An explicit construction of distinguished representations of polynomials nonnegative over finite sets

Pablo A. Parrilo
Automatic Control Laboratory
Swiss Federal Institute of Technology
Physikstrasse 3 - ETL
CH-8092 Zürich - Switzerland

IfA Technical Report AUT02-02
March 13, 2002

Abstract

We present a simple constructive proof of the existence of distinguished sum of squares representations for polynomials nonnegative over finite sets described by polynomial equalities and inequalities. A degree bound is directly obtained, as the cardinality of the support of the summands equals the number of points in the variety. Only basic results from commutative algebra are used in the construction.

1 Introduction

A recurring problem in combinatorial optimization concerns the minimization of a polynomial function $f(x)$ over basic semialgebraic sets of the form:

$$\mathcal{S} = \{x \in \mathbb{R}^n, \quad g_i(x) \geq 0, \quad i = 0, \ldots, r, \qquad h_j(x) = 0, \quad j = 1, \ldots, t\}, \tag{1}$$

where $f, g_i, h_i \in \mathbb{R}[x_1, \ldots, x_n]$. A particular case, very important in applications, is that of 0-1 programming.

There has been recent research activity [Par00, Las01, Par01] concerning the combination of numerical and algebraic techniques for problems in continuous and combinatorial optimization such as the one described above. One of the main driving forces behind this effort is the concrete possibility of applying convex optimization methods to the computation of sum of squares decompositions, a technique pioneered by Shor [Sho87] (see also [Nes00]).

Distinguished representations: Let Σ be the set of polynomials that can be written as sums of squares, i.e., $\Sigma := \{s \in \mathbb{R}[x] \quad | \quad s = \sum_i q_i(x)^2, \quad q_i \in \mathbb{R}[x]\}$. Recent work by Putinar [Put93], Jacobi-Prestel [JP01], and others (see [PD01] for an up-to-date detailed treatment of most available results), establish that if the polynomial $f(x)$ is *strictly* positive over a set $\mathcal{S}$ as in (1) that is *compact*, then under some mild additional assumptions, there exists an affine representation:

$$f(x) = s_0(x) + \sum_i s_i(x) g_i(x) + \sum_i \lambda_i(x) h_i(x), \tag{2}$$

where $s_i \in \Sigma$, $\lambda_i \in \mathbb{R}[x]$. Notice that the positivity of f is a direct consequence of the existence of such representation, as the right-hand side is obviously nonnegative on the feasible set. The main objective of this note is to present a simple *constructive* derivation of this result, with corresponding degree bounds, in the special but practically relevant case of zero dimensional varieties. The only tools employed are some basic results from commutative algebra.

These representations can be understood as specific instances of *Positivstellensatz* refutations, a general technique providing algebraic identities that certify certain properties (such as emptiness) of basic semialgebraic sets. It has been shown in [Par00, Par01] that the search for bounded degree Positivstellensatz refutations can be efficiently done using semidefinite programming. A detailed comparison between the Positivstellensatz and distinguished representations approaches for certifying polynomial nonnegativity will be presented elsewhere [Par02].

An important result by Lasserre [Las02], based on earlier work by Curto and Fialkow, focuses on the case when the feasible set is a grid of points in $\mathbb{R}^n$, and establishes the existence of identities as in (2) with *a priori bounded* degree. Boolean programming is a particularly interesting special case for which this result can be applied.

Our contribution in this paper extends those results in three different directions:

- The feasible set $\mathcal{S}$ is allowed to be an *arbitrary* finite set.
- Structural information on the support and degree of the polynomials s_i is obtained.
- A very simple, explicit *constructive* solution is provided.

In particular, the methods are purely algebraic: no convexity-based techniques (duality, Hahn-Banach, etc.) are employed.

The main idea in the paper boils down to recognizing that when the algebraic variety underlying the problem has only a finite number of elements, then nonnegativity can be established, at least conceptually, by performing only a finite number of elementary tests. At heart, the construction presented here formalizes the translation of this exhaustive enumeration approach into a particular kind of algebraic certificate. For this reason, the results are not particularly helpful from a computational viewpoint: a prerequisite for obtaining the representation is to completely solve the problem. Nevertheless, the results are relevant, because they provide an a priori guarantee of the existence and structure of the sought-after decomposition, as well as deeper insight into some existing results.

2 Representations for nonnegative polynomials

In this section, we present the first step of the construction, dealing with the case where no inequalities are present in (1) (i.e., when $r = 0$). In Section 3 the full case will be treated, building upon the results derived here.

In our setup, the standing assumption will be that the solution set $V = \{x \in \mathbb{C}^n, \quad h_i(x) = 0\}$ of the equality constraints is a zero-dimensional variety, i.e., that it consists only of a finite number of points v_i. Furthermore, we impose the restriction that the ideal I generated by the h_i be *radical* [CLO97, Chapter 4, §2]. This condition can be interpreted as requiring the solution points to have single multiplicity.

Given a polynomial $f(x) \in \mathbb{R}[x]$ nonnegative on the points $v_i \in V \cap \mathbb{R}^n$, we are interested in finding an identity as in (2) that certifies this property. Notice that we do not require all the points $v_i \in V$ to be real.

Remark 1 *For a decomposition (2) to exist, the requirement on the ideal I to be radical (or a suitable alternative) is necessary when f is nonnegative but not strictly positive. For instance, the polynomial $f := x$ is nonnegative over the variety defined by the (non-radical) ideal $\langle x^2 \rangle$, although no decomposition of the form*

$$x = \sigma + \lambda\, x^2, \quad \sigma \in \Sigma$$

can possibly exist.

Remark 2 *The important case of boolean or 0-1 minimization is included in the class of problems treated here. As is well-known, the 0-1 constraints on n variables x_i can be described by n equalities $\{x_i^2 - x_i = 0\}$. It is easy to verify that the generated ideal is indeed radical. The same comments apply,* mutatis mutandis*, for the more general grid problem considered in [Las02].*

Translating certificates If $f(x)$ is nonnegative on all the *real* points v_j, then in some sense there is already available a finite proof of that fact, namely the value of f at the real points in the variety. What needs to be done, therefore, is to "translate" that proof ($f(v_i) \geq 0$) into the required algebraic identity.

For this, we rely on two simple observations:

- In a sum of squares $\sum q_i(x)^2$, the polynomials $q_i(x)$ can always be replaced by their remainders modulo the ideal, incorporating the corresponding quotient terms into the $\lambda_i(x)$ in (2). Equivalently, we can interpret all polynomials in the representation

$$f(x) = s_0(x) + s_i(x) g_i(x), \tag{3}$$

  as elements in the quotient ring $\mathbb{R}[x]/I$.

- If the variety V is a *finite* set then $\mathbb{R}[x]/I$ is *finite dimensional* [CLO97, Chapter 5, §3, Theorem 3]. Furthermore, there exists a linear isomorphism between the quotient ring and the coordinate ring $\mathbb{C}[V]$ of complex-valued polynomials on the solution set (subject to complex-conjugate symmetry).

Provided with the two facts above, our main result can be stated:

Theorem 1 *Let the ideal $I = \langle h_i(x) \rangle$ be zero dimensional and radical. If $f(x)$ is nonnegative on $\mathcal{S}$, then there exists a representation as in (2), constructed by Algorithms 1 and 2 presented below. The monomials appearing on each q_i belong to a fixed subset of cardinality less than or equal to $|V|$.*

The proof of the theorem is a consequence of the constructions in Algorithm 1 below for the equality only case, and Algorithm 2 in the next section for the full case.

Algorithm 1 *Given $f(x)$, with $v_i \in (V \cap \mathbb{R}^n) \Rightarrow f(v_i) \geq 0$, compute an affine representation certifying nonnegativity.*

1. *Find $|V|$ polynomials $p_i(x)$, that satisfy $p_i(v_j) = \delta_{ij}$, where δ_{ij} is the Kronecker delta function. The polynomials p_i are essentially the "indicator function" of the point v_i, taking there the value one and vanishing at the remaining points. They can be easily found using Lagrange interpolation, or given a basis for the quotient ring, by solving a $|V| \times |V|$ system of linear equations.*

2. *For every point $v_i \in \mathbb{R}^n$, or pair of complex conjugate solutions $v_i, v_j \in \mathbb{C}^n$ $(v_i = v_j^*)$, define*

   $$q_i(x) = \gamma\, p_i, \qquad or \qquad q_i(x) = \gamma\, p_i + \gamma^*\, p_j,$$

   respectively, where $\gamma = \sqrt{f(v_i)}$. Notice that $q_i(x) \in \mathbb{R}[x]$: in the first case, because v_i is real and $\gamma \geq 0$, and in the second, as a consequence of the complex-conjugate symmetry.

   With these definitions, it holds that $f(x) = \sum_i q_i^2(x) \quad \forall x \in V$, where only one term per pair of complex conjugate roots appears in the sum.

   Since the ideal I is radical, it follows that

   $$f(x) \equiv \sum_i q_i^2(x) \quad \mod I.$$

   Notice that f is then a sum of squares in the quotient ring.

3. *To put the expression in the standard form (2), choose a basis for the quotient, and reduce the q_i modulo the ideal, to obtain:*

   $$f(x) = \sum_i \tilde{q}_i^2 + \lambda_i(x) h_i(x). \tag{4}$$

□

In the representation, only *standard* monomials [CLO97] (i.e., monomials *not* in the ideal of leading terms $\langle \mathrm{LT}(I) \rangle$) appear in $\tilde{q}_i$, directly providing a degree bound. In the general case, the degree bound may depend on the specific basis chosen for $R[x]/I$ (equivalently, on the specific Gröbner basis for I), though of course the number of distinct monomials in the basis will always be the same, and equal to $|V|$.

For the boolean programming case mentioned in Remark 2, the defining polynomials are already a Gröbner basis with respect to any term ordering, as the leading terms x_i^2 are relatively prime. Therefore, a complete basis for the quotient ring are the 2^n monomials of the form $\prod_i x_i^{\epsilon_i}$, where $\epsilon_i \in \{0, 1\}$, providing the upper bound n on the degree. This corresponds to the case analyzed in [Las01].

Remark 3 *In general, the coefficients of the constructed polynomials do not necessarily belong to the same field as those of the input polynomial, but rather to some finite algebraic extension.*

We present next two simple examples of the application of the proposed method.

Example 1 *Consider the polynomial and constraints:*

$$f := x + y^2 - z^2 + 1, \qquad \begin{cases} h_1 := xy - z = 0 \\ h_2 := yz - x = 0 \\ h_3 := zx - y = 0 \end{cases}$$

The zero-dimensional ideal generated by the constraints g_i is radical, with the corresponding variety having five isolated real points, namely:

$$v_1 = (0,0,0), \quad v_2 = (1,1,1), \quad v_3 = (1,-1,-1), \quad v_4 = (-1,1,-1), \quad v_5 = (-1,-1,1).$$

We construct the interpolating polynomials, already reduced with respect to the quotient basis $\{1, x, y, z, z^2\}$, and the corresponding functional values:

$$\begin{array}{ll} p_1 = 1 - z^2, & f(v_1) = 1 \\ p_2 = (z^2 + z + x + y)/4, & f(v_2) = 2 \\ p_3 = (z^2 - z + x - y)/4, & f(v_3) = 2 \\ p_4 = (z^2 - z - x + y)/4, & f(v_4) = 0 \\ p_4 = (z^2 + z - x - y)/4, & f(v_5) = 0 \end{array}$$

And from this the representation:

$$f = p_1^2 + 2p_2^2 + 2p_3^2 + h_1(5z^3 - 3z)/4 + h_2(x - 5xz^2 - 4)/4 + h_3(-3y - 2z - 5zx)/4$$

is directly obtained. □

It should be noticed that much more concise representations of the nonnegativity of f may conceivably exist. This is exactly the reason why the convex optimization approaches in [Par00, Las01] work well in practice, as these search directly for "short proofs" of a priori bounded support. For this particular example, for instance, it is possible to restrict the support of the squares to just three monomials, rather than the full set of five, as can be seen from the representation:

$$f = (1 + \alpha x + (\alpha - 1)z^2)^2 + \lambda_1 h_1 + \lambda_2 h_2 + \lambda_3 h_3,$$

where $\alpha = \frac{1}{\sqrt{2}}$ and:

$$\begin{array}{rcl} \lambda_1 & = & (1 + \alpha^2 - 2\alpha)z^3 + (2\alpha - 2\alpha^2)z \\ \lambda_2 & = & 2\alpha - 2\alpha^2 + \alpha^2 x + (2\alpha - 1 - \alpha^2)z^2 x \\ \lambda_3 & = & -y + (2\alpha - 1 - \alpha^2)zx + (2\alpha - 2\alpha^2)z. \end{array}$$

Example 2 *In this example, we show how the proposed method can be used to construct algebraic certificates of the nonexistence of real solutions of polynomial equations (as always in this paper, only for the case of zero dimensional systems). Consider the equations:*

$$\begin{array}{c} h_1 := xy + z^2 + 1 = 0 \\ h_2 := yz + x^2 + 1 = 0 \\ h_3 := zx + y^2 + 1 = 0 \end{array}$$

The equations define a zero-dimensional radical ideal, with eight purely imaginary solutions:

$$(0, \pm i, \pm i), \qquad (\pm i, 0, \pm i), \qquad (\pm i, \pm i, 0) \qquad (\pm\frac{i}{\sqrt{2}}, \pm\frac{i}{\sqrt{2}}, \pm\frac{i}{\sqrt{2}}).$$

A good approach to proving that all the solutions are complex, is to show that the polynomial -1 *is nonnegative over the set of real solutions. As this would be clearly absurd, it follows directly that no real solutions can exist. Applying the method, using the quotient basis* $\{x, y, z, z^3\}$*, we have:*

$$\begin{aligned} q_1 &= (-x + y - z - 2z^3)/2 \\ q_2 &= (x - y - z - 2z^3)/2 \\ q_3 &= (x + y - 3z - 2z^3)/2 \\ q_4 &= 2\sqrt{2}z + 2\sqrt{2}z^3 \end{aligned}$$

and defining

$$\begin{aligned} \lambda_1 &= (7 + 9zx + 9yz + 40z^2 + 44z^4 - 22yz^2x - 9xy)/4 \\ \lambda_2 &= (3 - 9yz + 9z^2 + 22y^2z^2 + 9y^2)/4 \\ \lambda_3 &= (-6 - 13z^2 - 9zx - 22yz^3 - 9yz)/4 \end{aligned}$$

we obtain the desired proof:

$$-1 = q_1^2 + q_2^2 + q_3^2 + q_4^2 + h_1\lambda_1 + h_2\lambda_2 + h_3\lambda_3.$$

□

3 Adding inequalities

The constructive methodology outlined in the previous section can be easily extended to the case where inequalities are included in the problem definition. In other words, here we explicitly construct representations of the nonnegativity of f over the semialgebraic set given by $\{g_i(x) \geq 0, h_i(x) = 0\}$, under the same radicality assumptions on the ideal generated by the h_i.

Again, the key insight here is understanding the linear isomorphism between the values of a polynomial at the variety points and its coefficients in the coordinate ring. In a parallel fashion to our earlier construction, we design the polynomials in this transformed domain first, and then map them back into the conventional monomial basis.

The procedure is as follows:

Algorithm 2 *Given the functional values at the variety points* $f(v_j), g_i(v_j)$*, construct polynomials* s_0, s_i *that satisfy (2).*

For every $v_j \in V$ *construct values* $s_i(v_j)$ *as follows:*

1. *If* $v_j \notin \mathbb{R}^n$ *or* $f(v_j) \geq 0$*, then choose:*

$$s_0(v_j) = f(v_j), \quad s_i(v_j) = 0, \quad i = 1, \ldots, m$$

2. If $f(v_j) < 0$, then there is at least one i such that $g_i(v_j) < 0$. Pick any such i, say $i = i^*$, and set:

$$s_0(v_j) = 0, \quad s_i(v_j) = \begin{cases} f(v_j)/g_i(v_j) & \text{if } i = i^* \\ 0 & \text{otherwise} \end{cases}$$

By construction, the values $s_i(v_j)$ are always nonnegative if v_j is real. Furthermore, they satisfy the identity:

$$f(v_j) = s_0(v_j) + \sum_{i=1}^{m} s_i(v_j) g_i(v_j). \tag{5}$$

Now, using Algorithm 1, we can convert by interpolation the nonnegative functional values s_i into sums of squares polynomials. This way, a decomposition as in (2) is finally obtained. is obtained, where the s_i are sums of squares. □

The specific rules for choosing s_i in the algorithm above are just a particular choice out of many possible valid ones. It would be interesting to further explore the possibilities of exploiting the many degrees of freedom that seem to be available.

Example 3 *We return to the setup of Example 1, but now we add the inequality*

$$g_1 := 2x + 1 \geq 0.$$

This has the effect of "cutting off" the two points v_4, v_5 where the minimum was previously achieved. Instead, the smallest value of f over the remaining points is now equal to 1, or equivalently, $f^* := f - 1$ is nonnegative over the feasible set.

To construct an algebraic certificate of this fact, we choose the values of s_0, s_1 according to the procedure described in the previous section. The functional values are:

	v_1	v_2	v_3	v_4	v_5
f^*	0	1	1	−1	−1
g	1	3	3	−1	−1
s_0	0	1	1	0	0
s_1	0	0	0	1	1

Interpolating, and reducing modulo the ideal, we obtain:

$$f - 1 = p_2^2 + p_3^2 + (p_4^2 + p_5^2) g_1 + \lambda_1 h_1 + \lambda_2 h_2 + \lambda_3 h_3,$$

where

$$\begin{aligned} \lambda_1 &= (5z - y - zx + z^3)/4 \\ \lambda_2 &= (-4 - z^2 + x^2 + x - z^2 x)/4 \\ \lambda_3 &= (-3y - 3z + zx - z^3)/4. \end{aligned}$$

□

Acknowledgments: A partial version of the results described here was presented first at the Oberwolfach meeting "Positivität von Polynomen." The author would like to acknowledge the attendants' comments, in particular those of E. Becker, J.B. Lasserre, and M.-F. Roy.

References

[CLO97] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra.* Springer, 1997.

[JP01] T. Jacobi and A. Prestel. Distinguished representations of strictly positive polynomials. *J. Reine Angew. Math.*, 532:223–235, 2001.

[Las01] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817, 2001.

[Las02] J. B. Lasserre. Polynomials nonnegative on a grid and discrete optimization. *Trans. Amer. Math. Soc.*, 354(2):631–649, 2002.

[Nes00] Y. Nesterov. Squared functional systems and optimization problems. In J.B.G. Frenk, C. Roos, T. Terlaky, and S. Zhang, editors, *High Performance Optimization*, pages 405–440. Kluwer Academic Publishers, 2000.

[Par00] P. A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization.* PhD thesis, California Institute of Technology, May 2000. Available at `http://www.cds.caltech.edu/~pablo/`.

[Par01] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. Submitted. Preprint available at `http://www.cds.caltech.edu/~pablo/`, 2001.

[Par02] P. A. Parrilo. Positivstellensatz and distinguished representations approaches for optimization: a comparison. In preparation, 2002.

[PD01] A. Prestel and C. N. Delzell. *Positive polynomials: from Hilbert's 17th problem to real algebra.* Springer Monographs in Mathematics. Springer, 2001.

[Put93] M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.*, 42(3):969–984, 1993.

[Sho87] N. Z. Shor. Class of global minimum bounds of polynomial functions. *Cybernetics*, 23(6):731–734, 1987. (Russian orig.: Kibernetika, No. 6, (1987), 9–11).