**MATHEMATICS OF OPERATIONS RESEARCH**
Vol. 00, No. 0, Xxxxx 0000, pp. 000–000
ISSN 0364-765X | EISSN 1526-5471 | 00 | 0000 | 0001

**INFORMS**
DOI 10.1287/xxxx.0000.0000
© 0000 INFORMS

# Equivariant semidefinite lifts of regular polygons

Hamza Fawzi
Laboratory for Information and Decision Systems, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, hfawzi@mit.edu

James Saunderson
Department of Electrical Engineering, University of Washington, Seattle, WA 98195. jamesfs@uw.edu

Pablo A. Parrilo
Laboratory for Information and Decision Systems, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, parrilo@mit.edu

Given a polytope $P \subset \mathbb{R}^n$, we say that $P$ has a positive semidefinite lift (psd lift) of size $d$ if one can express $P$ as the projection of an affine slice of the $d \times d$ positive semidefinite cone. Such a representation allows us to solve linear optimization problems over $P$ using an SDP of size $d$ and can be useful in practice when $d$ is much smaller than the number of facets of $P$. If a polytope $P$ has symmetry, we can consider *equivariant* psd lifts, i.e., those psd lifts that respect the symmetries of $P$. One of the simplest families of polytopes with interesting symmetries is regular polygons in the plane. In this paper we give tight lower and upper bounds on the size of equivariant psd lifts for regular polygons. We give an explicit construction of an equivariant psd lift of the regular $2^n$-gon of size $2n-1$, and we prove that our construction is essentially optimal by proving a lower bound of $\Omega(\log N)$ on the size of any equivariant psd lift of the regular $N$-gon. Our construction is exponentially smaller than the (equivariant) psd lift obtained from the Lasserre/sum-of-squares hierarchy, and it also gives the first example of a polytope with an exponential gap between equivariant psd lifts and equivariant LP lifts.

*Key words*: Semidefinite programming, extended formulations, sums of squares
*MSC2000 subject classification*: Primary: 90C22; secondary: 52B15, 68Q17
*OR/MS subject classification*: Primary: programming/linear, theory; secondary: mathematics/convexity

## 1. Introduction

**1.1. Preliminaries** Semidefinite programming is the problem of minimizing (or maximizing) a linear function subject to linear matrix inequalities. The feasible set of a semidefinite program is known as a *spectrahedron* and corresponds to an affine slice of the cone of positive semidefinite matrices. An important question that has attracted a lot of attention in optimization is to give representations of convex sets as feasible sets of semidefinite programs.

In this paper we are interested in *lifted* semidefinite representations. We say that a convex set $C$ has a *positive semidefinite lift* (psd lift) if it can be written as the linear projection of a spectrahedron. More formally, we have the following definition of psd lift (we work with Hermitian lifts for convenience):

DEFINITION 1. (Gouveia et al. [13]) Let $C$ be a convex set in $\mathbb{R}^n$. Let $\mathbf{H}^d$ be the space of $d \times d$ Hermitian matrices, and $\mathbf{H}^d_+$ be the cone of $d \times d$ Hermitian positive semidefinite matrices. We say that $C$ has a $\mathbf{H}^d_+$-lift, or a *psd lift of size* $d$, if there exists a linear map $\pi : \mathbf{H}^d \to \mathbb{R}^n$ and an affine subspace $L \subset \mathbf{H}^d$ such that:

$$C = \pi(\mathbf{H}^d_+ \cap L).$$

An interesting question that has gained a lot of interest recently is, for a given polytope $P$, to characterize the size of the *smallest psd lift* of $P$. This quantity, known as the *psd rank* of $P$, was

introduced in Gouveia et al. [13] and studied in e.g., Fiorini et al. [8], Gouveia et al. [14], Briët et al. [3] and Fawzi et al. [6]. Positive semidefinite lifts are interesting in practice when the size of the psd lift is much smaller than the number of facets of $P$ (which is the size of the trivial representation of $P$). Indeed, if $P$ has a psd lift of size $d$, then one can formulate any linear optimization problem over $P$ as a semidefinite program of size $d$.

The definition of a psd lift given here was first formulated in Gouveia et al. [13] and is the generalization of the notion of *LP lift* (also called *LP extended formulation*) to the case of semidefinite programming. The definition of an LP lift of size $d$ is similar to that of a psd lift except that the psd cone $\mathbf{H}^d_+$ is replaced by $\mathbb{R}^d_+$ (see Appendix B for the formal statement of the definition). The size of the smallest LP lift of a polytope $P$ is called the *LP extension complexity*. An important question in the area of lifted representations of polytopes is to know whether there exist polytopes with large gaps between sizes of LP lifts and psd lifts. The following open question is taken from [5]:

Question 1. Find a family of polytopes that exhibits a large (e.g. exponential) gap between its psd rank and LP extension complexity.

One of the results of this paper shows that regular polygons constitute an example of such a gap when we restrict to lifts that respect symmetry, in a sense that we now make precise. Note that the recent paper [7] gives an example with a multiplicative gap of $O(\frac{\log k}{k})$ between sizes of LP and psd lifts without symmetry requirement, for a family of trigonometric cyclic polytopes in $\mathbb{R}^{2k}$ (trigonometric cyclic polytopes can be seen as multidimensional generalizations of regular polygons).

***Equivariant lifts*** In many situations, the polytope $P$ of interest has certain symmetries. The symmetries of a polytope $P \subset \mathbb{R}^n$ are the geometric transformations that leave $P$ invariant: more precisely if $G$ is a group linearly acting on $\mathbb{R}^n$, we say that $P$ is invariant under the action of $G$ if $g \cdot x \in P$ for any $x \in P$ and $g \in G$. For example the regular $N$-gon in the plane, is invariant under the action of the dihedral group which consists of $N$ rotations and $N$ reflections. In Fawzi et al. [6], we studied so-called *equivariant psd lifts* of polytopes, which are psd lifts that respect the symmetry of a polytope $P$. Intuitively, a psd lift $P = \pi(\mathbf{H}^d_+ \cap L)$ respects the symmetry of $P$ if any transformation $g \in G$ that leaves $P$ invariant can be *lifted* to a transformation $\Phi(g)$ of $\mathbf{H}^d$ that leaves the cone $\mathbf{H}^d_+$ and the subspace $L$ invariant and such that the following natural *equivariance* condition holds: $\pi(\Phi(g)Y) = g \cdot \pi(Y)$ for all $Y \in \mathbf{H}^d_+ \cap L$. Since the transformations that leave the psd cone $\mathbf{H}^d_+$ invariant are precisely the congruence transformations (i.e., transformations of the form $Y \mapsto RYR^*$ where $R \in GL_d(\mathbb{C})$, cf. Tunçel [22, Theorem 9.6.1]), the transformation $\Phi(g)$ is required to have the form $\Phi(g) : Y \mapsto \rho(g)Y\rho(g)^*$ where $\rho : G \to GL_d(\mathbb{C})$ is a group homomorphism. This leads to the following definition of *equivariant psd lift* from [6]:

Definition 2. Let $P \subseteq \mathbb{R}^n$ be a polytope and assume $P$ is invariant under the action of some group $G$. Let $P = \pi(\mathbf{H}^d_+ \cap L)$ be a $\mathbf{H}^d_+$-lift of $P$, where $L \subset \mathbf{H}^d$ is an affine subspace of the space of Hermitian $d \times d$ matrices. The lift is called *$G$-equivariant* if there exists a homomorphism $\rho : G \to GL_d(\mathbb{C})$ such that:

(i) The subspace $L$ is invariant under congruence transformations by $\rho(g)$, for all $g \in G$, i.e.:

$$\rho(g)Y\rho(g)^* \in L \quad \forall g \in G, \forall Y \in L. \tag{1}$$

(ii) The following equivariance relation holds:

$$\pi\left(\rho(g)Y\rho(g)^*\right) = g \cdot \pi(Y) \quad \forall g \in G, \forall Y \in \mathbf{H}^d_+ \cap L. \tag{2}$$

In [6] we studied equivariant psd lifts of a general class of symmetric polytopes known as *orbitopes*. An *orbitope*, cf. Sanyal et al. [21], is a polytope of the form $P = \mathrm{conv}(G \cdot x_0)$ where $G \cdot x_0$ is the orbit of $x_0 \in \mathbb{R}^n$ under the action of a finite group $G$. In [6] we established a connection

between equivariant psd lifts of such polytopes and sum-of-squares certificates for its facet-defining inequalities from an invariant subspace. This connection allowed us to prove exponential lower bounds on sizes of equivariant psd lifts for two families of polytopes, namely the cut polytope and the parity polytope.

Note that when working with LP lifts (i.e., lifts with the cone $\mathbb{R}^d_+$) one can also give a natural definition of *equivariant LP lift* (also known as symmetric LP lift in the literature). The definition of an equivariant LP lift is similar to that of an equivariant psd lift, except that the action by congruence transformations $Y \mapsto \rho(g) Y \rho(g)^*$ is replaced by a permutation action $y \mapsto \Phi(g)y$ where $\Phi : G \to \mathfrak{S}_d$ is a homomorphism from $G$ to the permutation group on $d$ elements (see Appendix B for the formal statement).

Equivariant LP lifts of various polytopes have been studied before in e.g., Yannakakis [23], Kaibel et al. [18], Pashkovich [20], Gouveia et al. [13], Chan et al. [4] and it was shown that the requirement of equivariance can affect the size of the lift: several examples have been provided of polytopes with an exponential gap between sizes of LP lifts and equivariant LP lifts. One of the simplest such examples are regular $N$-gons in the plane which are known to have an LP lift of size $\log N$ (cf. Ben-Tal and Nemirovski [1]), and yet any equivariant LP lift must have size at least $N$ when $N$ is a power of a prime (cf. Gouveia et al. [13] and also Appendix B for more details).

Further results about lifts of non-regular polygons were obtained in Fiorini et al. [9] where it was shown that generic $N$-gons have LP extension complexity at least $\sqrt{2N}$ (where generic means that the coordinates of the vertices are algebraically independent over $\mathbb{Q}$). For psd lifts of $N$-gons much less is known. The only asymptotic lower bound on the *psd rank* of $N$-gons is $\Omega\left(\sqrt{\frac{\log N}{\log\log N}}\right)$ which comes from quantifier elimination theory [13, 15]. It is also known that generic $N$-gons have psd rank at least $(2N)^{1/4}$, cf. Gouveia et al. [15].

**1.2. Summary of contributions** In this paper we propose to study equivariant psd lifts of regular polygons. Our contribution is threefold:

1. To obtain an equivariant psd lift of the regular polygon, one way is to use the Lasserre/sum-of-squares hierarchy, cf. Lasserre [19] and Gouveia et al. [12]. Our first contribution is to show that the sum-of-squares hierarchy for the regular $N$-gon requires exactly $\lceil N/4 \rceil$ iterations. The lower bound of $\lceil N/4 \rceil$ seems to be known in the community, though not written explicitly anywhere. Our main contribution here is to show that the $\lceil N/4 \rceil$'th iteration is exact (the previously known upper bound was $\lceil N/2 \rceil - 1$). We prove this new upper bound by exploiting the fact that the regular $N$-gon is a $\lceil N/2 \rceil$-*level* polytope and by showing that in some cases —and in the particular case of regular polygons— $k$-level polytopes only require $\lceil k/2 \rceil$ levels of the sum-of-squares hierarchy, instead of the previously known bound of $k-1$, cf. Gouveia and Thomas [16, Theorem 11]. The results developed here are of independent interest and can be applied to other $k$-level polytopes.

2. The second contribution of the paper is to give an explicit construction of an *equivariant psd lift* of the regular $2^n$-gon of size $2n-1$. The main feature of our construction is that it is *equivariant* (with respect to the full dihedral group), unlike the LP lift of Ben-Tal and Nemirovski [1] which is not equivariant. It was actually shown in [13, Proposition 3] that any equivariant LP lift of the regular $N$-gon must have size at least $N$ when $N$ is a prime or a power of a prime (cf. Appendix B for more details). Our construction thus gives an exponential gap between sizes of equivariant psd and linear programming lifts and thus gives an answer to a restricted version of Question 1, where the restriction is to the case of equivariant lifts. Also note that the size of our construction is exponentially smaller than the lift obtained from the Lasserre/sum-of-squares hierarchy, which has size $1+2^{n-1}$. Theorem 1 below describes our lift which uses the Cartesian product cone $(\mathbf{H}^3_+)^{n-1}$ and which is easier to state (we refer the reader to Section 4 for an alternative lift over the cone $\mathbf{H}^{2n-1}_+$).

THEOREM 1. *Let $\mathcal{X}_N$ be the $N$ roots of unity in $\mathbb{C} \simeq \mathbb{R}^2$. Then* $\mathrm{conv}(\mathcal{X}_{2^n})$ *is the set of $y_0 \in \mathbb{C}$ such that there exist $y_1, \dots, y_{n-2} \in \mathbb{C}$ and $y_{n-1} \in \mathbb{R}$ such that*

$$\begin{bmatrix} 1 & y_{k-1} & \overline{y_{k-1}} \\ \overline{y_{k-1}} & 1 & \overline{y_k} \\ y_{k-1} & y_k & 1 \end{bmatrix} \in \mathbf{H}^3_+ \text{ for } k = 1, 2, \dots, n-2 \text{ and } \begin{bmatrix} 1 & y_{n-2} & \overline{y_{n-2}} \\ \overline{y_{n-2}} & 1 & y_{n-1} \\ y_{n-2} & y_{n-1} & 1 \end{bmatrix} \in \mathbf{H}^3_+. \tag{3}$$

REMARK 1. Note that the semidefinite lift (3) uses rational numbers only, whereas the LP lift of Ben-Tal and Nemirovski [1] involves irrational numbers.

REMARK 2. The construction we give in this paper only works for $2^n$-gons. In the recent paper [7] we show that for any integer $N$, the regular $N$-gon has an equivariant psd lift of size $O(\log N)$.

3. Lastly, we prove that our equivariant lift is optimal by proving a lower bound on the sizes of equivariant psd lifts of the regular $N$-gon. In fact we show that any equivariant Hermitian psd lift of the regular $N$-gon must have size at least $\ln(N/2)$.

THEOREM 2. *Any Hermitian psd lift of the regular $N$-gon that is equivariant with respect to the rotation group* $\mathrm{Rot}_N$ *of order $N$ has size at least* $\ln(N/2)$.

TABLE 1. Bounds on the size of the smallest LP/PSD lifts for the regular $2^n$-gon in both the equivariant and non-equivariant cases. The main contributions of this paper are highlighted in bold.

| | Equivariant | Non-equivariant |
|---|---|---|
| LP | Lower bound: $2^n$ (Gouveia et al. [13])<br>Upper bound: $2^n$ (trivial) | Lower bound: $n$ (Goemans [10])<br>Upper bound: $2n+1$ (Ben-Tal and Nemirovski [1]) |
| SDP | **Lower bound:** $(\ln 2)(n-1)$ **(Theorem 2)**<br>**Upper bound:** $2n-1$ **(Section 4)** | Lower bound: $\Omega\left(\sqrt{\frac{n}{\log n}}\right)$ (Gouveia et al. [13, 15])<br>Upper bound: $2n-1$ (Section 4) |

Table 1 summarizes our contributions as well as previously known bounds on LP/PSD lifts of the regular $2^n$-gon in both the equivariant and non-equivariant cases.

The proofs of our results rely on the connection between equivariant psd lifts and sum-of-squares certificates of facet inequalities for the regular $N$-gon. In fact the main ingredient to prove Theorem 1 is to show that the facet inequalities of the regular $2^n$-gon admit a certain *sparse* sum-of-squares certificate that only requires a small number of monomials. Similarly the proof of Theorem 2 consists in obtaining a lower bound on the sparsity of polynomials that arise in any sum-of-squares certificate of the facet-defining inequalities of the regular $N$-gon.

***Organization*** The paper is organized as follows: In Section 2 we describe some of the notations used in this paper, and we provide precise statements about the connection between equivariant psd lifts and sums of squares, that will be crucial for the rest of the paper. In Section 3 we prove that the Lasserre/sum-of-squares hierarchy of the regular $N$-gon requires exactly $\lceil N/4 \rceil$ iterations. Then in Section 4 we show a construction of an equivariant psd lift of the regular $2^n$-gon of size $2n-1$. Finally in Section 5 we show that any equivariant psd lift of the regular $N$-gon must have size at least $\ln(N/2)$.

## 2. Notations

In this section we introduce some notations and we describe more formally the connection between equivariant psd lifts and sum-of-squares certificates.

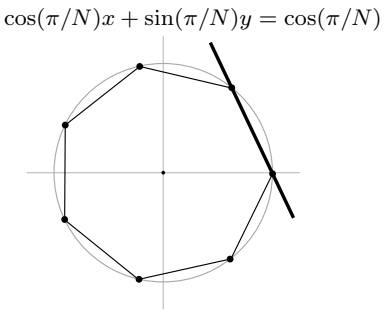


FIGURE 1. The regular 7-gon.

***Regular $N$-gon*** The regular $N$-gon we consider in this paper has vertices the $N$'th roots of unity:

$$\mathcal{X}_N = \{(\cos(2\pi t/N), \sin(2\pi t/N)) : t \in \mathbb{Z}_N\}$$

where $\mathbb{Z}_N$ is the set of integers modulo $N$. Figure 1 shows a picture for $N = 7$. The symmetry group of the regular $N$-gon is the dihedral group $\mathrm{Dih}_{2N}$ of order $2N$ which consists of $N$ rotations and $N$ reflections. We denote by $\mathrm{Rot}_N$ the subgroup of rotations, isomorphic to $\mathbb{Z}_N$.

The "first" facet of the regular $N$-gon is defined by the linear inequality $\cos(\pi/N) - \cos(\pi/N)x - \sin(\pi/N)y \geq 0$. Throughout this paper, we denote by $\ell$ the restriction of this facet on the vertices of the $N$-gon:

$$\ell(t) = \cos(\pi/N) - \cos(\pi/N)\cos(2\pi t/N) - \sin(\pi/N)\sin(2\pi t/N), \quad t \in \mathbb{Z}_N. \tag{4}$$

Concretely $\ell$ is an element of $\mathbb{C}^N$ (or, more precisely, $\mathbb{C}^{\mathbb{Z}_N}$) whose components are all nonnegative.

***Fourier basis*** It is well-known that any element of $\mathbb{C}^N$ admits a decomposition in the Fourier basis. The elements of the Fourier basis are given by

$$e_k(t) = e^{2i\pi kt/N} \quad \forall t \in \mathbb{Z}_N$$

where $k \in \mathbb{Z}_N$. For convenience we are going to define the elements $c_k$ and $s_k$ which play the role $\cos(2\pi kt/N)$ and $\sin(2\pi kt/N)$:

$$c_k = \frac{e_k + e_{-k}}{2}, \quad s_k = \frac{e_k - e_{-k}}{2i}.$$

With the notations above, the element $\ell$ defined earlier in Equation (4) can be written as:

$$\begin{aligned} \ell &= \cos(\pi/N)c_0 - \cos(\pi/N)c_1 - \sin(\pi/N)s_1 \\ &= \cos(\pi/N)e_0 - \frac{1}{2}e^{-i\pi/N}e_1 - \frac{1}{2}e^{i\pi/N}e_{-1}. \end{aligned} \tag{5}$$

***Equivariant lifts and sum-of-squares certificates*** A sum-of-squares certificate for $\ell$ takes the form:

$$\ell = \sum_i |h_i|^2 \tag{6}$$

where $h_i \in \mathbb{C}^N$ and where $|h_i|^2$ is the componentwise modulus square of $h_i$. The next theorem, which is a special case of results in [12, 19], shows that to construct an equivariant psd lift of the regular $N$-gon, it suffices to find a sum-of-squares certificate of $\ell$ of the form (6) where the $h_i$s are sparse in the Fourier basis.

THEOREM 3 **(Special case of [12, 19])**. *Assume that $\ell$ defined in (5) admits a sum-of-squares certificate of the form:*

$$\ell = \sum_{i=1}^{q} \sum_{j} |h_{ij}|^2 \tag{7}$$

*where for each $i = 1, \dots, q$ and each $j$ the function $h_{ij}$ is in $\bigoplus_{k \in K_i} \mathbb{C} e_k$ where $K_i \subseteq \mathbb{Z}_N$. Then the regular $N$-gon admits the following Hermitian psd lift over the Cartesian product $\mathbf{H}_+^{d_1} \times \dots \mathbf{H}_+^{d_q}$ where $d_i = |K_i|$ for each $i = 1, \dots, q$:*

$$\operatorname{conv}(\mathcal{X}_N) = \left\{ (\operatorname{Re}[y_1], \operatorname{Im}[y_1]) : y_0 = 1, [y_{k'-k}]_{k,k' \in K_i} \in \mathbf{H}_+^{d_i} \; \forall i = 1, \dots, q \right\}. \tag{8}$$

*Furthermore this lift is equivariant with respect to the rotation group $\mathrm{Rot}_N$. Also if $K_i = -K_i$ for all $i$, then the lift is equivariant with respect to the dihedral group $\mathrm{Dih}_{2N}$.*

*Proof.* We include a proof in Appendix C for completeness. The reason such sum-of-squares certificates lead to $\mathrm{Rot}_N$-equivariant lifts is that any subspace of $\mathbb{C}^N$ of the form $\oplus_{k \in K} \mathbb{C} e_k$ is invariant under the action of $\mathrm{Rot}_N$ which shifts the vertices of the regular $N$-gon. We refer the reader to [6] for more information. □

REMARK 3. The additional ("lifting") variables in (8) are the $y_{k'-k}$ for $k, k' \in K_i$ and $i = 1, \dots, q$, where $k' - k$ is understood modulo $N$. Note that the Hermitian psd constraint on the matrices $[y_{k'-k}]_{k,k' \in K_i}$ automatically implies that $y_{-j} = \overline{y_j}$. For example if $N = 6$ and $K = \{0, 1, -1, 3\}$ then the constraint $[y_{k'-k}]_{k,k' \in K} \succeq 0$ together with $y_0 = 1$ corresponds to:

$$\begin{bmatrix} 1 & y_1 & \overline{y_1} & y_3 \\ \overline{y_1} & 1 & \overline{y_2} & y_2 \\ y_1 & y_2 & 1 & \overline{y_2} \\ y_3 & \overline{y_2} & y_2 & 1 \end{bmatrix} \succeq 0.$$

Note that $3 = -3 \bmod 6$ and so this is why the $(1,4)$ and $(4,1)$ entries of the matrix above are both $y_3$. This in particular implies that $y_3$ has to be real (for the matrix to be Hermitian).

The next theorem is a converse to Theorem 3. It shows that any equivariant psd lift corresponds to a certain sum-of-squares certificate for $\ell$. This theorem is a special case of the structure theorem in [6].

THEOREM 4 **(Special case of [6])**. *Assume that the regular $N$-gon has a Hermitian psd lift of size $d$ that is equivariant with respect to $\mathrm{Rot}_N$, the rotation group of order $N$. Then there exists a set $K \subseteq \mathbb{Z}_N$ with $|K| \leq d$ and functions $h_i \in \bigoplus_{k \in K} \mathbb{C} e_k$ such that*

$$\ell = \sum_{i} |h_i|^2.$$

*Proof.* See Appendix D. □

This result shows that in order to prove a lower bound on the size of equivariant psd lifts of the regular $N$-gon, it suffices to prove a lower bound on the sparsity of sum-of-squares certificates for $\ell$. This is the approach we adopt in Section 5 to prove a lower bound of $\ln(N/2)$ on the size of $\mathrm{Rot}_N$-equivariant psd lifts of the regular $N$-gon.

**3. Sum-of-squares hierarchy and nonnegative polynomial interpolation** In this section we study the Lasserre/sum-of-squares hierarchy for the regular $N$-gon and we show that the hierarchy is exact after $\lceil N/4 \rceil$ levels.

The Lasserre/sum-of-squares hierarchy for the regular $N$-gon seeks to certify the nonnegativity of the facet $\ell$ using low-degree sum-of-squares. We say that an element $h \in \mathbb{C}^N$ has *degree* at most $k$ if it is in the subspace

$$\bigoplus_{i \in \{-k,\dots,k\}} \mathbb{C} e_i.$$

Equivalently one can show that $\deg h \leq k$ if and only if $h$ is the restriction of a bivariate polynomial in $\mathbb{C}[x,y]$ of degree $k$ to the vertices of the regular $N$-gon. With this definition, the $k$'th level of the sum-of-squares hierarchy is *exact* if there exist $h_i \in \mathbb{C}^N$ with $\deg h_i \leq k$ such that[1] $\ell = \sum_i |h_i|^2$. The smallest $k$ for which such a certificate exists is called the *theta-rank* of the $N$-gon, in reference to the terminology on theta-bodies [12]. In this section we prove that the theta-rank of the regular $N$-gon is exactly $\lceil N/4 \rceil$:

THEOREM 5. *The facet functional $\ell = \cos(\pi/N)c_0 - \cos(\pi/N)c_1 - \sin(\pi/N)s_1 \in \mathbb{C}^N$ admits a sum-of-squares certificate $\ell = \sum_i |h_i|^2$ where each $h_i$ has degree at most $\lceil N/4 \rceil$. Furthermore if $\ell$ has a sum-of-squares certificate $\ell = \sum_i |h_i|^2$ then at least one $h_i$ has degree $\geq N/4$.*

We first prove the lower bound which is apparently well-known though does not seem to be written explicitly anywhere. The argument we present below is due to G. Blekherman.

PROPOSITION 1. *If $\ell$ has a sum-of-squares certificate $\ell = \sum_i |h_i|^2$ then at least one $h_i$ has degree $\geq N/4$.*

*Proof.* In this proof we will think of $\ell$ as the linear function $\ell(x,y) = \cos(\pi/N) - x\cos(\pi/N) - y\sin(\pi/N)$ in $\mathbb{R}^2$, and of $h_i$ as polynomials in $\mathbb{C}[x,y]$. Let $g(x,y) = \ell(x,y) - \sum_i |h_i(x,y)|^2$. By assumption $g$ vanishes on the vertices of the $N$-gon. Since $g$ is not identically zero ($g(1,0) \leq \ell(1,0) < 0$) it follows that $g$ must have degree at least $N/2$ (recall that a nonzero polynomial in $\mathbb{C}[x,y]$ of degree $d$ can have at most $2d$ zeros on the unit circle). Since $\deg \ell = 1$ it follows directly that at least of one of the $h_i$'s has degree $\geq N/4$. □

The rest of this section is mainly devoted to the proof that $\lceil N/4 \rceil$ levels of the sum-of-squares hierarchy are sufficient for the regular $N$-gon. Namely we show that $\ell$ admits a sum-of-squares certificate (6) where $\deg h_i \leq \lceil N/4 \rceil$ for all $i$. To do so we exploit the fact that the regular $N$-gon is a *$k$-level* polytope where $k = \lceil N/2 \rceil$. In fact we develop new general results about the theta-rank of $k$-level polytopes.

**3.1. $k$-level polytopes and nonnegative polynomial interpolation** In this section we study polytopes that are *$k$-level*, and we see how this property implies an upper bound on the sum-of-squares hierarchy. The material presented in this section concerns general polytopes $P$, and is not restricted to the case of regular $N$-gons.

We first recall the definition of a $k$-level polytope (see e.g., [16]):

DEFINITION 3. A polytope $P$ is called *$k$-level* if every facet-defining linear function of $P$ takes at most $k$ different values on the vertices of the polytope.

EXAMPLE 1 (REGULAR POLYGONS). It is easy to verify that the regular $N$-gon is a $\lceil N/2 \rceil$-level polytope. Indeed the values taken by the facet-defining linear function $\ell(x,y) = \cos(\pi/N) - x\cos(\pi/N) - y\sin(\pi/N)$ on the $N$ vertices of the polytope are:

$$0,\ x_{1,N} - x_{2,N},\ \dots,\ x_{1,N} - x_{\lceil N/2 \rceil,N} \quad \text{where} \quad x_{k,N} = \cos\left(\frac{(2k-1)\pi}{N}\right).$$

By symmetry, the number of values taken by the other facet-defining linear functions is also $\lceil N/2 \rceil$, and thus the regular $N$-gon is $\lceil N/2 \rceil$-level.

[1] Note that the sum-of-squares hierarchy is exact at level $k$ if *all* the facet inequalities can be certified using functions of degree at most $k$. However since all the facets are equivalent up to rotation it is sufficient to consider just one of them.

It was shown in [16, Theorem 11], via a Lagrange interpolation argument, that if a polytope $P$ is $k$-level, then the $(k-1)$'st level of the sum-of-squares hierarchy is exact. To prove this result, the idea is to look at a "one-dimensional projection" of the problem: Let $\ell(\boldsymbol{x}) \geq 0$ be a facet-defining linear inequality for $P$ and assume that $\ell(\boldsymbol{x})$ takes the $k$ values $0 = a_0 < a_1 < \cdots < a_{k-1}$ on the vertices of $P$. To get an upper bound on the sum-of-squares hierarchy for $P$, we need to express the function $\ell$ on the vertices of $P$ as a sum-of-squares. To do this, one can proceed as follows: let $p$ be a *univariate* polynomial that satisfies $p(a_i) = a_i$ for all $i = 0, \ldots, k-1$ and that is *globally nonnegative* on $\mathbb{R}$. Since nonnegative univariate polynomials are sums of squares (see e.g., [2, Exercise 3.30]), this means that we can write $p = \sum_i h_i^2$ for some polynomials $h_i$. Then observe that for any vertex $\boldsymbol{x}$ of the polytope $P$ we have

$$\ell(\boldsymbol{x}) \overset{(*)}{=} p(\ell(\boldsymbol{x})) = \sum_i h_i(\ell(\boldsymbol{x}))^2,$$

where equality $(*)$ follows from the fact $\ell(x) \in \{a_0, \ldots, a_{k-1}\}$ since $\boldsymbol{x}$ is a vertex of $P$. This shows that $\ell$ coincides on the vertices of $P$ with a sum-of-squares polynomial of degree $d = \deg p$. If one can find such a sum-of-squares certificate of degree $d$ for all the facet-defining linear functions of $P$, then this shows that the $d/2$-level of the sum-of-squares hierarchy is exact.

Note that there is a simple way to construct a polynomial $p$ that satisfies the required conditions, i.e., $p(a_i) = a_i$ for all $i = 0, \ldots, k-1$ and $p$ globally nonnegative: One can simply take a Lagrange interpolating polynomial $r$ of degree $k-1$ such that $r(a_i) = \sqrt{a_i}$ and then take $p(x) = r(x)^2$. The resulting polynomial $p$ has degree $2(k-1)$ and thus gives an upper bound of $k-1$ for the sum-of-squares hierarchy of $k$-level polytopes. This is the construction used in [16, Theorem 11].

It turns out however that one can sometimes find a polynomial $p$ that has smaller degree. This motivates the following definition:

Definition 4. Let $0 = a_0 < a_1 < \cdots < a_{k-1}$ be $k$ points on the real line. We say that the sequence $(a_0, \ldots, a_{k-1})$ has *nonnegative interpolation degree* $d$ if there exists a globally nonnegative polynomial $p$ with $\deg p = d$ such that $p(a_i) = a_i$ for all $i = 0, \ldots, k-1$.

The construction outlined above with Lagrange interpolating polynomials shows that any sequence of length $k$ has nonnegative interpolation degree at most $2(k-1)$. Also note that the nonnegative interpolation degree of any sequence with $k$ elements must be at least $k$: indeed if $p$ has degree $\leq k-1$ and $p(a_i) = a_i$ for all $i = 0, \ldots, k-1$ then $p$ must be equal to the linear polynomial $x$, which is clearly not nonnegative.

The previous discussion concerning the sum-of-squares hierarchy for $k$-level polytopes can be summarized in the following proposition:

Proposition 2. *Let $P$ be a $k$-level polytope in $\mathbb{R}^n$. Assume that for any facet-defining linear functional $\ell$ of $P$, the $k$ values taken by $\ell$ on the vertices of $P$ have nonnegative interpolation degree $d$. Then the $d/2$-level of the sum-of-squares hierarchy for $P$ is exact (note that $d$ is necessarily even).*

In the rest of this section we study sequences of length $k$ that have nonnegative interpolation degree equal to $k$ (i.e., the minimum possible value). Let $k$ be an even integer and let $0 = a_0 < a_1 < \cdots < a_{k-1}$ be $k$ points on the positive real axis. The question that we thus consider is: does there exist a univariate polynomial $p$ such that:

$$\begin{cases} \deg p = k \\ p(a_i) = a_i \quad \forall i = 0, \ldots, k-1 \\ p(x) \geq 0 \quad \forall x \in \mathbb{R}. \end{cases} \tag{9}$$

The next proposition gives a simple geometric characterization of the existence of a polynomial $p$ that satisfies (9):

PROPOSITION 3. *Let $q(x) = \prod_{i=0}^{k-1}(x - a_i)$ be the monic polynomial of degree $k$ that vanishes at the $a_i$'s. Then the following are equivalent:*
*(i) There exists a polynomial $p$ that satisfies (9);*
*(ii) The curve of $q(x)$ is above its tangent at $x = 0$, i.e.:*

$$q(x) \geq q'(0)x \quad \forall x \in \mathbb{R}. \tag{10}$$

*Proof.* Note that if a polynomial $p$ satisfies (9) then it must be of the form:

$$p(x) = \alpha q(x) + x$$

where $\alpha$ is a scalar. Furthermore, since $p$ is nonnegative and $p(0) = 0$, then 0 must be a double root of $p$, i.e., $p'(0) = 0$. This means that we must have $\alpha q'(0) + 1 = 0$ which implies $\alpha = -1/q'(0)$. In other words, the unique $p$ which can satisfy conditions (9) is the polynomial:

$$p(x) = -\frac{q(x)}{q'(0)} + x.$$

Observe that $p$ is, up to scaling, equal to the difference between $q(x)$ and its linear approximation at $x = 0$:

$$p(x) = -\frac{1}{q'(0)}(q(x) - q'(0)x).$$

Since $q'(0) < 0$ (since $k$ is even), we see that $p(x) \geq 0$ if and only if the curve of $q$ is above its linear approximation at $x = 0$. □

EXAMPLE 2 (EQUISPACED AND SUBADDITIVE SEQUENCES). To illustrate this result consider the sequence $a_i = i$ for $i = 0, \ldots, k-1$. Figure 2 shows the plot of the polynomial $q(x) = \prod_{i=0}^{k-1}(x - a_i)$ for $k = 6$ and its tangent at $x = 0$. We see from the figure that the curve of $q$ is always above its linear approximation at $x = 0$. This means, by Proposition 3, that the nonnegative interpolation degree of the sequence $0, 1, \ldots, 5$ is 6. One can actually prove that the nonnegative interpolation

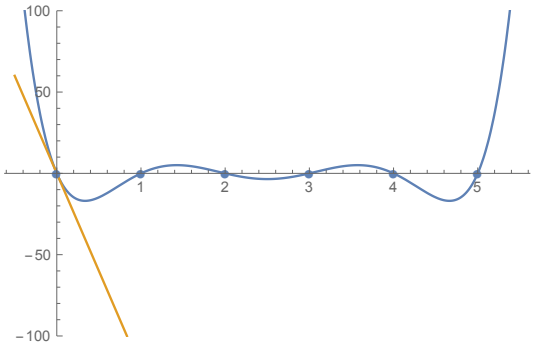


FIGURE 2. Plot of the polynomial $q(x) = \prod_{i=0}^{5}(x - i)$ and its tangent at $x = 0$. We see that the tangent is always below the curve of $q$. Thus from Proposition 3 there is a polynomial $p$ of degree 6 that satisfies (9) for the sequence $a_i = i$, $(i = 0, \ldots, 5)$.

degree of the sequence $a_i = i$ for $i = 0, \ldots, k-1$ is equal to $k$ for any $k$ even. In fact this is true even more generally for any sequence $a_0, \ldots, a_{k-1}$ that is *subadditive*, i.e., that satisfies $a_{i+j} \leq a_i + a_j$ for all $i, j$ such that $i + j \leq k - 1$. This is the object of the next proposition:

PROPOSITION 4. *Let $k$ be an even integer and assume that $0 = a_0 < a_1 < \cdots < a_{k-1}$ is a subadditive sequence, i.e., $a_{i+j} \leq a_i + a_j$ for all $i, j$ such that $i + j \leq k$. Then $(a_i)_{i=0,\ldots,k-1}$ has nonnegative interpolation degree $k$; in other words there exists a globally nonnegative polynomial $p$ of degree $k$ such that $p(a_i) = a_i$ for all $i = 0, \ldots, k-1$.*

*Proof.* Let $q(x) = \prod_{i=0}^{k-1}(x-a_i)$ and note that $q'(0) = -A$ where $A = \prod_{i=1}^{k-1} a_i$. To use Proposition 3, we need to show that the polynomial

$$q(x) - q'(0)x = x\left[A + \prod_{i=1}^{k-1}(x-a_i)\right] \tag{11}$$

is nonnegative for all $x \in \mathbb{R}$. We first show that (11) is nonnegative for $x \in (0, a_{k-1})$. Let $x \in (0, a_{k-1})$ and let $j$ be the index in $\{0,1,\dots,k-2\}$ such that $a_j \le x \le a_{j+1}$. Then we have:

$$\begin{aligned}
-\prod_{i=1}^{k-1}(x-a_i) \le \left|\prod_{i=1}^{k-1}(x-a_i)\right| &= \prod_{i=1}^{j}(x-a_i)\cdot\prod_{i=j+1}^{k-1}(a_i-x)\\
&= [(x-a_1)(x-a_2)\dots(x-a_j)]\cdot[(a_{j+1}-x)\dots(a_{k-1}-x)]\\
&\overset{(a)}{\le} [(a_{j+1}-a_1)(a_{j+1}-a_2)\dots(a_{j+1}-a_j)]\cdot[(a_{j+1}-a_j)\dots(a_{k-1}-a_j)]\\
&\overset{(b)}{\le} (a_j a_{j-1}\dots a_1)(a_1\dots a_{k-1-j})\\
&\overset{(c)}{\le} (a_1\dots a_j)(a_{j+1}\dots a_{k-1}) = A
\end{aligned}$$

where in $(a)$ we used that $a_j \le x \le a_{j+1}$; in $(b)$ we used the subadditivity property of the sequence $(a_0,\dots,a_{k-1})$, and in $(c)$ we simply used the fact that $a_1 \le a_{j+1}, a_2 \le a_{j+2}, \dots, a_{k-1-j} \le a_{k-1}$. This shows that (11) is nonnegative for all $x \in (0, a_{k-1})$. Since (11) is also clearly nonnegative for all $x \le 0$ and $x \ge a_{k-1}$, we can thus use Proposition 3 to conclude the proof. □

***Application for the parity polytope:*** Consider the *parity polytope* $\mathrm{PAR}_n$ defined as the convex hull of points in $\{-1,1\}^n$ that have an even number of $-1$'s:

$$\mathrm{PAR}_n = \mathrm{conv}\left\{x \in \{-1,1\}^n \,:\, \prod_{i=1}^{n} x_i = 1\right\}. \tag{12}$$

It is known that the theta-rank of the parity polytope is exactly equal to $\lceil n/4 \rceil$, see [11, Corollary 5.7] (see also [6] for a proof of the lower bound). Using the interpolation argument given above for equispaced sequences, one can give another proof that the theta-rank of the parity polytope is at most $\lceil n/4 \rceil$. Indeed, it is not difficult to verify that the parity polytope is a $\lceil n/2 \rceil$-level polytope, and that the levels of each facet are *equispaced*. Thus, by Proposition 2 and since equispaced sequences of length $k$ have nonnegative interpolation degree $k$ (when $k$ is even) it follows that the theta-rank of the parity polytope is $\lceil n/4 \rceil$.

Any 2-level polytope has theta-rank one (see, e.g. [16]). One way to see this is to note that any sequence $0 = a_0 < a_1$ of length 2 has nonnegative interpolation degree 2. One can see this from the Lagrange interpolation argument given earlier, but perhaps more directly from Proposition 3. In this case the polynomial $q(x) = (x-a_0)(x-a_1) = x(x-a_1)$ is convex and so its graph is certainly above its linear approximation at $x = 0$.

Any sequence of length 4 has nonnegative interpolation degree either 4 or 6 (since the Lagrange interpolation argument constructs a nonnegative interpolant of degree 6). Furthermore, there is a simple characterization of those sequences of length 4 that have nonnegative interpolation degree 4.

PROPOSITION 5. *A sequence $0 = a_0 < a_1 < a_2 < a_3$ of length 4 has nonnegative interpolation degree 4 if and only if*

$$(a_1 + a_2 + a_3)^2 \le 4(a_1a_2 + a_1a_3 + a_2a_3). \tag{13}$$

*Proof.* We appeal to Proposition 3. In this case $q(x) - q'(0)x = x^2(x^2 - (a_1+a_2+a_3)x + (a_1a_2 + a_1a_3 + a_2a_3))$. This is nonnegative for all $x$ if and only if the quadratic polynomial $x^2 - (a_1+a_2+a_3)x + (a_1a_2 + a_1a_3 + a_2a_3)$ is nonnegative for all $x$. This occurs precisely when the discriminant is nonpositive, i.e.

$$(a_1+a_2+a_3)^2 - 4(a_1a_2 + a_1a_3 + a_2a_3) \leq 0.$$

□

Geometrically, the set of $(a_1, a_2, a_3)$ satisfying (13) is the largest convex quadratic cone centered at $(1,1,1)$ that fits inside the nonnegative orthant. It is remarkable that these sequences form a convex cone.

It would be interesting to understand, for general $k$, the set of sequences $0 = a_0 < a_1 < \cdots < a_{k-1}$ of length $k$ with nonnegative interpolation degree $k$. For example, motivated by the construction of psd lifts of polytopes we pose the following problem.

QUESTION 2. Give a simple (i.e., easy-to-check) sufficient condition for a sequence $0 = a_0 < a_1 < \cdots < a_{k-1}$ to have nonnegative interpolation degree $k$.

In this section we worked with ordered sequences $(a_i)_{i=0,\ldots,k-1}$ that start at $a_0 = 0$ and we considered the problem of finding a nonnegative polynomial $p$ that takes the same values as the linear polynomial $x$ at the points $a_0, \ldots, a_{k-1}$. For the regular polygon it will be convenient to work with shifted sequences, and with linear polynomials that have negative slope. We record the following result which we will use later, and which is an equivalent formulation of Proposition 3:

PROPOSITION 6. *Let $k$ be an even integer and let $a_0 > a_1 > \cdots > a_{k-1}$ be $k$ points on the real axis. Let $l(x)$ be a* decreasing *linear function with $l(a_i) \geq 0$ for $i = 1, \ldots, k-1$ and $l(a_0) = 0$. Let $q$ be the monic polynomial that vanishes on the $a_i$'s, $q(x) = \prod_{i=0}^{k-1}(x - a_i)$.*

*If the curve of $q(x)$ is above its tangent at $x = a_0$ then there exists a polynomial $p$ of degree $k$ that is globally nonnegative and such that $p(a_i) = l(a_i)$ for all $i = 0, \ldots, k-1$.*

**3.2. Application to the theta-rank of regular polygons** We now go back to the regular $N$-gon and use the results from the previous section to show that the theta-rank of the $N$-gon is $\lceil N/4 \rceil$. We focus on the facet inequality of the regular $N$-gon introduced earlier:

$$\ell(x,y) = \cos(\pi/N) - x\cos(\pi/N) - y\sin(\pi/N). \tag{14}$$

Our main result in this section is:

THEOREM 6. *The linear function $\ell(x,y)$ agrees with a sum-of-squares polynomial of degree $2\lceil N/4 \rceil$ on the vertices of the $N$-gon, i.e., there exist polynomials $h_i \in \mathbb{R}[x,y]$ with $\deg h_i \leq \lceil N/4 \rceil$ such that*

$$\cos(\pi/N) - x\cos(\pi/N) - y\sin(\pi/N) = \sum_i h_i(x,y)^2 \quad \forall (x,y) \in \mathcal{X}_N.$$

*Proof.* The proof of this theorem relies mainly on Proposition 6. We consider first the case where $N$ is a multiple of 4; the other cases are similar but slightly more technical and are treated in Appendix A. Thus assume $N = 4m$ where $m$ is an integer. Define

$$a_i = \cos\left(\frac{(2i+1)\pi}{4m}\right) \quad i = 0, \ldots, 2m-1$$

and note that $a_0 > a_1 > \cdots > a_{2m-1}$. Let $l$ be the univariate linear polynomial $l(x) = a_0 - x$. Observe that $l(a_0), l(a_1), \ldots, l(a_{2m-1})$ are precisely the values that the linear functional $\ell(x,y) = \cos(\pi/4m) - x\cos(\pi/4m) - y\sin(\pi/4m)$ takes on the vertices of the regular $4m$-gon (see Example 1). Consider the polynomial $q$ which vanishes at the $a_i$'s:

$$q(x) = \prod_{i=0}^{2m-1}(x - a_i) = \prod_{i=0}^{2m-1}\left(x - \cos\left(\frac{(2i+1)\pi}{4m}\right)\right). \tag{15}$$

Note that, up to scaling, the polynomial $q$ is nothing but the Chebyshev polynomial of order $2m$. Indeed recall that the Chebyshev polynomial of degree $r$ has roots $\cos((2i+1)\pi/2r)$, $i = 0,\dots,r-1$ and coincides with the function $\cos(r\arccos(x))$ on $x \in [-1,1]$. Using this observation it is not difficult to show, by properties of Chebyshev polynomials, that $q$ satisfies the condition of Proposition 6, namely that the curve of $q$ lies above its linear approximation at $x = a_0$ (cf. Figure 3 for a picture ($N = 8$) and Lemma 1 in Appendix A for a formal proof).

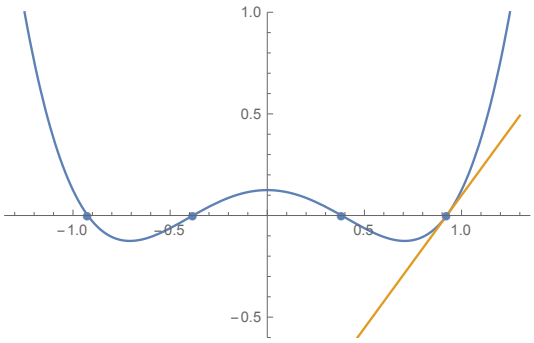


FIGURE 3. Plot of the polynomial $q(x)$ of Equation (15) for $2m = 4$ and its tangent at $x = a_0 = \cos(\pi/8)$. We see that the tangent is always below the curve of $q$ (for a proof, cf. Lemma 1 in Appendix A). Thus from Proposition 3 there is a polynomial $p$ of degree 4 that is globally nonnegative and such that $p(a_i) = a_0 - a_i$ for all $i = 0,\dots,2m-1$ where $a_i = \cos((2i+1)\pi/(4m))$.

Thus from Proposition 6 it follows that there exists a nonnegative polynomial $p$ of degree $2m$ such that $p(a_i) = l(a_i) = a_0 - a_i$ for all $i = 0,\dots,2m-1$. Since nonnegative univariate polynomials are sums of squares we can write $p = \sum_i g_i^2$ where $g_i$ are polynomials of degree at most $m$. Thus it follows that for any vertex $(x,y)$ of the regular $N$-gon, we can write:

$$\begin{aligned}\ell(x,y) &= a_0 - x\cos(\pi/4m) - y\sin(\pi/4m)\\ &= l(x\cos(\pi/4m) + y\sin(\pi/4m))\\ &\overset{(*)}{=} p(x\cos(\pi/4m) + y\sin(\pi/4m))\\ &= \sum_i g_i(x\cos(\pi/4m) + y\sin(\pi/4m))^2 \end{aligned} \tag{16}$$

where in $(*)$ we used the fact that $x\cos(\pi/4m) + y\sin(\pi/4m) \in \{a_i\}_{i=0,\dots,2m-1}$ for $(x,y) \in \mathcal{X}_N$ and that $p$ agrees with $l$ on the $a_i$'s. Defining $h_i(x,y) = g_i(x\cos(\pi/4m) + y\sin(\pi/4m))$ establishes the result in the case where $N$ is a multiple of four.

The proof when $N$ is not a multiple of four is slightly more technical for two reasons: the polynomial $q(x)$ is not necessarily a Chebyshev polynomial (though it is related), and the number of values that the facet $\ell(x,y)$ takes is not necessarily even. These cases are treated in detail in Appendix A. □

**4. Construction** In this section we construct two equivariant psd lifts of the regular $2^n$-gon. The first is a $(\mathbf{H}_+^3)^{n-1}$-lift, i.e., it expresses the regular $2^n$-gon using $n-1$ linear matrix inequalities of size $3\times 3$ each, whereas the second is a $\mathbf{H}_+^{2n-1}$-lift and uses a single linear matrix inequality of size $2n-1$. Both of our constructions arise from a sum of squares certificate of the nonnegativity of $\ell = \cos(\pi/2^n)c_0 - \cos(\pi/2^n)c_1 - \sin(\pi/2^n)s_1$ (see Proposition 7 to follow). Applying Theorem 3 in two different ways then gives the two different equivariant psd lifts of the regular $2^n$-gon.

We now establish the following sum of squares representation of the linear functional $\ell$.

PROPOSITION 7. *Let $\ell = \cos(\pi/2^n)c_0 - \cos(\pi/2^n)c_1 - \sin(\pi/2^n)s_1 \in \mathbb{C}^{2^n}$. Then we have the following sum-of-squares certificate for $\ell$:*

$$\ell = \sum_{k=0}^{n-2} \frac{\sin\left(\frac{\pi}{2^n}\right)}{2^k \sin\left(2^{k+1}\cdot\frac{\pi}{2^n}\right)} \left(\cos\left(\frac{\pi}{2^{n-k}}\right)c_0 - \cos\left(\frac{\pi}{2^{n-k}}\right)c_{2^k} - \sin\left(\frac{\pi}{2^{n-k}}\right)s_{2^k}\right)^2.$$

*Proof.* To prove that $\ell$ has such a decomposition, it is sufficient to establish that

$$\frac{\cos\left(\frac{\pi}{2^n}\right) - \cos\left(\frac{\pi}{2^n}\right)\cos(\phi) - \sin\left(\frac{\pi}{2^n}\right)\sin(\phi)}{\sin\left(\frac{\pi}{2^n}\right)} = -\frac{\sin(2^{n-1}\phi)}{2^{n-1}} + \sum_{k=0}^{n-2} \frac{\left(\cos\left(2^k\cdot\frac{\pi}{2^n}\right) - \cos\left(2^k\cdot\frac{\pi}{2^n}\right)\cos(2^k\phi) - \sin\left(2^k\cdot\frac{\pi}{2^n}\right)\sin(2^k\phi)\right)^2}{2^k \sin\left(2^{k+1}\cdot\frac{\pi}{2^n}\right)} \tag{17}$$

for all $n \geq 1$ and all $\phi \in \mathbb{R}$. This is enough to prove Proposition 7 because $c_k$ (respectively $s_k$) is the restriction of $\cos(k\phi)$ (respectively $\sin(k\phi)$) to the angles $\phi = \theta_k = \frac{2k\pi}{2^n}$ for $k = 0, 1, \ldots, 2^n - 1$ corresponding to the vertices of the regular $2^n$-gon, and $s_{2^{n-1}} = 0$ in $\mathbb{C}^{2^n}$. By using the change of variables $\theta = \phi - \frac{\pi}{2^n}$ and the identity $\cos(2^k\theta) = \cos(2^k\phi)\cos(2^k\cdot\pi/2^n) + \sin(2^k\phi)\sin(2^k\cdot\pi/2^n)$ (for positive integers $k$), we see that (17) is equivalent to

$$\frac{\cos\left(\frac{\pi}{2^n}\right) - \cos(\theta)}{\sin\left(\frac{\pi}{2^n}\right)} = -\frac{\cos(2^{n-1}\theta)}{2^{n-1}} + \sum_{k=0}^{n-2} \frac{\left(\cos\left(2^k\cdot\frac{\pi}{2^n}\right) - \cos(2^k\theta)\right)^2}{2^k \sin\left(2^{k+1}\cdot\frac{\pi}{2^n}\right)} \qquad \text{for all } n \geq 1 \text{ and all } \theta \in \mathbb{R}. \tag{18}$$

We now establish the identity in (18) by induction. For the base case, observe that $\frac{\cos(\pi/2)-\cos(\theta)}{\sin(\pi/2)} = -\cos(\theta)$ which agrees with (18) for $n = 1$.

To take the induction step, we first prove the following simple trigonometric identity that holds for all $N \geq 3$ and all $\theta$:

$$\frac{\cos\left(\frac{\pi}{N}\right) - \cos(\theta)}{\sin\left(\frac{\pi}{N}\right)} = \frac{\left(\cos\left(\frac{\pi}{N}\right) - \cos(\theta)\right)^2}{\sin\left(2\cdot\frac{\pi}{N}\right)} + \frac{1}{2}\cdot\frac{\cos\left(2\cdot\frac{\pi}{N}\right) - \cos(2\theta)}{\sin\left(2\cdot\frac{\pi}{N}\right)}. \tag{19}$$

To prove this identity, we start with the right-hand side, expand the square and use the identity $\cos(2t) = 2\cos^2(t) - 1$, then rewrite the denominator using $\sin(2t) = 2\sin(t)\cos(t)$, i.e.,

$$\begin{aligned}\text{RHS} = \frac{\left[\cos^2\left(\frac{\pi}{N}\right) - 2\cos\left(\frac{\pi}{N}\right)\cos(\theta) + \cos^2(\theta)\right] + \cos^2\left(\frac{\pi}{N}\right) - \cos^2(\theta)}{\sin\left(2\cdot\frac{\pi}{N}\right)} &= \frac{2\cos\left(\frac{\pi}{N}\right)\left(\cos\left(\frac{\pi}{N}\right) - \cos(\theta)\right)}{\sin\left(2\cdot\frac{\pi}{N}\right)} \\ &= \frac{\cos\left(\frac{\pi}{N}\right) - \cos(\theta)}{\sin\left(\frac{\pi}{N}\right)}\end{aligned}$$

which is exactly the left-hand side.

With (19) established, we return to our argument by induction. Assume that (17) holds for some $n \geq 1$. By first using (19) (with $N = 2^{n+1}$), then applying the induction hypothesis (17) evaluated at $2\theta$ we have that:

$$\begin{aligned}\frac{\cos\left(\frac{\pi}{2^{n+1}}\right) - \cos(\theta)}{\sin\left(\frac{\pi}{2^{n+1}}\right)} &= \frac{\left(\cos\left(\frac{\pi}{2^{n+1}}\right) - \cos(\theta)\right)^2}{\sin\left(\frac{\pi}{2^n}\right)} + \frac{1}{2}\cdot\frac{\cos\left(\frac{\pi}{2^n}\right) - \cos(2\theta)}{\sin\left(\frac{\pi}{2^n}\right)} \\ &= \frac{\left(\cos\left(2^0\cdot\frac{\pi}{2^{n+1}}\right) - \cos(2^0\cdot\theta)\right)^2}{2^0\sin\left(2^{0+1}\cdot\frac{\pi}{2^{n+1}}\right)} + \frac{1}{2}\left[\sum_{\ell=0}^{n-2}\frac{\left(\cos\left(2^\ell\cdot\frac{\pi}{2^n}\right) - \cos(2^\ell(2\theta))\right)^2}{2^\ell\sin\left(2^{\ell+1}\cdot\frac{\pi}{2^n}\right)} - \frac{\cos(2^{n-1}(2\theta))}{2^{n-1}}\right] \\ &= \frac{\left(\cos\left(2^0\cdot\frac{\pi}{2^{n+1}}\right) - \cos(2^0\cdot\theta)\right)^2}{2^0\sin\left(2^{0+1}\cdot\frac{\pi}{2^{n+1}}\right)} + \left[\sum_{\ell=0}^{n-2}\frac{\left(\cos\left(2^{\ell+1}\cdot\frac{\pi}{2^{n+1}}\right) - \cos(2^{\ell+1}\theta)\right)^2}{2^{\ell+1}\sin\left(2^{\ell+2}\cdot\frac{\pi}{2^{n+1}}\right)} - \frac{\cos(2^n\theta)}{2^n}\right] \\ &= \sum_{k=0}^{n-1}\frac{\left(\cos\left(2^k\cdot\frac{\pi}{2^{n+1}}\right) - \cos(2^k\theta)\right)^2}{2^k\sin\left(2^{k+1}\cdot\frac{\pi}{2^{n+1}}\right)} - \frac{\cos(2^n\theta)}{2^n}\end{aligned}$$

completing the proof. □

In the context of Theorem 3 there are two natural ways to interpret the sum of squares decompostion of $\ell$ given in Proposition 7. Both of these lead to different equivariant lifts of the regular $2^n$-gon. In Sections 4.1 and 4.2 we describe these lifts.

**4.1. An equivariant $(\mathbf{H}_+^3)^{n-1}$-lift of the regular $2^n$-gon** We can apply Theorem 3 with the sum-of-squares certificate of Proposition 7 to get a Hermitian psd lift of the regular $N$-gon. Indeed the certificate of Proposition 7 has the form:

$$\ell = \sum_{i=0}^{n-2} \sum_{j=1}^{1} |h_{ij}|^2$$

where $h_{i1} \in \mathbb{C}e_0 \oplus \mathbb{C}e_{2^i} \oplus \mathbb{C}e_{-2^i}$ for $i = 0, \dots, n-2$. Thus by applying Theorem 3 we get the following Hermitian psd lift of the regular $2^n$-gon:

$$\begin{aligned} \operatorname{conv}(\mathcal{X}_{2^n}) = \Bigg\{ & (\operatorname{Re}[y_0], \operatorname{Im}[y_0]) : \exists y_1, \dots, y_{n-2} \in \mathbb{C}, y_{n-1} \in \mathbb{R} \text{ such that} \\ & \begin{bmatrix} 1 & y_{k-1} & \overline{y_{k-1}} \\ \overline{y_{k-1}} & 1 & \overline{y_k} \\ y_{k-1} & y_k & 1 \end{bmatrix} \in \mathbf{H}_+^3 \quad \text{for } k = 1, 2, \dots, n-2 \\ & \text{and } \begin{bmatrix} 1 & y_{n-2} & \overline{y_{n-2}} \\ \overline{y_{n-2}} & 1 & y_{n-1} \\ y_{n-2} & y_{n-1} & 1 \end{bmatrix} \in \mathbf{H}_+^3 \Bigg\}. \end{aligned} \tag{20}$$

***Real equivariant psd lift*** Observe that Proposition 7 actually gives a *real* sum-of-squares certificate of $\ell$, i.e., the functions $h_i$ in $\ell = \sum_i |h_i|^2$ are real-valued. This sum-of-squares certificate can be used to get a psd lift of the regular $2^n$-gon using the cone of real symmetric psd matrices (instead of Hermitian psd matrices). The real psd lift can be shown to take the form ($\mathbf{S}_+^3$ denotes the cone of $3 \times 3$ real symmetric positive semidefinite matrices):

$$\begin{aligned} \operatorname{conv}(\mathcal{X}_{2^n}) = \Bigg\{ & (x_0, y_0) : \exists (x_i, y_i)_{i=1}^{n-2}, x_{n-1} \in \mathbb{R}, \quad \begin{bmatrix} 1 & x_{k-1} & y_{k-1} \\ x_{k-1} & \frac{1+x_k}{2} & \frac{y_k}{2} \\ y_{k-1} & \frac{y_k}{2} & \frac{1-x_k}{2} \end{bmatrix} \in \mathbf{S}_+^3 \quad \text{for } k = 1, 2, \dots, n-2 \\ & \text{and} \quad \begin{bmatrix} 1 & x_{n-2} & y_{n-2} \\ x_{n-2} & \frac{1+x_{n-1}}{2} & 0 \\ y_{n-2} & 0 & \frac{1-x_{n-1}}{2} \end{bmatrix} \in \mathbf{S}_+^3 \Bigg\}. \end{aligned} \tag{21}$$

**4.2. An equivariant $\mathbf{H}_+^{2n-1}$-lift of the regular $2^n$-gon** By applying Theorem 3 in a different way we can get a different Hermitian psd lift of the regular $N$-gon. Indeed note that we can write the sum-of-squares certificate of Proposition 7 as:

$$\ell = \sum_{i=1}^{1} \sum_{j=0}^{n-2} h_{ij}^2$$

where $h_{1j} \in \bigoplus_{k \in K} (\mathbb{C}e_k \oplus \mathbb{C}e_{-k})$ where $K = \{0, 2^0, 2^1, \dots, 2^{n-2}\}$. Note that $|K| = 2n-1$. With this decomposition we get the following $\mathbf{H}_+^{2n-1}$-lift of the regular $2^n$-gon:

$$\operatorname{conv}(\mathcal{X}_{2^n}) = \left\{ (\operatorname{Re}[y_1], \operatorname{Im}[y_1]) : y_0 = 1 \text{ and } [y_{k'-k}]_{k,k' \in K} \in \mathbf{H}_+^{2n-1} \right\}.$$

For example for $N = 16$ we get that $\text{conv}(\mathcal{X}_{16})$ is the set of $(\text{Re}[y_1], \text{Im}[y_1]) \in \mathbb{R}^2$ such that the following $7 \times 7$ Hermitian matrix is positive semidefinite:

$$\begin{bmatrix} 1 & y_1 & \overline{y_1} & y_2 & \overline{y_2} & y_4 & \overline{y_4} \\ \overline{y_1} & 1 & \overline{y_2} & y_1 & \overline{y_3} & y_3 & \overline{y_5} \\ y_1 & y_2 & 1 & y_3 & \overline{y_1} & y_5 & \overline{y_3} \\ \overline{y_2} & \overline{y_1} & \overline{y_3} & 1 & \overline{y_4} & y_2 & \overline{y_6} \\ y_2 & y_3 & y_1 & y_4 & 1 & y_6 & \overline{y_2} \\ \overline{y_4} & \overline{y_3} & \overline{y_5} & \overline{y_2} & \overline{y_6} & 1 & y_8 \\ y_4 & y_5 & y_3 & y_6 & y_2 & y_8 & 1 \end{bmatrix}.$$

Note that the auxiliary variables are $y_2, y_3, y_4, y_5, y_6, y_8$ and that $y_8$ is a real variable whereas the others are complex.

***Real equivariant psd lift*** Like in the previous section, since the sum-of-squares certificate constructed in Proposition 7 is real, one can obtain a version of the lift given above over the cone of real symmetric positive semidefinite matrices. For example for the case $N = 16$ we get that the regular 16-gon is the set of $(x_1, y_1)$ such that the following $7 \times 7$ real symmetric matrix is positive semidefinite:

$$\begin{bmatrix} 2 & 2x_1 & 2y_1 & 2x_2 & 2y_2 & 2x_4 & 2y_4 \\ 2x_1 & 1+x_2 & y_2 & x_1+x_3 & y_1+y_3 & x_3+x_5 & y_3+y_5 \\ 2y_1 & y_2 & 1-x_2 & -y_1+y_3 & x_1-x_3 & -y_3+y_5 & x_3-x_5 \\ 2x_2 & x_1+x_3 & -y_1+y_3 & 1+x_4 & y_4 & x_2+x_6 & y_2+y_6 \\ 2y_2 & y_1+y_3 & x_1-x_3 & y_4 & 1-x_4 & -y_2+y_6 & x_2-x_6 \\ 2x_4 & x_3+x_5 & -y_3+y_5 & x_2+x_6 & -y_2+y_6 & 1+x_8 & 0 \\ 2y_4 & y_3+y_5 & x_3-x_5 & y_2+y_6 & x_2-x_6 & 0 & 1-x_8 \end{bmatrix}.$$

**5. Lower bound on equivariant psd lifts of regular polygons** In this section we are interested in obtaining lower bounds on equivariant psd lifts of the regular $N$-gon. The main result of this section is the following:

THEOREM 2. *Any Hermitian psd lift of the regular $N$-gon that is equivariant with respect to $\text{Rot}_N$ has size at least $\ln(N/2)$.*

Using the relation between equivariant psd lifts of $\text{conv}(\mathcal{X}_N)$ and sum-of-squares certificates for $\ell$ (see Theorem 4) this section is dedicated to proving Theorem 7:

THEOREM 7. *Let $\ell \in \mathbb{C}^N$ be as defined in (5) and assume that we can write*

$$\ell = \sum_i |h_i|^2 \quad \text{where} \quad h_i \in \bigoplus_{k \in K} \mathbb{C} e_k \ \forall i \tag{22}$$

*for some set $K \subseteq \mathbb{Z}_N$. Then necessarily $|K| \geq \ln(N/2)$.*

Theorem 2 then follows directly from Theorems 7 and 4. We introduce some notations which will be used throughout the section.

DEFINITION 5. Given $h \in \mathbb{C}^N$ and $K \subseteq \mathbb{Z}_N$, we say that $h$ is *supported on* $K$ and we write $\text{supp}\, h \subseteq K$ if $h \in \bigoplus_{k \in K} \mathbb{C} e_k$.

DEFINITION 6. A set $K \subseteq \mathbb{Z}_N$ is called *sos-valid* if $\ell$ admits a sum-of-squares certificate $\ell = \sum_i |h_i|^2$ where $\text{supp}\, h_i \subseteq K$ for all $i$.

Our proof of Theorem 7 proceeds in two steps. In the first step, we give necessary conditions in terms of the "geometry" for a set $K$ to be sos-valid: we show that if the elements in $K$ can be *clustered* in a certain way then $K$ is not sos-valid. In the second step we propose an algorithm to cluster any given set $K$, and we prove that our algorithm finds a valid clustering whenever the set $K$ is small enough, i.e., whenever $|K| < \ln(N/2)$.

**5.1. Necessary conditions for a set to be sos-valid** In this section we give a necessary condition on the "geometry" of a set $K$ to be sos-valid. Before stating the theorem, we make some observations and definitions:

First, observe that if $K$ is a set that is sos-valid, then any *translation* $K' = K + t$ of $K$ is also sos-valid, where $t \in \mathbb{Z}_N$. This is because if $\ell = \sum_i |h_i|^2$ where $\operatorname{supp} h_i \subseteq K$, then we also have $\ell = \sum_i |h'_i|^2$ where $h'_i = e_t h_i$ are supported on $K'$ (since $e_t e_k = e_{t+k}$).

Second, it is useful to think of $\mathbb{Z}_N$ as the nodes of a cycle graph of length $N$, and of a set of frequencies $K \subseteq \mathbb{Z}_N$ as a subset of the nodes of this graph. For example Figure 4 shows a set $K$ with $|K| = 7$ for the $N = 12$-gon (the elements of $K$ are the black dots). Note that since the property of being sos-valid is invariant under translation, the cycle graph need not be labeled. The only information that matters are the relative distances of the elements of $K$ with respect to each other.

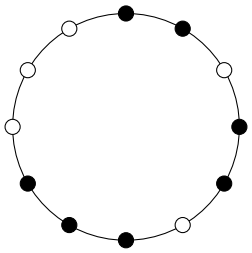

FIGURE 4. A set of frequencies $K$ for the regular 12-gon.

We endow $\mathbb{Z}_N$ with the natural distance $d$ on the cycle graph. The distance between two frequencies $k, k' \in \mathbb{Z}_N$ is denoted by $d(k, k')$; also if $C, C'$ are two subsets of $\mathbb{Z}_N$ we let

$$d(C, C') = \min_{k \in C, k' \in C'} d(k, k').$$

If $x \in \mathbb{Z}_N$ and $r$ is a positive integer, we can define the ball $B(x, r)$ centered at $x$ and with radius $r$ to be the set $B(x, r) := \{y \in \mathbb{Z}_N : d(x, y) \leq r\}$. We also let $[x, x+r]$ be the interval $\{x, x+1, \ldots, x+r\} \subseteq \mathbb{Z}_N$. Note that the ball centered at $x$ of radius $r$ is simply the interval $[x - r, x + r]$.

In Section 3, Proposition 1 we showed that the linear functional $\ell$ of the regular $N$-gon does not admit any sum-of-squares certificate with polynomials of degree smaller than $N/4$. One can state this result in a different way as follows: If $K$ is a set of frequencies that is included in a ball of radius smaller than $N/4$, then $K$ is not sos-valid. The goal of this section is to extend this result and give a more general necessary condition for a set $K$ to be sos-valid in terms of its geometry.

To state the main theorem, it will be more convenient to work with diameters instead of radii of balls (mainly to avoid the issue of dividing by two). We introduce the notion of *in-diameter* of a set $K$ which is essentially twice the radius of the smallest ball containing $K$. More formally we have:

DEFINITION 7. Let $K \subseteq \mathbb{Z}_N$. We define the *in-diameter* of $K$, denoted $\operatorname{indiam}(K)$ to be the smallest positive integer $r$ such that $K$ is included in an interval of the form $[x, x+r]$ where $x \in \mathbb{Z}_N$.

REMARK 4. Note that the in-diameter of a set $K$ is in general different from the usual notion of *diameter* (largest distance between two elements in $K$). Note for example that $\operatorname{indiam}(\mathbb{Z}_N) = N$ whereas the diameter of $\mathbb{Z}_N$ is equal to $\lfloor N/2 \rfloor$.

We are now ready to state the main result of this section:

THEOREM 8. *Let $N$ be an integer and let $K \subseteq \mathbb{Z}_N$ be a set of frequencies. Assume that $K$ can be decomposed into disjoint clusters $(C_\alpha)_{\alpha \in A}$:*

$$K = \bigcup_{\alpha \in A} C_\alpha,$$

*such that the following holds for some* $1 \leq \gamma < N/2$*:*
*(i) For any* $\alpha \in A$*,* $C_\alpha$ *has in-diameter* $\leq \gamma$*.*
*(ii) For any* $\alpha \neq \alpha'$*,* $d(C_\alpha, C_{\alpha'}) > \gamma$*.*
*Then the set* $K$ *is* not *sos-valid (i.e., it is* not *possible to write the linear function* $\ell$ *as a sum of squares of functions supported on* $K$*).*

*Proof.* To prove this theorem, we will construct a linear functional $\mathcal{L}$ on $\mathbb{C}^N$ such that:
(a) $\mathcal{L}(\ell) < 0$, and;
(b) for any $h$ supported on $K$ we have $\mathcal{L}(|h|^2) \geq 0$.
Clearly this will show that we cannot have $\ell = \sum_i |h_i|^2$ where $\operatorname{supp} h_i \subseteq K$.

We first introduce a piece of notation that will be needed for the definition of $\mathcal{L}$: Given $k \in \mathbb{Z}_N$, we let $k \bmod N$ be the unique element in

$$\Big\{-\lceil N/2 \rceil + 1, \ldots, \lfloor N/2 \rfloor\Big\}$$

that is equal to $k$ modulo $N$. The main property that will be used about this operation is the following, which can be verified easily: If $k, k' \in [0, \gamma]$ where $\gamma < N/2$ then:

$$(k' - k) \bmod N = (k' \bmod N) - (k \bmod N). \tag{23}$$

Let $p = e^{i\pi/N}$ and note that $p$ does not belong to our regular $N$-gon. We define the linear functional $\mathcal{L} : \mathbb{C}^N \to \mathbb{C}$ as follows, for all $k \in \mathbb{Z}_N$:

$$\mathcal{L}(e_k) = \begin{cases} p^{k \bmod N} & \text{if } d(0,k) \leq \gamma \\ 0 & \text{else.} \end{cases} \tag{24}$$

Note that the map $\mathcal{L}$ can be interpreted as the composition of two maps:

$$\mathcal{L} = \mathsf{Eval}_p \circ \mathcal{E}$$

where $\mathcal{E}$ is a map that extrapolates a function $h \in \mathbb{C}^N$ defined on the vertices of the $N$-gon to a function on the unit circle, and $\mathsf{Eval}_p$ is a map that evaluates a function on the unit circle to the point $p$. The extrapolation map $\mathcal{E}$ is defined on the Fourier basis as follows: $\mathcal{E}(e_k)(z) = z^{k \bmod N}$ if $d(0,k) \leq \gamma$ and 0 otherwise, for $z$ in the unit circle.

We now prove that $\mathcal{L}$ satisfies properties (a) and (b) above.

(a) It is easy to see that $\mathcal{L}(\ell) < 0$. Indeed since $\gamma \geq 1$ we have $\mathcal{L}(e_1) = e^{i\pi/N}$ and $\mathcal{L}(e_{-1}) = e^{-i\pi/N}$ which implies that:

$$\mathcal{L}(\ell) = \mathcal{L}\Big(\cos(\pi/N)e_0 - (e^{-i\pi/N}e_1 + e^{i\pi/N}e_{-1})/2\Big) = \cos(\pi/N) - 1 < 0.$$

(b) We now show that if $h$ is a function supported on $K$, then $\mathcal{L}(|h|^2) \geq 0$. Since $K = \cup_{\alpha \in A} C_\alpha$, we can write

$$h = \sum_{k \in K} h_k e_k = \sum_{\alpha \in A} \sum_{k \in C_\alpha} h_k e_k.$$

Thus

$$|h|^2 = h^* h = \underbrace{\sum_{\alpha \in A} \left| \sum_{k \in C_\alpha} h_k e_k \right|^2}_{P} + \underbrace{\sum_{\alpha \neq \alpha'} \sum_{k \in C_\alpha, k' \in C_{\alpha'}} h_k^* h_{k'} e_k^* e_{k'}}_{Q}. \tag{25}$$

Let $P$ and $Q$ be the first and second terms in the equation above. We will show that $\mathcal{L}(Q) = 0$ and that $\mathcal{L}(P) \geq 0$. Observe that if $k \in C_\alpha$ and $k' \in C_{\alpha'}$ where $\alpha \neq \alpha'$ then we have:

$$\mathcal{L}(e_k^* e_{k'}) = \mathcal{L}(e_{k'-k}) = 0$$

where the last equality follows since $d(k'-k, 0) = d(k', k) > \gamma$ (cf. assumption (ii) on the clustering). Thus this shows that $\mathcal{L}(Q) = 0$.

We will now show that $\mathcal{L}(P) \geq 0$, by showing that for any $\alpha \in A$ we have

$$\mathcal{L}\left(\left|\sum_{k \in C_\alpha} h_k e_k\right|^2\right) \geq 0.$$

Let $\alpha \in A$. By assumption (i) on the clustering, we know that the in-diameter of $C_\alpha$ is $\leq \gamma$, i.e., that $C_\alpha$ is included in an interval $[x, x+\gamma]$. Note that since

$$\left|\sum_{k \in C_\alpha} h_k e_k\right|^2 = \left|e_{-x} \sum_{k \in C_\alpha} h_k e_k\right|^2 = \left|\sum_{k \in C_\alpha} h_k e_{k-x}\right|^2$$

we can assume without loss of generality that $x = 0$. Now since $C_\alpha \subseteq [0, \gamma]$, we have from (23) that for any $k, k' \in C_\alpha$:

$$(k'-k) \bmod N = (k' \bmod N) - (k \bmod N) \tag{26}$$

Using this we have:

$$\begin{aligned}\mathcal{L}\left(\left|\sum_{k \in C_\alpha} h_k e_k\right|^2\right) = \sum_{k,k' \in C_\alpha} h_k^* h_{k'} \mathcal{L}(e_{k'-k}) &\overset{(a)}{=} \sum_{k,k' \in C_\alpha} h_k^* h_{k'} p^{(k'-k) \bmod N} \\ &\overset{(b)}{=} \sum_{k,k' \in C_\alpha} h_k^* h_{k'} p^{k' \bmod N} p^{-(k \bmod N)} \\ &= \left|\sum_{k \in C_\alpha} h_k p^{k \bmod N}\right|^2 \geq 0\end{aligned}$$

where in $(a)$ we used the fact that $d(0, k'-k) = d(k', k) \leq \gamma$ and in $(b)$ we used identity (26). Thus this shows that $\mathcal{L}(|h|^2) \geq 0$ for all $h$ supported on $C_\alpha$, which implies that $\mathcal{L}(P) \geq 0$ (since $P = \sum_{\alpha \in A} \left|\sum_{k \in C_\alpha} h_k e_k\right|^2$) which is what we wanted.

□

Remark 5. To illustrate the previous theorem consider the following two simple applications:

- Note that the lower bound of $N/4$ on the theta-rank of the $N$-gon (cf. Proposition 1 in Section 3) can be obtained as a direct corollary of Theorem 8. Indeed if $K$ is contained in the open interval $(-\lceil N/4 \rceil, \lceil N/4 \rceil)$, then the in-diameter of $K$ is $< N/2$ which means that if we consider $K$ as a single cluster, it satisfies conditions (i) and (ii) of the theorem with $\gamma = \text{indiam}(K)$. Thus such a $K$ is not sos-valid.
- We can also give another simple application of the previous theorem: Assume $K$ is a set of frequencies that has no two consecutive frequencies, i.e., for any $k, k' \in K$ where $k \neq k'$ we have $d(k, k') \geq 2$. It is not hard to see that such a set $K$ cannot be sos-valid: indeed if $h$ is a function supported on $K$, then the expansion of $|h|^2$ does not have any term involving the frequencies $e_1$ or $e_{-1}$. Thus it is not possible to write $\ell$ as a sum-of-squares of elements supported on such $K$. This simple fact can be obtained as a consequence of Theorem 8 if we consider each frequency of $K$ as its own cluster (i.e., we write $K = \cup_{k \in K} \{k\}$) and conditions (i) and (ii) of the theorem are satisfied with $\gamma = 1$.

**5.2. An algorithm to find valid clusterings and a logarithmic lower bound** We now study sets $K$ which admit a clustering that satisfies points (i) and (ii) of Theorem 8. The main purpose of this section is to show that any set $K$ with $|K| < \ln(N/2)$ admits such a clustering, which implies that it cannot be sos-valid. This would thus show that any $\mathrm{Rot}_N$-equivariant Hermitian psd lift of the regular $N$-gon has to have size at least $\ln(N/2)$.

For convenience we call a *valid clustering* of a set $K$, any clustering that satisfies points (i) and (ii) of Theorem 8. We state this in the following definition for future reference:

DEFINITION 8. Let $K \subseteq \mathbb{Z}_N$. We say that $K$ has a *valid clustering* if $K$ can be decomposed into disjoint clusters $(C_\alpha)_{\alpha \in A}$:

$$K = \bigcup_{\alpha \in A} C_\alpha,$$

such that the following holds for some $1 \leq \gamma < N/2$:

(i) For any $\alpha \in A$, $C_\alpha$ has in-diameter $\leq \gamma$.

(ii) For any $\alpha \neq \alpha'$, $d(C_\alpha, C_{\alpha'}) > \gamma$.

We propose a simple greedy algorithm to search for a valid clustering for any set $K \subseteq \mathbb{Z}_N$: We start with each point of $K$ in its own cluster and at each iteration we merge the two closest clusters. We keep doing this until we get a clustering that satisfies the required condition, or until all the points are in the same cluster. We show in this section that if the number of points of $K$ is small enough, if $|K| < \ln(N/2)$, then this algorithm terminates by producing a valid clustering of $K$. For reference we describe the algorithm more formally in Algorithm 1.

**Algorithm 1** Algorithm to produce a clustering of a set $K$

**Input:** A set $K \subseteq \mathbb{Z}_N$

**Output:** A *valid clustering* of $K$ (in the sense of Definition 8) or "0" if no valid clustering found.

• Consider initial clustering where each element of $K$ is in its own cluster. If this clustering is already valid (which is equivalent to say that for any distinct elements $k, k' \in K$ we have $d(k, k') \geq 2$) then output this clustering as a valid clustering with parameter $\gamma = 1$.

• Precompute the pairwise distances between points in $K$ and sort these distances in increasing order $d_1 \leq d_2 \leq d_3 \leq \ldots$ (cf. Figure 5; note that two distances $d_i$ and $d_j$ could be equal).

**for** $i = 1, 2, \ldots, |K| - 1$ **do**

Let $x, y \in K$ be the $i$'th closest points in $K$ so that $d(x, y) = d_i$. If $x$ and $y$ are in different clusters, then merge these two clusters.

If the current clustering satisfies points (i) and (ii) of Definition 8 (with $\gamma$ equal to the largest in-diameter in all the clusters) stop and output the current clustering.

**end for**

If no valid clustering was found, output "0"

In the next theorem, we show that any set $K \subseteq \mathbb{Z}_N$ with $|K| < \ln(N/2)$ has a valid clustering.

THEOREM 9. *If a set $K \subseteq \mathbb{Z}_N$ satisfies $|K| < \ln(N/2)$, then a valid clustering of $K$ exists and Algorithm 1 will produce one.*

*Proof.* Observe that at the end of iteration $i$ of the algorithm, the distance between any pair of clusters is greater than or equal $d_{i+1}$: Assume for contradiction that there are two clusters $C, C'$ at iteration $i$ where $d(C, C') < d_{i+1}$. This means that there exist $x \in C$, $y \in C'$ such that $d(x, y) < d_{i+1}$. But this is impossible because the algorithm processes distances in increasing order, and so $x$ and $y$ must have merged in the same cluster at some iteration $\leq i$.

Now, to prove that the algorithm terminates and produces a valid clustering, we need to show that at some iteration $i$, each cluster has in-diameter smaller than $\min(d_{i+1}, N/2)$. Note that one can get a simple upper bound on the in-diameter of the clusters at iteration $i$: indeed, it is not hard to show that at iteration $i$ any cluster has in-diameter at most $S_i$, where $S_i$ is defined as:

$$S_i := d_1 + d_2 + \cdots + d_i = \sum_{j=1}^{i} d_j.$$

Figure 5 shows a simple illustration of this bound.

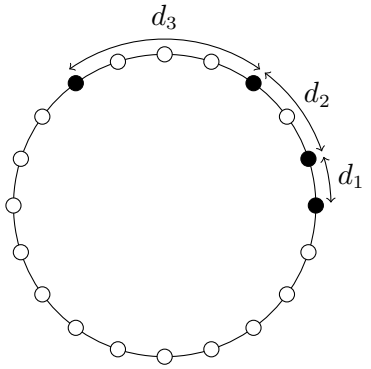


FIGURE 5. A set of frequencies $K$. At iteration 0 of the algorithm each frequency is in its own cluster. At iteration 1 of the algorithm, the two nodes at distance $d_1$ from each other are merged in a single cluster. At iteration 2, the two nodes at distance $d_2$ are merged and we get one cluster having 3 nodes with in-diameter $d_1 + d_2$. In general, at iteration $i$ the clusters cannot have in-diameter larger than $d_1 + \cdots + d_i$.

Let $a$ be the largest index $i$ where $d_i = 1$, and let $b$ the largest index $i$ where $S_i < N/2$.[2] If $i \in [a, b]$, then at the end of the $i$'th iteration, the distance between any two clusters is greater than 1 (since $d_{i+1} > 1$) and the in-diameter of any cluster is smaller than $N/2$. To prove that the algorithm terminates and produces a valid clustering, it suffices to show that there exists $i \in [a, b]$ such that $d_{i+1} > S_i$.

Assume for contradiction that this is not the case. Then this means that we have:

$$\begin{aligned} d_{a+1} &\leq d_1 + \cdots + d_a \\ d_{a+2} &\leq d_1 + \cdots + d_{a+1} \\ &\vdots \\ d_{b+1} &\leq d_1 + \cdots + d_b \end{aligned}$$

We will now show that this implies that $|K| \geq \ln(N/2)$ which contradicts the assumption of the theorem. Define the function $f(x) = 1/x$ and note that, on the one hand we have:

$$\sum_{i=a}^{b} d_{i+1} f(S_i) = \sum_{i=a}^{b} d_{i+1} \frac{1}{d_1 + \cdots + d_i} \leq \sum_{i=a}^{b} 1 = b - a + 1.$$

On the other hand, since $f$ is a decreasing function we have (cf. Figure 6):

$$\sum_{i=a}^{b} d_{i+1} f(S_i) \geq \int_{S_a}^{S_{b+1}} f(x)dx = [\ln(x)]_{S_a}^{S_{b+1}} = \ln(S_{b+1}) - \ln(S_a).$$

[2] Note that we can assume $\operatorname{indiam}(K) \geq N/2$ which implies that $S_{|K|-1} \geq N/2$. Indeed, if the in-diameter of $K$ is smaller than $N/2$, then we have a valid clustering of $K$ by considering $K$ as a single cluster.

Thus we get that:

$$b - a + 1 \geq \ln(S_{b+1}) - \ln(S_a).$$

Now note that $S_a = a$ since $d_i = 1$ for all $1 \leq i \leq a$. Thus we have:

$$b \geq \ln(S_{b+1}) - \ln(S_a) + a - 1 \geq \ln(S_{b+1})$$

since $a - \ln(S_a) \geq 1$ (we assume here that $a \geq 1$ because otherwise the distance between any two elements in $K$ is at least 2 in which case $K$ is clearly not sos-valid). Now since $|K| \geq b$ and $S_{b+1} \geq N/2$ we get

$$|K| \geq \ln(N/2)$$

as desired.

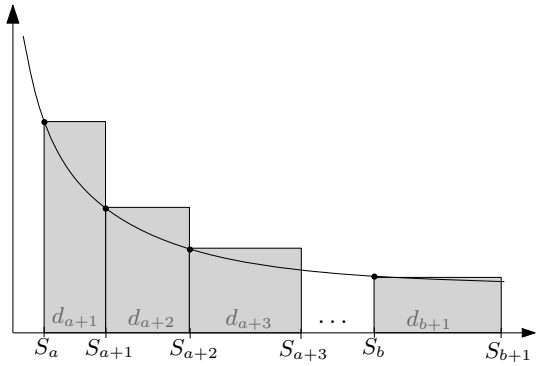


FIGURE 6.

□

**6. Conclusion** Regular polygons in the plane have played an important role in the study of extended formulations. In this paper we studied equivariant psd lifts of regular polygons. One of the main techniques to obtain equivariant psd lifts of polytopes is using the Lasserre/sum-of-squares hierarchy. The first contribution of this paper was to show that the hierarchy requires exactly $\lceil N/4 \rceil$ iterations for the regular $N$-gon. To prove this we used a specific property about the levels of the facet defining linear functionals of the regular $N$-gon. The techniques we developed are actually quite general and can be used to study the theta-rank of general $k$-level polytopes. For example they may be useful for understanding the theta-rank of other families of $k$-level polytopes, such as matroid base polytopes, which were studied in this context in the recent work of Grande and Sanyal [17].

The second contribution of this paper is the construction of an explicit equivariant psd lift of the regular $2^n$-gon of size $2n - 1$. This lift was obtained by showing that the facet-defining linear functionals admit a *sparse* sum-of-squares representation that requires only a small number of "frequencies". This construction gives the first example of a polytope with an exponential gap between equivariant psd lifts and equivariant LP lifts. Also it shows that one can construct equivariant psd lifts that are exponentially smaller than the lift produced by the sum-of-squares hierarchy. In our recent paper [7] we exploited further the idea of sparse sum-of-squares representations to produce small semidefinite lifts for trigonometric cyclic polytopes (in particular we generalize the lift of size $O(\log N)$ given in the present paper to the case where $N$ is not necessarily a power of two).

Finally we proved that the size of our equivariant psd lift is essentially optimal by showing that any equivariant psd lift of the regular $N$-gon has size at least $\ln(N/2)$. An important question that remains open in the study of regular polygons is to know whether one can obtain smaller psd lifts by relaxing the equivariance condition. Currently the only lower bound on the psd rank of $N$-gons in the plane is $\Omega\left(\sqrt{\frac{\log N}{\log\log N}}\right)$ which comes from quantifier elimination theory [13, 15].

**Appendix A: Finishing the proof on theta-rank of the regular $N$-gon** In this appendix we complete the proof of Theorem 6 concerning the theta-rank of the $N$-gon, when $N$ is not a multiple of four. We first prove the following lemma:

LEMMA 1. *Let $N$ be a positive integer and let $T_N$ be the Chebyshev polynomial of degree $N$. Then for any $u \geq \cos(\pi/N)$, the curve of $T_N(x)$ lies above its tangent at $x = u$ on the interval $[-1, \infty)$, i.e.,*

$$T_N(x) \geq T_N(u) + T_N'(u)(x-u) \quad \forall x \in [-1, \infty). \tag{27}$$

*Furthermore, when $N$ is even the inequality (27) is true for all $x \in \mathbb{R}$.*

An illustration of Lemma 1 is given in Figure 7.

*Proof.* First observe that $T_N''(x) \geq 0$ for all $x \in [\cos(\pi/N), \infty)$: indeed note that $\cos(\pi/N)$ is the largest root of $T_N'$, and thus, since the roots of $T_N''$ interlace the roots of $T_N'$ we have necessarily that $T_N'' \geq 0$ on $[\cos(\pi/N), \infty)$. Thus this shows that $T_N$ is convex on the interval $[\cos(\pi/N), \infty)$ and in particular shows that inequality (27) holds for all $x \in [\cos(\pi/N), \infty)$. It remains to show that the inequality (27) holds for $x \in [-1, \cos(\pi/N))$. Since $\cos(\pi/N)$ is a minimum of $T_N$ on the interval $[-1, 1]$ we have, for any $x \in [-1, \cos(\pi/N))$:

$$T_N(x) \geq T_N(\cos(\pi/N)) \overset{(a)}{\geq} T_N(u) + T_N'(u)(\cos(\pi/N) - u) \overset{(b)}{\geq} T_N(u) + T_N'(u)(x-u)$$

where $(a)$ follows from the first part of the argument which shows that inequality (27) holds for $x = \cos(\pi/N)$ and, where in $(b)$ we used the fact that $x \leq \cos(\pi/N)$ and that $T_N'(u) \geq 0$. Thus this proves inequality (27).

When $N$ is even inequality (27) is clearly true for $x \leq -1$ also since for $x \leq -1$, $T_N(x) \geq 0$ whereas the linear function $T_N(u) + T_N'(u)(x-u)$ is negative. □

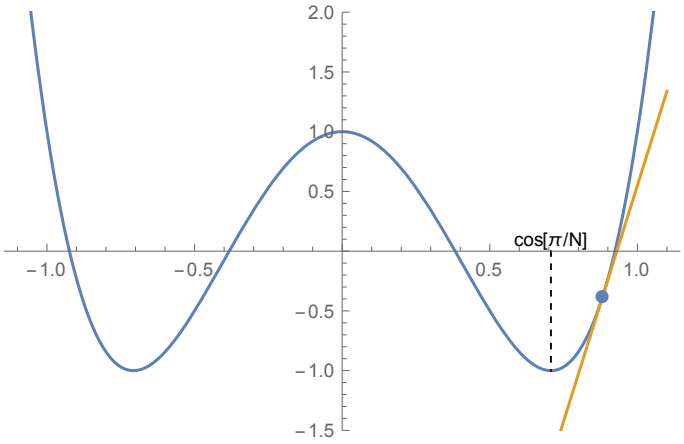


FIGURE 7. Illustration of Lemma 1 with $N = 4$ and some value $u \geq \cos(\pi/N)$.

We now complete the proof of Theorem 6 by considering the cases where $N$ is not a necessarily a multiple of four. For $i = 0, \ldots, \lceil N/2 \rceil - 1$, let $a_i = x_{i+1,N} = \cos((2i+1)\pi/N)$ and let $q_N$ be the polynomial that vanishes at the $a_i$'s:

$$q_N(x) = \prod_{i=0}^{\lceil N/2 \rceil - 1} (x - a_i) = \prod_{i=0}^{\lceil N/2 \rceil - 1} \left( x - \cos\left( \frac{(2i+1)\pi}{N} \right) \right). \tag{28}$$

To complete the proof of Theorem 6 we need to show that the tangent of the curve of $q_N$ at $\cos(\pi/N)$ lies below the curve of $q_N$ (cf. Proposition 6). We have already proved this in the case where $N$ is

a multiple of four, by showing that in this case $q_N(x)$ is, up to a scalar, the Chebyshev polynomial $T_{N/2}(x)$. The next lemma expresses the polynomial $q_N$ in terms of Chebyshev polynomials for any $N$:

LEMMA 2. *The polynomial $q_N$ satisfies:*

$$q_N(x) \propto \begin{cases} T_{N/2}(x) & \text{if } N \text{ is even} \\ (T_{\lfloor N/2 \rfloor}(x) + T_{\lceil N/2 \rceil}(x))/2 & \text{if } N \text{ is odd.} \end{cases}$$

*where the symbol $\propto$ indicates equality up to multiplicative constant.*

*Proof.* The case where $N$ is even is clear by comparing the roots of $q_N$ and those of $T_{N/2}$. For the case $N$ odd, observe that if $\cos\alpha$ is a root of $q_N$ then $\pm\cos(\alpha/2)$ are roots of $q_N(T_2(x)) = q_N(2x^2-1)$. Since the roots of $q_N$ are the $\{\cos((2i-1)\pi/N), i = 1, \ldots, \lceil N/2 \rceil\}$, the roots of $q_N(2x^2-1)$ are thus $\{\pm\cos((2i-1)\pi/(2N)), i = 1, \ldots, \lceil N/2 \rceil\}$ (with a double root at 0). Note that these are exactly the roots of $xT_N(x)$ (the multiplication by $x$ is for the double root at 0). Thus from this observation we have for any $x \in \mathbb{R}$:

$$\begin{aligned} q_N(T_2(x)) \propto xT_N(x) = T_1(x)T_N(x) &\overset{(a)}{=} (T_{N-1}(x) + T_{N+1}(x))/2 \\ &\overset{(b)}{=} (T_{(N-1)/2}(T_2(x)) + T_{(N+1)/2}(T_2(x)))/2. \end{aligned}$$

Equality $(a)$ follows from the identity $T_a(x)T_b(x) = \frac{1}{2}(T_{a+b}(x) + T_{a-b}(x))$ and equality $(b)$ follows from $T_a(T_b(x)) = T_{ab}(x)$. Thus since we are working with polynomials and since $\{T_2(x) : x \in \mathbb{R}\}$ is infinite we have the desired identity:

$$q_N(x) \propto T_{\lfloor N/2 \rfloor}(x) + T_{\lceil N/2 \rceil}(x).$$

□

We are now ready to finish the proof of Theorem 6 by proving that the tangent of $q_N$ (defined in (28)) at $\cos(\pi/N)$ lies below the curve of $q_N$. Since the case where $N$ is a multiple of four was already treated, we distinguish in what follows the three remaining cases according to the residue class of $N$ modulo 4:

- Case $N = 4m-1$: In this case the polynomial $q_N$ is even degree and we want to show that $q_N(x)$ is above its linear approximation at $x = \cos(\pi/N)$. From Lemma 2 we have that $q_N(x) \propto T_{2m-1}(x) + T_{2m}(x)$. Since, for all $x \in [-1, \infty)$, $T_{2m}(x)$ and $T_{2m-1}(x)$ are both above their linear approximations at $\cos(\pi/N)$ (using Lemma 1 and because $\cos(\pi/N) \geq \cos(\pi/(2m))$ and $\cos(\pi/N) \geq \cos(\pi/(2m-1))$) it follows that the same holds for $q_N$ on $[-1, \infty)$. Since, in addition $q_N$ has even degree and $q_N(-1) \geq 0$ this shows that $q_N(x)$ is above its linear approximation at $\cos(\pi/N)$ for all $x$, which is what we wanted.
- Case $N = 4m-2$: In this case the polynomial $q_N$ is $q_N(x) = T_{2m-1}(x)$ (from Lemma 2). Note that $q_N$ has odd degree. Thus to apply Proposition 6 we will add an additional "dummy" root for $q$ to make it even degree (the resulting interpolating polynomial $p$ we get will interpolate the linear function $l$ at this additional "dummy" point). Consider the polynomial $\widetilde{q_N}(x) = xq_N(x)$. We will show that the assumption of Proposition 6 holds for $\widetilde{q_N}(x)$. Observe that

$$\widetilde{q_N}(x) = xq_N(x) \propto T_1(x)T_{2m-1}(x) = (T_{2m}(x) + T_{2m-2}(x))/2.$$

Since both $T_{2m}$ and $T_{2m-2}$ are globally above their linear approximations at $\cos(\pi/N)$ (by Lemma 1 and because $\cos(\pi/N) \geq \cos(\pi/(2m))$ and $\cos(\pi/N) \geq \cos(\pi/(2m-1))$), the same holds for $\widetilde{q_N}(x) = xq_N(x)$. Thus this shows that $\widetilde{q_N}(x)$ lies above its tangent at $x = \cos(\pi/N)$, which is what we want.

- Case $N = 4m-3$: In this case we have, from Lemma 2, $q_N(x) = (T_{2m-1}(x) + T_{2m-2}(x))/2$. Note that the polynomial $q_N$ has odd degree and thus we need to add an additional "dummy" root to make it even degree. Take $\widetilde{q_N}(x) = xq_N(x)$ and note that

$$\widetilde{q_N}(x) \propto (T_{2m}(x) + T_{2m-2}(x) + T_{2m-1}(x) + T_{2m-3}(x))/4.$$

Using Lemma 1, for $x \in [-1, \infty)$, each of the four Chebyshev polynomials are above their linear approximation at $\cos(\pi/N)$ (because $\cos(\pi/N) \geq \cos(\pi/(2m))$ and $\cos(\pi/N) \geq \cos(\pi/(2m-1))$ and $\cos(\pi/N) \geq \cos(\pi/(2m-2))$ and $\cos(\pi/N) \geq \cos(\pi/(2m-3))$). Since $\widetilde{q_N}(x)$ has even degree and $\widetilde{q_N}(-1) \geq 0$, it holds that $\widetilde{q_N}$ is globally above its linear approximation at $x = \cos(\pi/N)$.

**Appendix B: Linear programming lifts** In this section we recall the definitions of LP lifts and equivariant LP lifts. For reference we also provide the proof from [13] that any equivariant LP lift of the regular $N$-gon must have size at least $N$ when $N$ is a power of a prime.

We first recall the definition of a linear programming (LP) lift:

DEFINITION 9. Let $P \subset \mathbb{R}^n$ be a polytope. We say that $P$ has a LP lift of size $d$ if we can write $P = \pi(\mathbb{R}^d_+ \cap L)$ where $\pi : \mathbb{R}^d \to \mathbb{R}^n$ is a linear map and $L$ is an affine subspace of $\mathbb{R}^d$.

We now give the definition of an equivariant LP lift, from [13, 18] (also known as symmetric LP lift). We denote by $\mathfrak{S}_d$ the group of permutations on $d$ elements. If $\sigma \in \mathfrak{S}_d$ and $y \in \mathbb{R}^d$, we denote by $\sigma y$ the left action of $\mathfrak{S}_d$ on $\mathbb{R}^d$ which permutes the coordinates according to $\sigma$.

DEFINITION 10. Let $P \subset \mathbb{R}^n$ be a polytope and assume that $P$ is invariant under the action of a group $G$. Let $P = \pi(\mathbb{R}^d_+ \cap L)$ be a LP lift of size $d$. The lift is called $G$-equivariant if there exists a homomorphism $\Phi : G \to \mathfrak{S}_d$ such that:

(i) The subspace $L$ is invariant under the permutation action of $\Phi(g)$, for all $g \in G$:

$$\Phi(g)y \in L \quad \forall g \in G, \forall y \in L. \tag{29}$$

(ii) The following equivariance relation holds:

$$\pi(\Phi(g)y) = g \cdot \pi(y) \quad \forall g \in G, \forall y \in \mathbb{R}^d_+ \cap L. \tag{30}$$

Given integer $N$, let $\mathrm{Rot}_N$ be the subgroup of rotations of the dihedral group of order $2N$. Note that $\mathrm{Rot}_N \cong \mathbb{Z}_N$.

PROPOSITION 8. *[13, Proposition 3] If $N$ is a prime or a power of a prime, then any $\mathrm{Rot}_N$-equivariant LP lift of the regular $N$-gon has size $N$.*

*Proof.* Let $P$ be the regular $N$-gon and assume that $P$ has a LP lift of size $d$ that is $\mathrm{Rot}_N$-equivariant. By Definition 10 there exists a homomorphism $\Phi : \mathrm{Rot}_N \to \mathfrak{S}_d$ such that (29) and (30) are satisfied. It is not hard to show that $\Phi$ must be injective: indeed if $\Phi(g) = 1$ for some $g \in \mathrm{Rot}_N$ then by the equivariance relation (30) we must have $\pi(y) = g \cdot \pi(y)$ for all $y \in \mathbb{R}^d_+ \cap L$, which means that $x = gx$ for all $x \in P$. Since $P$ is full-dimensional this means that $g$ is the identity element in $\mathrm{Rot}_N$.

Since $\Phi$ is injective, we have that $\Phi(\mathrm{Rot}_N)$ is a cyclic subgroup of $\mathfrak{S}_d$ of size $N$ and thus $\mathfrak{S}_d$ has an element of order $N$. One can show that if $\mathfrak{S}_d$ has an element of order $p^t$ where $p$ is a prime and $t \geq 1$, then $d \geq p^t$: to see this one can use the decomposition of a permutation into cycles with disjoint support, and recall that the order of a permutation is the least common multiple of the cycle lengths; thus if the order of a permutation is $p^t$ then at least one of the cycle lengths must be divisible by $p^t$ which implies that $d \geq p^t$. Thus this shows that when $N$ has the form $N = p^t$ then we must have $d \geq p^t$.

REMARK 6. When $N$ is a prime we easily see that we must have $d \geq N$ by the simple fact that $N$ is a prime and that it has to divide $d!$.

□

**Appendix C: Lifts from sum-of-squares certificates** In this appendix we sketch a proof of Theorem 3 which shows how to obtain a psd lift of the regular $N$-gon from a sum-of-squares certificate of $\ell$.

To prove the inclusion $\subseteq$ in (8), consider a point $(\cos\theta_j, \sin\theta_j) \in \mathcal{X}_N$ where $\theta_j = 2j\pi/N$. Define $y_t = e^{2ijt\pi/N}$. Then clearly $(\mathrm{Re}[y_1], \mathrm{Im}[y_1]) = (\cos\theta_j, \sin\theta_j)$ and $y_0 = 1$, and it is not hard to show that the sequence $(y_t)$ satisfies the psd constraints in the right-hand side of (8).

To prove the inclusion $\supseteq$, let $(y_t)$ be as in the right-hand side of (8). We will show that the point $(\mathrm{Re}[y_1], \mathrm{Im}[y_1])$ satisfies the facet inequality defined by $\ell$, i.e., that

$$\cos(\pi/N) - \cos(\pi/N)\,\mathrm{Re}[y_1] - \sin(\pi/N)\,\mathrm{Im}[y_1] \geq 0.$$

For $i = 1, \ldots, q$ let $T_i : \mathbf{H}^{|K_i|} \to \mathbb{C}^N$ be the map defined by:

$$T_i(Q) = \sum_{r,s \in K_i} Q_{r,s} \overline{e_r} e_s$$

where $\overline{e_r} e_s$ is the pointwise multiplication of $\overline{e_r}$ and $e_s$ which are both elements of $\mathbb{C}^N$. One can show that since $\ell$ has a sum-of-squares certificate (7), there exist positive semidefinite Hermitian matrices $Q_1, \ldots, Q_q$ (the Gram matrices in the sum-of-squares representation) such that

$$\ell = \sum_{i=1}^{q} T_i(Q_i).$$

Let $y$ be in the dual space $(\mathbb{C}^N)^*$ defined by $y(e_t) = y_t$. The main observation is that the moment matrix $[y_{k'-k}]_{k,k'} \in K_i$ is precisely $T_i^*(y)$ where $T_i^*$ is the adjoint of $T_i$. Thus we have:

$$\langle y, \ell \rangle = \sum_{i=1}^{q} \langle y, T_i(Q_i) \rangle = \sum_{i=1}^{q} \langle T_i^*(y), Q_i \rangle \geq 0$$

since $T_i^*(y)$ is positive semidefinite by assumption. But since $\langle y, \ell \rangle = \cos(\pi/N) - \cos(\pi/N)\,\mathrm{Re}[y_1] - \sin(\pi/N)\,\mathrm{Im}[y_1]$ this shows that the point $(\mathrm{Re}[y_1], \mathrm{Im}[y_1])$ satisfies the facet inequality defined by $\ell$.

To conclude the proof note that since $\ell$ has a sum-of-squares certificate (7), then all the other facet inequalities of the regular $N$-gon also have sum-of-squares certificates of the same type: this is because all the other facet inequalities can be obtained from $\ell$ by rotation, and the spaces $\oplus_{k \in K_i} \mathbb{C} e_i$ are invariant under the action of $\mathrm{Rot}_N$ (which shifts the vertices of the $N$-gon). The argument given above can thus be used to show that the point $(\mathrm{Re}[y_1], \mathrm{Im}[y_1])$ satisfies all the facet inequalities of the regular $N$-gon, which means that it is in $\mathrm{conv}(\mathcal{X}_N)$.

The reason the psd lift is $\mathrm{Rot}_N$-equivariant is that subspaces of $\mathbb{C}^N$ of the form $\oplus_{k \in K} \mathbb{C} e_k$ are invariant under the action of $\mathrm{Rot}_N$, see [6, Appendix A] for details.

**Appendix D: Proof of the structure theorem for regular polygons** In this appendix we prove Theorem 4 concerning the structure of equivariant psd lifts for regular polygons. This theorem is a special case of the results in [6] but we include the proof here for completeness.

THEOREM 10. *Assume that the regular $N$-gon has a Hermitian psd lift of size $d$ that is equivariant with respect to the rotation group $\mathrm{Rot}_N$ of order $N$. Then there exists a set $K \subseteq \mathbb{Z}_N$ with $|K| \leq d$ and functions $h_i \in \bigoplus_{k \in K} \mathbb{C} e_k$ such that*

$$\ell = \sum_i |h_i|^2$$

*where $\ell$ is the facet-defining function (5).*

*Proof.* In this proof we identify the vertices of the regular $N$-gon with $\mathbb{Z}_N$ and we also identify the rotation group $\mathrm{Rot}_N$ with $\mathbb{Z}_N$. As such the action of $\mathrm{Rot}_N$ on the vertices of the regular $N$-gon can be described as follows: if $r$ is an element of $\mathrm{Rot}_N \cong \mathbb{Z}_N$ and $t \in \mathbb{Z}_N$ represents a vertex of the regular $N$-gon then the result of rotating $t$ by $r$ is the vertex $r+t \in \mathbb{Z}_N$.

Since we have an $\mathrm{Rot}_N$-equivariant Hermitian psd lift of the regular $N$-gon of size $d$, the *factorization theorem* [6, Theorem A] says that there exists a map $A : \mathbb{Z}_N \to \mathbf{H}^d_+$ and $B \in \mathbf{H}^d_+$ such that the following holds:

1. For all $t \in \mathbb{Z}_N$, $\ell(t) = \langle A(t), B\rangle$.
2. The following equivariance relation:

$$A(r+t) = \rho(r)A(t)\rho(r)^* \quad \forall r \in \mathbb{Z}_N, \forall t \in \mathbb{Z}_N$$

where $\rho : \mathbb{Z}_N \to GL_d(\mathbb{C})$ is a group homomorphism.
Note that $\rho$ is nothing but a $d$-dimensional linear representation of $\mathbb{Z}_N$. Since the irreducible representations of $\mathbb{Z}_N$ are all one-dimensional, there is a change-of-basis matrix $T \in GL_d(\mathbb{C})$ so that $\rho(r)$ is diagonal, i.e., we can write:

$$\rho(r) = T\,\mathrm{diag}(\phi(r))T^{-1} \quad \forall r \in \mathbb{Z}_N,$$

where $\phi = (\phi_1, \ldots, \phi_d) : \mathbb{Z}_N \to (\mathbb{C}^*)^d$. Note that for each $j = 1, \ldots, d$, the map $\phi_j : \mathbb{Z}_N \to \mathbb{C}^*$ is a group homomorphism and thus takes the form

$$\phi_j(r) = e^{2ik_j r\pi/N} = e_{k_j}(r) \quad \forall r \in \mathbb{Z}_N \tag{31}$$

where $k_j \in \mathbb{Z}_N$. Let

$$K = \{k_1, \ldots, k_d\} \subseteq \mathbb{Z}_N \tag{32}$$

and note that $|K| \leq d$. We will now show that $K$ is sos-valid, i.e., that $\ell$ has a sum-of-squares representation using functions supported on $K$.

Observe that, by the equivariance relation on $A$, we have: $A(r) = \rho(r)A(0)\rho(r)^*$ for any $r \in \mathbb{Z}_N$. Thus we have, for any $r \in \mathbb{Z}_N$ (denoting $T^{-*} := (T^{-1})^*$):

$$\begin{aligned}
\ell(r) &= \mathbf{Tr}[\rho(r)A(0)\rho(r)^*B^*] \\
&= \mathbf{Tr}[T\,\mathrm{diag}(\phi(r))T^{-1}A(0)T^{-*}\,\mathrm{diag}(\phi(r))^*T^*B^*] \\
&\overset{(a)}{=} \mathbf{Tr}[\mathrm{diag}(\phi(r))A'\,\mathrm{diag}(\phi(r))^*B'^*] \\
&\overset{(b)}{=} \phi(r)^*(A' \circ B')\phi(r)
\end{aligned}$$

where in $(a)$ we used $A' = T^{-1}A(0)T^{-*}$ and $B' = T^*BT$ and in $(b)$ we denoted by $A' \circ B'$ the Hadamard (componentwise) product of $A'$ and $B'$. Since $A', B'$ are positive semidefinite, $A' \circ B'$ is positive semidefinite too (by the Schur product theorem) and thus we can write

$$A' \circ B' = \sum_i v_i v_i^*$$

where $v_i \in \mathbb{C}^d$. Thus we finally get that:

$$\ell(r) = \sum_i |v_i^*\phi(r)|^2 = \sum_i |h_i(r)|^2 \quad \forall r \in \mathbb{Z}_N \tag{33}$$

where $h_i := v_i^*\phi : \mathbb{Z}_N \to \mathbb{C}$ are linear combinations of the $\phi_j = e_{k_j}$ given in (31), i.e., $\mathrm{supp}\, h_i \subseteq K$. This completes the proof. □

**Acknowledgments.** This work was supported by AFOSR grants #FA9550-11-1-0305 and #FA9550-12-1-0287. This work was done while the second author was at the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology. The authors would like to thank Greg Blekherman for giving them the permission to include his proof of Proposition 1.

**References**

[1] Ben-Tal A, Nemirovski A (2001) On polyhedral approximations of the second-order cone. *Mathematics of Operations Research* 26(2):193–205.

[2] Blekherman G, Parrilo PA, Thomas RR (2013) *Semidefinite optimization and convex algebraic geometry* (SIAM).

[3] Briët J, Dadush D, Pokutta S (2013) On the existence of 0/1 polytopes with high semidefinite extension complexity. *Algorithms–ESA 2013*, 217–228 (Springer).

[4] Chan SO, Lee JR, Raghavendra P, Steurer D (2013) Approximate constraint satisfaction requires large LP relaxations. *IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS)*, 350–359.

[5] Fawzi H, Gouveia J, Parrilo PA, Robinson RZ, Thomas RR (2015) Positive semidefinite rank. *Mathematical Programming* 153(1):133–177.

[6] Fawzi H, Saunderson J, Parrilo PA (2015) Equivariant semidefinite lifts and sum-of-squares hierarchies. *SIAM Journal on Optimization* 25(4):2212–2243.

[7] Fawzi H, Saunderson J, Parrilo PA (2015) Sparse sums of squares on finite abelian groups and improved semidefinite lifts. *To Appear in Mathematical Programming* .

[8] Fiorini S, Massar S, Pokutta S, Tiwary HR, de Wolf R (2012) Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds. *Proceedings of the 44th Symposium on Theory of Computing*, 95–106 (ACM).

[9] Fiorini S, Rothvoß T, Tiwary HR (2012) Extended formulations for polygons. *Discrete & Computational Geometry* 48(3):658–668.

[10] Goemans M (2015) Smallest compact formulation for the permutahedron. *Mathematical Programming* 153(1):5–11, URL http://dx.doi.org/10.1007/s10107-014-0757-1.

[11] Gouveia J, Laurent M, Parrilo PA, Thomas RR (2012) A new semidefinite programming hierarchy for cycles in binary matroids and cuts in graphs. *Mathematical Programming* 133(1-2):203–225.

[12] Gouveia J, Parrilo PA, Thomas RR (2010) Theta bodies for polynomial ideals. *SIAM Journal on Optimization* 20(4):2097–2118.

[13] Gouveia J, Parrilo PA, Thomas RR (2013) Lifts of convex sets and cone factorizations. *Mathematics of Operations Research* 38(2):248–264.

[14] Gouveia J, Robinson RZ, Thomas RR (2013) Polytopes of minimum positive semidefinite rank. *Discrete & Computational Geometry* 50(3):679–699.

[15] Gouveia J, Robinson RZ, Thomas RR (2015) Worst-case results for positive semidefinite rank. *Mathematical Programming* 153(1):201–212.

[16] Gouveia J, Thomas R (2012) Convex hulls of algebraic sets. *Handbook on Semidefinite, Conic and Polynomial Optimization*, 113–138 (Springer).

[17] Grande F, Sanyal R (2014) Theta rank, levelness, and matroid minors. *arXiv preprint arXiv:1408.1262* .

[18] Kaibel V, Pashkovich K, Theis DO (2012) Symmetry matters for sizes of extended formulations. *SIAM Journal on Discrete Mathematics* 26(3):1361–1382.

[19] Lasserre JB (2009) Convex sets with semidefinite representation. *Mathematical Programming* 120(2):457–477.

[20] Pashkovich K (2014) Tight lower bounds on the sizes of symmetric extensions of permutahedra and similar results. *Mathematics of Operations Research* 39(4):1330–1339.

[21] Sanyal R, Sottile F, Sturmfels B (2011) Orbitopes. *Mathematika* 57(02):275–314.

[22] Tunçel L (2000) Potential reduction and primal-dual methods. *Handbook of semidefinite programming*, 235–265 (Springer).

[23] Yannakakis M (1991) Expressing combinatorial optimization problems by linear programs. *Journal of Computer and System Sciences* 43(3):441–466.