On the Dimension of an Arbitrary Ascending Chain

Xiao-Shan Gao
Institute of Systems Science, Academia Sinica, Beijing 100080
Shang-Ching Chou
Department of Computer Sciences
University of Texas at Austin, Austin Texas 78712, USA

1993

Abstract

We show that the length of an arbitrary ascending chain has geometric meaning and hence describes certain natural properties for the ascending chain. The results proved in this paper can be used to enhance the efficiency of the Ritt-Wu's decomposition algorithm and to obtain an *unmixed decomposition* for an algebraic variety more easily.

Keywords. Ascending chain, dimension of a variety, Ritt-Wu's decomposition, unmixed decomposition.

We know that the dimension for an irreducible ascending chain ASC is a crucial concept in Ritt-Wu's constructive theory of algebraic geometry [WU1]. We can also define the dimension for an arbitrary ascending chain similarly. But one may say that this definition has no geometric meaning. In this paper, we will show that the dimension of an arbitrary ascending chain does have geometric meaning and hence describes certain natural properties for the ascending chain. The results proved in this paper can be used to enhance the efficiency of the Ritt-Wu's decomposition algorithm and to obtain an unmixed decomposition for an algebraic variety more easily.

1. The Dimension of an Arbitrary Ascending Chain

Let K be a field of characteristic zero and $K[y_1, ..., y_n]$ or $K[y]$ be the ring of polynomials for the variables $y_1, ..., y_n$. All polynomials in this paper are in $K[y]$ unless explicitly mentioned otherwise. Let P be a polynomial. The *class* of P, denoted by $class(P)$, is the largest p such that some y_p actually occurs in P. If $P \in K$, $class(P) = 0$. Let a polynomial P be of class $p > 0$. The coefficient of the highest power of x_p in P considered as a polynomial of x_p is called the *initial* of P. For polynomials P and G with $class(P) > 0$, let $prem(G; P)$ be the *pseudo remainder* of G wrpt (ab. with respect to) P [WU1].

A sequence of polynomials $ASC = A_1, ..., A_p$ is said to be a *quasi ascending chain*, if either $r = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \leq i < j$. ASC is called *nontrivial* if $class(A_1) > 0$. A quasi ascending chain $ASC = A_1, ..., A_p$ is called an *ascending chain* if either ASC is trivial or A_j is of higher degree than A_i $(i = j+1, ..., p)$ in y_{n_j} where $n_j = class(A_j)$.

For a non-trivial quasi ascending chain $ASC = A_1, ..., A_p$ and a polynomial G, we define the pseudo remainder of G wrpt ASC inductively as

$$prem(G; ASC) = prem(prem(G; A_p); A_1, ..., A_{p-1}).$$

Let $R = prem(G; ASC)$, then we have the following important *remainder formula* [WU1]:

$$JG - R \in Ideal(A_1, ..., A_p) \tag{1.1}$$

where J is a product of the initials of the polynomials in ASC and $Ideal(A_1, ..., A_p)$ is the ideal generated by $A_1, ..., A_p$.

Definition 1.1. The dimension of a quasi ascending chain $ASC = A_1, ..., A_p$ is defined to be $DIM(ASC) = n - p$.

For a quasi ascending chain $ASC = A_1, ..., A_p$, let A_i be of class m_i, then we call $\{y_1, ..., y_n\} - \{y_{m_1}, ..., y_{m_p}\}$ the *parameter set* of ASC. Thus $DIM(ASC)$ is equal to the number of parameters of ASC.

Definition 1.2. For a quasi ascending chain ASC, we define

$$QD(ASC) = \{g \mid \exists J, Jg \in Ideal(ASC)\}$$

where J is a product of powers of the initials of the polynomials in ASC.

It is obvious that $QD(ASC)$ is an ideal. By (1.1), we have that if $prem(P; ASC) = 0$ then $P \in QD(ASC)$. Let PS and DS be polynomial sets. For an algebraic closed extension field E of K, let

$$Zero(PS) = \{x = (x_1, ..., x_n) \in E^n \mid \forall P \in PS, P(x) = 0\}$$

and $Zero(PS/DS) = Zero(PS) - \cup_{g \in DS} Zero(g)$.

Theorem 1.3. Let $ASC = \{A_1, ..., A_r\}$ be a non-trivial quasi ascending chain, $J = \{I_1, ..., I_r\}$ where I_i are the initials of A_i. Then either $Zero(ASC/J)$ is empty or

$$Zero(ASC/J) = \cup_{1 \leq i \leq l} Zero(QD(ASC_i)/J)$$

where each ASC_i is *irreducible* and with the same parameter set as ASC. (For the concept of irreducible ascending chain, see [WU1]).

Proof. It is a direct consequence of Theorem 4.4 in [CG1] and the affine dimension theorem (p48, [HA1]). ∎

If ASC is an irreducible ascending, then it is known that $QD(ASC)$ is a prime ideal of dimension $DIM(ASC)$ [WU1]. A variety whose irredundant components have the same dimension is called an *unmixed or pure variety.* Theorem 1.3 means that $Zero(ASC/J)$

is contained in an unmixed variety of dimension $DIM(ASC)$. Moreover, this unmixed variety satisfies a property that all its components have the same parameter set. We call such a variety a *parameter unmixed variety.*

2. An Unmixed Decomposition for $QD(ASC)$

For a polynomial set PS, let $M(PS)$ be the multiplicative set generated by PS, i.e. the products of the powers of finite polynomials in PS. For two polynomial sets PS and DS, let

$$QD(PS:DS) = \{g \in K[y] \mid \exists J \in M(DS), Jg \in Ideal(PS)\}$$

then it is obvious that $QD(ASC) = QD(ASC:J)$ where J is the initial set of ASC.

Theorem 2.1. For two polynomial sets $PS = \{f_1, ..., f_k\}$ and $DS = \{d_1, ..., d_s\}$ in $K[y]$, let $PD = Ideal(PS, d_1 z_1 - 1, \cdots, d_s z_s - 1)$ in $K[y, z_1, ..., z_s]$ where z_i are new variables. Then $QD(PS:DS) = PD \cap K[y]$.

Proof. For $P \in QD(PS:DS)$, there is a $J = d_1^{n_1} \cdots d_s^{n_s} \in M(DS)$ such that $JP \in Ideal(PS)$. Note that $(z_i d_i)^{n_i} \equiv 1 \; mod \; PD$, then we have $z^{n_1} \cdots z_s^{n_s} JP \equiv \prod_{i=1}^{s} (z_i d_i)^{n_i} P \equiv P \equiv 0 \; mod \; PD$, i.e., $P \in PD$. We have proved $QD(PS:DS) \subset PD \cap K[y]$. For the other direction, let $P \in PD \cap K[y]$, then $P = \sum B_i f_i + \sum C_i(z_i d_i - 1)$ for some polynomials B_i and C_i in $K[y, z]$. Set $z_i = 1/d_i$ and clear the denominators. We have $JP = \sum B_i' f_i$ where $J \in M(DS)$, i.e., $P \in QD(PS:DS)$. ∎

Theorem 2.1 together with the following result give a method to compute a basis for $QD(PD:DS)$.

Lemma 2.2. (Lemma 6.8 in [BU1]) For an ideal $ID \subset K[x_1, ..., x_n, y_1, ..., y_k]$, if GB is a Gröbner basis of ID under the pure lexicographic ordr $x_1 < ... < x_n < y_1 < ... < y_k$ then $GB \cap K[x_1, ..., x_n]$ is a Gröbner basis of $ID \cap K[x_1, ..., x_n]$.

Let G be a polynomial ideal and S be a multiplicative polynomial set, the fraction of G by S is defined to be $S^{-1}G = S \times G/\sim$ where $\sim$ satisfies that $(s, a) \sim (s', a')$ iff $sa' = s'a$. Certain elements of $S^{-1}G$ can be treated like polynomials. Here, we always treat (s, sa) and a as the same element (for more details, see [AM1]).

Theorem 2.3. Let $S = M(DS)$, then $QD(PS:DS) = (S^{-1}Ideal(PS)) \cap K[y]$.

Proof. Define a map $\phi : QD(PS:DS) \to (S^{-1}Ideal(PS)) \cap K[y]$ by setting $\phi(P) = (J, JP)$ where $J \in S$ satisfies $JP \in Ideal(PS)$. It is easy to see that ϕ is a well defined injective map. By the explanation in the previous paragraph, an elements in $(S^{-1}Ideal(PS)) \cap K[y]$ must have the form (J, JP) where $J \in S$ and $JP \in Ideal(PS)$. Thus $P \in QD(PS:DS)$, and therefore ϕ is also surjective. ∎

The following result permits us to obtain the irreducible components of $QD(PS:DS)$ from PS and DS directly using Ritt-Wu's decomposition algorithm.

Theorem 2.4. For polynomial sets PS and DS in $K[y]$,

$$Zero(PS/DS) = \cup_{i=1}^{m} Zero(QD(ASC_i)/DS)$$

is an irreducible irredundant decomposition for $Zero(PS/DS)$ iff

$$Zero(QD(PS:DS)) = \cup_{i=1}^{m} Zero(QD(ASC_i))$$

is an irreducible irredundant decomposition for $Zero(QD(PS:DS))$.

Proof. This theorem comes from the following lemma and Theorem 2.1 immediately. ▮

Lemma 2.5. For polynomial sets PS and $DS = \{d_1, ..., d_s\}$ in $K[y]$, let $PD = Ideal(PS,$ $d_1z_1 - 1,\ ...\ ,d_sz_s - 1)$ where z_i are new variables. If

$$Zero(PS/DS) = \cup_{i=1}^{m} Zero(QD(ASC_i)/DS) \tag{A.1}$$

is an irreducible irredundant decomposition for $Zero(PS/DS)$, then we have an irredundant decomposition for $Zero(PD)$

$$Zero(PD) = \cup_{i=1}^{m} Zero(QD(ASC_i')) \tag{A.2}$$

where $ASC_i' = ASC_i, d_1z_1 - 1, \cdots, d_sz_s - 1$, and vice versa.

Proof. Suppose we have (A.1). Note that the pseudo remainders of the generators of PD w.r.p ASC_i' are zero, then by (1.1) we have $PD \subset QD(ASC_i')$, $i = 1, ...m$. One direction of (A.2) is proved. For the other direction, let $\eta = (x', z_1', ..., z_s')$ be a zero of $Zero(PD)$, then $d_i(x')z_i' - 1 = 0$ which implies $d_i(x') \neq 0$, $i = 1, ..., s$. Thus $x' \in Zero(PS/DS)$, and hence $x' \in Zero(QD(ASC_i)/DS)$ for some i, say $i = 1$. We will prove $\eta \in Zero(QD(ASC_1'))$. Let $h \in QD(ASC_1')$, then $Jh = P + \sum C_i(z_id_i - 1)$, where $P \in QD(ASC_1)$ and J is a product of the the powers of some d_i. As the $d_i(x') \neq 0$, then η is a zero of h. Hence (A.2) is true. It is similar to derive (A.1) from (A.2) ▮

We now give some properties for $QD(ASC)$. First, the algorithm to compute a finite basis of the prime ideal $QD(ASC)$ for an irreducible ascending chain ASC in p85 [CH1] can be generalized to the following form.

Theorem 2.6. For a quasi ascending chain ASC in $K[y]$, let $ID = Ideal(ASC, I_1z_1 - 1, \cdots, I_pz_p - 1)$ in $K[y, z]$, where I_i are the initials of the polynomials in ASC and z_i are new variables, then $QD(ASC) = ID \cap K[y]$.

Proof. Since $QD(ASC) = QD(ASC : J)$, this is a direct consequence of Theorem 2.1. ▮

A finite basis of $QD(ASC)$ can be found by Lemma 2.2.

Theorem 2.7. For a quasi ascending chain ASC in $K[y]$, either $Zero(QD(ASC))$ is empty, or we have

$$Zero(QD(ASC)) = \cup_i Zero(QD(ASC_i))$$

where each ASC_i is irreducible and has the same parameter set as ASC.

Proof. This is a consequence of Theorem 1.3 and Theorem 2.4. ▮

Theorem 2.7 shows that $Zero(QD(ASC))$ is a parameter unmixed variety for an arbitrary ascending chain ASC.

3. Applications

Theorem 2.6 and Theorem 2.7 provide more information for Ritt-Wu's decomposition algorithm. For example, if we need an unmixed decomposition for a variety as in [CA1], i.e., to decompose a variety into the union of some unmixed varieties, then we need only to get a coarse decomposition using Ritt-Wu's decomposition algorithm.

Theorem 3.1. [WU2] (Ritt-Wu's Zero Decomposition Algorithm: the Coarse Form) For two finite sets of polynomials PS and DS, we can either detect the emptiness of $Zero(PS/DS)$ or furnish a decomposition of the following forms:

$$Zero(PS/DS) = \cup_{i=1}^{l} Zero(ASC_i/DS \cup J_i)(3.1)$$
$$Zero(PS/DS) = \cup_{i=1}^{l} Zero(QD(ASC_i)/DS)(3.2)$$

where for each $i \leq l$, ASC_i is an ascending chain such that $prem(G, ASC_i) = 0$ for $\forall G \in PS$, $prem(P, ASC_i) \neq 0$ for $P \in DS$ and J_i is the initial set of ASC_i.

By the affine dimension theorem (p48 [HA1]) and Theorem 2.7, we have two conclusions:

(1). Since each $Zero(QD(ASC_i)/DS)$ is either empty or an unmixed variety, (3.2) actually provides **an unmixed decomposition** for $Zero(PS/DS)$.

(2). Let PS contain m polynomials then the components $Zero(QD(ASC_i)/DS)$ with more then m polynomials in ASC_i are redundant and can be deleted from (3.2).

As another application, we give a new proof for a nontrivial theorem in algebraic geometry. An irreducible variety V over K may become reducible over an extension field K^* of K. Such a variety is called a *relatively irreducible variety* [HP1]. We have the following refinement for a result about a relatively irreducible variety.

Theorem 3.2. If V is an irreducible variety of dimension d over the ground field K then over any extension K^* of K, V is an (parameter) unmixed variety of dimension d.

Proof. As V is irreducible, we have $V = Zero(QD(ASC))$ for an irreducible ascending chain ASC in $K[y]$ with $DIM(ASC) = d$ [WU1]. Now the result comes from Theorem 2.7. ∎

Reference

[AM1] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison Wesley Publ. Comp., 1969.

[BU1] B. Buchberger, Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, *Recent Trends in Multidimensional Systems theory* (ed. N.K. Bose), D.Reidel Publ. Comp., 1985.

[CA1] L. Caniglia, How to Compute the Chow Form of an Unmixed Polynomial Ideal in Single Exponential Time, AAECC, vol 1, 1990, pp. 25–42, Springer-Verlag.

[CH1] S.C. Chou, *Mechanical Geometry Theorem Proving*, D.Reidel Pub. Company, 1988.

[CG1] S.C. Chou and X.S. Gao, Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving, *10th International Conference on Automated Deduction*, M.E. Stickel (Ed.) pp 207–220, Lect. Notes in Comp. Sci., No. 449, Springer-Verlag, 1990.

[HA1] R. Hartshorne, *Algebraic Geometry*, Springer-verlag, 1977.

[HP1] W.V.D. Hodge and D. Pedoe, *Methods of Algebraic Geometry Vol. 2*, Cambridge, 1952.

[WU1] Wu Wen-tsün, Basic Principles of Mechanical Theorem Proving in Elementary Geometries, J. Sys. Sci. & Math. Scis., 4(1984), 207 –235.

[WU2] Wu Wen-tsün, On Zeros of Algebraic Equations — An Applications of Ritt Principle, Kexue Tongbao, 31(1986), 1–5.

Appendix. A Proof of the Dimension Theorem

Theorem (4.1). Let n be the number of polynomials in S, $length(ASC_i)$ be the number of polynomials in ASC_i. Those components $Zero(PD(ASC_i)/G)$ in (1.2) (or $Zero(QD(ASC_i)/G)$ in (1.3)) for which $length(ASC_i) > n$ are redundant, thus can be removed from (1.2) (or from (1.3)).

Proof of the Theorem (4.1). First we assume E is algebraically closed and $G = \{1\}$. If $Zero(S)$ is empty, then nothing is needed to prove. Assume $Zero(S)$ is non-empty. Then we can rearrange the order on the right side of (1.2) as follows:

$$\begin{aligned} Zero(S) &= \bigcup_{1\le i\le l} Zero(ASC_i/I_i) \cup \bigcup_{l<i\le k} Zero(ASC_i/I_i) \\ &= \bigcup_{1\le i\le l} Zero(PD(ASC_i)) \cup \bigcup_{l<i\le k} Zero(ASC_i/I_i) \end{aligned}$$

where $length(ASC_i) \le n$ for $i \le l$ and $length(ASC_i) > n$ for $i > l$. By the Affine Dimension Theorem (page 48 in), the dimensions of all *irredundant* (irreducible) components of $Zero(S)$ are greater than or equal to $m - n$. (Remember that m is the number of variables $y_1, ..., y_m$). By Lemma (2.2) below, $Zero(ASC_i/I_i)$ is contained in the union of irreducible varieties of $Zero(PD(ASC_i))$ with dimension $\le m - length(ASC_i)$. Thus, if $i > l$, $m - length(ASC_i) < m - n$ and each such irreducible variety of $Zero((PD(ASC_i))$ with dimension $< m - n$ must be in one of the components of $Zero(S)$. Therefore, $l > 0$ and each component of $Zero(S)$ must be contained in some $Zero(PD(ASC_i))$ for $i \le l$. Hence,

$$Zero(S) = \bigcup_{1\le i\le l} Zero(PD(ASC_i)). \tag{2.1}$$

Since any extension E of K is contained in an algebraically closed extension of K, (2.1) is valid for any extension E of K. Hence for any polynomial set G, Theorem (1.4) follows from (2.1).

Lemma (2.2). Let $ASC = f_1, ..., f_r$ be a non-trivial *quasi* ascending chain, I_i be the initials of f_i, and $J = \{I_1, ..., I_r\}$. Then $Zero(ASC/J)$ is contained in the union of irreducible varieties $\subset Zero(PD(ASC))$ with dimensions $\le m - r$.

Proof. We use induction on $m - r$.

(1) Base case: $m - r = 0$. In that case, the parameter set of ASC is empty.

Case (1.1) ASC is not in weak sense, i.e., $prem(I_j; f_1, ..., f_{j-1}) = 0$ for some $j > 1$, then $Zero(ASC/J)$ is empty.

Case (1.2) ASC is irreducible. Then $Zero(ASC/J)$ is contained in the (irreducible) variety $Zero(PD(ASC))$, the dimension of which is $m - r = 0$. The theorem is true.

Case (1.3) ASC is reducible. Suppose $f_1, .., f_{k-1}$ is irreducible, and $f_1, ..., f_k$ is reducible ($1 \le k$). For simplicity and without loss of generality, we can assume f_k has only two irreducible factors, i.e., there are two polynomials f'_k and f''_k with the same class as $class(f_k)$ such that $f_1, ..., f'_k$ and $f_1, ..., f''_k$ are irreducible, $f'_k f''_k \in Ideal(f_1, ..f_k)$,

$prem(f_k; f_1, ..., f'_k) = 0$ and $prem(f_k; f_1, ..., f''_k) = 0$. Furthermore, we can chose f'_k and f''_k in such a way that the initials $I'_k = lc(f'_k)$ and $I''_k = lc(f''_k)$ *contain parameters only.* Thus

$$\begin{aligned} Zero(ASC/J) = \quad & Zero(ASC'/J \cup \{I'_k\}) \bigcup Zero(ASC''/J \cup \{I''_k\}) \\ & \bigcup Zero(ASC \cup \{I'_k\}/J) \bigcup Zero(ASC \cup \{I''_k\}/J), \quad (2.2.1) \end{aligned}$$

where

$$\begin{aligned} ASC' &= f_1, ..., f_{k-1}, f'_k, f_{k+1}, ..., f_r, \\ ASC'' &= f_1, ..., f_{k-1}, f''_k, f_{k+1}, ..., f_r. \end{aligned}$$

In this base case, since parameter set is empty, I'_k and I''_k are constants. Thus (2.2.1) actually is

(2.2.2) $$Zero(ASC/J) = Zero(ASC'/J \cup \{I'_k\}) \bigcup Zero(ASC''/J \cup \{I''_k\}).$$

For quasi ascending ASC' (or ASC'') we have three cases:

Case (1.3.1) ASC' is not in the weak sense, i.e., $prem(I_j; ASC') = 0$ for some $j > k$, then $Zero(ASC'/J \cup \{I'_k\})$ is empty. We can delete it from the union (2.2.2).

Case (1.3.2) ASC' is irreducible. Then

(2.2.3) $$prem(f_j; ASC') = 0 \text{ for all } i = 1, ..., r.$$

Thus $PD(ASC) \subset PD(ASC')$ by Lemma (2.3) below. Hence

$$Zero(ASC'/J \cup \{I'_k\}) \subset Zero(PD(ASC')) \subset Zero(PD(ASC)).$$

$Zero(PD(ASC'))$ is a variety of dimension $m - r$.

Case (1.3.3) ASC' is reducible. We recursively repeat the same procedure of $Zero(ASC/J)$ as for $Zero(ASC'/J')$, until either case (1.3.1) or case (1.3.2) happen, here $J' = \{I_1, ..., I'_k, ..., I_r\}$. When case (1.3.2) happens, (2.2.3) is still valid.

Thus we conclude that $Zero(ASC/J)$ is contained in the union of those components of the algebraic set $Zero(PD(ASC))$ whose dimension is $m - r = 0$.

(2) Induction case: suppose the theorem is true for quasi ascending chains $g_1, ..., g_d$ with $m - d < m - r$. We want to show it is also true for $f_1, ..., f_r$. We can use the same argument as in the base case.

Case (2.1) ASC is not in weak sense, then $Zero(ASC/J)$ is empty.

Case (2.2) ASC is irreducible. Then as before, the theorem is true.

Case (2.3) ASC is reducible. We can repeat the same argument as in case (1.3) and also have 3 cases for each of ascending chains ASC' and ASC''. Here we emphasize that I'_k and I''_k contain only the parameters of ASC. Decomposition (2.2.1) is valid, but (2.2.2) is no longer valid. Instead, we can decompose (Ritt–Wu's Algorithm again), say, $Zero(\{I'_k\})$, into

$$Zero(\{I'_k\}) = \bigcup_i Zero(ASC'_i/I'_{k,i}).$$

Here for each i, $I'_{k,i}$ is the initial set of the ascending chain ASC'_i. Then

$$Zero(ASC \cup \{I'_k\}/J) = \bigcup_i Zero(ASC'_i \cup ASC/I'_{k,i} \cup J).$$

Note that $ASC'_i \cup ASC$ forms another quasi ascending chain since ASC'_i involves only the parameters of ASC. For each $Zero(ASC'_i \cup ASC/I'_{k,i} \cup J)$, we now can use the induction hypothesis to conclude that it is contained in the union of varieties (with dimension $\leq m-r+1) \subset Zero(PD(ASC'_i \cup ASC)) \subset Zero(PD(ASC))$. Thus the proof is completed. ∎

Lemma (2.3). Let ASC_1 and ASC_2 be two irreducible asc chains. $PD(ASC_1) \subset PD(ASC_2)$ only if $prem(p, ASC_2) = 0$ for all $p \in ASC_1$. If this is the case and $prem(lc(p), ASC_2) \neq 0$ for all $p \in ASC_1$, then $PD(ASC_1) \subset PD(ASC_2)$.

Proof. t is trivial. ∎