ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 1, Number 4, Fall 1971

UNIFORM FINITE GENERATION OF THE ROTATION GROUP

FRANKLIN LOWENTHAL

I. **Introduction.** Since the rotation group $SO(3)$ has no two dimensional connected Lie subgroups, the subgroup generated by two different one-parameter rotation groups T_ϕ and S_θ is in fact just $SO(3)$. If a Lie group H is generated by two one-parameter subgroups, one says H is uniformly finitely generated by them if there exists a positive integer n such that every element of H can be expressed as a product of elements chosen alternately from the two one-parameter subgroups whose length is at most n. Define the least such n as the order of generation of H.

The fact that $SO(3)$ is uniformly finitely generated by T_ϕ and S_θ is a simple consequence of its being compact; an elegant proof of this involving Baire category theory was suggested to the author by R. B. Burckel and is included in the Appendix. The goal of this paper is to compute the order of generation of $SO(3)$ by T_ϕ and S_θ. This will be determined as a function of the angle ψ, $0 < \psi \leqq \pi/2$, between the axes of the rotation groups T_ϕ and S_θ without any prior knowledge that $SO(3)$ was uniformly finitely generated by them. It turns out that if $\psi = \pi/2$, the order of generation is 3; if $\pi/(k+1) \leqq \psi < \pi/k$, then the order of generation is $k + 2$ ($k \geqq 2$).

Instead of working with $SO(3)$ itself, it will be more convenient to work with the induced subgroup of the Möbius group, called the isometry group of the spherical geometry and denoted by G. This has the disadvantage that the role of the angle π/k is obscured. It is, of course, possible to translate the entire proof back to the sphere where π/k enters in a natural manner; this will be described briefly at the end of the paper. However, the author believes the ideas involved in the proof are easier to visualize in the extended complex plane. Further, it will be interesting that the Tchebyshev polynomials turn out to play a central role in the proof presented here.

II. **Preliminaries.** Let the sphere have center at $(0, 0, \frac{1}{2})$ and radius $\frac{1}{2}$; let the axes of the rotation groups be the z axis and the line: $y = 0$, $z = \frac{1}{2} - (\cot \psi)x$. These determine as fixed points of the rotations the respective pair of points $(0, 0, 1)$, $(0, 0, 0)$ and $(-(\sin \psi)/2, 0, (1 + \cos \psi)/2)$, $((\sin \psi)/2, 0, (1 - \cos \psi)/2)$ on the sphere. Under

Received by the editors January 5, 1970.

AMS 1970 *subject classifications.* Primary 50C05; Secondary 33A65, 22E99.

Copyright © Rocky Mountain Mathematics Consortium

stereographic projection, T_ϕ and S_θ correspond respectively to the one-parameter subgroups of the Möbius group

$$(1)\qquad W = T_t(z) = e^{it}z, \qquad 0 \leqq t \leqq 2\pi,$$

$$(2)\qquad W = S_s'(z) = K^{-1}(e^{is}K(z)), \qquad 0 \leqq s \leqq 2\pi,$$

where

$$K(z) = \frac{z - r}{z + 1/r}, \qquad r = \tan\frac{\psi}{2}.$$

These are just all elliptic transformations with fixed points 0, ∞ and r, $-1/r$ respectively; T_t and S_s' generate G. The Möbius transformation $W = L(z) = rz$ leaves 0 and ∞ fixed and takes 1 into r, $-1/r^2$ into $-1/r$; let $x = 1/r^2$. The inner automorphism induced by $L(z)$ leaves T_t invariant and transforms S_s' into S_s^x, the group of all elliptic transformations with fixed points 1 and $-x$; $x = \cot^2(\psi/2)$. T_t and S_s^x generate the group $G_x = L^{-1}GL$ ($G_1 = G$). The order of generation of G by T_t and S_s' is the same as the order of generation of G_x by T_t and S_s^x.

The infinitesimal generators of T_t and S_s^x are $\epsilon = iw$, $\eta_x = i(w-1)(w+x)$ respectively, i.e., $T_t(z)$ and $S_s^x(z)$ are respectively the solutions of the differential systems [1]

$$(3)\qquad dw/dt = iw, \qquad w(0, z) = z,$$

$$(4)\qquad dw/ds = i(w-1)(w+x), \quad w(0, z) = z.$$

$SO(3)$ is transitive; in fact, if P_1, Q_1 and P_2, Q_2 are two pairs of points such that the distance on the sphere between P_1 and Q_1 equals the distance between P_2 and Q_2, then there is a rotation taking P_1 into P_2 and Q_1 into Q_2 and there is a rotation taking P_1 into Q_2 and Q_1 into P_2. Applying this result to the fixed points of the rotations T_ϕ and S_θ that lie in the northern and southern hemisphere respectively, i.e. $(0, 0, 1)$ and $(-(\sin\psi)/2, 0, (1+\cos\psi)/2)$ and $(0, 0, 0)$ and $((\sin\psi)/2, 0, (1-\cos\psi)/2)$, it is seen that there are Möbius transformations $V_x(z)$ and $W_x(z)$ in G_x such that

$$(5)\qquad V_x(\infty) = 0, \qquad V_x(-x) = 1,$$

$$(6)\qquad W_x(\infty) = 1, \qquad W_x(-x) = 0.$$

Since G_x is transitive, it is meaningful to define for any pair of points α and β in the extended complex plane the order of α with respect to β, written $\mathrm{ord}_\beta(\alpha)$, as the smallest positive integer n such that there exists a product of T_t and $S_s{}^x$ of length n taking α into β.

The set of all rotations of the sphere taking a prescribed point P into a prescribed point Q transform a point P' different from P (and from the antipodal point of P) into a circle on the sphere; thus under the set of all Möbius transformations of G_x taking α into β the possible images of a point $\alpha' \neq \alpha$, $\alpha' \neq -1/r^2\bar{\alpha}$ constitute either a circle or a line in the extended complex plane. In particular if $\beta = 0$, this set is a circle centered at the origin. If $R(z)$ is a transformation in G_x such that $R(\alpha) = 0$ then every Möbius transformation in G_x taking α into 0 has a representation of the form

$$T_t\, R(z) \qquad \text{for some } t,\ 0 \leqq t \leqq 2\pi. \tag{7}$$

Hence, if $m(x) = \operatorname{ord}_0(\alpha)$, then every Möbius transformation in G_x taking α into 0 can be represented as a product of T_t and S_s of length $\leqq m(x) + 1$.

III. Since $x = \cot^2(\psi/2)$, the result about $SO(3)$ mentioned in the Introduction is an immediate consequence of the theorem below:

THEOREM. *The order of generation of G by T_t and $S_s{}^1$ is three. For x satisfying*

$$\cot^2\frac{\pi}{2k} < x \leqq \cot^2\frac{\pi}{2(k+1)}, \tag{8}$$

the order of generation of G_x by T_t and $S_s{}^x$ is $k+2$ for $k = 2, 3, 4, \cdots$.

PROOF. Define the orbit of z_0 under ϵ to be $\{T_t(z_0) : 0 \leqq t \leqq 2\pi\}$; for $z_0 \neq 0, \infty$, these orbits are the circles $|z| = k$. For $z_0 \neq 1, -x$, the orbit of z under η_x is the circle of Apollonius with respect to 1 and $-x$ that passes through z_0.

Case $x = 1$. The orbit of 0 under η_1 is the imaginary axis. Clearly $\operatorname{ord}_0(\alpha) = 2$ if α is not on the imaginary axis and $\operatorname{ord}_0(\alpha) = 1$ if $\alpha = ai$, a real, $a \neq 0$. Hence by the remark at the end of §II, order of generation of G is at most 3. But the transformation W_1 that takes $\infty \to 1$, $-1 \to 0$ cannot be expressed as a product of length 2 since in fact the first element of the product must leave either -1 or ∞ fixed and $\operatorname{ord}_{-1}(0) = \operatorname{ord}_\infty(1) = 2$.

For $x > 1$, the orbit of 0 under η_x is the circle $|(z-1)/(z+x)| = 1/x$; this circle (denoted by K_x) intersects the real axis at the points 0 and $2x/(x-1)$. The line $R(z) = (1-x)/2$ is the orbit of ∞ under η_x; the circles of Apollonius $|(z-1)/(z+x)| = k$ with $0 < k < 1$ lie in the half-plane $R(z) > (1-x)/2$; those with $k > 1$ lie in the half-plane $R(z) < (1-x)/2$.

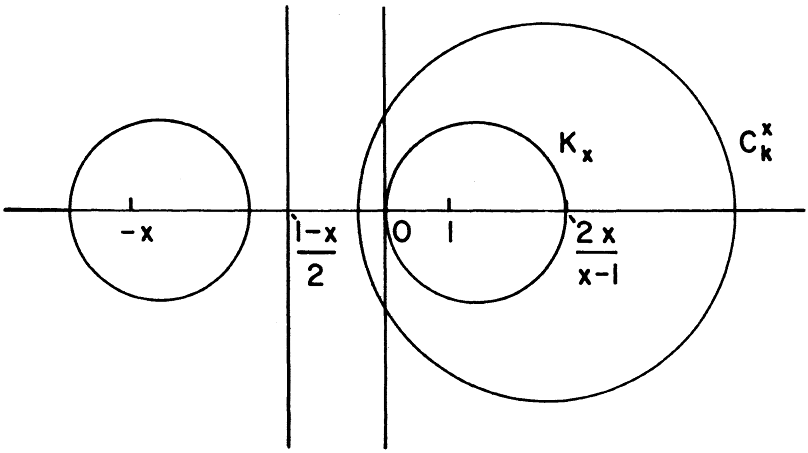

FIGURE 1. Orbits under η_x.

For $1/x < k < 1$, the circle of Apollonius $|(z-1)/(z+x)| = k$, denoted by $C_k{}^x$, intersects the negative real axis at a point greater than $(1-x)/2$; this point minimizes the distance between points on $C_k{}^x$ and the origin. Observe that this minimum distance increases from 0 to $(x-1)/2$ as k increases from $1/x$ to 1 or if one expresses this minimum distance from $C_k{}^x$ to 0 as a function of the point where $C_k{}^x$ intersects the positive real axis, then as the latter increases from $2x/(x-1)$ to ∞, the distance increases from 0 to $(x-1)/2$. Note that the circle of Apollonius through the point u on the positive real axis, $u \geqq 2x/(x-1)$, lies, except for the point of tangency, in the interior of the circle $|z| = u$. Further the distance of the circle of Apollonius through $z = ue^{i\theta}$ from the origin, considered as a function of θ, is a minimum when $\theta = 0$, i.e., for the point $z = u$.

To determine $m(x) = \mathrm{ord}_0(\alpha)$, it suffices to find the smallest positive integer such that there is a product of T_t and $S_s{}^x$ of that length taking α into some point on K_x and then to add one to that integer. Observe that a transformation on G_x of minimum length taking α to 0 must end with an $S_s{}^x$. Thus $\mathrm{ord}_0(-x)$ must always be even, as a transformation of minimum length taking $-x$ into 0 must begin with a T_t; similarly $\mathrm{ord}_0(\infty)$ is odd.

LEMMA 1. *If* $\mathrm{ord}_0(-x) = 2q$, *q a positive integer, then*

$$S_s{}^xT_tS_\pi{}^xT_\pi \cdots S_\pi{}^xT_\pi(z),$$

a product of length $2q$, *takes* $-x$ *into* 0 *for appropriate choices of* t *and* s.

Proof. If $q = 1$ there is nothing to prove; assume $q > 1$. It suffices to prove that $|S_\pi^x T_\pi \cdots S_\pi^x T_\pi(-x)| \leqq 2x/(x-1)$, where the product $S_\pi^x T_\pi$ is repeated $q-1$ times. As the $\text{ord}_0(-x) = 2q$, there is a product

$$S_{s_{q-1}}^x T_{t_{q-1}} \cdots T_{t_2} S_{s_1}^x T_{t_1}$$

which takes $-x$ into a point whose absolute value is at most $2x/(x-1)$. Note that S_π^x takes the real axis into itself so that $S_\pi^x(u)$, $u > 2x/(x-1)$, is the point on the orbit of u under η_x closest to the origin. Since $q > 1$, $T_\pi(-x) > 2x/(x-1)$. Clearly

$$-S_\pi^x T_\pi(-x) \leqq |S_{s_1}^x T_{t_1}(-x)|. \tag{9}$$

If $q = 2$, the lemma is proved; if $q > 2$ then if $p = S_\pi^x T_\pi(-x)$, $-p > 2x/(x-1)$. If $|z_0| \geqq -p$, then

$$-S_\pi^x T_\pi(p) \leqq |S_s^x T_t(z_0)| \tag{10}$$

for all possible s, t. Hence by induction

$$\underbrace{-S_\pi^x T_\pi \cdots S_\pi^x T_\pi}_{(2q-2 \text{ factors})}(-x) \leqq |S_{s_{q-1}}^x T_{t_{q-1}} \cdots S_{s_1}^x T_{t_1}(-x)|. \tag{11}$$

Lemma 2. *If* $\text{ord}_0(\infty) = 2q + 1$, *then for some choice of* s, t, *there exists a product:* $S_s^x T_t S_\pi^x T_\pi \cdots S_\pi^x T_\pi S_\pi^x$ *of length* $2q + 1$ *taking* ∞ *into* 0.

Proof. Same as Lemma 1. Observe that $S_\pi^x(\infty) = (1-x)/2$.

Lemma 3. $\text{ord}_0(-x) \geqq \text{ord}_0((1-x)/2)$.

Proof. This is clear as $x \geqq (x-1)/2$ and as the first element in a product of minimum length taking $-x$ into 0 must be a T_t.

Lemma 4. $\text{ord}_0(\infty) = \text{ord}_0((1-x)/2) + 1$.

Proof. Since $S_\pi^x(\infty) = (1-x)/2$. $\text{ord}_0(\infty) \leqq \text{ord}_0((1-x)/2) + 1$. Further there must be at least one point on $R(z) = (1-x)/2$ whose order with respect to zero is one less than the order of ∞ with respect to zero. But clearly $\text{ord}_0((1-x)/2) \leqq \text{ord}_0(z)$ for all z satisfying $R(z) = (1-x)/2$.

Lemma 5. $\text{ord}_0(\infty) = \text{ord}_0(-x) \pm 1$.

From the previous two lemmas $\text{ord}_0(-x) \geqq \text{ord}_0(\infty) - 1$. If $x \leqq 2x/(x-1)$, then $\text{ord}_0(-x) = \text{ord}_0((1-x)/2) = 2$. If $x > 2x/(x-1)$, then $(1-x)/2 < S_\pi^x T_\pi(-x) < 0$ and hence: $\text{ord}_0(-x) \leqq \text{ord}_0((1-x)/2) + 2 = \text{ord}_0(\infty) + 1$. Since $\text{ord}_0(-x)$ is even, and $\text{ord}_0(\infty)$ is odd, the lemma is proved.

LEMMA 6. *Let α be any point of the extended complex plane. Then* $\mathrm{ord}_0(\alpha) \leqq \mathrm{ord}_0(-x) + 1$ *and* $\mathrm{ord}_0(\alpha) \leqq \mathrm{ord}_0(\infty) + 1$.

PROOF. If $\alpha \neq -x$, then there exists an element S_s^x such that $-x < S_s^x(\alpha) \leqq 1$. If $\beta = S_s^x(\alpha)$, then for $0 \leqq \beta \leqq 1$, $\mathrm{ord}_0(\beta) \leqq 2$, and if $-x < \beta < 0$, clearly $\mathrm{ord}_0(-x) \geqq \mathrm{ord}_0(\beta)$ so the first part of the lemma is proved. Similarly there exists an element T_t such that either $T_t(\alpha)$ is on the line $R(z) = (1-x)/2$ or $(1-x)/2 < T_t(\alpha) \leqq 0$. If $\beta = T_t(\alpha)$, it is clear in either case that $\mathrm{ord}_0(\infty) \geqq \mathrm{ord}_0(\beta)$ and the second inequality is proved.

LEMMA 7. $\mathrm{ord}_0(\infty) = \mathrm{ord}_1(-x)$; $\mathrm{ord}_1(\infty) = \mathrm{ord}_0(-x)$.

Since there is a rotation that interchanges the axes of T_ϕ and S_θ, there is a transformation $W = R'(z)$ in G such that

(12) $R'(0) = r, \qquad R'(r) = 0, \qquad R'(-1/r) = \infty, \qquad R'(\infty) = -1/r.$

Let $R(z) = L^{-1}R'L$; then $R(z)$ is in G_x and

(13) $R(0) = 1, \qquad R(1) = 0, \qquad R(-x) = \infty \quad \text{and} \quad R(\infty) = -x.$

Hence the inner automorphism induced on G_x by R leaves G_x invariant and interchanges the two one parameter subgroups T_t and S_s^x. If $W(z) = S_{s_q}^x T_{t_q} \cdots S_{s_1}^x t_{t_1}$ takes $-x$ into 0, then $R^{-1}WR$ takes ∞ into 1; but

$$
\begin{aligned}
R^{-1}WR &= R^{-1}S_{s_q}^x R\, R^{-1}T_{t_q}R \cdot \cdots \cdot R^{-1}S_{s_1}^x R\, R^{-1}T_{t_1}R \\
&= T_{s_q}S_{t_q}^x \cdot \cdots \cdot T_{s_1}S_{t_1}^x;
\end{aligned}
\tag{14}
$$

this has the same length as $W(z)$.

Thus $\mathrm{ord}_0(-x) \geqq \mathrm{ord}_1(\infty)$; similarly $\mathrm{ord}_1(\infty) \geqq \mathrm{ord}_0(-x)$. Similarly one shows $\mathrm{ord}_0(\infty) = \mathrm{ord}_1(-x)$.

It follows from the above lemmas that the order of generation of G_x is just

$$n = \max\{\mathrm{ord}_0(-x), \mathrm{ord}_0(\infty)\} + 1. \tag{15}$$

First observe that $\max\{\mathrm{ord}_0(-x), \mathrm{ord}_0(\infty)\}$ is by Lemma 5 either equal to $\mathrm{ord}_0(-x) + 1$ or it is equal to $\mathrm{ord}_0(\infty) + 1$. By Lemma 6 $\mathrm{ord}_0(\alpha) \leqq \max\{\mathrm{ord}_0(-x), \mathrm{ord}_0(\infty)\}$ for all α in the extended complex plane. In view of the remark made subsequent to (7), it is clear that the order of generation of G_x is less than or equal to

$$\max\{\mathrm{ord}_0(\infty), \mathrm{ord}_0(-x)\} + 1.$$

Consider the transformation V_x of G_x described in (5). If V_x were expressible as a product of length equal to $\mathrm{ord}_0(\infty)$, such a product would have to start with an $S_s{}^x$. Hence $-x$ would remain fixed under the first element of the product and thus $\mathrm{ord}_1(-x) \leqq \mathrm{ord}_0(\infty) - 1$ in contradiction to Lemma 7. Hence the order of generation of G_x is at least $\mathrm{ord}_0(\infty) + 1$. Similarly, as W_x in (6) is in G_x, the order of generation of G_x is at least $\mathrm{ord}_0(-x) + 1$ and (15) is thus established.

It suffices to determine $\mathrm{ord}_0(-x)$ and $\mathrm{ord}_0(\infty)$ in G_x relative to T_t and $S_s{}^x$. It is clear that if t_1 is the largest real solution of $x = 2x/(x-1)$, then for $1 \leqq x \leqq t_1$, $\mathrm{ord}_0(-x) = 2$ (in fact, $t_1 = 3$). By Lemma 1, $\mathrm{ord}_0(-x) = 4$ if and only if $T_\pi S_\pi{}^x(x) \leqq 2x/(x-1)$ and $x > 2x/(x-1)$; further, it follows from the same lemma that for $n \geqq 3$, $\mathrm{ord}_0(-x) = 2n$ if and only if

$$(16) \qquad \underbrace{T_\pi S_\pi{}^x T_\pi S_\pi{}^x \cdots \quad \cdots T_\pi S_\pi{}^x}_{(2n-2 \text{ factors})}(x) \leqq 2x/(x-1)$$

and

$$(17) \qquad \underbrace{T_\pi S_\pi{}^x \cdots \quad \cdots T_\pi S_\pi{}^x}_{(2n-4 \text{ factors})}(x) > 2x/(x-1)$$

both hold.

Now a simple calculation shows

$$(18) \qquad T_\pi S_\pi{}^x(u) = \frac{(x-1)\,u - 2x}{2u + x - 1}.$$

If one now defines $F_1(x) = x$, $F_n(x)$ recursively by

$$(19) \qquad F_n(x) = \frac{(x-1)\,F_{n-1}(x) - 2x}{2F_{n-1}(x) + x - 1}; \qquad n \geqq 2,$$

then $F_{n-1}(x)$ is the expression consisting of $2n-4$ factors in (17) (if $n = 2$, it is just x) and $F_n(x)$ is the expression in (16). Thus $\mathrm{ord}_0(-x) = 2n$ if and only if $F_{n-1} > 2x/(x-1)$ but $F_n(x) \leqq 2x/(x-1)$, $n \geqq 2$.

$F_n(x)$ is a rational function and the asymptotic expression

$$(20) \qquad \lim_{x \to +\infty} \frac{F_n(x)}{x} = \frac{1}{2n-1}$$

is easily established by induction.

Define $t_0 = 1$; then t_1 is the only solution of $F_1(x) = 2x/(x-1)$ that is greater than t_0; further clearly F_1 is finite and $F_1 > 0$ for $x \geqq t_0$. In fact it is possible to construct a strictly increasing sequence of real numbers $\langle t_n \rangle$ such that

$F_n(x)$ is finite for $x \geqq t_{n-1}$ and $F_n{}'(x) > 0$ for $x \geqq t_{n-1}$; and t_n is the *only* solution of:

$$F_n(x) = 2x/(x-1) \qquad \text{that is} > t_{n-1}. \tag{21}$$

To prove this note that it is true for $n = 1$; if $F_{n-1}(t_{n-1}) = 2x/(x-1)$, then $F_n(t_{n-1}) = 0$ by (19); a simple computation shows

$$F_n{}'(x) = \frac{(x+1)^2 F_{n-1}'(x) + 2(F_{n-1}(x) - 1)^2}{[2F_{n-1}(x) + (x-1)]^2}. \tag{22}$$

Since $F_{n-1}'(x) > 0$ for $x \geqq t_{n-2}$ and $F_{n-1}(t_{n-1}) > 0$ it is clear that $F_{n-1}(x) > 0$ for all $x \geqq t_{n-1}$, so that $F_n(x)$ is defined for $x \geqq t_{n-1}$ and clearly by (22) $F_n{}' > 0$ for $x \geqq t_{n-1}$. Now $F_n(t_{n-1}) = 0$, $F_n{}' > 0$ for $x \geqq t_{n-1}$ together with (20) imply that

$$\begin{matrix} F_n(x) = 2x/(x-1) \text{ must have one and} \\ \text{only one root greater than } t_{n-1}; \end{matrix} \tag{23}$$

denote it by t_n. This completes the inductive argument; note in fact that (21) holds for $x \geqq t_{n-2}$, $n \geqq 2$, since $F_{n-1}(t_{n-2}) = 0$, $n \geqq 3$ $(F_1(t_0) = 1)$.

Thus for $t_{n-1} < x \leqq t_n$, $\text{ord}_0(-x) = 2n$. Further $\lim_{n\to\infty} t_n = \infty$; this follows from the fact that if $\lim_{n\to\infty} t_n = T$ is finite, then for all $x \geqq T$, $F_n(x) > 2x/(x-1)$ for all n, and hence $\text{ord}_0(-x)$ would not be finite for such x.

The above properties of $\langle t_n \rangle$ will be, in fact, trivial once they are explicitly determined. To do this, write

$$F_n(x) = P_n(x)/Q_n(x), \tag{24}$$

where $P_n(x)$ and $Q_n(x)$ are relatively prime polynomials with real coefficients, P_n monic. Note that P_n and Q_n are thus relatively prime over the complex numbers. From (20) it follows that degree P_n = degree $Q_n + 1$, for all n, and the leading coefficient of Q_n is $2n - 1$. Now

$$F_{n+1}(x) = \frac{(x-1)P_n(x) - 2x\,Q_n(x)}{2P_n(x) + (x-1)Q_n(x)} = \frac{P_{n+1}}{Q_{n+1}}. \tag{25}$$

LEMMA 8. $P_{n+1}^* = (x-1)P_n - 2xQ_n$ *and* $Q_{n+1}^* = 2P_n + (x-1)Q_n$ *are relatively prime.*

PROOF. First it is easily shown by induction that $F_n(-1) = -1$, for all n, and hence $P_n(-1) = -Q_n(-1) \neq 0$. Hence $P_{n+1}^*(-1) = -2P_n(-1) + 2Q_n(-1) = +4Q_n(-1) \neq 0$. Further at a zero of Q_n, $Q_{n+1}^* \neq 0$, since otherwise P_n would be zero. Hence if P_{n+1}^* and Q_{n+1}^* have a common zero, then

$$\left.\begin{aligned}(x-1)P_n &= 2xQ_n \\ 2P_n &= -(x-1)Q_n\end{aligned}\right\} \to \begin{aligned}2(x-1)P_n &= 4xQ_n \\ 2(x-1)P_n &= -(x-1)^2 Q_n\end{aligned} \tag{26}$$

and hence $4x = -(x-1)^2$, i.e., $x = -1$; but $P^*_{n+1}(-1) \neq 0$.

Since P^*_{n+1} is monic, the recurrence formula

$$P_{n+1} = (x-1)P_n - 2xQ_n; \qquad Q_{n+1} = 2P_n + (x-1)Q_n, \tag{27}$$

are established; $P_1 = x$, $Q_1 = 1$; degree $P_n = n$.

To find the root of (22) that is greater than t_{n-1}, it suffices to find the root of the polynomial equation of degree $n+1$:

$$(x-1)P_n - 2xQ_n = 0 \tag{28}$$

that is greater than t_{n-1}. But (28) is just

$$P_{n+1} = 0 \qquad (n\text{th equation}). \tag{29}$$

P_{n+2} can be expressed in terms of P_n and Q_n; it is more illuminating to get a recurrence relation involving only the P_n.

$$\begin{aligned}P_{n+2} &= (x-1)P_{n+1} - 2xQ_{n+1} \\ &= (x-1)P_{n+1} - 2x(2P_n + (x-1)Q_n) \\ &= (x-1)P_{n+1} - 4xP_n + (x-1)(P_{n+1} - (x-1)P_n) \\ &= 2(x-1)P_{n+1} - (x+1)^2 P_n, \qquad n \geqq 1.\end{aligned} \tag{30}$$

A simple calculation yields $P_2 = x^2 - 3x$ and $P_3 = x^3 - 10x^2 + 5x$. Observe that by (30) it follows that x is a factor of all P_n. Define $R_n = P_{n+1}/x$. Then the nth equation is given by $R_n = 0$, degree $R_n = n$ and the root of $R_n = 0$ that is greater than t_{n-1} is the same as the root of $P_{n+1} = 0$ that is greater than t_{n-1} ($t_1 = 3 > 0$). Thus $R_1 = x - 3$, $R_2 = x^2 - 10x + 5$ and R_n satisfy the same recurrence relation (30).

Since $x = \cot^2(\psi/2) = (1 + \cos\psi)/(1 - \cos\psi)$, it is expedient to introduce a new variable y by the equation

$$x = \frac{1+y}{1-y}; \quad y = \frac{x-1}{x+1}. \tag{31}$$

Let $D_n(y) = (1-y)^n R_n((1+y)/(1-y))$; substitution in (30) yields

$$\begin{aligned}D_{n+1}(y) &= 4yD_n(y) - 4D_{n-1}(y); \qquad n \geqq 2, \\ D_1(y) &= 4y - 2, \qquad D_2(y) = 16y^2 - 8y - 4.\end{aligned} \tag{32}$$

Thus $D_n(y) = 0$ is a polynomial equation of degree n and there is precisely one root in the interval $(t_{n-1} - 1)/(t_{n-1} + 1) < y < 1$. Now finally define $V_n = D_n/2^n$; then $V_1 = 2y - 1$, $V_2 = 4y^2 - 2y - 1$ and the recurrence relation for V_n is by (32)

$$\frac{D_{n+1}}{2^{n+1}} = \frac{4}{2}\frac{y}{1}\frac{D_n}{2^n} - \frac{4}{4}\frac{D_{n-1}}{2^{n-1}}, \qquad n \geqq 2, \tag{33}$$

or

$$V_{n+1} = 2yV_n - V_{n-1}, \qquad n \geqq 2. \tag{34}$$

But (34) is the recurrence relation for the Tchebyshev polynomials; in fact, if $U_n(y)$ is the Tchebyshev polynomial of type II then $U_n - U_{n-1}$ satisfies (34) and $V_1 = U_1 - U_0$, $V_2 = U_2 - U_1$ so that

$$V_n(y) = U_n(y) - U_{n-1}(y) = \frac{\sin(n+1)\theta - \sin n\theta}{\sin\theta}, \qquad \theta = \cos^{-1} y. \tag{35}$$

Some elementary trigonometry yields

$$V_n(y) = \frac{2\cos((2n+1)/2)\,\theta\sin(\theta/2)}{\sin\theta}, \qquad \theta = \cos^{-1} y, \tag{36}$$

and hence the roots of $V_n(y) = 0$ are

$$\cos\frac{\pi}{2n+1}, \qquad \cos\frac{3\pi}{2n+1}, \cdots, \qquad \cos\frac{(2n-1)\pi}{(2n+1)}. \tag{37}$$

The largest root is $\cos(\pi/(2n+1))$ and one can now directly verify that the only root of $V_n(y) = 0$ that is greater than $\cos(\pi/(2n-1))$ is $\cos(\pi/(2n+1))$. Hence $t_n = \cot^2(\pi/2(2n+1))$.

To determine $\mathrm{ord}_0(\infty)$ one may, in view of Lemma 2, follow the above procedure; let $G_1 = (x-1)/2$ and let G_n be defined recursively by (19). Again $G_n(-1) = -1$ for all n; (20) is replaced by

$$\lim_{x \to +\infty} \frac{G_n(x)}{x} = \frac{1}{2n}. \tag{20$'$}$$

Let $s_0 = 1$; again it is possible to construct a strictly increasing sequence of real numbers $\langle s_n \rangle$ such that the only solution of $G_n(x) = 2x/(x-1)$ that is greater than s_{n-1} is s_n. Then for $s_{n-1} < x \leqq s_n$, $\mathrm{ord}_0(\infty) = 2n+1$. Clearly by Lemma 5, $t_n < s_n < t_{n+1}$, $n \geqq 1$. One obtains, exactly as above except that $R_n = P_{n+1}$ replaces $R_n = P_{n+1}/x$, a sequence of polynomials $C_n(y)$ satisfying the recurrence relation of the Tchebyshev polynomials with $C_1 = 2y^2 - 1$, $C_2 = 8y^3 - 6y$ for which the solution of the equation $C_n(y) = 0$ in the interval $(s_{n-1} - 1)/(s_{n-1} + 1) < y < 1$ is desired. But one observes that now if one denotes by $T_n(y)$ the Tchebyshev polynomials of type I:

$$(38)\qquad C_n(y) = T_{n+1}(y) = \cos(n+1)\,\theta, \qquad \theta = \cos^{-1}(y).$$

Hence the n zeros of $C_n(y) = 0$ are

$$(39)\qquad \cos\frac{\pi}{2(n+1)}, \qquad \cos\frac{3\pi}{2(n+1)}, \qquad \cdots, \qquad \cos\frac{(2n+1)\pi}{2(n+1)}.$$

The largest root is $\cos(\pi/(2n+2))$ and this is the only root greater than $\cos(\pi/2n)$. Hence $s_n = \cot^2(\pi/2(2n+2))$.

Thus it has been established that for

$$(40)\qquad \cot^2\frac{\pi}{2(2n)} < x \leqq \cot^2\frac{\pi}{2(2n+1)},$$

$\mathrm{ord}_0(-x) = 2n$, $\mathrm{ord}_0(\infty) = 2n+1$, and thus the order of generation of G_x is $2n+2$, and for

$$(41)\qquad \cot^2\frac{\pi}{2(2n+1)} < x \leqq \cot^2\frac{\pi}{2(2n+2)},$$

$\mathrm{ord}_0(-x) = 2n+2$, $\mathrm{ord}_0(\infty) = 2n+1$, and thus order of generation of G_x is $2n+3$. This establishes (8) in case k is even and odd respectively.

Remark. This proof admits a simple interpretation on the sphere. The "optimal" method of taking either of the two fixed points in the northern hemisphere into the South pole involves successive rotations by π until the last two elements in the product (Lemmas 1 and 2). The "critical" values of ψ, the angle between the axes of rotation, are those for which a product consisting entirely of rotations by π is needed to take one of those fixed points into the South pole. For example, if $\psi = \pi/3$, two rotations by π are needed to take the point $(-(\sin\psi)/2, 0, (1+\cos\psi)/2)$ into the South pole; if $\psi < \pi/3$ the order of this point becomes at least 4; in fact, the order of this point is 4 for $\pi/5 \leqq \psi < \pi/3$. If $\psi = \pi/4$, three rotations by π take the North pole into the South pole; if $\psi < \pi/4$, the order of the North pole becomes at least 5 and is in fact equal to 5 for $\pi/6 \leqq \psi < \pi/4$.

Remark. If the order of generation of $SO(3)$ by T_θ and S_ϕ is n, then every rotation can be written as a product of length exactly n by insertion of $T_0 = S_0 =$ Identity an appropriate number of times.

Corollary. *Let the order of generation of $SO(3)$ by T_θ and S_ϕ be n. Then every rotation can be expressed as a product of length n whose last element is a T_ϕ. Further every rotation can also be expressed as a product of length n whose last element is an S_θ.*

Proof. If the rotation can be expressed as a product of length less than n the result is trivial. If the rotation cannot be expressed as a product of length less than n, then the point taken into the South pole must have order $n-1$ so every rotation taking that point into the South pole can be written as a product of length n whose last element is T_ϕ. Similarly, the point taken by the rotation into $((\sin\psi)/2,\ 0,\ (1-\cos\psi)/2)$ has order $n-1$ so that every such rotation can be expressed as a product of length n with last element S_θ.

Appendix.

THEOREM. *Let G be a compact, connected Lie group; suppose X and Y generate the Lie algebra g and that e^{tX}, e^{sY} are compact. Then G is uniformly finitely generated by e^{tX}, e^{sY}.*

PROOF. Let G_n be all products of e^{tX}, e^{sY} of length $\leqq n$; G_n is clearly compact; $\bigcup_{n=1}^{\infty} G_n = G$. By the Baire category theorem as G is a complete metric space, some G_N (and hence G_n, $n \geqq N$) contains an open set U. $\bigcup_{T\in G} TU = G$; since the sets TU are open, this is an open cover of G and has a finite subcover. Hence $\exists T_1, \cdots, T_k$ such that $\bigcup_{i=1}^{k} T_i U = G$. But each T_i, $i = 1, \cdots, k$, is a finite product of e^{tX}, e^{sY} and as $U \subset G_N$, the theorem is proved.

BIBLIOGRAPHY

1. F. Lowenthal, *On generating subgroups of the Moebius group by pairs of infinitesimal transformations*, Pacific J. Math. **26** (1968), 141-147. MR 38 #266.

UNIVERSITY OF OREGON, EUGENE, OREGON 97403