ can be written as a product of elements from $e^{\tau A_1}$ and $e^{\tau A_2}$ ($t \in \mathbf{R}$) by using (4.4) and (4.5), respectively, if $k$ is even, or (4.5) and (4.4), respectively, if $k$ is odd. Now, using (4.3) and taking into account the composition of terms with the same generator, the relations (4.6) and (4.7) follow. □

*Proof of the Main Theorem.* When $\psi = \pi/2$, the result is an immediate consequence of Lemma 4.2 with $x = z = a_1$ and $y = a_2$; the order of generation is then equal to three. When $\psi \in [\pi/2(k-1), \pi/2(k-2))$ it was seen that $\exists\ x \in \mathbf{R}^3$, $x$ perpendicular to $a_1$, such that $R = \exp(t_1 A_1) \exp(t_2 X) \exp(t_3 A_1)$, for every $R \in SO(3)$ and $t_i \in \mathbf{R}$. But $\exp(t_2 X)$ can be written as a product of $2(k-3)+3$ elements from the one-parameter subgroups $\exp(\tau_1 A_1)$ and $\exp(\tau_2 A_2)$ (Lemma 4.4) and so, the order of generation of $SO(3)$ is, in this case, $2(k-3)+3+2 = 2k-1$, $\forall k \geq 3$, which completes the proof. □

*Remark* . Since there exists an automorphism of $SO(3)$ that interchanges the two one-parameter subgroups $\exp(tA_1)$ and $\exp(\tau A_2)$, every element of $SO(3)$ can also be written as a product of $2k-1$ elements from those subgroups whose first and last elements belong to $\exp(tA_2)$.

We now apply the results on the uniform finite generation of $SO(3)$ to the study of the controllability properties of systems which are described by an equation in $SO(3)$, of the form

$$\dot{x}(t) = (u(t)A + v(t)B)x(t) \tag{4.8}$$

where $\{A, B\}_{\text{L.A.}} = so(3)$ and $u(t)$ and $v(t)$ are piecewise continuous control functions. A system (4.8) is said to be uniformly controllable if there exists a positive integer $N$ such that every pair of points in $G$ can be joined by a trajectory of $\{u(t)A + v(t)B\}$ which involves, at most, $N$ switches.

**Theorem 4.2.** *If $k$ is the order of generation of $SO(3)$ by* $\exp(tA)$ *and* $\exp(tB)$*, then the system* (4.8) *is uniformly controllable by a trajectory of $\{A, B\}$ in, at most, $N = k - 1$ switches.*

*Proof.* Since the one-parameter subgroups of $SO(3)$ are compact,

$$\forall \theta > 0, \ \exists \, \zeta > 0 : \ \forall X \in so(3), \ \exp(-\theta X) = \exp(\zeta X).$$

Then, in the decomposition of $SO(3)$ as a product of one-parameter subgroups, we can always make the parameters positive. Using the definition of uniform controllability we can conclude that every point in $SO(3)$ can be reached from the identity of the group by a trajectory of $\{A, B\}$ involving at most $k - 1$ switches. Now, the result follows since $SO(3)$ is a group.

The easy way of calculating the order of generation of $SO(3)$, by any two one-parameter subgroups and the complete characterization of generators $\{A, B\}$ of $so(3)$, have as a consequence that not just symmetric systems on $SO(3)$ (as (4.8)) but also systems of the form

$$\dot{x}(t) = (A + v(t)B)x(t), \qquad x \in SO(3) \tag{4.9}$$

($v(t)$ a piecewise continuous control function) are uniformly controllable.

**Lemma 4.5.** *If $[A, B] \neq 0$, the systems* (4.8) *and* (4.9) *are uniformly controllable, and there exist controls such that every pair of points in* $SO(3)$ *can be joined by a trajectory of the system only with two switches.*

*Proof.* $a$ and $b$ denote the axes of the rotations $\exp(tA)$ and $\exp(\tau B)$, respectively. Let $\psi = \measuredangle(a, b) \in [\pi/(k+1), \pi/k)$, $k \geq 2$. For every pair of vectors $(a, b)$ in $\mathbf{R}^3$, there exist constants $u_1$ and $v_1$ such that $(u_1 a + v_1 b) \perp a$. So $\forall g \in SO(3)$, $\exists \ t_1, t_2, t_3 \in \mathbf{R}$ such that

$g = \exp(t_1 A)\exp((u_1 A + v_1 B)t_2)\exp(At_3)$ (Lemma 4.2). Clearly, the $t$'s can be taken nonnegative. Now choose

$$u(t) = \begin{cases} u_1, & t \in (t_3, t_2 + t_3] \\ 1, & t \in [0, t_3] \cup (t_2 + t_3, t_2 + t_3 + t_1] \end{cases}$$
$$v(t) = \begin{cases} v_1, & t \in (t_3, t_2 + t_3] \\ 0, & \text{otherwise.} \end{cases}$$

Then, every pair of points of $SO(3)$ can be joined by a trajectory of the system (4.8) (trajectory of $A$ and $u_1 A + v_1 B$) involving two switches. For the system (4.9) just make $u_1 = 1$ and the result follows.

Applications of the uniform finite generation problem of $SO(n)$ and other Lie groups to control theory will be considered in a forthcoming article.

## REFERENCES

**1.** P. Crouch and F. Silva Leite, *On the uniform finite generation of* $SO(n, \mathbf{R})$, Systems Control Lett. II (4).

**2.** P. Davenport, *Rotations about nonorthogonal axes*; AIAA J. **11** (6) (1973).

**3.** S. Helgason, *Differential Geometry, Lie groups and symmetric spaces*, Academic Press, New York, 1978.

**4.** V. Jurdjevic and I. Kupka, *Control Systems on semi-simple Lie groups and their homogeneous spaces*, Ann. Inst. Fourier (Grenoble) **31** (4) (1981), pp. 151–179.

**5.** V. Jurdjevic and H. Sussmann, *Controllability of nonlinear systems*, J. Differential Equations **12** (1972), pp. 95–116.

**6.** ——— and ———, *Control systems on Lie groups*, J. Differential Equations **12** (1972), pp. 313–329.

**7.** R. Koch and F. Lowenthal, *Uniform finite generation of three-dimensional linear Lie groups*, Canad. J. Math. **27** (1975), pp. 396–417.

**8.** ——— and ———, *Uniform finite generation of Lie groups locally isomorphic to* $SL(2, \mathbf{R})$, Rocky Mountain J. Math. **7** (4) (1977), pp. 707–724.

**9.** ——— and ———, *Uniform finite generation of complex Lie groups of dimension two and three*, Rocky Mountain J. Math. **10** (2) (1980), pp. 319–331.

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

**11.** N. Levitt and H. Sussmann, *On controllability by means of two vector fields*, SIAM J. Control **13** (6) (1975), pp. 1271–1281.

**12.** F. Lowenthal, *Uniform finite generation of the isometry groups of Euclidean and non-Euclidean geometry*, Canad. J. Math. **23** (1971), pp. 364–373.

**13.** ———, *Uniform finite generation of the rotation group*, Rocky Mountain J. Math. **1** (1971), pp. 575–586.

**14.** ———, *Uniform finite generation of the affine group*, Pacific J. Math. **40** (1972), pp. 341–348.

**15.** ———, *Uniform finite generation of $SU(2)$ and $SL(2, \mathbf{R})$*, Canad. J. Math. **24** (1972), pp. 713–727.

**16.** J. Marsden and R. Abraham, *Foundation of Mechanics*; Benjamin, Menlo Park, 1978.

**17.** F. Silva Leite, *Uniform finite generation of the orthogonal group and applications to Control theory*, Ph.D. Thesis, Warwick Univ., Nov. 1982.

**18.** S. Sternberg, *Lectures on Differential Geometry*, Prentice-Hall, Englewood Cliffs, New York, 1964.

**19.** J. Wolf, *Spaces of constant curvature*, Publish or Perish, Houston, 1977.

Departamento de Matemática, Universidade de Coimbra, 3000 Coimbra, Portugal