MIT 6.972 Algebraic techniques and semidefinite optimization March 9, 2006

Lecture 9

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

In this lecture, we study first a relatively simple type of polynomial equations, namely *binomial equations*. As we will see, in this case there exists a quite efficient solution method. We define next an important geometric and combinatorial object associated with every multivariate polynomial, called the *Newton polytope*. Finally, we put together these two notions in the formulation of a family of bounds on the number of solutions of systems of polynomial equations. Our presentation of the material here is inspired by [Stu02, Chapter 3].

1 Binomial equations

We introduce in this section a particular kind of polynomial equations, that have nice computational properties. A *binomial* system of polynomial equations is one where each equation has only two terms. We also assume that the system has only a finite number of solutions, i.e., the solution set is a finite set of points in $\mathbb{C}^n$. We are interested in determining the exact number of solutions, and in efficient computational procedures for solving the system.

Let's start with an example. Consider the binomial system given by

$$\begin{aligned} 8x^2y^3 - 1 &= 0 \\ 2x^3y^2 - yx &= 0. \end{aligned} \tag{1}$$

If we assume that the solutions satisfy $x \neq 0, y \neq 0$, then we can put these equations in the more symmetric form

$$\begin{aligned} 8x^2y^3 &= 1 \\ 2x^2y &= 1. \end{aligned} \tag{2}$$

Now, by dividing the first equation by the second one, we obtain $4y^2 = 1$, which has two solutions ($y = \frac{1}{2}$ and $y = -\frac{1}{2}$). Substituting into the resulting equations for every value of y we have two corresponding values of x, so the system has a big total of four complex solutions.

Let's try to understand in a big more detail what manipulations we where performing here. For this, let's define the integer matrix

$$B = \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix}$$

corresponding to the exponents in (2). Notice that when we divided the two equations, that is equivalent to an elementary row operation in the matrix B, namely subtracting the second row of B from the first one. Thus, the operations we have done can be understood as the matrix multiplication $UB = C$, where

$$U = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}, \qquad C = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}.$$

The fact that the matrix C is lower triangular, is what allows us to start solving the system for y, and then backsolving for the other variable.

It is not too difficult to understand from this example how to generalize this. Let $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, and consider a system of binomial equations in n variables, where we are interested in computing (or bounding the number of) solutions in $(\mathbb{C}^*)^n$. We can always put the system in the normalized form in (2). Notice that, in general, the entries of the integer B could be either positive or negative (i.e., we write polynomials in x_i and x_i^{-1}, which is fine since $x_i \neq 0$).

Then, a well-known result in integer linear algebra (the Hermite normal form of an integer matrix) guarantees the existence of a matrix $U \in SL_n(\mathbb{Z})$ (an integer matrix, with determinant equal to one),

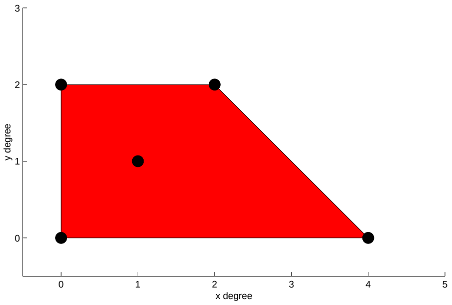

Figure 1: Newton polytope of the polynomial $p(x, y) = 5 - xy - x^2y^2 + 3y^2 + x^4$.

such that $C = UB$ is a lower triangular matrix. We can then use this expression to obtain values for the last variable, and backsolve to obtain all solutions.

How can we determine the number of solutions from this factorization? When backsubstituting using C, at each step we have to solve an equation of the type $x_i^{c_{ii}} = d_i$, and thus the current number of possible solutions is multiplied by $|c_{ii}|$. Therefore, the total number of solutions in $(\mathbb{C}^*)^n$ will then be equal to $|\det(C)| = |\det(U)\det(B)| = |\det(B)|$.

Remark 1. *To compute the Hermite normal form of an integer matrix in Maple, you can use the command `ihermite`. In Mathematica, use instead `HermiteNormalForm`.*

2 Newton polytopes

Many of the polynomial systems that appear in practice are far from being "generic," but rather present a number of structural features that, when properly exploited, allow for much more efficient computational techniques. This is quite similar to the situation in numerical linear algebra, where there is a big difference in performance between algorithms that take into account the sparsity structure of a matrix and those that do not. For matrices, the standard notion of sparsity is relatively straightforward, and relates mostly to the number of nonzero coefficients. In computational algebra, however, there exists a much more refined notion of sparsity that refers not only to the number of zero coefficients of a polynomial, but also to the underlying combinatorial structure.

This notion of sparsity for multivariate polynomials is usually presented in terms of the *Newton polytope* of a polynomial, defined below.

Definition 2. *Consider a multivariate polynomial $p(x_1, \ldots, x_n) = \sum_\alpha c_\alpha x^\alpha$. The* Newton polytope *of p, denoted by New(f), is defined as the convex hull of the set of exponents α, considered as vectors in $\mathbb{R}^n$.*

Thus, the Newton polytope of a polynomial always has integer extreme points, given by a subset of the exponents of the polynomial.

Example 3. *Consider the polynomial $p(x, y) = 5 - xy - x^2y^2 + 3y^2 + x^4$. Its Newton polytope New(f), displayed in Figure 1, is the convex hull of the points $(0, 0), (1, 1), (2, 2), (0, 2), (4, 0)$.*

Example 4. *Consider the polynomial $p(x, y) = 1 - x^2 + xy + 4y^4$. Its Newton polytope New(p) is the triangle in $\mathbb{R}^2$ with vertices $\{(0, 0), (2, 0), (0, 4)\}$.*

Newton polytopes are an essential tool when considering polynomial arithmetic because of the following fundamental identity:

$$\text{New}(g \cdot h) = \text{New}(g) + \text{New}(h),$$

where + denotes the Minkowski addition of polytopes.

Example 5. *Let $p(a,b,c,d) = (a^4+1)(b^4+1)(c^4+1)(d^4+1) + 2a + 3b + 4c + 5d$. Its Newton polytope is the hypercube in $\mathbb{R}^4$ of side length equal to 4, and with opposing vertices at $(0,0,0,0)$ and $(4,4,4,4)$.*

It is a general theme in computational algebra that the complexity of many problems involving polynomials is directly related to some measure of the size of the corresponding Newton polytopes. We discuss an example below, in terms of the number of solutions of polynomial equations. We will encounter Newton polytopes again later in the course, when discussing the semidefinite characterization of polynomials that are sums of squares.

3 The Bézout and BKK bounds

Consider a system of two polynomial equations, $p(x,y) = 0$, $q(x,y) = 0$. As we have seen in previous lectures, we can solve this by computing the resultant of the polynomials p and q with respect to either variable, and then factorizing the corresponding univariate polynomial. If the degree of the polynomials is d_1 and d_2, respectively, then the degree of the resultant is bounded by $d_1 \cdot d_2$, and thus the number of zeros of the system is at most this number.

However, when the polynomials p and q are sparse (in the sense defined earlier) then the number of solutions can be much smaller. For instance, the system

$$\begin{aligned} a + bx + cy + dy^2 &= 0 \\ ex + fy + gxy &= 0 \end{aligned} \tag{3}$$

has, for a generic choice of the coefficients $\{a,\ldots,g\}$, exactly three complex roots, while the bound based on the individuals degrees (usually called the Bézout bound) will give a total of $2 \times 2 = 4$. As we will see, much sharper bounds can be obtained by considering the Newton polytopes of the individual equations.

To introduce the main theorem, we need to introduce the following concept, that generalizes the notion of volume of a polytope, to a collection of them.

Definition 6. *Consider polytopes $P_1,\ldots,P_n \subset \mathbb{R}^n$, nonnegative scalars $\lambda_1,\ldots,\lambda_n$, and let $V(\lambda) = \mathrm{Vol}(\lambda_1 P_1 + \cdots + \lambda_n P_n)$. It can be shown that $V(\lambda)$ is a homogeneous polynomial of degree n. The* mixed volume *$MV(P_1,\ldots,P_n)$ is the coefficient of this polynomial, corresponding to the monomial $\lambda_1\lambda_2\cdots\lambda_n$.*

The main result in this area, with different versions due to Bernstein, Kouchnirenko, and Khovanskii, relates the number of solutions of a sparse polynomial system with the mixed volume of the Newton polytopes of the individual equations. Formally, we have

Theorem 7. *The number of solutions in $(\mathbb{C}^*)^n$ of a sparse polynomial system of n equations and n unknowns is less than or equal to the mixed volume of the n Newton polytopes. If the coefficients are "generic" enough, then the upper bound is achieved.*

The basic idea behind the derivation of the theorem is to introduce an additional parameter t in the equations, in such a way that for $t = 1$ we have the original system, while for $t = 0$ the system is binomial, which as we have seen can be solved in an efficient manner. This process is usually called a *toric deformation*, and is somewhat similar in spirit to the homotopies used in interior point methods. To make our words a bit more precise, an important fact is that we will not deform to just one binomial system, but actually to a collection of them, given by what is called a *mixed subdivision* of the sum of Newton polytopes. The important fact is that the sum of the number of roots of all these binomial systems is exactly equal to the mixed volume of the collection of polytopes.

Example 8. *Consider the univariate polynomial*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_m x^m,$$

where $n \geq m$. It is clear that the Newton polytope is the line segment with endpoints in n and m. The mixed volume (in this case, just the volume) is equal to $n - m$. Thus, the BKK bound for this polynomial is equal to $n - m$, which is clearly exact for generic choices of the coefficients.

Example 9. *Let us consider again the example discussed in (1). The Newton polytope of the first polynomial is the line segment with endpoints* $(0,0)$ *and* $(2,3)$*, while the second one has endpoints* $(1,1)$ *and* $(3,2)$*. If we denote these by* P_1 *and* P_2*, it is easy to see that*

$$\mathrm{Vol}(\lambda_1 P_1 + \lambda_2 P_2) = 4\lambda_1\lambda_2,$$

and thus the mixed volume of (P_1, P_2) *is equal to* 4*, which is the number of solutions of (1).*

4 Application: Nash equilibria

We can use the results described, to give a bound on the number of Nash equilibria of a game. For simplicity, consider the three player case, where each player has two pure strategies. We are interested here only in totally mixed equilibria, i.e., those where the players randomize among all their pure strategies with nonzero probability (if this is not the case, then by eliminating the never played strategies we can reduce the game to the totally mixed case). Thus, the mixed strategies can be parametrized in terms of three variables $a, b, c \in (0,1)$, representing the probabilities with which they play their different strategies.

It can be shown that the Nash equilibrium condition result in a polynomial system of the structure

$$\begin{aligned} p_{11}bc + p_{12}b + p_{13}c + p_{14} &= 0 \\ p_{21}ca + p_{22}c + p_{23}a + p_{24} &= 0 \\ p_{31}ab + p_{32}a + p_{33}b + p_{34} &= 0, \end{aligned} \tag{4}$$

where the coefficients p_{ij} are explicit linear functions of the payoffs. The mixed volume of the Newton polytopes of these three equations is equal to 2, so the maximum number of totally mixed Nash equilibria that a three-player, two-strategy game can have is equal to two.

Theorem 10 ([Stu02, p.82])**.** *The maximum number of isolated totally mixed Nash equilibria for an* n*-person game where each player has two pure strategies is equal to the mixed volume of the* n *facets of the* n *cube. This number is the closest integer to* $n!/e$*.*

There are extensions of this result to the graphical case; see [Stu02] and the references therein for details.

References

[Stu02] B. Sturmfels. *Solving Systems of Polynomial Equations.* AMS, Providence, R.I., 2002.