Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition

George E. Collins*
University of Wisconsin, Madison
University of Kaiserslautern

1. Introduction. Tarski in 1948, [18] published a quantifier elimination method for the elementary theory of real closed fields (which he had discoverd in 1930). As noted by Tarski, any quantifier elimination method for this theory also provides a decision method, which enables one to decide whether any sentence of the theory is true or false. Since many important and difficult mathematical problems can be expressed in this theory, any computationally feasible quantifier elimination algorithm would be of utmost significance.

However, it became apparent that Tarski's method required too much computation to be practical except for quite trivial problems. Seidenberg in 1954, [17], described another method which he thought would be more efficient. A third method was published by Cohen in 1969, [3]. Some significant improvements of Tarski's method have been made by W. Böge, [20], which are described in a thesis by Holthusen, [21].

This paper describes a completely new method which I discoverd in February 1973. This method was presented in a seminar at Stanford University in March 1973 and in abstract form at a symposium at Carnegie-Mellon University in May 1973. In August 1974 a full presentation of the method was delivered at the EUROSAM 74 Conference in Stockholm, and a preliminary version of the present paper was published in the proceedings of that conference, [8].

*This research was partially supported by National Science Foundation grants GJ-30125X and DCR74-13278.

The method described here is much more efficient than the previous methods, and therefore offers renewed hope of practical applicability. In fact, it will be shown that, for a prenex input formula ϕ, the maximum computing time of the method is dominated, in the sense of [5], by $(2n)^{2^{2r+8}} m^{2^{r+6}} d^3 a$, where r is the number of variables in ϕ, m is the number of polynomials occurring in ϕ, n is the maximum degree of any such polynomial in any variable, d is the maximum length of any integer coefficient of any such polynomial, and a is the number of occurrences of atomic formulas in ϕ. Thus, for fixed r, the computing time is dominated by a polynomial function $P_r(m,n,d,a)$. In contrast, it can be shown that the maximum computing times of the methods of Tarski and Seidenberg are exponential in both m and n for every fixed r, including even r=1, and this is likely the case for Cohen's method also. (In fact, Cohen's method is presumbly not intended to be efficient.) Böge's improvement of Tarski's method eliminates the exponential dependency on m, but the exponential dependency on n remains.

Fischer and Rabin, [9], have recently shown that every decision method, deterministic or non-deterministic, for the first order theory of the additive group of the real numbers, a fortiori for the elementary theory of a real closed field, has a maximum computing time which dominates 2^{cN} where N is the length of the input formula and c is some positive constant. Since m, n, d, r and a are all less than or equal to N (assuming that x^n must be written as $x \cdot x \cdot \ldots \cdot x$), the method of this paper has a computing time dominated by $2^{2^{kN}}$ where in fact $k \leq 8$. The result of Fischer and Rabin suggests that a bound of this form is likely the best achievable for any deterministic method.

In a letter received from Leonard Monk in April 1974, I was informed that he and R. Solovay had found a decision method, but not a quantifier elimination method, with a maximum computing bound of the form $2^{2^{2^{kN}}}$. However, the priority and superiority of the method described below are easily established.

The most essential observation underlying the method to be described is that if $\mathcal{A}$ is any finite set of polynomials in r variables with real coefficients, then there is a decomposition of r-dimensional real space into a finite number of disjoint connected sets called cells, in each of which each polynomial in $\mathcal{A}$ is invariant in sign. Moreover, these

cells are cylindrically arranged with respect to each of the r variables, and they are algebraic in the sense that their boundaries are the zeros of certain polynomials which can be derived from the polynomials in $\mathcal{A}$. Such a decomposition is therefore called an $\mathcal{A}$-invariant cylindrical algebraic decomposition. The sign of a polynomial in $\mathcal{A}$ in a cell of the decomposition can be determined by computing its sign at a sample point belonging to the cell. In the application of cylindrical algebraic decomposition to quantifier elimination, we assume that we are given a quantified formula ϕ in prenex form, and we take $\mathcal{A}$ to be the set of all polynomials occurring in ϕ. From a set of sample points for a decomposition, we can decide in which cells the unquantified matrix of the formula ϕ is true. The decomposition of r-dimensional space induces, and is constructed from, a decomposition of each lower-dimension space. Each cylinder is composed of a finite number of cells, so universal and existential quantifiers can be treated like conjunctions and disjunctions, and one can decide in which cells of a lower-dimension space the quantified formula is true. The quantifier elimination can be completed by constructing formulas which define these cells.

The polynomials whose zeros form the boundaries of the cells are the elements of successive "projections" of the set $\mathcal{A}$. The projection of a set of polynomials in r variables is a set of polynomials in r-1 variables. The cylindrical arrangement of cells is ensured by a condition called delineability of roots, which is defined in Section 2. Several theorems giving sufficient conditions for delineability are proved, culminating in the definition of projection and the fundamental theorem that if each element of the projection of a set $\mathcal{A}$ is invariant on a connected set S then the roots of A are delineable on S. This theorem implicitly defines an $\mathcal{A}$-invariant cylindrical algebraic decomposition. Section 2 also defines the "augmented projection", a modification of the projection which is applied in certain contexts in order to facilitate the construction of defining formulas for cells. Section 2 is concluded with the specification of the main algebraic algorithms which are required as subalgorithms of the quantifier elimination algorithm described in Section 3. These algebraic algorithms include algorithms for various operations on real algebraic numbers and on polynomials with rational integer or real algebraic number coefficients.

Section 3 describes the quantifier elimination algorithm, ELIM, and its subalgorithms, which do most of the work. ELIM invokes successively its two subalgorithms, DECOMP (decomposition) and EVAL (evaluation).

DECOMP produces sample points and cell definitions, given a set of polynomials. EVAL uses the sample points and cell definitions, together with the prenex formula ϕ, to produce a quantifier-free formula equivalent to ϕ. DECOMP itself uses a subalgorithm, DEFINE, to aid in the construction of defining formulas for cells. These algorithms are described in a precise but informal style with extensive interspersed explanatory remarks and assertions in support of their validity.

Section 4 is devoted to an analysis of the computing time of the quantifier elimination algorithm. Since some of the required algebraic subalgorithms have not yet been fully analyzed, and since in any case improved subalgorithms are likely to be discovered from time to time, the analysis is carried out in terms of a parameter reflecting the computing times of the subalgorithms.

Section 5 is devoted to further discussion of the algorithm, including possible modifications, examples, special cases, and the observed behavior of the method.

It should be noted that the definition of the projection operator has been changed in an important way since the publication of the preliminary version of this paper. This change is justified by a new definition of delineability in Section 3 and a new proof of what is now Theorem 5. This change in the projection operator contributes greatly to the practical feasibility of the algorithm.

2. Algebraic Foundations. In this section we make some needed definitions, prove the basic theorems which provide a foundation for the quantifier elimination algorithm to be presented in Section 3, and define and discuss the main subalgorithms which will be required.

By an integral polynomial in r variables we shall mean any element

of the ring $I[x_1,\ldots,x_r]$, where I is the ring of the rational integers. As observed by Tarski, any atomic formula of elementary algebra can be expressed in one of the two forms $A = 0$, $A > 0$, where A is an integral polynomial. Also, any quantifier-free formula can be easily expressed in disjunctive normal form as a disjunction of conjunctions of atomic formulas of these two types. However, for the quantifier elimination algorithm to be presented in this paper, there is no reason to be so restrictive, and we define a standard atomic formula as a formula of one of the six forms $A = 0$, $A > 0$, $A < 0$, $A \neq 0$, $A \geq 0$, and $A \leq 0$. A standard formula is any formula which can be constructed from standard atomic formulas using propositional connectives and quantifiers. A standard prenex formula is a standard formula of the form

$$(Q_k x_k)(Q_{k+1} x_{k+1}) \ \ldots \ (Q_r x_r)\phi(x_1,\ldots,x_r), \tag{1}$$

where $\phi(x_1,\ldots,x_r)$ is a quantifier-free standard formula, $1 \leq k \leq r$, and each $(Q_i x_i)$ is either an existential quantifier $(\exists x_i)$ or a universal quantifier $(\forall x_i)$.

The variables x_i range over the ordered field R of all real numbers, or over any other real closed field. For additional background information on elementary algebra, the reader is referred to Tarski's excellent monograph, [18], and van der Waerden, [19], has an excellent chapter on real closed fields.

The quantifier elimination algorithm to be described in the next section accepts as input any standard prenex formula of the form (1), with $1 \leq k \leq r$, and produces as output an equivalent standard quantifier-free formula $\psi(x_1,\ldots,x_{k-1})$.

$\mathcal{R}$ will denote an arbitrary commutative ring with identity. Unless otherwise specified, we will always regard a polynomial $A(x_1,\ldots,x_r) \in \mathcal{R}[x_1,\ldots,x_r]$ as an element of $\mathcal{R}[x_1,\ldots,x_{r-1}][x_r]$; that is, A is regarded as a polynomial in its main variable, x_r, with coefficients in the polynomial ring $\mathcal{R}[x_1,\ldots,x_{r-1}]$. Thus, for example, the leading coefficient of A, denoted by ldcf(A), is an element of $\mathcal{R}[x_1,\ldots,x_{r-1}]$. Similarly, deg(A) denotes the degree of A in x_r. If $A(x_1,\ldots,x_r) = \sum_{i=0}^{n} A_i(x_1,\ldots,x_{r-1})\cdot x_r^i$ and deg(A)=n, then ldcf(A)=A_n and ldt(A)=$A_n(x_1,\ldots,x_{r-1})\cdot x_r^n$, the leading term of A. Following Tarski, red(A), the reductum of A is the difference A-ldt(A). By convention, deg(0)=ldcf(0)=0, and hence also ldt(0)=red(0)=0. A' will denote the derivative of A.

R^k will denote the k=fold Cartesian product R x ... x R, $k \geq 1$. If f and g are real-valued functions defined on a set $S \subseteq R^k$, we write $f > 0$ on S in case $f(x) > 0$ for all $x \in S$, $f = 0$ on S in case $f(x) = 0$ for all $x \in S$; $f < 0$ on S, $f \neq 0$ on S, $f < g$ on S and other such relations are similarly defined. We say that f is invariant on S in case $f > 0$ on S, $f = 0$ on S, or $f < 0$ on S. These definitions are also applied to real polynomials, which may be regarded as real-valued functions.

The field of complex numbers will be denoted by C. We will regard R as a subset, and hence a subfield, of C. A polynomial $A(x_1,...,x_r)$ belonging to $R[x_1,...,x_r]$ will be called a real polynomial.

Let $A(x_1,...,x_r)$ be a real polynomial, $r \geq 2$, S a subset of R^{r-1}. We will say that $f_1,...,f_m$, $m \geq 1$, delineate the roots of A on S in case the following conditions are all satisfied:

(1) $f_1,...,f_m$ are distinct continuous functions from S to C.

(2) There is a positive integer e_i such that $f_i(a_1,...,a_{r-1})$ is a root of $A(a_1,...,a_{r-1},x)$ of multiplicity e_i for $(a_1,...,a_{r-1}) \in S$ and $1 \leq i \leq m$.

(3) If $(a_1,...,a_{r-1}) \in S$, $b \in C$ and $A(a_1,...,a_{r-1},b) = 0$ then for some i, $1 \leq i \leq m$, $b = f_i(a_1,...,a_{r-1})$.

(4) For some k, $0 \leq k \leq m$, $f_1,...,f_k$ are real-valued with $f_1 < f_2 < ... < f_k$ and the values of $f_{k+1},...,f_m$ are all non-real.

e_i will be called the multiplicity of f_i. If $k \geq 1$, we will say that $f_1,...,f_k$ delineate the real roots of A on S. The roots of A are delineable on S in case there are functions $f_1,...,f_m$ which delineate the roots of A on S.

Note that if the roots of A are delineable on S then $A(a_1,..,a_{r-1},x)$ is a non-zero polynomial for $(a_1,...,a_{r-1}) \in S$, and the number of distinct roots of $A(a_1,...,a_{r-1},x)$ is independent of the choice of $(a_1,...,a_{r-1})$ in S. The number of roots, multiplicities counted, $\Sigma_{i=1}^{m} e_i = n$, must also be invariant on S. Hence deg(A)=n is also invariant on S, so ldcf(A)≠0 on S. The following basic theorem shows that if these necessary conditions are satisfied and additionally S is connected, then the roots of A are delineable on S.

Theorem 1. Let $A(x_1,...,x_r)$ be a real polynomial, $r \geq 2$. Let S be a connected subset of R^{r-1}. If ldcf(A)≠0 on S and the number of distinct roots of A is invariant on S, then the roots of A are delineable on S.

Proof. We may assume S is non-empty and deg(A) = n > 0 since otherwise the theorem is trivial. Let $(a_1,\ldots,a_{r-1})=a \in S$ and let $\alpha_1,\ldots,\alpha_m$ be the distinct roots of $A(a_1,\ldots,a_{r-1},x)$. We may assume that $\alpha_1 < \alpha_2 < \ldots < \alpha_k$ are real and $\alpha_{k+1},\ldots,\alpha_m$ are non-real. If m=1 let $\delta=1$ and otherwise let $\delta=\frac{1}{2}\min_{i<j}|\alpha_i-\alpha_j|$. Let C_i be the circle with center α_i and radius δ. Let $A(x_1,\ldots,x_r)=\sum_{i=0}^{n} A_i(x_1,\ldots,x_{r-1})x_r^i$. Since the A_i are continuous functions on S and $A_n \neq 0$ on S, by Theorem (1,4) of [7] there exists $\epsilon>0$ such that if $a'=(a'_1,\ldots,a'_{r-1}) \in S$ and $||a-a'||<\epsilon$ then $A(a',x)$ has exactly e_i roots, multiplicities counted, inside C_i, where e_i is the multiplicity of α_i. Since by hypothesis $A(a',x)$ has exactly m distinct roots and the interiors of the m circles C_i are disjoint, each circle must contain a unique root of $A(a',x)$, whose multiplicity is e_i. Since the non-real roots of A(a,x) occur in conjugate pairs, the interiors of the circles $C_{k+1},\ldots,C_m$ contain no real numbers and hence the roots of $A(a',x)$ in $C_{k+1},\ldots,C_m$ are non-real. If $i \leq k$ and C_i contained a non-real root of $A(a',x)$ then its conjugate would also be a non-real root of $A(a',x)$ in C_i since the center of C_i is real. So the roots of $A(a',x)$ in $C_1,\ldots,C_k$ are real.

Let $N=\{a' : a' \in S \& ||a-a'||<\epsilon\}$. For $a' \in N$ define $f_i(a')$ to be the unique root of $A(a',x)$ inside C_i. Then $f_1<f_2<\ldots<f_k$ are real functions and $f_{k+1},\ldots,f_m$ are non-real valued. By another application of Theorem (1,4) of [7], the f_i are continuous functions on N, which is an open neighborhood of a in S. Hence if $0 \leq k \leq m$ and S_k is the set of all $a \in S$ such that A(a,x) has exactly k distinct real roots, then S_k is open in S. Since a connected set is not a union of two disjoint non-empty subsets, there is a unique k such that $S=S_k$.

We can now define $f_i(a)$ to be the ith real root of A(a,x) for $a \in S$ and $1 \leq i \leq k$, so that $f_1<f_2<\ldots<f_k$ on S. By the preceding paragraph it is immediate that $f_1,\ldots,f_k$ are continuous. By another application of the connectivity, the multiplicity of f_i as a root of A is an invariant e_i throughout S since, as we have already shown, the multiplicity is locally invariant.

The proof of the existence of the non-real functions $f_{k+1},\ldots,f_m$ is somewhat more difficult because the topology of C is not induced by a linear order. Choose a fixed point a of S and arbitrarily denote the non-real roots of A(a,x) by $\alpha_{k+1},\ldots,\alpha_m$. For any $a' \in S$ there is a path P in S from a to a' since S is connected. For any point a'' of P there is an open neighborhood N of a'' and m-k continuous functions defined on N

which are non-real roots of A. These open neighborhoods for all points a'' of P constitute an open cover of the set P. Since P is compact, this cover has a finite subcover. Since P is connected, the elements of the finite subcover can be arranged into a chain $N_1,\ldots,N_h$ such that $a\varepsilon N_1$, $a'\varepsilon N_h$ and $N_i \cap N_{i+1}$ is non-empty for $1\leq i<h$. The functions defined on N_1 can be designated by $f_{k+1}^{(1)},\ldots,f_m^{(1)}$ in such a manner that $f_j^{(1)}(a)=\alpha_j$. The functions on N_{i+1} can be uniquely designated by $f_j^{(i+1)}$ so that $f_j^{(i+1)}(a'') = f_j^{(i)}(a'')$ for all $a''\varepsilon N_i \cap N_{i+1}$. Finally we can set $\alpha_j'=f_j^{(h)}(a')$ for $k+1 \leq j\leq m$. In this way we can define the jth root of $A(a',x)$ for $k+1\leq j\leq m$ and $a'\varepsilon S$. Then we define $f_j(a')$ to be the jth root of $A(a',x)$ and easily prove that f_j is continous, non-real valued, and of invariant multiplicity. ∎

We say that the polynomials $A,B,\varepsilon\mathfrak{R}[x]$ are similar, and write $A\approx B$, in case there exist non-zero $a,b\varepsilon\mathfrak{R}$ such that $aA = bB$.

We define $red^k(A)$, the kth reductum of the polynomials A, for $k\geq 0$, by induction on k as follows: $red^0(A)=A$ and $red^{k+1}(A)=red(red^k(A))$ for $k\geq 0$. We say that B is a reductum of A in case $B=red^k(A)$ for some $k\geq 0$.

We repeat some definitions from [4]. Let A and B be polynomials over $\mathfrak{R}$ with $deg(A)=m$ and $deg(B)=n$. The Sylvester matrix of A and B is the m+n by m+n matrix M whose successive rows contain the coefficients of the polynomials $x^{n-1}A(x),\ldots,A(x),x^{n-1}B(x),\ldots,xB(x),B(x)$, with the coefficients of x^i occuring in column m+n-i. We allow either m=0 or n=0. As is well known, res(A,B), the resultant of A and B, is det(M), the determinant of M. (We adopt the convention det(N)=0 in case N is a zero by zero determinant.) For $0\leq i\leq j\leq \min(m,n)$ let $M_{j,i}$ be the matrix obtained from M by deleting the last j rows of A coefficients, the last j rows of B coefficients, and all of the last 2j+1 columns except column m+n-i-j. The jth subresultant of A and B is the polynomial $S_j(A,B) = \Sigma_{i=0}^{j} det(M_{j,i})\cdot x^i$, a polynomial of degree j or less. We define also the jth principal subresultant coefficient of A and B by $psc_j(A,B)=det(M_{j,j})$. Thus $psc_j(A,B)$ is the coefficient of x^j in $S_j(A,B)$. We note, for subsequent application, that if $deg(A)=m>0$ then $psc_{m-1}(A,A')=m\cdot ldcf(A)$.

Theorem 2. Let A and B be non-zero polynomials over a unique factorization domain. Then $deg(gcd(A,B))=k$ if and only if k is the least j such that $psc_j(A,B)\neq 0$.

Proof. Let $k=\deg(\gcd(A,B))$. By the fundamental theorem of polynomial remainder sequences, [2], $\mathcal{S}_j(A,B)=0$ for $0\leq j<k$, and $\gcd(A,B)\approx\mathcal{S}_k(A,B)$. Hence $\mathrm{psc}_j(A,B)=0$ for $0\leq j<k$, $\deg(\mathcal{S}_k(A,B))=k$, and $\mathrm{psc}_k(A,B)\neq 0$. ∎

Theorem 3. Let $A(x)$ be a real univariate polynomial with $\deg(A)=m\geq 1$ and let $k=\deg(\gcd(A,A'))$. Then $m-k$ is the number of distinct roots of A.

Proof. Let A have the distinct roots $\alpha_1,\ldots,\alpha_n$ with respective multiplicities $e_1,\ldots,e_n$. By a familiar argument, α_i is a root of A' with multiplicity e_i-1 (meaning that α_i is not a root of A' if $e_i=1$). Hence α_i is a root of $\gcd(A,A')$ with multiplicity e_i-1. Since every root of $\gcd(A,A')$ is some α_i, $k=\deg(\gcd(A,A'))=\Sigma_{i=0}^{h}(e_i-1)=\Sigma_{i=0}^{h}e_i-h=m-h$ and $m-k=h$. ∎

Using reducta and principal subresultant coefficients, we now obtain a more useful sufficient condition for the delineability of the roots of a polynomial.

Theorem 4. Let $A(x_1,\ldots,x_r)$ be a real polynomial, $r\geq 2$, S a connected subset of R^{r-1}. Let $\mathcal{B}=\{\mathrm{red}^k(A):k\geq 0\ \&\ \deg(\mathrm{red}^k(A))\geq 1\}$, $\mathcal{L}=\{\mathrm{ldcf}(B):B\in\mathcal{B}\}$, $\mathcal{S}=\{\mathrm{psc}_k(B,B'):B\in\mathcal{B}\ \&\ 0\leq k<\deg(B')\}$ and $\mathcal{P}=\mathcal{L}\cup\mathcal{S}$. If every element of $\mathcal{P}$ is invariant on S, then the roots of A are delineable on S.

Proof. If $\deg(A)\leq 1$ then the theorem is obvious, so let $A(x_1,\ldots,x_r)=\Sigma_{i=0}^{n}A_i(x_1,\ldots,x_{r-1})x_r^i$ with $\deg(A)=n\geq 2$. If $i\geq 1$ and $A_i\neq 0$ then $A_i\in\mathcal{L}$ so A_i is invariant on S for $1\leq i\leq n$. If $A_i=0$ on S for $1\leq i\leq n$ then the theorem is obvious, so let $m\geq 1$ be maximal such that $A_m\neq 0$ on S and let k be such that $\mathrm{red}^k(A)=\Sigma_{i=0}^{m}A_i(x_1,\ldots,x_{r-1})x_r^i=B$. Then $A=B$ on S so it suffices to show that the roots of B are delineable on S. $B\in\mathcal{B}$ so $\mathrm{psc}_j(B,B')$ is invariant on S for $0\leq j<m-1$. Also $\mathrm{psc}_{m-1}(B,B')=mA_m\neq 0$ on S. By Theorem 2, $\deg(\gcd(B,B'))$ is invariant on S, that is, for some k, $\deg(\gcd(B(a,x),B'(a,x)))=k$ for all $a\in S$. By Theorem 3, the number of distinct roots of B on S is the invariant $m-k$. By Theorem 1, the roots of B are delineable on S. ∎

Let $\mathcal{A}$ be a set of real polynomials in r variables, $r\geq 2$. Let $\mathcal{B}=\{\mathrm{red}^k(A):A\in\mathcal{A}\ \&\ k\geq 0\ \&\ \deg(\mathrm{red}^k(A))\geq 1\}$, $\mathcal{L}=\{\mathrm{ldcf}(B):B\in\mathcal{B}\}$, $\mathcal{S}_1=\{\mathrm{psc}_k(B,B'):B\in\mathcal{B}\ \&\ 0\leq k<\deg(B')\}$, $\mathcal{S}_2=\{\mathrm{psc}_k(B_1,B_2):B_1,B_2\in\mathcal{B}\ \&\ 0\leq k<\min(\deg(B_1),\deg(B_2))\}$ and $\mathcal{P}=\mathcal{L}\cup\mathcal{S}_1\cup\mathcal{S}_2$. Then $\mathcal{P}$ will be called the projection of $\mathcal{A}$. If $\mathcal{A}=\{A_1,\ldots,A_n\}$ is a non-empty finite set of non-zero polynomials, we will say that the roots

of $\mathcal{A}$ are delineable on a set S in case the roots of the product $A=\Pi_{i=1}^{n}A_i$ are delineable on S. Note that the roots of each A_i could be delineable on S without the roots of $\mathcal{A}$ being delineable on S. The next theorem shows how the inclusion of the set $\mathcal{S}_2$ in the projection $\mathcal{P}=\text{proj}(\mathcal{A})$ helps to ensure the delineability of the roots of $\mathcal{A}$.

Theorem 5. Let $\mathcal{A}=\{A_1,\ldots,A_n\}$ be a non-empty set of non-zero real polynomials in r real variables, $r\geq 2$. Let S be a connected subset of R^{r-1}. Let $\mathcal{P}$ be the projection of $\mathcal{A}$. If every element of $\mathcal{P}$ is invariant on S, then the roots of $\mathcal{A}$ are delineable on S.

Proof. By Theorem 4, the roots of A_i are delineable on S for $1\leq i\leq n$. Let $\mathcal{J}_i$ be the set of delineating functions for A_i and let $\mathcal{J}=\bigcup_{i=1}^{n}\mathcal{J}_i$. If $f_1,\ldots,f_m$ are the distinct elements of $\mathcal{J}$, with $f_1<f_2<\ldots<f_k$ real valued, $f_{k+1},\ldots,f_m$ non-real valued, and if $f_i(a)\neq f_j(a)$ for $i\neq j$ and $a\in S$, then $f_1,\ldots,f_m$ delineate the roots of $\mathcal{A}$. For if $A=\Pi_{i=1}^{n}A_i$ then (1), (2) and (4) of the definition of delineation are obviously satisfied. Also, if $f_i(a)$ is a root of A_j of multiplicity $e_{i,j}$ then $f_i(a)$ is a root of A of multiplicity $e_i=\Sigma_{j=1}^{m}e_{i,j}$. Hence if $f_i(a)\neq f_j(a)$ for $i\neq j$ then $e_{i,j}>0$ just in case f_i is a delineating function of A_j. So if $f_i(a)\neq f_j(a)$ for all $a\in S$ then the multiplicity of f_i as a root of A on S is the invariant $e_i=\Sigma_j e_{i,j}$ where the sum is taken over all j such that f_i is a delineating function of A_j.

Hence it suffices to show that if $f_i\neq f_j$ then $f_i(a)\neq f_j(a)$ for all $a\in S$. Without loss of generality we may assume that f_i is a delineating function of A_1 and g_j is a delineating function of A_2. Let $g_1,\ldots,g_s$ be the delineating functions of A_1, $h_1,\ldots,h_t$ the delineating functions of A_2. Let M be any s by t matrix of zeros and ones and let S_M be the set of all $a\in S$ such that $g_i(a)=h_j(a)$ if $M_{i,j}=0$ and $g_i(a)\neq h_j(a)$ if $M_{i,j}=1$ for all i and all j. Assume S_M is non-empty, and let $a\in S_M$. By continuity there is an open neighborhood N of a in S such that if $M_{i,j}=1$ then $g_i(a')\neq h_j(a')$ for all $a'\in N$. Since S_M is non-empty, there is for each i at most one j such that $M_{i,j}=0$. Let $(i_1,j_1),\ldots,(i_l,j_l)$ be all the distinct pairs (i,j) such that $M_{i,j}=0$. Let d_i be the multiplicity of f_i as a root of A_1, e_j the multiplicity of g_j as a root of A_2. Then $\deg(\gcd(A_1(a,x),A_2(a,x)))=\Sigma_{k=1}^{l}\min(d_k,e_k)$. Since $\text{psc}_h(A_1,A_2)$ is in $\mathcal{P}$ for $0\leq h<\min(\deg(A_1),\deg(A_2))$, $\deg(\gcd(A_1(a',x),A_2(a',x)))$ is invariant for all $a'\in S$. Hence if $a'\in N$ and $g_{i_1}(a')\neq h_{j_1}(a')$ then $\deg(\gcd(A_1(a',x),A_2(a',x)))=\Sigma_{k=2}^{l}\min(d_k,e_k)<\Sigma_{k=1}^{l}\min(d_k,e_k)$, a contradiction.

So $a' \varepsilon S_M$ for all $a' \varepsilon N$. It follows that each S_M is an open subset of S. Since S is connected and the sets S_M are disjoint, there is a unique M such that $S=S_M$, which M must obviously satisfy $M_{i,j}=0$ if and only if $g_i=h_j$. Hence if $a \varepsilon S$ and $g_i \neq h_j$ then $g_i(a) \neq h_j(a)$, completing the proof. ∎

Let us write der(A) for A', the derivative of A. We define $der^0(A)=A$ and, inductively, $der^{k+1}(A)=der(der^k(A))$ for $k \geq 0$.

Let $\mathcal{A}$ be a set of real polynomials in r variables, $r \geq 2$. Let $\mathcal{B}=\{red^k(A): A \varepsilon \mathcal{A} \& k \geq 0 \& deg(red^k(A)) \geq 1\}$, $\mathcal{D}=\{der^k(B): B \varepsilon \mathcal{B} \& 0<k<deg(B)\}$ and $\mathcal{P}'=\{psc_k(D,D'): D \varepsilon \mathcal{D} \& 0 \leq k < deg(D')\}$. Then $\mathcal{P} \cup \mathcal{P}'$, where $\mathcal{P}$ is the projection of $\mathcal{A}$, will be called the augmented projection of $\mathcal{A}$.

Theorem 6. Let $\mathcal{A}$ be a set of real polynomials in r variables, $r \geq 2$. Let S be a connected subset of R^{r-1}. Let $\mathcal{P}^*$ be the augmented projection of $\mathcal{A}$. If every element of $\mathcal{P}^*$ is invariant on S then the roots of $der^j(A)$ are delineable on S for every $A \varepsilon \mathcal{A}$ and every $j \geq 0$.

Proof. Let $A \varepsilon \mathcal{A}$, $j \geq 0$, $A^*=der^j(A)$, $\mathcal{B}=\{red^k(A^*): k \geq 0 \& deg(red^k(A^*)) \geq 1\}$, $\mathcal{L}=\{ldcf(B): B \varepsilon \mathcal{B}\}$, $\mathcal{D}=\{psc_h(B,B'): 0 \leq h < deg(B')\}$, and $\mathcal{P}=\mathcal{L} \cup \mathcal{D}$. By Theorem 4, it suffices to show that each element of $\mathcal{P}$ is invariant on S. If $k \geq 0$ and $deg(red^k(A^*)) \geq 1$ then $red^k(A^*)=red^k(der^j(A))=der^j(red^k(A))$ so $ldcf(red^k(A^*))=ldcf(der^j(red^k(A))=a \cdot ldcf(red^k(A))$ for some positive integer a. Also $deg(red^k(A)) \geq deg(red^k(A^*)) \geq 1$ so $ldcf(red^k(A))$ is in the projection of $\mathcal{A}$. Hence every element of $\mathcal{L}$ is invariant on S. If $j=0$ then the roots of $A=der^j(A)$ are delineable on S by Theorem 5, so assume $j>0$. If $j \geq deg(red^k(A))$ then $der^j(red^k(A))$ is an integer and hence invariant on S. Otherwise, $0<j<deg(red^k(A))$ so if $B=red^k(der^j(A))=der^j(red^k(A))$ then $psc_h(B,B')$ belongs to the augmented projection of $\mathcal{A}$ and is invariant on S for $0 \leq h < deg(B')$. Hence every element of $\mathcal{D}$ is invariant on S. ∎

We now complete this section with discussion and specification of the more important subalgorithms which will be needed for the quantifier elimination algorithm.

The quantifier elimination algorithm of the next section will require computation of the projection or augmented projection of $\mathcal{A}$ just in case $\mathcal{A}$ is finite and $\mathcal{P}=I[x_1,\ldots,x_{r-1}]$, $r \geq 2$. Thus we assume the availability of an algorithm with the following specifications.

B = PROJ(A)

Input: $\mathcal{A}=(A_1,\ldots,A_m)$ is a list of distinct integral polynomials in r variables, $r\geq 2$.

Output: $\mathcal{B}=(B_1,\ldots,B_n)$ is a list of distinct integral polynomials in r-1 variables, such that $\{B_1,\ldots,B_n\}$ is the projection of $\{A_1,\ldots,A_m\}$.

Another like algorithm, APROJ, is assumed for computing the augmented projection.

Now let $\mathcal{U}$ be a unique factorization domain, abbreviated u.f.d. If $a,b\in\mathcal{U}$ we say that a and b are associates, and write $a\sim b$, in case $a=ub$ for some unit u. An ample set for $\mathcal{U}$ (see [10]) is a set $\mathcal{A}\subseteq\mathcal{U}$ which contains exactly one element from each equivalence class of associates. Relative to $\mathcal{A}$ we can define a function gcd on $\mathcal{U}\times\mathcal{U}$ into $\mathcal{U}$ such that $\gcd(a,b)\in\mathcal{A}$ and $\gcd(a,b)$ is a greatest common divisor of a and b for all $a,b\in\mathcal{U}$. We will assume, moreover, that $\mathcal{A}$ is multiplicative, i.e. closed under multiplication, from which $1\in\mathcal{A}$. Whenever $\mathcal{U}$ is a field we will have $\mathcal{A}=\{0,1\}$. For $\mathcal{U}=I$, we set $\mathcal{A}=\{0,1,2,\ldots\}$. $\mathcal{U}[x]$ is also a u.f.d and if $\mathcal{A}$ is an ample set for $\mathcal{U}$ we take $\{A:\mathrm{ldcf}(A)\in\mathcal{A}\}$ as ample set for $\mathcal{U}[x]$ (see [14]).

If $A(x)=\Sigma_{i=0}^{n}a_ix^i$ is a non-zero polynomial over $\mathcal{U}$, we set $\mathrm{cont}(A)=\gcd(a_n,a_{n-1},\ldots,a_0)$, the content of A, and we set $\mathrm{cont}(0)=0$. If $A\neq 0$ we define $\mathrm{pp}(A)$, the primitive part of A, to be the ample associate of $A/\mathrm{cont}(A)$, and we set $\mathrm{pp}(0)=0$. The polynomial A is primitive in case $\mathrm{cont}(A)=1$. Clearly $\mathrm{pp}(A)$ is primitive and $A\sim\mathrm{cont}(A)\cdot\mathrm{pp}(A)$ for all $A\neq 0$.

Let $\mathcal{A}$ be a set of primitive polynomials of positive degree over $\mathcal{U}$. A basis for $\mathcal{A}$ is a set $\mathcal{B}$ of ample primitive polynomials of positive degree over $\mathcal{U}$ satisfying the following three conditions:

(a) If $B_1,B_2\in\mathcal{B}$ and $B_1\neq B_2$ then $\gcd(B_1,B_2)=1$.

(b) If $B\in\mathcal{B}$, then $B\mid A$ for some $A\in\mathcal{A}$.

(c) If $A\in\mathcal{A}$, there exist $B_1,\ldots,B_n\in\mathcal{B}$ and positive integers $e_1,\ldots,e_n$ such that

$$A\sim\prod_{i=1}^{n}B_i^{e_i}\ (\text{with } n=0 \text{ if } A\sim 1).$$

If $\mathcal{A}$ is an arbitrary set of polynomials over $\mathcal{U}$, then a basis for $\mathcal{A}$ is a set $\mathcal{B}=\mathcal{B}_1\cup\mathcal{B}_2$ where $\mathcal{B}_1=\{\mathrm{cont}(A):A\in\mathcal{A}\ \&A\neq 0\}$ and $\mathcal{B}_2$ is a basis for $\{\mathrm{pp}(A):A\in\mathcal{A}\ \&\deg(A)>0\}$.

If $\mathcal{A}$ is a set of primitive polynomials of positive degree then the

set $\mathcal{P}$ of ample irreducible divisors of elements of $\mathcal{A}$ is clearly a basis for $\mathcal{A}$. If $\mathcal{B}_1$ and $\mathcal{B}_2$ are bases for $\mathcal{A}$, we say that $\mathcal{B}_1$ is a refinement of $\mathcal{B}_2$ in case every element of $\mathcal{B}_1$ is a divisor of some element of $\mathcal{B}_2$. $\mathcal{P}$ is the finest basis for $\mathcal{A}$ in the sense that it is a refinement of every other basis.

Every set $\mathcal{A}$ also has a coarsest basis, $\mathcal{C}$, in the sense that every basis for $\mathcal{A}$ is a refinement of $\mathcal{C}$, as we will now see. Let $\mathcal{P}$ be the set of all ample irreducible divisors of positive degree of elements of $\mathcal{A}$. For $P \in \mathcal{P}$, let $\sigma(P)$ be the set of all positive integers i such that, for some $A \in \mathcal{A}$, $P^i | A$ but not $P^{i+1} | A$. Let $e(P)$ be the greatest common divisor of the elements of $\sigma(P)$. For P,Q in $\mathcal{P}$, define $P \equiv Q$ in case, for every $A \in \mathcal{A}$, the orders of P and Q in A are identical. Let $\mathcal{C}$ be the set of all products $\{\Pi_{Q \equiv P} Q^{e(P)}\}$ with $P \in \mathcal{P}$. Then it can be shown that $\mathcal{C}$ is a coarsest basis for $\mathcal{A}$.

If $\mathcal{A}$ is finite, its coarsest basis can be computed by g.c.d. calculation. Set $\mathcal{C} = \mathcal{A}$. If A and B are distinct elements of $\mathcal{C}$, set $C=\gcd(A,B)$, $\bar{A}=A/C$, $\bar{B}=B/C$. If $C \neq 1$, replace A and B in $\mathcal{C}$ by the non-units from among C, $\bar{A}$ and $\bar{B}$. Eventually the elements of $\mathcal{C}$ will be pairwise relatively prime and $\mathcal{C}$ will be a coarsets basis for $\mathcal{A}$.

A squarefree basis for $\mathcal{A}$ is a basis each of whose elements is squarefree. If A is any primitive element of $\mathcal{U}[x]$ of positive degree, there exist ample, squarefree, relatively prime polynomials $A_1,\ldots,A_k$ and integers $e_1<\ldots<e_k$ such that $A \sim \Pi_{i=1}^{k} A_i^{e_i}$. $(A_1,\ldots,A_k)$ and $(e_1,\ldots,e_k)$ constitute the squarefree factorization of A. Musser, [14] and [15], discusses algorithms for squarefree factorization, which require if $\mathcal{U}$ has characteristic zero, only differentiation, division and greatest common divisor calculations. We assume the availability of an algorithm for squarefree factorization in $\mathcal{U}[x]$ for the cases $\mathcal{U}=I[x_1,\ldots,x_{r-1}]$, $r \geq 1$, and $\mathcal{U}=Q(\alpha)$, where $Q(\alpha)$ is the real algebraic number field resulting from adjoining the real algebraic number α to the field Q of the rational numbers. For the case $\mathcal{U}=Q(\alpha)$ we assume the following specifications.

SQFREF(α,A,$\mathcal{A}$,e)

Inputs: α is a real algebraic number. A is a primitive element of $Q(\alpha)[x]$ of positive degree.
Outputs: $\mathcal{A}=(A_1,\ldots,A_k)$ and $e=(e_1,\ldots,e_k)$ constitute the squarefree factorization of A.

A similar algorithm for the case $\mathcal{A}=I[x_1,\ldots,x_{r-1}]$ is needed in order to compute a coarsest squarefree basis for integral polynomials, as follows.

If $A \sim \prod_{i=1}^{k} A_i^{e_i}$ is the squarefree factorization of A, then $\{A_1,\ldots,A_k\}$ is clearly a coarsest squarefree basis for $\{A\}$. Let $\bar{\mathcal{A}}=\{A_1,\ldots,A_m\}$ be a squarefree basis for $\mathcal{A}$, $\bar{\mathcal{B}}=\{B_1,\ldots,B_n\}$ a squarefree basis for $\mathcal{B}$. Consider the following algorithm proposed by R. Loos:

(1) For j=1,...,n set $\bar{B}_j \leftarrow B_j$.

(2) For i=1,...,m do $[\bar{A}_i \leftarrow A_i$; for j=1,...,n do $(C_{i,j} \leftarrow \gcd(\bar{A}_i,\bar{B}_j)$; $\bar{A}_i \leftarrow \bar{A}_i/C_{i,j}$; $\bar{B}_j \leftarrow \bar{B}_j/C_{i,j})]$.

(3) Exit.

Upon termination, the distinct nonunits among the $\bar{A}_i$, the $\bar{B}_j$ and the $C_{i,j}$ constitute a squarefree basis $\bar{\mathcal{C}}$ for $\mathcal{C}=\mathcal{A}\cup\mathcal{B}$. Moreover, if $\bar{\mathcal{A}}$ and $\bar{\mathcal{B}}$ are coarsest squarefree bases, then so is $\bar{\mathcal{C}}$. Thus by squarefree factorization and application of Loos' algorithm we can successively obtain coarsest squarefree bases for $\{A_1\}$, $\{A_1,A_2\}$,..,$\{A_1,A_2,\ldots,A_m\}$. Thus we assume the availability of the following basis algorithm.

$$\mathcal{B} = \text{BASIS}(\mathcal{A})$$

Input: $\mathcal{A}=(A_1,\ldots,A_m)$ is a list of distinct integral polynomials in r variables, $r \geq 1$.

Output: $\mathcal{B}=(B_1,\ldots,B_n)$ is a list of distinct integral polynomials in r variables such that $\{B_1,\ldots,B_n\}$ is a coarsest squarefree basis for $\{A_1,\ldots,A_m\}$.

A similar algorithm, ABASIS, with an additional input α, a real algebraic number, will be assumed for computing the coarsest squarefree basis when $\mathcal{A}$ is a finite list of univariate polynomials over $Q(\alpha)$.

A recent Ph.D. thesis by Rubald, [16], provides algorithms for the arithmetic operations in the field $Q(\alpha)$ and in the polynomial domain $Q(\alpha)[x]$. Rubald also provides an efficient modular homomorphism algorithm for g.c.d. calculation in $Q(\alpha)[x]$. An important feature of Rubald's work is that the minimal polynomial of α is not required. Instead, α is represented by any pair (A,I) such that A is a primitive squarefree integral polynomial of positive degree with $A(\alpha)=0$, and I=(r,s) is an open interval with rational number endpoints such that α is the unique

zero of A in I. This feature is important because as yet (see [6]) no algorithm with polynomial-dominated maximum computing time is known for factoring a primitive univariate integral polynomial into its irreducible factors. A non-zero element β of $Q(\alpha)$ is then represented by any polynomial $B(x) \in Q[x]$ such that $\deg(B) < \deg(A)$ and $B(\alpha) = \beta$. Although this representation fails to be unique whenever A is reducible, no difficulties arise.

The next algorithm is easily obtained using Sturm's theorem, since Rubald's work provides an efficient algorithm for determining the sign of any element of $Q(\alpha)$, and because his algorithm for g.c.d. calculation in $Q(\alpha)[x]$ can be extended to the computation of Sturm sequences.

ISOL(α, $\mathcal{A}$, I ,ν)

Inputs: α is a real algebraic number. $\mathcal{A}=(A_1,..,A_m)$ is a list of non-zero squarefree and pairwise relatively prime polynomials over $Q(\alpha)$.

Outputs: $I=(I_1,\ldots,I_n)$ is a list of open intervals with rational endpoints with $I_1<I_2<\ldots<I_n$ such that each I_j contains exactly one real zero of $A=\Pi_{i=1}^{m} A_i$, and every real zero of A belongs to some I_j. $\nu=(\nu_1,\ldots,\nu_n)$ is such that the zero of A in I_j is a zero of A_{ν_j}.

The Algorithm ISOL can be easily obtained by application of Sturm's theorem and repeated interval bisection. Heindel, [11], presents an algorithm of this type for the case of a single univariate integral polynomial. If the real zeros of each A_i are separately isolated, then the resulting intervals can be refined until they no longer overlap, while retaining the identity of the polynomials from which they came.

In the quantifier elimination algorithm, occasion will arise to reduce a multiple real algebraic extension of the rationals, $Q(\alpha_1,\ldots,\alpha_m)$, to a simple extension $Q(\alpha)$. This can be accomplished by iterating an algorithm of Loos, [12], based on resultant theory, with the following specifications.

SIMPLE(α,β,γ, A,B)

Inputs:α and β are real algebraic numbers.
Outputs: γ is a real algebraic number. A and B are polynomials which represent α and β respectively as elements of $Q(\gamma)$.

Finally, one additional subalgorithm, also provided in [12], is the following.

NORMAL(α,A,I,$\bar{A}$,$\bar{I}$)

Inputs: α is a real algebraic number. A is a non-zero polynomial over $Q(\alpha)$. $I=(I_1,\ldots,I_m)$ is a list of rational isolating intervals, $I_1<I_2<\ldots<I_m$, for the real zeros of A.
Outputs: $\bar{A}$ is a non-zero squarefree primitive integral polynomial such that every real zero of A is a real zero of $\bar{A}$.
$\bar{I}=(\bar{I}_1,\ldots,\bar{I}_m)$ is a list of rational intervals with $\bar{I}_j \subseteq I_j$ such that if α_j is the zero of A in I_j then α_j is the unique zero of $\bar{A}$ in $\bar{I}_j$, $1 \leq j \leq m$.

3. The Main Algorithms. We define, by induction on r, a cylindrical algebraic decomposition of R^r, abbreviated c.a.d. For r=1, a c.a.d. of R is a sequence $(S_1,S_2,\ldots,S_{2\nu+1})$, where either $\nu=0$ and $S_1=R$, or $\nu>0$ and there exist ν real algebraic numbers $\alpha_1<\alpha_2<\ldots<\alpha_\nu$ such that $S_{2i}=\{\alpha_i\}$ for $1\leq i\leq\nu$, S_{2+1} is the open interval (α_i,α_{i+1}) for $1\leq i<\nu$, $S_1=(-\infty,\alpha_1)$ and $S_{2\nu+1}=(\alpha_\nu,\infty)$. Now let $r>1$, and let $(S_1,\ldots,S_\mu)$ be any c.a.d. of R^{r-1}. For $1\leq i\leq\mu$, let $f_{i,1}<f_{i,2}<\ldots<f_{i,\nu_i}$ be continuous realvalued algebraic functions on S_i. If $\nu_i=0$, set $S_{i,1}=S_i\times R$. If $\nu_i>0$ set $S_{i,2j}=f_{i,j}$, that is, $S_{i,2j}=\{(a,b):a\in S_i \& b=f_{i,j}(a)\}$ for $1\leq j\leq\nu_i$, set $S_{i,2j+1}=\{(a,b):a\in S_i \& f_{i,j}(a)<b<f_{i,j+1}(a)\}$ for $1\leq j<\nu_i$, set $S_{i,1}=\{(a,b):a\in S_i \& b<f_{i,1}(a)\}$, and set $S_{i,2\nu_i+1}=\{(a,b):a\in S_i \& f_{i,\nu_i}(a)<b\}$. A c.a.d. of R^r is any sequence $(S_{1,1},\ldots,S_{1,2\nu_1+1},\ldots,S_{\mu,1},\ldots,S_{\mu,2\nu_\mu+1})$ which can be obtained by this construction from a c.a.d. of R^{r-1} and functions $f_{i,j}$ as just described.

It is important to observe that the cylinder $S_i\times R$ is the disjoint union $\bigcup_{j=1}^{2\nu_i+1} S_{i,j}$ for $1\leq i\leq\mu$. If $S=(S_1,\ldots,S_\mu)$ is any c.a.d. of R^r, the S_i will be called the cells of S. Clearly every cell of a c.a.d. is a connected set. If $\mathcal{A}$ is a set of real polynomials in r variables, the

c.a.d. S or R^r is $\mathcal{A}$-invariant in case each A in $\mathcal{A}$ is invariant on each cell of S.

A sample of the c.a.d. $S=(S_1,\ldots,S_\mu)$ is a tuple $\beta=(\beta_1,\ldots,\beta_\mu)$ such that $\beta_i \varepsilon S_i$ for $1\leq i\leq \mu$. The sample β is algebraic in case each β_i is an algebraic point, i.e. each coordinate of β_i is an algebraic number. A cylindrical sample is defined by induction on r. For r=1, any sample is cylindrical. For r>1, let $S=(S_{1,1},\ldots,S_{1,2\nu_1+1},\ldots,S_{\mu,1},\ldots,S_{\mu,2\nu_\mu+1})$ be a c.a.d. of R^r constructed from a c.a.d. $S^*=(S_1,\ldots,S_\mu)$ of R^{r-1}, and let $\beta^*=(\beta_1,\ldots,\beta_\mu)$ be a sample of S^*. The sample $\beta=(\beta_{1,1},\ldots,\beta_{1,2\nu_1+1},\ldots,\beta_{\mu,1},\ldots,\beta_{\mu,2\nu_\mu+1})$ of S is cylindrical if the first r-1 coordinates of $\beta_{i,j}$ are, respectively, the coordinates of β_i, for all i and j, and β^* is cylindrical. Cylindrical algebraic sample will be abbreviated c.a.s.

Since a c.a.d. of R^r can be constructed from a unique c.a.d of R^{r-1}, any c.a.d. S of R^r determines, for $1\leq k<r$, a c.a.d. S^* of R^k, which will be called the c.a.d. of R^k induced by S. Similarly any c.a.s. β of S induces a unique c.a.s. β^* of S .

If S is an arbitrary subset of R^r, the standard formula $\phi(x_1,\ldots,x_r)$ containing just $x_1,\ldots,x_r$ as free variables, defines S in case $S=\{(a_1,\ldots,a_r):a_1,\ldots,a_r \varepsilon R \& \phi(a_1,\ldots,a_r)\}$. A standard definition of the c.a.d. $S=(S_1,\ldots,S_\mu)$ is a sequence $(\phi_1,\ldots,\phi_\mu)$ such that, for $1\leq i\leq \mu$, ϕ_i is a standard quantifier-free formula which defines S_i.

We are now prepared to describe a decomposition algorithm, DECOMP. The inputs to DECOMP are a finite set $\mathcal{A}$ of integral polynomials in r variables, $r\geq 1$, and an integer k, $0\leq k\leq r$. The outputs of DECOMP are a c.a.s. β of some $\mathcal{A}$-invariant c.a.d. S of R^r and, if $k\geq 1$, a standard definition ψ of the c.a.d. S^* of R^k induced by S.

Before proceeding to describe DECOMP we first explain its intended use in the quantifier elimination algorithm, ELIM, which will be described subsequently. ELIM has two distinct stages. Given as input a standard prenex formula ϕ, namely $(Q_{k+1}x_{k+1})\ldots(Q_r x_r)\,\hat{\phi}(x_1,\ldots,x_r)$, ELIM applies DECOMP to the set $\mathcal{A}$ of all non-zero polynomials occurring in $\hat{\phi}$, and the integer k. The outputs β and ψ of DECOMP, together with the formula ϕ, are then input to an "evaluation" algorithm, EVAL, which produces a standard quantifier-free formula $\phi^*(x_1,\ldots,x_k)$ which is equivalent to ϕ. Thus, ELIM does little more than to successively invoke DECOMP and

EVAL.

DECOMP uses a subalgorithm, DEFINE, for construction of the standard definition. The inputs to DEFINE are an integral polynomial $A(x_1,\ldots,x_r)$, $r\geq 2$, such that for some connected set $S\subseteq R^{r-1}$ the real roots of A and of each derivative of A are delineable on S, and an algebraic point $\beta\in S$. The output of DEFINE is a sequence $(\phi_1,\ldots,\phi_{2m+1})$ of standard quantifier-free formulas ϕ_i such that if ϕ is any formula which defines S, then the conjunction $\phi\wedge\phi_i$ defines the ith cell of the cylinder SxR determined by the m real roots of A on S, as in the definition of a c.a.d. The description of DEFINE will be given following that of DECOMP.

DECOMP($\mathcal{A}$,k,β,ψ)

Inputs: $\mathcal{A}=(A_1,\ldots,A_m)$ is a list of distinct integral polynomials in r variables, $r\geq 1$. k is an integer such that $0\leq k\leq r$.
Outputs: β is a c.a.s. for some $\mathcal{A}$-invariant c.a.d. S of R^r. ψ is a standard definition of the c.a.d. S of R^k induced by S if k>0, and ψ is the null list if k=0.

Algorithm Description

(1) If r>1, go to (4). Apply BASIS to $\mathcal{A}$, obtaining a coarsest squarefree basis $\mathcal{B}=(B_1,\ldots,B_h)$ for $\mathcal{A}$. Apply ISOL to $\mathcal{B}$, obtaining outputs $I=(I_1,\ldots,I_n)$ and $\nu=(\nu_1,\ldots,\nu_n)$. (Each I_j contains a unique zero, say α_j, of B_{ν_j}, and $\alpha_1<\alpha_2<\ldots<\alpha_n$ are all the real zeros of elements of $\mathcal{A}$. Thus the α_j determine an $\mathcal{A}$-invariant c.a.d. S of R, and (B_{ν_j},I_j) represents α_j).

(2) For j=1,...,n, where $I_j=(r_j,s_j)$, set $\beta_{2j-1}\leftarrow r_j$ and $\beta_{2j}\leftarrow\alpha_j$. If n=0, set $\beta_{2n+1}\leftarrow 0$ and if n>0, set $\beta_{2n+1}\leftarrow s_n$. Set $\beta\leftarrow(\beta_1,\ldots,\beta_{2n+1})$. ($\beta$ is now a c.a.s. of S.)

(3) If k=0, set $\psi\leftarrow()$ and exit. If n=0, set $\psi_1\leftarrow$"0=0", $\psi\leftarrow(\psi_1)$ and exit. For i=1,...,h do [$\sigma_{i,n}\leftarrow$sign(ldcf(B_i)); for j=n-1,...,0 set $\sigma_{i,j}\leftarrow(-\sigma_{i,j+1}$ if $i=\nu_{j+1}$, $\sigma_{i,j+1}$ otherwise)]. (Now $\sigma_{i,j}$ is the sign of B_i in S_{2j+1}, where $S=(S_1,\ldots,S_{2n+1})$.) For j=1,...,n, where $r_j=a_j/b_j$ and $s_j=c_j/d_j$ with $b_j>0$ and $d_j>0$, set $\psi_{2j}\leftarrow$"$B_{\nu_j}=0\&b_jx_1-a_j>0\&d_jx_1-c_j<0$". (Now ψ_{2j} defines $S_j=\{\alpha_j\}$.)

For $j=1,\ldots,n-1$, set $\psi_{2j+1} \leftarrow$ "$\sigma_{\nu_j,j}{}^B\nu_j > 0 \& \sigma_{\nu_{j+1},j}{}^B\nu_{j+1} > 0 \& b_j x_1 - a_j > 0 \& d_{j+1} x_1 - c_{j+1} < 0$". (If $\nu_j = \nu_{j+1}$ then the first two conjuncts are identical, so one can be omitted.) Set $\psi_1 \leftarrow$ "$\sigma_{\nu_1,o}{}^B\nu_1 > 0 \& d_1 x_1 - c_1 < 0$" and $\psi_{2n+1} \leftarrow$ "$\sigma_{\nu_n,n}{}^B\nu_n > 0 \& b_n x_1 - a_n > 0$". Set $\psi \leftarrow (\psi_1,\ldots,\psi_{2n+1})$. ($\psi$ is now a standard definition of S.) Exit.

(4) Apply BASIS to $\mathcal{A}$, obtaining $\mathcal{B}$, a coarsest squarefree basis for $\mathcal{A}$. (This action is inessential; we could set $\mathcal{B} \leftarrow \mathcal{A}$. But the algorithm is likely more efficient if the coarsest squarefree basis is used, and it may be still more efficient, on the average, if the finest basis is computed here.) If $k<r$, apply PROJ to $\mathcal{B}$, obtaining the projection, $\mathcal{P}$, of $\mathcal{B}$. If $k=r$, apply APROJ to $\mathcal{B}$, obtaining the augmented projection, $\mathcal{P}$, of $\mathcal{B}$.

(5) If $k=r$, set $k' \leftarrow k-1$; otherwise, set $k' \leftarrow k$. Apply DECOMP (recursively) to $\mathcal{P}$ and k', obtaining outputs β' and ψ'. (For some $\mathcal{P}$-invariant c.a.d. S' of R^{r-1}, β' is a c.a.s. of S' and ψ' is a standard definition of the c.a.d. S^* of $R^{k'}$ induced by S', except that $\psi'=()$ if $k'=0$. Since $\mathcal{P}$ contains the projection of $\mathcal{B}$ and S' is $\mathcal{P}$-invariant the real zeros of $\mathcal{B}$ are delineable on each cell of S' by Theorem 5. Hence S', together with the real algebraic functions defined by elements of $\mathcal{B}$ on the cells of S', determines a c.a.d. S of R^r. S is $\mathcal{B}$-invariant and therefore also $\mathcal{A}$-invariant since $\mathcal{B}$ is a basis for $\mathcal{A}$. Also, S^* is induced by S.)

(6) (This step extends the c.a.s. β' of S' to a c.a.s. β of S. Let $\beta' = (\beta'_1,\ldots,\beta'_l)$ and $\beta'_j = (\beta'_{j,1},\ldots,\beta'_{j,r-1})$. We assume, inductively, that there is associated with each algebraic point β'_j an algebraic number α'_j such that $Q(\beta'_{j,1},\ldots,\beta'_{j,r-1}) = Q(\alpha'_j)$ and polynomials $B'_{j,k}$ which represent the $\beta'_{j,k}$. The basis for this induction is trivial since the polynomial x represents $\beta'_{j,1} = \alpha'_j$ as an element of $Q(\alpha'_j)$ if α'_j is irrational, and if α'_j is rational it represents itself as an element of $Q = Q(\alpha'_j)$.) Let $\mathcal{B} = (B_1,\ldots,B_h)$. For $j=1,\ldots,l$ do [For $i=1,\ldots,h$ set $B^*_{j,i}(x) \leftarrow B_i(\beta'_{j,1},\ldots,\beta'_{j,r-1},x)$. ($B^*_{j,i}$ is a polynomial over $Q(\alpha'_j)$.) Apply ABASIS to α'_j and $(B^*_{j,1},\ldots,B^*_{j,h})$, obtaining $\hat{B}_j = (\hat{B}_{j,1},\ldots,\hat{B}_{j,m_j})$ a coarsest squarefree basis. Apply ISOL to α'_j and $\hat{B}_j$, obtaining outputs $I_j = (I_{j,1},\ldots,I_{j,n_j})$ and $\nu_j = (\nu_{j,1},\ldots,\nu_{j,n_j})$. ($\hat{B}_{j,\nu_{j,k}}$ has a unique real zero $\gamma_{j,k}$ in $I_{j,k}$, and $\gamma_{j,1} < \ldots < \gamma_{j,n_j}$ are all the real zeros of elements of $\hat{\mathcal{B}}_j$. For $k=1,\ldots,m_j$ do [Set $\hat{I}_{j,k}$ to the subsequence of I_j consisting of those $I_{j,l}$ such that $\nu_{j,l}=k$. (Then $\hat{I}_{j,k}$ is a list of rational isolating intervals for the real roots of $\hat{B}_{j,k}$.) Apply NORMAL to $\alpha'_j, \hat{B}_{j,k}$ and $\hat{I}_{j,k}$, obtaining as out-

puts $\bar{B}_{j,k}$ and $I^*_{j,k}$.] Merge the sequences $I^*_{j,k}$ into a single sequence $\bar{I}_j=(\bar{I}_{j,1},\ldots,\bar{I}_{j,n_j})$ with $\bar{I}_{j,1}<\bar{I}_{j,2}<\ldots<\bar{I}_{j,n_j}$. (Now $\gamma_{j,k}$ is represented by $(\bar{B}_{j,k},\bar{I}_{j,k})$.) If $n_j=0$, set $\delta_{j,1}\leftarrow 0$. If $n_j>0$, for $k=1,\ldots,n_j$, where $\bar{I}_{j,k}=(r_{j,k},s_{j,k})$, set $\delta_{j,2k-1}\leftarrow r_{j,k}$ and $\delta_{j,2k}\leftarrow\gamma_{j,k}$; also set $\delta_{j,2n_j+1}\leftarrow s_{j,n_j}$. For $k=1,\ldots,2n_j+1$, set $\beta_{j,k}\leftarrow(\beta'_{j,1},\ldots,\beta'_{j,r-1},\delta_{j,k})$. For $k=1,\ldots,2n_j+1$ apply SIMPLE to α'_j and $\delta_{j,k}$, obtaining outputs $\alpha_{j,k}$, $A_{j,k}$ and $B_{j,k}$. (Now $Q(\beta'_{j,1},\ldots,\beta'_{j,r-1},\delta_{j,k})=Q(\alpha'_j,\delta_{j,k})=Q(\alpha_{j,k})$, $A_{j,k}$ represents α'_j in $Q(\alpha_{j,k})$, and $B_{j,k}$ represents $\delta_{j,k}$ in $Q(\alpha_{j,k})$.) For $h=1,\ldots,r-1$ and $k=1,\ldots,2n_j+1$, where $\alpha_{j,k}$ is represented by $(C_{j,k},I'_{j,k})$, set $D_{j,h,k}(x)\rightarrow B'_{j,h}(A_{j,k}(x))$ modulo $C_{j,k}(x)$. $(\alpha'_j=A_{j,k}(\alpha_{j,k}),\beta'_{j,h}=B'_{j,h}(\alpha'_j)$ and $C_{j,k}(\alpha_{j,k})=0$, so $D_{j,h,k}$ represents $\beta'_{j,h}$ in $Q(\alpha_{j,k})$.)] Set $\beta\leftarrow(\beta_{1,1},\ldots,\beta_{1,2n_1+1},\ldots,\beta_{l,1},\ldots,\beta_{l,2n_l+1})$. (Now β is a c.a.s. of S.)

(7) If $k<r$, set $\psi\leftarrow\psi'$ and exit. (If $k<r$, then $k'=k$ so ψ' is a standard definition of the c.a.d. S^* of R^k induced by S', and hence induced also by S. Otherwise $k=r,k'=r-1$ and we next proceed to extend the standard definition ψ' of S' to a standard definition ψ of S. Since $k=r$, $\mathcal{P}$ is the augmented projection of $\mathcal{B}$ and, by Theorem 6, the real roots of every derivative of every element of $\mathcal{B}$ are delineable on every cell of S' because S' is $\mathcal{P}$-invariant.) For $j=1,\ldots,l$ do [For $i=1,\ldots,h$ apply DEFINE to B_i and β'_j, obtaining as output a sequence $\chi_{i,j}=(\chi_{i,j,1},\ldots,\chi_{i,j,2n_{i,j}+1})$. ($\chi_{i,j,k}$ is a standard quantifier-free formula such that $\psi'_j\&\chi_{i,j,k}$ defines the kth cell of the cylinder $S'_j\times R$ as determined by the real zeros of B_i on S'_j. We next proceed to use the $\chi_{i,j,k}$ to define the cells of the cylinder $S'_j\times R$ as determined by the real zeros of $B=\Pi_{i=1}^{h}B_i$, that is, the cells of the jth cylinder of S, using the results of step (6). Observe that B has n_j real zeros on S_j and that the kth real zero is a zero of $\hat{B}_{j,\nu_{j,k}}$.) For $i=1,\ldots,h$ and $k=1,\ldots,n_j$, set $\delta_{i,j,k}=1$ if $\hat{B}_{j,\nu_{j,k}}$ is a divisor of $B^*_{j,i}$, and $\delta_{i,j,k}=0$ otherwise. (Now $\delta_{i,j,k}=1$ just in case $B^*_{j,i}(\gamma_{j,k})=0$. For $k=1,\ldots,n_j$, set $\lambda_{j,k}$ to the least i such that $\delta_{i,j,k}=1$. (Now $\gamma_{j,k}$ is a root of $B^*_{j,\lambda_{j,k}}$.) For $k=1,\ldots,n_j$, set $\mu_{j,k}\leftarrow\Sigma_{i=1}^{\lambda_{j,k}}\delta_{i,j,k}$. (Now $\gamma_{j,k}$ is the $\mu_{j,k}$th real root of $B^*_{j,\lambda_{j,k}}$. Hence the kth real root of B on S'_j is the $\mu_{j,k}$th real root of $B_{\lambda_{j,k}}$ on S'_j.) For $k=1,\ldots,n_j$ set $\psi_{j,2k}\leftarrow\psi'_j\&\chi_{\lambda_{j,k},j,2\mu_{j,k}}$. For $k=1,\ldots,n_j-1$ set $\psi_{j,2k+1}\leftarrow\psi'_j\&\chi_{\lambda_{j,k},j,2\mu_{j,k}+1}\&\chi_{\lambda_{j,k+1},j,2\mu_{j,k+1}-1}$. If $\nu_{j,k}=\nu_{j,k+1}$ then the last two conjuncts of $\psi_{j,2k+1}$ coincide so one may be omitted.) If $n_j>0$, set $\psi_{j,1}\leftarrow\psi'_j\&\chi_{\lambda_{j,1},j,1}$ and $\psi_{j,2n_j+1}\leftarrow\psi'_j\&\chi_{\lambda_{j,n},j,2\mu_{j,n_j}+1}$. If $n_j=0$, set $\psi_{j,1}\leftarrow\psi'_j$.]

Set $\psi \leftarrow (\psi_{1,1},\ldots,\psi_{1,2n_1+1},\ldots,\psi_{l,2n_l+1})$. (Now ψ is a standard definition of S.) Exit.

Next we describe the algorithm DEFINE.

$$\phi = \text{DEFINE}(B,\beta)$$

Inputs: B is an integral polynomial in r variables, $r \geq 2$, such that for some connected set $S \subseteq R^{r-1}$ the real roots of B and of each derivative of B are delineable on S. β is an algebraic point of S.

Output: $\phi=(\phi_1,\ldots,\phi_{2m+1})$ is a sequence of standard quantifier-free formulas ϕ_i such that if ψ defines S then $\psi \& \phi_i$ defines the ith cell of the cylinder SxR as determined by the m real roots of B on S.

Algorithm Description

(1) (We let $\beta=(\beta_1,\ldots,\beta_{r-1})$. As in DECOMP, we may assume that we are given an algebraic number α such that $Q(\beta_1,\ldots,\beta_{r-1})=Q(\alpha)$, and polynomials B_i which represent β_i as elements of $Q(\alpha)$. Set $B^*(x)=B(\beta_1,\ldots,\beta_{r-1},x)$. Apply SQFREE to α and B^*, obtaining the list $\mathcal{B}^*=(B_1^*,\ldots,B_h^*)$ of squarefree factors of B^* and the list $(e_1,\ldots,e_h)$ of corresponding exponents. Apply ISOL to α and $\mathcal{B}^*$, obtaining as outputs the lists $(I_1,\ldots,I_m)$ and $(\nu_1,\ldots,\nu_m)$. (I_j isolates the jth real zero, γ_j, of the elements of $\mathcal{B}^*$, and γ_j is a zero of B_{ν_j}.) If m=0, set $\phi_1 \leftarrow$"0=0", $\phi \leftarrow (\phi_1)$, and exit. For i=1,...,m set $\mu_i \leftarrow e_{\nu_i}$. (Now γ_i is a zero of $B^*_{\nu_i}$ of multiplicity μ_i.) Set $\sigma_m \leftarrow \text{sign}(\text{ldcf}(B^*))$. For j=m-1,...,0 set $\sigma_j \leftarrow (-1)^{\mu_{j+1}}\sigma_{j+1}$. (Now σ_j is the sign of B in the (2j+1) th cell of the B-invariant decomposition of the cylinder SxR.) If m=1 and μ_1 is odd, set $\phi_1 \leftarrow$"σ_0B>0", $\phi_2 \leftarrow$"B=0", $\phi_3 \leftarrow$"σ_1B>0", $\phi \leftarrow (\phi_1,\phi_2,\phi_3)$, and exit.

(2) Set $B^{*\prime} \leftarrow \text{der}(B^*)$, $G \leftarrow \text{gcd}(B^*,B^{*\prime})$ and $H \leftarrow B^{*\prime}/G$. (Now $H(\delta)=0$ if and only if $B^{*\prime}(\delta)=0$ and $B^*(\delta)\neq 0$.) Set $\bar{H} \leftarrow \text{gcd}(H,H')$. ($\bar{H}$ is squarefree and has the same roots as H.) Apply ISOL to α and the list $(\bar{H})$, obtaining as output the list $I'=(I_1',\ldots,I_n')$ of isolating intervals for the roots of $B^{*\prime}$ which are not roots of B. For j=1,...,m and k=1,...,n, if I_j and I_k' are non-disjoint, replace I_j by its left or right half, whichever contains a root of B^*, and replace I_k' by its left or right half, whichever contains a root of B', and repeat until I_j and I_k' are disjoint. Set n_0 to the number of intervals I_k' such that $I_k' < I_1$. For j=1,...,m-1, set n_j

to the number of intervals I'_k such that $I_j<I'_k<I_{j+1}$. Set n_m to the number of intervals I'_k such that $I_m<I'_k$. Set $\lambda_1 \leftarrow n_o$. For $j=1,\ldots,m$ set $\lambda_{2j} \leftarrow \{\lambda_{2j-1}$ if $\mu_j=1$; $\lambda_{2j-1}+1$ if $\mu_j>1\}$, and $\lambda_{2j+1} \leftarrow \lambda_{2j}+n_j$. (Now λ_{2j-1} is the number of zeros of $B^{*'}$ less than γ_j, λ_{2j} is the number less than or equal to γ_j, and λ_{2m+1} is the number of all the zeros.)

(3) Set $B' \leftarrow der(B)$. Apply DEFINE to B' and β, obtaining $(\phi'_1,\ldots,\phi'_l)$ as output. (Thus DEFINE is a recursive algorithm; its termination is assured because $deg(B')<deg(B)$.)

(4) (This step computes ϕ_{2i} for $1\leq i\leq m$.) For $i=1,\ldots,m$ if $\mu_i>1$ set $\phi_{2i} \leftarrow \phi'_{2\lambda_{2i}}$. (If $\mu_i>1$ then the ith real zero of B is the λ_{2i}-th real zero of B'.) For $i=1,\ldots,m$ if $\mu_i=1$ set $\phi_{2i} \leftarrow$"$B=0 \& \phi'_{2\lambda_{2i-1}+1}$". (There are λ_{2i-1} zeros of B less than the ith zero of B, so the ith zero of B is in the $\lambda_{2\lambda_{i-1}+1}$-th cell of the B' decomposition. By Rolle's theorem, any two real zeros of B are separated by a zero of B' so there is only one zero of B in this cell.)

(5) (This step defines ϕ_{2i+1} for $1\leq i<m$. There are four cases.) For $i=1,\ldots,m-1$ if $\mu_i>1$ and $\mu_{i+1}>1$ set $\phi_{2i+1} \leftarrow \bigvee_{2\lambda_{2i}+1\leq j\leq 2\lambda_{2i+2}-1} \phi'_j$. (In this case the ith zero of B is the λ_{2i}th zero of B' and the (i+1)th zero of B is the λ_{2i+2}th zero of B'.) For $i=1,\ldots,m-1$ if $\mu_i=1$ and $\mu_{i+1}>1$ set $\phi_{2i+1} \leftarrow \{\sigma_i B>0 \& \phi'_{2\lambda_{2i}+1}\} \vee \{\bigvee_{2\lambda_{2i}+2\leq j\leq 2\lambda_{2i+2}-1} \phi'_j\}$. (There are λ_{2i} zeros of B' less than the ith zero of B. By Rolle's theorem the ith zero of B is only zero of B in the $(2\lambda_{2i}+1)$th cell of the B' decomposition. Since $\mu_i=1$, B changes sign from σ_{i-1} to σ_i at this zero.) For $i=1,\ldots,m-1$ if $\mu_i>1$ and $\mu_{i+1}=1$ set $\phi_{2i+1} \leftarrow \{\sigma_i B>0 \& \phi'_{2\lambda_{2i+2}+1}\} \vee \{\bigvee_{2\lambda_{2i}+1\leq j\leq 2\lambda_{2i+2}} \phi'_j\}$. (This case is similar to the preceding case.) For $i=1,\ldots,m-1$ if $\mu_i=1$ and $\mu_{i+1}=1$ set $\phi_{2i+1} \leftarrow \{\sigma_i B>0 \& \sigma'_{2\lambda_{2i}+1}\} \vee \{\sigma_i B>0 \& \phi'_{2\lambda_{2i+2}+1}\} \vee \{\bigvee_{2\lambda_{2i}+2\leq j\leq 2\lambda_{2i+2}} \phi'_j\}$.

(6) (This step defines ϕ_1 and ϕ_{2m+1}.) If $\mu_1>1$ set $\phi_1 \leftarrow \bigvee_{1\leq j\leq 2\lambda_2-1} \phi'_j$. If $\mu_1=1$ set $\phi_1 \leftarrow \{\sigma_o B>0 \& \phi'_{2\lambda_2+1}\} \vee \{\bigvee_{1\leq j\leq 2\lambda_2} \phi'_j\}$. If $\mu_m>1$ set $\phi_{2m+1} \leftarrow \bigvee_{2\lambda_{2m}+1\leq j\leq 2\lambda_{2m+1}+1} \phi'_j$. If $\mu_m=1$ set $\phi_{2m+1} \leftarrow \{\sigma_m B>0 \& \phi'_{2\lambda_{2m}+1}\} \vee \{\bigvee_{2\lambda_{2m}+2\leq j\leq 2\lambda_{2m+1}+1} \phi'_j\}$. Set $\phi \leftarrow (\phi_1,\ldots,\phi_{2m+1})$ and exit.

Let ϕ be any formula in r free variables and let $S \subseteq R^r$. ϕ is <u>invariant on</u> S in case either $(a_1,\ldots,a_r)$ is true for all $(a_1,\ldots,a_r) \in S$ or $(a_1,\ldots,a_r)$ is false for all $(a_1,\ldots,a_r) \in S$. If S is a c.a.d. of R^r, we say that S is <u>ϕ-invariant</u> in case ϕ is invariant on each cell of S. If ϕ is a standard quantifier-free formula in r variables, $\mathcal{A}$ is the set of all non-zero polynomials which occur in ϕ , and S is an $\mathcal{A}$-invariant c.a.d. of R^r, then clearly S is also ϕ-invariant.

If ϕ is a sentence, we will denote by $v(\phi)$ the truth value of ϕ, with "true" represented by 1, "false" by 0. Accordingly, if $(v_1,\ldots,v_n)$ is a vector of zeros and ones, then we define $\bigwedge_{i=1}^n v_i = 1$ if each $v_i = 1$ and $\bigwedge_{i=1}^n v_i = 0$ otherwise. Similarly, we define $\bigvee_{i=1}^n v_i = 0$ if each $v_i = 0$ and $\bigvee_{i=1}^n v_i = 1$ otherwise. If ϕ is a formula in r free variables and $a = (a_1,\ldots,a_r) \in R^r$, we set $v(\phi,a) = v(\phi(a_1,\ldots,a_r))$. If ϕ is invariant on S, we set $v(\phi,S) = v(\phi,a)$ for any $a \in S$.

The following theorem is fundamental in the use of a c.a.d. for quantifier elimination.

<u>Theorem 7.</u> Let $\phi(x_1,\ldots,x_r)$ be a formula in r free variables and let ϕ^* be $(\forall x_r)\phi$ or $(\exists x_r)\phi$. If $r>1$, let S be a ϕ-invariant c.a.d. of R^r, S^* the c.a.d. of R^{r-1} induced by S. Then S^* is ϕ -invariant. If $S^* = (S_1,\ldots,S_m)$ and $S = (S_{1,1},\ldots,S_{1,n_1},\ldots,S_{m,1},\ldots,S_{m,n_m})$ where $(S_{i,1},\ldots,S_{i,n_i})$ is the <u>ith</u> cylinder of S, then $v((\forall x_r)\phi,S_i) = \bigwedge_{j=1}^{n_i} v(\phi,S_{ij})$ and $v((\exists x_r)\phi,S_i) = \bigvee_{j=1}^{n_i} v(\phi,S_{i,j})$. If $r=1$ and $S=(S_1,\ldots,S_n)$ is a c.a.d. of R, then $v((\forall x_1)\phi) = \bigwedge_{i=1}^n v(\phi,S_i)$ and $v((\exists x_1)\phi) = \bigvee_{i=1}^n (\phi,S_i)$.

<u>Proof.</u> We will prove this theorem only for $r>1$, and only for the case that ϕ^* is $(\forall x_r)\phi$. The omitted cases are similar. So let $S=(S_{1,1},\ldots,S_{1,n_1},\ldots,S_{m,1},\ldots,S_{m,n_m})$ be a ϕ-invariant c.a.d. of R^r, $S^*=(S_1,\ldots,S_m)$ the c.a.d. of R^{r-1} induced by S. Let $1 \le i \le m$ and choose $(a_1,\ldots,a_{r-1}) \in S_i$. Assume $\phi^*(a_1,\ldots,a_{r-1})$ is true. Let $(b_1,\ldots,b_{r-1}) \in S_i$. Let $b_r \in R$. Then for some j, $(b_1,\ldots,b_r) \in S_{i,j}$. Choose a_r so that $(a_1,\ldots,a_r) \in S_{i,j}$. Since $\phi^*(a_1,\ldots,a_{r-1})$ is true, $\phi(a_1,\ldots,a_{r-1},a)$ is true for all $a \in R$. In particular, $\phi(a_1,\ldots,a_r)$ is true. Since S is ϕ-invariant, ϕ is invariant on $S_{i,j}$. So $\phi(b_1,\ldots,b_r)$ is true. Since b_r is an arbitrary element of R, $\phi^*(b_1,\ldots,b_{r-1})$ is true. Since $(b_1,\ldots,b_{r-1})$ is an arbitrary element of S_i, ϕ^* is invariant on S_i. Since S_i is an arbitrary element of S, ϕ^* is

S-invariant. This completes the proof of the first part.

Now assume $v(\phi^*, S_i)=1$. Let $1\leq j\leq n_i$. Choose $(a_1,\ldots,a_{r-1})\varepsilon S_i$. By the first part, ϕ^* is S-invariant so $\phi^*(a_1,\ldots,a_{r-1})$ is true. Hence $\phi(a_1,\ldots,a_r)$ is true for all $a_r\varepsilon R$. Choose a_r so that $(a_1,\ldots,a_r)\varepsilon S_{i,j}$. By the ϕ-invariance of S, $v(\phi,S_{i,j})=1$. Since j is arbitrary, $\bigwedge_{j=1}^{n_i} v(\phi,S_{i,j})=1$.

Next assume $v(\phi^*,S_i)=0$. Choose $(a_1,\ldots,a_{r-1})\varepsilon S_i$. Since ϕ^* is S-invariant, $\phi^*(a_1,\ldots,a_{r-1})$ is false. Hence for some $a_r\varepsilon R$, $\phi(a_1,\ldots,a_r)$ is false. Let $(a_1,\ldots,a_r)\varepsilon S_{i,j}$. By the ϕ-invariance of S, $v(\phi,S_{i,j})=0$. Hence $\bigwedge_{j=1}^{n_j} v(\phi,S_{i,j})=0$. ∎

Let $a,b,\varepsilon R^r$ with $a=(a_1,\ldots,a_r)$ and $b=(b_1,\ldots,b_r)$. We define $a\sim_k b$ in case $a_i=b_i$ for $1\leq i\leq k$. Note that $a\sim_r b$ if and only if a=b, while $a\sim_0 b$ for all $a,b\varepsilon R_r$. We define $a<b$ in case $a\sim_k b$ and $a_{k+1}<b_{k+1}$ for some k, $0\leq k<r$. The relation $a<b$ is a linear order on R^r, which we recognize as the lexicographical order on R^r induced by the usual order on R. We note that if $(\beta_1,\ldots,\beta_m)$ is a cylindrical sample of a c.a.d. S, then $\beta_1<\beta_2<\ldots<\beta_m$.

The cylindrical structure of a c.a.d. S is obtainable from any c.a.s. β of S. We define a grouping function g. Let $\beta=(\beta_1,\ldots,\beta_m)$ by any sequence of elements of R^r. Then for $0\leq k\leq r$, $g(k,\beta)=((\beta_1,\ldots,\beta_{n_1}),(\beta_{n_1+1},\ldots,\beta_{n_2}),\ldots,(\beta_{n_{l-1}+1},\ldots,\beta_{n_l}))$ where $1\leq n_1<n_2<\ldots<n_{l-1}<n_l=m, \beta_j\sim_k\beta_{j+1}$ for $n_i<j<n_{i+1}$, and $\beta_{n_i}\not\sim_k\beta_{n_i+1}$. Note that $g(0,\beta)=((\beta_1,\ldots,\beta_m))$ and $g(r,\beta)=((\beta_1),\ldots,(\beta_m))$. Also, if S is a c.a.d. of R^r, $S^*=(S_1,\ldots,S_m)$ is the c.a.d. of R^k induced by S, and β is a c.a.s. of S, then $g(k,\beta)=(\beta_1^*,\ldots,\beta_m^*)$ where β_i^* is the list of those points in β which belong to $S_i^*xR^{r-k}$.

We define now an evaluation function e. Let $\phi(x_1,\ldots,x_r)$ be a standard quantifier-free formula, S a ϕ-invariant c.a.d. of R^r, β a c.a.s. of S, and let $\phi^*(x_1,\ldots,x_k)$ be $(Q_{k+1}x_{k+1})\ldots(Q_rx_r)\phi(x_1,\ldots,x_r)$, $0\leq k\leq r$. Let $S^*=(S_1^*,\ldots,S_m^*)$ be the c.a.d. of R^k induced by S, $\beta^*=(\beta_1^*,\ldots,\beta_m^*)=g(k,\beta)$. Then we define $e(\phi^*,\beta_i^*)$ by induction on r-k, as follows. If k=r, then ϕ^* is ϕ, $\beta_i^*=(\beta_i)$, and we define $e(\phi^*,\beta_i^*)=v(\phi,\beta_i)$. If k<r, let $g(k+1,\beta_i^*)=(\hat{\beta}_1,\ldots,\hat{\beta}_n)=\hat{\beta}$. Then each $\hat{\beta}_j$ is in the sequence $g(k+1,\beta)$. Let $\hat{\phi}(x_1,\ldots,x_{k+1})$ be $(Q_{k+2}x_{k+2})\ldots(Q_rx_r)\phi(x_1,\ldots,x_r)$. Then we define

$$e(\phi^*, \beta_i^*) = \bigwedge_{j=1}^{n} e(\hat{\phi}, \hat{\beta}_j), \text{ if } Q_{k+1} = \forall,$$

$$e(\phi^*, \beta_i^*) = \bigvee_{j=1}^{n} e(\phi, \beta_j), \text{ if } Q_{k+1} = \exists.$$

Theorem 8. Let $\phi(x_1,\ldots,x_r)$ be a standard quantifier-free formula, S a ϕ-invariant c.a.d. of R^r, β a cylindrical algebraic sample of S. Let $\phi^*(x_1,\ldots,x_k)$ be $(Q_{k+1}x_{k+1})\ldots(Q_r x_r)\phi(x_1,\ldots,x_r)$, $0 \leq k \leq r$. If $k>0$, let $S^* = (S_1^*,\ldots,S_m^*)$ be the c.a.d. of R^k induced by S and let $g(k,\beta) = \beta^* = (\beta_1^*,\ldots,\beta_m^*)$. Then $e(\phi^*,\beta_i^*) = v(\phi^*, S_i^*)$ for $1 \leq i \leq m$. If $k=0$, then $e(\phi^*,\beta) = v(\phi^*)$.

Proof. By an induction on r-k, paralleling the definition of e and using Theorem 7. ∎

By Theorem 8, if $k=0$, then $e(\phi^*,\beta)$ is the truth value of ϕ^*. If $k>0$, let $\psi = (\psi_1,\ldots,\psi_m)$ be a standard definition of the c.a.d. S^*, as produced by DECOMP, and let ψ^* be the disjunction of those ψ_i such that $e(\phi^*, \beta_i^*) = 1$. Then ψ^* is a standard quantifier-free formula equivalent to ϕ^*.

The function e can be computed by an algorithm based directly on the definition of e. $e(\phi^*, \beta_i^*)$ is ultimately just some Boolean function of the truth values of ϕ at the sample points β_j in the list β_i^*, that is, of the $v(\phi,\beta_j)$. It is important to note, however, that usually not all $v(\phi,\beta_j)$ need be computed. For example, if $Q_{k+1} = \forall$ then the computation of $e(\phi^*,\beta_i^*)$ can be terminated as soon as any j is found for which $e(\hat{\phi},\beta_j) = 0$. Similarly, the computation of $v(\phi,\beta)$, β an algebraic point, is Boolean-reducible to the case in which ϕ is a standard atomic formula. This case itself amounts to determining the sign of $A(\beta_1,\ldots,\beta_r)$ where A is an integral polynomial and $\beta = (\beta_1,\ldots,\beta_r)$ is a real algebraic point. With β we are given an algebraic number α such that $Q(\beta_1,\ldots,\beta_r) = Q(\alpha)$ and rational polynomials B_i such that $\beta_i = B_i(\alpha)$. We then obtain sign $(A(\beta_1,\ldots,\beta_r)) = \text{sign}(A(B_1(\alpha),\ldots,B_r(\alpha))) = \text{sign}(C(\alpha))$ using an algorithm of [16]

Since a standard formula ϕ may contain several occurences of the same polynomial, we assume that the polynomials occurring in ϕ are stored uniquely in a list $\mathcal{A}$ inside the computer, and that the formula ϕ is stored so that the atomic formulas of ϕ contain references to this list in place of the polynomials themselves. Note also that the list $\mathcal{A}$ need not contain two different polynomials whose ratio is a non-

zero rational number. In computing $v(\phi,\beta)$, a list σ should be maintained, containing $\text{sign}(A(\beta))$ for various polynomials $A \in \mathcal{A}$. Whenever the computation of $v(\phi,\beta)$ requires the computation of $\text{sign}(A(\beta))$ the list σ should be searched to determine whether $\text{sign}(A(\beta))$ was previously computed; if not, $\text{sign}(A(\beta))$ should be computed and placed on the list. Thus the computation of $v(\phi,\beta)$ will require at most one computation of $\text{sign}(A(\beta))$ for each $A \in \mathcal{A}$, and in some cases $\text{sign}(A(\beta))$ will not be computed for all $A \in \mathcal{A}$.

In terms of the functions g and e, the evaluation algorithm can now be described as follows.

$$\psi^* = \text{EVAL}(\phi^*,\beta,\psi)$$

Inputs: ϕ^* is a standard prenex formula $(Q_{k+1}x_{k+1})\ldots(Q_r x_r)\phi(x_1,\ldots,x_r)$ where $0 \leq k \leq r$ and ϕ is quantifier-free. β is a c.a.s. of some ϕ-invariant c.a.d. S of R^r. ψ is a standard definition of the c.a.d. S^* of R^k induced by S if $k>0$, the null list if $k=0$.

Output: $\psi^* = \psi(x_1,\ldots,x_k)$ is a standard quantifier-free formula equivalent to ϕ^*.

Algorithm Description

(1) If $k>0$ go to (2). Set $v=e(\phi^*,\beta)$. If $v=0$ set $\psi^* \leftarrow$ "1=0". If $v=1$, set $\psi^* \leftarrow$ "0=0". Exit.
(2) Set $\beta^* \leftarrow g(k,\beta)$. Let $\beta^* = (\beta_1^*,\ldots,\beta_m^*)$ and $\psi = (\psi_1,\ldots,\psi_m)$. Set $\psi^* \leftarrow$ "1=0". For $i=1,\ldots,m$ if $e(\phi^*,\beta_i^*)=1$ set $\psi^* \leftarrow \psi_i \vee \psi$. Exit.

Finally we have the following quantifier elimination algorithm.

$$\psi^* = \text{ELIM}(\phi^*)$$

Input: ϕ^* is a standard prenex formula $(Q_{k+1}x_{k+1})\ldots(Q_r x_r)\phi(x_1,\ldots,x_r)$ where $0 \leq k \leq r$ and ϕ is quantifier-free.

Output: ψ^* is a standard quantifier-free formula equivalent to ϕ^*.

Algorithm Description

(1) Determine k. Extract from ϕ the list $\mathcal{A} = (A_1,\ldots,A_m)$ of distinct non-zero polynomials occurring in ϕ.

(2) Apply DECOMP to $\mathcal{A}$ and k, obtaining β and ψ as outputs.
(3) Set $\psi^* \leftarrow EVAL(\phi^*, \beta, \psi)$ and exit.

4. Algorithm Analysis. Step (4) of the algorithm DECOMP provides for the optional computation of a basis $\mathcal{B}$ for a set $\mathcal{A}$ of integral polynomials. Experience with the algorithm provides a strong indication that this basis calculation is very important in reducing the total computing time of the algorithm. If the set $\mathcal{A}$ is the result of two or more projections, as in general it will be, then it appears that the polynomials in $\mathcal{A}$ have a considerable probability of having factors, common factors, and multiple factors. This will be discussed further in Section 5. But, as remarked in Section 3, the basis calculation of step (4) is not essential to the validity of the algorithm. In order to simplify the analysis of the algorithm, we will assume that this basis calculation is not performed. In general, the polynomials in the basis $\mathcal{B}$ will have smaller degrees than the polynomials of $\mathcal{A}$, but the number of polynomials in $\mathcal{B}$ may be either greater or less than the number in $\mathcal{A}$.

In Section 3 we gave conceptually simple definitions of projection and augmented projection, which definitions can be improved somewhat in order to reduce the sizes of these sets. It is easy to see that in the definition of the projection we can set $\mathcal{B}_2 = \{psc_k(red^i(A), red^j(B)) : A,B \in \mathcal{A} \& A<B \& i \geq 0 \& j \geq 0 \& 0 \leq k < \min(\deg(red^i(A)), \deg(red^j(B)))\}$, where "<" is an arbitrary linear ordering of the elements of $\mathcal{A}$. Also, in the definition of the augmented projection, we can set $\mathcal{P}' = \{psc_k(der^j(red^i(A)), der^{j+1}(red^i(A))) : A \in \mathcal{A} \& i \geq 0 \& j \geq 0 \& 0 \leq k < \deg(der^{j+1}(red^i(A)))\}$. Then the set $\mathcal{B}_1$ in the definition of the projection is contained in $\mathcal{P}'$, and the augmented projection of $\mathcal{A}$ is $\mathcal{L} \cup \mathcal{B}_2 \cup \mathcal{P}'$.

Now suppose that the set $\mathcal{A}$ contains m polynomials, with the degree of each polynomial in each variable at most n. Assume $m \geq 1$ and $n \geq 1$. Then the set $\mathcal{L}$ contains at most mn elements. In the set $\mathcal{B}_2$, the pair

(A,B) can be chosen in $\binom{m}{2}$ ways. Since $k<\min(\deg(\mathrm{red}^i(A)), \deg(\mathrm{red}^j(B)))$ $\leq \min(n-i,n-j)=n-\max(i,j)$, we have $0\leq i,j\leq n-k-1$. Hence for given k, $0\leq k\leq n-1$, the pair (i,j) can be chosen in at most $(n-k)^2$ ways. Hence (i,j,k) can be chosen in $\sum_{k=0}^{n-1}(n-k)^2=\frac{n(n+1)(2n+1)}{6}$ ways. So $\mathcal{B}_2$ has at most $\binom{m}{2}\frac{n(n+1)(2n+1)}{6}$ elements. In the definition of the set $\mathcal{P}'$, we must have $k<n-i-j-1$. For given k, $0\leq k\leq n-2$, (i,j) can be chosen in $\sum_{h=0}^{n-k-2}(h+1)=\binom{n-k}{2}$ ways. Hence (i,j,k) can be chosen in $\sum_{k=0}^{n-2}\binom{n-k}{2}=\binom{n+1}{3}$ ways. So $\mathcal{P}'$ has at most $m\binom{n+1}{3}$ elements. Altogether, the augmented projection has at most $\binom{m}{2}\frac{n(n+1)(2n+1)}{6}$ $+ m\binom{n+1}{3}+mn$ elements. For n=1, this reduces to $\binom{m}{2}+m=\binom{m+1}{2}\leq m^2$. For $n\geq 2$, $\binom{m}{2}\frac{n(n+1)(2n+1)}{6} + m\binom{n+1}{3}+mn\leq\frac{m^2}{2}\cdot\frac{(15/4)n^3}{6} + m\frac{n^3}{6} + \frac{1}{4}mn^3<m^2n^3$. So in all cases the augmented projection of $\mathcal{A}$ has at most m^2n^3 elements.

By the definition of a principle subresultant coefficient, each element of $\mathcal{B}_2$ or $\mathcal{P}'$ is the determinant of a matrix with at most 2n rows and columns, whose entries are coefficients of elements of $\mathcal{A}$. Hence the degree of any element of the augmented projection, in any variable, is at most $2n^2$.

In order to analyze the growth of coefficient length under the augmented projection operation, we need the concept of the norm of a polynomial. If A is any integral polynomial, the norm of A, denoted by $|A|_1$, is defined to be sum of the absolute values of the integer coefficients of A. This "norm" is actually just a semi-norm, having the important properties $|A+B|_1\leq|A|_1+|B|_1$ and $|A\cdot B|_1\leq|A|_1\cdot|B|_1$. Using these properties, it is easy to show (see [22]) that if deg(A)=m and deg(B) =n, then any square submatrix of the Sylvester matrix of A and B has a determinant whose norm is at most $|A|_1^n|B|_1^m$.

Let c be the maximum of the norms of the elements of $\mathcal{A}$. For any polynomials A with deg(A)=n, $|A'|_1\leq n|A|_1$. Hence it is easy to see that if $P\in\mathcal{P}'$ then $|P|_1\leq(n^jc)^{n-j-1}(n^{j+1}c)^{n-j}\leq n^{n^2/2}c^{2n}$, while if $P\in\mathcal{L}\cup\mathcal{B}_2$ then $|P|_1\leq c^{2n}$.

The length of any non-zero integer a, L(a), is the number of bits in the binary representation of a, and L(0)=1. It is easy to show that $L(ab)\leq L(a)+L(b)$ and hence $L(a^n)\leq nL(a)$ if n>0. Also, $L(a)\leq a$ if a>0. So if P is any element of the augmented projection of $\mathcal{A}$, then $L(|P|_1)\leq\frac{1}{2}n^2$ $L(n)+2nL(c)\leq\frac{1}{2}n^3+2nL(c)$.

The following theorem summarizes the several things we have proved.

Theorem 9. Let $\mathcal{A}$ be a non-empty finite set of integral polynomials in r variables, $r \geq 2$. Let $\mathcal{A}^*$ be the augmented projection of $\mathcal{A}$. Let m be the number of elements of $\mathcal{A}$, n the maximum degree of any element of $\mathcal{A}$ in any variable , $n \geq 1$. Let d be the maximum of the lengths of the norms of the elements of $\mathcal{A}$. Let m^*, n^* and d^* be the same functions of $\mathcal{A}^*$. Then

$$m^* \leq m^2 n^3, \tag{2}$$

$$n^* \leq 2n^2, \tag{3}$$

$$d^* \leq \frac{1}{2} n^3 + 2nd. \tag{4}$$

When $\mathcal{A}$ is a set of polynomials in r variables, algorithm DECOMP computes a sequence of r-1 projections or augmented projections. Using Theorem 9 we can now derive bounds for all such projections.

Theorem 10. Let $\mathcal{A}$, m, n and d be defined as in Theorem 9. Let $\mathcal{A}_1 = \mathcal{A}$ and let $\mathcal{A}_{i+1}$ be the augmented projection of $\mathcal{A}_i$ for $1 \leq i < r$. Let m_k be the number of elements of $\mathcal{A}_k$, n_k the degree maximum for $\mathcal{A}_k$, d_k the norm length maximum for $\mathcal{A}_k$. Then

$$m_k \leq (2n)^{3^k} m^{2^{k-1}}, \tag{5}$$

$$n_k \leq \frac{1}{2} (2n)^{2^{k-1}}, \tag{6}$$

$$d_k \leq (2n)^{2^k} d. \tag{7}$$

Proof. One may first prove (6) by a simple induction on k, using (3). (5) obviously holds for k=1. Assuming (5) holds for k, by (2) we have $m_{k+1} \leq \frac{1}{8} (2n)^a m^{2^k}$ where $a = 2 \cdot 3^k + 3 \cdot 2^{k-1} \leq 6 \cdot 3^{k-1} + 3 \cdot 3^{k-1} = 3^{k+1}$, proving (5). (7) obviously holds for k=1. Assuming (7) holds for k, by (4) we have $d_{k+1} \leq \frac{1}{16} (2n)^a + (2n)^a d \leq 2(2n)^a d \leq (2n)^{a+1} d$ where $a = 3 \cdot 2^{k-1}$. But $a+1 \leq 2^{k+1}$ so (7) is established.

Using Theorem 10, we can now bound the time to compute all projections.

Theorem 11. Let $\mathcal{A}$, m, n, d and $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be defined as in Theorem

10. Then there is an algorithm which computes $\mathcal{A}_2,\ldots,\mathcal{A}_r$ from $\mathcal{A}_1=\mathcal{A}$ in time dominated by $(2n)^{3^{r+1}}m^{2^r}d^2$.

Proof. Let A and B be integral polynomials in r variables, with degrees in each variable not exceeding $n\geq 2$, and with norms of lengths d or less. There is described in (5) an algorithm for computing the resultant of A and B, whose computing time is dominated by $n^{2r+2}d^2$. It is easy to see how to generalize this algorithm to compute $psc_k(A,B)$, for any k, within the same time bound. By (6) and (7), any derivative of any element of $\mathcal{A}_k$ has a norm whose length is at most $d_k+L(n_k!)\leq d_k+n_k^2 \leq \frac{5}{4}(2n)^{2^k}d=d_k'$. Since the elements of $\mathcal{A}_k$ have r-k+1 variables, each p.s.c. of $\mathcal{A}_{k+1}$ can be computed in time dominated by $n_k^{2(r-k+1)}d_k'^2$, and there are at most m_{k+1} such p.s.c.'s to be computed. Using the inequality $2(r-k+1)\leq 2^{r-k+1}$, we thus find that the time to compute all p.s.c.'s of $\mathcal{A}_{k+1}$ is dominated by $(2n)^a m^{2^k}d^2$ where $a=3^{k+1}+2^r+2^{k+1}\leq 3^r+2^r+2^r\leq 9\cdot 3^{r-2}+8\cdot 3^{r-2}\leq 17\cdot 3^{r-2}<2\cdot 3^r$. Hence the p.s.c.'s of $\mathcal{A}_{k+1}$ can be computed in time $(2n)^{2\cdot 3^r}m^{2^r}d^2$. Multiplying by r and using $r\leq 2^{r-1}$, the p.s.c.'s of $\mathcal{A}_2,\ldots,\mathcal{A}_r$ can be computed in time $(2n)^{3^{r+1}}m^{2^r}d^2$. We have ignored the time required to compute reducta and derivatives, but this is relatively trivial. ∎

Let S be the c.a.d. of R^r computed by DECOMP and let S_k be the c.a.d. of R^k induced by S, for $1\leq k\leq r$. Thus $S=S_r$. Let c_k be the number of cells in S_k. The cells of S_1 are determined by the real roots of m_r polynomials, each of degree n_r at most. There are at most $m_r n_r$ such roots and hence $c_1\leq 2m_r n_r+1$. For each value of k, $2\leq k\leq r$, step (6) substitutes the k-1 coordinates of each sample point of S_{k-1} for the first k-1 variables of the k-variable polynomials in $\mathcal{A}_{r-k+1}$, thereby obtaining $u_{r-k+1}\leq c_{k-1}m_{r-k+1}$ univariate polynomials with real algebraic number coefficients, each of degree n_{r-k+1} at most. These polynomials have at most $c_{k-1}m_{r-k+1}n_{r-k+1}$ real roots, and hence $c_k\leq 2m_{r-k+1}n_{r-k+1}c_{k-1}+1$. For convenience, we set $u_r=m_r$. We can now prove the following theorem

Theorem 12. For $1\leq k\leq r$, both u_k and c_k are less than $(2n)^{3^{r+1}}m^{2^r}$.

Proof. We have shown above that $c_1\leq 2m_r n_r+1$; hence $c_1\leq 4m_r n_r$. Similarly, from $c_k\leq 2m_{r-k+1}n_{r-k+1}c_{k-1}+1$ it follows that $c_k\leq 4m_{r-k+1}n_{r-k+1}c_{k-1}$.

By induction on k, we then have $c_k \leq \prod_{i=r-k+1}^{r} 4m_i n_i$. Hence $c_k \leq 2^{2r} \prod_{i=1}^{r} m_i n_i$ for all k. In a similar manner it is easy to show that $u_k \leq 2^{2r} \prod_{i=1}^{r} m_i n_i$ for all k. By (5) and (6) we then deduce that $2^{2r} \prod_{i=1}^{r} m_i n_i \leq (2n)^{a+b+2r} m^b$ where $a=\sum_{k=1}^{r} 3^k < \frac{1}{2} \cdot 3^{r+1}$ and $b=\sum_{k=1}^{r} 2^{k-1} < 2^r$. Hence it suffices to show that $2^r+2r \leq \frac{1}{2} \cdot 3^{r+1}$. But $2^r+2r \leq 2 \cdot 2^r \leq 4 \cdot 2^{r-1} \leq 4 \cdot 3^{r-1} < \frac{1}{2} \cdot 3^{r+1}$. ∎

Our next goal is to bound the time for step (1) of DECOMP. We must first obtain bounds for the computing times of the subalgorithms BASIS and ISOL.

There exist (see [6]) polynomial greatest common divisor algorithms for univariate integral polynomials which, when applied to two polynomials of degree n or less and with norms of length d or less, have a maximum computing time dominated by n^3d^2, Mignotte has recently shown, [23], that if A is a univariate integral polynomial with degree n and norm c, and if B is any divisor of A, then $|B|_1 \leq 2^n c$. From these two facts it easily follows that the squarefree factorization of A can be computed by the algorithm described in [14] in time dominated by $n^6+n^4d^2$ where d is the length of $c=|A|_1$ and $n=\deg(A)$.

Now suppose the coarsest squarefree basis algorithm outlined in Section 3 is applied to a set of m univariate integral polynomials, with degrees and norm lengths bounded by n and d respectively. In each of the m applications of Loos' algorithm, each input basis set will contain at most mn polynomials, with degrees and norm lengths bounded by n and n+d respectively. Hence the time for all applications of Loos' algorithm will be dominated by $m(mn)^2n^3(n+d)^2$, hence by $m^3n^5(n^2+d^2) \leq m^3n^7d^2$. The time required for the m squarefree factorizations will be dominated by mn^6d^2. Hence we arrive at a maximum computing time of $m^3n^7d^2$ for BASIS.

Now consider the computing time of ISOL when applied to a set $\mathcal{A}$ of m univariate integral squarefree and pairwise relatively prime polynomials, with a degree bound of n and a norm length bound of d. Collins has shown, [22], that if A is a univariate integral squarefree polynomial with $\deg(A)=n$ and $|A|_1=c$, then the distance between any two roots of A is at least $\frac{1}{2}(e^{1/2}n^{3/2}c)^{-n}$. This theorem on root separation, together with the discussion of Heindel's algorithm in [6], implies that Heindel's algorithm will isolate the real roots of A in time dominated by $n^8+n^7d^3$. Hence the real roots of the m polynomials in $\mathcal{A}$ can be sepa-

rately isolated in time dominated by $mn^8+mn^7d^3$. An isolating interval for a root of $A_i \in \mathcal{A}$ can be refined to length less than 2^{-h} in time dominated by $n^2h^3+n^2d^2h$. By application of the root separation theorem to the product $A=\Pi_{i=1}^{m}A_i$ of the elements of $\mathcal{A}$, the distance between any two roots of A is at least $\frac{1}{2}(e^{1/2}(mn)^{3/2}c^m)^{-mn}=\delta$. Hence if the isolating intervals for each A_i are refined to length 2^{-h} with $\delta/4 \leq 2^{-h} < \delta/2$ then all intervals for all A_i are disjoint. We then have h codominant with $mnL(mn)+m^2nd$, so the time to refine each interval is dominated by $m^3n^5L(mn)^3+m^6n^5d^3$, hence by $m^4n^6+m^6n^5d^3$. Since there are at most mn intervals to refine, the total time for ISOL is dominated by $(mn^8+mn^7d^3)+mn(m^4n^6+m^6n^5d^3)$, hence by $mn^8+m^7n^7d^3$.

Theorem 13. The computing time for step (1) of DECOMP is dominated by $(2n)^{3^{r+3}}m^{2^{r+2}}d^3$.

Proof. The time to apply BASIS in step (1) is dominated by $m_r^3n_r^7d^2$. By Theorem 10, since $d+1 \leq 2d$, $m_r^3n_r^7d^2$ is dominated by $(2n)^a m^b d^2$ where $b=3\cdot 2^{r-1} < 2^{r+1}$ and $a \leq 3\cdot 3^r+7\cdot 2^{r-1}+2\cdot 2^r \leq 9\cdot 3^{r-1}+7\cdot 2^{r-1}+4\cdot 2^{r-1} \leq 20\cdot 3^{r-1} < 3^{r+2}$. The coarsest squarefree basis $\mathcal{B}$ obtained will have at most m_rn_r elements, with degrees bounded by n_r and norm length bounded by n_r+d_r by Mignotte's theorem. Hence the time to apply ISOL will be dominated by $(m_rn_r)n_r^8 + (m_rn_r)^7n_r^7(n_r+d_r)^3$, which is dominated by $m_r^7n_r^{17}d^3$. By Theorem 10, $m_r^7n_r^{17}d^3 \leq (2n)^a m^b d^3$ where $b \leq 7\cdot 2^{r-1} < 2^{r+2}$ and $a \leq 7\cdot 3^r+17\cdot 2^{r-1}+3\cdot 2^r \leq 21\cdot 3^{r-1}+17\cdot 3^{r-1} +6\cdot 3^{r-1}=44\cdot 3^{r-1} < 3^{r+3}$. ∎

Next we turn our attention to the "sizes" of the real algebraic numbers which arise in DECOMP. Two different representations are used, and hence there are two different definitions of "size". Regarded as an element of the field P of all real algebraic numbers, a real algebraic number α is represented by a primitive squarefree integral polynomial $A(x)$ such that $A(\alpha)=0$ and an interval $I=(r,s)$ with rational endpoints r and s such that α is the unique root of A in I. We will assume moreover that r and s are binary rationals, that is, numbers of the form $a\cdot 2^{-k}$ where a and k are integers, $k \geq 0$, and a is odd if $k>0$. Let λ be the minimum distance between two real roots of A. By the root separation theorem, $\lambda^{-1} \leq 2(e^{1/2}n^{3/2}c)^n$ where $n=\deg(A)$ and $c=|A|_1$. Hence $\log_2 \lambda^{-1} < 1+n(1+\frac{3}{2}L(n)+d)$ and $2^{-k}<\lambda$ if $k>1+n(1+\frac{3}{2}L(n)+d)$, where $d=L(c)$. Hence we assume that $r=a\cdot 2^{-h}$ and $s=b\cdot 2^{-k}$ with h, $k \leq n(2+2L(n)+d)$. Since it follows from $A(\alpha)=0$ that $|\alpha|<c$, we may also assume that $L(a), L(b) \leq$

$2n(1+L(n)+d)$. Then the "size" of α will be characterized by $n=\deg(A)$ and $d=L(|A|_1)$.

Regarded as an element of the real algebraic number field $Q(\alpha)$, the real algebraic number β is represented by a polynomial $B(x)\varepsilon Q[x]$ with $\deg(B)<n=\deg(A)$. The rational polynomial $B(x)$ is itself represented in the form $B(x)=b^{-1}\cdot\bar{B}(x)$ where b is an integer, $\bar{B}(x)$ is an integral polynomial, and $\gcd(b,\bar{B})=1$. In this case the "size" of β is characterized by $L(b)$ and $L(|\bar{B}|_1)$.

Let P_k be the set of all points $\beta=(\beta_1,\ldots,\beta_k)$ belonging to the c.a.s. computed by DECOMP for the c.a.d. S_k. For each such point there is computed a real algebraic number α such that $Q(\beta_1,\ldots,\beta_k)=Q(\alpha)$, and a pair (A,I) which represents α. A is a squarefree univariate integral polynomial such that $A(\alpha)=0$ and I is an isolating interval for α as a root of A. Let $\mathcal{A}_k^*$ be the set of all such polynomials A. Let n_k be the maximum degree of the elements of $\mathcal{A}_k^*$ and let d_k^* be the maximum norm length of the elements of $\mathcal{A}_k^*$.

For each coordinate β_i of a point $\beta\varepsilon P_k$, DECOMP computes a rational polynomial $B_i=b_i^{-1}\bar{B}_i$ which represents β_i as an element of $Q(\alpha)$. Let $\mathcal{B}_k'$ be the set of all such rational polynomials B_i associated in this way with points β of P_k, and let d_k' be the maximum of $\max(L(b),L(|\bar{B}|_1))$ taken over all $B=b^{-1}B\varepsilon\,\mathcal{B}_k'$.

Our next goal is to obtain recurrence relations for n_k^*, d_k^* and d_k'. For $k=1$, each algebraic number β_1 is a root of some element of $\mathcal{A}_r$, $\alpha=\beta_1$, and the polynomial A is an element of the basis for $\mathcal{A}_r$ which is computed in step (1). By Mignotte's theorem,

$$n_1^*\leq n_r, \tag{8}$$

$$d_1^*\leq n_r+d_r. \tag{9}$$

If β_1 is irrational, then $B(x)=x$ represents $\beta_1=\alpha$ as an element of $Q(\alpha)$. If β_1 is rational then $B(x)=\beta_1$ represents $\beta_1=\alpha$ as an element of $Q(\alpha)$. Referring to step (2) of DECOMP, β_1 arises as an endpoint of an isolating interval produced in step (1) by the application of ISOL to a basis $\mathcal{B}$ for $\mathcal{A}_r$. Let $\bar{B}$ be the product of the elements of $\mathcal{B}$. Then $\deg(\bar{B})\leq m_r n_r$ and, since $\bar{B}$ is the product of at most $m_r n_r$ polynomials, each having a norm length of at most n_r+d_r, the norm length of $\bar{B}$ is at most

$m_r n_r (n_r+d_r)$. In accordance with our previous discussion of the root separation theorem, we may therefore assume that the numerator and denominator of β_1 have lengths not exceeding $2m_r n_r\{1+L(m_r n_r)+m_r n_r(n_r+d_r)\} \leq 4m_r^2 n_r^2 (n_r+d_r)$. Hence,

$$d_1' \leq 4m_r^2 n_r^2 (n_r+d_r) \tag{10}$$

For each point $\beta=(\beta_1,\ldots,\beta_k)$ in P_k, and each polynomial $C(x_1,\ldots,x_{k+1})$ in $\mathcal{A}_{r-k}$, step (6) of DECOMP substitutes β_i for x_i, obtaining a polynomial $C^*(x)=C(\beta_1,\ldots,\beta_k,x)$ belonging to $Q(\alpha)[x]$, $Q(\alpha)=Q(\beta_1,\ldots,\beta_k)$. This substitution may be performed in two stages. In the first stage we substitute $B_i(y)$ for x_i, where B_i represents β_i as an element of $Q(\alpha)$, resulting in $\hat{C}(y,x)=C(B_1(y),\ldots,B_k(y),x)$, an element of $Q[y,x]$. In the second stage, $\hat{C}(y,x)$ is reduced modulo $A(y)$, where A represents α, resulting in $C^*(y,x)\in Q[y,x]$. $C^*(y,x)$ may be identified with $C^*(x)$ since the coefficients of $C^*(y,x)$ are elements of $Q[y]$ which represent the coefficients of $C^*(x)$ as elements of $Q(\alpha)$.

Instead of computing $\hat{C}(y,x)$ directly, we compute instead the integral polynomial $\bar{C}(y,x)=\{\Pi_{i=1}^{k} b_i^{\nu_i}\}\hat{C}(y,x)$, where ν_i is the degree of C in x_i. To illustrate, suppose $k=1$ and let $C(x_1,x_2)=\Sigma_{i=0}^{\nu_1} C_i(x_2)x_1^i$. Then $\bar{C}(y,x)=\Sigma_{i=0}^{\nu_1} C_i(x)\bar{B}_1(y)^i b_1^{\nu_1-i}$. Since $|C|_1=\Sigma_{i=0}^{\nu_1}|C_i|_1$, we see that $|\bar{C}|_1 \leq |C|_1 \cdot f^{\nu_1}$ where $f=\max(|b_1|,|B_1|_1)$. In general, recalling the definition of d_k', we see that the length of the norm of $\bar{C}$ is at most $d_{r-k}+kn_{r-k}d_k'$. Also, $\hat{C}(y,x)=c^{-1}\bar{C}(y,x)$ with $L(c)\leq kn_{r-k}d_k'$. Furthermore, the degree of $\bar{C}(y,x)$ in y is at most $kn_{r-k}n_k^*$ since the degree of each B_i is less than n_k^*.

In reducing $\hat{C}(y,x)$ modulo $A(y)$, we compute the pseudo-remainder, $C'(y,x)$, of $\bar{C}(y,x)$ with respect to $A(y)$. $C'(y,x)\in Z[y,x]$ and we have $c'\bar{C}(y,x)=A(y)\cdot Q(y,x)+C'(y,x)$ for some $c'\in Z$ and some $Q(y,x)\in Z[y,x]$, with the degree of C' in y less than $\deg(A)$. Hence $\hat{C}(y,x)=A(y)\{(cc')^{-1}Q(y,x)\}+(cc')^{-1}C'(y,x)$, and $C^*(y,x)=(cc')^{-1}C'(y,x)$. Regarding the pseudo-remainder as a subresultant, we have $|C'|_1 \leq |\bar{C}|_1 \cdot |A|_1^n$ where n is the degree of $\bar{C}$ in y. Since $L(|\bar{C}|_1)\leq d_{r-k}+kn_{r-k}d_k'$, $L(|A|_1)\leq d_k^*$ and $n\leq kn_{r-k}n_k^*$, $L(|C'|_1)\leq d_{r-k}+kn_{r-k}d_k'+kn_{r-k}n_k^*d_k^*$. Also, $c'=\{\mathrm{ldcf}(A)\}^h$ with $h\leq n$, so $L(cc')\leq kn_{r-k}d_k'+kn_{r-k}n_k^*d_k^*$.

The polynomial $C^*(x)$ arises from a point $\beta\in P_k$ and a polynomial

$C \in \mathcal{A}_{r-k}$. Keeping β fixed while C ranges over all elements of $\mathcal{A}_{r-k}$, we obtain a set $\mathcal{C}^*$ of univariate polynomials over $Q(\alpha)$. Step (6) of DECOMP specifies the application of ABASIS to $\mathcal{C}^*$ to produce a coarsest squarefree basis $\mathcal{B}^*$. However, at present no theorem is known which provides a reasonable bound for the "sizes" of the coefficients of the elements of $\mathcal{B}^*$. As an alternative we may therefore apply the algorithm NORMAL to α and $C^*(x)$, for each C^* in $\mathcal{C}^*$, producing an integral polynomial D(x) such that every root of C^* is a root of D. Let $\mathcal{D}$ be the set of all polynomials D so obtained as C^* ranges over $\mathcal{C}^*$.

Given α, represented by the integral polynomial A(y) and the isolating interval I, and the rational polynomial $C^*(y,x)=c^{-1}C'(y,x)$ representing $C^*(x)$, NORMAL proceeds as follows. Let $C'(y,x)=\sum_{i=0}^{m} C'_i(y)x^i$, where $C_m(\alpha)\neq 0$. The integral polynomial C'(y,x) is divided by gcd($C_m(x)$, A(x)), producing an integral polynomial C''(y,x). Then D(x) is the resultant, with respect to y, of C''(y,x) and A(y).

deg(A) and the degree in y of C''(y,x) in y are both at most n_k^*. The degree of C'(y,x) in x is at most n_{r-k}, the degree of $C(x_1,\ldots,x_{k+1})$ in x_{k+1}. Hence the degree of D is at most $n_k^* n_{r-k}$. Since the norm length of C'(y,x) is at most $d_{r-k}+kn_{r-k}d'_k+kn_{r-k}n_k^*d_k^*$ and the norm length of A is at most d_k^*, the norm length of D is at most $n_k^*d_k^*+n_k^*d_{r-k}+kn_{r-k}n_k^*d'_k+kn_{r-k}n_k^{*2}d_k^*$.

Let $\bar{\mathcal{D}}$ be the coarsest squarefree basis of $\mathcal{D}$. Then every β_{k+1} with $(\beta_1,\ldots,\beta_k,\beta_{k+1})\in P_{k+1}$ will be represented by a polynomial $\bar{D}\in\bar{\mathcal{D}}$ and, by Mignotte's theorem, the norm length of $\bar{D}$ is at most $n_k^*n_{r-k}+n_k^*d_k^*+n_k^*d_{r-k}+kn_{r-k}n_k^*d'_k+kn_{r-k}n_k^{*2}d_k^*$.

Next algorithm SIMPLE is applied to α and β_{k+1}, producing α' such that $Q(\alpha,\beta_{k+1})=Q(\alpha')$. α and β_{k+1} are represented by the polynomials A and $\bar{D}$. α' is represented by a polynomial A'(x), which is the resultant of A(x-hy) and $\bar{D}(y)$ with respect to y, where h is some integer with $|h|<\deg(A)\cdot\deg(\bar{D})$. Since $|x-hy|_1=|h|+1$, we have $|A(x-hy)|_1\leq|A|_1\cdot(|h|+1)^{\deg(A)}$. Hence $L(|A(x-hy)|_1)\leq d_k^*+n_k^*(2L(n_k^*)+L(n_{r-k}))$. Since $\deg(\bar{D})\leq n_k^*n_{r-k}$ and the degree of A(x-hy) in y is $\deg(A)\leq n_k^*$, we have $L(|A|_1)\leq n_k^*n_{r-k}\{d_k^*+2n_k^*L(n_k^*)+n_k^*L(n_{r-k})\}+n_k^*\{n_k^*n_{r-k}+n_k^*d_k^*+n_k^*d_{r-k}+kn_{r-k}n_k^*d'_k+kn_{r-k}n_k^{*2}d_k\}$. Since the degree of A(x-hy) in x is $\deg(A)\leq n_k^*$, we have $\deg(A')\leq n_k^{*2}n_{r-k}$. Thus we have proved

$$n^*_{k+1} \leq n^{*2}_k n_{r-k}. \qquad (11)$$

Also, replacing $L(n^*_k)$ by n^*_k, $L(n_{r-k})$ by n_{r-k}, and making other simplifications in the inequality above for $L(|A'|_1)$, we have also

$$d^*_{k+1} \leq (d^*_k n_{r-k}) n^*_k + (2n^2_{r-k} + d_{r-k} + d^*_k + k n_{r-k} d'_k) n^{*2}_k + (k+2) n_{r-k} d^*_k n^{*3}_k. \qquad (12)$$

It remains to obtain a relation for d'_{k+1}. Algorithm SIMPLE, when applied to α and β_{k+1}, produces, besides α' such that $Q(\alpha, \beta_{k+1}) = Q(\alpha')$, rational polynomials E and F which represent α and β_{k+1} as elements of $Q(\alpha')$. The polynomial $A'(y)$ which represents α' is the resultant of $A(x-hy)$ and $\bar{D}(y)$. The monic greatest common divisor of $A(\alpha'-hx)$ and $\bar{D}(x)$ in $Q(\alpha')$ is the polynomial $x-\beta_{k+1}$. This implies that if $G(y,x) = G_1(y)x + G_0(y)$ is the first subresultant of $A(y-hx)$ and $\bar{D}(x)$ then $\beta_{k+1} = -G_0(\alpha')/G_1(\alpha')$. Let $H = \gcd(A', G_1)$ and $\bar{A}' = A'/H$. Since A' is squarefree, $\bar{A}'$ and G_1 are relatively prime integral polynomials. Applying the extended Euclidean algorithm, we obtain integral polynomials U and V such that $\bar{A}'U + G_1 V = c$, where $c \neq 0$ is the resultant of $\bar{A}'$ and G_1. Also, $G_1(\alpha') \neq 0$ so $H(\alpha') \neq 0$ and $\bar{A}'(\alpha') = 0$. Hence $G_1(\alpha')V(\alpha') = c$. Let $G_2 = -G_0 V$. Then $c^{-1}G_2(\alpha') = -G_0(\alpha')c^{-1}V(\alpha') = -G_0(\alpha')/G_1(\alpha') = \beta_{k+1}$. Hence if $bG_2(y) = Q(y)A'(y) + G_3(y)$ where G_3 is the pseudo-remainder of G_2 and A', then $(bc)^{-1}G_3$ represents β_{k+1}. Also, $\alpha' = \alpha + h\beta_{k+1}$ so if $G_4(y) = bcy - hG_3(y)$ then $(bc)^{-1}G_4(y)$ represents α in $Q(\alpha')$.

The same degree and norm length bounds, (11) and (12), which were derived for the resultant A' apply also to the subresultant coefficients G_0 and G_1. Since $\bar{A}'$ is a divisor of A', $\deg(\bar{A}') \leq n^*_{k+1}$ and, by Mignotte's theorem, $L(|\bar{A}'|_1) \leq n^*_{k+1} + d^*_{k+1}$. $\deg(V) \leq \deg(\bar{A}') \leq n^*_{k+1}$ and resultant bounds apply to c and $|V|_1$. Thus $L(c)$, $L(|V|_1) \leq n^*_{k+1}(2n^*_{k+1} + d^*_{k+1})$. Hence $\deg(G_2) \leq 2n^*_{k+1}$ and $L(|G_2|_1) \leq 2n^{*2}_{k+1} + n^*_{k+1} d^*_{k+1} + d^*_{k+1}$. Therefore, $L(|G_3|_1) \leq (2n^{*2}_{k+1} + n^*_{k+1} d^*_{k+1} + d^*_{k+1}) + 2n^*_{k+1} d^*_{k+1} = 2n^{*2}_{k+1} + 3n^*_{k+1} d^*_{k+1} + d^*_{k+1}$, $L(b) \leq 2n^*_{k+1} d^*_{k+1}$ and $L(bc) \leq 2n^*_{k+1} + 3n^*_{k+1} d^*_{k+1}$. Since $L(|h|+1) \leq L(n^*_{k+1}) \leq n^*_{k+1}$, $L(|G_4|_1) \leq 2n^{*2}_{k+1} + 3n^*_{k+1} d^*_{k+1} + n^*_{k+1} + d^*_{k+1} \leq 2n^{*2}_{k+1} + 4n^*_{k+1} d^*_{k+1}$.

Let $B_i = b_i^{-1}\bar{B}_i$ represent β_i as an element of $Q(\alpha)$, $i \leq k$. Let $G' = g^{-1}\bar{G}'$ where $g = bc$ and $\bar{G}' = G_4$. Then G' represents α as an element of $Q(\alpha')$. Hence $G'(\alpha') = \alpha$ and $B_i(\alpha) = \beta_i$ so $B_i(G'(\alpha')) = \beta_i$. Let $B^*_i(y) = q^{\nu_i}\bar{B}(G'(y))$ where $\nu_i = \deg(\bar{B}_i)$. B^*_i is an integral polynomial with $\deg(B^*_i) \leq \deg(\bar{B}_i) \cdot \deg(G') \leq n^*_k n^*_{k+1}$ and $L(|B^*_i|_1) \leq L(|\bar{B}_i|_1) + \deg(\bar{B}_i) \cdot (2n^{*2}_{k+1} + 4n^*_{k+1} d^*_{k+1}) \leq d'_k + n^*_k (2n^*_{k+1} + 4n^*_{k+1} d^*_{k+1})$. Also,

$L(b_i g^{\nu_i}) \le d_k' + n_k^*(2n_{k+1}^{*2} + 4n_{k+1}^* d_{k+1}^*)$. Let $\bar{B}_i'$ be the pseudo-remainder of B_i^* and A', $b_i^* B_i^* = A'Q + \bar{B}_i'$, and $b_i' = b_i^* b_i g^{\nu_i}$. Then $B_i' = b_i'^{-1}\bar{B}_i'$ represents β_i as an element of $Q(\alpha')$. $L(|\bar{B}_i'|_1) \le L(|B_i^*|_1) + n_k^* n_{k+1}^* d_{k+1}^* \le d_k' + 2n_k^* n_{k+1}^{*2} + 5n_k^* n_{k+1}^* d_{k+1}^*$, and $L(b_i')$ satisfies the same bound.

Combining the last two paragraphs, $d_k' + 2n_k^* n_{k+1}^{*2} + 5n_k^* n_{k+1}^* d_{k+1}^*$ is a norm length bound for the polynomials which represent $\beta_1, \ldots, \beta_{k+1}$ as elements of $Q(\alpha')$ whenever β_{k+1} is a root of one of the polynomials which is obtained by substituting $\beta_1, \ldots, \beta_k$ for $x_1, \ldots, x_k$ in a polynomial of $\mathcal{A}_{r-k}$. But we must also consider the case that β_{k+1} is a rational endpoint of some isolating interval. We have seen that, for fixed $\beta_1, \ldots, \beta_k$, the isolated roots are all roots of the polynomials in the basis $\bar{\mathcal{B}}$ of $\mathcal{B}$. Let $\hat{D}$ be the product of the elements of $\mathcal{B}$. $\mathcal{B}$ has at most m_{r-k} elements, each of degree $n_k^* n_{r-k}$ at most. Hence $\bar{\mathcal{B}}$ has at most $m_{r-k} n_k^* n_{r-k}$ elements, each of degree $n_k^* n_{r-k}$ at most. We observed previously that $n_k^* d_k^* + n_k^* d_{r-k} + k n_{r-k} n_k^* d_k' + k n_{r-k} n_k^{*2} d_k^*$ is a norm length bound for the elements of $\mathcal{B}$. Hence $\deg(\hat{D}) \le n_k^* m_{r-k} n_{r-k}$ and $L(|\hat{D}|_1) \le (n_k^* d_k^* + n_k^* d_{r-k} + k n_{r-k} n_k^* d_k' + k n_{r-k} n_k^{*2} d_k^*) m_{r-k}$. If D^* is the greatest squarefree divisor of $\hat{D}$ then by Mignotte's theorem $L(|D^*|_1) \le (n_k^* n_{r-k} + n_k^* d_k^* + k n_{r-k} n_k^* d_k' + k n_{r-k} n_k^{*2} d_k^*) m_{r-k} = L_k$, say. According to our earlier discussion, we may assume that the lengths of the numerators and denominators of the rational endpoints of isolating intervals for the roots of D^* do not exceed $2n_k^* m_{r-k} n_{r-k}(1 + L(2n_k^* m_{r-k} n_{r-k}) + L_k) \le 2n_k^* m_{r-k} n_{r-k} + 4n_k^{*2} m_{r-k}^2 n_{r-k}^2 + 2n_k^* m_{r-k} n_{r-k} L_k \le 2\{k n_{r-k} d_k' + n_{r-k} d_{r-k} + (k+4) n_k^* n_{r-k}^2 d_k^*\} n_k^{*2} m_{r-k}^2$. Adding to this the bound $d_k' + 2n_k^* n_{k+1}^{*2} + 5n_k^* n_{k+1}^* d_{k+1}^*$, we find that

$$d_{k+1}' \le d_k' + 2n_k^* n_{k+1}^{*2} + 5n_k^* n_{k+1}^* d_{k+1}^* + 2\{k n_{r-k} d_k' + n_{r-k} d_{r-k} + (k+4) n_k^* n_{r-k}^2 d_k^*\} n_k^{*2} m_{r-k}^2. \tag{13}$$

Now we use the recurrence relations (11), (12) and (13) to prove the following theorem.

Theorem 14. With n_k^*, d_k^* and d_k' as defined above, we have

$$n_k^* \le (2n)^{2^{r+k-1}}, \tag{14}$$

$$d_k^* \le (2n)^{2^{r+k+2}} (2n)^{3^{r+1}} m^{2^{r+1}} d, \tag{15}$$

$$d_k' \le (2n)^{2^{r+k+2}} (2n)^{3^{r+1}} m^{2^{r+1}} d. \tag{16}$$

Proof. To establish (14), we will show that $n^*_k \le (2n)^{s_k}$ where $s_k = \Sigma_{i=1}^{k} 2^{r+k-2i}$. For k=1, by (8) and (6), $n^*_1 \le n_r \le (2n)^{s_1}$ since $s_1 = 2^{r-1}$. Assuming $n^*_k \le (2n)^{s_k}$, by (11) and (6), $n^*_{k+1} \le (2n)^a$ where $a \le 2s_k + 2^{r-k-1}$. But $2s_k + 2^{r-k-1} = \Sigma_{i=1}^{k} 2^{r+k+1-2i} + 2^{r+k+1-2(k+1)} = s_{k+1}$, completing the induction. And $s_k \le 2^{r+k-2}(1+2^{-2}+2^{-4}+\ldots) < 2^{r+k-1}$, proving (14).

Using (14), we can now simplify the recurrence relation (12). We observe first that $k+2 \le 2^{2^k}$, from which it follows by (6) that $(k+2)n_{r-k} \le (2n)^{2^r}$. It is then not difficult to derive from (12), using (6), (7) and (14), the inequality

$$d^*_{k+1} \le (2n)^{2^{r+k+1}} (d + d^*_k + d'_k). \tag{17}$$

Similarly, we can simplify (13) using (5), (6), (7) and (14). We obtain

$$d'_{k+1} \le (2n)^{2^{r+2}} (2n)^{2 \cdot 3^{r-k}} m^{2^{r-k}} (d + d^*_k + d^*_{k+1} + d'_k). \tag{18}$$

Let $\bar{D}_k$ be the common right hand side of (15) and (16). Substituting from (17) for d^*_{k+1} into (18), we obtain

$$d_{k+1} \le 2\,(2n)^{2^{r+k+1} + 2^{r+2}} (2n)^{2 \cdot 3^{r-k}} m^{2^{r-k}} (d + d^*_k + d'_k). \tag{19}$$

Since, by (17), (19) also holds with d or d^*_{k+1} in place of d'_{k+1}, we have

$$D_{k+1} \le 6\left\{(2n)^{2^{r+k+1} + 2^{r+2}} (2n)^{2 \cdot 3^{r-k}} m^{2^{r-k}}\right\} D_k, \tag{20}$$

where $D_k = d + d^*_k + d'_k$. It suffices then to show that $D_k \le \bar{D}_k$ for $1 \le k \le r$. We will prove instead the stronger inequality

$$D_k \le (2n)^{2^{r+k+2}} (2n)^{u_k} m^{v_k} d, \tag{21}$$

where $u_k = 2\Sigma_{i=1}^{k} 3^{r-i+1}$ and $v_k = \Sigma_{i=1}^{k} 2^{r-i+1}$. For $k \ge 2$, $6 \le 2^3 \le (2n)^3$ and $2^{r+k+2} + 2^{r+k+1} + 2^{r+2} + 3 \le 2^{r+k+3}$. Since also $u_k + 2 \cdot 3^{r-k} = u_{k+1}$ and $v_k + 2^{r-k} = v_{k+1}$, (20) implies that (21) holds for k+1 if it holds for $k \ge 2$. It remains then to prove (21) for k=1 and k=2. By (9), (6) and (7),

$$d^*_1 \le (2n)^{3 \cdot 2^{r-1}} d. \tag{22}$$

By (10), (5), (6) and (7),

$$d'_1 \leq (2n)^{5\cdot 2^{r-1}} (2n)^{2\cdot 3^r} m^{2^r} d. \tag{23}$$

If r=1, then (22) and (23) imply (15) and (16). Otherwise, $r \geq 2$, $3 \leq (2n)^2$ and $5\cdot 2^{r-1}+2 \leq 2^{r+2}$, so (22) and (23) imply

$$D_1 \leq (2n)^{3\cdot 2^r} (2n)^{u_1} m^{v_1} d, \tag{24}$$

which proves (21) for k=1. Now (20) and (24) yield (21) for k=2 since $6 \leq (2n)^3$ and $2^{r+3}+2^{r+2}+3\cdot 2^r+3 \leq 2^{r+4}$. ∎

As an easy corollary of Theorem 14, we obtain the following theorem.

Theorem 15. For $1 \leq k \leq r$,

$$n^*_k \leq (2n)^{2^{2r-1}}, \tag{25}$$

$$d^*_k, d'_k \leq (2n)^{2^{2r+3}} m^{2^{r+1}} d. \tag{26}$$

Proof. This follows immediately from Theorem 14 by observing that $3^h \leq 2^{2h}$. ∎

We now have all of the information necessary to complete an analysis of the computing time of algorithm DECOMP. Theorem 12 bounds the number of cells in the decomposition as a function of m, n and r. Theorems 10 and 15 together bound the degrees and coefficient lengths of all polynomials which arise in the mainstream of the calculation. From these bounds and from known computing time bounds for the various subalgorithms, it is straightforward, but tedious, to complete the analysis. We have given above computing time bounds for some, but not all of these subalgorithms. Those which we have not given may be found by the interested reader in the various references listed at the end of this paper. The critical property of these subalgorithms is that their computing times are all dominated by fixed powers of natural parameters such as degree products and maximum coefficient lengths or, as in the case of the BASIS algorithm, the number of polynomials in a list. Theorems 11 and 13 have illustrated the analysis of the computing time of certain parts of DECOMP. Thus the completion of the analysis of DECOMP does not involve any novel techniques or subtleties. The seriously interested

or skeptical reader may complete the analysis for himself. We therefore now state without additional proof the result of such analysis.

Theorem 16. The computing time of DECOMP is dominated by $(2n)^{2^{2r+8}} m^{2^{r+6}} d^3$.

The exponents occurring in this theorem can likely be decreased in several ways. In the first place, the computing times used for the subalgorithms all presuppose that classical algorithms are used for integer multiplication and division. With the use of fast algorithms such as the Schönberg-Strassen algorithm, [25], for integer arithmetic, it is evident that the exponent of d can be reduced from 3 to $2+\epsilon$ for every $\epsilon > 0$. Secondly, it is probable that a tighter analysis without change of the subalgorithm would yield some improvement, for example perhaps the 2r+8 could be reduced to 2r+4. Thirdly, it is likely that improved mathematical knowledge would also improve the bound without change of the algorithms. For example, the analysis depends strongly on the root separation theorem, and it seems likely that this theorem is far from optimal. It should also be noted that the theorem bounds the maximum computing time, and the average computing time is likely much smaller.

By the remarks preceding the algorithm EVAL, if ϕ^* is a standard prenex formula with matrix ϕ, $\mathcal{A}$ is the set of polynomials occurring in ϕ, and β is a sample point, the truth value of each atomic formula in ϕ can be determined by at most one evaluation of sign(A(β)) for each $A \in \mathcal{A}$. Thus the application of EVAL to ϕ^*, a c.a.s. β, and a standard definition ψ involves mainly the evaluation of sign(A(β_i)) for each $A \in \mathcal{A}$ and each sample point $\beta_i \in \beta$. This is not essentially different from the calculations performed during the last phase of the application of DECOMP, and the bound of Theorem 16 again applies. However, one must not overlook the time required to compute the truth value of ϕ from the truth values of its atomic formulas, for each sample point β. The time required for this is obviously dominated, for each β, by the number, a, of occurrences of atomic formulas in ϕ. Thus the computing time bound of DECOMP, multiplied by a, is a bound for EVAL. Finally, consider step (1) of ELIM, which extracts from ϕ the set $\mathcal{A}$ of distinct polynomials occuring in ϕ. This involves, at most, ma polynomial comparisons, one comparison for each atomic formula with each element of the list of distinct polynomials already extracted. The time for each comparison is at most $(n+1)^r d \leq (2n)^r d \leq (2n)^{2^r} d$. We therefore obtain our final

result:

Theorem 17. The computing time of ELIM is dominated by $(2n)^{2^{2r+8}} m^{2^{r+6}} d^3 a$.

As a corollary of this analysis, we can obtain a computing time bound for ELIM as a function only of the length N of the formula ϕ. Obviously we must have m,r,d and a less than or equal to N and, assuming as is usual that x^k must be expressed as the product of k x's, we also have $n \leq N$. Since $r \geq 1$ and $N \geq 3$ for every formula, we have $2r+8 \leq 5N$ and $r+6 \leq 3N$. Hence by Theorem 17, the computing time is dominated by $(2N)^{2^{5N}} N^{2^{3N}} N^4$. But it is easy to prove by induction on h that $h^{2^k} \leq 2^{2^{h+k}}$. Hence $(2N)^{2^{5N}} N^{2^{3N}} N^4 \leq 2^{2^{7N}} 2^{2^{4N}} 2^{2^{2N}} \leq 2^{2^{8N}}$.

Theorem 18. For a fomula of length N, the computing time of ELIM is dominated by $2^{2^{8N}}$.

In Theorem 17, d is the maximum norm length of the polynomials in ϕ, whereas in the Introduction the result of Theorem 17 was stated with coefficient d defined as the maximum coefficient length. But if d' is the maximum coefficient length then, since a polynomial in r variables with degrees bounded by n has at most $(n+1)^r$ integer coefficients, $d \leq L(n+1)^r) + d' \leq rL(2n) + d' \leq 2rL(n) + d' \leq 2rn + d' \leq 2rnd'$, and $d^3 \leq (2n)^3 r^3 d'^3 \leq (2n)^{2^2} 2^{2^{2r}} d'^3 \leq (2n)^{2^{2r+1}} d'^3$. Thus as a corollary of Theorem 17, the computing time of ELIM is dominated by $(2n)^{2^{2r+9}} m^{2^{r+6}} d'^3 a$. But in fact the exponent 2r+9 can be replaced by 2r+8 by converting from d to d' while carrying out the proof of Theorem 17.

5. Observations. For the sake of conceptual simplicity, and to facilitate the analysis, we have kept our quantifier elimination algorithm as simple as possible. But for practical application many refinements

and improvements are possible, some of which will now be described.

It is unnecessary to form reducta when projecting a set of polynomials in two variables. The leading coefficient of a non-zero bivariate polynomial A is a non-zero univariate polynomial, which vanishes at only a finite number of points. If the leading coefficient of A is invariant on a connected set $S \subseteq R$ then either S is a one-point set, on which the roots of A are trivially delineable, or else $ldcf(A) \neq 0$ on S.

We recall ([19], Chapter 4) that the discriminant of a polynomial A, which we will denote by discr(A), satisfies $discr(A) = res(A, A')/ldcf(A)$. If A is a squarefree bivariate polynomial, then discr(A) is also a non-zero univariate polynomial, which vanishes at only a finite number of points. Thus it is easy to prove (confer Theorem 4) that if $A(x_1, x_2)$ is a squarefree polynomial, $\mathcal{L} = \{ldcf(A) : deg(A) \geq 1\}$, $\mathcal{D} = \{discr(A) : deg(A) \geq 2\}$, S is a connected subset of R, and every element of $\mathcal{L} \cup \mathcal{D}$ (there are at most two elements) is invariant on S, then the roots of A are delineable on S.

If now $\mathcal{A}$ is a set of bivariate polynomials and $\mathcal{B}$ is a squarefree basis for $\mathcal{A}$ then any two distinct elements of $\mathcal{B}$ have a non-zero resultant, which again vanishes at only a finite number of points. Thus we see that in this case we can define $proj(\mathcal{A}) = \mathcal{P} = \mathcal{L} \cup \mathcal{D} \cup \mathcal{R}$ where $\mathcal{L} = \{ldcf(B) : B \in \mathcal{B} \ \& deg(B) \geq 1\}$, $\mathcal{D} = \{discr(B) : B \in \mathcal{B} \ \& deg(B) \geq 2\}$ and $\mathcal{R} = \{res(B_1, B_2) : B_1, B_2 \in \mathcal{B} \ \& B_1 < B_2 \& deg(B_1) \geq 1 \& deg(B_2) \geq 1\}$, and Theorem 5 will still hold.

For the augmented projection of a set of bivariate polynomials, we must be cautious; although A is squarefree, some derivative of A may fail to be squarefree. But if A is any polynomial, $\mathcal{B}$ is a squarefree basis for $\{A\}$, and the roots of $\mathcal{B}$ are delineable on a connected set S, then the roots of A are delineable on S. So, with $proj(\mathcal{A})$ defined as in the preceeding paragraph, we can define the augmented projection of $\mathcal{A}$ as follows. Let $\mathcal{D} = \{der^j(A) : A \in \mathcal{A} \ \& 1 \leq j \leq deg(A) - 2\} = \{D_1, \ldots, D_k\}$. Let $\mathcal{B}_i$ be a squarefree basis for $\{D_i\}$ and $\mathcal{P}_i = proj(\mathcal{B}_i)$. Then $proj(\mathcal{A}) = \cup\{\cup_{i=1}^{k} \mathcal{P}_i\}$ will suffice for the augmented projection of $\mathcal{A}$. Actually, this still gives us a little more than necessary; the leading coefficients of the elements of the $\mathcal{B}_i$ are superfluous. One might suppose that these basis calculations would be time-consuming, but in most cases one will quickly discover that D_i is squarefree so that $\mathcal{B}_i = \{D_i\}$ and for $\mathcal{P}_i$ we can then use just $\{discr(D_i)\}$.

Now let $\mathcal{A}$ be a set of polynomials in three variables. According to our earlier definition, we begin the projection by forming the set $\mathcal{B}$ of all reducta of elements of $\mathcal{A}$ such that the degree of the reductum is positive. In general, this set $\mathcal{B}$ is much larger than necessary. The objective is just to ensure that for each $A\in\mathcal{A}$, $\mathcal{B}$ contains some reductum of A whose leading coefficient is invariantly non-zero on each cell S of the induced c.a.d. Indeed even this is unnecessary for one-point cells S, because then the roots of A are trivially delineable on S. So if the first i coefficients of A are simultaneously zero at only a finite number of points of R^2, then $red^k(A)$ can be excluded from $\mathcal{B}$ for $k\geq i$. Also, if the leading coefficient of A has no zeros in R^2, as when its degree in both x_1 and x_2 is zero, then $red^k(A)$ can be excluded from $\mathcal{B}$ for $k\geq 1$.

For the case i=2, let $A_1=ldcf(A)$, $A_2=ldcf(red(A))$. If $A_1(\alpha_1,\alpha_2)=A_2(\alpha_1,\alpha_2)=0$ then $R_1(\alpha_1)=0$ where $R_1(x_1)$ is the resultant of $A_1(x_1,x_2)$ and $A_2(x_1,x_2)$ with respect to x_2. Hence if $R_1\neq 0$ there are only a finite number of α_1's. Similarly, if R_2 is the resultant with respect to x_1 and if $R_2\neq 0$ then there are only finitely many α_2's. If $R_1\neq 0$ and $R_2\neq 0$ then there are only finitely many points (α_1,α_2).

Of course if either A_1 or A_2 has degree zero in either x_1 or x_2, then the resultants R_1 and R_2 can not both be formed, but then there are alternatives. If A_1 is of degree zero in x_2 and A_2 is of degree zero in x_1 (or vice versa) then there are only finitely many solutions. Suppose A_1 is of degree zero in x_2 and A_2 is of positive degree in both x_1 and x_2, say $A_2(x_1,x_2)=\Sigma_{i=o}^{n}A_{2,i}(x_1)\cdot x_2^i$. Then there are only finitely many solutions if $gcd(A_1,A_{2,n},\ldots,A_{2,1})$ is of degree zero. Also, there are only finitely many solutions if A_1 and A_2 are both degree zero in x_2(or x_1) and the degree of $gcd(A_1,A_2)$ in x_1(respectively x_2) is zero.

If the cases i=1 and i=2 fail, then we may try i=3. Let $A_3=ldcf(red^2(A))$. Then it suffices to show, as above, that A_1 and A_3, or A_2 and A_3, have only finitely many common solutions. Better still, we may compute $res(gcd(A_1,A_2),A_3)$.

There are obvious reasons to expect that in most cases it will be unnecessary to include in $\mathcal{B}$ $red^k(A)$ for $k\geq 2$ when $\mathcal{A}$ is a set of polynomials in three variables. The reader can easily see for himself how to extend these methods to polynomials in $r\geq 4$ variables. For example, when r=4 we can compute $res(A_1,A_2)$, $res(A_2,A_3))$ with respect to x_1,x_2 and x_3. It will usually be unnecessary to include in $\mathcal{B}$ $red^k(A)$ for $k\geq r-1$.

By a similar argument, for a given $B \in \mathcal{B}$, it is in general unnecessary to include in the set $\mathcal{B}_1$ $\mathrm{psc}_k(B,B')$ for all k such that $0 \leq k < \deg(B')$. If we can show that the equations $\mathrm{psc}_i(B,B')=0$, for $0 \leq i \leq k$, have only a finite number of solutions then $\mathrm{psc}_i(B,B')$ may be omitted from $\mathcal{B}_1$ for $i>k$.

Thus, if A is a polynomial in r variables, it will usually suffice to include in $\mathcal{B}_1$ $\mathrm{psc}_j(\mathrm{red}^i(A), \mathrm{der}(\mathrm{red}^i(A)))$ only for $0 \leq i \leq r-2$ and $0 \leq j \leq r-2$, a total of $(r-1)^2$ polynomials. One can even do better than this. For example, if the equations $\mathrm{ldcf}(A)=0$ and $\mathrm{psc}_0(\mathrm{red}(A), \mathrm{der}(\mathrm{red}(A)))=0$ have only finitely many common solutions, then we need not include $\mathrm{psc}_1(\mathrm{red}(A),\mathrm{der}(\mathrm{red}(A)))$. Thus we will usually need to include $\mathrm{psc}_j(\mathrm{red}^i(A),\mathrm{der}(\mathrm{red}^i(A)))$ only for $0 \leq i+j \leq r-2$, a total of $\binom{r}{2}$ polynomials. Similar considerations apply to the set $\mathcal{B}_2$ of the projection and to the set $\mathcal{B}'$ of the augmented projection. Whereas we derived an upper bound of m^2n^3 for the number of polynomials in the augmented projection, the expected number will now be about m^2r^2 when n is larger than r.

It is important to realize that the resultants used in testing for finitely many solutions need not be computed; it is only necessary to decide whether or not they are zero. If, in fact, a resultant is non-zero then this can usually be ascertained very quickly by computing the resultant modulo a large single-precision prime and modulo linear polynomials $x_i - a_i$.

As an experiment, we have computed the two successive projections of a set $\mathcal{A}=\{A_1(x_1,x_2,x_3), A_2(x_1,x_2,x_3)\}$ where A_1 and A_2 are polynomials of total degree two with random integers from the interval $[-9,+9]$ as coefficients. Each A_i is then a polynomial with 10 terms, of degree 2 in x_3, with constant leading coefficient. $\mathcal{A}_1$, the projection of $\mathcal{A}$, is then a set consisting of four elements, $B_1=\mathrm{discr}(A_1)$, $B_2=\mathrm{discr}(A_2)$, $B_3=\mathrm{res}(A_1,A_2)$ and $B_4=\mathrm{psc}_1(A_1,A_2)$. The leading coefficient of each B_i has degree zero in x_1 so the content of B_i is an integer. Dividing B_1 by its content, we obtained the primitive part $\bar{B}_i$. We then found that each $\bar{B}_i$ was an irreducible polynomial in $Z[x_1,x_2]$ so $\mathcal{B}_1=\{\bar{B}_1,\bar{B}_2,\bar{B}_3,\bar{B}_4\}$ was a finest basis for $\mathcal{A}_1$. $\bar{B}_1$ and $\bar{B}_2$ are of degree 2 in each variable and have total degree 2. Their integer coefficients are two of three decimal digits in length. $\bar{B}_3$ is of degree 4, in each x_i separately and in total, with 4-digit coefficients. $\bar{B}_4$ has degree 1 and 2-digit coefficients.

$\mathcal{A}_2$, the projection of $\mathcal{B}_1$, has as its elements $D_i=\text{discr}(\bar{B}_i)$ for $i=1,2,3$ and $R_{i,j}=\text{res}(\bar{B}_i,\bar{B}_j)$ for $1\leq i<j\leq 4$. Again we set $\bar{\bar{D}}_i=\text{pp}(D_i)$ (the primitive part of D_i) and $\bar{R}_{i,j}=\text{pp}(R_{i,j})$. The contents of the D_i and $R_{i,j}$ are from 1 to 5 decimal digits in length. The largest of these primitive parts is $\bar{D}_3$, with degree 12 and coefficients about 22 to 24 decimal digits in length. Now we factor each $\bar{D}_i$ and each $\bar{R}_{i,j}$ to obtain a finest basis, $\mathcal{B}_2$, for $\mathcal{A}_2$. The results are as follows:

$$\begin{aligned}
&\bar{D}_1,\bar{D}_2,\bar{R}_{1,2},\bar{R}_{1,4},\bar{R}_{2,4} \text{ irreducible,}\\
&\bar{D}_3=P_1P_2^2,\\
&\bar{R}_{3,4}=P_2^2,\\
&\bar{R}_{1,3}=P_4^2,\\
&\bar{R}_{2,3}=P_5^2.
\end{aligned} \tag{27}$$

Here each P_i is irreducible. Note that P_2 is a common factor of $\bar{D}_3$ and $\bar{R}_{3,4}$.

Since random polynomials are almost always irreducible, the factorizations (27) strongly suggest some theorems. To help preclude chance events, the entire experiment was repeated using polynomials A_1 and A_2 with different random coefficients, With the new A_1 and A_2, the structure of the factorization (27) was exactly repeated; even the degrees of the irreducible factors remained the same.

Let us consider briefly what kinds of theorems are suggested by (27). Ignoring primitive parts, $\bar{D}_3=\text{discr}(\text{res}(A_1,A_2))$, $R_{1,3}=\text{res}(\text{discr}(A_1),\text{res}(A_1,A_2))$, $\bar{R}_{2,3}=\text{res}(\text{discr}(A_2),\text{res}(A_1,A_2))$ and $\bar{R}_{3,4}=\text{res}(\text{psc}_0(A_1,A_2),\text{psc}_1(A_1,A_2))$. Note that in each case the general form is a resultant ot two psc's with "common ancestors". On the other hand, there are no "common ancestors" in the irreducible cases $\bar{D}_i=\text{discr}(\text{discr}(A_i))$ and $\bar{R}_{1,2}=\text{res}(\text{discr}(A_1),\text{discr}(A_2))$. The cases $\bar{R}_{i,4}=\text{res}(\text{discr}(A_i),\text{psc}_1(A_1,A_2))$ appear anomalous.

A number of other experiments have been performed which tend to substantiate the rather vague conclusions suggested by the above results. For example, we find that, "in general", $\text{res}(\text{res}(A_1,A_2),\text{res}(A_2,A_3))$ is reducible. These observations suggest very strongly the merit of performing basis calculations preceding each projection. How-

ever, it is not entirely clear whether a finest or coarsest squarefree basis should be used. Note that in the above example the two coincide.

We have seen now how to reduce substantially the number of polynomials which arise when the projections are performed, and we have seen empirical evidence, though not yet theorems, which indicates that the growth of degrees can be controlled somewhat by basis calculations. Also, the factorizations which reduce degrees tend to reduce coefficient lengths correspondingly. Hence there is some reason for optimism regarding the potential applicability of this method. A full implementation of the method within the SAC-1 computer algebra system [6], is still in progress. Nearly all of the necessary algebraic subalgorithms are already available, and some parts of the elimination algorithm itself exist in preliminary form. The completion of the implementation and its application to several non-trivial "real" problems within the next year or two is anticipated.

Ferrante and Rackoff, [26] , have recently published a quantifier elimination method for the first order theory of the additive ordered group of the real numbers, which they show to have a computing time dominated by $2^{2^{cN}}$ for some unknown constant c. We obtain an alternative to their method as the special case of the method above in which every polynomial occurring in the formula ϕ has total degree 1. Setting n=1 in Theorem 18, we obtain their result with c=8. Their computing time bound is obtained as a function of N, the length of ϕ, only. Setting n=1 in Theorem 17, we obtain the more informative bound $2^{2^{2r+8}} m^{2^{r+6}} d^3 a$.

We can easily improve this result. It is easy to see that in the special case we are considering, we may define $\mathrm{proj}(\mathcal{A})=\{\mathrm{res}(A_i,A_j): 1\leq i<j\leq m\}$ where $\mathcal{A}=\{A_1,\ldots, A_m\}$. Thus $\mathrm{proj}(\mathcal{A})$ has at most $\binom{m}{2}\leq m^2/2$ members, and the augmented projection is never needed. With m_k and d_k defined as before, we then easily obtain

$$m_k \leq 2(m/2)^{2^{k-1}}, \tag{28}$$

$$d_k \leq 2^{k-1} d. \tag{29}$$

Instead of isolating roots, since they are rational, we now compute them exactly. If $r_1<r_2<\ldots<r_l$ are all the roots of a set of polynomials, then for the sample points s_i between roots we use the averages

$(r_i+r_{i+1})/2$. If $r_1<0$ then we also use the sample point $s_o=2r_1<r_1$; if $r\geq 0$ then we use instead the sample point $s_o=-1$. Similarly we use $s_1=2r_1$ or +1 as a greatest sample point. The rational number r=a/b is represented by the linear integral polynomial bx-a with norm $|a|+|b|$; we may call this the norm, $|r|_1$ of r. Note that $|s_i|_1\leq 2|r_i|_1\cdot|r_{i+1}|_1$, $|s_o|_1 \leq 2|r_1|_1$ and $|s_{l+1}|_1\leq 2|r_l|_1$.

The result of substituting r=a/b for x_1 in a polynomial $C(x_1,\ldots,x_k)$ $=c_1x_1+\ldots+c_kx_k+c_o$ and then multiplying by b to obtain an integral polynomial is the same as the resultant of bx_1-a and $C(x_1,\ldots,x_k)$ with respect to x_1.

If c_k is the number of cells as before, then we have $c_1\leq 2m_r+1$ and $c_{k+1}\leq 2c_k m_{r-k}+1$, from which it follows that

$$c_k\leq 2^{k+1}(m/2)^{2^r}. \tag{30}$$

Let d'_k be the maximum norm length of the kth coordinate of any sample point. Then $d'_1\leq 2d_r+1$ amd $d'_{k+1}\leq 2(d_{r-k}+d'_1+d'_2+\ldots+d'_k)+1$. It follows that

$$d'_k\leq 2^{r+k}d. \tag{31}$$

Using the bounds (28) to (31), it is not difficult to show that the computing time of the method is dominated by $m^{2^r}d^2a$ using classical arithmetic algorithms, $m^{2^r}d^{1+\epsilon}$ a using fast arithmetic algorithms.

Acknowledgements. I am indebted to numerous persons in various ways in connection with this paper. First to Frank Beckman, who first made it possible for me to pursue my interest in Tarski's method at IBM Corp. in 1955. Secondly, the late Abraham Robinson encouraged my interests in this subject at various times in the 1960's, as did also C. Elgot and D.A. Quarles, Jr. I am perhaps most indebted to R. Loos who, during several weeks at Stanford University in early 1973, through his keen appreciation and insightful discussions, persuaded me to persist to the final

discovery of this method. Most recently I have become greatly indebted to H. Brakhage, who made it possible for me to spend a year at the University of Kaiserslautern in unencumbered pursuit of the further development of this method.

References

1. Brown, W.S., On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors, J. ACM, vol. 18, no.4 (Oct. 1971) pp.478-504.

2. Brown, W.S., and Traub, J.F., On Euclid's Algorithm and the Theory of Subresultants, J. ACM, vol. 18, no.4 (Oct. 1971), pp. 505-514.

3. Cohen, P.J., Decision Procedures for Real and p-adic Fields, Comm. Pure and Applied Math., vol. XXII, no. 2 (March 1969), pp. 131-151.

4. Collins, G.E., Subresultants and Reduced Polynomial Remainder Sequences, J. ACM, vol. 14, no. 1, (Jan. 1967), pp. 128-142.

5. Collins, G.E., The Calculation of Multivariate Polynomial Resultants, J. ACM, vol. 18, no. 4 (Oct. 1971), pp. 515-532.

6. Collins, G.E., Computer Algebra of Polynomials and Rational Functions, Am. Math. Monthly, vol. 80, no. 7 (Aug.-Sept. 1973), pp. 725-755.

7. Collins, G.E., Efficient Quantifier Elimination for Elementary Algebra (abstract), Symposium on Complexity of Sequential and Parallel Numerical Algorithms, Carnegie-Mellon University, May 1973.

8. Collins, G.E., Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition - Preliminary Report, Proceedings of EUROSAM 74, SIGSAM Bulletin, Vol.8, No.3 (August 1974), pp. 80 - 90.

9. Fischer, M.J., and Rabin, M.O., Super-Exponential Complexity of Presburger Arithmetic, M.I.T. MAC Tech. Memo. 43, Feb. 1974.

10. Goldhaber, J.K., and Ehrlich, G., Algebra, MacMillan Co., 1970.

11. Heindel, L.E., Integer Arithmetic Algorithms for Polynomial Real Zero Determination, J. ACM, vo. 18, no. 4 (Oct. 1971), pp. 533-548.

12. Loos, R.,G.K., A Constructive Approach to Algebraic Numbers, SIAM Journal on Computing, to appear.

13. Marden, M., The Geometry of the Zeros of a Polynomial in a Complex Variable, Am. Math. Soc., Providence, 1949.

14. Musser, D.R., Algorithms for Polynomial Factorization (Ph.D. Thesis), Univ. of Wisconsin Computer Sciences Dept. Tech. Report No. 134, Sept. 1971.

15. Musser, D.R., Multivariate Polynomial Factorization, J.ACM., Vol. 22, No. 2 (April 1975), pp. 291-308.

16. Rubald, C.M., Algorithms for Polynomials over a Real Algebraic Number Field (Ph.D. Thesis), Computer Sciences Dept. Tech. Report No. 206, Jan. 1974.

17. Seidenberg, A., A New Decision Method for Elementary Algebra, Annals of Math., vol. 60, no. 2 (Sept. 1954), pp. 365-374.

18. Tarski, A., A Decision Method for Elementary Algebra and Geometry, second ed., rev., Univ. of California Press, Berkeley, 1951.

19. van der Waerden, B.L., Modern Algebra, vol. I, F. Ungar Co., New York, 1953.

20. Böge, W., private communication, June 1973

21. Holthusen, C., Vereinfachungen für Tarski's Entscheidungsverfahren der Elementaren Reelen Algebra (Diplomarbeit, University of Heidelberg), January 1974.

22. Collins, G.E., and E. Horowitz, The Minimum Root Separation of a

Polynomial, Math. of Comp., Vol. 28, No. 126, (April 1974), pp. 589-597.

23. Mignotte, M., An Inequality About Factors of Polynomials, Math. of Comp., Vol. 28, No. 128 (October 1974), pp. 1153-1157.

24. Knuth, D.E., The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, Addison-Wesley, Reading, 1969.

25. Schönhage, A., and V. Strassen, Schnelle Multiplikation großer Zahlen, Computing, Vol. 7, pp. 281-292.

26. Ferrante, J., and C. Rackoff, A Decision Procedure for the First Order Theory of Real Addition with Order, SIAM Journal on Computing, Vol. 4, No. 1 (March 1975), pp. 69-76.