INFORMATION AND COMPUTATION 97, 262–276 (1992)

Polynomial Time Algorithms for Sentences over Number Fields*

SHIH PING TUNG

Department of Mathematics, Chung Yuan Christian University, Chung Li, Taiwan 32023, Republic of China

We call φ a $\forall\exists$ sentence if and only if φ is logically equivalent to a sentence of the form $\forall x\,\exists y\,\psi(x, y)$, where $\psi(x, y)$ is a quantifier free formula constructed with logical and arithmetical symbols. Now let φ be a $\forall\exists$ sentence in conjunctive or disjunctive normal form. We show that given an arbitrary algebraic number field K there is a polynomial time algorithm to decide whether φ is true in K or not. We also show that ther are polynomial time algorithms to decide whether or not φ is true in every algebraic number field or every radical extension field of Q. © 1992 Academic Press, Inc.

INTRODUCTION

An arithmetical sentence is a sentence constructed from the language of rings and usual logical symbols. Godel's incompleteness theorem shows that there is no algorithm to decide whether an arithmetical sentence is true in the set of natural numbers N or not. It follows that there is no algorithm to decide whether an arithmetical sentence is true in the ring of integers Z or not. The same is true for the rational number field Q (J. Robinson, 1949), the algebraic number field (J. Robinson, 1959), the purely transcendental extension of Q (R. M. Robinson, 1964), and fields (J. Robinson, 1949). With the same arguments as in J. Robinson (1949), there is no algorithm to decide whether or not an arithmetical sentence is true in every field with characteristic 0. Having all these negative results, we may ask for what subsets of arithmetical sentences there are algorithms to decide the truth. Also, what are the computational complexities of these algorithms?

We call φ a $\forall\exists$ or $\exists\forall$ sentence if and only if φ is logically equivalent to a sentence of the form $\forall x\,\exists y\,\psi(x, y)$ or $\exists x\,\forall y\,\psi(x, y)$, respectively, where $\psi(x, y)$ is a formula containing no quantifiers and no other free variables except x and y. There are algorithms to decide the truth of $\forall\exists$ or $\exists\forall$ sentences in N, Z, and Q (Tung, 1986). The decision problems of $\exists\forall$ sentences of the form $\exists x\,\forall y\ f(x, y)\neq 0$, $f(x, y)\in Z[x, y]$, true in N or Z are

* This research was supported by the National Science Council of ROC.

0890-5401/92 $3.00

NP-complete (Tung, 1987), whereas the similar problem over Q can be decided in polynomial time (Tung, 1987). With logical methods, it has been shown that there are algorithms to decide the truth of $\forall\exists$ sentences over algebraic number fields and related decision problems (Tung, 1990). With this approach we also obtain other interesting results and we use some of these results in this paper. However, we do not know the computational complexities of these problems. In this paper we show that there are polynomial time algorithms to decide these problems if sentences are in conjunctive or disjunctive normal form. Every formula can be transformed to one in conjunctive or disjunctive normal form. In general, this transformation will cause the size of formulas to grow exponentially.

The main tools we used in this paper are polynomial time algorithms for factorization of polynomials (Lenstra, 1987 or Landau, 1985) and Theorem A (Tung, 1990) below. Theorem A is deduced from Schinzel's theorem (1982) on Diophantine equations with parameters.

THEOREM A. *Let K be an algebraic number field and $\varphi(x, y)$ a formula in disjunctive normal form, i.e.,*

$$\varphi(x, y) = \bigvee_{i=1}^{s} \left[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right],$$

where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over K. If for every arithmetic progression P in Z there exist integers x' of P and y' of K such that $\varphi(x', y')$ is true in K then there exist an i and polynomials $F(x)$, $G(x) \not\equiv 0$ over K such that $G(x)\,y - F(x)$ is an irreducible common factor of the polynomials $f_{i,j}(x, y)$ $(1 \leqslant j \leqslant m_i)$ but not the factor of any one of the polynomials $g_{i,k}(x, y)$ $(1 \leqslant k \leqslant n_i)$ over the ring $K[x, y]$.

In another paper to appear elsewhere (Tung, 1991), we discuss similar problems over algebraic integer rings. For example, we show that the decision problem of $\exists\forall$ sentences in conjunctive or disjunctive normal form in an algebraic integer ring is NP-complete. We also prove that there is a polynomial time algorithm to decide whether or not a $\forall\exists$ sentence is true in every algebraic integer ring.

1. PRELIMINARIES

The language L used in this paper contains all the usual logical symbols, arithmetical symbols $+$, $\cdot$, and variables and constants of Q. If the decision problem is posed over a specified field then L is augmented with all the constants of the field. A formula ψ is in conjunctive normal form if it has the form $\psi = \psi_1 \wedge \psi_2 \wedge \cdots \wedge \psi_n$, where $\psi_i = \varphi_{i,1} \vee \varphi_{i,2} \vee \cdots \vee \varphi_{i,m_i}$ and

each $\varphi_{i,j}$ is an equation $f=0$ or inequality $g\neq 0$. A disjunctive normal form formula is defined analogously except the symbols $\vee$ and $\wedge$ are interchanged. When the computational complexity of the sentences is measured, the polynomials are input in non-sparse form. That is, for the polynomial $f(x, y)$, if $f(x, y)$ contains the monomial $ax^m y^n$ with $a\neq 0$ and the monomial $bx^i y^j$ with $i\leqslant m$, $j\leqslant n$, then b must be input even if $b=0$.

An element α is algebraic over K if α satisfies an equation with coefficients in the field K. Otherwise the element α is transcendental over K. An extension field F is algebraic over K if every element of F is algebraic over K. It is well known that every finite extension of a field is algebraic; the finite extensions of Q are called the algebraic number fields. Every algebraic number field is expressible as $Q(\alpha)$ for a suitable α. The field $Q(\alpha)$ is isomorphic to $Q[t]/F(t)$, where $F(t)$ is the minimal (irreducible) polynomial for α. In our algorithms we work with the algebraic number field in its formulation as $Q[t]/F(t)$, although certain of our proofs will be in terms of $Q[\alpha]$.

Let $\varphi(x, y)$ be a formula in disjunctive normal form, i.e., $\varphi(x, y)=\bigvee_{i=1}^{s}[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y)=0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y)\neq 0]$, where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over an algebraic number field K. We may also interchange the symbols $\bigvee$ and $\bigwedge$, $\vee$ and $\wedge$, and make $\varphi(x, y)$ a conjunctive normal form. In this paper we show that there is a polynomial time algorithm to decide whether $\forall x\,\exists y\ \varphi(x, y)$ is true in K or not. In order to analyze the time complexity more precisely, we give all the parameters used in the analysis. Here we follow Lenstra's notations (Lenstra, 1987) closely, because we use his algorithm several times. Let $K=Q(\alpha)$ and $F(t)=\sum_{i=0}^{I} a_i t^i\in Z[t]$, $a_I=1$, be the minimal polynomial of α over Q, and define $|F|=(\sum_{i=0}^{I}(a_i)^2)^{1/2}$. For any polynomial

$$f(x, y)=\sum_{i_1=0}^{t_1}\sum_{i_2=0}^{t_2}\sum_{j} a_{i_1,i_2,j}\alpha^j x^{i_1} y^{i_2}\in Q(\alpha)[x, y],$$

$|f|$ is defined as $(\sum_{i_1}\sum_{i_2}\sum_{j}(a_{i_1,i_2,j})^2)^{1/2}$, $N_f=(t_1+1)(t_2+1)$, and $\delta_f=t_1+t_2$. Also let d_f be the positive integer such that $f\in(1/d_f)Z[\alpha][x, y]$. Let $\varphi(x, y)$ be a normal form formula as above. We then define $|\varphi|=\max_{i,j,k}(|f_{i,j}|, |g_{i,k}|)$, $N=\max_{i,j,k}(N_{f_{i,j}}, N_{g_{i,k}})$, $d=\mathrm{LCM}_{i,j,k}(d_{f_{i,j}}, d_{g_{i,k}})$, and $M=\sum_{i=1}^{s}(\sum_{j=1}^{m_i}\delta_{f_{i,j}}+\sum_{k=1}^{n_i}\delta_{g_{i,k}})$. We prove that we can decide whether $\forall x\,\exists y\ \varphi(x, y)$ is true in K or not in $O(M^2(IN)^5(IN+\log(d|\varphi|)+I\log(I|F|)))$ arithmetic operations on integers having binary length $O(M(IN)^2(IN+\log(d|\varphi|)+I\log(I|F|)))$.

2. Sentences over a Field

In this section we study the sentences over an algebraic number field K. A sentence φ is called a $\forall$ or $\exists$ sentence if and only if φ is logically

equivalent to a sentence of the form $\forall x\ \psi(x)$ or $\exists x\ \psi(x)$, respectively, where $\psi(x)$ is a formula containing no quantifiers and no other variables except x. We first show that there is a polynomial time algorithm to decide whether a $\exists$ sentence in disjunctive or conjunctive normal form is true in K or not. We need this to prove our main results.

We emphasize that sentences in this section may contain the constants of K. This is, we extend the language L to contain all constants of K.

LEMMA 1. *Let K be an algebraic number field and $\exists x\ \varphi(x)$ a $\exists$ sentence in conjunctive or disjunctive normal form; then there is a polynomial time algorithm to decide whether $\exists x\ \varphi(x)$ is true in K or not. This algorithm needs $O(M(IN)^5\ (IN+\log(d\,|\varphi|)+I\log(I\,|F|)))$ arithmetic operations on integers having binary length $O((IN)^2\ (IN+\log(d\,|\varphi|)+I\log(I\,|F|)))$.*

Proof. We first prove the case of $\exists x\ \varphi(x)$ in conjunctive normal form, i.e.,

$$\varphi(x)=\bigwedge_{i=1}^{s}\left[\bigvee_{j=1}^{m_i} f_{i,j}(x)=0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x)\neq 0\right],$$

where $f_{i,j}(x)$ and $g_{i,k}(x)$ are polynomials over K. If for every i there is a k such that $g_{i,k}(x)\not\equiv 0$ then $\exists x\ \varphi(x)$ is true. Now suppose that there is an i such that $g_{i,k}(x)\equiv 0$ for every $k\leqslant n_i$. Without loss of generality, we may write that

$$\varphi(x)=\bigwedge_{i=1}^{p}\left[\bigvee_{j=1}^{m_i} f_{i,j}(x)=0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x)\neq 0\right]\wedge\left[\bigvee_{l=1}^{t} f_l(x)=0\right].$$

We apply Lenstra's algorithm (Lenstra, 1982) to solve the equation $f_l(x)=0$, i.e., to find linear factors $x-\beta$ of $f_l(x)$ with $\beta\in K$, for every $l\leqslant t$ in K. Let A be the set of all these solutions. If there is a β of A such that

$$\bigwedge_{i=1}^{p}\left[\bigvee_{j=1}^{m_i} f_{i,j}(\beta)=0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(\beta)\neq 0\right]$$

is true then $\exists x\ \varphi(x)$ is true in K. Otherwise, $\exists x\ \varphi(x)$ is false in K. Since the evaluations of polynomials can be done fast (cf. Knuth, 1981), the time complexity is dominated by $\sum_{i=1}^{s} m_i\leqslant M$ times factorizations of polynomials. With Lenstra's algorithm (Lenstra, 1982), we need $O(M(IN)^5\ (IN+\log(d\,|\varphi|)+I\log(I\,|F|)))$ arithmetic operations on integers having binary length $O((IN)^2\ (IN+\log(d\,|\varphi|)+I\log(I\,|F|)))$.

Now let $\varphi(x)$ be a formula in disjunctive normal form, i.e.,

$$\varphi(x)=\bigvee_{i=1}^{s}\left[\bigwedge_{j=1}^{m_i} f_{i,j}(x)=0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x)\neq 0\right],$$

where $f_{i,j}(x)$ and $g_{i,k}(x)$ are polynomials over K. We apply Lenstra's algorithm to solve the equation $f_{i,j}(x)$ for every i and j. (If $m_i > 1$ for some i, it will be more efficient to find the greatest common divisor, GCD, of the polynomials $f_{i,j}(x)$ for $1 \leqslant j \leqslant m_i$, then find the roots of GCD.) Now let A_i be the set of common roots of $f_{i,j}(x) = 0$ for $1 \leqslant j \leqslant m_i$. Then for every β of A_i we check whether $\bigwedge_{k=1}^{n_i} g_{i,k}(\beta) \neq 0$ or not. If there are an i and a β of A_i such that $\bigwedge_{k=1}^{n_i} g_{i,k}(\beta) \neq 0$ then $\exists x\ \varphi(x)$ is true. Otherwise, $\exists x\ \varphi(x)$ is false in K. It should be easy to see that the computational complexity for this case is exactly the same as for the previous case. ▮

What we do in general is as follows. Given an arithmetical $\forall\exists$ sentence $\forall x\, \exists y\ \varphi(x, y)$, we eliminate the initial quantifier by constructing the set S, so that

$$\forall x\, \exists y\ \varphi(x, y) \Leftrightarrow \bigwedge_{a \in S} \exists y\ \varphi(a, y),$$

and then each existential sentence $\exists y\ \varphi(a, y)$ can be solved by the method of Lemma 1. To obtain the set S we need to apply the Theorem A mentioned before. The statement of this theorem is similar to, but more general than, what we have in Tung (1990). The proofs are analogous. For the sake of completeness, we give the proof here.

THEOREM A. *Let K be an algebraic number field and $\varphi(x, y)$ a formula in disjunctive normal form, i.e.,*

$$\varphi(x, y) = \bigvee_{i=1}^{s} \left[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right],$$

where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over K. If for every arithmetic progression P in Z there exist integers x' of P and y' of K such that $\varphi(x', y')$ is true in K then there exist an i and polynomials $F(x)$, $G(x) \not\equiv 0$ over K such that $G(x)\, y - F(x)$ is an irreducible common factor of the polynomials $f_{i,j}(x, y)$ $(1 \leqslant j \leqslant m_i)$ but not the factor of any one of the polynomials $g_{i,k}(x, y)$ $(1 \leqslant k \leqslant n_i)$ over the ring $K[x, y]$.

Proof. If for some i, j, and k the polynomials $f_{i,j}(x, y)$ exist and have common factors then we can omit the common factors from the polynomial $f_{i,j}(x, y)$. This will not affect the truth of the formula $\varphi(x, y)$. Hence, without loss of generality, we may assume that for every i, j, and k the polynomials $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are relatively prime. For every x' and y' of K, if $\varphi(x', y')$ is true then $\bigvee_{i=1}^{s} f_{i,1}(x', y') = 0$ or $\prod_{i=1}^{s} f_{i,1}(x', y') = 0$ is true. Hence for every arithmetic progression P in Z there exist integers x' of P and y' of K such that $\prod_{i=1}^{s} f_{i,1}(x', y') = 0$. By Schinzel's theorem (Schinzel, 1982, Theorem 34) there exists a rational function $r(x)$ over K

such that $\prod_{i=1}^{s} f_{i,1}(x, r(x)) \equiv 0$. Let $r(x) = F_1(x)/G_1(x)$, where $F_1(x)$ and $G_1(x) \not\equiv 0$ are relatively prime polynomials over K. Since $K[x]$ is a unique factorization domain, by the Gauss Lemma (Lang, 1971) $G_1(x)\,y - F_1(x)$ is an irreducible factor of $\prod_{i=1}^{s} f_{i,1}(x, y)$. Then $G_1(x)\,y - F_1(x)$ must be an irreducible factor of the polynomial $f_{l,1}(x, y)$ for an l, $1 \leqslant l \leqslant s$. Since $f_{l,1}(x, y)$ and $g_{l,k}(x, y)$ are relatively prime $G_1(x)\,y - F_1(x)$ is not a factor of any one of the polynomials $g_{l,k}(x, y)$ for $1 \leqslant k \leqslant n_l$. Now suppose that $G_1(x)\,y - F_1(x)$ is not a factor of one of the polynomials $f_{l,j}(x, y)$ for $1 \leqslant j \leqslant m_l$. Let A be the set of the x's of the common roots of the equations $G_1(x)\,y - F_1(x) = 0$ and $f_{l,j}(x, y) = 0$, A a finite set. If a set T intersects every arithmetic progression in Z, then T intersects every arithmetic progression with infinitely many terms. Let R be the set of x' of K such that there exists an integer y' of K, $\varphi(x', y')$ is true. By our assumption, R intersects every arithmetic progression in Z. Therefore $R - A$ still intersects every arithmetic progression in Z. For every x' of $R - A$ there exists an integer y' of K such that $h(x', y') = 0$, where $h(x, y) = \prod_i f_{i,1}(x, y)/(G_1(x)\,y - F_1(x))$. By Schinzel's theorem again, there must exists an irreducible factor $G_2(x)\,y - F_2(x)$ of the polynomial $\prod_i f_{i,1}(x, y)/(G_1(x)\,y - F_1(x))$. The polynomials $F_2(x)$, $G_2(x)$ might not satisfy the condition of conclusion; then with the same arguments there must exist another irreducible factor $G_3(x)\,y - F_3(x)$ of the polynomial $\prod_i f_{i,1}(x, y)/((G_1(x)\,y - F_1(x)) \cdot (G_2(x)\,y - F_2(x))$. Since the degree of y of the polynomial $\prod_i f_{i,1}(x, y)$ is finite, there must exist polynomials $F(x)$, $G(x)$ satisfying our conclusion. ▮

Now we are able to prove our first main theorem.

THEOREM 1. *Let K be an algebraic number field and φ be a $\forall\exists$ or $\exists\forall$ sentence in conjunctive or disjunctive normal form; then there is a polynomial time algorithm to decide whether φ is true in K or not. This algorithm need $O(M^2(IN)^5\,(IN + \log(d\,|\varphi|) + I\log(I\,|F|)))$ arithmetic operations on integers having binary length $O(M(IN)^2\,(IN + \log(d\,|\varphi|) + I\log(I\,|F|)))$.*

Proof. The negation of a $\forall\exists$ sentence is a $\exists\forall$ sentence. Also, the negation of a conjunctive normal form formula is a disjunctive normal form formula and vice versa. It suffices to prove the cases of $\forall\exists$ sentences. We first prove the case where $\forall x\,\exists y\,\varphi(x, y)$ is in disjunctive normal form. Let

$$\varphi(x, y) = \bigvee_{i=1}^{s} \left[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right],$$

where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over K.

(S_1) We apply Lenstra's polynomial time algorithm (Lenstra, 1987) to factor each $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ over K. We need to factorize polynomials $\sum_{i=1}^{s}(m_i+n_i)$ times. Because $\sum_{i=1}^{s}(m_i+n_i)\leqslant M$, this step can be done in $O(M^2(IN)^5(IN+\log(d|\varphi|)+I\log(I|F|)))$ arithmetic operations on integers having binary length $O(M(IN)^2(IN+\log(d|\varphi|)+I\log(I|F|)))$. By Theorem A if $\forall x\,\exists y\,\varphi(x, y)$ is true then there exist an i and polynomials $F(x)$, $G(x)\not\equiv 0$ over K such that $G(x)y-F(x)$ is an irreducible common factor of the polynomials $f_{i,j}(x, y)$ $(1\leqslant j\leqslant m_i)$ but not the factor of any one of the polynomials $g_{i,k}(x, y)$ $(1\leqslant k\leqslant n_i)$ over the ring $K[x, y]$. Now we suppose that this is the case, otherwise $\forall x\,\exists y\,\varphi(x, y)$ is false in K.

(S_2) Let $G_{i,k}(x)=g_{i,k}(x, F(x)/G(x))\cdot[G(x)]^M$; then $G_{i,k}(x)$ is a polynomial over K. We solve the equations $G(x)=0$ and $G_{i,k}(x)=0$, $1\leqslant k\leqslant n_i$, in K. Let A be the set of roots of these equations. Note that if x' is not in A then we can take $y'=F(x')/G(x')$ and $\varphi(x', y')$ is true in K. Now we check the sentence $\exists y\,\varphi(x', y)$ in K for every x' of A. Since the number of the elements of A is bounded by $O(M)$, this step can be done in $O(M^2(IN)^5(IN+\log(d|\varphi|)+I\log(I|F|)))$ arithmetic operations on integers having binary length $O((IN)^2(IN+\log(d|\varphi|)+I\log(I|F|)))$ by Lemma 1. Clearly, if there is an x' of A such that $\exists y\,\varphi(x', y)$ is false in K then $\forall x\,\exists y\,\varphi(x, y)$ is false in K. If $\exists y\,\varphi(x', y)$ is true in K for every x' of A then $\forall x\,\exists y\,\varphi(x, y)$ is true in K.

Now we need to prove the case $\forall x\,\exists y\,\varphi(x, y)$ in conjunctive normal form. Let

$$\varphi(x, y)=\bigwedge_{i=1}^{s}\left[\bigvee_{j=1}^{m_i} f_{i,j}(x, y)=0\vee\bigvee_{k=1}^{n_i} g_{i,k}(x, y)\neq 0\right],$$

where $f_{i,j}(x, y)$, $g_{i,k}(x, y)$ are polynomials over K.

(T_1) We apply the Euclidean Algorithm (cf. Knuth, 1981) to find the greatest common divisor (GCD) of $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ for every i, j, and k. We then omit the GCD from $g_{i,k}(x, y)$. Thus without loss of generality, we may assume that for every i the polynomials $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$, $1\leqslant j\leqslant m_i$ and $1\leqslant k\leqslant n_i$, are relatively prime.

(T_2) Suppose that for each i there is a k such that $g_{l,k}(x, y)\equiv 0$. Then for every i we are trying to find the number x' of K such that $g_{i,k}(x', y)\equiv 0$ for all $k\leqslant n_i$. This means that for an equation $g(x, y)=h_m(x)y^m+\cdots+h_0(x)=0$ we need to find the common solutions of $\{h_m(x)=0, \ldots, h_0(x)=0\}$. Therefore we apply the Euclidean Algorithm to find the GCD, $h(x)$, of the polynomials $h_m(x), \ldots, h_0(x)$, then solve the equation $h(x)=0$ in K. Let $A_{i,k}$ be the subset of K such that $g_{i,k}(x', y)\equiv 0$

if $x' \in A_{i,k}$ and $A = \bigcup_{i=1}^{s} \bigcap_{k=1}^{n_i} A_{i,k}$. Note that if for some x' of K the sentence

$$\exists y \bigwedge_{i=1}^{s} \left[\bigvee_{j=1}^{m_i} f_{i,j}(x', y) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x', y) \neq 0 \right]$$

is false then x' must be an element of A. Now we check the truth of the sentence $\exists y\ \varphi(x', y)$ for every x' of A. The number of the elements of A is bounded by $O(M)$; this step can be done in polynomial time by Lemma 1. If there is an x' of A such that $\exists y\ \varphi(x', y)$ is false then $\forall x\, \exists y\ \varphi(x, y)$ is false. Otherwise, $\forall x\, \exists y\ \varphi(x, y)$ is true. We can see that (T_2) is dominated by the last step with its complexity the same as (S_2).

Now we assume that for some i, $g_{i,k}(x, y) \equiv 0$ for every $k \leqslant n_i$. Since for any a, b of K, $a = 0 \vee b = 0$ if and only if $a \cdot b = 0$, we can combine several equations into one and obtain that

$$\varphi(x, y) = \bigwedge_{i=1}^{t} \left[\bigvee_{j=1}^{m_i} f_{i,j}(x, y) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right] \wedge \bigwedge_{l=1}^{p} F_l(x, y) = 0,$$

where $f_{i,j}$, $g_{i,k}$, F_l are polynomials over K and $g_{i,k}(x, y) \not\equiv 0$. (In most cases, combining equations will increase the computation time in the following steps. However, by our doing so our formulas and proof are much simplified.)

(T_3) We apply the Euclidean Algorithm to find the GCD, $G(x, y)$, of the polynomials $F_l(x, y)$, $1 \leqslant l \leqslant p$, then factor $G(x, y)$ over K by Lenstra's algorithm (Lenstra, 1987). We may write that

$$G(x, y) = G_0(x, y) \prod_{\beta=1}^{q} (G_\beta(x)\, y - F_\beta(x)),$$

where $G_0(x, y)$ has no factor of the form $G(x)\, y - F(x)$. If $q = 0$, i.e., $G(x, y)$ has no factor of the form $G(x)\, y - F(x)$, then $\forall x\, \exists y$ $\bigwedge_{l=1}^{p} F_l(x, y) = 0$ is false by Theorem A. Hence $\forall x\, \exists y\ \varphi(x, y)$ is false. The complexity of this step is the complexity of factoring $G(x, y)$. Now we assume that $q \neq 0$.

(T_4) Let $H_{i,k,\beta}(x) = g_{i,k}(x, F_\beta(x)/G_\beta(x)) \cdot [G_\beta(x)]^M$, $T_{i,k}$ be the set of polynomials $G_\beta(x)\, y - F_\beta(x)$ such that $H_{i,k,\beta}(x) \equiv 0$, and $T = \bigcup_{i=1}^{t} \bigcap_{k=1}^{n_i} T_{i,k}$. Let $G'(x, y) = G_0(x, y) \cdot \prod_{\delta=1}^{r} (G_\delta(x)\, y - F_\delta(x))$, where $G'(x, y)$ is the polynomial in which any factors $G(x)\, y - F(x)$ in T are omitted from $G(x, y)$. We claim that if $r = 0$, i.e., $G'(x, y)$ has no factor

of the form $G(x)\,y - F(x)$, then $\forall x\,\exists y\ \varphi(x, y)$ is false. Suppose, on the contrary, that

$$\forall x\,\exists y \bigwedge_{i=1}^{t} \left[\bigvee_{j=1}^{m_i} f_{i,j}(x, y) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right] \wedge \bigwedge_{l=1}^{p} F_l(x, y) = 0$$

is true. Now let A be a subset of K such that if a is in A then $G_\beta(a) \neq 0$ for a polynomial $G_\beta(x)\,y - F_\beta(x)$ of T and

$$\bigwedge_{i=1}^{t} \left[\bigvee_{j=1}^{m_i} f_{i,j}(a, F_\beta(a)/G_\beta(a)) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(a, F_\beta(a)/G_\beta(a)) \neq 0 \right].$$

This implies that there is an i such that $\bigvee_{j=1}^{m_i} f_{i,j}(a, F_\beta(a)/G_\beta(a)) = 0$. Since for each i, $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are relatively prime, $f_{i,j}(x, F_\beta(x)/G_\beta(x)) \not\equiv 0$. Hence A is finite. For every x' of $K - A$,

$$\exists y \bigwedge_{j=1}^{t} \left[\bigvee_{j=1}^{m_i} f_{i,j}(x', y) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x', y) \neq 0 \right] \wedge \bigwedge_{l=1}^{p} F_l'(x', y) = 0$$

is true in K, where $F_l'(x, y)$ is the polynomial from in which any factors $G(x)\,y - F(x)$ in T are omitted from $F_l(x, y)$. Then for every x of $K - A$, $\exists y \bigwedge_{l=1}^{p} F_l'(x', y) = 0$ is true. By Theorem A, $G'(x, y)$ has factors of the form $G(x)\,y - F(x)$. This proves our claim. Now we assume that $r \neq 0$. We solve $G_1(x) = 0$, $H_{i,k,l}(x) = 0$ for every i, k. Let B be the set of solutions of the equation $G_1(x) = 0$ and $B_{i,k}$ the set of solutions of the equation $H_{i,k,l}(x) = 0$. Let $D = (\bigcup_{i=1}^{t} \bigcap_{k=1}^{n_i} B_{i,k}) \cup B$; the number of the elements of D is bounded by $O(M)$. Note that if $\exists y\ \varphi(x', y)$ is false for an x' of K then x' must be an element of D. We check the truth of the sentence $\exists y \varphi(x', y)$ for every x' of D. If there is an x' of D such that $\exists y\ \varphi(x', y)$ is false then, of course, $\forall x\,\exists y\ \varphi(x, y)$ is false. Otherwise, $\forall x\,\exists y\ \varphi(x, y)$ is true. We can see that (T_4) is dominated by this step with complexity the same as for (S_2). Thus the computational complexity of the whole algorithm is dominated by (S_1). This completes our proof. ∎

A field F is called a purely transcendental extension of a field K if $F = K(S)$, where S is algebraically independent over K. For example, $K(x)$, the rational function field over K, is a purely transcendental extension of the field K.

COROLLARY 1. *Let F be a purely transcendental extension of the algebraic number field K and φ a $\forall\exists$ or $\exists\forall$ sentence over K in conjunctive or disjunctive normal form; then there is a polynomial time algorithm to decide whether φ is true in F or not. This algorithm needs $O(M^2(IN)^5\,(IN + \log(d\,|\varphi|) + I\log(I\,|F|)))$ arithmetic operations on integers having binary length $O(M(IN)^2\,(IN + \log(d\,|\varphi|) + I\log(I\,|F|)))$.*

Proof. A $\forall\exists$ or $\exists\forall$ sentence φ is true in K if and only if φ is true in F (Tung, 1990). Our result follows from Theorem 1. ▮

Note that in Corollary 1, we do not have to know what the field F really is. We need only know that F is a purely transcendental extension of K. Hence we only input the sentence φ and the polynomial $F(t)$ such that $K = Q[t]/F(t)$.

3. Sentence over a Class of Fields

In this section we apply Theorem 1 to show that the decision problems of $\forall\exists$ sentences in conjunctive or disjunctive normal form true in many different classes of fields are in polynomial time. These classes include algebraic number fields, radical extension fields of Q, abelian extension fields of Q, and cyclic extension fields of Q. It is well known that with the order of this list every class properly contains the next one and there are equations solvable in fields of the former classes but not solvable in all fields of the latter classes. Hence there are sentences of the form $\forall x\, f(x) \neq 0$ true in every field of the latter classes but not of the former classes. Therefore the sets of $\forall\exists$ sentences true in different classes are different. However, we show that there are similar algorithms to decide these different sets of $\forall\exists$ sentences and all in polynomial time if sentences are in conjunctive or disjunctive normal forms.

The basic idea of Theorem 2 below is as follows. Given an arithmetical $\forall\exists$ sentence $\forall x\, \exists y\, \varphi(x, y)$, we find a finite set T of algebraic number fields such that $\forall x\, \exists y\, \varphi(x, y)$ is true in every algebraic number field if and only if $\forall x\, \exists y\, \varphi(x, y)$ is true in every field in T. We then apply Theorem 1 to check whether or not $\forall x\, \exists y\, \varphi(x, y)$ is true in every field in T. Since the arguments have much in common with Theorem 1, we will omit some reasonings.

Theorem 2. *There is a polynomial time algorithm to decide whether or not an $\forall\exists$ sentence $\forall x\, \exists y\, \varphi(x)$ in conjunctive or disjunctive normal form is true in every algebraic number field. This algorithm needs $O(M^4(MN)^5(N+M+\log|\varphi|))$ arithmetic operations on integers having binary length $O(M^4N^2(N+M+\log|\varphi|))$.*

Proof. We prove the case of disjunctive normal form first. Let $\forall x\, \exists y\, \varphi(x, y)$ be a $\forall\exists$ sentence and

$$\varphi(x, y) = \bigvee_{i=1}^{s} \left[\bigwedge_{j=1}^{m_i} f_{i,j}(x, y) = 0 \wedge \bigwedge_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right],$$

where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over Q.

(S_1) We factor each $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ in $Q[x, y]$. With Lenstra's algorithm (Lenstra, 1987) this can be done in $O(M^2N^5(N+\log|\varphi|))$ arithmetic operations on integers having binary length $O(MN^2(N+\log|\varphi|))$. If $\forall x\,\exists y\ \varphi(x, y)$ is true in every algebraic number field then it is true in Q. (Q is an algebraic number field too.) By Theorem A, there exist an i and polynomials $F(x)$, $G(x) \not\equiv 0$ over Q such that $G(x)y - F(x)$ is an irreducible common factor of the polynomials $f_{i,j}(x, y)$ $(1 \leqslant j \leqslant m_i)$ but not the factor of any one of the polynomials $g_{i,k}(x, y)$ $(1 \leqslant k \leqslant n_i)$ over the ring $Q[x, y]$. Now we assume that this is the case.

(S_2) We factor $G(x)$ and $g_{i,k}(x, F(x)/G(x)) \cdot [G(x)]^M$ over Q for every $k \leqslant n_i$. This can be done in polynomial time (Lenstra *et al.*, 1982). Let S be the set of all irreducible factors of these polynomials. Note that if $\exists y\ \varphi(x', y)$ is false for an x' in an algebraic number field K then there must exist an $h(x)$ in S such that $h(x') = 0$.

(S_3) We check the sentence $\forall x\,\exists y\ \varphi(x, y)$ in Q and $Q[x]/h(x)$ for every $h(x)$ of S. Without loss of generality, we may assume that $h(x)$ is monic. If $h(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_n \neq 1$, let $H(x) = x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + a_n^2 a_{n-3}x^{n-3} + \cdots + a_n^{n-1}a_0$, then $Q[x]/h(x) \simeq Q[x]/H(x)$ (Pollard and Diamond, 1975). Note that the degrees of $h(x)$ and $H(x)$ are the same, and $\log|H| = O(n + \log|h|)$. Thus the estimate of complexity will not be affected. The number of the elements of S is $O(M)$; so is the degree of $h(x)$. Mignotte's Theorem (Mignotte, 1974) implies that $\log|h| \leqslant O(M + \log|\varphi|)$. With Theorem 1 this step needs arithmetic operations on integers having binary length $O(M^4N^2(N + M + \log|\varphi|))$. Clearly, if $\forall x\,\exists y\ \varphi(x, y)$ is false in Q or a certain field $Q[x]/h(x)$ then $\forall x\,\exists y\ \varphi(x, y)$ is not true in every algebraic number field. Now we claim that if $\forall x\,\exists y\ \varphi(x, y)$ is true in Q and $Q[x]/h(x)$ for every $h(x)$ of S then $\forall x\,\exists y\ \varphi(x, y)$ is true in every algebraic number field. Suppose that $\forall x\,\exists y\ \varphi(x, y)$ is false in an algebraic number field K. Let x' be the element of K such that $\exists y\ \varphi(x', y)$ is false in K. Then there is an $h(x)$ of S such that $h(x') = 0$. Since $\forall x\,\exists y\ \varphi(x, y)$ is true in $Q[x]/h(x) \simeq Q(x')$, $\exists y\ \varphi(x', y)$ is true in $Q(x')$. The field K contains $Q(x')$, hence the sentence $\exists y\ \varphi(x', y)$ is also true in K. This is a contradiction. This proves our claim and the case of disjunctive normal form.

Now let $\varphi(x, y)$ be in conjunctive normal form, i.e.,

$$\varphi(x, y) = \bigwedge_{i=1}^{s} \left[\bigvee_{j=1}^{m_i} f_{i,j}(x, y) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right],$$

where $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ are polynomials over Q.

(T_1) We omit from $g_{i,k}(x, y)$ the GCD of $f_{i,j}(x, y)$ and $g_{i,k}(x, y)$ over Q for every i, j, and k as we did in the step (T_1) of Theorem 1.

(T_2) First, we assume that for every i there is a k such that $g_{i,k}(x, y) \not\equiv 0$. Given the polynomial $g_{i,k}(x, y) = h_m(x)\, y^m + \cdots + h_0(x)$, let $G_{i,k}(x)$ be the GCD of the polynomials $\{h_m(x), ..., h_0(x)\}$ and $G_i(x)$ the GCD of $G_{i,k}(x)$ for $k \leqslant n_i$. Now we factor $G_i(x)$ over Q (Lenstra *et al.*, 1982) and let S be the set of all irreducible factors of the polynomials $G_i(x)$ for $1 \leqslant i \leqslant s$.

(T_3) We check the sentence $\forall x\, \exists y\ \varphi(x, y)$ in the field Q and $Q[x]/h(x)$ for every $h(x)$ of S as we did in the step (S_3) of this proof. With similar arguments, $\forall x\, \exists y\ \varphi(x, y)$ is true in the field Q and $Q[x]/h(x)$ for every $h(x)$ of S if and only if $\forall x\, \exists y\ \varphi(x, y)$ is true in every algebraic number field. Thus we settle the case that for every i there is a k, $g_{i,k}(x, y) \not\equiv 0$. Now we may assume that for some i, $g_{i,k}(x, y) \equiv 0$ for every $k \leqslant n_i$. We may combine several equations into one and write that

$$\varphi(x, y) = \bigwedge_{i=1}^{t} \left[\bigvee_{j=1}^{m_i} f_{i,j}(x, y) = 0 \vee \bigvee_{k=1}^{n_i} g_{i,k}(x, y) \neq 0 \right]$$

$$\wedge \bigwedge_{l=1}^{p} F_l(x, y) = 0$$

(T_4) We apply the Euclidean Algorithm to find the GCD, $G(x, y)$, of polynomials $F_l(x, y)$ for $1 \leqslant l \leqslant p$, then factor $G(x, y)$ over Q. We may write that

$$G(x, y) = G_0(x.\ q) \prod_{\beta=1}^{q} (G_\beta(x)\, y - F_\beta(x)),$$

where $G_0(x, y)$ has no factors of the form $G(x)\, y - F(x)$. If $q = 0$, then $\forall x\, \exists y \bigwedge_{l=1}^{p} F_l(x, y) = 0$ is false in Q by Theorem A. Hence $\forall x\, \exists y\ \varphi(x, y)$ is false in Q. Now we assume that $q \neq 0$.

(T_5) Let $H_{i,k,\beta} = g_{i,k}(x, F_\beta(x)/G_\beta(x))$ and $T_{i,k}$ be the set of polynomials $G_\beta(x)\, y - F_\beta(x)$ such that $H_{i,k,\beta}(x) \equiv 0$ and $T = \bigcup_{i=1}^{t} \bigcap_{k=1}^{n_i} T_{i,k}$. Let $G'(x, y) = G_0(x, y) \prod_{\delta=1}^{r} (G_\delta(x)\, y - F_\delta(x))$, where $G'(x, y)$ is the polynomial in which any factors $G(x)\, y - F(x)$ of T are omitted from $G(x, y)$. With the same arguments as in the step (T_4) of Theorem 1, we obtain that $r \neq 0$ or $\forall x\, \exists y\ \varphi(x, y)$ is false in Q.

(T_6) Let $G(x)\, y - F(x)$ be an irreducible factor of $G'(x, y)$. We factor $G(x)$ and $g_{i,k}(x, F(x)/G(x)) \cdot [G(x)]^M$ over Q for $1 \leqslant i \leqslant s$, $1 \leqslant k \leqslant n_i$. Let R be the set of all irreducible factors of these polynomials. We then check the sentence $\forall x\, \exists y\ \varphi(x, y)$ in Q and $Q[x]/h(x)$ for every $h(x)$ of R. With the same arguments as for the step (S_3) of this proof $\forall x\, \exists y\ \varphi(x, y)$ is true in every algebraic number field if and only if $\forall x\, \exists y\ \varphi(x, y)$ is true in Q and

$Q[x]/h(x)$ for every $h(x)$ of R. This completes our algorithm. Our total running time is dominated by (S_3), (T_3), or (T_6), all of which have the same complexity. ▮

COROLLARY 2. *There is a polynomial time algorithm to decide whether or not an* $\forall\exists$ *sentence* $\forall x\, \exists y\, \varphi(x, y)$ *in conjunctive or disjunctive normal form is true in every field with characteristic* 0. *This algorithm needs* $O(M^4(MN)^5(N+M+\log|\varphi|))$ *arithmetic operations on integers having length* $O(M^4N^2(N+M+\log|\varphi|))$.

Proof. A $\forall\exists$ sentence is true in every field with characteristic 0 if and only if it is true in every algebraic number field (Tung, 1990). Our result follows from Theorem 2. ▮

Remark. There are some classes of fields with characteristic 0; e.g., the class of all algebraic extension fields of Q, which contain all algebraic number fields. Thus with the same algorithm as Theorem 2, we can decide whether or not an $\forall\exists$ sentence true in every algebraic extension field of Q.

With similar arguments to those for Theorem 2 we can prove that the decision problems of $\forall\exists$ sentences true in some other classes of fields are also in polynomial time. We give some well-known definitions on extension fields first. An extension field F of Q is cyclic or abelian if and only if F is algebraic and Galois over Q and the Galois group of F over Q is cyclic or abelian, respectively. An extension field F of the field Q is a radical extension of Q if and only if $F=Q(\mu_1, ..., \mu_n)$, some power of μ_1 lies in Q, and for each $i\geqslant 2$, some power of μ_i lies in $Q(\mu_1, ..., \mu_{i-1})$.

Let $f(x)$ be an irreducible polynomial over Q. Then the equation $f(x)=0$ is not solvable by radicals if and only if $\forall x\, f(x)\neq 0$ (a very simple $\forall$ sentence) is true in every radical extension field of Q. Landau and Miller (1985) proved that solvability by radicals can be decided in polynomial time. This is equivalent to proving that the decision problem of sentences of the form $\forall x\ f(x)\neq 0$ being true in every radical extension field of Q is in polynomial time. Applying this result we extend the result to $\forall\exists$ sentences.

THEOREM 3. *There is a polynomial time algorithm to decide whether or not a* $\forall\exists$ *sentence in conjunctive or disjunctive normal form is true in every radical extension field of* Q.

Proof. Since the arguments are analogous to those in Theorem 2, we only sketch the proof of an $\forall\exists$ sentence in disjunctive normal form. All the steps are similar with what we did in Theorem 2. The only difference is in (S_2). Now let S' be the subset of S such that all the polynomials of S' are also solvable by radicals. Solvability by radicals is in polynomial time

(Landau and Miller, 1985). We can obtain the set S' in polynomial time. Now we claim that $\forall x\, \exists y\, \varphi(x, y)$ is true in every radical extension field of Q if and only if $\forall x\, \exists y\, \varphi(x, y)$ is true in Q and $Q[x]/h(x)$ for every $h(x)$ of S'. Since $Q[x]/h(x)$ is a subfield of the splitting field of $h(x)$, which is a radical extension field of Q, $Q[x]/h(x)$ is a radical extension field of Q (Lang, 1971). This proves the "only if" part. Now we prove the other direction. Let F be a radical extension field of Q and $\forall x\, \exists y\, \varphi(x, y)$ be false in F. Then there exists a β in F such that $\exists y\, \varphi(\beta, y)$ is false in F. This implies that either $G(\beta) = 0$ or $g_{i,k}(\beta, F(\beta)/G(\beta)) = 0$. Hence β must be a root of the equation $h(x) = 0$ for an $h(x)$ of S. Since F is a radical extension field of Q and β is an element of F, β can be expressed in terms of radicals. If $h(x) = 0$ has a root expressed in terms of radicals, then $h(x) = 0$ is solvable by radicals (Lang, 1971). Hence $h(x)$ must be an element of S'. Clearly, $Q(\beta) \simeq Q[x]/h(x)$ is a subfield of F. Then $\exists y\, \varphi(\beta, y)$ is false in $Q(\beta)$, hence $\exists y\, \varphi(x, y)$ is false in $Q[x]/h(x)$ by taking x as an element of $Q[x]/h(x)$. Therefore $\forall x\, \exists y\, \varphi(x, y)$ is false in $Q[x]/h(x)$. This proves our claim and completes our proof. ∎

The special properties of the radical extension fields of Q used in the proof of Theorem 3 are as follows:

(1) There is a polynomial time algorithm to decide whether the Galois group of equation $h(x) = 0$ is solvable or not.

(2) Let K be a radical extension over Q. If F is an intermediate field, then F is a radical extension field of Q.

(3) Let K be an radical extension field of Q and $h(x)$ be an irreducible polynomial over Q. If $h(x) = 0$ is solvable in K then the Galois group of equation $h(x) = 0$ is solvable.

From Galois theory (Lang, 1971) and the results in (Landau, 1985), cyclic extension fields of Q and abelian extension fields of Q also share these properties. We then obtain the following corollary.

COROLLARY 3. *There is a polynomial time algorithm to decide whether or not a* $\forall\exists$ *sentence in conjunctive or disjunctive normal form is true in every cyclic (abelian) extension field of* Q.

ACKNOWLEDGMENT

The author thanks the anonymous referees for helpful suggestions for improving the presentation of this paper.

RECEIVED January 19, 1989; FINAL MANUSCRIPT RECEIVED August 21, 1990

REFERENCES

KNUTH, D. E. (1981), "The Art of Computer Programming, Vol. 2: Semi-Numerical Algorithms," 2nd ed., Addison–Wesley, Reading, MA.

LANDAU, S. (1985), Factoring polynomials over algebraic number fields, *SIAM J. Comput.* **14**, 184–195.

LANDAU, S., AND MILLER, G. L. (1985), Solvability by radicals is in polynomial time, *J. Comput. System Sci.* **30**, 179–208.

LANG, S., (1971), "Algebra," Addison–Wesley, Reading, MA.

LENSTRA, A. K. (1982), "Factoring Polynomials over Algebraic Number Fields," Report IW 213/82, Mathematisch Centrum, Amsterdam.

LENSTRA, A. K. (1987), Factoring multivariate polynomials over algebraic number fields, *SIAM J. Comput.* **16**, 591–598.

LENSTRA, A. K., LENSTRA, H. W., AND LOVASZ, L. (1982), Factoring polynomials with rational coefficients, *Math. Ann.* **261**, 515–534.

MIGNOTTE, M. (1974), An inequality about factors of polynomials, *Math. Comp.* **28**, 1153–1157.

POLLARD, H., AND DIAMOND, H. (1975), "The Theory of Algebraic Numbers," 2nd ed., Math. Assoc. of America, Buffalo, NY.

ROBINSON, J. (1949), Definability and decision problems in arithmetic, *J. Symbolic Logic* **14**, 98–114.

ROBINSON, J. (1959), The undecidability of algebraic rings and fields, *Proc. Amer. Math. Soc.* **10**, 950–957.

ROBINSON, R. M. (1964), The undecidability of pure transcendental extensions of real fields, *Z. Math. Logik Grundlag. Math.* **10**, 275–282.

SCHINZEL, A. (1982), "Selected Topics on Polynomials," Univ. of Michigan Press, Ann Arbor.

TUNG, S. P. (1986), Provability and decidability of arithmetical universal–existential sentences, *Bull. London Math. Soc.* **18**, 241–247.

TUNG, S. P. (1987), Computational complexities of diophantine equations with parameters, *J. Algorithms* **8**, 324–336.

TUNG, S. P. (1990), Decidable fragments of field theories, *J. Symbolic Logic* **55**, 1007–1018.

TUNG, S. P. (1991), Complexity of sentences over number rings, *SIAM J. Comput.* **20**, 126–143.