MIT 6.972 Algebraic techniques and semidefinite optimization April 11, 2006

Lecture 16

Lecturer: Pablo A. Parrilo *Scribe: ???*

1 Generalizing the Hermite matrix

Recall the basic construction of the Hermite matrix $H_q(p)$ in the univariate case, whose signature gave important information on the signs of the polynomial $q(x)$ on the real roots of $p(x)$.

In a very similar way to the extension of the companion matrix to the multivariate case, we can parallel the Hermite form to general zero-dimensional ideals. The basic idea is again to consider the zero-dimensional ideal $I \subset \mathbb{R}[x_1, \ldots, x_n]$, and an associated basis of the quotient ring $B = \{x^{\alpha_1}, \ldots, x^{\alpha_m}\}$, where the elements of B are standard monomials.

For simplicity, we assume first that I is radical. In this case, the corresponding finite variety is given by m distinct points, i.e., $V(I) = \{r_1, \ldots, r_m\} \subset \mathbb{C}^n$. Notice first that, by the definition of the matrices M_{x_i}, we have $\sum_{i=1}^m r_i^\alpha = \mathrm{Tr}[M_{x_1}^{\alpha_1} \cdots M_{x_n}^{\alpha_n}]$. Thus, in a similar way as we did in the univariate case, for any polynomial $q = \sum_\beta q_\beta x^\beta$ we have

$$\sum_{i=1}^m q(r_i) = \mathrm{Tr}[q(M_{x_1}, \ldots, M_{x_n})]. \tag{1}$$

Once again, this implies that if we have access to matrix representations $M_{x_1}, \ldots, M_{x_n}$, then we can explicitly evaluate these expressions. Notice also that, if both q and the generators of the ideal have rational coefficients, then the expression above is also a rational number (even if the roots are not).

Example 1. *Consider the system in Example 4 of the previous lecture, and the polynomial* $p(x, y, z) = (x + y + z)^2$. *To evaluate the sum of the values that this polynomial takes on the variety, we compute:*

$$p(M_x, M_y, M_z) = \mathrm{Tr}\,(M_x + M_y + M_z)^2 = \mathrm{Tr} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 3 & 2 & 2 & 2 \\ 3 & 2 & 3 & 2 & 2 \\ 2 & 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 2 & 3 \end{bmatrix} = 12.$$

As expected, the squares of the sum of the coordinates of each of the five roots are $\{0, 9, 1, 1, 1\}$, *with the total sum being equal to 12.*

Given any $q \in \mathbb{R}[x_1, \ldots, x_n]$, we can then define a Hermite-like matrix $H_q(I)$ as

$$[H_q(I)]_{jk} := \sum_{i=1}^m q(r_i) r_i^{\alpha_j + \alpha_k}. \tag{2}$$

Notice that the rows and columns of $H_q(I)$ are indexed by standard monomials.

Consider now a vector $f = [f_1, \ldots, f_m]^T$, and the quadratic form

$$\begin{aligned} f^T H_q(I) f &:= \sum_{j,k=1}^m \sum_{i=1}^m q(r_i)(f_j r_i^{\alpha_j})(f_k r_i^{\alpha_k}) \\ &= \sum_{i=1}^m q(r_i)(f_1 r_i^{\alpha_1} + \cdots + f_m r_i^{\alpha_m})^2 \\ &= \mathrm{Tr}[(qf^2)(M_{x_1}, \ldots, M_{x_n})]. \end{aligned} \tag{3}$$

As we see, the matrix $H_q(I)$ is a specific representation, in a basis given by standard monomials, of a quadratic form $H_q : \mathbb{C}[x]/I \to \mathbb{C}$, with $H_q : f \to \sum_{i=1}^{m}(qf^2)(r_i)$. The expressions in (3) allow us to explicitly compute a matrix representation of this quadratic map. (What is the other "natural" representation of this map?)

The following theorem then generalizes the results of the univariate case, and enable, among other things, to do root counting.

Theorem 2. *The signature of the matrix $H_q(I)$ is equal to the number of real points r_i in $V(I)$ for which $q(r_i) > 0$, minus the number of real points for which $q(r_i) < 0$.*

Corollary 3. *Consider a zero dimensional ideal I. The signature of the matrix $H_1(I)$ is equal to the number of real roots, i.e., $|V(I) \cap \mathbb{R}^n|$.*

In the general (non-radical) case, we would take the property (3) as the definition of $H_q(I)$, instead of (2). Also, in Theorem 2, multiple real zeros are counted only once.

2 Parametric versions

One of the most appealing properties of Groebner-based eigenvalue methods is that they allow us to extend many of the results to the *parametric* case, i.e., when we are interested in obtaining all solutions of a polynomial system as a function of some additional parameters η_i.

Consider for simplicity the case of a single parameter η, and a polynomial system defined by $p_i(x, \eta) = 0$. In order to solve this for any fixed η, we need to compute a Groebner basis of the corresponding ideal. However, when η changes, it is possible that the resulting set of polynomials is no longer a GB. A way of fixing this inconvenience is to compute instead a *comprehensive Groebner basis*, which is a set of polynomials with the the property that it remains a Groebner basis of I for all possible specializations of the parameters. Using the corresponding monomials as a basis for the quotient space, we can give an eigenvalue characterization of the solutions for all values of η.

3 SOS on quotients

For simplicity, we assume throughout that the ideal I is radical. We can interpret the previous result as essentially stating the fact that when a polynomial is nonnegative on a finite variety, then it is a sum of squares on the quotient ring; see [Par02].

Theorem 4. *Let $f(x)$ be nonnegative on $\{x \in \mathbb{R}^n | h_i(x) = 0\}$. If the ideal $I = \langle h_1, \ldots, h_m \rangle$ is radical, then $f(x)$ is a sum of squares in the quotient ring $\mathbb{R}[x]/I$, i.e.. there exist polynomials q_i, λ_i, such that*

$$f(x) = \sum_i q_i^2(x) + \sum_{i=1}^{m} \lambda_i(x) h_i(x).$$

Remark 5. *The assumption that I is radical (or a suitable local modification) is necessary when $f(x)$ 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 $x = s_0(x) + \lambda(x)x^2$ (where s_0 is SOS), can possibly exist.*

References

[Par02] P. A. Parrilo. An explicit construction of distinguished representations of polynomials nonnegative over finite sets. Technical Report IfA Technical Report AUT02-02. Available from `http://control.ee.ethz.ch/~parrilo`, ETH Zürich, 2002.