Computations on Quasi-Algebraic Sets[1]

William Sit

Department of Mathematics, City College of New York, New York, NY 10031

Email: wyscc@cunyvm.cuny.edu

February 17, 2001

Abstract

The decomposition of a constructible set into a union of quasi-algebraic sets is often a first step to solve many problems and it is sometimes desirable to have as few cases to consider as possible. We derive decision criteria and algorithms for testing inclusion and equality relations between two unions of quasi-algebraic sets and between rational functions defined on them. We emphasize flexibility in practical representations of these geometry objects and in implementation of the criteria. The algorithms are implemented in *Axiom* and used to refine Sit's algorithm for parametric linear systems. Our main result can be applied to obtain an irredundant decomposition of a constructible set.

1 Introduction

Let k be a field, and let K be its algebraic closure. Let $R = k[x_1, \cdots, x_n]$ be the polynomial ring with n indeterminates over k. For any subset $F = \{ f_1, \cdots, f_s \} \subseteq R$, we recall that the set of common zeros in K^n of F is a Zariski closed set (or algebraic set, defined over k) which we denote by $V(F)$ or $V(f_1, \cdots, f_s)$. For a single polynomial h, we denote the complement of $V(h)$ in K^n by $\overline{V}(h)$. Such a set $\overline{V}(h)$ is a basic Zariski open set. A *quasi-algebraic* set is the intersection of a Zariski closed set with a basic Zariski open set. A quasi-algebraic set is a *locally closed* set (that is, the intersection of an open and a closed set), and conversely, every locally closed set is a finite union of quasi-algebraic sets (since R is noetherian). A finite union of locally closed sets is called a *constructible* set (Eisenbud [5, p. 309], Hartshore [7, p. 94]). Thus any constructible set is a finite union of quasi-algebraic sets.

Constructible sets occurred naturally as the set of parametric values for which a parametric system has solutions. This is a consequence of

Theorem 1 (Chevalley's Theorem) *Let $R' = k[x_1, \ldots, x_n, z_1, \ldots, z_m]$ be a polynomial ring over a field k with algebraic closure K. Let E be an ideal in R', and let C be the set of all points $(a_1, \ldots, a_n) \in K^n$ such that there exists a $(b_1, \ldots, b_m) \in K^m$ for which $(a_1, \ldots, a_n, b_1, \ldots, b_m)$ is a common zero of E. Then C is constructible.*

For a more general version of Chevalley's Theorem, see Eisenbud [5, pp. 311, 315]. For examples of specific constructions related to symbolic computation, see Gao and Chou [6] or Sit [12, Prop. 4.4].

[1]This paper is an expanded version of the talk, with new results.

Quasi-algebraic sets are also the key objects in geometric theorem proving using the Wu-Ritt method (see Ko [10], and Chou [3]). Ko introduced the following notion: A geometric statement (S) is said to have *algebraic characteristics* (C) if there exist a field k, an extended field K of k, a positive integer n, a non-empty finite set of polynomials F, and a polynomial g in the polynomial ring $K[x_1, \ldots, x_n]$ such that (S) is true if and only if the quasi-algebraic set $V(F) \cap \overline{V}(g)$ is empty, or equivalently, $V(F) \subseteq V(g)$. This condition is also equivalent to the existence of k, K, n, F, g as before, and in addition, $h \in K[x_1, \ldots, x_n]$ such that (S) is true if and only if $V(F) \cap \overline{V}(h) \subseteq V(g)$. In other words, a geometric statement may be translated into a statement about the emptiness of, or inclusion between, quasi-algebraic sets. The Wu-Ritt method decomposes such a quasi-algebraic set into a disjoint union of more special quasi-algebraic sets (called triangular sets) whose emptiness may be easily decided. Similar techniques are used by Boulier *et al.* [2] to decompose the solution sets of partial differential equations.

More generally, a difficult problem often breaks down into easier cases under the additional properties and constraints given by each quasi-algebraic set making up the constructible set. For this reason, the decomposition of a constructible set into quasi-algebraic sets is often a first step to solve many problems and it is sometimes desirable to have as few cases to consider as possible. Unfortunately, in practice, a constructible set is often decomposed into a *disjoint* union of quasi-algebraic sets because of pivoting and branching, such as in a Gaussian elimination approach to a parametric linear system or in the Wu-Ritt method. These decomposition algorithms typically lead to a much larger number of quasi-algebraic sets than may be necessary. The alternative is to reduce the number by combining or merging several disjoint quasi-algebraic sets into one to obtain a possibly overlapping union while keeping the irredundancy of the decomposition. For example, Sit [12, Theorems 4.1, 6.4] has shown that for parametric linear systems, it is possible to decompose the set of parametric values for which the system is consistent into an almost irredundant union of quasi-algebraic sets using a built-in merging algorithm. The following table is derived from the bound and formula proved in Sit [12, Theorem 4.1, Theorem 9.1: Eqn. (14)] comparing the worst case complexity using Cramer's rule (on which merging algorithm is based) and using Gaussian elimination,

Size n	Cramer's Rule $\sum \binom{n}{i}^2 = \binom{2n}{n}$	Gaussian Method $\sum_{i=0}^{n} \binom{n}{i}^2 i!(n-i+1)$
1	2	3
2	6	13
3	20	73
4	70	501
5	252	4,051
6	924	37,633
7	3,432	394,353
8	12,870	4,596,553
9	48,620	58,941,091
10	184,756	824,073,141

It shows the number of quasi-algebraic sets (including possibly empty sets counted redundantly) in each decomposition for the case of a generic linear system of n equations in n unknowns. It is clear that there may be a substantial gain in efficiency both in computation time and space if the overlapping union approach is used. As noted in Sit [12], this gain is particularly prominent when further computations are to be performed on each quasi-algebraic set. These computations may range from determining whether the quasi-algebraic set is empty or not, to simplifying rational functions, which are usually associated with some properties of the quasi-algebraic sets that make up a constructible set. For our purpose, a rational function on a quasi-algebraic set S is a function $\phi : S \to k$ where ϕ is given as the quotient of two polynomials $p, q \in R$, and q does not vanish on S. Note in particular, ϕ is *everywhere defined* on S. Rational functions appear in solving a parametric system of linear equations in solution functions in Sit [12]. In *Mathematica* (Wolfram [14]), the built-in function `Reduce` can be used to solve parametric linear systems[2] giving the set of all possible solutions in the form of rational functions defined on quasi-algebraic sets.

In this paper, we discuss and solve the problem of deciding inclusion (and hence also equality) between two unions of quasi-algebraic sets each of which is given in terms of defining equations like $f_1 = 0, \cdots, f_s = 0$ and a defining inequation like $h \neq 0$. We also discuss and solve the problem of deciding equality between rational functions defined on quasi-algebraic sets. All decision algorithms will only be based on radical ideal membership tests. Some of these results are likely well-known and used by programmers, and we include them here for completeness. However, we did not find our main result (Theorem 15) in the literature, even though the proof is elementary. The main result may be applied to remove redundancy and perform merging of solution functions defined on quasi-algebraic sets in Sit's algorithm for parametric linear systems in a way more general than indicated in [12]. The proof is constructive and can be applied to obtain a minimally irredundant decomposition of a constructible set.

2 Representations

We use the notation (F) for the ideal generated by F and $\sqrt{F}$ for the radical ideal generated by F. If a property remains the same whether we use F or (F), we often use the simpler form F, or even just f if F has only one element f. An algebraic set defined by the equations $f = 0$ for $f \in F$ may be defined equally by $g = 0$ for $g \in G$, where G is any set of polynomials such that $(F) \subseteq (G) \subseteq \sqrt{F}$. This is because $\sqrt{G} = \sqrt{F}$ and hence $V(F) = V(G) = V(\sqrt{F})$. This flexibility has practical as well as theoretical implications. If our object of study is an algebraic set (rather than a polynomial ideal), we may represent it by any such set G. During the course of a computation, we may change from one representation to another if that suits our purpose. For example, we may replace any f by its square free part to lower the degree (see Cox *et. al.* [4, pp. 178–180]). In general, the closer (G) is to $\sqrt{F}$, the "simpler" the set of equations, but also the more expensive to compute G. A method to solve the inclusion problem between two algebraic sets must therefore be valid for any

[2] `Reduce` is not limited to linear systems.

representation[3]. By the Nullstellensatz, if F' is another finite set of polynomials, then $V(F) \subseteq V(F')$ if and only if $F' \subset \sqrt{F}$. It is well-known that this can be decided by means of a radical ideal membership algorithm as follows. Let $>$ be a given term-ordering on R and let t be an auxilliary indeterminate over R. We extend $>$ to an elimination term ordering in $R^+ = k[x_1, \cdots, x_n, t]$ such that any power of t is $>$ than any monomial in x alone. Then $p \in \sqrt{F}$ if and only if $1 \in (F, tp-1)$ (see Cox *et. al.* [4], p. 177), or equivalently, $1 \in G^+$, where G^+ is a reduced Gröbner basis of the ideal $(F, tp-1)$ in R^+ with respect to the elimination order $>$. By the above discussion, we may replace $p, f \in F$ by their square free parts. More generally, we may replace F (resp. F') by another set of generators G (resp. G') such that $(F) \subseteq (G) \subseteq \sqrt{F}$ (resp. $(F') \subseteq (G') \subseteq \sqrt{F'}$).

We observe that the radical ideal membership test is independent of the field of definition of F and p. In other words, if k' is a field extension of k contained in K, then $1 \in (F, tp-1) \iff 1 \in (F, tp-1) \cdot k'[x_1, \ldots, x_n]$. This can be proved easily by taking a k-vector space basis of k' over k that includes 1. This observation provides flexibility in implementation since we are free to extend k to any algebraic extension, or restrict it to any subfield containing all the coefficients.

In a similar way, a quasi-algebraic set given as $S = V(F) \cap \overline{V}(h)$ may be represented differently, and we need to generalize the above characterization for algebraic sets. Most texts in algebraic geometry include a discussion on the closure of a quasi-algebraic set, whose corresponding ideal is given by the saturation of (F) by h (see for example, Cox *et. al.* [4], pp. 191–195). More specifically, the *saturation ideal* $(F): h^\infty$ of (F) by h is the set of all $g \in R$ such that there is some $e \in \mathbb{N}$ and $h^e g \in (F)$. A closely related ideal is the *quotient ideal* $(F):(H)$ (also called the *colon ideal*) of (F) by another ideal (H). This is defined as the set of all $g \in R$ such that $hg \in (F)$ for all $h \in (H)$. When $H = \{ h \}$, the variety of the quotient ideal $(F): h$ contains the Zariski closure of S. Both quotient and saturation ideals are computable. However, inclusion relations between the closures of quasi-algebraic sets do not necessarily reflect the inclusion relations between the quasi-algebraic sets themselves. The following is an easy exercise.

Proposition 2 *Let $F \subset R$, $h \in R$, let $S = V(F) \cap \overline{V}(h)$, and let $I = (F): h^\infty$. Then*

(a). $\sqrt{F}: h \supseteq I \supseteq (F): h \supseteq (F)$;

(b). $\sqrt{F}: \sqrt{h} = \sqrt{F}: h = \sqrt{I} \supseteq \sqrt{(F): h} \supseteq \sqrt{F}$;

(c). $S \subseteq V(I) \subseteq V((F): h) \subseteq V(F)$.

If (F) is a radical ideal, then $(F): h$ is a radical ideal and equals I.

[3]The CASA system [8] allows four different representations of an algebraic set: implicit, parametric, projected, and by places. According to this latest manual, inclusion and equality testing have been implemented for the Zariski closure of the difference of two algebraic sets using the implicit representation, the one we consider in this paper.

Example 3 All containments in Proposition 2 may be strict. Let $F = \{ x^3y^2z \}$, $h = x^2z$. Then S is the xz-plane without the x and z-axes. We have $(F)\colon h = (xy^2)$, $\sqrt{F} = (xyz)$, $\sqrt{(F)\colon h} = (xy)$, $I = (y^2)$, $\sqrt{I} = \sqrt{F}\colon h = \sqrt{F}\colon\sqrt{h} = (y)$. This example shows that $S \subset V(I) \subset V((F)\colon h) \subset V(F)$, and $\sqrt{I} \supset \sqrt{(F)\colon h} \supset \sqrt{F}$.

We note that any finite intersection of quasi-algebraic sets is a quasi-algebraic set:

Proposition 4 *Let $A = V(F_1), B = \overline{V}(h_1), C = V(F_2)$ and $D = \overline{V}(h_2)$, where $F_1, F_2 \subset R$ and $h_1, h_2 \in R$. Let $S_1 = A \cap \overline{B}$, $S_2 = C \cap \overline{D}$, and $S = S_1 \cap S_2$. Then $S = V(F_1, F_2) \cap \overline{V}(h_1h_2)$.*

Proof. Clearly $S = (A \cap C) \cap (\overline{B \cup D})$ where $A \cap C = V(F_1, F_2)$ and $B \cup D = V(h_1h_2)$ by Cox *et. al.* [4, Chapter 4, Theorems 7 and 15]. $\square$

3 Inclusion and Equality Testing

We recall two results (Propositions 6.2 and 7.4) from Sit [12]. The first one gives a decision procedure for deciding inclusion for families of quasi-algebraic sets under a special situation. The second one, where we state the version for ideals (a similar result holds for radical ideals), provides the foundation for simplification of polynomial functions and their representations on quasi-algebraic sets.

Proposition 5 *Let $\{ H^i = V(F) \cap \overline{V}(p_i) \}$ and $\{ K^j = V(F) \cap \overline{V}(q_j) \}$, where $\{ p_i \}$, $\{ q_j \}$, and F are finite subsets of R, be two families of quasi-algebraic sets. Then*

$$\cup H^i \subseteq \cup K^j \iff \{ p_i \} \subseteq \sqrt{F \cup \{ q_j \}}. \tag{1}$$

Proposition 6 (Ideal version). *Let $F \subset R$, $h \in R$ and let S be the quasi-algebraic set $V(F) \cap \overline{V}(h)$. Let G^+ be a Gröbner basis of $(F, th - 1)$ in R^+ relative to the elimination order $>$. Let $G = G^+ \cap R$ and let $\widehat{h}$ be a normal form of h modulo G. Then*

(a). *G is a Gröbner basis for the ideal $(F, th - 1) \cap R$ in R with respect to the given term order $>$.*

(b). *If G^+ is a reduced Gröbner basis, so is G.*

(c). *If $p \in R$, then the normal form of p with respect to G is the same as the normal form $\widehat{p}$ of p with respect to G^+.*

(d). *$(G) \supseteq (F)$.*

(e). *$S = V(G) \cap \overline{V}(\widehat{h})$.*

Remark 7 The ideal $I = (F, th-1) \cap R$ in Proposition 6 in fact equals the saturation of (F) by h (see Cox *et. al.* [4], p. 196). It plays a prominent role in the representation of S since $(G) = I$. Proposition 6 provides an algorithm to compute I, or any saturation ideal. The radical membership test $h \in \sqrt{F}$ is then equivalent to $1 \in (F) : h^\infty$. We shall use this latter form of the test in stating our results. Note also that $I \subseteq R$ and if $g \in R$, then

$$(I, tg-1) \cap R = ((F) : h^\infty) : g^\infty = (F) : (hg)^\infty = (F, thg-1) \cap R.$$

The next proposition provides a theoretical basis for choice of representations of a quasi-algebraic set. The freedom with which we can choose any set F' with $I \subseteq (F') \subseteq \sqrt{I}$ allows various degrees of simplifications and emphasizes that quasi-algebraic sets are geometric objects even though we are computing with polynomials. For example, we can replace any $f \in F$ by the product of its irreducible factors (using a square-free factorization). It is at least theoretically conceivable that F' may be found without first computing F.

Proposition 8 *Let $F \subset R$, $h \in R$, let S be the quasi-algebraic set $V(F) \cap \overline{V}(h)$ and let $I = (F) : h^\infty$. Let $F' \subset R$ be such that $I \subseteq (F') \subseteq \sqrt{I}$ and let $h' \in R$ be congruent to h modulo (F'). Then $S = V(F') \cap \overline{V}(h')$.*

Proof. Let $S' = V(F') \cap \overline{V}(h')$. Clearly $(F) \subseteq I \subseteq (F') \subseteq \sqrt{I}$. Taking radicals shows $\sqrt{F} \subseteq \sqrt{I} = \sqrt{F'}$ and hence $V(F') \subseteq V(F)$. Clearly, $S' \subseteq \overline{V}(h)$ since $h' - h \in (F')$ and so $S' \subseteq S$. Conversely, by Proposition 6(e), $S = V(G) \cap \overline{V}(\widehat{h})$ where G and $\widehat{h}$ are as defined there. Since $V(G) = V(I) = V(F')$, $S \subseteq V(F')$. Thus $S \subseteq \overline{V}(h')$ and this completes the proof. $\square$

We now state some results which provide decision procedures for testing inclusion relations between two quasi-algebraic sets. The easy extensions to testing equality are omitted. We use a bar above a set to denote its complement.

Proposition 9 *Let $A = V(F_1)$, $\overline{B} = \overline{V}(h)$, and $C = V(F_2)$, where $F_1, F_2 \subseteq R$ and $h \in R$. Then*

$$A \cap \overline{B} \subseteq C \iff 1 \in \cap_{f_2 \in F_2} (F_1) : (hf_2)^\infty.$$

Proof. Let $I = (F_1, th-1) \cap R$. The inclusion $A \cap \overline{B} \subseteq C$ is equivalent to $V(I) \subseteq C$ because C is Zariski closed and $V(I)$ is the Zarisiki closure of $A \cap \overline{B}$. Hence we have

$$A \cap \overline{B} \subseteq C \iff F_2 \subseteq \sqrt{I} \iff 1 \in \cap_{f_2 \in F_2} (I, tf_2 - 1) = \cap_{f_2 \in F_2} (F_1) : (hf_2)^\infty,$$

where the last equality comes from Remark 7. $\square$

Proposition 10 *Let* $A = V(F)$, $\overline{B} = \overline{V}(h_1)$, *and* $\overline{D} = \overline{V}(h_2)$, *where* $F \subset R$ *and* $h_1, h_2 \in R$. *Then*

$$A \cap \overline{B} \subseteq \overline{D} \iff 1 \in (F, h_2) : h_1^{\infty} \tag{2}$$

Proof. We have $A \cap \overline{B} \subseteq \overline{D} \iff A \cap D \cap \overline{B} = \emptyset \iff A \cap D \subseteq B \iff h_1 \in \sqrt{(F, h_2)}$. □

The next two corollaries follow easily. We give the second one also because it is slightly more general, and depending on the actual defining equations for the quasi-algebraic sets, a Gröbner basis for $(F_1, \widetilde{F_2}, h_2, th_1 - 1)$ for some non-empty $\widetilde{F_2} \subseteq F_2$ may be easier to compute than one for $(F_1, h_2, th_1 - 1)$. Thus the second corollary provides some flexibility in implementation.

Corollary 11 *Let* $A = V(F_1)$, $\overline{B} = \overline{V}(h_1)$, $C = V(F_2)$, *and* $\overline{D} = \overline{V}(h_2)$, *where* $F_1, F_2 \subset R$ *and* $h_1, h_2 \in R$. *Then*

$$A \cap \overline{B} \subseteq C \cap \overline{D} \iff 1 \in (\cap_{f_2 \in F_2} (F_1) : (h_1 f_2)^{\infty})) \cap (F_1, h_2) : h_1^{\infty}. \tag{3}$$

Moreover, if (F_1) *is a radical ideal, then*

$$A \cap \overline{B} \subseteq C \cap \overline{D} \iff 1 \in (F_1) : (h_1 F_2) \cap (F_1, h_2) : h_1^{\infty}. \tag{4}$$

Proof. When (F_1) is radical, $(F_1) : (h_1 f_2)^{\infty} = (F_1) : h_1 f_2$ by Proposition 2. The last statement then follows from the intersection properties of quotient ideals (Cox *et. al.* [4, p. 194, Proposition 10]). □

Corollary 12 *Let* $A = V(F_1)$, $\overline{B} = \overline{V}(h_1)$, $C = V(F_2)$, *and* $\overline{D} = \overline{V}(h_2)$, *where* $F_1, F_2 \subset R$ *and* $h_1, h_2 \in R$. *Let* $\widetilde{F_2} \subseteq F_2$. *Then*

$$A \cap \overline{B} \subseteq C \cap \overline{D} \iff 1 \in (\cap_{f_2 \in F_2} (F_1) : (h_1 f_2)^{\infty}) \cap (F_1, \widetilde{F_2}, h_2) : h_1^{\infty}. \tag{5}$$

Proof. Let $\widetilde{C} = V(\widetilde{F_2})$. Then $C \subseteq \widetilde{C}$. From set theory, it is easy to see that $A \cap \overline{B} \subseteq C \cap \overline{D}$ if and only if $A \cap \overline{B} \subseteq C$ and $(A \cap \widetilde{C}) \cap \overline{B} \subseteq (A \cap \widetilde{C}) \cap \overline{D}$. By Proposition 5, the second condition is equivalent to $h_1 \in \sqrt{(F_1, \widetilde{F_2}, h_2)}$, and by Proposition 9 above, the first is equivalent to $1 \in \cap_{f_2 \in F_2} (I, tf_2 - 1)$. □

Noting that when $h_1 = 1$, we have $h_1 \in \sqrt{(F_1, \widetilde{F_2}, h_2)} \iff 1 \in (F_1, \widetilde{F_2}, h_2)$, we have

Corollary 13 *With same notation as in Corollary 12,*

$$A \subseteq C \cap \overline{D} \iff 1 \in (\cap_{f_2 \in F_2} (F_1) : f_2^{\infty}) \cap (F_1, \widetilde{F_2}, h_2). \tag{6}$$

As examples, we recall several basic properties listed in Ko [10], which are special applications of this proposition to geometric theorem proving. In the setting, we follow Ko's notation and write $V(F/h)$ for $V(F) \cap \overline{V}(h)$.

Proposition 14 *For any polynomials f_1, f_2, g, h, h_1, h_2, sets of polynomials F, F_1, F_2, the following holds:*

1. *Square-free simplification: If f_1, f_2 have the same collection of prime factors and h_1, h_2 have the same collection of prime factors, then $V(f_1/h_1) = V(f_2/h_2)$.*
2. *Common factor elimination: If $g \neq 0$, then $V(g \cdot F/h) = V(F/g \cdot h)$.*
3. *Inclusion of no-harm polynomials: If $V(F/h) = V(F_1/h_1) \cup V(F_2/h_2)$, then $V(F, f/gh) = V(F_1, f/gh_1) \cup V(F_2, f/gh_2)$.*

Our main result is the following theorem, which generalizes Proposition 5 and Corollary 12 to arbitrary families of quasi-algebraic sets. While we do not spell out the detail algorithm, our proof is constructive.

Theorem 15 *Let $S_i = A_i \cap \overline{B_i}$ and $Q_j = C_j \cap \overline{D_j}$ for $1 \leq i \leq s$ and $1 \leq j \leq q$, where A_i, C_j are Zariski-closed sets and B_i, D_j are basic Zariski open sets. Then we can decide whether $\cup_{i=1}^{s} S_i \subseteq \cup_{j=1}^{q} Q_j$.*

Proof. Clearly, we may assume that $s = 1$ and write $S = S_1$. Now $S \subseteq \cup_{j=1}^{q} Q_j \iff S \cap \overline{(\cup_{j=1}^{q} Q_j)} = \emptyset$. On the other hand,

$$\overline{(\cup_{j=1}^{q} Q_j)} = \cap_{j=1}^{q} \overline{Q_j} = \cap_{j=1}^{q} (\overline{C_j} \cup D_j) = \cup_{\ell} T_{\ell}$$

where the last union runs over all possible choices of $T_\ell = E_1 \cap \cdots \cap E_q$ with each $E_j = \overline{C_j}$ or D_j. It now suffices to be able to decide if for each ℓ, $S \cap T_\ell = \emptyset$. Without loss of generality, we may assume that a typical T_ℓ has the form $\overline{C_1} \cap \cdots \cap \overline{C_\mu} \cap D_{\mu+1} \cap \cdots \cap D_q$ for some $\mu, 0 \leq \mu \leq q$. Then $T_\ell = \overline{C^\ell} \cap D^\ell$, where $C^\ell = C_1 \cup \cdots \cup C_\mu$ and $D^\ell = D_{\mu+1} \cap \cdots \cap D_q$ are Zariski closed sets (if $\mu = 0$, then $C^\ell = K^n$, and if $\mu = q$, then $D^\ell = K^n$). Suppose the algebraic set C^ℓ is defined by the equations $f_{\ell\nu} = 0$ for $\nu = 1, \ldots, m_\ell$, where $f_{\ell\nu} \in R$. We may write $\overline{C^\ell} = \cup_{\nu=1}^{m_\ell} \overline{C_{\ell\nu}}$, where $\overline{C_{\ell\nu}}$ is the basic Zariski open set defined by $f_{\ell\nu} = 0$. Hence $T_\ell = \cup_{\nu=1}^{m_\ell} (\overline{C_{\ell\nu}} \cap D^\ell)$. It now suffices to decide if $S \cap (\overline{C_{\ell\nu}} \cap D^\ell)$ is empty, but this is the intersection of two quasi-algebraic sets and hence by Proposition 4, is itself a quasi-algebraic set. Since a quasi-algebraic set $V(F) \cap \overline{V}(h)$ is empty if and only if $1 \in (F) : h^\infty$, this completes the proof.

4 Equality Test for Rational Functions

We now turn our attention to equality of polynomial and rational functions on quasi-algebraic sets. Just as the representation of S (as given by F and h) is not unique, the representation of ϕ as given by p and q is not unique. Two rational functions $\phi_1 = p_1/q_1$ and $\phi_2 = p_2/q_2$ are equal on S if $p_1 q_2 - p_2 q_1$ vanishes identically on S. Thus to test equality of two rational functions ϕ_1, ϕ_2 on S, it is sufficient to have a procedure to decide when a given polynomial p represents the zero function on S. This is easy to do if S is non-empty and if the Zariski closure of S is irreducible, since by Cox *et. al.* [4, p. 249, Proposition 6], p is the zero function on S if and only if p is zero on the Zariski closure of S and hence if and only if $p \in \sqrt{(F):h}$. We slightly generalize this result to give a decision criterion which allows the same flexibility for implementation as the representation of quasi-algebraic sets and avoids having to know *a priori* or separately test that S is non-empty. Our proof is elementary and does not depend on Proposition 6 in Cox or the irreducibility of the Zariski closure of S.

Proposition 16 *Let $S = V(F) \cap \overline{V}(h)$ be a quasi-algebraic set and let $p \in R$. Let $I = (F):h^\infty$. Let $F' \subset R$ be such that $I \subseteq (F') \subseteq \sqrt{I}$. Then $p(a) = 0$ for all $a \in S$ if and only if $1 \in (F'):p^\infty$.*

Proof. The condition $1 \in (F'):p^\infty$ is equivalent to $p \in \sqrt{F'}$. Assuming this condition holds, let $a \in S$. By Proposition 8, $g(a) = 0$ for all $g \in F'$ and hence $p(a) = 0$. Conversely, suppose $p(a) = 0$ for all $a \in S$. Let G^+ be the Gröbner basis of the ideal $(F, th - 1)$, and let $G = G^+ \cap R$, as in Proposition 6. Let $b = (b_1, \cdots, b_{n+1}) \in K^{n+1}$ be such that $g(b) = 0$ for all $g \in G^+$. Because $(G^+) = (F, th - 1)$, it follows that $h(b_1, \cdots, b_n) \neq 0$ and $f(b_1, \cdots, b_n) = 0$ for all $f \in F$. Thus $(b_1, \cdots, b_n) \in S$ and $p(b_1, \cdots, b_n) = p(b) = 0$. Since p vanishes on every zero of G^+, by the Nullstellensatz, for some natural number m, $p^m \in (G^+)$ in R^+. Hence $p^m \in (G^+) \cap R = (G)$ and $p \in \sqrt{G} = \sqrt{F'}$. $\square$

Remark 17 If we take $F' = I$, we obtain $p(a) = 0$ for all $a \in S$ if and only if $1 \in (F):(hp)^\infty$. By specialising h to be 1, we reprove that p is zero on S if and only if p is zero on its Zariski closure. Note that if F' is a Gróbner basis for the *radical* ideal $\sqrt{I}$, the condition $p \in \sqrt{F'}$ is equivalent to $p' = 0$, where p' is the normal form of p with respect to F'. However, in general, the Proposition 16 is false if we replace the condition $p \in \sqrt{F'}$ by $p \in (F')$, or by $p \in \sqrt{F}$, or by $p' = 0$ (in case F' is a Gröbner basis and p' is the normal form of p with respect to F'). Here is an example. Let x, y be indeterminates over k, let t be the auxilliary indeterminate, $F = \{ xy^2 \}$, $h = x^2$, and $p = y$. Then S is the x-axis without the origin. A Gröbner basis of $(F, th - 1)$ is $G^+ = \{ y^2, tx^2 - 1 \}$ and $G = \{ y^2 \}$. Taking $I = (y^2)$ and $F' = G$, we have p vanishes everywhere on S, but $p \notin (G)$, $p \notin \sqrt{F} = (xy)$, and $p' = y \neq 0$.

Equality between two rational functions on quasi-algebraic sets S_1, S_2 can now be tested by testing first that the domains S_1 and S_2 are equal and then testing that the difference of $\phi_1 - \phi_2$ is zero on the common domain. More generally, equality of rational maps $\phi_1 : S_1 \to K^m, \phi_2 : S_2 \to K^m$ can also be done by individual tests on the corresponding coordinates functions that represents ϕ_1, ϕ_2. Since the intersection of two quasi-algebraic set is also a quasi-algebraic set (Proposition 4), we can test whether the restrictions of two rational functions to an intersection are equal. This then allows us to see if the two functions may be "merged" into one over the union of the two quasi-algebraic sets by relaxation.

5 Applications

This study originated from the author's work on parametric linear equations, which has applications in computing first integrals of dynamical systems and computing initial value conditions for differential algebraic systems (Sit [11], [12], Pritchard and Sit [13]). A key challenge implicitly raised by the author in [12] is:

> If a constructible set C is given by a finite (possibly disjoint) union of quasi-algebraic sets $S_1, \ldots, S_k$, and if on each set S_i, a rational map $\phi_i : S_i \to K^m$ is given, is there a "merging" algorithm to rewrite the decomposition into a finite irredundant union (but not necessarily disjoint) of quasi-algebraic sets $T_1, \ldots, T_\ell$ and compute rational maps $\psi_j : T_j \to K^m$ such that ℓ is minimal, and for every $a \in C$, $a \in S_i \cap T_j$ implies that $\phi_i(a) = \psi_j(a)$?

This problem is still unsolved, but the current work, with implementation in *Axiom* (Jenks *et. al.* [9]) in a new version of the domain `QuasiAlgebraicSet` and new domains `RationalMapsOnQuasiAlgebraicSet` and `SolutionFunctionsOnQuasiAlgebraicSet`, provides tools for experimentation and further discoveries. We can now compare two unions of quasi-algebraic sets even if we do not yet know how to merge. The ability to test inclusion already allows us to avoid computations of radical ideals entirely in solving parametric linear equations. As indicated in [12], we can proceed using computations with ideals, and after we obtain a list of regimes (which are quasi-algebraic sets) and their solution functions (which are rational maps), we can check for redundancies through inclusion of the regimes and equality of the restricted rational maps. We can also manually experiment with merging by testing whether, through relaxation of the constraints, the union of several disjoint regimes may be covered by another union. As an example, we illustrate this process below using results from *Mathematica* on the linear system in [12, Example 2.1].

Example 18 `Reduce`$[\{\, (b-a)x+ay+(a^2-1)z == 0, bx+(a^2+1)y+a^3z == 0 \,\}, \{\, x, y, z \,\}]$ produces three cases:

1. $\delta_1 \neq 0, x = \dfrac{z}{\delta_1}, y = -\dfrac{\delta_2 z}{\delta_1}$
2. $a = 0, b = 0, y = 0, z = 0$
3. $\delta_1 = 0, a \neq 0, 1 - a + a^2 \neq 0, x = \dfrac{(a - 1 - a^2)y}{a}, z = 0$

where $\delta_1 = -a - a^3 + b - a\,b + a^2\,b$ and $\delta_2 = (a^3 - a^2 + 1)b - a^4$. It seems natural to see whether the most general case, namely, case 1, already includes the other two. As it stands, this is of course not true. By relaxing the constraints in case 1, we come up with a general solution with no constraints: $y = -\delta_2 x, z = \delta_1 x$. We easily verify that case 2 is included when $x = 0$. Under the assumptions of case 3, the function $-\delta_2 x - \dfrac{ax}{a - 1 - a^2} = \dfrac{a^3 - a^2 + 1}{a^2 - a + 1}\delta_1 x$ is the zero function when restricted to case 3. So is the function $\delta_1 x$. Thus case 3 is indeed included also in the general solution.

Based on examples in [12], we found that for these parametric linear systems, `Reduce` from *Mathematica* gave more cases than Sit's algorithm, and thus some merging operations after using `Reduce` seems possible.

References

[1] Aubry, P., Maza, M. M. (1999)/ Triangular Sets for Solving Polynomial Systems: a Comparative Implementation of Four Methods. J. Sym. Comput. **28** (1999), 125–154.

[2] Boulier, F., Lazard, D., Ollivier, F., Petitot, M. (1995). Representation for the Radical of a Finitely Generated Differential Ideal. Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ACM Press, 158–166.

[3] Chou, S. C. (1988). *Mechanical Geometry Theorem Proving.* D. Reidel Pub. Co., 1988, Dordrecht, Holland.

[4] Cox, D., Little, J., and O'Shea, D. (1992). *Ideals, Varieties, and Algorithms.* Springer-Verlag.

[5] Eisenbud, D. *Commutative Algebra, with a View Toward Algebraic Geometry.* GTM 150, Springer-Verlag, 1995, New York.

[6] Gao, X. S. and Chou, S. C. (1993). A zero structure theorem for differential parametric systems. J. Symbolic Comput. **16** (1993), no. 6, 585–595.

[7] Hartshore, R. (1977). *Algebraic Geometry.* GTM 52, Springer-Verlag, 1977, New York.

[8] Hemmecke, R. and Winkler, F. (2000). CASA User Manual (Version 2.5), RISC Linz Report Series 00-30, 2000, ftp://ftp.risc.uni-linz.ac.at/pub/techreports/2000/00-30.ps.gz

[9] Jenks, R. D. and Sutor, R. S. (1992). *Axiom, The Scientific Computation System*, Springer-Verlag, New York, 1992.

[10] Ko, H. P. (1988). Geometry theorem proving by decomposition of quasi-algebraic sets: an application of the Ritt-Wu principle. Geometric reasoning (Oxford, 1986). Artificial Intelligence **37** (1988), no. 1-3, 95–122.

[11] Sit, W. Y. (1988). On Goldman's algorithm for solving first-order multinomial autonomous systems. Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988), 386–395, Lecture Notes in Comput. Sci., **357**, Springer, Berlin-New York, 1989.

[12] Sit, W. Y. (1992). An Algorithm for Solving Parametric Linear Systems. *J. Sym. Comp.* **13**, 353–394.

[13] Pritchard, F. L. and Sit, W. Y. (2000). On Initial Value Problems for Ordinary Differential-Algebraic Equations. Submitted to J. Symbolic Comput.

[14] Wolfram, S. (1999). The Mathematica Book, 4^{th}-ed. Wolfram Media, Champaign, Illinois.