Finding positive instances of parametric polynomials

Salvador Lucas
Departamento de Sistemas Informáticos y Computación (DSIC)
Universidad Politécnica de Valencia, Spain
Motivation: automatic proofs of termination

Finding positive instances of parametric polynomials
Motivation: automatic proofs of termination

Example

Consider the following Term Rewriting System (TRS) \( \mathcal{R} \) (cf. [Der95]):

\[
\begin{align*}
\text{fact}(0) & \rightarrow s(0) \quad \text{fact}(s(x)) & \rightarrow & s(x) \times \text{fact}(p(s(x)))) \\
0 \times y & \rightarrow 0 \quad s(x) \times y & \rightarrow & (x \times y) + y \\
x + 0 & \rightarrow x \quad x + s(y) & \rightarrow & s(x + y) \\
p(s(x)) & \rightarrow x
\end{align*}
\]

together with the following dependency pairs [AG00] associated to \( \mathcal{R} \):

\[
\begin{align*}
\text{FACT}(s(x)) & \rightarrow s(x) \times^\# \text{fact}(p(s(x)))) & \text{FACT}(s(x)) & \rightarrow & \text{FACT}(p(s(x))) \\
\text{FACT}(s(x)) & \rightarrow P(s(x)) \quad s(x) \times^\# y & \rightarrow & x \times^\# y \\
s(x) \times^\# y & \rightarrow (x \times y) +^\# y \quad x +^\# s(y) & \rightarrow & x +^\# y
\end{align*}
\]

During the proof of termination, we have to show that \( p(s(x)) \succsim x \) and \( \text{FACT}(s(x)) \sqsubseteq \text{FACT}(p(s(x))) \) for some (appropriate) quasi-ordering \( \succsim \) and well-founded ordering \( \sqsubseteq \) (on terms).
Motivation: automatic proofs of termination

A fruitful approach: polynomial interpretations, where the $k$-ary symbols $f$ are given polynomial functions $[f]: A^k \rightarrow A$ (for some numeric domain $A$) which are defined by some polynomial $[f] \in \mathbb{R}[X_1, \ldots, X_k]$. Terms are interpreted inductively.

Example

The following polynomial interpretation (where $A = [0, +\infty)$)

$$
[p](x) = \frac{1}{2}x \\
[s](x) = 2x + \frac{1}{2} \\
[FACT](x) = 2x
$$

can be used to prove the previous constraints (for all $x \in A$):

$$
[p(s(x))]) = x + \frac{1}{4} \geq x = [x] \\
[FACT(s(x))] = 4x + 1 > 2x + \frac{3}{4} = [FACT(p(s(x))])
$$
## Relevant issues

1. **The shape of the polynomials in the interpretation.** *Linear polynomials* lead to linear constraints (easy to check), but polynomials of *bigger degree* are often *required* in practice.
Motivation: automatic proofs of termination

Relevant issues

1. The *shape* of the polynomials in the interpretation. *Linear polynomials* lead to linear constraints (easy to check), but polynomials of *bigger degree* are often *required* in practice.

2. We can obtain *arbitrary* polynomials $P_{s,t} = [s] - [t]$ when dealing with constraints $s \succeq t$ or $s \sqsupseteq t$ as $P_{s,t} \geq 0$ and $P_{s,t} > 0$ (for variables ranging in $A$), respectively.
Motivation: automatic proofs of termination

Relevant issues

1. The shape of the polynomials in the interpretation. Linear polynomials lead to linear constraints (easy to check), but polynomials of bigger degree are often required in practice.

2. We can obtain arbitrary polynomials $P_{s,t} = [s] - [t]$ when dealing with constraints $s \succeq t$ or $s \sqsupseteq t$ as $P_{s,t} \geq 0$ and $P_{s,t} > 0$ (for variables ranging in $A$), respectively.

3. We face the problem of testing (semidefinite) positiveness of arbitrary polynomials (on a restricted domain $A$).
Motivation: automatic proofs of termination

### Relevant issues

1. The *shape* of the polynomials in the interpretation. *Linear polynomials* lead to linear constraints (easy to check), but polynomials of *bigger degree* are often *required* in practice.

2. We can obtain *arbitrary* polynomials $P_{s,t} = [s] - [t]$ when dealing with constraints $s \trianglerighteq t$ or $s \sqsubseteq t$ as $P_{s,t} \geq 0$ and $P_{s,t} > 0$ (for variables ranging in $A$), respectively.

3. We face the problem of *testing (semidefinite) positiveness* of arbitrary polynomials (on a *restricted domain* $A$).

4. We have to *generate* the interpretations. In practice, we use *parametric* polynomials whose coefficients are *parameters*. 

---

<table>
<thead>
<tr>
<th>1</th>
<th>The <em>shape</em> of the polynomials in the interpretation. <em>Linear polynomials</em> lead to linear constraints (easy to check), but polynomials of <em>bigger degree</em> are often <em>required</em> in practice.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>We can obtain <em>arbitrary</em> polynomials $P_{s,t} = [s] - [t]$ when dealing with constraints $s \trianglerighteq t$ or $s \sqsubseteq t$ as $P_{s,t} \geq 0$ and $P_{s,t} &gt; 0$ (for variables ranging in $A$), respectively.</td>
</tr>
<tr>
<td>3</td>
<td>We face the problem of <em>testing (semidefinite) positiveness</em> of arbitrary polynomials (on a <em>restricted domain</em> $A$).</td>
</tr>
<tr>
<td>4</td>
<td>We have to <em>generate</em> the interpretations. In practice, we use <em>parametric</em> polynomials whose coefficients are <em>parameters</em>.</td>
</tr>
</tbody>
</table>
Motivation: automatic proofs of termination

Relevant issues

1. The *shape* of the polynomials in the interpretation. *Linear polynomials* lead to linear constraints (easy to check), but polynomials of *bigger degree* are often *required* in practice.

2. We can obtain *arbitrary* polynomials $P_{s,t} = [s] - [t]$ when dealing with constraints $s \succeq t$ or $s \sqsupseteq t$ as $P_{s,t} \geq 0$ and $P_{s,t} > 0$ (for variables ranging in $A$), respectively.

3. We face the problem of *testing (semidefinite) positiveness* of arbitrary polynomials (on a *restricted domain* $A$).

4. We have to *generate* the interpretations. In practice, we use *parametric* polynomials whose coefficients are *parameters*.

5. *Time* is important: all should be done within a *fraction of second*.
Motivation: automatic proofs of termination

Relevant issues

1. The *shape* of the polynomials in the interpretation. *Linear polynomials* lead to linear constraints (easy to check), but polynomials of *bigger degree* are often *required* in practice.

2. We can obtain *arbitrary* polynomials $P_{s,t} = [s] - [t]$ when dealing with constraints $s \succcurlyeq t$ or $s \sqsubseteq t$ as $P_{s,t} \geq 0$ and $P_{s,t} > 0$ (for variables ranging in $A$), respectively.

3. We face the problem of *testing (semidefinite) positiveness* of arbitrary polynomials (on a *restricted domain* $A$).

4. We have to *generate* the interpretations. In practice, we use *parametric* polynomials whose coefficients are *parameters*.

5. *Time* is important: all should be done within a *fraction of second*.

6. We have to provide *certificates* of the proofs. The users should be able to *check* the proofs either by hand or by using automatic tools (based on theorem provers like *Coq* or *Isabelle*).
Motivation: automatic proofs of termination

Some history

1. In his IPL’79 paper, Dershowitz pointed out that the use of Tarski’s results would ‘circumvent’ the practical difficulties of solving polynomial interpretations over the naturals (after Matjasevich).

Conveniently, these are all decidable properties for polynomials over the reals [11]. By the same token, it is decidable if there exists any polynomial of degree less than any given n that demonstrates termination. In this manner, the undecidability for polynomials over the natural numbers, encountered in the method of [6], is circumvented.
Motivation: automatic proofs of termination

**Some history**

1. In his IPL’79 paper, Dershowitz pointed out that the use of Tarski’s results would ‘circumvent’ the practical difficulties of solving polynomial interpretations over the naturals (after Matjasevich).

   Conveniently, these are all decidable properties for polynomials over the reals [11]. By the same token, it is decidable if there exists any polynomial of degree less than any given \( n \) that demonstrates termination. In this manner, the undecidability for polynomials over the natural numbers, encountered in the method of [6], is circumvented.

2. Giesl, in his RTA’95 paper, says the following

   But even the most efficient known decision method (the *cylindrical algebraic decomposition* algorithm by G. E. Collins [Col75]) is very time-consuming. For that reason these methods have been rarely used for automated termination proofs.
Some history

1. In his IPL’79 paper, Dershowitz pointed out that the use of Tarski’s results would ‘circumvent’ the practical difficulties of solving polynomial interpretations over the naturals (after Matjasevich).

   Conveniently, these are all decidable properties for polynomials over the reals [11]. By the same token, it is decidable if there exists any polynomial of degree less than any given $n$ that demonstrates termination. In this manner, the undecidability for polynomials over the natural numbers, encountered in the method of [6], is circumvented.

2. Giesl, in his RTA’95 paper, says the following

   But even the most efficient known decision method (the cylindrical algebraic decomposition algorithm by G. E. Collins [Col75]) is very time-consuming. For that reason these methods have been rarely used for automated termination proofs.

3. Since 2005 [Luc05], polynomials over the reals are really used (and useful) in proofs of termination. But we can hardly say that the specific theory of the area is used in the implementations.
Motivation: automatic proofs of termination

Definition (Parametric polynomial interpretation)

Let $\mathcal{F}$ be a signature. A **parametric polynomial interpretation** for $\mathcal{F}$ is a pair $\mathcal{A} = (A, F_A)$ where $A$ is a **numeric domain** and $F_A$ consists of **parametric polynomials**, i.e., for all $k$-ary symbols $f \in \mathcal{F}$, $\lfloor f \rfloor$ is a polynomial $\lfloor f \rfloor \in \mathbb{Z}[C_1, \ldots, C_M, X_1, \ldots, X_k]$. Here, $C_1, \ldots, C_M$ are variables, often called **parameters**, and $X_1, \ldots, X_k$ are the usual **domain variables**.

State-of-the-art

1. Tests of (semidefinite) positiveness proceed as follows:
   - $P \in \mathbb{Z}[C_1, \ldots, C_M][X_1, \ldots, X_n]$ is PSD on $[0, +\infty)^n$ if all **coefficients** in $P$ are non-negative.
   - $P \in \mathbb{Z}[C_1, \ldots, C_M][X_1, \ldots, X_n]$ is PD on $[0, +\infty)^n$ if all **coefficients** in $P$ are non-negative and the constant coefficient is positive.

2. Dealing with **parametric** polynomials, polynomial constraints are translated into constraint solving problems by using this rule.
Summary

Our goal:

1. Review the existing literature about testing P(S)Dness of polynomials and devise how to *apply* it in our setting.

2. We contribute with a *new technique*.
Our goal:

1. Review the existing literature about testing P(S)Dness of polynomials and devise how to *apply* it in our setting.
2. We contribute with a *new technique*.

Summary:

1. A parametric vector basis for positive polynomials in one variable
2. Correctness and completeness
3. Cost analysis
4. Related work
5. Conclusions
A parametric basis for positive polynomials in one variable

Observation

The current approach to PSDness corresponds to checking (or imposing, in the parametric case) that the coordinates $[P]_{S_d} \in \mathbb{R}^{d+1}$ of $P$ are non-negative (w.r.t. the standard vector base $S_d = (1, x, \ldots, x^d)$ for polynomials $P \in \mathbb{P}_d$ of degree $d$).

Idea:

If we change the vector base $B = (v_0, v_1, \ldots, v_d)$, then some polynomials $P$ with negative coefficients could get non-negative coordinates $[P]_B$. If the $v_i$ are PSD on $[0, +\infty)$, then $P$ is PSD on $[0, +\infty)$ as well.

Example

Consider $Q(x) = x^3 - 4x^2 + 6x + 1$ and $B = \{1, x, x^2, x(x - 2)^2\}$. Since $[Q]_B = (1, 2, 0, 1)^T \geq 0$, we conclude that $Q$ is PSD on $[0, +\infty)$. Moreover, since the first coordinate is $1 > 0$, $Q$ is actually PD on $[0, +\infty)$. 
A parametric basis for positive polynomials in one variable

For $d \in \mathbb{N}$, and $2 \leq i \leq d$, consider the *parametric* univariate polynomials:

\[
\begin{align*}
P_0(x) &= 1 \\
P_1(x) &= x \\
P_i(x) &= \prod_{j=1}^{2^\left\lfloor \frac{i}{2} \right\rfloor} (x - \gamma_{ij})^2 \quad \text{if } i \text{ is even} \\
P_i(x) &= x \prod_{j=1}^{\left\lfloor \frac{i-1}{2} \right\rfloor} (x - \gamma_{ij})^2 \quad \text{if } i \text{ is odd}
\end{align*}
\]

where the $\gamma_{ij}$ are *parameters*. This sequence $\mathcal{P}_d$ of $d + 1$ polynomials is a *vector base* for $\mathbb{P}_d$, the set of polynomials $P \in \mathbb{R}[X]$ whose degree does not exceed $d$.

If the *coordinates* $[P]_{\mathcal{P}_d} \in \mathbb{R}^{d+1}$ of $P$ are non-negative, then $P$ is non-negative on $[0, +\infty)$.

**Theorem**

Let $P \in \mathbb{P}_n$. If $[P]_{\mathcal{P}_n} \geq \vec{0}$ (resp. $[P]_{\mathcal{P}_n} > \vec{0}$), then $P(x) \geq 0$ (resp. $P(x) > 0$) for all $x \geq 0$. 

Salvador Lucas – MAP’10
Finding positive instances of parametric polynomials
On the other hand, for all $P \in \mathbb{P}_n$ which is non-negative on $[0, +\infty)$, there is an instance of $\mathcal{P}_d$ for which $P$ has non-negative coordinates only.

**Theorem**

Let $P \in \mathbb{R}[X]$ be a polynomial of degree $n$. If $P(x) \geq 0$ ($P(x) > 0$) for all $x \geq 0$, then $[P]_{\mathcal{P}_n} \succeq \vec{0}$ (resp. $[P]_{\mathcal{P}_n} > \vec{0}$) for some assignment of values $\gamma_{ij} \geq 0$ to the parameters in $\mathcal{P}_n$.

**Example**

With $\gamma_{21} = 0$ and $\gamma_{31} = 2$ we obtain the required instance of $\mathcal{P}_n$:

$\mathcal{B} = \{1, x, x^2, x(x - 2)^2\}$. 
A parametric basis for positive polynomials in one variable

In order to prove (semidefinite) positiveness of $P \in \mathbb{P}_d$ we compute a (parametric) cb-matrix $M = M_{S_d \mapsto \mathbb{P}_d}$, where $S_d = (1, x, \ldots, x^d)$ is the standard basis for $\mathbb{P}_d$.

The matrix-vector product $M [P]_{S_d}$ yields the coordinates of $P$ w.r.t. $\mathbb{P}_d$.

Then, $M [P]_{S_d} > \vec{0}$ (resp. $M [P]_{S_d} \geq \vec{0}$) yields a set of $d + 1$ constraints which we have to solve w.r.t. the parameters $\gamma_{ij}$.

**Theorem (Incremental computation of the cb-matrix)**

We have $M_0 = I_1$ and for all $n > 1$,

$$M_n = \begin{pmatrix} M_{n-1} & -M_{n-1}[P_n(x)]_{S_n}^{1,\ldots,n} \\ 0 & I_1 \end{pmatrix}$$

where $[P_n(x)]_{S_n}^{1,\ldots,n}$ is the $n$-dimensional vector containing the first $n$ coordinates of $[P_n(x)]_{S_n}$ (the last one is 1).
A parametric basis for positive polynomials in one variable

Example

$Q$ is PD on $[0, +\infty)$. Since $[Q]_{S_3} = (1, 6, -4, 1)^T$, we impose

$$[Q]_{P_3} = M_3[Q]_{S_3} = \begin{pmatrix}
1 & 0 & -\gamma_2^2 & -2\gamma_2^2 \gamma_3^1 \\
0 & 1 & 2\gamma_2^1 & 4\gamma_2^1 \gamma_3^1 - \gamma_3^2 \\
0 & 0 & 1 & 2\gamma_3^1 \\
0 & 0 & 0 & 1
\end{pmatrix} \begin{pmatrix}
1 \\
6 \\
-4 \\
1
\end{pmatrix}$$

$$= \begin{pmatrix}
1 + 4\gamma_2^2 - 2\gamma_2^2 \gamma_3^1 \\
6 - 8\gamma_2^1 + 4\gamma_2^1 \gamma_3^1 - \gamma_3^2 \\
-4 + 2\gamma_3^1 \\
1
\end{pmatrix} > \begin{pmatrix}
0 \\
0 \\
0 \\
0
\end{pmatrix}$$

Thus, we have to solve the following constraints:

$$1 + 4\gamma_2^2 - 2\gamma_2^2 \gamma_3^1 > 0 \quad 6 - 8\gamma_2^1 + 4\gamma_2^1 \gamma_3^1 - \gamma_3^2 \geq 0 \quad 2\gamma_3^1 - 4 \geq 0$$

With $\gamma_2^1 = 0$ and $\gamma_3^1 = 2$, we prove $Q$ positive on $[0, +\infty)$ through the representation $[Q]_{P_3} = (1, 2, 0, 1)^T$ where $P_3 = \{1, x, x^2, x(x - 2)^2\}$. 
Cost analysis

1. The number $V(d)$ of auxiliary variables $\gamma_{ij}$ which are needed is

$$V(d) = \begin{cases} 
\frac{d^2}{4} & \text{if } d \text{ is even} \\
\frac{d^2-1}{4} & \text{otherwise}
\end{cases}$$

2. The number $I(d)$ of inequalities to be solved is $I(d) = d$.

3. The degree of the polynomial in the inequalities goes from 1 to $d$. A constraint of degree $n$ contains terms of degree $0, 1, \ldots, n$.

Note

The method is able to deal with parametric polynomials.
Our approach can be compared with other well-known techniques for proving (semidefinite) positiveness of polynomials on $[0, +\infty)$:

1. Pólya and Szegö representation (PSD).
2. Karlin and Studden (PD).
3. Goursat’s transformation and Bernstein base.
4. PSD as SOS representation through the change of variables $X \mapsto X^2$ (e.g., use of Gram matrices).
Pólya and Szegö representation (for PSD polynomials)

**Proposition (Pólya-Szegö)**

If $P$ is PSD on $[0, +\infty)$, then there are SOS polynomials $f, g$ such that $P(x) = f(x) + xg(x)$ and $\deg(f), \deg(xg) \leq \deg(p)$.

According to Hilbert, we can assume that both $f$ and $g$ consists of a sum of two squares $f_1^2, f_2^2$ and $g_1^2, g_2^2$, respectively.

If $\deg(P) = d$, the two $f_i$ have at most degree $d_1 = \lfloor \frac{d}{2} \rfloor$, and the two $g_i$ have at most degree $d_2 = \lfloor \frac{d-1}{2} \rfloor$.

Write $f_i = a_{i,d_1}x^{d_1} + \cdots + a_{i,1}x + a_{i,0}$ and $g_i = b_{i,d_2}x^{d_2} + \cdots + b_{i,1}x + b_{i,0}$ for $i = 1, 2$.

Try to *match* this representation against the *target* polynomial $P$ through appropriate *equalities* between the coefficients of the monomials.
Example

Consider the polynomial

\[ Q(X) = X^3 - 4X^2 + 6X + 1 = f_1(X) + f_2(X) + X(g_1(X) + g_2(X)) \]

where \( f_i(X) = (a_iX + b_i)^2 \) and \( g_i(X) = (c_iX + d_i)^2 \) for \( i = 1, 2 \).

\[ Q(X) = (c_1^2 + c_2^2)X^3 + (a_1^2 + a_2^2 + 2c_1d_1 + 2c_2d_2)X^2 + (2a_1b_1 + 2a_2b_2 + d_1^2 + d_2^2)X + b_1^2 + b_2^2 \]

which amounts at solving the following equalities:

\[
\begin{align*}
  c_1^2 + c_2^2 &= 1 \\
  a_1^2 + a_2^2 + 2c_1d_1 + 2c_2d_2 &= -4 \\
  2a_1b_1 + 2a_2b_2 + d_1^2 + d_2^2 &= 6 \\
  b_1^2 + b_2^2 &= 1
\end{align*}
\]

The following assignment solves the system:

\[
\begin{align*}
  a_1 &= 0 \\
  a_2 &= 0 \\
  b_1 &= 1 \\
  b_2 &= 0 \\
  c_1 &= 1 \\
  c_2 &= 0 \\
  d_1 &= -2 \\
  d_2 &= \sqrt{2}
\end{align*}
\]

and proves that \( Q \) is PSD on \([0, +\infty)\).
Pólya and Szegö representation (variant 1)

The Pythagoras number of $\mathbb{Z}$ and $\mathbb{Q}$ is 4 (for instance, there is no $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = 3$, but $1^2 + 1^2 + 1^2 = 3$).

If we want to restrict the attention to $\mathbb{Z}$ or $\mathbb{Q}$ when solving these quadratic equalities, we have to use four additive components for $f$ and $g$.

**Example**

Now we have

$$Q(X) = (\sum_{i=1}^{4} c_i^2)X^3 + (\sum_{i=1}^{4} a_i^2 + 2c_id_i)X^2 + (\sum_{i=1}^{4} 2a_ib_i + d_i^2)X + \sum_{i=1}^{4} b_i^2$$

which amounts at solving the following equalities:

$$\sum_{i=1}^{4} c_i^2 = 1 \quad \sum_{i=1}^{4} a_i^2 + 2c_id_i = -4 \quad \sum_{i=1}^{4} 2a_ib_i + d_i^2 = 6 \quad \sum_{i=1}^{4} b_i^2 = 1$$

The following assignment (without irrationals) solves the system:

$$a_1 = 0 \quad a_2 = 0 \quad a_3 = 0 \quad a_4 = 0 \quad b_1 = 1 \quad b_2 = 0 \quad b_3 = 0 \quad b_4 = 0$$

$$c_1 = 1 \quad c_2 = 0 \quad c_3 = 0 \quad c_4 = 0 \quad d_1 = -2 \quad d_2 = 1 \quad d_3 = 1 \quad d_4 = 0$$
**Proposition**

Let $P, Q \in \mathbb{R}[X_1, \ldots, X_n]$ be polynomials $P = \sum_\alpha a_\alpha X^\alpha$ and $Q = \sum_\alpha b_\alpha X^\alpha$. If $a_\alpha \geq b_\alpha$ for all $\alpha \in \mathbb{N}^n$ and $Q(x_1, \ldots, x_n) \geq 0$ for all $x_1, \ldots, x_n \geq 0$, then $P(x_1, \ldots, x_n) \geq 0$ for all $x_1, \ldots, x_n \geq 0$.

**Example**

Instead of equalities, we solve now the following inequalities:

\[
\begin{align*}
c_1^2 + c_2^2 & \leq 1 \\
2a_1b_1 + 2a_2b_2 + d_1^2 + d_2^2 & \leq 6 \\
a_1^2 + a_2^2 + 2c_1d_1 + 2c_2d_2 & \leq -4 \\
b_1^2 + b_2^2 & \leq 1
\end{align*}
\]

which now is solved with the following assignment:

\[
\begin{align*}
a_1 &= 0 \\
a_2 &= 0 \\
b_1 &= 1 \\
b_2 &= 0 \\
c_1 &= 1 \\
c_2 &= 0 \\
d_1 &= -2 \\
d_2 &= 1
\end{align*}
\]

which does not require irrational numbers.
Theorem (Karlin and Studden)

Let $P_{2m}$ be a polynomial of degree $2m$ for some $m \geq 0$ with leading coefficient $a_{2m} > 0$. If $P_{2m} > 0$ on $[0, +\infty)$, then there exists a unique representation

$$P_{2m}(X) = a_{2m} \prod_{j=1}^{m} (X - \alpha_j)^2 + \beta X \prod_{j=2}^{m} (X - \gamma_j)^2$$

where $\beta > 0$ and $0 = \gamma_1 < \alpha_1 < \gamma_2 < \cdots < \gamma_m < \alpha_m < \infty$. Similarly, if $P_{2m+1}$ is a polynomial of degree $2m + 1$ for some $m \geq 0$, with leading coefficient $a_{2m+1} > 0$ and $P_{2m+1} > 0$ on $[0, +\infty)$, then there exists a unique representation

$$P_{2m+1}(X) = a_{2m+1} X \prod_{j=2}^{m+1} (X - \alpha_j)^2 + \beta \prod_{j=1}^{m} (X - \gamma_j)^2$$

where $\beta > 0$ and $0 = \alpha_1 < \gamma_1 < \alpha_2 < \gamma_2 < \cdots < \gamma_m < \alpha_{m+1} < \infty$. 
Since the degree of $Q$ is odd, we let

$$K_Q(X) = X(X - \alpha_2)^2 + \beta(X - \gamma_1)^2 = X^3 + (\beta - 2\alpha_2)X^2 + (\alpha_2^2 - 2\beta\gamma_1)X + \beta\gamma_1^2$$

Thus, we have the following constraints:

- $-4 \geq \beta - 2\alpha_2$  \hspace{1cm} 1 > 0
- $6 \geq \alpha_2^2 - 2\beta\gamma_1$  \hspace{1cm} \beta > 0
- $1 \geq \beta\gamma_1^2$  \hspace{1cm} 0 < \gamma_1 < \alpha_2$

The satisfaction of the $1 \geq \beta\gamma_1^2$ requires the use of positive numbers below 1 (note that $\beta\gamma_1^2 > 0$). The following assignment solves the system:

$$\alpha_2 = \frac{9}{4} \hspace{1cm} \beta = \frac{1}{4} \hspace{1cm} \gamma_1 = \frac{1}{2}$$
# Goursat’s transformation and Bernstein basis

## Theorem (Goursat transform)

Given \( P \in \mathbb{R}[X] \) of degree \( d \), we let \( \tilde{P}(X) = (1 + X)^d P \left( \frac{1-X}{1+X} \right) \). Then, \( P \) is \( P(S)D \) on \([-1, 1]\) if and only if \( \tilde{P} \) is \( P(S)D \) on \([0, +\infty)\).

## Theorem (Use of Bernstein’s basis)

If \( [P]_{B_p} \geq \vec{0} \) (for the Bernstein basis \( B_d \) which consists of polynomials of degree \( d \) only) then \( P \) is positive on \([-1, 1]\).

## Theorem (Bernstein’s Theorem)

If \( P \) is \( PD \) on \([-1, 1]\), there is \( p \geq d \) (Bernstein degree) s.t. \( [P]_{B_p} \geq \vec{0} \).

## Problems

1. \( p \) can be much higher than \( n \). Furthermore,
2. We have to (over)estimate \( p \) as \( q \geq p \) and use \( B_q \).
Example

For $Q(X) = X^3 - 4X^2 + 6X + 1$, we get $\tilde{Q}(X) = -10X^3 + 4X^2 + 10X + 4$.

For $B_3 = \{ \frac{1}{8}(1 - 3x + 3x^2 - x^3), \frac{3}{8}(1 - x - x^2 + x^3), \frac{3}{8}(1 + x - x^2 - x^3), \frac{1}{8}(1 + 3x + 3x^2 + x^3) \}$

we obtain

$$[\tilde{Q}]_{B_3} = S_{S_3 \mapsto B_3} [\tilde{Q}]_{S_3} = \begin{pmatrix}
1 & -1 & 1 & -1 \\
1 & -\frac{1}{3} & -\frac{1}{3} & 1 \\
1 & \frac{1}{3} & -\frac{1}{3} & 1 \\
1 & 1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
4 \\
10 \\
4 \\
-10
\end{pmatrix}
= \begin{pmatrix}
8 \\
-32 \\
3 \\
16
\end{pmatrix}$$

which does not prove PDness of $Q$ on $[0, +\infty)$.

By using available estimations for the Bernstein degree of $\tilde{Q}$ [BCR08], we obtain $q = 40$, which amounts at computing a cb-matrix of $40 \times 40$ entries.
Goursat’s transformation and Bernstein basis

Note

The method is not well-suited to deal with parametric polynomials: current estimations of Bernstein’s degree require lower bounds $\lambda$ on the value which is reached by $\tilde{P}$ on $[-1, 1]$. Then, $q \propto \frac{1}{\lambda}$.

With parametric polynomials we would obtain $\lambda = 0$ and $q = +\infty$. 
Since we have the following

**Proposition**

Let \( P \in \mathbb{R}[X_1, \ldots, X_n] \) and \( Q(X_1, \ldots, X_n) = P(X_1^2, \ldots, X_n^2) \). Then, \( P \) is P(S)D on \([0, +\infty)^n\) if and only if \( Q \) is P(S)D on \( \mathbb{R}^n \).

we can use all available techniques for proving P(S)Dness on \( \mathbb{R} \) in proofs of P(S)Dness on \([0, +\infty)\). In particular:

**Proposition (Hilbert)**

*If \( P \) is PSD on \( \mathbb{R} \), then \( P \) is a sum of two squares of polynomials.*

**Note**

This transformation *duplicates* the degree of \( P \).
Example

Consider the polynomial

\[ Z(X) = Q(X^2) = X^6 - 4X^4 + 6X^2 + 1 = f_1(X) + f_2(X) \]

where \( f_i(X) = (a_iX^3 + b_iX^2 + c_iX + d_i)^2 \) for \( i = 1, 2 \).

\[ Z(X) = \sum_{i=1}^{2} a_i^2 X^6 + 2a_i b_i X^5 + (b_i^2 + 2a_i c_i) X^4 + 2(b_i c_i + a_i d_i) X^3 \]
\[ + (2b_i d_i + c_i^2) X^2 + 2c_i d_i X + d_i^2 \]

which amounts at solving the following equalities:

\[ \sum_{i=1}^{2} a_i^2 = 1 \quad \sum_{i=1}^{2} a_i b_i = 0 \quad \sum_{i=1}^{2} b_i^2 + 2a_i c_i = -4 \]
\[ \sum_{i=1}^{2} b_i c_i + a_i d_i = 0 \quad \sum_{i=1}^{2} 2b_i d_i + c_i^2 = 6 \quad \sum_{i=1}^{2} c_i d_i = 0 \quad \sum_{i=1}^{2} d_i^2 = 1 \]

A solution to this set of equations can be obtained by using Mathematica, but it yields (quite involved) irrational numbers.
Let $P$ be a polynomial of degree $2m$ and $z(X)$ be the vector of all monomials $X^\alpha$ such that $|\alpha| \leq m$. Then, $P$ is a sum of squares in $\mathbb{R}[X]$ if and only if there exists a real, symmetric, psd matrix $B$ such that $P = z(X)^T B z(X)$.

The problem of proving that $P$ is SOS is translated into the problem of proving whether a matrix $B$ is positive semidefinite. This can be done (in practice) in several ways:

1. Compute the characteristic polynomial of $B$ and require that all its roots are non-negative [PW98]. Powers and Wörmann show that this can be translated into a constraint solving problem involving $\frac{d^2 - d}{2}$ new parameters $\lambda_i$.

2. Use semidefinite programming techniques [PP08].
Quantitative comparison

In the following table, \( V(d) \) is the number of auxiliary variables which are introduced by the method and \( I(d) \) is the number of (in)equalities which are obtained.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( V(d): )</td>
<td>( \frac{d^2}{4} + 2 )</td>
<td>( 2d + 2 )</td>
<td>( 4d + 4 )</td>
<td>( 2d + 2 )</td>
<td>( d + 1 )</td>
<td>( 2d + 2 )</td>
<td>( \frac{d^2 - d}{2} )</td>
</tr>
<tr>
<td>( I(d): )</td>
<td>( \frac{d}{d} + 1 )</td>
<td>( d + 1 )</td>
<td>( d + 1 )</td>
<td>( d + 1 )</td>
<td>( 2d + 1 )</td>
<td>( 2d + 1 )</td>
<td>( d )</td>
</tr>
</tbody>
</table>

Note that P&S (1) and Hilbert yield equations.

Summary

The most critical aspect is the number of variables \( V(d) \) which are introduced. In this sense, we have the following:

1. For proving PSDness on \([0, +\infty)\), Vector is the best choice for \( 1 \leq d \leq 9 \) and P&S (2) is the best choice for \( d \geq 10 \).
2. For proving PDness on \([0, +\infty)\), Vector is the best choice for \( 1 \leq d \leq 5 \) and K&S is the best choice for \( d \geq 6 \).
Conclusions and future work

1. We have introduced a new method for proving P(S)Dness of univariate polynomials.
Conclusions and future work

1. We have introduced a new method for proving P(S)Dness of univariate polynomials.
2. The method is sound and complete and well-suited for dealing with parametric polynomials.

Future work

1. The method can be extended to multivariate polynomials. A thorough analysis and comparison with existing techniques (Positivstellensatz, Pólya's theorem, (S)DS, SOS representation, etc., should be addressed).
2. The possibility of restricting the attention to consider rational and even integer solutions for the constraints (as in P&S (1)) should be investigated for Vector.
3. Implementation and benchmarks.
Conclusions and future work

1. We have introduced a new method for proving P(S)Dness of univariate polynomials.
2. The method is sound and complete and well-suited for dealing with parametric polynomials.
3. The quantitative analysis of the method shows that it can work better than other methods for polynomials of small degree (below 10).

Future work

1. The method can be extended to multivariate polynomials. A thorough analysis and comparison with existing techniques (Positivstellensatz, Pólya's theorem, (S)DS, SOS representation, etc., should be addressed).
2. The possibility of restricting the attention to consider rational and even integer solutions for the constraints (as in P&S (1)) should be investigated for Vector.
3. Implementation and benchmarks.
We have introduced a new method for proving P(S)Dness of univariate polynomials. The method is sound and complete and well-suited for dealing with parametric polynomials. The quantitative analysis of the method shows that it can work better than other methods for polynomials of small degree (below 10).

Future work

The method can be extended to multivariate polynomials. A thorough analysis and comparison with existing techniques (Positivstellensatz, Pólya’s theorem, (S)DS, SOS representation, etc., should be addressed).
Conclusions and future work

1. We have introduced a new method for proving P(S)Dness of univariate polynomials.
2. The method is sound and complete and well-suited for dealing with parametric polynomials.
3. The quantitative analysis of the method shows that it can work better than other methods for polynomials of small degree (below 10).

Future work

1. The method can be extended to multivariate polynomials. A thorough analysis and comparison with existing techniques (Positivstellensatz, Pólya’s theorem, (S)DS, SOS representation, etc., should be addressed).
2. The possibility of restricting the attention to consider rational and even integer solutions for the constraints (as in P&S (1)) should be investigated for Vector.
Conclusions and future work

1. We have introduced a new method for proving P(S)Dness of univariate polynomials.
2. The method is sound and complete and well-suited for dealing with parametric polynomials.
3. The quantitative analysis of the method shows that it can work better than other methods for polynomials of small degree (below 10).

Future work

1. The method can be extended to multivariate polynomials. A thorough analysis and comparison with existing techniques (Positivstellensatz, Pólya’s theorem, (S)DS, SOS representation, etc., should be addressed).
2. The possibility of restricting the attention to consider rational and even integer solutions for the constraints (as in P&S (1)) should be investigated for Vector.
3. Implementation and benchmarks.