South Bohemia Mathematical Letters
Volume 18, (2010), No. 1, 1-16.

ONE EXAMPLE OF APPLICATION OF SUM OF SQUARES PROBLEM IN GEOMETRY

ONDŘEJ DAVÍDEK

Abstract. Positivity (or nonnegativity) of a polynomial is one of important characteristics in mathematical proving and deriving. A sum of squares, thanks to the semidefinite programming, can handle this better and faster than classical methods. We concentrate on how a positive polynomial in one variable can be effectively decomposed to a sum of two squares and show the interesting application of this decomposition.

Introduction

Notation in this article is mostly standard. A monomial x^α has the form $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$, and its degree d is a nonnegative integer $\sum_{i=1}^n \alpha_i$. A *polynomial* $p \in \mathbb{R}[x_1, ..., x_n]$ is a finite linear combination of monomials and has a degree m which is equal to the maximal degree of the used monomials, i.e.,

$$p = \sum_\alpha p_\alpha x^\alpha = \sum_\alpha p_\alpha x_1^{\alpha_1}\cdots x_n^{\alpha_n},\ p_\alpha \in \mathbb{R}. \tag{0.1}$$

A *form* is a polynomial where all monomials have the same degree.

A polynomial p is said to be *positive semidefinite* (PSD) or *positive definite* (PD) if $p(a_1, ..., a_n) \geq 0$ or $p(a_1, ..., a_n) > 0$ for all $(a_1, ..., a_n) \in \mathbb{R}^n$. Similarly, a symmetric matrix A is PSD (i.e., $A \succeq 0$) or PD (i.e., $A \succ 0$) if $x^T Ax \geq 0$ or $x^T Ax > 0$ for all $x \in \mathbb{R}^n$ and $A \succeq B$ or $A \succ B$ means that $A - B$ is PSD or PD.

We say p is a *sum of squares* (SOS) if the degree of p is even, say $2d$, and it can be written as a sum of t squares of other polynomials $q_i \in \mathbb{R}[x_1, ..., x_n]$ of degree $\leq d$, i.e.,

$$p = \sum_{i=1}^t q_i^2(x).$$

Suppose that s different monomials occur in polynomials q_i, then we denote $\overline{x} = (x^{\beta_1}, \ldots, x^{\beta_s})^T$ a vector of this monomials ordered in a suitable way and let $B = (b_1, \ldots, b_s)$ be the $s \times t$ matrix with i-th column containing the coefficients of q_i. Now if p is SOS it can be written as

$$p = (\overline{x}^T \cdot B) \cdot (\overline{x}^T \cdot B)^T = \overline{x}^T \cdot B \cdot B^T \cdot \overline{x}, \tag{0.2}$$

where $A = BB^T$ is a symmetric PSD $s \times s$ matrix and polynomials $q_i = \overline{x}^T \cdot b_i$.

To find the PSD matrix A we can use *semidefinite programming* (SDP). SDP is a method from convex optimization, it is a broad generalization of linear programming, to the case of symmetric matrices (more details can be found in [22]). An

Received by the editors 20th November 2010.
Key words and phrases. Sum of squares, canal surfaces, rational parametrization.

SDP in a standard primal form leads to find a PSD matrix A which satisfies (0.2), i.e.,

$$A \succeq 0, \; p = \overline{x}^T \cdot A \cdot \overline{x}, \tag{0.3}$$

for more details see [13].

Other goal is to assign a vector $\overline{x}$. It can be simply chosen as a subset of the set of monomials of degree less than or equal to d, of cardinality $\binom{n+d}{d}$. Mostly it is not necessary to use all monomials from this set. We want to have $\overline{x}$ with minimum of monomials which leads to the matrix A having the least dimension.

Define the *cage* (or *Newton polytope*) $\mathrm{new}(p)$ of polynomial p as the integer lattice points in the convex hull of the degrees α in (0.1), considered as vectors in $\mathbb{R}^n$. Then it can be shown that the only monomials x^β that can appear in the sum of squares representation are those such that 2β is in the cage of p. It means that

$$\mathrm{new}(q_i) \subseteq \frac{1}{2}\mathrm{new}(p).$$

This elimination of monomials is called the *sparsity*.

Using the cage we can formulate the necessary condition of nonnegativity of polynomial p: if p is PSD then every vertex of $\mathrm{new}(p)$ has even coordinates and a positive coefficient. For more details see [13]. Let us demonstrate this in the following example.

Example 1. *Let $p(x,y) = x^4y^6 + x^2 - xy^2 + y^2$. Then we arrive at (see Figure 1) $\overline{x}^T = (x^2y^3, xy^2, xy, x, y)$. So we need only 5 monomials instead of all 21 monomials of degree ≤ 5.*

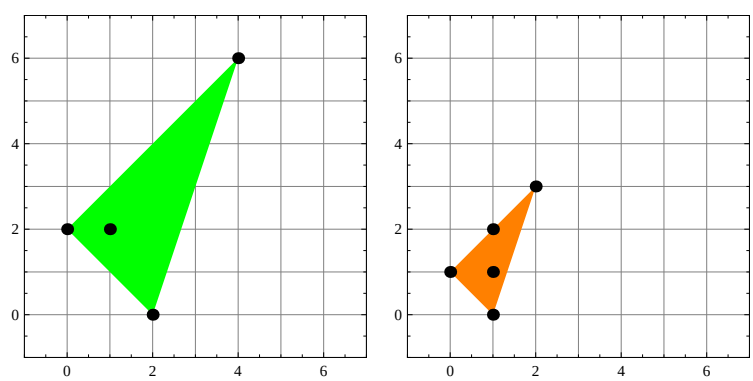

FIGURE 1. The cage of the polynomial p (left) and polynomials q_i (right).

The necessary condition for p to be PSD is complied because vertices $\alpha_1 = (4,6)$, $\alpha_2 = (2,0)$, $\alpha_3 = (0,2)$ of $\mathrm{new}(p)$ have even coordinates and positive coefficients. So the polynomial p could be written as SOS (i.e., $p = \sum_{i=1}^t q_i^2$) and also it is. One of SOS decomposition of the polynomial p is

$$p = \frac{3}{4}x^2y^4 + \frac{2}{3}x^4y^6 + \left(x - \frac{xy^2}{2}\right)^2 + \left(y - \frac{xy}{2} - \frac{x^2y^3}{2}\right)^2 + \frac{3}{4}\left(xy - \frac{x^2y^3}{3}\right)^2.$$

It is obvious that SOS decomposition of p implies its nonnegativity. However in general the converse is not true. The construction of PSD polynomials which are not sums of squares was first described by Hilbert in 1888 but no explicit example appeared until late 1960s, when Motzkin presented such polynomial (see [19] and [3]). On the other hand, the positive solution of Hilbert's 17th problem implies that every PSD polynomial is the sum of squares of rational functions.

The general problem of testing global nonnegativity of a polynomial (of the degree at least four) is in fact NP-hard. However to find SOS decomposition is thanks to SDP solvable in a polynomial time.

An interesting case is to certify nonnegativity over a general compact interval, i.e.,

$$\forall x \in \langle a, b\rangle : p(x) \geq 0 \tag{0.4}$$

It can be transformed to above PSD problem by substitution $x(y) = \frac{a+by^2}{1+y^2}$ and then

$$\forall x \in \mathbb{R} : p(y) = p\left(\frac{a+by^2}{1+y^2}\right) \geq 0 \tag{0.5}$$

is equivalent to (0.4). To be the function $p(y)$ in (0.5) a polynomial we have to multiply $p(y)$ by $(1+y^2)^m$, where m is the degree of $p(x)$. The disadvantage of this step is that the degree of polynomial p increases to $2m$.

1. PSD equivalent to SOS

In 1888, Hilbert showed that there are only three cases where polynomials are PSD iff they are SOS (see [5], [16]). The first one is the case of forms in two variables (i.e., $n = 2$) which are equivalent by dehomogenization to polynomials in one variable. The second one is the case of quadratic forms (i.e., $m = 2$) and the third one is the surprising case of quartic forms in three variables (i.e., the ternary quartic forms where $n = 3$ and $m = 4$).

1.1. Univariate polynomials.

Since univariate polynomials and forms in two variables are equivalent we will only deal with the first case.

Every PSD univariate polynomial is a sum just two squares. The graph of PSD polynomial is whole above the x-axis or touching it, so roots of such polynomial are either complex in conjugate pairs or real with even multiplicity. Thus the roots have the form $a_j \pm ib_j$ and we can write such polynomial as

$$\begin{aligned} p(x) &= [(x-[a_1+ib_1])\cdots(x-[a_n+ib_n])]\cdot \\ &\quad\ [(x-[a_1-ib_1])\cdots(x-[a_n-ib_n])] \\ &= [q_1(x)+iq_2(x)]\cdot[q_1(x)-iq_2(x)] \\ &= q_1(x)^2+q_2(x)^2. \end{aligned}$$

It is not easy to get this decomposition, because in general we are not able to find out exact form of roots. The other limitation appears when we want to work only with polynomials with rational coefficients, then SOS can include more than two squares (see [5]).

1.2. **Quadratic polynomials.** Every PSD quadratic form, in any number of variables, is a sum of squares. One can see that quadratic form is equivalent again by dehomogenization to a quadratic polynomial.

Theorem 1.1. *Given a quadratic form* $p(x_1,\dots,x_n)=\sum_{i=1}^n\sum_{j=1}^n p_{ij}x_ix_j$ *in variables* $x_1,\dots,x_n$ *with rational coefficients* p_{ij} *and* $p_{ij}=p_{ji}$*, we can either construct a decomposition*

$$p(x_1,\dots,x_n)=\sum_{i=1}^n b_i g_i(x_1,\dots,x_n)^2,$$

where b_i *are nonnegative rational numbers and* $g_i(x_1,\dots,x_n)$ *are linear functions with rational coefficients, or find particular rational numbers* $u_1,\dots,u_n$ *such that* $p(u_1,\dots,u_n)<0$.

The proof of this theorem is a straightforward elaboration of the elementary technique of "completing the square" by induction on the number of variables and it can be seen in [5]. The approach will be presented in next example.

Example 2. *We show that the polynomial* $p=3x^2-18xy+31y^2+12xz-76yz+119z^2$ *is an SOS and hence also PSD.*

$$\begin{aligned}
p &= 3x^2-18xy+31y^2+12xz-76yz+119z^2\\
&= 3(x^2-6xy+4xz)+(31y^2-76yz+119z^2)\\
&= 3(x-3y+2z)^2-3(-3y+2z)^2+(31y^2-76yz+119z^2)\\
&= 3(x-3y+2z)^2+(4y^2-40yz+107z^2)\\
&= 3(x-3y+2z)^2+4(y^2-10yz)+107z^2\\
&= 3(x-3y+2z)^2+4(y-5z)^2-4(5z)^2+107z^2\\
&= 3(x-3y+2z)^2+4(y-5z)^2+7z^2.
\end{aligned}$$

1.3. **Quartic polynomials in two variables.** Every PSD ternary quartic form is a sum of three squares of quadratic forms. Hilbert's proof is short but difficult and incomprehensible to the modern reader. There are some modern expositions, e.g. see [21] or [16]. Like above by dehomogenization ternary quartic form is equivalent to quartic polynomial in two variables.

1.4. **Motzkin polynomial.** As we mentioned above, the first explicit example of polynomial which is PSD and not SOS was the Motzkin polynomial (or form here for $n=3$), i.e.,

$$M(x,y,z)=x^4y^2+x^2y^4+z^6-3x^2y^2z^2.$$

Nonnegativity can be easily shown using the inequality of arithmetic-geometric means

$$\frac{x_1+x_2+\ldots+x_n}{n}\geq\sqrt[n]{x_1\cdot x_2\cdots x_n}.$$

Put $n=3$ and $x_1=x^4y^2$, $x_2=x^2y^4$, $x_3=z^6$ then we get

$$\frac{x^4y^2+x^2y^4+z^6}{3}\geq\sqrt[3]{x^6y^6z^6}=x^2y^2z^2$$

and therefore $M(x,y,z)$ is PSD.

Now we show that there is no SOS decomposition of the Motzkin form. The cage $\mathrm{new}(M)$ of M has vertices $\alpha_1=(4,2,0)$, $\alpha_2=(2,4,0)$, $\alpha_3=(0,0,6)$ and then the cage $\mathrm{new}(q_i)$ must have vertices $\beta_1=(2,1,0)$, $\beta_2=(1,2,0)$, $\beta_3=$

$(0,0,3)$, so new(q_i) includes also lattice point $\beta_4 = (1,1,1)$. Hence we have $\overline{x}^T = (x^2y, xy^2, xyz, z^3)$ and matrix $A = \mathrm{diag}(1,-3,1,1)$. It is clear that this diagonal matrix A is not PSD, e.g. by reason of its negative determinant.

Every PSD polynomial is a sum of squares of rational functions, so Motzkin form can be written as

$$\begin{aligned} M(x,y,z) &= \left(\frac{(x^2-y^2)z^3}{x^2+y^2}\right)^2 + \left(\frac{x^2y(x^2+y^2-2z^2)}{x^2+y^2}\right)^2 + \\ &+ \left(\frac{xy^2(x^2+y^2-2z^2)}{x^2+y^2}\right)^2 + \left(\frac{xyz(x^2+y^2-2z^2)}{x^2+y^2}\right)^2. \end{aligned}$$

This decomposition can be found by SOS decomposition of polynomial $(x^2+y^2)^2M(x,y,z)$, but in general it is difficult to find such factor $(x^2+y^2)^2$.

2. Sum of squares by semidefinite programming

Semidefinite programming is the problem to find such values a_{ij} $(i,j = 1,\dots,s)$, which comply a set of linear equational constraints, to make a matrix $A = (a_{ij})$ PSD. This problem is studied in (0.3). There are powerful semidefinite programming tools, e.g. command line program CSDP (see [2]), or SOSTOOLS (see [18]) directly SOS optimization toolbox for MATLAB using SDP solver SeDuMi (see [20]).

2.1. Sum of squares of univariate polynomial.

We show how SOS problem of univariate polynomial $p(x) = \sum_{i=0}^{2m} p_i x^i$ can be solved by SDP. First we need to set a vector of monomials $\overline{x}$. The degree of $p(x)$ is $2m$ and therefore

$$\overline{x} = (1, x, x^2, \dots, x^m)^T.$$

Now polynomial $p(x)$ can be written as a quadratic form in $\overline{x}$:

$$p(x) = \overline{x}^T \cdot A \cdot \overline{x} =$$

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^m \end{pmatrix}^T \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0m} \\ a_{01} & a_{11} & \cdots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0m} & a_{1m} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^m \end{pmatrix} \tag{2.1}$$

where the matrix $A = BB^T$ and the matrix B can and will be later determined by the Cholesky decomposition. That means B will be a lower triangular matrix with strictly positive diagonal entries and therefore the matrix A and even a polynomial p must be PD.

PSD polynomial can be zero only in real roots which, as we said, must occur with even multiplicity. Factors included this roots can be easily eliminated by taking $g = \gcd(p, p')$ and writing $p = g^2h$. Then the polynomial h has no real roots and is PD.

The other option to get our matrix B is eigendecomposition of symmetric matrix A (see [6]), where $A = Q \cdot \Lambda \cdot Q^T$, Λ is the diagonal matrix whose diagonal elements are the eigenvalues of A and Q is the square $s \times s$ matrix whose columns are the corresponding eigenvectors of A. Then $B = Q \cdot \sqrt{\Lambda}$. Another option is Takagi's factorization (see [6]) conformable to eigendecomposition. However both this matrix decomposition are more complicated than the Cholesky.

The equation (2.1) leads to a set of equations:

$$\begin{array}{rcl} p_0 & = & a_{00} \\ p_1 & = & 2a_{01} \\ p_2 & = & 2a_{02} + a_{11} \\ p_3 & = & 2a_{03} + 2a_{12} \\ p_4 & = & 2a_{04} + 2a_{13} + a_{22} \\ \vdots & \vdots & \vdots \\ p_{2m-1} & = & 2a_{m-1,m} \\ p_{2m} & = & a_{m,m} \end{array} \tag{2.2}$$

which is $2m+1$ equations for $(m+2)(m+1)/2$ variables. Thus for $m > 1$ the set (2.2) has infinitely many solutions, but we are only interested in such which comply $A \succeq 0$.

A matrix is PSD iff all eigenvalues are nonnegative. So we need some conditions for a_{ij} to the matrix A be PSD. Let

$$P(y) = y^k + a_{k-1}y^{k-1} + \ldots + a_0$$

be the characteristic polynomial of A, where $a_i \in \mathbb{R}[a_{ij}]$. By Descartes' rule of signs $P(y)$ has only nonnegative roots iff $(-1)^{i+k}a_i \geq 0$ for all $i = 0, \ldots, k-1$.

So we have got a completing of the set (2.2) by inequalities $(-1)^{i+k}a_i \geq 0$. If this set of equations and inequalities has a solution then there is a PSD matrix A, which satisfies (0.3), and polynomial p is SOS (otherwise there is a $x_0 \in \mathbb{R}$ that $p(x_0) < 0$).

Thus we have a PSD matrix A and can use the Cholesky decomposition to get a matrix B which gives us a solution of SOS problem

$$\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_t \end{pmatrix}^T = \begin{pmatrix} 1 \\ x \\ \vdots \\ x^m \end{pmatrix}^T \begin{pmatrix} b_{00} & 0 & \cdots & 0 \\ b_{01} & b_{11} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_{0m} & b_{1m} & \cdots & b_{mm} \end{pmatrix}. \tag{2.3}$$

However this approach has one disadvantage, namely in general polynomials q_i do not have to be rational even if p is.

Example 3. *By SOS decomposition we determine whether the following univariate polynomial p is PSD,*

$$p(x) = 650 - 2150x + 2899x^2 - 2168x^3 + 1049x^4 - 350x^5 + 81x^6 - 12x^7 + x^8.$$

To find a factor $g = \gcd(p, p')$, where

$$p'(x) = -2150 + 5798x - 6504x^2 + 4196x^3 - 1750x^4 + 486x^5 - 84x^6 + 8x^7,$$

we can use e.g. the Gröbner basis for the ideal generated by polynomials $p(x)$ and $p'(x)$ and we get $g(x) = x - 1$. Then a polynomial $p = g^2h$ and

$$h(x) = 650 - 850x + 549x^2 - 220x^3 + 60x^4 - 10x^5 + x^6.$$

Now we solve the equation $h(x) = \sum_{i=0}^{6} h_i x^i = \overline{x}^T \cdot A \cdot \overline{x}$, where $\overline{x} = (1, x, x^2, x^3)^T$, which leads to the set of equation

$$\begin{array}{rclcl} 650 & = & h_0 & = & a_{00} \\ -850 & = & h_1 & = & 2a_{01} \\ 549 & = & h_2 & = & 2a_{02}+a_{11} \\ -220 & = & h_3 & = & 2a_{03}+2a_{12} \\ 60 & = & h_4 & = & 2a_{13}+a_{22} \\ -10 & = & h_5 & = & 2a_{23} \\ 1 & = & h_6 & = & a_{33} \end{array}$$

and so

$$A=\begin{pmatrix} 650 & -425 & \frac{549}{2}-\frac{a_{11}}{2} & -110-a_{12} \\ -425 & a_{11} & a_{12} & 30-\frac{a_{22}}{2} \\ \frac{549}{2}-\frac{a_{11}}{2} & a_{12} & a_{22} & -5 \\ -110-a_{12} & 30-\frac{a_{22}}{2} & -5 & 1 \end{pmatrix}.$$

This matrix A is PSD e.g. for $a_{11}=311$, $a_{12}=-(429/5)$ and $a_{22}=101/4$ and after assigning we have

$$A=\begin{pmatrix} 650 & -425 & 119 & -\frac{121}{5} \\ -425 & 311 & -\frac{429}{5} & \frac{139}{8} \\ 119 & -\frac{429}{5} & \frac{101}{4} & -5 \\ -\frac{121}{5} & \frac{139}{8} & -5 & 1 \end{pmatrix}.$$

By the Cholesky decomposition of matrix A we get

$$B=\begin{pmatrix} 5\sqrt{26} & 0 & 0 & 0 \\ -\frac{85}{\sqrt{26}} & \sqrt{\frac{861}{26}} & 0 & 0 \\ \frac{119}{5\sqrt{26}} & -\frac{239}{\sqrt{22386}} & \frac{\sqrt{\frac{35779}{861}}}{5} & 0 \\ -\frac{23}{5\sqrt{26}} & 17\sqrt{\frac{3}{7462}} & -\frac{1756}{5}\sqrt{\frac{3}{10268573}} & \sqrt{\frac{1214}{35779}} \end{pmatrix}$$

and

$$\begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix} = B^T\cdot\overline{x} = \begin{pmatrix} 5\sqrt{26}-\frac{85x}{\sqrt{26}}+\frac{119x^2}{5\sqrt{26}}-\frac{23x^3}{5\sqrt{26}} \\ \sqrt{\frac{861}{26}}x-\frac{239x^2}{\sqrt{22386}}+17\sqrt{\frac{3}{7462}}x^3 \\ \frac{1}{5}\sqrt{\frac{35779}{861}}x^2-\frac{1756}{5}\sqrt{\frac{3}{10268573}}x^3 \\ \sqrt{\frac{1214}{35779}}x^3 \end{pmatrix}$$

Then SOS decomposition of the polynomial p is

$$p(x)=g(x)^2\cdot\overline{x}^T\cdot A\cdot\overline{x}=g(x)^2\sum_{i=1}^{4}q_i(x)^2.$$

This example is computed using the above algorithm which was programmed in Mathematica. It can be solved by SOOSTOOLS in Matlab too, but the coefficients of polynomials q_i will be rounded.

2.2. **Sum of squares of bivariate polynomial.** According to Section 1 a bivariate polynomial p is SOS iff it is PSD only in two cases: p is a form or quartic. If we want to find a SOS decomposition we will proceed analogously to univariate polynomial. In the case of form a bivariate polynomial can be homogenized to a univariate polynomial.

As we said the proceeding is like in univariate case, therefore we only show SOS decomposition on the following example.

Example 4. *We show the SOS decomposition of the polynomial from the Example 1, so* $p(x,y) = x^4y^6 + x^2 - xy^2 + y^2$ *and with sparsity* $\overline{x}^T = (x^2y^3, xy^2, xy, x, y)$. *The equation, which must be solved, is*

$$p(x,y) = \overline{x}^T \cdot A \cdot \overline{x} =$$

$$\begin{pmatrix} x^2y^3 \\ xy^2 \\ xy \\ x \\ y \end{pmatrix}^T \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} & a_{04} \\ a_{01} & a_{11} & a_{12} & a_{13} & a_{14} \\ a_{02} & a_{12} & a_{22} & a_{23} & a_{24} \\ a_{03} & a_{13} & a_{23} & a_{33} & a_{34} \\ a_{04} & a_{14} & a_{24} & a_{34} & a_{44} \end{pmatrix} \begin{pmatrix} x^2y^3 \\ xy^2 \\ xy \\ x \\ y \end{pmatrix}. \tag{2.4}$$

Then the matrix A *has the form*

$$A = \begin{pmatrix} 1 & 0 & 0 & -\frac{a_{22}}{2} & 0 \\ 0 & 1 & -\frac{1}{2} & 0 & -\frac{a_{33}}{2} \\ 0 & -\frac{1}{2} & a_{22} & 0 & 0 \\ -\frac{a_{22}}{2} & 0 & 0 & a_{33} & 0 \\ 0 & -\frac{a_{33}}{2} & 0 & 0 & 1 \end{pmatrix}$$

and we have to determine the coefficients a_{22} *and* a_{33} *to be* $A \succeq 0$. *This is fulfilled for example for* $a_{22} = 1$ *and* $a_{33} = 1$. *Now*

$$A = \begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} & 0 \\ 0 & 1 & -\frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 1 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 1 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 & 1 \end{pmatrix}$$

and by Cholesky decomposition

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} \end{pmatrix},$$

which leads to

$$p(x,y) = \frac{3}{4}x^2y^4 + \frac{2}{3}x^4y^6 + \left(x - \frac{xy^2}{2}\right)^2 + \left(y - \frac{xy}{2} - \frac{x^2y^3}{2}\right)^2 + \frac{3}{4}\left(xy - \frac{x^2y^3}{3}\right)^2.$$

3. A sum of two squares

Some practical problems (e.g. problem of parametrization of canal surfaces) leads to the problem of decomposing a positive polynomial into a sum of two squares. Therefore in this section we introduce several methods to solve such a decomposition. In regard of a possible application and a computational complexity we confine to polynomials in one variable.

The first method is a numeric decomposition resulting from Section 1.1 and numerically determinated roots of polynomials. The following algorithm introduces this method.

Algorithm 1: naive-so2s

input : a nonnegative polynomial p of degree $2n, n \geq 1$
output: polynomials g, h such that $p = g^2 + h^2$

compute roots x_i of p such that
$p = p_{2n}(x - x_1) \cdots (x - x_n) \cdot (x - \overline{x_1}) \cdots (x - \overline{x_n})$;
separate g, h from $\sqrt{p_{2n}}(x - x_1) \cdots (x - x_n) = g + ih$;
return (g, h);

Remark 3.1. If we decompose p into a sum of two squares g, h, then also $(ag + bh), (bg - ah)$, where $a, b \in \mathbb{R}$ and $a^2 + b^2 = 1$, determinate a decomposition of p. It follows from

$$p = (ag + bh)^2 + (bg - ah)^2 = (a^2 + b^2)g^2 + (a^2 + b^2)h^2 = g^2 + h^2.$$

Then we say ([9]) that decompositions g, h and $(ag + bh), (bg - ah)$ are equivalent.

A squarefree PSD polynomial of degree $2d$ has exactly 2^{d-1} inequivalent SOS decompositions.

The second method uses a polynomial factorization in the certain field extension. Let k be an arbitrary computable field of characteristic $\neq 2$ and $p(x) \in k[x]$, then the following algorithm (taken from [9]) gives us such a method.

Algorithm 2: factor-so2s

input : a nonnegative polynomial $p \in k[x]$ of degree $2n, n \geq 1$
output: polynomials g, h such that $p = g^2 + h^2$

compute the factorization $p = c\Pi_j f_j^{e_j}$ into monic irreducible polynomials;
if *c is not a sum of two squares* **then**
  return (NotExist);
else
  choose two constants g, h such that $g^2 + h^2 = c$;
for *each j* **do**
  if *e_j is even* **then**
    $(g, h) = (f_j^{e_j/2} g, f_j^{e_j/2} h)$;
  else
    $k' = k[x]/\langle f_j \rangle$;
    if *$x^2 + 1$ is irreducible over k'* **then**
      return (NotExist);
    else
      $r(x) :=$ a polynomial such that $r^2 + 1 = 0$ in k';
      $u + iv := gcd(r + i, f_j)$ in $k(i)[x]$;
      $(g, h) := (gu + hv, gv - hu)$;
return (g, h);

This algorithm produces a solution depending on a choice of the field k, so the solution need not be found. For details of this method, we refer to [9].

Example 5. *Consider the polynomial* $p(x) = 4x^6 - 11x^4 + 70x^3 + 50x^2 - 126x + 65$ *and* $k = \mathbb{Q}$. *The factorization* p *into monic irreducible polynomials is*

$$p(x) = 4\left(x^6 - \frac{11}{4}x^4 + \frac{35}{2}x^3 + \frac{25}{2}x^2 - \frac{63}{2}x + \frac{65}{4}\right) = 4f.$$

Because 4 *is a sum of two squares* ($4 = 2^2 + 0^2$) *and* $x^2 + 1$ *is irreducible over* $\mathbb{Q}[x]/\langle f\rangle$, *we get, e.g. by Maple, that* $-1 = r^2$ *in* $\mathbb{Q}[x]/\langle f\rangle$, *where*

$$r = -\frac{443}{434} + \frac{477x}{434} + \frac{617x^2}{434} - \frac{53x^3}{434} - \frac{2x^4}{217} + \frac{22x^5}{217}.$$

Next we compute

$$gcd(r + i, f) = \left(\frac{7}{2} + 2i\right) - \left(\frac{5}{2} + \frac{7i}{2}\right)x - \frac{3ix^2}{2} + x^3$$

and get the decomposition

$$p = 2^2\left(\frac{7}{2} - \frac{5x}{2} + x^3\right)^2 + 2^2\left(2 - \frac{7x}{2} - \frac{3x^2}{2}\right)^2.$$

The last method, we introduce here, is based on the matrix representation. Consider again a polynomial p in a quadratic form (0.2). To decompose p into a sum of two squares, the matrix B must be a $s \times 2$ matrix, i.e. $B = (c, d)$. It leads to

$$A = BB^T = \begin{pmatrix} c_1 & d_1 \\ c_2 & d_2 \\ \vdots & \vdots \\ c_s & d_s \end{pmatrix} \cdot \begin{pmatrix} c_1 & d_1 \\ c_2 & d_2 \\ \vdots & \vdots \\ c_s & d_s \end{pmatrix}^T = \begin{pmatrix} c_1c + d_1d \\ c_2c + d_2d \\ \vdots \\ c_sc + d_sd \end{pmatrix}, \tag{3.1}$$

where $c = (c_1, c_2, \cdots, c_s)^T$ and $d = (d_1, d_2, \cdots, d_s)^T$. So we are finding a symmetric PSD matrix A with rank 2. To find such a matrix A is crucial but also difficult. The algorithm, which we programmed in Mathematica, is based on the Gröbner basis and exploiting the fact that every principal square submatrix of A is also PSD and has rank ≤ 2.

Once A is obtained, then a matrix B is determinated by solving the equations $a_{11} = c_1^2 + d_1^2,\ a_{1s} = c_1c_s + d_1d_s,\ a_{ss} = c_s^2 + d_s^2$, which has always a solution, e.g.

$$c_1 = \sqrt{\frac{a_{11}a_{ss} - a_{1s}^2}{a_{ss}}},\ d_1 = \frac{a_{1s}}{\sqrt{a_{ss}}},\ c_s = 0,\ d_s = \sqrt{a_{ss}}$$

(p is SOS $\Rightarrow a_{11} > 0 \wedge a_{ss} > 0$ and A is PSD $\Rightarrow a_{11}a_{ss} - a_{1s}^2 \geq 0$). Now we get $d = \frac{a_s}{d_s}$ and for $c_1 > 0$ we have $c = \frac{a_1 - d_1d}{c_1}$, where a_i is row of the matrix A. If $c_1 = 0$, then c is determinated from some other row of A (according to rank 2 of A $\exists i$: $c_i \neq 0 \implies c = \frac{a_i - d_id}{c_i}$).

It is obvious that all equivalent decomposition of A has form: $B = (c, d) \cdot Q$, where Q is a orthogonal matrix of the size 2.

The main advantage of this approach in front with methods above is that it produces an exact solution (if it exists and size of A is not too big) and we do not have to know the field k where such a solution can be found. Let us show it on an example.

Example 6. *Consider the polynomial*

$$p = 943 - 1050x + 375x^2 - 104x^3 + 210x^4 - 150x^5 + 13x^6 + 15x^8,$$

which can be written as the following sum of two squares

$$p = 13\left(-4 + x^3\right)^2 + 15\left(7 - 5x + x^4\right)^2. \tag{3.2}$$

Such a decomposition can be found by Algorithm 2 for $k = \mathbb{Q} \cup \{\sqrt{13}, \sqrt{15}\}$*, but practically we do not have this a priori information and in general it is not easy to find it.*

Therefore we will show how our method deals with it. We find a quadratic form of p

$$p(x) = \overline{x}^T \cdot A \cdot \overline{x} =$$

$$\begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \end{pmatrix}^T \begin{pmatrix} 15 & 0 & 0 & -75 & 105 \\ 0 & 13 & 0 & 0 & -52 \\ 0 & 0 & 0 & 0 & 0 \\ -75 & 0 & 0 & 375 & -525 \\ 105 & -52 & 0 & -525 & 943 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \end{pmatrix},$$

where A *is the PSD matrix with rank* 2*. Then the equation* $A = BB^T$ *produces one of the solution*

$$B = \begin{pmatrix} -4\sqrt{\frac{195}{943}} & -\frac{105}{\sqrt{943}} \\ -7\sqrt{\frac{195}{943}} & \frac{52}{\sqrt{943}} \\ 0 & 0 \\ 20\sqrt{\frac{195}{943}} & \frac{525}{\sqrt{943}} \\ 0 & -\sqrt{943} \end{pmatrix}.$$

Considering the Remark 3.1 this decomposition is equivalent to (3.2) with $a = -4\sqrt{\frac{13}{943}}$*,* $b = -7\sqrt{\frac{15}{943}}$*.*

4. Application of sum of squares

Sum of squares decomposition has many applications especially in theorem proving and deriving programs, e.g. in HOL Light (see [4]). In particular, it can be used in the proof of a geometric inequality for circle packings (see [14]) or in computing rational parametrizations of canal surfaces (see [15]).

4.1. **Canal Surfaces.**

Consider a real-valued rational function $r(t)$ and a rationally parametrized space curve

$$m(t) = (m_1(t), m_2(t), m_3(t)),$$

$t \in \mathbb{R}$ (i.e. $m_i(t)$ are rational functions). The offset at distance $r(t)$ to a curve $m(t)$ in $\mathbb{R}^3$ can be defined as the envelope of the set of spheres centered at $m(t)$ with a radius $r(t)$. In general such a surface is called a *canal surface* or specially for constant radius ($r(t) \equiv const.$) a *pipe surface* with *spine curve* $m(t)$.

This surfaces have wide applications (e.g. pipe surfaces: shape reconstruction, robotic path planning; canal surfaces: blend surfaces, transition surfaces between pipes) and therefore because of CAD systems and further manipulations they need to be rationally parametrized (see e.g. [1]). Surprisingly, this requirement can be

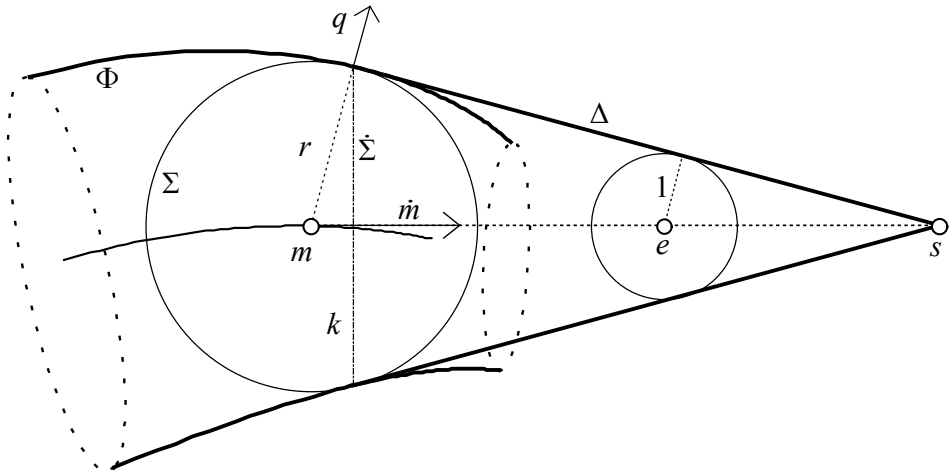

FIGURE 2. A representation of a canal surface.

always fulfilled. A general construction of rational parametrizations for real canal surfaces will be given in this section (for more details see [15] or [10]).

As above a canal surface Φ is defined as envelope of a one parameter set of spheres, centered at a spine curve $m(t)$ with a radius $r(t)$. Hence its defining equations are

$$\Sigma(t) : (x - m(t))^2 - r(t)^2 = 0, \tag{4.1}$$

$$\dot{\Sigma}(t) : (x - m(t)) \cdot \dot{m}(t) - r(t)\dot{r}(t) = 0, \tag{4.2}$$

and every point $x = (x_1, x_2, x_3)$ of Φ lies on so called *characteristic circle* $k(t) = \Sigma(t) \cap \dot{\Sigma}(t)$ (see Figure 2). Substituting $y = x - m$ in (4.1) and (4.2), we obtain $(y \cdot \dot{m})^2 = y^2\dot{r}^2$ and according to Figure 2 it follows that

$$1 \geq \cos^2 \alpha = \frac{(y \cdot \dot{m})^2}{y^2\dot{m}^2} = \frac{\dot{r}^2}{\dot{m}^2}.$$

Thus a canal surface Φ is real, if $\dot{m}^2 - \dot{r}^2 \geq 0$ (see [15]).

Further let q be the unit normals of Φ (for fixed t_0 the vector field $q(t_0, u)$ represents the unit normals at points of $k(t_0)$), then a parametric representation of Φ is given by

$$\Phi : x(t, u) = m(t) + r(t)q(t, u). \tag{4.3}$$

To get a rational parametrization of Φ we have to find a rational representation of the unit normals $q(t, u)$. Now we show how such $q(t, u)$ can be constructed.

A canal surface Φ can also be interpreted as the envelope of a one parameter set of cones $\Delta(t)$ with the vertex $s(t)$ (see [15] and Figure 2). The curve $e(t)$ is a set of centers of spheres with radius 1 tangent to $\Delta(t)$. One obtains

$$s = m - \frac{r}{\dot{r}}, \; e = m + \frac{1 - r}{\dot{r}}\dot{m}.$$

Let $\gamma : \Phi \to S^2$ be the Gauss map, where S^2 is the unit sphere centered at the origin. γ maps the cones $\Delta(t)$ onto circles $c(t)$ and the circles $c(t)$ define cones

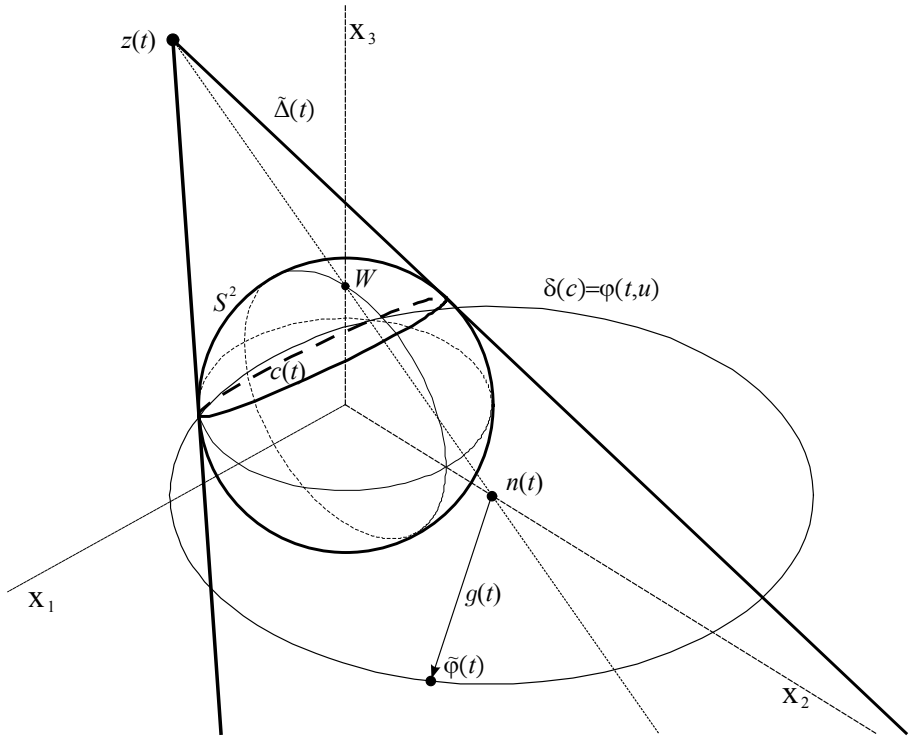

FIGURE 3. Stereographic projection of a circle $c(t)$ on the unit sphere S^2.

$\tilde{\Delta}(t)$, which are tangent to S^2 along $c(t)$ (Figure 3). The vertices of the cones $\tilde{\Delta}(t)$ are given by

$$z = s - e = -\frac{\dot{m}}{\dot{r}}.$$

It is obvious that the vector field $q(t,u)$ describes a circle $c(t) \subset S^2$. Hence a rational parametrization of $c(t)$ define a rational parametrization of $q(t,u)$. We use a stereographic projection to derive such parametrizations. A stereographic projection $\delta : S^2 \to \pi$ whith center $W = (0,0,1)$ and π defined by $x_3 = 0$ is a rational conformal map. δ maps a circle $c(t)$ to a circle $\delta(c)$ with center $n = \delta(z)$ and radius ρ given by

$$n = -\frac{(\dot{m}_1, \dot{m}_2, 0)}{\dot{m}_3 + \dot{r}}, \tag{4.4}$$

$$\rho^2 = \frac{\dot{m}^2 - \dot{r}^2}{(\dot{m}_3 + \dot{r})^2}, \tag{4.5}$$

see Figure 3. A planar curve $n(t)$ is rational, but in general radius ρ is not. Therefore any point $\tilde{\varphi}$ on a circle $\delta(c)$ has to be of the form

$$\tilde{\varphi}(t) = n(t) + g(t) = \frac{1}{\dot{m}_3 + \dot{r}}(g_1 - \dot{m}_1, g_2 - \dot{m}_2, 0), \tag{4.6}$$

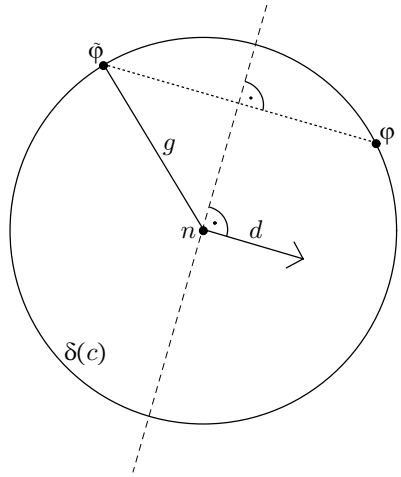

FIGURE 4. A reflection of $\tilde{\varphi}$.

where $g(t) = (g_1(t), g_2(t), 0)$ is a rational planar vector satisfying $g^2 = g_1^2 + g_2^2 = \rho^2$. It leads to a sum of two squares decomposition of ρ^2 (especially decomposition of the numerator in (4.5)). For any real canal surface ($\dot{m}^2 - \dot{r}^2 \geq 0$) such a decomposition exists as mentioned in Section 1.1 (or see [9]).

Having a rational parametrization of points $\tilde{\varphi}$ on circles $\delta(c)$ we want to derive the complete parametrization of $\delta(c)$. This can be constructed by reflecting $\tilde{\varphi}$ at all diameters of $\delta(c)$ (see Figure 4), which leads to

$$\varphi(t,u) = \tilde{\varphi} - 2\frac{g(t)\cdot d(u)}{d(u)^2}d(u),$$

where $d(u) = (u, 1, 0)$ are normals of a pencil of lines, $u \in \mathbb{R}$.

The last step is the inverse projection $\delta^{-1} : \pi \to S^2$, which maps circles φ to the unit normals

$$q(t,u) = \frac{1}{\varphi_1^2 + \varphi_2^2 + 1}(2\varphi_1, 2\varphi_2, \varphi_1^2 + \varphi_2^2 - 1)(t,u) \tag{4.7}$$

such that (4.3) is a rational parametrization of Φ.

By the choice of a coordinate system (i.e., the choice of the center W of stereographic projection δ) we can affect the degree of this parametrization, more details in [15] and [7]. Low degree is of course suitable for practical use.

Example 7. *Consider a spine curve*

$$m(t) = (t^3 - 2t^2 + 5t - 7, t^3 + 2t^2, 3t + 10)$$

and a radius function $r(t) = t^3 + 2t + 1$. *By the above approach with the center* $W = (0, 0, 1)$ *of stereographic projection we get*

$$\rho^2 = \frac{30 - 40t + 50t^2 + 9t^4}{(5 + 3t^2)^2} = \frac{(-5 + 3t^2)^2 + 5(1 - 4t)^2}{(5 + 3t^2)^2}$$

and the parametrization $x(t,u)$ *of the resulting canal surface* Φ *(Figure 5) is of degree 7 in* t *and 4 in* u.

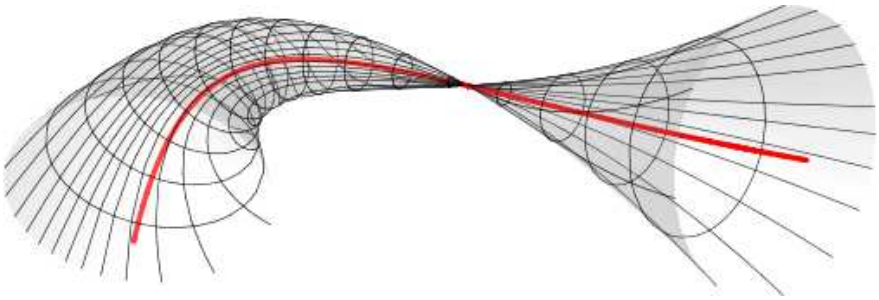

FIGURE 5. A canal surface with spine curve (red).

By the suitable choice of the center W (for details see [15]*) the resulting parametrization $x(t,u)$ can be improved to be of degree 5 in t and 2 in u.*

Acknowledgment

An essential part of this article has been presented at 30th Conference on Geometry and Graphics, and published in Proceedings of this conference ([23]).

References

[1] E. Aras: *Generating cutter swept envelopes in five-axis milling by two-parameter families of spheres,* Computer-Aided Design, Vol. 41, Issue 2 (February 2009), 95–105.

[2] B. Borchers: *CSDP: A software package for semidefinite programming,* 2010, Available `http://www.coin-or.org/projects/Csdp.xml`.

[3] C. N. Delzell, L. González-Vega and H. Lombardi: *A continuous and rational solution to Hilbert's 17th problem and several cases of the Positivstellensatz,* Computational Algebraic Geometry, F. Eyssette, A. Galligo, eds., Birkhäuser (1993), Progress in Math., Vol. 109, 61–75.

[4] J. Harrison: *The HOL Light theorem prover,* 2009, Available from `http://www.cl.cam.ac.uk/~jrh13/hol-light/`.

[5] J. Harrison: *Verifying Nonlinear Real Formulas Via Sums of Squares,* In: Schneider, K., Brandt, J. (eds.) TPHOLs 2007. LNCS, Vol. 4732, 102—118. Springer, Heidelberg (2007).

[6] R. A. Horn and C. R. Johnson: *Matrix Analysis,* Cambridge University Press, 1985.

[7] R. Krasauskas: *Minimal rational parametrizations of canal surfaces,* Computing Vol. 79, No. 2 (April 2007), 281–290.

[8] S. Lall, Slides available on `http://junction.stanford.edu/~lall/mtns06/`.

[9] G. Landsmann, J. Schicho and F. Winkler: *The Parametrization of Canal Surfaces and the Decomposition of Polynomials into a Sum of Two Squares,* J. Symbolic Computation (2001) 32, 119–132.

[10] G. Landsmann, J. Schicho, F. Winkler and E. Hillgarter: *Symbolic parametrization of pipe and canal surfaces,* Proceedings of the 2000 international symposium on Symbolic and algebraic computation, ISSAC 2000, St. Andrews, Scotland, 202–208.

[11] W. Lü and H. Pottmann: *Pipe surfaces with rational spine curve are rational.* Computer Aided Geometric Design, Volume 13, Issue 7, October 1996, 621–628.

[12] P. A. Parrilo: *Sum of Squares Programs and Polynomial Inequalities.* Available at: `http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-972-algebraic-techniques-and-semidefinite-optimization-spring-2006/lecture-notes/lecture_22.pdf`.

[13] P. A. Parrilo: *Structured Semidefnite Programs and Semialgebraic Geometry Methods in Robustness and Optimization,* PhD Thesis, California Institute of Technology, Pasadena, CA, May 2000.

[14] P. A. Parrilo and R. Peretz: *A Geometric Inequality for Circle Packings,* Discrete Comput. Geom., vol. 31, no. 3, 2004.

[15] M. Peternell and H. Pottmann: *Computing Rational Parametrizations of Canal Surfaces,* J. Symbolic Computation (1997) 23, 1995.

[16] V. Powers and B. Reznick: *Notes towards a constructive proof of Hilbert's theorem on ternary quartics,* Quadratic Forms and Their Applications (Dublin, 1999), Contemp. Math. 272, Am. Math. Soc., Providence, RI, 2000, pp. 209—227.

[17] V. Powers and T. Wörmann: *An Algorithm for Sums of Squares of Real Polynomials,* Journal of Pure and Applied Algebra, Volume 127, Number 1, 1 May 1998 , 99–104.

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

[19] B. Reznick: *On Hilberts Construction Of Positive Polynomials,* to appear (2007), available on `http://www.math.uiuc.edu/~reznick/paper53.pdf`.

[20] J. Sturm: *SeDuMi version 1.3,* 2010, Available from `http://sedumi.ie.lehigh.edu`.

[21] R. G. Swan: *Hilbert's Theorem on Positive Ternary Quartics,* In: Quadratic Forms and Their Applications, Contemp. Math. 272, 2000, 287–293.

[22] L. Vandenberghe and S. Boyd: *Semidefinite programming,* SIAM Review, Vol. 38, No. 1. (March 1996), 49–95.

[23] O. Davídek: *SOS problem in geometry,* Proceedings of 30th Conference on Geometry and Graphics, 2010, 65–74, available on `http://www.csgg.cz/30zlenice/sbornik2010.pdf`.

Department of Mathematics, University of West Bohemia, Univerzitní 22, Plzeň, Czech Republic

E-mail address: `odavidek@kma.zcu.cz`