Quantifier Elimination in the Theory of an Algebraically-closed Field

Doug Ierardi
Department of Computer Science
Cornell University
Ithaca, New York 14853

Abstract

In this paper we develop a fast parallel procdure for deciding when a set of multivariate polynomials with coefficients in an arbitrary field K have a common algebraic solution. Moreover, since the proposed algorithm is algebraic, it easily yields a procedure for quantifier elimination in the theory of an arbitrary algebraically closed field.

More precisely, we show how to decide whether m polynomials in n variables, each of degree at most d, with coefficients in an arbitrary field K have a common zero in the algebraic closure of K, using sequential time $(mn)^{O(n)}d^{O(n^2)}$, or parallel time $O(n^3 \log^3 d \log m)$ with $(mn)^{O(n)}d^{O(n^2)}$ processors, in the operations of the coefficient field K. Using randomization, this may be improved to $(mn)^{O(1)}d^{O(n)}$ time.

In addition, the construction is used give a direct EXPSPACE algorithm for quantifier elimination in the theory of an algebraically-closed field, which runs in PSPACE or parallel polynomial time when restricted to formulas with a fixed number of alternations of quantifiers.

1 Introduction

A cornerstone of elimination theory and early algebraic geometry was the development of constructive methods for deciding when a set of multivariate polynomials has a common algebraic solution. Algorithms for this problem were developed by Hermann, Kronecker and others using iterated resultant computations [17,21]; the work of Tarski on the theories of the real and the complex numbers also addressed this issue. More recently, the search for efficient algorithms has received renewed attention, not only because of the historical significance of the problem, but also because of its importance in algebraic computation.

In this paper we develop a fast parallel algorithm for solving this decision problem; moreover, since the proposed algorithm is algebraic, it easily yields a procedure for quantifier elimination in the theory of an arbitrary algebraically closed field. More precisely, we show how to decide whether m polynomials in n variables, each of degree at most d, with coefficients in an arbitrary field K have a common zero in the algebraic closure of K, using sequential time $(mn)^{O(n)}d^{O(n^2)}$ or parallel time $O(n^3 \log^3 d \log m)$ in the operations of K. This yields an NC$_k$ algorithm for a fixed number of variables. With randomization, we can achieve a better time bound of $O(n^3 \log^2 md)$, which approaches the lower bound of $n \log d$ for algebraic solutions to this problem (when $m = n+1$). For a prenex formula ϕ in the theory of an algebraically closed field with n variables and a alternations of quantifiers, we can find an equivalent quantifier-free formula in parallel time $n^{O(a)} \log^{O(1)} |\phi|$. This yields an exponential space procedure for quantifier elimination which, when restricted to formulas with a bounded number of quantifier alternations, can be executed in PSPACE.

These new algorithms represent a significant improvement over the sequential double-exponential time procedures of Heintz [14], and the parallel procedures of Fitchas, Galligo and Morgenstern [7] which are exponential in the number of variables. Although we match the sequential time complexity which Chistov and Grigor'ev achieve through their imposing suite of papers [5,6,10,11,12], our construction has the advantage of being both *significantly* simpler and efficiently parallelizable.

Recall that Hilbert's Nullstellensatz states that polynomials $f_1, \cdots, f_m \in k[x_1, \cdots, x_n]$ have no common zeros in the algebraically closed field k if and only if there are polynomials $g_1, \cdots, g_m \in k[x_1, \cdots, x_n]$ such that $\sum_{i=1}^{m} f_i g_i = 1$. Given a bound on the degrees of these g_j's, the problem of deciding whether the f_i's have a common solution can be reduced to problem of solving a large systems of linear equations [22,7]. The known bounds for the general case (arbitrary polynomials over a field of arbitrary characteristic) have until recently been double-exponential, making the obvious reduction too costly. Recently, improvements on this bound by Caniglia, Galligo and Heintz [2] and Kollàr have yielded deterministic sequential and parallel algorithms for these problems, similar, although somewhat less efficient, than those presented in this paper [7]. The algorithms which we propose instead rely on previously established results for the special case of 0-dimensional homogeneous ideals — where the degree bound is substantially smaller — and the classical construction of multivariate resultants, as in [17]. As a consequence, our algorithms are faster, and (in the probabilistic version) more closely approach the known lower bound for the problem. As in the algorithms of Chistov and Grigoriev, we can also construct a witness (a solution) when one exists (although we do not construct a complete decomposition of an algebraic set into irreducible components). The methods we use are of independent interest. They generalize aspects of the constructions employed in the recent PSPACE decision procedures for

© 1989 ACM 0-89791-307-8/89/0005/0138 $1.50

the existential theory of real-closed fields, achieved by Canny and by Renegar. In particular, we adapt homotopy methods for solving systems of polynomial equations — as in Zulehner [25] — to fields of finite characteristic.

1.1 Outline

We begin first with an informal sketch of our approach. Let k be an algebraically closed field and K an arbitrary subfield of k; for now we will assume that K is infinite. Let $f_1, \cdots, f_m$ be polynomials in the ring $K[x_1, \cdots, x_n]$, and with total degree bounded by d. If the polynomial equations

$$f_1(\overline{x}) = \quad \cdots \quad = f_m(\overline{x}) = 0 \tag{1}$$

have a common solution in k^n, then one can effectively "construct" a small solution $\overline{\alpha} \in k^n$. Such a point will be specified by n additional polynomials $g_1, \cdots, g_n \in F[\overline{x}]$ with only *finitely many* common zeros such that

$$g_1(\overline{\alpha}) = \quad \cdots \quad = g_n(\overline{\alpha}) = 0 \tag{2}$$

§2 develops a resultant-based procedure for deciding when some solution of (2) is also a solution of (1). In §3 we outline a deterministic procedure by which we can construct such polynomials $g_1, \cdots, g_n$. Together with the algorithm of §2, this yields a parallelizable algebraic procedure for deciding when a set of multivariate polynomials has a common algebraic solution. §4 applies this decision procedure to the problem of quantifier elimination in the theory of the field k, and hence yields a decision procedure for sentences in this theory. Finally, in §5 we present a lower bound for parallel algebraic algorithms solving each of these problems.

1.2 Notation and terminology

I will assume some familiarity with multivariate resultants and elementary algebraic geometry, as in Macaulay [17] Chapter 1 and Hartshorne [13] Chapter 1 (respectively).

Hereafter k is a fixed algebraically closed field, and K a subfield with algebraic closure k. A^n_x (respectively P^n_x) denotes the n-dimensional affine (projective) space over k with coordinate functions $\overline{x} = x_1, \cdots, x_n$ (homogeneous coordinates $\overline{x} = x_0, \cdots, x_n$), given the Zariski topology. The zero-set of a collection of polynomials I is denoted $V(I)$.

The closed set $\{x_0 = 0\} \subset \mathsf{P}^n$ is called the hyperplane at infinity. A^n is homoeomorphic to the open set $\{x_0 \neq 0\}$ under the embedding

$$\mathsf{A}^n \hookrightarrow \mathsf{P}^n \quad : \quad (a_1, \cdots, a_n) \mapsto (1 : a_1 : \cdots : a_n)$$

I will identify A^n with its image in P^n under this map. Projective points in A^n will be called *affine*; similarly, if Z is an irreducible subset of P^n, then Z will be called *affine* if $Z \cap \{x_0 \neq 0\} \neq \emptyset$.

The homogenization of $f \in k[x_1, \cdots, x_n]$ is defined

$$f^h(x_0, \cdots, x_n) \quad = \quad x_0^{\deg f} f(x_1/x_0, \ldots, x_n/x_0)$$

Note that if $f_1, \cdots, f_m \in k[x_1, \cdots, x_n]$, then

$$\overline{V(f_1, \cdots, f_m)} \quad \subset \quad V(f_1^h, \ldots, f_m^h)$$

as subsets of P^n_x, and the containment may be proper. Here $\overline{X}$ denotes the closure of $X \subset \mathsf{P}^n$.

In a similar manner, the closed (algebraic) subsets of the space $\mathsf{A}^m \times \mathsf{P}^n$ are defined by the zeros of sets of polynomials in $k[y_1, \cdots, y_m][x_0, \cdots, x_n]$ which are homogeneous in $\overline{x}$, For each of these spaces, it is true that all closed sets can be uniquely decomposed into an irredundant finite union of closed irreducible sets, called its *irreducible components.* Dimension is defined in a standard manner.

I adopt the convention of using lower case roman letters for arbitrary polynomials $f \in k[x_1, \cdots, x_n]$ and upper case for homogeneous polynomials $F \in k[x_0, \cdots, x_n]$. I write $f \equiv 0$ to mean that the polynomial f vanishes identically. When $\overline{u}$ and $\overline{v}$ are sequences of the length m, I will write $\overline{u} \cdot \overline{v}$ for the sum $\sum_{i=1}^m u_i v_i$.

The space and time complexity of the algorithms will be measured with respect to a PACDAG model in which the basic operations of the processors are the ring operations ($+, -$ and $\times$) of the field k (or K). For $\Sigma \subset K[x_1, \cdots, x_n]$, $||\Sigma||$ will denote the "size" of this set, which is an integer dominating the number of polynomials in Σ, the number of variables occuring in these polynomials, and the maximum (total) degree of the polynomials. When K is the field of rationals Q or a finite field F_q, we also implicitly consider the size of the coefficients of these polynomials and the complexity of these algorithms in terms of bit-operations. In this case, it is assumed that elements of these fields are given a standard encoding. See [23] and [9] for further discussion of the models and related issues.

2 Deformations of an algebraic set

I will say that the polynomials $g_1, \cdots, g_n \in K[x_1, \cdots, x_n]$ *define* a point $\overline{\alpha} \in \mathsf{A}^n$ if $\overline{\alpha} \in V(g_1, \cdots, g_n)$ and the g_i's have only a finite number of solutions. In this section we show how to decide when n polynomials in n variables define a witness to the non-emptiness of an algebraic set. This will be done using the multivariate resultant. The constructions in this section implicily extend the applications of Canny's so-called "generalized characteristic polynomials" [4] to field of finite characteristic.

It is well known that $n+1$ homogeneous polynomials in $n+1$ variables have a common zero in P^n_x exactly when their resultant vanishes identically [21]. If n homogeneous polynomials $G_1, \cdots, G_n \in k[x_0, \cdots, x_n]$ have only finitely many common zeros, then the intersection of the set $V = V(G_1, \cdots, G_n)$ and a hyperplane $\overline{u} \cdot \overline{x}$ will be empty, for any sufficiently generic choice of $\overline{u} = u_0, \cdots, u_n \in k$. Taking $\overline{u}$ to be indeterminates, we find that the resultant of these $n + 1$ polynomials with respect to the variables $\overline{x}$ is a polynomial $r(\overline{u})$ which factors into linear forms $\overline{\alpha} \cdot \overline{u}$, where $\overline{\alpha} = (\alpha_0 : \ldots : \alpha_n)$ ranges over all points in V. The points in V can be recovered from a factorization of this polynomial r, called the *u-resultant* of the G_i's.

The following variant of this technique will be used in algorithm we develop. Assume that we are given m additional homogeneous polynomials $F_1, \cdots, F_m \in k[x_0, \cdots, x_n]$, each of degree d, and consider the map

$$\begin{aligned} \overline{F} \quad &: \quad \mathsf{P}^n_x \to \mathsf{A}^m \\ &: \quad (x_0 : \ldots : x_n) \mapsto (F_1(\overline{x}), \ldots, F_n(\overline{x})) \end{aligned}$$

We can recover information about the image $\overline{F}(V)$ by constructing the polynomial

$$H_1(\overline{x},\overline{v}) \quad = \quad \sum_{j=0}^{m} v_j F_j(\overline{x})$$

where the v_j's are also new indeterminates. Invoking the characterization of resultants [17] and then Nullstellensatz, we can show that the resultant of H_1 and the G_i's with respect to $\overline{x}$ is a polynomial in the variables $\overline{v}$ which factors into linear forms

$$\sum_{j=1}^{m} F_j(\overline{\alpha})v_j$$

for $\overline{\alpha} \in V$. Hence, if V is finite, this resultant vanishes identically exactly when $V \cap V(F_1, \cdots, F_m) \neq \emptyset$.

Since we in fact want information about *affine* points, we will instead try to construct such a representation of points in the graph of $\overline{F}$, viewed as a subset of P^{n+m} The resultant of the G_i's and H_2

$$H_2(\overline{x},\overline{u},\overline{v}) \quad = \quad \sum_{i=0}^{n} u_i x_i^d + \sum_{j=0}^{m} v_j F_j(\overline{x})$$

with respect to $\overline{x}$ is a homogeneous polynomial $R(\overline{u},\overline{v})$ which does not vanish identically (if V is finite), and factors into linear forms

$$\sum_{i=0}^{n} \alpha_i^d u_i + \sum_{j=1}^{m} F_j(\overline{\alpha})v_j$$

where $\overline{\alpha} = (\alpha_0 : \ldots : \alpha_n)$ ranges over all points in V. From this polynomial, we can recover useful information about affine points in $V \cap V(F_1, \cdots, F_m)$; specifically, a point $\alpha \in \mathsf{A}^n$ is in this intersection if and only if R has a factor of the form $u_0 + \sum_{i=1}^{n} \alpha_i^d u_i$.

There are two difficulties with this approach, which are resolved in the remainder of this section. The first problem arises when we return to the original statement of the problem, where the polynomials $g_1, \cdots, g_n$ are not necessary homogeneous; the inhomogeneity of this new system makes the application of the resultant somewhat less straightforward. We cannot, for example, merely homogenize the g_i's by introducing a new variable, since the homogenized system may now have infinitely many projective zeros at infinity. To overcome this obstacle we use an "infinitesimal deformation" [8] or "generic perturbation" of these algebraic sets [16]. Similar methods appear in [25] when k is the field of complex numbers C.

We will limit ourselves primarily to elementary geometric arguments. The following Proposition will be used below.

Proposition 2.1 *The set-theoretic projection $\pi : \mathsf{A}^m \times \mathsf{P}^n \rightarrow \mathsf{A}^m$ is a closed continuous map. Let $X \subset \mathsf{A}^m \times \mathsf{P}^n$.*

1. *$\overline{\pi(X)} = \pi(\overline{X})$.*

2. *If X is irreducible, $\pi(X)$ is also irreducible.*

Proof. Continuity is obvious. That π is closed follows from the existence of resultant systems [22]. The other claims are straightforward consequences of these facts. □

2.1 Technical Lemmas

Let $G_1, \cdots, G_n$ be homogeneous polynomials in $k[x_0, \cdots, x_n]$ of degrees $d_1, \cdots, d_n \leq d$ respectively. We begin with a construction which always yields an "interesting" finite subset of $V(G_1, \cdots, G_n)$. The proofs of these Lemmas have been relegated to the Appendix.

Let t be a new indeterminate and define the polynomials $\hat{G}_1, \cdots, \hat{G}_n \in k[t][\overline{x}]$

$$\hat{G}_i(t,\overline{x}) \quad = \quad t x_i^{d_i} + (1-t)G_i(\overline{x}) \tag{3}$$

Let $V = V(\hat{G}_1, \cdots, \hat{G}_n) \subset \mathsf{A}_t^1 \times \mathsf{P}_x^n$. If X is a closed subset of $\mathsf{A}^1 \times \mathsf{P}^n$ and $\tau \in k$, write X_τ for set $X \cap \{t = \tau\} \hookrightarrow \mathsf{P}^n$, *i.e.* the fiber of the projection π at τ. Note that, for V as defined above, $V_0 = V(G_1, \cdots, G_n)$ and V_1 contains only the point $(1 : 0 : \ldots : 0)$. As τ varies continuously in A^1, the fibers V_τ yield a continuous deformation of the 0-dimensional set V_1 into V_0. The next Lemma investigates the structure of V.

Lemma 2.2 *For every irreducible component Z of V either*

1. *$\pi(Z)$ is a singleton and cod $Z \leq n$; or*

2. *$\pi(Z) = \mathsf{A}^1$ and cod $Z = n$.*

Moreover, there are always components of the second type.

Lemma 2.2 shows that the fibers V_τ are almost always 0-dimensional. We obtain a finite subset of $V_0 = V(G_1, \cdots, G_n)$ by taking a *limit* of these 0-dimensional systems as $\tau \rightarrow 0$.

Definition. Let X be a closed subset of $\mathsf{A}^1 \times \mathsf{P}^n$. Define $X^* = \overline{X \cap \{t \neq 0\}}$, *i.e.* the components of X^* are just the components of X not contained entirely in $\{t = 0\}$. Write X_0^* for fiber of X^* at $t = 0$. The set X_0^* is also denoted $\lim_{t \rightarrow 0} X_t$ in Fulton [8] Section 11.1.

Lemma 2.3 *V_0^* is a finite subset of $V_0 = V(G_1, \cdots, G_n)$ and contains all isolated points of V_0.*

Remark. The previous lemma still holds if we instead define the polynomials $\hat{G}_i$ by

$$\hat{G}_i(t',\overline{x}) \quad = \quad t' x_i^{d_i} + G_i(\overline{x}) \tag{4}$$

setting $t' = t/(1-t)$ in (3). This definition of the polynomials $\hat{G}_i$. will be used in the remainder of this section, since it simplifies the algorithms and their analyses.

2.2 A Resultant-based Decision Procedure

In this section we assume some familiarity with multivariate resultants, as in [17] or [21]. For further discussion of the computation of resultants, see [19].

Let $F_1, \cdots, F_m \in k[x_0, \cdots, x_n]$ be homogeneous polynomials of degree d. As in the previous section, $G_1, \cdots, G_n$ are homogeneous polynomials in $k[\overline{x}]$ of degrees $d_1, \cdots, d_n \leq d$, and $V = V(G_1, \cdots, G_n)$.

Let $\overline{u} = u_0, \cdots, u_n$ and $\overline{v} = v_1, \cdots, v_m$ be new indeterminates and define $\hat{V} = V(\hat{G}_1, \cdots, \hat{G}_n) \subset \mathsf{P}_{u,v}^{m+n} \times \mathsf{A}_t^1 \times \mathsf{P}_x^n$. It is clear that $\hat{V} = \mathsf{P}^{m+n} \times V$, and that the irreducible components of $\hat{V}$ are all sets of the form $\mathsf{P}^{m+n} \times Z$, for Z an irreducible component of V. So it is also true that $\hat{V}^* = \mathsf{P}^{m+n} \times V^*$.

Now define a homogeneous polynomial $L \in k[\overline{u}, \overline{v}][t][\overline{x}]$

$$L(\overline{x}, \overline{u}, \overline{v}) = \sum_{i=0}^{n} u_i x_i^d + \sum_{j=1}^{k} v_j F_j(\overline{x})$$

Note that L is an irreducible polynomial, and hence $V(L) \subset \mathsf{P}^{n+m} \times \mathsf{A}^1 \times \mathsf{P}^n$ is an irreducible hypersurface; we also denote this hypersurface by L. It is follows that

Lemma 2.4
$$(\hat{V} \cap L)^* = \hat{V}^* \cap L = (\mathsf{P}^{n+m} \times V^*) \cap L \ .$$

The proof of this Lemma is found in the Appendix.

Write $\pi : \mathsf{P}^{n+m} \times \mathsf{A}^1 \times \mathsf{P}^n \longrightarrow \mathsf{P}^{n+m} \times \mathsf{A}^1$ for the set-theoretic projection. The following Proposition summarizes some well known facts about the resultant.

Proposition 2.5 *The resultant of the G_i's and L with respect to $\overline{x}$ is a polynomial $R \in k[t, \overline{u}, \overline{v}]$ such that $V(R) = \pi(\hat{V} \cap L)$. R may be computed as a quotient of polynomials $M(t, \overline{u}, \overline{v})$ and $A(t)$, each of which is the determinant of a matrix of size $\leq \binom{nd+1}{n+1} < (3d)^n$ constructed uniformly from the coefficients of the G_i's and F_j's. The polynomial M is homogeneous in $\overline{u}$,$\overline{v}$ of degree $\leq nd^n$, and both M and A have degree $< (3d)^n$ in t. Neither M nor A vanishes identically, and both M and A can be constructed in sequential time $d^{O(n)}$, or parallel time $O(n^2 \log^2 d)$ using $O(\binom{nd+1}{n+1}^3)$ processors, in the elementary operations of $k[t, \overline{u}, \overline{v}]$ using the algorithm of [1].*

As noted by Renegar [20], it is never the case that $A(t) \equiv 0$, because $A(t)$ is the determinant of a matrix of the form $tI + B$, where all of the entries of B are field elements of k.

For notational convenience, write

$$L_{\overline{\alpha}}(\overline{u}, \overline{v}) = \sum_{i=0}^{n} \alpha_i^d u_i + \sum_{j=1}^{m} F_j(\overline{\alpha})$$

for $\overline{\alpha} \in \mathsf{P}^n$. Note that for no $\overline{\alpha}$ does $L_{\overline{\alpha}}$ vanish identically, and each polynomial $L_{\overline{\alpha}}$ is a linear form, hence irreducible.

Definition. Let $R \in k[t, \overline{u}, \overline{v}]$ be the resultant of $\hat{G}_1, \cdots, \hat{G}_n$ and L with respect to the variables $\overline{x}$. Define $R^*(t, \overline{u}, \overline{v})$ so that $R^* t^e = R$ and t does not divide R^*, and let $R_0^* = R^* \mid_{t=0}$; *i.e.* if

$$R(t, \overline{u}, \overline{v}) = \sum_{i=0}^{r} R_i(\overline{u}, \overline{v}) t^i$$

then $R_0^* = R_s$ for the least s such that $R_s \not\equiv 0$. This notation will be used more generally below.

Lemma 2.6

$$V(R_0^*) = V\left(\prod_{\overline{\alpha} \in V_0^*} L_{\overline{\alpha}}\right)$$

In particular, R_0^* can be written as a product of powers of the polynomials $L_{\overline{\alpha}}$ for $\overline{\alpha} \in V_0^*$.

Proof. Let $W = V(\hat{G}_1, \cdots, \hat{G}_n, L)$. By Lemma 2.4, $W^* = (\mathsf{P}^{n+m} \times V_0^*) \cap L$; but also

$$\begin{aligned}
\pi(W^*) &= \pi(\overline{W - \{t = 0\}}) \\
&= \overline{\pi(W) - \{t = 0\}} && (5) \\
&= \overline{V(R) - \{t = 0\}} && (6) \\
&= V(R)^* \\
&= V(R^*)
\end{aligned}$$

where (5) follows from Proposition 2.1-1, and (6) from Proposition 2.5. Hence

$$V(R_0^*) = V\left(\prod_{\overline{\alpha} \in V_0^*} L_{\overline{\alpha}}\right)$$

Since each $L_{\overline{\alpha}}$ is irreducible, the Nullstellensatz implies that

$$\text{radical}(R_0^*) = \left(\prod_{\overline{\alpha} \in V_0^*} L_{\overline{\alpha}}\right)$$

so the linear forms $L_{\overline{\alpha}}$ comprise all factors of R_0^*. □

These observations lead to the following efficient algorithm for problem considered in this section. Let $f_1, \cdots, f_m$ and $g_1, \cdots, g_n$ be polynomials in the ring $K[x_1, \cdots, x_n]$, with $deg\ f_i \leq d$ and $d_j = deg\ g_j \leq d$. For the moment we also assume that $V(g_1, \cdots, g_n)$ is finite. To apply the previous Lemmas, first homogenize all of the f_i's to the same degree; so for $i = 1, \cdots, m$, define

$$F_i(\overline{x}) = x_0^d f_i(x_1/x_0, \cdots, x_n/x_0)$$

Also homogenize each g_j in the standard manner and construct a suitable generic perturbation, as in (3) or (4) above; so for each $j = 1, \cdots, n$, define

$$G_j(t, \overline{x}) = t x_j^{d_j} + x_0^{d_j} g_j(x_1/x_0, \cdots, x_n/x_0)$$

Let $V = V(G_1, \cdots, G_n)$.

The algorithm now consists of two steps: first of constructing the polynomial $R_0^*(\overline{u}, \overline{v})$, as described above, from the resultant R of $G_1, \cdots, G_n$ and L, and then of determining whether R_0^* has a factor of the form $u_0 + p(u_1, \cdots, u_n)$. By Lemma 2.6, this occurs if and only if there is an *affine* point $\overline{\alpha} \in V_0^*$ which is a common zero of all of the F_i's (and hence of all f_i's). Since the set V_0^* contains all isolated points of V_0 — and hence also of $V_0 \cap \mathsf{A}^n = V(g_1, \cdots, g_n)$ — we have decided whether $V(g_1, \cdots, g_n) \cap V(f_1, \cdots, f_m) = \emptyset$.

Note also that for a suitable choice of elements $\beta_0, \cdots, \beta_n$ and $\gamma_1, \cdots, \gamma_m \in k$, it suffices to construct a representation of the points

$$(\alpha_0 : \sum_{i=0}^{n} \beta_i \alpha_i^d : \sum_{j=1}^{m} \gamma_j F_j(\overline{\alpha}))$$

for $\overline{\alpha} \in V_0^*$, *i.e.* we can recover the same information from these points. We will use this observation to reduce the complexity of the procedure sketched above by reducing the number of new variables in the computation from $n + m + 2$ to 4. (Below we take $\beta_i = b^{i-1}$ and $\gamma_j = c^{j-1}$, for b and c new indeterminates.)

Step 1. Recall that there are determinants M and A such that

$$A(t) R(t, \overline{u}, \overline{v}) = M(t, \overline{u}, \overline{v})$$

and $M, A \not\equiv 0$. Then it is clear that

$$A_0^* R_0^*(\overline{u}, \overline{v}) = R_0^*(\overline{u}, \overline{v})$$

and, since $A_0^* \in k$,

$$R_0^* \doteq M_0^*$$

i.e. they differ by only a non-zero constant factor. So it suffices to construct the polynomial M and determine whether M_0^* has a factor of the appropriate form. It is clear that the polynomial M_0^* is easily constructed from M.

Step 2. Now it remains to determine whether M_0^* has a factor of the form $u_0 + p(u_1, \cdots, u_n)$ for some linear p. Let a, b, c be new indeterminates and let M' be the image of M_0^* under the substitution

$$\begin{aligned} u_0 &\mapsto a \\ u_i &\mapsto b^i \quad \text{for } i = 1, \cdots, n \\ v_j &\mapsto c^j \quad \text{for } j = 1, \cdots, m \end{aligned}$$

Then the factors of M' are

$$\alpha_0^d a + \sum_{i=0}^{n} \alpha_i^d b^i + \sum_{j=1}^{m} F_j(\overline{\alpha}) c^j$$

for $\overline{\alpha} \in V_0^*$. The only factors of M' which are divisible by b are those arising from a point at infinity in $V_0^* \cap V(F_1, \cdots, F_m)$. Let M^* be the polynomial such that $b^e M^* = M'$ (for some e) and b does not divide M^*. Then no factor of $M^*(a, b, c)$ is divisible by b and $M_0^*(a, c) = M^* |_{b=0} \not\equiv 0$. It follows immediately that M', and hence also R_0^*, has a factor of the appropriate form if and only if $M_0^* |_{a=0} \equiv 0$.

For applications of this algorithm in the next section we will need to know its behavior when given *arbitrary* polynomials $g_1, \cdots, g_n$. We characterize this behavior in the statement of the Theorem.

Theorem 2.7 *The algorithm above decides whether there is a point $\overline{\alpha} \in V(g_1, \cdots, g_n)$ such that*

$$f_1(\overline{\alpha}) = \cdots = f_m(\overline{\alpha}) = 0 \tag{7}$$

subject to the following restrictions:

1. *if $V(g_1, \cdots, g_n)$ contains an isolated point $\overline{\alpha}$ which satisfies (7), then the procedure answers affirmatively; and*
2. *if the procedure answers affirmatively, then there is a point in $\overline{\alpha} \in V(g_1, \cdots, g_n)$ which satisfies (7).*

It requires sequential time $O((n+m)^5 d^{O(n)})$, or parallel time $O(n^3 \log^3 m \log d)$ using $(n+m)^{O(1)} d^{O(n)}$ processors, in the ring operations of the field K. When $K = \mathrm{Q}$ or $K = \mathrm{F}_q$, and b is a bound on the bit-length of the coefficients of the input polynomials, then the can be executed in sequential time $(b \log q + md)^{O(n)}$, or in sequential space polynomial in n and polylog in q, b, m and d.

The complexity of the algorithm is dominated by the construction of the polynomial m, which requires computing the deteminant of a matrix of size $\binom{D+n+1}{n+1} < (3d)^{n+1}$ over $K[t, \overline{u}, \overline{v}]$. Since substitution defines a ring homomorphism, construction of the determinant commutes with the substitution defined in *Step 2* above; so we may first apply the substitution, and then extract the polynomial M from the computed determinant. Hence it suffices to compute the determinant of a matrix of size $< (3d)^n$ with entries which are polynomials in $K[t, a, b, c]$ of degree $\leq max\{m, n\}$. This computation requires parallel time $O(n^3 \log^3 d \log m)$ or sequential time $O((n+m)^5 d^{O(n)})$ in the operations of K. The remaining operations on the polynomials require only selecting terms of least degree in some variable (t, b or a).

3 Deciding the emptiness of algebraic sets

Using the algorithm of the previous section, we now wish to show how, given m polynomials $f_1, \cdots, f_m$ in n variables, to construct n additional polynomials which define some common zero of the f_i's, if such a point exists. A sketch of the argument follows.

Let $X = V(f_1, \cdots, f_m)$ and assume that $\dim X = s \geq 0$. By a geometric argument, we may show that for almost every $a_{ij} \in k$ $(0 \leq i \leq n-s, \leq j \leq m)$, the polynomials

$$g_i(\overline{x}) \;=\; \sum_{j=1}^{m} a_{ij} f_j(\overline{x}) \qquad \text{for } i = 1, \ldots, n-s \tag{8}$$

form a regular sequence; in other words, $X_s = V(g_1, \cdots, g_{n-s})$ is a pure (unmixed) s-dimensional set. Since $X \subset X_s$ and V contains an s-dimensional component, component of X_s is also a component of X. By the Noether Normalization Theorem, any sufficiently generic $(n-s)$-dimensional linear variety meets every component of X_s properly; so again, for almost every choice of $b_1, \cdots, b_s \in k$, the polynomials

$$h_i(\overline{x}) \;=\; \sum_{j=1}^{n} b_i^{j-1} x_j \qquad \text{for } i = 1, \ldots, s \tag{9}$$

define a variety $L_s = V(h_1, \cdots, h_s) \subset \mathrm{A}^n$ with $L_s \cap X_s$ a non-empty finite set containing at least one point in each component of X_s. Since some component of X_s is also a component of X, $L_s \cap X_s$ contains a witness to the non-emptiness of X.

So to determine whether $X = \emptyset$, we will construct such polynomials for each possible dimension $s = 0, \ldots, n-1$, and then determine whether

$$X \cap V(g_1, \cdots, g_{n-s}, h_1, \cdots, h_s) \;=\; \emptyset$$

using the algorithm of Theorem 2.7. If $X \neq \emptyset$, then the polynomials constructed for $s = \dim X$ contain a witness, with probability 1 (appropriately defined with repsect to the Zariski topology on the space of parameters). To construct these polynomials *deterministically*, we will make use of counting arguments based on the degree of irreducible sets to show that the "random elements" may be chosen from any sufficiently large fixed subset of k. Such counting arguments are also used in the constructions of [6,11,14]. We rely on the following well known fact.

Lemma 3.1 *If $F_1, \cdots, F_m \in k[x_0, \cdots, x_n]$ are homogeneous polynomials of degree $\leq d$, then $V(F_1, \cdots, F_m)$ has at most d^s irreducible components of codimension $\leq s$.*

Proof. This may be proved by a straightforward induction, using Bezout's Theorem [13] Theorem 1.7. See also Heintz [14]. □

To begin, fix $f_1, \cdots, f_m \in K[x_0, \cdots, x_n]$ of maximum degree d. We may show

Lemma 3.2 *For each s, $0 \leq s \leq n+1$, there are s polynomials $g_1, \cdots, g_s$ of degree d such that*

1. *every component of $V(g_1, \cdots, g_s)$ has codimension $\leq s$;*
2. *every component of $V(f_1, \cdots, f_m)$ of codimension $< s$ is a component of $V(g_1, \cdots, g_s)$; and*

3. $V(f_1, \cdots, f_m) \subset V(g_1, \cdots, g_s)$.

If $A_1, \ldots, A_{n+1}$ are any fixed subsets of k with $|A_i| > (m-1)d^{i-1}$, then for some choice of elements $a_1, \cdots, a_{n+1}$, with each $a_i \in A_i$,

$$g_i(\overline{x}) \;=\; \sum_{j=1}^{m} a_i^{j-1} g_j(\overline{x}) \qquad \textit{for } i = 1, \cdots, n+1$$

satisfy these conditions.

The proof is similar to that of Lemma 3.3 below, and has been omitted.

To complete the algorithm sketched earlier, we show how to choose a sufficiently generic linear variety which meets the constructed set properly (*i.e.* in a finite set of points). The next Lemma shows how we may find one such hyperplane.

Lemma 3.3 *Let $s < n$ and let $B \subset k$ be a fixed finite set of cardinality $> (n-1)d^s$. Let $g_1, \cdots, g_s \in k[x_0, \cdots, x_n]$ be polynomials of degree $\leq d$ such that every component of $V(g_1, \cdots, g_s)$ has codimension s. Then for some element $b \in B$, the hyperplane*

$$h(\overline{x}) \;=\; \sum_{i=1}^{n} b^{i-1} x_i$$

has the following properties:

1. *every component of $V(g_1, \cdots, g_s) \cap V(h)$ has codimension $s+1$;*
2. *every affine component of $V(g_1, \cdots, g_s)$ contains an affine component of the set $V(g_1, \cdots, g_s) \cap V(h)$.*

Proof. To simplify the argument, we work in projective space and homogenize the given polynomials.

We want to choose the hyperplane H so that it meets every affine component of $V(g_1^h, \ldots, g_s^h)$ properly, and the intersection with each such component contains an affine component. Let P be a set of points which meets every component of $V(g_1^h, \ldots, g_s^h) \cap \{x_0 = 0\}$. Since this set has no more than d^s components, we may assume that $|P| = d^s$.

Choose an element b such that

$$\sum_{i=1}^{n} \alpha_i b^{i-1} \neq 0 \qquad \text{for all } \overline{\alpha} \in P \tag{10}$$

As above, there are at most $(n-1)d^s$ elements $b \in k$ which do not satisfy this condition, so some element $b \in B$ must work. Define $H(\overline{x}) = \sum_{i=1}^{n} b^{i-1} x_i$. We wish to show that whenever H satisfies (10), it satisfies the conditions of the Lemma.

1. Since $s < n$, each affine component Z of $V(g_1^h, \ldots, g_s^h)$ is at least 1-dimensional and so has a non-empty intersection with the hyperplane at infinity $\{x_0 = 0\}$ by the Projective Dimension Theorem (Hartshorne [13] Section 1.7). This implies that there is a point $\overline{\alpha} \in Z \cap P$ such that $H(\overline{\alpha}) \neq 0$; hence $Z \not\subset V(H)$. By Proposition A.1, every component of $Z \cap V(H)$ has codimension $s+1$.
2. Assume that for some affine component Z of $V(g_1^h, \ldots, g_s^h)$, $Z \cap V(H) \subset Z \cap \{x_0 = 0\}$. Since every component of each of these sets has codimension $s+1$, every component of $Z \cap V(H)$ is a component of $Z \cap \{x_0 = 0\}$. But, because $Z \cap V(H) \neq \emptyset$, this contradicts (10); so no component of $Z \cap V(H)$ is contained in $\{x_0 = 0\}$.

So we may take h in the statement of the Lemma to be this polynomial H. □

Now let $f_1, \cdots, f_m \in k[x_1, \cdots, x_n]$ be arbitrary polynomials, $V = V(f_1, \cdots, f_m)$ and let $d = \max\{deg\ f_i\}$. Let A be a fixed subset of k of cardinality $> \max\{m-1, n-1\}d^n$. For each $s = 0, \cdots, n-1$ — a "guess" of the dimension of V — and for each choice of elements $a_1, \cdots, a_n \in A$ we may define the n polynomials

$$g_i^{s,a_1 \cdots a_n}(\overline{x}) \;=\; \sum_{j=1}^{n} a_i^{j-1} x_j \qquad i = 1, \cdots, s \tag{11}$$

$$g_i^{s,a_1 \cdots a_n}(\overline{x}) \;=\; \sum_{j=1}^{m} a_i^{j-1} f_j(\overline{x}) \quad i = s+1, \cdots, n \tag{12}$$

By Lemmas 3.2 and 3.3, it follows that if $\dim V = s$, then for some choice of $a_1, \cdots, a_n$, the set $V(g_1^{s,a_1 \cdots a_n}, \cdots, g_n^{s,a_1 \cdots a_n}) \subset \mathsf{A}^n$ is 0-dimensional, and contains a point $\overline{\alpha}$ in every s-dimensional component of V. Hence, if V is non-empty, then some such sequence of polynomials will define a set with an isolated solution in V, and so the algorithm will answer affirmatively. On the other hand, if the algorithm gives an affirmative answer for *any* such sequence of polynomials $g_1, \cdots, g_n$, then some zero of these polynomials is a witness to the fact that $V \neq \emptyset$.

Theorem 3.4 *Let K be a subfield of k and $f_1, \cdots, f_m \in K[x_1, \cdots, x_n]$ polynomials of degree $\leq d$. It can be decided whether the polynomials $f_1, \cdots, f_m$ have a common solution in the algebraic closure of the coefficient field K in k. The decision procedure requires sequential time $(mn)^{O(c)} d^{O(cn)}$, where $c = cod\, V(f_1, \cdots, f_m)$, or parallel time $O(n^3 \log^3 d \log m)$ using $(mn)^{O(n)} d^{O(n^2)}$ processors, in the ring operations of the coefficient field K.*

The bound on the complexity, with respect to the field operations of k, follows immediately from the analysis of Theorem 2.7 and the number of different choices for the parameters parameters s and $a_1, \cdots, a_n$ which must be tried (fewer than $(n+m)^n d^{n^2}$ of them). It is clear that all computation occurs in the coefficient field K, when K is infinite, or a sufficiently large finite field. In the case where $K = \mathsf{F}_q$ is a small finite field, the algorithm requires a finite extension containing enough elements; hence it suffices to construct some $\overline{\alpha} \in k$ of sufficiently large degree over F_q. The straightforward approach entails finding an irreducible polynomial $f(X) \in \mathsf{F}_q[X]$ of this degree (or higher), and using the standard algorithms for the field operations of $K[X]/(f)$; this incurs no significant overhead in the sequential algorithm described above. Alternatively, we may choose $\alpha \in k$, of "sufficiently large degree" over F_q (so that we may effectively treat α as an indeterminate); since the elements of $\mathsf{F}_q[\alpha]$ which arise in the construction and verification procedures will all be polynomials in α of degree strictly less than $(n+1)(n+m+1)(3d)^{n+1}$, the parallel algorithm has the complexity stated below, with respect to the operations of the coefficient field.

Corollary 3.5 *When $K = \mathsf{Q}$ or $F = \mathsf{F}_q$, then the algorithm requires sequential time $||f_1, \cdots, f_m||^{O(c)} d^{O(cn)}$ or space polynomial in n and polylog in $||f_1, \cdots, f_m||$.*

It is clear that, if the A_i are chosen sufficiently large, we may also choose the elements $a_1, \cdots, a_n$ uniformly at random from the sets $A_1, \ldots, A_n$ to guarantee that the algorithm above succeeds with sufficiently high probability.

4 Deciding the Emptiness of Semialgebraic Sets

The problem of quantifier elimination is well known in logic. It figures prominently in Tarski's original proof of the completeness of the theory of real-closed fields. Quantifier elimination in the theory of an algebraically-closed field was first shown using the familiar univariate resultant and the construction of resolvents; this procedure, however, can produce formulas which are double-exponentially larger than the original formula. Most recently, Grigor'ev and Chistov produced a double-exponential time algorithm which runs in exponential time when restricted to formulas with a bounded number of alternations of quantifiers. Below we improve upon these results with a parallel algorithm which requires only polynomial time under this same restriction. We begin by reviewing some terminology.

The *atomic formulas* in the first-order theory of algebraically-closed fields may always be written in the form $f(x_1, \cdots, x_n) = 0$, where f is a polynomial. Strictly speaking, the only constants in the language of this theory are the elements 0 and 1, hence f may be assumed to have integral coefficients; however, to attain greater generality, we will allow these coefficients to range over any fixed field K. It is well known that every quantifier-free formula is equivalent to a formula in disjunctive normal-form (DNF). It is also well known that any formula in the theory of algebraically-closed fields is equivalent to a quantifier-free formula (also called a *resultant* of the formula).

In the next section we give a parallel algorithm for putting a formula into DNF. The following section will use this DNF algorithm, together with the decision procedures of the previous two sections, to give an algorithm for quantifier elimination in the theory of the algebraically-closed field k.

4.1 Disjunctive normal form

If $\Sigma \subset k[x_1, \cdots, x_n]$ is a finite set of polynomials and $T \subset \Sigma$, then the set of points $V(T) - V(\Sigma - T)$ is called a Σ-cell. (The terminology is due to Heintz.) This set may also be defined as the set of points satisfying the conjunctive formula

$$\bigwedge_{f \in T} f(\overline{x}) = 0 \quad \wedge \quad \bigwedge_{g \in \Sigma - T} g(\overline{x}) \neq 0$$

Such a formula will also be called a Σ-cell.

Let $\phi(\overline{x})$ be any quantifier-free formula and $\Sigma = \{f_1, \cdots, f_m\}$ the collection of all polynomials occurring in the atomic formulas of $\phi(\overline{x})$ Then

$$\phi(\overline{x}) \quad \Leftrightarrow \quad \bigwedge_{\psi \Rightarrow \phi} \psi\overline{x} \tag{13}$$

where ψ ranges over all non-empty Σ-cells, is an equivalent DNF formula. So it is sufficient to show that we can efficiently enumerate all non-empty Σ-cells which imply ϕ. In fact, if we can enumerate *all* non-empty Σ-cells, then we can efficiently filter out those which do not imply ϕ. Since each cell ψ is a conjunction of atomic formulas and negations of atomic formulas which occur in ϕ, checking each implication reduces to evaluating a propositional formula (ϕ) given a truth assignment (ψ) to its atomic propositions; this problem can be solved in parallel time logarithmic in the number of logical connectives in ϕ using fast parallel expression evaluation, as in [9].

So we only need to show that if $\Sigma = \{f_1, \cdots, f_m\}$ then all Σ-cells can be enumerated in parallel. What makes this possible is the following theorem of Heintz ([14] Corollary 2).

Theorem 4.1 (Heintz) *If $d = max_i\{\deg f_i\}$, then there are at most $(1+md)^n$ non-empty $\{f_1, \cdots, f_m\}$-cells.*

Given this fact, one can construct the list of all Σ-cells using a straightforward divide-and-conquer scheme. We partition $\Sigma = \Sigma_1 \cup \Sigma_2$ into sets of roughly equal size and recursively find all non-empty Σ_1- and Σ_2-cells. Then we construct all Σ-cells which are consistent with those constructed for the subsets Σ_1 and Σ_2; *i.e.* for each Σ_1-cell ψ_1 and each Σ_2-cell ψ_2, we construct the Σ-cell $\psi_1 \wedge \psi_2$, which may be written

$$\bigwedge_{f \in T} f(\overline{x}) = 0 \quad \wedge \quad \bigwedge_{g \notin T} g(\overline{x}) \neq 0 \tag{14}$$

for some $T \subset \Sigma$. By Heintz's Theorem, this yields a collection of at most $(\frac{1}{2}md+1)^{2n}$ Σ-cells, which must include all non-empty ones.

We note that at the basis of the recursion, when $\Sigma = \{f\}$, there are always exactly two non-empty cells. In the general case, we will weed out all of the empty cells using Rabinowitsch's trick [15] and the algorithm of Theorem 3.4. For example, to determine whether the Σ-cell (14) is non-empty we choose w a new indeterminate and ask whether there exists a solution (in $\overline{x}$ and w) to the polynomial equations $f(\overline{x}) = 0$, for all $f \in T$, and

$$w \prod_{f \notin T} f(\overline{x}) - 1 \quad = \quad 0$$

This new system of polynomials has a solution if and only if the Σ-cell (14) is non-empty. By Heintz's Theorem, at most $(1+md)^n$ of these cells will be identified as non-empty. There are thus $\log m$ levels in this construction, each requiring approximately $(md)^{2n}$ parallel invocations of the algorithm of Theorem 3.4; in each case, this algorithm is applied to a set of $\leq m$ polynomials in $n+1$ variables of degree at most $md+1$.

Theorem 4.2 (DNF) *Let $\phi(\overline{x})$ be a quantifier-free formula with l logical connectives. Assume that $f_1, \cdots, f_m$ are the polynomials which occur in the atomic formulas of $\phi(\overline{x})$, and that these are elements of the ring $K[x_1, \cdots, x_n]$ of degree $\leq d$. Then an equivalent DNF formula $\phi'(\overline{x})$ can be computed in parallel time $O(n^3 \log^2 md + \log l)$ or sequential time $(nmd)^{n^2+O(n)} + (lmd)^{O(n)}$. In addition, every polynomial occurring in $\phi'(\overline{x})$ also occurs in $\phi(\overline{x})$, and the number of logical connectives occurring in $\phi'(\overline{x})$ is no more than $m(md+1)^n$.*

4.2 Quantifier elimination

We first assume that all formulas are in prenex form — written

$$(Q_1 x_1) \cdots (Q_n x_n)\ \phi(\overline{y}, \overline{x}) \qquad \text{where } Q_i = \exists \text{ or } Q_i = \forall$$

and ϕ is a quantifier-free formula. Write $(Q\overline{x})$ to abbreviate a string of like quantifiers $(Qx_1)(Qx_2)\cdots(Qx_n)$.

Fix a set of polynomials $\Sigma = \{f_1, \cdots, f_m\} \subset k[y_1, \cdots, y_{n_y}][x_1, \cdots, x_{n_x}]$ with $deg_x\ f_i \leq d$ and $deg_y\ f_i \leq d$. Using the algorithm of Theorem 3.4, for *any fixed* $\overline{y} \in k$ we can decide whether

$$(\exists \overline{x}) \quad f_1(\overline{y}, \overline{x}) = \cdots = f_m(\overline{y}, \overline{x}) = 0$$

Now applying this same algorithm *symbolically* to the polynomials $f_1, \cdots, f_m$ — considered as polynomials in $\overline{x}$ with coefficients in $k[\overline{y}]$ — gives a criterion for the existence of such a point $\overline{x}$ in terms of $\overline{y}$. Recall that the algorithm begins with a fixed subset A of k, and for each integer s $(0 \leq s < n)$ and each sequence $a_1, \cdots, a_n \in A^n$ constructs a determinant $M^{s,a_1,\cdots,a_n}$. To simplify notation, write

$$\begin{aligned} M^{s,a_1\cdots a_n}(\overline{y})(t,a,b,c) &= \sum_{i=0}^{nd^s} M_i^{s,a_1\cdots a_n}(\overline{y})(a,b,c)t^i \\ M_i^{s,a_1\cdots a_n}(\overline{y})(a,b,c) &= \sum_{j=0}^{nd^s} M_{ij}^{s,a_1\cdots a_n}(\overline{y})(a,c)b^j \\ M_{ij}^{s,a_1\cdots a_n}(\overline{y})(a,c) &= \sum_{k=0}^{md^s} M_{ijk}^{s,a_1\cdots a_n}(\overline{y})(a)c^k \end{aligned}$$

Then, by Theorem 3.4, the formula presented in Figure 1 is true for all fixed $\overline{y} \in \mathsf{A}^n$. (This formula merely spells out the conditions under which the polynomial M_0^* constructed in the previous algorithm is M_{ij}, and when the latter is divisible by a.) Note that an assertion of the form "$M_i^{s,a_1\cdots a_n} \equiv 0$", for example, states only that all coefficients of this polynomial are zero; so if we construct this formula symbolically — *i.e.* where the coefficients are polynomials in $\overline{y}$ — then Figure 1 represents an equivalent quantifier-free formula in $\overline{y}$. By this construction, there will be fewer than $(md)^{n^2+O(n)}$ atomic formulas in this quantifier-free formula, and each polynomial will have degree less than $n(1+md)^{n+1}$ in the remaining variables.

To eliminate quantifiers from an arbitrary existential formula $(\exists \overline{x})\ \phi(\overline{y}, \overline{x})$, in which ϕ is quantifier-free, we first find an equivalent DNF formula for ϕ, then push the quantifiers through the outermost disjunction and finally apply the above transformation to each disjunct. The final formula now has fewer than $(md)^{n^2+O(n)}$ atomic formulas, featuring at most $(md)^{n^2+O(n)}$ distinct polynomials of degree $\leq n(md)^{n+1}$ in the remaining variables $\overline{y}$.

Theorem 4.3 *Let $(\exists \overline{x})$ $\phi(\overline{y}, \overline{x})$ be a formula as described above, with l logical connective and $\overline{y} = y_1, \cdots, y_r$. Then it is possible to compute an equivalent quantifier-free formula $\phi'(\overline{y})$ in parallel time $O(n^3 \log^2 md + \log l)$ or sequential time $(lmd)^{n^2+O(n)}$ in the operations of $K[\overline{y}]$, or $O((r+n)^4 log^3 dm + \log l)$ parallel and $O((lmd)^{n^2+rn+O(n+r)})$ sequential time in the operations of K.*

Recall that any formula in prenex form may be written as

$$\begin{aligned} &\exists \overline{x}^{(1)}\ \forall \overline{x}^{(2)}\ \ldots \exists \overline{x}^{(a)}\ \phi(\overline{y}, \overline{x}^{(1)}, \cdots, \overline{x}^{(a)}) \Leftrightarrow \\ &\qquad \exists \overline{x}^{(1)}\ \neg(\exists \overline{x}^{(2)}\ \ldots \neg(\exists \overline{x}^{(a)}\ \phi(\overline{y}, \overline{x}^{(1)}, \cdots, \overline{x}^{(a)}))\cdots) \end{aligned}$$

where ϕ is quantifier free; we say that such a formula has a alternations of quantifiers. It is clear that a iterations of the previous algorithm can now be used to eliminate quantifiers from any such prenex formula. For arbitrary formulas (not in prenex form), we may apply the algorithm recursively to eliminate quantifiers from all subformulas.

Corollary 4.4 *Let $\psi(\overline{y})$ be a prenex formula*

$$Q_1\overline{x}^{(1)} \cdots Q_a\overline{x}^{(a)}\ \phi(\overline{y}, \overline{x}^{(1)}, \cdots, \overline{x}^{(a)})$$

in the first-order theory of algebraically closed fields (of arbitrary characteristic). Assume that all constants occurring in ϕ are elements of the field K. Let a be the number of alternations of quantifiers, n the number of variables in ϕ, m the number of atomic formulas of ϕ, l the number of logical connectives in ϕ, and d the maximum degree of any polynomial occurring in ϕ. Then the algorithm sketched above will construct an equivalent quantifier-free formula $\psi'(\overline{y})$ in parallel time $(n \log md)^{O(a)} + O(\log l)$ or sequential time $(lmnd)^{O(n^{2a})}$ in the operations of the field K. The resulting formula ψ' will have fewer than $(mnd)^{O(n^{2a})}$ atomic formulas and degree no more than $(mnd)^{O(n^{2a-1})}$ in the variables $\overline{y}$.

If $K = \mathsf{Q}$ or $K = \mathsf{F}_q$, then the time complexity of the algorithm, in terms of bit operations, is bounded by $n^{O(a)} \log^{O(1)} \|f_1, \cdots, f_m\|$ for parallel execution, or $\|f_1, \cdots, f_m\|^{O(n)^{(2a)}}$ for sequential execution. In particular, the construction yields an EXPSPACE algorithm for quantifier elimination, which requires only PSPACE when the number of alternations of quantifiers is bounded.

5 Lower Bounds

In this section we address the problem of lower bounds for the problems treated in the previous sections. We consider lower bounds only for parallel algebraic algorithms over an algebraically closed field k (*i.e.* the arithmetic operations are the field operations of k) [23]. We make no uniformity assumptions.

We first consider the problem of deciding the emptiness of an algebraic set. For simplicity, we treat only the case of $n+1$ polynomials in n variables; by lemma 3.2, there is always a random reduction of the problem of m polynomials $f_1, \cdots, f_m$ to one of exactly $n+1$ polynomials.

Proposition 5.1 *Let $f_1, \cdots, f_{n+1} \in k[x_1, \cdots, x_n]$ with $d_i = \deg f_i$. Any parallel algebraic procedure which decides whether*

$$(\exists \overline{x}) \qquad f_1(\overline{x}) = \cdots = f_{n+1}(\overline{x}) = 0$$

for all $f_1, \cdots, f_{n+1} \in k[\overline{x}]$ requires depth (parallel time) at least $\log \prod_{i=1}^{n+1} d_i - 1$.

Proof. For simplicity we will assume that $\deg f_1 = \ldots = \deg f_{n+1} = d$; the general case is similar.

Choose d so that the characteristic of k does not divide d. We consider the polynomials

$$\begin{aligned} \alpha &= x_1^d \\ x_i &= x_{i+1}^d \qquad \text{for } i = 1, \ldots, n-1 \\ x_n &= \beta \end{aligned}$$

for $\alpha, \beta \in k$. Clearly this set of polynomials has a common zero if and only if $\alpha = \beta^{d^n}$.

Since the assumed decision procedure is algebraic, we may consider α and β indeterminates and use the given procedure to construct a formula (perhaps large) which is true if and only if $\alpha = \beta^{d^n}$. If the given procedure is division-free, then the constructed formula defines semi-algebraic set in A^2. But this set is just $\{\alpha = \beta^{d^n}\}$, which is both closed and irreducible. Hence it follows that some polynomial occurring

$$(\exists\overline{x})\ f_1(\overline{y},\overline{x}) = \cdots f_m(\overline{y},\overline{x}) = 0 \quad\Leftrightarrow\quad \bigvee_{0\le s<n}\ \bigvee_{a_1\cdots a_n\in A^n}\ \bigvee_{0\le i\le nd^s} M_i^{s,a_1\cdots a_n} \not\equiv 0 \ \wedge \bigwedge_{i'<i} M_{i'}^{s,a_1\cdots a_n} \equiv 0 \ \wedge$$
$$\bigvee_{0\le j\le nd^s}\left(M_{ij}^{s,a_1\cdots a_n} \not\equiv 0 \wedge \bigwedge_{j'<j} M_{ij'}^{s,a_1\cdots a_n} \equiv 0 \wedge M_{ij0}^{s,a_1\cdots a_n} \equiv 0 \right)$$

Figure 1: Quantifier free formula derived from the decision procedure

in the constructed formula is divisible by $\alpha = \beta^{d^n}$, and has degree $\geq d^n$. Since the degree of the resulting formula is determined only by the depth of the given computation, this depth must be $\geq \log_2 d^n - 1 = n\log_2 d - 1$.

It is not difficult to see that, when the computation is not division-free, a similar formula can be constructed in which the degree of the polynomials is still related to the depth of the computation. □

Two additional points are worth noting. First, using a similar argument one may show that the degree of the projection of this closed set is at least d^n; the algorithm of §3 gives an upper bound of nd^{n+1} on this degree. Second, the test polynomials used above are sparse. Hence an one cannot hope to significantly improve the performance of algebraic algorithms for this problem on sparse polynomials.

For the decision problem in the theory of an algebraically-closed field, we adapt the argument above and the test formula of [14] or [2] to show

Proposition 5.2 *Any procedure for quantifier elimination in the theory of k requires sequential time $\geq ((n-4)^{a/2} - 1)\log d - 1$ on formulas with a alternations of quantifiers and polynomials in n variables of degree at most d. Any parallel algebraic decision procedure for sentences in this theory requires depth $\geq ((n-4)^{a/2} - 1)\log d - 1$. Moreover, there are sparse formulas for which these bounds are attained.*

6 Summary

In this paper we have given a parallel polynomial time algorithm for deciding when a set of multivariate polynomials has a common zero over the algebraic closure of its coefficient field; this was then extended to yield an algorithm for quantifier elimination in the first-order theory of an algebraically closed field k, and hence a decision procedure for sentences in that theory. In particular, when the coefficient field is Q or F_q there is a PSPACE decision procedure for sentences with a bounded number of quantifier alternations. In addition, the constructions introduced in §2 extend the algorithmic use of homotopy methods to fields of finite characteristic.

One noteworthy application occurs in the area of computational commutative algebra. It is know that the problem of ideal membership is hard for EXPSPACE; *i.e.* given polynomials $g, f_1, \cdots, f_m$, determine whether g is in the ideal generated by the f_i's. On the other hand, the previous results have shown that testing membership in a *radical ideal* of the polynomial ring $k[x_1, \cdots, x_n]$ is in PSPACE. The radical of an ideal I is defined

$$\text{radical}(I) \quad = \quad \{g \mid g^N \in I \text{ for some } N\}$$

and I is a radical ideal if radical$(I) = I$. By the Nullstellensatz,

$$\begin{aligned} & g \in \text{radical}(f_1, \cdots, f_m) \Leftrightarrow \\ & \quad \Leftrightarrow \quad g \text{ vanishes on all points in } V(f_1, \cdots, f_m) \\ & \quad \Leftrightarrow \quad (\forall\overline{x}) \left(\bigwedge_{i=1}^{m} f_i(\overline{x}) = 0\right) \Rightarrow g(\overline{x}) = 0 \end{aligned}$$

This last question is decidable in PSPACE by the results of §4.

7 Acknowledgements

I am indebted to Jim Renegar for many helpful discussions, and to Dexter Kozen for reading and commenting on an earlier draft of this paper. I would also like to thank the participants in the Computational Algebra Seminar at Cornell University — especially Mike Stillman and Lorenzo Robbiano — for their useful comments.

A Proof of Lemmas

The following Theorem will be used below.

Proposition A.1 *Let $X \subset \mathsf{A}^m \times \mathsf{P}^n$ be an irreducible closed set of codimension r and H a hypersurface. Then if $X \not\subset H$, every irreducible component of $X \cap H$ has codimension $r+1$.*

Proof. See Matsamura [18] Theorem 13.6 and Hartshorne [13] 1.11A. □

The two Lemmas following are used in Section 2.1.

Lemma A.2 *For every irreducible component Z of V either*

1. *$\pi(Z)$ is a singleton and cod $Z \leq n$; or*
2. *$\pi(Z) = \mathsf{A}^1$ and cod $Z = n$.*

Moreover, there are always components of the second type.

Proof. If Z is an irreducible closed set, then $\pi(Z)$ is an irreducible closed set as well. But the only irreducible closed subsets of A^1 are the single points and the entire space. By Proposition A.1, every component of V is at least 1-dimensional. However, if Z is a component such that $\pi(Z) = \mathsf{A}^1$, then Z_1 is a non-empty set containing only the point $(1:0:\cdots:0)$; hence Z is at most 1-dimensional (Proposition A.1).

To see that there are always components of the second type, note that $V_1 = \{(1:0:\cdots:0)\}$. It follows that this point lies on some 1-dimensional component Z of V. Clearly this component can not lie entirely within $\{t = 1\}$, so $\pi(Z) = \mathsf{A}^1$. □

Lemma A.3 *V_0^* is a finite subset of $V_0 = V(G_1, \cdots, G_n)$ and contains all isolated points of V_0.*

Proof. V^* is just the union of all components of V not contained in $\{t = 0\}$. So V_0^* is the set of all points where some component Z of V, with $\pi(Z) = \mathsf{A}^1$, meets the set $\{t = 0\}$. Since each such Z is an irreducible 1-dimensional set and $Z \cap \{t = 0\}$ a proper closed subset of Z, Z_0 is a 0-dimensional set. Since V has only finitely many components, V_0^* is also 0-dimensional.

Assume that $\overline{\alpha}$ is an isolated point of V_0. As above, we note that $(0, \overline{\alpha})$ must lie on a higher dimensional component Z of V, and that $\pi(Z) = \mathsf{A}^1$. Hence $\overline{\alpha} \in V_0^*$. □

This final Lemma is used in Section 2.2.

Lemma A.4

$$(\hat{V} \cap L)^* \quad = \quad \hat{V}^* \cap L \quad = \quad (\mathsf{P}^{n+m} \times V^*) \cap L$$

Proof. It is clear that $(\hat{V} \cap L)^* \subset \hat{V}^* \cap L$. So it suffices to show that if $\hat{Z}$ is any component of $\hat{V}$ not contained in $\{t = 0\}$, then no component of $\hat{Z} \cap L$ is contained in $\{t = 0\}$.

Let $\hat{Z} = \mathsf{P}^{n+m} \times Z$ be an irreducible component of $\hat{V}$, for Z a component of V. Assume also that $Z \not\subset \{t = \tau\}$ for all $\tau \in k$, so cod $\hat{Z} = n$ (Lemma 2.2). Since L is an irreducible hypersurface and $\hat{Z} \not\subset L$, every component of $\hat{Z} \cap L$ has codimension $n + 1$. On the other hand, Lemma 2.2 and the definition of L imply that every irreducible component of $\hat{Z} \cap L \cap \{t = 0\}$ is a set of the form

$$\{L(\overline{\alpha}, \overline{u}, \overline{v}) = 0\} \times \{0\} \times \{\overline{\alpha}\} \subset \mathsf{P}^{n+m}_{u,v} \times \mathsf{A}^1_t \times \mathsf{P}^n_x$$

for some point $\overline{\alpha} \in V_0^*$. Since such a set has codimension $n + 2$, no component of $\hat{Z} \cap L$ is contained in $\{t = 0\}$. Hence no component of $\hat{V}^* \cap L$ is contained in $\{t = 0\}$, which implies that $\hat{V}^* \cap L \subset (\hat{V} \cap L)^*$. □

References

[1] S. J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18:147–150, 1984.

[2] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. manuscript.

[3] J. Canny. *The Complexity of robot motion planning.* PhD thesis, MIT, 1987.

[4] J. Canny. Generalized characteristic polynomials. manuscript, 1988.

[5] A. L. Chistov. Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time. *J. Soviet Math.*, 34:1838–1882, 1986.

[6] A. L. Chistov and D. Y. Grigor'ev. Complexity of quantifier elimination in the theory of algebraically closed fields. *LNCS*, pages 17–31, 1985.

[7] N. Fitchas, A. Galligo, and J. Morgenstern. Algorithmes rapides en séquentiel et en parallele pour l'élimination de quantificateurs en géométrie élémentaire. Revised preprint. To appear in: Séminaire Structures Algébriques Ordonnées, UER de Mathématiques Université de Paris VII.

[8] W. Fulton. *Intersection Theory.* Springer Verlag, 1980.

[9] A. Gibbons and W. Rytter. *Efficient Parallel Algorithms.* Cambridge University Press, 1988.

[10] D. Y. Grigor'ev. Factorization of polynomials over a finite field and the solution of systems of algebraic equations. *J. Soviet Math.*, 34(4):1762–1803, 1986.

[11] D. Y. Grigor'ev. The complexity of the decision problem for the first order theory of algebraically closed fields. *Math. USSR Izvestiya*, 29(2):459 - 475, 1987.

[12] D. Y. Grigor'ev and A. L. Chistov. Fast decomposition of polynomials into irreducible ones and the solution of systems of algebraic equations. *Soviet Math. Dokl.*, 29(2), 1984.

[13] R. Hartshorne. *Algebraic Geometry.* Springer Verlag, 1980.

[14] J. Heintz. Definibility and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24:239–277, 1983.

[15] W. Hodges. *Building Models by Games.* LMS Student Texts 2, 1986.

[16] Lazarsfeld. Excess intersection of divisors. *Compositio Math.*, 38:287–297, 1974.

[17] F. S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge Tracts in Mathematics and Mathematical Physics. Cambridge University Press, 1916.

[18] H. Matsamura. *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics 8. Cambridge U. Press, 1988.

[19] J. Renegar. On the worst case arithmetic complexity of approximating zeros of systems of polynomials. Technical Report 748, School of Operations Research and Industrial Engineering, Cornell University, 1987.

[20] J. Renegar. A faster PSPACE algorithm for deciding the existential theory of the reals. Technical Report 792, School of Operations Research and Industrial Engineering, Cornell University, 1988.

[21] van der Waerden. *Modern Algebra*, volume 2. F. Ungar Publishing Co., third edition, 1950.

[22] van der Waerden. *Modern Algebra*, volume 2. F. Ungar Publishing Co., fifth edition, 1970.

[23] J. van zur Gathen. Parallel algorithms for algebraic problems. *SIAM J. Comput.*, 13(4):802–824, 1984.

[24] N. N. Vorob'ev and D. Y. Grigor'ev. Finding real solutions of systems of algebraic inequalities in subexponential time. *J. Soviet Math.*, 32:316–320, 1985.

[25] W. Zulehner. A simple homotopy method for determining all isolated solutions to polynomial systems. *Mathematics of Computation*, 50(181):167–177, 1988.