Witness Sets

Witness sets offer an efficient numerical representation of positive dimensional solution sets of polynomial systems. Motivated by applications from mechanical design, the numerical treatment of solution sets of any dimension inspired the field numerical algebraic geometry [3, 4]. We consider the design of sevenbar mechanisms [5, 6]. A cascade of homotopies [2] leads to a refined version of Bézout’s theorem.

1 Dimension and Degree

The two most important attributes of a positive dimensional solution set are its dimension and the degree. Consider for example the twisted cubic, defined by

\[
\begin{align*}
  f(x) &= \begin{cases} 
    x_2 - x_1^2 = 0 \\
    x_3 - x_1^3 = 0 
  \end{cases} \\
  (x_1, x_2, x_3) &= (t, t^2, t^3), t \in \mathbb{C}. 
\end{align*}
\]

The curve is displayed in Figure 1.

![Figure 1: The twisted cubic as defined by the intersection of a quadratic and a cubic surface.](image)

For system which defines a solution set of dimension \(k\), we may add \(k\) random hyperplanes to cut the solution set with, so that we end up with isolated solutions. If we then count the isolated solutions that satisfy the system and lie on the added hyperplanes, then we obtain the degree of the solution set. For the twisted cubic we thus consider the system

\[
\begin{align*}
  E(f)(x) &= \begin{cases} 
    x_2 - x_1^2 = 0 \\
    x_3 - x_1^3 = 0 \\
    c_0 + c_1x_1 + c_2x_2 + c_3x_3 = 0 
  \end{cases} \\
  c_0, c_1, c_2, c_3 \in \mathbb{C}, 
\end{align*}
\]

where the complex coefficients of the last equation are random numbers. The substitution \(x_2 = x_1^2\) and \(x_3 = x_1^3\) in the last equation shows that the degree of \(f^{-1}(0)\) equals three.

A witness point is a solution of a polynomial system which lies on a set of generic hyperplanes. The number of generic hyperplanes used to isolate a point from a solution component equals the dimension of the solution set. The number of witness points on one component cut out by the same set of generic hyperplanes equals the degree of the solution set. A witness set for a \(k\)-dimensional solution set consists of \(k\) random hyperplanes and the set of isolated solutions comprising the intersection of the component with those hyperplanes.

For the example of the twisted cubic, the witness set consists in the extended polynomial system \(E(f) = 0\) along with its three isolated solutions. Because of the random choice of the complex coefficients of the hyperplane, the three isolated solutions are regular (as a consequence of Bertini’s theorems). Via a homotopy which moves the hyperplane, we sample the solution set.
2 Sevenbar Mechanisms

An assembly problem in mechanical design may be formulated as follows: given pieces (joints and links) and desired postures of the mechanism, find an assembly that realizes the desired postures. The formulation of design problems like these as polynomial systems is described in [5, 6]; see also [4]. In Figure 2 we the pieces of a sevenbar mechanism, assembled in Figure 2 once as an isolated solution (a mechanism that does not move), and once as a solution curve (a mechanism that moves).

Figure 2: Seven pieces assembled into a sevenbar mechanism.

To formulate the problem with polynomials, points are represented a complex numbers and a rotation with angle $\theta$ is performed multiplying with the complex number $e^{i\theta}$, $i = \sqrt{-1}$. Closure equations express that the vectors along a path in the linkage sum up to zero. In addition to the closure equations, we have $\Theta \overline{\Theta} = 1$, where $\overline{c}$ represents the complex conjugate of the complex number $c$.

A 7-bar mechanism which permits motion gives rise to the following polynomial system:

$$f(t, T) =
\begin{cases}
t_1T_1 - 1 = 0 \\
t_2T_2 - 1 = 0 \\
t_3T_3 - 1 = 0 \\
t_4T_4 - 1 = 0 \\
t_5T_5 - 1 = 0 \\
t_6T_6 - 1 = 0 \\
0.71035834160605t_1 + 0.46t_2 - 0.41t_3 + 0.24076130055512 + 1.07248215701824i = 0 \\
(-0.11 + 0.49i)t_2 + 0.41t_3 - 0.50219518117959t_4 + 0.41t_5 = 0 \\
0.50219518117959t_4 + (-0.09804347826087 + 0.43673913043478i)t_5 \\
-0.7751855666366T_6 - 1.2 = 0 \\
0.71035834160605T_1 + 0.46T_2 - 0.41T_3 + 0.24076130055512 - 1.07248215701824i = 0 \\
(-0.11 - 0.49i)T_2 + 0.41T_3 - 0.50219518117959T_4 + 0.41T_5 = 0 \\
0.50219518117959T_4 + (-0.09804347826087 - 0.43673913043478i)T_5 \\
-0.7751855666366T_6 - 1.2 = 0
\end{cases}
$$

where $t = (t_1, t_2, \ldots, t_6)$ and $T = (T_1, T_2, \ldots, T_6)$. The solutions to this system are a curve of degree six and six isolated solutions. One isolated solution is represented in Figure 2 along with a moving platform.
3 A Cascade of Homotopies

To deal locally with overdetermined nonlinear systems we can use the Gauss-Newton method. But if we want to determine the degree of a planar curve, given to us by a system of two equations, then we must be able to deal with the extended system globally, i.e.: we must know all solutions to an overdetermined polynomial system. For example, to solve \( E(f)(x) = 0 \), we use \( E_1(f)(x, z_1) = 0 \):

\[
E(f)(x) = \begin{cases}
  f_1(x_1, x_2) = 0 \\
  f_2(x_1, x_2) = 0 \\
  c_0 + c_1 x_1 + c_2 x_2 = 0
\end{cases}
\]

\[
E_1(f)(x, z_1) = \begin{cases}
  f_1(x_1, x_2) + b_{11} z_1 = 0 \\
  f_2(x_1, x_2) + b_{21} z_1 = 0 \\
  c_0 + c_1 x_1 + c_2 x_2 + z_1 = 0
\end{cases}
\]

In the embedded system \( E_1(f)(x, z_1) = 0 \), the extra variable \( z_1 \) is a slack variable and the coefficients \( b_{11} \) and \( b_{21} \) are random complex numbers. In case \( f(x) = 0 \) is over- or under-determined:

\[
\begin{cases}
  f_1(x_1, x_2) + b_{10} z_0 + b_{11} z_1 = 0 \\
  f_2(x_1, x_2) + b_{20} z_0 + b_{21} z_1 = 0 \\
  f_3(x_1, x_2) + b_{30} z_0 + b_{31} z_1 = 0 \\
  c_0 + c_1 x_1 + c_2 x_2 + z_1 = 0
\end{cases}
\]

The embedded system has always as many equations as unknowns. In the embedding \( E_i \), the number \( i \) of slack variables equals the dimension \( i \) of a solution set.

The polynomial system

\[
f(x) = \begin{cases}
  (x_1^2 - x_2)(x_1 - 0.5) = 0 \\
  (x_3^3 - x_2)(x_2 - 0.5) = 0 \\
  (x_1 x_2 - x_3)(x_3 - 0.5) = 0
\end{cases}
\]

has a one dimensional solution set, i.e.: the twisted cubic, and four isolated points. To compute numerical representations of the twisted cubic and the four isolated points, as given by the solution set of the system (5), we use the following homotopy:

\[
H(x, z_1, t) = \begin{bmatrix}
  (x_1^2 - x_2)(x_1 - 0.5) \\
  (x_3^3 - x_2)(x_2 - 0.5) \\
  (x_1 x_2 - x_3)(x_3 - 0.5)
\end{bmatrix}
+ t \begin{bmatrix}
  \gamma_1 \\
  \gamma_2 \\
  \gamma_3
\end{bmatrix}
\begin{bmatrix}
  z_1 \\
  z_1 \\
  z_1
\end{bmatrix}
= 0.
\]

At \( t = 1 \): \( H(x, z_1, t) = E_1(f)(x, z_1) = 0 \). At \( t = 0 \): \( H(x, z_1, t) = f(x) = 0 \). As \( t \) goes from 1 to 0, the hyperplane is removed from the embedded system, and \( z_1 \) is forced to zero. Figure 4 below summarizes...
the number of solution paths traced in the cascade of homotopies. The general algorithm is summarized in Algorithm 3.1.

Figure 4: Summary of a superwitness set cascade, starting with 13 paths of the embedded system, the cascade produces three witness points for the cubic and 9 points which may be isolated or on lie on the cubic.

**Theorem 3.1 (superwitness set generation [2])** For an embedding $\mathcal{E}_i(f)(x,z)$ of $f(x) = 0$ with $i$ random hyperplanes and $i$ slack variables $z = (z_1, z_2, \ldots, z_i)$, we have (1) solutions with $z = 0$ contain $\deg W$ generic points on every $i$-dimensional component $W$ of $f(x) = 0$; (2) solutions with $z \neq 0$ are regular; and (3) the solution paths defined by the cascading homotopy starting at $t = 0$ with all solutions with $z_i \neq 0$ reach at $t = 1$ all isolated solutions of $\mathcal{E}_{i-1}(f)(x,z) = 0$.

Theorem 3.1 leads to Algorithm 3.1. If $d$ is the top dimension, then $\mathcal{E}_d(f)(x,z) = 0$ has only isolated solutions. Usually, in many applications, one has some idea about what the top dimension $d$ could be. Otherwise, the default value for $d$ is $n - 1$, where $n$ equals the number of variables.

**Algorithm 3.1** SuperWitnessCascade($f,d$)

Input: $f(x) = 0$ a polynomial system;
$d$ the top dimension of $f^{-1}(0)$.
Output: $\hat{W} = [\hat{W}_d, \hat{W}_{d-1}, \ldots, \hat{W}_0]$ super witness sets for all dimensions.

$V := \text{Solve}(\mathcal{E}_d(f)(x,z) = 0)$;
for $k$ from $d$ down to 1 do
$\hat{W}_k := \{ (x,z) \in V \mid z = 0 \};$
$V := \{ (x,z) \in V \mid z_k \neq 0 \};$
if $V = \emptyset$ then
return $\hat{W}$;
else
$h(x,z,t) := (1 - t)\mathcal{E}_k(f)(x,z) + t \left( \frac{\mathcal{E}_{k-1}(f)(x,z)}{z_k} \right)$;
$V := \{ (x,z) \mid h(x,z,1) = 0 \};$
end if;
end for;
$\hat{W}_0 := \{ (x,z) \in V \mid z = 0 \}$.

The first stage in Algorithm 3.1 is often the most expensive stage, as the number of paths in the algorithm thereafter only decreases. Geometrically, the algorithm peels off in each step one hyperplane from the embedding.
4 Numerical Elimination Methods

Path tracking algorithms provide an implementation for Algorithm 4.1 to sample points from a solution set.

Algorithm 4.1 SampleSet($W_L, K$)

Input: $W_L$ is witness set for $k$ hyperplanes $L$;
$K$ is a new set of $k$ hyperplanes.
Output: $W_K$ is witness set for hyperplanes $K$.

By moving the new planes in special position, we arrive at numerical elimination methods. Suppose the system $f(x, y) = 0$, with $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_k)$ defines a $k$-dimensional solution set. Restricting the $k$ hyperplanes in the embedding $E_k(f)$ to have only nonzero coefficients with the $y$-variables, we can eliminate $x$ from the solution set and via interpolation construct defining equations for the projection of the solution set onto the $y$-variables.

Consider for example the twisted cubic. The twisted cubic is a curve in three space defined by the intersection of a quadratic and a cubic surface: $y = x^2$ and $z = x^3$, respectively. These two surfaces are the projections of the twisted cubic on the respective $(x, y)$ and $(x, z)$-planes. We can realize these projections by restricting the slicing hyperplanes appropriately. Consider the following three systems:

\[
\begin{align*}
\{ y - x^2 &= 0 \\
 z - x^3 &= 0 \\
 c_0 + c_1 x + c_2 y + c_3 z &= 0
\}
\end{align*}
\]

Substituting $y$ by $x^2$ and $z$ by $x^3$ in the last equation of the first system, we obtain a cubic in one single variable $x$, defining three generic points on the twisted cubic. Similarly, for the second system, we find only two solutions. Dropping the $z$ from the samples, i.e. $(x, y, z) \mapsto (x, y)$, we sample from $y - x^2 = 0$. The last equation in the third system defines a plane parallel to the $(x, y)$-plane. Applying $(x, y, z) \mapsto (x, z)$ to the sampled points executes the projection of the twisted cubic on $z - x^3 = 0$. With multivariate interpolation through the projected samples we eliminate in this way the variables $z$ or $y$ from the system.

5 A Membership Test

Algorithm 3.1 returns super witness sets: except for the top dimension, each witness set may contain points on higher dimensional solution sets. To obtain the true witness sets, we must filter out those junk points. Algorithm 5.1 decides whether a point does belong to a witness set or not, using a homotopy. The idea is illustrated in Figure 5.

Algorithm 5.1 HomotopyMembershipTest($W_L, y$)

Input: $W_L$ is witness set for a solution set;
$y$ is any point in space.
Output: yes or no, depending whether $y$ belongs to the set.

\[
h(x, t) = (1 - t) \begin{pmatrix} f(x) = 0 \\ L(x) = 0 \end{pmatrix} + t \begin{pmatrix} f(x) = 0 \\ L(x) = L(y) \end{pmatrix} = 0;
\]

\[
V := \{ x \mid h(x, 1) = 0 \};
\]
return $y \in V$.

Solution paths start at $t = 0$ at the witness points in $W_L$ and end at $t = 1$ at the solutions of a new witness set with hyperplanes passing through the point $y$. 
Figure 5: The curve \( V \) is represented by three witness points on \( L \). To decide whether \( y \in V \), we create a new witness set for a line \( L_y \) through \( y \). As \( y \notin V \cap L_y \), we conclude \( y \notin V \).

6 A Refined Version of Bézout’s Theorem

Observe that the linear equations added to \( f(x) = 0 \) in the cascade of homotopies do not increase the total degree of the system. As the total number of solution paths in the cascade we start with does not exceed the total degree, and as solution paths which land on higher dimensional solution sets terminate, we gain some intuition for the following refined version of Bézout’s theorem.

Theorem 6.1 (refined version of Bézout’s theorem) For a system \( f(x) = 0 \) of \( N \) polynomials \( f = (f_1, f_2, \ldots, f_N) \) in \( n \) unknowns \( x = (x_1, x_2, \ldots, x_n) \), the total degree \( D \),

\[
D = \prod_{i=1}^{N} \deg(f_i) \geq \sum_{j=0}^{n} \mu_j \deg(W_j),
\]

(8)

bounds the degree of all \( j \)-dimensional solution sets \( W_j \), each properly counted with their multiplicity \( \mu_j \).

Note: the case \( j = 0 \) gives the “classical” theorem of Bézout.

In [1], Bertini’s theorem is stated as “The generic element of a linear system is smooth away from the base locus of the system.” We formulate this theorem below.

Theorem 6.2 (Bertini’s Theorem) Let \( f = (f_1, f_2, \ldots, f_N) \) be a tuple of \( N \) polynomials representing a collection of \( N \) hypersurfaces \( f_i^{-1}(0) \) in \( \mathbb{C}^n \), for \( i = 1, 2, \ldots, N \). Consider

\[
g = \lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_f N, \quad \lambda_i \in \mathbb{C}, i = 1, 2, \ldots, N.
\]

(9)

Then, for generic choices of \( \lambda_i \): \( \frac{\partial g}{\partial x_j}(z) \neq 0 \), for all \( z \notin \bigcap_{i=1}^{N} f_i^{-1}(0) \).

In [1], the combination (9) is called a linear system and the intersection of all hypersurfaces is the base locus. We apply this theorem when we construct an embedding of a given system, taking the given polynomials and the added linear equations in the embedding in the linear system (9).

Sketch of Proof of Bertini’s theorem (from [1]). It suffices to show the theorem for two hypersurfaces: \( p \) and \( q \) and consider \( p(x) + \lambda q(x) = 0 \). Let \( z \) be a singular point outside the base locus, in particular: \( q(z) \neq 0 \). We must show that singular points can only happen for finitely many values of \( \lambda \). We then have that \( z \) satisfies the system

\[
\begin{cases}
p(x) + \lambda q(x) = 0 \\
\frac{\partial p}{\partial x_i} + \lambda \frac{\partial q}{\partial x_i} = 0, i = 1, 2, \ldots, n,
\end{cases}
\]

(10)

which defines an algebraic set \( V \subset \mathbb{C}^n \times \mathbb{C} \).
At \( z \) we have \( \lambda = -\frac{p(z)}{q(z)} \) and therefore: \( \frac{\partial}{\partial x_i} \left( \frac{p(z)}{q(z)} \right) = \frac{\partial p}{\partial x_i} - \frac{p \partial q}{q \partial x_i} = 0 \), for \( i = 1, 2, \ldots, n \). Consider

\[
\frac{\partial}{\partial x_i} \left( \frac{p}{q} \right) = \frac{\partial p}{\partial x_i} - \frac{p \partial q}{q \partial x_i} = 0.
\]  

At \( z \): \( \frac{\partial}{\partial x_i} \left( \frac{p}{q} \right) = 0 \). So at singular points, \( \frac{p}{q} \) is constant. But singular points belong to the algebraic set \( V \) and \( p/q \) can only be constant over finitely many points.

\[\Box\]

### 7 Exercises

1. Consider the system

\[
f(x_1, x_2, x_3) = \begin{cases} 
x_1^2 + x_2^2 - 1 = 0 \\
x_2^2 + x_3^2 - 1 = 0 \\
c_0 + c_1 x_1 + c_2 x_2 + c_3 x_3 = 0 
\end{cases}
\]  

where the coefficients \( c_0, c_1, c_2, \) and \( c_3 \) are randomly chosen complex numbers.

(a) Describe geometrically the solution set of this polynomial system, considering the last equation as a moving plane to sweep the curve defined by the intersection of the first two equations. Use Maple or Sage to illustrate the geometry. Can you see the degree of the curve defined by the first two equations?

(b) Explain what happens when \( c_3 = 0 \). Give a geometric interpretation of this special choice of hyperplane. Likewise, show that setting \( c_2 = 0 \) corresponds to projecting the solution set onto the \((x_1, x_3)\)-plane.

2. Solve the system in (3) as follows. Use \texttt{phc -c} (option #1) to construct \( \mathcal{E}(f) \), solve \( \mathcal{E}(f) = 0 \) with \texttt{phc -b}, and then call \texttt{phc -c} again to run the cascade. Check the output to verify whether a witness set for the curve has six points and check the size of the witness superset \( \hat{W}_0 \). Count how many paths have been tracked.

3. Consider (from [4, Exercise 13.2]) the systems

\[
f(x, y, z) = \begin{cases} 
y - x^2 = 0 \\
z - x^3 = 0 
\end{cases}
\quad \text{and} \quad g(x, y, z) = \begin{cases} 
xy - z^2 = 0 \\
xz - y^2 = 0.
\end{cases}
\]

(a) Construct witness sets for both \( f^{-1}(0) \) and \( g^{-1}(0) \).

(b) Take a generic point from \( f^{-1}(0) \) and test whether it belongs to \( g^{-1}(0) \) and vice versa.

(c) Do tests like these allow you to decide whether \( f^{-1}(0) \subseteq g^{-1}(0) \) or \( g^{-1}(0) \subseteq f^{-1}(0) \)? Explain.
References


