J. Symbolic Computation (2002) **33**, 239–254
doi:10.1006/jsco.2001.0505
Available online at http://www.idealibrary.com on IDEAL®

Approximate Solutions of Polynomial Equations

SHIH PING TUNG

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

In this paper, we introduce "approximate solutions" to solve the following problem: given a polynomial $F(\bar{x}, y)$ over Q, where $\bar{x}$ represents an n-tuple of variables, can we find all the polynomials $G(\bar{x})$ such that $F(\bar{x}, G(\bar{x}))$ is identically equal to a constant c in Q? We have the following: let $F(\bar{x}, y)$ be a polynomial over Q and the degree of y in $F(\bar{x}, y)$ be n. Either there is a unique polynomial $g(\bar{x}) \in Q[\bar{x}]$, with its constant term equal to 0, such that $F(\bar{x}, y) = \sum_{j=0}^{n} c_j(y - g(\bar{x}))^j$ for some rational numbers c_j, hence, $F(\bar{x}, g(\bar{x}) + a) \in Q$ for all $a \in Q$, or there are at most t distinct polynomials $g_1(\bar{x}), \ldots, g_t(\bar{x})$, $t \leq n$, such that $F(\bar{x}, g_i(\bar{x})) \in Q$ for $1 \leq i \leq t$. Suppose that $F(x, y)$ is a polynomial of two variables. The polynomial $g(x)$ for the first case, or $g_1(x), \ldots, g_t(x)$ for the second case, are approximate solutions of $F(x, y)$, respectively. There is also a polynomial time algorithm to find all of these approximate solutions. We then use Kronecker's substitution to solve the case of $F(\bar{x}, y)$.

1. Introduction

Finding factors of a polynomial is an interesting and important problem. However, in applications, there are cases where we may not have complete information on the polynomial we want to factor. Given a polynomial $f(x, y)$ over Q with its constant term not known, do we have an algorithm to find all the possible polynomials $g(x)$ such that $f(x, g(x)) = 0$? This is equivalent to the problem of whether, given a polynomial $f(x, y)$, we have an algorithm to find all the polynomials $g(x)$ such that $y - g(x)$ is a factor of $f(x, y) - c$, or $f(x, g(x)) \equiv c$, for some $c \in Q$. In a certain sense, this problem is not well posed, since given a polynomial $f(x, y)$ there may exist infinitely many distinct polynomials $g(x)$ such that $f(x, g(x)) \in Q$. If $f(x, y) = \sum_{j=0}^{n} c_j(y - g(x))^j$ for some $c_j \in Q$ and a polynomial $g(x) \in Q[x]$, then for any $a \in Q$, $f(x, g(x) + a) \in Q$. However, it will be shown that given a polynomial $f(x, y)$ this is the only case where there are infinitely many distinct polynomials $g(x)$ such that $f(x, g(x)) \in Q$. Hence, if for this case $g(x)$ is required with its constant term equal to 0, then such $g(x)$ is unique. Moreover, if there is no polynomial $g(x)$ such that $f(x, y) = \sum_{j=0}^{n} c_j(y - g(x))^j$, for some $c_j \in Q$, then the number of polynomials $h(x)$ such that $f(x, h(x)) \in Q$ is less than or equal to the degree of y in $f(x, y)$. We then may wonder whether there is a polynomial time algorithm to find all of these polynomials. The main result of this paper is showing that there is a polynomial time algorithm to find the unique $g(x)$, with its constant term equal to 0, for the first case, or all the polynomials $h(x)$ for the second case. The existing polynomial time algorithms for factoring multivariate polynomials apparently do not apply to this situation (Lenstra *et al.*, 1982; Kaltofen, 1985; Chistov, 1986; Lenstra, 1987, 1984). An

0747–7171/02/020239 + 16 $35.00/0

alternative method is needed. For this purpose, we introduce the concept of "approximate solutions" to solve this problem. Using iteration to find approximate solutions is common in numerical analysis. A similar idea is used here. $Q[x]$ is an Euclidean domain and its size function is the degree of polynomial (Dean, 1990). The size function of $Q[x]$ plays the role of the usual Euclidean norm of R^n. However, the "discreteness" of the size function here guarantees that we shall get all the possible factors. Whether we can have an algorithm which directly finds all such factors is an interesting problem.

To study this problem is motivated by the decision problem of diophantine equations with parameters. Given a polynomial $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$, diophantine equations with parameters ask whether for any numbers $a_1, \ldots, a_n$ the equation $f(a_1, \ldots, a_n, y_1, \ldots, y_m) = 0$ is solvable. This is equivalent to asking whether

$$\forall x_1 \cdots \forall x_n \exists y_1 \cdots \exists y_m f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$$

is true or not. The quantified variables range over N, Z or Q depending on whether the solvability of the equation is being asked over N, Z or Q, respectively. Schinzel (1982) gave a review of this topic. The computational complexities of various known decidable cases of diophantine equations with parameters are given in Tung (1987). In particular, it is shown that the decision problem of deciding whether

$$\forall x_1 \cdots \forall x_n \exists y f(x_1, \ldots, x_n, y) = 0$$

is true over Z is co-NP-complete if $n \geq 1$. We then may ask whether, given a polynomial $f(x_1, \ldots, x_n, y)$ over Z, there is a decision procedure to determine whether or not

$$\exists z \forall x_1 \cdots \forall x_n \exists y\ f(x_1, \ldots, x_n, y) = z$$

is true over Z. Let $f(x_1, \ldots, x_n, y) \in Q[x_1, \ldots, x_n, y]$, then

$$\exists z \forall x_1 \cdots \forall x_n \exists y\ f(x_1, \ldots, x_n, y) = z$$

is true over Z if and only if there is an $a \in Z$, and for any integer $a_1, \ldots, a_n$ there is a $g(x_1, \ldots, x_n) \in Q[x_1, \ldots, x_n]$ such that $y - g(x_1, \ldots, x_n)$ is a factor of $f(x_1, \ldots, x_n, y) - a$ in $Q[x_1, \ldots, x_n, y]$ and $g(a_1, \ldots, a_n) \in Z$ (Tung, 1985). Since the number a in the above formula is not known in advance, we need to find linear factors of $f(x_1, \ldots, x_n, y)$ over Q; assume that the constant term is not known. This paper shows that we can do it and in polynomial time. From this result, it is shown in Tung (unpublished) that, given a polynomial $f(x_1, \ldots, x_n, y)$ over Z, the decision problem of determining whether

$$\exists z \forall x_1 \cdots \forall x_n \exists y\ f(x_1, \ldots, x_n, y) = z$$

is true over Z is co-NP-complete. Various other related NP-complete number theoretic decision problems are also shown in Tung (unpublished).

All the results in this paper are stated over Q. It should be easy to see that these results also hold in more general fields. In fact, all the results in Section 2 are true for polynomials over an arbitrary field. A fact used repeatedly is $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$. That polynomial time algorithms for factoring polynomials are available is another fact used repeatedly in Section 3.

2. Approximate Solutions

In this section, we shall define approximate solutions of a polynomial equation. We first give some properties concerning linear factors of a polynomial. These properties then are used to show that the number of approximate solutions of a polynomial equation has a natural bound.

We fix some notation. We use $\bar{x}$ to represent an n-tuple of variables $\langle x_1, \ldots, x_n \rangle$. If $f(x)$ is a polynomial of one variable, then $\deg(f(x))$ is the degree of $f(x)$. For a multivariate polynomial $F(x_1, \ldots, x_n)$, $\deg_{x_i}(F(x_1, \ldots, x_n))$ denotes the degree of x_i, $1 \le i \le n$, in $F(x_1, \ldots, x_n)$.

Let $F(\bar{x}, y)$ be a polynomial over Q where $F(\bar{x}, g(\bar{x})) = b_1$, $F(\bar{x}, h(\bar{x})) = b_2$ for some polynomials $g(\bar{x})$, $h(\bar{x})$ and some rational numbers b_1, b_2, respectively. Thus,

$$F(\bar{x}, y) = (y - g(\bar{x}))G(\bar{x}, y) + b_1 = (y - h(\bar{x}))H(\bar{x}, y) + b_2.$$

If $b_1 = b_2$, then there are two possible cases. First, if $g(\bar{x}) = h(\bar{x})$ then $G(\bar{x}, y) = H(\bar{x}, y)$. If $g(\bar{x}) \neq h(\bar{x})$, then

$$F(\bar{x}, y) = (y - g(\bar{x}))(y - h(\bar{x}))f(\bar{x}, y) + b_1$$

for an $f(\bar{x}, y) \in Q[\bar{x}, y]$. What happens if $b_1 \neq b_2$? This is answered in the following proposition. Moreover, we combine the cases where $b_1 = b_2$ and $b_1 \neq b_2$ with one formula.

Proposition 2.1. *Let $F(\bar{x}, y)$, $g(\bar{x})$ and $h(\bar{x})$ be polynomials over Q. Let b_1 and b_2 be elements of Q. Suppose also that if $b_1 = b_2$, then $g(\bar{x}) \neq h(\bar{x})$. Then $F(\bar{x}, g(\bar{x})) \equiv b_1$ and $F(\bar{x}, h(\bar{x})) \equiv b_2$ if and only if there exists a d in Q and a polynomial $f(\bar{x}, y)$ in $Q[\bar{x}, y]$ such that*

$$F(\bar{x}, y) = [y - g(\bar{x})] \cdot [(y - h(\bar{x}))f(\bar{x}, y) + (b_2 - b_1)/d] + b_1$$

and if $b_1 \neq b_2$, then also such that $h(\bar{x}) = g(\bar{x}) + d$ with $d \neq 0$.

Proof. Clearly, if $b_1 = b_2$, then

$$F(\bar{x}, y) = [y - g(\bar{x})] \cdot [(y - h(\bar{x}))f(\bar{x}, y) + (b_2 - b_1)/d] + b_1$$

implies that

$$F(\bar{x}, y) = [y - g(\bar{x})] \cdot [(y - h(\bar{x}))f(\bar{x}, y)] + b_1.$$

This has been discussed in the above. Hence, we prove only the case where $b_1 \neq b_2$.

We first prove the direction ($\Leftarrow$). Suppose that

$$F(\bar{x}, y) = [y - g(\bar{x})] \cdot [(y - h(\bar{x}))f(\bar{x}, y) + (b_2 - b_1)/d] + b_1$$

for a $d \neq 0$ in Q and $h(\bar{x}) = g(\bar{x}) + d$. Then,

$$\begin{aligned} F(\bar{x}, g(\bar{x})) &= [g(\bar{x}) - g(\bar{x})] \cdot [(g(\bar{x}) - h(\bar{x}))f(\bar{x}, g(\bar{x})) + (b_2 - b_1)/d] + b_1 \\ &= b_1. \end{aligned}$$

Also,

$$\begin{aligned} F(\bar{x}, h(\bar{x})) &= [h(\bar{x}) - g(\bar{x})] \cdot [(h(\bar{x}) - h(\bar{x}))f(\bar{x}, h(\bar{x})) + (b_2 - b_1)/d] + b_1 \\ &= [h(\bar{x}) - h(\bar{x}) + d] \cdot [0 \cdot f(\bar{x}, h(\bar{x})) + (b_2 - b_1)/d] + b_1 \\ &= d \cdot [(b_2 - b_1)/d] + b_1 \\ &= b_2. \end{aligned}$$

Next, we prove the other direction ($\Rightarrow$). From the assumptions, there exist $G(\bar{x})$ and

$H(\bar{x})$ in $Q[\bar{x}]$ such that

$$F(\bar{x},y) = (y - g(\bar{x})) \cdot G(\bar{x},y) + b_1 = (y - h(\bar{x})) \cdot H(\bar{x},y) + b_2.$$

Substituting $y = h(\bar{x})$ in $F(\bar{x},y)$ we obtain that

$$(h(\bar{x}) - g(\bar{x})) \cdot G(\bar{x}, h(\bar{x})) = b_2 - b_1 \neq 0.$$

This implies that the degree of $h(\bar{x}) - g(\bar{x})$ must be zero; hence, $h(\bar{x}) - g(\bar{x}) = d$ for a rational number $d \neq 0$, and $d \cdot G(\bar{x}, h(\bar{x})) = b_2 - b_1$. This implies that $G(\bar{x},y) = (y - h(\bar{x}))f(\bar{x},y) + (b_2 - b_1)/d$, and

$$F(\bar{x},y) = [y - g(\bar{x})] \cdot [(y - h(\bar{x}))f(\bar{x},y) + (b_2 - b_1)/d] + b_1$$

for an $f(\bar{x},y) \in Q[\bar{x},y]$. □

This fact is the key of the algorithm in the next section. It means that whether $b_1 = b_2$ or not, one formula suffices. Hence, one algorithm suffices. This fact needs to be extended to the cases where the number of those polynomials $g(\bar{x})$ where $F(\bar{x}, g(\bar{x})) \in Q$ is more than two. This is what we do below.

Lemma 2.2. *Let $F(\bar{x},y)$ and $g_i(\bar{x})$, $1 \leq i \leq m$, be polynomials over Q, where $g_i(\bar{x})$ are all distinct, and there exist $1 \leq p < q \leq m$ such that $g_p(\bar{x}) \neq g_q(\bar{x}) + a$ for any $a \in Q$. Then, $F(\bar{x}, g_i(\bar{x})) \in Q$ for every i, $1 \leq i \leq m$, if and only if $F(\bar{x},y) = \left[\prod_{i=1}^{m}(y - g_i(\bar{x}))\right] \cdot G(\bar{x},y) + c$ for a $c \in Q$ and a $G(\bar{x},y) \in Q[\bar{x},y]$.*

Proof. ($\Leftarrow$) Clearly, if $F(\bar{x},y) = \left[\prod_{i=1}^{m}(y - g_i(\bar{x}))\right] \cdot G(\bar{x},y) + c$ for a $c \in Q$ and a $G(\bar{x},y) \in Q[\bar{x},y]$, then $F(\bar{x}, g_i(\bar{x})) = c \in Q$ for every i, $1 \leq i \leq m$.

Now, we prove the direction ($\Rightarrow$). Assume that $g_p(\bar{x}) \neq g_q(\bar{x}) + a$ for any $a \in Q$. From Proposition 2.1, we obtain that

$$F(\bar{x},y) = (y - g_p(\bar{x}))G_p(\bar{x},y) + c = (y - g_q(\bar{x}))G_q(\bar{x},y) + c$$

for some $c \in Q$. Then $F(\bar{x},y) = (y - g_p(\bar{x}))(y - g_q(\bar{x}))h(\bar{x},y) + c$ for some polynomial $h(\bar{x},y)$ over Q because $y - g_p(\bar{x})$ and $y - g_q(\bar{x})$ are relatively prime over $Q[\bar{x},y]$ and both are factors of $F(\bar{x},y) - c$. Now for any other polynomial $g_r(\bar{x})$, with $r \neq p$ and $r \neq q$, either $g_r(\bar{x}) \neq g_p(\bar{x}) + b$ or $g_r(\bar{x}) \neq g_q(\bar{x}) + b$ for all b in Q. Without loss of generality, we may assume that $g_r(\bar{x}) \neq g_p(\bar{x}) + b$ for any b in Q, then with the same arguments as above we obtain that $F(\bar{x},y) = (y - g_p(\bar{x}))(y - g_r(\bar{x}))H(\bar{x},y) + d$ for a polynomial $H(\bar{x},y)$ over Q and a d in Q. Since

$$F(\bar{x},y) = (y - g_p(\bar{x}))(y - g_q(\bar{x}))h(\bar{x},y) + c = (y - g_p(\bar{x}))(y - g_r(\bar{x}))H(\bar{x},y) + d,$$

we obtain that $d = c$ by substituting $g_p(\bar{x})$ for y. Then, $y - g_r(\bar{x})$ is a factor of $F(\bar{x},y) - c$. This argument shows that every $y - g_i(\bar{x})$, $1 \leq i \leq m$, is a factor of $F(\bar{x},y) - c$. Hence, $F(\bar{x},y) = \left[\prod_{i=1}^{m}(y - g_i(\bar{x}))\right] \cdot G(\bar{x},y) + c$ for a $G(\bar{x},y) \in Q[\bar{x},y]$. □

Now, we are ready to extend the results in Proposition 2.1 to more general cases. For simplicity, we do not state the results in all the detail which is done in Proposition 2.1. As we said previously, “one formula suffices”.

Theorem 2.3. *Let $F(\bar{x},y)$ and $g_i(\bar{x})$, $1 \leq i \leq m$, be polynomials over Q, and $g_i(\bar{x})$ are* *all distinct. Then,* $F(\bar{x}, g_i(\bar{x})) \in Q$ *for every* i, $1 \leq i \leq m$, *if and only if*

$$F(\bar{x}, y) = (y - g_1(\bar{x}))\{(y - g_2(\bar{x}))[(y - g_3(\bar{x}))(\cdots(G(\bar{x}, y)\cdots) + d_3] + d_2\} + d_1,$$

where $G(\bar{x}, y) \in Q[\bar{x}, y]$ *and* $d_i \in Q$ *for* $1 \leq i \leq m$.

Proof. Suppose that there exist $1 \leq p < q \leq m$ such that $g_p(\bar{x}) \neq g_q(\bar{x}) + a$ for any $a \in Q$. From Lemma 2.2, $F(\bar{x}, g_i(\bar{x})) \in Q$ for every i, $1 \leq i \leq m$, if and only if $F(\bar{x}, y) = \left[\prod_{i=1}^{m}(y - g_i(\bar{x}))\right] \cdot G(\bar{x}, y) + c$ for a $c \in Q$ and a $G(\bar{x}, y) \in Q[\bar{x}, y]$. Thus, we take $d_i = 0$ for $2 \leq i \leq m$, and $d_1 = c$.

Assume that these m polynomials $g_i(\bar{x})$ all differ only by a constant, i.e. there is a polynomial $g(\bar{x})$ over Q and rational numbers a_i, $1 \leq i \leq m$, such that $g_i(\bar{x}) = g(\bar{x}) + a_i$. We prove the direction (⇒) first. From Proposition 2.1, if

$$F(\bar{x}, y) = (y - g(\bar{x}) - a_1)G_1(\bar{x}, y) + b_1 = (y - g(\bar{x}) - a_2)G_2(\bar{x}, y) + b_2,$$

for some $b_1, b_2 \in Q$, then

$$F(\bar{x}, y) = (y - g(\bar{x}) - a_1)((y - g(\bar{x}) - a_2)f_1(\bar{x}, y) + (b_2 - b_1)/(a_2 - a_1)) + b_1$$

for an $f_1(\bar{x}, y) \in Q[\bar{x}, y]$. With the same argument and substituting y with $g(\bar{x}) - a_3$, we obtain that $f_1(\bar{x}, y) = (y - g(\bar{x}) - a_3)f_2(\bar{x}, y) + d$ with some $d \in Q$. By induction,

$$F(\bar{x}, y) = (y - g(\bar{x}) - a_1)\{(y - g(\bar{x}) - a_2)[(y - g(\bar{x}) - a_3)(\cdots(G(\bar{x}, y)\cdots) + d_3] + d_2\} + d_1,$$

where $G(\bar{x}, y) \in Q[\bar{x}, y]$ and $d_i \in Q$ for $1 \leq i \leq m$.

Now, we prove the other direction (⇐) and assume that

$$F(\bar{x}, y) = (y - g_1(\bar{x}))\{(y - g_2(\bar{x}))[(y - g_3(\bar{x}))(\cdots(G(\bar{x}, y)\cdots) + d_3] + d_2\} + d_1.$$

Since $g_i(\bar{x}) = g(\bar{x}) + a_i$ for some rational numbers a_i, with a similar calculation as is done in the proof of Proposition 2.1 we obtain that $F(\bar{x}, g_i(\bar{x})) \in Q$ for every i, $1 \leq i \leq m$. □

From Theorem 2.3, we also have the following lemma. This lemma gives us a case where for a given polynomial $F(\bar{x}, y)$ over Q there may exist infinitely many distinct polynomials $g(\bar{x}) \in Q[\bar{x}]$, such that $F(\bar{x}, g(\bar{x})) \in Q$. As will be shown, this is the only case where there are so many such polynomials.

Lemma 2.4. *Let* $F(\bar{x}, y)$ *be a polynomial over* Q *and* $\deg_y(F(\bar{x}, y)) = n$. *Let* $g(\bar{x}) \in Q[\bar{x}]$ *and* $a_1, \ldots, a_{n+1}$ *be distinct rational numbers. Then,* $F(\bar{x}, g(\bar{x}) + a_i) \in Q$ *for* $1 \leq i \leq n+1$, *if and only if* $F(\bar{x}, y) = \sum_{j=0}^{n} c_j(y - g(\bar{x}))^j$ *for some rational numbers* $c_0, \ldots, c_n$.

Proof. First we prove the direction (⇐). Suppose that $F(\bar{x}, y) = \sum_{j=0}^{n} c_j(y - g(\bar{x}))^j$ where c_j are rational numbers and $g(\bar{x}) \in Q[\bar{x}]$. Put $b_i = \sum_{j=0}^{n} c_j(a_i)^j$, $(i = 1, \ldots, n+1)$. Substitute $y = g(\bar{x}) + a_i$, $1 \leq i \leq n+1$, $F(\bar{x}, g(\bar{x}) + a_i) = \sum_{j=0}^{n} c_j(a_i)^j = b_i$.

Now we prove the direction (⇒). From Theorem 2.3, if $g(\bar{x}) \in Q[\bar{x}]$ and $a_1, \ldots, a_n$ are distinct rational numbers, and $F(\bar{x}, g(\bar{x}) + a_i) \in Q$ for $1 \leq i \leq n$, then

$$F(\bar{x}, y) = (y - g(\bar{x}) - a_1)\{(y - g(\bar{x}) - a_2)[(y - g(\bar{x}) - a_3)(\cdots(h(\bar{x}, y)\cdots) + d_3] + d_2\} + d_1,$$

where $h(\bar{x}, y) \in Q[\bar{x}, y]$ and $d_i \in Q$ for $1 \leq i \leq n$. In fact, $h(\bar{x}, y)$ has no variable y, i.e. $h(\bar{x}, y) \equiv h(\bar{x}) \in Q[\bar{x}]$ since $\deg_y(F(\bar{x}, y)) = n$. Moreover, $h(\bar{x})$ must be a number in Q, otherwise, $F(\bar{x}, g(\bar{x}) + a_{n+1})$ cannot be a number in Q. Therefore,

$$F(\bar{x}, y) = (y - g(\bar{x}) - a_1)\{(y - g(\bar{x}) - a_2)[(y - g(\bar{x}) - a_3)(\cdots(c)\cdots) + d_3] + d_2\} + d_1,$$

for some $c \in Q$. We may rewrite the term and obtain that

$$F(\bar{x}, y) = c(y - g(\bar{x}) - a_1)\{(y - g(\bar{x}) - a_2)[(y - g(\bar{x}) - a_3)(\cdots) + e_3] + e_2\} + e_1,$$

with all a_i, e_i, and c in Q and $F(\bar{x}, y) = \sum_{j=0}^{n} c_j(y - g(\bar{x}))^j$ for some rational number $c_0, \ldots, c_n$. □

Theorem 2.5. *Let $F(\bar{x}, y)$ be a polynomial over Q and $\deg_y(F(\bar{x}, y)) = n$. Either there is a unique polynomial $g(\bar{x}) \in Q[\bar{x}]$, with its constant term equal to 0, such that $F(\bar{x}, y) = \sum_{j=0}^{n} c_j(y - g(\bar{x}))^j$ for some rational numbers c_j, hence $F(\bar{x}, g(\bar{x}) + a) \in Q$ for all $a \in Q$, or there are at most n distinct polynomials $g_1(\bar{x}), \ldots, g_t(\bar{x})$, $t \le n$, such that $F(\bar{x}, g_i(\bar{x})) \in Q$ for $1 \le i \le t$.*

Proof. Let $g_i(\bar{x})$, $1 \le i \le t$, be distinct polynomials and $F(\bar{x}, g_i(\bar{x})) \in Q$. Assume that there exist $1 \le p < q \le t$ such that $g_p(\bar{x}) \ne g_q(\bar{x}) + a$ for any $a \in Q$. Then, by Lemma 2.2

$$F(\bar{x}, y) = \left[\prod_{i=1}^{t}(y - g_i(\bar{x}))\right] \cdot G(\bar{x}, y) + c$$

for a $c \in Q$ and a $G(\bar{x}, y) \in Q[\bar{x}, y]$. This implies that $\deg_y(F(\bar{x}, y)) = n \ge t$. On the other hand, if these t polynomials $g_i(\bar{x})$ all differ only by a constant, then there is a polynomial $g(\bar{x}) \in Q[\bar{x}]$ with its constant term equal to 0, and rational numbers b_i, $1 \le i \le t$, such that $g_i(\bar{x}) = g(\bar{x}) + b_i$. If $t > n$, then by Lemma 2.4, $F(\bar{x}, y) = \sum_{j=0}^{n} c_j(y - g(\bar{x}))^j$ where $c_j \in Q$. Thus, for all a in Q,

$$F(\bar{x}, g(\bar{x}) + a) = \sum_{j=0}^{n} c_j(g(\bar{x}) + a - g(\bar{x}))^j = \sum_{j=0}^{n} c_j a^j$$

is in Q. Now, let $h(\bar{x})$ be an arbitrary polynomial over Q but $h(\bar{x}) - g(\bar{x})$ is not a number in Q. Then,

$$F(\bar{x}, h(\bar{x})) = \sum_{j=0}^{n} c_j(h(\bar{x}) - g(\bar{x}))^j$$

is a polynomial but not a number in Q. This implies that polynomial $g(\bar{x})$ is unique if its constant term is required to be 0. □

The situation we have now is similar to the case of equations over Q. If an equation $f(x) = 0$ of degree n has $n + 1$ solutions, then $f(x) \equiv 0$. This implies that every $a \in Q$ is a solution of $f(x) = 0$. From Theorem 2.5, we can see that if the degree of y in $F(\bar{x}, y)$ is n and there are $n + 1$ distinct polynomials $\{g_1(\bar{x}), \ldots, g_{n+1}(\bar{x})\}$ such that $F(\bar{x}, g_i(\bar{x})) - b_i \equiv 0$ for some b_i in Q, then for every $a \in Q$, $F(\bar{x}, g_1(\bar{x}) + a)) - b \equiv 0$ for some $b \in Q$.

Now, we define "approximate solutions" which extends the meaning of "solutions" of equations in $Q[x]$. Here, we use the convention that a zero polynomial is of degree $-\infty$.

Definition. Let $F(x, y) \in Q[x, y]$ and z be an indeterminate.
1. Let $a \in Q$ and $a \ne 0$. If $\deg(F(x, ax^s)) < \deg_x(F(x, zx^s))$, then ax^s is called an approximate solution of $F(x, y) = 0$ of order s.
2. If $H(x) = \sum_{i=m+1}^{s} a_i x^i \in Q[x]$ is an approximate solution of $F(x, y) = 0$ of order

$m+1$, and $G(x) = H(x) + bx^m \in Q[x]$ with $\deg(F(x, G(x)) < \deg_x(F(x, H(x) + zx^m))$, then $G(x)$ is an approximate solution of $F(x, y)$ of order m.

Note that the coefficient b in $G(x)$ may equal zero. $G(x)$ is then written as $H(x)+0x^m$. Thus, $H(x)$ equals $G(x)$ mathematically. However, like significant figures in scientific measurements, they have different orders of accurracy. In this case, we shall view $G(x)$ and $H(x)$ as two approximate solutions of $F(x, y)$ of different orders. Let $F(x, y) \in Q[x, y]$, we may view $F(x, y) = \bar{F}(y)$ as a polynomial of one variable y over the ring $Q[x]$, and we may require the root of the equation $\bar{F}(y) = 0$ in $Q[x]$. From our definition of approximate solution, we can see that every solution of the polynomial equation $\bar{F}(y) = 0$ in $Q[x]$ is an approximate solution of $F(x, y) = 0$ too.

Example. Let $f(x, y) = (2y - x^3 - x^2 + 3x + 1)(2y - x^3 - x^2 + x + 2) + 5$. Then, $G(x) = x^3/2$ is an approximate solution of $f(x, y)$ of order 3, since

$$f(x, zx^3) = ((2z-1)x^3 - x^2 + 3x + 1)((2z-1)x^3 - x^2 + x + 2) + 5$$

is a polynomial with its x degree equal to 6 and $\deg(f(x, x^3/2)) = 4$. Similarly, $(x^3 + x^2)/2$ is an approximate solution of order 2. Since $\deg_x(f(x, (x^3 + x^2)/2 + zx)) = 2$, $\deg(f(x, (x^3 + x^2 - 3x)/2)) = 1$, and $\deg(f(x, (x^3 + x^2 - x)/2)) = 1$, $(x^3 + x^2 - 3x)/2$ and $(x^3 + x^2 - x)/2$ are approximate solutions of order 1, respectively. Polynomials $(x^3 + x^2 - 3x - 1)/2$ and $(x^3 + x^2 - x - 2)/2$ are approximate solutions with order 0, and the only two approximate solutions of order 0.

Let $F(x, y)$ be a polynomial over Q and $\deg_y(F(x, y)) = n$. If there is a polynomial $g(x) = \sum_{i=1}^{m} a_i x^i \in Q[x]$ such that $F(x, y) = \sum_{j=0}^{n} c_j(y - g(x))^j$ for some rational numbers c_j, then $g(x)$ is an approximate solution of $F(x, y)$ of order 1. Then, α is a root of the equation $f(z) = \sum_{j=0}^{n} c_j z^j = 0$ in Q if and only if $g(x) + \alpha$ is an approximate solution of $F(x, y)$ of order 0. If $F(x, y)$ is not in this case, by Theorem 2.5, there are at most n distinct polynomials $g_1(x), \ldots, g_t(x)$, $t \le n$, such that $F(x, g_i(x)) \in Q$ for $1 \le i \le t$. These polynomials $g_1(x), \ldots, g_t(x)$ are the only approximate solutions of order 0 of $F(x, y)$. Therefore, in either case there are at most n distinct approximate solutions of order 0. This is true for other orders by Theorem 2.7 below.

We may also discuss the approximate solutions from another point of view. Let $F(x, y)$ be a polynomial over Q and $Q(x)$ an approximate solution of $F(x, y)$ as defined above. We say $Q(x)$ is an approximate solution of rank s if $\deg(F(x, Q(x)) = s$. Previously, people focused on solving equations. Thus, we may say that given a polynomial $F(x, y)$ we want to find approximate solution $G(x)$ of rank $-\infty$, i.e. $F(x, g(x)) \equiv 0$. There are cases where such solutions do not exist, like the polynomial $f(x, y)$ in the above example. But, $f(x, y)$ has approximate solution of rank 0. We may say that for a given polynomial $F(x, y)$, in this paper, we wish to find all approximate solutions $g(x)$ of $F(x, y)$ of rank 0, i.e. $F(x, g(x)) \equiv c$ for some c in Q.

We next give two facts concerning approximate solutions, which will be needed to show the correctness and polynomial time complexity of the algorithm given in the next section.

Proposition 2.6. *Let $F(x, y) = \sum_{k=0}^{s} f_k(x) y^k = \sum_{k=0}^{s} \big(\sum_{l=0}^{t_k} b_{k,l} x^l\big) y^k$ be a polynomial with its degree of y equal to s. Let m be a positive integer such that $sm + t_s \ge km + t_k$ for $0 \le k < s$. Then, the degree of every approximate solution of $F(x, y)$ is less than or equal to m. In particular, the maximum of t_k, $0 \le k < s$, suffices.*

Proof. Let $F(x,y) = \sum_{k=0}^{s} f_k(x)y^k = \sum_{k=0}^{s}\big(\sum_{l=0}^{t_k} b_{k,l}x^l\big)y^k$, and m satisfy the assumption. Let $r(x) = \sum_{i=p}^{d} a_i x^i$, where $a_d \neq 0$ and $d > m$, then for every k,

$$\deg(f_k(x)\cdot(r(x))^k) = \deg(f_k(x)) + \deg((r(x))^k) = t_k + dk.$$

By our choice of d and m, $sd + t_s > kd + t_k$ for $0 \le k < s$. Thus,

$$\deg(F(x, r(x))) = \deg(f_s(x)\cdot(r(x))^s) = sd + t_s.$$

It is easy to see that with z an indeterminate $\deg_x(F(x, zx^d)) = sd + t_s$. Thus, $r(x)$ cannot be an approximate solution.

Clearly, if $m \ge t_k$ for $0 \le k < s$, then $(s-k)m \ge (t_k - t_s)$; hence, $sm + t_s \ge km + t_k$. □

This proposition gives us the upper bound on the degree of each approximate solution. Thus, if $F(x, g(x)) \in Q$, then $\deg(g(x)) \le m$. The next theorem gives us the upper bound on the number of approximate solutions at each order.

Theorem 2.7. *Let $F(x,y)$ be a polynomial with its degree in y equal to n, then at each order there are at most n distinct approximate solutions.*

Proof. We prove this theorem by induction on the degree of y in $F(x,y)$. Let $\deg_y(F(x,y)) = 1$ and $F(x,y) = f_1(x)y + f_0(x)$ where $f_1(x)$ and $f_0(x)$ are in $Q[x]$. If $\deg(f_1(x)) > \deg(f_0(x))$, then $F(x,y)$ has no approximate solutions since

$$\deg_x(F(x, zx^s)) = \deg(F(x, ax^s)) = \deg(f_1(x)) + s$$

for any $a \in Q$, $a \neq 0$, and any $s \ge 0$. Now, assume that $\deg(f_1(x)) \le \deg(f_0(x))$. By the division algorithm, $f_0(x) = q(x)f_1(x) + r(x)$ where $q(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, and $\deg(r(x)) < \deg(f_1(x))$. Then,

$$\deg(F(x, -a_n x^n)) < \deg(f_0(x)) = \deg_x(F(x, zx^n)).$$

Hence, $a_n x^n$ is an approximate solution of order n, and the only approximate solution of order n. Also, $q_j(x) = \sum_{i=j}^{n} a_i x^i$ is the only approximate solution of order j for each j, $n \ge j \ge 0$. This proves the case $\deg_y(F(x,y)) = 1$.

Assume that our hypothesis is true for any polynomial with its degree in y equal to n. Now, let $F(x,y)$ be a polynomial with its degree of y equal to $n+1$. Let S be an arbitrary set of approximate solutions of $F(x,y)$ and all are of order s. We need to show that the number of elements of S is at most $n+1$. Let $G(x)$ be an approximate solution of $F(x,y)$ in S for which the degree of $F(x, G(x))$ is minimal, i.e. if $H(x) \in S$, then $\deg(F(x, G(x))) \le \deg(F(x, H(x)))$. Assume that $\deg(F(x, G(x))) = t$. By the factor theorem,

$$F(x,y) = (y - G(x))F_1(x,y) - F(x, G(x))$$

for an $F_1(x,y)$ in $Q[x,y]$ and $\deg_y(F_1(x,y)) = n$. We want to show that every approximate solution $H(x)$ in S, except $G(x)$, is an approximate solution of $F_1(x,y)$ of the order s too.

Let $H(x) = H_1(x) + b_s x^s$ where $H_1(x) = \sum_{i=s+1}^{m} b_i x^i$, $s < m$, and $b_s \in Q$. Since $G(x)$ and $H(x)$ are different and both of order s, $\deg(H(x) - G(x)) \ge s$. Thus,

$$\deg(H(x) - G(x)) = \deg_x(H_1(x) + zx^s - G(x)).$$

Since $G(x)$ is chosen such that $\deg(F(x, G(x))) = t$ is minimal, $\deg(F(x, H(x))) \ge t$.

Hence,

$$t \le \deg(F(x, H(x))) < \deg_x(F(x, H_1(x) + zx^s)).$$

This implies that

$$\deg_x(F(x, H_1(x) + zx^s)) = \deg_x(F_1(x, H_1(x) + zx^s)) + \deg_x(H_1(x) + zx^s - G(x)),$$

and

$$t - \deg_x(H_1(x) + zx^s - G(x)) < \deg_x(F_1(x, H_1(x) + zx^s)).$$

Now, we have two possible cases.

Case 1: $\deg((H(x) - G(x)) + \deg(F_1(x, H(x))) < t$. Then

$$\begin{aligned}\deg(F_1(x, H(x))) < t - \deg(H(x) - G(x)) &= t - \deg_x(H_1(x) + zx^s - G(x)) \\ &< \deg_x(F_1(x, H_1(x) + zx^s)).\end{aligned}$$

Thus, $H(x)$ is an approximate solution of $F_1(x, y)$.

Case 2: $\deg((H(x) - G(x)) + \deg(F_1(x, H(x))) \ge t$. Then

$$\begin{aligned}\deg(F(x, H(x)) &= \deg(H(x) - G(x)) + \deg(F_1(x, H(x))) \\ &< \deg_x(F(x, H_1(x) + zx^s)) \\ &= \deg_x(H_1(x) + zx^s - G(x)) + \deg_x(F_1(x, H_1(x) + zx^s)).\end{aligned}$$

Then, $\deg(F_1(x, H(x))) < \deg_x(F_1(x, H_1(x)+zx^s))$ and $H(x)$ is an approximate solution of $F_1(x, y)$ too.

By the induction hypothesis, $F_1(x, y)$ has at most n different approximate solutions of order s. Therefore, the number of elements of S is at most $n + 1$. □

3. Algorithm

In this section we shall present a polynomial time algorithm called FACTOR which finds the unique polynomial $g(\bar{x})$ for the first case, or all $g_i(\bar{x})$ for the second case of Theorem 2.5. Hence, given a polynomial $F(\bar{x}, y)$ over Q, FACTOR finds all possible polynomials $g(\bar{x})$ such that $F(\bar{x}, g(\bar{x})) \in Q$, *even if the constant term of* $F(\bar{x}, y)$ *is not known.* This is so formulated since the constant term is allowed here to vary. This happens while studying the decision problem of determining whether

$$\exists z \forall x_1 \cdots \forall x_n \exists y \; f(x_1, \ldots, x_n, y) = z$$

is true over Z for an arbitrary polynomial $f(x_1, \ldots, x_n, y)$ over Q (Tung, unpublished).

In our algorithm, a polynomial $g(x) = \sum_{i=0}^{n} a_i x^i$ is represented by a sequence of numbers $\langle a_n, a_{n-1}, \ldots, a_0 \rangle$. This implies we input or output a polynomial in dense form. If a polynomial is not input in dense form, there is no polynomial time algorithm to factor an arbitrarily given polynomial. Elements of sets in this algorithm are listed in stack structure (Aho *et al.*, 1974). Thus, elements in a set will be chosen on a first-in, last-out basis.

To simplify the proof, we demonstrate the case of a polynomial with two variables first.

FACTOR

Input: Polynomial $F(x, y) \in Q[x, y]$.

Output: $g(x) = \sum_{i>0} \alpha_i x^i$ if $F(x,y) = \sum_{k=0}^{s} \beta_k (y - g(x))^k$ where $\beta_k \in Q$, otherwise, all $g_i(x) \in Q[x], 0 \leq i \leq n$, such that $F(x, g_i(x)) \in Q$.
Method: Step 1. Let $F(x,y) = \sum_{k=0}^{s} f_k(x) y^k = \sum_{k=0}^{s} \bigl(\sum_{l=0}^{t_k} b_{k,l} x^l\bigr) y^k$. Find a positive integer m such that $sm + t_s \geq km + t_k$ for $0 \leq k < s$. From Proposition 2.6, we may simply let m be the maximum of t_k for $0 \leq k < s$. Also, create two empty stacks S and T.

Step 2. Substitute y of $F(x,y)$ with zx^m where z is an indeterminant, and obtain that $F(x, zx^m) = \bar{F}(z,x)$. Let the polynomial $f_m(z)$ be the leading term of $\bar{F}(z,x)$ with respect to x, i.e. the coefficient term of the highest power of x in $\bar{F}(z,x)$. Solve the equation $f_m(z) = 0$ over Q by factoring $f_m(z)$ over Q with the algorithm (Lenstra *et al.*, 1982). Let S be the set of all distinct solutions of $f_m(z) = 0$. Each element of S is viewed as a one element sequence.

Step 3. Take the first sequence $L = \langle \alpha_m, \ldots, \alpha_l \rangle$ in S, and eliminate it from S. Then, substitute y of $F(x,y)$ with $\bigl(\sum_{i=l}^{m} \alpha_i x^i\bigr) + zx^{l-1}$ where z is an indeterminant, and obtain that

$$F\left(x, \left(\sum_{i=l}^{m} \alpha_i x^i\right) + zx^{l-1}\right) = \bar{F}_{l-1}(z,x).$$

Let $f_{l-1}(z)$ be the leading term of $\bar{F}_{l-1}(z,x)$ with respect to x. Solve the equation $f_{l-1}(z) = 0$ in Q and let $\{\beta_1, \ldots, \beta_r\}$ be the set of all distinct solutions. For every k, $1 \leq k \leq r$, check whether $F(x, \bigl(\sum_{i=l}^{m} \alpha_i x^i\bigr) + \beta_k x^{l-1})$ is a constant or not. If it is equal to a constant, put $\langle \alpha_m, \ldots, \alpha_l, \beta_k \rangle$ in T and go to step 4. Otherwise, put $\langle \alpha_m, \ldots, \alpha_l, \beta_k \rangle$ in S. However, if $l = 1$ and $F(x, \bigl(\sum_{i=1}^{m} \alpha_i x^i\bigr) + \beta_k)$ is not a constant, then omit this sequence. If $f_{l-1}(z) = 0$ is not solvable in Q, then simply eliminate the sequence L from S. After we finish this step with L, go back to Step 3 again until S is empty and output T.

Step 4. Let $G(x)$ be the corresponding polynomial in T, factor $F(x,y) - F(x, G(x))$ over Q with the algorithm in Lenstra (1987). Note that $F(x, G(x))$ is identically equal to a constant. If $F(x,y) - F(x,G(x))$ has factors of the form $y - G_k(x)$, $1 \leq k \leq r$, then include all such $G_k(x)$ in T too. If there are two polynomials $g(x)$ and $h(x)$ in T such that $g(x) - h(x)$ is not a constant, then output T and stop. Otherwise, go to Step 5.

Step 5. Choose a sequence $L = \langle \alpha_m, \ldots, \alpha_0 \rangle$ in T. (Here, α_0 may equal 0.) Substitute y of $F(x,y)$ with $\bigl(\sum_{i=1}^{m} \alpha_i x^i\bigr) + z$ where z is an indeterminant, and obtain that

$$F\left(X, \left(\sum_{i=1}^{m} \alpha_i x^i\right) + Z\right) = \bar{F}_0(z,x).$$

If $\bar{F}_0(z,x) \in Q[z]$, let $T = \{\langle \alpha_m, \ldots, \alpha_1 \rangle\}$ be the output and $F(x,y) = \sum_{j=0}^{n} c_j (y - g(x))^j$ where $g(x) = \sum_{i=1}^{m} \alpha_i x^i$ and $c_j \in Q$. Suppose that $\bar{F}_0(z,x)$ is not in $Q[z]$. Let $f_0(z)$ be the leading term of $\bar{F}_0(z,x)$ with respect to x. Solve the equation $f_0(z) = 0$ in Q and let $\{\beta_1, \ldots, \beta_r\}$ be the set of all distinct solutions. For every k, $1 \leq k \leq r$, check whether $F(x, \bigl(\sum_{i=1}^{m} \alpha_i x^i\bigr) + \beta_k)$ is a constant or not. If it is equal to a constant, put $\langle \alpha_m, \ldots, \alpha_1, \beta_k \rangle$ in T. Otherwise, simply omit the sequence $\langle \alpha_m, \ldots, \alpha_1, \beta_k \rangle$. Finally, output T and stop.

THEOREM 3.1. *Algorithm FACTOR is correct and in polynomial time.*

Proof. We first show that this algorithm is correct.

Step 1. If $F(x, g(x)) \equiv c$, then $g(x)$ is an approximate solution. By Proposition 2.6, $\deg(g(x)) \le m$.

Step 2. Substitute y of $F(x, y)$ with $G(x) = \sum_{i=0}^{m} c_i x^i$ where c_i are indeterminants. By our choice of m,

$$\begin{aligned}\deg_x\left(F\left(x, \sum_{i=0}^{m} c_i x^i\right)\right) &= \deg_x\left(\sum_{k=0}^{s}\left(f_k(x)\left(\sum_{i=0}^{m} c_i x^i\right)^k\right)\right)\\ &= \deg_x\left(\sum_{k=0}^{s}(f_k(x)(c_m x^m)^k)\right)\\ &= \deg_x(F(x, zx^m))\\ &= sm + t_s.\end{aligned}$$

We write that

$$F\left(x, \sum_{i=0}^{m} c_i x^i\right) = \bar{G}(c_m, \ldots, c_0, x) = \sum_{j=0}^{t} g_j(c_m, \ldots, c_0) x^j$$

for some t. Thus, $\deg_x(\bar{G}(c_m, \ldots, c_0, x)) = \deg_x(\bar{F}(z, x)) = t$. Let polynomial g_t $(c_m, \ldots, c_0)$ be the leading term of $\bar{G}(c_m, \ldots, c_0, x)$ with respect to x, which has only one variable c_m; hence, $f_m(z) \equiv g_t(z)$.

For any polynomial $h(x) = \sum_{r=0}^{m} b_r x^r$ over Q, $\deg(F(x, h(x))) < t$ if and only if $g_t(b_m) = 0$. Thus, we can obtain all the possible values of a_m such that $F\left(x, \sum_{i=0}^{m} a_i x^i\right) \in Q$ by solving $f_m(z) = 0$ over Q. Since $\deg(f_m(z))$ =s=$\deg_y(F(x, y))$, the number of distinct solutions of $f_m(z) = 0$ is less than or equal to $\deg_y(F(x, y))$.

Step 3. It is easy to see that if $g(x)$ is in T, then $F(x, g(x)) \in Q$. We want to prove that if there exist polynomials $g(x) \in Q[x]$ such that $F(x, g(x)) \in Q$, then with Step 3 of FACTOR we shall find one such polynomial. To avoid the complication of the indices, we demonstrate the case where there are only two distinct polynomials $U(x) = \sum_{i=0}^{m} u_i x^i$ and $V(x) = \sum_{i=0}^{m} v_i x^i$ over Q such that $F(x, U(x)) \equiv d_1 \in Q$ and $F(x, V(x)) \equiv d_2 \in Q$, respectively. This should suffice to convince the reader that the general case also holds true.

There are two possible cases, either $d_1 = d_2$ or $d_1 \neq d_2$. We demonstrate the case $d_1 = d_2$ first. If $d_1 = d_2$, then

$$F(x, y) = (y - U(x))(y - V(x))H(x, y) + d_1$$

for a polynomial $H(x, y) = \sum_{k=0}^{s-2} h_k(x) y^k$ over Q and

$$F\left(x, \sum_{i=0}^{m} c_i x^i\right) = \left(\sum_{i=0}^{m}(c_i - u_i)x^i\right)\left(\sum_{i=0}^{m}(c_i - v_i)x^i\right)H\left(x, \sum_{i=0}^{m} c_i x^i\right) + d_1.$$

Note that

$$\deg_x\left(H\left(x, \sum_{i=0}^{m} c_i x^i\right)\right) = \deg_x\left(\sum_{k=0}^{s-2}\left(h_k(x)\left(\sum_{i=0}^{m} c_i x^i\right)^k\right)\right)$$

$$= \deg_x\left(\sum_{k=0}^{s-2}(h_k(x)(c_m x^m)^k)\right)$$
$$= \deg_x(H(x, zx^m)).$$

The leading term $g_t(c_m) = f_m(c_m)$ of $F\bigl(x, \sum_{i=0}^m c_i x^i\bigr)$ is $(c_m - u_m)(c_m - v_m)F_m(c_m)$ where $F_m(c_m)$ is the leading term of $H\bigl(x, \sum_{i=0}^m c_i x^i\bigr)$. Therefore, u_m and v_m will be the solutions of equation $f_m(z) = 0$ as discussed in the proof of above step. If $u_m \neq v_m$ and $F_m(u_m) \neq 0$, then let

$$F(x, u_m x^m + zx^{m-1}) = \bar{F}_{m-1}(z, x).$$

Let $f_{m-1}(z)$ be the leading term of $\bar{F}_{m-1}(z, x)$ with respect to x, then

$$f_{m-1}(z) = (z - u_{m-1})(u_m - v_m)(F_m(u_m)).$$

Also,

$$g_{t-1}(u_m, c_{m-1}, \ldots, c_0) = (c_{m-1} - u_{m-1})(u_m - v_m)(F_m(u_m)).$$

Hence, $f_{m-1}(z) = g_{t-1}(z)$. We may obtain the value of u_{m-1} by factoring the polynomial $f_{m-1}(z)$. Then, with the procedure of FACTOR we may obtain the values of the remaining u_i for $0 \leq i \leq m-2$. This is also the case for the values of v_i, $0 \leq i < m$, if $F_m(v_m) \neq 0$.

Suppose that $u_m \neq v_m$ but $F_m(u_m) = 0$, then $g_{t-1}(u_m, c_{m-1}, \ldots, c_0) \equiv 0$. It may happen that $g_{t-k}(u_m, c_{m-1}, \ldots, c_0) \equiv 0$ for $1 \leq k \leq r$ and $r > 1$. However, as soon as we reach the term that $g_{t-k-1}(u_m, c_{m-1}, \ldots, c_0) \not\equiv 0$ then

$$g_{t-k-1}(u_m, c_{m-1}, \ldots, c_0) = (c_{m-1} - u_{m-1})(u_m - v_m)H(u_m, c_{m-1}, \ldots, c_0)$$

where $H(u_m, c_{m-1}, \ldots, c_0) \not\equiv 0$. Similarly,

$$\begin{aligned}\deg_x\left(H\left(x, u_m x^m + \sum_{i=0}^{m-1} c_i x^i\right)\right) &= \deg_x\left(\sum_{k=0}^{s-2}\left(h_k(x)\left(u_m x^m + \sum_{i=0}^{m-1} c_i x^i\right)^k\right)\right)\\ &= \deg_x\left(\sum_{k=0}^{s-2}(h_k(x)(u_m x^m + c_{m-1}x^{m-1})^k)\right)\\ &= \deg_x(H(x, u_m x^m + zx^{m-1})).\end{aligned}$$

Hence, $f_{m-1}(z) = g_{t-k-1}(z)$. We may obtain the value u_{m-1} by solving the equation $f_{m-1}(z) = 0$. Note that in this case $f_{m-1}(z) = 0$ may have more than one solution, because $H(u_m, \beta, \ldots, c_0)$ might be identically equal to 0 for some $\beta \in Q$. Then, sequence $\langle \alpha_m, \beta \rangle$ will be checked to see whether it should be put in T or in S, or simply omitted according to Step 3 of FACTOR.

Now, assume that $u_m = v_m$, then $g_{t-1}(u_m, c_{m-1}, \ldots, c_0) \equiv 0$. Like the case above where $F_m(u_m) = 0$, the leading term which is not identically equal to zero will be in the form

$$(c_{m-1} - u_{m-1})(c_{m-1} - v_{m-1})H(u_m, c_{m-1}, \ldots, c_0),$$

which is equal to $f_{m-1}(c_{m-1})$. Thus, u_{m-1} and v_{m-1} will be obtained by solving the equation $f_{m-1}(z) = 0$. Similarly, we may have solutions other than u_{m-1} and v_{m-1}, and we proceed as described in Step 3 of FACTOR. With the same reasoning, we may obtain the remaining values of u_i and v_i by FACTOR.

We now prove the case where $d_1 \neq d_2$. By Proposition 2.1 (or Theorem 2.3 for the more general cases),

$$F(x,y) = (y - U(x)) \cdot [(y - U(x) - d)G(x,y) + (d_1 - d_2)/d] + d_1$$

for a $G(x,y) \in Q[x,y]$ and a $d \in Q$. The proof of this case is similar to the proof of the previous case where $u_m = v_m$. Let $U(x) = \sum_{i=0}^m u_i x^i$, then

$$F\left(x, \sum_{i=0}^m c_i x^i\right) = \left(\sum_{i=0}^m (c_i - u_i) x^i\right) \left[\left(\sum_{i=0}^m (c_i - u_i) x^i - d\right) G\left(x, \sum_{i=0}^m c_i x^i\right) + (d_1 - d_2)/d\right] + d_1.$$

The value of u_m is obtained by solving $f_m(z) = 0$. Next, assume that sequence $\langle u_m, \ldots, u_l \rangle$ is obtained. Let $H(x) = \sum_{i=0}^m a_i x^i$ where $a_i = u_i$ for $i \geq l$ and $a_i = c_i$ for $i < l$. Then the leading term of $F(x, H(x))$ is equal to $f_{j-k}(c_{l-1})$ which must have a factor $c_{l-1} - u_{l-1}$. Thus, we shall obtain the value of u_{l-1} by solving $f_{j-k}(z) = 0$ over Q. Therefore, we may obtain the approximate solution of $F(x,y)$ successively with the algorithm FACTOR. Hence, if there exists an a polynomial $g(x)$ such that $F(x, g(x)) \in Q$, we shall get one such polynomial at the end of Step 3.

Once we get a polynomial $G(x)$ such that $F(x, G(x)) \in Q$, i.e. $G(x) \in T$, then two possible cases of $F(x,y)$ described in Theorem 2.5 are handled by Steps 4 and 5, respectively.

At first sight, one may feel that we may repeat Step 3 until all the sequences L in S has reached to $l = 0$. Then each sequence L in S corresponds to a solution. Thus, we may omit Steps 4 and 5. However, in this way we shall miss some solutions. For example, let

$$F(x,y) = (y - x^2)(y - x^2 - x)(x^2 + y^2) + 3.$$

Step 3 will give us the sequence $L = \langle 1, 0, 0 \rangle$ (corresponding to x^2), but we shall not be able to get the sequence $L = \langle 1, 1, 0 \rangle$ (corresponding to $x^2 + x$).

Case 1. There are two polynomials $g(x)$ and $h(x)$ over Q such that $F(x, g(x)) \in Q$, $F(x, h(x)) \in Q$, and $g(x) - h(x)$ is not in Q. This is handled with Step 4.

By Lemma 2.2, $F(x, g_i(x)) \in Q$ for every i, $1 \leq i \leq m$, if and only if $F(x,y) = \left[\prod_{i=1}^m (y - g_i(x))\right] \cdot G(x,y) + c$ for a $c \in Q$ and a $G(x,y) \in Q[x,y]$. Thus, $G(x) = g_i(x)$ for some i, and $F(x, G(x)) = c$. Hence, we shall get all $g_i(x)$, $1 \leq i \leq m$, such that $F(x, g_i(x)) = c$ by finding the factors of $F(x,y) - F(x, G(x))$ which are in the form $y - g_i(x)$.

Case 2. For any two polynomials $g(x)$ and $h(x)$ over Q, if $F(x, g(x)) \in Q$ and $F(x, h(x)) \in Q$, then $g(x) - h(x)$ is in Q. This is handled with Step 5.

Assume that $F(x,y)$ is in this case. Now, there may be more than one sequence in T obtained by Step 4. Choose a sequence $L = \langle \alpha_m, \ldots, \alpha_0 \rangle$ in T. (Here, α_0 may equal 0.) Let $G(x) = \sum_{i=1}^m \alpha_i x^i$. Note that for any polynomial $h(x) \in Q[x]$, if $F(x, h(x)) \in Q$, then $h(x) = G(x) + c$ for a $c \in Q$. Substitute y of $F(x,y)$ with $\left(\sum_{i=1}^m \alpha_i x^i\right) + z$ where z is an indeterminant, and obtain that

$$F\left(x, \left(\sum_{i=1}^m \alpha_i x^i\right) + z\right) = \bar{F}_0(z, x).$$

If $\bar{F}_0(z,x) \equiv \bar{F}_0(z) \in Q[z]$, then $F(x, G(x) + a)) = \bar{F}_0(a) \in Q$ for any $a \in Q$. Thus, $F(x,y) = \sum_{j=0}^n c_j (y - G(x))^j$ where $c_j \in Q$ by Theorem 2.5 (or Lemma 2.4). Therefore, let $T = \{\langle \alpha_m, \ldots, \alpha_1 \rangle\}$ be the output. Now, assume that $\bar{F}_0(z,x)$ is not in $Q[z]$. Note that for any polynomial $h(x) \in Q[x]$, if $F(x, h(x)) \in Q$, then $h(x) = G(x) + c$ for a $c \in Q$. Hence, if $F(x, h(x)) \in Q$, then $h(x) = G(x) + \beta_k$ for a k, $1 \leq k \leq r$. Therefore, $F(x, h(x)) \in Q$ if and only if $h(x) \in T$. This finishes our proof of correctness.

Polynomials over Q can be factored in polynomial time (Lenstra *et al.*, 1982; Lenstra, 1984; Kaltofen, 1985). It is easy to see that each step can be carried out in polynomial time. In the process of FACTOR, there may exist zero sequences in S, that is sequences in the form $\langle 0, \dots, 0\rangle$ for i consecutive zeros where $1 \leq i \leq m+1$. There are at most $m+1$ such sequences. Except the zero sequences, all the polynomials in S during the process of FACTOR are approximate solutions of $F(x,y)$. The order of each approximate solution is less than or equal to $m \leq \deg_x(F(x,y))$ by Proposition 2.6. Also, at each order there are at most $s = \deg_y(F(x,y))$ distinct approximate solutions by Theorem 2.7. Thus, the total number of elements having appeared in S, including those eliminated, is less than or equal to $(s+1)(m+1)$. This means that Step 3 runs at most $(s+1)(m+1)$ times. It follows that FACTOR is in polynomial time. □

If $F(x,y) = f_1(x)y - f_0(x)$, i.e. $\deg_y(F(x,y)) = 1$, then the coefficients $\alpha_m, \dots, \alpha_0$ found successively by Step 3 in the algorithm FACTOR are just the coefficients found successively with the usual division algorithm of $f_0(x)$ by $f_1(x)$. If the output of the algorithm FACTOR is $\sum_{i=0}^{m} \alpha_i x^i$, then it means that

$$f_0(x) = f_1(x) \cdot \left(\sum_{i=0}^{m} \alpha_i x^i\right) + c$$

where $c \in Q$. We may say that the algorithm FACTOR is an extension of the division algorithm.

Next, we extend the algorithm FACTOR to polynomials with more than two variables. We need to introduce a modified Kronecker substitution.

Definition. (Schinzel, 1982) If $F(x_1, x_2, \dots, x_n)$ is a polynomial over Q, and $d > \deg_{x_i}(F(\bar{x}))$ for each i, then $S_d : F \longrightarrow F(x, x^d, x^{d^2}, \dots, x^{d^{n-1}})$ is called a Kronecker substitution. Similarly, if $F(x_1, x_2, \dots, x_n, y)$ is a polynomial over Q, and $d > \deg_{x_i}$ $(F(\bar{x}, y))$ for each i, then $T_d : F \longrightarrow F(x, x^d, x^{d^2}, \dots, x^{d^{n-1}}, y)$ is called a modified Kronecker substitution.

It is easy to see that $T_d(y - h(\bar{x})) = y - S_d(h(\bar{x}))$. It is known that if $d > \deg_{x_i}(F(\bar{x}) \cdot G(\bar{x}))$ for each i, then $S_d(F \cdot G) = S_d(F) \cdot S_d(G)$. We also have that if $d > \deg_{x_i}(F(\bar{x}, y) \cdot G(\bar{x}, y))$ for each i, then $T_d(F \cdot G) = T_d(F) \cdot T_d(G)$.

Lemma 3.2. (Schinzel, 1982) *If $F_0[x] \in Q[x]$ satisfies deg$(F_0) \leq d^{n-1}$, then there exists a unique $F \in Q[x_1, \dots, x_n]$ with* $\deg_{x_i} F(\bar{x}) < d$ *such that* $S_d(F) = F_0$.

We may call the procedure of finding F from F_0 such that $S_d(F) = F_0$ an inverse Kronecker substitution, and write that $S_d^{-1}(F_0) = F$. We can define the inverse modified Kronecker substitution T_d^{-1} similarly. Since polynomials are input in dense form and n is fixed, the Kronecker substitution and modified Kronecker substitution are in polynomial time. Also, the input length of $H(x,y) = T_d(F(\bar{x}, y))$ is polynomially bounded by the input length of the original $F(\bar{x}, y)$. From the proof of above lemma in Schinzel (1982) we can see that inverse Kronecker substitution can be performed in polynomial time too. We then have the following lemma.

Lemma 3.3. *The Kronecker substitution S_d, inverse Kronecker substitution S_d^{-1}, modified Kronecker substitution T_d, and inverse modified Kronecker substitution T_d^{-1} are all in polynomial time.*

Now, we are ready to prove our final theorem.

Theorem 3.4. *There is a polynomial time algorithm which, given $f(\bar{x}, y) = \sum_{k=0}^{s} f_k(\bar{x})$ $y^k \in Q[\bar{x}, y]$, determines whether or not there is a unique $g(\bar{x}) \in Q[\bar{x}]$, with its constant term equal to 0, such that $f(\bar{x}, y) = \sum_{i=0}^{s} c_i(y - g(\bar{x}))^i$ for some $c_i \in Q$. If this is the case, then the polynomial $g(\bar{x})$ can be found in polynomial time. If it is not the case, then in polynomial time the algorithm finds all polynomials $\{g_1(\bar{x}), \ldots, g_t(\bar{x})\}$, $t \leq s$, such that $g_i(\bar{x}) \in Q[\bar{x}]$ and $f(\bar{x}, g_i(\bar{x})) \in Q$ for $1 \leq i \leq t$.*

Proof. Let $f(\bar{x}, y) = \sum_{k=0}^{s} f_k(x_1, \ldots, x_n)y^k$, and d be the maximum of $\deg_{x_j}(f_k(\bar{x}, y)) + 1$ for $1 \leq j \leq n$ and $0 \leq k \leq s$. We apply modified Kronecker substitution T_d on $f(\bar{x}, y)$ and let $F(x, y) = T_d(f(\bar{x}, y))$. We apply FACTOR on $F(x, y)$ and let T be the output of FACTOR. For each $g(x)$ in T, $\deg(g(x)) \leq d^n$ by Proposition 2.6. Hence, $S_d^{-1}(g(x))$ is well defined. Let $T' = \{S_d^{-1}(g(x)) : g(x) \in T\}$ be the output.

Since FACTOR is in polynomial time, with Lemma 3.3, this algorithm is in polynomial time. Now, we prove this algorithm is correct. We first prove that if $G(\bar{x}) \in T'$, then $f(\bar{x}, G(\bar{x}))$ is in Q. Let $G(\bar{x}) = S_d^{-1}(g(x))$ for a $g(x)$ in T. If $g(x) \in T$, then $F(x, y) - c = (y - g(x)) \cdot h(x, y)$ for some $c \in Q$ and some $h(x, y) \in Q[x, y]$. Then

$$\begin{aligned} f(\bar{x}, y) - c &= T_d^{-1}(F(x, y)) - c \\ &= T_d^{-1}(F(x, y) - c) \\ &= T_d^{-1}((y - g(x)) \cdot h(x, y)) \\ &= T_d^{-1}(y - g(x)) \cdot T_d^{-1}(h(x, y)) \\ &= (y - S_d^{-1}(g(x))) \cdot H(\bar{x}, y) \end{aligned}$$

for some $H(\bar{x}, y)$ over Q. Hence, $f(\bar{x}, S_d^{-1}(g(x))) = f(\bar{x}, G(\bar{x})) = c \in Q$.

Conversely, we need to prove that if $f(\bar{x}, G(\bar{x}))$ is in Q, then $G(\bar{x}) \in T'$. Assume that $f(\bar{x}, G(\bar{x})) = c$ for a c in Q. Then $f(\bar{x}, y) - c = (y - G(\bar{x})) \cdot H(\bar{x}, y)$ for some $H(\bar{x}, y)$ in $Q[\bar{x}, y]$. Let $S_d(G(\bar{x})) = g(x)$ and $T_d(H(\bar{x}, y)) = h(x, y)$. Then,

$$\begin{aligned} F(x, y) - c &= T_d(f(\bar{x}, y)) - c \\ &= T_d(f(\bar{x}, y) - c) \\ &= T_d((y - G(\bar{x})) \cdot H(\bar{x}, y)) \\ &= T_d((y - G(\bar{x})) \cdot T_d(H(\bar{x}, y)) \\ &= (y - S_d(G(\bar{x}))) \cdot T_d(H(\bar{x}, y)) \\ &= (y - g(x)) \cdot h(x, y). \end{aligned}$$

Hence, $F(x, g(x)) = c$ and $g(x)$ is in T. This implies that $G(\bar{x}) = S_d^{-1}(g(x))$ is in T'. □

Finally, we use an example to illustrate the algorithm FACTOR.

Example. Let $f(x, y) = 4y^2 - 4x^3y - 4x^2y + 8xy + 6y + x^6 + 2x^5 - 3x^4 - 7x^3 + 7x + k$ where k is an unknown constant. Then $m = 3$; substitute $y = zx^3$ in $f(x, y)$ and let

$f(x, zx^3) = F_3(z, x)$. Let $f_3(z)$ be the leading term of $F_3(z, x)$. Then, $f_3(z) = 4z^2 - 4z + 1$. Solving $f_3(z) = 0$, we obtain that $z = 1/2$ with multiplicity 2.

Substitute $y = x^3/2 + zx^2$ in $f(x, y)$ and let $f(x, x^3 + zx^2) = F_2(z, x)$. Let $f_2(z)$ be the leading term of $F_2(z, x)$. Then $f_2(z) = 4z^2 - 4z + 1$. Solving $4z^2 - 4z + 1 = 0$, we obtain that $z = 1/2$ with multiplicity 2.

Substitute $y = (x^3 + x^2)/2 + z$ in $f(x, y)$ and let $f(x, (x^3 + x^2)/2 + z) = F_1(z, x)$. Let $f_1(z)$ be the leading term of $F_1(z, x)$. Then $f_1(z) = 4z^2 + 8z + 3$. Solving $4z^2 + 8z + 3 = 0$, we obtain that $z = -3/2, -1/2$.

Substitute $y = (x^3 + x^2 - 3x)/2 + z$ in $f(x, y)$ and let $f(x, (x^3 + x^2 - 3x)/2 + z) = F_0(z, x)$. Let $f_0(z)$ be the leading term of $F_0(z, x)$. Then $f_0(z) = -4z - 2$, we obtain that $z = -1/2$.

Substitute $y = (x^3 + x^2 - x)/2 + z$ in $f(x, y)$ and let $f(x, (x^3 + x^2 - x)/2 + z) = G_0(z, x)$. Let $g_0(z)$ be the leading term of $G_0(z, x)$. Then $f_0(z) = 4z + 4$, we obtain that $z = -1$. Therefore,

$$\begin{aligned} f(x, y) &= 4y^2 - 4x^3y - 4x^2y + 8xy + 6y + x^6 + 2x^5 - 3x^4 - 7x^3 + 7x + k \\ &= 4(y - (x^3 - x^2 + 3x + 1)/2)(y - (x^3 - x^2 + x + 2)/2) - 2 + k \\ &= (2y - x^3 - x^2 + 3x + 1)(2y - x^3 - x^2 + x + 2) - 2 + k. \end{aligned}$$

Now, if x is an odd integer, $x^3 + x^2 - 3x - 1$ is even, then $y = (x^3 + x^2 - 3x - 1)/2$ is in Z and $f(x, y) = k - 2$. If x is an even integer, $x^3 + x^2 - x - 2$ is even, then $y = (x^3 + x^2 - x - 2)/2$ is in Z and $f(x, y) = k - 2$. Thus, $\exists z \forall x \exists y f(x, y) = z$ is true in Z by taking $z = k - 2$.

Acknowledgements

The author would like to thank an unknown referee, who pointed out a mistake in the previous version of this paper. This work is supported by a grant from the National Science Council of the Republic of China.

References

Aho, A. V., Hopcroft, J. E., Ullman, J. D. (1974). *The Design and Analysis of Computer Algorithms*. Reading, MA, Addison-Wesley.

Chistov, A. L. (1986). Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time. *J. Sov. Math.*, **34**, 1838–1882.

Dean, R. A. (1990). *Classical Abstract Algebra*. New York, Harper and Row.

Kaltofen, E. (1985). Polynomial-time reductions from multivariate to bi- and uni-variate integral polynomial factorization. *SIAM J. Comput.*, **14**, 469–489.

Lenstra, A. K. (1984). Factoring multivariate integral polynomials. *Theor. Comput. Sci.*, **34**, 207–213.

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

Lenstra, A. K., Lenstra, H. W. Jr, Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math. Ann.*, **261**, 515–534.

Schinzel, A. (1982). Diophantine equations with parameters. In Arimitage, J. V. ed., *Journées Arithmetiques 1980*, Volume 56 of London Mathematical Society Lecture Note Series, pp. 211–217. Cambridge, Cambridge University Press.

Schinzel, A. (1982). *Selected Topics on Polynomials*. Ann Arbor, MI, The University of Michigan Press.

Tung, S. P. (1985). On weak number theories. *Japan. J. Math.*, **11**, 203–232.

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

Tung, S. P. *Computational Complexities of Diophantine Inequalities*, manuscript.

Received 22 April 1999
Accepted 29 September 2001