Lifting Fibers

In this lecture we sketch a symbolic analogue to the witness sets, the lifting fibers to generalize the Rational Univariate Representation or Kronecker Parametrization to positive dimensional solution sets. The lifting fibers have their origin in geometric complexity results [2] and are described in [3], [4], and [1]. The symbolic solving refers to Kronecker's interpretation of solving a producing techniques for computing **with** the roots [5] (see also the sequel [6]), as executed by defining algebraic extensions of the integer or rational number field.

1 Specializing Variables

Consider equation of the sphere $f(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - 1 = 0$, as a hypersurface in $\mathbb{C}^3$. To compute generic points on this surface, we can add two random hyperplanes to it, or specialize two variables at random values, respectively described in the two systems below:

$$\left\{ \begin{array}{c} x_1^2 + x_2^2 + x_3^2 - 1 = 0 \\ c_{10} + c_{11}x_1 + c_{12}x_2 + c_{13}x_3 = 0 \\ c_{20} + c_{21}x_1 + c_{22}x_2 + c_{23}x_3 = 0 \end{array} \right. \qquad \left\{ \begin{array}{c} x_1^2 + x_2^2 + x_3^2 - 1 = 0 \\ x_1 = c_1 \\ x_2 = c_2. \end{array} \right. \tag{1}$$

Specializing variables is depicted at the left of Figure 1. At the right of Figure 1 is the special witness set.

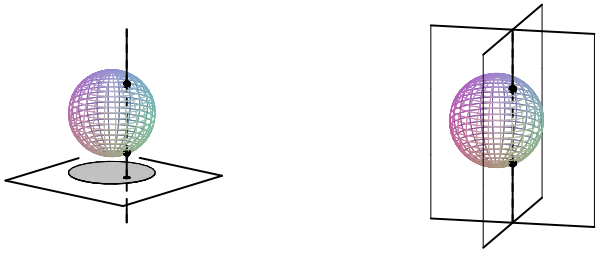

Figure 1: A sphere intersected by a vertical line at the left, specializing x_1 and x_2. As the line is the intersection of two planes, we see the equivalent witness set representation.

The two hyperplanes added to f determine a random line which cuts the sphere in two general points. If we bring the line in vertical position, parallel to the third coordinate axis, then with every choice (c_1, c_2) of the coordinates (x_1, x_2) (where the line crosses the horizontal plane $x_3 = 0$), there are two values for x_3 obtained via solving $f(c_1, c_2, x_3) = 0$.

Although Figure 1 is a real picture, intuitively we see that Bertini's theorem also applies when working with more specific intersections, i.e.: except for an algebraic set of special values, the points cut out by the intersection are regular. What does not hold generally is the number of points we may find. Consider for example $x_1^2 + x_2^2 + x_3 - 1$, then specializing x_1 and x_2 would lead to only one solution whereas the degree of the hypersurface is obviously still two.

We say that a r-dimensional ideal I is in Noether position if specializing the first r variables leads to a variety W so that $\deg(W) = \deg(V(I))$. This implies that the first r variables are free, while the last $n - r$ ones are the dependent variables. By a random coordinate change we can bring any ideal into Noether position. We will consider pure dimensional algebraic sets, i.e.: all solution sets have the same dimension.

2 cyclic n-roots, n has square divisor

When n has a divisor which is a square, like $n = 4$, 8, 9, 12, etc., then the cyclic n-roots problem is known to have a positive dimensional solution set. Consider for example the cyclic 4-roots problem:

$$f(\mathbf{x}) = \begin{cases} x_1 + x_2 + x_3 + x_4 = 0 \\ x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 = 0 \\ x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2 = 0 \\ x_1x_2x_3x_4 - 1 = 0. \end{cases} \tag{2}$$

This system has a one dimensional solution set. Like is often the case the solution set belongs to a linear space. The substitution $x_3 = -x_1$ and $x_4 = -x_2$ reduces the system (2) to one single equation $x_1^2x_2^2 - 1 = 0$. We see thus that there is a curve of degree four.

The cyclic 8-roots system has a curve of degree 144 and there is a two dimension set of cyclic 9-roots, of degree 18.

3 Geometric Resolution

In the table (constructed with the help of Anton Leykin, and taken from [7]) below we sketch the analogy between witness sets and lifting fibers. Both lead to to finding generic points on pure dimensional solution sets and to a geometric resolution. A fiber is the inverse of a map. Here the fiber π^{-1} is the inverse of the projection map π, projecting an r-dimensional algebraic set onto the space of the first r variables.

Generic Points on a Pure Dimensional Solution Set V	
Symbolic: lifting fiber $\pi^{-1}(\mathbf{p})$	Numeric: witness set $W(\mathbf{c})$
computational field $\mathbb{K}$: numbers in $\mathbb{Q}$ (or in a finite extension) field operations done *symbolically*	*numeric* field $\mathbb{C}$: floating point complex numbers with machine arithmetic
With a *symbolic* coordinate change we bring V to Noether position: replace $\mathbf{x}$ by $M\mathbf{y}$, $M \in \mathbb{K}^{n\times n}$	We slice V *numerically* with some randomly chosen hyperplanes: $A\mathbf{x} = \mathbf{c}$, $A \in \mathbb{C}^{r\times n}$, $\mathbf{c} \in \mathbb{C}^r$, $\text{rank}(A) = r$
choose M for coordinate change	*choose* A for slicing hyperplanes
$\dim V = r$: specialize r free variables	$\dim V = r$: cut with r hyperplanes
$\pi^{-1}(\mathbf{p}) = \{\ \mathbf{y} \in \mathbb{C}^n \mid f(\mathbf{y}) = \mathbf{0}$ and $y_1 = p_1, \ldots, y_r = p_r\ \}$	$W(\mathbf{c}) = \{\ \mathbf{x} \in \mathbb{C}^n \mid f(\mathbf{x}) = \mathbf{0}$ and $A\mathbf{x} = \mathbf{c}\ \}$
choice of values $\mathbf{p} = (p_1, p_2, \ldots, p_r)$ for free variables $(y_1, y_2, \ldots, y_r)$ such that the fiber $\pi^{-1}(\mathbf{p})$ is finite	*choice* of r constants $\mathbf{c} = (c_1, c_2, \ldots, c_r)$ so that $\begin{cases} f(\mathbf{x}) = \mathbf{0} \\ A\mathbf{x} = \mathbf{c} \end{cases}$ has isolated solutions
for almost all $\mathbf{p} \in k^r$: $\pi^{-1}(\mathbf{p})$ consists of $\deg V$ smooth points	*for almost all* $\mathbf{c} \in \mathbb{C}^r$: $W(\mathbf{c})$ consists of $\deg V$ smooth points
where *for almost all* means except for a proper algebraic subset of bad choices	

While the geometric analogue between lifting fibers and witness sets is made apparent by the dictionary given in the table above, the main difference lies in the choice of the number field. The choice between working in algebraic extensions of the rational number field (or of some finite field) and working with floating-point complex numbers has dramatic implications on the kind of algorithms that must be used and the type of applications that can be solved.

Figure 2 illustrates the idea of lifting segments onto an algebraic set. Consider

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + (x_3 - 2)^2 - 2 = 0. \tag{3}$$

Taking the origin as the lifting point, a univariate representation of $f^{-1}(\mathbf{0})$ has the form

$$q(T) = (T-2)^2 - 2 = 0, \quad \begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = T. \end{cases} \tag{4}$$

In Figure 2 we "release" the variable x_2, thus lifting the line $x_1 = 0$ to the curve on the sphere $f^{-1}(\mathbf{0})$.

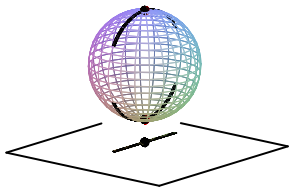

Figure 2: A line segment is lifted to two curves on the sphere.

Then the bivariate representation of this curve has the form

$$Q_1(x_2, T) = x_2^2 + (T-2)^2 - 2 = 0, \quad \begin{cases} x_1 = 0 \\ x_3 = T. \end{cases} \tag{5}$$

In general, this lifting step is executed via the Newton-Hensel algorithm. Suppose we now want to intersect the sphere with the parabolic cylinder $x_2 = x_3^2 - 1$, represented in lifted form as

$$Q_2(x_2, T) = x_2 - T^2 + 1, \quad \begin{cases} x_1 = 0 \\ x_3 = T. \end{cases} \tag{6}$$

To compute a univariate representation of the curve of intersection defined by the sphere and cylinder, we compute the resultant of Q_1 and Q_2, eliminating x_2, in Maple notation:

$$\text{resultant}(Q_1, Q_2, x_2) = T^4 - 2T^2 - 1. \tag{7}$$

Thus we obtained

$$q(T) = T^4 - T^2 - 4T + 3, \quad \begin{cases} x_1 = 0 \\ x_2 = T^2 - 1 \\ x_3 = T. \end{cases} \tag{8}$$

Observe $\deg(q) = 4$, as we may expect from Bézout's theorem when we intersect two quadratic surfaces, the curve of intersection is a quartic. For plotting, we now "release" the x_1 again, using the first equation of the sphere:

$$x_1^2 + (T^2-1)^2 + (T-2)^2 - 2 = 0 \quad \Rightarrow \quad x_1 = \pm\sqrt{-3 + 4T + T^2 - T^4}. \tag{9}$$

Figure 3 shows the plot of the curve of intersection.

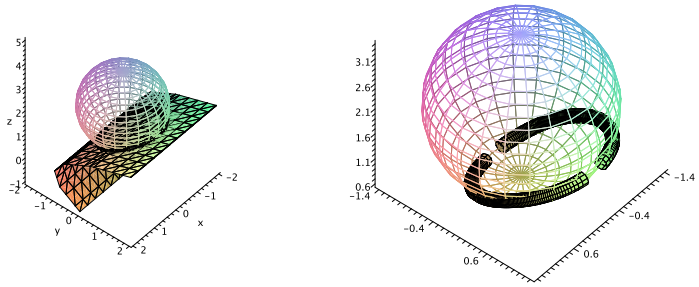

Figure 3: A quartic as the intersection of a sphere and a parabolic cylinder.

A lifting fiber of a pure dimensional solution set V, $r = \dim(V)$, consists thus of the following:

1. a matrix M to bring V in Noether position;
2. a lifting point $\mathbf{p}$ with special values for the first r variables;
3. a polynomial $q(T)$: $\deg(q) = \deg(V)$; and
4. $n - r$ polynomials in T to define the dependent variables.

4 Noether Position

To define Noether position properly, we need several concepts of commutative algebra. The definitions below are adapted from [1]. Denote by $\mathbb{K}$ a commutative field of characteristic zero (think of $\mathbb{Q}$) and let I be an ideal in $\mathbb{K}[x_1, x_2, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$.

Definition 4.1 The polynomials $e_1, e_2, \ldots, e_s \in \mathbb{K}[\mathbf{x}]$ are *algebraically dependent modulo* I if there exists a nonzero polynomial E in s variables: $E(e_1, e_2, \ldots, e_s) \in I$. Otherwise, if no such E exists, $e_1, e_2, \ldots, e_s$ are *algebraically independent modulo* I.

The notion of algebraic independence is used to define transcendence degree and dimension of an ideal (attributed to van der Waerden). Basically we will say that the dimension of a variety is the maximum number of independent functions on the variety.

Definition 4.2 A field extension $\mathbb{K}$ of $\mathbb{K}$ has *the transcendence degree* equal to the maximal number of elements in $\mathbb{K}$ which are algebraically independent.

Definition 4.3 If I is prime (or equivalently: $V(I)$ is irreducible), then *the dimension of* I is the transcendence degree of the quotient field of $\mathbb{K}[\mathbf{x}]/I$ over $\mathbb{K}$.

After settling on the dimension, we need to define degrees to make the notion of Noether position algebraic. Let $\mathbb{A}$ be a subring of $\mathbb{K}[\mathbf{x}]$ with unity.

Definition 4.4 The polynomial $e \in \mathbb{K}[\mathbf{x}]$ is *algebraic over* $\mathbb{A}$ *modulo* I if there exists a nonzero $q \in \mathbb{A}[T]$: $q(e) \in I$. Moreover, if q is monic (its leading coefficients equals one), then e is *integral over* $\mathbb{A}$ *modulo* I.

Definition 4.5 The ideal I is *in Noether position* if there exists an $r \in \{0, 1, \ldots, n\}$ such that

1. the variables $x_1, x_2, \ldots, x_r$ are algebraically independent modulo I; and
2. the variables $x_{r+1}, x_{r+2}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, x_2, \ldots, x_r]$ modulo I.

For an ideal I in Noether position, any $e \in \mathbb{K}[\mathbf{x}]$ is integral over $\mathbb{K}[x_1, x_2, \ldots, x_r]$ modulo I. We can then also say that $\mathbb{K}[\mathbf{x}]/I$ is an integral ring extension of $\mathbb{K}[x_1, x_2, \ldots, x_r]$. The trivial case where $I = \langle 1 \rangle$ (or $V(I) = \emptyset$) corresponds to $r = 0$.

Theorem 4.1 *Assume $I \neq \langle 1 \rangle$ and I is prime. Then*

1. *If $x_{r+1}, x_{r+2}, \ldots, x_n$ are integral over $\mathbb{K}[x_1, x_2, \ldots, x_r]$ modulo I, then* $\dim(I) \leq r$.
   Moreover, $\dim(I) = r \Leftrightarrow x_1, x_2, \ldots, x_r$ *are algebraically independent modulo I.*
2. *If $x_1, x_2, \ldots, x_r$ are algebraically independent modulo I, then* $\dim(I) \geq r$.
   Moreover, $\dim(I) = r \Leftrightarrow x_{r+1}, x_{r+2}, \ldots, x_n$ *are algebraic over $\mathbb{K}[x_1, x_2, \ldots, x_r]$ modulo I.*

In general, Noether position of an ideal does not imply that the corresponding homogeneous ideal is in Noether position. Therefore, we define a stronger notion of Noether position.

Definition 4.6 A polynomial $e \in \mathbb{K}[\mathbf{x}]$, integral over $\mathbb{A}$ modulo I is *generally integral over $\mathbb{A}$ modulo I* if for a monic $q \in \mathbb{A}[T]$, $q(e) \in I$:

$$\deg\left(q\left(\mathbf{x}, T^{\deg(e)}\right)\right) = \deg_T\left(q\left(\mathbf{x}, T^{\deg(e)}\right)\right) \tag{10}$$

where $\deg_T(\cdot)$ is the degree of q in T as we view $q \in \mathbb{K}[\mathbf{x}, T]$.

Definition 4.7 An ideal I, with $\dim(I) = r$, is *in general Noether position* if I is in Noether position and if additionally, the variables $x_1, x_2, \ldots, x_n$ are generally integral over $\mathbb{K}[\mathbf{x}]$ modulo I.

For example, $\langle x_1^2 - x_2 \rangle$ is in Noether position, but not in general Noether position. The ideal $\langle x_1 - x_2^2 \rangle$ is in general Noether position. Permuting the variables is not enough to bring an ideal in general Noether position.

We can bring I in (general) Noether position, using linear coordinate transformations defined by matrices $M \in \mathbb{K}^{n \times n}$. Denote the ideal I after transformation by M as

$$I \circ M = \langle\ f(M\mathbf{x}) \mid f \in I\ \rangle. \tag{11}$$

Repeated application of the following lemma allows for an incremental procedure to bring an ideal into Noether position.

Lemma 4.1 *Let $i \in \{1, 2, \ldots, n\}$ and assume*

1. *$x_{i+1}, x_{i+2}, \ldots, x_n$ are (generally) integral over $\mathbb{K}[x_1, x_2, \ldots, x_i]$ modulo I; and*
2. *$x_1, x_2, \ldots, x_i$ are algebraically dependent modulo I.*

Then, for any nonzero $p \in I \cap \mathbb{K}[x_1, x_2, \ldots, x_i]$ and for any point $(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, 1)$ that does not annihilate the highest degree part of p, the variables $x_i, x_{i+1}, \ldots, x_n$ are (generally) integral over $\mathbb{K}[x_1, x_2, \ldots, x_{i-1}]$ modulo $I \circ M$, where M is defined by

$$M \begin{bmatrix} x_1 \\ \vdots \\ x_{i-1} \\ x_i \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 + \alpha_1 x_i \\ \vdots \\ x_{i-1} + \alpha_{i-1} x_{i-1} \\ x_i \\ \vdots \\ x_n \end{bmatrix}. \tag{12}$$

Moreover: $\deg_{x_i}(p(M\mathbf{x})) = \deg(p(M\mathbf{x}))$.

5 Exercises

1. Permuting variables is just not enough to bring an ideal into Noether position. Give an example where the ideal cannot be brought into Noether position, even if we consider all permutations of the variables.

2. A coordinate change in n-space is defined by $\mathbf{x} = M\mathbf{y}$ for a matrix $M \in \mathbb{C}^{n \times n}$. Consider

$$M = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \tag{13}$$

   where the constants c_1, c_2, ..., c_n are random complex numbers. Would it be enough to take this kind of coordinate change to bring any ideal into Noether position? Justify your answer.

3. Consider the geometric resolution of two general spheres, whose curve of intersection is a real quartic. Do the lifting and intersection step of a geometric resolution. Make a plot of the final result.

References

[1] C. Durvye and G. Lecerf. A concise proof of the Kronecker polynomial system solver from scratch. *Expositiones Mathematicae*, 26:101–139, 2008.

[2] M. Giusti and J. Heintz. La détermination de la dimension et des points isolées d'une variété algébrique peuvent s'effectuer en temps polynomial. In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra, Cortona 1991*, volume XXXIV of *Symposia Mathematica*, pages 216–256. Cambridge University Press, 1993.

[3] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[4] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.

[5] T. Mora. *Solving Polynomial Equation Systems I: the Kronecker-Duval Philosophy*, volume 88 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, 2003.

[6] T. Mora. *Solving Polynomial Equation Systems II: Macaulay's Paradigm and Gröbner Technology*, volume 99 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, 2005.

[7] A.J. Sommese, J. Verschelde, and C.W. Wampler. Solving polynomial systems equation by equation. In *Algorithms in Algebraic Geometry*, volume 146 of *The IMA Volumes in Mathematics and Its Applications*, pages 133–152. Springer-Verlag, 2008.