Towards Extending Fulton's Algorithm for Computing Intersection Multiplicities Beyond the Bivariate Case

CASC 2021

Marc Moreno Maza, Ryan Sandford

Department of Computer Science, The University of Western Ontario, Canada

November 4, 2021

Example

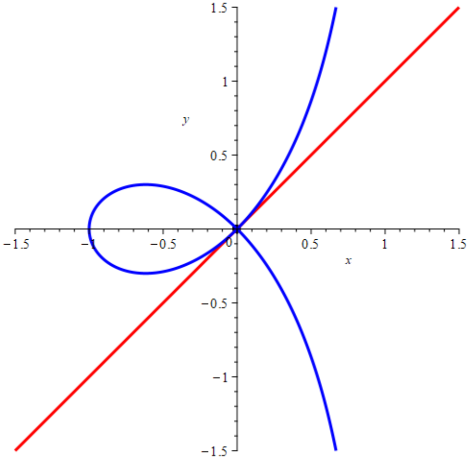

Figure: $\mathrm{Im}\big((0,0);\ y-x, x^3+xy^2+x^2-y^2\big)=3$

Table of Contents

Fulton

- In his work Algebraic Curves [Ful89], Fulton gave a constructive, axiomatic, characterization of intersection multiplicities for two bivariate, planar curves.
- His proof leads to a complete procedure for computing intersection multiplicities in the bivariate case.
- Fulton's approach uses seven properties to rewrite the input until the intersection multiplicity can either be computed or expressed as the sum of smaller intersection multiplicities.

Fulton's Properties

Theorem (Fulton's Properties)

Let $p = (p_1, p_2) \in \mathbb{A}^2(\mathbb{K})$ *and* $f, g \in \mathbb{K}[x, y]$.

(2-1) $\mathrm{Im}(p;\ f, g)$ *is a non-negative integer when* $\mathbf{V}(f)$ *and* $\mathbf{V}(g)$ *have no common component at* p. *When* $\mathbf{V}(f)$ *and* $\mathbf{V}(g)$ *do have a component in common at* p, $\mathrm{Im}(p;\ f, g) = \infty$.

(2-2) $\mathrm{Im}(p;\ f, g) = 0$ *if and only if* $p \notin \mathbf{V}(f, g)$.

(2-3) $\mathrm{Im}(p;\ f, g)$ *is invariant under affine changes of coordinates on* $\mathbb{A}^2$.

(2-4) $\mathrm{Im}(p;\ f, g) = \mathrm{Im}(p;\ g, f)$.

(2-5) $\mathrm{Im}(p;\ (x - p_1)^{m_1}, (y - p_2)^{m_2}) = m_1 m_2$ *for* $m_1, m_2 \in \mathbb{N}$.

(2-6) $\mathrm{Im}(p;\ f, gh) = \mathrm{Im}(p;\ f, g) + \mathrm{Im}(p;\ f, h)$ *for any* $h \in \mathbb{K}[x, y]$ *such that* $\mathrm{Im}(p;\ f, gh) \in \mathbb{N}$.

(2-7) $\mathrm{Im}(p;\ f, g) = \mathrm{Im}(p;\ f, g + hf)$ *for any* $h \in \mathbb{K}[x, y]$.

Fulton's Algorithm

Algorithm 1: Fulton's algorithm

Function $\mathrm{im}_2(f, g)$

Input: Let: $x \succ y$

1. $f, g \in \mathbb{K}[x, y]$ such that $\mathrm{gcd}(f, g)(0, 0) \neq 0$.

Output: $\mathrm{Im}((0, 0);\ f, g)$

if $f(0, 0) \neq 0$ **or** $g(0, 0) \neq 0$ **then**

  return 0

$r \leftarrow \deg_x (f(x, 0))$

$s \leftarrow \deg_x (g(x, 0))$

if $r > s$ **then**

  return $\mathrm{im}_2(g, f)$

if $r < 0$ **then** /* $y \mid f$ */

  write $g(x, 0) = x^m(a_m + a_{m+1}x + \ldots)$

  /* $\mathrm{im}_2(f, g) = \mathrm{im}_2(\mathrm{quo}(f, y; y), g) + \mathrm{im}_2(y, g)$ */

  return $\mathrm{im}_2(\mathrm{quo}(f, y; y), g) + m$

else

  $g' = \mathrm{lc}(f(x, 0)) \cdot g - (x)^{s-r}\mathrm{lc}(g(x, 0)) \cdot f$

  return $\mathrm{im}_2(f, g')$

Table of Contents

Related Work

- The first algorithmic solution to computing intersection multiplicities was proposed by Mora and is described in [DGPS18].
- Mora's solution is implemented in Singular and relies on the use of standard bases.
- Additionally, several standard basis free approaches were investigated in [MMV12, AMSV15, Vrb14], which apply an algorithmic criterion to reduce to the bivariate case.

Our Contribution

- Our approach to computing intersection multiplicities without the use of standard bases, was to extend Fulton's algorithm to the n-variate case, rather then reducing to the bivariate case.
- In doing so, we successfully developed a partial algorithm which generalizes the techniques used in Fulton's algorithm to the n-variate setting.
- Our generalization is not complete as Fulton's algorithm relies on a property which is not generically true beyond the bivariate case.

Table of Contents

Intersection Multiplicity and Local Rings

- Let $\mathbb{K}$ be an algebraically closed field and let $\mathbb{A}^n$ denote affine n space over $\mathbb{K}$.

Definition (Local Ring)

Take $p \in \mathbb{A}^n$, we define the local ring at p as

$$\mathcal{O}_{\mathbb{A}^n,p} := \left\{ \frac{f}{g} \mid f, g \in \mathbb{K}[x_1, \ldots, x_n] \text{ where } g(p) \neq 0 \right\}.$$

Definition (Intersection Multiplicity)

Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$. We define the intersection multiplicity of $f_1, \ldots, f_n$ at p as the dimension of the local ring at p modulo the ideal generated by $f_1, \ldots, f_n$ in the local ring at p, as a vector space over $\mathbb{K}$. That is,

$$\mathrm{Im}(p;\, f_1, \ldots, f_n) := \dim_{\mathbb{K}} (\mathcal{O}_{\mathbb{A}^n,p} / \langle f_1, \ldots, f_n \rangle).$$

Regular Sequences

- An assumption of Fulton's algorithm states that the input polynomials must not have a common factor which vanishes on p, where $p \in \mathbb{A}^n$ is the point which we wish to compute the intersection multiplicity over.
- This assumption generalizes to the condition that the input $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ must be a regular sequence in the local ring at p.
- Roughly this means given $f_1, \ldots, f_n$ as input, no f_i is a unit, zero, or a zero-divisor modulo the ideal generated by any subset of the remaining input polynomials, in the local ring at p.

Table of Contents

Generalizing Fulton's Properties

Theorem (Fulton's Properties)

Let $p = (p_1, \ldots, p_n) \in \mathbb{A}^n$ *and* $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$.

(*n*-1) $\mathrm{Im}(p;\ f_1, \ldots, f_n)$ *is a non-negative integer when* $\mathbf{V}(f_1, \ldots, f_n)$ *is zero-dimensional.*

(*n*-2) $\mathrm{Im}(p;\ f_1, \ldots, f_n) = 0$ *if and only if* $p \notin \mathbf{V}(f_1, \ldots, f_n)$.

(*n*-3) $\mathrm{Im}(p;\ f_1, \ldots, f_n)$ *is invariant under affine changes of coordinates on* $\mathbb{A}^n$.

(*n*-4) $\mathrm{Im}(p;\ f_1, \ldots, f_n) = \mathrm{Im}(p;\ \sigma(f_1, \ldots, f_n))$.

(*n*-5) $\mathrm{Im}(p;\ (x_1 - p_1)^{m_1}, \ldots, (x_n - p_n)^{m_n}) = m_1 \cdot \ldots \cdot m_n$ *for* $m_1, \ldots, m_n \in \mathbb{N}$.

(*n*-6) $\mathrm{Im}(p;\ f_1, \ldots, gh) = \mathrm{Im}(p;\ f_1, \ldots, g) + \mathrm{Im}(p;\ f_1, \ldots, h)$ *for any* $g, h \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $f_1, \ldots, gh$ *is a regular sequence in* $\mathcal{O}_{\mathbb{A}^n, p}$.

(*n*-7) $\mathrm{Im}(p;\ f_1, \ldots, f_n) = \mathrm{Im}(p;\ f_1, \ldots, f_n + g)$ *for any* $g \in \langle f_1, \ldots, f_{n-1} \rangle$.

Modular Degrees

- In Fulton's algorithm, we considered $r = \deg_x(f(x,0)), s = \deg_x(g(x,0))$ for $f, g \in \mathbb{K}[x,y]$.
- Using r, s we then determined an appropriate rewrite rule to apply to f, g.
- The following definition generalizes this notion to the n-variate case.

Definition (Modular Degree)

Take $p \in \mathbb{A}^n$, $v \in \{x_1, \ldots, x_n\}$, and $f \in \mathbb{K}[x_1, \ldots, x_n]$ where $x_1 \succ \ldots \succ x_n$. We define the modular degree of f at p with respect to v as

$$\deg_v(f \mod \langle V_{<v,p} \rangle),$$

where $V_{<v,p} = \{x_i - p_i | x_i \prec v\}$. If $V_{<v,p} = \emptyset$ then the modular degree of f at p with respect to v is simply the degree of f with respect to v.

- Often we will assume p is the origin, in which case we write $\text{moddeg}(f, v)$ to denote the modular degree of f at v.

Splitting

- The following lemma uses modular degrees to generalize the conditions of the splitting (yellow) case in Fulton's algorithm.

Lemma

Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ *forming a regular sequence in* $\mathcal{O}_{\mathbb{A}^n,p}$ *where* p *is the origin. Let* $V = \{x_1, \ldots, x_n\}$ *and let* $V_{>v} = \{x_i \in V \mid x_i > v\}$. *Define* $J : \{1, \ldots, n-1\} \to \{2, \ldots, n\}$ *such that* $J(i) = n - i + 1$.

Assume $\mathrm{moddeg}(f_i, v) < 0$ *holds for all* $i = 1, \ldots, n-1$ *and all* $v \in V_{>x_{J(i)}}$.

Then, we have $x_{J(i)} \mid f_i(x_1, \ldots, x_{J(i)}, 0, \ldots, 0)$. *Moreover, if we define* $q_i = quo(f_i(x_1, \ldots, x_{J(i)}, 0, \ldots, 0), x_{J(i)}; x_{J(i)})$ *then,*

$$\begin{aligned}\mathrm{Im}(p;\, f_1, \ldots, f_n) \quad &= \quad \mathrm{Im}(p;\, q_1, f_2, \ldots, f_n) + \mathrm{Im}(p;\, x_n, q_2, \ldots, f_n) \\ &+ \quad \ldots + \mathrm{Im}\left(p;\, x_n, \ldots, x_{J(i)+1}, q_i, f_{i+1}, \ldots, f_n\right) + \ldots \\ &+ \quad \mathrm{Im}(p;\, x_n, x_{n-1}, \ldots, q_{n-1}, f_n) + m_n\end{aligned}$$

where $m_n = max(m \in \mathbb{Z}^+ \mid f_n(x_1, 0, \ldots, 0) \equiv 0 \mod \langle x_1^m \rangle)$.

Splitting Continued

- Simply put, the above lemma states when the matrix of modular degrees has a triangular shape we may split the intersection multiplicity into smaller computations.

Example

Let $f_1, f_2, f_3 \in \mathbb{K}[x_1, x_2, x_3]$, let $x_1 \succ x_2 \succ x_3$ and let $p \in \mathbb{A}^3$ be the origin. Take $f_1 = x_3(x_2+1), f_2 = x_2^3 + x_3, f_3 = x_3^2 + x_2^3 + x_1^4(x_1+1)$. Write R the matrix of modular degrees such that $R_{i,j} = \mathrm{moddeg}(f_i, x_j)$

$$R = \begin{bmatrix} -\infty & -\infty & 1 \\ -\infty & 3 & 1 \\ 4 & 3 & 2 \end{bmatrix},$$

$$\begin{aligned} & \mathrm{Im}(p;\, f_1, f_2, f_3) = \mathrm{Im}(p;\, x_2+1, f_2, f_3) + \mathrm{Im}(p;\, x_3, f_2, f_3) \\ = \quad & \mathrm{Im}(p;\, x_2+1, f_2, f_3) + \mathrm{Im}\left(p;\, x_3, x_2^2, f_3\right) + \mathrm{Im}(p;\, x_3, x_2, f_3) \\ = \quad & 0 + 8 + 4 \end{aligned}$$

Why The Generalization is Not Complete

- Assume p is the origin.
- In the bivariate case for polynomials $f, g \in \mathbb{K}[x, y]$, one step of the algorithm may replace g with $g' := \mathrm{lc}(f(x, 0))g - x^d \mathrm{lc}(g(x, 0))f$ for some $d \in \mathbb{N}$. This preserves intersection multiplicity since $\mathrm{lc}(f(x, 0)) \in \mathbb{K}$ and hence $\langle f, g \rangle = \langle f, g' \rangle$, i.e. property (2-7) applies.
- When we generalize this, say with polynomials $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$, we replace some f_j with

  $$f_j' := \mathrm{lc}(f_i(x_1, \ldots, x_k, 0, \ldots, 0); x_k) f_j - x_k^d \mathrm{lc}(f_j(x_1, \ldots, x_k, 0, \ldots, 0); x_k) f_i,$$

  for some $i, j, k, d \in \mathbb{N}, i \neq j$.
- Unlike the bivariate case, $\mathrm{lc}(f_i(x_1, \ldots, x_k, 0, \ldots, 0); x_k)$ is not always invertible in $\mathcal{O}_p$, hence property (n-7) does not always apply.
- Hence, it is not generically true that $\langle f_1, \ldots, f_j, \ldots, f_n \rangle = \langle f_1, \ldots, f_j', \ldots, f_n \rangle$. That is, substituting f_j' for f_j does not necessarily preserve intersection multiplicity.

Generalizing Fulton's Algorithm (1/3)

Algorithm 2: Generalized Fulton's Algorithm

```
Function im_n(p; f_1, ..., f_n)
    Input: Let: x_1 ≻ ... ≻ x_n, n ≥ 2
        1. f_1, ..., f_n ∈ K[x_1, ..., x_n] such that f_1, ..., f_n form a regular sequence in O_{A^n,p} or some f_i is a unit in O_{A^n,p}.
    Output: Im(p; f_1, ..., f_n) or Fail, where p ∈ A^n is the origin
    if f_i(p) ≠ 0 for any i=1,...,n then
        return 0
    for i = 1, ..., n do
        for j = 1, ..., n − 1 do
            r_j^(i) ← moddeg(f_i, x_j)
```

- In this first section of our extension of Fulton's algorithm, we check if any of the polynomials do not vanish at p. That is, we check the base case of the algorithm.
- We also compute the $n \times n-1$ matrix of modular degrees, analogous to computing r, s in the bivariate algorithm.

Example

Let $f_1, f_2, f_3 \in \mathbb{K}[x, y, z]$ be given by $f_1 = x^2, f_2 = (x+1)y + x^3, f_3 = y^2 + z + x^3$. The matrix r computed in the first section of our generalization is:

$$r = \begin{bmatrix} 2 & 0 \\ 3 & 1 \\ 3 & 2 \end{bmatrix},$$

where the i-th row corresponds to the polynomial f_i and the j-th coloumn corresponds to the variable x_j. Hence, (i, j)-th entry is the modular degree of f_i with respect to x_j.

Generalizing Fulton's Algorithm (2/3)

Algorithm 3: Generalized Fulton's Algorithm

Function

  for $j = 1, \ldots, n-1$ **do**

    Reorder $f_1, \ldots, f_{n-j+1}$ so that $r_j^{(1)} \leq \ldots \leq r_j^{(n-j+1)}$

    $m \leftarrow min(i \mid r_j^{(i)} > 0)$ or $m \leftarrow \infty$ if no such i exists

    if $m \leq (n-j)$ **then**

      for $i = m+1, \ldots, n-j+1$ **do**

        $d \leftarrow r_j^{(i)} - r_j^{(m)}$

        $L_m \leftarrow \mathrm{lc}(f_m(x_1, \ldots, x_j, 0, \ldots, 0); x_j)$

        $L_i \leftarrow \mathrm{lc}(f_i(x_1, \ldots, x_j, 0, \ldots, 0); x_j)$

        if $L_m(p) \neq 0$ **then**

          $f_i' \leftarrow L_m f_i - x_j^d L_i f_m$

        else if $L_m \mid L_i$ **then**

          $f_i' \leftarrow f_i - x_j^d \frac{L_i}{L_m} f_m$

        else

          return Fail

      return $\mathrm{im_n}(p; f_1, \ldots, f_m, f'_{m+1}, \ldots, f'_{n-j+1}, \ldots, f_n)$

- In the second section, we seek to transform the matrix of modular degrees into a triangular shape.
- Namely, we seek to transform the matrix of modular degrees so that all entries above the anti-diagonal are $-\infty$.
- This is done through reordering polynomials by modular degree and applying (n-7) to rewriting polynomials in a way that decreases their modular degree with respect to x_j.

Example

Let $f_1, f_2, f_3 \in \mathbb{K}[x, y, z]$ be as above, given by
$f_1 = x^2, f_2 = (x+1)y + x^3, f_3 = y^2 + z + x^3$. Write

$$f_2' := f_2 - xf_1 = (x+1)y + x^3 - x^3 = (x+1)y,$$

and

$$f_3' := f_3 - xf_1 = y^2 + z + x^3 - x^3 = y^2 + z.$$

Example (continued)

Redefine $f_2 := f_2'$ and $f_3 := f_3'$. Hence, we consider $f_1 = x^2, f_2 = (x+1)y, f_3 = y^2 + z$. The matrix r computed in the first section is now:

$$r = \begin{bmatrix} 2 & 0 \\ -\infty & 1 \\ -\infty & 2 \end{bmatrix},$$

and after reordering f_1, f_2, f_3 by modular degree we have $f_1 = (x+1)y, f_2 = y^2 + z, f_3 = x^2$, with matrix of modular degrees:

$$r = \begin{bmatrix} -\infty & 1 \\ -\infty & 2 \\ 2 & 0 \end{bmatrix}.$$

- Now we apply the same procedure to reduce the modular degree with respect to y.

Example (continued)

Consider $f_1 = (x+1)y, f_2 = y^2 + z, f_3 = x^2$. Write

$$f_2' := (x+1)f_2 - yf_1 = (x+1)y^2 + (x+1)z - (x+1)y^2 = (x+1)z.$$

Redefining $f_2 := f_2'$ and reordering by modular degree in y, we have $f_1 = (x+1)z, f_2 = (x+1)y, f_3 = x^2$, and the matrix of modular degrees is now:

$$r = \begin{bmatrix} -\infty & -\infty \\ -\infty & 1 \\ 2 & 0 \end{bmatrix}.$$

- Notice (n-7) applies when computing f_2' above since $x+1$ is invertible in $\mathcal{O}_{\mathbb{A}^n,p}$.

Generalizing Fulton's Algorithm (3/3)

Algorithm 4: Generalized Fulton's Algorithm

```
Function
    m_n ← max(m ∈ ℤ^+ | f_n(x_1, 0, ..., 0) ≡ 0 mod ⟨x_1^m⟩)
    for i = 1, ..., n − 1 do
        q_i ← quo(f_i(x_1, ..., x_{n−i+1}, 0, ..., 0), x_{n−i+1}; x_{n−i+1})
    return
    im_n(p; q_1, f_2, ..., f_n)
    + im_{n−1}(p; q_2(x_1, ..., x_{n−1}, 0), ..., f_n(x_1, ..., x_{n−1}, 0))
    +
    ⋮
    +im_2(p; q_{n−1}(x_1, x_2, 0, ..., 0), f_n(x_1, x_2, 0, ..., 0))
    +m_n
```

Example (continued)

Applying the splitting lemma on $f_1 = (x+1)z, f_2 = (x+1)y, f_3 = x^2$ gives:

$$\begin{aligned}
&\mathrm{Im}(p;\ f_1, f_2, f_3) \\
&= \mathrm{Im}(p;\ x+1, f_2, f_3) + \mathrm{Im}(p;\ z, f_2, f_3) \\
&= \mathrm{Im}(p;\ x+1, f_2, f_3) + \mathrm{Im}(p;\ z, x+1, f_3) + \mathrm{Im}(p;\ z, y, f_3) \\
&= 0 + 0 + 2.
\end{aligned}$$

Table of Contents

Conclusion

- Fulton's algorithm generalizes to a partial, standard basis free, algorithm for computing intersection multiplicities in the n-variate case.
- Additionally, an observation made in the paper allows us to compute the intersection multiplicity of triangular regular sequences immediately, by means of evaluation.
- This observation also suggests a new approach to computing intersection multiplicities without the use of standard bases, by decomposing the input into triangular regular sequences.

References I

- Parisa Alvandi, Marc Moreno Maza, Éric Schost, and Paul Vrbik, *A standard basis free algorithm for computing the tangent cones of a space curve*, Computer Algebra in Scientific Computing (Cham) (Vladimir P. Gerdt, Wolfram Koepf, Werner M. Seiler, and Evgenii V. Vorozhtsov, eds.), Springer International Publishing, 2015, pp. 45–60.
- Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *4-1-1 — A computer algebra system for polynomial computations*, http://www.singular.uni-kl.de, 2018.
- William Fulton, *Algebraic curves - an introduction to algebraic geometry (reprint vrom 1969)*, Advanced book classics, Addison-Wesley, 1989.

References II

- Steffen Marcus, Marc Moreno Maza, and Paul Vrbik, *On fulton's algorithm for computing intersection multiplicities*, Computer Algebra in Scientific Computing - 14th International Workshop, CASC 2012, Maribor, Slovenia, September 3-6, 2012. Proceedings (Vladimir P. Gerdt, Wolfram Koepf, Ernst W. Mayr, and Evgenii V. Vorozhtsov, eds.), Lecture Notes in Computer Science, vol. 7442, Springer, 2012, pp. 198–211.

- P. Vrbik, *Computing intersection multiplicity via triangular decomposition*, Ph.D. thesis, The University of Western Ontario, 2014.