Generating O(n) with Reflections

by

Morris L. Eaton[1] and Michael Perlman[2]

University of Minnesota and University of Chicago

Technical Report No. 263

March, 1976

1. This research was supported in part by a grant from the National Science Foundation -- NSF-GP-34482.

2. This research was supported in part by a grant from the National Science Foundation -- NSF-MCS-72-04364-A03.

Abstract

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

<u>Theorem</u>: If G is infinite and irreducible, then $G = O(n)$.

American Mathematical Society 1970 Subject Classification:
Primary 20F15 Secondary 20F05, 20H15
<u>Key Words and Phrases</u>: Orthogonal group, generators, reflections.

Throughout this note, the following notation will be used. R^n denotes Euclidean n-space with the standard inner product, $O(n)$ is the orthogonal group of R^n, and $C_n = \{x|, x\epsilon R^n, \|x\| = 1\}$. If U is a subset of $O(n)$, $\langle U\rangle$ denotes the group generated algebraicially by U and $\overline{\langle U\rangle}$ denotes the closure of $\langle U\rangle$ so $\overline{\langle U\rangle}$ is the smallest closed subgroup of $O(n)$ containing U. For an integer k, $1 \leq k < n$, M_k denotes a k-dimensional linear subspace of R^n. If $r\epsilon C_n$, let $S_r = I - 2rr'$ where r is a column vector. Thus S_r is a reflection through r, henceforth called a reflection.

Suppose $R \subseteq C_n$ and let $\mathcal{R} = \{S_r | r\epsilon R\}$. Set $G = \overline{\langle\mathcal{R}\rangle}$. The group G is reducible if there is an M_k such that $gM_k \subseteq M_k$ for all $g\epsilon G$; 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. If $S_r \epsilon \mathcal{R}$ and $g\epsilon G$, then $gS_r g^{-1} = S_{gr} \epsilon G$. Let $\Delta = \{gr | g\epsilon G, r\epsilon R\}$ so Δ must be infinite as G is infinite (see Benson and Grove (1967), Proposition 4.1.3). Since every $\Gamma\epsilon O(n)$ is a product of a finite number of reflections, to show $G = O(n)$ it suffices to show that G is transitive on C_n, in which case $\Delta = C_n$, so $S_x \epsilon G$ for all $x\epsilon C_n$.

In order to show that G is transitive on C_n, we will show (Lemma 1, below) that there is a subspace M_2 and a subgroup $K_2 \subseteq G$ such that $kx = x$ if $x\epsilon M_2^{\perp}$ and K_2 is transitive on $C_2 \equiv M_2 \cap C_n$. Then, since G is irreducible, there is an $r_2 \epsilon R$ such that $r_2 \notin M_2$ and $r_2 \notin M_2^{\perp}$. Let $M_3 \equiv \text{span}\,\{r_2, M_2\}$ and let $K_3 \equiv \langle K_2, S_{r_2}\rangle \subseteq G$. Setting $C_3 = M_3 \cap C_n$, it follows that (Lemma 2, below) $kx = x$ for all $x\epsilon M_3^{\perp}, k\epsilon K_3$, and K_3 acts transitively on C_3. Again, since G is irreducible, there is an $r_3 \epsilon R$ such that $r_3 \notin M_3$ and $r_3 \notin M_3^{\perp}$. With $M_4 \equiv \text{span}\,\{r_3, M_3\}$, let $K_4 = \langle K_3, S_{r_3}\rangle \subseteq G$ and let $C_4 = M_4 \cap C_n$. Applying Lemma 2 again, $kx = x$ for all $x \in M_4^{\perp}$, $k \in K_4$, and K_4 acts transitively on C_4. An easy induction argument then completes the proof.

To fill in the gaps in the above proof, it remains to prove lemmas 1 and 2.

Lemma 1.: If G is irreducible and infinite, there is a subspace M_2 and a subgroup $K_2 \subseteq G$ such that $kx = x$ for all $x \in M_2^{\perp}$, $k \in K_2$ and K_2 acts transitively on $C_2 \equiv M_2 \cap C_n$.

Proof. Since the set $\Delta = \{gr | r \in R,\ g \in G\}$ is infinite, 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 $1 - \frac{1}{i} < r_i' t_i < r_{i+1}' t_{i+1} < 1$ for $i = 1, 2, \ldots$.

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

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

Define θ_i by $\cos\theta_i = r_i' t_i$, $0 \leq \theta_i < \pi$ 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

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

Let $H_i = \langle \Psi(2\theta_i) \rangle \subseteq O(2)$. Then, it is clear that

$$(3) \qquad \Gamma_i' \begin{pmatrix} H_i & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_i \subseteq G, \qquad i = 1, 2, \ldots.$$

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

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

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

$$(5) \qquad \Gamma_0' \begin{pmatrix} H_0 & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_0 \subseteq G$$

where H_0 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 rows of Γ_0, and set

$$K_2 = \Gamma_0' \begin{pmatrix} H_0 & 0 \\ 0 & I_{n-2} \end{pmatrix} \Gamma_0.$$

With $C_2 \equiv M_2 \cap C_n$, it is easy to check that $kx = x$ for all $x \epsilon M_2^{\perp}$, $k \epsilon K_2$ and that K_2 acts transitively on C_2. This completes the proof.

The remainder of this note is devoted to a proof of Lemma 2 below. Let $M_m \subseteq R^n$, $2 \leq m < n$ and suppose that K is a subgroup of $O(n)$ such that

$$(6) \qquad \begin{cases} kx = x \quad \text{for all } x \epsilon M_m^{\perp},\ k \epsilon K. \\ K \text{ is transitive on } C_m \equiv M_m \cap C_n. \end{cases}$$

Let $t \epsilon C_n$ such that $t \notin M_m$ and $t \notin M_m^{\perp}$. With $M_{m+1} \equiv \text{span}\{t, M_m\}$, let

$C_{m+1} = M_{m+1} \cap C_n$ and also set $K^* = \langle K, S_t \rangle$.

Lemma 2: K^* is transitive on C_{m+1} and $kx = x$ for all $x \in M_{m+1}^{\perp}$, $k \in K^*$.

Proof. That $kx = x$ for all $x \in M_{m+1}^{\perp}$, $k \in K^*$ is clear. To establish the transitivity of K^*, first let P denote the orthogonal projection onto M_m and define Z_c, $0 \leq c \leq 1$, by

$$(7) \qquad Z_c = \{x \mid x \in C_{m+1}, \|Px\|^2 \geq c\}.$$

Further, define φ by

$$(8) \qquad \varphi(c) \equiv \inf_{x \in Z_c} \|PS_t x\|^2, \qquad 0 \leq c \leq 1.$$

Since Z_c is compact and arcwise connected, as x ranges over Z_c, $\|PS_t x\|^2$ assumes all values between 1 and $\varphi(c)$. Note that $Z_1 = C_m$ and $Z_0 = C_{m+1}$.

Define a set $B_1 \subseteq C_{m+1}$ by

$$(9) \qquad B_1 = K(S_t(C_m)) = \{x \mid x = k_1 S_t u \text{ for some } u \in C_m, \text{ some } k_1 \in K\}$$

and let

$$(10) \qquad b_1 = \inf_{x \in B_1} \|Px\|^2$$

Since each $k \in K$ commutes with P, it is clear that

$$(11) \qquad b_1 = \inf_{k \in K} \inf_{x \in C_m} \|PkS_t x\|^2 = \inf_{x \in C_m} \|PS_t x\|^2 = \inf_{x \in Z_1} \|PS_t x\|^2 = \varphi(1).$$

We now claim that $B_1 = Z_{b_1}$. Clearly $B_1 \subseteq Z_{b_1}$. If $x \in Z_{b_1}$ then there is a $u \in C_m$ such that $\|Px\|^2 = \|PR_t u\|^2$. Let Q denote the orthogonal projection onto the one-dimensional subspace $M_m^\perp \cap M_{m+1}$. 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 $Qx = QS_t u$. As K is transitive on C_m, there is a $k \in K$ such that $kPS_t u = Px$. Thus $kS_t u = kPS_t u + kQS_t u = Px + QS_t u = Px + Qx = x$, so $x = kS_t u \in B_1$. Thus $B_1 = Z_{b_1}$ as claimed.

Set $B_2 \equiv K(S_t(B_1))$ so $B_2 = K(S_t(Z_{b_1}))$ and let

(12) $$b_2 \equiv \inf_{x \in B_2} \|Px\|^2 = \inf_{x \in Z_{b_1}} \|PS_t x\|^2 = \varphi(b_1).$$

Again, we claim that $B_2 = Z_{b_2}$. Clearly, $B_2 \subseteq Z_{b_2}$. If $x \in Z_{b_2}$, then $\|Px\| \geq b_2 = \varphi(b_1)$. Thus, there is $u \in Z_{b_1}$ such that $\|PS_t u\|^2 = \|Px\|^2$ and $QS_t u = Qx$. Arguing as before, the transitivity of K implies there is a $k \in K$ such that $kS_t u = x$. Hence $B_2 = Z_{b_2}$.

By induction, define $B_{i+1} = K(S_t(B_i))$, $i = 2, 3, \ldots$ and set $b_{i+1} = \inf_{x \in B_i} \|Px\|^2$. Arguing as before, $Z_{b_{i+1}} = B_{i+1}$ and $b_{i+1} = \varphi(b_i)$ for $i = 1, 2, \ldots$.

The proof of the Lemma will be complete if we can show there is an index i_0 such that $b_{i_0+1} = \varphi(b_{i_0}) = 0$. In this case, $B_{i_0+1} = Z_{b_{i_0+1}} = Z_0 = C_{m+1}$ which implies that

$$(13) \qquad C_{m+1} = \underbrace{K(S_t(K(\cdots K(S_t}_{(i_0+1)\text{ times}}(C_m)) \cdots)))$$

However, (13) together with the transitivity of K on C_m clearly implies that $K^* = \langle K, S_t \rangle$ is transitive on C_{m+1}.

We will now show that

$$(14) \qquad \varphi(b_{i_0}) = 0 \text{ for some index } i_0.$$

First, let

$$(15) \qquad z_0 = \frac{S_t Qt}{\|Qt\|} \in C_{k+1}$$

so $z_0 = Pz_0 + Qz_0$. Note that

$$(16) \qquad a \equiv \|Qz_0\|^2 = 4\,\|Qt\|^2(1 - \|Qt\|^2).$$

Since $Qt \neq 0$, $0 < a \leq 1$. From the definition of the projection Q, it follows that

$$(17) \qquad \|QS_t x\|^2 = (z_0' x)^2, \quad x \in R^n.$$

Now, for $0 \leq c \leq 1$,

$$(18) \qquad \varphi(c) = \inf_{x \in Z_c} \|PS_t x\|^2 = \inf_{x \in Z_c} (1 - \|QS_t x\|^2) = 1 - \sup_{x \in Z_c} (z_0' x)^2.$$

If $a = 1$, $z_0 \in Z_c$ so $\varphi(c) = 0$ for $c \in [0, 1]$. For $0 < a < 1$, consider $x \in Z_c$ and let $\gamma \equiv \|Px\|^2 \geq c$. Then

(19) $$z_0'x = z_0'Px + z_0'Qx = (Pz_0)'(Px) + (Qz_0)'(Qx)$$

$$\leq \|Pz_0\| \, \|Px\| + \|Qz_0\| \, \|Qx\| = \sqrt{a}\sqrt{\gamma} + \sqrt{1-a}\sqrt{1-\gamma}$$

with equality throughout in (19) for $x = x_0$ where

(20) $$x_0 = \sqrt{(\gamma/a)}\, Pz_0 + \sqrt{(1-\gamma)/(1-a)}\, Qz_0 \in Z_c.$$

If $c \leq a$, $\gamma = a$ maximizes (19) and the maximum is 1. For $c > a$, $\gamma = c$ maximizes (19).

Summarizing, φ is given by

(21) $$\varphi(c) = \begin{cases} 0 & \text{if} \quad 0 \leq c \leq a \\ 1 - \left[\sqrt{ac} + \sqrt{(1-a)(1-c)}\right]^2 & \text{if} \quad a \leq c \leq 1. \end{cases}$$

It is clear that $\varphi(0) = 0$ and $b_1 \equiv \varphi(1) < 1$. Also, it is easy to show that φ is a continuous convex function on $[0, 1]$. Thus, $b_2 \equiv \varphi(b_1) = \varphi((1-b_1)0 + b_1 1) \leq b_1\varphi(1) = b_1^2$. Proceeding by induction, $b_i \equiv \varphi(b_{i-1})$ and $b_i \leq b_1^i$, $i = 1, 2, \ldots$. Thus $\lim_{i\to\infty} b_i = 0$. Since φ is zero in the interval $[0, a]$, there exists an index i_0 such that $b_i = 0$ for all $i \geq i_0$. Thus (14) holds and the proof of Lemma 2 is complete.

<u>Corollary 1:</u> Let $G_1 = \langle \mathcal{R} \rangle$ where $\mathcal{R} = \{S_r | r \in R\}$. If G_1 is infinite and irreducible, then $\overline{G}_1 = O(n)$ and for each $x \in C_n$, $\{gx | g \in G_1\}$ is dense in C_n.

<u>Remark:</u> The assumption that G is generated by reflections cannot be removed. For example, consider $x \in R^4$ with x written as

$$x = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$$

for $g = (\Gamma_1, \Gamma_2)$ with $\Gamma_i \in O(2)$, $i = 1, 2$, consider $g(x) = \Gamma_1 x \Gamma_2'$. Then

$G = [g] \subseteq O(4)$ is infinite, closed, and irreducible, but G is certainly not transitive on R^4 so $G \neq O(4)$. 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] Benson, C. T. and Grove, L. C. (1971). Finite Reflection Groups. Bogden and Quigley, Tarrytown-on-Hudson, New York.

[2] Eaton, M. L. and Perlman, M. (1976). Generalized Schur Functions: G-Monotone Functions Invariant under Reflection Groups. University of Minnesota Technical Report.