Absolute Factorization

By absolute factorization we mean the factorization of a multivariate polynomial (or an algebraic set) over the complex numbers. This notion of factorization is closest to the geometry and allows for approximate input coefficients. This note is mainly based on [2] and [8]. Also [1] is insightful.

1 Linear Traces

Consider some polynomial equation $f(x,y) = 0$ where the degree of f equals 3. Assume we are able to sample f by fixing x and then computing the corresponding y variables on the curve $f^{-1}(0)$. For some fixed x^*, we then find three corresponding points, denoted as $(x^*, y_1(x^*))$, $(x^*, y_2(x^*))$, and $(x^*, y_3(x^*))$. Geometrically, we imagine this sampling as taking a vertical slice defined by $x = x^*$ of the cubic curve defined by $f(x,y) = 0$.

Suppose we want to decide whether f has a quadratic factor q. Then q has to vanish at two of the three samples. Assume $q(x, y_1(x)) = 0$ and $q(x, y_2(x)) = 0$, so we may write

$$\begin{aligned} q(x, y(x)) &= (y - y_1(x))(y - y_2(x)) \quad (1) \\ &= y^2 - (y_1(x) + y_2(x))y + y_1(x)y_2(x). \quad (2) \end{aligned}$$

Observe that, 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. In that case, we denote $t_1(x) = y_1(x) + y_2(x)$ and call t_1 the linear trace. For some coefficients a and b, we may write $t_1(x) = ax + b$. Via linear interpolation at x_1 and x_2, we compute the coefficients a and b:

$$\begin{cases} ax_1 + b = y_1(x_1) + y_2(x_1) \\ ax_2 + b = y_1(x_2) + y_2(x_2) \end{cases} \quad \text{or} \quad \begin{bmatrix} x_1 & 1 \\ x_2 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} y_1(x_1) + y_2(x_1) \\ y_1(x_2) + y_2(x_2) \end{bmatrix}. \quad (3)$$

To verify now that q is a quadratic factor which vanishes at the first two sample points, we take a third sample, for $x = x_3$ we obtain the points $(x_3, y_1(x_3)$ and $(x_3, y_2(x_3)$. Then the test consists in

$$t(x_3) = ax_3 + b \stackrel{?}{=} y_1(x_3) + y_2(x_3). \quad (4)$$

If the equality in the test holds, then q is indeed a quadratic factor of f. Otherwise, to decide if f has a quadratic factor, we need to repeat the whole process for the other possible choices, here in this case defined by (y_1, y_3) and (y_2, y_3). Figure 1 illustrates the computation of the linear trace via interpolation.

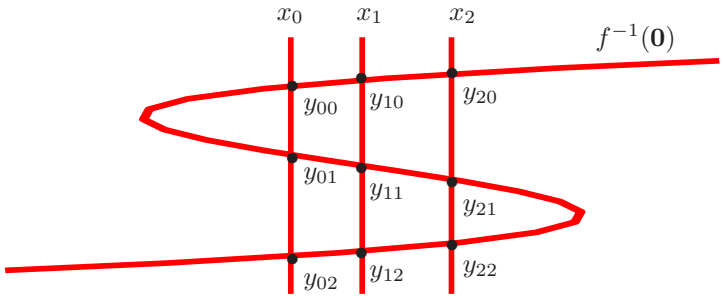

Figure 1: Use $\{(x_0, y_{00}), (x_0, y_{01}), (x_0, y_{02})\}$ and $\{(x_1, y_{10}), (x_1, y_{11}), (x_1, y_{12})\}$ to find $t_1(x) = c_0 + c_1 x$.

The accuracy of the test depends on the accuracy of the samples. For accurate computation of the linear trace, it is best to take the sample points well separated. Below is an illustration of the combinatorial method to factor a cubic, given by witness points 1, 2, 3. Every question is answered by a linear trace test.

```
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
```

While this combinatorial enumeration is efficient for polynomials of small degrees (or for polynomials with many factors of low degree), the complexity of the factorization is improved by the application of the LLL-algorithm to solve the knapsack problem formulation, see [2].

2 Adjacent Minors

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

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \end{bmatrix} \qquad f(\mathbf{x}) = \begin{cases} x_{11}x_{22} - x_{21}x_{12} = 0 \\ x_{12}x_{23} - x_{22}x_{13} = 0 \\ x_{13}x_{24} - x_{23}x_{14} = 0 \end{cases} \tag{5}$$

This is the simplest instance of a general family of problems introduced in [4], see [6] for special decomposition methods. 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).

3 Change of Coordinates

As an example (taken from [2]) for which a change of coordinates is needed, consider

$$f(x, y) = (x^2 + y^2)^3 - 4x^2y^2 = 0. \tag{6}$$

When we intersect at $x = 0.5$ we find six solutions, four real and two complex conjugate solutions. Because of the symmetry, if $f(a, b) = 0$, then also $f(\pm a, \pm b) = 0$. The plain application of the linear trace might lead to think there are 3 quadratic factors, but f is irreducible. Figure 2 shows the effect of a coordinate transformation.

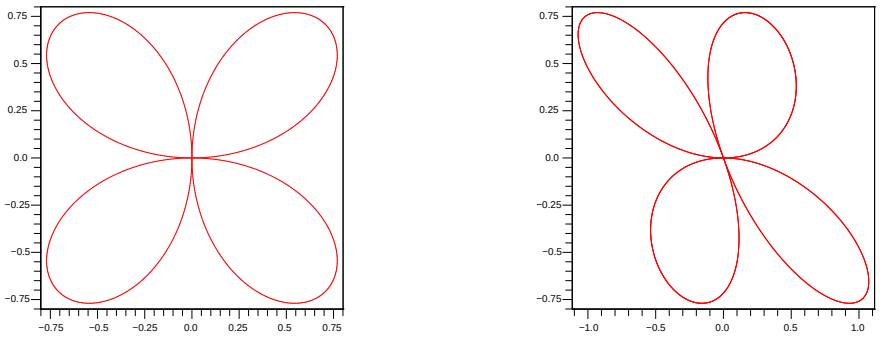

Figure 2: At the left is $f(x, y) = 0$ as in (6). At the right is the curve defined by $f(x + \frac{1}{2}y, y) = 0$.

If we work with a witness set for the curve defined by $f(x, y,) = 0$, then we consider the augmented system

$$\begin{cases} f(x,y) = 0 \\ c_0 + c_1 x + c_2 y = 0 \end{cases} \tag{7}$$

for random complex values of c_0, c_1, and c_2. To apply the linear trace test, we let only the constant term c_0 vary, taking samples on parallel hyperplanes. The coordinate transformation ϕ we then apply on the sample points (x, y) is given by

$$\phi : \mathbb{C}^2 \to \mathbb{C}^2 : \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \phi(x,y) = \begin{bmatrix} -c_1 & -c_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}. \tag{8}$$

As the samples satisfy the equation $c_0 + c_1 x + c_2 y = 0$, we have $\phi(x, y) = (c_0, y)$. The random choice of the coefficients of the hyperplane avoids the problems as with equation (6).

This construction applies to any witness set for an arbitrary polynomial system $f(\mathbf{x}) = \mathbf{0}$. If a curve obtained as a random section of the solution set factors, then the entire solution set factors as well.

4 Monodromy Actions

In complex space, an algebraic curve is seen as a Riemann surface. Figure 3 shows the Riemann surface of $z^3 - w = 0$. The height of the surface is the real part of $w = z^{1/3}$, while the gray scale corresponds to the imaginary part of $w = z^{1/3}$.

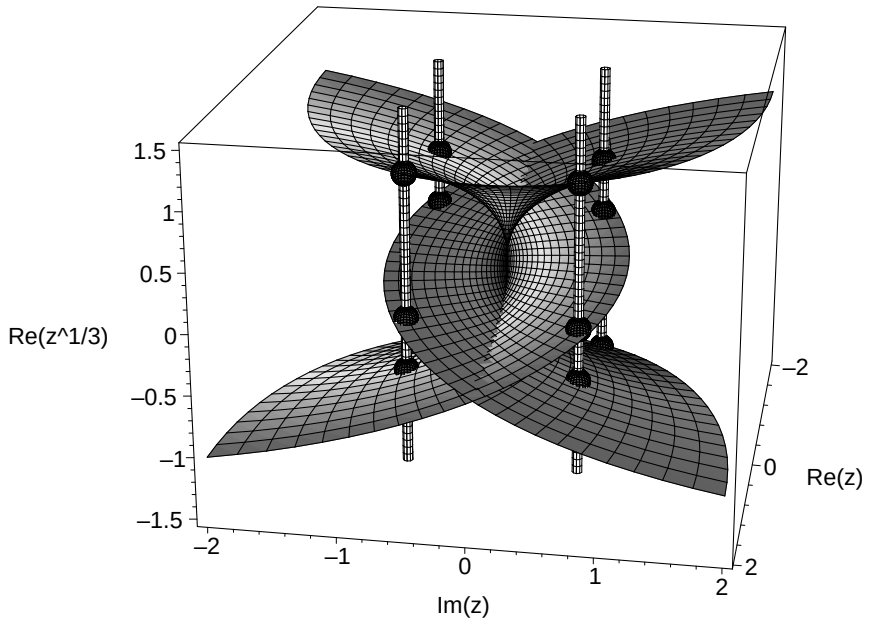

Figure 3: The Riemann surface for $z^3 - w = 0$.

Looking at the Riemann surface, focus on a line which intersects the surface in three points. Taking one complete turn of the line around the vertical axis $z = 0$ will cause the points to permute. For example, the point which was lowest will have moved up, while another point will have come down. Such a permutation can only happen if the corresponding algebraic curve is irreducible.

Based on this observation, we can decompose any pure dimensional set into irreducible components. Our monodromy algorithm returns a partition of the witness set for a pure dimensional component: points in

the same subset of the partition belong to the same irreducible component. Recall that witness points are defined by a system $f(\mathbf{x}) = \mathbf{0}$ and a set of hyperplanes $L(\mathbf{x}) = \mathbf{0}$. With the homotopy

$$h_{KL}(\mathbf{x},t) = \lambda \begin{pmatrix} f(\mathbf{x}) \\ K(\mathbf{x}) \end{pmatrix} (1-t) + \begin{pmatrix} f(\mathbf{x}) \\ L(\mathbf{x}) \end{pmatrix} t = \mathbf{0}, \quad \lambda \in \mathbb{C}, \tag{9}$$

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 another random constant $\mu \neq \lambda$, we move back from K to L, using the homotopy

$$h_{LK}(\mathbf{x},t) = \mu \begin{pmatrix} f(\mathbf{x}) \\ L(\mathbf{x}) \end{pmatrix} (1-t) + \begin{pmatrix} f(\mathbf{x}) \\ K(\mathbf{x}) \end{pmatrix} t = \mathbf{0}, \quad \mu \in \mathbb{C}. \tag{10}$$

The homotopies $h_{KL}(\mathbf{x},t) = \mathbf{0}$ and $h_{LK}(\mathbf{x},t) = \mathbf{0}$ implement one loop in the monodromy algorithm, moving witness points from L to K and then back from K to L. At the end of the loop we have the same witness set as the set we started with, except possibly permuted. Permuted points belong the same irreducible component.

Notice that the monodromy algorithm does not know the locations of the singularities. An efficient implementation of the monodromy exploits the transitivity of the monodromy actions, e.g.: if point 1 is connected to point 2 and point 2 is connected to point 3, then the points 1, 2, and 3 are witness points for the same factor.

The linear trace test is used to certify the connections made by the monodromy actions and provides also a test to decide when to stop generating new loops. Algorithm 4.1 formalizes the method, along parallel manager-worker model.

Algorithm 4.1 Monodromy Breakup certified by Linear Trace: $\mathcal{P} = \text{Breakup}(W_L, d, N)$

Input: W_L, d, N *witness set, degree, max #loops*
Output: $\mathcal{P}$ *partitioned witness set*

0. initialize $\mathcal{P}$ with d singletons; *done by manager node*
1. generate two slices L' and L'' parallel to the given L; *broadcast data to all nodes*
2. track d paths for witness set with L'; *executed in parallel by workers*
3. track d paths for witness set with L''; *executed in parallel by workers*
4. **for** k **from** 1 **to** N **do**
   - 4.1 generate new slices K and a random λ; *broadcast K and α to all nodes*
   - 4.2 track d paths defined by (9); *executed in parallel by workers*
   - 4.3 generate a random μ; *broadcast β to all nodes*
   - 4.4 track d paths defined by (10); *executed in parallel by workers*
   - 4.5 compute the permutation and update $\mathcal{P}$; *done by manager node*
   - 4.6 **if** linear trace test certifies $\mathcal{P}$
     then leave the loop;
     end if;

   end for.

The output of the factorization is a partition $\mathcal{P}$ of the points in the witness set. Initially, $\mathcal{P}$ consists of d singletons. If points switch order, we merge the sets they belong to.

The algorithms to compute the monodromy group of an algebraic curve in Maple (package algcurves) are described in [3]. An example of a Galois group computation in Maple is below:

```
[> 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.

5 Specializing, Lifting, and Projecting

We often reduce to the case of two variables by specializing variables to generic values. By this specialization (or projection) we will not turn an irreducible polynomial into a reducible one, as a consequence of the following theorem (adapted from [2], for a proof see [9]).

Theorem 5.1 (Hilbert's Irreducibility Theorem) *Let $f \in \mathbb{Q}[x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s]$ be an irreducible polynomial. Let $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ be a finite algebraic extension of $\mathbb{Q}$. 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 [1, Lecture 21].

To lift a factorization up to the original space, we apply Hensel lifting, proven in [1, Lecture 12]. Algorithms for the Hensel construction are given in [5, Chapter 6].

Lemma 5.1 (Hensel's Lemma) *Let f be a monic polynomial in x of degree d with coefficients power series in t over $\mathbb{Q}$:*

$$f(t,x) = x^d + a_1(t)x^{d-1} + \cdots + a_{d-1}(t)x + a_d(t) \in \mathbb{Q}[[t]][x]. \tag{11}$$

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. Denote

$$f = \sum_{i=0}^{\infty} f_i t^i \quad \text{with } f_i \in \mathbb{Q}[x]. \tag{12}$$

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

$$g = \sum_{i=0}^{\infty} g_i t^i,\ g_i \in \mathbb{Q}[x] \quad \text{and} \quad h = \sum_{i=0}^{\infty} h_i t^i,\ h_i \in \mathbb{Q}[x], \tag{13}$$

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

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

$$\sum_{i=0}^{n} g_i h_{n-i} = f_n, \quad n = 0, 1, \ldots. \tag{14}$$

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 then as follows:

$$\begin{aligned} f_n &= g_0 h_n + g_1 h_{n-1} + \cdots + g_{n-1} h_1 + g_n h_0 && (15)\\ &= g_0 h_n + g_n h_0 + u_n && (16) \end{aligned}$$

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

The assumption in the lemma that $\gcd(g_0, h_0) = 1$ implies the existence of cofactors $\alpha, \beta \in \mathbb{Q}[x]$ such that $\alpha g_0 + \beta h_0 = 1$ or multiplying with v_n we have $v_n\alpha g_0 + v_n\beta h_0 = v_n$. Abbreviating $v_n\alpha$ by A and $v_n\beta$ by B leads to

$$v_n = Ag_0 + Bh_0. \tag{17}$$

We divide A by h_0 and find quotient q and remainder w such that $A = h_0q + w$, with $\deg(w) < deg(h_0) = s$. Replacing A in the equation above gives

$$\begin{aligned} v_n &= (h_0q + w)g_0 + Bh_0 & (18)\\ &= wg_0 + (B + qg_0)h_0. & (19)\end{aligned}$$

Thus we find $h_n = w$ and $g_n = B + qg_0$. Because w is a remainder, we have $\deg(h_n) < s$. To show that $\deg(g_n) < r$, note that $g_nh_0 = v_n - h_ng_0$. Because $\deg(v_n) < n$ and $\deg(h_n) < s$ we have $\deg(g_nh_0) < n$. Thus $\deg(g_n) < r$. □

Below we specialize the theorem found in [7, page 139] to $\mathbb{C}$.

Theorem 5.2 (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.

6 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 $f(x, y) = (x - y)(x^2 + y^2 - 1)$.
   (a) Verify the factorization with the linear trace.
   (b) 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.
4. What is the multiplicity of the origin as a solution of the equation in (6)?
5. Consider the system of adjacent minors in (5).
   (a) 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.
   (b) Apply the monodromy factorization in `phc -f` to factor the witness set you created.

References

[1] S.S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*, volume 35 of *Mathematical Surveys and Monographs*. AMS, 1990.

[2] G. Chèze and A. Galligo. Four lectures on polynomial absolute factorization. In A. Dickenstein and I.Z. Emiris, editors, *Solving Polynomial Equations. Foundations, Algorithms and Applications*, volume 14 of *Algorithms and Computation in Mathematics*, pages 339–394. Springer–Verlag, 2005.

[3] B. Deconinck and M. van Hoeij. Computing Riemann matrices of algebraic curves. *Physica D*, 152:28–46, 2001.

[4] P. Diaconis, D. Eisenbud, and B. Sturmfels. Lattice walks and primary decomposition. In B.E. Sagan and R.P. Stanley, editors, *Mathematical Essays in Honor of Gian-Carlo Rota*, volume 161 of *Progress in Mathematics*, pages 173–193. Birkhäuser, 1998.

[5] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer, Boston, 1992.

[6] S. Hoşten and J. Shapiro. Primary decomposition of lattice basis ideals. *Journal of Symbolic Computation*, 29(4&5):625–639, 2000.

[7] I.R. Shafarevich. *Basic Algebraic Geometry 1. Varieties in Projective Space*. Springer-Verlag, second edition, 1994.

[8] A.J. Sommese, J. Verschelde, and C.W. Wampler. Introduction to numerical algebraic geometry. In A. Dickenstein and I.Z. Emiris, editors, *Solving Polynomial Equations. Foundations, Algorithms and Applications*, volume 14 of *Algorithms and Computation in Mathematics*, pages 301–337. Springer–Verlag, 2005.

[9] H. Völklein. *Groups as Galois Groups. An introduction*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1996.