SIAM J. OPTIM.
Vol. 25, No. 3, pp. 1314–1343

SEMIDEFINITE DESCRIPTIONS OF THE CONVEX HULL OF ROTATION MATRICES*

J. SAUNDERSON†, P. A. PARRILO†, AND A. S. WILLSKY†

Abstract. We study the convex hull of $SO(n)$, the set of $n \times n$ orthogonal matrices with unit determinant, from the point of view of semidefinite programming. We show that the convex hull of $SO(n)$ is *doubly spectrahedral*, i.e., both it and its polar have a description as the intersection of a cone of positive semidefinite matrices with an affine subspace. Our spectrahedral representations are explicit and are of minimum size, in the sense that there are no smaller spectrahedral representations of these convex bodies.

Key words. doubly spectrahedral, special orthogonal group, orbitope

AMS subject classifications. 90C22, 90C25, 52A41, 52A20

DOI. 10.1137/14096339X

1. Introduction.

Optimization problems where the decision variables are constrained to be in the set of orthogonal matrices

$$O(n) := \{X \in \mathbb{R}^{n\times n} : X^T X = I\} \tag{1.1}$$

arise in many contexts (see, e.g., [25, 26] and references therein), particularly when searching over Euclidean isometries or orthonormal frames. In some situations, especially those arising from physical problems, we require the additional constraint that the decision variables be in the set of rotation matrices

$$SO(n) := \{X \in \mathbb{R}^{n\times n} : X^T X = I, \ \det(X) = 1\} \tag{1.2}$$

representing Euclidean isometries that also *preserve orientation*. For example, these additional constraints arise in problems involving attitude estimation for spacecraft [27], in pose estimation in computer vision applications [19], or in understanding protein folding [23]. The unit determinant constraint is important in these situations because we typically cannot reflect physical objects such as spacecraft or molecules.

The set of $n \times n$ rotation matrices is nonconvex, so optimization problems over rotation matrices are ostensibly nonconvex optimization problems. An important approach to global nonconvex optimization is to approximate the original nonconvex problem with a tractable convex optimization problem. In some circumstances, it may even be possible to *exactly reformulate* the original nonconvex problem as a tractable convex problem. This approach to global optimization via convexification has been very influential in combinatorial optimization [34] and more generally in polynomial optimization via the machinery of moments and sums of squares [4]. As an example of a problem amenable to this approach, in section 2 we describe the problem of jointly estimating the attitude and spin-rate of a spinning satellite and show how to

*Received by the editors April 2, 2014; accepted for publication (in revised form) April 6, 2015; published electronically July 14, 2015. This research was funded by the Air Force Office of Scientific Research under grants FA9550-12-1-0287 and FA9550-11-1-0305.
http://www.siam.org/journals/siopt/25-3/96339.html
†Laboratory for Information and Decision Systems, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge MA 02139 (jamess@mit.edu, parrilo@mit.edu, willsky@mit.edu).

reformulate this ostensibly nonconvex problem as a convex optimization problem that, using the constructions in this paper, can be expressed as a semidefinite program.

When we attempt to convexify optimization problems involving rotation matrices, two natural geometric objects arise. The first of these is the *convex hull* of $SO(n)$, which we denote, throughout, by $\operatorname{conv} SO(n)$. The second convex body of interest in this paper is the *polar* of $SO(n)$, the set of linear functionals that take value at most one on $SO(n)$, i.e.,

$$SO(n)^\circ = \{Y \in \mathbb{R}^{n\times n} : \langle Y, X\rangle \leq 1 \text{ for all } X \in SO(n)\},$$

where we have identified $\mathbb{R}^{n\times n}$ with its dual space via the trace inner product $\langle Y, X\rangle = \operatorname{tr}(Y^T X)$. These two convex bodies are closely related. Since $\operatorname{conv} SO(n)$ is closed and contains the origin, it follows from basic results of convex analysis [31, Theorem 14.5] that $\operatorname{conv} SO(n) = (SO(n)^\circ)^\circ$.

We also study the convex hull and the polar of orthogonal matrices in this paper. It is well known that these correspond to commonly used matrix norms (see, e.g., [32]). The convex hull of $O(n)$ is the *operator norm ball*, the set of $n\times n$ matrices with largest singular value at most one, and the polar of $O(n)$ is the *nuclear norm ball*, the set of $n \times n$ matrices such that the sum of the singular values is at most one, i.e.,

$$\operatorname{conv} O(n) = \left\{X \in \mathbb{R}^{n\times n} : \sigma_1(X) \leq 1\right\} \text{ and } O(n)^\circ = \left\{X \in \mathbb{R}^{n\times n} : \sum_{i=1}^{n} \sigma_i(X) \leq 1\right\}.$$

Note that $O(n)$ is the (disjoint) union of $SO(n)$ and the set $SO^-(n) := \{X \in \mathbb{R}^{n\times n} : X^T X = I, \det(X) = -1\}$. As such, it follows from basic properties of the polar [31, Corollary 16.5.2] that

$$O(n)^\circ = SO(n)^\circ \cap SO^-(n)^\circ, \tag{1.3}$$

allowing us to deduce properties of $O(n)^\circ$ from those of $SO(n)^\circ$. On the other hand, we show in Proposition 4.6 that for $n \geq 3$,

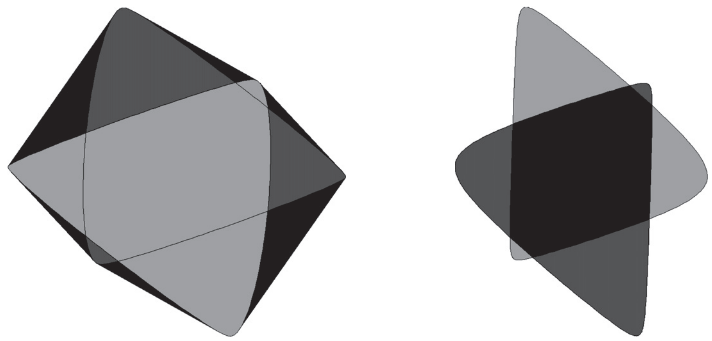
$$\operatorname{conv} SO(n) = (\operatorname{conv} O(n)) \cap (n-2)SO^-(n)^\circ, \tag{1.4}$$

allowing us to deduce properties of $\operatorname{conv} SO(n)$ from properties of $\operatorname{conv} O(n)$ and $SO^-(n)^\circ$. Figure 1 illustrates the differences between $\operatorname{conv} SO(n)$ and $\operatorname{conv} O(n)$ and the relationship described in (1.3).

The convex bodies $\operatorname{conv} SO(n)$ and $\operatorname{conv} O(n)$ are examples of *orbitopes*, a family of highly symmetric convex bodies that arise from representations of groups [2, 3, 32]. Suppose a compact group G acts on $\mathbb{R}^n$ by linear transformations and $x_0 \in \mathbb{R}^n$. Then the *orbit* of x_0 under G is

$$G \cdot x_0 = \{g \cdot x_0 : g \in G\} \subseteq \mathbb{R}^n$$

and the corresponding *orbitope* is $\operatorname{conv}(G \cdot x_0)$, the convex hull of the orbit. The sets $O(n)$ and $SO(n)$ defined above can be thought of as the orbit of the identity matrix $I \in \mathbb{R}^{n\times n}$ under the linear action of the groups $O(n)$ and $SO(n)$, respectively, by right multiplication on $n\times n$ matrices. The corresponding orbitopes are known as the *tautological* $O(n)$ *orbitope* and the *tautological* $SO(n)$ *orbitope*, respectively [32]. The set $SO^-(n)$ can be viewed as the orbit of $R := \operatorname{diag}^*(1, 1, \ldots, 1, -1)$, the diagonal matrix with diagonal entries $(1, 1, \ldots, 1, -1)$, under the same $SO(n)$ action on $n \times n$



(a) A two-dimensional projection of $\operatorname{conv} SO(3)$ (light gray), $\operatorname{conv} SO^-(3)$ (dark gray), and $\operatorname{conv} O(3) = \operatorname{conv}[SO(3) \cup SO^-(3)]$ (black).

(b) The corresponding two-dimensional section of $SO(3)^\circ$ (light gray), $SO^-(3)^\circ$ (dark gray), and $O(3)^\circ = SO(3)^\circ \cap SO^-(3)^\circ$ (black).

FIG. 1. *Pictures of some of the convex bodies considered in this paper. These were created by optimizing* 100 *linear functionals over each of these sets to obtain* 100 *boundary points. The optimization was performed by implementing our spectrahedral representations in the parser YALMIP* [22] *and solving the semidefinite programs numerically using SDPT*3 [36].

matrices. Note that $SO^-(n)$ is then the image of $SO(n)$ under the invertible linear map $X \mapsto R \cdot X$.

Spectrahedra. For convex reformulations or relaxations involving the convex hull of $SO(n)$ to be useful from a computational point of view, we need an effective description of the convex body $\operatorname{conv} SO(n)$. One effective way to describe a convex body is to express it as the intersection of the cone of symmetric positive semidefinite matrices with an affine subspace. Such convex bodies are called *spectrahedra* [28] and are natural generalizations of polyhedra. Algebraically, a convex subset C of $\mathbb{R}^n$ (containing the origin in its interior[1]) is a spectrahedron if it can be expressed as the feasible region of a linear matrix inequality of the form

$$C = \left\{ x \in \mathbb{R}^n : I_m + \sum_{i=1}^{n} A^{(i)} x_i \succeq 0 \right\}, \tag{1.5}$$

where I_m is the $m \times m$ identity matrix, $A^{(1)}, A^{(2)}, \ldots, A^{(n)}$ are $m \times m$ real symmetric matrices, and $M \succeq 0$ means that M is a symmetric positive semidefinite matrix. If the matrices $A^{(i)}$ are $m \times m$, we call the description (1.5) a *spectrahedral representation of size m*.

Giving a spectrahedral representation for a convex set has algebraic, geometric, and algorithmic implications. Algebraically, a spectrahedral representation of C of size m as in (1.5) tells us that the degree m polynomial $p(x) = \det(I + \sum_{i=1}^{n} A^{(i)} x_i)$ vanishes on the boundary of C and that C itself can be written as the region defined by m polynomial inequalities (i.e., it is a basic closed semialgebraic set) [30, Theorem 20]. Geometrically, a spectrahedral representation of C gives information about its facial structure. For example, it is known that all faces of a spectrahedron are exposed (i.e., can be obtained as the intersection of the spectrahedron with a supporting hyperplane), since the same is true for the positive semidefinite cone.

[1] We can assume this without loss of generality by translating C and restricting to its affine hull.

From the point of view of optimization, problems involving minimizing a linear functional over a spectrahedron are called *semidefinite optimization* problems [4] and are natural generalizations of the more well-known class of linear programming problems. Semidefinite optimization problems can be solved (to any desired accuracy) in time polynomial in n and m.

The convex sets that can be obtained as the images of spectrahedra under linear maps are also of interest. Indeed, to minimize a linear functional over a projection of a spectrahedron, one can simply lift the linear functional and minimize it over the spectrahedron itself using methods for semidefinite optimization. We say a convex body has a *PSD lift* if it has a description as a projection of a spectrahedron (see section 5.2). PSD lifts are important because they form a strictly larger family of convex sets than spectrahedra and because some spectrahedra have PSD lifts that are much more concise than their smallest spectrahedral representations (see Example 1.5), generalizing the notion of extended formulations for polyhedra. On the other hand, convex bodies that have PSD lifts do not enjoy the same nice algebraic and geometric properties as spectrahedra—indeed, they are semialgebraic but not necessarily basic semialgebraic and are not necessarily facially exposed [4].

Throughout much of the paper, we consider only spectrahedral representations, confining our discussion of PSD lifts to section 5.2.

Doubly spectrahedral convex sets. In this paper, we are interested in both $SO(n)^\circ$ and $\operatorname{conv} SO(n)$, and so we study both from the point of view of semidefinite programming. For finite sets S, both S° and $\operatorname{conv} S$ are polyhedra. On the other hand, for infinite sets S, usually neither S° nor $\operatorname{conv} S$ are spectrahedra. Even if a convex set is a spectrahedron, typically its polar is not a spectrahedron (see section 6). We use the term *doubly spectrahedral convex sets* to refer to those very special convex sets C with the property that both C and C° are spectrahedra.

Main contribution. The main contribution of this paper is to establish that $\operatorname{conv} SO(n)$ is doubly spectrahedral and to give explicit spectrahedral representations of both $SO(n)^\circ$ and $\operatorname{conv} SO(n)$.

Main proof technique. The main idea behind our representations is that we start with a *parameterization* of $SO(n)$, rather than working with the defining equations in (1.2). The parameterization is a direct (and classical) generalization of the widely used unit quaternion parameterization of $SO(3)$. In higher dimensions, the unit quaternions are replaced with $\mathrm{Spin}(n)$, a multiplicative subgroup of the invertible elements of a Clifford algebra. In the cases $n = 2$ and $n = 3$, it is relatively straightforward to produce our semidefinite representations directly from this parameterization. For $n \geq 4$, the parameterization does not immediately yield our semidefinite representations. The additional arguments required to establish the correctness of our representations for $n \geq 4$ form the main technical contribution of the paper.

1.1. Statement of results. In this section, we explicitly state the spectrahedral representations that we prove are correct in subsequent sections of the paper. In particular, we state spectrahedral representations for $SO(n)^\circ$ and $\operatorname{conv} SO(n)$, as well as a spectrahedral representation of $O(n)^\circ$, the nuclear norm ball. All the spectrahedral representations stated in this section are of minimum size (see Theorem 1.4). The reader primarily interested in implementing our semidefinite representations should find all the information necessary to do so in this section.

Matrices of the spectrahedral representations. Our main results are stated in terms of a collection of symmetric $2^{n-1} \times 2^{n-1}$ matrices denoted $(A^{(ij)})_{1\leq i,j\leq n}$. We give concrete descriptions of them here in terms of the Kronecker product of 2×2 matrices, deferring more invariant descriptions to Appendix A. The matrices $A^{(ij)}$ can be expressed as

$$A^{(ij)} = -P_{\text{even}}^T \lambda_i \rho_j P_{\text{even}}, \tag{1.6}$$

where $(\lambda_i)_{i=1}^n$ and $(\rho_i)_{i=1}^n$ are the $2^n \times 2^n$ skew-symmetric matrices defined concretely by

$$\lambda_i = \overbrace{\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}}^{i-1} \otimes \begin{bmatrix}0 & -1\\1 & 0\end{bmatrix} \otimes \overbrace{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}}^{n-i}$$

$$\rho_i = \underbrace{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}}_{i-1} \otimes \begin{bmatrix}0 & -1\\1 & 0\end{bmatrix} \otimes \underbrace{\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}}_{n-i}$$

and P_{even} is the $2^n \times 2^{n-1}$ matrix with orthonormal columns

$$P_{\text{even}} = \frac{1}{2}\begin{bmatrix}1\\1\end{bmatrix} \otimes \overbrace{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}}^{n-1} + \frac{1}{2}\begin{bmatrix}1\\-1\end{bmatrix} \otimes \overbrace{\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}}^{n-1}.$$

Note that $P_{\text{even}}^T M P_{\text{even}}$ just selects a particular $2^{n-1} \times 2^{n-1}$ principal submatrix of M. For any $1 \leq i \leq n$, λ_i and ρ_i are both skew-symmetric since they are formed by taking the Kronecker product of $n-1$ symmetric matrices and one skew-symmetric matrix. Furthermore, for any pair $1 \leq i, j \leq n$, the product $\lambda_i \rho_j$ is symmetric. This is because if $i \geq j$, $\lambda_i \rho_j$ is the Kronecker product of n symmetric matrices, and if $i < j$, $\lambda_i \rho_j$ is the Kronecker product of $n-2$ symmetric matrices and two skew-symmetric matrices. It follows that each $A^{(ij)}$ is symmetric. Furthermore, since λ_i and ρ_j are signed permutation matrices, so is $-\lambda_i \rho_j$. From this we can see that all of the entries of the $A^{(ij)}$ are 0, 1, or -1.

Spectrahedral representations. The following, which we prove in section 4, is the main technical result of the paper.

THEOREM 1.1. *The polar of $SO(n)$ is a spectrahedron. Explicitly,*

$$SO(n)^\circ = \left\{ Y \in \mathbb{R}^{n \times n} : \sum_{i,j=1}^n A^{(ij)} Y_{ij} \preceq I_{2^{n-1}} \right\}, \tag{1.7}$$

where the $2^{n-1} \times 2^{n-1}$ matrices $A^{(ij)}$ are defined in (1.6).

Since $O(n) = SO(n) \cup SO^-(n)$, as a corollary of Theorem 1.1 we obtain a spectrahedral representation of $O(n)^\circ = SO(n)^\circ \cap SO^-(n)^\circ$.

THEOREM 1.2. *The polar of $O(n)$ is a spectrahedron. Explicitly,*

$$O(n)^\circ = \left\{ Y \in \mathbb{R}^{n \times n} : \sum_{i,j=1}^n A^{(ij)} Y_{ij} \preceq I_{2^{n-1}},\ \sum_{i,j=1}^n A^{(ij)} [RY]_{ij} \preceq I_{2^{n-1}} \right\},$$

where $R = \operatorname{diag}^*(1, 1, \ldots, 1, -1)$.

Just because a convex set C is a spectrahedron does not, in general, mean that its polar is also spectrahedron. (See section 6 for a simple example.) Even if we are in the special case where C is doubly spectrahedral, it is not straightforward to obtain a spectrahedral representation of C° from a spectrahedral representation of C. For example, if C is a polyhedron (and so certainly doubly spectrahedral), this is the problem of computing a facet description of C° (i.e., the vertices of C) from a facet description of C.

Nevertheless, we obtain a spectrahedral representation of $\operatorname{conv} SO(n)$ by showing that, for $n \geq 3$, $\operatorname{conv} SO(n) = (\operatorname{conv} O(n)) \cap (n-2)SO^-(n)^\circ$ (Proposition 4.6), expressing $\operatorname{conv} SO(n)$ as the intersection of two spectrahedra. We explain how this works in detail in section 4.3.

THEOREM 1.3. *The convex hull of $SO(n)$ is a spectrahedron. Explicitly,*

(1.8)
$$\operatorname{conv} SO(n) = \left\{ X \in \mathbb{R}^{n\times n} : \begin{bmatrix} 0 & X \\ X^T & 0 \end{bmatrix} \preceq I_{2n},\ \sum_{i,j=1}^{n} A^{(ij)}[RX]_{ij} \preceq (n-2)I_{2^{n-1}} \right\}.$$

In the special cases $n = 2$ and $n = 3$, we have

(1.9)
$$\operatorname{conv} SO(2) = \left\{ \begin{bmatrix} c & -s \\ s & c \end{bmatrix} \in \mathbb{R}^{2\times 2} : \begin{bmatrix} 1+c & s \\ s & 1-c \end{bmatrix} \succeq 0 \right\} \quad \text{and}$$

(1.10)
$$\operatorname{conv} SO(3) = \left\{ X \in \mathbb{R}^{3\times 3} : \sum_{i,j=1}^{3} A^{(ij)}[RX]_{ij} \preceq I_4 \right\}$$

(1.11)
$$= \left\{ X \in \mathbb{R}^{3\times 3} : \begin{bmatrix} 1-X_{11}-X_{22}+X_{33} & X_{13}+X_{31} & X_{12}-X_{21} & X_{23}+X_{32} \\ X_{13}+X_{31} & 1+X_{11}-X_{22}-X_{33} & X_{23}-X_{32} & X_{12}+X_{21} \\ X_{12}-X_{21} & X_{23}-X_{32} & 1+X_{11}+X_{22}+X_{33} & X_{31}-X_{13} \\ X_{23}+X_{32} & X_{12}+X_{21} & X_{31}-X_{13} & 1-X_{11}+X_{22}-X_{33} \end{bmatrix} \succeq 0 \right\}.$$

We note that the representation of $\operatorname{conv} SO(3)$ described by Sanyal, Sottile, and Sturmfels [32, Proposition 4.1] can be obtained from the spectrahedral representation for $\operatorname{conv} SO(3)$ given here by conjugating by a signed permutation matrix, establishing that the two representations are equivalent.

In section 5, we prove that our spectrahedral representations in Theorems 1.1, 1.2, 1.3 are of minimum size. We do so by establishing lower bounds on the minimum size of spectrahedral representations of $SO(n)^\circ$, $\operatorname{conv} SO(n)$, and $O(n)^\circ$ that match the upper bounds given by our constructions.

THEOREM 1.4. *If $n \geq 1$, the minimum size of a spectrahedral representation of $O(n)^\circ$ is 2^n. If $n \geq 2$, the minimum size of a spectrahedral representation of $SO(n)^\circ$ is 2^{n-1}. If $n \geq 4$, the minimum size of a spectrahedral representation of* $\operatorname{conv} SO(n)$ *is $2^{n-1}+2n$. The minimum size of a spectrahedral representation of* $\operatorname{conv} SO(3)$ *is* 4.

Representations as PSD lifts. Given a spectrahedral representation of size m of a convex set C (with the origin in its interior), by applying a straightforward conic duality argument (see, for example, [14, Proposition 3.1]) we can obtain a PSD lift of C°. This representation, however, is usually *not* a spectrahedral representation.

Example 1.5. Theorems 1.2 and 1.4 tell us that the smallest spectrahedral representation of $O(n)^\circ$, the nuclear norm ball, has size 2^n. Yet by dualizing the size

$2n$ spectrahedral representation of $\operatorname{conv} O(n)$ (given in Proposition 4.7 to follow), we obtain a PSD lift of $O(n)^\circ$ of size $2n$

$$O(n)^\circ = \left\{ Z \in \mathbb{R}^{n\times n} : \exists X, Y \ \text{ s.t. } \begin{bmatrix} X & Z \\ Z^T & Y \end{bmatrix} \succeq 0,\ \operatorname{tr}(X) + \operatorname{tr}(Y) = 2 \right\}.$$

This is equivalent to the representation given by Fazel [11] for the nuclear norm ball.

By dualizing, in a similar fashion, the spectrahedral representation of $SO(n)^\circ$, we obtain a representation of $\operatorname{conv} SO(n)$ as the projection of a spectrahedron, i.e., a PSD lift of $\operatorname{conv} SO(n)$. In some situations, it may be preferable to use this representation of $\operatorname{conv} SO(n)$ rather than the spectrahedral representation in Theorem 1.3.

COROLLARY 1.6. *The convex hull of $SO(n)$ can be expressed as a projection of the $2^{n-1} \times 2^{n-1}$ positive semidefinite matrices with trace one as*

$$\operatorname{conv} SO(n) = \left\{ \begin{bmatrix} \langle A^{(11)}, Z\rangle & \langle A^{(12)}, Z\rangle & \cdots & \langle A^{(1n)}, Z\rangle \\ \langle A^{(21)}, Z\rangle & \langle A^{(22)}, Z\rangle & \cdots & \langle A^{(2n)}, Z\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle A^{(n1)}, Z\rangle & \langle A^{(n2)}, Z\rangle & \cdots & \langle A^{(nn)}, Z\rangle \end{bmatrix} : Z \succeq 0,\ \operatorname{tr}(Z) = 1 \right\}.$$

We note that a straightforward application of [14, Proposition 3.1] to our spectrahedral representation of $SO(n)^\circ$ gives a PSD lift of $\operatorname{conv} SO(n)$ with the condition $\operatorname{tr}(Z) \leq 1$, whereas Corollary 1.6 has $\operatorname{tr}(Z) = 1$. That these two conditions describe the same set follows from the fact that there is a point Z_0 satisfying $\operatorname{tr}(Z_0) = 1$, $Z_0 \succeq 0$, and $\langle A^{(ij)}, Z_0\rangle = 0$ for all $1 \leq i, j \leq n$. One can take $Z_0 = I/2^{n-1}$, since $\operatorname{tr}(A^{(ij)}) = 0$ for all $1 \leq i, j \leq n$, a fact we establish in Lemma A.11 using properties of the linear maps represented by the matrices $A^{(ij)}$.

1.2. Related work. That the convex hull of $O(n)$ is a spectrahedron is a classical result. (We give a self-contained proof of this fact in Proposition 4.7.) It was not until recently that Sanyal, Sottile, and Sturmfels [32] established that $O(n)^\circ$ is a spectrahedron by explicitly giving a (nonoptimal) size $\binom{2n}{n}$ spectrahedral representation. In the same paper, the authors study numerous $SO(n)$- and $O(n)$-orbitopes considering both convex geometric aspects, such as their facial structure and Carathéodory number, and algebraic aspects, such as their algebraic boundary and whether they are spectrahedra. They describe (previously known) spectrahedral representations of $\operatorname{conv} SO(2)$ and $\operatorname{conv} SO(3)$. The representation for $\operatorname{conv} SO(3)$ given in [32, equation 4.1] is equivalent to our representation in Theorem 1.3, and the representation given in [32, equation 4.2] is equivalent to

$$\operatorname{conv} SO(3) = \left\{ \begin{bmatrix} Z_{11}-Z_{22}-Z_{33}+Z_{44} & -2Z_{13}-2Z_{24} & -2Z_{12}+2Z_{34} \\ 2Z_{13}-2Z_{24} & Z_{11}+Z_{22}-Z_{33}-Z_{44} & -2Z_{14}-2Z_{23} \\ 2Z_{12}+2Z_{34} & 2Z_{14}-2Z_{23} & Z_{11}-Z_{22}+Z_{33}-Z_{44} \end{bmatrix} : Z \succeq 0,\ \operatorname{tr}(Z) = 1 \right\},$$

which can be obtained by specializing Corollary 1.6. Sanyal, Sottile, and Sturmfels raise the general question of whether $\operatorname{conv} SO(n)$ is a spectrahedron for all n (which we answer in the affirmative) and more broadly ask for a classification of the $SO(n)$-orbitopes that are spectrahedra.

Earlier work on orbitopes in the context of convex geometry includes the work of Barvinok and Vershik [3], who consider orbitopes of finite groups in the context of combinatorial optimization, Barvinok and Blekherman [2], who used asymptotic volume computations to show that there are many more nonnegative polynomials than sums of squares (among other things), and Longinetti, Sgheri, and Sottile [23], who studied $SO(3)$-orbitopes with a view to applications in protein structure determination. More recently, Sinn [35] has studied in detail the algebraic boundary of four-dimensional $SO(2)$-orbitopes as well as the Barvinok–Novik orbitopes.

1.3. Notation. In this section, we gather notation not explicitly defined elsewhere in the paper. We use $\mathcal{S}^m$ and $\mathcal{S}^m_+$ to denote the space of symmetric $m \times m$ matrices and the cone of positive semidefinite matrices, respectively. If $\mathcal{U} \subseteq \mathbb{R}^n$ is a subspace, then $\pi_\mathcal{U} : \mathbb{R}^n \to \mathcal{U}$ is the orthogonal projector onto $\mathcal{U}$ and $\pi^*_\mathcal{U} : \mathcal{U} \to \mathbb{R}^n$ is its adjoint. If the subspace in question is the subspace of diagonal matrices $\mathcal{D} \subseteq \mathbb{R}^{n\times n}$, we occasionally also use $\mathrm{diag} := \pi_\mathcal{D}$ and $\mathrm{diag}^* := \pi^*_\mathcal{D}$. We frequently use the matrix $R = \mathrm{diag}^*(1, 1, \ldots, 1, -1) \in \mathbb{R}^{n\times n}$. It could be replaced, throughout, by any orthogonal self-adjoint matrix with determinant -1. We use the shorthand $[n]$ for the set $\{1, 2, \ldots, n\}$ and $\mathcal{I}_{\mathrm{even}}$ for the set of subsets of $[n]$ with even cardinality.

1.4. Outline. The remainder of the paper is organized as follows. In section 2, we describe a problem in satellite attitude estimation that can be reformulated as a semidefinite program using the ideas in this paper. Section 3 focuses on the symmetry properties of $\mathrm{conv}\, SO(n)$ and $\mathrm{conv}\, O(n)$, as well as certain convex polytopes that naturally arise when studying these convex bodies. With these preliminaries established, section 4 outlines the main arguments required to establish the correctness of the spectrahedral representations of $SO(n)^\circ$, $O(n)^\circ$, $\mathrm{conv}\, SO(n)$, and $\mathrm{conv}\, O(n)$. Details of some of the constructions required for these arguments are deferred to Appendix A. Section 5 establishes lower bounds on the size of spectrahedral representations of $SO(n)^\circ$, $O(n)^\circ$, $\mathrm{conv}\, SO(n)$, and $\mathrm{conv}\, O(n)$ as well as a lower bound on the size of equivariant PSD lifts of $\mathrm{conv}\, SO(n)$.

Many of the properties of the convex bodies of interest in this paper are summarized in Table 1, which may serve as a useful navigational aid for the reader.

2. An illustrative application—joint satellite attitude and spin-rate estimation. In this section, we discuss a problem in satellite attitude estimation that can be reformulated as a semidefinite program using the representation of $SO(n)^\circ$ described in section 1.1. Our aim here is to give a concrete example of situations where the semidefinite representations we describe in this paper arise naturally. The problem of interest is one of estimating the attitude (i.e., orientation) and spin-rate of a spinning satellite, and it is a slight generalization of a problem posed recently by Psiaki [27]. We first focus on describing the basic attitude estimation problem in section 2.1 before describing the joint attitude and spin-rate estimation problem in section 2.2.

2.1. Attitude estimation. The *attitude* of a satellite is the element of $SO(3)$ that transforms a reference coordinate system (the *inertial system*) in which, say, the sun is fixed, into a local coordinate system fixed with respect to the satellite's body (the *body system*). We are given unit vectors $x_1, x_2, \ldots, x_T$ (e.g., the alignment of the Earth's magnetic field, directions of landmarks such as the sun or other stars, etc.) in the inertial coordinate system and noisy measurements $y_1, y_2, \ldots, y_T$ of these directions in the body coordinate system. Let $Q \in SO(3)$ denote the unknown attitude of

Table 1
Summary of results related to the convex bodies considered in the paper.

S	$SO(n)$		$O(n)$	
Definition	$\{X \in \mathbb{R}^{n\times n} : X^TX = I, \det(X) = 1\}$		$\{X \in \mathbb{R}^{n\times n} : X^TX = I\}$	
S°	$SO(n)^\circ$		$O(n)^\circ$ = Nuclear norm ball	
Diagonal slice	Polar of parity polytope	(Prop. 3.4)	Cross-polytope	(Prop. 3.4)
Spectrahedral representation	Size: 2^{n-1} Optimal? Yes	(Thm 1.1) (Thm 1.4)	Size: 2^n Optimal? Yes	(Thm 1.2) (Thm 1.4)
PSD lift	Size: 2^{n-1} Optimal? Unknown	 (Cor. 5.6, Q. 6.2)	Size: $2n$	(Eg. 1.5)
$(S^\circ)^\circ = \operatorname{conv} S$	$\operatorname{conv} SO(n)$		$\operatorname{conv} O(n)$ = Operator norm ball	
Diagonal slice	Parity polytope	(Prop. 3.4)	Hypercube	(Prop. 3.4)
Spectrahedral representation	Size: $\begin{cases} 2^{n-1}+2n & n \geq 4 \\ 4 & n = 3 \end{cases}$ Optimal? Yes	(Thm 1.3) (Thm 1.4)	Size: $2n$ Optimal? Yes	(Prop. 4.7) (Thm 1.4)
PSD lift	Size: 2^{n-1} Optimal? Unknown	(Cor. 1.6) (Cor. 5.6, Q. 6.2)	Size: $2n$	

the satellite. The aim is to estimate (in the maximum likelihood sense) Q given the y_k, the x_k, and a description of the measurement noise.

The simplest noise model assumes that each y_k is independent and has a von Mises–Fisher distribution [24] (a natural family of probability distributions on the sphere) with mean Qx_k and concentration parameter κ, i.e., its probability density function is, up to a proportionality constant that does not depend on Q, $p(y_k; Q) \propto \exp(\kappa\langle y_k, Qx_k\rangle)$. Then the maximum likelihood estimate of Q is found by solving

$$\max_{Q\in SO(3)} \sum_{k=1}^{T} \kappa\langle y_k, Qx_k\rangle = \max_{Q\in SO(3)} \left\langle Q, \kappa \sum_{k=1}^{T} y_k x_k^T \right\rangle$$

$$(2.1) \qquad = \max_{Q\in \operatorname{conv} SO(3)} \left\langle Q, \kappa \sum_{k=1}^{T} y_k x_k^T \right\rangle.$$

This is a probabilistic interpretation of a problem known as *Wahba's problem* in the astronautical literature, posed by Grace Wahba in the July 1965 *SIAM Review* problems and solutions section [38, Problem 65-1].

Our spectrahedral representation of $\operatorname{conv} SO(n)$ allows us to express the optimization problem in (2.1) as a semidefinite program. In the astronautical literature, it is common to solve this problem via the q-method [21], which involves parameterizing $SO(3)$ in terms of unit quaternions and solving a symmetric eigenvalue problem. Our semidefinite programming-based formulation could be thought of as a much more flexible generalization of this eigenvalue problem-based approach that works for any n, not just the case $n = 3$.

2.2. Joint attitude and spin-rate estimation. A significant benefit of having a semidefinite programming-based description of a problem (such as Wahba's problem) is that it often allows us to devise semidefinite programming-based solutions to more complicated related problems by composing semidefinite representations in different ways. An example of this is given by the following generalization of Wahba's problem posed by Psiaki [27].[2]

Consider a satellite rotating at a constant unknown angular velocity ω rad/sample around a known axis (e.g., its major axis). Assume the body coordinate system is chosen so that the rotation is around the axis defined by the first coordinate direction. Then the attitude matrix at the kth sample instant is of the form

$$Q(k) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(k\omega) & -\sin(k\omega) \\ 0 & \sin(k\omega) & \cos(k\omega) \end{bmatrix} Q,$$

where $Q \in SO(3)$ is the initial attitude. Suppose, now, the satellite *sequentially* obtains measurements $y_0, y_1, \ldots, y_T$ in the body coordinate system of known landmarks in the directions $x_0, x_1, \ldots, x_T$ in the inertial coordinate system. As before, assume that the y_k are independent and have von Mises–Fisher distribution with mean $Q(k)x_k$ and concentration parameter κ_1. Furthermore, the satellite obtains a sequence $\omega_1, \omega_2, \ldots, \omega_T$ of noisy measurements of the unknown constant spin rate ω. Suppose the ω_k are independent and each ω_k has a von Mises distribution [24] (a natural distribution for angular-valued quantities) with mean ω and concentration parameter κ_2, i.e., its probability density function (up to a constant independent of ω) is given by $p(\omega_k; \omega) \propto \exp(\kappa_2 \cos(\omega_k - \omega))$. If the ω_k and the y_k are independent, then the maximum likelihood estimate of Q and ω can be found by solving

$$\max_{\substack{Q \in SO(3) \\ \omega \in [0,2\pi)}} \sum_{k=0}^{T} \left\langle y_k, \kappa_1 \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(k\omega) & -\sin(k\omega) \\ 0 & \sin(k\omega) & \cos(k\omega) \end{bmatrix} Q x_k \right\rangle + \kappa_2 \sum_{k=0}^{T} \cos(\omega_k - \omega). \tag{2.2}$$

Note that the optimization problem (2.2) can be rewritten as

$$\max_{\substack{Q \in SO(3) \\ \omega \in [0,2\pi)}} a_1 \cos(\omega) + b_1 \sin(\omega) + \langle A_0, Q \rangle + \sum_{k=1}^{T} \langle A_k, \cos(k\omega) Q \rangle + \langle B_k, \sin(k\omega) Q \rangle, \tag{2.3}$$

i.e., the maximization of a linear functional over

$$\mathcal{M}_{3,T} = \{(\cos(\omega), \sin(\omega), Q, \cos(\omega)Q, \sin(\omega)Q, \ldots, \cos(T\omega)Q, \sin(T\omega)Q) : \\ Q \in SO(3),\ \omega \in [0, 2\pi)\}.$$

We can reformulate this as a semidefinite program if we have a PSD lift of $\operatorname{conv}(\mathcal{M}_{3,T})$, because the optimization problem (2.3) is equivalent to the maximization of the same linear functional over $\operatorname{conv}(\mathcal{M}_{3,T})$. Using the fact that $SO(n)^\circ$ has a spectrahedral representation of size 2^{n-1}, it can be shown that that $\operatorname{conv}(\mathcal{M}_{n,T})$ has a PSD lift of size $2^{n-1}(T+1)$. Describing this in detail is beyond the scope of the present paper. Instead, we discuss this reformulation in further detail in a separate report [33].

3. Basic properties of conv $SO(n)$ and conv $O(n)$. In this section, we consider the convex bodies $\operatorname{conv} SO(n)$ and $\operatorname{conv} O(n)$ purely from the point of view of convex geometry, leaving the discussion of aspects related to their semidefinite representations for section 4. In this section, we describe their symmetries and how the

[2]Psiaki's formulation only considers the $\kappa_2 = 0$ case, where measurements of the spin rate are not considered.

full space $\mathbb{R}^{n\times n}$ of $n \times n$ matrices decomposes with respect to these symmetries, via the (special) singular value decomposition. To a large extent, one can characterize $\operatorname{conv} SO(n)$ and $\operatorname{conv} O(n)$ in terms of their intersections with the subspace of diagonal matrices. These diagonal sections are well-known polytopes—the parity polytope and the hypercube, respectively. The properties of these diagonal sections are crucial to establishing our spectrahedral representation of $\operatorname{conv} SO(n)$ in section 4.3 and the lower bounds on the size of spectrahedral representations given in section 5.

All of the results in this section are (sometimes implicitly) in the literature in various forms. Here, we aim for a brief yet unified presentation to make the paper as self-contained as possible.

3.1. Symmetry and the special singular value decomposition. In this section, we describe the symmetries of $\operatorname{conv} O(n)$ and $\operatorname{conv} SO(n)$.

The group $O(n) \times O(n)$ acts on $\mathbb{R}^{n\times n}$ by $(U, V) \cdot X = UXV^T$. This action leaves the set $O(n)$ invariant and hence leaves the convex bodies $\operatorname{conv} O(n)$ and $O(n)^\circ$ invariant. It is also useful to understand how the ambient space of $n \times n$ matrices decomposes under this group action. Indeed, by the well-known singular value decomposition, every element $X \in \mathbb{R}^{n\times n}$ can be expressed as $X = U\Sigma V^T = (U, V) \cdot \Sigma$, where $(U, V) \in O(n) \times O(n)$ and Σ is diagonal with $\Sigma_{11} \geq \cdots \geq \Sigma_{nn} \geq 0$. These diagonal elements are the *singular values*. We denote them by $\sigma_i(X) = \Sigma_{ii}$. Note that for most of what follows, we only use the fact that Σ is diagonal, not that its elements can be taken to be nonnegative and sorted.

Similarly the group

$$S(O(n) \times O(n)) = \{(U, V) : U, V \in O(n),\ \det(U)\det(V) = 1\}$$

acts on $\mathbb{R}^{n\times n}$ by $(U, V)\cdot X = UXV^T$. This action leaves the sets $SO(n)$ and $SO^-(n)$ invariant and hence leaves the convex bodies $\operatorname{conv} SO(n)$, $\operatorname{conv} SO^-(n)$, $SO(n)^\circ$, $SO^-(n)^\circ$, $\operatorname{conv} O(n)$, and $O(n)^\circ$ invariant. A variant on the singular value decomposition, known as the *special singular value decomposition* [32], describes how the space of $n\times n$ matrices decomposes under this group action. Indeed, every $X \in \mathbb{R}^{n\times n}$ can be expressed as $X = U\tilde{\Sigma}V^T = (U, V) \cdot \tilde{\Sigma}$, where $(U, V) \in S(O(n) \times O(n))$ and $\tilde{\Sigma}$ is diagonal with $\tilde{\Sigma}_{11} \geq \cdots \geq \tilde{\Sigma}_{n-1,n-1} \geq |\tilde{\Sigma}_{nn}|$. These diagonal elements are the *special singular values*. We denote them by $\tilde{\sigma}_i(X) = \tilde{\Sigma}_{ii}$. Again, in what follows, we typically only use the fact that $\tilde{\Sigma}$ is diagonal for our arguments.

The special singular value decomposition can be obtained from the singular value decomposition. Suppose that $X = U\Sigma V^T$ is a singular value decomposition of X so that $(U, V) \in O(n) \times O(n)$. If $\det(U)\det(V) = 1$, this is also a valid special singular value decomposition. Otherwise, if $\det(U)\det(V) = -1$, then $X = UR(R\Sigma)V^T$ gives a decomposition where $(UR, V) \in S(O(n) \times O(n))$ and $R\Sigma$ is again diagonal, but with the last diagonal entry being negative. As such, the singular values and special singular values of an $n\times n$ matrix are related by $\sigma_i(X) = \tilde{\sigma}_i(X)$ for $i = 1, 2, \ldots, n-1$ and $\tilde{\sigma}_n(X) = \operatorname{sign}(\det(X))\sigma_n(X)$.

The importance of these decompositions of $\mathbb{R}^{n\times n}$ under the action of $O(n)\times O(n)$ and $S(O(n) \times O(n))$ is that they allow us to reduce many arguments, by invariance properties, to arguments about diagonal matrices.

3.2. Polytopes associated with $\operatorname{conv} O(n)$ and $\operatorname{conv} SO(n)$. The convex hull of $O(n)$ is closely related to the *hypercube*

$$\mathrm{C}_n = \operatorname{conv}\{x \in \mathbb{R}^n : x_i^2 = 1 \text{ for } i \in [n]\}; \tag{3.1}$$

the convex hull of $SO(n)$ is closely related to the *parity polytope*

$$\mathrm{PP}_n = \mathrm{conv}\{x \in \mathbb{R}^n : \textstyle\prod_{i=1}^n x_i = 1,\ \ x_i^2 = 1,\ \ \text{for } i \in [n]\}; \tag{3.2}$$

the convex hull of $SO^-(n)$ is closely related to the *odd parity polytope*

$$\mathrm{PP}_n^- = \mathrm{conv}\{x \in \mathbb{R}^n : \textstyle\prod_{i=1}^n x_i = -1,\ \ x_i^2 = 1,\ \ \text{for } i \in [n]\}. \tag{3.3}$$

In this section, we briefly discuss properties of these polytopes and show that they are the diagonal sections of $\mathrm{conv}\, O(n)$, $\mathrm{conv}\, SO(n)$, and $\mathrm{conv}\, SO^-(n)$, respectively.

Facet descriptions. The hypercube has $2n$ facets corresponding to the linear inequality description

$$\mathrm{C}_n = \{x \in \mathbb{R}^n : -1 \leq x_i \leq 1 \text{ for } i \in [n]\}. \tag{3.4}$$

The parity polytope PP_n has the linear inequality description

$$\begin{aligned}\mathrm{PP}_n = \Bigg\{ x \in \mathbb{R}^n : & -1 \leq x_i \leq 1 \text{ for } i \in [n], \\ & \sum_{i \notin I} x_i - \sum_{i \in I} x_i \leq n-2 \ \text{ for } I \subseteq [n],\, |I| \text{ odd} \Bigg\}.\end{aligned} \tag{3.5}$$

This description is due to Jeroslow [20]. (See, e.g., [9, Theorem 5.3] for a self-contained proof.) If $n \geq 4$, all $2n + 2^{n-1}$ linear inequalities in (3.5) define facets. By symmetry, it suffices to check one inequality of each type. Indeed, if we remove the inequality $x_1 \leq 1$, then $(n-2, 0, \ldots, 0)$ satisfies all the other inequalities but is not in PP_n (for $n \geq 4$). Similarly, if we remove the inequality $-x_1 + x_2 + \cdots + x_n \leq n-2$, then $(-1, 1, \ldots, 1)$ satisfies all the other inequalities but is not in PP_n. In the cases $n = 2$ and $n = 3$, (3.5) simplifies to

$$\mathrm{PP}_2 = \left\{ \left[\begin{smallmatrix} x \\ x \end{smallmatrix}\right] \in \mathbb{R}^2 : -1 \leq x \leq 1 \right\} \quad \text{and} \tag{3.6}$$

$$\begin{aligned}\mathrm{PP}_3 = \{x \in \mathbb{R}^3 : & \ x_1 - x_2 + x_3 \leq 1,\ -x_1 + x_2 + x_3 \leq 1, \\ & \ x_1 + x_2 - x_3 \leq 1,\ -x_1 - x_2 - x_3 \leq 1\},\end{aligned} \tag{3.7}$$

showing that PP_3 has only four facets.

The polar of the hypercube is the *cross-polytope*. We denote it by C_n°. It is clear from (3.1) that C_n° has 2^n facets and corresponding linear inequality description

$$\mathrm{C}_n^\circ = \left\{ x \in \mathbb{R}^n : \sum_{i \notin I} x_i - \sum_{i \in I} x_i \leq 1 \quad \text{for } I \subseteq [n] \right\}. \tag{3.8}$$

The polar of the parity polytope is denoted by PP_n°. It is clear from (3.2) that PP_n° has 2^{n-1} facets and corresponding linear inequality description

$$\mathrm{PP}_n^\circ = \left\{ x \in \mathbb{R}^n : \sum_{i \notin I} x_i - \sum_{i \in I} x_i \leq 1 \quad \text{for } I \subseteq [n],\, |I| \text{ even} \right\}. \tag{3.9}$$

Similarly,

$$\mathrm{PP}_n^{-\circ} = \left\{ x \in \mathbb{R}^n : \sum_{i \notin I} x_i - \sum_{i \in I} x_i \leq 1 \quad \text{for } I \subseteq [n],\, |I| \text{ odd} \right\}. \tag{3.10}$$

To get a sense of the importance of these polytopes for understanding $\operatorname{conv} SO(n)$, it may be instructive to compare (3.5) with (1.8), (3.6) with (1.9), (3.7) with (1.10), and (3.9) with (1.7).

We conclude the discussion of these polytopes with another description of PP_n.

LEMMA 3.1. *If $n \geq 3$, the parity polytope can be expressed as*

$$\mathrm{PP}_n = \mathrm{C}_n \cap (n-2) \cdot \mathrm{PP}_n^{-\circ}.$$

If $n = 3$, this simplifies to $\mathrm{PP}_3 = \mathrm{PP}_3^{-\circ}$. *If $n = 2$,* $\mathrm{PP}_2 = \mathrm{C}_2 \cap \operatorname{span}(1,1)$.

Proof. For the general case, we need only examine the facet descriptions in (3.4), (3.5), and (3.10). If $n = 3$, the result follows by comparing (3.7) with (3.10). The case $n = 2$ is a restatement of (3.6). ∎

Diagonal projections and sections. We now establish the link between the hypercube and the convex hull of $O(n)$, and the parity polytope and the convex hull of $SO(n)$. First, we prove a result that says that the subspace $\mathcal{D}$ of diagonal matrices interacts particularly well with these convex bodies. The lemma applies for the convex bodies $\operatorname{conv} O(n)$, $\operatorname{conv} SO(n)$, and $\operatorname{conv} SO^-(n)$ because whenever g is a diagonal matrix with diagonal entries in $\{-1, 1\}$ (a diagonal sign matrix), each of these convex bodies is invariant under the conjugation map $X \mapsto gXg^T$. Note that Lemma 3.2 holds in much greater generality than the statement we give here (see, e.g., [8, Proposition 3.5]).

LEMMA 3.2. *Let $C \subseteq \mathbb{R}^{n\times n}$ be a convex body that is invariant under conjugation by diagonal sign matrices. Then $\pi_{\mathcal{D}}(C) = \pi_{\mathcal{D}}(C\cap\mathcal{D})$ and $[\pi_{\mathcal{D}}(C\cap\mathcal{D})]^\circ = \pi_{\mathcal{D}}(C^\circ\cap\mathcal{D})$.*

Proof. We first establish that $\pi_{\mathcal{D}}(C) = \pi_{\mathcal{D}}(C\cap\mathcal{D})$. Note that clearly $\pi_{\mathcal{D}}(C\cap\mathcal{D}) \subseteq \pi_{\mathcal{D}}(C)$. For the reverse inclusion, let G denote the group (of cardinality 2^n) of diagonal sign matrices and observe that $\mathcal{D}$ is the subspace of $n \times n$ matrices fixed pointwise by the conjugation action of diagonal sign matrices. Then consider the linear map

$$P(X) = \frac{1}{2^n}\sum_{g\in G} gXg^T. \tag{3.11}$$

Since the trace inner product is invariant under the action of G, it is straightforward to show that P is self-adjoint. For any $X \in \mathbb{R}^{n\times n}$ and any $g \in G$, $gP(X)g^T = P(X)$, implying that the image of P is $\mathcal{D}$. Furthermore, if $X \in \mathcal{D}$, then $P(X) = X$. Together, these observations imply that $P = \pi_{\mathcal{D}}^*\pi_{\mathcal{D}}$, the orthogonal projection onto $\mathcal{D}$.

Now, if C is invariant under the action of G and $X \in C$, then (3.11) gives a description of $\pi_{\mathcal{D}}^*\pi_{\mathcal{D}}(X)$ as a convex combination of the gXg^T, each of which is an element of the convex set C. Hence, $\pi_{\mathcal{D}}^*\pi_{\mathcal{D}}(X) \in C \cap \mathcal{D}$ and so $\pi_{\mathcal{D}}(X) \in \pi_{\mathcal{D}}(C \cap \mathcal{D})$.

Now, we establish that $[\pi_{\mathcal{D}}(C\cap\mathcal{D})]^\circ = \pi_{\mathcal{D}}(C^\circ\cap\mathcal{D})$. For any $y \in \mathcal{D}$, we have that

$$\max_{x\in\pi_{\mathcal{D}}(C\cap\mathcal{D})}\langle y, x\rangle = \max_{x\in\pi_{\mathcal{D}}(C)}\langle y, x\rangle = \max_{z\in C}\langle y, \pi_{\mathcal{D}}(z)\rangle = \max_{z\in C}\langle \pi_{\mathcal{D}}^*(y), z\rangle.$$

Hence, $y \in [\pi_{\mathcal{D}}(C \cap \mathcal{D})]^\circ$ if and only if $\pi_{\mathcal{D}}^*(y) \in C^\circ$, or, equivalently, $y \in \pi_{\mathcal{D}}(C^\circ \cap \mathcal{D})$. ∎

The key fact that relates the parity polytope and the convex hull of $SO(n)$ is the following celebrated theorem of Horn [18].

THEOREM 3.3 (Horn). *The projection onto the diagonal of $SO(n)$ is the parity polytope, i.e., $\pi_{\mathcal{D}}(SO(n)) = \mathrm{PP}_n$.*

Note that we do not need the full strength of Horn's theorem. We only use the corollaries that

$$\pi_{\mathcal{D}}(\operatorname{conv} SO(n)) = \operatorname{conv} \pi_{\mathcal{D}}(SO(n)) = \operatorname{conv} \mathrm{PP}_n = \mathrm{PP}_n \quad \text{and} \tag{3.12}$$

$$\begin{aligned} \pi_{\mathcal{D}}(\operatorname{conv} SO^-(n)) &= \pi_{\mathcal{D}}(R \cdot \operatorname{conv} SO(n)) \\ &= R \cdot \pi_{\mathcal{D}}(\operatorname{conv} SO(n)) = R \cdot \mathrm{PP}_n = \mathrm{PP}_n^-. \end{aligned} \tag{3.13}$$

We are now in a position to establish the main result of this section.

PROPOSITION 3.4. *Let $\mathcal{D} \subseteq \mathbb{R}^{n\times n}$ denote the subspace of diagonal matrices. Then*

$$\begin{aligned} \pi_{\mathcal{D}}(\mathcal{D} \cap \operatorname{conv} O(n)) &= \mathrm{C}_n, & \pi_{\mathcal{D}}(\mathcal{D} \cap O(n)^\circ) &= \mathrm{C}_n^\circ, \\ \pi_{\mathcal{D}}(\mathcal{D} \cap \operatorname{conv} SO(n)) &= \mathrm{PP}_n, & \pi_{\mathcal{D}}(\mathcal{D} \cap SO(n)^\circ) &= \mathrm{PP}_n^\circ, \\ \pi_{\mathcal{D}}(\mathcal{D} \cap \operatorname{conv} SO^-(n)) &= \mathrm{PP}_n^-, & \pi_{\mathcal{D}}(\mathcal{D} \cap SO^-(n)^\circ) &= \mathrm{PP}_n^{-\circ}. \end{aligned}$$

Proof. First note that by (3.12) and (3.13), we know that $\pi_{\mathcal{D}}(\operatorname{conv} SO(n)) = \mathrm{PP}_n$ and that $\pi_{\mathcal{D}}(\operatorname{conv} SO^-(n)) = \mathrm{PP}_n^-$. Consequently,

$$\pi_{\mathcal{D}}(\operatorname{conv} O(n)) = \operatorname{conv} \pi_{\mathcal{D}}(SO(n) \cup SO^-(n)) = \operatorname{conv}(\mathrm{PP}_n \cup \mathrm{PP}_n^-) = \mathrm{C}_n.$$

Since each of $\operatorname{conv} O(n)$, $\operatorname{conv} SO(n)$, $\operatorname{conv} SO^-(n)$ is invariant under conjugation by diagonal sign matrices, we can apply Lemma 3.2. Doing so, and using the characterization of the diagonal projections of each of these convex bodies from the previous paragraph, completes the proof. ∎

4. Spectrahedral representations of $SO(n)^\circ$ and conv $SO(n)$. This section is devoted to outlining the proofs of Theorems 1.1, 1.2, and 1.3, giving spectrahedral representations of $SO(n)^\circ$, $O(n)^\circ$, and $\operatorname{conv} SO(n)$. For the sake of exposition, we initially focus on $SO(2)^\circ$, as in this case all the ideas are familiar. Low-dimensional coincidences do mean that some issues are simpler in the 2×2 case than in general. After discussing the 2×2 case, in section 4.2 we generalize the argument, deferring some details to Appendix A. Finally, in section 4.3 we construct our spectrahedral representation of $\operatorname{conv} SO(n)$.

4.1. The 2×2 case. We begin by giving a spectrahedral representation of $SO(2)^\circ$. We make crucial use of the trigonometric identities $\cos(\theta) = \cos^2(\theta/2) - \sin^2(\theta/2)$ and $\sin(\theta) = 2\cos(\theta/2)\sin(\theta/2)$. Recall that elements of $SO(2)$ have the form

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} \cos^2(\frac{\theta}{2}) - \sin^2(\frac{\theta}{2}) & -2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) \\ 2\cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & \cos^2(\frac{\theta}{2}) - \sin^2(\frac{\theta}{2}) \end{bmatrix}$$

and that $(\cos(\theta/2), \sin(\theta/2))$ parameterizes the unit circle in $\mathbb{R}^2$. Hence, $SO(2)$ is the image of the unit circle $\{(x_1, x_2) : x_1^2 + x_2^2 = 1\}$ under the quadratic map

$$Q(x_1, x_2) = \begin{bmatrix} x_1^2 - x_2^2 & -2x_1x_2 \\ 2x_1x_2 & x_1^2 - x_2^2 \end{bmatrix}.$$

As such, $Y \in SO(2)^\circ$ if and only if, for all (x_1, x_2) in the unit circle,

$$\begin{aligned} \langle Y, Q(x_1, x_2) \rangle &= \left\langle \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix}, \begin{bmatrix} x_1^2 - x_2^2 & -2x_1x_2 \\ 2x_1x_2 & x_1^2 - x_2^2 \end{bmatrix} \right\rangle \\ &= \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} Y_{11} + Y_{22} & Y_{21} - Y_{12} \\ Y_{21} - Y_{12} & -Y_{11} - Y_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \le 1. \end{aligned}$$

This is equivalent to the spectrahedral representation

$$SO(2)^\circ = \left\{ Y : \begin{bmatrix} Y_{11} + Y_{22} & Y_{21} - Y_{12} \\ Y_{21} - Y_{12} & -Y_{11} - Y_{22} \end{bmatrix} \preceq I \right\},$$

which coincides with the $n = 2$ case of Theorem 1.1.

To summarize, the main idea of the argument is that we use a parameterization of $SO(2)$ as the image of the unit circle under a quadratic map. This parameterization allows us to rewrite the maximum of a linear functional on $SO(2)$ as the maximum of a quadratic form on the unit circle which can be expressed as a spectrahedral condition.

We note that a very similar argument works in the case $n = 3$ to directly produce the representations of $SO(3)^\circ$ and $\operatorname{conv} SO(3)$ in Theorem 1.1 and Corollary 1.6, respectively. Indeed, the unit quaternion parameterization of rotations gives a parameterization of $SO(3)$ as the image of the unit sphere in $\mathbb{R}^4$ under a quadratic mapping. This allows us to rewrite the maximum of a linear functional on $SO(3)$ as the maximum of a quadratic form on the unit sphere or, equivalently, as a spectrahedral condition.

4.2. Outline of the general argument. For the general case, we first need a quadratic parameterization of $SO(n)$. There is a classical construction of a quadratic map $Q : \mathbb{R}^{2^{n-1}} \to \mathbb{R}^{n\times n}$ and a subset $\operatorname{Spin}(n)$ of the unit sphere in $\mathbb{R}^{2^{n-1}}$ such that $SO(n) = Q(\operatorname{Spin}(n))$. (We recall this construction in Appendix A, only discussing those aspects relevant for our argument here.)

Unfortunately, for $n \geq 4$, $\operatorname{Spin}(n)$ is a *strict* subset of the unit sphere in $\mathbb{R}^{2^{n-1}}$, so we cannot simply follow the argument for the $n = 2$ case verbatim. The key difficulty is that we need a spectrahedral characterization of the maximum *over* $\operatorname{Spin}(n)$ of the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ (for arbitrary Y). It is not obvious how to do this when $\operatorname{Spin}(n)$ is a strict subset of the sphere.

We achieve this by showing that, for any Y, the maximum of the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ over the entire sphere coincides with its maximum over the strict subset $\operatorname{Spin}(n)$ of the sphere (see Proposition 4.4, to follow). To establish this, we exploit additional structure in $\operatorname{Spin}(n)$ and certain equivariance properties of Q. The specific properties we use are stated in Propositions 4.1, 4.2, and 4.3. We prove these in Appendix A.

PROPOSITION 4.1. *There exist a 2^{n-1}-dimensional inner product space,* $\mathrm{Cl}^0(n)$*, a subset* $\operatorname{Spin}(n)$ *of the unit sphere in* $\mathrm{Cl}^0(n)$ *and a quadratic map* $Q : \mathrm{Cl}^0(n) \to \mathbb{R}^{n\times n}$ *such that* $Q(\operatorname{Spin}(n)) = SO(n)$.

From now on fix $\mathrm{Cl}^0(n)$, $\operatorname{Spin}(n)$, and Q that satisfy the previous proposition and are explicitly constructed in Appendix A. The quadratic mapping Q interacts well with left and right multiplication by elements of $SO(n)$.

PROPOSITION 4.2. *If $U, V \in SO(n)$, then there is a corresponding invertible linear map* $\Phi_{(U,V)} : \mathrm{Cl}^0(n) \to \mathrm{Cl}^0(n)$ *such that for any* $x \in \mathrm{Cl}^0(n)$*,* $UQ(x)V^T = Q(\Phi_{(U,V)}x)$ *and* $\Phi_{(U,V)}(\operatorname{Spin}(n)) = \operatorname{Spin}(n)$.

Recall that $\mathcal{I}_{\text{even}}$ denotes the collection of subsets of $[n]$ of even cardinality.

PROPOSITION 4.3. *Given any orthonormal basis $u_1, \ldots, u_n$ for $\mathbb{R}^n$, there is a corresponding orthonormal basis* $(u_I)_{I\in\mathcal{I}_{even}}$ *for* $\mathrm{Cl}^0(n)$ *such that*

- $u_I \in \operatorname{Spin}(n)$ *for all* $I \in \mathcal{I}_{even}$ *and*
- *for all* $i \in [n]$*, if* $x = \sum_{I\in\mathcal{I}_{even}} x_I u_I \in \mathrm{Cl}^0(n)$*, then*

$$\langle u_i, Q\,(x)\,u_i\rangle = \sum_{I\in\mathcal{I}_{even}} x_I^2 \langle u_i, Q(u_I)u_i\rangle.$$

The following proposition, the crux of our argument, implies that for any $n \times n$ matrix Y, the maximum of the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ over the whole sphere and over the (strict) subset $\mathrm{Spin}(n)$ coincide.

PROPOSITION 4.4. *Given any $Y \in \mathbb{R}^{n\times n}$, the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ has a basis of eigenvectors that are elements of* $\mathrm{Spin}(n)$.

Proof. Suppose that $Y \in \mathbb{R}^{n\times n}$ is arbitrary. Then by the special singular value decomposition, Y can be expressed as $Y = U^T D V$, where U and V are in $SO(n)$ and D is diagonal. Then by Proposition 4.2,

$$\langle Y, Q(x)\rangle = \langle U^T DV, Q(x)\rangle = \langle D, UQ(x)V^T\rangle = \langle D, Q(\Phi_{(U,V)}x)\rangle.$$

Consider the quadratic form $z \mapsto \langle D, Q(z)\rangle$ and let $e_1, \dots, e_n$ denote the standard basis for $\mathbb{R}^n$. By Proposition 4.3, there is a basis $(e_I)_{I\in\mathcal{I}_{\mathrm{even}}}$ such that if $z = \sum_{I\in\mathcal{I}_{\mathrm{even}}} z_I e_I$, then

$$\langle D, Q(z)\rangle = \sum_{i=1}^n D_{ii}\langle e_i, Q(z)e_i\rangle = \sum_{I\in\mathcal{I}_{\mathrm{even}}} z_I^2 \left(\sum_{i=1}^n D_{ii}\langle e_i, Q(e_I)e_i\rangle\right).$$

Hence, $z \mapsto \langle D, Q(z)\rangle$ has $(e_I)_{I\in\mathcal{I}_{\mathrm{even}}}$ as a basis of eigenvectors. Hence, the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ has $\Phi_{(U,V)}^{-1} e_I$ for $I \in \mathcal{I}_{\mathrm{even}}$ as a basis of eigenvectors. Since the e_I are in $\mathrm{Spin}(n)$ (by Proposition 4.3), $\Phi_{(U,V)}$ is invertible, and $\Phi_{(U,V)}^{-1}$ preserves $\mathrm{Spin}(n)$ (by Proposition 4.2), we can conclude that the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ has a basis of eigenvectors all of which are elements of $\mathrm{Spin}(n)$. ∎

Assuming Propositions 4.1 and 4.4, we can prove Theorem 1.1 using an embellishment of the same argument we used in the 2×2 case.

THEOREM 1.1. *The polar of $SO(n)$ is a spectrahedron. Explicitly,*

$$SO(n)^\circ = \left\{ Y \in \mathbb{R}^{n\times n} : \sum_{i,j=1}^n A^{(ij)} Y_{ij} \preceq I_{2^{n-1}} \right\},$$

where the $2^{n-1} \times 2^{n-1}$ matrices $A^{(ij)}$ are defined in (1.6).

Proof. Since the image of $\mathrm{Spin}(n)$ under Q is $SO(n)$, an $n \times n$ matrix Y is in $SO(n)^\circ$ if and only if

$$\max_{X\in SO(n)} \langle Y, X\rangle = \max_{x\in \mathrm{Spin}(n)} \langle Y, Q(x)\rangle \le 1.$$

Since $\mathrm{Spin}(n)$ is a subset of the unit sphere in $\mathrm{Cl}^0(n)$, we have that

$$\max_{x\in\mathrm{Spin}(n)} \langle Y, Q(x)\rangle \le \max_{\substack{x\in \mathrm{Cl}^0(n)\\ \langle x,x\rangle = 1}} \langle Y, Q(x)\rangle.$$

The maximum of the quadratic form $x \mapsto \langle Y, Q(x)\rangle$ over the unit sphere in $\mathrm{Cl}^0(n)$ occurs at any eigenvector corresponding to the largest eigenvalue of the quadratic form. By Proposition 4.4, we can always find such an eigenvector in $\mathrm{Spin}(n)$, establishing that

$$\max_{x\in\mathrm{Spin}(n)} \langle Y, Q(x)\rangle = \max_{\substack{x\in \mathrm{Cl}^0(n)\\ \langle x,x\rangle = 1}} \langle Y, Q(x)\rangle.$$

Hence, $Y \in SO(n)^\circ$ if and only if for all $x \in \mathrm{Cl}^0(n)$ such that $\langle x, x\rangle = 1$,

$$\langle Y, Q(x)\rangle = \sum_{i,j=1}^{n} Y_{ij}\langle e_i, Q(x)e_j\rangle \leq 1. \tag{4.1}$$

In Appendix A.4, we explicitly describe a choice of coordinates for $\mathrm{Cl}^0(n)$ such that the matrix representing the quadratic form $x \mapsto \langle e_i, Q(x)e_j\rangle$ in those coordinates is precisely the matrix $A^{(ij)}$ defined in (1.6). Hence, (4.1) is equivalent to the spectrahedral representation given in Theorem 1.1. ∎

Remark 4.5. We briefly describe a more geometric dual interpretation of the arguments that establish Theorem 1.1. Throughout this remark, let $S = \{x \in \mathrm{Cl}^0(n) : \langle x, x\rangle = 1\}$ be the unit sphere in $\mathrm{Cl}^0(n)$. We have seen that there is a quadratic map Q such that $SO(n) = Q(\mathrm{Spin}(n)) \subseteq Q(S)$ with the inclusion being strict for $n \geq 4$. The remainder of the proof of Theorem 1.1 shows, from this viewpoint, that $\mathrm{conv}\, SO(n) = \mathrm{conv}\, Q(\mathrm{Spin}(n)) = \mathrm{conv}\, Q(S)$, i.e., all the points in S that are not in $\mathrm{Spin}(n)$ are mapped by Q inside the convex hull of $Q(\mathrm{Spin}(n))$. One may wonder whether $Q(S) = \mathrm{conv}\, SO(n)$, i.e., whether the image of the sphere under Q is actually convex. This is not the case—already for $n = 2$, we can see that $Q(S) = SO(2) \neq \mathrm{conv}\, SO(2)$.

It is now straightforward to prove Theorem 1.2, giving a spectrahedral representation of $O(n)^\circ$ of size 2^n.

THEOREM 1.2. *The polar of $O(n)$ is a spectrahedron. Explicitly,*

$$O(n)^\circ = \left\{ Y \in \mathbb{R}^{n\times n} : \sum_{i,j=1}^{n} A^{(ij)} Y_{ij} \preceq I_{2^{n-1}},\ \sum_{i,j=1}^{n} A^{(ij)} [RY]_{ij} \preceq I_{2^{n-1}} \right\},$$

where $R = \mathrm{diag}^*(1, 1, \ldots, 1, -1)$.

Proof. Since $O(n)^\circ = SO(n)^\circ \cap SO^-(n)^\circ$ (see (1.3)) and we have already constructed a spectrahedral representation of $SO(n)^\circ$, it remains to give a spectrahedral representation of $SO^-(n)^\circ$. Since $SO^-(n) = R \cdot SO(n)$, it follows that $Y \in SO^-(n)^\circ$ if and only if $\langle Y, RX\rangle = \langle RY, X\rangle \leq 1$ for all $X \in SO(n)$. Hence, $Y \in SO^-(n)^\circ$ if and only if $RY \in SO(n)^\circ$.

The stated spectrahedral representation of $O(n)^\circ$ of size 2^n follows from these observations and Theorem 1.1. ∎

4.3. A spectrahedral representation of conv $SO(n)$. In this section, we give a spectrahedral representation of $\mathrm{conv}\, SO(n)$ using a description of $\mathrm{conv}\, SO(n)$ which is inherited from the corresponding description of the parity polytope.

PROPOSITION 4.6. *If $n \geq 3$, the convex hull of $SO(n)$ can be expressed as*

$$\mathrm{conv}\, SO(n) = (\mathrm{conv}\, O(n)) \cap (n-2)SO^-(n)^\circ.$$

If $n = 3$, this simplifies to $\mathrm{conv}\, SO(3) = SO^-(3)^\circ$. *In the case $n = 2$,*

$$\mathrm{conv}\, SO(2) = (\mathrm{conv}\, O(2)) \cap \mathrm{span}\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Proof. Suppose that $X \in \mathbb{R}^{n\times n}$ is arbitrary and $n \geq 3$. By the special singular value decomposition, $X = U\tilde{\Sigma}V^T$, where $(U, V) \in S(O(n) \times O(n))$ and $\tilde{\Sigma} = \mathrm{diag}^*(\tilde{\sigma})$ is diagonal. Then since $SO(n)$ is invariant under the action of $S(O(n) \times O(n))$, it follows that $X \in \operatorname{conv} SO(n)$ if and only if $\tilde{\Sigma} \in (\operatorname{conv} SO(n)) \cap \mathcal{D}$. Similarly, since $\operatorname{conv} O(n)$ and $SO^-(n)^\circ$ are invariant under the action of $S(O(n) \times O(n))$, it follows that $X \in (\operatorname{conv} O(n)) \cap (n-2)SO^-(n)^\circ$ if and only if $\tilde{\Sigma} \in (\operatorname{conv} O(n)) \cap \mathcal{D}$ and $\tilde{\Sigma} \in (n-2)SO^-(n)^\circ \cap \mathcal{D}$.

Since the diagonal section of $\operatorname{conv} SO(n)$ is the parity polytope, $X \in \operatorname{conv} SO(n)$ if and only if $\tilde{\sigma} \in \mathrm{PP}_n$. Since the diagonal section of $\operatorname{conv} O(n)$ is the hypercube, $\tilde{\sigma} \in \mathrm{C}_n$ if and only if $\tilde{\Sigma} \in (\operatorname{conv} O(n)) \cap \mathcal{D}$. Since the diagonal section of $SO^-(n)^\circ$ is $\mathrm{PP}_n^{-\circ}$, $\tilde{\sigma} \in (n-2)\mathrm{PP}_n^{-\circ}$ if and only if $\tilde{\Sigma} \in (n-2)SO^-(n)^\circ \cap \mathcal{D}$.

Finally, we use the fact that $\mathrm{PP}_n = \mathrm{C}_n \cap (n-2)\mathrm{PP}_n^{-\circ}$ (see Lemma 3.1). Then $X \in \operatorname{conv} SO(n)$ if and only if $\tilde{\sigma} \in \mathrm{PP}_n$, which occurs if and only if $\tilde{\sigma} \in \mathrm{C}_n$ and $\tilde{\sigma} \in (n-2)\mathrm{PP}_n^{-\circ}$, which occurs if and only if $X \in (\operatorname{conv} O(n)) \cap (n-2)SO^-(n)^\circ$.

In the case $n = 3$, the description $\mathrm{PP}_n = \mathrm{C}_n \cap (n-2)\mathrm{PP}_n^{-\circ}$ simplifies to $\mathrm{PP}_3 = \mathrm{PP}_3^{-\circ}$. The corresponding simplification propagates through the above argument to give $\operatorname{conv} SO(3) = SO^-(3)^\circ$. The result in the case $n = 2$ follows from the same argument but uses the description $\mathrm{PP}_2 = \mathrm{C}_2 \cap \operatorname{span}(1,1)$ and the fact that $\tilde{\sigma} \in \operatorname{span}(1,1)$ if and only if $X \in \operatorname{span}\left\{\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\right\}$. ∎

Since the description of $\operatorname{conv} SO(n)$ in Proposition 4.6 involves $\operatorname{conv} O(n)$, we first give the well-known spectrahedral representation of $\operatorname{conv} O(n)$.

PROPOSITION 4.7. *The convex hull of $O(n)$ is a spectrahedron. An explicit spectrahedral representation of size $2n$ is given by*

$$\operatorname{conv} O(n) = \left\{ X \in \mathbb{R}^{n \times n} : \begin{bmatrix} 0 & X \\ X^T & 0 \end{bmatrix} \preceq I_{2n} \right\}. \tag{4.2}$$

Proof. Let $Q \in O(n)$ be arbitrary. Then since $Q^T Q = I_n$, it follows that

$$\begin{bmatrix} I_n & -Q \\ -Q^T & I_n \end{bmatrix} = \begin{bmatrix} I_n \\ -Q^T \end{bmatrix} \begin{bmatrix} I_n & -Q \end{bmatrix} \succeq 0,$$

and so Q is an element of the right-hand side of (4.2). Since the right-hand side of (4.2) is convex, it follows that $\operatorname{conv} O(n) \subseteq \left\{ X \in \mathbb{R}^{n\times n} : \left[\begin{smallmatrix} 0 & X \\ X^T & 0 \end{smallmatrix}\right] \preceq I_{2n} \right\}$.

For the reverse inclusion, suppose that X is an element of the right-hand side of (4.2). By the singular value decomposition, there is a diagonal matrix Σ such that $X = U\Sigma V^T$, where $U, V \in O(n)$. Conjugating by the orthogonal matrix $\left[\begin{smallmatrix} U^T & 0 \\ 0 & V^T \end{smallmatrix}\right]$, we see that

$$\begin{bmatrix} 0 & X \\ X^T & 0 \end{bmatrix} \preceq I_{2n} \iff \begin{bmatrix} 0 & \Sigma \\ \Sigma & 0 \end{bmatrix} \preceq I_{2n},$$

which is equivalent to $-1 \le \Sigma_{ii} \le 1$ for $i \in [n]$. Since $\pi_{\mathcal{D}}(\mathcal{D} \cap \operatorname{conv} O(n))$ is the hypercube, it follows that $\Sigma \in \mathcal{D} \cap \operatorname{conv} O(n)$ and so that $U\Sigma V^T \in \operatorname{conv} O(n)$. ∎

We now restate (omitting the explicit description of $\operatorname{conv} SO(3)$) and prove Theorem 1.3.

THEOREM 1.3. *The convex hull of $SO(n)$ is a spectrahedron. Explicitly,*

$$\operatorname{conv} SO(n) = \left\{ X \in \mathbb{R}^{n\times n} : \begin{bmatrix} 0 & X \\ X^T & 0 \end{bmatrix} \preceq I_{2n},\ \sum_{i,j=1}^{n} A^{(ij)}[RX]_{ij} \preceq (n-2) I_{2^{n-1}} \right\}.$$

In the special cases $n = 2$ and $n = 3$, we have

$$\operatorname{conv} SO(2) = \left\{ \begin{bmatrix} c & -s \\ s & c \end{bmatrix} \in \mathbb{R}^{2\times 2} : \begin{bmatrix} 1+c & s \\ s & 1-c \end{bmatrix} \succeq 0 \right\} \quad \textit{and}$$
$$\operatorname{conv} SO(3) = \left\{ X \in \mathbb{R}^{3\times 3} : \sum_{i,j=1}^{3} A^{(ij)}[RX]_{ij} \preceq I_4 \right\}.$$

Proof. Since we now have a spectrahedral representation of $\operatorname{conv} O(n)$ (from (4.2)) and of $SO^-(n)^\circ$ (from the proof of Theorem 1.2), by Proposition 4.6 their intersection gives the spectrahedral representation of $\operatorname{conv} SO(n)$ valid for $n \geq 3$. In the case $n = 3$, Proposition 4.6 tells us that $\operatorname{conv} SO(3) = SO^-(3)^\circ$, giving the stated simplification (which can be expressed explicitly as in (1.11) by using the definition of the $A^{(ij)}$ in (1.6)). In the case $n = 2$, from Proposition 4.6 we have that

$$\operatorname{conv} SO(2) = \left\{ \begin{bmatrix} c & -s \\ s & c \end{bmatrix} \in \mathbb{R}^{2\times 2} : \begin{bmatrix} 1 & 0 & -c & s \\ 0 & 1 & -s & -c \\ -c & -s & 1 & 0 \\ s & -c & 0 & 1 \end{bmatrix} \succeq 0 \right\}.$$

This is still a spectrahedral representation of size 4, but the constraint has symmetry—it is invariant under simultaneously reversing the order of the rows and columns—suggesting that it can be block diagonalized [13]. Under the change of coordinates

$$\frac{1}{2}\begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & -c & s \\ 0 & 1 & -s & -c \\ -c & -s & 1 & 0 \\ s & -c & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & -1 & 0 \end{bmatrix}^T$$
$$= \begin{bmatrix} 1+c & s & 0 & 0 \\ s & 1-c & 0 & 0 \\ 0 & 0 & 1+c & s \\ 0 & 0 & s & 1-c \end{bmatrix}, \tag{4.3}$$

we see that the size 4 spectrahedral representation in (4.3) is actually two copies of the same size 2 representation, giving the stated result. ∎

5. Lower bounds on the size of representations.

5.1. Spectrahedral representations. Whenever a convex set has a polyhedral section, we can immediately obtain a simple lower bound on the possible size of a spectrahedral representation of that convex set in terms of the number of facets of that polyhedron. The bound is based on the following result of Ramana [29, Corollary 2.5].

LEMMA 5.1. *If $P \subseteq \mathbb{R}^p$ is a polyhedron with f facets and P has a spectrahedral representation of size m, then $m \geq f$.*

The following combines Ramana's result with the simple fact that restricting a spectrahedral representation of C to an affine subspace U gives a spectrahedral representation of $C \cap U$ of the same size.

LEMMA 5.2. *Suppose that $C \subseteq \mathbb{R}^n$ has a spectrahedral representation of size m. If $U \subseteq \mathbb{R}^n$ is an affine subspace and $C \cap U$ is a polyhedron with f facets, then $m \geq f$.*

Proof. Parameterize the subspace U as $U = \{Ax + b : x \in \mathbb{R}^p\}$, where $A \in \mathbb{R}^{n\times p}$ and $b \in \mathbb{R}^n$. Let C have a spectrahedral representation $C = \{x : \sum_{i=1}^n A^{(i)}x_i + A^{(0)} \succeq$

$0\}$ of size m, so the symmetric matrices $A^{(i)}$ are $m \times m$. Let $B^{(j)} = \sum_{i=1}^{n} A^{(i)} A_{ij}$ for $j = 1, 2, \ldots, p$ and let $B^{(0)} = A^{(0)} + \sum_{i=1}^{n} A^{(i)} b_i$. Then $C \cap U$ is affinely isomorphic to $\{x \in \mathbb{R}^p : \sum_{j=1}^{p} B^{(j)} x_j + B^{(0)} \succeq 0\}$, which has a spectrahedral representation of size m. Since $C \cap U$ has f facets, it follows from Ramana's result (Lemma 5.1) that $m \geq f$. □

Remarkably, this simple observation allows us to establish that our spectrahedral representations are of minimum size.

THEOREM 1.4. *If $n \geq 1$, the minimum size of a spectrahedral representation of $O(n)^\circ$ is 2^n. If $n \geq 2$, the minimum size of a spectrahedral representation of $SO(n)^\circ$ is 2^{n-1}. If $n \geq 4$, the minimum size of a spectrahedral representation of* $\operatorname{conv} SO(n)$ *is $2^{n-1} + 2n$. The minimum size of a spectrahedral representation of* $\operatorname{conv} SO(3)$ *is* 4.

Proof. The diagonal slice of $O(n)^\circ$ is the cross-polytope, which (for $n \geq 1$) has 2^n facets. Hence, for $n \geq 1$, any spectrahedral representation of $O(n)^\circ$ has size at least 2^n. The diagonal slice of $SO(n)^\circ$ is the polar of the parity polytope, which (for $n \geq 2$) has 2^{n-1} facets. Hence, for $n \geq 2$, any spectrahedral representation of $SO(n)^\circ$ has size at least 2^{n-1}. The diagonal slice of $\operatorname{conv} SO(n)$ is the parity polytope, which for $n \geq 4$ has $2^{n-1} + 2n$ facets, and for $n = 3$ has 4 facets. It follows that any spectrahedral representation of $\operatorname{conv} SO(n)$ has size at least $2^{n-1} + 2n$ for $n \geq 4$ and size at least 4 for $n = 3$. □

The spectrahedral representations we construct in section 4 achieve these lower bounds and so are of minimum size.

5.2. Equivariant PSD lifts. As is established in Theorem 1.4, our spectrahedral representations are necessarily of exponential size. While they are useful in practice for very small n (such as the physically relevant $n = 3$ case), this is not the case for larger n.

PSD lifts. In general, if C is a spectrahedron, it may be possible to give a much smaller *projected spectrahedral* representation of C. In other words, it may be the case that $C = \pi(D)$, where π is a linear map[3] and D has a spectrahedral representation that has a much smaller size than any spectrahedral representation of C. Note that throughout this section, if D has a spectrahedral representation of size m, we express it as $D = L \cap \mathcal{S}_+^m$, where L is an affine subspace of $\mathcal{S}^m$, the space of $m \times m$ symmetric matrices, and $\mathcal{S}_+^m \subseteq \mathcal{S}^m$ is the cone of positive semidefinite $m \times m$ symmetric matrices. The following definition is a specialization of [15, Definition 1].

DEFINITION 5.2. *Suppose that $C \subseteq \mathbb{R}^n$ is a convex body. If $C = \pi(L \cap \mathcal{S}_+^m)$ where L is an affine subspace of $m \times m$ symmetric matrices and $\pi : \mathcal{S}^m \to \mathbb{R}^n$ is a linear map, we say that C has a* PSD lift *of size m.*

It is straightforward to show that if C has a PSD lift of size m, then C° also has a PSD lift of size m [15]. This simple observation already yields examples of convex bodies for which there is an exponential gap between the size of the smallest spectrahedral representation and the size of the smallest PSD lift. For instance, as demonstrated in Example 1.5, the smallest possible spectrahedral representation of $O(n)^\circ$ has size 2^n and yet it has a PSD lift of size $2n$.

Equivariant PSD lifts. While there has been some recent progress in obtaining lower bounds on the size of PSD lifts of some polytopes [5, 16], little is understood about lower bounds on the size of PSD lifts of convex bodies in general. Recently, new techniques have been developed for obtaining lower bounds on the size of *equivariant*

[3]In this section only, to conform with standard notation for PSD lifts, we use π to mean an arbitrary linear map

PSD lifts of orbitopes. These are PSD lifts that "respect" (in a precise sense to be defined below) the symmetries of that orbitope.

In the remainder of this section, we show that any projected spectrahedral representation of $\operatorname{conv} SO(n)$ that is equivariant with respect to the action of $S(O(n) \times O(n))$ must have size exponential in n. The argument works by showing that from any PSD lift of $\operatorname{conv} SO(n)$ that is equivariant with respect to the action of $S(O(n) \times O(n))$, we can construct a PSD lift of the parity polytope that is equivariant with respect to a certain group action on $\mathbb{R}^n$. We then apply a recent result that gives an exponential lower bound on the size of appropriately equivariant PSD lifts of the parity polytope.

The following definition (from [10]) makes the notion of equivariant PSD lift precise.

DEFINITION 5.3. *Let $C \subseteq \mathbb{R}^n$ be a convex body invariant under the action of a group G by linear transformations. Assume that $C = \pi(L \cap \mathcal{S}_+^m)$ is a PSD lift of C of size m. The lift is called G-*equivariant *if there is a group homomorphism $\rho : G \to GL(m)$ such that*

$$\begin{aligned} &\rho(g) X \rho(g)^T \in L \qquad \text{for all } g \in G \text{ and all } X \in L \qquad \text{and} \\ &\pi(\rho(g) X \rho(g)^T) = g \cdot \pi(X) \quad \text{for all } g \in G \text{ and all } X \in L \cap \mathcal{S}_+^m. \end{aligned} \tag{5.1}$$

In the present setting we are interested in two particular cases of equivariant PSD lifts: $S(O(n) \times O(n))$-equivariant PSD lifts of $\operatorname{conv} SO(n)$ and Γ_{parity}-equivariant PSD lifts of the parity polytope. Here, Γ_{parity} can be thought of concretely as the group of evenly signed permutation matrices—signed permutation matrices where there are an even number of entries that take the value -1. These act on $\mathbb{R}^n$ by matrix multiplication.

We are now in a position to relate $S(O(n) \times O(n))$-equivariant PSD lifts of $\operatorname{conv} SO(n)$ with Γ_{parity}-equivariant PSD lifts of PP_n.

PROPOSITION 5.4. *If $\operatorname{conv} SO(n)$ has an equivariant PSD lift of size m, then PP_n has an equivariant PSD lift of size m.*

Proof. Suppose $\operatorname{conv} SO(n) = \pi(L \cap \mathcal{S}_+^m)$ is a $S(O(n) \times O(n))$-equivariant PSD lift of $\operatorname{conv} SO(n)$ of size m and let $\rho : S(O(n) \times O(n)) \to GL(m)$ be the associated homomorphism. Since the projection of $\operatorname{conv} SO(n)$ onto the subspace of diagonal matrices is PP_n (Theorem 3.3), it follows that

$$\text{PP}_n = (\pi_{\mathcal{D}} \circ \pi)(L \cap \mathcal{S}_+^m)$$

is a PSD lift of PP_n of size m. It remains to show that this lift of PP_n is Γ_{parity}-equivariant. In other words, we need to construct a homomorphism $\tilde{\rho} : \Gamma_{\text{parity}} \to GL(m)$ satisfying the requirements of Definition 5.3.

First, observe that any element of Γ_{parity} can be uniquely expressed as DP, where D is a diagonal sign matrix with determinant one, and P is a permutation matrix. Furthermore, note that if D_1P_1 and D_2P_2 are elements of Γ_{parity}, then

$$(D_1P_1)(D_2P_2) = (D_1P_1D_2P_1^T)(P_1P_2)$$

gives the associated factorization of the product. Hence, define $\phi : \Gamma_{\text{parity}} \to S(O(n) \times O(n))$ by $\phi(DP) = (DP, P)$. Observe that this is a homomorphism because

$$\begin{aligned} \phi((D_1P_1)(D_2P_2)) &= \phi((D_1P_1D_2P_1^T)(P_1P_2)) \\ &= ((D_1P_1)(D_2P_2), P_1P_2) = \phi(D_1P_1) \cdot \phi(D_2P_2). \end{aligned}$$

Define a homomorphism $\tilde{\rho} : \Gamma_{\text{parity}} \to GL(m)$ by $\tilde{\rho} = \rho \circ \phi$. For any symmetric matrix X, it is the case that $DP \cdot \pi_{\mathcal{D}}(X) = \pi_{\mathcal{D}}(DPXP^T)$. Hence, the following establishes that the lift is Γ_{parity}-equivariant:

$$\begin{aligned} DP \cdot \pi_{\mathcal{D}}(\pi(X)) &= \pi_{\mathcal{D}}(DP\pi(X)P^T) \\ &= \pi_{\mathcal{D}}(\phi(DP) \cdot \pi(X)) \\ &\overset{*}{=} \pi_{\mathcal{D}}(\pi(\rho(\phi(DP))X\rho(\phi(DP))^T)) \\ &= \pi_{\mathcal{D}}(\pi(\tilde{\rho}(DP)X\tilde{\rho}(DP)^T)) \quad \text{by the definition of } \tilde{\rho}, \end{aligned}$$

where the equality marked with an asterisk holds because the lift of $\operatorname{conv} SO(n)$ is equivariant. □

The following lower bound on the size of Γ_{parity}-equivariant PSD lifts of the parity polytope is one of the main results of [10].

THEOREM 5.5. *Any* Γ_{parity}*-equivariant PSD lift of* PP_n *for* $n \geq 8$ *must have size at least* $\binom{n}{\lceil \frac{n}{4} \rceil}$.

Combining Proposition 5.4 with Proposition 5.5, we obtain the following exponential lower bound on the size of any equivariant PSD lift of $\operatorname{conv} SO(n)$.

COROLLARY 5.6. *Any* $S(O(n) \times O(n))$*-equivariant PSD lift of* $\operatorname{conv} SO(n)$ *for* $n \geq 8$ *must have size at least* $\binom{n}{\lceil \frac{n}{4} \rceil}$.

6. Summary and open questions. In this work, we have constructed minimum size spectrahedral representations for the convex hull of $SO(n)$ and its polar. We have also constructed a minimum-size spectrahedral representation of $O(n)^\circ$ (the nuclear norm ball). We conclude the paper by discussing some natural questions raised by our results.

6.1. Doubly spectrahedral convex sets. We have seen that both the convex hull of $SO(n)$ and its polar are spectrahedra. The same is true of the convex hull of $O(n)$ (the operator norm ball) and its polar (the nuclear norm ball), as established by Sanyal, Sottile, and Sturmfels [32, Corollary 4.9]. This is a very special phenomenon—the polar of a spectrahedron is not, in general, a spectrahedron. For example, the intersection of the second-order cone $\{(x, y, z) : z \geq \sqrt{x^2 + y^2}\}$ and the nonnegative orthant is a spectrahedron, but its polar has nonexposed faces and so is not a spectrahedron [28].

If a convex set C and its polar are both spectrahedra, we say that C is a *doubly spectrahedral* convex set. Apart from $\operatorname{conv} O(n)$ and $\operatorname{conv} SO(n)$, two distinct families of doubly spectrahedral convex sets are the following:

Polyhedra. Every polyhedron is a spectrahedron, and the polar of a polyhedron is again a polyhedron. Hence, polyhedra are doubly spectrahedral.

Homogeneous cones. A convex cone K is *homogeneous* if the automorphism group of K acts transitively on the interior of K. Using Vinberg's classification of homogeneous cones in terms of T-algebras [37], Chua gave spectrahedral representations for all homogeneous cones [7]. Furthermore, K is homogeneous if and only its dual cone $K^* = -K^\circ$ is homogeneous [37, Proposition 9]. From these two observations, it follows that any homogeneous cone is doubly spectrahedral.

We have seen that the doubly spectrahedral convex sets are a strict subset of all spectrahedra that includes all polyhedra, all homogeneous convex cones, and $\operatorname{conv} O(n)$ and $\operatorname{conv} SO(n)$.

PROBLEM 6.1. *Characterize doubly spectrahedral convex sets.*

6.2. Non-equivariant PSD lifts. In section 5, we showed that our spectrahedral representations of $\operatorname{conv} SO(n)$ and $SO(n)^\circ$ are necessarily of exponential size and that any $S(O(n) \times O(n))$-equivariant PSD lift of $\operatorname{conv} SO(n)$ must also have exponential size. Our lower bound on the size of $S(O(n) \times O(n))$-equivariant PSD lifts of $\operatorname{conv} SO(n)$ used the fact that any Γ_{parity}-lift of the parity polytope has exponential size. Nevertheless, the parity polytope is known to have a PSD lift (in fact, it is an LP lift) of size $4(n-1)$ [6, section 2.6.3] that is *not* Γ_{parity}-equivariant. It is quite possible that by appropriately breaking symmetry, we can find a small PSD lift of $\operatorname{conv} SO(n)$.

QUESTION 6.2. *Does* $\operatorname{conv} SO(n)$ *have a PSD lift with size polynomial in* n*?*

Appendix A. Clifford algebras and Spin(n). In this section, we describe and establish the key properties of the quadratic mapping Q from Proposition 4.1 that underlies our spectrahedral representation of $SO(n)^\circ$ given in Theorem 1.1. The mapping Q is most naturally described in terms of an algebraic structure known as a Clifford algebra, which generalizes some properties of complex numbers and quaternions. The first part of this section is devoted to describing the basic properties of Clifford algebras we require. In section A.2, we define the set Spin(n) and establish some of its properties. In section A.3, we describe the mapping Q and establish Propositions 4.1, 4.2, and 4.3. Section A.4 gives explicit constructions of the matrices $A^{(ij)}$ appearing in our spectrahedral representations.

Many of the constructions and properties we describe here are standard and can be found, for example, in [1, 17]. We highlight those aspects of the development that are novel as they arise.

A.1. Clifford algebras. The Clifford algebra Cl(n) is the associative algebra[4] (over the reals) with generators $e_1, e_2, \ldots, e_n$ and relations

$$e_i^2 = -\mathbf{1} \quad \text{and} \quad e_i e_j = -e_j e_i \quad \text{for } i \neq j. \tag{A.1}$$

Here, $\mathbf{1}$ denotes the multiplicative identity in the algebra.

Standard basis. When thought of as a real vector space, Cl(n) has dimension 2^n. A basis for Cl(n) is given by all elements of the form

$$e_I := e_{i_1} e_{i_2} \cdots e_{i_k},$$

where $I = \{i_1, i_2, \ldots, i_k\}$ is a subset of $[n]$ and $i_1 < i_2 < \cdots < i_k$. Note that $e_\emptyset := \mathbf{1}$. Let us call $(e_I)_{I \subseteq [n]}$ the *standard basis* for Cl(n). With respect to this basis we can think of an arbitrary element $x \in \mathrm{Cl}(n)$ as

$$x = \sum_{I \subseteq [n]} x_I e_I$$

where the $x_I \in \mathbb{R}$. We equip Cl(n) with the inner product $\langle x, y \rangle = \sum_{I \subseteq [n]} x_I y_I$. Clearly, the standard basis is orthonormal with respect to this inner product.

Left and right multiplication. Any element $x \in \mathrm{Cl}(n)$ acts linearly on Cl(n) by left multiplication and by right multiplication. In other words, given $x \in \mathrm{Cl}(n)$, there are linear maps $\lambda_x, \rho_x : \mathrm{Cl}(n) \to \mathrm{Cl}(n)$ defined by $\lambda_x(y) = xy$ and $\rho_x(y) = yx$ for all $y \in \mathrm{Cl}(n)$.

[4]That such an algebra exists and is unique up to isomorphism follows because it can be realized as a quotient of the tensor algebra (see, e.g., [17, Definition 9.4]).

Conjugation. A straightforward computation shows that with respect to the inner product on $\mathrm{Cl}(n)$, the adjoint of left multiplication by e_i is left multiplication by $-e_i$, i.e., $\lambda_{e_i}^* = \lambda_{-e_i}$. Similarly, the adjoint of right multiplication by e_i is right multiplication by $-e_i$. In fact, it is the case that for any $x \in \mathrm{Cl}(n)$, there is $\overline{x} \in \mathrm{Cl}(n)$ such that $\lambda_x^* = \lambda_{\overline{x}}$ and $\rho_x^* = \rho_{\overline{x}}$. To see this, define a *conjugation* map $x \mapsto \overline{x}$ on the standard basis by

$$\overline{e_I} = (-1)^{|I|} e_{i_k} \cdots e_{i_2} e_{i_1}$$

and extend by linearity. We use this conjugation map repeatedly in what follows, usually via the relations

$$\langle xy, z\rangle = \langle \lambda_x y, z\rangle = \langle y, \lambda_x^* z\rangle = \langle y, \lambda_{\overline{x}} z\rangle = \langle y, \overline{x} z\rangle \tag{A.2}$$

and

$$\langle yx, z\rangle = \langle \rho_x y, z\rangle = \langle y, \rho_x^* z\rangle = \langle y, \rho_{\overline{x}} z\rangle = \langle y, z\overline{x}\rangle. \tag{A.3}$$

Copy of $\mathbb{R}^n$ *in* $\mathrm{Cl}(n)$. Throughout this appendix, we use the notation $\mathbb{R}^n$ to denote the n-dimensional subspace of $\mathrm{Cl}(n)$ spanned by the generators $e_1, e_2, \ldots, e_n$. Elements of $\mathbb{R}^n \subseteq \mathrm{Cl}(n)$ satisfy the following coordinate-free version of the defining relations of $\mathrm{Cl}(n)$ given in (A.1).

LEMMA A.1. *If* $u, v \in \mathbb{R}^n$*, then* $uv + vu = -2\langle u, v\rangle\, \mathbf{1}$.

Proof. First, note that $uv + uv = -2\langle u, v\rangle\, \mathbf{1}$ is bilinear in u and v, so it suffices to verify the identity for $u = e_i$ and $v = e_j$ (for all $1 \leq i, j \leq n$). That the statement holds for $u = e_i$ and $v = e_j$ (for all $1 \leq i, j \leq n$) is equivalent to the relations (A.1) (since $\langle e_i, e_j\rangle = \delta_{ij}$). ∎

The sphere in $\mathbb{R}^n$. We use the notation $S^{n-1} \subseteq \mathbb{R}^n \subseteq \mathrm{Cl}(n)$ to denote the set of elements $x \in \mathbb{R}^n$ satisfying $\langle x, x\rangle = 1$. We next state and prove some basic properties of the elements of $S^{n-1} \subseteq \mathrm{Cl}(n)$.

LEMMA A.2. *If* $u \in S^{n-1} \subseteq \mathrm{Cl}(n)$*, then* $u\overline{u} = \mathbf{1} = \overline{u}u$*. Consequently,* $\langle uy, uz\rangle = \langle y, z\rangle = \langle yu, zu\rangle$ *for all* $y, z \in \mathrm{Cl}(n)$.

Proof. The second statement follows from the first together with (A.2) and (A.3). That $u\overline{u} = \mathbf{1}$ whenever $u \in S^{n-1}$ follows from a direct application of Lemma A.1. ∎

The following can be established by repeatedly applying Lemma A.2.

COROLLARY A.3. *If* $u_1, u_2, \ldots, u_k \in S^{n-1}$*, then* $\langle u_1 u_2 \cdots u_k, u_1 u_2 \cdots u_k\rangle = 1$.

Even subalgebra. Consider the subspaces $\mathrm{Cl}^0(n)$ and $\mathrm{Cl}^1(n)$ of $\mathrm{Cl}(n)$ defined by

$$\mathrm{Cl}^0(n) = \mathrm{span}\{e_I : I \subseteq [n],\ |I| \text{ even}\} \quad \text{and} \quad \mathrm{Cl}^1(n) = \mathrm{span}\{e_I : I \subseteq [n],\ |I| \text{ odd}\}.$$

It is straightforward to show that if $x, y \in \mathrm{Cl}^0(n)$, then $xy \in \mathrm{Cl}^0(n)$, and if $x, y \in \mathrm{Cl}^1(n)$, then $xy \in \mathrm{Cl}^0(n)$. The first of these properties, states that $\mathrm{Cl}^0(n)$ is a subalgebra of $\mathrm{Cl}(n)$, which we call the *even subalgebra*. With these properties, we have that the product of an even number of elements of S^{n-1} is in the even subalgebra.

LEMMA A.4. *If* $u_1, u_2, \ldots, u_{2k} \in S^{n-1}$*, then* $x = u_1 u_2 \cdots u_{2k} \in \mathrm{Cl}^0(n)$.

Proof. Since $S^{n-1} \subseteq \mathbb{R}^n \subseteq \mathrm{Cl}^1(n)$, each $u_i \in \mathrm{Cl}^1(n)$. Hence, $u_{2i-1}u_{2i} \in \mathrm{Cl}^0(n)$ for $i = 1, 2, \ldots, k$. So $u_1 u_2 \cdots u_{2k} = (u_1 u_2)(u_3 u_4) \cdots (u_{2k-1} u_{2k})$ is the product of elements in $\mathrm{Cl}^0(n)$, and so is itself an element of $\mathrm{Cl}^0(n)$. ∎

A.2. Spin(n). We now define Spin(n) and establish some of its basic properties.

DEFINITION A.5. *Spin(n) is the set of all even length products of elements of S^{n-1}, i.e.,*

$$\mathrm{Spin}(n) = \{x \in \mathrm{Cl}(n) : x = u_1 u_2 \cdots u_{2k}, \text{ where } k \text{ is a positive integer and } u_1, \ldots, u_{2k} \in S^{n-1}\}.$$

Although we do not require this fact, it can be shown that in the above definition it is enough to take $k = \lfloor n/2 \rfloor$. We note that a common alternative definition [1] is to take Spin(n) to be the elements of $\mathrm{Cl}^0(n)$ satisfying $x\overline{x} = \mathbf{1}$ and $xv\overline{x} \in \mathbb{R}^n$ for every $v \in \mathbb{R}^n$ (which defines a real algebraic variety specified by the vanishing of a collection of quadratic equations). It is fairly straightforward to establish that these two definitions are equivalent.

The following observation follows directly from Lemma A.4 and Corollary A.3.

LEMMA A.6. *The set Spin(n) is a subset of the unit sphere in $\mathrm{Cl}^0(n)$, i.e., $\mathrm{Spin}(n) \subseteq \{x \in \mathrm{Cl}^0(n) : \langle x, x\rangle = 1\}$.*

The next result establishes that Spin(n) is a group under multiplication.

LEMMA A.7. *If $x \in \mathrm{Spin}(n)$, then $\overline{x}x = x\overline{x} = \mathbf{1}$. If $x, y \in \mathrm{Spin}(n)$, then $xy \in \mathrm{Spin}(n)$.*

Proof. That Spin(n) is closed under multiplication is clear from the definition. That conjugation and inversion coincide on Spin(n) follows from Lemma A.2. ∎

A.3. The quadratic mapping. We now define and establish the relevant properties of the quadratic mapping $Q : \mathrm{Cl}^0(n) \to \mathbb{R}^{n\times n}$ that plays a prominent role in section 4.2. First, define $\widetilde{Q} : \mathrm{Cl}(n) \to \mathbb{R}^{n\times n}$ by

$$\widetilde{Q}(x)(u) = \pi_{\mathbb{R}^n}\lambda_x\rho_{\overline{x}}(u) = \pi_{\mathbb{R}^n}(xu\overline{x}).$$

Note that $\widetilde{Q}(x)$ is quadratic in x. Then define $Q : \mathrm{Cl}^0(n) \to \mathbb{R}^{n\times n}$ as the restriction of $\widetilde{Q}$ to the subalgebra $\mathrm{Cl}^0(n)$.

When we express the linear map $\widetilde{Q}(x)$ as a matrix (with respect to the standard basis), we see that $[\widetilde{Q}(x)]_{ij} = \langle e_i, xe_j\overline{x}\rangle$. Furthermore, $\widetilde{Q}$ (and hence Q) interacts nicely with the conjugation map.

LEMMA A.8. *If $x \in \mathrm{Cl}(n)$, then $\widetilde{Q}(\overline{x}) = \widetilde{Q}(x)^T$.*

Proof. Simply observe that $[\widetilde{Q}(x)]_{ij} = \langle e_i, xe_j\overline{x}\rangle = \langle \overline{x}e_i x, e_j\rangle = [\widetilde{Q}(\overline{x})]_{ji}$. ∎

The definition of $\widetilde{Q}$ is motivated by the fact that if $u \in S^{n-1}$, then $-\widetilde{Q}(u)$ is the reflection in the hyperplane orthogonal to u.

LEMMA A.9. *Let $u \in S^{n-1}$. Then whenever $v \in \mathbb{R}^n$, $-uv\overline{u} \in \mathbb{R}^n$ is the reflection of v in the hyperplane normal to u. In particular, $-uv\overline{u} \in \mathbb{R}^n$.*

Proof. Let $u \in S^{n-1}$. Then by Lemma A.1, if $v \in \mathbb{R}^n$, then $-uv = 2\langle u, v\rangle\mathbf{1} + vu$. Since $u\overline{u} = \mathbf{1}$ and $\overline{u} = -u$, it follows that

$$-uv\overline{u} = 2\langle u, v\rangle\overline{u} + vu\overline{u} = v - 2\langle u, v\rangle u,$$

which is the reflection in the hyperplane orthogonal to u and is certainly in $\mathbb{R}^n$. ∎

Note that our definition of $\widetilde{Q}$ is one possible extension to all of Cl(n) of the map that sends $u \in S^{n-1}$ to the reflection in the hyperplane orthogonal to u. It is specifically chosen so as to be quadratic on all of Cl(n). Our choice is different from the typical extension used in the literature—the *twisted adjoint representation* [1]—which is *not* quadratic in x on all of Cl(n) and is not suitable for our purposes.

LEMMA A.10. *Let $x \in \mathrm{Cl}(n)$ and $u \in S^{n-1}$. Then*

$$\widetilde{Q}(xu) = \widetilde{Q}(x)\widetilde{Q}(u) \quad \text{and} \quad \widetilde{Q}(ux) = \widetilde{Q}(u)\widetilde{Q}(x),$$

where the product on the right-hand side in each case is composition of linear maps.

Proof. If $u \in S^{n-1}$, we know from the previous lemma that $v \mapsto uv\overline{u}$ leaves the subspace $\mathbb{R}^n$ (and hence its orthogonal complement) invariant. So by the definition of $\widetilde{Q}$, we see that

$$\widetilde{Q}(xu)(v) = \pi_{\mathbb{R}^n}(xuv\overline{u}\,\overline{x}) = \pi_{\mathbb{R}^n}(x\pi_{\mathbb{R}^n}^*\pi_{\mathbb{R}^n}(uv\overline{u})\overline{x}) = \widetilde{Q}(x)(\widetilde{Q}(u)(v)).$$

Similarly, since $\pi_{\mathbb{R}^n}^*\pi_{\mathbb{R}^n} + \pi_{\mathbb{R}^{n\perp}}^*\pi_{\mathbb{R}^{n\perp}} = I$,

$$\begin{aligned}\widetilde{Q}(ux)(v) &= \pi_{\mathbb{R}^n}(uxv\overline{x}\,\overline{u})\\ &= \pi_{\mathbb{R}^n}(u\pi_{\mathbb{R}^n}^*\pi_{\mathbb{R}^n}(xv\overline{x})\overline{u}) + \pi_{\mathbb{R}^n}(u\pi_{\mathbb{R}^{n\perp}}^*\pi_{\mathbb{R}^{n\perp}}(xv\overline{x})\overline{u}) = Q(u)(Q(x)(v)) + 0,\end{aligned}$$

where we have used the fact that $uy\overline{u} \in \mathbb{R}^{n\perp}$ whenever $y \in \mathbb{R}^{n\perp}$. ∎

We are now in a position to prove Propositions 4.1, 4.2, and 4.3. We restate them here for convenience.

PROPOSITION 4.1. *There is a 2^{n-1}-dimensional inner product space,* $\mathrm{Cl}^0(n)$*, a subset* $\mathrm{Spin}(n)$ *of the unit sphere in* $\mathrm{Cl}^0(n)$ *and a quadratic map* $Q : \mathrm{Cl}^0(n) \to \mathbb{R}^{n\times n}$ *such that* $Q(\mathrm{Spin}(n)) = SO(n)$.

Proof. The construction of $\mathrm{Cl}^0(n)$ is given in section A.1. The set $\mathrm{Spin}(n)$ is defined in A.5. That $\mathrm{Spin}(n)$ is a subset of the sphere in $\mathrm{Cl}^0(n)$ is the content of Lemma A.6. The quadratic mapping Q is defined in section A.3. It remains to show that $Q(\mathrm{Spin}(n)) = SO(n)$.

Let $X \in SO(n)$. By the Cartan–Dieudonné theorem [12], any such X can be expressed as the composition of an even number (at most n) of reflections in hyperplanes with normal vectors, say, $u_1, u_2, \ldots, u_{2k} \in S^{n-1}$. Let $x = u_1u_2\cdots u_{2k-1}u_{2k} \in \mathrm{Spin}(n)$. Then by Lemmas A.9 and A.10 and the fact that Q is the restriction of $\widetilde{Q}$ to $\mathrm{Cl}^0(n)$,

$$X = \widetilde{Q}(u_1)\widetilde{Q}(u_2)\cdots\widetilde{Q}(u_{2k-1})\widetilde{Q}(u_{2k}) = \widetilde{Q}(x) = Q(x) \in Q(\mathrm{Spin}(n)).$$

Hence, $SO(n) \subseteq Q(\mathrm{Spin}(n))$. On the other hand, if $x = u_1u_2\cdots u_{2k-1}u_{2k} \in \mathrm{Spin}(n)$, then $Q(x)$ is the product of an even number of reflections in hyperplanes and so is an element of $SO(n)$, establishing the reverse inclusion. ∎

PROPOSITION 4.2. *If $U, V \in SO(n)$, then there is a corresponding invertible linear map $\Phi_{(U,V)} : \mathrm{Cl}^0(n) \to \mathrm{Cl}^0(n)$ such that for any $x \in \mathrm{Cl}^0(n)$, $UQ(x)V^T = Q(\Phi_{(U,V)}x)$ and $\Phi_{(U,V)}(\mathrm{Spin}(n)) = \mathrm{Spin}(n)$.*

Proof. By Proposition 4.1, there are $u, v \in \mathrm{Spin}(n)$ such that $Q(u) = U$ and $Q(v) = V$. Define $\Phi_{(U,V)} : \mathrm{Cl}^0(n) \to \mathrm{Cl}^0(n)$ by $\Phi_{(U,V)}(x) = ux\overline{v}$. Then $\Phi_{(U,V)}$ is invertible with inverse $\Phi_{(U,V)}^{-1}(x) = \overline{u}xv$. By Lemmas A.8 and A.10, for any $x \in \mathrm{Cl}^0(n)$,

$$UQ(x)V^T = Q(u)Q(x)Q(v)^T = Q(u)Q(x)Q(\overline{v}) = Q(ux\overline{v}).$$

Finally, if $x \in \mathrm{Spin}(n)$, then $\Phi_{(U,V)}(x) = ux\overline{v} \in \mathrm{Spin}(n)$ by Lemma A.7. Hence, $\Phi_{(U,V)}(\mathrm{Spin}(n)) \subseteq \mathrm{Spin}(n)$. For the reverse inclusion, if $x \in \mathrm{Spin}(n)$, then $\Phi_{(U,V)}^{-1}(x) = \overline{u}xv \in \mathrm{Spin}(n)$ by Lemma A.7. Hence, $\Phi_{(U,V)}(\mathrm{Spin}(n)) \supseteq \mathrm{Spin}(n)$, establishing that $\Phi_{(U,V)}(\mathrm{Spin}(n)) = \mathrm{Spin}(n)$. ∎

PROPOSITION 4.3. *Given any orthonormal basis $u_1, \ldots, u_n$ for $\mathbb{R}^n$, there is a corresponding orthonormal basis $(u_I)_{I\in\mathcal{I}_{even}}$ for $\mathrm{Cl}^0(n)$ such that*

- $u_I \in \mathrm{Spin}(n)$ *for all* $I \in \mathcal{I}_{even}$ *and*
- *for all* $i \in [n]$, *if* $x = \sum_{I\in\mathcal{I}_{even}} x_I u_I$, *then*

$$\langle u_i, Q(x)u_i\rangle = \sum_{I\in\mathcal{I}_{even}} x_I^2 \langle u_i, Q(u_I)u_i\rangle.$$

Proof. Let $u_1, u_2, \ldots, u_n \in \mathbb{R}^n$ be orthonormal with respect to the usual inner product on $\mathbb{R}^n$. When thought of as elements of $\mathbb{R}^n \subset \mathrm{Cl}(n)$, these satisfy $u_i^2 = -\mathbf{1}$ for all i and $u_iu_j = -u_ju_i$ when $i \neq j$ (by Lemma A.1). As such, we can construct from $u_1, u_2, \ldots, u_n$ a basis for $\mathrm{Cl}^0(n)$ just as we did for the standard basis. Indeed, let $I = \{i_1, \ldots, i_{2k}\} \subseteq [n]$, where $i_1 < i_2 < \cdots < i_{2k}$, and define $u_I = u_{i_1}u_{i_2}\cdots u_{i_{2k}}$. This realizes u_I as the product of an even number of elements of S^{n-1}, showing that $u_I \in \mathrm{Spin}(n)$. For the second statement, note that if $x = \sum_{I\in\mathcal{I}_{\mathrm{even}}} x_I u_I$ and $i \in [n]$,

$$\begin{aligned}
\langle u_i, Q(x)u_i\rangle &= \langle u_i, x u_i \overline{x}\rangle \\
&= \sum_{I,J\in\mathcal{I}_{\mathrm{even}}} x_I x_J \langle u_i, u_I u_i \overline{u_J}\rangle \\
&\overset{*}{=} \sum_{I,J\in\mathcal{I}_{\mathrm{even}}} x_I x_J \delta_{IJ} \langle u_i, u_I u_i \overline{u_I}\rangle \\
&= \sum_{I\in\mathcal{I}_{\mathrm{even}}} x_I^2 \langle u_i, Q(u_I)u_i\rangle
\end{aligned}$$

where $\delta_{IJ} = 1$ if $I = J$ and zero otherwise, and the equality marked with an asterisk follows directly from the coordinate-free version of the defining relations of the Clifford algebra (Lemma A.1). ∎

A.4. Matrices of the quadratic mapping. For $1 \leq i, j \leq n$, let $A^{(ij)} : \mathrm{Cl}^0(n) \to \mathrm{Cl}^0(n)$ be the self-adjoint linear map such that, for all $x \in \mathrm{Cl}^0(n)$,

$$[Q(x)]_{ij} = \langle e_i, x e_j \overline{x}\rangle = \langle x, A^{(ij)}x\rangle.$$

First, we note that the $A^{(ij)}$ have trace zero.

LEMMA A.11. *For* $1 \leq i, j \leq n$, $\mathrm{tr}(A^{(ij)}) = 0$.

Proof. For $i \in [n]$ and $I \in \mathcal{I}_{\mathrm{even}}$, define $\delta_{[i\in I]} = 1$ if $i \in I$ and 0 otherwise. Observe that from the definition of $A^{(ij)}$ and the defining relations of the Clifford algebra,

$$\mathrm{tr}(A^{(ij)}) = \sum_{I\in\mathcal{I}_{\mathrm{even}}} \langle e_I, A^{(ij)} e_I\rangle = \sum_{I\in\mathcal{I}_{\mathrm{even}}} \langle e_i, e_I e_j \overline{e_I}\rangle = \sum_{I\in\mathcal{I}_{\mathrm{even}}} (-1)^{\delta_{[j\in I]}} \langle e_i, e_j\rangle.$$

If $i \neq j$, every term in the sum vanishes. If $i = j$, observe that there are 2^{n-2} elements of $\mathcal{I}_{\mathrm{even}}$ containing j and 2^{n-2} elements of $\mathcal{I}_{\mathrm{even}}$ not containing j, and hence $\sum_{I\in\mathcal{I}_{\mathrm{even}}} (-1)^{\delta_{[j\in I]}} \langle e_j, e_j\rangle = 0$. ∎

For the remainder of the section, we show that with respect to the standard basis $(e_I)_{I\in\mathcal{I}_{\mathrm{even}}}$ for $\mathrm{Cl}^0(n)$, the $A^{(ij)}$ are represented by the $2^{n-1}\times 2^{n-1}$ symmetric matrices described in (1.6).

Let $\widetilde{A}^{(ij)} : \mathrm{Cl}(n) \to \mathrm{Cl}(n)$ be the self-adjoint linear map such that, for all $x \in \mathrm{Cl}(n)$, $[\widetilde{Q}(x)]_{ij} = \langle e_i, x e_j \overline{x}\rangle = \langle x, \widetilde{A}^{(ij)}x\rangle$. Since

$$\langle e_i, x e_j \overline{x}\rangle = \langle e_i x, x e_j\rangle = \langle x, \lambda_{\overline{e_i}} \rho_{e_j} x\rangle = -\langle x, \lambda_{e_i} \rho_{e_j} x\rangle,$$

it follows that $\widetilde{A}^{(ij)} = -\lambda_{e_i}\rho_{e_j}$. Since $A^{(ij)}$ is the restriction of $\widetilde{A}^{(ij)}$ to the subspace $\mathrm{Cl}^0(n)$, we have that

$$A^{(ij)} = \pi_{\mathrm{Cl}^0(n)}(-\lambda_{e_i}\rho_{e_j})\pi^*_{\mathrm{Cl}^0(n)}. \tag{A.4}$$

It remains to derive the matrices that represent the λ_{e_i} and ρ_{e_i} for $i = 1, 2, \ldots, n$, as well as the matrix representing $\pi_{\mathrm{Cl}^0(n)}$, in terms of the standard basis $(e_I)_{I\subseteq[n]}$ for $\mathrm{Cl}(n)$ (ordered in a particular way). To describe the ordering, define $\delta_{[i\in I]} = 1$ if $i \in I$ and zero otherwise, and define $\delta_{[i\notin I]} = 1$ if $i \notin I$ and zero otherwise. We order the basis elements in such a way that, in coordinates,

$$[e_I] = \begin{bmatrix}\delta_{[1\notin I]}\\ \delta_{[1\in I]}\end{bmatrix} \otimes \begin{bmatrix}\delta_{[2\notin I]}\\ \delta_{[2\in I]}\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}\delta_{[n\notin I]}\\ \delta_{[n\in I]}\end{bmatrix}.$$

It is straightforward to verify (by checking that the relations of (A.1) are satisfied) that in these coordinates,

$$\lambda_i := [\lambda_{e_i}] = \overbrace{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}}^{i-1} \otimes \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} \otimes \overbrace{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}^{n-i} \quad \text{and}$$

$$\rho_i := [\rho_{e_i}] = \underbrace{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}_{i-1} \otimes \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} \otimes \underbrace{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}}_{n-i}.$$

Now, $\pi^*_{\mathrm{Cl}^0(n)}\pi_{\mathrm{Cl}^0(n)} : \mathrm{Cl}(n) \to \mathrm{Cl}(n)$ is represented in these coordinates by

$$[\pi^*_{\mathrm{Cl}^0(n)}\pi_{\mathrm{Cl}^0(n)}] = \frac{1}{2}\overbrace{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}^{n} + \frac{1}{2}\overbrace{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}}^{n}.$$

This can be verified by noting that if $|I|$ is odd, $[\pi^*_{\mathrm{Cl}^0(n)}\pi_{\mathrm{Cl}^0(n)}][e_I] = 0$, and if $|I|$ is even, $[\pi^*_{\mathrm{Cl}^0(n)}\pi_{\mathrm{Cl}^0(n)}][e_I] = [e_I]$. Defining the $2^n \times 2^{n-1}$ matrix

$$P_{\text{even}} = \frac{1}{2}\begin{bmatrix}1\\ 1\end{bmatrix} \otimes \overbrace{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}^{n-1} + \frac{1}{2}\begin{bmatrix}1\\ -1\end{bmatrix} \otimes \overbrace{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \otimes \cdots \otimes \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}}^{n-1}$$

and checking that it satisfies $P_{\text{even}}P_{\text{even}}^T = [\pi^*_{\mathrm{Cl}^0(n)}\pi_{\mathrm{Cl}^0(n)}]$ and that the columns of P_{even} are orthonormal establishes that $P_{\text{even}} = [\pi^*_{\mathrm{Cl}^0(n)}]$. It then follows that in these coordinates,

$$A^{(ij)} = -P_{\text{even}}^T\lambda_i\rho_j P_{\text{even}}$$

as stated in (1.6).

REFERENCES

[1] M. F. Atiyah, R. Bott, and A. Shapiro, *Clifford modules*, Topology, 3 (1964), pp. 3–38.
[2] A. Barvinok and G. Blekherman, *Convex geometry of orbits*, in Combinatorial and Computational Geometry, J. E. Goodman, J. Pach, and E. Welzl, eds., MSRI Publications 52, Cambridge University Press Cambridge, 2005, pp. 51–77.

[3] A. Barvinok and A. M. Vershik, *Convex hulls of orbits of representations of finite groups and combinatorial optimization*, Funct. Anal. Appl., 22 (1988), pp. 224–225.
[4] G. Blekherman, P. A. Parrilo, and R. R. Thomas, eds., *Semidefinite Optimization and Convex Algebraic Geometry*, MOS-SIAM Ser. Optim. 13, SIAM, Philadelphia, 2013.
[5] J. Briët, D. Dadush, and S. Pokutta, *On the existence of* $0/1$ *polytopes with high semidefinite extension complexity*, in Algorithms–ESA 2013, Lecture Notes in Comput. 8125, Springer, New York, 2013, pp. 217–228.
[6] R. D. Carr and G. Konjevod, *Polyhedral combinatorics*, in Tutorials on Emerging Methodologies and Applications in Operations Research, Springer, New York, 2005, pp. 2-1–2-46.
[7] C. B. Chua, *Relating homogeneous cones and positive definite cones via T-algebras*, SIAM J. Optim., 14 (2003), pp. 500–506.
[8] S. Cimprič, J. Kuhlmann, and C. Scheiderer, *Sums of squares and moment problems in equivariant situations*, Trans. Amer. Math. Soc., 361 (2009), pp. 735–765.
[9] M. Conforti, G. Cornuéjols, and G. Zambelli, *Extended formulations in combinatorial optimization*, Ann. Oper. Res., 204 (2013), pp. 97–143.
[10] H. Fawzi, J. Saunderson, and P. A. Parrilo, *Equivariant semidefinite lifts and sum-of-squares hierarchies*, preprint, arXiv:1312.6662.
[11] M. Fazel, *Matrix Rank Minimization with Applications*, Ph.D. thesis, Stanford University, Stanford, CA, 2002.
[12] J. Gallier, *The Cartan–Dieudonné theorem*, in Geometric Methods and Applications, Springer, New York, 2001, pp. 197–247.
[13] K. Gatermann and P. A. Parrilo, *Symmetry groups, semidefinite programs, and sums of squares*, J. Pure Appl. Algebra, 192 (2004), pp. 95–128.
[14] J. Gouveia and T. Netzer, *Positive polynomials and projections of spectrahedra*, SIAM J. Optim., 21 (2011), pp. 960–976.
[15] J. Gouveia, P. A. Parrilo, and R. R. Thomas, *Lifts of convex sets and cone factorizations*, Math. Oper. Res., 38 (2013), pp. 248–264.
[16] J. Gouveia, R. Z. Robinson, and R. R. Thomas, *Worst-case results for positive semidefinite rank*, Math. Program., DOI:10.1007/s10107-015-0867-4, 2015.
[17] F. R. Harvey, *Spinors and Calibrations*, Perspect. Math. 9, Academic Press, Boston, 1990.
[18] A. Horn, *Doubly stochastic matrices and the diagonal of a rotation matrix*, Amer. J. Math., 76 (1954), pp. 620–630.
[19] M. B. Horowitz, N. Matni, and J. W. Burdick, *Convex relaxations of* $SE(2)$ *and* $SE(3)$ *for visual pose estimation*, in Proceedings of the IEEE International Conference on Robotics Automation (ICRA), 2014, pp. 1148–1154.
[20] R. G. Jeroslow, *On defining sets of vertices of the hypercube by linear inequalities*, Discrete Math., 11 (1975), pp. 119–124.
[21] J. E. Keat, *Analysis of Least-Squares Attitude Determination Routine DOAOP*, Technical report CSC/TM-77/6034, Computer Sciences Corporation, 1977.
[22] J. Löfberg, *YALMIP: A toolbox for modeling and optimization in MATLAB*, in Proceedings of the CACSD Conference, Taipei, Taiwan, 2004, pp. 284–289.
[23] M. Longinetti, L. Sgheri, and F. Sottile, *Convex hulls of orbits and orientations of a moving protein domain*, Discrete Comput. Geom., 43 (2010), pp. 54–77.
[24] K. V. Mardia and P. E. Jupp, *Directional Statistics*, Vol. 494, John Wiley & Sons, New York, 2009.
[25] A. Naor, O. Regev, and T. Vidick, *Efficient rounding for the noncommutative Grothendieck inequality*, in Proceedings of the 45th Annual ACM Symposium on Symposium on Theory of Computing, ACM, 2013, pp. 71–80.
[26] A. Nemirovski, *Sums of random symmetric matrices and quadratic optimization under orthogonality constraints*, Math. Program., 109 (2007), pp. 283–317.
[27] M. L. Psiaki, *Generalized Wahba problems for spinning spacecraft attitude and rate determination*, J. Astronaut. Sci., 57 (2009), pp. 73–92.
[28] M. Ramana and A. J. Goldman, *Some geometric results in semidefinite programming*, J. Global Optim., 7 (1995), pp. 33–50.
[29] M. V. Ramana, *Polyhedra, spectrahedra, and semidefinite programming*, in Topics in Semidefinite and Interior-point Methods, P. M. Pardalos and H. Wolkowicz, eds., Fields Inst. Commun. 18, AMS, Providence, RI, 1998, pp. 27–38.
[30] J. Renegar, *Hyperbolic programs, and their derivative relaxations*, Found. Comput. Math., 6 (2006), pp. 59–79.
[31] R. T. Rockafellar, *Convex Analysis*, Princeton University Press, Princeton, NJ, 1997.
[32] R. Sanyal, F. Sottile, and B. Sturmfels, *Orbitopes*, Mathematika, 57 (2011), pp. 275–314.
[33] J. Saunderson, P. A. Parrilo, and A. S. Willsky, *A convex solution to a joint attitude and spin-rate estimation problem*, J. Guid. Control Dyn., DOI:10.2514/1.G001107, 2015.

[34] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, Springer, New York, 2003.

[35] R. Sinn, *Algebraic boundaries of* SO(2)*-orbitopes*, Discrete Comput. Geom., 50 (2013), pp. 219–235.

[36] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, *SDPT3—A MATLAB software package for semidefinite programming*, version 1.3, Optim. Methods Softw., 11 (1999), pp. 545–581.

[37] È. B. Vinberg, *The theory of homogeneous convex cones*, Trans. Moscow Math. Soc., 12 (1965), pp. 340–403.

[38] G. Wahba, *A least squares estimate of satellite attitude*, SIAM Rev., 7 (1965), pp. 409–409.