Pacific Journal of Mathematics

GENERATING $O(n)$ WITH REFLECTIONS

MORRIS LEROY EATON AND MICHAEL DAVID PERLMAN

Vol. 73, No. 1 March 1977

PACIFIC JOURNAL OF MATHEMATICS
Vol. 73, No. 1, 1977

GENERATING $O(n)$ WITH REFLECTIONS

MORRIS L. EATON AND MICHAEL PERLMAN

For $r \in C_n \equiv \{x | x \in R^n, ||x|| = 1\}$, let $S_r = I_n - 2rr'$ where r is a column vector. $O(n)$ denotes the orthogonal group on R^n. If $R \subseteqq C_n$, let $\mathscr{R} = \{S_r | r \in R\}$ and let G be the smallest closed subgroup of $O(n)$ which contains $\mathscr{R}$. G is *reducible* if there is a nontrivial subspace $M \subseteqq R^n$ such that $gM \subseteqq M$ for all $g \in G$. Otherwise, G is *irreducible*.

THEOREM. **If G is infinite and irreducible, then $G = O(n)$.**

In what follows, R^n denotes Euclidean n-space with the standard inner product, $O(n)$ is the orthogonal group of R^n, and $C_n = \{x | x \in R^n, ||x|| = 1\}$. If U is a subset of $O(n)$, $\langle U \rangle$ denotes the group generated algebraically by U and $\langle \bar{U} \rangle$ denotes the closure of $\langle U \rangle$. Thus, $\langle \bar{U} \rangle$ is the smallest closed subgroup of $O(n)$ containing U. For an integer k, $1 \leqq k < n$, M_k denotes a k-dimensional linear subspace of R^n. If $r \in C_n$, let $S_r = I - 2rr'$ where r is a column vector. Thus S_r is a reflection through r-henceforth called a reflection.

Suppose $R \subseteqq C_n$ and let $\mathscr{R} = \{S_r | r \in R\}$. Set $G = \langle \bar{\mathscr{R}} \rangle$. The group G is *reducible* if there is an M_k such that $gM_k \subseteqq M_k$ for all $g \in G$; otherwise, G is *irreducible*. The main result of this note is the following.

THEOREM 1. *If G is infinite and irreducible, then $G = O(n)$.*

Proof of Theorem 1. First note that if $S_r \in \mathscr{R}$ and $g \in G$, then $gS_rg^{-1} = S_{gr} \in G$. Let $\Delta = \{gr | g \in G, r \in R\}$. Thus, $t \in \Delta$ implies that $S_t \in G$. Since G is infinite, Δ must be infinite (see Benson and Grove (1971), Proposition 4.1.3). Since every Γ in $O(n)$ is a product of a finite number of reflections, to show that $G = O(n)$, it suffices to show that G is transitive on C_n (if G is transitive on C_n, then $\Delta = C_n$ so every reflection is an element of G and hence $G = O(n)$).

The proof that G is transitive on C_n follows. By Lemma 1 (below), there is a subgroup $K_2 \subseteqq G$ and a subspace $M_2 \subseteqq R^n$ such that $kx = x$ if $x \in M_2^\perp$ and $k \in K_2$ and K_2 is transitive on $D_2 \equiv M_2 \cap C_n$. Since G is irreducible, there is an $r_2 \in R$ such that $r_2 \notin M_2$ and $r_2 \notin M_2^\perp$. Let $M_3 = \text{span}\{r_2, M_2\}$ and let $K_3 = \langle \{K_2, S_{r_2}\} \rangle > \subseteqq G$. With $D_3 \equiv M_3 \cap C_n$, Lemma 3 (below) implies that $kx = x$ for all $x \in M_3^\perp$ and $k \in K_3$, and K_3 is transitive on D_3. Again, since G is irreducible, there is an $r_3 \in R$ such that $r_3 \notin M_3$ and $r_3 \notin M_3^\perp$. With $M_4 = \text{span}\{r_3, M_3\}$, let $K_4 = \langle \{K_3, S_{r_3}\} \rangle > \subseteqq G$ and let $D_4 \equiv M_4 \cap C_n$. By Lemma 3 (below)

$kx = x$ for $x \in M_4^{\perp}$ and $k \in K_4$ and K_4 is transitive on D_4. Applying this argument $(n-2)$ times, we obtain $K_n \subseteqq G$ and K_n is transitive on $D_n = C_n$. Thus, G is transitive on C_n and the proof is complete.

To fill in the gaps in the above argument, it remains to prove Lemmas 1, 2, and 3. Lemma 1 provides the starting point for the stepwise argument used in the proof of Theorem 1.

LEMMA 1. *If G is irreducible and infinite, there is a subspace M_2 and a subgroup $K_2 \subseteqq G$ such that $kx = x$ for $x \in M_2^{\perp}$, $k \in K_2$ and K_2 acts transitively on $D_2 \equiv M_2 \cap C_n$.*

Proof. As noted in the proof of Theorem 1, the set $\Delta = \{gr \mid r \in R, g \in G\}$ is infinite. Thus, there is a point $\delta_0 \in C_n$ such that every neighborhood of δ_0 contains infinitely many points in Δ. Thus we can select a sequence of pairs (r_i, t_i), $r_i, t_i \in \Delta$, such that r_i and t_i are linearly independent and $1 - 1/i < r_i' t_i < r_{i+1}' t_{i+1} < 1$ for $i = 1, 2, \cdots$.

For $0 \leqq \eta < 2\pi$, set

$$\Psi(\eta) = \begin{pmatrix} \cos\eta & \sin\eta \\ -\sin\eta & \cos\eta \end{pmatrix} \in O(2)\,. \tag{1}$$

Define θ_i by $\cos\theta_i = r_i' t_i$, $0 \leqq \theta_i < \pi$ so $\theta_i \to 0$ as $i \to \infty$. Let $\Gamma_i \in O(n)$ have first row t_i' and second row

$$(r_i - t_i' r_i t_i)' / \| r_i - t_i' r_i t_i \|\,.$$

Then an easy calculation shows that

$$S_{t_i} S_{r_i} = \Gamma_i' \begin{pmatrix} \Psi(2\theta_i) & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_i\,, \qquad i = 1, 2, \cdots \tag{2}$$

where I_{n-2} is an $(n-2) \times (n-2)$ identity matrix. Setting $H_i = \langle \Psi(2\theta_i) \rangle \subseteqq O(2)$, it is clear that

$$\left\{ \Gamma_i' \begin{pmatrix} h & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_i \,\middle|\, h \in H_i \right\} \subseteqq G\,, \qquad i = 1, 2, \cdots\,. \tag{3}$$

By selecting an appropriate subsequence, we can assume without loss of generality that $\Gamma_i \to \Gamma_0 \in O(n)$, as $i \to \infty$.

If $\Psi(\eta)$ is given by (1), we now claim that

$$\Gamma_0' \begin{pmatrix} \Psi(\eta) & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_0 \in G\,. \tag{4}$$

Since G is closed and (3) holds, to establish (4), it suffices to show there is a subsequence i_j and $h_{i_j} \in H_{i_j}$ such that $h_{i_j} \to \Psi(\eta)$ as $i_j \to \infty$. However, the existence of such a sequence is assured since $\theta_i \to 0$ as $i \to \infty$. Thus (4) holds. Hence we see that

$$K_2 \equiv \left\{ \Gamma_0' \begin{pmatrix} h & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_0 \middle| h \in H^* \right\} \subseteq G \tag{5}$$

where H^* is the full rotation group of R^2.

To complete the proof of Lemma 1, let M_2 be the span of the first two columns of Γ_0'. With $D_2 \equiv M_2 \cap C_n$, it is easy to check that $kx = x$ for all $x \in M_2^{\perp}$, $k \in K_2$ and that K_2 acts transitively on D_2. This completes the proof.

The following result is used in the proof of Lemma 3.

LEMMA 2. *For $u_0 \in (0, 1]$, define a function f: $[0, 1] \to [0, 1]$ by*

$$f(u) = \begin{cases} 0 & \text{if } 0 \leqq u \leqq u_0 \\ 1 - [\sqrt{uu_0} + \sqrt{(1-u)(1-u_0)}]^2 & \text{if } u_0 \leqq u \leqq 1 . \end{cases} \tag{6}$$

Let $v_1 = f(1)$ and define $v_i = f(v_{i-1})$ for $i = 2, 3, \cdots$. Then, there exists an index i_0 such that $v_i = 0$ for $i \geqq i_0$.

Proof. It is not hard to verify that f is a continuous convex function. Since $0 \leqq v_1 < 1$, $v_2 = f(v_1) = f((1 - v_1)0 + v_1 1) \leqq v_1 f(1) = v_1^2$. Proceeding by induction, $v_i \leqq v_1^i$ so $\lim_{i\to\infty} v_i = 0$. Since f is 0 in the interval $[0, u_0]$, there is an index i_0 such that $v_i = 0$ for $i \geqq i_0$. This completes the proof.

After establishing Lemma 1, the key to Theorem 1 is Lemma 3. Although the proof of Lemma 3 is quite long, the geometric idea behind the proof is fairly simple. Consider R^3 and let $D_2 = \{x \mid x \in R^3, x_3 = 0, x_1^2 + x_2^2 = 1\}$. Also, let $H = \left\{ \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \middle| k \text{ is any rotation of } R^2 \right\}$. Thus H acts transitively on D_2. Consider a fixed vector $t \in R^3$ with $\|t\| = 1$ such that t is not in the (x_1, x_2) plane and t is not in the x_3-line. Let $S_t = I\text{-}2tt'$ be the reflection across the plane $\{t\}^{\perp}$ and let $\tilde{H}$ be the group generated by S_t and H. The claim is that $\tilde{H}$ is transitive on $D_3 = \{x \mid x \in R^3, \|x\| = 1\}$. For example, suppose the angle between t and the (x_1, x_2) plane is 45°. Geometrically, it is clear that the set $H(S_t(D_2)) \equiv \{x \mid x = hS_t u$ for some $h \in H$, and some $u \in D_2\}$ is just D_3—that is, $S_t(D_2)$ is a circle passing through $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and the transitivity of H implies that H moves the set $S_t(D_2)$ everywhere onto D_3 (picture this on the surface of a basketball). Thus, given

$v_1, v_2 \in D_3$, $v_i = h_i S_t u_i$, for $h_i \in H$ and $u_i \in D_2$ for $i = 1, 2$. Since $u_1 = h_0 u_2$ for some $h_0 \in H$, it follows that $v_1 = h_1 S_t h_0 S_t h_2^{-1} v_2$ so $\tilde{H}$ is transitive on D_3. For other t-vectors, D_3 does not get covered by one application of HS_t to D_2, but D_3 is covered by a finite number of applications of HS_t to D_2—that is, $D_3 = (H(S_t(\cdots)H)S_t)(D_2)$ for some finite string $HS_tHS_t \cdots HS_t$. Again, this implies the transitivity of $\tilde{H}$ on D_3. Lemma 3 and its proof make all of the above precise.

LEMMA 3. *Consider a subspace $M_m \subseteqq R^n$, $2 \leqq m < n$, and suppose that K is a subgroup of $O(n)$ such that*

$$\begin{cases} kx = x \quad \text{for all} \quad x \in M_m^{\perp}, k \in K \\ K \text{ is transitive on } D_m \equiv M_m \cap C_n . \end{cases} \tag{7}$$

Let $t \in C_n$ be such that $t \notin M_m$ and $t \notin M_m^{\perp}$. With $M_{m+1} = \operatorname{span}\{t, M_m\}$, let $D_{m+1} \equiv M_{m+1} \cap C_n$. Then the group $K^* \subseteqq O(n)$ generated by K and $S_t = I - 2tt'$ satisfies

$$\begin{cases} kx = x \quad \text{for all} \quad x \in M_{m+1}^{\perp}, k \in K^* \\ K^* \text{ is transitive on } D_{m+1} . \end{cases} \tag{8}$$

Proof. That $kx = x$ for all $x \in M_{m+1}^{\perp}$ and $k \in K^*$ is not hard to verify. To establish the transitivity of K^* on D_{m+1}, define a set B_1 by

$$B_1 = K(S_t(D_m)) = \{x \mid x = kS_t u \text{ for some } u \in D_m, \text{ some } k \in K\} \tag{9}$$

and then define B_i inductively by

$$B_i = K(S_t(B_{i-1})) = \{x \mid x = kS_t u \text{ for some } u \in B_{i-1}, \text{ some } k \in K\} \tag{10}$$

$i = 2, 3, \cdots$. Since $K(S_t(D_{m+1})) \subseteqq D_{m+1}$, it follows that $B_i \subseteqq D_{m+1}$ for all i. The remainder of the proof is devoted to showing that there is an index i_0 such that $B_{i_0} = D_{m+1}$, because this implies the transitivity of K^* on D_{m+1}.

Claim 1. If $B_{i_0} = D_{m+1}$, then K^* is transitive on D_{m+1}.

Proof of Claim 1. Consider $z_1, z_2 \in D_{m+1}$. If $B_{i_0} = D_{m+1}$, then

$$\underbrace{K(S_t(K(S_t \cdots (D_m))))}_{i_0\text{-terms}} = D_{m+1} .$$

Thus, there exists $k_1, \cdots, k_{i_0} \in K$ and $g_1, \cdots, g_{i_0} \in K$ such that

$$z_1 = \left[\prod_{j=1}^{i_0} (k_j S_t)\right] u_1 \equiv h_1 u_1$$

and

$$z_2 = \left[\prod_{j=1}^{i_0} (g_j s_t)\right] u_2 \equiv h_2 u_2$$

for some $u_1, u_2 \in D_m$. Since K is transitive on D_m, there exists a $k_0 \in K$ such that $k_0 u_1 = u_2$. Thus, $z_2 = h_2 k_0 h_1^{-1} z_1$ which shows that K^* is transitive on D_{m+1} as $h_2 k_0 h_1^{-1} \in K^*$. This completes the proof of Claim 1.

We now continue with the proof. Let P denote the orthogonal projection onto M_m and define Z_c, $0 \leqq c \leqq 1$ by

(11) $$Z_c = \{x \mid x \in D_{m+1}, \|Px\|^2 \geqq c\} .$$

Note that $Z_1 = D_m$ and $Z_0 = D_{m+1}$.

REMARK. Geometrically, Z_c is an equatorial zone (with equator D_m) which partially covers D_{m+1}. Smaller values of c correspond to more of D_{m+1} being covered.

Define φ on $[0, 1]$ by

(12) $$\varphi(c) = \inf_{x \in Z_c} \|PS_t x\|^2 , \quad 0 \leqq c \leqq 1 ,$$

and let

(13) $$b_1 = \inf_{x \in B_1} \|Px\|^2 .$$

Since each $k \in K$ commutes with P, we have

(14) $$b_1 = \inf_{k \in K} \inf_{x \in D_m} \|PkS_t x\|^2 = \inf_{x \in D_m} \|PS_t x\|^2 = \inf_{x \in Z_1} \|PS_t x\|^2 = \varphi(1) .$$

Claim 2. $B_1 = Z_{b_1}$.

Proof of Claim 2. If $x \in B_1$, $\|Px\|^2 \geqq b_1$ which implies that $x \in Z_{b_1}$. Conversely, consider $x \in Z_{b_1}$ and let Q denote the orthogonal projection onto the one-dimensional subspace $M_m^\perp \cap M_{m+1}$ which is spanned by the vector $t^* \equiv (I - P)t/\|(I - P)t\|$. Since Z_c is compact and arcwise connected, the continuous function $u \rightarrow \|PS_t u\|^2 (u \in Z_c)$ takes on all values between 1 and $\varphi(c)$. As $x \in Z_{b_1}$,

$$\|Px\|^2 \geqq b_1 = \varphi(1) = \inf_{u \in D_m} \|PS_t u\|^2 .$$

Hence, there exists a $u \in D_m$ such that $\|PS_t u\|^2 = \|Px\|^2$. Thus, $1 = \|Px\|^2 + \|Qx\|^2 = \|PS_t u\|^2 + \|QS_t u\|^2$, so $\|QS_t u\|^2 = \|Qx\|^2$. Since Q is a projection onto a one-dimensional subspace, u can be chosen (by changing to $-u$ if necessary) such that $Qx = QS_t u$. The transitivity of K on D_m implies there is a $k \in K$ such that $kPS_t u = Px$. Thus,

$kS_tu = kPS_tu + kQS_tu = Px + kQS_tu = Px + QS_tu = Px + Qx = x$, so $x = kS_tu \in B_1$. This completes the proof of Claim 2.

Using Claim 2, $B_2 = K(S_t(B_1)) = K(S_t(Z_{b_1}))$. Consider

$$b_2 \equiv \inf_{x \in B_2} ||Px||^2 . \tag{15}$$

Using (15) and the fact that each $k \in K$ commutes with P, we have

$$b_2 = \inf_{x \in B_2} ||Px||^2 = \inf_{x \in Z_{b_1}} \inf_{k \in K} ||PkS_tx||^2 = \inf_{x \in Z_{b_1}} ||PS_tx||^2 = \varphi(b_1) . \tag{16}$$

Claim 3. $B_2 = Z_{b_2}$.

Proof of Claim 3. If $x \in B_2$, then $x \in D_{m+1}$ and $||Px||^2 \geqq b_2$, so $x \in Z_{b_2}$. Conversely, consider $x \in Z_{b_2}$. As u varies over Z_{b_1}, the function $u \to ||PS_tu||^2$ takes on all values between 1 and b_2. Since $||Px||^2 \geqq b_2$, there is a $u \in Z_{b_1}$ such that $||PS_tu||^2 = ||Px||^2$. As in the proof of Claim 2, $1 = ||Px||^2 + ||Qx||^2 = ||PS_tu||^2 + ||QS_tu||^2$ so $||Qx||^2 = ||QS_tu||^2$, and we can choose u such that $Qx = QS_tu$. The transitivity of K implies that there is a $k \in K$ such that $kPS_tu = Px$. Thus, $x = Px + Qx = kPS_tu + QS_tu = kPS_tu + kQS_tu = kS_tu \in B_2$ since $u \in Z_{b_1} = B_1$. The proof of Claim 3 is complete.

Arguing as in the proof of Claim 3, it is an easy matter to show that $B_i = Z_{b_i}$ and $b_i = \varphi(b_{i-1})$ where

$$b_i = \inf_{x \in B_i} ||Px||^2, \ i = 3, 4, \cdots . \tag{17}$$

As noted earlier, the proof of Lemma 3 will be complete if we can show there is an index i_0 such that $B_{i_0} = Z_0 = D_{m+1}$. To establish the existence of an i_0, we will explicitly calculate the function φ defined in (12) and then apply Lemma 2. Define $z_0 \in D_{m+1}$ by

$$z_0 = S_tt^* \tag{18}$$

where $t^* = (I - P)t/||(I - P)t||$. Then,

$$\begin{aligned} a \equiv ||Pz_0||^2 &= \frac{||PS_t(I-P)t||^2}{||(I-P)t||^2} = \frac{||P(I-2tt')(I-P)t||^2}{||(I-P)t||^2} \\ &= \frac{4||Pt||^2(t'(I-P)t)^2}{||(I-P)t||^2} = \ = 4||Pt||^2(1 - ||Pt||^2) . \end{aligned} \tag{19}$$

Since $t \notin M_m$ and $t \notin M_m^{\perp}$, $0 < ||Pt||^2 < 1$ so $0 < a \leqq 1$.

Claim 4. The function φ is given by

$$\varphi(c) = \begin{cases} 0 & \text{if} \quad 0 \leqq c \leqq a \\ 1 - [\sqrt{ac} + \sqrt{(1-a)(1-c)}]^2 & \text{if} \quad a \leqq c \leqq 1 \,. \end{cases} \tag{20}$$

Proof of Claim 4. Since $Q = t^* t^{*\prime}$ (see the proof of Claim 2), for each $x \in R^n$, $\|QS_t x\|^2 = x'S_t Q S_t x = x' S_t t^* t^{*\prime} S_t x = (z_0' x)^2$. Thus,

$$\varphi(c) = \inf_{x \in Z_c} \|PS_t x\|^2 = \inf_{x \in Z_c} (1 - \|QS_t x\|^2) = 1 - \sup_{x \in Z_c} (z_0' x)^2 \,. \tag{21}$$

If $a = 1$, then $z_0 \in D_m \subseteqq Z_c$, so $\sup_{x \in Z_c} (z_0'x)^2 = 1$ and $\varphi(c) = 0$ for all $c \in [0, 1]$.

Now, consider $a \in (0, 1)$. For $x \in Z_c$, let $\gamma = \|Px\|^2 \geqq c$. Then, by the Cauchy-Schwarz inequality, we have

$$\begin{aligned} z_0'x &= z_0'Px + z_0'Qx = (Pz_0)'Px + (Qz_0)'Qx \\ &\leqq \|Pz_0\| \, \|Px\| + \|Qz_0\| \, \|Qx\| = \sqrt{a}\sqrt{\gamma} + \sqrt{1-a}\sqrt{1-\gamma} \,. \end{aligned} \tag{22}$$

Further, there is equality in the above inequality for $x = x_0$ where

$$x_0 = \sqrt{\gamma/a}\,Pz_0 + \sqrt{(1-\gamma)/(1-a)}\,Qz_0 \,. \tag{23}$$

Clearly, $\|Px_0\|^2 = \gamma \geqq c$ so $x_0 \in Z_c$. Thus,

$$\varphi(c) = 1 - \sup_{\gamma \in [c,1]} [\sqrt{a\gamma} + \sqrt{(1-a)(1-\gamma)}]^2 \,. \tag{24}$$

If $c \leqq a$, then $\gamma = a \in [c, 1]$ and $\varphi(c) = 0$. If $c > a$, then the sup in (24) is achieved at $\gamma = c$. Thus φ is given by (20) and the proof of Claim 4 is complete.

Now, by Lemma 2, there is an index i_0 such that $b_{i_0} = 0$ since $b_1 = \varphi(1)$ and $b_i = \varphi(b_{i-1})$. Thus, $B_{i_0} = Z_0 = D_{m+1}$ and by Claim 1, K^* is transitive on D_{m+1}. This completes the proof of Lemma 3.

The following is an immediate consequence of Theorem 1.

COROLLARY 1. *Let $G_1 = \langle \mathscr{R} \rangle$ where $\mathscr{R} = \{S_r \mid r \in R\}$. If G_1 is infinite and irreducible, then the closure of G_1 is $O(n)$. Also, for each $x \in C_n$, $\{gx \mid g \in G_1\}$ is dense in C_n.*

REMARK. The assumption that G is generated by reflections cannot be removed since $O^+(n)$, $n \geqq 2$ is infinite, closed and irreducible but $O^+(n) \neq O(n)$. Our interest in Theorem 1 arose in connection with results for G-monotone functions when G is generated by reflections (see Eaton and Perlman (1976)).

REFERENCES

1. C. T. Benson and L. C. Grove, *Finite Reflection Groups*, Bogden and Quigley, Tarrytown-on-Hudson, New York, 1971.

2. M. L. Eaton and M. D. Perlman, Reflection Groups, Generalized Schur Functions and the Geometry of Majorization. To appear in the Annals of Probability, 1976.

Received February 11, 1977 and in revised form July 28, 1977. The research for the first author was supported in part by a grant from the National Science Foundation—NSF-GP-34482.

The research for the second author was supported in part by a grant from the National Science Foundation—NSF-MCS-72-04364-A03.

UNIVERSITY OF COPENHAGEN
5, UNIVERSITETSPARKEN
DK 2100 COPENHAGEN, Ø DENMARK

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 73, No. 1 March, 1977