Absolute Factorization

1. Linear Traces
   - factoring a polynomial in two variables
2. Adjacent Minors
   - an example from algebraic statistics
3. Changing Coordinates
   - avoiding wrong factorizations
4. Monodromy Actions
   - viewing an algebraic curve as a Riemann surface
5. Specializing, Lifting, and Projecting
   - Hilbert irreducibility theorem, Hensel lifting, Bertini

MCS 563 Lecture 28
Analytic Symbolic Computation
Jan Verschelde, 19 March 2014

Absolute Factorization

1. Linear Traces
   - factoring a polynomial in two variables
2. Adjacent Minors
   - an example from algebraic statistics
3. Changing Coordinates
   - avoiding wrong factorizations
4. Monodromy Actions
   - viewing an algebraic curve as a Riemann surface
5. Specializing, Lifting, and Projecting
   - Hilbert irreducibility theorem, Hensel lifting, Bertini

the linear trace

Consider $f \in \mathbb{C}[x, y]$, $\deg(f) = 3$. Does f factor?

Assume f has a quadratic factor q.

We view $f \in \mathbb{C}[x][y]$ and write q as

$$\begin{aligned} q(x, y(x)) &= (y - y_1(x))(y - y_2(x)) \\ &= y^2 - (y_1(x) + y_2(x))y + y_1(x)y_2(x). \end{aligned}$$

Observe: if q is a quadratic factor of f,
then $y_1(x) + y_2(x)$ must be a linear function of x,
otherwise the degree of q would be higher than two.

Denote $t_1(x) = y_1(x) + y_2(x)$ and call t_1 the linear trace.

interpolating the linear trace

Fix $x = x_1$ and solve $f(x_1, y) = 0$ for y.

As $\deg(f) = 3$, we find three roots and write them as as $(x_1, y_1(x^*))$, $(x_1, y_2(x^*))$, and $(x_1, y_3(x^*))$.

If f has a quadratic factor q, its linear trace t_1 is $t_1(x) = y_1(x) + y_2(x) = ax + b$, for some $a, b \in \mathbb{C}$.

Take $x_2 \neq x_1$ and consider

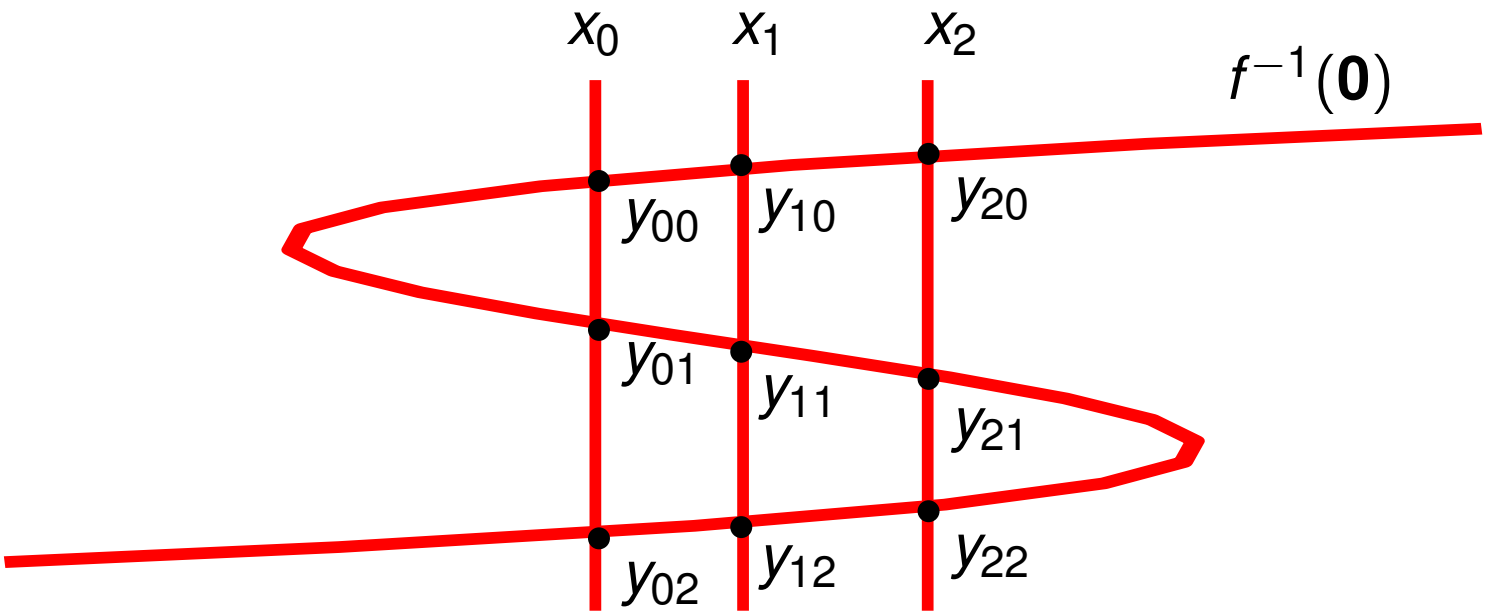
$$\begin{cases} ax_1 + b = y_1(x_1) + y_2(x_1) \\ ax_2 + b = y_1(x_2) + y_2(x_2) \end{cases}$$

Solving the linear system for a and b determines $t_1(x)$.

Take a third sample set, at $x = x_3$ and test

$$t(x_3) = ax_3 + b \stackrel{?}{=} y_1(x_3) + y_2(x_3).$$

an example



Use $\{(x_0, y_{00}), (x_0, y_{01}), (x_0, y_{02})\}$ and $\{(x_1, y_{10}), (x_1, y_{11}), (x_1, y_{12})\}$ to find $t_1(x) = c_0 + c_1 x$.
At $\{(x_2, y_{20}), (x_2, y_{21}), (x_2, y_{22})\}$: $c_0 + c_1 x_2 = y_{20} + y_{21} + y_{22}$?

combinatorial enumeration

A linear trace test answers each question:

```
Is 1 a factor?
 |- Yes: Is 2 a factor?
 |    |- Yes: 1,2,3 is the factorization
 |    |- No: 1,23 is the factorization
 |- No: Is 12 a factor?
      |- Yes: 12,3 is the factorization
      |- No: is 13 a factor?
           |- Yes: 13,2 is the factorization
           |- No: 123 is the factorization
```

This combinatorial enumeration works for low degrees, and is improved via LLL to solve the knapsack problem.

Absolute Factorization

1. Linear Traces
   - factoring a polynomial in two variables
2. Adjacent Minors
   - an example from algebraic statistics
3. Changing Coordinates
   - avoiding wrong factorizations
4. Monodromy Actions
   - viewing an algebraic curve as a Riemann surface
5. Specializing, Lifting, and Projecting
   - Hilbert irreducibility theorem, Hensel lifting, Bertini

adjacent minors

Consider the adjacent minors of a general 2×4-matrix:

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \end{bmatrix} \qquad f(\mathbf{x}) = \begin{cases} x_{11}x_{22} - x_{21}x_{12} = 0 \\ x_{12}x_{23} - x_{22}x_{13} = 0 \\ x_{13}x_{24} - x_{23}x_{14} = 0 \end{cases}$$

This family arises in algebraic statistics.

For a general $2 \times (n+1)$-matrix, the number of irreducible components equals the nth Fibonacci number
(e.g.: for $n = 4$, we find 5 irreducible factors).

Absolute Factorization

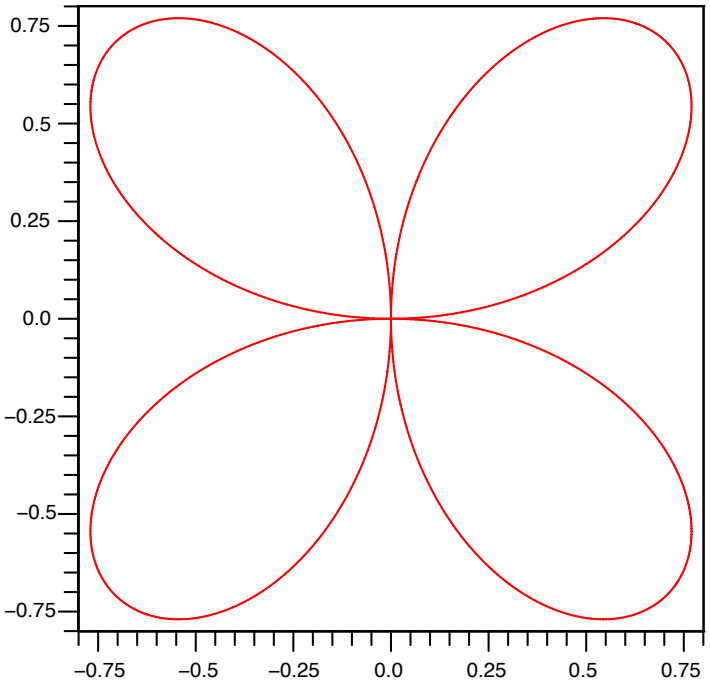
1. Linear Traces
   - factoring a polynomial in two variables
2. Adjacent Minors
   - an example from algebraic statistics
3. Changing Coordinates
   - avoiding wrong factorizations
4. Monodromy Actions
   - viewing an algebraic curve as a Riemann surface
5. Specializing, Lifting, and Projecting
   - Hilbert irreducibility theorem, Hensel lifting, Bertini

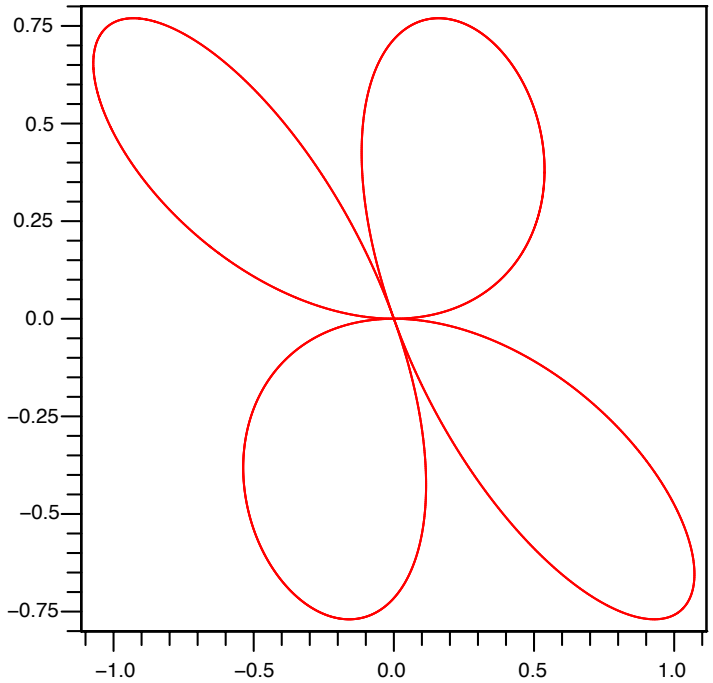
an example

Consider $f(x,y) = (x^2+y^2)^3 - 4x^2y^2 = 0$.

By symmetry: if $f(a,b) = 0$, then also $f(\pm a, \pm b) = 0$.

Pictures of $f(x,y) = 0$ and $f(x + \frac{1}{2}y, y) = 0$:





factoring witness sets

Consider $\begin{cases} f(x,y) = 0 \\ c_0 + c_1 x + c_2 y = 0 \end{cases}$ for random c_0, c_1, and c_2.

To sample points, we apply the coordinate transformation:

$$\phi : \mathbb{C}^2 \to \mathbb{C}^2 : \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \phi(x,y) = \begin{bmatrix} -c_1 & -c_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

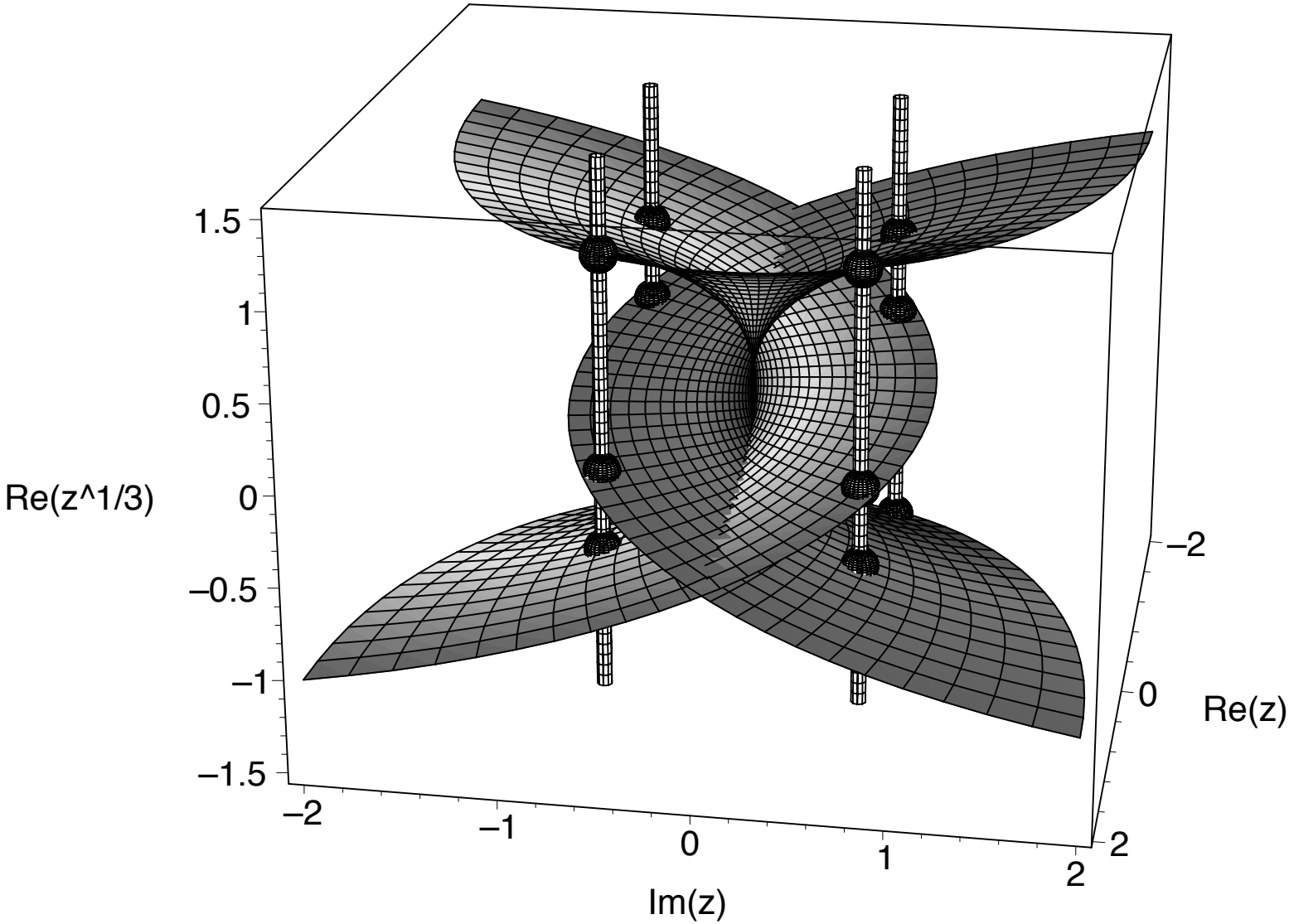
As the samples satisfy the equation $c_0 + c_1 x + c_2 y = 0$,
we have $\phi(x,y) = (c_0, y)$.

The coordinate transformation applies in any dimension.

Absolute Factorization

1. Linear Traces
   - factoring a polynomial in two variables
2. Adjacent Minors
   - an example from algebraic statistics
3. Changing Coordinates
   - avoiding wrong factorizations
4. Monodromy Actions
   - viewing an algebraic curve as a Riemann surface
5. Specializing, Lifting, and Projecting
   - Hilbert irreducibility theorem, Hensel lifting, Bertini

$z^3 - w = 0$ as Riemann surface



monodromy loops

Moving between witness sets:

$$h_{KL}(\mathbf{x},t) = \lambda \begin{pmatrix} f(\mathbf{x}) \\ K(\mathbf{x}) \end{pmatrix} (1-t) + \begin{pmatrix} f(\mathbf{x}) \\ L(\mathbf{x}) \end{pmatrix} t = \mathbf{0}, \quad \lambda \in \mathbb{C},$$

we find new witness points on the hyperplanes $K(\mathbf{x}) = \mathbf{0}$, starting at those witness points satisfying $L(\mathbf{x}) = \mathbf{0}$,
letting t move from one to zero.

Choosing a random $\mu \neq \lambda$, we move back from K to L:

$$h_{LK}(\mathbf{x},t) = \mu \begin{pmatrix} f(\mathbf{x}) \\ L(\mathbf{x}) \end{pmatrix} (1-t) + \begin{pmatrix} f(\mathbf{x}) \\ K(\mathbf{x}) \end{pmatrix} t = \mathbf{0}, \quad \mu \in \mathbb{C}.$$

After h_{KL} and h_{LK} we arrive at the same witness set.
Permuted points belong to the same irreducible component.

monodromy breakup algorithm

Input: W_L, d, N
Output: $\mathcal{P}$
0. initialize $\mathcal{P}$ with d singletons;
1. generate two slices L' and L'' parallel to the given L;
2. track d paths for witness set with L';
3. track d paths for witness set with L'';
4. **for** k **from** 1 **to** N **do**
   4.1 generate new slices K and a random λ;
   4.2 track d paths defined by h_{KL};
   4.3 generate a random μ;
   4.4 track d paths defined by h_{LK};
   4.5 compute the permutation and update $\mathcal{P}$;
   4.6 **if** linear trace test certifies $\mathcal{P}$
   then leave the loop;
   end if;
   end for.

Galois groups in Maple

```
[> f := (x^2 + y^2)^3 - 4*x*y^2:
[> algcurves[monodromy](f,x,y,group);

permgroup(6, {[[1, 3], [4, 6]], [[1, 4],

    [3, 6]], [[2, 3], [4, 5]],

    [[1, 5, 6, 2], [3, 4]]})
```

Replacing `x` by `x+y/2` gives the same result.

The implementation uses analytic contuation looping around explicitly computed discriminant points.

Absolute Factorization

1. Linear Traces
   - factoring a polynomial in two variables
2. Adjacent Minors
   - an example from algebraic statistics
3. Changing Coordinates
   - avoiding wrong factorizations
4. Monodromy Actions
   - viewing an algebraic curve as a Riemann surface
5. Specializing, Lifting, and Projecting
   - Hilbert irreducibility theorem, Hensel lifting, Bertini

specialization of variables

Theorem (Hilbert's Irreducibility Theorem)

Let $f \in \mathbb{Q}[x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s]$ *be irreducible.*
Let $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ *be a finite algebraic extension.*
For almost all $(t_1, t_2, \ldots, t_r) \in \mathbb{K}^r$*:* $f(t_1, t_2, \ldots, t_r, y_1, y_2, \ldots, y_s)$ *is irreducible in* $\mathbb{K}[y_1, y_2, \ldots, y_s]$*.*

Observe that if we would take $\mathbb{C}$ instead of $\mathbb{K}$ and $s = 1$,
the theorem would not be true because of the fundamental theorem of algebra.

The connection with Galois theory is nevertheless relevant as the monodromy groups are isomorphic to Galois groups.

Hensel lifting

To lift a factorization up to the original space,
we apply Hensel lifting.

Lemma (Hensel's Lemma)

Let f be a monic polynomial in x of degree d with coefficients power series in t over $\mathbb{Q}$, $f \in \mathbb{Q}[[t]][x]$:

$$f(t,x) = x^d + a_1(t)x^{d-1} + \cdots + a_{d-1}(t)x + a_d(t).$$

If $f(0,x) = g_0(x)h_0(x)$, $g_0, h_0 \in \mathbb{Q}[x]$, $\deg(g_0) > 0$, $\deg(h_0) > 0$, such that $\gcd(g_0, h_0) = 1$,
then there exist unique monic polynomials $g, h \in \mathbb{Q}[[t]][x]$:
$\deg(g) = \deg(g_0)$, $\deg(h) = \deg(h_0)$, *such that* $g(0,x) = g_0(x)$, $h(0,x) = h_0(x)$, *and* $f(t,x) = g(t,x)h(t,x)$.

proof = algorithm

Denote

$$f = \sum_{i=0}^{\infty} f_i t^i \quad \text{with } f_i \in \mathbb{Q}[x].$$

Because f is monic, $\deg(f_0) = d = \deg(f)$
and furthermore $\deg(f_i) < d$ for $i > 0$.

We look for monic polynomials $g, h \in \mathbb{Q}[[t]][x]$
such that $f = gh$ where we write g and h as

$$g = \sum_{i=0}^{\infty} g_i t^i, \ g_i \in \mathbb{Q}[x] \quad \text{and} \quad h = \sum_{i=0}^{\infty} h_i t^i, \ h_i \in \mathbb{Q}[x],$$

with $\deg(g_i) < r = \deg(g)$ for $i > 0$
and $\deg(h_i) < s = \deg(h)$ for $i > 0$.

system of polynomials

The condition $f = gh$ is then equivalent to the system

$$\sum_{i=0}^{n} g_i h_{n-i} = f_n, \quad n = 0, 1, \ldots.$$

We solve this system by induction on n.
For $n = 0$, we have $g_0 h_0 = g(0, x)h(0, x) = f(0, x) = f_0$.

For $n > 0$, assume all g_i and h_j for $i < n$ and $j < n$ have already been computed. We write the nth equation as

$$\begin{aligned} f_n &= g_0 h_n + g_1 h_{n-1} + \cdots + g_{n-1} h_1 + g_n h_0 \\ &= g_0 h_n + g_n h_0 + u_n, \quad \deg(u_n) < d. \end{aligned}$$

We determine g_n and h_n as solutions of $g_0 h_n + g_n h_0 = f_n - u_n = v_n$, $\deg(v_n) < n$.

$g_0 h_n + g_n h_0 = v_n$

By $\gcd(g_0, h_0) = 1$ we have $\alpha, \beta \in \mathbb{Q}[x]$: $\alpha g_0 + \beta h_0 = 1$.

Multiplying with v_n gives $v_n \alpha g_0 + v_n \beta h_0 = v_n$.

Abbreviating $v_n \alpha$ by A and $v_n \beta$ by B leads to

$$v_n = A g_0 + B h_0.$$

We divide A by h_0 and find q and w: $A = h_0 q + w$,
with $\deg(w) < deg(h_0) = s$. Replacing A gives

$$v_n = (h_0 q + w) g_0 + B h_0 = w g_0 + (B + q g_0) h_0.$$

Thus we find $h_n = w$ and $g_n = B + q g_0$.
As $w = h_n$, $\deg(h_n) < s$. To show $\deg(g_n) < r$, note: $g_n h_0 = v_n - h_n g_0$.
Because $\deg(v_n) < n$ and $\deg(h_n) < s$ we have $\deg(g_n h_0) < n$.
Thus $\deg(g_n) < r$. □

regularity

Theorem (the First Bertini Theorem)

Let X and Y be irreducible varieties over $\mathbb{C}$
and $f : X \to Y$ a regular map such that $f(X)$ is dense in Y.
Then there exists an open dense subset $U \subset Y$
such that all the fibers $f^{-1}(\mathbf{y})$ over $\mathbf{y} \in U$ are irreducible.

When we work with witness set representations,
the map f is usually defined via the projection onto a set of hyperplanes in general position.

Summary + Exercises

Monodromy actions lead to an efficient factorization method.

Exercises:

1. Compare $x^3 - y^2 = 0$ and $x^2 - y^3 = 0$. What is the difference in sampling these two polynomials?
2. Consider $f(x, y) = (x - y)(x^2 + y^2 - 1)$.
   1. Verify the factorization with the linear trace.
   2. Expand f and compute the factorization via combinatorial enumeration.
3. Write an algorithm to implement the combinatorial enumeration of all trace tests for any degree.

more exercises

4. What is the multiplicity of the origin as a solution of the equation $f(x,y) = (x^2+y^2)^3 - 4x^2y^2 = 0$?
5. Consider the system of adjacent minors.
   1. Verify that $\dim(f^{-1}(\mathbf{0})) = 5$ and $\deg(f^{-1}(\mathbf{0})) = 8$. With `phc -c` you can add five random hyperplanes to the system. Solving this augmented system with `phc -b` gives a witness set.
   2. Apply the monodromy factorization in `phc -f` to factor the witness set you created.