The Mathematics Enthusiast

Volume 3 | Number 1 Article 2

2-2006

Automated Geometric Theorem Proving: Wu's Method

Joran Elias

Automated Geometric Theorem Proving: Wu's Method

Joran Elias
University of Montana

Abstract: *Wu's Method for proving geometric theorems is well known. We investigate the underlying algorithms involved, including the concepts of pseudodivision, Ritt's Principle and Ritt's Decomposition algorithm. A simple implementation for these algorithms in Maple is presented, which we then use to prove a few simple geometric theorems to illustrate the method.*

1 Introduction

This article will discuss algebraic methods in automatic geometric theorem proving, specifically Wu's Method. Proving geometric statements algorithmically is an area of research which has particular importance in the fields of robotics and artificial intelligence. While a computer implementing Wu's Method can hardly be said to be "thinking" geometrically in the same sense as a human might, it can lend a computer the ability to interact with its physical environment in a fairly sophisticated and independent manner (see the discussion of robotic arms in [4]).

In general, we will follow the subject as presented in [1]. First, we will discuss the translation of geometric statements to the realm of algebra. After considering some examples we will move on to record some basic algebraic results needed throughout the rest of the paper. Next, we motivate Wu's Method with a brief discussion of geometry theorem proving using Groebner basis techniques. Third, we introduce the details of Wu's Method including the concepts of pseudodivision, ascending chains and characteristic sets and Ritt's Decomposition Algorithm. Next, we illustrate how Wu's Method is used to prove geometric theorems. The last section consists of a very basic implementation of Wu's Method in Maple, and its application to several examples.

Here we briefly outline Wu's Method:

- Translate a geometric theorem into a system of algebraic equations, yielding a set of hypotheses equations $f_1, \ldots, f_r$ and a conclusion g (Section 2).
- Transform our system of hypothesis equations into a triangular form using pseudodivision (Section 4.1). By triangular form, we mean that the hypothesis equations can be written as:

$$\begin{aligned} f_1 &= f_1(u_1, \ldots, u_d, x_1) \\ f_2 &= f_2(u_1, \ldots, u_d, x_1, x_2) \\ &\vdots \\ f_r &= f_r(u_1, \ldots, u_d, x_1, \ldots, x_r) \end{aligned}$$

***The Montana Mathematics Enthusiast*, ISSN 1551-3440, Vol. 3, no.1, pp. 3-50.**

and the variety $V(f_1, \ldots, f_r)$ contains the irreducible components of the original variety defined by the hypothesis equations (see Section 4.2 for details on this special triangular form).

- Perform successive pseudodivision (Section 4.1.1) on the transformed hypotheses in triangular form and the conclusion equation, yielding a final remainder. If this final remainder is zero, we will say that the conclusion g follows from the hypotheses $f_1, \ldots, f_r$.
- Examine the nondegenerate conditions that arose while triangulating the hypotheses (Section 5). In particular, we conclude that g follows from the hypotheses $f_1, \ldots, f_r$ given that the nondegenerate conditions hold. These conditions take the form $p \neq 0$ where p is a polynomial that arises naturally during our triangulation process.

2 Algebraic Formulation of Geometric Theorems

To illustrate the translation of geometric statements into a suitable system of algebraic equations, we consider a few examples. The simplest place to start is the theorem stating that the intersection of the diagonals of a parallelogram in the plane bisects the diagonals (this theorem is used repeatedly as an example in both [1] and [4]). The situation we have in mind is illustrated below.

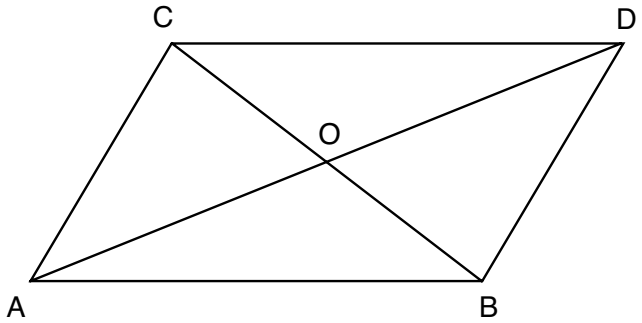


Figure 1: Parallelogram

Example 1 The basic idea is to place the figure above in the coordinate plane and then to interpret the hypotheses of the theorem as statements in coordinate, rather than Euclidean, geometry. So we begin by coordinatizing the parallelogram by placing the point A at the origin, so $A = (0, 0)$. Now we can say that the point B corresponds to $(u_1, 0)$, and that C corresponds to (u_2, u_3). The last vertex, D, is completely determined by the other three. We indicate this distinction in its coordinates by labeling D with the coordinates (x_1, x_2).

It will always be the case that some coordinates will depend upon our choices for other points. In other words, some points will be arbitrary while others

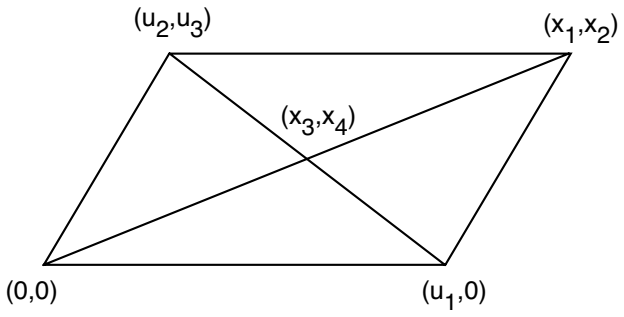


Figure 2: Coordinatized Parallelogram

will be completely determined. We will distinguish these points by using the u_i for arbitrary coordinates and the x_i for the completely determined points. Finally, the coordinates for the intersection of the diagonals, O, are also completely determined by the previous points so we let $O = (x_3, x_4)$.

The first hypothesis in our theorem is that $ABCD$ is a parallelogram. This can be restated as saying that both $\overline{AB} \| \overline{CD}$ and $\overline{AC} \| \overline{BD}$. We can translate these statements into equations by relating their slopes. For example, the slope of the line determined by the points A and B is the same as the slope of the line determined by C and D. After clearing denominators, this yields the equations:

$$\begin{aligned} x_2 - u_3 &= 0 \\ (x_1 - u_1)u_3 - x_2 u_2 &= 0 \end{aligned}$$

We label the polynomials on the left hand sides in the above equations h_1 and h_2. (The labels h_1, h_2 etc. will always refer to the *polynomials* in the equations we get upon translating our theorem. For brevity, we will not call attention to this distinction from now on. If we speak of assigning a label to an equation, we mean the polynomials as in above.) Now we must consider the assumption that O is indeed the intersection of the two diagonals. In other words, we mean that A, O, D and B, O, C are sets of collinear points. Again using the slope formula we get the equations:

$$\begin{aligned} x_4 x_1 - x_3 u_3 &= 0 \\ x_4(u_2 - u_1) - (x_3 - u_1)u_3 &= 0 \end{aligned}$$

Call these h_3 and h_4. Hence we have a system of four equations representing the hypotheses. A simple use of the distance formula gives us the following equations representing the conclusion of our theorem:

$$\begin{aligned} x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2 &= 0 \\ 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 &= 0 \end{aligned}$$

which we label g_1 and g_2. So the algebraic version of our theorem states that $g_1 = 0$ and $g_2 = 0$ should hold whenever $h_1 = 0, h_2 = 0, h_3 = 0, h_4 = 0$ also hold.

Note that our conclusion is represented by two equations, not just one. In general, our conclusion may involve several algebraic equations.

See Example 2 in Section A for a demonstration of the remaining steps in Wu's Method.

The following two examples are taken from exercises in [4].

Example 2 Another standard geometry theorem states that the altitudes of a triangle $\triangle ABC$ all meet in a single point, H, called the orthocenter (see Figure 3).

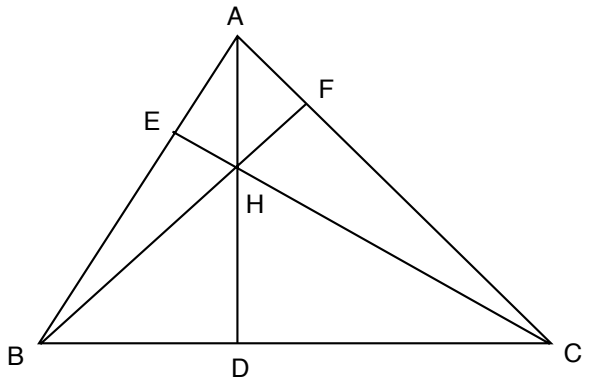


Figure 3: Orthocenter Diagram

First we construct the triangle in the coordinate plane by letting $A = (u_2, u_3)$, $B = (0, 0), C = (u_1, 0)$, as in Figure 3. Next we construct the altitudes. For example, if we let D be the point given by $(u_2, 0)$ then the line segment $\overline{AD}$ is the altitude from A. The other two altitudes require more work.

Let $E = (x_1, x_2)$ and $F = (x_3, x_4)$ be points such that $\overline{BF}, \overline{CE}$ are the altitudes from B, C respectively. This means that we must have B, E, A and C, F, A collinear. Also, we must have $\overline{CE} \perp \overline{AB}, \overline{BF} \perp \overline{AC}$. This yields the following four hypotheses:

$$\begin{aligned} x_2u_2 - x_1u_3 &= 0 \\ x_4(u_2 - u_1) - u_3(x_3 - u_1) &= 0 \\ x_2u_3 + u_2(x_1 - u_1) &= 0 \\ x_4u_3 + x_3(u_2 - u_1) &= 0 \end{aligned}$$

labeling the polynomials as h_1, h_2, h_3 and h_4. Now, we want to conclude that all three altitudes meet at a single point. Hence we construct the following two additional points: $G = (u_2, x_5)$ and $H = (u_2, x_6)$. We intend that G should be the intersection of $\overline{AD}$ and $\overline{CE}$ while H should be the intersection of the line segments $\overline{AD}$ and $\overline{BF}$. Hence we need the additional hypotheses that G, E, C and H, B, F are collinear yielding the following two equations:

$$\begin{aligned}(x_2 - x_5)(x_1 - u_1) - x_2(x_1 - u_2) &= 0\\ x_6x_3 - x_4u_2 &= 0\end{aligned}$$

which we call h_5 and h_6. Finally, our conclusion becomes the assertion that the points G and H are in fact identical. Hence, we get the equation:

$$x_5 - x_6 = 0.$$

Call this polynomial g. We should mention here that the translation of geometric problems is in general much more difficult than establishing their validity algorithmically. For example, it should be clear from our examples that we could have performed these translations in slightly different ways. We frequently have a certain degree of latitude in translating geometry theorems. While this will typically not alter the validity of the conclusion (for an exception see Example 6 in Appendix A) some translations may be substantially easier to work with. For these reasons, a human is usually needed to perform the translation accurately.

A common difficulty that arises while translating theorems is that the typical statement of geometry theorems contains implicit assumptions that are easy to overlook. As an example of what can go wrong, consider the following example.

Example 3 Let $\triangle ABC$ be a triangle in the plane. Construct three points A', B', C' so that $\triangle ABC', \triangle AB'C, \triangle A'BC$ are equilateral triangles. This situation we have in mind is illustrated below (ignore imperfections in the figure).

A theorem of classical geometry states that the line segments $\overline{AA'}, \overline{BB'}, \overline{CC'}$ all meet at a single point, S, called the Steiner point.

If we translate the theorem directly as stated above, and then attempt to use the methods described below to prove the theorem, we will fail. The reason is that we tacitly assumed that the point A' should be on a specific side of the segment $\overline{AC}$ (and similarly for B', C'). We could have constructed the figure with the equilateral triangles "folded over" so that they overlapped the original triangle:

This construction is consistent with the theorem (again ignoring imperfections in the figure), but it is obviously not what we intended. Indeed, in this case the three lines in question do not meet in a single point S. If we reformulate the theorem in such a way that this alternate construction is excluded, then

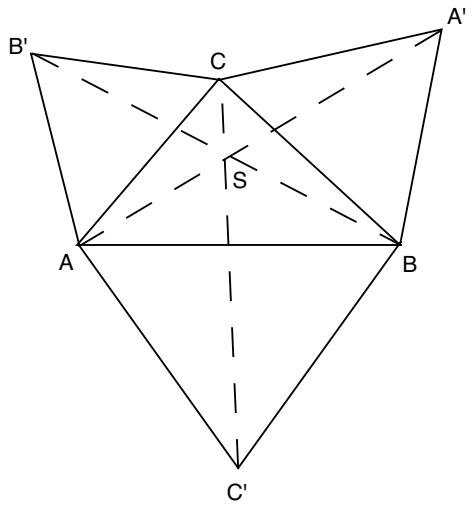


Figure 4: Steiner Point Theorem

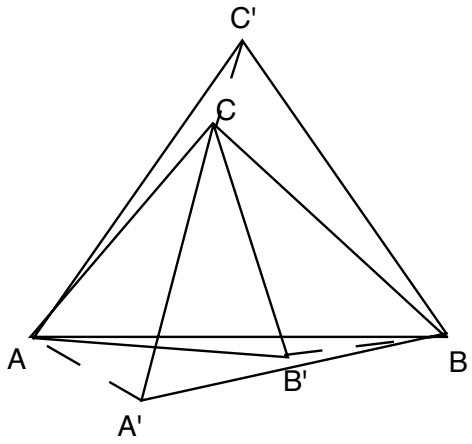


Figure 5: Incorrect Steiner Point Theorem

Wu's Method will be successful. Specifically, we could include the hypothesis that the distance from A to A' is equal to the sum of the distances from A to S and from S to A', which is easily translated using the distance formula.

Now that we've seen how to translate plane geometry theorems into systems of algebraic equations, in the next section we will summarize the algebraic results assumed for the rest of the article. Then we will specify what it means for an algebraic equation to "follow" from a system of additional algebraic equations (see Section 3.2).

3 Preliminaries

3.1 Algebraic Results

Here we set out the prerequisite notation and results from algebra that we will need in developing the notions underlying Wu's Method. In general we assume the reader is familiar with basic results involving rings, fields, ideals, prime and radical ideals, and algebraic and transcendental field extensions. If the reader is interested in proofs of these results, see [4], or any standard algebra text (e.g. [5]).

Let k be a field and denote by $k[x_1, \ldots, x_n]$ the polynomial ring in n variables over k. Similarly, $k(x_1, \ldots, x_n)$ is the field of rational functions of k in n variables. We need the following theorem due to Hilbert,

Theorem 3.1 (Hilbert Basis Theorem)**.** *Every ideal I of $k[x_1, \ldots, x_n]$ is finitely generated, or equivalently, $k[x_1, \ldots, x_n]$ has no infinite strictly increasing sequences of ideals.*

In particular, given any ideal I in $k[x_1, \ldots, x_n]$, we can write $I = \langle f_1, \ldots, f_r \rangle$ where the f_i are a finite set of polynomials. We denote the radical of the ideal I by $\sqrt{I}$.

We say that a field F is an **extension** of the field k if k is a subfield of F. Let F be an extension of k and let α be an element of F. Then α is said to be **algebraic** over k if it is the root of some nonzero polynomial with coefficients in k. Otherwise, α is **transcendental**. Let $\alpha_1, \ldots, \alpha_r$ be elements of an extension F, of k. The subfield generated by $\alpha_1, \ldots, \alpha_r$ over k is denoted by $k(\alpha_1, \ldots, \alpha_r)$ (the respective subring is given by $k[\alpha_1, \ldots, \alpha_r]$). We need the following theorem.

Theorem 3.2. *Let F be an extension of the field k and let $\alpha \in F$. If α is algebraic over k then,*

(i) $k(\alpha) = k[\alpha]$

(ii) $k(\alpha) \cong k[x]/\langle f \rangle$ *where x is an indeterminate and f is an irreducible polynomial of degree $n \geq 1$ and $f(\alpha) = 0$.*

(iii) Every element of $k(\alpha)$ can be expressed uniquely in the form $c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$, where $c_i \in k$.

We also need the ability to factor polynomials in our polynomial ring, and also in algebraic extensions, so we include the following theorems.

Theorem 3.3. *If D is a unique factorization domain, then so is the polynomial ring $D[x_1, \ldots, x_n]$. In particular, $k[x_1, \ldots, x_n]$ is a UFD.*

Theorem 3.4. *Let D be a UFD with quotient field k. Let α be in any extension of k that is algebraic over k. If there is an algorithm for factoring in D then,*

(i) there is an algorithm for factorization in the polynomial rings $D[x]$ and $k[x]$.

(ii) there is an algorithm for factorization in the polynomial ring $k(\alpha)[x]$.

This last theorem is certainly not trivial. For proofs see [9], or [10, Section 25]. Chou developed an algorithm in [2] for factoring polynomials over successive quadratic extensions over fields of rational functions that worked efficiently for most of the geometry theorems proved in [1].

We also need some basic results from affine algebraic geometry. Again, let F be an extension of the field k and let $k[x_1, \ldots, x_n]$ be the polynomial ring in n variables over k.

Definition 3.5. *Given a nonempty set of polynomials $S \subset k[x_1, \ldots, x_n]$, the **variety** $V(S)$ is defined to be the set of common zeroes of all the elements of S, i.e.*

$$V(S) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}$$

We can define varieties in terms of ideals as well. If I is the ideal generated by the polynomial set S in $k[x_1, \ldots, x_n]$ then $V(S) = V(I)$ and by the Hilbert Basis Theorem we can write, $V(I) = V(f_1, \ldots, f_r)$ where the ideal I is generated by the f_i. Hence, every algebraic variety is the set of common zeroes of a finite polynomial set.

We may also define an ideal using a nonempty subset U of k^n by letting

$$I(U) = \{f \mid f \in k[x_1, \ldots, x_n] \text{ and } f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in U\}$$

The following useful properties of V and I are easy to check: $S \subset I(V(S))$ and $U \subset V(I(U))$.

Proposition 3.6. *Let S_1 and S_2 be polynomial sets and S_1S_2 be the set of all products of an element of S_1 with an element of S_2. Then,*

(i) $V(S_1 \cup S_2) = V(S_1) \cap V(S_2)$

(ii) $V(S_1 S_2) = V(S_1) \cup V(S_2)$

It is often possible to decompose varieties into unions of smaller varieties.

Definition 3.7. *A nonempty variety V is **irreducible** if whenever V is written in the form $V = V_1 \cup V_2$ where V_1, V_2 are varieties, then either $V = V_1$ or $V = V_2$.*

Definition 3.8. *Let V be a variety. A decomposition $V = V_1 \cup \cdots \cup V_s$, where each V_i is irreducible and $V_i \not\subset V_j$ for all $i \neq j$ is called a **minimal decomposition**.*

Note that the irreducibility of a variety depends on whether or not k is algebraically closed.

When k is algebraically closed we have the following convenient characterization of irreducible varieties,

Proposition 3.9. *Let V be a nonempty variety over an algebraically closed field k. Then V is irreducible if and only if $I(V)$ is a prime ideal. If k is not algebraically closed, the converse still holds.*

Theorem 3.10. *Let V be a variety. Then V has a minimal decomposition, $V = V_1 \cup \cdots \cup V_s$, and this decomposition is unique up to the order in which the V_i are written.*

Definition 3.11. *The **dimension of a prime ideal** P (also known as its co-height) is the transcendence degree of the quotient field of the integral domain $k[x_1, \ldots, x_n]/P$ over the field k. Equivalently, its dimension is the supremum of the lengths of chains of distinct prime ideals containing P. The dimension of an irreducible variety V is the dimension of its prime ideal $I(V)$. The dimension of a (reducible) variety V is the highest dimension of one of its components.*

The following definition is crucial in light of our distinction between dependent and independent variables when translating geometric theorems.

Definition 3.12. *Let V be an irreducible variety with $P = I(V)$ its prime ideal. Let U be a subset of the variables x_i in the ring $k[x_1, \ldots, x_n]$. The variables in U are said to be **algebraically independent** on V if P does not contain a nonzero polynomial involving only variables from U. Otherwise, the variables in U are said to be **algebraically dependent**.*

Definition 3.13. *A **generic zero** of an ideal $I \lhd k[x_1, \ldots, x_n]$ is a zero $\alpha = (a_1, \ldots, a_n)$ of I in an extension of k such that $f \in I$ if and only if $f(a_1, \ldots, a_n) = 0$.*

Theorem 3.14. *An ideal I has a generic zero α in some extension of k if and only if it is a proper prime ideal.*

Proof. First suppose that I has a generic zero α in some extension of k. Since $1 \notin I$, I is proper. Let f, g be polynomials such that $fg \in I$. Then $(fg)(\alpha) = f(\alpha)g(\alpha) = 0$, which implies that either $f(\alpha)$ or $g(\alpha)$ is zero. Hence either f or g must be in I, so I is prime.

Now suppose that I is a proper prime ideal. Let $R = k[x_1, \ldots, x_n]_I$ be the localization of $k[x_1, \ldots, x_n]$ at I, and consider the field R/I_I containing k. Let $\alpha = (\bar{x}_1, \ldots, \bar{x}_n)$ where $\bar{x}_i \in R/I_I$ is the canonical image of x_i. So α is the canonical image under the mappings:

$$x_i \mapsto \frac{x_i}{1} \mapsto \frac{x_i}{1} + I_I = \bar{x}_i$$

We claim that α is a generic zero of I. To see this, let $f \in I$. Then $f = \sum_J a_J x_J$ where each x_J is a product of the variables x_i and $a_J \in k$. Evaluating at α we get:

$$f(\alpha) = \sum_J a_J \bar{x}_J = \sum_J a_J x_J + I_I = 0$$

The last equality above holds since $\sum_J a_J x_J \in I \subset I_I$.

Now, for an arbitrary $g \in k[x_1, \ldots, x_n]$, suppose that $g(\alpha) = 0$. This implies (by the equalities above) that in fact $g \in I_I$. So $g = \sum_{i=1}^{r} \frac{h_i}{p_i} f_i$ where $p_i \notin I$ and $f_i \in I$. So we have that $p_1 \cdots p_r g \in I$, and since I is prime and $p_i \notin I$, we conclude that $g \in I$. □

Corollary 3.15. *If $\alpha = (a_1, \ldots, a_n)$ is a generic zero of I, then $k[a_1, \ldots, a_n]$ is isomorphic to the quotient ring $k[x_1, \ldots, x_n]/I$ under the mapping $a_i \mapsto \tilde{x}_i$ where $\tilde{x}_i$ is the canonical image of x_i in $k[x_1, \ldots, x_n]/I$. Also, $(\tilde{x}_1, \ldots, \tilde{x}_n)$ is a generic zero of I and the dimension of I is the transcendence degree of $a_1, \ldots, a_n$ over k.*

Proof. That the mapping described in the corollary is an isomorphism is easily checked. Suppose that $f(\tilde{x}_1, \ldots, \tilde{x}_n) = 0$ in $k[x_1, \ldots, x_n]/I$. By our isomorphism, we have that $f(a_1, \ldots, a_n) = 0$, and hence $f \in I$. Also, if $f \in I$ then $f(\tilde{x}_1, \ldots, \tilde{x}_n) = 0$. Hence $(\tilde{x}_1, \ldots, \tilde{x}_n)$ is a generic zero of f. Finally, the dimension of I is just the transcendence degree of $\mathrm{Frac}(k[x_1, \ldots, x_n]/I) \cong k[\tilde{x}_1, \ldots, \tilde{x}_n]$ over k and our isomorphism shows that this is the same as the transcendence degree of $k(a_1, \ldots, a_n)$ over k. □

Remark The best way to interpret this degree is the size of any maximally algebraically independent subset of $a_1, \ldots, a_n$.

For the following results, and henceforth, we assume that k is algebraically closed. There are two equivalent forms of Hilbert's Nullstellensatz and one important consequence (we present them as in [1]).

Theorem 3.16 (Hilbert's Weak Nullstellensatz)**.** *If I is a proper ideal in $k[x_1, \ldots, x_n]$ then $V(I) \neq \emptyset$.*

Theorem 3.17 (Hilbert's Strong Nullstellensatz)**.** *Given any ideal I in the polynomial ring $k[x_1, \ldots, x_n]$, we have that $I(V(I)) = \sqrt{I}$.*

Proposition 3.18. *If P is a proper prime ideal in $k[x_1, \ldots, x_n]$ then $V(P)$ is irreducible and $I(V(P)) = P$.*

3.2 Proving Translated Theorems

We have seen that we can translate a geometric theorem into a system of algebraic equations in the ring $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$: $h_1, \ldots, h_r$ (the hypotheses) and $g_1, \ldots, g_s$ (the conclusions). From now on we will assume that our translation only yielded one conclusion ($s = 1$) since we can always consider each g_i individually. In what sense then does our conclusion, g, follow from the hypotheses, $h_1, \ldots, h_r$?

The basic idea is that we want g to be satisfied by every point that satisfies $h_1, \ldots, h_r$. In other words, we want every point in the variety defined by the hypotheses to satisfy g. Hence we start with the following definition.

Definition 3.19. *The conclusion g* ***follows strictly*** *from the hypotheses $h_1, \ldots, h_r$ if $g \in I(V) \subset k[u_1, \ldots, u_d, x_1, \ldots, x_r]$ where $V = V(h_1, \ldots, h_r)$.*

We will briefly investigate a straightforward attempt to use this definition which will serve to motivate both a revised definition and the practicality of Wu's Method. The techniques employed for this brief discussion rest upon Groebner Basis methods that we will not treat in any detail here. If the reader is unfamiliar with the concepts used below, see [4]. We use this approach simply because it allows us a direct way to motivate Definition 3.21.

In general, the field k may not be algebraically closed, so we cannot rely on computing $I(V)$ directly using Hilbert's Nullstellensatz. We can, however, use the following test.

Proposition 3.20. *If $g \in \sqrt{(h_1, \ldots, h_r)}$, then g follows strictly from $h_1, \ldots, h_r$.*

Proof. The hypothesis $g \in \sqrt{(h_1, \ldots, h_r)}$ means that $g^s \in \langle h_1, \ldots, h_r \rangle$ for some s. Hence $g^s = \sum_{i=1}^{n} A_i h_i$, where $A_i \in k[u_1, \ldots, u_d, x_1, \ldots, x_r]$. Then g^s must vanish whenever the h_i vanish, and hence g does as well. □

This test is useful because we have an algorithm for determining if $g \in \sqrt{(h_1, \ldots, h_r)}$.[1] Let us recall Example 1, and consider attempting to show that the first conclusion follows from our hypotheses. Hence we have the following hypotheses:

[1] Specifically, we have containment if and only if $\{1\}$ is the reduced Groebner basis for the ideal $\langle h_1, \ldots, h_r, 1 - yg \rangle \subset k[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y]$. See Chapter 6 Section 4 in [4] for more details.

$$\begin{aligned} h_1 &= x_2 - u_3 \\ h_2 &= (x_1 - u_1)u_3 - x_2u_2 \\ h_3 &= x_4x_1 - x_3u_3 \\ h_4 &= x_4(u_2 - u_1) - (x_3 - u_1)u_3. \end{aligned}$$

The conclusion we are interested in is

$$g_1 = x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2.$$

To use Proposition 3.20 we compute a Groebner basis for the ideal, $\langle h_1, h_2, h_3, h_4, 1 - yg_1\rangle$ in the polynomial ring $\mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y]$. Unfortunately, we do not get the Groebner basis $\{1\}$ as we should. The cause of our problem lies in the variety defined by the hypotheses: $V(h_1, h_2, h_3, h_4)$. If one computes a Groebner basis for these four equations one sees [2] that this variety is actually reducible. In particular, after some calculation we see that the variety defined by our hypotheses actually has four components, $V = V' \cup U_1 \cup U_2 \cup U_3$ defined by:

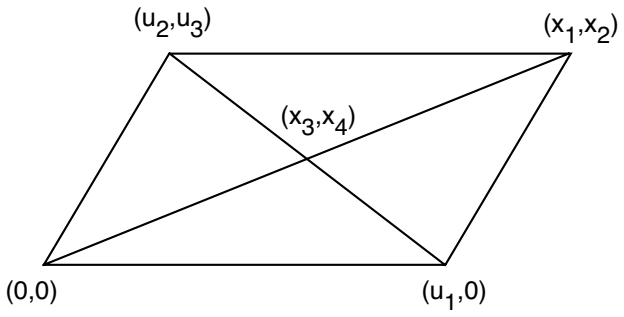
$$\begin{aligned} V' &= V\left(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}\right) \\ U_1 &= V(x_2, x_4, u_3) \\ U_2 &= V(x_1, x_2, u_1 - u_2, u_3) \\ U_3 &= V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1). \end{aligned}$$

Our original strategy revolved around showing that the conclusion, $g_1 = x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2$, vanishes on the variety defined by our hypotheses. But this clearly cannot happen on some of the components above. Consider the U_i. Each has as one of its defining equations an expression that involves only the u_i. But now recall our construction of our theorem concerning the diagonals of a parallelogram

In our construction, the coordinates corresponding to the u_i were intended to be arbitrary. But in U_1 for example, we must have $u_3 = 0$. In this case, we won't have a genuine parallelogram. It now becomes clear that $u_3 = 0$ is a degenerate case of our diagram. Since each of the U_i contain equations that involve only the u_i, each U_i corresponds to degenerate cases of our theorem. If we repeated our approach using only the component V', then Proposition 3.20 will work as we intended.

Now it should be clear that our goal is to develop a general method for establishing the validity of our conclusion only on those components of V that do not correspond

[2] In fact, we get $\{x_1x_4 + x_4u_1 - x_4u_2 - u_1u_3, x_1u_3 - u_1u_3 - u_2u_3, x_2 - u_3, x_3u_3 + x_4u_1 - x_4u_2 - u_1u_3, x_4u_1^2 - x_4u_1u_2 - \frac{1}{2}u_1^2u_3 + \frac{1}{2}u_1u_2u_3, x_4u_1u_3 - \frac{1}{2}u_1u_3^2\}$, which is reducible. Specifically, we can factor three of these equations.



to degenerate cases of our theorem. In other words, we are only interested in those components of V on which the u_i are algebraically independent. Let us revise Definition 3.19 accordingly.

Definition 3.21. *A conclusion g **follows generically** from the hypotheses $h_1, \ldots, h_r$ if $g \in I(V') \subset k[u_1, \ldots, u_d, x_1, \ldots, x_r]$ where V' is the union of those irreducible components of $V(h_1, \ldots, h_r)$ on which the u_i are algebraically independent.*

Now that we have a clearer definition to work with we can move on to discuss Wu's Method. The approach we used in Proposition 3.20 relied upon Groebner Basis techniques. While it is possible to design theorem provers around these techniques Wu's Method is tailored more specifically to the task and hence is often more computationally efficient (see [3],[6],[7]).

4 Wu's Method

4.1 Pseudodivision

The primary tool in Wu's Method is a variation on the division algorithm for multivariable polynomials (see [4] for a description) called pseudodivision. Let $f, g \in k[x_1, \ldots, x_n, y]$, with $g = a_p y^p + \cdots + a_0$ and $f = b_m y^m + \cdots + b_0$, where the a_i, b_j are polynomials in the $x_1, \ldots, x_n$. Then we have the following result.

Proposition 4.1. *Let f, g be as above and assume that $m \leq p$ and that $f \neq 0$. Then,*

(i) There is an equation

$$b_m^s g = qf + r$$

where $q, r \in k[x_1, \ldots, x_n, y]$, $s \geq 0$, and r is either the zero polynomial or its degree in y is less than m.

(ii) r is in the ideal $\langle f, g \rangle$ in the ring $k[x_1, \ldots, x_n, y]$.

Proof. First, we will use the notations $\deg(f,y)$ and $\text{LC}(f,y)$ to denote the degree of f in the variable y and the leading coefficient of f as a polynomial in y. We will establish the proposition using the following algorithm:

Input: f, g
Output: r, q

$r := g, q := 0$
While $r \neq 0$ and $\deg(r,y) \geq m$ Do
$r := b_m r - \text{LC}(r,y) f y^{\deg(r,y)-m}$
$q := b_m q + \text{LC}(r,y) y^{\deg(r,y)-m}$

We begin by using induction to show that the first part of (i) holds at each iteration of the above algorithm, or that after the i^{th} iteration we have $b_m^i g = q_i f + r_i$. For the base case, consider the situation after one time through the above algorithm. We get that

$$q_1 f + r_1 = a_p y^{p-m} f + b_m g - a_p y^{p-m} f = b_m g.$$

So indeed we have that $b_m g = q_1 f + r_1$. Now suppose that $b_m^i g = q_i f + r_i$ and consider what happens on interation $i+1$. We get:

$$\begin{aligned} q_{i+1} f + r_{i+1} &= \left(b_m q_i + \text{LC}(r_i,y) y^{\deg(r_i,y)-m}\right) f + \left(b_m r_i - \text{LC}(r_i,y) f y^{\deg(r_i,y)-m}\right) \\ &= b_m q_i f + b_m r_i \\ &= b_m (q_i f + r_i) \\ &= b_m^{i+1} g. \end{aligned}$$

The assertion that either $r = 0$ or $\deg(r,y) < m$ follows from the While statement in the algorithm assuming that the algorithm terminates. Now we show that the algorithm terminates. The claim is that the degree of r_i in y is strictly decreasing with each iteration of the algorithm. To see this, consider r_{i+1}.

$$r_{i+1} = b_m r_i - \text{LC}(r_i,y) f y^{\deg(r_i,y)-m}.$$

Now, the highest y-degree term in both $b_m r_i$ and $\text{LC}(r_i,y) f y^{\deg(r_i,y)-m}$ are both of degree $\deg(r_i,y)$, and they have the same coefficient. Hence these terms cancel, meaning that the degree of r_{i+1} in y is strictly less than that of r_i. Hence the algorithm does terminate. Part (ii) follows trivially. $\square$

The proof of Proposition 4.1 shows that if the variable x_i does not occur in f then $\deg(r, x_i)$ and $\deg(q, x_i)$ are less than or equal to $\deg(g, x_i)$.

Note that this algorithm outputs a unique q, r. However, if no restrictions (beyond being nonegative) are placed on the exponent s then there are not unique q, r such that $b_m^s g = qf + r$. In particular, q and r are unique if s is minimal(For a brief discussion of this, see Chapter 6 of [4]). For our purposes, it is enough that our algorithm outputs a unique q, r. Hence, we denote the remainder on pseudodivision (pseudoremainder) of f by g with respect to the variable y by $\text{prem}(f, g, y)$.

4.1.1 Successive Pseudodivision

The critical use of the pseudodivision algorithm comes in performing successive pseudodivision. Suppose that $f_1, \ldots, f_r$ are a set of hypothesis equations that are in triangular form, so that we can write them as:

$$\begin{aligned} f_1 &= f_1(u_1, \ldots, u_d, x_1) \\ f_2 &= f_2(u_1, \ldots, u_d, x_1, x_2) \\ &\vdots \\ f_r &= f_r(u_1, \ldots, u_d, x_1, \ldots, x_r). \end{aligned}$$

Let $g = g(u_1, \ldots, u_d, x_1, \ldots, x_r)$ be our conclusion equation. Performing successive pseudodivision simply involves the following: set $R_r = g$, $R_{r-1} = \text{prem}(R_r, f_r, x_r)$, $R_{r-2} = \text{prem}(R_{r-1}, f_{r-1}, x_{r-1}), \ldots$ etc. Continuing in this fashion, we get a final remainder $R_0 = \text{prem}(R_1, f_1, x_1)$. R_0 is called the final remainder upon successive pseudodivision of g by $f_1, \ldots, f_r$ and is denoted $\text{prem}(g, f_1, \ldots, f_r)$. We have the following result.

Proposition 4.2. *Suppose that the polynomials $f_1, \ldots, f_r$ are in triangular form and $g = g(u_1, \ldots, u_d, x_1, \ldots, x_r)$ is our conclusion. Let $R_0 = prem(g, f_1, \ldots, f_r)$ and let d_j be the leading coefficient of f_j as a polynomial in x_j. Then*

(i) There exist integers $s_1, \ldots, s_r \geq 0$ and polynomials $A_1, \ldots, A_r$ such that

$$d_1^{s_1} \cdots d_r^{s_r} g = A_1 f_1 + \cdots + A_r f_r + R_0$$

(ii) Either $R_0 = 0$ or $deg(R_0, x_i) < deg(f_i, x_i)$ for $i = 1, \ldots, r$.

Proof. To establish (i) and (ii) we use induction on r. If $r = 1$ then we are simply performing normal pseudodivision (see Proposition 4.1) and the result holds. Suppose that (i) and (ii) hold for $r - 1$, so that we have

$$d_1^{s_1} \cdots d_{r-1}^{s_{r-1}} R_{r-1} = A_1 f_1 + \cdots + A_{r-1} f_{r-1} + R_0$$

with $\deg(R_0, x_i) < \deg(f_i, x_i)$ for $i = 1, \ldots, r-1$. Now note that R_{r-1} can also be written $R_{r-1} = d_r^{s_r} g - A_r f_r$ and substitute this into the equation above. The result follows. □

Example For a simple illustration of this process consider the following system of equations in triangular form:

$$\begin{aligned} f_1 &= u_1 x_1 - u_1 u_3 \\ f_2 &= u_3 x_2 - (u_2 - u_1) x_1 \\ f_3 &= (u_3 x_2 - u_2 x_1 - u_1 u_3) x_3 + u_1 u_3 x_1 \\ f_4 &= u_3 x_4 - u_2 x_3 \end{aligned}$$

and let $g = 2u_2 x_4 + 2u_3 x_3 - u_3^2 - u_2^2$. Now if we perform successive pseudodivision on this system we get:

$$\begin{aligned} R_3 =& \text{prem}(g, f_4, x_4) = (2u_3^2 + 2u_2^2) x_3 - u_3^3 - u_2^2 u_3 \\ R_2 =& \text{prem}(R_3, f_3, x_3) = (-u_3^4 - u_2^2 u_3^2) x_1 + \\ & ((u_2 - 2u_1) u_3^3 + (u_2^3 - 2u_1 u_2^2) u_3) x_1 + u_1 u_3^4 + u_1 u_2^2 u_3^2 \\ R_1 =& \text{prem}(R_2, f_2, x_2) = (-u_1 u_3^4 - u_1 u_2^2 u_3^2) x_1 + u_1 u_3^5 \\ & + u_1 u_2^2 u_3^3 \\ R_0 =& \text{prem}(R_1, f_1, x_1) = 0. \end{aligned}$$

Since the final remainder upon successive pseudodivision is zero, we have shown that g follows from the hypothesis equations f_1, f_2, f_3, f_4.

Remark - We can still calculate $\text{prem}(g, f_1, \ldots, f_r)$ even if the f_i are not quite in triangular form. Specifically, as long as the leading variables in each f_i are distinct we can find $\text{prem}(g, f_1, \ldots, f_r)$ inductively by defining it to be $\text{prem}(\text{prem}(g, f_2, \ldots, f_r), f_1)$. The above remainder formula still holds. The reason for presenting successive pseudodivision in the context of a system in triangular form is that this will be the form our system will be in when actually performing Wu's Method (see the discussion of the Dimensionality Requirement following Definition 4.13).

4.2 Ascending Chains and Characteristic Sets

The next several sections focus on specifically how Wu's Method takes our hypothesis equations and transforms them into a triangular form. To do this we need to

discuss the notions of ascending chains and characteristic sets. First we introduce some notation: all polynomials under consideration are in $k[x_1, \ldots, x_n]$ (here we temporarily abandon our distinction between the u_i and x_i to simplify our notation). We say that the **class** of a polynomial f, denoted class(f), is the smallest integer c such that $f \in k[x_1, \ldots, x_c]$. If $f \in k$ then class(f) $= 0$. We call x_c the **leading variable** of f, denoted LV(f). Similarly, we say that LC(f) is the **leading coefficient** of f as a polynomial in x_c. We will sometimes refer to this coefficient as the **initial** of f. Also, the degree of f in its leading variable is denoted LD(f).

A polynomial g is **reduced** with respect to f if $\deg(g, x_c) < \deg(f, x_c)$ where class(f) $= c > 0$. In other words, $\text{prem}(g, f, x_c) = g$. Note that by our pseudo-division algorithm, $\text{prem}(g, f, x_c)$ is always reduced with respect to f. Also, for any finite set of polynomials, $f_1, f_2, \ldots, f_r$, we say that g is **reduced with respect** to $f_1, f_2, \ldots, f_r$ if $\deg(g, x_i) < \deg(f_i, x_i)$ for each $1 \leq i \leq r$ where x_i is the leading variable of each f_i.

The basic ideas introduced here are that ascending chains are polynomial sets that are close to being triangular, and characteristic sets will be defined to be "minimal" ascending chains in a sense to be explained below.

Definition 4.3. *Let $C = f_1, f_2, \ldots, f_r$ be a sequence of polynomials in $k[x_1, \ldots, x_n]$. It is a **quasi-ascending chain** if either*

(i) $r = 1$ and $f_1 \neq 0$ or,

(ii) $r > 1$ and $0 < class(f_1) < \cdots < class(f_r)$.

*We say that a quasi-ascending chain is an **ascending chain** if f_j is reduced with respect to f_i for all $i < j$.*

Note that in a quasi-ascending chain, f_j is automatically reduced with respect to f_i for all $i > j$. So in an ascending chain, f_j is reduced with respect to f_i for all $i \neq j$.

We will briefly illustrate this definition with a few examples.

Example The set $\{f_1 = y_1^5, f_2 = y_1^6 + y_2\}$ is not an ascending chain since the degree of f_2 in y_1 is greater than that in f_1 (it is still a quasi-ascending chain). However, the set $\{f_1 = y_1^2, f_2 = y_1 + y_2^3\}$ is an ascending chain.

Example If $f_1, \ldots, f_n$ is an ascending chain, then f_j is reduced with respect to f_i for all $i < j$. Specifically, this means that the variable x_i must appear with a lower degree in f_j than it does in f_i, for each $i < j$. In particular, this implies that the class variable of f_i appears to a lower degree in the initial of f_j. Hence, the initials of f_j are reduced with respect to f_i for $i < j$.

Example Additionally, if $f_1, \ldots, f_n$ is an ascending chain, then since the initials of the f_j are reduced with respect to all the previous elements of the ascending chain, then we must have that $\text{prem}(d_i, f_1, \ldots, f_n) \neq 0$ for $i = 1, \ldots, n$ (Here

d_i is the initial, or leading coefficient of f_i). This can be seen if we use the recursive definition of successive pseudodivision. Since d_i is reduced with respect to $f_1, \ldots, f_{i-1}$ we have that $\text{prem}(d_i, f_1, \ldots, f_{i-1}) = d_i$. And since d_i is clearly reduced with respect to the remaining polynomials in the ascending chain we get that $\text{prem}(d_i, f_1, \ldots, f_n) = d_i \neq 0$.

Now we define the following partial ordering on the ring $k[x_1, \ldots, x_n]$.

Definition 4.4. *Given $f, g \in k[x_1, \ldots, x_n]$ we say that $f < g$ (g is **higher**, or of **higher rank**) if either*

(i) $\text{class}(f) < \text{class}(g)$, or

(ii) $\text{class}(f) = \text{class}(g)$ and $\text{LD}(f) < \text{LD}(g)$.

*Polynomials f and g have the **same rank** if they are not comparable, i.e. if $\text{class}(f) = \text{class}(g)$ and $\text{LD}(f) = \text{LD}(g)$.*

Note that distinct polynomials may have the same rank.

Proposition 4.5. *The partial ordering $<$ defined above on $k[x_1, \ldots, x_n]$ is a well-ordering. In other words, under this ordering, every set has a (not necessarily unique) minimal element.*

Proof. Let $S \subseteq k[x_1, \ldots, x_n]$. If S contains an element of k, than this element is minimal. Otherwise, by the fact that the positive intergers are well-ordered, let S_1 be the subset of S consisting of polynomials of minimal class. Again, by the well-ordering of the positive integers, choose an element of S_1 of minimal leading degree. This is a minimal element of S. □

Now we use this ordering to define a partial order on ascending chains,

Definition 4.6. *Let $C = f_1, \ldots, f_r$ and $C_1 = g_1, \ldots, g_m$ be ascending chains. We say that $\mathbf{C < C_1}$ if either,*

(i) $\exists s \leq \min(r, m)$ such that f_i, g_i are of the same rank for $i < s$ and $f_s < g_s$, or

(ii) $m < r$ and f_i and g_i are of the same rank for $i \leq m$.

Not surprisingly, this ordering is also a well-ordering,

Proposition 4.7. *Let Γ be a set of ascending chains. Then Γ has a minimal element with respect to our ordering $<$ on ascending chains.*

Proof. By our well-ordering on polynomials defined above, we can let Γ_1 be the subset of Γ consisting of ascending chains whose first polynomials are minimal among

all the first polynomials in all ascending chains in Γ. If all the ascending chains in Γ_1 have only one polynomial, than any of them are minimal. Otherwise, define Γ_2 similarly as above: take the subset of Γ_1 whose second polynomials are minimal among all second polynomials in the ascending chains in Γ_1.
Repeat this process at most m times where m is the size of the largest ascending chain in Γ. Any of the ascending chains in Γ_m are minimal. □

An obvious use for a well-ordering on ascending chains is that it allows us to pick out a minimal ascending chain. In this way we introduce the idea of a characteristic set.

Definition 4.8. *Let S be a nonempty set of polynomials in $k[x_1, \ldots, x_n]$. A minimal ascending chain among all ascending chains formed by polynomials in S is called a* ***characteristic set****.*

If $C = f_1, \ldots, f_r$ is a characteristic set, then we say that g is reduced with respect to C if for each $f \in C$ with $\text{class}(f) = i$, $\deg(g, x_i) < \deg(f, x_i)$ for all $i = 1, \ldots, r$.

We are particularly interested in the algorithmic contruction of characteristic sets. The following two results will help us show that characteristic sets can be found algorithmically.

Proposition 4.9. *Let $C = f_1, \ldots, f_r$ be a characteristic set of the polynomial set S with class$(f_1) > 0$. Let g be a nonzero polynomial that is reduced with respect to C. Then $S_1 = S \cup \{g\}$ has a characteristic set less than C.*

Proof. If $\text{class}(g) \leq \text{class}(f_1)$ then the set $\{g\}$ is a characteristic set strictly lower than C. This is true since $g < f_1$.

Now suppose that $\text{class}(g) > \text{class}(f_1)$, and let $j = \max\{i \,|\, \text{class}(f_i) < \text{class}(g)\}$. So f_j is the "biggest" element of C that is still lower than than g. Then we claim that the set $f_1, \ldots, f_j, g$ is an ascending chain lower than C.

It is an ascending chain since we have that $\text{class}(f_1) < \cdots < \text{class}(f_j) < \text{class}(g)$ and each polynomial is reduced with respect to the previous polynomials (g is reduced with respect to C). It is lower than C since the polynomials are of the same rank except for $g < f_{j+1}$. □

Proposition 4.10. *Let $C = f_1, \ldots, f_r$ be an ascending chain in the polynomial set S with class$(f_1) > 0$. Then C is a characteristic set of S if and only if S contains no nonzero polynomials reduced with respect to C.*

Proof. First, suppose that C is a characteristic set of S. If there were some g in S reduced with respect to C then by Proposition 4.9, we can find a smaller ascending chain, contradicting the minimality of C.

To prove the opposite direction, suppose that C is not a characteristic set of S, i.e. there is a $C_1 = g_1, \ldots, g_m$ that is strictly lower than C. Now we have the following two cases;

Case 1 There exists $s \leq \min(r, m)$ with f_i, g_i having the same rank for $i < s$ and $g_s < f_s$. Then g_s is reduced with respect to all the preceding f_i's since they are of the same rank as the corresponding g_i's and g_s is reduced with respect to the other f_i's since $g_s < f_i$ for $i \geq s$.

Case 2 $r < m$ and f_i, g_i are of the same rank for $i \leq r$. Then g_{r+1} is reduced with respect to C.

So in either case there exists an element of S reduced with respect to C. □

Now we can say something about the actual construction of characteristic sets.

Theorem 4.11. *Every nonempty polynomial set S has a characteristic set. When S is finite, there is an algorithm for constructing this characteristic set.*

Proof. This first statement follows from the well-ordering property proved above. Suppose that S is finite, and let f_1 be a polynomial of minimal rank in S. If $\text{class}(f_1) = 0$ then the set f_1 is a characteristic set, so suppose further that $\text{class}(f_1) > 0$.

We can construct the set

$$S_1 = \{g \in S \mid g \text{ is reduced w/respect to } f_1\}$$

by computing $\deg(g, \text{LV}(f_1))$ for every $g \in S$. If S_1 is empty then f_1 is a characteristic set. Otherwise, every polynomial in S_1 is of higher class than f_1. Now let f_2 be a polynomial of minimal rank in S_1 and let S_2 be the set

$$S_2 = \{g \in S_1 \mid g \text{ is reduced w/respect to } f_2\}$$

If S_2 is empty then $\{f_1, f_2\}$ is a characteristic set. Otherwise repeat this process. Since S was finite, this process must terminate, yielding a characteristic set $\{f_1, \ldots, f_r\}$. □

We end this section by noting a property of characteristic sets for polynomial ideals.

Proposition 4.12. *Let $C = f_1, \ldots, f_r$ be a characteristic set of the ideal $I \lhd k[x_1, \ldots, x_n]$.*

(i) If $g \in I$ then prem$(g, f_1, \ldots, f_r) = 0$

(ii) If I is a prime ideal, then prem$(g, f_1, \ldots, f_n) = 0 \Rightarrow g \in I$.

Proof. First recall that finding pseudoremainders in this situation is still possible even though C may not be in triangular form. See the Remark at the end of Section 4.1.1.

(i) Let $g \in I$. By the properties of pseudodivision, we see that prem$(g, f_1, \ldots, f_r)$ $\in I$ and is reduced with respect to C. But by Proposition 4.10, it must be zero, for otherwise C would not be a characteristic set.

(ii) Let I be a prime ideal, and suppose that prem$(g, f_1, \ldots, f_r) = 0$. Again, by the properties of pseudodivision, we get that

$$d_1^{s_1} \cdots d_r^{s_r} g = A_1 f_1 + \cdots + A_r f_r$$

where d_i is the initial (leading coefficient) of f_i. Note that the d_i are in fact nonzero and reduced with respect to C (see the examples following Definition 4.3), so by Proposition 4.10 $d_i \notin I$. Hence $g \in I$.

□

4.2.1 Irreducible Ascending Chains

Recall that our goal is to develop a method for "triangulating" our system of hypotheses in such a way that we can use successive pseudodivision and Definition 3.21 to establish our geometric result. Our introduction of the concepts of ascending chains and characteristic sets has taken us a long way in that direction. However, recall our attempt to prove the geometric theorem in Example 1 using a Groebner basis. We discovered that we ran into difficulties if the variety defined by the hypotheses was reducible. In particular, we saw that we could factor several of the equations in the Groebner bases for this variety, and that this yielded subvarieties corresponding to degenerate conditions of our theorem.

Since the "triangular form" we've been heading towards involves ascending chains, we might attempt to investigate the irreducibility of polynomials in ascending chains. This suggests the following definition.

Definition 4.13. *Let $C = f_1, \ldots, f_r$ be an ascending chain with no constants and with each $f_i \in k[x_1, \ldots, x_n]$. Rename the variables x_i in such a way that we can write:*

$$\begin{aligned} f_1 &= f_1(u_1, \ldots, u_d, x_1) \\ f_2 &= f_2(u_1, \ldots, u_d, x_1, x_2) \\ &\vdots \\ f_r &= f_r(u_1, \ldots, u_d, x_1, \ldots, x_r) \end{aligned}$$

*so that $n = d + r$. An **irreducible ascending chain** is an ascending chain in the form above such that each $f_i \in C$ is irreducible in the ring $k(u_1, \ldots, u_d)[x_1, \ldots, x_i]/\langle f_1, \ldots, f_{i-1}\rangle$.*

Example The ascending chain $f_1 = x_1^2 - u_1, f_2 = x_2^2 - 2x_1x_2 + u_1$ is reducible since f_2 is reducible over $F_1 = \mathbb{Q}(u_1)[x_1]/\langle f_1\rangle$. In particular, $f_2 = (x_2 - x_1)^2$ where $x_1^2 = u_1$.

Notice that at this point we have resumed the distinction in variables between the dependent and independent coordinates. In practice, any relabeling of variables is rarely necessary, since most properly translated geometric theorems are in this form already. However, occasionally we may translate a theorem and find that some dependent coordinate x_i actually does not appear in any of our hypothesis equations.[3] This is the only situation in which relabeling the variables may be necessary. As Chou notes (see [1, pages 52-53]) this often implies that something deeper is taking place in the theorem then previously thought. In particular, a hidden hypothesis is usually to blame, as in Example 3. Reformulating the problem with this in mind generally solves the problem. Chou actually excludes this from occurring by adding what he calls a Dimensionality Requirement, which demands that each dependent variable, x_i actually occur as the leading variable in f_i in our ascending chain. We will follow Chou and assume this as well.

Remark 4.14 (Dimensionality Requirement)**.** *In an ascending chain, each dependent variable x_i must actually appear as the leading variable in the polynomial f_i.*

Some other notes on the above definition are necessary. First, the ideals $\langle f_1\rangle, \langle f_1, f_2\rangle$, etc. are in fact ideals in the ring $k(u_1, \ldots, u_d)[x_1]$, etc. So we are allowing denominators in the u_i. Second, if we do have an irreducible ascending chain C as above, then the following sequence forms a tower of field extensions

[3] As an example, consider the triangle $\triangle ABC$ with medians $\overline{AD}, \overline{BE}, \overline{CF}$. Let $G = \overline{AD} \cap \overline{BE}$ and let $H = \overline{CF} \cap \overline{AD}$. Finally, let P be a point on the line $\overline{GH}$. If we translate these hypotheses (there are ten) we will find that the ascending chain we obtain does not include the variable x_{10}. In this case, the cause is the fact that $G = H$ is always true.

$$\begin{aligned} F_0 &= k(u_1, \ldots, u_d) \\ F_1 &= F_0[x_1]/\langle f_1 \rangle \\ F_2 &= F_1[x_2]/\langle f_2 \rangle \\ &\vdots \\ F_r &= F_{r-1}[x_r]/\langle f_r \rangle, \end{aligned}$$

and each $f_i \in C$ may be considered as a polynomial in x_i over the field F_{i-1}. We have the following result on irreducible ascending chains.

Theorem 4.15. *Let $C = f_1, \ldots, f_r$ be an irreducible ascending chain as in Definition 4.13 and let $g \in k[u_1, \ldots, u_d, x_1, \ldots, x_r]$ and $F_r = k(u_1, \ldots, u_d)[x_1, \ldots, x_r]/\langle f_1, \ldots, f_r \rangle$. Then the following statements are equivalent:*

(i) $prem(g, f_1, \ldots, f_r) = 0$

(ii) Let E be any extension of the field k. If $\mu = (\tilde{u}_1, \ldots, \tilde{u}_d, \tilde{x}_1, \ldots, \tilde{x}_r) \in E^{d+r}$ is in $V(f_1, \ldots, f_r)$ with $\tilde{u}_1, \ldots, \tilde{u}_d$ transcendental over k, then $\mu \in V(g)$.

(iii) Viewed as an element of F_r, g is zero. In other words, the canonical image of g in F_r is 0.

(iv) There exist finitely many nonzero polynomials $c_1, \ldots, c_s \in k[u_1, \ldots, u_d]$ such that $c_1 \cdots c_s g$ belongs to the ideal in $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$ generated by $f_1, \ldots, f_r$.

First we must establish the following lemma.

Lemma 1. *Let $p = a_s x_m^s + \cdots + a_0$ be a polynomial with $1 \leq m \leq r$, $0 \leq s$, where the a_i are polynomials in $k[u_1, \ldots, u_d, x_1, \ldots, x_{m-1}]$, and suppose that p is reduced with respect to $f_1, \ldots f_r$. Then if μ from (ii) in Theorem 4.15 is a zero of p then p is in fact the zero polynomial.*

Proof. First note that the Lemma is trivial when $s = 0$, so we assume that $s \geq 1$. We use induction on m. Let $\tilde{p}$ denote the polynomial obtained upon substitution of μ. Suppose that $m = 1$. Then $p(\mu) = 0$ implies that

$$\tilde{p} = \tilde{a}_s \tilde{x}_1^s + \cdots + \tilde{a}_0 = 0$$

(recall that the a_i are polynomials as well, so we denote the substitution of μ in the a_i with a tilde). Since p is reduced with respect to f_1, we may assume that $s < \deg(f_1, x_1)$. Now recall the uniqueness of an algebraic expression in an extension of k (Theorem 3.2 (*iii*)). Specifically, if we evaluate f_1 only at the $\tilde{u}_i$'s, we get the

polynomial $f_1(\tilde{u}_1, \ldots, \tilde{u}_d, x_1)$ which is irreducible in the ring $k(\tilde{u}_1, \ldots, \tilde{u}_d)[x_1]$ and has a root $\tilde{x}_1$. So we can consider $\tilde{p}$ above to be in the extension field of k given by

$$k(\tilde{u}_1, \ldots, \tilde{u}_d)(\tilde{x}_1) \cong k(\tilde{u}_1, \ldots, \tilde{u}_d)[x_1]/\langle f_1(\tilde{u}_1, \ldots, \tilde{u}_d, x_1)\rangle$$

Then by the uniqueness of an expression equal to zero in this extension, we must have $\tilde{a}_j = 0$. But the $\tilde{u}_1, \ldots, \tilde{u}_d$ were chosen to be transcendental over k, so the only way the $\tilde{a}_j$ could evaluate to zero is if each a_j is the zero polynomial. Hence p is the zero polynomial.

Now assume that the Lemma holds for $m-1$, and let $p(\mu) = 0$ where $p = a_s x_m^s + \cdots + a_0$. Then we get that

$$\tilde{p} = \tilde{a}_s \tilde{x}_m^s + \cdots + \tilde{a}_0 = 0$$

Again, since $s < \deg(f_m, x_m)$ we can use the unique representation of an algebraic expression in an extension (using a similar argument as above) to conclude that all $\tilde{a}_j = 0$. So μ is a zero of all the a_j. Now note that each a_j is in fact reduced with respect to $f_1, \ldots, f_r$, so we can use the induction hypothesis on each to conclude that each a_j is the zero polynomial. Hence, p is the zero polynomial, as desired. □

Now we can prove the theorem using this lemma.

Proof. $(ii) \Rightarrow (i)$ Let μ be as in (ii) (such a μ always exists, consider for example the canonical images of $u_1, \ldots, u_d, x_1, \ldots, x_r$ in F_r viewed as an extension of k), and suppose that $g(\mu) = 0$. Let $R = \text{prem}(g, f_1, \ldots, f_r)$ so that we have

$$d_1^{s_1} \cdots d_r^{s_r} g = A_1 f_1 + \cdots + A_r f_r + R.$$

Hence $R(\mu) = 0$ (recall that $f_i(\mu) = 0$ for all i since $\mu \in V(f_1, \ldots, f_r)$). But by Proposition 4.2(ii), R is reduced with respect to $f_1, \ldots, f_r$ so we may invoke the Lemma to conclude that $R = 0$.

$(i) \Rightarrow (ii)$ Now suppose that $\text{prem}(g, f_1, \ldots, f_r) = 0$, so upon pseudodivision we have the equation

$$d_1^{s_1} \cdots d_r^{s_r} g = A_1 f_1 + \cdots + A_r f_r.$$

Since $f_1, \ldots, f_r$ is an ascending chain, it has the property that $\text{prem}(d_k, f_1, \ldots, f_r) \neq 0$ (see Example 3 following Definition 4.3). But by the proof of $(ii) \Rightarrow (i)$ this implies that $d_k(\mu) \neq 0$, which in turn implies that $g(\mu) = 0$.

$(i) \Leftrightarrow (iii)$ (iii) is a particular case of (ii) using μ defined as the canonical images of the variables $u_1, \ldots, u_d, x_1 \ldots, x_r$ as noted above in $(ii) \Rightarrow (i)$, and so our previous arguments give us $(iii) \Leftrightarrow (i)$.

$(iv) \Rightarrow (i)$ Suppose, as in (iv), there exist finitely many nonzero polynomials $c_1, \ldots, c_s \in k[u_1, \ldots, u_d]$ such that $c_1 \cdots c_s g \in \langle f_1, \ldots, f_r \rangle$, the ideal generated by the f_i in the ring $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$. Let μ be as in (ii). Then since the $\tilde{u}_i$ are transcendental over k and the c_i are nonzero we must have $c_i(\mu) \neq 0$. But $\mu \in V(f_1, \ldots, f_r)$, so we must have $g(\mu) = 0$. Hence, since $(ii) \Rightarrow (i)$, we can conclude that $\text{prem}(g, f_1, \ldots, f_r) = 0$.

$(i) \Rightarrow (iv)$ Suppose that $\text{prem}(g, f_1, \ldots, f_r) = 0$. In other words,

$$d_1^{s_1} \cdots d_r^{s_r} g = A_1 f_1 + \cdots + A_r f_r. \tag{1}$$

In the field $F_r = k(u_1, \ldots, u_d)[x_1, \ldots, x_r]/\langle f_1, \ldots, f_r \rangle$, we claim that $p = d_1^{s_1} \cdots d_r^{s_r}$ is not zero. If this were not the case, then we would have the formula

$$d_1^{s_1} \cdots d_r^{s_r} = Q_1 f_1 + \cdots + Q_r f_r$$

which implies that $\text{prem}(d_r, f_1, \ldots, f_r) = 0$. But this contradicts the fact that the initial d_r is reduced with respect to f_r.

This means that p has an inverse in F_r, or in other words that there is a $q \in k(u_1, \ldots, u_d)[x_1, \ldots, x_r]$ such that $qp - 1 \in \langle f_1, \ldots, f_r \rangle$ (viewed as an ideal in the ring $k(u_1, \ldots, u_d)[x_1, \ldots, x_r]$). So we have

$$qp - 1 = Q_1 f_1 + \cdots + Q_r f_r$$

Clearing denominators yields

$$q_1 p - c = \bar{Q}_1 f_1 + \cdots + \bar{Q}_r f_r$$

Where c involves only the variables $u_1, \ldots, u_d$. Now if we multiply (1) by q_1 we get

$$\begin{aligned} q_1(A_1 f_1 + \cdots + A_r f_r) &= d_1^{s_1} \cdots d_r^{s_r} g q_1 \\ &= p g q_1 \\ &= (\bar{Q}_1 f_1 + \cdots + \bar{Q}_r f_r + c) g \end{aligned}$$

Upon rearranging the last equation we see that $gc \in \langle f_1, \ldots, f_r \rangle$ as an ideal in the ring $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$. But c involves only the u_i, so we are done.

□

The point $\mu = (\tilde{u}_1, \ldots, \tilde{u}_d, \tilde{x}_1, \ldots, \tilde{x}_r)$ discussed in (ii) of the previous theorem is of particular importance, so we give it a name: any point $\mu \in E$ that is in $V(f_1, \ldots, f_r)$ with the $\tilde{u}_1, \ldots, \tilde{u}_d$ transcendental over k we call a **generic point** of the ascending chain $f_1, \ldots, f_r$ in an extension E of k. (Not to be confused with a *generic zero* discussed in Section 3.1.)

Proposition 4.16. *Let $f_1, \ldots, f_r$ be an irreducible ascending chain and g any polynomial. If prem$(g, f_1, \ldots, f_r) \neq 0$ then there are polynomials q, p with $p \neq 0$ such that $qg - p \in \langle f_1, \ldots, f_r \rangle$ and $p \in k[u_1, \ldots, u_d]$.*

Proof. If $\text{prem}(g, f_1, \ldots, f_r) \neq 0$ then we have that

$$d_1^{s_1} \cdots d_r^{s_r} g = A_1 f_1 + \cdots + A_r f_r + R, \tag{2}$$

where $R \neq 0$. As in the proof that $(i) \Rightarrow (iv)$ in Theorem 4.15, we conclude that R has an inverse in the ring

$$F_r = k(u_1, \ldots, u_d)[x_1, \ldots, x_r]/\langle f_1, \ldots, f_r \rangle$$

.

In other words we have that

$$Rq - 1 \in \langle f_1, \ldots, f_r \rangle \subset k(u_1, \ldots, u_d)[x_1, \ldots, x_r]$$

for some (rational) polynomial q. Now if we clear denominators we get

$$R\tilde{q} - c = Q_1 f_1 + \cdots + Q_r f_r \tag{3}$$

Note that since only q had a denominator, R remains unchanged and $c \in k[u_1, \ldots, u_d]$. Multiply equation (2) on both sides by $\tilde{q}$ to get

$$d_1^{s_1} \cdots d_r^{s_r} \tilde{q} g = \tilde{A}_1 f_1 + \cdots + \tilde{A}_r f_r + R\tilde{q}.$$

Now use equation (3) to rewrite $R\tilde{q}$ in the above equation, yielding

$$\bar{q} g - c = \bar{A}_1 f_1 + \cdots + \bar{A}_r f_r$$

which establishes the result. □

The following theorem gives us a method for transforming reducible ascending chains into irreducible ones while preserving most of our "triangular" properties.

Theorem 4.17. *Let $f_1, \ldots, f_r$ be an ascending chain. Suppose that $f_1, \ldots, f_{k-1}$ is irreducible, but that $f_1, \ldots, f_k$ is reducible. Then there exist polynomials g, h in the ring $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$ that are reduced with respect to $f_1, \ldots, f_r$ and such that class(g) = class(h) = class(f_k), and $gh \in \langle f_1, \ldots, f_k \rangle$.*

Proof. Suppose that f_k is reducible in the ring $F_{k-1}[x_k]$. Then we can factor f_k viewed as a member of the one variable polynomial ring $F_{k-1}[x_k]$ (this is often the most difficult computational hurdle in Wu's Method; we need factorization over algebraic extensions).

Hence there exist polynomials $g'', h'' \in k(u_1, \ldots, u_d)[x_1, \ldots, x_k]$ of positive degree in x_k such that $f_k - g''h'' = 0$ in $F_{k-1}[x_k]$. Specifically, we get an equation

$$f_k - g''h'' = A_m x_k^m + \cdots + A_0 \tag{4}$$

where each A_i belongs to $k(u_1, \ldots, u_d)[x_1, \ldots, x_{k-1}]$ and is zero in

$$F_{k-1} = k(u_1, \ldots, u_d)[x_1, \ldots, x_{k-1}]/\langle f_1, \ldots, f_{k-1} \rangle.$$

The equality in (4) still holds if we evaluate the right hand side at $x_k = 1$. Then clear denominators to get $Qf_k - g'h' = p$ where p is the resulting polynomial from the right hand side of (4) and p is a polynomial in $k[u_1, \ldots, u_d, x_1, \ldots, x_{k-1}]$ (since we evaluated at $x_k = 1$).

Now note that $p \equiv 0$ in the ring $F_{k-1}[x_k]$, so we can use $(iii) \Rightarrow (i)$ of Theorem 4.15 to conclude that $\text{prem}(p, f_1, \ldots, f_{k-1}) = 0$. Then a simple series of algebraic manipulations yields the following series of equations:

$$\begin{aligned} d_1^{s_1} \cdots d_{k-1}^{s_{k-1}} p &= Q_1 f_1 + \cdots + Q_{k-1} f_{k-1} \\ d_1^{s_1} \cdots d_{k-1}^{s_{k-1}} (Qf_k - g'h') &= Q_1 f_1 + \cdots + Q_{k-1} f_{k-1} \\ -(d_1^{s_1} \cdots d_{k-1}^{s_{k-1}}) g'h' &= Q_1 f_1 + \cdots + Q_{k-1} f_{k-1} - \tilde{Q} f_k. \end{aligned}$$

So we have that $(d_1^{s_1} \cdots d_{k-1}^{s_{k-1}}) g'h'$ is in the ideal $\langle f_1, \ldots, f_k \rangle$. Let

$$\begin{aligned} g &= \text{prem}((d_1^{s_1} \cdots d_{k-1}^{s_{k-1}}) g', f_1, \ldots, f_{k-1}) \\ h &= \text{prem}(h', f_1, \ldots, f_{k-1}). \end{aligned}$$

It is an easy calculation using the remainder formula from pseudodivision to check that $gh \in \langle f_1, \ldots, f_k \rangle$. Also, the properties of pseudoremainders ensure that g, h are both reduced with respect to $f_1, \ldots, f_{k-1}$. We noted above that g'', h'' were both reduced with respect to f_k. This implies that g', h' are as well, and in turn that g, h are reduced with respect to f_k. Since both g, h were obtained from f_k by factoring and division, the highest variable appearing in each must be x_k, so they must be reduced with respect to $f_{k+1}, \ldots, f_r$ since f_k was as well.

Finally, we need to check that $\text{class}(g) = \text{class}(h) = \text{class}(f_k)$. First, in the factorization of f_k, we must have that the class of both g'', h'' are the same as f_k. Second, when we rationalized the denominator, this contributed only u_i's, so the class of g', h' remained the same. Third, pseudodivision by $f_1, \ldots, f_{k-1}$ won't effect the appearance of x_k, so the class of g, h will remain the same. Hence g, h have all the desired properties. □

The usefulness of irreducible chains is illustrated by the following theorem.

Theorem 4.18. *Let $f_1, \ldots, f_r$ be an irreducible ascending chain and let P be defined by*

$$P = \{g \mid g \in k[u_1, \ldots, u_d, x_1, \ldots, x_r] \text{ and } prem(g, f_1, \ldots, f_r) = 0\}$$

Then the following assertions are true:

(i) P is a prime ideal with $f_1, \ldots, f_r$ as a characteristic set.

(ii) A generic point of $f_1, \ldots, f_r$ is a generic zero of P.

(iii) If k is algebraically closed, then a polynomial g vanishes on $V(P)$ if and only if $prem(g, f_1, \ldots, f_r) = 0$.

(iv) For any field k, $dim(V(P)) \geq d$ (the number of independent variables, u_i) where $V(P) = \{x \in k^n \mid f(x) = 0 \ \forall f \in P\}$. If $prem(g, f_1, \ldots, f_r) = 0$ then g vanishes on $V(P) \subseteq k^{d+r}$.

Proof. First recall a result from Section 3.1, Theorem 3.14. Let μ be a generic point of the irreducible ascending chain $f_1, \ldots, f_r$. Then by $(i) \Leftrightarrow (ii)$ in Theorem 4.15 we have that $P = \{g \mid g(\mu) = 0\}$. This establishes (ii), and also easily implies that P is in fact an ideal. So μ is a generic zero of the ideal P which by Theorem 3.14 mentioned above implies that P is in fact a proper prime ideal.

In addition, since everything in P has remainder of zero when divided by $f_1, \ldots, f_r$, we have that there are no nonzero polynomials in P that are reduced with respect to $f_1, \ldots, f_r$. Hence by Proposition 4.10 we see that $f_1, \ldots, f_r$ is in fact a characteristic set of P. This establishes (i).

If k is algebraically closed, then we have that $I(V(P)) = P$ by Theorem 3.17 and the fact that all prime ideals are radical. Hence a polynomial g vanishes on $V(P)$ if and only if $g \in P$, i.e. $\text{prem}(g, f_1, \ldots, f_r) = 0$. This establishes (iii).

If k is any field (not necessarily algebraically closed) then the dimension of $V(P)$ is the same as the dimension of its prime ideal $I(V(P))$. Note that $I(V(P)) \supset P$ so we have that $\dim I(V(P)) \geq \dim P$. Now, the dimension of the prime ideal P is the transcendence degree of the quotient field of $k[u_1, \ldots, u_d, x_1, \ldots, x_r]/P$ over k.

From the proof of $(ii) \Rightarrow (i)$ in Theorem 4.15 we know that the characteristic set $f_1, \ldots, f_r$ has a generic point μ, and by (ii) in the present theorem we see that μ is a generic zero of P. Then by Corollary 3.15 we see that

$$k[u_1, \ldots, u_d, x_1, \ldots, x_r]/P \cong k[\tilde{u}_1, \ldots, \tilde{u}_d, \tilde{x}_1, \ldots, \tilde{x}_r].$$

Since μ is a generic point, the $\tilde{u}_1, \ldots, \tilde{u}_d$ are algebraically independent over k. Hence the transcendence degree of the quotient field of $k[u_1, \ldots, u_d, x_1, \ldots, x_r]/P$ over k is at least d. Hence $\dim I(V(P)) \geq d$, so we have that $\dim V(P) \geq d$.

The remaining statement in (iv) follows easily from the fact that every prime ideal is radical and for any field we have $\sqrt{P} \subset I(V(P))$. □

We should note here what happens with $V(P)$ if k is not algebraically closed. In particular, we cannot conclude that the variety $V(P)$ is irreducible. This is troublesome because we wish to use characteristic sets and their prime ideals P in order to find an irreducible decomposition of the original variety defined by the hypothesis equations. However, we do have the following statement.

Proposition 4.19. *In the situation above, if $V(P)$ is of dimension d, then it is irreducible.*

Proof. Suppose that k is not algebraically closed, and that $V(P)$ is of dimension d. Let $V_1 \subset V(P)$ be a component of dimension d. Then if we take the ideal of both sides we get that $I(V_1) \supset I(V(P)) \supset P$. Now $I(V_1)$ is a prime ideal with dimension d and it contains P. We also have that the dimension of P is d, since the u_i's are assumed to be algebraically independent over P.

Now recall that the dimension of a prime ideal is also defined as the supremum of the lengths of chains of distinct prime ideals that contain it.

Hence we claim that $P = I(V_1) = P_1$. Specifically, if $P \neq P_1$ then the dimension of P_1 would be strictly smaller than that of P.

We conclude that $V(P) = V(P_1) = V_1$, so $V(P)$ is irreducible. □

We've seen that we can generate prime ideals from irreducible ascending chains. The following theorem allows us to move in the opposite direction.

Theorem 4.20. *Let P be a nontrivial prime ideal of $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$, and let $f_1, \ldots, f_r$ be a characteristic set of P. Then $f_1, \ldots, f_r$ is irreducible.*

Proof. From Proposition 4.12 we know that $P = \{g \mid \text{prem}(g, f_1, \ldots, f_r) = 0\}$. Suppose, to get a contradiction, that $f_1, \ldots, f_r$ is reducible. Then there is a $k > 0$ such that $f_1, \ldots, f_{k-1}$ is irreducible but $f_1, \ldots, f_k$ is reducible. By Theorem 4.17 we can find polynomials g, h such that they are reduced with respect to $f_1, \ldots, f_r$ and $gh \in \langle f_1, \ldots, f_k \rangle \subset P$ (also, the degrees of g, h in x_k are positive).

Since g, h are both reduced with respect to $f_1, \ldots, f_r$, we have that $\text{prem}(g, f_1, \ldots, f_r) \neq 0$ (the same is true of h as well). But this implies that neither are contained in P, while their product is in P. This contradicts P being a prime ideal. □

4.3 Ritt's Principle

Previously, our construction of characteristic sets always involved picking polynomials from the original polynomial set. Here we introduce a slight generalization, called an extended characteristic set, where the elements of the characteristic set are not necessarily in our original polynomial set, but they are in the ideal generated by our original polynomial set. The definition we have in mind is the following:

Definition 4.21. *Let $S = \{h_1, \ldots, h_m\}$ be a finite nonempty set of polynomials in the ring $k[x_1, \ldots, x_n]$, and let $I = \langle h_1, \ldots, h_m \rangle$. An **extended characteristic set** is an ascending chain C such that either*

(i) C consists of just an element of $k \cap I$, or

(ii) $C = \{f_1, \ldots, f_r\}$ with class$(f_1) > 0$ such that $f_i \in I$ and prem$(h_j, f_1, \ldots, f_r) = 0$ for all i, j.

Note the differences between this definition and our definition of characteristic sets. Before we only required that no element of S be reduced with respect to C, here we demand that the remainder actually is zero. Also, as noted above, here the elements of C may not come from S, although they will be in the ideal I.

We also note that every extended characteristic set of a polynomial set $S = \{h_1, \ldots, h_m\}$ is also a characteristic set of the ideal $I = \langle h_1, \ldots, h_m \rangle$.

Proposition 4.22. *Let $S = \{h_1, \ldots, h_r\}$ be a polynomial set in $k[x_1, \ldots, x_n]$, with extended characteristic set $C_e = f_1, \ldots, f_r$. Then C_e is also a characteristic set of the ideal $I = \langle h_1, \ldots, h_m \rangle$.*

Proof. If the extended characteristic set C_e consists of only an element from the field k, then I certainly doesn't contain any nonzero elements that are reduced with respect to C_e and so by Proposition 4.10, it is a characteristic set.

If C_e is not a trivial extended characteristic set, we proceed by contradiction. Suppose that $g \in I$ is a nonzero polynomial that is reduced with respect to C_e. Then we see that $\text{prem}(g, f_1, \ldots, f_r) = g$. We also know that $f_i \in I$ and that $\text{prem}(h_j, f_1, \ldots, f_r) = 0$ for all $i = 1, \ldots, r$ and all $j = 1, \ldots, m$. Hence for each $j = 1, \ldots, m$ we can write the equation

$$d_1^{s_{1j}} \cdots d_r^{s_{rj}} h_j = Q_{1j} f_1 + \cdots + Q_{rj} f_r. \tag{5}$$

Now let $\overline{s}_i = \max \{s_{ij} \,|\, j = 1, \ldots, m\}$. But from the fact that $g \in I$ we see that

$$g = A_1 h_1 + \cdots + A_m h_m$$

for some polynomials $A_1, \ldots, A_m$. Now multiply this equation on both sides by the polynomial $d_1^{\overline{s}_1} \cdots d_r^{\overline{s}_r}$, yielding

$$d_1^{\overline{s}_1} \cdots d_r^{\overline{s}_r} g = \overline{A}_1 \left(d_1^{s_{11}} \cdots d_r^{s_{r1}} h_1\right) + \cdots + \overline{A}_m \left(d_1^{s_{1m}} \cdots d_r^{s_{rm}} h_m\right)$$

Then by using the equations (for $j = 1, \ldots, m$) mentioned in (5) above we see that we can write g as

$$d_1^{\overline{s}_1} \cdots d_r^{\overline{s}_r} g = \overline{Q}_1 f_1 + \cdots + \overline{Q}_r f_r.$$

But this contradicts the fact g is reduced with respect to $f_1, \ldots, f_r$ noted above. Hence I must not contain any polynomials reduced with respect to C_e, and so C_e must be a characteristic set by Proposition 4.10. □

Theorem 4.23 (Ritt's Principle)**.** *Let $S = \{h_1, \ldots, h_m\}$ be a finite, nonempty set of polynomials in $k[x_1, \ldots, x_n]$, and let $I = \langle h_1, \ldots, h_m \rangle$. There is an algorithm to find an extended characteristic set C of S.*

Proof. By Theorem 4.11 we can construct a characteristic set C_1 of the polynomial set $S = S_1$. If C_1 contains only a constant, then we have (i) in Definition 4.21. Otherwise we expand S_1 by adding all nonzero remainders of elements of S_1 on pseudodivision by $C_1 = f_1, \ldots, f_r$ to get a new polynomial set S_2. Specifically, we find $\text{prem}(h_j, f_1, \ldots, f_r)$ for all j. If the remainder is nonzero we include it in S_2. If $S_1 = S_2$ then we are in (ii) of Definition 4.21. Otherwise repeat this process on S_2, yielding the characteristic set C_2. By Proposition 4.9 we know that S_2 has a

characteristic set that is strictly lower than C_1. Then the characteristic set found by our algorithm in Theorem 4.11 must be lower than C_1; i.e. we have that $C_1 > C_2$.

Repeating this process yields a sequence of polynomial sets

$$S_1 \subset S_2 \subset \cdots$$

and a corresponding decreasing sequence of characteristic sets

$$C_1 > C_2 \cdots$$

Since characteristic sets are well-ordered, this strictly decreasing chain must terminate, i.e. we must have that $S_k = S_{k+1}$ or C_k consisting of only a constant. We claim that in either case C_k has the properties in Definition 4.21. If C_k is only a constant, this is trivial.

By the construction of $C_k = f_1, \ldots, f_r$ we have that $\text{prem}(h_j, f_1, \ldots, f_r) = 0$ for all j. It remains to show that $f_i \in I$ for all i. We use induction to show that for all i, both $S_i \subset I$ and $C_i \subset I$. The base case ($i = 1$) is trivial. Now suppose that $C_i \subset I$ and $S_i \subset I$. To get the characteristic set C_{i+1} we add the nonzero remainders of elements of S_i upon pseudodivision by C_i. It is an easy consequence of the remainder formula for pseudodivision that this remainder also lies in I. This establishes the result. □

We emphasize here that this algorithm produced an increasing sequence of sets and a corresponding decreasing sequence of characteristic sets. When the algorithm terminates, we have a final characteristic set, which we call C and a final polynomial set which we call S'.

We need the following property of extended characteristic sets.

Proposition 4.24. *Let $S = \{h_1, \ldots, h_n\}$, and suppose that $C = f_1, \ldots, f_r$ is an extended characteristic set of S (with no constants). Let d_j denote the initials (leading coefficients) of the f_j and let $S_j = S \cup \{d_j\}$. Finally let $P = \{g \mid prem(g, f_1, \ldots, f_r) = 0\}$. Then we have that*

(i) $V(f_1, \ldots, f_r) - (V(d_1) \cup \cdots \cup V(d_r)) \subset V(P) \subset V(S) \subset V(f_1, \ldots, f_r)$

(ii) $V(S) = V(P) \cup V(S_1) \cup \cdots \cup V(S_r)$

Proof. (i) Let $p \in V(f_1, \ldots, f_r) - (V(d_1) \cup \cdots \cup V(d_r))$. Then we have that $f_i(p) = 0$ but $d_i(p) \neq 0$ for all i. For any $g \in P$ we have by pseudodivision the following formula,

$$d_1^{s_1} \cdots d_r^{s_r} g = Q_1 f_1 + \cdots + Q_r f_r$$

and this forces us to conclude that $g(p) = 0$. So $p \in V(P)$. The same reasoning using the pseudoremainder property of extended characteristic sets shows that $p \in V(S)$.

(ii) First we claim that $V(S) \subset V(P) \cup (V(d_1) \cup \cdots \cup V(d_r))$. To see this note that using (i) we get:

$$\begin{aligned} V(S) \subset V(f_1, \ldots, f_r) &\Rightarrow V(S) - (V(d_1) \cup \cdots \cup V(d_r)) \subset V(f_1, \ldots, f_r) - \\ &\qquad (V(d_1) \cup \cdots \cup V(d_r)) \\ &\Rightarrow V(S) - (V(d_1) \cup \cdots \cup V(d_r)) \subset V(P) \\ &\Rightarrow V(S) \subset V(P) \cup (V(d_1) \cup \cdots \cup V(d_r)) \,. \end{aligned}$$

Now suppose that $p \in V(S)$. Then by the claim above, p is contained in $V(P) \cup (V(d_1) \cup \cdots \cup V(d_r))$. Then $p \in V(P)$ or $p \in V(d_j)$ for some j. In either case, we have $V(S) \subset V(P) \cup V(S_1) \cup \cdots \cup V(S_r)$, since $V(S \cup \{d_j\}) = V(S_j)$.

Now suppose that $p \in V(P) \cup V(S_1) \cup \cdots \cup V(S_r)$. If $p \in V(S_j)$ for some j, then clearly $p \in V(S)$. And finally, if $p \in V(P)$, then we have $p \in V(S)$ by (i).

□

4.4 Ritt's Decomposition Algorithm

Now we are ready to present Ritt's full algorithm for completely decomposing varieties. Recall the situation presented in Section 2. We have a collection of hypotheses $h_1, \ldots, h_r$ and a conclusion equation g, all in the polynomial ring $k[u_1, \ldots, u_d, x_1, \ldots, x_r]$. Our method depends upon deciding if g vanishes on the irreducible components of the variety $V(h_1, \ldots, h_r)$ that do not correspond to degenerate cases of our theorem.

Theorem 4.25. *Let S be a finite nonempty polynomial set in the ring $k[x_1, \ldots, x_n]$. There is an algorithm to determine whether $\langle S \rangle = k[x_1, \ldots, x_n]$ or otherwise to decompose the variety,*

$$V(S) = V(P_1) \cup \cdots \cup V(P_s)$$

where each P_i is the prime ideal given by an irreducible characteristic set as in Theorem 4.18 (i).

Proof. Let D be a set of characteristic sets, which to begin our algorithm is empty. We can apply Theorem 4.23 to the polynomial set S to get an extended characteristic set C and also the corresponding polynomial set S' (the final polynomial set in the increasing sequence that arose in the algorithm in Ritt's Principle). Then we have the following cases:

Case 1 C consists of just a constant. In this case we conclude that $V(S)$ is empty and $\langle S\rangle = k[x_1,\ldots,x_n]$.

Case 2 $C = \{f_1,\ldots,f_r\}$ is an irreducible ascending chain. Let d_k be the initials of the f_k, and let $S_k = S' \cup \{d_k\}$. Then by (ii) of Proposition 4.24 we have that

$$V(S) = V(P_1) \cup V(S_1) \cup \cdots \cup V(S_r)$$

where P_1 is the prime ideal with characteristic set C, so that

$$P_1 = \{g \mid \mathrm{prem}(g, f_1,\ldots,f_r) = 0\}$$

by Theorem 4.18 (i). Then by Proposition 4.9 we know that each S_k has a characteristic set strictly lower than C.

Add the characteristic set C to D and repeat this algorithm on each S_k.

Case 3 $C = \{f_1,\ldots,f_r\}$ is a reducible ascending chain. Specifically, there is a $k > 0$ such that $f_1,\ldots,f_{k-1}$ is irreducible but $f_1,\ldots,f_k$ is reducible. In this case we use Theorem 4.17 (here we need to be able to factor polynomials over algebraic extensions) to conclude that there are polynomials g, h, both of the same class as f_k and reduced with respect to $f_1,\ldots,f_r$ such that

$$gh \in \langle f_1,\ldots,f_k\rangle$$

We claim that $V(S) = V(S') = V(S_1) \cup V(S_2)$ where $S_1 = S' \cup \{g\}$ and $S_2 = S' \cup \{h\}$.

Since $S \subset S'$ we have that $V(S) \supset V(S')$. To establish the opposite containment it suffices to show that $V(S_i) \subset V(S_{i+1})$ for all i in the algorithm outlined in Ritt's Principle (Theorem 4.23).

Let $p \in V(S_i)$, where S_i is a polynomial set in the increasing sequence generated in the algorithm for Ritt's Principle. The polynomials that are in S_{i+1} but not in S_i are all remainders given by the formula

$$d_{1_i}^{s_{1_i}} \cdots d_{m_i}^{s_{m_i}} g = Q_{i_1} h_{1_i} + \cdots + Q_{i_r} h_{m_i} + R$$

where $g \in S_i$ and $h_{1_i},\cdots,h_{m_i}$ is the characteristic set of S_i. Now, $g(p) = 0$ and we also must have that $h_{j_i}(p) = 0$ for all j since $h_{j_i} \in S_i$ (by our construction of characteristic sets). But this forces $R(p) = 0$. Hence $V(S) \subset V(S')$ and we have the opposite containment.

Now note that $V(S_1) \cup V(S_2) \subset V(S')$ is trivial, so let $p \in V(S') = V(S)$. This means that $p \in V(f_1,\ldots,f_r)$. But we know that

$$gh \in \langle f_1,\ldots,f_k\rangle$$

so we must have either $g(p) = 0$ or $h(p) = 0$. Hence $p \in V(S_1) \cup V(S_2)$. This establishes the claim.

Now repeat this algorithm on S_1 and S_2.

The above algorithm only adds characteristic sets to D that are strictly lower than the previous ones. Hence this process must terminate in one of the following two cases:

(i) $D = \emptyset$. In this case $V(S) = \emptyset$ and $\langle S \rangle = k[x_1, \ldots, x_n]$.

(ii) $D = \{C_1, \ldots, C_s\}$ and $V(S) = V(P_1) \cup \cdots \cup V(P_s)$ where each P_k is the prime ideal given by a characteristic set C_k.

□

5 Using Wu's Method to Prove Theorems

Now we wish to use Ritt's Decomposition algorithm to describe a method for actually proving geometric theorems. To see how this is done, first recall from the end of Chapter 3 our definition of what it means for a conclusion g to follow generically from $h_1, \ldots, h_r$:

Definition 5.1. *A conclusion g **follows generically** from the hypotheses $h_1, \ldots, h_r$ if $g \in I(V') \subset k[u_1, \ldots, u_d, x_1, \ldots, x_r]$ where V' is the union of those irreducible components of $V(h_1, \ldots, h_r)$ on which the u_i are algebraically independent.*

The idea is to first apply Ritt's Decomposition algorithm to our hypotheses. This will yield a collection of extended characteristic sets, $D = \{C_1, \ldots, C_s\}$, which correspond to components of $V(h_1, \ldots, h_r)$ defined by the prime ideals $P_1, \ldots, P_s$. Note that if k is algebraically closed, we may conclude that these varieties are irreducible, but that if k is not algebraically closed we may not.

We wish to pick out those irreducible $V(P_i)$ on which the u_i's are algebraically independent. (In other words, we are looking for the P_i that do not contain any nonzero u-polynomials.) Identifying on which components the u_i are independent is simple: we pick those $V(P_i)$ such that the corresponding extended characteristic set C_i contains no polynomials involving only the u_i's.

To see that this is sufficient, consider some C_k that contains no polynomials only in the u_i. Suppose that some u-polynomial $g \in P_k$. This implies that $\text{prem}(g, C_k) = 0$, which is impossible, since g must be reduced with respect to C_k.

It is possible that of the components on which the u_i are algebraically independent, some have dimension higher than d. (Recall that in Theorem 4.18 (iv) we only proved that $\dim V(P) \geq d$.) However, as Chou notes ([1] p. 47) this is very rare. He observes that among the 600 theorems proved by his implementation, none had any components that fit this description. Thus, we will treat this occurrence as a degenerate condition (as Chou does), and ignore these components with dimension greater than d.

The remaining components are all of dimension d, so by Proposition 4.19 we know that they are irreducible.

Recall that we have assumed that the C_k, which are irreducible ascending chains, all satisfy the Dimensionality Requirement (See Remark 4.14). In other words we are requiring that each of the x_i's actually appear as the leading variable of a polynomial in our ascending chain. If they do not, and some dependent variable x_i is missing, we should reexamine the translation of the problem.

Let $\text{prem}(g, C_k)$ denote successive pseudodivision of g by the elements of the characteristic set C_k. Now, by (iv) of Proposition 4.18, we know that if $\text{prem}(g, C_k) = 0$ then g vanishes on $V(P_k)$, the component of $V(h_1, \ldots, h_n)$ corresponding to C_k.

Hence to check the conditions in the definition above simply find $\text{prem}(g, C_k)$ for each C_k that does not contain a polynomial involving only the u_i. If in each case the pseudoremainder is zero, then g follows generally from $h_1, \ldots, h_n$.

This last comment omitted an important exception. When we find each pseudoremainder, we get an expression of the form

$$d_1^{s_1} \cdots d_r^{s_r} g = Q_1 f_1 + \cdots + Q_r f_r + R.$$

So in order to conclude that g does indeed vanish on the component of $V(h_1, \ldots, h_r)$ corresponding to this characteristic set we must additionally assume that each $d_j \neq 0$. These comprise our nondegenerate conditions for our geometric theorem. This discussion establishes the following result

Theorem 5.2. *Let $h_1, \ldots, h_r, g$ be as above and let $D = \{C_1, \ldots, C_s\}$ be just those extended characteristic sets obtained from Ritt's Decomposition algorithm on which the u_i are algebraically independent. Then if $\text{prem}(g, C_k) = 0$ for all k then g is generically true under the degenerate conditions $d_j \neq 0$, where the d_j are the initials of the polynomials in each C_k.*

It may be that we get a pseudoremainder of zero on some but not all of the components in the above theorem. In this case the formulation of the geometric theorem should be reexamined for errors or hidden hypotheses. However, if we get a nonzero remainder on every component in the above theorem, then we may safely conclude that g is generally false.

We note again that we have assumed throughout that our hypothesis (and hence all resulting characteristic sets) satisfy the Dimensionality Requirement (Remark 4.14), since a failure to meet this condition usually implies a need to reformulate the theorem.

Finally, as noted by Chou ([1, page 54]), it is very rare that Ritt's Decomposition algorithm will yield more than one characteristic set. Specifically, it is usually the

case that the variety V' in Definition 5.1 above is actually irreducible.

A Implementing Wu's Method in Maple

We present in this appendix some very basic Maple code that performs the essential elements of Wu's Method. If the reader is interested, a more extensive implementation was created by Dongming Wang in the Maple package CharSet. For our purposes, we wish only to implement the basic parts of Ritt's Decomposition algorithm.

We begin with some very simple procedures that we will need as tools later on in Ritt's Algorithm. First we have a procedure that returns the class of a given polynomial.

```
class:= proc(p::polynom,depvars::list)
        local V,test,i;
        V:=indets(p);
        V:=V[];
        V:=[V];
        V:=sort(V);
        for i from 0 to nops(depvars)-1 do
              if member(depvars[nops(depvars)-i],V)
                       then RETURN(nops(depvars)-i);
              fi;
        od;
        RETURN(0);
end;
```

In general, our code requires the input of the dependent variables, i.e. the x_i. This is not a terribly restrictive requirement, since a human must typically translate the theorem. Next, recall that we discussed an ordering on polynomials using the notion of class. Hence we have a procedure that compares two polynomials and returns TRUE if the first is less than the second:

```
PolyCompare:= proc(f::polynom,g::polynom,depvars::list)
              if class(f,depvars) < class(g,depvars) then
                      RETURN(true);
              elif class(f,depvars)=class(g,depvars) then
                      i:=class(f,depvars);
                      if degree(f,depvars[i])< degree(g,depvars[i]) then
                               RETURN(true);
                      else RETURN(false);
                      fi;
              else RETURN(false);
```

```
              fi;
end;
```

Now in the algorithm described in Theorem 4.11 we have a sequence of polynomial sets from which we must select the least polynomial. Our next procedure performs this task on a polynomial set.

```
LeastPoly:=proc(S::list,depvars::list)
               if nops(S)=1 then
                      RETURN(S[1]);
               fi;
               i:=1;
               j:=1;
               counter:=1;
               IsLeastPoly:=false;
               while IsLeastPoly = false do
                      if i=jthen
                            j:=j+1;
                            counter:=counter+1;
                      elif PolyCompare(S[j],S[i],depvars)=true then
                            i:=j;
                            j:=1;
                            counter:=1;
                      else
                            counter:=counter+1;
                            j:=j+1;
                      fi;
                      if counter=nops(S)+1 then
                            IsLeastPoly:=true;
                      fi;
               od;
               RETURN(S[i]);
end;
```

The algorithm in Theorem 4.11 also requires that we decide whether one polynomial is reduced with respect to another. So we introduce a procedure that performs this simple task.

```
Reduced:=proc(f::polynom,g::polynom,depvars::list)
             gClass:=class(g,depvars);
             fDegree:=degree(f,depvars[gClass]);
             gDegree:=degree(g,depvars[gClass]);
             if fDegree< gDegree then
                       RETURN(true);
             else
```

```
                        RETURN(false);
            fi;
end;
```

Now we are ready to write a procedure that performs the algorithm in Theorem 4.11. Since our implementation is intended to be used on geometric theorems, we have ignored the possibility that our starting polynomial set may contain a constant. This in general will not occur in a properly translated theorem. The following procedure yields a characteristic set of a given polynomial set (as usual we require the input of the list of independent variables).

```
CharSet:=proc(S::list,depvars::list)
         C:=[];
         S1:=S;
         SCopy:=S;
         isCharSet:=false;
         while isCharSet=false do
               C:=[op(C),LeastPoly(SCopy,depvars)];
               S1:=[];
               for j from1 to nops(SCopy) do
                         isReduced:=true;
                         for i from1 to nops(C) do
                                   Check:=Reduced(SCopy[j],C[i],depvars);
                                   if Check=falsethen
                                                isReduced:=false;
                                   fi;
                         od;
               if isReduced=true then
                         S1:=[op(S1),SCopy[j]];
               fi;
               od;

               if nops(S1)=0 then
                         isCharSet:=true;
               fi;
               SCopy:=S1;
         od;
         RETURN(C);
end;
```

Before we present the code for producing an extended characteristic set, we need procedures that perform successive pseudodivision. For completeness, we include both a version that handles polynomials that are in triangular form and another that performs the recursively defined version mentioned at the end of Section 4.1.1. We call them SuccessivePrem and RecursivePrem respectively.

```
SuccessivePrem:=proc(g,L::list,depvars::list)
          local i,R;
          R:=g;
          for ifrom  0 to nops(L)-1 do
               R:=prem(R,L[nops(depvars)-i],depvars[nops(depvars)-i]);
          od;
end;
```

```
RecursivePrem:=proc(g::polynom,S::list,depvars::list)
   r:=g;
   for ifrom 0 to nops(S)-1 do
        r:=prem(r,S[nops(S)-i],depvars[eval(class(S[nops(S)-i],depvars))]);
   od;
   RETURN(r);
end;
```

Now we have the tools necessary to write a procedure that performs the algorithm described in Ritt's Principle. This procedure takes a set of polynomials (and the list of independent variables) and returns an extended characteristic set.

```
ExtCharSet:=proc(S::list,depvars::list)
                S1:=S;
                S2Unchanged:=false;
                S2:=[];

                while S2Unchanged=false do
                C1:=CharSet(S1,depvars);
                counter:=0;
                       for i from 1 to nops(S1) do
                             r:=RecursivePrem(S1[i],C1,depvars);
                             if member(r,C1) then
                             fi;
                             if r<>0then
                                     S2:=[op(S2),r];
                                     counter:=counter+1;
                             fi;
                       od;
                       if counter=0 then
                             S2Unchanged:=true;
                       fi;
                       S1:=[op(S1),op(S2)];
                od;
                RETURN(C1);
end;
```

Obviously, this procedure does not check if the resulting extended characteristic set is irreducible. This can certainly be done, as Maple has numerous tools for factoring polynomials. However, we were more interested in the implementation of algorithms for producing characteristic sets than in algorithms for factoring polynomials. Also, as we've noted before, in most cases in plane geometry the resulting extended characteristic set will indeed be irreducible. If this is not the case, the user can easily check each polynomial in the extended characteristic set for factorability, and then repeat the process on each resulting polynomial set using the code above.

We have tested our code on the following examples: (These examples were drawn from theorems proven mechanically by Chou's implementation in [1]. Our implementation differs somewhat from his, so the extended characteristic sets found in these examples may be different than in [1].) Also, in all of these examples, the characteristic set is irreducible.

Example 1 Let $ABCD$ be a square, with $\overline{CG}$ parallel to $\overline{BD}$. Construct a point E on $\overline{CG}$ such that $\overline{BE} \equiv \overline{BD}$. F is the intersection of $\overline{BE}$ and $\overline{DC}$. Then $\overline{DF} \equiv \overline{DE}$.

If we let $A = (0,0), B = (u_1,0), C = (u_1,u_1), D = (0,u_1), E = (x_1,x_2)$ and $F = (x_3,u_1)$, then we can express the hypotheses as $h_1 = x_2^2 + x_1^2 - 2u_1x_1 - u_1^2, h_2 = -u_1x_2 - u_1x_1 + 2u_1^2, h_3 = -x_2x_3 + u_1x_2 + u_1x_1 - u_1^2$. The conclusion is given by $g = x_3^2 - x_2^2 + 2u_1x_2 - x_1^2 - u_1^2$. Using the code above, our calculations in Maple are as follows:

```
> S1:=[x2^2+x1^2-2*u1*x1-u1^2,-u1*x2-u1*x1+2*u1^2,
-x2*x3+u1*x2+u1*x1-u1^2]:
> g:=x3^2-x2^2+2*u1*x2-x1^2-u1^2:
> C:=ExtCharSet(S1,[x1,x2,x3]);
```

$$[2u1^2x1^2 - 6u1^3x1 + 3u1^4, -u1x2 - u1x1 + 2u1^2, -u1^3 - u1x1x3 + 2u1^2x3]$$

```
> SuccessivePrem(g,C,[x1,x2,x3]);
                                0
```

Recall from our discussions above that this means we have proven this theorem under certain degenerate conditions. Specifically, these degenerate conditions are the leading coefficients of the polynomials in the extended characteristic set C. So the theorem is true under the conditions:

$$\begin{aligned} 2u_1^2 &\neq 0 \\ -u_1 &\neq 0 \\ 2u_1^2 - u_1x_1 &\neq 0. \end{aligned}$$

Under these restrictions, the above theorem holds. For example, the first condition requires that A and B are distinct points.

Example 2 We use the same situation as in Example 1 in Section 2. Then we get the following calculations in Maple:

```
> S1:=[x2-u3,(x1-u1)*u3-x2*u2,x4*x1-x3*u3,x4*(u2-u1)-(x3-u1)*u3]:
> g:=x1^2-2*x1*x3-2*x4*x2+x2^2:
> C:=ExtCharSet(S1,[x1,x2,x3,x4]);
```

$$[u3\,x1 - u1\,u3 - u3\,u2,\, x2 - u3,\, 2u1\,u3^2x3 - u1^2u3^2 - u3^2u2\,u1,$$
$$-u1^2u3^4 - u3^4u2\,u1 + 2u1^2u3^3x4 + 2u1\,u3^3x4\,u2]$$

```
> SuccessivePrem(g,C,[x1,x2,x3,x4]);
                                    0
```

The degenerate conditions are:

$$u_3 \neq 0$$
$$2u_1u_3^2 \neq 0$$
$$2u_1^2u_3^3 + 2u_1u_3^3u_2 \neq 0.$$

Example 3 Next we present Pascal's Theorem, as translated in [1]. Let O be a circle, and let A, B, C, D, E, F be points on O. Let $P = \overline{AB} \cap \overline{DF}, Q = \overline{BC} \cap \overline{FE}$ and $S = \overline{CD} \cap \overline{EA}$. Then the points P, Q and S are collinear. If we let $A = (0,0), O = (u_1, 0), B = (x_1, u_2), C = (x_2, u_3), D = (x_3, u_4), F = (x_4, u_5), E = (x_5, u_6), P = (x_7, x_6), Q = (x_9, x_8)$ and finally $S = (x_{11}, x_{10})$, then we get the following system of equations:

$$\begin{aligned}
h_1 &= x_1^2 - 2u_1x_1 + u_2^2 = 0\\
h_2 &= x_2^2 - 2u_1x_2 + u_3^2 = 0\\
h_3 &= x_3^2 - 2u_1x_3 + u_4^2 = 0\\
h_4 &= x_4^2 - 2u_1x_4 + u_5^2 = 0\\
h_5 &= x_5^2 - 2u_1x_5 + u_6^2 = 0\\
h_6 &= (u_5 - u_4)x_7 + (-x_4 + x_3)x_6 + u_4x_4 - u_5x_3 = 0\\
h_7 &= u_2x_7 - x_1x_6 = 0\\
h_8 &= (u_6 - u_5)x_9 + (-x_5 + x_4)x_8 + u_5x_5 - u_6x_4 = 0\\
h_9 &= (u_3 - u_2)x_9 + (-x_2 + x_1)x_8 + u_2x_2 - u_3x_1 = 0\\
h_{10} &= u_6x_{11} - x_5x_{10} = 0\\
h_{11} &= (u_4 - u_3)x_{11} + (-x_3 + x_2)x_{10} + u_3x_3 - u_4x_2 = 0\\
g &= (x_8 - x_6)x_{11} + (-x_9 + x_7)x_{10} + x_6x_9 - x_7x_8 = 0.
\end{aligned}$$

Then Maple gives us the following:

```
> S4:=[x1^2-2*u1*x1+u2^2,x2^2-2*u1*x2+u3^2,x3^2-2*u1*x3+u4^2,
x4^2-2*u1*x4+u5^2,x5^2-2*u1*x5+u6^2,(u5-u4)*x7+(-x4+x3)*x6+u4*x4-
u5*x3,u2*x7-x1*x6,(u6-u5)*x9+(-x5+x4)*x8+u5*x5-u6*x4,(u3-u2)*x9+
(-x2+x1)*x8+u2*x2-u3*x1,u6*x11-x5*x10,(u4-u3)*x11+(-x3+x2)*x10+
u3*x3-u4*x2]:
> g:=(x8-x6)*x11+(-x9+x7)*x10+x6*x9-x7*x8:
> C:=ExtCharSet(S4,[x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11]);
```

$$C = [x1^2-2u1\,x1+u2^2, x2^2-2u1\,x2+u3^2, x3^2-2x3\,u1+u4^2, x4^2-2u1\,x4+u5^2,$$
$$x5^2-2u1\,x5+u6^2, -x1\,x6\,u5+x1\,x6\,u4+u2\,x6\,x4-u2\,x6\,x3-u2\,u4\,x4+u2\,u5\,x3,$$
$$-x1\,u5^2x7+2x1\,u5\,x7\,u4-x1\,u5\,u4\,x4+x1\,u5^2x3-x1\,u4^2x7+x1\,u4^2x4-x1\,u4\,u5\,x3+$$
$$u2\,x4\,x7\,u5-u2\,x4\,x7\,u4-u2\,x3\,x7\,u5+u2\,x3\,x7\,u4, -u6\,x8\,x2+u6\,x8\,x1+u6\,u2\,x2-$$
$$u6\,u3\,x1+u5\,x8\,x2-u5\,x8\,x1-u5\,u2\,x2+u5\,u3\,x1+x8\,x5\,u3-x8\,x5\,u2-x8\,x4\,u3+$$
$$x8\,x4\,u2-u5\,x5\,u3+u5\,x5\,u2+u6\,x4\,u3-u6\,x4\,u2, -x1\,u5^2x5+x1\,u5^2x9+u5^2x2\,x5-$$
$$u5^2x2\,x9-u6^2x1\,x4+u6^2x1\,x9+u6^2x2\,x4-u6^2x2\,x9+x1\,u5\,u6\,x4+x5\,u3\,x9\,u6-$$
$$x5\,u3\,x9\,u5-x5\,u2\,x9\,u6+x5\,u2\,x9\,u5-x4\,u3\,x9\,u6+x4\,u3\,x9\,u5+u2\,x4\,x9\,u6-$$
$$u2\,x4\,x9\,u5+u6\,u2\,x2\,x5-u6\,u2\,x2\,x4-u6\,u3\,x1\,x5+u6\,u3\,x1\,x4-u5\,u2\,x2\,x5+$$
$$u5\,u2\,x2\,x4+u5\,u3\,x1\,x5-u5\,u3\,x1\,x4+2u6\,x2\,x9\,u5-u6\,x2\,u5\,x5-2u6\,x1\,x9\,u5+$$
$$u6\,x1\,u5\,x5-u5\,x2\,u6\,x4, -u6\,x10\,x3+u6\,x10\,x2+u6\,u3\,x3-u6\,u4\,x2+x5\,x10\,u4-$$
$$x5\,x10\,u3, -u6^2x11\,x3+u6^2x11\,x2+u6\,x11\,x5\,u4-u6\,x11\,x5\,u3+x5\,u6\,u3\,x3-$$
$$x5\,u6\,u4\,x2]$$

```
> SuccessivePrem(g,C,[x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11]);
                                    0
```

The degenerate conditions are:

$$\begin{aligned}
-x_1u_5 + x_1u_4 + u_2x_4 - u_2x_3 &\neq 0\\
-x_1u_5^2 + 2x_1u_5u_4 - x_1u_4^2 + u_2x_4u_5 - u_2x_4u_4 - u_2x_3u_5 + u_2x_3u_4 &\neq 0\\
-u_5x_1 + u_5x_2 - x_4u_3 + x_5u_3 - u_6x_1 + x_4u_2 &\neq 0\\
x_1u_5^2 + u_6x_4u_2 - u_5^2x_2 + \cdots - 2u_6x_1u_5 - u_6^2x_2 &\neq 0\\
-u_6x_3 + u_6x_2 + x_5u_4 - x_5u_3 &\neq 0\\
u_6x_5u_4 - x_5u_3u_6 - u_6^2x_3 + u_6^2x_2 &\neq 0.
\end{aligned}$$

Example 4 This example uses the same theorem as in Example 2 in Section 2 which stated that the altitudes of a triangle all meet in a single point (called the orthocenter). As we saw in that example our hypotheses and conclusion equations are given by:

$$\begin{aligned} h_1 &= x_2u_2 - x_1u_3 = 0 \\ h_2 &= x_4(u_2 - u_1) - u_3(x_3 - u_1) = 0 \\ h_3 &= x_2u_3 + u_2(x_1 - u_1) = 0 \\ h_4 &= x_4u_3 + x_3(u_2 - u_1) = 0 \\ h_5 &= (x_2 - x_5)(x_1 - u_1) - x_2(x_1 - u_2) = 0 \\ h_6 &= x_6x_3 - x_4u_2 = 0 \\ g &= x_5 - x_6 = 0. \end{aligned}$$

When entered into Maple we get the following calculations:

```
> S1:=[x2*u2-x1*u3,x4*(u2-u1)-u3*(x3-u1),
x2*u3+u2*(x1u1),x4*u3+x3*(u2-u1),
(x2-x5)*(x1-u1)-x2*(x1-u2),x6*x3-x4*u2]:
> g:=x5-x6:
> C:=ExtCharSet(S1,[x1,x2,x3,x4,x5,x6]);
```

$$C = [-u2^2u1 + u2^2x1 + u3^2x1, u2^3x2 + u2x2u3^2 - u2^2u1u3, x3u2^2 - 2u2x3u1 + x3u1^2 + u3^2x3 - u3^2u1, u2^3x4 - 3u2^2u1x4 + u2^2u1u3 + 3u2u1^2x4 - 2u2u1^2u3 - u1^3x4 + u1^3u3 + u3^2u2x4 - u3^2u1x4, u3^2u1x5u2 + u3u1u2^3 - u3u1^2u2^2, u3u1u2^3 - 2u3u1^2u2^2 + u3u1^3u2 + u2x6u1u3^2 - u3^2u1^2x6]$$

```
> SuccessivePrem(g,C,[x1,x2,x3,x4,x5,x6]);
                                0
```

The degenerate conditions are:

$$\begin{aligned} u_2^2 + u_3^2 &\neq 0 \\ u_2^3 + u_2u_3^2 &\neq 0 \\ u_2^2 - 2u_2u_1 + u_1^2 + u_3^2 &\neq 0 \\ u_2^3 - 3u_2^2u_1 + 3u_2u_1^2 - u_1^3 + u_3^2u_2 - u_3^2u_1 &\neq 0 \\ u_3^2u_1u_2 &\neq 0 \\ u_2u_1u_3^2 - u_3^2u_1^2 &\neq 0. \end{aligned}$$

Example 5 Here we prove the well known theorem due to Pappus. Let A, B, C and A', B', C' be two sets of collinear points. Then let $P = \overline{AB'} \cap \overline{A'B}$, $Q = \overline{AC'} \cap \overline{A'C}$ and finally let $R = \overline{BC'} \cap \overline{B'C}$. Then the points P, Q, R are collinear.

For our translation, let $A = (0,0), B = (u_1, 0), C = (u_2, 0), A' = (u_3, u_4), B' = (u_5, u_6), C' = (u_7, x_1), P = (x_2, x_3), Q = (x_4, x_5), R = (x_6, x_7)$. Note that

the point C' is partially dependent on our choices of A, B, A', B', so one of its coordinates is x_1. Then we have the following seven hypotheses and conclusion:

$$\begin{aligned}
h_1 &= (u_6 - u_4)(u_7 - u_3) - (x_1 - u_4)(u_5 - u_3) \\
h_2 &= x_3u_5 - u_6x_2 \\
h_3 &= u_4(x_2 - u_1) - x_3(u_3 - u_1) \\
h_4 &= x_5u_7 - x_1x_4 \\
h_5 &= x_5(u_3 - u_2) - u_4(x_4 - u_2) \\
h_6 &= x_7(u_7 - u_1) - x_1(x_6 - u_1) \\
h_7 &= u_6(x_6 - u_2) - x_7(u_5 - u_2) \\
g &= (x_5 - x_3)(x_6 - x_2) - (x_7 - x_3)(x_4 - x_2).
\end{aligned}$$

In Maple, this translation yields the following:

```
> pappus:=[(u6-u4)*(u7-u3)-(x1-u4)*(u5-u3),x3*u5-u6*x2,u4*(x2-u1)-
x3*(u3-u1),
x5*u7-x1*x4,x5*(u3-u2)-u4*(x4-u2),x7*(u7-u1)-x1*(x6-u1),u6*(x6-u2)-
x7*(u5-u2)]:
> c:=(x5-x3)*(x6-x2)-(x7-x3)*(x4-x2):
> C:=ExtCharSet(pappus,[x1,x2,x3,x4,x5,x6,x7]);
```

$$C = [(u6 - u4)\,(u7 - u3) - (x1 - u4)\,(u5 - u3)\ldots]$$

```
> SuccessivePrem(c,C,[x1,x2,x3,x4,x5,x6,x7]);
                                    0
```

The (extremely large) set C has been omitted for space reason. Here the degenerate conditions are:

$$\begin{aligned}
-u_5 + u_3 &\neq 0 \\
u_5u_4 - u_6u_3 + u_6u_1 &\neq 0 \\
u_5^2u_4 - u_5u_6u_3 + u_5u_6u_1 &\neq 0 \\
-u_5u_7u_4 + u_6u_7u_3 - u_6u_7u_2 - u_6u_3^2 + u_6u_3u_2 + u_4u_7u_2 + u_4u_5u_3 - u_4u_5u_2 &\neq 0 \\
u_7^2u_4u_5^2 - u_5u_7^2u_6u_3 + \cdots + u_7^2u_6u_3^2 - u_3u_7^2u_6u_3 &\neq 0 \\
u_5u_6u_3 - u_6u_7u_3 + \cdots + u_4u_5u_2 - u_6u_3u_2 &\neq 0.
\end{aligned}$$

Example 6 Finally, we include an example in which we discovered an error in Chou's proof of Simson's Theorem as presented in [1]. Chou states the theorem as follows: Let D be a point on the circumscribed circle (with center O) of triangle ABC. From D draw three perpendiculars to the sides of the triangle,

$\overline{BC}, \overline{CA}, \overline{AB}$. Let E, F, G be the three feet respectively. Then E, F, G are collinear.

Chou translates the theorem as follows: let $A = (0,0), B = (u_1, 0), C = (u_2, u_3), O = (x_2, x_1), D = (x_3, x_4), E = (x_5, x_4), F = (x_7, x_6), G = (x_3, 0)$. The hypotheses are:

$h_1 = 2u_2x_2 + 2u_3x_1 - u_3^2 - u_2^2 = 0$	$\overline{OA} \equiv \overline{OC}$
$h_2 = 2u_1x_2 - u_1^2 = 0$	$\overline{OA} \equiv \overline{OB}$
$h_3 = -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0$	$\overline{OA} \equiv \overline{OD}$
$h_4 = u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0$	E, B, C collinear
$h_5 = (u_2 - u_1)x_5 + u_3x_4 + (-u_2 + u_1)x_3 - u_3u_4$	$\overline{DE} \perp \overline{BC}$
$h_6 = u_3x_7 - u_2x_6 = 0$	F, A, C collinear
$h_7 = u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0$	$\overline{DF} \perp \overline{AC}$

and the conclusion is given by $g = x_4x_7 + (-x_5 + x_3)x_6 - x_3x_4 = 0$. Chou then triangulates these hypotheses yielding the irreducible ascending chain:

$$f_1 = 4u_1u_3x_1 - 2u_1u_3^2 - 2u_1u_2^2 + 2u_1^2u_2 = 0$$
$$f_2 = 2u_1x_2 - u_1^2 = 0$$
$$f_3 = -x_3^2 + 2x_2x_3 + 2u_4x_1 - u_4^2 = 0$$
$$f_4 = (-u_3^2 - u_2^2 + 2u_1u_2 - u_1^2)x_4 + (u_2 - u_1)u_3x_3 + u_3^2u_4 + (-u_1u_2 + u_1^2)u_3 = 0$$
$$f_5 = u_3x_5 + (-u_2 + u_1)x_4 - u_1u_3 = 0$$
$$f_6 = (-u_3^2 - u_2^2)x_6 + u_2u_3x_3 + u_3^2u_4 = 0$$
$$f_7 = u_2x_7 + u_3x_6 - u_2x_3 - u_3u_4 = 0.$$

However, it is easy to verify using Maple that successive pseudodivision on this set of equations does not yield a remainder of zero, as it should. We believe that Chou's error lies in his translation of the problem. His construction of the point $D = (x_3, u_4)$ is incorrect. If one constructs each point of the triangle ABC in succession, then we are left in a serious difficulty in constructing D. The coordinates for D are only partially restricted by our choices for the coordinates of A, B and C. In particular, we must have that x_3 doesn't force D to lie beyond our circle. Hence, x_3 cannot really be completely determined from the previous points.

Instead, we translated the theorem as follows: Let A, C, B, D be four point on a circle centered at O. From D draw three perpendiculars to the sides of the triangle ABC: $\overline{BC}, \overline{CA}, \overline{AB}$. Let E, F, G be the three feet respectively. Then E, F, G are collinear.

Our version is clearly equivalent, and yields the following translation: $A = (0,0), O = (u_1, 0), B = (x_1, u_2), C = (x_2, u_3), D = (x_3, u_4), E = (x_4, x_5), F = (x_6, x_7), G = (x_8, x_9)$. This gives us the following nine hypotheses:

$$
\begin{aligned}
h_1 &= u_1^2 - (x_1 - u_1)^2 - u_2^2 = 0 && \overline{AO} \equiv \overline{BO} \\
h_2 &= u_1^2 - (x_2 - u_1)^2 - u_3^2 = 0 && \overline{AO} \equiv \overline{CO} \\
h_3 &= u_1^2 - (x_3 - u_1)^2 - u_4^2 = 0 && \overline{AO} \equiv \overline{DO} \\
h_4 &= -x_4 u_2 + x_5 x_1 = 0 && E, A, B \text{ collinear} \\
h_5 &= x_6(u_3 - x_7) + x_7(x_6 - x_2) = 0 && A, F, C \text{ collinear} \\
h_6 &= (x_1 - x_8)(x_9 - u_3) - (u_2 - x_9)(x_8 - x_2) = 0 && B, G, C \text{ collinear} \\
h_7 &= -(x_3 - x_4)x_1 - (u_4 - x_5)u_2 = 0 && \overline{DE} \perp \overline{AB} \\
h_8 &= (x_3 - x_6)x_2 + (u_4 - x_7)u_3 = 0 && \overline{DF} \perp \overline{AC} \\
h_9 &= (x_3 - x_8)(x_1 - x_1) + (u_4 - x_9)(u_2 - u_3) = 0 && \overline{DG} \perp \overline{BC}
\end{aligned}
$$

and the conclusion is given by $g = (x_4 - x_6)(x_7 - x_9) - (x_5 - x_7)(x_6 - x_8) = 0$. Using these equations, we get the extended characteristic set:

```
> Simsons:=[u1^2-(x1-u1)^2-u2^2,u1^2-(x2-u1)^2-u3^2,u1^2-
(x3-u1)^2-u4^2,-x4*u2+x5*x1,x6*(u3-x7)+x7*(x6-x2),(x1-x8)*
(x9-u3)-(u2-x9)*(x8-x2),(x3-x4)*(-x1)+(u4-x5)*(-u2),(x3-x6)*x2
+(u4-x7)*u3,(x3-x8)*(x1-x2)+(u4-x9)*(u2-u3)]:
> SimsonConclusion:=(x4-x6)*(x7-x9)-(x5-x7)*(x6-x8):
> C:=ExtCharSet(Simsons,[x1,x2,x3,x4,x5,x6,x7,x8,x9]));
```

C=[$u1^2-(x1-u1)^2-u2^2$, $u1^2-(x2-u1)^2-u3^2$, $u1^2-(x3-u1)^2-u4^2$, $x1\,u2\,u4+2x1\,u1\,x3-2x1\,u1\,x4-u2^2x3$, $-x1\,u2^2u4-2u2\,x1\,u1\,x3+u2^3x3+4u1^2x5\,x1-2u1\,x5\,u2^2$,
$x2\,u3\,u4+2x2\,u1\,x3-2x2\,u1\,x6-u3^2x3$, $x2\,u3^2u4+2u3\,x2\,u1\,x3-u3^3x3-4u1^2x7\,x2+2u1\,x7\,u3^2$, $-2x1\,x2\,x3+2x1\,x8\,x2+x1\,u2\,u4-x1\,u3\,u4-x2\,u2\,u4+x2\,u3\,u4-x1\,u3\,u2+x1\,u3^2+2x8\,u3\,u2+u2^2x2-u2\,x2\,u3+2x2\,u1\,x3-2x2\,u1\,x8-u3^2x3+2x1\,u1\,x3-2x1\,u1\,x8-u2^2x3$, $-4x2\,u1^2u2+2u2\,x1\,u1\,x3-2u3\,x2\,u1\,x3-2x1\,x2\,x3\,u2+2x1\,x2\,x3\,u3-2x1\,u2\,u4\,u3+2x2\,u2\,u4\,u3+2x2\,u1\,x3\,u2-2x1\,u1\,x3\,u3+2u3\,u2\,x1\,x9-2u3\,u2\,x9\,x2-2x2\,u1\,x1\,u3+2x1\,u1\,u2\,x2+x1\,u2^2u4-u2^3x3+u3^3x3-x2\,u3^2u4-x1\,u3^3+u2^3x2+x1\,u3^2u4-x2\,u2^2u4-x1\,u3\,u2^2-2x1\,u3^2u2+u2\,x2\,u3^2+2u2^2x2\,u3-u3^2x3\,u2+u2^2x3\,u3+4x2\,u1^2x9+2u3^2x1\,x9+2u3^2u1\,u2-2u3^2u1\,x9-4x1\,u1^2x9+4x1\,u1^2u3-2u2^2x9\,x2+2u2^2u1\,x9-2u2^2u1\,u3$]

And then under successive pseudodivision we get:

```
> SuccessivePrem(SimsonConclusion,C,[x1,x2,x3,x4,x5,x6,x7,x8,x9]);
                                    0
```

References

[1] Shang-Ching Chou. *Mechanical Geometry Theorem Proving*, D. Reidel Publishing Company, Dordrecht, Holland, 1988.

[2] Shang-Ching Chou. "Proving Elementary Geometry Theorems Using Wu's Algorithm", in *Automated Theorem Proving: After 25 years*, Edited by W.W. Bledsoe and D. Loveland, AMS Contemporary Mathematics Series **29** (1984), 243-286.

[3] S.C. Chou and W.F. Schelter, "Proving Geometry Theorems with Rewrite Rules", *Journal of Automated Reasoning*, 2(4) (1986), 253-273.

[4] David Cox, John Little, Donal O'Shea. *Ideals, Varieties, and Algorithms*, 2nd Edition, Springer-Verlag, New York, NY, 1997.

[5] T.W. Hungerford, *Algebra*, Springer-Verlag,1978.

[6] D. Kapur, "Geometry Theorem Proving Using Hilbert's Nullstellensatz", in Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation, 202-208.

[7] B. Kutzler and S. Stifter, "Automated Geometry Theorem Proving Using Buchberger's Algorithm", in Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation, 209-214.

[8] Bhubaneswar Mishra. *Algorithmic Algebra*, Springer-Verlag, New York, NY, 1993.

[9] B. H. Träger, "Algebraic Factoring and Rational Function Integration", Proceedings of 176 ACM Symposium On Symbolic and Algebraic Computation, 1976, 219-226.

[10] B. L. Van Der Waerden, *Modern Algebra*, English Edition, Frederick Ungar Publishing Company, 1948.