The classical way of viewing varieties is through the lense of commutative algebra, namely, the ideal-variety correspondence studied in Chapter 4. While this approach has its indisputable advantages, its main deficiency is the reliance on Gröbner bases techniques for computation: the worst case complexity of Buchberger-type algorithms is doubly exponential in the number of variables and Gröbner bases are not suited well for approximate computation.

What this chapter introduces is a relatively novel approach of the *numerical algebraic geometry*, which uses numerical polynomial homotopy continuation of Chapter 2 as its main computational engine. Unlike Gröbner bases algorithms, algorithms for homotopy continuation are numerical in their essence (they may use appoximate computations) and also allow for straightforward parallelization.

5.1. Witness sets

Recall two properties of an irreducible variety $V \subset \mathbb{C}^n$ of dimension m:

- There is a local regular sequence $F \subset R = \mathbb{C}[x_1, \ldots, x_n]$ with respect to V. (See Algorithm 4.2.1.) In particular, $|F| = n - m$ and V is an irreducible component of $\mathbb{V}(F)$.
- Every generic $(n-m)$-plane L intersects V in finitely many (but not zero) points. (See Remark 4.2.4.)

5.1.1. Definition. Let $F \subseteq R$ be a system of $n-m$ polynomials and $V_1, \ldots, V_r$ be irreducible components of $\mathbb{V}(F)$ of dimension m. Note that F is a local regular sequence with respect to every component V_i. The union $V = V_1 \cup \cdots \cup V_r$ is an *equidimensional variety*, i.e., a variety whose irreducible components have the same dimension.

A *witness set* w representing an equidimensional variety V of dimension m is a triple $w = [F, L, W]$ where

(1) $F \subseteq R = \mathbb{C}[x_1, \ldots, x_n]$ is a polynomial system that is a local regular sequence with respect to every irreducible component of V;
(2) L is a generic $(n-m)$-plane, a so-called *slicing plane*;
(3) $W = V \cap L \subseteq \mathbb{V}(F) \cap L$, a finite set of points referred to as *witness points*.

We denote the variety repsesented by a witness set w by $\mathbb{V}(w)$. A witness set w is an *irreducible witness set* if $\mathbb{V}(w)$ is irreducible.

Example 5.1.1. *The variety*

$$\mathbb{V}\begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \mathbb{V}\begin{pmatrix} (x^2+y^2+z^2-4)(y-x^2)(y+x^2) \\ (x^2+y^2+z^2-4)(y-1)z \\ (x^2+y^2+z^2-4)(z-1)z \end{pmatrix} \subseteq \mathbb{C}^3$$

breaks into the following irreducible components:

dim=2: *the sphere* $V_\circ = \mathbb{V}\big(x^2+y^2+z^2-4\big)$ *(corresponding to the common factor present in all defining polynomials);*

dim=1: *two parabolas* $V_\cup = \mathbb{V}\big(y-x^2, z\big)$ *and* $V_\cap = \mathbb{V}\big(y+x^2, z\big)$ *in* (x, y) *coordinate plane (corresponding to the case when* $x^2+y^2+z^2-4 \neq 0$*, but* $z = 0$*);*

dim=0: *four points* $V_1, \ldots, V_4$ *that are irreducible components of*

$$\mathbb{V}\big((y-x^2)(y+x^2), y-1, z-1\big)$$

(corresponding to the case $x^2+y^2+z^2-4\neq 0$ and $z\neq 0$), namely,

$$V_1=\{(1,1,1)\},\ V_2=\{(-1,1,1)\},\ V_3=\{(\boldsymbol{i},1,1)\},\ \text{and } V_4=\{(-\boldsymbol{i},1,1)\}.$$

To represent $V_\circ$ with a witness set we need a generic line (1-plane): let us take $L_\circ=\mathbb{V}(x-z-1,y-z-2)$. The two points of the intersection $V_\circ\cap L_\circ$ are

$$(z+1,z+2,z),\ \text{where } z=-1\pm\sqrt{\frac{2}{3}}.$$

Now $\mathbb{V}(w_\circ)=V_\circ$ for a witness set

$$w_\circ=\left[(f_1),L_\circ,\left\{(z+1,z+2,z)\,|\,z=-1\pm\sqrt{\frac{2}{3}}\right\}\right].$$

Note that there is a lot of freedom in constructing a witness set $w_\circ$: for intance, we can

- *replace f_1 with f_2 or f_3;*
- *choose any other generic line instead of $L_\circ$ above.*

We can represent the equidimensional variety $V_\cup\cup V_\cap$ with one witness set: take the 2-plane $L_{\cup\cap}=\mathbb{V}(y+z-4)$ and construct

$$w_{\cup\cap}=[(f_1,f_2),L_{\cup\cap},\{(2,4,0),(-2,4,0),(2\boldsymbol{i},4,0),(-2\boldsymbol{i},4,0)\}].$$

Again, there is a lot of freedom of choice here: for example, f_2 can be replaced with f_3 since (f_1,f_3) is also a regular sequence with respect to both $V_\cup$ and $V_\cap$.

Now, to represent one of the irreducible components – $V_\cup$, for instance – we need to make only a small change in $w_{\cup\cap}$: namely, keep only the witness points that belong to $V_\cup$, i.e.,

$$w_\cup=[(f_1,f_2),L_{\cup\cap},\{(2,4,0),(-2,4,0)\}].$$

To represent the equidimensional variety $V_1\cup V_2\cup V_3\cup V_4$ we need a 3-plane: the only 3-plane is the whole space $\mathbb{C}^3$ making a witness set

$$w_{1234}=\left[(f_1,f_2,f_3),\mathbb{C}^3,\{(1,1,1),(-1,1,1),(\boldsymbol{i},1,1),(-\boldsymbol{i},1,1)\}\right].$$

EXERCISE 5.1.2. *For the varieties $V_\circ$ and $V_\cup$ of Example 5.1.1 construct witness sets corresponding to alternative choices of slicing planes $L_\circ=\mathbb{V}(x+y+z-3,x-y+2z-5)$ and $L_\cup=\mathbb{V}(x-y+2z-5)$.*

EXERCISE 5.1.3. *Show that for a hypersurface $V=\mathbb{V}(f)$ the number of witness points (for any generic slicing line) equals $d=\deg f$. (Hint: Eliminate all variables but one.)*

5.1.2. Numerical construction. Let $F=(f_1,\dots,f_c)$ be a polynomial system that defines an equidimensional variety $V=\mathbb{V}(F)\subseteq\mathbb{C}^n$ of codimension c. Then we already have the first ingredient for a witness set: F is a locally regular sequence with respect to the irreducible components of V. For the second ingredient take a generic c-plane $L=\mathbb{V}(\ell_1,\cdots,\ell_m)$, where $m=n-c=\dim V$ and ℓ_i are linear independent linear functions. The third (missing) ingredient is $V\cap L$.

To compute points in $V \cap L$ one needs to solve the square polynomial system $(f_1, \ldots, f_c, \ell_1, \cdots, \ell_m)$. To that end we can apply Theorem 2.1.5; in fact, we can fix the linear equations defining the slicing plane in the homotopy:

$$H_t = \begin{pmatrix} (1-t)G + \gamma t F \\ \ell_1 \\ \vdots \\ \ell_m \end{pmatrix}, \quad t \in [0,1],$$

where $G = (g_1, \ldots, g_c)$ are the first c polynomials in the total-degree start system and $\gamma \in \mathbb{C}$ is generic.

This is the driving idea behind respresenting varieties with witness sets, since for their construction we can rely exclusively on numerical polynomial homotopy continuation algorithms. Since we intend to use witness sets as a practical data structure, instead of the witness points their numerical approximations are stored.

5.1.3. Equivalence of witness sets. Two witness sets $[F, L, W]$ and $[F, L', W']$ are *equivalent* if $|W| = |W'|$ and for the homotopy

$$H_t^{[F, L \to L', \gamma]} = \begin{pmatrix} F \\ (1-t)\ell_1 + \gamma t \ell_1' \\ \vdots \\ (1-t)\ell_m + \gamma t \ell_m' \end{pmatrix}, \quad t \in [0,1], \tag{5.1.1}$$

with $\gamma \in \mathbb{C}$ generic there are $d = |W| = |W'|$ homotopy paths that

- do not intersect,
- start with witness points W at $t = 0$, and
- end with the witness points W' at $t = 1$.

Equivalent witness sets represent the same (equidimensional) variety.

We define the *degree* of an equidimensional variety V to be the number of witness points d in any witness set that represents V. Geometrically, the degree of V is a typical number of points one obtains intersecting V with a random $(\operatorname{codim} V)$-plane.

Note: We make no assumption that the starting points W in the homotopy $H_t^{[F, L \to L', \gamma]}$ in (5.1.1) are regular.

However, due to genericity of the slicing planes L and L', the points on the homotopy paths starting at W all have "similar singularity structure". This enables the deflation technique of §2.2.2 to regularize all points on the paths uniformly making it possible to track $H_t^{[F, L \to L', \gamma]}$ with a numerical algorithm.

5.1.4. Sampling and the membership test. Given a witness set

$$w = [F, L, W]$$

representing a positive-dimensional variety, one can sample infinitely many points on $\mathbb{V}(w)$ repeatedly picking a random slicing plane L' in (5.1.1) and tracking the resulting homotopy to get new points $\mathbb{V}(w) \cap L'$.

On the other hand, given a point $p \in \mathbb{C}^n$ one can perform a *membership test*, i.e., determine whether $p \in \mathbb{V}(w)$. To test membership,

- pick a random slicing plane L' that contains the point p;

- track the homotopy $H_t^{[F,L\to L',\gamma]}$ in (5.1.1) for a random $\gamma \in \mathbb{C}$ to get points $W' = \mathbb{V}(w) \cap L'$;
- $p \in \mathbb{V}(w)$ iff $p \in W'$.

Note that $[F, L', W']$ may not form a witness set; nevertheless, W' is a finite set with $|W'| \leq |W| = \deg \mathbb{V}(w)$ for a generic choice L' passing through p.

EXERCISE 5.1.4. *For the varieties $V_\circ$ and $V_\cup$ in Example 5.1.1*

- *determine their degrees;*
- *show that the slicing line $L_\circ = \mathbb{V}(y, z-2)$ does not produce a witness set for $V_\circ$;*
- *give an example of an exceptional slicing plane $L_\cup$, one that can not be a part of a witness set representing $V_\cup$.*

REMARK 5.1.5. *The membership test can be used to perform determine containment (with probability 1): for a witness set $\widetilde{w} = \left[\widetilde{F}, \widetilde{L}, \widetilde{W}\right]$ the variety $\mathbb{V}(\widetilde{w}) \subseteq \mathbb{V}(w)$ iff $\widetilde{W} \subseteq \mathbb{V}(w)$.*

5.2. Numerical irreducible decomposition

In this section we discuss the following problem:

> Given a witness set
> $$w = [F, L, W]$$
> representing an equidimensional variety, how does one obtain the partition of the witness points
> $$W = W_1 \sqcup \cdots \sqcup W_r$$
> such that $V_i = \mathbb{V}([F, L, W_i])$, $i = 1, \ldots, r$, are the irreducible components of $V = \mathbb{V}(w)$?

For instance, for the witness set $w_{\cup\cap}$ in Example 5.1.1 we would like to have an algorithmic way to produce $w_\cup$ and $w_\cap$ using only the data of $w_{\cup\cap}$.

5.2.1. Irreducible witness sets. Let us assume that we have the required partition
$$W = W_1 \sqcup \cdots \sqcup W_r.$$
Pick a generic slicing plane L' and consider homotopy paths starting at the points of W_i traced out by $H_t^{[F,L\to L',\gamma]}$ in (5.1.1). Due to genericity of L,L', and γ, all points on the paths are generic: in particular, they do not belong to intersections $V_i \cap V_j$, $i \neq j$, of the irreducible components. We conclude that the set of endpoints W_i' is contained in the same component V_i and, therefore, gives another (equivalent to $[F, L, W_i]$) witness set $[F, L, W_i']$ for V_i.

Now consider a map $\phi_{L',\gamma,\gamma'} : W \to W$ which maps a witness point $p \in W$ to the result of tracking of two homotopy paths:

- the path of $H_t^{[F,L\to L',\gamma]}$ starting at p and ending at some point $q \in W'$,
- then the path of $H_t^{[F,L'\to L,\gamma']}$ starting at q and ending at some point $\phi(p) \in W$.

Assuming that all ingredients (L, L', γ, γ') are generic, the map $\phi_{L',\gamma,\gamma'}$

- is a permutation of W,
- restricts to a permutation of each W_i (according to our discussion above).

PROPOSITION 5.2.1. *Using the setting of this section, restrict to W_i, the witness points corresponding to an irreducible component V_i of V.*

Then the group generated by permutations $\phi_{L',\gamma,\gamma'}|_{W_i} : W_i \to W_i$, where L', γ, γ' are generic, acts transitively on W_i.

In other words, for every pair of points points $p, q \in W_i$, there exists $L_i', \gamma_i, \gamma_i'$, $i = 1, \ldots, r$, such that
$$\left(\phi_{L_r',\gamma_r,\gamma_r'} \circ \cdots \circ \phi_{L_1',\gamma_1,\gamma_1'}\right)(p) = q,$$
i.e., there is a finite number of "moves", whose composition maps p to q.

PROOF. add a reference □

5.2.2. Monodromy breakup algorithm. The modern numerical algebraic geometry software often uses the following probabilistic algorithm, Algorithm 5.2.1, for *numerical irreducible decomposition* of an equidimensional variety.

The only missing ingredient in this algorithm is a stopping criterion. We postpone the proof of correctness until the end of the next section.

Algorithm 5.2.1 $P = \textsc{MonodromyBreakup}(F, L, W)$

Require: $[F, L, W]$, a witeness set representing an equidimensional variety of dimension m:

- $F = (f_1, \dots, f_{n-m})$, a polynomial system in $R = \mathbb{C}[x_1, \dots, x_n]$;
- $L = \mathbb{V}(\ell_1, \dots, \ell_m)$, an $(n-m)$-plane given by a system of linearly independent linear functions;
- $W \subseteq \mathbb{C}^n$, a finite number of points.

Ensure: $P = \{W_1, \dots, W_r\}$ is a partition of the set of witness points W according to the irreducible decomposition of $\mathbb{V}([F, L, W])$.

$P \leftarrow \{\, \{p\} \mid p \in W \,\}$ --
initialize P with the partition into singletons
while a stopping criterion is not satisfied **do**
Pick randomly

- linear functions ℓ_i' to get an $(n-m)$-plane $L' = \mathbb{V}(\ell_1', \dots, \ell_m')$;
- constants $\gamma, \gamma' \in \mathbb{C}$.

$\phi \leftarrow \phi_{L',\gamma,\gamma'}$
In the partition P merge parts $A \subseteq W$ and $B \subseteq W$ if there exists a pair of points $p \in A$ and $q \in B$ such that $\phi(p) = \phi(q)$.
end while

5.2.3. Linear trace test. Here we describe an idea of a stopping criterion for Algorithm 5.2.1 in the case of a curve in a plane (1-equidimensional variety in $\mathbb{C}^2$), however the approach generalizes to varieties of arbitrary dimension and codimension.

A curve V in a plane has $\dim V = \operatorname{codim} V = 1$ and can be represented by a witness set $w = [\{f\}, \mathbb{V}(\ell), W]$, i.e., with

(1) one polynomial $f \in \mathbb{C}[x, y]$,
(2) one linear function $\ell \in \mathbb{C}[x, y]$, and
(3) a finite set of witness points $W = \mathbb{V}(f) \cap \mathbb{V}(\ell) \subseteq \mathbb{C}^2$.

Moreover, after a linear change of coordinates, we may assume that

- the monomial x^d, where $d = \deg f$, occurs in f with coefficient 1 and
- the slicing line $L = \mathbb{V}(\ell)$ is the x-axis, i.e., $\ell = y$.

Consider the family of lines parallel to L defined by

$$\ell_t = y - t, \quad t \in \mathbb{C}$$

and the witness sets obtained by deforming W into $W_t \subseteq \mathbb{V}(f) \cap \mathbb{V}(\ell_t)$ as the parameter t changes. There may be finitely many values of t that go not give a generic line $\mathbb{V}(\ell_t)$, i.e., the intersection $V \cap \mathbb{V}(\ell_t)$ would be not typical: recall that typically $|V \cap \mathbb{V}(\ell_t)| = |W| = d$, where $d = \deg V = \deg f$.

Let $W_t = \{(x_1(t), t), \dots, (x_d(t), t)\}$, then $x_i(t)$ are the roots of the univariate polynomial

$$\begin{aligned} f(x,t) &= x^n + a_{n-1}(t)x^{n-1} + \cdots + a_1(t)x + a_0(t) \\ &= (x - x_1(t)) \cdots (x - x_d(t)) \\ &= x^d - \boxed{(x_1(t) + \cdots + x_d(t))} x^{d-1} + \cdots + (-1)^d (x_1 \cdots x_n) \end{aligned}$$

The *trace* $\operatorname{tr}(f)$ of a univariate monic polynomial f is defined to be the sum of its roots. In our case the $\lambda(t) = \operatorname{tr}(f(x,t)) = x_1(t) + \cdots + x_d(t) = -a_{n-1}$ is a linear function in t: indeed, we substituted the parameter t for y in the bivariate polynomial f of degree d, therefore, only terms with monomials x^{d-1} and tx^{d-1} contribute to the term $a_{n-1}(t)x^{n-1}$.

The idea of the *linear trace test* is to check the linearity of the trace numerically. In practice, it is enough to compute the trace $\lambda(t)$ for three distinct generic values of parameter t to conclude whether $\lambda(t)$ is linear.

PROPOSITION 5.2.2. *Consider a witness set $[F, L, W]$, $L = \mathbb{V}(\ell_1, \ldots, \ell_m)$, representing an m-equidimensional variety in $\mathbb{C}^n$ and a subset of witness points $W' \subseteq W$. Let $W'_t \subseteq W_t \subseteq \mathbb{V}(F) \cap L_t$, where*

$$L_t = \mathbb{V}(\ell_1 - t, \ldots, \ell_m - t), \quad t \in \mathbb{C},$$

be the points obtained by homotopy continuation along a homotopy that defines regular paths. (Note that W_t does not depend on the choice of homotopy; however, in order for W'_t to be well defined one needs to prescribe a particular homotopy for each t.)

Then $W' = W \cap V$ for some subvariety of $V \subseteq \mathbb{V}([F, L, W])$ iff

$$\lambda(t) = \sum_{p \in W'_t} p \ \in \ \mathbb{C}^n$$

is a linear function of t.

PROOF. add a reference □

Using this proposition we can design a stopping criterion for Algorithm 5.2.1: the algorithm should stop when all parts W' in the partition P pass the linear trace test, i.e., $\lambda(t)$ in Proposition 5.2.2 is linear.

PROOF OF CORRECTNESS OF ALGORITHM 5.2.1. (with a linear trace test as a stopping criterion)

Parts in the partition P are merged by the algorithm if points in distinct parts are discovered to be in the same irreducible component in accordance with Proposition 5.2.1. Since the algorithm starts with partitioning W into single-element sets, during the run of the algorithm it is always true that every part in the partition is contained in exactly one irreducible component.

The algorithm stops when each part in P is a "complete" set of witness points corresponding to a subvariety according to Proposition 5.2.2.

Putting these two observations together, we coclude that the parts of P represent an irreducible components when the algorithm terminates. □

EXERCISE 5.2.3. *For the ellipsoid $V = \mathbb{V}(x^2 + 2y^2 + 3z^2 - 5)$*

1. *find the points p_0 and q_0 of the intersection $V \cap L$, where $L = \mathbb{V}(y - x - 1, z - x)$;*
2. *find the points p_t and q_t of the intersection $V \cap L_t$, where $L = \mathbb{V}(y - x - 1 - t, z - x - t)$, where t is a parameter;*
3. *show that $p_t + q_t$ is a linear function in t, while p_t and q_t are not.*

5.3. Numerical variety

A *numerical variety* $\mathbf{w}$ is defined a finite collection of witness sets $\{w_1, \ldots, w_r\}$.

A numerical variety is viewed as a (non-unique) representation of the variety $\mathbb{V}(\mathbf{w}) = \mathbb{V}(w_1) \cup \cdots \cup \mathbb{V}(w_r)$. Note that we **do not** require

- witness sets w_i to be irreducible, although one can produce a numerical variety with irreducible witness sets by using the numerical irreducible decomposition;
- the collection $\mathbf{w}$ to be *irredundant*, i.e,

$$\mathbb{V}(w_i) \not\subseteq \mathbb{V}(w_j), \quad i \neq j,$$

  although one can easily use the containment test (see Remark 5.1.5) to discard the redundant parts.

In this section we explain the basic operations for numerical varieties and describe an algorithm for constructing a numerical variety representing $\mathbb{V}(F)$ where F is an arbitrary polynomial system.

5.3.1. Union and difference. While both taking a union and subtracting two varieties is a nontrivial operation using the ideal-variety correspondence, these two operations are simple in the numerical setting. Let $V = \mathbb{V}(\mathbf{w})$ and $\widetilde{V} = \mathbb{V}(\widetilde{\mathbf{w}})$.

Then the union is

$$V \cup \widetilde{V} = \mathbb{V}(\mathbf{w} \cup \widetilde{\mathbf{w}})$$

and the Zariski closure of the difference is

$$\overline{V \setminus \widetilde{V}} = \mathbb{V}\left\{ w \in \mathbf{w} \,|\, w \not\subseteq \mathbb{V}(\widetilde{w}) \text{ for all } \widetilde{w} \in \widetilde{\mathbf{w}} \right\}.$$

5.3.2. Intersection. On the other hand, the intersection is a simple operation when varieties are represented by ideals, but intersecting numerical varieties is a nontrivial task. Here we shall show only how to intersect a numerical variety with a hypersurface. In the general case intersection is an even more intricate operation.

Consider a numerical variety $\mathbf{w}$ and a polynomial $g \in R = \mathbb{C}[x_1, \ldots, x_n]$. Our goal is to construct a numerical variety $\mathbf{w}'$ such that

$$\mathbb{V}(\mathbf{w}') = \mathbb{V}(\mathbf{w}) \cap \mathbb{V}(g).$$

For a witness set $w = [F, L, W] \in \mathbf{w}$ the following scenarios and corresponding actions are possible:

(1) $\mathbb{V}(w) \cap \mathbb{V}(g) = \mathbb{V}(w)$, i.e., $\mathbb{V}(w) \subseteq \mathbb{V}(g)$ or, equivalently, g vanishes on all witness points W.
   Action: append w "as is" to $\mathbf{w}'$.

(2) $\mathbb{V}(w) \cap \mathbb{V}(g) \neq \mathbb{V}(w)$, but $\mathbb{V}(w) \cap \mathbb{V}(g) = \dim \mathbb{V}(w)$. That means g vanishes on a proper subset $W' \neq \emptyset$ of witness points W.
   Action: append $[F, L, W']$ to $\mathbf{w}'$; process the intersection of $\mathbb{V}([F, L, W \setminus W'])$ with $\mathbb{V}(g)$ separately.

(3) $\dim(\mathbb{V}(w) \cap \mathbb{V}(g)) < \dim(\mathbb{V}(w))$, which is the case when $W \cap \mathbb{V}(g) = \emptyset$. There are two subcases, both addressed by Algorithm 5.3.1:
   (a) $\dim(\mathbb{V}(w) \cap \mathbb{V}(g)) = \dim(\mathbb{V}(w)) - 1$.
      Action: append $[F \cup \{g\}, L', W']$ to $\mathbf{w}'$, where L' is a random plane of dimension $n - \dim(\mathbb{V}(w)) + 1$ and W' is constructed by Algorithm 5.3.1.

(b) $\mathbb{V}(w) \cap \mathbb{V}(g) = \emptyset$.
Action: discard.

Algorithm 5.3.1 *output* = HypersurfaceIntersection$([F, L, W], g, L')$

Require: $[F, L, W]$, a witeness set representing an equidimensional variety of dimension m:

- $F = (f_1, \ldots, f_{n-m})$, a polynomial system in $R = \mathbb{C}[x_1, \ldots, x_n]$;
- $L = \mathbb{V}(\ell_1, \ldots, \ell_m)$, an $(n-m)$-plane given by a system of linearly independent linear functions;
- $W \subseteq \mathbb{C}^n$, a finite number of points;

$g \in R$ such that $W' \cap \mathbb{V}(g) = \emptyset$;
$L' = \mathbb{V}\big(\ell'_1, \ldots, \ell'_{m-1}\big)$, a generic $(n-m+1)$-plane.
Ensure: *output* $= [F \cup \{g\}, L', W']$ such that

$$\mathbb{V}([F \cup \{g\}, L', W']) = \mathbb{V}(W set F, L, W) \cap \mathbb{V}(g)$$

or *output* $= \emptyset$ if $\mathbb{V}([F, L, W]) \cap \mathbb{V}(g) = \emptyset$.

$d \leftarrow \deg g$
for $i = 1$ to d **do**
  Pick a random linear function $\ell^{(i)}$.
  $L^{(i)} \leftarrow \big\{\ell^{(i)}, \ell'_1, \ldots, \ell'_{m-1}\big\}$
  Track the homotopy $H_t^{[F, L \to L', \gamma]}$

- starting with points W
- to get witness points $W^{(i)}$.

  -- Note that $\big[F, L^{(i)}, W^{(i)}\big]$ is a witness set equivalent to $[F, L, W]$.

end for
For a random $\gamma \in \mathbb{C}$, track the homotopy

$$H_t = \begin{pmatrix} F \\ (1-t)(\ell^{(1)}\ell^{(2)} \cdots \ell^{(d)}) + \gamma t g \\ \ell'_1 \\ \vdots \\ \ell'_{m-1} \end{pmatrix}, \quad t \in [0, 1], \tag{5.3.1}$$

starting with the points $W^{(1)} \cup \cdots \cup W^{(d)}$. Let W' be the set of points obtained as the result.
if $W = \emptyset$ **then**
  output $\leftarrow \emptyset$
else
  output $\leftarrow [F \cup \{g\}, L', W']$
end if

Note that the only part homotopy H_t in (5.3.1) that depends on t,

$$h_t = (1-t)(\ell^{(1)}\ell^{(2)} \cdots \ell^{(d)}) + \gamma t g,$$

evaluates to a constant multiple of g at $t = 1$ and

$$h_0 = \ell^{(1)}\ell^{(2)} \cdots \ell^{(d)}$$

at $t = 0$. While g is an arbitrary polynomial, h_0 factors into a product of linear functions; also, $\deg h_0 = \deg g$.

REMARK 5.3.1. *Going from $t = 1$ to $t = 0$ above is commonly referred to as* degeneration*: a general polynomial* degenerates *into a polynomial of the same "kind" (in this case, of the same degree), but with special properties (in this case, factors into a product of linear functions).*

Going in the opposite direction, from $t = 0$ to $t = 1$ can be called undegeneration *or* regeneration*.*

The special form of h_0 makes the problem simpler than that given by a general polynomial g. Indeed, intersecting $V = \mathbb{V}([F, L, W])$ with $\mathbb{V}(h_0)$ breaks into d smaller problems:

$$V \cap \mathbb{V}(h_0) = \left(V \cap \mathbb{V}\left(\ell^{(1)}\right)\right) \cup \cdots \cup \left(V \cap \mathbb{V}\left(\ell^{(d)}\right)\right).$$

Not only is each $\mathbb{V}\left(\ell^{(i)}\right)$ a hyperplane, but we also have a solution for this smaller problem,

$$V \cap \mathbb{V}\left(\ell^{(i)}\right) = \mathbb{V}\left(\left[F, L^{(i)}, W^{(i)}\right]\right),$$

which is precomputed in the initial steps of the algorithm.

PROOF OF CORRECTNESS OF ALGORITHM 5.3.1. The algorithm works assuming the genericity of all random ingredients, which we do not prove here. add a reference □

Note: One can readily modify the hypersurface intersection procedure to work for a hypersurface represented with a witness set, in particular, in the case when the hypersurface in question is a proper subset of $\mathbb{V}(g)$ (i.e., a union of some but not all irreducible components of $\mathbb{V}(g)$).

5.3.3. Constructing a numerical variety. One major, yet basic, question is: how to pass from a representation of variety $V = \mathbb{V}(F)$ with a polynomial system F to a representation with a witness set?

Algorithm 5.3.2 provides an answer using a cascade of intersections with hypersurfaces that summarizes the discussion of possible cases in §5.3.2 and uses Algorithm 5.3.1.

The numerical variety produced by Algorithm 5.3.2 depends not only on the random choices, but also notably on the order of polynomials in the input polynomial system.

EXERCISE 5.3.2. *Apply (ideas of) Algorithm 5.3.2 to the system of three polynomials in the Example 5.1.1 where polynomials are sorted in the following order $F = (f_3, f_1, f_2)$.*

Making suitable choices of random ingredients, compute **w**

(1) *at the step when $\mathbb{V}(\mathbf{w}) = \mathbb{V}(f_3)$,*
(2) *at the step when $\mathbb{V}(\mathbf{w}) = \mathbb{V}(f_3, f_1)$, and*
(3) *at the end of the algorithm,*

describing the transitions between these three points in the algorithm.

Algorithm 5.3.2 $\mathbf{w} = \text{NumericalVariety}(F)$

Require: $F = (f_1, \ldots, f_r)$, a polynomial system in $R = \mathbb{C}[x_1, \ldots, x_n]$.
Ensure: $\mathbf{w}$ is a numerical variety such that $\mathbb{V}(F) = \mathbb{V}(\mathbf{w})$.

Create a witness set w representing the hypersurface $\mathbb{V}(f_1)$ using the homotopy discussed in §5.1.2.
$\mathbf{w} \leftarrow w$
for $i = 2$ to r **do**
  $g \leftarrow f_i$
  $\mathbf{w}' \leftarrow \emptyset$
  while $\mathbf{w} \neq \emptyset$ **do**
    Pick $w = [F, L, W] \in \mathbf{w}$.
    $\mathbf{w} \leftarrow \mathbf{w} \setminus \{w\}$
    if $g(p) = 0$ for all $p \in W$ **then**
      $\mathbf{w}' \leftarrow \mathbf{w}' \cup \{w\}$
    else if $W' = \{\, p \in W \mid g(p) = 0 \,\} \neq \emptyset$, but $W' \neq W$ **then**
      $\mathbf{w} \leftarrow \mathbf{w} \cup \{[F, L, W'], [F, L, W \setminus W']\}$
    else if $g(p) \neq 0$ for all $p \in W$ **then**
      Pick a random $(n - \dim(\mathbb{V}(w)) + 1)$-plane L'.
      $w' \leftarrow \text{HypersurfaceIntersection}(w, g, L')$
      if $w' \neq \emptyset$ **then**
        $\mathbf{w}' \leftarrow \mathbf{w}' \cup \{w'\}$
      end if
    end if
  end while
  $\mathbf{w} \leftarrow \mathbf{w}'$
end for

5.4. Trilingual dictionary

Before giving the dictionary let us fill in the pieces of missing notation

- We denote by $\mathbb{W}(F)$ the output of Algorithm 5.3.2 given a polynomial system F as input: $\mathbb{W}(F)$ is a numerical variety representing the variety $\mathbb{V}(F)$.
- The *numerical intersection* operation $\cap_{\mathbb{W}}$ is discussed in §5.3.2: for numerical varieties $\mathbf{w}$ and $\widetilde{\mathbf{w}}$ it produces a numerical variety denoted $\mathbf{w} \cap_{\mathbb{W}} \widetilde{\mathbf{w}}$ such that
$$\mathbb{V}(\mathbf{w} \cap_{\mathbb{W}} \widetilde{\mathbf{w}}) = \mathbb{V}(\mathbf{w}) \cap \mathbb{V}(\widetilde{\mathbf{w}}).$$
- For a set of points $S \subset \mathbb{C}^n$, we denote by $\mathbb{I}(S)$ the radical ideal obtained by *interpolation* from the points sampled on the variety $V = \overline{S}$.

  Also, $\mathbb{I}(\mathbf{w})$ stands for the interpolating ideal for the set of points $S \subset \mathbb{V}(\mathbf{w})$ obtained by sampling each component of $\mathbb{V}(\mathbf{w})$ using the corresponding witness set of a numerical variety $\mathbf{w}$.

ALGEBRA	GEOMETRY	NUMERICAL ALGEBRAIC GEOMETRY
radical ideal	variety	numerical variety
$\mathbb{I}(V) = \mathbb{I}(\mathbf{w})$	V	$\mathbf{w}$ such that $V = \mathbb{V}(\mathbf{w}) = \bigcup_{w \in \mathbf{w}} \mathbb{V}(w)$
I (not necessarily radical)	$\mathbb{V}(I)$	$\mathbb{W}(F)$ for a finite generating set F of I
inclusion (checked by membership test)	reversed inclusion	inclusion/containment test
$I \subseteq J$	$\mathbb{V}(I) \supseteq \mathbb{V}(J)$	
$\mathbb{I}(V) \subseteq \mathbb{I}(V')$	$V \supseteq V'$	$\forall w' \in \mathbf{w}',\ \exists w \in \mathbf{w}$ such that $\mathbb{V}(w) \supseteq \mathbb{V}(w')$
addition of ideals	intersection of varieties	numerical intersection
$I + J$	$\mathbb{V}(I) \cap \mathbb{V}(J)$	
$\sqrt{\mathbb{I}(V) + \mathbb{I}(V')}$	$V \cap V'$	$\mathbf{w} \cap_{\mathbb{W}} \mathbf{w}' = \bigcup_{w \in \mathbf{w}, w' \in \mathbf{w}'} (w \cap_{\mathbb{W}} w')$
product or intersection of ideals	union of varieties	union of numerical varieties
IJ or $I \cap J$	$\mathbb{V}(I) \cup \mathbb{V}(J)$	
$\sqrt{\mathbb{I}(V)\mathbb{I}(V')}$ or $\mathbb{I}(V) \cap \mathbb{I}(V')$	$V \cup V'$	$\mathbf{w} \cup \mathbf{w}'$
quotient (saturation) of ideals	difference of varieties	difference of numerical varieties
$I : J^\infty$	$\overline{\mathbb{V}(I) \setminus \mathbb{V}(J)}$	
$\mathbb{I}(V) : \mathbb{I}(V')$	$\overline{V \setminus V'}$	$\{w \in \mathbf{w} \,\vert\, \mathbb{V}(w) \not\subset \mathbb{V}(w') \text{ for any } w' \in \mathbf{w}'\}$
elimination of variables	projection of varieties	interpolation from projected points
$\sqrt{I \cap k[x_{m+1}, \ldots, x_n]}$	$\overline{\pi_m(V(I))}$	$\mathbb{I}(\pi_m(S))$ where points S are sampled using $\mathbf{w}$
prime ideal	irreducible variety	irreducible witness set
maximal ideal	point of affine space	approximation of a point of affine space
ascending chain condition (for a chain of ideals)	descending chain condition (for a chain of varieties)	numerical variety is a finite collection of witness sets