Verifying Nonlinear Real Formulas via Sums of Squares

John Harrison

Intel Corporation

TPHOLs, Kaiserslautern

Thu 13th September 2007 (11:30 – 12:00)

Proving nonnegativity of polynomials

We want to prove a polynomial is *positive semidefinite* (PSD):

$$\forall \overline{x}.\, p(\overline{x}) \geq 0$$

Proving nonnegativity of polynomials

We want to prove a polynomial is *positive semidefinite* (PSD):

$$\forall \overline{x}.\, p(\overline{x}) \geq 0$$

For a simple example:

$$x^2 - 2x + 1 \geq 0$$

Proving nonnegativity of polynomials

We want to prove a polynomial is *positive semidefinite* (PSD):

$$\forall \overline{x}.\, p(\overline{x}) \geq 0$$

For a simple example:

$$x^2 - 2x + 1 = (x-1)^2 \geq 0$$

it's a perfect square.

A more complicated example

$$23x^2 + 6xy + 3y^2 - 20x + 5 \geq 0$$

A more complicated example

$$23x^2 + 6xy + 3y^2 - 20x + 5 = 5 \cdot (2x - 1)^2 + 3 \cdot (x + y)^2 \geq 0$$

A more complicated example

$$23x^2 + 6xy + 3y^2 - 20x + 5 = 5 \cdot (2x - 1)^2 + 3 \cdot (x + y)^2 \geq 0$$

$$23x^2 + 6xy + 3y^2 - 20x + 5 = \tfrac{1}{23}(23x + 3y - 10)^2 + \tfrac{15}{23}(2y + 1)^2 \geq 0$$

A more complicated example

$$23x^2 + 6xy + 3y^2 - 20x + 5 = 5 \cdot (2x - 1)^2 + 3 \cdot (x + y)^2 \geq 0$$

$$23x^2 + 6xy + 3y^2 - 20x + 5 = \tfrac{1}{23}(23x + 3y - 10)^2 + \tfrac{15}{23}(2y + 1)^2 \geq 0$$

We have found *sum of squares* (SOS) decompositions, which suffice to prove nonnegativity.

From Zeng et al, JSC vol 37, 2004, p83-99

$$w^6 + 2z^2w^3 + x^4 + y^4 + z^4 + 2x^2w + 2x^2z +$$
$$3x^2 + w^2 + 2zw + z^2 + 2z + 2w + 1 \geq 0$$

From Zeng et al, JSC vol 37, 2004, p83-99

$$w^6 + 2z^2w^3 + x^4 + y^4 + z^4 + 2x^2w + 2x^2z +$$
$$3x^2 + w^2 + 2zw + z^2 + 2z + 2w + 1 =$$
$$(y^2)^2 + (x^2 + w + z + 1)^2 + x^2 + (w^3 + z^2)^2 \geq 0$$

Pros and cons

- Provides simple certificate for a theorem prover (or person) to verify

But:

- Polynomial nonnegativity is a rather special problem
- SOS decomposition may not exist even if the polynomial is PSD
- Not easy to find the SOS decomposition even if it does exist

Not quite so special

Nonnegativity over an interval

$$\forall x.\, 0 \leq x \leq 1 \Rightarrow p(x) \geq 0$$

Not quite so special

Nonnegativity over an interval

$$\forall x.\, 0 \leq x \leq 1 \Rightarrow p(x) \geq 0$$

can be reduced to

$$\forall x.\, p(x^2/(1+x^2)) \geq 0$$

and then clear denominators by multiplying through by $(1+x^2)^{\partial(p)}$.

Not quite so special

Nonnegativity over an interval

$$\forall x.\, 0 \leq x \leq 1 \Rightarrow p(x) \geq 0$$

can be reduced to

$$\forall x.\, p(x^2/(1+x^2)) \geq 0$$

and then clear denominators by multiplying through by $(1+x^2)^{\partial(p)}$.

A more complete answer to this problem is coming up . . .

Insufficiency of Sum-of-squares

In general, a PSD polynomial may not have a SOS decomposition, e.g. the *Motzkin form* $1 + x^4y^2 + x^2y^4 - 3x^2y^2$.

Insufficiency of Sum-of-squares

In general, a PSD polynomial may not have a SOS decomposition, e.g. the *Motzkin form* $1 + x^4y^2 + x^2y^4 - 3x^2y^2$.

By Artin's positive solution of Hilbert's 17th problem, a PSD polynomial *is* always a sum of *rational* squares, e.g.

$$1 + x^4y^2 + x^2y^4 - 3x^2y^2 =$$
$$\left(\frac{x^2y(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy^2(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{x^2-y^2}{x^2+y^2}\right)^2$$

Insufficiency of Sum-of-squares

In general, a PSD polynomial may not have a SOS decomposition, e.g. the *Motzkin form* $1 + x^4y^2 + x^2y^4 - 3x^2y^2$.

By Artin's positive solution of Hilbert's 17th problem, a PSD polynomial *is* always a sum of *rational* squares, e.g.

$$1 + x^4y^2 + x^2y^4 - 3x^2y^2 =$$
$$\left(\frac{x^2y(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy^2(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{x^2-y^2}{x^2+y^2}\right)^2$$

However, no good algorithm is known for finding these decompositions, and the known bounds are spectacularly bad.

Sufficiency of sum-of-squares

PSD and SOS are equivalent in several special cases, the most important being

- Univariate polynomials of any degree
- Quadratic forms (all terms have degree exactly 2) in any number of variables (‘complete the square’)

Moreover, one can base complete approaches on various “Positivstellensatz” results that also depend essentially on sums of squares.

The usual Nullstellensatz

Over algebraically closed fields like $\mathbb{C}$ we have a nice simple equivalence.

The polynomial equations $p_1(\overline{x}) = 0, \ldots, p_k(\overline{x}) = 0$ in an algebraically closed field have *no* common solution iff there are polynomials $q_1(\overline{x}), \ldots, q_k(\overline{x})$ such that the following polynomial identity holds:

$$q_1(\overline{x}) \cdot p_1(\overline{x}) + \cdots + q_k(\overline{x}) \cdot p_k(\overline{x}) = 1$$

Thus we can reduce equation-solving to ideal membership and solve it efficiently using Gröbner bases.

The real Nullstellensatz

In the analogous Nullstellensatz result over $\mathbb{R}$, sums of squares play a central role:

The polynomial equations $p_1(\overline{x}) = 0, \ldots, p_k(\overline{x}) = 0$ in a real closed closed field have *no* common solution iff there are polynomials $q_1(\overline{x})$, $\ldots, q_k(\overline{x})$, $s_1(\overline{x}), \ldots, s_m(\overline{x})$ such that

$$q_1(\overline{x}) \cdot p_1(\overline{x}) + \cdots + q_k(\overline{x}) \cdot p_k(\overline{x}) + s_1(\overline{x})^2 + \cdots + s_m(\overline{x})^2 = -1$$

The real Positivstellensatz

There are still more general "Positivstellensatz" results about the inconsistency of a set of equations, negated equations, strict and non-strict inequalities.

Can use this to prove any universally quantified formula in the first-order language of reals, e.g. prove

$$\forall a\ b\ c\ x.\ ax^2 + bx + c = 0 \Rightarrow b^2 - 4ac \geq 0$$

via the following SOS certificate:

$$b^2 - 4ac = (2ax + b)^2 - 4a(ax^2 + bx + c)$$

Reduction to semidefinite programming

Can reduce finding SOS decompositions, and PSatz certificates of bounded degree, to *semidefinite programming* (SDP).

SDP is basically optimizing a linear function of parameters while making a matrix linearly parametrized by those parameters PSD.

Can be considered a generalization of linear programming, and similarly is solvable in polynomial time using interior-point algorithms.

There are many efficient tools to solve the problem effectively in practice. I mostly use CSDP.

Experience and problems

This approach is often much more efficient than competing techniques such as general quantifier elimination.

Lends itself very well to a separation of proof search and LCF-style checking, so fits very well with HOL Light.

Still some awkward numerical problems where the PSD is tight (can become zero) and the rounding to rationals causes loss of PSD-ness.

Available with HOL Light since 2.0 in `Examples/sos.ml`, and seems quite useful. (Includes over-engineered and under-optimized `SOS_CONV`.)

Coq port by Laurent Théry.

The univariate case

Alternative based on the simple observation that every nonnegative univariate polynomial is a sum of squares of *real* polynomials.

All roots, real or complex, must occur in conjugate pairs. Thus the polynomial is a product of factors

$$(x - [a_k + ib_k])(x - [a_k - ib_k])$$

and so is of the form

$$(q(x) + ir(x))(q(x) - ir(x)) = q(x)^2 + r(x)^2$$

To get an exact rational decomposition, we need a more intricate algorithm, but this is the basic idea.

Experience of univariate case

Numerical problems can be particularly annoying with some polynomial bound problems in real applications where the coefficients are non-trivial (60-200 bits).

For example, proving $\forall x.\ |x| \leq k \Rightarrow |f(x) - p(x)| < \epsilon$ where p is a short approximation to a longer polynomial f.

The direct approach is often better than SDP-based methods, for numerical reasons, in such examples.

Conclusion

Very effective technique for universal theory of reals.

Typically more efficient than traditional quantifier elimination, and much better suited to formal certification.

Still some numerical problems. Would be good to experiment with high-precision SDP solver.