AN ALGORITHM FOR SUMS OF SQUARES OF REAL POLYNOMIALS

Victoria Powers and Thorsten Wörmann

Introduction

We present an algorithm to determine if a real polynomial is a sum of squares (of polynomials), and to find an explicit representation if it is a sum of squares. This algorithm uses the fact that a sum of squares representation of a real polynomial corresponds to a real, symmetric, positive semi-definite matrix whose entries satisfy certain linear equations.

Sums of squares and Gram matrices

We fix n and use the following notation in $R := \mathbb{R}[x_1, \ldots, x_n]$: For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, let x^α denote $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$. For $m \in \mathbb{N}_0$, set $\Lambda_m := \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n \mid \alpha_1 + \cdots + \alpha_n \leq m\}$. Then $f \in R$ of degree m can be written $f = \sum_{\alpha \in \Lambda_m} a_\alpha x^\alpha$. We say f is **sos** if f is a sum of squares of elements in R.

Suppose f is sos, say f is a sum of t squares in R, then f must have even degree, say $2m$. Thus $f = \sum_{i=1}^t h_i^2$, where each h_i has degree $\leq m$. Suppose $|\Lambda_m| = k$, then we order the elements of Λ_m in some way: $\Lambda_m = \{\beta_1, \ldots, \beta_k\}$. Set $\bar{x} := (x^{\beta_1}, \ldots, x^{\beta_k})$ and let A be the $k \times t$ matrix with ith column the coefficients of h_i. Then the equation $f = \sum h_i^2$ can be written

$$f = \bar{x} \cdot (AA^T) \cdot \bar{x}^T.$$

The symmetric $k \times k$ matrix $B := AA^T$ is sometimes called a **Gram matrix** of f (associated to the h_i's). Note that B is psd (= "positive semi-definite"), i.e., $\bar{y} \cdot B \cdot \bar{y}^T \geq 0$ for all $\bar{y} = (y_1, \ldots, y_k) \in \mathbb{R}^k$.

The following theorem, in a different form, can be found in [CLR]. However we include the theorem and its proof for the convenience of the reader.

Theorem 1. *Suppose $f \in R$ is of degree $2m$ and $\bar{x}$ is as above. Then f is a sum of squares in R iff there exists a real, symmetric, psd matrix B such that*

$$f = \bar{x} \cdot B \cdot \bar{x}^T.$$

Given such a matrix B of rank t, then we can can construct polynomials $h_1, \ldots, h_t$ such that $f = \sum h_i^2$ and B is a Gram matrix of f associated to the h_i's.

Proof. If $f = \sum h_i^2$ is sos, then as above we take $B = A \cdot A^T$, where A is the matrix whose columns are the coefficients of the h_i's.

Typeset by $\mathcal{AMS}$-TEX

Suppose there exists a real, symmetric, psd matrix B such that $f = \bar{x} \cdot B \cdot \bar{x}^T$ and rank $B = t$. Since B is real symmetric of rank t, there exists a real matrix V and a real diagonal matrix $D = \mathrm{diag}(d_1, \ldots, d_t, 0, \ldots, 0)$ such that $B = V \cdot D \cdot V^T$ and $d_i \neq 0$ for all i. Since B is psd we have $d_i > 0$ for all i. Then

$$(*) \qquad f = \bar{x} \cdot V \cdot D \cdot V^T \cdot \bar{x}^T.$$

Suppose $V = (v_{i,j})$, then for $i = 1, \ldots, t$, set $h_i := \sqrt{d_i} \sum_{j=1}^{k} v_{j,i} x^{\beta_i} \in R$. It follows from $(*)$ that $f = h_1^2 + \cdots + h_t^2$. $\square$

Thus to find a representation of f as a sum of squares, we need only find a matrix B which satisfies the theorem. Further, if we can show that no such B exists, then we know that f is not a sum of squares in R. Note that if $f = \sum a_\alpha x^\alpha$ and $B = (b_{i,j})$ is a $k \times k$ symmetric matrix then by "term inspection", $f = \bar{x} \cdot B \cdot \bar{x}^T$ iff for all $\alpha \in \Lambda_{2m}$,

$$(**) \qquad \sum_{\beta_i + \beta_j = \alpha} b_{i,j} = a_\alpha.$$

The algorithm

Given $f \in R$ of degree $2m$.

1. Let $B = (b_{i,j})$ be a symmetric matrix with variable entries. Solve the linear system that arises from $f = \bar{x} \cdot B \cdot \bar{x}^T$, i.e., solve the linear system defined by equations of the form $(**)$ above, with one equation for each $\alpha \in \Lambda_{2m}$. Note that each variable $b_{i,j}$ appears in only one equation, hence the solution is found by setting all but one variable in each row equal to a parameter and solving for the remaining variable. Then the solution is given by $B = B_0 + \lambda_1 B_1 + \cdots + \lambda_l B_l$, where each B_i is a real symmetric $k \times k$ matrix and $\lambda_1, \ldots, \lambda_l$ are the parameters. In this case $l = k(k+1)/2 - |\Lambda_{2m}|$.

Remark. In general, the size of the matrix B grows rapidly as the number of variables and the degree of the polynomial increases, since $k = |\Lambda_m| = \binom{n+m}{n}$. However for a particular polynomial we can sometimes decrease the size of the Gram matrix by eliminating unnecessary elements of Λ_m. For example, suppose $\alpha \in \Lambda_{2m}$, $\alpha = 2\beta$, and α cannot be written in any other way as a sum of elements in Λ_m. Then if the coefficient of α in f is 0, we know x^β cannot occur in any h_i, cf. [CL, §2] and [CLR, 3.7].

2. We want to find values for the λ_r's that make $B = B_0 + \lambda_1 B_1 + \cdots + \lambda_l B_l$ psd. As is well known, B is psd iff all eigenvalues are non-negative. Let $F(y) = y^k + b_{k-1} y^{k-1} + \cdots + b_0$ be the characteristic polynomial of B. Note that each $b_i \in \mathbb{R}[\lambda_1, \ldots, \lambda_l]$. By Descarte's rule of signs, which is exact for a polynomial with only real roots, $F(y)$ has only non-negative roots iff $(-1)^{(i+k)} b_i \geq 0$ for all $i = 0, \ldots, k-1$. Hence we consider the semi-algebraic set

$$S := \{(\lambda_1, \ldots, \lambda_l) \in \mathbb{R}^l \mid (-1)^{(i+k)} b_i(\lambda_1, \ldots, \lambda_l) \geq 0\}.$$

Then f is sos iff S is nonempty, and a point in S corresponds to a matrix satisfying the conditions of Theorem 1.

Remark. There are several different algorithms for determining whether or not a semi-algebraic set is empty, for example using quantifier elimination. Unfortunately, none of these algorithms are practical apart from "small" examples. For more on this topic, see e.g. [BCR], [C], [GV], [R].

3. Given a matrix $B = (b_{i,j})$ which satisfies the conditions of Theorem 1, then we use the procedure in the proof of the theorem to find a representation of f as a sum of squares.

Example 1. Let $f = x^2y^2 + x^2 + y^2 + 1$, then f is visibly a sum of squares. We want to find all possible representations of f as a sum of squares. Note that by the remark above, if $f = \sum h_i^2$ then the only monomials that can occur in the h_i's are $xy, x, y, 1$. So set $\beta_1 = (1,1)$, $\beta_2 = (1,0)$, $\beta_3 = (0,1)$, and $\beta_4 = (0,0)$. Then the linear system in step 1 of the algorithm is

$$\begin{aligned}
&b_{1,1} = 1,\ 2b_{1,2} = 0,\ 2b_{1,3} = 0,\ 2b_{1,4} + 2b_{2,3} = 0\\
&b_{2,2} = 1,\ 2b_{2,4} = 0\\
&b_{3,3} = 1,\ 2b_{3,4} = 0\\
&b_{4,4} = 1
\end{aligned}$$

Thus the general form of a Gram matrix for f is

$$B = \begin{bmatrix} 1 & 0 & 0 & \lambda \\ 0 & 1 & -\lambda & 0 \\ 0 & -\lambda & 1 & 0 \\ \lambda & 0 & 0 & 1 \end{bmatrix}.$$

The characteristic polynomial of B is

$$y^4 - 4y^3 + (6 - 2\lambda^2)y^2 + (4\lambda^2 - 4)y + (\lambda^4 - 2\lambda^2 + 1),$$

thus B is psd iff $-1 \le \lambda \le 1$. Note that rank $B = 2$ if $\lambda = \pm 1$, otherwise rank $B = 4$. Hence f can be written as a sum of 2 or 4 squares.

We have $B = V \cdot D \cdot V^T$, where $D = \mathrm{diag}(1, 1, 1 - \lambda^2, 1 - \lambda^2)$ and $V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -\lambda & 1 & 0 \\ \lambda & 0 & 0 & 1 \end{bmatrix}$. This yields

$$f = (xy + \lambda)^2 + (x - \lambda y)^2 + (\sqrt{1 - \lambda^2}\, y)^2 + (\sqrt{1 - \lambda^2})^2.$$

Note that $\lambda = 0$ yields the original representation of f as a sum of 4 squares.

Example 2. Let $f(x, y, z) = x^4 + 2x^2y^2 + x^3z + z^4$. A Gram matrix for f would be of the form

$$\begin{bmatrix} 1 & 0 & 2 & \lambda \\ 0 & 2 & 0 & 0 \\ 2 & 0 & -2\lambda & 0 \\ \lambda & 0 & 0 & 1 \end{bmatrix}.$$

In this case, $S \subseteq \{-8 - 4\lambda + 4\lambda^3 \geq 0, -8 - 4\lambda \geq 0\} = \emptyset$. Hence f is not sos.

Example 3. Let $f(x, y, z) = x^6 + 4x^3y^2z + y^6 + 2y^4z^2 + y^2z^4 + 4z^6$. In this case the only exponents that can occur in the h_i's are $\{(3, 0, 0), (0, 3, 0), (0, 2, 1), (0, 1, 2), (0, 0, 3)\}$. We get

$$B = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & r & s \\ 2 & 0 & 2-2r & -s & t \\ 0 & r & -s & 1-2t & 0 \\ 0 & s & t & 0 & 4 \end{bmatrix}$$

as the general form of a Gram matrix.

The corresponding semi-algebraic set is $S = \{-2r - 2t + 9 \geq 0, -r^2 + 4rt - 14r - 2s^2 - t^2 - 16t + 25 \geq 0, 2r^3 - 7r^2 + 2rs^2 + 24rt - 30r + 2s^2t - 10s^2 + 2t^3 - 3t^2 - 34t + 19 \geq 0, 10r^3 + r^2t^2 - 10r^2 - 2rs^2t + 4rs^2 + 36rt - 26r + s^4 + 6s^2t - 10s^2 + 4t^3 - 3t^2 - 4t - 6 \geq 0, 8r^3 + r^2t^2 + 8r^2 + -2rs^2t + 2rs^2 + 16rt - 8r + s^4 - 4s^2t - 2s^2 + 2t^3 - t^2 + 16t - 8 \geq 0\}$. If we set $s = t = 0$, we see $(-1, 0, 0) \in S$, and setting $s = 0$ and $r = -2$ we see $(-2, 0, -3/2) \in S$. In particular, S is nonempty and so f is a sum of squares.

Using $(-1, 0, 0)$,

$$B = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 2 & 0 & 4 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}.$$

Note that rank $B = 3$, so this gives f as a sum of 3 squares. In this case we get

$$f = (x^3 + 2y^2z)^2 + (y^3 - yz^2)^2 + (2z^3)^2.$$

Using $(-2, 0, -3/2)$,

$$B = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 \\ 2 & 0 & 6 & 0 & -3/2 \\ 0 & -2 & 0 & 4 & 0 \\ 0 & 0 & -3/2 & 0 & 4 \end{bmatrix}.$$

Note rank $B = 4$. Proceeding as before we get

$$f = (x^3 + 2y^2z)^2 + (y^3 - 2yz^2)^2 + (\sqrt{2}y^2z - 3\sqrt{2}/4z^3)^2 + (\sqrt{23/8}z^3)^2.$$

Remark. Let $(K, \leq)$ be any ordered field with real closure R, and suppose $f \in K[x_1, \ldots, x_n]$. Then we can easily extend the algorithm to decide whether or not f is a sum of squares in $R[x_1, \ldots, x_n]$.

Acknowledgements

This paper was written while the first author was a visitor at Dortmund University. She gratefully thanks the Deutscher Akademischer Austauschdienst for funding for this visit, as well as Professor E. Becker and his assistants for their warm hospitality during her stay.

References

[BCR] J. Bochnak, M. Coste and M.-F. Roy, *Géométrie Algébrique Réelle*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3. Folge), vol. 12, Springer Verlag, Berlin Heidelberg New York, 1987.

[C] J. Canny, *Improved algorithms for sign determination and existential quantifier elimination*, The Computer Journal **36** (1993), 409–418.

[CL] M.D. Choi and T.Y. Lam, *An old question of Hilbert*, Proceedings of a Conference on Quadratic Forms (G. Orzech, editor), Queen's Papers on Pure and Applied Mathematics, vol. 46, 1977, pp. 385–405.

[CLR] M.D. Choi, T.Y. Lam, and B. Reznick, *Sums of squares of real polynomials*, Symp. in Pure Math., vol. 58, Amer. Math. Soc., Providence, R.I., 1995, pp. 103–126.

[GV] D. Grigor'ev and N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, J. Symb. Comp. **5** (1988), 37–64.

[R] J. Renegar, *Recent progress on the complexity of the decision problem for the reals*, Discrete and Computational Geometry: Papers from the DIMACS Special Year, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 6, American Math. Soc., Providence, RI, 1991, pp. 287–308.

Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322, USA

Fakultät für Mathematik, Universität Dortmund, Lehrstuhl VI, Dortmund 44221, Germany