MIT 6.972 Algebraic techniques and semidefinite optimization April 13, 2006

Lecture 17

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

One of our main goals in this course is to achieve a better understanding of the techniques available for polynomial systems over the real field. Today we discuss how to certify infeasibility for polynomial equations over the reals, and contrast these approaches with well-known results in linear algebra, linear programming, and complex algebraic geometry.

We will discuss the possible convergence of these schemes in the general case later in the course, concentrating today on an elementary proof of the finite convergence in the zero-dimensional case [Par02].

1 Infeasibility of real polynomial equations

Based on what we have learned in the past weeks, we have a quite satisfactory answer to the question of when a system of polynomial equations has solutions over the complex field. Indeed, as we have seen, given a system of polynomial equations $\{h_i(x) = 0,\ i = 1, \dots, m\}$, we can form the associated ideal $I = \langle h_1, \dots, h_m \rangle$. By the Nullstellensatz, the associated complex variety $V(I)$ (i.e., the solution set $\{x \in \mathbb{C}^n \,|\, h_i(x) = 0\}$) will be empty if and only if $I = \mathbb{C}[x]$, or equivalently, $1 \in I$. Computationally, this condition can be checked by computing a reduced Groebner basis of I (with respect to any term ordering), which will be equal to $\{1\}$ if this holds.

What happens, however, when we are interested in *real* solutions, and not just complex ones? Or, if not only we have equations, but also inequalities? Consider, for instance, the basic semialgebraic set given by

$$S = \{x \in \mathbb{R}^n \mid f_i(x) \geq 0, \quad h_i(x) = 0\}. \tag{1}$$

How to decide if the set S is empty? Can we give a Groebner-like criterion to that demonstrate the infeasibility of this system of equations? Even worse, do we even know that this question can be decided algorithmically[1]?

Fortunately for us, a famous result, the Tarski-Seidenberg theorem, guarantees the algorithmic solvability of this problem (in fact, of a much larger class of problems, that may include quantifiers). We will discuss this powerful approach in more detail later, when presenting cylindrical algebraic decomposition (CAD) techniques, concentrating instead in a more direct way of tackling the feasibility problem.

2 Certificates

Discuss certificates: NP/co-NP, Linear algebra, LP, Nullstellensatz, P-satz

ToDo

3 The zero-dimensional case

What happens in the case where the equations in the system (1) define a zero dimensional ideal? It should be intuitively obvious that, in some sense, such a finite certificate exists. Indeed, *if* we had access to all the roots, of which there are a finite number, just by evaluating the corresponding expressions we could decide the feasibility or infeasibility. As we will see, we can actually "encode" this process in a set of polynomials, that prove the existence of these certificates.

[1] There are certainly similar-looking problems that are *not* decidable. A famous one is the solvability of polynomial equations over the integers. This is Hilbert's 10th problem, solved in 1970 by Matiyasevich; see [Dav73] for a full account of the solution and historical remarks. This result implies, in particular, the nonexistence of an algorithm to solve integer quadratic programming; see [Jer73].

Theorem 1. *Consider the set S in (1), and assume the ideal $I = \langle h_1, \ldots, h_m \rangle$ is radical. Then, S if empty if and only if there exists a decomposition*

$$-1 = s_0(x) + \sum_{i=1} s_i(x) f_i(x) + \sum_{i=1} \lambda_i(x) h_i(x).$$

where the s_i are sums of squares.

Notice that we can equivalently write

$$-1 \equiv s_0(x) + \sum_{i=1} s_i(x) f_i(x) \qquad \bmod I.$$

It should be clear that one direction of the implication is obvious (which one?).

4 Optimization

Since optimization can be interpreted as a parametrized family of feasibility problems, we can directly apply these results towards optimization of polynomial or rational functions. For instance, we have the following result:

Theorem 2. *Let $p(x)$ be nonnegative on $S = \{x \in \mathbb{R}^n | f_i(x) \geq 0,\ h_i(x) = 0\}$, and assume that the ideal $I = \langle h_1, \ldots, h_m \rangle$ is radical. Consider the optimization problem*

$$\max \gamma \qquad s.t. \quad p(x) - \gamma = s_0(x) + \sum_{i=1} s_i(x) f_i(x) + \sum_{i=1} \lambda_i(x) h_i(x).$$

where the s_i are sums of squares, and the decision variables are γ and the coefficients of the polynomials $s_i(x)$, $\lambda_i(x)$. Then, the optimal value of γ is exactly equal to the minimum of $p(x)$ over S.

Notice that this is exactly a sum of squares program, since all the constraints are linear and/or sum of squares constraints.

Remark 3. *The assumption that I is radical (or a suitable local modification) is necessary when $p(x)$ is nonnegative but not strictly positive. For instance, the polynomial $p = x$ 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.*

More details will follow...

References

[Dav73] M. Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80:233–269, 1973.

[Jer73] R.G. Jeroslow. There cannot be any algorithm for integer programming with quadratic constraints. *Operations Res.*, 21:221–224, 1973.

[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.