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

Marc Moreno Maza[1], Ryan Sandford[2]

Department of Computer Science, The University of Western Ontario, London, Canada
[1] moreno@csd.uwo.ca, [2] rsandfo@uwo.ca

Abstract. We provide a procedure which partially extends Fulton's intersection multiplicity algorithm to the general case, using a generalization of his seven properties. This procedure leads to a novel, standard basis free approach for computing intersection multiplicities beyond the case of two planar curves, which can cover cases the current standard basis free techniques cannot.

The final authenticated version is available online at https://doi.org/10.1007/978-3-030-85165-1_14.

1 Preface

This is the author's modified version of “Towards Extending Fulton's Algorithm for Computing Intersection Multiplicities Beyond the Bivariate Case”, published in the proceedings of the CASC 2021 conference [8] and differs by only a few minor changes.

1.1 Copyright

2 Introduction

The study of singularities in algebraic sets is one of the driving application areas of computer algebra and has motivated the development of numerous algorithms and software, see the books [2,4] for an overview. One important question in that area is the computation of intersection multiplicities. The first algorithmic solution was proposed by Mora, for which a modern presentation is given in [4]. Mora's approach relies on the computation of standard bases. An alternative approach has been investigated in the 2012 and 2015 CASC papers [1,6], following an observation made by Fulton in [3, Section 3-3] where he exhibits an algorithm for computing the intersection multiplicity of two plane curves.

Fulton's algorithm is based on 7 properties (see section 3.4 of the present paper) which uniquely define the intersection multiplicity of two plane curves at the origin, and yield a procedure for computing it, see algorithm 1. If the input is a pair (f_0, g_0) of bivariate polynomials over some algebraically closed field $\mathbb{K}$, then Fulton's 7 properties acts as a set of *rewrite rules* replacing (f_0, g_0), by a sequence of pairs $(f_1, g_1), (f_2, g_2), \ldots$ of bivariate polynomials over $\mathbb{K}$, which preserves the intersection multiplicity at the origin. This process may split the computation and terminates in each branch once reaching a pair for which the intersection multiplicity at the origin can be determined. This is an elegant process, which, experimentally, outperforms Mora's algorithm, as reported in [10].

Extending Fulton's algorithm to a general setting was discussed but not solved in [1, 6]. Given n polynomials $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ generating a zero-dimensional ideal, and a point $p \in \mathbf{V}(f_1, \ldots, f_n)$, the authors of [1,6] propose an algorithmic criterion for reducing the intersection multiplicity of p in $\mathbf{V}(f_1, \ldots, f_n)$, to computing another intersection multiplicity with $n-1$ polynomials in $n-1$ variables. For this criterion to be applicable, a transversality condition must hold. Unfortunately, this assumption is not generically true.

The present paper makes three contributions towards the goal of extending Fulton's algorithm to the general, multivariate case.

1. In section 4, we propose and prove an adaptation of Fulton's algorithm to handle polynomials in three variables. For $f, g, h \in \mathbb{K}[x, y, z]$ which form a regular sequence in the local ring at $p \in \mathbb{A}^3$, the proposed algorithm either returns the intersection multiplicity of p in $\mathbf{V}(f, g, h)$, or returns "Fail". We show that this algorithm can cover cases which were out of reach of the algorithmic criterion [1, 6].
2. In section 5, we extend the algorithm proposed in section 4 to the general setting of n-polynomials in n variables, where $n \geq 2$.
3. In section 6, we prove that if n polynomials $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ form both a triangular set and a regular sequence in the local ring at $p \in \mathbb{A}^n$, then the intersection multiplicity of p in $\mathbf{V}(f_1, \ldots, f_n)$ can be obtained immediately by evaluating $f_1, \ldots, f_n$.

The result of section 6 has two important consequences. First, it provides an optimization for Fulton's algorithm as well as for the algorithms of sections 4 and 5: indeed, when these algorithms are applied to a triangular regular sequence, they immediately return the intersection multiplicity at p of such input system. Second, this result suggests a new direction towards the goal of extending Fulton's algorithm: develop an algorithm which would decide whether an arbitrary regular sequence $f_1, \ldots, f_n$ (in the local ring at p) can be transformed into a triangular regular sequence.

Lastly, the present paper considers only the theoretical aspects of extending Fulton's algorithm. The current implementation, and other interesting topics such as optimizations, relative performance, and complexity analysis, will be discussed in a future paper.

3 Preliminaries

3.1 Notation

Let $\mathbb{K}$ be an algebraically closed field. Let $\mathbb{A}^n$ denote $\mathbb{A}^n(\mathbb{K})$, the affine space of dimension n over $\mathbb{K}$. Assume variables $x_1, \ldots, x_n$ are ordered $x_1 \succ \ldots \succ x_n$. We define the degree of the zero polynomial to be $-\infty$ with respect to any variable.

If I is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, we denote by $\mathbf{V}(I)$ the algebraic set (aka variety) consisting of the common zeros to all polynomials in I. An algebraic set $\mathbf{V}$ is irreducible, whenever $\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2$ for some algebraic sets $\mathbf{V}_1, \mathbf{V}_2$, implies $\mathbf{V} = \mathbf{V}_1$ or $\mathbf{V} = \mathbf{V}_2$. The ideal of an algebraic set $\mathbf{V}$, denoted by $\mathbf{I}(\mathbf{V})$, is the set of all polynomials which vanish on all points in $\mathbf{V}$. For $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$, we say $\mathbf{V}(f_1), \ldots, \mathbf{V}(f_n)$ have a common component which passes through $p \in \mathbb{A}^n$ if when we write $\mathbf{V}(f_1, \ldots, f_n)$ as a union of its irreducible components, say $\mathbf{V}_1 \cup \ldots \cup \mathbf{V}_m$, there is a $\mathbf{V}_i$ which contains p. Similarly, we say $f_1, \ldots, f_n$ have a common component through p when $\mathbf{V}(f_1), \ldots, \mathbf{V}(f_n)$ have a common component which passes through p. We say an algebraic set is zero-dimensional if it contains only finitely many points in $\mathbb{A}^n$.

3.2 Local Rings and Intersection Multiplicity

Definition 1. *Let $\mathbf{V}$ be an irreducible algebraic set with $p \in \mathbf{V}$. We define the local ring of $\mathbf{V}$ at p as*

$$\mathcal{O}_{\mathbf{V},p} := \left\{ \frac{f}{g} \mid f, g \in \mathbb{K}[x_1, \ldots, x_n]/\mathbf{I}(\mathbf{V}) \textit{ where } g(p) \neq 0 \right\}.$$

Often, we will refer to the local ring of $\mathbb{A}^n$ at p, in which case we will simply say the local ring at p and write

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

Local rings have a unique maximal ideal. In the case of $\mathcal{O}_{\mathbb{A}^n,p}$ all elements which vanish on p are in the maximal ideal and all of those that do not are units. Hence, given an element $f \in \mathbb{K}[x_1, \ldots, x_n]$ we can test whether f is invertible in $\mathcal{O}_{\mathbb{A}^n,p}$ by testing $f(p) \neq 0$.

Definition 2. *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 $p \in \mathbb{A}^n$ 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,*

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

The following observation allows us to write the intersection multiplicity of a system of polynomials as the intersection multiplicity of a smaller system of polynomials, in fewer variables, when applicable. It follows from an isomorphism between the respective residues of local rings in the definition of intersection multiplicity.

Remark 1. Let $f_1, \dots f_n \in \mathbb{K}[x_1, \dots, x_n]$ and $p = (p_1, \dots, p_n) \in \mathbb{A}^n$. If there are some f_i such that $f_i = x_i - p_i$, say $f_m, \dots, f_n$ where $1 < m \leq n$, then

$$\mathrm{Im}(p;\, f_1, \dots, f_n) = \mathrm{Im}((p_1, \dots, p_{m-1});\, F_1, \dots, F_{m-1})\,,$$

where F_j is the image of f_j modulo $\langle x_m - p_m, \dots, x_n - p_n \rangle$.

3.3 Regular Sequences

Regular sequences are one of the primary tools leveraged in our approach to compute intersection multiplicities. Given a regular sequence, corollary 1, along side propositions 3 and 4, describe a set of permissible modifications which maintain regularity.

Later we will encounter a property of intersection multiplicities which requires the input polynomials form a regular sequence. Hence, our approach will be to start with a regular sequence, perform a set of operations on the input system which are permissible as to maintain being a regular sequence, and compute the intersection multiplicity.

Proposition 1 can be found in [5, Section 3-1] and proposition 2 in [7, Section 6-15]. We believe propositions 3, 4, and 5 can also be found in the literature but include proofs for completeness, as we refer to these propositions frequently in later sections.

Definition 3. *Let R be a commutative ring and M an R module. Let $r_1, \dots, r_d$ be a sequence of elements in R. Then $r_1, \dots, r_d$ is an M-regular sequence if r_i is not a zero divisor on $M/\langle r_1, \dots, r_{i-1} \rangle M$ for all $i = 1, \dots, d$ and $M \neq \langle r_1, \dots, r_d \rangle M$.*

When $R, M = \mathcal{O}_{\mathbb{A}^n,p}$, we will often refer to a M-regular sequence as a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$ or simply as a regular sequence.

Proposition 1. *Let $r_1, \dots, r_d$ form a regular sequence in a Noetherian local ring R, and suppose all r_i are in the maximal ideal, then any permutation of $r_1, \dots, r_d$ is a regular sequence in R.*

Corollary 1. *Let $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$ where $f_1, \dots, f_n$ vanish on some $p \in \mathbb{A}^n$ and form a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$. Then any permutation of $f_1, \dots, f_n$ is a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$.*

Proof: Since $f_1, \dots, f_n$ vanish at p they are in the maximal ideal of $\mathcal{O}_{\mathbb{A}^n,p}$. The conclusion follows from proposition 1. □

With corollary 1, we can now give a more intuitive explanation of regular sequences in the local ring at p. Regular sequences in the local ring at p can be thought of as systems which behave nicely at p. That is, if $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$ is a regular sequence in the local ring at p, no f_i is zero, a zero-divisor, or a unit modulo any subset of the remaining polynomials. Moreover, we can say there is no pair f_i, f_j where $i \neq j$, modulo any subset of the remaining polynomials, which has a common component through p.

Proposition 2. *If $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ is a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$ then the irreducible component of $\mathbf{V}(f_1, \ldots, f_n)$ which passes through p is zero-dimensional.*

We may assume $\mathbf{V}(f_1, \ldots, f_n)$ is equal to its component which contains p since the other components do not affect the intersection multiplicity.

Proposition 3. *Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ where $f_1, \ldots, f_n$ vanish on some $p \in \mathbb{A}^n$. Fix some $g \in \{f_1, \ldots, f_n\}$ and choose some subset $I \subseteq \{i \in \mathbb{N} \mid 1 \leq i \leq n, f_i \neq g\}$. For each $i = 1, \ldots, n$, define*

$$F_i^I = \begin{cases} f_i & \text{if } i \notin I \\ s_i f_i - r_i g & \text{if } i \in I \end{cases}$$

where s_i, r_i are in $\mathbb{K}[x_1 \ldots, x_n]$ and each s_i is invertible in $\mathcal{O}_{\mathbb{A}^n,p}$.

Then $f_1, \ldots, f_n$ forms a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$ if and only if $F_1^I, \ldots, F_n^I$ forms a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$.

Proof: By corollary 1, $f_1, \ldots, f_n$ is a regular sequence under permutation, thus we may reorder so that all polynomials with indices in I are at the end of the sequence. That is, we may assume $I = \{i \in \mathbb{N} \mid N < i \leq n\}$ for some $N \in \mathbb{N}$. Moreover, we may reorder so that $g = f_N$.

It suffices to show F_k^I is regular modulo $\langle F_1^I, \ldots, F_{k-1}^I \rangle$ for each k such that $N < k \leq n$. First observe,

$$\begin{aligned} \langle F_1^I, \ldots, F_k^I \rangle &= \langle f_1, \ldots, f_N, s_{N+1} f_{N+1} - r_{N+1} f_N, \ldots, s_k f_k - r_k f_N \rangle \\ &= \langle f_1, \ldots, f_N, s_{N+1} f_{N+1}, \ldots, s_k f_k \rangle \\ &= \langle f_1, \ldots, f_k \rangle. \end{aligned}$$

Hence, we will show F_k^I is regular modulo $\langle f_1, \ldots, f_{k-1} \rangle$. Suppose it was not, thus there are $q, a_1, \ldots, a_{k-1}$ in $\mathcal{O}_{\mathbb{A}^n,p}$ where $q \notin \langle f_1, \ldots, f_{k-1} \rangle$ such that,

$$\begin{aligned} qF_k^I &= a_1 f_1 + \ldots + a_{k-1} f_{k-1} \\ q s_k f_k - q r_k f_N &= a_1 f_1 + \ldots + a_{k-1} f_{k-1} \\ q f_k &= s_k^{-1}(a_1 f_1 + \ldots + (q r_k + a_N) f_N + \ldots + a_{k-1} f_{k-1}). \end{aligned}$$

Since $q \notin \langle f_1, \ldots, f_{k-1} \rangle$, this contradicts the regularity of f_k modulo $\langle f_1, \ldots, f_{k-1} \rangle$. The converse follows by the same argument. □

Let $\langle f_1, \ldots, \widehat{f_r}, \ldots, f_n \rangle$ denote the ideal generated in the local ring by $f_1, \ldots, f_n$ with f_r ommited.

Proposition 4. *Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ where $f_1, \ldots, f_n$ vanish on some $p \in \mathbb{A}^n$. Suppose for some k we have $f_k = q_1 q_2$ for some $q_1, q_2 \in \mathbb{K}[x_1, \ldots, x_n]$ which are not units in $\mathcal{O}_{\mathbb{A}^n,p}$. Then $f_1, \ldots, f_n$ is a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$ if and only if both $f_1, \ldots, q_1, \ldots, f_n$ and $f_1, \ldots, q_2, \ldots, f_n$ are regular sequences in $\mathcal{O}_{\mathbb{A}^n,p}$.*

Proof:

Suppose $f_1, \ldots, f_n$ is not a regular sequence. We may assume neither $q_1, q_2 \in \langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$ since otherwise the claim clearly holds. Since $f_1, \ldots, f_n$ is not a regular sequence there exists coefficients $Q_1, \ldots, Q_n$ and an index r such that

$$\sum_{i=1}^{n} Q_i f_i = 0,$$

and $Q_r \notin \langle f_1, \ldots, \widehat{f_r}, \ldots, f_n \rangle$.

If $r = k$ write

$$Q_1 f_1 + \ldots + Q_k q_1 q_2 + \ldots + Q_n f_n = 0,$$

and $Q_k \notin \langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$. If $Q_k q_1 \notin \langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$ then q_2 is a zero divisor since the image of q_2 is not zero modulo $\langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$. If $Q_k q_1 \in \langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$ then q_1 is a zero divisor since the image of Q_k and q_1 modulo $\langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$ are not zero. Hence, one of $f_1, \ldots, q_1, \ldots, f_n$ or $f_1, \ldots, q_2, \ldots, f_n$ is not a regular sequence.

Suppose $r \neq k$. Since $Q_r \notin \langle f_1, \ldots, f_k, \ldots, \widehat{f_r}, \ldots, f_n \rangle$, Q_r can not be in both $\langle f_1, \ldots, q_1, \ldots, \widehat{f_r}, \ldots, f_n \rangle$ and $\langle f_1, \ldots, q_2, \ldots, \widehat{f_r}, \ldots, f_n \rangle$. Say $Q_r \notin \langle f_1, \ldots, q_1, \ldots, \widehat{f_r}, \ldots, f_n \rangle$. Defining $Q'_i = Q_i$ for all $i \neq k$ and $Q'_k = Q_k q_2$ gives

$$Q'_1 f_1 + \ldots + Q'_k q_1 + \ldots + Q'_n f_n = 0,$$

and $Q'_r \notin \langle f_1, \ldots, q_1, \ldots, \widehat{f_r}, \ldots, f_n \rangle$, and hence $f_1, \ldots, q_1, \ldots, f_n$ is not a regular sequence.

Conversely, suppose one of $f_1, \ldots, q_1, \ldots, f_n$ or $f_1, \ldots, q_2, \ldots, f_n$ is not a regular sequence, say $f_1, \ldots, q_1, \ldots, f_n$. Then there are $Q_1, \ldots, Q_n \in \mathcal{O}_{\mathbb{A}^n,p}$ such that, $Q_1 f_1 + \ldots + Q_k q_1 + \ldots + Q_n f_n = 0$

Consider Q_k, if $Q_k \notin \langle f_1, \ldots, \widehat{q_1}, \ldots, f_n \rangle$, then multiplying by q_2 gives us $q_2 Q_1 f_1 + \ldots + Q_k(q_1 q_2) + \ldots + q_2 Q_n f_n = 0$ and hence $q_2 Q_1 f_1 + \ldots + Q_k f_k + \ldots + q_2 Q_n f_n = 0$. Defining $Q'_i = Q_i q_2$ for all $i \neq k$ and $Q'_k = Q_k$ gives us

$$\sum_{i=1}^{n} Q'_i f_i = 0,$$

and $Q_k \notin \langle f_1, \ldots, \widehat{f_k}, \ldots, f_n \rangle$, hence $f_1, \ldots, f_n$ is not a regular sequence.

If $Q_k \in \langle f_1, \ldots, \widehat{q_1}, \ldots, f_n \rangle$ then we can write $Q'_1 f_1 + \ldots + 0 q_1 + \ldots + Q'_n f_n = 0$ for some $Q'_1, \ldots, Q'_n \in \mathcal{O}_{\mathbb{A}^n,p}$. Since $f_1, \ldots, q_1, \ldots, f_n$ is not a regular sequence, there must be some index r such that $Q'_r \notin \langle F_1, \ldots, \widehat{F_r}, \ldots, F_n \rangle$ where $F_i = f_i$ for all $i \neq k$ and $F_k = q_1$. Hence $Q'_r \notin \langle f_1, \ldots, \widehat{f_r}, \ldots, f_n \rangle$. Moreover, we may replace q_1 with f_k without affecting the sum, hence we write $Q'_1 f_1 + \ldots + 0 f_k + \ldots + Q'_n f_n = 0$. Thus, $f_1, \ldots, f_n$ is not a regular sequence.

□

Proposition 5. *Let $f_1, \dots, f_n$ be polynomials in $\mathbb{K}[x_1, \dots, x_n]$ which vanish on p. Suppose $f_1, \dots, f_n$ form a regular sequence in $\mathbb{K}[x_1, \dots, x_n]$, then $f_1, \dots, f_n$ form a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$.*

Proof: The case where $n = 1$ is straight forward, assume $n > 1$. Suppose $f_1, \dots, f_n$ is not a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$. Then there is some $i > 1$ such that f_i is not regular modulo $\langle f_1, \dots, f_{i-1} \rangle$. Write,

$$\frac{Q_1}{q_1} f_1 + \ldots + \frac{Q_{i-1}}{q_{i-1}} f_{i-1} = \frac{Q}{q} f_i,$$

for some $Q_1, \dots, Q_{i-1}, q_1, \dots, q_{i-1}, Q, q \in \mathbb{K}[x_1, \dots, x_n]$ where $q_1, \dots, q_{i-1}$ do not vanish on p and $Q \notin \langle f_1, \dots, f_{i-1} \rangle$. Observe we have,

$$(\widehat{q_1} \cdot \ldots \cdot q_{i-1} q) Q_1 f_1 + \ldots + (q_1 \cdot \ldots \cdot \widehat{q_{i-1}} q) Q_{i-1} f_{i-1} = (q_1 \cdot \ldots \cdot q_{i-1}) Q f_i,$$

where $q_1 \cdot \ldots \cdot \widehat{q_j} \cdot \ldots \cdot q_{i-1}$ is the product of $q_1 \cdot \ldots \cdot q_{i-1}$ with q_j omitted. Since $Q \notin \langle f_1, \dots, f_{i-1} \rangle$ and since none of $q_1, \dots, q_{i-1}$ vanish on p and all of $f_1, \dots, f_{i-1}$ vanish on p, we must have $(q_1 \cdot \ldots \cdot q_{i-1}) Q \notin \langle f_1, \dots, f_{i-1} \rangle$, hence f_i is not regular modulo $\langle f_1, \dots, f_{i-1} \rangle$ in the polynomial ring. □

Unlike corollary 1, and propositions 3 and 4, proposition 5 does not give a permissible modification we can make to a regular sequence. Instead, proposition 5 states that to test for a regular sequence in the local ring, it is sufficient to test for a regular sequence in the polynomial ring.

As mentioned earlier, our approach initially requires the input system to be a regular sequence. Proposition 5 tells us this is a reasonable requirement which can be tested using techniques for polynomial ideals.

3.4 Bivariate Intersection Multiplicity

It is shown in [3, Section 3-3] that the following seven properties characterize intersection multiplicity of bivariate curves. Moreover, these seven properties lead to a constructive procedure which computes the intersection multiplicity of bivariate curves, which is given in algorithm 1.

Proposition 6 (Fulton's Properties). *Let $p = (p_1, p_2) \in \mathbb{A}^2$ 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, otherwise* $\mathrm{Im}(p;\, f, g) = \infty$.

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

(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) $\mathrm{Im}(p;\, f, g) \geq m_f m_g$ *where m_f and m_g are the respective tailing degrees of f and g expressed in* $\mathbb{K}[x - p_1, y - p_2]$. *Moreover,* $\mathrm{Im}(p;\, f, g) = m_f m_g$ *when* $\mathbf{V}(f)$ *and* $\mathbf{V}(g)$ *intersect transversally, i.e. have no tangent lines in common.*

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

Algorithm 1: Fulton's algorithm

```
Function im($p; f, g$)
    Input: Let: $x \succ y$
      1. $p \in \mathbb{A}^2$ the origin.
      2. $f, g \in \mathbb{K}[x, y]$ such that $\gcd(f, g)(p) \neq 0$.
    Output: $\mathrm{Im}(p;\ f, g)$
    if $f(p) \neq 0$ or $g(p) \neq 0$ then                          /* Red */
        return $0$
    $r \leftarrow \deg_x(f(x, 0))$
    $s \leftarrow \deg_x(g(x, 0))$
    if $r > s$ then                                                 /* Green */
        return $\mathrm{im}(p; g, f)$
    if $r < 0$ then                                       /* $y \mid f$, Yellow */
        write $g(x, 0) = x^m(a_m + a_{m+1}x + \ldots)$
        return $m + \mathrm{im}(p; \mathrm{quo}(f, y; y), g)$
    else                                                            /* Blue */
        $g' = \mathrm{lc}(f(x, 0)) \cdot g - (x)^{s-r}\mathrm{lc}(g(x, 0)) \cdot f$
        return $\mathrm{im}(p; f, g')$
```

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

The following proposition was proved by Fulton in [3, Section 3-3]. It is included here for the readers convenience, as we will use similar arguments in later sections.

Proposition 7. *Algorithm 1 is correct and terminates.*

Proof: By (2-3) we may assume p is the origin. Let f, g be polynomials in $\mathbb{K}[x, y]$ with no common component through the origin. By (2-1), $\mathrm{Im}(p;\ f, g)$ is finite. We induct on $\mathrm{Im}(p;\ f, g)$ to prove termination. Suppose $\mathrm{Im}(p;\ f, g) = 0$, then by (2-2), at least one of f or g does not vanish at the origin and algorithm 1 correctly returns zero.

Now suppose $\mathrm{Im}(p;\ f, g) = n > 0$ for some $n \in \mathbb{N}$. Let r, s be the respective degrees of f, g evaluated at $(x, 0)$. By (2-4) we may reorder f, g to ensure $r \leq s$. Notice $r, s \neq 0$ since f, g vanish at the origin.

If $r < 0$, then f is a univariate polynomial in y which vanishes at the origin, hence f is divisible by y. By (2-6) we have,

$$\mathrm{Im}(p;\ f, g) = \mathrm{Im}(p;\ y, g) + \mathrm{Im}(p;\ \mathrm{quo}(f, y; y), g)\,.$$

By definition of intersection multiplicity $\mathrm{Im}(p;\ y, g) = \mathrm{Im}(p;\ y, g(x, 0))$. Since $g(x, 0)$ vanishes at the origin and since g has no common component with f at the origin, $g(x, 0)$ is a non-zero univariate polynomial divisible by x. Write

$g(x,0) = x^m(a_m + a_{m+1}x + \ldots)$ for some $a_m, a_{m+1}, \ldots \in \mathbb{K}$ where m is the largest positive integer such that $a_m \neq 0$. Applying (2-6), (2-5), and (2-2) yields

$$\operatorname{Im}(p;\ f, g) = m + \operatorname{Im}(p;\ \operatorname{quo}(f, y; y), g)\,.$$

Thus, algorithm 1 returns correctly when $r < 0$. Moreover, we can compute $\operatorname{Im}(p;\ \operatorname{quo}(f, y; y), g) < n$ by induction.

Now suppose $0 < r < s$. By (2-7), replacing g with g' preserves the intersection multiplicity. Notice such a substitution strictly decreases the degree in x of $g(x,0)$. After finitely many iterations, we will obtain curves F, G such that $\operatorname{Im}(p;\ f, g) = \operatorname{Im}(p;\ F, G)$ and the degree in x of $F(x,0) < 0$. □

3.5 A Generalization of Fulton's Properties

The following theorem gives a generalization of Fulton's Properties for n polynomials in n variables. This generalization of Fulton's Properties was first discovered by the authors of [6] and proved in [10].

Theorem 1. *Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ such that $\mathbf{V}(f_1, \ldots f_n)$ is zero-dimensional. Let $p = (p_1, \ldots, p_n) \in \mathbb{A}^n$. The $\operatorname{Im}(p;\ f_1, \ldots, f_n)$ satisfies (n-1) to (n-7) where:*

(n-1) $\operatorname{Im}(p;\ f_1, \ldots, f_n)$ *is a non-negative integer.*
(n-2) $\operatorname{Im}(p;\ f_1, \ldots, f_n) = 0$ *if and only if* $p \notin \mathbf{V}(f_1, \ldots, f_n)$.
(n-3) $\operatorname{Im}(p;\ f_1, \ldots, f_n)$ *is invariant under affine changes of coordinates on* $\mathbb{A}^n$.
(n-4) $\operatorname{Im}(p;\ f_1, \ldots, f_n) = \operatorname{Im}(p;\ \sigma(f_1, \ldots, f_n))$ *where σ is any permutation.*
(n-5) $\operatorname{Im}(p;\ (x_1 - p_1)^{m_1}, \ldots, (x_n - p_n)^{m_n}) = m_1 \cdots m_n$ *for any* $m_1, \ldots, m_n \in \mathbb{N}$.
(n-6) $\operatorname{Im}(p;\ f_1, \ldots, f_{n-1}, gh) = \operatorname{Im}(p;\ f_1, \ldots, f_{n-1}, g) + \operatorname{Im}(p;\ f_1, \ldots, f_{n-1}, h)$ *for any $g, h \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f_1, \ldots, f_{n-1}, gh$ is a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$.*
(n-7) $\operatorname{Im}(p;\ f_1, \ldots, f_n) = \operatorname{Im}(p;\ f_1, \ldots, f_{n-1}, f_n + g)$ *for any* $g \in \langle f_1, \ldots, f_{n-1} \rangle$.

4 Trivariate Fulton's Algorithm

In this section we show how the n-variate generalization of Fulton's properties can be used to create a procedure to compute intersection multiplicity in the trivariate case. Later we will see this approach generalizes to the n-variate case, although, it is helpful to first understand the algorithms behaviour in the trivariate case.

This procedure is not complete since the syzygy computations, analogous to those used in algorithm 1, do not necessarily preserve intersection multiplicity under (n-7). When this is the case, the procedure returns Fail to signal an error.

When the procedure succeeds, we obtain a powerful tool for computing intersection multiplicities in the trivariate case. This allows us to compute intersection multiplicities that previously could not be computed by other, standard basis free approaches, namely that of [1] and [10].

Throughout this section we assume $p \in \mathbb{A}^3$ is the origin.

Definition 4. *Let f be in $\mathbb{K}[x, y, z]$ where $x \succ y \succ z$. We define the modular degree of f with respect to a variable $v \in V$ as $\deg_v(f \mod \langle V_{<v}\rangle)$, where $V = \{x, y, z\}$ is the set of variables and $V_{<v}$ is the set of all variables less than v in the given ordering. If $V_{<v} = \emptyset$, we define the modular degree of f with respect to v to be the degree of f with respect to v. Write $\mathrm{moddeg}(f, v)$ to denote the modular degree of f with respect to v.*

Remark 2. The definition of modular degree can be generalized to a point $p = (p_1, p_2, p_3) \in \mathbb{A}^3$ by replacing $V_{<v}$ with $V_{<v,p} = \{x - p_1, y - p_2, z - p_3\}$ in definition 4.

The modular degree is used to generalize the computation of r, s in algorithm 1. If we fix some variable v, the modular degree with respect to v is the degree of a polynomial modulo all variables smaller than v in a given ordering.

Below we formally define cases in terms of the colour they are highlighted with in algorithm 2. Although not necessary, using a name to distinguish between cases rather then a set of conditions makes the proof far more readable, especially when the set of cases is small, as is the case for trivariate intersection multiplicity.

In the n-variate case, we will see that some of these cases are not distinct and in fact, instances of the same case. We will describe this in more detail later. For now, we make this distinction to illustrate the similarities to algorithm 1 and to help the reader build intuition for this procedure in a more general setting.

Definition 5 (Colour Cases). *Consider $f, g, h \in \mathbb{K}[x, y, z]$.*

1. *We say we are in the red case if one of f, g, h does not vanish on p.*
2. *We say we are in the blue case if:*
   (a) *We are not in the red case.*
   (b) *The modular degrees of f, g, h in x are in ascending order.*
   (c) *At least one of f or g has modular degree in x greater than zero.*
3. *We say we are in the orange case if:*
   (a) *We are not in the red case.*
   (b) *The modular degrees of f, g, h in x are in ascending order.*
   (c) *Both f and g have modular degrees in x less than zero.*
4. *We say we are in the yellow case if:*
   (a) *We are in the orange case.*
   (b) *The modular degrees of f, g, h in x and the modular degrees of f, g in y are in ascending order.*
   (c) *The modular degree of f in y is less than zero.*
5. *We say we are in the pink case if:*
   (a) *We are in the orange case.*
   (b) *The modular degrees of f, g, h in x and the modular degrees of f, g in y are in ascending order.*
   (c) *The modular degree of f in y is greater than zero.*

Remark 3. Note that when we are not in the red case for f, g, h the modular degrees of f, g, h can never be zero as f, g, h vanish at p.

Algorithm 2: Trivariate Fulton's Algorithm

```
Function $\mathrm{im}_3(p; f, g, h)$
    Input: Let: $x \succ y \succ z$
        1. $p \in \mathbb{A}^3$ the origin.
        2. $f, g, h \in \mathbb{K}[x, y, z]$ such that $f, g, h$ form a regular sequence in $\mathcal{O}_{\mathbb{A}^3,p}$ or one
           of $f, g, h$ is a unit in $\mathcal{O}_{\mathbb{A}^3,p}$.
    Output: $\mathrm{Im}(p;\ f, g, h)$ or Fail
    if $f(p) \neq 0$ or $g(p) \neq 0$ or $h(p) \neq 0$ then                  /* Red */
        return 0
    $r_y \leftarrow \mathrm{moddeg}(f, y)$, $r_x \leftarrow \mathrm{moddeg}(f, x)$
    $s_y \leftarrow \mathrm{moddeg}(g, y)$, $s_x \leftarrow \mathrm{moddeg}(g, x)$
    $t_y \leftarrow \mathrm{moddeg}(h, y)$, $t_x \leftarrow \mathrm{moddeg}(h, x)$
    Reorder $f, g, h$ so that $r_x \leq s_x \leq t_x$                          /* Green */
    if $r_x < 0$ and $s_x < 0$ then                                        /* Orange */
        Reorder $f, g$ so that $r_y \leq s_y$                                /* Green */
        if $r_y < 0$ then                                                  /* Yellow */
            $m_h \leftarrow max(m \in \mathbb{N} \mid h \mod \langle y, z\rangle = x^m(a_0 + a_1 x + \ldots))$
            $q_f \leftarrow \mathrm{quo}(f, z; z)$
            $q_g \leftarrow \mathrm{quo}(g(x, y, 0), y; y)$
            return $\mathrm{im}_3(p; q_f, g, h) + \mathrm{im}(p; q_g, h(x, y, 0)) + m_h$
        else                                                               /* Pink */
            $L_f \leftarrow \mathrm{lc}(f(x, y, 0); y)$
            $L_g \leftarrow \mathrm{lc}(g(x, y, 0); y)$
            if $L_f(p) \neq 0$ then
                $g' \leftarrow L_f g - y^{s_y - r_y} L_g f$
                return $\mathrm{im}_3(p; f, g', h)$
            else if $L_f \mid L_g$ then
                $g' \leftarrow g - y^{s_y - r_y} \frac{L_g}{L_f} f$
                return $\mathrm{im}_3(p; f, g', h)$
            else
                return Fail
    else                                                                   /* Blue */
        if $r_x < 0$ then
            $h' \leftarrow \mathrm{lc}(g(x, 0, 0); x)h - x^{t_x - s_x}\mathrm{lc}(h(x, 0, 0); x)g$
            return $\mathrm{im}_3(p; f, g, h')$
        else
            $g' \leftarrow \mathrm{lc}(f(x, 0, 0); x)g - x^{s_x - r_x}\mathrm{lc}(g(x, 0, 0); x)f$
            $h' \leftarrow \mathrm{lc}(f(x, 0, 0); x)h - x^{t_x - r_x}\mathrm{lc}(h(x, 0, 0); x)f$
            return $\mathrm{im}_3(p; f, g', h')$
```

Algorithm 2 generalizes Fulton's approach in the trivariate case. The key to generalizing Fulton's approach to 3 polynomials in 3 variables is generalizing the splitting computation. When the yellow case holds, we can split the intersection multiplicity computation into the sum of smaller intersection multiplicity computations. Thus, the rest of the algorithm is designed to reduce to the yellow case, or return Fail, in finitely many iterations.

At this time there is no clear way to characterize when algorithm 2 fails since it is difficult to determine before runtime which cases will be reached after rewriting and splitting. Namely, it is difficult to characterize all inputs which will eventually reach a branch which satisfies the conditions of the pink case. Given an input that does satisfy the conditions of pink case, it is easy to check whether algorithm 2 fails in that iteration, as we will see in the proof of theorem 2.

Theorem 2. *Algorithm 2 correctly computes the intersection multiplicity of a regular sequence $f, g, h \in \mathbb{K}[x, y, z]$ or returns Fail.*

Proof: Let $f, g, h \in \mathbb{K}[x, y, z]$ be a regular sequence in $\mathcal{O}_{\mathbb{A}^3,p}$. By ($n$-3) we may assume p is the origin. By proposition 2, $\mathbf{V}(f, g, h)$ is zero-dimensional, hence by (n-1), $\mathrm{Im}(p;\ f, g, h) \in \mathbb{N}$.

To prove termination we induct on $\mathrm{Im}(p;\ f, g, h)$ and show that when algorithm 2 does not fail, we can either compute $\mathrm{Im}(p;\ f, g, h)$ directly or strictly decrease $\mathrm{Im}(p;\ f, g, h)$ through splitting.

Suppose $\mathrm{Im}(p;\ f, g, h) = 0$, then by ($n$-2), one of f, g, h does not vanish on p, hence, algorithm 2 correctly returns zero. Assume that $\mathrm{Im}(p;\ f, g, h) = N$ for some positive $N \in \mathbb{N}$.

By (n-4) and corollary 1, we may reorder f, g, h so that their modular degrees with respect to x are in ascending order.

Suppose f, g, h satisfy the conditions of the blue case, that is, at most one polynomial has modular degree in x less than zero. Depending on how many polynomials have modular degree in x less than zero, we perform slightly different syzygy computations, since there is no need to reduce a modular degree in x of a polynomial that already has modular degree in x less than zero. Notice the syzygy computations in the blue case preserve intersection multiplicity by (n-7) and regular sequences by proposition 3. Since the modular degrees in x of the resulting polynomials is strictly decreasing, we will reach the orange case in finitely many iterations.

By (n-4) and corollary 1, we may reorder f, g so that their modular degrees with respect to y are in ascending order.

Suppose f, g, h satisfy the conditions of the pink case. Define,

$$L_f = \mathrm{lc}(f(x, y, 0); y)$$

$$L_g = \mathrm{lc}(g(x, y, 0); y).$$

If L_f is not a unit in $\mathcal{O}_{\mathbb{A}^n,p}$ and does not divide L_g, algorithm 2 returns Fail since (n-7) cannot be applied to the syzygy computations.

Suppose either $L_f(p) \neq 0$ or $L_f \mid L_g$. Then the respective syzygy computations preserve intersection multiplicity by (n-7) and regular sequences by proposition 3. Moreover, if g' is the polynomial resulting from either of the respective syzygy computations, then $\text{moddeg}(g', y) < \text{moddeg}(g, y)$ and $\text{moddeg}(g', x) < 0$. The latter statement follows from both f and g having modular degree in x less than zero as a result of being in the orange case. Since the modular degree of g' with respect to y strictly decreases, we will reach the yellow case or return Fail in finitely many iterations.

Suppose f, g, h satisfy the conditions of the yellow case. Since $\text{moddeg}(f, x) < 0$, $\text{moddeg}(f, y) < 0$, f is non-zero, and f vanishes at the origin, we have $z \mid f$.

By proposition 4, the sequence z, g, h is regular, hence $g(x, y, 0)$ is non-zero and vanishes at the origin. Since $\text{moddeg}(g, x) < 0$ holds, we have $y \mid g(x, y, 0)$.

Write $f = zq_f$, $g(x, y, 0) = yq_g$, and $m_h = max(m \in \mathbb{Z}^+ \mid h(x, 0, 0) \equiv 0 \mod \langle x^m \rangle)$. By ($n$-6) and proposition 4, it is correct to compute:

$$\begin{aligned}
\text{Im}(p;\, f, g, h) &= \text{Im}(p;\, q_f, g, h) + \text{Im}(p;\, z, q_g, h) + \text{Im}(p;\, z, y, h) \\
&= \text{Im}(p;\, q_f, g, h) + \text{Im}(p;\, z, q_g, h) + m_h \\
&= \text{Im}(p;\, q_f, g, h) + \text{Im}(p;\, q_g, h(x, y, 0)) + m_h.
\end{aligned}$$

Since m_h is a positive integer, we have:

$$\text{Im}(p;\, q_f, g, h)\,, \text{Im}(p;\, q_g, h(x, y, 0)) < \text{Im}(p;\, f, g, h) = N.$$

Thus, when algorithm 2, called on the input q_f, g, h, does not fail, termination follows from induction. □

To illustrate the utility of this approach we will work through an example where the available standard basis free techniques used to compute intersection multiplicity fail. A full description of these techniques can be found in [1] and [10], although we give a brief overview below.

Suppose for $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$, we have $\mathbf{V}(f_1, \ldots, f_n)$ is a zero-dimensional, that is, $\text{Im}(p;\, f_1, \ldots, f_n) \in \mathbb{N}$, and at least one of $f_1, \ldots, f_n$, say f_n is non-singular at p. Theorem 1 of [1], states that when the above conditions hold, and under an additional transversality constraint between $\mathbf{V}(f_1, \ldots, f_{n-1})$ and $\mathbf{V}(f_n)$, an n-variate intersection multiplicity can be reduced to an $n-1$-variate intersection multiplicity computation.

In [10], the above reduction is combined with an additional reduction procedure referred to as cylindrification. The idea behind this second reduction procedure is to use pseudo-division by a polynomial, say f_n, to reduce the degree of $f_1, \ldots, f_{n-1}$ with respect to some variable, say x_n. The cylindrification procedure assumes that f_n has a term containing x_n with a non-zero coefficient invertible in $\mathcal{O}_{\mathbb{A}^n, p}$.

The following example contains 3 polynomials which are singular at p, hence the above reduction cannot be applied. Moreover, one can check that applying cylindrification does not reduce the input in a way that the first reduction criterion holds. Hence, the current standard basis free techniques fail. Additionally, this can be verified using the *Maple* implementation of the techniques in [10].

Example 1. Compute $\operatorname{Im}\big(p;\ zy^2, y^5-z^2, x^5-y^2\big)$ using Algorithm 2.

Notice, zy^2, y^5-z^2, x^5-y^2 form a regular sequence. We compute the modular degrees with respect to x: $r_x < 0, s_x < 0, t_x = 5$, hence, we begin in the orange case. Since additionally, $r_y < 0$, we are in the yellow case and the computation reduces to:

$$\operatorname{Im}\big(p;\ zy^2, y^5-z^2, x^5-y^2\big) = \operatorname{Im}\big(p;\ y^2, y^5-z^2, x^5-y^2\big) + \operatorname{Im}\big(p;\ y^4, x^5-y^2\big) + 5.$$

Start with $\operatorname{Im}\big(p;\ y^4, x^5-y^2\big)$, applying Fulton's bivariate algorithm we get,

$$\begin{aligned}\operatorname{Im}\big(p;\ y^4, x^5-y^2\big) &= \operatorname{Im}\big(p;\ y^3, x^5-y^2\big) + 5\\ &= \operatorname{Im}\big(p;\ y^2, x^5-y^2\big) + 10\\ &= \operatorname{Im}\big(p;\ y, x^5-y^2\big) + 15\\ &= 20.\end{aligned}$$

Next we compute $\operatorname{Im}\big(p;\ y^2, y^5-z^2, x^5-y^2\big)$. Here we have modular degrees in x: $r_x < 0, s_x < 0, t_x = 5$, thus we are in the orange case. Computing the modular degrees in y we get: $r_y = 2, s_y = 5$, hence we enter the pink case. The leading coefficient in y of $y^5 - z^2$ evaluated at $z = 0$ is a unit, hence the pink case computation is valid. Thus, let $g' = (y^5 - z^2) - y^3(y^2) = -z^2$ and compute $\operatorname{Im}\big(p;\ y^2, -z^2, x^5-y^2\big)$.

Computing the modular degrees with respect to y we get: $r_y = 2, s_z < 0$, hence we reorder y^2 and $-z^2$. Again, we enter the yellow case and the computation reduces to

$$\operatorname{Im}\big(p;\ -z^2, y^2, x^5-y^2\big) = \operatorname{Im}\big(p;\ -z, y^2, x^5-y^2\big) + \operatorname{Im}\big(p;\ y, x^5-y^2\big) + 5.$$

Clearly $\operatorname{Im}\big(p;\ y, x^5-y^2\big) = 5$ by Fulton's bivariate algorithm. The computation $\operatorname{Im}\big(p;\ -z, y^2, x^5-y^2\big)$ immediately satisfies the yellow case, hence we may split,

$$\begin{aligned}\operatorname{Im}\big(p;\ -z, y^2, x^5-y^2\big) &= \operatorname{Im}\big(p;\ -1, y^2, x^5-y^2\big) + \operatorname{Im}\big(p;\ y, x^5-y^2\big) + 5\\ &= 0+5+5\\ &= 10\end{aligned}$$

Combining the intermediate computations, we get,

$$\operatorname{Im}\big(p;\ zy^2, y^5-z^2, x^5-y^2\big) = 45.$$

5 Generalized Fulton's Algorithm

In this section, we give a generalization of algorithm 1 using properties (n-1) to (n-7). Unfortunately, the natural generalization using these properties does not characterize intersection multiplicities as in the bivariate case. There are two main reasons for this.

First, property (n-6) requires the input polynomials form a regular sequence in order to split. In the bivariate case, splitting with (2-6) was always possible. Thus, for our generalization, we must assume our input is a regular sequence whenever the intersection multiplicity is not zero.

Second, syzygy computations do not necessarily preserve intersection multiplicity in the n-variate case. In particular, if a leading coefficient used in the syzygy computation is not invertible in the local ring, (n-7) may not be applicable. In the bivariate case, all leading coefficients considered in such a computation were units in the local ring. When such a case arises, other techniques must be used to complete the computation, and hence our generalization will signal an error.

Throughout this section we assume $p \in \mathbb{A}^n$ is the origin and $n > 1$.

Definition 6. *Let f be in $\mathbb{K}[x_1, \ldots, x_n]$ where $x_1 \succ \ldots \succ x_n$. We define the modular degree of f with respect to a variable $v \in V$ as $\deg_v(f \mod \langle V_{<v} \rangle)$, where $V = \{x_1, \ldots, x_n\}$ is the set of variables and $V_{<v}$ is the set of all variables less than v in the given ordering. If $V_{<v} = \emptyset$, we define the modular degree of f with respect to v to be the degree of f with respect to v. Write* $\mathrm{moddeg}(f, v)$ *to denote the modular degree of f with respect to v.*

Remark 4. The definition of modular degree can be generalized to a point $p = (p_1, \ldots, p_n) \in \mathbb{A}^n$ by replacing $V_{<v}$ with $V_{<v,p} = \{x_i - p_i \,|\, x_i < v\}$ in definition 6.

Remark 5. When $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ form a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$, the modular degrees of $f_1, \ldots, f_n$ can never be zero since $f_1, \ldots, f_n$ vanish at p.

Unlike in the trivariate case, it is no longer practical to partition the algorithm into coloured cases. Moreover, we will see that this does not accurately reflect the structure of the procedure. The main reason for this is that several of the cases we encountered in the past are instances of the same, more general case.

Roughly speaking, algorithm 3 can be divided into 2 key parts. The first is the main loop which modifies the input using syzygy computations and reordering polynomials. The second is the splitting part, which occurs as a result of the main loop successfully terminating.

The purpose of the main loop, in the j-th iteration, is to create $n - j$ polynomials with modular degrees less than zero in x_j and in any variable larger than x_j. When we examine algorithm 2 in this context, we see the orange and yellow case were simply conditions necessary to move forward an iteration in the main loop. Moreover, the syzygy computations in the blue and pink case were separate instances of the same process, which is used to reduce modular degrees for different iterations of the main loop. We highlight line 7 of algorithm 3 with the colour orange to illustrate the similarities between moving forward an iteration in the loop and satisfying the orange case in algorithm 2.

Recall in algorithm 2 there were several possible syzygy computations that could be performed in the blue case, the deciding factor being, how many of the input polynomials had modular degree in x less than zero. Extending this to the context of the n-variate algorithm, in each iteration of the main loop, we check how many polynomials already satisfy the condition required to move forward an iteration. As in the blue case, this determines how many syzygy computations to perform and which polynomials will be used in said computations. To illustrate these similarities, we highlight line 11 of algorithm 3 with the colour blue.

When the main loop terminates, assuming the procedure did not fail, our input system will have a of triangular shape with respect to modular degrees. That is, consider R, the $n \times n$ matrix of modular degrees, where $R_{i,j}$ is the modular degree of f_i with respect to x_j. Upon successful termination of the main loop, any entry of R which lies above the anti-diagonal will be negative infinity. Lemma 1, describes the implications of this triangular shape in terms of splitting intersection multiplicity computations. To illustrate the similarities between this splitting procedure, and the procedure used in the yellow case of algorithm 2, we highlight line 22 of algorithm 3 with the colour yellow.

As in the trivariate case, we cannot clearly characterize all cases for which algorithm 3 fails before runtime, due to the difficulty in determining how an input will be rewritten and split. Nonetheless, it is still easy to determine whether an input will cause algorithm 3 to fail in a given iteration of the main loop, as described in the proof of theorem 3.

Lemma 1. *Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ which form 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 the map $J : \{1, \ldots, n-1\} \to \{2, \ldots, n\}$ such that $J(i) = n - i + 1$.*

Suppose for all $i = 1, \ldots, n-1$ we have $\operatorname{moddeg}(f_i, v) < 0$ for 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,

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

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

Proof: First we will show that we can write $f_i(x_1, \ldots, x_{J(i)}, 0, \ldots, 0) = x_{J(i)} q_i$ for all $i = 1, \ldots, n-1$.

Suppose $x_n, \ldots, x_{J(i)+1}, f_i, \ldots, f_n$ is a regular sequence for some $1 \le i < n$. The hypothesis $\operatorname{moddeg}(f_i, x_1), \ldots, \operatorname{moddeg}(f_i, x_{J(i)-1}) < 0$ and the fact that f_i is regular modulo $\langle x_{J(i)+1}, \ldots, x_n \rangle$ and vanishes at the origin implies $x_{J(i)}$ divides $f_i(x_1, \ldots, x_{J(i)}, 0, \ldots, 0)$.

To show $x_n, \ldots, x_{J(i)+1}, f_i, \ldots, f_n$ is a regular sequence for all $1 \le i < n$, it suffices to show $x_n, f_2, \ldots, f_n$ is a regular sequence, since repeated applications of proposition 4, and the above implication will yield the desired result.

Observe $\operatorname{moddeg}(f_1, x_1), \ldots, \operatorname{moddeg}(f_1, x_{n-1}) < 0$ and f_1 is a non-zero polynomial which vanishes at the origin, and hence, must be divisible by x_n. By applying proposition 4 we get $x_n, f_2, \ldots, f_n$ is a regular sequence.

Algorithm 3: Generalized Fulton's Algorithm

```
Function $\mathrm{im_n}(p; f_1, \ldots, f_n)$
    Input: Let: $x_1 \succ \ldots \succ x_n$, $n \geq 2$
      1. $p \in \mathbb{A}^n$ the origin.
      2. $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f_1, \ldots, f_n$ form a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$
         or one such $f_i$ is a unit in $\mathcal{O}_{\mathbb{A}^n,p}$.

    Output: $\mathrm{Im}(p;\ f_1, \ldots, f_n)$ or Fail
    if  $f_i(p) \neq 0$ for any i=1, ..., n then                                   /* Red */
        return 0
    for $i = 1, \ldots, n$ do
        for $j = 1, \ldots, n-1$ do
            $r_j^{(i)} \leftarrow \mathrm{moddeg}(f_i, x_j)$
    for $j = 1, \ldots, n-1$ do                                                     /* Orange */
        Reorder $f_1, \ldots, f_{n-j+1}$ so that $r_j^{(1)} \leq \ldots \leq r_j^{(n-j+1)}$   /* Green */
        $m \leftarrow min(i \mid r_j^{(i)} > 0)$ or $m \leftarrow \infty$ if no such $i$ exists
        if $m \leq (n-j)$ then
            for $i = m+1, \ldots, n-j+1$ do                                         /* Blue */
                $d \leftarrow r_j^{(i)} - r_j^{(m)}$
                $L_m \leftarrow \mathrm{lc}(f_m(x_1, \ldots, x_j, 0, \ldots, 0); x_j)$
                $L_i \leftarrow \mathrm{lc}(f_i(x_1, \ldots, x_j, 0, \ldots, 0); x_j)$
                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 $\mathrm{im_n}(p; f_1, \ldots, f_m, f_{m+1}', \ldots, f_{n-j+1}', \ldots, f_n)$
                                                                                    /* Yellow */
    $m_n \leftarrow max(m \in \mathbb{Z}^+ \mid f_n(x_1, 0, \ldots, 0) \equiv 0 \mod \langle x_1^m \rangle)$
    for $i = 1, \ldots, n-1$ do
        $q_i \leftarrow \mathrm{quo}(f_i(x_1, \ldots, x_{n-i+1}, 0, \ldots, 0), x_{n-i+1}; x_{n-i+1})$
    return
    $\mathrm{im_n}(p; q_1, f_2, \ldots, f_n)$
    $+ \mathrm{im_{n-1}}(p; q_2(x_1, \ldots, x_{n-1}, 0), \ldots, f_n(x_1, \ldots, x_{n-1}, 0))$
    $+$
    $\vdots$
    $+\mathrm{im_2}(p; q_{n-1}(x_1, x_2, 0, \ldots, 0), f_n(x_1, x_2, 0, \ldots, 0))$
    $+m_n$
```

Since $f_1, \ldots, f_n$ is a regular sequence we may apply (n-6) to get

$$\mathrm{Im}(p;\ f_1, \ldots, f_n) = \mathrm{Im}(p;\ x_n, f_2, \ldots, f_n) + \mathrm{Im}(p;\ q_1, f_2, \ldots, f_n)\,.$$

By definition of intersection multiplicity,

$$\mathrm{Im}(p;\ x_n, f_2, \ldots, f_n) = \mathrm{Im}(p;\ x_n, f_2(x_1, \ldots, x_{n-1}, 0), \ldots, f_n(x_1, \ldots, x_{n-1}, 0))\,.$$

Continuing in this way we get,

$$\begin{aligned}\mathrm{Im}(p;\ f_1, \ldots, f_n) &= \mathrm{Im}(p;\ q_1, f_2, \ldots, f_n) + \mathrm{Im}(p;\ x_n, q_2, \ldots, f_n) + \ldots \\ &\quad + \mathrm{Im}(p;\ x_n, x_{n-1}, \ldots, q_{n-1}, f_n) + \mathrm{Im}(p;\ x_n, \ldots, x_2, f_n)\,.\end{aligned}$$

By definition of intersection multiplicity,

$$\mathrm{Im}(p;\ x_n, \ldots, x_2, f_n) = max(m \in \mathbb{Z}^+ \mid f_n(x_1, 0, \ldots, 0) \equiv 0 \mod \langle x_1^m \rangle),$$

which completes the proof.
□

Corollary 2. *When the conditions of lemma 1 hold,*

$$\begin{aligned}\mathrm{Im}(p;\ f_1, \ldots, f_n) &= \mathrm{Im}(p;\ q_1, f_2, \ldots, f_n) \\ &\quad + \mathrm{Im}(p;\ q_2(x_1, \ldots, x_{n-1}, 0), \ldots, f_n(x_1, \ldots, x_{n-1}, 0)) + \\ &\quad\ \vdots \\ &\quad + \mathrm{Im}(p;\ q_{n-1}(x_1, x_2, 0, \ldots, 0), f_n(x_1, x_2, 0, \ldots, 0)) \\ &\quad + m_n.\end{aligned}$$

Proof: Follows from lemma 1 and the definition of intersection multiplicity. □

Theorem 3. *Algorithm 3 correctly computes the intersection multiplicity of a regular sequence $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ or returns Fail.*

Proof: Let $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ be a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$. By ($n$-3) we may assume p is the origin. By proposition 2, $\mathbf{V}(f_1, \ldots, f_n)$ is zero-dimensional, hence by (n-1) we may assume $\mathrm{Im}(p;\ f_1, \ldots, f_n) \in \mathbb{N}$.

To prove termination we induct on $\mathrm{Im}(p;\ f_1, \ldots, f_n)$, and show that when algorithm 3 does not return Fail, we can either compute $\mathrm{Im}(p;\ f_1, \ldots, f_n)$ directly or strictly decrease $\mathrm{Im}(p;\ f_1, \ldots, f_n)$ through splitting.

Suppose $\mathrm{Im}(p;\ f_1, \ldots, f_n) = 0$, then by ($n$-2), one of $f_1, \ldots, f_n$ does not vanish at p, hence algorithm 3 correctly returns zero. Thus, we may assume $\mathrm{Im}(p;\ f_1, \ldots, f_n) = N$ for some positive $N \in \mathbb{N}$.

First, we claim that either algorithm 3 returns Fail or the input polynomials can be modified while preserving intersection multiplicity such that they satisfy the conditions of lemma 1. Moreover, we claim such modifications can be performed in finitely many iterations. To modify the input such that they satisfy the conditions of lemma 1, we proceed iteratively.

Fix some x_j where $1 \leq j \leq n-1$, and suppose $f_1, \ldots, f_{n-j+k}$ all have modular degree in x_{j-k} less than zero for any $1 \leq k < j$ whenever $j > 1$. Notice $f_1, \ldots, f_{n-j+1}$ are the polynomials which have modular degree less than zero in all variables greater then x_j. By (n-4) and corollary 1 we may rearrange $f_1, \ldots, f_{n-j+1}$ so that their modular degrees with respect to x_j are ascending.

To satisfy the conditions of lemma 1, in the j-th iteration we must have $n-j$ polynomials in $\{f_1, \ldots, f_{n-j+1}\}$ with modular degree in x_j less than zero. Since the modular degrees are in ascending order we may compute,

$$m = \begin{cases} min(i \mid \text{moddeg}(f_i, x_j) > 0) & \text{if such an } i \text{ exists,} \\ \infty & \text{otherwise.} \end{cases}$$

If $m > n-j$ then $f_1, \ldots, f_{n-j}$ satisfy the conditions of lemma 1 for the variable x_j and hence we are done.

Suppose $m \leq n-j$. We will use f_m in a syzygy computation with f_i for all $i = m+1, \ldots, n-j+1$ to reduce the modular degree of each f_i with respect to x_j. Define,

$$L_m = \text{lc}(f_m(x_1, \ldots, x_j, 0, \ldots, 0); x_j),$$

$$L_i = \text{lc}(f_i(x_1, \ldots, x_j, 0, \ldots, 0); x_j),$$

and

$$d = \text{moddeg}(f_i, x_j) - \text{moddeg}(f_m, x_j).$$

If $L_m(p) = 0$ and there is an i such that $L_i \not| L_m$, then (n-7) will not preserve intersection multiplicity under the syzygy computation since L_m is not a unit in the local ring. When this case occurs, we return Fail.

Suppose either $L_m(p) \neq 0$ or for all i we have $L_m \mid L_i$. In which case, (n-7) allows us to replace f_i with $f_i' = L_m f_i - x^d L_i f_m$ or $f_i' = f_i - x^d \frac{L_i}{L_m} f_m$ respectively. Moreover, proposition 3 tells us such a substitution preserves regular sequences.

Notice if $j > 1$, then $\text{moddeg}(f_i', x_{j-k}) < 0$ for all $1 \leq k < j$, since, by assumption, both f_i and f_m have modular degree in x_{j-k} less than zero. Thus, making such a substitution preserves the assumptions of our hypothesis. Lastly, since $\text{moddeg}(f_i', x_j) < \text{moddeg}(f_i, x_j)$, we will have $n-j$ polynomials with modular degree in x_j less than zero or return Fail, in finitely many iterations.

Thus we may now assume $f_1, \ldots, f_n$ satisfy the conditions of lemma 1, hence the algorithm correctly splits computations by lemma 1 and corollary 2.

To show termination, we may suppose none of the split computations fail, since in such a case, termination is immediate. Since m_n, as defined in lemma 1, is a positive integer, each term has intersection multiplicity strictly less than $\text{Im}(p; f_1, \ldots, f_n) = N$ and hence termination follows by induction. □

6 Triangular Regular Sequences

In this section we consider input systems with a triangular shape. We observe that under a mild constraint, such a system is a regular sequence. Moreover, the triangular shape combined with being a regular sequence allows us to compute the intersection multiplicity of such a system using (n-6).

At this time there are no known triangular decomposition techniques that preserve intersection multiplicity for a polynomial ideal in the local ring; although, if such a technique were to be discovered, the following observation could lead to a complete algorithm for computing intersection multiplicity.

Definition 7. *The main variable of a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ where $x_1 \succ \ldots \succ x_n$ is the largest variable x_i such that $\mathrm{lc}(f; x_i)$ is non-zero.*

Theorem 4 (McCoy's Theorem). *Let f be a non-zero polynomial in $R[x]$ where R is a commutative ring. Then f is a regular element of $R[x]$ if and only if ever non-zero $s \in R$ is such that $sf \neq 0$.*

McCoy's Theorem is a well-known result proven in [9].

Corollary 3. *Consider a sequence $t_1, \ldots, t_n$ such that for $i = 1, \ldots, n$, each t_i is a non-zero polynomial in $\mathbb{K}[x_i, \ldots, x_n]$ with main variable x_i.*

If at least one non-zero coefficient of t_{i-1} is invertible modulo $\langle t_i, \ldots, t_n \rangle$ for all $1 < i \leq n$, then $t_1, \ldots, t_n$ is a regular sequence in $\mathbb{K}[x_1, \ldots, x_n]$. If $t_1, \ldots, t_n$ also vanish on $p \in \mathbb{A}^n$ then $t_1, \ldots, t_n$ is a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$.

Proof: The first statement follows from theorem 4, the second statement follows from the first statement and proposition 5. □

Proposition 8. *Consider a sequence $t_1, \ldots, t_n$ such that for $i = 1, \ldots, n$, each t_i is a non-zero polynomial in $\mathbb{K}[x_i, \ldots, x_n]$ with main variable x_i.*

Suppose each $t_1, \ldots, t_n$ vanish at the origin, which we denote by p, and suppose at least one non-zero coefficent of t_{i-1} is invertible modulo $\langle t_i, \ldots, t_n \rangle$ for $1 < i \leq n$.

Then we may write $t_i(x_i, 0, \ldots, 0)$ as $x_i^{m_i} f_i$ where m_i is the least positive integer such that $f_i \in \mathbb{K}[x_i]$ does not vanish at the origin. Moreover,

$$\mathrm{Im}(p; t_1, \ldots, t_n) = m_1 \cdot \ldots \cdot m_n.$$

Proof: The result is trivial for $n = 1$, so we may assume $n > 1$. Since $t_i(x_i, 0, \ldots, 0)$ is a non-zero univariate polynomial in $\mathbb{K}[x_i]$ which vanishes at the origin, we may write $t_i(x_i, 0, \ldots, 0) = x_i^{m_i} f_i$ for a positive integer m_i and f_i a unit in the local ring at p.

By corollary 3, $t_1, \ldots, t_n$ is a regular sequence in $\mathcal{O}_{\mathbb{A}^n,p}$. Hence, we may apply ($n$-6) and proposition 4 repeatedly and finally (n-5) to get,

$$\begin{aligned}
\mathrm{Im}(p;\, t_1, \ldots, t_n) &= \mathrm{Im}(p;\, t_1, \ldots, t_{n-1}, x_n^{m_n} f_n) \\
&= \mathrm{Im}(p;\, t_1, \ldots, t_{n-1}, x_n^{m_n}) + \mathrm{Im}(p;\, t_1, \ldots, f_n) \\
&= m_n \mathrm{Im}(p;\, t_1, \ldots, t_{n-1}(x_{n-1}, 0), x_n) + 0 \\
&= m_n \mathrm{Im}\big(p;\, t_1, \ldots, x_{n-1}^{m_{n-1}} f_{n-1}, x_n\big) \\
&= m_n m_{n-1} \mathrm{Im}(p;\, t_1, \ldots, x_{n-1}, x_n) + 0 \\
&\vdots \\
&= m_1 \cdot \ldots \cdot m_n \mathrm{Im}(p;\, x_1, \ldots, x_n) \\
&= m_1 \cdot \ldots \cdot m_n.
\end{aligned}$$

□

References

1. Alvandi, P., Maza, M.M., Schost, É., Vrbik, P.: A standard basis free algorithm for computing the tangent cones of a space curve. In: Gerdt, V.P., Koepf, W., Seiler, W.M., Vorozhtsov, E.V. (eds.) Computer Algebra in Scientific Computing. pp. 45–60. Springer International Publishing, Cham (2015)
2. Cox, D., Little, J., O'Shea, D.: Using Algebraic Geometry. Graduate Text in Mathematics, 185, Springer-Verlag, New-York (1998)
3. Fulton, W.: Algebraic curves - an introduction to algebraic geometry (reprint vrom 1969). Advanced book classics, Addison-Wesley (1989)
4. Greuel, G.M., Pfister, G.: A Singular introduction to commutative algebra. Springer Science & Business Media (2012)
5. Kaplansky, I.: Commutative rings. The University of Chicago Press, Chicago, Ill.-London, revised edn. (1974)
6. Marcus, S., Moreno Maza, M., Vrbik, P.: On fulton's algorithm for computing intersection multiplicities. In: Gerdt, V.P., Koepf, W., Mayr, E.W., Vorozhtsov, E.V. (eds.) Computer Algebra in Scientific Computing - 14th International Workshop, CASC 2012, Maribor, Slovenia, September 3-6, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7442, pp. 198–211. Springer (2012), `https://doi.org/10.1007/978-3-642-32973-9_17`
7. Matsumura, H.: Commutative algebra, Mathematics Lecture Note Series, vol. 56. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edn. (1980)
8. Maza, M.M., Sandford, R.: Towards extending fulton's algorithm for computing intersection multiplicities beyond the bivariate case. In: Boulier, F., England, M., Sadykov, T.M., Vorozhtsov, E.V. (eds.) Computer Algebra in Scientific Computing - 23rd International Workshop, CASC 2021, Sochi, Russia, September 13-17, 2021, Proceedings. Lecture Notes in Computer Science, vol. 12865, pp. 232–251. Springer (2021). https://doi.org/10.1007/978-3-030-85165-1_14, `https://doi.org/10.1007/978-3-030-85165-1_14`
9. McCoy, N.H.: Remarks on divisors of zero. Amer. Math. Monthly **49**, 286–295 (1942). https://doi.org/10.2307/2303094, `https://doi-org.proxy1.lib.uwo.ca/10.2307/2303094`

10. Vrbik, P.: Computing Intersection Multiplicity via Triangular Decomposition. Ph.D. thesis, The University of Western Ontario (2014)