ACTA ARITHMETICA
123.2 (2006)

Near solutions of polynomial equations

by

Shih Ping Tung (Chung Li)

1. Introduction. Let K be a field and $K[x]$ be the polynomial ring over K. Given a polynomial $f(y)$ with coefficients in $K[x]$, we may ask what the solutions of $f(y) = 0$ are in $K[x]$. Moreover, is there a notion of "near solution", which includes the usual solution as a special case? This is what we are dealing with in this paper.

Let $F(x, y)$ be a polynomial over K and m be a nonnegative integer. We call a polynomial $g(x)$ over K an *m-near solution* of $F(x, y)$ if there exists a $c \in K$ such that $F(x, g(x)) = cx^m$; then c is called the *m-value* of $F(x, y)$ corresponding to $g(x)$. In particular, c can be zero. Now we view $F(x, y)$ as a polynomial over $K[x]$ with variable y, and denote it as $\overline{F}(y)$. Then every solution of $\overline{F}(y) = 0$ in $K[x]$ is also an m-near solution of $F(x, y)$ with m-value 0. Thus, the definition of m-near solution extends the usual definition of solutions of polynomial equations.

We can also consider this problem from another point of view. Given a polynomial $F(x, y) = \sum_{i=0}^{n} f_i(x)y^i$ over K as above, we want to find a solution of $\overline{F}(y) = 0$. In [2], we considered the case where the constant term of $f_0(x)$ is zero. This problem arises from our study of the decision problem of diophantine equations (cf. [2]). Now, we study a more general case. Suppose that the coefficient of the term x^m ($m \geq 0$) in the polynomial $f_0(x)$ is zero; can we still find the solutions of $\overline{F}(y) = 0$? How many solutions of $\overline{F}(y) = 0$ are there? In this paper we will show that except for some special cases, which are given explicitly, the number of possible solutions is still bounded by the degree of $\overline{F}(y) = 0$. In [1] we have considered a related problem over the rational function field; here we only consider the problem over polynomial rings.

The results of this paper are new. They are stated over an arbitrary field K. However, the reader can take this field to be the rational number field $\mathbb{Q}$ or the real number field $\mathbb{R}$. In this way, this author believes that

2000 *Mathematics Subject Classification*: Primary 11C08.
Supported by a grant from the National Science Council of ROC.

the proofs in this paper can be read by any diligent high school student. Many interesting problems remain unanswered in this paper. For example, given a polynomial $F(x, y)$, can we tell whether $F(x, y)$ has an m-near solution or not? Is there a characterization of the polynomials having m-near solutions? May a given polynomial have m-near solutions for different values of m? These surely deserve further studies. In a companion paper we give a polynomial time algorithm to find all the m-near solutions of a given polynomial for a given m if there is a polynomial time algorithm to solve equations of one variable in K.

2. Basic properties of near solutions. We first give the notations used throughout this paper. We will use K to denote a field, and $\mathbb{N}$ the set of all nonnegative integers. The *degree* of a nonzero polynomial $f(x) = \sum_{i=0}^{s} a_i x^i$, written $\deg(f(x))$, is the maximal index n for which $a_n \neq 0$; usually $a_s \neq 0$. The *rank* of $f(x)$, written $\operatorname{rank}(f(x))$, is the minimal index m for which $a_m \neq 0$. For a multivariate polynomial $F(x_1, \ldots, x_n)$, $\deg_{x_i}(F(x_1, \ldots, x_n))$ denotes the degree of $F(x_1, \ldots, x_n)$ in the variable x_i.

Given a polynomial $F(x, y)$ in $K[x, y]$, we may view $F(x, y)$ as an element in $(K[x])[y]$, i.e. a polynomial $\overline{F}(y)$ of one variable y with coefficients in $K[x]$. The equation $\overline{F}(y) = 0$ is solvable in $K[x]$ if and only if there is a $g(x)$ in $K[x]$ such that $\overline{F}(g(x)) = F(x, g(x)) = 0$. We are interested in the situation that $F(x, g(x))$ has only one term, i.e., $F(x, g(x))$ is a monomial.

Now, we give the definition of near solutions of a polynomial.

Definition. Let $F(x, y)$ be a polynomial over K and m be a nonnegative integer. We call a polynomial $g(x)$ over K an *m-near solution* of $F(x, y)$ if there exists a $c \in K$ such that $F(x, g(x)) = cx^m$; then c is called the *m-value* of $F(x, y)$ corresponding to $g(x)$.

Remark 1. The c in the definition of m-near solution can be zero. Thus, for a given polynomial $F(x, y)$ over K if $g(x)$ is a solution of $\overline{F}(y) = 0$ in $K[x]$, then $g(x)$ is also an m-near solution of $F(x, y)$ for any m in $\mathbb{N}$. Thus, over polynomial rings, the m-near solution we defined extends the usual notion of solutions of equations.

Remark 2. In our definition, we consider the near solutions to polynomial rings only. It seems natural to generalize it to rational function fields as in [1]. We will study this generalization elsewhere. As will be shown in the Final Example of this paper, the situation then becomes much more complicated. In particular, the results and proofs of this paper need to be extensively modified. For simplicity, we restrict our attention to polynomial rings in this paper.

Next, we will show some basic properties of m-near solutions.

THEOREM 2.1. *Let $F(x,y)$ be a polynomial over K and m be a nonnegative integer. Let $g_1(x), g_2(x)$ be two m-near solutions of $F(x,y)$ with distinct m-values. Then there exists an $r \in \mathbb{N}$, $0 \le r \le m$, and a $b \in K - \{0\}$ such that $g_1(x) - g_2(x) = bx^r$, i.e., $g_1(x) - g_2(x)$ is a monomial.*

Proof. Suppose that $F(x, g_1(x)) = a_1 x^m$ and $F(x, g_2(x)) = a_2 x^m$ where a_1 and a_2 are distinct elements in K. Then, by the Factor Theorem we may assume that

$$F(x,y) = (y - g_2(x))h(x,y) + a_2 x^m$$

where $h(x,y)$ is a polynomial over K. Hence,

$$F(x, g_1(x)) = (g_1(x) - g_2(x))h(x, g_1(x)) + a_2 x^m = a_1 x^m.$$

Thus, $g_1(x) - g_2(x)$ is a factor of the monomial $(a_1 - a_2)x^m$. This implies that there exists an $r \in \mathbb{N}$, $0 \le r \le m$, and a $b \in K$ such that $g_1(x) - g_2(x) = bx^r$. ∎

COROLLARY 2.2. *Let $F(x,y)$ be a polynomial over K and m be a nonnegative integer. If $F(x,y)$ has at least two different m-values, then the difference between any two distinct m-near solutions of $F(x,y)$ is either a monomial or a binomial.*

Proof. Let $g(x)$ and $h(x)$ be two distinct m-near solutions of $F(x,y)$. If $F(x,g(x)) \neq F(x,h(x))$, then $g(x) - h(x)$ is a monomial by Theorem 2.1. If $F(x,g(x)) = F(x,h(x))$, then by assumption there is another m-near solution $p(x)$ such that $F(x,p(x)) \neq F(x,g(x))$. From Theorem 2.1, $p(x) - g(x)$ and $p(x) - h(x)$ are monomials. It follows that $g(x) - h(x) = (p(x) - h(x)) - (p(x) - g(x))$ is a monomial or a binomial. ∎

REMARK. The assumption in the above corollary that $F(x,y)$ has two different m-values is necessary. This is easily shown by the following example. Let $F(x,y) = (y-x)(y-x^2-x^3)+x^4$. Both x and x^2+x^3 are 4-near solutions of $F(x,y)$. However, $(x^3 + x^2) - x$ is not a monomial or a binomial.

THEOREM 2.3. *Let $F(x,y)$ be a polynomial over K and m be a nonnegative integer. Assume that $F(x,y)$ has more than two distinct m-values. Then there is a nonnegative integer t such that for any two different m-near solutions $g(x)$ and $h(x)$ there is an $\alpha \in K$ such that $g(x) - h(x) = \alpha x^t$.*

Proof. Let $p(x), q(x)$ and $r(x)$ be three m-near solutions of $F(x,y)$ corresponding to three different m-values. By Theorem 2.1, there exist three nonzero elements a_1, a_2, a_3 in K and three nonnegative integers r_1, r_2, r_3 such that $p(x) - q(x) = a_1 x^{r_1}$, $q(x) - r(x) = a_2 x^{r_2}$, and $p(x) - r(x) = a_3 x^{r_3}$. Then

$$p(x) - r(x) = (p(x) - q(x)) + (q(x) - r(x)) = a_1 x^{r_1} + a_2 x^{r_2} = a_3 x^{r_3}.$$

This implies that $r_1 = r_2 = r_3$.

Now, let $g(x)$ and $h(x)$ be two arbitrary m-near solutions of $F(x,y)$. Then the corresponding m-values of $g(x)$ and $h(x)$ must be different from at least two out of the three m-values of $p(x)$, $q(x)$ and $r(x)$. Without loss of generality, we may assume that the m-values of $g(x)$, $p(x)$ and $q(x)$ are all different, and that the m-values of $h(x)$, $p(x)$ and either $q(x)$ or $r(x)$ are all different. Then with the same arguments as above, there exist a and b in K such that $p(x)-g(x)=ax^{r_1}$ and $p(x)-h(x)=bx^{r_1}$. Let $t=r_1$ and $b-a=\alpha$. Then

$$g(x)-h(x)=(p(x)-h(x))-(p(x)-g(x))=bx^t-ax^t=\alpha x^t. \ \blacksquare$$

REMARK. We discussed the cases of a polynomial with more than one m-value above. The case that $F(x,y)$ has exactly one m-value can be easily handled. Let $g_i(x)$, $1\le i\le n$, be arbitrary elements in $K[x]$. They are m-near solutions of $F(x,y)$ with the same m-value $a\in K$ if and only if there is a $G(x,y)\in K[x,y]$ such that

$$F(x,y)=\Big[\prod_{i=1}^{n}(y-g_i(x))\Big]\cdot G(x,y)+ax^m.$$

We will study more general cases in the next section.

3. Presentations of near solutions. Let $f(x)$ be a polynomial over an integral domain D. Let $a_1,\dots,a_n$ be the solutions of the equation $f(x)=0$ in D. Then there exists $g(x)\in D[x]$ such that $f(x)=(\prod_{i=1}^{n}(x-a_i))g(x)$. Do we have a similar presentation for m-near solutions? The answer is "yes". Suppose that $F(x,y)$ has two different m-near solutions. Our next proposition shows that we can use a single formula to represent $F(x,y)$ whether or not the corresponding m-values are the same.

PROPOSITION 3.1. *Let $F(x,y)$, $g_1(x),\dots,g_s(x)$ and $h(x)$ be polynomials over K, $g_i(x)\ne h(x)$, and m be a nonnegative integer. Let $b_1,b_2\in K$. Then $F(x,g_i(x))=b_1x^m$ for $1\le i\le s$ and $F(x,h(x))=b_2x^m$ if and only if there exists a $d\ne 0$ in K, nonnegative integers $t,r_1,\dots,r_s$ with $t+\sum_{i=1}^{s}r_i=m$, a polynomial $f(x,y)$ in $K[x,y]$, and an integer $p>0$ with either $f(x,h(x))\ne 0$ or $f(x,y)=0$ such that*

$$F(x,y)=\Big(\prod_{i=1}^{s}[y-g_i(x)]\Big)\cdot\left[(y-h(x))^pf(x,y)+\frac{b_2-b_1}{d}\,x^t\right]+b_1x^m$$

where $h(x)=g_i(x)+d_ix^{r_i}$ for $b_1\ne b_2$, and $d=\prod_{i=1}^{s}d_i$.

Proof. Assume that $b_1=b_2$. Then $F(x,g_i(x))=F(x,h(x))=b_1x^m$ if and only if

$$F(x,y)=\Big(\prod_{i=1}^{s}[y-g_i(x)]\Big)\cdot[(y-h(x))^pf(x,y)]+b_1x^m$$

as desired. Notice that in this case $p\ge 1$.

Now, we consider the case that $b_1 \neq b_2$. The direction ($\Leftarrow$) is a straightforward check. From the assumption that $F(x, g_i(x)) = b_1 x^m$ for $1 \leq i \leq s$, there is a polynomial $G(x, y)$ such that

$$F(x,y) = \Big(\prod_{i=1}^{s}[y - g_i(x)]\Big) \cdot G(x,y) + b_1 x^m.$$

From Theorem 2.1, there are $r_i \in \mathbb{N}$, $0 \leq r_i \leq m$, and $d_i \in K$ such that $h(x) = g_i(x) + d_i x^{r_i}$. Let $r = \sum_{i=1}^{s} r_i$. Thus,

$$\begin{aligned} F(x,h(x)) &= \prod_{i=1}^{s}[h(x) - g_i(x)] \cdot G(x,h(x)) + b_1 x^m \\ &= \Big(\prod_{i=1}^{s} d_i\Big) x^r \cdot G(x,h(x)) + b_1 x^m = b_2 x^m. \end{aligned}$$

This implies that $G(x,h(x)) = ((b_2 - b_1)/d)x^{m-r}$. If $\deg_y(F(x,y)) = s$, then $G(x,y) = ((b_2 - b_1)/d)x^{m-r}$. Thus, $f(x,y) = 0$ in our presentation of $F(x,y)$. If $\deg_y(F(x,y)) > s$, then

$$G(x,y) = (y - h(x))^p f(x,y) + \frac{b_2 - b_1}{d}\, x^{m-r}$$

where $p > 0$ and $f(x,y) \in K[x,y]$ with $f(x,h(x)) \neq 0$. Now, let $m - r = t$. We then have $h(x) = g_i(x) + d_i x^{r_i}$, and

$$F(x,y) = \Big(\prod_{i=1}^{s}[y - g_i(x)]\Big) \cdot \left[(y - h(x))^p f(x,y) + \frac{b_2 - b_1}{d}\, x^t\right] + b_1 x^m. \ \blacksquare$$

Note that in Proposition 3.1, $f(x,y) = 0$ if and only if $\deg_y(F(x,y)) = s$.

The following lemma concerns polynomials with exactly two distinct m-values. As regards the bound for the number of m-near solutions, these cases are very special. This will be shown later. We, therefore, give their specific representations.

LEMMA 3.2. *Let $F(x,y)$ be a polynomial over K and m be a nonnegative integer. If $F(x,y)$ has exactly two distinct m-values, then one of the following three cases holds*:

CASE 1: *The difference between any two m-near solutions is a monomial. In this case, there is a nonnegative integer t such that the difference between any two m-near solutions is a monomial of degree t. Thus, there is an $h(x)$ and for every m-near solution $g_i(x)$ there is an a_i in K such that $g_i(x) = h(x) + a_i x^t$.*

CASE 2: *Only one of the two m-values has a pair of m-near solutions $g_1(x)$ and $g_2(x)$ such that $g_1(x) - g_2(x)$ is a binomial. In this case, there exist nonnegative integers t, $r_1, \ldots, r_s$ with $t + \sum_{i=1}^{s} r_i = m$, $a_i, b \in K$, a*

polynomial $G(x,y)$ *in* $K[x,y]$ *with either* $G(x,h(x)) \neq 0$ *or* $G(x,y)=0$, *and an integer* $q>0$ *such that*

$$F(x,y)=\Big[\prod_{i=1}^{s}(y-h(x)-a_ix^{r_i})\Big]\cdot[(y-h(x))^qG(x,y)+bx^t]+ax^m$$

where $h(x), h(x)+a_ix^{r_i}$ *for* $1\leq i\leq s$ *are all the* m*-near solutions of* $F(x,y)$.

Case 3: *For each* m*-value there exists a pair of* m*-near solutions whose difference is a binomial. In this case, there exist* $a,b\in K$, $g_i(x)\in K[x]$ *for* $1\leq i\leq 4$, *a polynomial* $G(x,y)$ *in* $K[x,y]$ *with either* $G(x,g_3(x))\neq 0$ *and* $G(x,g_4(x))\neq 0$, *or* $G(x,y)=0$, *and integers* $p,q>0$ *such that*

$$F(x,y)=(y-g_1(x))(y-g_2(x))[(y-g_3(x))^p(y-g_4(x))^q\cdot G(x,y)+bx^t]+ax^m$$

where $g_i(x)$, $1\leq i\leq 4$, *are all the* m*-near solutions of* $F(x,y)$. *Moreover, there is a polynomial* $g(x)$ *over* K, $u,v\in\mathbb{N}$, *and* $a_1,a_2,a_3,a_4\in K$ *such that* $g_1(x)=g(x)+a_1x^u+a_2x^v$, $g_2(x)=g(x)+a_3x^u+a_4x^v$, $g_3(x)=g(x)+a_1x^u+a_4x^v$, *and* $g_4(x)=g(x)+a_3x^u+a_2x^v$.

Proof. Case 1. Let $g(x)$, $h(x)$, $r(x)$ and $s(x)$ be four arbitrary m-near solutions of $F(x,y)$ such that $g(x)-h(x)=ax^p$ and $r(x)-s(x)=bx^q$ where $a,b\in K$. Assume that $p\neq q$. Let $h(x)-r(x)=cx^u$ where $c\in K$. We have

$$g(x)-s(x)=(g(x)-h(x))+(h(x)-r(x))+(r(x)-s(x))=ax^p+cx^u+bx^q.$$

Then $g(x)-s(x)$ being a monomial implies that $ax^p=-cx^u$ or $bx^q=-cx^u$. However, if $ax^p=-cx^u$, then

$$h(x)-s(x)=(h(x)-r(x))+(r(x)-s(x))=cx^u+bx^q$$

is not a monomial. Similarly, if $bx^q=-cx^u$ then $g(x)-r(x)$ is not a monomial. This contradicts the assumption that the difference between any two m-near solutions is a monomial. Hence, $p=q$. This means that there is a nonnegative integer t such that the difference between any two m-near solutions is a monomial of degree t. Let $g_1(x)=h(x)$. Then for every m-near solution $g_i(x)$ there is an a_i in K such that $g_i(x)=h(x)+a_ix^t$.

Case 2. Let c and d be the distinct m-values of $F(x,y)$. Suppose there exist $g_1(x)$ and $g_2(x)$ in $K[x]$ such that $F(x,g_1(x))=F(x,g_2(x))=cx^m$ and $g_1(x)-g_2(x)$ is a binomial, but the m-value d does not have two m-near solutions whose difference is a binomial. We claim that in this case there is exactly one m-near solution corresponding to the m-value d.

Indeed, suppose $h_1(x)$ and $h_2(x)$ are two distinct m-near solutions in $K[x]$ such that

$$F(x,h_1(x))=F(x,h_2(x))=dx^m,$$

but $h_1(x)-h_2(x)$ is not a binomial. From Corollary 2.2, $h_1(x)-h_2(x)$ is a monomial. By Theorem 2.1, there exist $\alpha,\beta,\gamma,\delta$ in K and u,v,p,q in $\mathbb{N}$

such that $h_1(x) - g_1(x) = \alpha x^u$, $h_1(x) - g_2(x) = \beta x^v$, $h_2(x) - g_1(x) = \gamma x^p$, and $h_2(x) - g_2(x) = \delta x^q$. Then

$$g_1(x) - g_2(x) = (g_1(x) - h_1(x)) + (h_1(x) - g_2(x)) = -\alpha x^u + \beta x^v,$$
$$g_1(x) - g_2(x) = (g_1(x) - h_2(x)) + (h_2(x) - g_2(x)) = -\gamma x^p + \delta x^q.$$

Since $g_1(x) - g_2(x)$ is a binomial, it follows that $u \neq v$ and $p \neq q$. Also,

$$h_1(x) - h_2(x) = (h_1(x) - g_1(x)) - (h_2(x) - g_1(x)) = \alpha x^u - \gamma x^p,$$
$$h_1(x) - h_2(x) = (h_1(x) - g_2(x)) - (h_2(x) - g_2(x)) = \beta x^v - \delta x^q.$$

Since $h_1(x) - h_2(x)$ is a monomial, we obtain $u = p$ and $v = q$. Then from the fact that

$$g_1(x) - g_2(x) = -\alpha x^u + \beta x^v = -\gamma x^p + \delta x^q,$$

we have $\alpha = \gamma$ and $\beta = \delta$. Thus, $h_1(x) - h_2(x) = \alpha x^u - \gamma x^p = 0$. This contradicts the assumption that $h_1(x)$ and $h_2(x)$ are distinct and proves our claim.

Now, let $g_1(x), \ldots, g_s(x)$ be the m-near solutions corresponding to the m-value c and $h(x)$ be the only m-near solution corresponding to d. From Proposition 3.1 for every i, $1 \leq i \leq s$, there exist $a_i \in K - \{0\}$ and $r_i \in \mathbb{N}$ such that $g_i(x) - h(x) = a_i x^{r_i}$. Then we may write

$$\begin{aligned} F(x,y) &= \Big(\prod_{i=1}^{s}(y - g_i(x))\Big)[(y - h(x))^q G(x,y) + bx^t] + ax^m \\ &= \Big(\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})\Big)[(y - h(x))^q G(x,y) + bx^t] + ax^m \end{aligned}$$

where $q > 0$, $G(x,y) \in K[x,y]$ with either $G(x,h(x)) \neq 0$ or $G(x,y) = 0$, and $a = c, b \in K$.

Case 3. Let c and d be the distinct m-values of $F(x,y)$. There exist $g_1(x)$ and $g_2(x)$ in $K[x]$ such that $F(x,g_1(x)) = F(x,g_2(x)) = cx^m$ and $g_1(x) - g_2(x)$ is a binomial. Also, there exist $h_1(x)$ and $h_2(x)$ in $K[x]$ such that $F(x,h_1(x)) = F(x,h_2(x)) = dx^m$ and $h_1(x) - h_2(x)$ is also a binomial.

By Theorem 2.1, there exist α, β in K and u, v in $\mathbb{N}$ such that $h_1(x) - g_1(x) = \alpha x^u$ and $h_1(x) - g_2(x) = \beta x^v$. By Theorem 2.1 again, $h_2(x) - g_1(x) = \gamma x^p$ and $h_2(x) - g_2(x) = \delta x^q$ where $\gamma, \delta \in K$ and $p, q \in \mathbb{N}$. Then

$$g_1(x) - g_2(x) = (g_1(x) - h_1(x)) + (h_1(x) - g_2(x)) = -\alpha x^u + \beta x^v,$$
$$g_1(x) - g_2(x) = (g_1(x) - h_2(x)) + (h_2(x) - g_2(x)) = -\gamma x^p + \delta x^q.$$

Since $g_1(x) - g_2(x)$ is a binomial, we infer that $u \neq v$ and $p \neq q$. Also,

$$h_1(x) - h_2(x) = (h_1(x) - g_1(x)) - (h_2(x) - g_1(x)) = \alpha x^u - \gamma x^p,$$
$$h_1(x) - h_2(x) = (h_1(x) - g_2(x)) - (h_2(x) - g_2(x)) = \beta x^v - \delta x^q.$$

These two equalities and $u \neq v$ imply that $\beta x^v = -\gamma x^p$ (and $\alpha x^u = -\delta x^q$), i.e., $h_2(x) - g_1(x) = -\beta x^v$ (and $h_2(x) - g_2(x) = -\alpha x^v$). We see that $h_1(x) + h_2(x) = g_1(x) + g_2(x)$. Hence, once $g_1(x), g_2(x)$ and $h_1(x)$ are given, then $h_2(x)$ is determined. Therefore, there are exactly two m-near solutions corresponding to the m-value d.

By the same arguments, there are exactly two m-near solutions corresponding to the m-value c. This means that $g_1(x), g_2(x), h_1(x)$ and $h_2(x)$ are the only four m-near solutions of $F(x, y)$ for this case. We may write

$$F(x, y) = (y - g_1(x))(y - g_2(x))H(x, y) + cx^m$$

where $H(x, y) \in K[x, y]$. Then

$$\begin{aligned} F(x, h_1(x)) &= (h_1(x) - g_1(x))(h_1(x) - g_2(x))H(x, h_1(x)) + cx^m \\ &= (\alpha x^u)(\beta x^v)H(x, h_1(x)) + cx^m = dx^m \end{aligned}$$

and

$$\begin{aligned} F(x, h_2(x)) &= (h_2(x) - g_1(x))(h_2(x) - g_2(x))H(x, h_2(x)) + cx^m \\ &= (-\beta x^u)(-\alpha x^v)H(x, h_2(x)) + cx^m = dx^m. \end{aligned}$$

Hence,

$$H(x, h_1(x)) = H(x, h_2(x)) = ((d - c)/\alpha\beta)x^{m-u-v}.$$

Therefore,

$$H(x, y) = (y - h_1(x))^p (y - h_2(x))^q G(x, y) + bx^t$$

where $G(x, y) \in K[x, y]$, $p, q \in \mathbb{N}$, $b = (d - c)/\alpha\beta$ and $t = m - u - v$. If $\deg_y(H(x, y)) = 0$, i.e. $H(x, y) = ((d - c)/\alpha\beta)x^{m-u-v}$, then $G(x, y) = 0$ in our representation of $F(x, y)$. If $\deg_y(H(x, y)) = 1$, then $H(x, h_1(x)) = H(x, h_2(x))$ implies that $h_1(x) = h_2(x)$. This contradicts $h_1(x) - h_2(x)$ being a binomial. This means that $\deg_y(F(x, y)) \neq 3$ for this case. If $\deg_y(H(x, y)) > 1$, then there exist $G(x, y) \in K[x, y]$, $a, b \in K$, and positive integers p, q such that

$$F(x, y) = (y - g_1(x))(y - g_2(x))[(y - g_3(x))^p (y - g_4(x))^q \cdot G(x, y) + bx^t] + ax^m$$

where $g_i(x)$, $1 \leq i \leq 4$, are the only four possible m-near solutions of $F(x, y)$. The nonnegative integers p and q in the formula will be zero or nonzero simultaneously. Now, let $g(x) \in K[x]$ and $a_i \in K$ for $1 \leq i \leq 4$ be such that $g_1(x) = g(x) + a_1 x^u + a_2 x^v$ and $g_2(x) = g(x) + a_3 x^u + a_4 x^v$. Then $g_3(x) = g(x) + a_1 x^u + a_4 x^v$ and $g_4(x) = g(x) + a_3 x^u + a_2 x^v$. This completes our proof. ∎

We now give examples for these three cases.

Examples.

Case 1. Let

$$F(x, y) = (y - x)(y - 2x)(y - 3x)[(y - 4x)[(y - 5x) - 3x^3] + 4x^4] + x^7.$$

Then $F(x,x) = F(x,2x) = F(x,3x) = x^7$, $F(x,4x) = 25x^7$, and $F(x,5x) = 25x^7$. It will be seen later that for this case the number of m-near solutions is at most $\deg_y(F(x,y))$. Thus, $x, 2x, 3x, 4x$ and $5x$ are the only m-near solutions of $F(x,y)$.

Case 2. Let

$$F(x,y) = \Big[\prod_{i=1}^{s}(y - g(x) + x^i)\Big] \cdot x^{m-s(s+1)/2} + x^m$$

where $g(x) \in K[x]$ is arbitrary and $m \geq s(s+1)/2$. Here, the polynomial $G(x,y)$ in the presentation of $F(x,y)$ in Lemma 3.2 is equal to 0. Then $F(x, g(x) - x^i) = x^m$ for $1 \leq i \leq s$. Also,

$$F(x,g(x)) = \Big(\prod_{i=1}^{s} x^i\Big) \cdot x^{m-s(s+1)/2} + x^m = 2x^m.$$

Notice that $\deg_y(F(x,y)) = s$, and $F(x,y)$ has $s+1$ m-near solutions.

Case 3. Let

$$F(x,y) = (y - 2x^2 - x)(y - x^2 - 2x) \cdot x^{m-3} + x^m.$$

Here, also, the polynomial $G(x,y)$ in the presentation of $F(x,y)$ in Lemma 3.2 is zero. We find that $F(x, 2x^2 + x) = F(x, x^2 + 2x) = x^m$, $F(x, x^2 + x) = (-x^2)(-x)x^{m-3} + x^m = 2x^m$, and $F(x, 2x^2 + 2x) = x \cdot x^2 \cdot x^{m-3} + x^m = 2x^m$. Notice that $\deg_y(F(x,y)) = 2$, and $F(x,y)$ has four m-near solutions.

Remark. If $F(x,y) = f(x) \in K[x]$, then $F(x,y)$ has an m-near solution if and only if $f(x) = cx^m$ for a $c \in K$. In this case, we may say that every $g(x) \in K[x]$ is an m-near solution of $F(x,y)$ with m-value c.

Now, we are ready to extend the results in Proposition 3.1 to the general case. For simplicity, we do not state the results in detail as done in Proposition 3.1.

Theorem 3.3. *Let $F(x,y)$ and $g_i(x)$, $1 \leq i \leq n$, be polynomials over K with the $g_i(x)$ all distinct. Then $F(x, g_i(x)) = a_i x^m$ where $a_i \in K$ for every i, $1 \leq i \leq n$, if and only if $F(x,y)$ can be represented in nested parentheses of the form*

$$F(x,y) = (y - g_1(x))$$
$$\times\{(y - g_2(x))[(y - g_3(x))(\cdots(G(x,y)\cdots) + d_3 x^{m-r_1-r_2}] + d_2 x^{m-r_1}\} + d_1 x^m,$$

where $G(x,y) \in K[x,y]$, $d_i \in K$ for $1 \leq i \leq n$ and $d_i = 0$ if $g_i(x) - g_{i+1}(x)$ is not a monomial, while $r_i = \deg(g_i(x) - g_{i+1}(x))$ when $d_i \neq 0$.

Proof. Assume that $F(x,y)$ has only one m-value a, and let $g_i(x)$, $1 \leq i \leq n$, be the m-near solutions of $F(x,y)$. Then $F(x, g_i(x)) = ax^m$ for

every i. We may write

$$F(x,y) = \Big[\prod_{i=1}^{n}(y - g_i(x))\Big] \cdot G(x,y) + ax^m.$$

This means that the numbers d_i for $2 \le i \le n$ in the above formula are all zero. From the Remark above, it can be seen that this presentation is also true for $\deg_y(F(x,y)) = 0$.

We next consider the case when $F(x,y)$ has exactly two m-values. We deduce our result from Lemma 3.2. The proof for Case 1 in Lemma 3.2 is the same as the proof given below for the case that $F(x,y)$ has more than two distinct m-values. What is needed here is that the differences between any two m-near solutions are monomials of the same degree.

We need to show that the polynomials in Cases 2 and 3 can be rewritten in the required form. The m-near solutions in those presentations have been rearranged: those with the same m-values are put together. Here, we show that our representation is true for an arbitrary order of m-near solutions.

Case 2. Only one of the two m-values has a pair of corresponding m-near solutions $g_1(x)$ and $g_2(x)$ such that $g_1(x) - g_2(x)$ is a binomial. In this case,

$$F(x,y) = \Big[\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})\Big] \cdot [(y - h(x))^q G(x,y) + bx^t] + ax^m$$

where $h(x), h(x) + a_i x^{r_i}$ for $1 \le i \le s$ are all the m-near solutions of $F(x,y)$, $a_i, b \in K$, $r_i, q, t \in \mathbb{N}$, and $G(x,y) \in K[x,y]$. Note that here $t = m - \sum_{i=1}^{s} r_i$. For simplicity, we deal only with the case $q = 1$ and we may interchange the last term $y - h(x) - a_s x^{r_s}$ in the product $\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})$ with $y - h(x)$. Then

$$\begin{aligned}
F(x,y) &= \Big[\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})\Big] \cdot [(y - h(x))G(x,y) + bx^t] + ax^m \\
&= \Big[\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})\Big](y - h(x))G(x,y) \\
&\quad + \Big[\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})\Big]bx^t + ax^m \\
&= \Big[\prod_{i=1}^{s}(y - h(x) - a_i x^{r_i})\Big](y - h(x))G(x,y) \\
&\quad + \Big[\prod_{i=1}^{s-1}(y - h(x) - a_i x^{r_i})\Big](y - h(x))bx^t \\
&\quad - \Big[\prod_{i=1}^{s-1}(y - h(x) - a_i x^{r_i})\Big]a_s x^{r_s} bx^t + ax^m
\end{aligned}$$

$$= \Big[\prod_{i=1}^{s-1}(y - h(x) - a_i x^{r_i})\Big]$$
$$\times \{(y - h(x))[(y - h(x) - a_s x^{r_s})G(x,y) + bx^t] + b_1 x^{t+r_s}\} + ax^m,$$

where $b_1 = -a_s b$. This is in the required form since the coefficients d_j for $1 < j < s-1$ of the term $d_j x^{m-\sum_{i=1}^{j-1} r_i}$ in the required form are all zero.

Case 3. For each m-value there exists a pair of corresponding m-near solutions whose difference is a binomial. In this case,

$$F(x,y) = (y - g_1(x))(y - g_2(x))[(y - g_3(x))^p (y - g_4(x))^q \cdot G(x,y) + bx^t] + ax^m$$

where $g_i(x)$, $1 \le i \le 4$, are all the possible m-near solutions of $F(x,y)$, $p, q, t \in \mathbb{N}$, $G(x,y) \in K[x,y]$, and $a, b \in K$. Moreover, there is a polynomial $g(x)$ over K, $u, v \in \mathbb{N}$, and $a_1, a_2, a_3, a_4 \in K$ such that $g_1(x) = g(x) + a_1 x^u + a_2 x^v$, $g_2(x) = g(x) + a_3 x^u + a_4 x^v$, $g_3(x) = g(x) + a_1 x^u + a_4 x^v$, and $g_4(x) = g(x) + a_3 x^u + a_2 x^v$. Note that here $t = m - u - v$. By symmetry, we need only show that we may interchange the term $y - g_2(x)$ with $y - g_3(x)$. For simplicity, we handle only the case of $p = q = 1$. We have

$$\begin{aligned}
F(x,y) &= (y - g_1(x)) \\
&\quad \times \{(y - g_2(x))[(y - g_3(x))(y - g_4(x)) \cdot G(x,y) + bx^{m-u-v}]\} + ax^m \\
&= (y - g_1(x))\{(y - g_2(x))(y - g_3(x))(y - g_4(x)) \cdot G(x,y) \\
&\quad + (y - g_2(x))bx^{m-u-v}\} + ax^m \\
&= (y - g_1(x))\{(y - g_3(x))(y - g_2(x))(y - g_4(x)) \cdot G(x,y) \\
&\quad + (y - g_3(x))bx^{m-u-v} + (g_3(x) - g_2(x))bx^{m-u-v}\} + ax^m \\
&= (y - g_1(x))\{(y - g_3(x))[(y - g_2(x))(y - g_4(x)) \cdot G(x,y) + bx^{m-u-v}] \\
&\quad + (a_1 - a_3)x^u \cdot bx^{m-u-v}\} + ax^m \\
&= (y - g_1(x))\{(y - g_3(x))[(y - g_2(x))(y - g_4(x)) \cdot G(x,y) + bx^{m-u-v}] \\
&\quad + b_1 x^{m-v}\} + ax^m
\end{aligned}$$

where $b_1 = (a_1 - a_3)b$. Thus, the second and third cases of Lemma 3.2 with exactly two m-values are in the required form.

Finally, we assume that $F(x,y)$ has more than two distinct m-values. From Theorem 2.3 there is a nonnegative integer t such that for any two different m-near solutions $g_i(x)$ and $g_j(x)$ there is an $\alpha_{i,j} \in K$ such that $g_i(x) - g_j(x) = \alpha_{i,j} x^t$. Our proof below is based on this fact only, i.e. not on the number of m-values. Hence, this proof is also valid for Case 1 of Lemma 3.2.

Now, we argue by induction on the y-degree of the polynomial. We have

$$F(x,y) = (y - g_1(x))G_1(x,y) + a_1 x^m.$$

If $\deg_y(F(x,y)) = 1$, then $G_1(x,y) = G_1(x) \in K[x]$. Then, for every $2 \le i \le n$,

$$\begin{aligned} F(x, g_i(x)) &= (g_i(x) - g_1(x))G_1(x) + a_1x^m \\ &= \alpha_{i,1}x^t \cdot G_1(x) + a_1x^m = a_ix^m. \end{aligned}$$

Thus, $G_1(x) = ((a_i - a_1)/\alpha_{i,1})x^{m-t}$, and

$$F(x,y) = (y - g_1(x))((a_i - a_1)/\alpha_{i,1})x^{m-t} + a_1x^m.$$

This finishes the proof of the case of $\deg_y(F(x,y)) = 1$ ([1]). Now, assume that $\deg_y(F(x,y)) > 1$. Then, for every $2 \le i \le n$,

$$\begin{aligned} F(x, g_i(x)) &= (g_i(x) - g_1(x))G_1(x, g_i(x)) + a_1x^m \\ &= \alpha_{i,1}x^t \cdot G_1(x, g_i(x)) + a_1x^m = a_ix^m. \end{aligned}$$

Hence, $G_1(x, g_i(x)) = b_ix^{m-t}$ for every $2 \le i \le n$ where $b_i = (a_i - a_1)/\alpha_{i,1}$. Notice that $\deg_y(G_1(x,y)) = \deg_y(F(x,y)) - 1$. By induction hypothesis,

$$G_1(x,y) = (y - g_2(x))[(y - g_3(x))(\cdots G(x,y)\cdots) + d_3x^{m-2t}] + d_2x^{m-t}$$

where $G(x,y) \in K[x,y]$ and $d_i \in K$ for $2 \le i \le n$. Therefore,

$$\begin{aligned} F(x,y) = (y - g_1(x))\{&(y - g_2(x)) \\ &\times [(y - g_3(x))(\cdots G(x,y)\cdots) + d_3x^{m-2t}] + d_2x^{m-t}\} + d_1x^m. \ \blacksquare \end{aligned}$$

4. Bounds for near solutions. In this section we will show some bounds for m-near solutions. We first give an upper bound on the degrees of m-near solutions of a given polynomial.

PROPOSITION 4.1. *Let $F(x,y) = \sum_{k=0}^{s} f_k(x)y^k = \sum_{k=0}^{s}(\sum_{l=0}^{t_k} b_{k,l}x^l)y^k$ be a polynomial of y-degree s. Let r be a positive integer such that $r \ge (t_k - t_s)/(s-k)$ for $0 \le k < s$ and $r \ge (m - t_s)/s$. Then the degree of every m-near solution of $F(x,y)$ is less than or equal to r. In particular, the maximum of $\{t_1, \ldots, t_{s-1}, (m - t_s)/s\}$ suffices as an upper bound.*

Proof. Let $p(x) = \sum_{i=0}^{d} a_ix^i$, where $a_d \ne 0$ and $d > r$. Then for every k, $0 \le k \le s$,

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

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

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

Also, $sd + t_s > sr + t_s \ge m$, which implies that $p(x)$ cannot be an m-near solution of $F(x,y)$. $\blacksquare$

([1]) Here, the number of distinct m-near solutions is greater than the y-degree of $F(x,y)$. The polynomial $F(x,y)$ is also in the special form given in Theorem 4.2 of the next section.

Now, we show that unless the given polynomial is in a special form, the number of m-near solutions is bounded by its y-degree.

THEOREM 4.2. *Let $F(x,y)$ be a polynomial over K of y-degree t, and m be a nonnegative integer. Except when $F(x,y)$ has exactly two m-values, the number of distinct m-near solutions of $F(x,y)$ is greater than t if and only if the number of elements of K is greater than t and there exists a polynomial $g(x)$ over K and a nonnegative integer r with $r \le m/t$ such that*

$$F(x,y) = \sum_{i=0}^{t} c_i (y - g(x))^i x^{m-ir}$$

where $c_i \in K$. In this case, unless $t = 0$, a polynomial $h(x)$ is an m-near solution of $F(x,y)$ if and only if $h(x) = g(x) + ax^r$ for an $a \in K$.

Proof. We prove the second part first. Let

$$F(x,y) = \sum_{i=0}^{t} c_i (y - g(x))^i x^{m-ir}$$

where $c_i \in K$. For any $a \in K$, a straightforward calculation shows that $g(x) + ax^r$ is an m-near solution of $F(x,y)$ with m-value $\sum_{i=0}^{t} c_i(a)^i$.

Now, let $h(x)$ be an m-near solution of $F(x,y)$. We want to show that $h(x) - g(x)$ is a monomial of degree r. Let $h(x) - g(x) = d(x) \in K[x]$ have degree p and rank q. If $p > r$, then

$$\deg(c_i(d(x))^i x^{m-ir}) = pi + m - ir = m + i(p-r) \ge 0$$

for each i, $0 \le i \le t$. Thus, $\deg(c_i(d(x))^i x^{m-ir}) > \deg(c_j(d(x))^j x^{m-jr})$ if $i > j$, and

$$\begin{aligned}\deg(F(x,h(x))) &= \deg\Big(\sum_{i=0}^{t} c_i(d(x))^i x^{m-ir}\Big) = \deg(c_t(d(x))^t x^{m-tr}) \\ &= tp + m - tr > m.\end{aligned}$$

This implies that $h(x)$ cannot be an m-near solution of $F(x,y)$. Thus, $p \le r$. Similarly, assume that $q < r$. Then

$$\operatorname{rank}(F(x,h(x))) \le \operatorname{rank}(c_t(d(x))^t x^{m-tr}) \le m - tr + tq < m.$$

This implies that $h(x)$ is not an m-near solution of $F(x,y)$. Thus, $q \ge r$. Combining these facts, we see that $d(x)$ is a monomial of degree r. Therefore, $h(x)$ is an m-near solution of $F(x,y)$ if and only if there is an a in K such that $h(x) = g(x) + ax^r$. Thus, if

$$F(x,y) = \sum_{i=0}^{t} c_i (y - g(x))^i x^{m-ir}$$

where $t > 0$ and $c_i \in K$, then the number of m-near solutions of $F(x, y)$ is equal to the number of elements of K. In particular, if the latter is greater than $\deg_y(F(x, y))$, then the number of m-near solutions of $F(x, y)$ is greater than $\deg_y(F(x, y))$.

Next, assume that the number of m-near solutions of $F(x, y)$ is greater than $\deg_y(F(x, y))$ and the number of distinct m-values of $F(x, y)$ is not two. We need to prove that there exists a polynomial $g(x)$ over K and a nonnegative integer $r \leq m/t$ such that

$$F(x, y) = \sum_{i=0}^{t} c_i (y - g(x))^i x^{m-ir}$$

where $c_i \in K$. We prove this fact by induction on $\deg_y(F(x, y))$. Assume that $\deg_y(F(x, y)) = 0$. Then $F(x)$ has an m-near solution if and only if that $F(x) = cx^m$ for a c in K. Thus, $F(x, y)$ has the desired form with $t = 0$. Now, we assume that the hypothesis holds for any polynomial of y-degree n. Let $F(x, y)$ be a polynomial with $\deg_y(F(x, y)) = n + 1$ and assume that $F(x, y)$ has $n + 2$ distinct m-near solutions $g_1(x), \ldots, g_{n+2}(x)$. If $F(x, y)$ has exactly one m-value, say a, then $F(x, y) - ax^m = 0$ has $n + 2$ distinct zeros in $K[x]$. This implies that $F(x, y) - ax^m$ is identically zero. Therefore, $F(x, y) = ax^m$, which contradicts the fact that $\deg_y(F(x, y)) = n + 1$. This implies that $F(x, y)$ cannot have exactly one m-value.

The case of two m-values being excluded by assumption, we now assume that $F(x, y)$ has more than two m-values. From Theorem 2.3, there is an $r \in \mathbb{N}$ such that for any $1 \leq i, j \leq n + 2$, $g_i(x) - g_j(x) = a_{i,j}x^r$ where $a_{i,j} \in K$. Now, we continue the proof with the assumption that the difference between any two m-near solutions is a monomial. Let $F(x, g_1(x)) = ax^m$ for an $a \in K$. Then

$$F(x, y) = (y - g_1(x))G(x, y) + ax^m$$

for a $G(x, y) \in K[x, y]$ with $\deg_y(G(x, y)) = n$. For every i, $2 \leq i \leq n + 2$, let $b_i \in K$ be the corresponding m-value of $g_i(x)$. Then

$$\begin{aligned} F(x, g_i(x)) &= (g_i(x) - g_1(x))G(x, g_i(x)) + ax^m \\ &= a_{i,1}x^r G(x, g_i(x)) + ax^m = b_i x^m. \end{aligned}$$

Thus, $G(x, g_i(x)) = ((b_i - a)/a_{i,1})x^{m-r}$. This means that every $g_i(x)$, $2 \leq i \leq n+2$, is an $(m-r)$-near solution of $G(x, y)$. We see that $\deg_y(G(x, y)) = n$, and $G(x, y)$ has $n+1$ $(m-r)$-near solutions. Also, the difference between any two $(m-r)$-near solutions of $G(x, y)$ is a monomial. By induction hypothesis, there is a $p \in \mathbb{N}$ with $np \leq m - r$ and such that

$$G(x, y) = \sum_{i=0}^{n} d_i (y - g(x))^i x^{m-r-ip}$$

where $d_i \in K$ and $g(x) \in K[x]$. Since $F(x,y)$ has at least three distinct m-values, $F(x,y)$ has at least three distinct m-near solutions. Now, $g_2(x)$ and $g_3(x)$ are $(m-r)$-near solutions of $G(x,y)$, so from the second part of this theorem, there exist α and β in K such that $g_2(x) = g(x) + \alpha x^p$ and $g_3(x) = g(x) + \beta x^p$, respectively. Thus, $g_2(x) - g_3(x) = (\alpha - \beta)x^p$. We know that $g_2(x) - g_3(x) = a_{2,3}x^r$ for an $a_{2,3} \neq 0$ in K. This means that $p = r$ and

$$g_1(x) = g_2(x) + a_{1,2}x^r = g(x) + \alpha x^r + a_{1,2}x^r = g(x) + dx^r$$

for a $d \in K$. Then

$$\begin{aligned}
F(x,y) &= (y - g_1(x))G(x,y) + ax^m \\
&= (y - g(x) - dx^r)\Big[\sum_{i=0}^{n} d_i(y - g(x))^i x^{m-r-ir}\Big] + ax^m \\
&= \Big(\sum_{i=0}^{n} d_i(y - g(x))^{i+1}\Big)x^{m-(i+1)r} \\
&\quad - \sum_{i=0}^{n} d_i(y - g(x))^i \cdot d \cdot x^{m-ir} + ax^m \\
&= \sum_{i=1}^{n+1} d_{i-1}(y - g(x))^i x^{m-ir} - \sum_{i=0}^{n} d \cdot d_i(y - g(x))^i x^{m-ir} + ax^m \\
&= \sum_{i=0}^{n+1} c_i(y - g(x))^i x^{m-ir}
\end{aligned}$$

where $c_0 = -d \cdot d_0 + a$, $c_i = d_{i-1} - d \cdot d_i$ for $1 \leq i \leq n$, and $c_{n+1} = d_n$. Note also that $np \leq m - r$ and $p = r$ imply that $(n+1)r \leq m$. Therefore, $F(x,y)$ is of the form in the assumption. The number of m-near solutions of $F(x,y)$ is thus equal to the number of elements of K. As we assume that the number of m-near solutions of $F(x,y)$ is greater than the $\deg_y(F(x,y))$, we conclude that the number of elements of K is greater than $\deg_y(F(x,y))$. This completes the proof. ∎

Remark. If $F(x,y)$ has exactly two m-values and $F(x,y)$ is in Case 1 of Lemma 3.2, then the difference between any two m-near solutions is a monomial. Then, with the same proof it can be shown that the number of m-near solutions of $F(x,y)$ is less than or equal to the y-degree of $F(x,y)$.

For an equation we may have multiple solutions. Similarly, we can define the multiplicity of an m-near solution.

Definition. Let $g(x)$ be an m-near solution of $F(x,y)$ with m-value a. Then there exists a greatest integer r such that $F(x,y) = (y - g(x))^r H(x,y) + ax^m$ where $H(x,y) \in K[x,y]$ and $y - g(x)$ does not divide $H(x,y)$. The integer r is called the *multiplicity* of the m-near solution $g(x)$ of $F(x,y)$.

We then have the following result.

THEOREM 4.3. *Let $F(x,y)$ be a polynomial over K with y-degree t, and m be a nonnegative integer. Except when $F(x,y)$ has exactly two m-values, if the number of m-near solutions of $F(x,y)$ counting multiplicity is greater than t, then there exist a polynomial $g(x)$ over K and an nonnegative integer r with $r \le m/t$ such that*

$$F(x,y) = \sum_{i=0}^{t} c_i (y - g(x))^i x^{m-ir}$$

where $c_i \in K$.

Sketch of proof. We demonstrate only the induction step. Let $F(x,y)$ be a polynomial with y-degree n and assume that $F(x,y)$ has $n+1$ m-near solutions counting multiplicity, and more than two distinct m-values. Let $g_1(x), \dots, g_s(x)$ be all the distinct m-near solutions of $F(x,y)$, with possibly different multiplicities. Since $F(x,y)$ has more than two distinct m-values, $s > 2$. Moreover, the difference between any two distinct m-near solutions is a nonzero monomial of degree r.

Let $g_1(x)$ be an m-near solution of multiplicity t and $F(x, g_1(x)) = ax^m$ for an $a \in K$. Then

$$F(x,y) = (y - g_1(x))^t G(x,y) + ax^m$$

for a $G(x,y) \in K[x,y]$ with $\deg_y(G(x,y)) = n - t$. For every i, $2 \le i \le s$, let $g_i(x) - g_1(x) = a_{i,1}x^r$ and $b_i \in K$ be the corresponding m-value of $g_i(x)$. Then

$$\begin{aligned} F(x, g_i(x)) &= (g_i(x) - g_1(x))^t G(x, g_i(x)) + ax^m \\ &= (a_{i,1}x^r)^t G(x, g_i(x)) + ax^m = b_i x^m. \end{aligned}$$

Thus, $G(x, g_i(x)) = ((b_i - a)/(a_{i,1})^t)x^{m-rt}$. This means that every $g_i(x)$, $2 \le i \le s$, is an $(m-rt)$-near solution of $G(x,y)$. We have $\deg_y(G(x,y)) = n - t$, and $G(x,y)$ has $n+1-t$ $(m-r)$-near solutions counting multiplicity. Also, the difference between any two $(m-r)$-near solutions of $G(x,y)$ is a monomial of degree r. By induction hypothesis, there is a $p \in \mathbb{N}$ with $np \le m - r$ and such that

$$G(x,y) = \sum_{i=0}^{n-t} d_i (y - g(x))^i x^{m-rt-ip}$$

where $d_i \in K$ and $g(x) \in K[x]$. We deduce that $p = r$ and $g_1(x) = g(x) + dx^r$ for a $d \in K$. Then, by the Binomial Theorem, the $c(t,j)$ being the binomial coefficients, we have

$$\begin{aligned} F(x,y) &= (y - g_1(x))^t G(x,y) + ax^m \\ &= (y - g(x) - dx^r)^t \Big[\sum_{i=0}^{n-t} d_i (y - g(x))^i x^{m-rt-ir} \Big] + ax^m \end{aligned}$$

$$= \Big[\sum_{j=0}^{t} c(t,j)(y-g(x))^j(-dx^r)^{t-j}\Big]\Big[\sum_{i=0}^{n-t} d_i(y-g(x))^i x^{m-rt-ir}\Big] + ax^m$$

$$= \sum_{k=0}^{n} c_k(y-g(x))^k x^{m-kr}$$

where $c_0 = (-d)^t d_0 + a$, $c_k = \sum_{i+j=k} c(t,j)(-d)^{t-j}(d_i)$. Hence, $F(x,y)$ is of the desired form. ∎

Example. Let $K = \mathbb{F}_3$ be the finite field with three elements, and $F(x,y) = (y-x^3)^3x^2 - (y-x^3)x^6$. Then $F(x, x^3+ax^2) = (a^3-a)x^8$. For every $a \in \mathbb{F}_3$, we have $a^3 - a = 0$. Therefore, although $F(x,y)$ has three m-near solutions, it has only one m-value. Note that $F(x,y)$ has the form of Corollary 4.3. Hence, the converse of Corollary 4.3 (and of Corollaries 4.4, 4.5 below) is not true. Of course, if K is a field with infinitely many elements, then these converses are easily seen to be true.

We also have a natural bound on the number of m-values, which can be stated more elegantly as compared with Theorem 4.2.

Corollary 4.4. *Let $F(x,y)$ be a polynomial over K with y-degree t, and m be a nonnegative integer. If the number of distinct m-values of $F(x,y)$ is greater than t, then there exists a polynomial $g(x)$ over K and a nonnegative integer r with $r \le m/t$ such that*

$$F(x,y) = \sum_{i=0}^{t} c_i(y-g(x))^i x^{m-ir}$$

where $c_i \in K$.

Proof. Assume that $\deg_y(F(x,y)) = 0$. Then $F(x,y)$ has an m-value if and only if $F(x,y) = ax^m$ for an $a \in K$. This means that $F(x,y)$ is as in the statement.

It is easy to see that the number of m-values is less than or equal to the number of distinct m-near solutions. If the number of m-values of $F(x,y)$ is greater than $\deg_y(F(x,y))$, then the number of distinct m-near solutions is greater than $\deg_y(F(x,y))$. From Theorem 4.2, we need only handle the case when $F(x,y)$ has exactly two m-values. We then only need to handle the case of $\deg_y(F(x,y)) = 1$. However, in that case none of the three cases of Lemma 3.2 hold. We can also prove this directly. Let $F(x,y) = f_1(x)y + f_0(x)$ have two m-values, say a and b. Then there exist $g(x)$ and $h(x)$ in $K[x]$ such that $F(x,g(x)) = ax^m$ and $F(x,h(x)) = bx^m$. Thus, $F(x,y) = (y-g(x))G(x) + ax^m$ for a $G(x) \in K[x]$. Then $F(x,h(x)) = (h(x)-g(x))G(x) + ax^m = bx^m$. This implies that $h(x) - g(x) = cx^r$ for a $c \in K$ and an $r \in \mathbb{N}$ where $r \le m$. Then $G(x) = ((b-a)/c)x^{m-r}$ and $F(x,y) = (y-g(x))((b-a)/c)x^{m-r} + ax^m$. Hence $F(x,y)$ is of the desired form. ∎

As above, we may define the multiplicity of an m-value.

DEFINITION. Let $F(x,y)$ be a polynomial over K and m be a nonnegative integer. Let $c \in K$, $\{g_1(x), \ldots, g_t(x)\}$ be the set of all m-near solutions of $F(x,y)$ with m-value c, and r_i be the multiplicity of $g_i(x)$. Then $s = \sum_{i=1}^{t} r_i$ is called the *multiplicity* of the m-value c of $F(x,y)$.

Note that the number of m-values is equal to the number of m-near solutions (counting multiplicity). We then have the following corollary.

COROLLARY 4.5. *Let $F(x,y)$ be a polynomial over K with y-degree t, and m be a nonnegative integer. Except when $F(x,y)$ has exactly two m-values, if the number of m-values of $F(x,y)$ counting multiplicity is greater than t, then there exists a polynomial $g(x)$ over K and a nonnegative integer r with $r \le m/t$ such that*

$$F(x,y) = \sum_{i=0}^{t} c_i (y - g(x))^i x^{m-ir}$$

where $c_i \in K$.

The situation is much more complicated if we extend our definition of near solution to rational functions. This is shown by the following example which was provided by Mr. Li Yang Gan.

FINAL EXAMPLE. Let

$$F(x,y) = (x^3 + 6x^2 + 11x + 6)y^2 - (3x^2 + 12x + 11)y + (2x + 6).$$

Then

$$\begin{aligned} F(x,y) &= ((x+1)y - 1)((x+2)(x+3)y - (2x+5)) + 1 \\ &= ((x+2)y - 1)((x+1)(x+3)y - (2x+4)) + 2 \\ &= ((x+3)y - 1)((x+1)(x+2)y - (2x+3)) + 3. \end{aligned}$$

From this presentation, it can be seen that $F(x,y)$ has three 0-values and six 0-value "rational" near solutions. That is,

$$\begin{aligned} F(x, 1/(x+1)) &= F(x, (2x+5)/(x+2)(x+3)) = 1, \\ F(x, 1/(x+2)) &= F(x, (2x+4)/(x+1)(x+3)) = 2, \\ F(x, 1/(x+3)) &= F(x, (2x+3)/(x+1)(x+2)) = 3. \end{aligned}$$

The bound on the number of near solutions given in Theorem 4.2 and the bound on the number of m-values given in Theorem 4.4, are no longer valid.

Acknowledgements. The author wishes to express his sincere thanks to an unknown referee for his carefulness and suggestions. Especially, the proof of Theorem 4.2 was simplified following his suggestion.

References

[1] R. Dvornicich, S. P. Tung and U. Zannier, *On polynomials taking small values at integral arguments II*, Acta Arith. 106 (2003), 115–121.
[2] S. P. Tung, *Approximate solutions of polynomial equations*, J. Symbolic Comput. 33 (2002), 239–254.

Department of Applied Mathematics
Chung Yuan Christian University
Chung Li, 32023 Taiwan
Republic of China
E-mail: sptung@cycu.edu.tw

Received on 15.4.2005
and in revised form on 13.2.2006 (4978)