Centrum voor Wiskunde en Informatica

REPORT*RAPPORT*

PNA

Probability, Networks and Algorithms

Probability, Networks and Algorithms

Symmetric, positive polynomials, which are not sums of squares

H. Bosse

REPORT PNA-E0706 DECEMBER 2007

Centrum voor Wiskunde en Informatica (CWI) is the national research institute for Mathematics and Computer Science. It is sponsored by the Netherlands Organisation for Scientific Research (NWO).
CWI is a founding member of ERCIM, the European Research Consortium for Informatics and Mathematics.

CWI's research has a theme-oriented structure and is grouped into four clusters. Listed below are the names of the clusters and in parentheses their acronyms.

Probability, Networks and Algorithms (PNA)

Software Engineering (SEN)

Modelling, Analysis and Simulation (MAS)

Information Systems (INS)

P.O. Box 94079, 1090 GB Amsterdam (NL)
Kruislaan 413, 1098 SJ Amsterdam (NL)
Telephone +31 20 592 9333
Telefax +31 20 592 4199

ISSN 1386-3711

Symmetric, positive polynomials, which are not sums of squares

ABSTRACT
This paper presents a construction for symmetric, non-negative polynomials, which are not sums of squares. It explicitly generalizes the Motzkin polynomial and the Robinson polynomials to families of non-negative polynomials, which are not sums of squares. The degrees of the resulting polynomials can be chosen in advance.

2000 Mathematics Subject Classification: 12Y05, 20C30, 12D10, 26C10, 12E10
Keywords and Phrases: polynomial, sums of squares, SOS, PSD, polynomial optimization

SYMMETRIC, POSITIVE SEMIDEFINITE POLYNOMIALS WHICH ARE NOT SUMS OF SQUARES.

HARTWIG BOSSE

ABSTRACT. This paper presents a construction for symmetric, non-negative polynomials, which are not sums of squares. It explicitly generalizes the Motzkin polynomial and the Robinson polynomials to families of non-negative polynomials, which are not sums of squares. The degrees of the resulting polynomials can be chosen in advance.

1. INTRODUCTION

The aim of this paper is twofold. It generalizes some well known polynomials, which are positive but not sums of squares. Moreover it demonstrates the use of group-representation theory in the analysis of positive polynomials. The main result is an explicit construction for a family of symmetric polynomials, which are positive but not sums of squares. To our best knowledge, this is the first explicit construction of such polynomials, in which the degrees of the resulting polynomials are not fixed. The proof uses group representation theory to limit the possible composites of symmetric sums of squares.

1.1. **Motivation.** A real polynomial p in n variables is called **p**ositive **s**emi-**d**efinite (PSD), if $p(x) \geq 0$ holds for all $x \in \mathbb{R}^n$. A subclass of these are polynomials p which are a ***sum of squares*** (SOS) of other polynomials $q_1, \ldots, q_n$, i.e. , $p = \sum_{i=1}^n q_i^2$ holds. Clearly, every SOS polynomial is PSD. Surprising at first sight only, not every PSD polynomial is an SOS – a classic result from 1888 by Hilbert [Hi] (For an excellent overview on Hilbert's related work, see [Re]).

Aside of being a challenging, classic topic, by today, knowledge on PSD and SOS polynomials has become *crucial* in solving polynomial optimization problems. By relatively recent results ([La], [Pa]) we understand now, that the complexity of polynomial optimization actually comes in via the difference between PSD and SOS polynomials: Note that the infimum of any polynomial p is the minimal constant term that makes p a PSD polynomial. More precisely one finds

$$\text{(POP)} \qquad \inf_{x \in \mathbb{R}^n} p(x) \;=\; \sup_{\lambda \in \mathbb{R}} \lambda \quad \text{s.t.} \quad p - \lambda \geq 0.$$

The class of problems of the shape (POP) is $\mathcal{NP}$-hard. Therefore it is not surprising, that efficient methods to check whether a polynomial is PSD are not known. There is however a widely used certificate, which is (relatively) easy to check: An SOS polynomial is always non-negative. This leads to the following relaxation of (POP)

$$\text{(POP}^*\text{)} \qquad \sup_{\lambda \in \mathbb{R}} \lambda \quad \text{s.t.} \quad p - \lambda \text{ is SOS.}$$

The current strategy is to approximate (POP*) by a series of semi-definite programs, each of which can be solved close to optimality in satisfactory time with current solvers (see [HG], [Glop]). Unfortunately, in some cases the gap between a solution of (POP*) and (POP) is fixed to infinity, i.e., when $p - \lambda$ is not an SOS for any λ. For further information on this topic we refer to Monique Laurent's excellent overview article [Lau].

In review of the above, understanding why some polynomials are PSD but not SOS, would greatly help to improve current solution techniques for (POP). But to this day, there are few known explicit examples of such polynomials. The construction of these uses the "perturbation method" due to Hilbert, resulting in polynomials of degree 6. Moreover,

⋆ Supported by CWI Amsterdam.

the proofs that these examples are PSD but not SOS have not resulted in some general, satisfying framework.

This paper sheds some light on the latter. The polynomials introduced in this paper are positive and not sums of squares, because their "amount of asymmetry" does not match the possible asymmetry of sums of squares of the same degree.

1.2. **Known results.** In 1888, Hilbert devised the "perturbation method" (s. [Hi]) to create PSD polynomials which are not SOS; the resulting polynomials have degree exactly 6. Since the method is not completely constructive (due to an existence-quantifier) it took another 80 years until first examples where explicitly constructed. All *known* polynomials which are PSD but not SOS, have been constructed using Hilbert's method[1] – as a result, all are of degree 6. Moreover, they all have even symmetry, i.e., they are invariant under permutation and sign-changes of the input-variables.

The following polynomials in 2 variables are positive but not SOS:

- the Motzkin polynomial (see [Mo]),

  $\mathcal{P}_{\mathrm{M}}(x,y) := 1 - 3x_1^2x_2^2 + x_1^4x_2^2 + x_1^2x_2^4,$
- and the Robinson polynomial (see [Ro]),

  $\mathcal{P}_{\mathrm{R}}(x,y) := x_1^2(-1+x_1^2)^2 + x_2^2(-1+x_2^2)^2 - (-1+x_1^2)(-1+x_2^2)(-1+x_1^2+x_2^2).$
- Moreover in [CLR] Reznick and Lam classified all S_n-invariant, homogeneous sextics that are PSD.

1.3. **Contributions.** Theorem 6.1 generalizes the known examples in 2 variables into a family of PSD-polynomials which are not SOS – the Robinson-Motzkin family of polynomials. To our best knowledge, this is the first example of a family of such polynomials with unrestricted degree.

Moreover, in contrast to Hilbert's method, the polynomials are constructed as sums of squares of rational functions (proving their non-negativity). This offers not only a new, explicit construction method for difficult cases in polynomial optimization, but –for the special case of *symmetric* PSD-polynomials– it also might help to strengthen Polyá' s representation theorem.

1.4. **Tools.** Aside of the result itself, it may be worth wile taking a look at the tools used. The proof that the constructed polynomials are not SOS involves symmetry reduction of their representation by semi-definite matrices. We exploit, that the symmetry of an SOS $\mathcal{F}$ implies that it's defining linear matrix inequality (LMI) $\mathcal{F} = \vec{p}^T A\vec{p}$ is invariant under some group-action (here $A \in \mathbb{R}^N$, $A \succeq 0$ and $\vec{p} \in \mathbb{R}[x]^N$). We then use group-representation theory to blockdiagonalize A, which will give a necessary condition for symmetric SOS. In this procedure harmonic polynomials will come in as a basis of polynomials with "basic symmetry".

The approach of reducing the size of group-invariant LMIs by blockdiagonalizing has been used in several practical applications, see [GP], [GS], [BV], and [KMPRS]. A nice summary of this method for the symmetric group can be found in [Va].

The difference to all existing work is that here we examine the dihedral group (as opposed to the symmetric group) and use the reduced LMIs in an abstract proof (as opposed to in numerical calculations).

1.5. **The origin of this paper.** Aside of being symmetric, the Robinson polynomial and Motzkin polynomial have something in common, which is not obvious at first sight. When translated into polar coordinates, $\mathcal{P}_{\mathrm{M}}, \mathcal{P}_{\mathrm{R}}$ have the following structure:

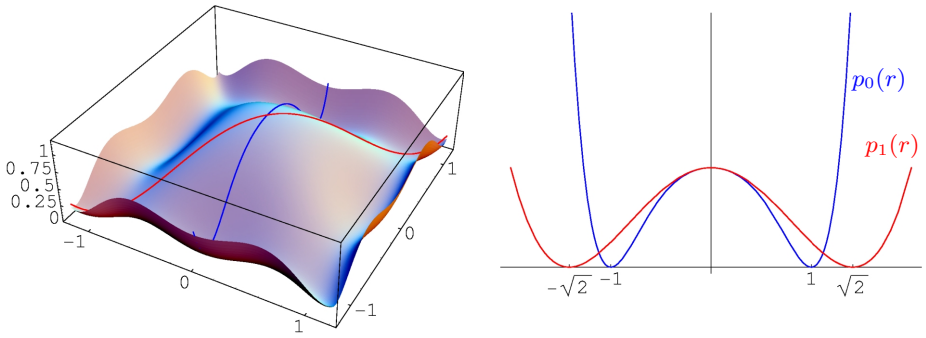
$$\mathcal{P}(r\cos(t), r\sin(t)) \quad = \quad \cos(2t)^2 p_0(r^2) + \sin(2t)^2 p_1(r^2) \tag{1.1}$$

where the $p_0(r^2), p_1(r^2)$ are non-negative, univariate polynomials. So all involved terms in the right hand side of (1.1) are PSD – a certificate that $\mathcal{P}$ is PSD.

But (1.1) also reveals *rotational symmetry*: For fixed angle t, $\mathcal{P}$ is an interpolation [note $\sin^2 + \cos^2 = 1$] between $p_0(r^2)$ and $p_1(r^2)$, where the ratios are periodic in t. So along the lines $x = 0$, $y = 0$ [resp. $t = 0$, $t = \pi/2$] $\mathcal{P}$ restricts to $\mathcal{P}(x,0) = \mathcal{P}(0,x) = p_0(x^2)$.

[1] That this was unavoidably so is a nice result of an upcoming paper of Bruce Reznick [Re].

FIGURE 1. The Robinson polynomial $\mathcal{P}_{\mathrm{R}}$.



The Robinson Polynomial has rotational symmetry. It consists of two non-negative univariate polynomials "glued together" by non-negative, angular functions $\cos^2, \sin^2$.

Similarly, along $x = +y$, $x = -y$ [resp. $t = \pi/4$, $t = 3\pi/4$], $\mathcal{P}$ restricts to $\mathcal{P}(x,x) = \mathcal{P}(x,-x) = p_1(x^2)$. Figure 1 depicts the Robinson Polynomial and its restrictions to these lines.

Now to prove that such a polynomial $\mathcal{P}$ is not SOS, requires to examine its zeros. For symmetric sextics $\mathcal{P}$ (such as $\mathcal{P}_{\mathrm{R}}$), Choi, Lam and Reznick showed in [CLR], that if $\mathcal{P}$ is an SOS, the zeros of $\mathcal{P}$ lie on a circle. Taking a close look at the structure of (1.1), this shows that if the p_i have real zeros, these must coincide. This is not the case for $\mathcal{P}_{\mathrm{R}}$ (see Figure 1 and Example 6.2), so this polynomial is a not sums of squares.

How can this be generalized to polynomials of degree more than 6? It turns out that this is possible for a class of special polynomials. In Theorem 6.1 we show that a polynomial fulfilling (1.1), can only be an SOS if one has $\sum_{i=1}^{m} 1/\beta_{0,i} = \sum_{j=1}^{m} 1/\beta_{1,j}$ where the $\beta_{k,i} \neq 0$ are the real zeros of the p_k.

2. Structure

This paper is organized as follows:

First we introduce some notation in Sections 3 and 4. In Section 5 we present a general construction for symmetric PSD-polynomials, which we extend to explicit examples of PSD-polynomials which are not SOS in Sections 6 and 7. In Section 8 we introduce some basic notation on group-invariant polynomials, which we use in Section 9 to prove the main theorem. Finally we give some outlook and concluding remarks in Section 10

3. Notation

Let $\mathbb{R}_{\geq 0} := \{t \in \mathbb{R} \ : \ t \geq 0\}$. In this paper all polynomials used are either univariate or bivariate polynomials with *real* coefficients. The corresponding ring of real polynomials in *two* variables x and y is denoted by $\mathbb{R}[x,y]$.

A polynomial $p \in \mathbb{R}[x,y]$ is called positive semi-definite (PSD), if $p(x,y) \geq 0$ holds for all $(x,y) \in \mathbb{R}^2$. Moreover, p is a *sum of squares* (SOS), if it can be rewritten as $p(x,y) = \sum_{i=1}^{n} q_i(x,y)^2$ for some $q_i \in \mathbb{R}[x,y]$ and $n \in \mathbb{N}$. The latter certifies that p is PSD.

By $[x^k y^l]^d$ denote the column-vector of monomials $x^k y^l$ with degree at most d, e.g., $[x^k y^l]^2 = (1, x, y, x^2, xy, y^2)^T$. A classification of SOS polynomials is the following; a polynomial $p(x,y)$ of degree $2d$ is an SOS, if and only if there is a positive-semidefinite (PSD) matrix $A \in \mathbb{R}^{N \times N}$ (of appropriate size N), such that

$$p(x,y) = \left([x^k y^l]^d\right)^T A \, [x^k y^l]^d.$$

This certificate of positivity is easy to check, so it is of high practical importance and widely used in relaxations of polynomial optimization problems.

Co-PSD polynomials. Later on, we evaluate univariate polynomials at x^2+y^2, the following characterizes polynomials where the result is non-negative:

Definition 3.1. *A univariate polynomial $\mathfrak{p}(t)$ is called co-positive-semidefinite (co-PSD) if $\mathfrak{p}(t) \geq 0$ holds for every $t \geq 0$.*

Corollary 3.2. *A co-PSD polynomial $\mathfrak{p}$ has a positive leading coefficient and $\mathfrak{p}(\alpha) = 0$ for some $\alpha \geq 0$ implies $\mathfrak{p}'(\alpha) = 0$ (in fact the order of such zeros is even).*

Lemma 3.3. *Let $\mathfrak{p} \in \mathbb{R}[t]$ be a univariate co-PSD polynomial with a zero of order $2k \in \mathbb{N}$ at $\alpha \in \mathbb{R}_{\geq 0}$. If $\mathfrak{p} = \sum_{i=1}^n \mathfrak{q}_i$ holds for some co-PSD polynomials $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$, then each $\mathfrak{q}_i$ has a zero of order at least $2k$ at α, i.e., $\mathfrak{q}_i$ is in the ideal generated by $(t-\alpha)^{2k}$.*

Note that for $2k = 2$, Lemma 3.3 just states that each $\mathfrak{q}_i$ must have zeros in $\mathbb{R}_{\geq 0}$ wherever $\mathfrak{p}$ does, which is trivial. The interesting part of Lemma 3.3 is, that the *multiplicity* of non-negative real zeros is preserved.

Proof of Lemma 3.3. Induction: Lemma 3.3 is true for $k = 1$, since $0 = \mathfrak{p}(\alpha) = \sum \mathfrak{q}_i(\alpha)$, implies $\mathfrak{q}_i(\alpha) = 0$, which together with Corollary 3.2 proves the lemma. For arbitrary k, we observe that by Corollary 3.2, one can factor out $(t-\alpha)^2$ on both sides.

$$\mathfrak{p}(t) = \tilde{\mathfrak{p}}(t)(t-\alpha)^2 = \sum_{i=1}^n \tilde{\mathfrak{q}}_i(t)(t-\alpha)^2$$

where $\mathfrak{q}_i(t) = \tilde{\mathfrak{q}}_i(t)(t-\alpha)^2$ and $\tilde{\mathfrak{p}}, \tilde{\mathfrak{q}}_1, \ldots, \tilde{\mathfrak{p}}_n$ are co-PSD. Dividing by $(t-\alpha)^2$ on both sides, one reduces the proof to the case of $k-1$. □

4. Polynomials expressed in harmonic basis

One of the main tools of this paper is the use of harmonic polynomials as a basis of $\mathbb{R}[x,y]$.

Definition 4.1. *For $k \in \mathbb{N}$ the k^{th} harmonic polynomials $g_k, h_k \in \mathbb{R}[x,y]$ are defined by*

$$g_k(x,y) := \operatorname{Re}\left((x+iy)^k)\right) \quad \text{and} \quad h_k(x,y) := \operatorname{Im}\left((x+iy)^k)\right). \tag{4.1}$$

Define in addition $r(x,y) := \sqrt{x^2+y^2}$ (observe that $r^2(x,y)$ is a polynomial).

Lemma 4.2. *The polynomials $r^{2\ell}$, $r^{2\ell}g_k$, and $r^{2\ell}h_k$ with $k, \ell \in N$ and $k > 0$ form a basis of $\mathbb{R}[x,y]$.*

For a proof see [AAR]. This representation of p is of particular interest in this paper, since the polynomials $r^{2\ell}$, $r^{2\ell}g_k$, and $r^{2\ell}h_k$ have "elementary symmetries". This is a bit more obvious in polar-coordinates. Rewriting $x+iy = re^{i\phi}$ with some $\phi \in [0, 2\pi]$, one obtains

$$g_k(x,y) = \operatorname{Re}((re^{i\phi})^k) = r^k \cos(k\phi) \qquad h_k(x,y) = \operatorname{Im}((re^{i\phi})^k) = r^k \sin(k\phi).$$

From this one directly derives the addition formulas (known from trigonometric functions)

$$\begin{array}{lcl} g_k^2 + h_k^2 & = & r^{2k}, \\ g_k g_\ell - h_k h_\ell & = & g_{k+\ell}. \end{array} \tag{4.2}$$

5. Marrying polynomials

In this work we essentially "glue together" two univariate polynomials in a process we call "marrying". The 'glue' we use is a nonnegative partition of unity, i.e., $g_k^2/r^{2k} + h_k^2/r^{2k} = 1$. As in real life, polynomials that can be married must fit to some extent: Two univariate polynomials P, Q satisfy $(P(t) \equiv Q(t) \bmod t^k)$ if and only if they differ only in the coefficients for $t^k, t^{k+1}, \ldots$, i.e.,

$$\begin{array}{lcl} P(t) & = & a_0 + a_1 t + \ldots + a_{k-1}t^{k-1} + t^k \overline{P}(t) \\ Q(t) & = & a_0 + a_1 t + \ldots + a_{k-1}t^{k-1} + t^k \overline{Q}(t) \end{array}$$

holds for some univariate polynomials $\overline{P}, \overline{Q}$ and coefficients $a_0, \ldots, a_{k-1} \in \mathbb{R}$. In this work we are only interested in polynomials P, Q with non-trivial zeros, which we normalize such that $P(0) = Q(0) = 1$. The Newton-Girard formulas ([S00]) give a characterization of such "matching" polynomials in terms of their zeros:

Lemma 5.1 (algebraic characterization)**.** *For $P, Q \in \mathbb{R}[t]$, let $P(t) = \prod_{i=1}^{m}(\alpha_i t - 1)$ and $Q(t) = \prod_{i=1}^{n}(\beta_i t - 1)$, where $\alpha_i, \beta_i \in \mathbb{C} \setminus \{0\}$. For any $k \in \mathbb{N}$, one finds*

$$P(t) \equiv Q(t) \mod t^k \quad \Longleftrightarrow \quad \sum_{i=1}^{m} \alpha_i^\ell = \sum_{i=1}^{n} \beta_i^\ell \quad \forall \ell = 1, \ldots, k-1.$$

The proof is a direct application of the Newton-Girard formulas ([S00]) for symmetric polynomials. As an example one might check that for $k = 2$ we find $P(t) \equiv 1 - t\sum_{i=1}^{m} \alpha_i \mod t^2$ and $Q(t) \equiv 1 - t\sum_{i=1}^{n} \beta_i \mod t^2$ proving the lemma for $k = 2$.

Lemma 5.2. *Let $P, Q \in \mathbb{R}[t]$ be univariate polynomials where $P(t) \equiv Q(t) \mod t^k$. Then*

$$\mathrm{M}_k(P, Q) := \frac{g_k^2 P(r^2) + h_k^2 Q(r^2)}{r^{2k}}$$

is (i) a polynomial in two variables which results from marrying P and Q. Moreover,(ii) if P and Q are co-PSD, then $\mathrm{M}_k(P, Q)$ is PSD.

As we will see later, the resulting polynomials have D_{2k}-symmetry, i.e., the function stays invariant under rotation of the input (x, y) by an angle of $2\pi/2k$. Take a look at Figure 1, how the graph of such a function looks like.

Proof. The coefficients of $r^0, r^2, \ldots, r^{2k-2}$ in both $P(r^2)$ and $Q(r^2)$ are equal, therefore there are $p_0,\ \overline{P},\ \overline{Q} \in \mathbb{R}[t]$ such that

$$P(r^2) = p_0(r^2) + r^{2k}\overline{P}(r^2) \qquad Q(r^2) = p_0(r^2) + r^{2k}\overline{Q}(r^2).$$

With this it becomes clear that r^{2k} divides $g_k^2 P(r^2) + h_k^2 Q(r^2)$:

$$\begin{array}{rcll} g_k^2 P(r^2) & = & g_k^2 p_0(r^2) & +g_k^2\ r^{2k}\ \overline{P}(r^2) \\ h_k^2 Q(r^2) & = & +h_k^2 p_0(r^2) & +h_k^2\ r^{2k}\ \overline{Q}(r^2) \\ \hline g_k^2 P(r^2) + h_k^2 Q(r^2) & = & \underbrace{\left(g_k^2 + h_k^2\right)}_{=r^{2k}\ \text{[see (4.2)]}}\ p_0(r^2) & +r^{2k}\left(g_k^2\overline{P}(r^2) + h_k^2\overline{Q}(r^2)\right). \end{array}$$

Therefore $\mathrm{M}_k(P, Q)$ is a polynomial. If in addition P and Q are co-PSD, then $P(r^2)$ and $Q(r^2)$ are non-negative, since r^2 only attains positive values. All other terms in $\mathrm{M}_k(P, Q)$ are squares, so $\mathrm{M}_k(P, Q)$ is non-negative. □

5.1. **Basic cases I.** Marrying polynomials that trivially fit leads to an SOS:

Lemma 5.3. *Let $\mathfrak{p}, \mathfrak{q} \in \mathbb{R}[t]$ be univariate co-PSD polynomials and let $k \in \mathbb{N}$ Then $\mathrm{M}_k(t^k\mathfrak{p}, t^k\mathfrak{q})$ is SOS.*

Proof. Direct calculation shows

$$\mathrm{M}_k(t^k\mathfrak{p}, t^k\mathfrak{q}) = \frac{g_k^2 r^{2k}\ \mathfrak{p}(r^2) + h_k^2 r^{2k}\ \mathfrak{q}(r^2)}{r^{2k}} = g_k^2\ \mathfrak{p}(r^2) + h_k^2\ \mathfrak{q}(r^2),$$

where $\mathfrak{p}(r^2)$ and $\mathfrak{q}(r^2)$ are non-negative *univariate* polynomials with respect to r and thus SOS with respect to r (see [Hi]). □

5.2. **Basic cases II.** Marrying squares leads to an SOS:

Lemma 5.4. *Let $P, Q \in \mathbb{R}[t]$ be univariate PSD polynomials where $P^2(0) = Q^2(0) \neq 0$ and $P^2(t) \equiv Q^2(t) \mod t^k$ holds for some $k, \ell \in \mathbb{N}$. Then $\mathrm{M}_k(P^2, Q^2)$ is SOS.*

Proof. First of all $M_k(P^2, Q^2)$ is a *polynomial* due to Lemma 5.2 which now we prove is SOS. With a bit of work and the addtion formulas in (4.2), one first verifies $2M_k(P^2, Q^2) = P^2(r^2) + Q^2(r^2) + (P^2(r^2) - Q^2(r^2))g_{2k}/r^{2k}$ and then

$$4M_k(P^2, Q^2) = \left(P(r^2) + Q(r^2) + g_{2k}\frac{P(r^2) - Q(r^2)}{r^{2k}}\right)^2 \quad + \left(h_{2k}\frac{P(r^2) - Q(r^2)}{r^{2k}}\right)^2.$$

So what is left to prove is that r^{2k} divides $P(r^2) - Q(r^2)$, or equivalently $P(t) \equiv Q(t) \mod t^k$. Due to $P^2(0) = Q^2(0) \neq 0$ we might assume w.l.o.g that $P(0) = Q(0)$ holds, implying that $P(t) = c\prod_{i=1}^{m}(\alpha_i t - 1)$ and $Q(t) = c\prod_{i=1}^{n}(\beta_i t - 1)$ hold for some $c \in \mathbb{R}$ and $\alpha_i, \beta_i \in \mathbb{C} \setminus \{0\}$. Comparing the formulas in Lemma 5.1 for the pairs P^2, Q^2 and

P, Q one sees that $P^2(t) \equiv Q^2(t) \mod t^k$ implies $P(t) \equiv Q(t) \mod t^k$. This proves that $M_k(P^2, Q^2)$ is an SOS. □

5.3. **Interesting cases.** So marrying squares or trivially fitting co-PSD polynomials yields an SOS. But when is the result not SOS? We provide the following *necessary* condition for $\mathrm{M}_k(P, Q)$ to be SOS, and then show constructions violating this condition.

Theorem 5.5. *Let P, Q be two co-PSD polynomials with $P \equiv Q \mod t^k$. Then if the polynomial $M_k(P, Q)$ is SOS, there are polynomials $p, q \in \mathbb{R}[t]$ and co-PSD polynomials $\mathfrak{p}, \mathfrak{q} \in \mathbb{R}[t]$ such that*

$$P(t) = p^2(t) + t\mathfrak{p}(t) \quad \text{and} \quad Q = q^2(t) + t\mathfrak{p}(t) \quad \text{where} \tag{5.1}$$

$$p(t) \equiv q(t) \mod t^k \quad \text{and} \quad t\mathfrak{p}(t) \equiv t\mathfrak{q}(t) \mod t^k \tag{5.2}$$

This means that $M_k(P, Q) = M_k(p^2, q^2) + r^2 M_k(\mathfrak{p}, \mathfrak{q})$ where $M_k(p^2, q^2)$ and $r^2 M_k(\mathfrak{p}, \mathfrak{q})$ are (PSD) polynomials.

Proof. Theorem 5.5 is a direct consequence of Theorem 9.1. □

Concerning the dissection (5.1) there is something special about positive zeros. The positive zeros of P are inherited – including their multiplicity – by both p^2 and $\mathfrak{p}$ – in contrast other zeros of P. Similar, q^2 and $\mathfrak{q}$ share the positive zeros with Q.
Before we come to the proof of Theorem 5.5 we shall actually construct polynomials P, Q violating (5.2). The idea is to make sure that the zeros of P and Q uniquely determine p, q, ensuring that (5.2) fails to hold.

6. Construction I: The Motzkin-Robinson Family

The following presents a symmetric polynomial, defined via its zeros, which is not an SOS if these zeros violate a single (non-linear) equation. The corresponding family of polynomials generalizes the well known Robinson and Motzkin polynomials. The construction involves marrying two univariate, co-PSD polynomials via spherical harmonics. The following procedure can by the way be extended to polynomials in an arbitrary amount of variables, as we shall indicate in the final section.

Theorem 6.1 (The Motzkin-Robinson family of polynomials)**.** *Let $m, n \in \mathbb{N}$ be some integers, and $\alpha_1, \dots, \alpha_m \in \mathbb{R}_+$ and $\beta_1, \dots, \beta_n \in \mathbb{R}_+$ positive numbers. Choose further some $\gamma \in \mathbb{R}$ with $\gamma \geq -2\min\{\sum_{i=1}^m \alpha_i, \sum_{i=1}^n \beta_i\}$. Define $\gamma_1 := \gamma + 2\sum_{i=1}^m \alpha_i$ and $\gamma_2 := \gamma + 2\sum_{i=1}^n \beta_i$. Then*

$$\begin{array}{rcccc} \mathcal{F}_{MR} & := & (g_2)^2/r^4 & (1+\gamma_1 r^2)\prod_{i=1}^m(\alpha_i r^2 - 1)^2 \\ & + & (h_2)^2/r^4 & (1+\gamma_2 r^2)\prod_{i=1}^n(\beta_i r^2 - 1)^2 \end{array} \tag{6.1}$$

is (i) a PSD *polynomial, that (ii) is an SOS if and only if $\sum_{i=1}^m \alpha_i = \sum_{i=1}^n \beta_i$.*

Note that the α_i do not need to be pairwise different (nor do the β_i). Though defined as a rational function, P is indeed a polynomial: Due to the choice of γ_1, γ_2, one has $\mathcal{F}_{MR} = \mathrm{M}_2(P, Q)$ for some $P(t) \equiv Q(t) \mod t^2$. Before we fully prove Theorem 6.1, here are two famous examples (note: $g_2(x, y) = 2xy$ and $h_2(x, y) = x^2 - y^2$):

Example 6.1 (The Motzkin Polynomial)**.** *Set $m = 0$, $n = 1$ and $\beta_1 = 1/2$ and $\gamma = 0$. This leads to $\gamma_1 = 0$ and $\gamma_2 = 1$ resulting in the Motzkin Polynomial*

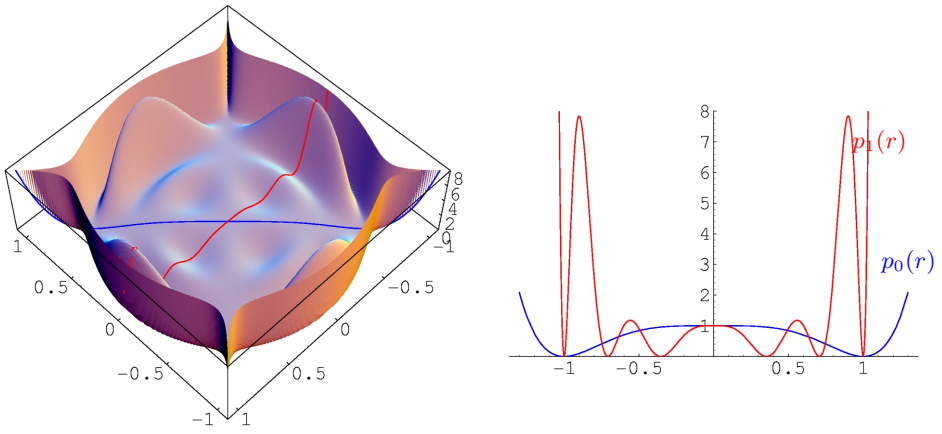
$$\begin{array}{rcl} P_{\mathrm{M}}(x, y) & = & 1 + (x^2+y^2)^2 \frac{(2xy)^2}{(x^2+y^2)^2}(-3 + x^2 + y^2)/4 \\ & = & 1 - 3x^2y^2 + x^4y^2 + x^2y^4. \end{array}$$

Example 6.2 (The Robinson Polynomial)**.** *Set $m = n = 1$ and $\alpha_1 = 1$, $\beta_1 = 1/2$ and $\gamma = -1 = -2\min\{\alpha_1, \beta_1\}$. This leads to $\gamma_1 = 1$ and $\gamma_2 = 0$ resulting in the Robinson Polynomial*

$$\begin{array}{rcl} P_{\mathrm{R}}(x, y) & = & \frac{(x^2-y^2)^2}{(x^2+y^2)^2}(1 + x^2 + y^2)(x^2 + y^2 - 1)^2 + \frac{x^2y^2}{(x^2+y^2)^2}(2x^2 + 2y^2 - 1)^2 \\ & = & x^2(-1+x^2)^2 + y^2(-1+y^2)^2 - (-1+x^2)(-1+y^2)(-1+x^2+y^2). \end{array}$$

The last equation requires to observe that $(x^2 - y^2)^2 + 4x^2y^2 = (x^2 + y^2)^2$, or expressed in harmonics: $g_2^2 + h_2^2 = r^4$.

FIGURE 2. Example 6.3: a PSD-polynomial which is not SOS



Example 6.3. *The following polynomial was chosen due to its "nice" graph depicted in Figure 2: Setting* $m = 3$, $\beta = (1, 2, 8)$, $n = 1$, $\alpha_1 = 1$ *and* $\gamma = 0$ *leads to the following PSD polynomial which is not SOS:*

$$1 - 311x^4 + 3202x^6 - 12260x^8 + 21784x^{10} - 18048x^{12} + 5632x^{14} + 610x^2y^2 - 3194x^4y^2 \\ +21784x^8y^2 - 36096x^{10}y^2 + 16896x^{12}y^2 - 311y^4 - 3194x^2y^4 + 24520x^4y^4 - 43568x^6y^4 \\ +18048x^8y^4 + 5632x^{10}y^4 + 3202y^6 - 43568x^4y^6 + 72192x^6y^6 - 28160x^8y^6 - 12260y^8 \\ +21784x^2y^8 + 18048x^4y^8 - 28160x^6y^8 + 21784y^{10} - 36096x^2y^{10} + 5632x^4y^{10} - 18048y^{12} \\ +16896x^2y^{12} + 5632y^{14}.$$

Proof of Theorem 6.1. Assume the prerequisites of Theorem 6.1 hold.
(i) One finds that $\mathcal{F}_{MR} = M_2(P, Q)$ holds for the polynomials

$$P(t) := (1 + \gamma_1 t) \prod_{i=1}^{m} (\alpha_i t - 1)^2 \quad \textbf{and} \quad Q(t) := (1 + \gamma_2 t) \prod_{i=1}^{n} (\beta_i t - 1)^2. \tag{6.2}$$

Expanding P and Q yields

$$P(t) = 1 + t \left(\gamma_1 - 2 \sum_{i=1}^{m} \alpha_i \right) + t^2 \mathfrak{p}(t) \quad \textbf{and} \quad Q(t) = 1 + t \left(\gamma_2 - 2 \sum_{i=1}^{m} \beta_i \right) + t^2 \mathfrak{q}(t)$$

for some polynomials $\mathfrak{p}$, $\mathfrak{q}$. So the special choice of γ_1, γ_2 leads to $P \equiv Q \mod t^2$. Moreover, P and Q are co-PSD since in (6.2) $\gamma_1, \gamma_2 \geq 0$ holds. So by Lemma 5.2, $\mathcal{F}_{MR}$ is a PSD polynomial.

(ii) if-part Assume $\mathcal{F}_{MR}$ is SOS. Then by Theorem 5.5, we can decompose

$$P(t) = p^2(t) + t\mathfrak{p}(t) \quad \textbf{and} \quad Q(t) = q^2(t) + t\mathfrak{q}(t), \tag{6.3}$$

where p, q are some univariate polynomials and $\mathfrak{p}, \mathfrak{q}$ are some co-PSD polynomials fulfilling $p \equiv q \mod t^2$ and $\mathfrak{q} \equiv \mathfrak{q} \mod t$.
Both p^2 and $t\mathfrak{p}$ are co-PSD so their degrees can not exceed $\deg(P) = 2m + 1$, implying $\deg(p^2), \deg(\mathfrak{p}) \leq 2m$. Now Lemma 3.3 states that p^2 and $t\mathfrak{p}$ are in the ideal generated by $\prod_{i=1}^{m}(\alpha_i t - 1)^2$, and thus they either have degree *at least* $2m$ or they are the zero polynomial. The polynomial p can not be zero (it carries the constant term of P), thus $\deg(p^2) = 2m$. Comparing the zeros and constant terms of P and p^2, one finds that $p^2(t) = \prod_{i=1}^{m}(\alpha_i t - 1)^2$. The same argumentation holds for q and $\mathfrak{q}$ leading to $q^2(t) = \prod_{i=1}^{n}(\beta_i t - 1)^2$. So if $\mathcal{F}_{MR}$ is SOS then $\prod_{i=1}^{m}(\alpha_i t - 1)^2 \equiv \prod_{i=1}^{n}(\beta_i t - 1)^2 \mod t^2$ holds, equivalent to $\sum_{i=1}^{m} \alpha_i = \sum_{i=1}^{n} \beta_i$.

(ii) only-if-part Assume $\sum_{i=1}^{m} \alpha_i = \sum_{i=1}^{n} \beta_i$ holds, which by choice of $\gamma_1, \gamma_2 \geq 0$ implies $\gamma_1 = \gamma_2$. Define $p(t) := \prod_{i=1}^{m}(\alpha_i t - 1)$ and $q(t) := \prod_{i=1}^{n}(\beta_i t - 1)$. From (6.2)

one concludes $P(t) = p^2(t)(1+\gamma_1 t)$ **and** $Q(t) = q^2(t)(1+\gamma_1 t)$ **and thus by linearity of** $M_2(\cdot,\cdot)$ **one has**

$$M_2(P,Q) = (1+\gamma_1 r^2) M_2(p^2, q^2),$$

where $M_2(p^2,q^2)$ **is SOS by Lemma 5.4.** □

7. Construction II: The Motzkin Family

In contrast to the last section, the polynomials derived here have a higher order dihedral symmetry. To keep things relatively easy, we restrict to marrying a rather simple univariate polynomial to a constant polynomial. This results in a family of polynomials with the shape of the Motzkin polynomial, see Example 7.1. Note that exploiting the upcoming Theorem 7.2, one can certainly do more.

Theorem 7.1 (The Motzkin-family)**.** *Let* $k \in \mathbb{N}$ *where* $k \geq 2$*. Then*

$$\mathcal{F}_M \quad := \quad 1 + g_k^2(-(k+1) + kr^2) \tag{7.1}$$

is (i) a PSD polynomial, which is (ii) is not SOS.

Before we give the proof of Theorem 7.1, here are some examples, the first is the scaled Motzkin-Polynomial $1 - 3x^2y^2 + 4x^4y^2 + 4x^2y^4$:

Example 7.1. *Here are some examples of the polynomials resulting from Theorem 7.1:*

k	$1 + (g_k)^2(kr^2 - k - 1)$
2	$1 - 12x^2y^2 + 8x^4y^2 + 8x^2y^4$
3	$1 - 36x^4y^2 + 27x^6y^2 + 24x^2y^4 + 9x^4y^4 - 4y^6 - 15x^2y^6 + 3y^8$
4	$1 - 80x^6y^2 + 64x^8y^2 + 160x^4y^4 - 64x^6y^4 - 80x^2y^6 - 64x^4y^6 + 64x^2y^8$
5	$1 - 150x^8y^2 + 120x^2y^8 - 6y^{10} - 660x^4y^6 + 600x^6y^4 +$ $+125x^{10}y^2 - 375x^8y^4 + 50x^6y^6 + 450x^4y^8 - 95x^2y^{10} + 5y^{12}$

These polynomials have a (dihedral) D_{2k}*-symmetry and* $2k$ *zeros at* $(\cos(t_{k,\ell}), \sin(t_{k,\ell})) \in \mathbb{R}^2$ *where* $t_{k,\ell} := \frac{1+4\ell}{4k} 2\pi$*. A plot can be found in Figure 3.*

Proof of Theorem 7.1. Theorem 7.1 is a direct consequence of Theorem 7.2. Note that $\mathcal{F}_M$ is actually a marriage between $P_k(t) := 1 - (k+1)t^k + kt^{k+1}$ and $Q(t) := 1$, i.e., one finds

$$\mathcal{F}_M \;=\; M_k(P_k, Q) \;=\; \frac{g_k^2 P_k(r^2) + h_k^2 Q(r^2)}{r^{2k}}.$$

We now show that $\mathcal{F}_M$ can not be an SOS, since the degree of $\deg(P_k)$ is too low.
Observe that P_k is co-PSD, since it is the product of two co-PSD polynomials $P_k(t) = (1-t)^2(\sum_{i=0}^{k-1}(i+1)t^i)$ – see proof of Lemma 7.3. Since $P_k(1) = 0$, and P_k is co-PSD we conclude from Theorem 7.2, that if $M_k(P_k, 1)$ was SOS, then $\deg(P_k) = k+1 = 2k$ should hold, implying $k = 1$. This contradicts the assumptions on k, showing that $\mathcal{F}_M$ is not SOS. □

Theorem 7.2. *Let* $k \in \mathbb{N}$ *and let* P *be any co-PSD polynomial with* $P(1) = 0$*,* $\deg(P) \leq 2k$ *and* $P(t) \equiv 1 \mod t^k$*.*
Then $M_k(P,1)$ *is (i) a PSD polynomial, which is (ii) SOS if and only if*

$$P(t) = (1-t^k)^2 + t^k\, \mathfrak{p}(t) \tag{7.2}$$

holds for some co-PSD polynomial $\mathfrak{p}(t)$*, implying* $\deg(P) = 2k$*.*

Proof. From Lemma 5.2 we derive that $M_k(P,1)$ is a PSD polynomial, proving part (i). Assume that (7.2) holds, then $M_k(P,1)$ is SOS: exploiting linearity of $\mathrm{M}_k(\cdot,\cdot)$ yields

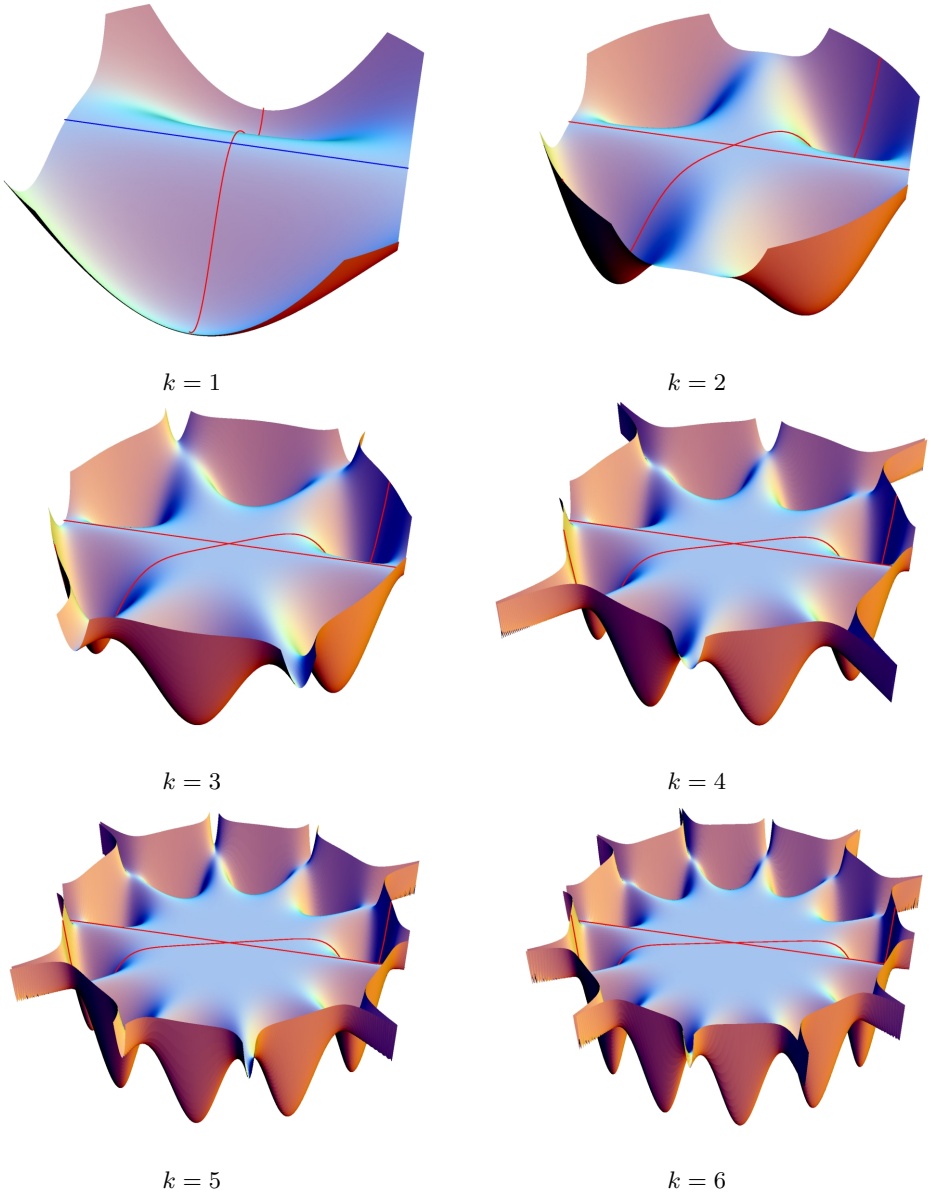
$$M_k(P,1) \quad = \quad M_k((1-t^k)^2, 1^2) \;+\; M_k(t^k\mathfrak{p}, t^k\, 0),$$

where the first summand is SOS since it is the marriage of two squares (Lemma 5.4) and the second is SOS since it is the marriage of to trivially fitting co-PSD polynomials (Lemma 5.3).
Now assume that $M_k(P,1)$ is SOS, then according to Theorem 5.5, we can split

$$P(t) = p(t)^2 + t\tilde{\mathfrak{p}}(t) \quad \text{and} \quad 1 = q(t)^2 + t\mathfrak{q}(t)$$

where $\mathfrak{p}, \mathfrak{q}$ are co-PSD, and moreover $p \equiv q \mod t^k$ and $t\tilde{\mathfrak{p}} \equiv t\mathfrak{q} \mod t^k$ hold.

FIGURE 3. The family of Motzkin-polynomials $\mathcal{F}_M = (1 + g_{2k}(kr^2 - (k+1))$.



The equation $1 = q(t)^2 + t\mathfrak{q}(t)$ directly implies $\mathfrak{q} = 0$ and $q^2 = 1$, implying $t\tilde{\mathfrak{p}}(t) \equiv 0 \mod t^k$. So there is some co-PSD polynomial $\mathfrak{p}$, fulfilling $t\tilde{\mathfrak{p}}(t) = t^k\mathfrak{p}(t)$.
Finally, since both p^2 and $\mathfrak{p}$ are co-PSD, $p(1) = \mathfrak{p}(1) = P(1) = 0$ must hold. Lemma 7.3 states that this implies $p^2(t) = (1-t^k)^2$, finally proving the theorem. □

Lemma 7.3. *Fix $k \in \mathbb{N}\setminus\{0\}$. The polynomial $p^2(t) := (1-t^k)^2$ is the only square fulfilling*

(7.3) $\quad (i)\ \deg(p^2) \le 2k, \quad (ii)\ p(1) = 0 \quad \textit{and} \quad (iii)\ p(t) \equiv 1 \mod t^k.$

Proof. Let $k \in \mathbb{N}$ and let $q^2 \in \mathbb{R}[t]$ fulfill (7.3). Then due to (ii) we find $q(t) = c(t)(1-t)$ for some $c(t) \in \mathbb{R}[t]$ where $\deg(c) \le k-1$ due to (i). To find first coefficients of $c(t)$, we exploit the equations arising from (iii), i.e., $c^2(t)(1-t)^2 \equiv 1 \mod t^k$, which uniquely determine $a_0, \dots, a_{k-1}$, the first $k-2$ coefficients of c^2. Writing $(1-t)^2 \sum_{i=0}^{k-1} a_i t^i \equiv 1$

mod t^k, one obtains the recurrence relations

$$\begin{array}{lrcll} t^0: & a_0 & = & 1 & \\ t^1: & -2a_0+a_1 & = & 0 & \\ t^\ell: & a_{\ell-2}-2a_{\ell-1}+a_\ell & = & 0 & \text{for } \ell=2,\dots k-1. \end{array}$$

Induction on ℓ shows $a_\ell = \ell+1$, implying $c^2(t) \equiv \sum_{i=0}^{k-1}(i+1)t^i \mod t^k$, or expanded:

$$(1-2t+t^2)\left(1+2t+3t+\cdots+(k-1)t^{k-2}\right) = 1+0t+\cdots+0t^{k-1}-(k-1)t^k+kt^{k+1}.$$

Comparing coefficients in $c^2(t) \equiv \sum_{i=0}^{k-2}(i+1)t^i \mod t^k$ we get the following recurrence relations for the coefficients $c_0,\dots,c_{k-1}$ of c

$$\begin{array}{lrcll} t^0: & c_0^2 & = & 1 & \\ t^1: & 2c_0c_1 & = & 2 & \\ t^\ell: & 2c_0c_\ell+\sum_{i=1}^{\ell-1}c_{\ell-i}c_i & = & \ell & \text{for } \ell=2,\dots k-1. \end{array}$$

Induction on ℓ shows that either $c_0=\ldots=c_{k-1}=1$ or $c_0=\ldots=c_{k-1}=-1$ hold. In both cases we obtain a telescope sum:

$$q^2(t) = (1-t)^2c(t)^2 = \left((1-t)(\sum_{i=1}^{k-1}t^i)\right)^2 = (1-t^k)^2.$$

□

8. Symmetry - the invariant spaces of D_{2k}

8.1. **Motivation.** The goal of this section is to prepare results for Theorem 9.1. This theorem limits the shape of an SOS $\mathcal{F}$ which has some rotational symmetry, see Figure 3 for a plot of such a function.
We exploit, that the symmetry of $\mathcal{F}$ implies symmetry of the linear matrix inequality (LMI) $\mathcal{F} = \vec{p}^T A\vec{p}$, where $A \in \mathbb{R}^N$ with $A \succeq 0$ and $\vec{p} \in \mathbb{R}[x]^N$ is some vector of polynomials. We use group-representation theory to blockdiagonalize A.
Symmetries of a polynomial $p \in \mathbb{R}[x,y]$ are essentially automorphisms $f: \mathbb{R}^2 \to \mathbb{R}^2$, that leave p invariant, i.e., $p(f(x,y)) = p(x,y)$. Its immediately clear, that the automorphisms under which p is invariant form a group G. If the corresponding polynomial p is SOS, then it can written as $p = \sum p_i^2 + \sum q_j^2$, where the p_i are again G-invariant polynomials and the q_j are "semi-invariant" (see [GP]).

Example 8.1. *Let's look at* even *SOS: Every univariate even SOS is the sum of squared odd or squared even polynomials, e.g.*

$$t^4+t^2+1 = (\underbrace{t^2-1}_{even})^2 + (\underbrace{t}_{odd})^2.$$

Here the group is $\mathbb{Z}_2 = \{-id, id\}$ and its action on $\mathbb{R}[t]$ is defined by $id(p(t)) = p(t)$ and $-id(p(t)) = p(-t)$. A univariate polynomial p is $\mathbb{Z}_2$-invariant if p is even, i.e., if $p(t) = p(-t)$, and p is semi-invariant if p is odd, i.e. $p(t) = -p(-t)$ holds.

To generalize Example 8.1 we need some notation from group-representation theory:
We first need to take a look at the group of automorphisms of $\mathbb{R}^2$ we consider in this paper. We then check which spaces of polynomials it leaves invariant.

8.2. **Representations of the even dihedral group.** The group of automorphisms examined in this paper is the even dihedral group D_{2n}, a subgroup of the symmetric group S_n, which represents a set of finite rotations and reflections in $\mathbb{R}^2$.

Definition 8.1. *The dihedral group D_{2n} is the non-commutative group generated by a, b where $a^2 = id$, $b^{2n} = id$, and $aba = b^{-1}$ (Here id is the identity of D_{2n}).*

Due to $ba = ab^{-1} = ab^{2n-1}$ every element of D_{2n} is of the form a^ib^j, $i \in \{0,1\}$ and $j \in \{1,\dots,2n-1\}$. Therefore D_{2n} has $4n$ elements. From group-representation theory we employ the following terminology:

Definition 8.2. *A representation of D_{2n} is a D_{2n}-homomorphism $\rho : D_{2n} \to GL(m)$, where $GL(m) \in \mathbb{R}^{m\times m}$ is the group of nonsingular matrices of dimension m. Two representations ρ_1, ρ_2 of D_{2n} are called* equivalent *($\rho_1 \simeq \rho_2$), if there is some $A \in \mathbb{R}^{m\times n}$ of rank $\min\{m,n\}$ such that $\rho_1 = A^T\rho_2 A$. The* character *of a representation of D_{2n} is the vector $\chi(\rho) := (Tr(\rho(g))_{g\in D_{2n}}$.*

Laymenly expressed, a representation ρ for D_{2n} is a set of matrices $\rho(g)$ mimicking the behavior of the elements $g_i \in D_{2n}$, i.e. , $\rho(g_1g_2) = \rho(g_1)\rho(g_2)$. And roughly, two representations are equivalent, if their matrices are the same, up to a basis-change.

Lemma 8.3. *Two representations ρ_1, ρ_2 of D_{2n} are equivalent if and only if $\chi(\rho_1) = \chi(\rho_2)$ (For a proof see* [GW]*).*

Definition 8.4. *For $\alpha \in [0, 2\pi]$ set*

$$A := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad B(\alpha) := \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}. \tag{8.1}$$

Lemma 8.5. *For $k \in \mathbb{N}$ define $\rho_k : D_{2n} \to O(2)$ by $\rho_k(a^ib^j) := A^i(B(\pi/n))^{kj}$. Then ρ_k is a representation of D_{2n}. Moreover $\rho_k \simeq \rho_{k'}$ if and only if either $(k \equiv k' \mod 2n)$ or $(k \equiv -k' \mod 2n)$ hold.*

Proof. Fix $k, n \in \mathbb{N}$ and set $\rho := \rho_k$ and $\widetilde{B} := B(\pi/n)^k$. To check that ρ is a representation of D_{2n}, it suffices to check $\rho(A)^2 = I$, $\rho(\widetilde{B})^{2n} = I$, and $\rho(A\widetilde{B}A) = \rho(\widetilde{B}^{-1})$. Concerning this, $A^2 = I$ and $\rho(A\widetilde{B}A) = \rho(\widetilde{B}^{-1})$ follow from direct calculation. Since $B(\alpha)$ is a rotation of $\mathbb{R}^2$ by an angle of α, one finds $B(\alpha)B(\beta) = B(\alpha+\beta)$. This proves $B(\pi/n)^{(2nk)} = B(2k\pi) = I$.

Choose $k, k' \in \mathbb{N}$ arbitrary. To check $\rho_k \simeq \rho_{k'}$, it suffices to examine the generators of D_{2n}: $\chi(\rho_k) = \chi(\rho_{k'})$ holds if and only if $Tr(\rho_k(a)) = Tr(\rho_{k'}(a))$ and $Tr(\rho_k(b)) = Tr(\rho_{k'}(b))$ (see Lemma 8.3). The first equation holds trivially by $\rho_k(a) = A = \rho_{k'}(a)$. The second is equivalent to $2\cos(k\pi/n) = 2\cos(k'\pi/n)$ which is equivalent to $(k \equiv \pm k' \mod 2n)$, which eventually proves the lemma. □

8.3. **Group action of D_{2n} and invariant subspaces.** The action of D_{2n} on $\mathbb{R}[x, y]$ finally is what defines a "symmetric" polynomial in the setting of this paper.

Definition 8.6. *The* **canonic action** *of $D_{2n} =< a, b >$ on $\mathbb{R}[x, y]$ is defined by*

$$(a^ib^j(p))\,(x, y) := p\left(A^iB(\pi/n)^j\begin{pmatrix} x \\ y \end{pmatrix}\right) \quad \text{for every } p \in \mathbb{R}[x, y].$$

A polynomial p is called **$\mathbf{D_{2n}}$-invariant** *if $g(p) = p$ holds for every $g \in D_{2n}$.*

The latter is essentially a "sophisticated" way of saying that $p(x, y)$ is invariant under rotating (x, y) by an angle of π/n.

Definition 8.7. *A subspace V of $\mathbb{R}[x, y]$ is called* **$\mathbf{D_{2n}}$-invariant** *if $g(p) \in V$ holds for every $p \in V$ and $g \in D_{2n}$, in addition V is* **minimally** *D_{2n}-invariant if V contains no nontrivial, D_{2n}-invariant subspace.*

Restricting of the group action to an invariant subspace yields a representation of D_{2n}:

Lemma 8.8. *Let $V \subseteq \mathbb{R}[x, y]$ be a d-dimensional D_{2n}-invariant subspace with some basis $\mathcal{B}$. For each $g \in D_{2n}$ let $\rho_{\mathcal{B}}(g) \in \mathbb{R}^{d\times d}$ be the representing matrix relative to the basis $\mathcal{B}$ of the linear mapping $g : V \to V$. Then $\rho_{\mathcal{B}} : D_{2n} \to \mathbb{R}^{d\times d}$ is a representation of D_{2n}. (For a proof see* [GW].*)*

Definition 8.9. *Two D_{2n}-invariant subspaces $V, W \subset \mathbb{R}[x, y]$ with bases $\mathcal{B}_V$, $\mathcal{B}_W$ are called* **$\mathbf{D_{2n}}$-isomorphic** *($V \simeq W$) if the corresponding representations $\rho_{\mathcal{B}_V}(g)$ and $\rho_{\mathcal{B}_W}(g)$ are equivalent.*

In other words, two invariant subspaces are equivalent, if the group action of D_{2n} looks the same on both. Observe that this definition is independent on the choice of the bases $\mathcal{B}_V$, $\mathcal{B}_W$, see [GW]. As seen later, the following minimally D_{2n}-invariant subspaces are the core of the characterization of D_{2n}-invariant SOS. The invariant spaces group by "mod$2n$":

Lemma 8.10. *The following spaces are minimally D_{2n}-invariant subspaces of $\mathbb{R}[x,y]$:*

$$\begin{array}{ll} V_{0,k,\ell} :=< r^{2\ell} g_{2kn} >, & W_{0,k,\ell} :=< r^{2\ell} h_{2kn} >, \\ V_{j,k,\ell} :=< r^{2\ell} g_{j+2nk}, r^{2\ell} h_{j+2nk} > & \\ V_{n,k,\ell} :=< r^{2\ell} g_{n+2nk} >, & W_{n,k,\ell} :=< r^{2\ell} h_{n+2nk} > \end{array}$$

where $k,\ell \in \mathbb{N}$ and $j \in \{1,\dots,2n-1\}$, $j \neq n$. Moreover $V_{i,k,\ell}$ and $V_{i',k',\ell'}$ are D_{2n}-isomorphic if and only if $i = i$ or $i = 2n - i$. Any two $V_{i,k,\ell}$ and $W_{i',k',\ell'}$ are not D_{2n}-isomorphic.

Note: The spaces $< r^{2\ell} g_k, r^{2\ell} h_k >$ are invariant under the canonic action of the matrix-group $O(2)$. Since $\rho(D_{2n})$ is a subgroup of $O(2)$, the spaces $< r^{2\ell} g_k, r^{2\ell} h_k >$ are D_{2n} invariant. Nevertheless, we prove this in detail to obtain the D_{2n}-isomorphic subspaces.

Proof. For each $k,\ell \in \mathbb{N}$ let $\mathcal{B}_{k,l} := \{r^{2l} g_k, r^{2l} h_k\}$ be the basis of the space $U_{k,\ell} :=< r^{2\ell} g_k, r^{2\ell} h_k >$. Fix $(i,j) \in \{0,1\} \times \{0,\dots,n-1\}$ and some $k,\ell \in \mathbb{N}$. Set $B_n := B(\pi/n)$, see (8.1).
We first show that the action of $a^i b^j \in D_{2n}$ on $U_{k,\ell}$, is a linear mapping $a^i b^j : U_{k,\ell} \to U_{k,\ell}$, whose defining matrix relative to the basis $\mathcal{B}_{k,l}$ is $\rho_k(a^i b^j) := A^i (B_n)^{jk}$.
Define $z(x,y) := x + iy$. By definition of g_k, h_k this leads to $g_k(x,y) = \mathrm{Re}(z(x,y)^k)$ and $h_k(x,y) = \mathrm{Im}(z(x,y)^k)$. Observe $z(A\binom{x}{y}) = \overline{z(x,y)}$ and $z(B_n\binom{x}{y}) = e^{i\frac{\pi}{n}} z(x,y)$. Defining $\alpha := jk\pi/n$ This leads to

$$\begin{array}{rcccl} b^j(g_k)(x,y) & = & g_k(B_n^j\binom{x}{y}) = \mathrm{Re}(e^{i\alpha} z(x,y)^k) & = & \cos(\alpha) g_k(x,y) - \sin(\alpha) h_k(x,y) \\ b^j(h_k)(x,y) & = & h_k(B_n^j\binom{x}{y}) = \mathrm{Im}(e^{i\alpha} z(x,y)^k) & = & \sin(\alpha) g_k(x,y) + \cos(\alpha) h_k(x,y), \end{array}$$

$$\begin{array}{rcccl} ab^j(g_k)(x,y) & = & g_k(AB_n^j\binom{x}{y}) = \mathrm{Re}(\overline{e^{i\alpha} z(x,y)^k}) & = & \cos(\alpha) g_k(x,y) - \sin(\alpha) h_k(x,y) \\ ab^j(h_k)(x,y) & = & h_k(AB_n^j\binom{x}{y}) = \mathrm{Im}(\overline{e^{i\alpha} z(x,y)^k}) & = & -\sin(\alpha) g_k(x,y) - \cos(\alpha) h_k(x,y). \end{array}$$

This proves that $U_{k,\ell}$ is D_{2n}-invariant. Moreover, expressing the actions of b^j and ab^j on $U_{k,\ell}$ in the basis $\mathcal{B}_{k,l}$ yields

$$\begin{array}{rcccl} \begin{pmatrix} b^j(g_k) \\ b^j(h_k) \end{pmatrix} & = & \begin{pmatrix} \cos(jk\pi/n) & -\sin(jk\pi/n) \\ \sin(jk\pi/n) & \cos(jk\pi/n) \end{pmatrix} \begin{pmatrix} g_k \\ h_k \end{pmatrix} & = & (B_n)^{jk} \begin{pmatrix} g_k \\ h_k \end{pmatrix} \\ \begin{pmatrix} ab^j(g_k) \\ ab^j(h_k) \end{pmatrix} & = & \begin{pmatrix} \cos(jk\pi/n) & -\sin(jk\pi/n) \\ -\sin(jk\pi/n) & -\cos(jk\pi/n) \end{pmatrix} \begin{pmatrix} g_k \\ h_k \end{pmatrix} & = & A(B_n)^{jk} \begin{pmatrix} g_k \\ h_k \end{pmatrix}. \end{array}$$

So the representing matrix of the linear mapping $a^i b^j : U_{k,\ell} \to U_{k,\ell}$ relative to the basis $\mathcal{B}_{k,l}$ expresses as $\rho_k(a^i b^j) = A^i (B_n)^{jk}$.
Assume $\widetilde{U}_{k,\ell} \subsetneq U_{k,\ell}$ is a non-trivial D_{2n}-invariant subspace of $U_{k,\ell}$. Since $U_{k,\ell}$ is two-dimensional, $\widetilde{U}_{k,\ell}$ is one-dimensional. Assume $\widetilde{U}_{k,\ell} =<u>$ for some polynomial $u = \widetilde{u}_1 g_k + \widetilde{u}_2 h_k$. Then $\widetilde{u} \in \mathbb{R}^2$ is an eigenvector of A and B_n^k. As an eigenvector of A –see (8.1)– we may assume w.l.o.g. that either $\widetilde{u} = (1,0)$ or $\widetilde{u} = (0,1)$ hold (implying $u = g_k$ or $u = h_k$). As a rotation matrix B_n^k has real eigenvectors only if the rotation angle is zero mod π. This leads to $(k\pi/n \equiv 0 \mod \pi)$ implying $k \equiv 0 \mod n$. Therefore spaces $< g_k >, < h_k >$ are G_n-invariant if and only if $k \equiv 0 \mod n$. In case $k \not\equiv 0 \mod n$, the space $U_{k,\ell}$ is minimally invariant.
Fix $k',\ell' \in \mathbb{N}$, then $U_{k,\ell} \equiv U_{k',\ell'}$ holds if and only if $\rho_k \simeq \rho_{k'}$. According to Lemma 8.5, $\rho_k \simeq \rho_{k'}$ holds if and only if either $(k \equiv k' \mod 2n)$ or $(k \equiv -k' \mod 2n)$ holds. This finishes the proof of Lemma 8.10. □

9. Proof of the main theorem

Theorem 9.1. *Let $\mathcal{F}$ be a D_{2k}-invariant SOS with $\deg(\mathcal{F}) = 2d$. Then*

$$\mathcal{F} = \Big(a_0 r^0 + a_1 r^2 + \ldots + a_k r^{2k} + \mathfrak{p}\Big)^2 + \mathfrak{q} \tag{9.1}$$

where the $a_0,\dots,a_k \in \mathbb{R}$ and (i) $\mathfrak{p}$ is a polynomial with monomials of degree at least $2k$, (ii) $\mathfrak{q}$ is a D_{2k}-invariant SOS with monomials of degree at least 2.

The interesting part of this theorem is that the first summand in (9.1) is a *square* who's first few coefficients are rotation-invariant!

Proof. By $\mathbb{R}_d[x,y]$ we denote the polynomials in 2 variables of degree at most d.
For the *finite* group D_{2k} there are only finitely many irreducible, non-equivalent representations $\Lambda := \{\rho_1, \dots, \rho_N\}$, such that $\rho_i \not\sim \rho_j$ if $i \neq j$ ([GW]). Moreover, Maschke's theorem ([GW]) guarantees a decomposition of $\mathbb{R}_d[x,y]$ into irreducible isomorphic-components,

$$\mathbb{R}_d[x,y] = \bigoplus_{\lambda\in\Lambda} \bigoplus_{i=1}^{N_\lambda} V_{\lambda,i} \tag{9.2}$$

where $V_{\lambda,i}$ are irreducible D_{2k}-invariant subspaces of $\mathbb{R}[x,y]$ and $V_{\lambda,i} \sim V_{\mu,j}$ holds if and only if $\lambda = \mu$. By $W_0 := \mathbb{R}_d[x,y]^{D_{2k}}$ denote the space of D_{2k}-invariant polynomials of degree at most d, then we can simplify (9.2) to

$$\mathbb{R}_d[x,y] = W_0 \oplus W_1$$

where $W_0 \not\sim W_1$ as D_{2k}-modules. Let $\{p_1, \dots, p_m\}$ be a basis of W_0 and $\{q_1, \dots, q_n\}$ be a basis of W_1, and set $\vec{p} := (p_1, \dots, p_m)^T$, $\vec{q} := (q_1, \dots, q_n)^T$, and $\binom{\vec{p}}{\vec{q}} = (\vec{p}^T, \vec{q}^T)^T$. Then $\mathcal{F}$ is SOS if and only if there is a matrix $A \in \mathbb{R}^{(m+n)\times(m+n)}$, such that

$$\mathcal{F} = \begin{pmatrix}\vec{p}\\ \vec{q}\end{pmatrix}^T A \begin{pmatrix}\vec{p}\\ \vec{q}\end{pmatrix} \quad \text{and } A = A^T,\ A \succeq 0.$$

The elements $g \in D_{2k}$ act on all $f \in (\mathbb{R}[x,y])^{(m+n)}$ by $g : (f_1, \dots, f_{m+n}) \mapsto (gf_1, \dots, gf_{m+n})$. Thus the matrices $\rho(g) \in \mathbb{R}^{(m+n)\times(m+n)}$ defined by $g\binom{\vec{p}}{\vec{q}} = \rho(g)\binom{\vec{p}}{\vec{q}}$ form a representation of D_{2k}, which due to $g\vec{p} = \vec{p}$ and $gq_i \in W_1$ have the shape

$$\rho(g) = \begin{pmatrix} \bar{\rho}_0(g) & 0 \\ 0 & \bar{\rho}_1(g) \end{pmatrix}.$$

Here $\bar{\rho}_0(g) = \mathbb{I}_m \in \mathbb{R}^{m\times m}$ is the trivial representation of D_{2k} and $\bar{\rho}_1$ is a representation of D_{2k} with $\bar{\rho}_1(g) \in \mathbb{R}^{n\times n}$ and $\bar{\rho}_1 \not\sim \bar{\rho}_0$. By the preliminaries one has $g\mathcal{F} = \mathcal{F}$ for all $g_n \in D_{2k}$ where

$$g\mathcal{F} = \begin{pmatrix}g\vec{p}\\ g\vec{q}\end{pmatrix}^T A \begin{pmatrix}g\vec{p}\\ g\vec{q}\end{pmatrix} = \begin{pmatrix}\vec{p}\\ \vec{q}\end{pmatrix}^T \rho(g)^T A \rho(g) \begin{pmatrix}\vec{p}\\ \vec{q}\end{pmatrix}.$$

We can therefore assume w.l.o.g. that A is D_{2k}-invariant, i.e. $A = \rho(g)^T A \rho(g)$ holds – by replacing A with its symmetrization $1/|G| \sum_{g\in G} \rho(g)^T A \rho(g)$. Assume A has the following blockstructure

$$A = \begin{pmatrix} A_{00} & A_{01} \\ A_{01}^T & A_{11} \end{pmatrix},$$

with $A_{00} \in \mathbb{R}^{m\times m}$, $A_{01} \in \mathbb{R}^{m\times n}$, and $A_{11} \in \mathbb{R}^{n\times n}$. Then the equation $\rho(g)^T A \rho(g) = A$ implies $\bar{\rho}_0(g)^T A_{01} \bar{\rho}_1(g) = A_{01}$, which due to Schur's Lemma implies that $A_{01} = 0$. All in all this implies

$$\mathcal{F} = \vec{p}^T A_{00} \vec{p} + \vec{q}^T A_{11} \vec{q} \quad \text{where } A_{00}, A_{11} \succeq 0.$$

Lemma 8.10 gives explicit bases p, q for W_0 and W_1:

$$\begin{array}{rcl} p & = & \{r^{2\ell} g_{2kn} : n,\ell \in \mathbb{N},\ 2\ell + 2kn \leq d\} \quad \text{and} \\ q & = & \{r^{2\ell} g_n \ : n,\ell \in \mathbb{N},\ 2\ell + n \leq d,\ n \not\equiv 0 \mod 2k\} \ \cup \\ & & \{r^{2\ell} h_n \ : n,\ell \in \mathbb{N},\ 2\ell + n \leq d,\ n \geq 1\} \end{array}$$

The homogeneous polynomials g_n, h_n have degree n, so we find that every polynomial in q (and thus in W_1) has monomials of degree at least 1. Therefore the polynomial $\vec{q}^T A_{11} \vec{q}$ has monomials of degree at least 2. Moreover, if we order the monomials in p such that $p_0 = r^0, p_1 = r^2, \dots, p_k = r^{2k}$, then the remaining polynomials $p_{k+1}, \dots, p_m$ are of degree $\deg(p_i) \geq 2k$. Further, we can decompose A_{11} into a rank-1 matrix and a rest $X \in \mathbb{R}^{(m-1)\times(m-1)}$

$$A_{11} = \begin{pmatrix} a^2 & b^T \\ b & bb^T + X \end{pmatrix} \quad \text{where } X \succeq 0,\ a \in \mathbb{R} \text{ and } b \in \mathbb{R}^{m-1}.$$

From this we obtain

$$\mathcal{F} = (\underbrace{ar^0 + b_1 r^2 + \ldots + b_k r^{2k}}_{\text{rotation invariant}} + \underbrace{\sum_{i=k}^{m} b_i p_i}_{\text{even monomials of deg} \geq 2k})^2 + \overbrace{\begin{pmatrix}\vec{p}\\ \vec{q}\end{pmatrix}^T \begin{pmatrix} 0 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & A_{11} \end{pmatrix} \begin{pmatrix}\vec{p}\\ \vec{q}\end{pmatrix}^T}^{\text{SOS, monomials of deg} \geq 2}$$

which proves the theorem.

□

10. Conclusion and Outlook

This paper gives a generalization of the *known symmetric* polynomials that are non-negative but not sums-of-squares. Moreover it demonstrates the use of group-representation theory in the analysis of positive polynomials.
The main result is Theorem 5.2, an explicit construction for a family of symmetric polynomials, which are positive but not sums of squares. To our best knowledge, this is the first explicit construction of such polynomials without degree-restrictions. Moreover the construction can be extended to polynomials in arbitrarily many variables.
We use block-diagonalization of group-invariant matrices to state the restrictions of symmetric sums of squares. This tool has been widely used in polynomial optimization (see [GP], [KMPRS]), in contrast we use it in an abstract proof.

10.1. **Outlook.** The construction presented in this paper can be extended to polynomials in arbitrarily many variables – by using harmonics in more than 2 variables (the proofs are similar). To this end, one exploits the addition-formulas as done in Theorem 5.2. It is not yet clear if it is possible to construct the resulting polynomials such, that they do not contain a 2-variate certificate of not being SOS. For example one can check that

$$6(x^6 + y^6 + x^4z^2 + y^4z^2) - 6(x^4y^2 + x^2y^4 + 2x^2y^2z^2) - 9(x^4 + y^4) + 18x^2y^2 + 1$$

is PSD but not SOS, by setting $z = 0$.

We construct our polynomials $\mathcal{F}$ as sums of squares of *rational functions*, such that they have zeros, that a sum of squares of *polynomials* can not have. So we implicitly use some positivstellensatz, when looking at zeros of "semi-invariant" polynomials in order to disprove that $\mathcal{F}$ is SOS.
A non-symmetric version of our result could be obtained using a positivstellensatz for multivariate polynomials, alike the one recently presented by Gyula Károlyi ([Ka]).

11. Acknowledgments

I personally would like to thank Bruce Reznick for his detailed introduction into Hilbert's work, Frank Vallentin for a lot of listening, and very much Monique Laurent and Lex Schrijver for all their support.

References

[AAR] George E. Andrews, Richard Askey, and Ranjan Roy, *Special Functions*, Cambridge University Press, Cambridge 1999.
[BV] C. Bachoc, F. Vallentin, *Semidefinite programming, multivariate orthogonal polynomials, and codes in spherical caps*, arXive, 2007
[CLR] M. D. Choi, T. Y. Lam, and B. Reznick, *Even symmetric sextics*, Math. Z., 195 (1987), 559-580 (MR 88j.11019). Even symmetric sextics, Math. Z., 195 (1987), 559-580 (MR 88j.11019).
[GW] Goodman and Wallach, *Representations of finite groups*, John Wiley and Sons, New York, 1990.
[GP] K. Gatermann, P. Parrilo, *Symmetry groups, semidefinite programs, and sums of squares*, Journal of Pure and Appl. Algebra, Vol. 192, No. 1-3, pp. 95-128, 2004
[GS] D. Gijswijt, A. Schrijver, H. Tanaka *New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming*, Journal of Comb. Theory, Series A 113 (8) (2006), 1719–1731
[HG] D. Henrion, J.-B. Lasserre, *Solving nonconvex optimization problems*, Control Systems Magazine, IEEE Volume 24, Issue 3, Jun 2004 Page(s):72 - 83
[Glop] D. Henrion, J.-B. Lasserre, *GloptiPoly : Global Optimization over Polynomials with Matlab and SeDuMi*, ACM Trans. Math. Soft. 29, pp. 165–194.
[Hi] David Hilbert, *Über die darstellung definiter Formen als summe von Formenquadraten*, Math. Ann. 32, 342-350 (1888)

[Ka] *The Combinatorial Nullstellensatz and the Polynomial Method*, private communication at CWI, 2007

[KMPRS] E. de Klerk, J. Maharry, D.V. Pasechnik, B. Richter, and G. Salazar, *Improved bounds for the crossing numbers of $K_{m,n}$ and K_n*, SIAM J. Discrete Math., Volume 20, Issue 1, pp. 189-202, 2006.

[La] J. B. Lasserre, *Global Optimization with Polynomials and the Problem of Moments* SIOPT Volume 11 Issue 3, Pages 796-817

[Lau] M. Laurent, *Sums of squares, moment matrices and optimization over polynomials*, preprint 2007

[Mo] T. S. Motzkin, *The arithmetic-geometric inequality*, Shisha, O. (ed.) Inequalities, pp. 205-224, New York: Academic Press 1967, (Selected Papers, pp. 203-222), (MR 36 #6569).

[Pa] *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*, Ph.D. thesis, California Institute of Technology, Pasadena, CA, May 2000.

[Re] Bruce Reznick, *On Hilberts Construction Of Positive Polynomials*, to appear (2007)

[Riv] Theodore J. Rivlin, *Chebyshev Polynomials (2nd ed.)*, John Wiley and Sons, New York, 1990.

[Ro] R. M. Robinson, *Some definite polynomials which are not sums of squares of real polynomials*, pp. 264-282, Acad. Sci. USSR, 1973 (see abstract in Notices AMS **16**,554 (1969).

[PPPS] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo, *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*, version 2.00, available from `http://www.cds.caltech.edu/sostools` and `http://www.mit.edu/~parrilo/sostools`, 2004

[S00] R. Sroul, *Programming for Mathematicians,10.12*, Springer-Verlag, Berlin, pp. 278-279, 2000.

[S77] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, 1977.

[Va] F. Vallentin, *Symmetry in semidefinite programs*, arXive, 2007

Hartwig Bosse
E-mail address: `bosse@cwi.nl`