Complexity of Deciding Solvability of Polynomial Equations over p-adic Integers

Alexander Chistov * Marek Karpinski†

December, 1997

Abstract

Consider a system of polynomial equations in n variables of degrees less than d with integer coefficients with the lengths less than M. We show using the construction close to smooth stratification of algebraic varieties that an integer

$$\Delta < 2^{Md^{2^{n(1+o(1))}}}$$

corresponds to these polynomials such that for every prime p the considered system has a solution in the ring of p-adic numbers if and only if it has a solution modulo p^N for the least integer N such that p^N does not divide Δ. This improves the previously known result by B. J. Birch and K. McCann.

*St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia, 14th line 39, St. Petersburg 199178, Russia and Department of Computer Science, University of Bonn, 53117 Bonn. Research supported by the Volkswagen–Stiftung, Program on Computational Complexity.

†Department of Computer Science, University of Bonn, 53117 Bonn and International Computer Science Institute, Berkeley, California.

Introduction

Let $f_1, \dots, f_k \in \mathbb{Z}[X_1, \dots, X_n]$ be polynomials. The degrees

$$\deg_{X_1,\dots,X_n} f_i < d$$

and the length of every coefficient of f_i is less than M (it means that the absolute value of every coefficient is less than 2^{M-1}) for all i. We shall suppose without loss of generality that $f_1, \dots, f_k$ are linearly independent over $\mathbb{Q}$ and $k \geq 1$.

Let $\mathbb{Q}_p$ be the field of p-adic numbers and $\mathbb{Z}_p$ the ring of p-adic integers.

THEOREM 1 *For given polynomials $f_1, \dots, f_k$ there is an integer*

$$\Delta < 2^{M d^{2^{n(1+o(1))}}}$$

such that for every prime p the system

$$f_1 = \dots = f_k = 0 \tag{1}$$

has a solution in $\mathbb{Z}_p^n$ if and only if it has a solution in $(\mathbb{Z}/p^N\mathbb{Z})^n$ for the least integer N such that p^N does not divide Δ, herewith $o(1)$ is an infinitesimal when $n \to \infty$. The integer Δ can be constructed within the time polynomial in Md^{2^n}.

The previous result was obtained in the well known paper by B. J. Birch and K. McCann [1] for the case of one polynomial $k = 1$, $f = f_1$. Let $L(f)$ denote the maximum of absolute values of coefficients of f. Then [1] gives

$$\Delta < (2^n d L(f))^{(2d)^{4^n n!}}$$

i.e.

$$\Delta < 2^{M d^{(cn)^n}}.$$

for a constant $c \geq 1$. So our result improves the highest level exponent from $n \log(cn)$ to $n(1 + o(1))$. Note also that the infinitesimal $o(1)$ in the formulation of Theorem 1 can be obtained explicitly from the proof. It is a rational function of n, $\log n$, $\log\log n$.

Note also that the analogs of Theorem 1 and Theorem 4, see below, are true if one consider homogeneous polynomials $f_1, \dots, f_k \in \mathbb{Z}[X_0, \dots, X_n]$ and their non–zero solutions, i.e. the solutions in $\mathbb{Z}_p^{n+1} \setminus \{(0, \dots, 0)\}$ and $(\mathbb{Z}/p^N\mathbb{Z})^{n+1} \setminus \{(0, \dots, 0)\}$ respectively. The proofs are similar if we consider projective spaces instead affine spaces. Further, for homogeneous polynomials the existence of a solution of a system of polynomial equations in $\mathbb{P}^n(\mathbb{Q}_p)$ is equivalent to the existence of a non–zero solution $\mathbb{Z}_p^{n+1} \setminus \{(0, \dots, 0)\}$.

The proof of Theorem 1 is based on the construction which iterates the decomposition of a given algebraic variety into the union of irreducible components and taking the proper closed subset containing all singular points of a component. So the results of [2] is used for the proof. But for recursive estimations we need to prove basing on [2] also some additional facts related to decomposition of algebraic varieties into irreducible components, see Lemma 2. The construction required for the proof of Theorem 1 is closely related to the smooth stratification of algebraic varieties. So we shall define and consider at first the latter.

A related problem of deciding existence of a non-zero of a polynomial given by a black box over p-adics was currently studied in [5].

Denote by $\mathcal{Z}(f_1, \ldots, f_k)$ the algebraic variety of all zeroes of the polynomials $f_1, \ldots, f_k$ in the affine space $\mathbb{A}^n(\overline{\mathbb{Q}})$ over the algebraic closure $\overline{\mathbb{Q}}$ of the field of rational numbers $\mathbb{Q}$.

DEFINITION 1 *Denote*

$$V_1 = \mathcal{Z}(f_1, \ldots, f_k).$$

Suppose that the closed in $\mathbb{A}^n(\overline{\mathbb{Q}})$ *algebraic variety* V_r *is defined for some* $1 \leq r \leq n$. *If* $V_r \neq \emptyset$ *consider the decomposition*

$$V_r = \bigcup_{i \in I_r} W_i$$

into the union of irreducible and defined over $\mathbb{Q}$ *algebraic varieties* W_i. *Denote by* $\operatorname{Sing} W_i$ *the set of singular points of* W_i *and set*

$$V'_{r+1} = \bigcup_{i \in I_r} \operatorname{Sing} W_i \cup \bigcup_{i,j \in I_r,\, i \neq j} (W_i \cap W_j).$$

Let the closed in $\mathbb{A}^n(\overline{\mathbb{Q}})$ *algebraic variety* V_{r+1} *be such that* $V_r \supset V_{r+1} \supset V'_{r+1}$ *and* $W_i \setminus V_{r+1} \neq \emptyset$ *for all* $i \in I_r$. *Set*

$$S_r = V_r \setminus V_{r+1}, \quad U_i = W_i \setminus V_{r+1}.$$

Then the quasiprojective algebraic variety S_r *consists of smooth points of different dimensions of the algebraic variety* V_r, *the quasiprojective algebraic varieties* U_i *are irreducible defined over* $\mathbb{Q}$ *and smooth for all* i. *We have the decomposition*

$$S_r = \bigcup_{i \in I_r} U_i$$

into the union of irreducible and defined over $\mathbb{Q}$ components. We can suppose without loss of generality that $I_{r_1} \cap I_{r_2} = \emptyset$ for all $r_1 \neq r_2$. Denote by n_0 the maximal r for which $V_r \neq \emptyset$. Set $I = \cup_{1 \le r \le n_0} I_r$. We have the decomposition

$$\mathcal{Z}(f_1, \ldots, f_k) = \bigcup_{i \in I} U_i \tag{2}$$

which gives the smooth stratification of $\mathcal{Z}(f_1, \ldots, f_k)$ with smooth stratums U_i.

Note that this construction depends on the choice of the varieties $V_{r+1} \supset V'_{r+1}$. If we have $V_{r+1} = V'_{r+1}$ for all r then (2) is uniquely defined and we shall call it *canonical smooth stratification of $\mathcal{Z}(f_1, \ldots, f_k)$*. Note also that the codimension of every component of V_r is at least r.

Denote by $V_r^{(s)}$ the union of all irreducible and defined over $\mathbb{Q}$ components of codimensions s of the algebraic variety V_r where $r \le s \le n$. Note that $V_r^{(s)}$ can be empty for some s. So we shall suppose that:

(a) The degree of the algebraic variety $V_r^{(s)}$ is less than $D_r^{(s)}$ for some $D_r^{(s)} \ge 1$ for all $r \le s \le n$, $1 \le r \le n_0$.

(b) Each irreducible and defined over $\mathbb{Q}$ component W_i of this union $V_r^{(s)}$ is given as a set of common zeroes of a family of polynomials $h_{i,\alpha} \in \mathbb{Z}[X_1, \ldots, X_n]$, $\alpha \in A_i$, herewith the number of polynomials $\#A \le \mathcal{P}((D_r^{(s)})^n)$ and the lengths of their integer coefficients are less than $M_r^{(s)}$ for some $M_r^{(s)} \ge 1$ and a polynomial $\mathcal{P}$.

(c) For every smooth point $x \in W_i$ there are $\alpha_1, \ldots, \alpha_s \in A$ such that $h_{\alpha_1}, \ldots, h_{\alpha_s}$ is a system of local local parameters of W_i in the point x (i.e. $h_{\alpha_1}, \ldots, h_{\alpha_s}$ generate the ideal of W_i in the local ring $\mathcal{O}_{x, \mathbb{A}^n(\overline{Q})}$ of the point x in $\mathbb{A}^n(\overline{Q})$).

DEFINITION 2 *Let an algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$ be given. Set*

$$V_1 = \mathcal{Z}(f_1, \ldots, f_k).$$

Let an algebraic variety $V_{i_1, \ldots, i_k}$ be defined for some $1 \le k < n$, herewith $i_1 = 1$. Let $V_{i_1, \ldots, i_k} \neq \emptyset$. Consider the decomposition

$$V_{i_1, \ldots, i_k} = \bigcup_{i_{k+1} \in I_{i_1, \ldots, i_k}} W_{i_1, \ldots, i_k, i_{k+1}}$$

into the union of irreducible and defined over $\mathbb{Q}$ components $W_{i_1, \ldots, i_k, i_{k+1}}$. Let a smooth quasiprojective algebraic variety $U_{i_1, \ldots, i_k, i_{k+1}}$ be a non–empty open in the Zariski topology subset of $W_{i_1, \ldots, i_k, i_{k+1}}$. Set

$$V_{i_1, \ldots, i_k, i_{k+1}} = W_{i_1, \ldots, i_k, i_{k+1}} \setminus U_{i_1, \ldots, i_k, i_{k+1}}$$

for all $i_{k+1} \in I_{i_1,\dots,i_k}$. Let n_0 be maximal k such that there exists $V_{i_1,\dots,i_k}$ which is non–empty. Then the family of all $U_{i_1,\dots,i_{k+1}}$ for all indices i_j with the described structure and all $1 \le k \le n_0$ defines branched smooth stratification of the algebraic variety $\mathcal{Z}(f_1,\dots,f_k)$.

So the branched smooth stratification depends on the choice of $U_{i_1,\dots,i_k,i_{k+1}}$. If $U_{i_1,\dots,i_k,i_{k+1}}$ is always the set of all smooth points of $W_{i_1,\dots,i_k,i_{k+1}}$ then such a branched smooth stratification is uniquely defined and we shall call it *canonical branched smooth stratification of* $\mathcal{Z}(f_1,\dots,f_k)$.

Note that the codimension of every algebraic variety $W_{i_1,\dots,i_r,i_{r+1}}$ is at least r. For every $1 \le r \le n_0$, $r \le s \le n$ denote by $V_r^{(s)}$ the union of all the algebraic varieties $W_{i_1,\dots,i_r,i_{r+1}}$ (for all indices $i_1,\dots,i_r,i_{r+1}$) which have the codimension s. We shall suppose that for branched smooth stratification (a)–(c) are satisfied if we replace in them W_i by $W_{i_1,\dots,i_r,i_{r+1}}$, and i by $i_1,\dots,i_r,i_{r+1}$.

We shall prove in Section 1 the following results

THEOREM 2 *For given polynomials $f_1,\dots,f_k$ one can construct the canonical smooth stratification of $\mathcal{Z}(f_1,\dots,f_k)$ satisfying (a)–(c) with*

$$D_r^{(s)} \le (sd)^{2^s-1}, \quad M_r^{(s)} \le (M+n^2)\mathcal{P}((sd)^{2^s-1})$$

for some polynomial $\mathcal{P}$. The working time of the algorithm for constructing smooth stratification is polynomial in $(nd)^{2^n}$ and M.

THEOREM 3 *For given polynomials $f_1,\dots,f_k$ one can construct the canonical branched smooth stratification of $\mathcal{Z}(f_1,\dots,f_k)$ described above satisfying (a)–(c) (with corresponding changes) and such that*

$$D_r^{(s)} \le (sd)^{2^s-1}, \quad M_r^{(s)} \le (M+n^2)\mathcal{P}((sd)^{2^s-1})$$

for some polynomial $\mathcal{P}$. The working time of the algorithm for constructing this branched smooth stratification is polynomial in $(nd)^{2^n}$ and M.

Recall that $\mathbb{Z}_p$ denotes the ring of p-adic integers. Denote

$$M_s = \max_{1 \le r \le n_0} M_r^{(s)}, \quad D_s = \max_{1 \le r \le n_0} D_r^{(s)}$$

for all $1 \le s \le n$. We shall deduce Theorem 1 from Theorem 3 and the following result which will be proved in Section 2.

THEOREM 4 *Let polynomials $f_1, \ldots, f_k$ be given with the set of zeroes V_1. Let a branched smooth stratification of V_1 be given with corresponding D_s and M_s. Then there is an integer*

$$\Delta < 2^{M\mathcal{P}(d^{n^2})+\sum_{1\le s\le n} M_s \mathcal{P}((sD_s)^{n^2})\prod_{0\le t<s}(tD_t)^n}$$

(for a polynomial $\mathcal{P}$) such that for every prime p the system

$$f_1 = \ldots = f_k = 0$$

has a solution in $\mathbb{Z}_p^n$ if and only if it has a solution in $(\mathbb{Z}/p^N\mathbb{Z})^n$ for the least integer $N > 0$ such that p^N does not divide Δ. The integer Δ can be constructed within the time polynomial in n^{n^2}, M, M_s, d^{n^2}, $D_s^{n^2}$, $1 \le s \le n$.

1 Construction of the smooth stratification and branched smooth stratification of an algebraic variety

Our aim now is to prove Theorem 2 and Theorem 3 for the described canonical smooth stratification and branched smooth stratification of $\mathcal{Z}(f_1, \ldots, f_k)$.

Let $u_{i,j}$, $i = 0, s, s+1, \ldots, n$, $0 \le j \le n$ be algebraically independent elements over $\mathbb{Q}$. Denote for brevity the family

$$\mathcal{U} = \{u_{i,j}\}_{i=0,s,s+1,\ldots,n,\, 0\le j\le n}.$$

Set $U_i = \sum_{0\le j\le n} u_{i,j}X_j$. Let $V \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ be an irreducible projective algebraic variety defined over $\mathbb{Q}$ of dimension $n-s$, $1 \le s \le n$. Then there is a unique (up to a factor ± 1) irreducible polynomial

$$H \in \mathbb{Z}[\mathcal{U}, Z_0, Z_s, \ldots, Z_n]$$

homogeneous relative to the variables $Z_0, Z_s, \ldots, Z_n$ such that $H(\mathcal{U}, U_0, U_s, \ldots, U_n)$ is vanishing on V considered as a subvariety of $\mathbb{P}^n(\overline{\mathbb{Q}(\mathcal{U})})$. The polynomial H has the degrees $\deg_{u_{i,0},\ldots,u_{i,n}} H = \deg V$ for every i and $\deg_{Z_0,Z_s,\ldots,Z_n} H = \deg V$, c.f. [4], [2].

Let V be an irreducible component of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$. Let us show that the lengths of integer coefficients of the polynomial H are bounded from above by $(M + n^2)\mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$. Indeed, consider the resultant

$$R_H = \mathrm{Res}_{Z_0}(H'_{Z_0}, H) \in \mathbb{Z}[\mathcal{U}, Z_s, \ldots, Z_n] \tag{3}$$

of the polynomial H relative to Z_0.

There are finite sets of integers $A_{i,j}$, $i = 0, s, s+1, \ldots, n$, $0 \le j \le n$ such that $\# A_{i,j} = \deg V + 1 \le d^s$, the length of every element of $A_{i,j}$ is $O(n^2 \log(\deg V + 1))$ for all i, j and if

$$\mathcal{D} = (d_{i,j}) \in \prod_{i=0,s,s+1,\ldots,n,\, 0 \le j \le n} A_{i,j}$$

then

$$R_H(\mathcal{D}, Z_s, \ldots, Z_n) \neq 0. \qquad (4)$$

The construction of system of polynomial equations for the components of an algebraic variety from [2] and (4) imply that the lengths of integer coefficients of the polynomial $H(\mathcal{D}, Z_0, Z_s, \ldots, Z_n)$ are bounded from above by $(M+n^2)\mathcal{P}(d^s)$. Using multiple interpolation by all $\mathcal{D}$ we get that the lengths of integer coefficients of the polynomial H are bounded from above by $(M + n^2)\mathcal{P}(d^s)$ and the required assertion is proved.

Let us show that one can construct the polynomial H within the time polynomial in M, d^s, $(\deg V + 1)^{n^2}$. Indeed, it is sufficient using [2] to construct a generic point of V within the time polynomial in M, d^s and n. Then substituting the values of U_i/U_0 (obtained from this generic point) in H, constructing and solving a linear system relative to the integer coefficients of H we get these coefficients. The required assertion is proved.

Represent

$$H(\mathcal{U}, U_0, U_s, \ldots, U_n) = \sum_{e=(e_{i,j}) \in \mathbb{Z}^{(n-s+2)(n+1)}} \prod_{i=0,s,s+1,\ldots,n,\, 0 \le j \le n} u_{i,j}^{e_{i,j}} H_e \qquad (5)$$

where $H_e \in \mathbb{Z}[X_0, \ldots, X_n]$ are homogeneous polynomials. Note that if $H_e \neq 0$ then $\sum_j e_{i,j} \le 2 \deg V$ for all i. Denote $E' = \{e : H_e \neq 0\}$. Then $\# E' \le \mathcal{P}((\deg V + 1)^{n^2})$ for a polynomial $\mathcal{P}$. Choose a maximal subset $E \subset E'$ such that the polynomials H_e, $e \in E$ are linearly independent. So $\# E \le \mathcal{P}((\deg V + 1)^n)$ for a polynomial $\mathcal{P}$.

We have, c.f. the construction of the system of polynomial equations for the components of an algebraic variety from [2], $\mathcal{Z}(H_e, e \in E) = V$. Thus, if the polynomial H is known then one can construct within the polynomial time the system of homogeneous polynomial equations giving V.

DEFINITION 3 *We shall say that the algebraic variety V is given by the generic projection if the corresponding polynomial H is given. The system $H_e = 0$, $e \in E$ for the algebraic variety V will be called system of polynomial equations corresponding to the generic projection of the algebraic variety V. So this system depends on the choice of E.*

It should be underlined that each index $e \in E$ in this definition has the form $e = (e_{i,j})$ described above.

LEMMA 1 *Let $V \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ be an irreducible projective algebraic variety of degree $\deg V = D$ and dimension $n-s$ where $1 \le s \le n$. Let V be given by the generic projection and $H_e = 0$, $e \in E$, be the corresponding system of polynomial equations. Let $x \in V$ be a smooth point. Let $L \in \overline{\mathbb{Q}}[X_0, \dots, X_n]$ be a linear form such that $L(x) \neq 0$. Then there are $e_1, \dots, e_s \in E$ such that $H_{e_1}/L^D, \dots, H_{e_s}/L^D$ is a system of local parameters of V in the point x.*

PROOF Let $Y_0, \dots, Y_n$ be linearly independent linear forms with integer coefficients. Consider the projections

$$\pi : V \setminus \mathcal{Z}(Y_0, Y_{s+1}, \dots, Y_n) \to \mathbb{P}^{n-s}(\overline{\mathbb{Q}}), (X_0 : \dots : X_n) \mapsto (Y_0 : Y_{s+1} : \dots : Y_n),$$

and

$$\pi_i : V \setminus \mathcal{Z}(Y_0, Y_i, Y_{s+1}, \dots, Y_n) \to \mathbb{P}^{n-s+1}(\overline{\mathbb{Q}}),$$
$$(X_0 : \dots : X_n) \mapsto (Y_0 : Y_i : Y_{s+1} : \dots : Y_n), \quad 1 \le i \le s.$$

There are linear forms $Y_0, \dots, Y_n$ such that $Y_0(x) \neq 0$ and

(i) the projection π is finite, i.e. $V \cap \mathcal{Z}(Y_0, Y_{s+1}, \dots, Y_n) = \emptyset$,

(ii) $\pi^{-1}(\pi(x))$ consists of $\deg V$ different points,

(iii) $\#(Y_i/Y_0)(\pi^{-1}(\pi(x))) = \#\pi^{-1}(\pi(x))$ for every $1 \le i \le s$.

By (ii) the differential $d_x\pi$ in the point x of the projection π is an isomorphism. The projection π_i is also finite for every $1 \le i \le s$. Hence the set $\pi_i(V)$ is closed in the Zariski topology and $\pi_i(V)$ is a set of zeroes of a homogeneous polynomial $h_i \in \mathbb{Z}[Y_0, Y_i, Y_{s+1}, \dots, Y_n]$ of the degree $\deg h_i = \deg V$ by (iii). By the Zariski main theorem the point $\pi_i(x)$ is smooth on $\pi_i(V)$. The implicit function theorem implies now $h_1/L^D, \dots h_s/L^D$ is a system of local parameters of V in the point x. But $h_1, \dots h_s$ are linear combinations of polynomials H_e, $e \in E$. Therefore, the required system of local parameters can be chosen among polynomials H_e/L^D, $e \in E$. The lemma is proved.

LEMMA 2 *Let $V \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ be an irreducible and defined over $\mathbb{Q}$ projective algebraic variety of dimension $n-s$, $1 \le s \le n$. Let V be given by the generic projection and $H = H_V$ be the corresponding polynomial. Let the degree $\deg V < D'$ and lengths of integer coefficients of H_V be less than M'. Let $F \in \mathbb{Q}[X_0, \dots, X_n]$ be a homogeneous polynomial of the degree D'', $D'' \ge 1$, and lengths of integer* *coefficients less than M''. Suppose that F is not vanishing on V. Let W_1 be an arbitrary irreducible and defined over $\mathbb{Q}$ component of the algebraic variety $V \cap \mathcal{Z}(F)$. Let the degree* $\deg W_1 = D'''$. *Then the degree of the intersection $V \cap \mathcal{Z}(F)$ is less than $D'D''$ and the component W_1 can be given by the generic projection. The corresponding polynomial H_{W_1} has integer coefficients with the lengths less than*

$$(M' + M'' + n^2)\mathcal{P}(D'D'') \tag{6}$$

for a polynomial $\mathcal{P}$. These polynomials H_{W_1} giving all the components W_1 can be constructed within the time polynomial in $(D'D'')^{n^2}$, M', M''.

PROOF Set $W = V \cap \mathcal{Z}(F)$. Denote $H = H_V$.

Let $U_0, U_s, \ldots, U_n$ be generic linear forms such as above. Denote for brevity

$$\mathcal{U}' = \{u_{i,j}\}_{i=0,s+1,\ldots,n,\, 0\le j\le n}$$

and the fields $K = \mathbb{Q}(\mathcal{U}')$, $K_1 = \mathbb{Q}(\mathcal{U}', Z_0, Z_{s+1}, \ldots, Z_n)$

Set

$$R_H^{(1)} = \mathrm{Res}_{Z_s}(H'_{Z_s}, H) \in K_1[u_{s,0}, \ldots, u_{s,n}]$$

and

$$R_H^{(2)} = \prod_{0\le i\ne j\le n} (u_{s,i} - u_{s,j}) \prod_{1\le i\le n+2} R^{(1)}(u^i_{s,0}, \ldots, u^i_{s,n})$$

There are integers $u_0, u_{s+1}, \ldots, u_n$ with lengths $O(\log(nD'))$ such that

$$R_H^{(2)}(u_0, u_{s+1}, \ldots, u_n) \ne 0.$$

Set $Y = \sum_{0\le j\le n} u_j X_j$ and $L_i = \sum_{0\le j\le n} u_j^{i+2} X_j$, $0 \le i \le n$. Note that $X_0, \ldots, X_n$ are linear combinations of $L_0, \ldots, L_n$ with rational coefficients with lengths of numerators and denominators $O(n\log(nD'))$.

Denote by $\Phi \in \mathbb{Z}[\mathcal{U}', Z_0, Z, Z_{s+1}, \ldots, Z_n]$ (here Z is a new variable) the homogeneous relative to $Z_0, Z, Z_{s+1}, \ldots, Z_n$ polynomial

$$\Phi(\mathcal{U}', Z_0, Z, Z_{s+1}, \ldots, Z_n) = H(\mathcal{U}, Z_0, Z, Z_{s+1}, \ldots, Z_n)|_{u_{s,j}=u_j,\, 0\le j\le n}$$

(one should substitute here the coefficients u_j instead of generic coefficients $u_{s,j}$, $0 \le j \le n$). Similarly denote by $\Phi_i \in \mathbb{Z}[\mathcal{U}', Z_0, Z, Z_{s+1}, \ldots, Z_n]$, $0 \le i \le n$, the homogeneous relative to $Z_0, Z, Z_{s+1}, \ldots, Z_n$ polynomial

$$\Phi_i(\mathcal{U}', Z_0, Z, Z_{s+1}, \ldots, Z_n) = H(\mathcal{U}, Z_0, Z, Z_{s+1}, \ldots, Z_n)|_{u_{s,j}=u_j^{i+2},\, 0\le j\le n}.$$

Denote by $R = \mathrm{Res}_{Z_s}(\Phi'_{Z_s}, \Phi)$ and $R_i = \mathrm{Res}_{Z_s}((\Phi_i)'_{Z_s}, \Phi_i)$, $0 \le i \le n$, the discriminants of the polynomials Φ and Φ_i respectively. So

$$R = (R_H^{(1)})|_{u_{s,j}=u_j,\, 0\le j\le n}, \quad R_i = (R_H^{(1)})|_{u_{s,j}=u_j^{i+2},\, 0\le j\le n},\ 0 \le i \le n.$$

The polynomials Φ and Φ_i are non–zero separable and, therefore, irreducible since V is irreducible. Hence all the elements $\theta = Y/U_0$ and L_i/U_0, $0 \le i \le n$ are primitive elements of the extension

$$K(V) \supset K(U_{s+1}/U_0, \ldots, U_n/U_0).$$

For every $0 \le i \le n$ factor using the algorithm from [2] the polynomial Φ_i over the field $K(U_{s+1}/U_0, \ldots, U_n/U_0)[\theta]$ and construct the generic point

$$\chi_i = (L_i/U_0)|_V \in K(U_{s+1}/U_0, \ldots, U_n/U_0)[\theta],\ 0 \le i \le n \tag{7}$$

$$\chi_i = \sum_{0 \le j < \deg_Y \Phi} \chi_{i,j}\theta^j,\ \chi_{i,j} \in K(U_{s+1}/U_0, \ldots, U_n/U_0) \tag{8}$$

of the algebraic variety V over the field K. So we can write

$$\chi_{i,j} = \chi_{i,j}(U_0, U_{s+1}, \ldots, U_n).$$

According to the algorithm for factoring polynomials from [2] the degrees of numerators and denominators (they belong to $\mathbb{Z}[\mathcal{U}', U_0, U_{s+1}, \ldots, U_n]$) of all $\chi_{i,j}$ relative to every U_i, $i = 0, s+1, \ldots, n$, and every $u_{i,j}$, $i = 0, s+1, \ldots, n$, $0 \le j \le n$ are bounded from above by a polynomial in D'. The lengths of integer coefficients of these numerators and denominators are bounded from above by $(M' + n^2)\mathcal{P}(D')$ for a polynomial $\mathcal{P}$.

Denote by $R = \mathrm{Res}_Z(\Phi'_Z, \Phi) \in \mathbb{Z}[\mathcal{U}', Z_0, Z_{s+1}, \ldots, Z_n]$ the discriminant of Φ relative to Z. Similarly define the discriminants R_i for the polynomials Φ_i, $0 \le i \le n$.

Now we have

$$Z_0^{a_{i,j}} R R_i \chi_{i,j}(Z_0, Z_{s+1}, \ldots, Z_n) \in K[Z_0, Z_{s+1}, \ldots, Z_n]$$

for some integers $a_{i,j}$ since
$R_i(1, U_{s+1}/U_0, \ldots, U_n/U_0)\chi_i$ is integral over $K[U_{s+1}/U_0, \ldots, U_n/U_0]$ and the integral closure of $K[U_{s+1}/U_0, \ldots, U_n/U_0]$ in $K(U_{s+1}/U_0, \ldots, U_n/U_0)[\theta]$ is contained in

$$(1/R(1, U_{s+1}/U_0, \ldots, U_n/U_0)) \sum_{0 \le j < \deg_Y \Phi} K[U_{s+1}/U_0, \ldots, U_n/U_0]\theta^j.$$

Let $\varepsilon > 0$ be an infinitesimal relative to the field K. Then the mapping of standard part

$$\mathrm{st} : \mathbb{P}^n(\overline{K(\varepsilon)}) \to \mathbb{P}^n(\overline{K})$$

is defined, see [3] (the standard part of the element $z \in \mathbb{P}^n(\overline{K(\varepsilon)})$ is an element $z_1 \in \mathbb{P}^n(\overline{K})$ which is infinitesimal close to z). Consider the algebraic variety

$$W_\varepsilon = V \cap \mathcal{Z}(F - \varepsilon U_0^{D''}) \subset \mathbb{P}^n(\overline{K(\varepsilon)}).$$

Let W_2 be an irreducible and defined over $K(\varepsilon)$ component of W_ε. Then we have $\mathrm{st}(W_\varepsilon) = W$ and $\mathrm{st}(W_2)$ is a union of some irreducible and defined over K components of W, c.f. [3]. Further, the dimension of every component W_2 of W_ε is $n - s - 1$. Choose and fix W_2 such that $\mathrm{st}(W_2) \supset W_1$. So there exists a uniquely defined irreducible polynomial from $\mathbb{Z}[\mathcal{U}', \varepsilon, Z_0, Z_{s+1}, \ldots, Z_n]$ homogeneous relative to $Z_0, Z_{s+1}, \ldots, Z_n$ which is vanishing on W_2.

Let us show that R is not vanishing on W_2. Indeed, if $R(W_2) = \{0\}$ then $W_2 \subset V \cap \mathcal{Z}(R)$. But all the components of $V \cap \mathcal{Z}(R)$ are defined over K and have the dimension $n - s - 1$ since Φ is separable. Therefore, W_2 is also defined over K. Hence, the polynomials F and U_0 are vanishing on W_2 which contradicts to the fact that no components of W lie in $\mathcal{Z}(U_0)$.

Similarly one can prove that R_i is not vanishing on W_2 for every $0 \le i \le n$.

Now the polynomial $H_1 = H_{W_1}$ can be obtained from the following construction. Denote by

$$N_\theta : K(\varepsilon, U_{s+1}/U_0, \ldots, U_n/U_0)[\theta] \to K(\varepsilon, U_{s+1}/U_0, \ldots, U_n/U_0)$$

the mapping of the norm of the extension of fields. Denote by $\widetilde{F}$ the polynomial with rational coefficients in $n+1$ variables such that $\widetilde{F}(L_0, \ldots, L_n) = F$. Consider the rational function

$$F_1(\varepsilon, U_0, U_{s+1}, \ldots, U_n) = N_\theta(\widetilde{F}(\chi_0, \ldots, \chi_n) - \varepsilon) \in K(\varepsilon, U_{s+1}/U_0, \ldots, U_n/U_0).$$

Represent

$$F_1(\varepsilon, U_0, U_{s+1}, \ldots, U_n) = F_2(\varepsilon, U_0, U_{s+1}, \ldots, U_n)/F_3(\varepsilon, U_0, U_{s+1}, \ldots, U_n)$$

where $F_2, F_3 \in K[\varepsilon, Z_0, Z_{s+1}, \ldots, Z_n]$ are homogeneous relative to Z_0, Z_{s+1}, $\ldots, Z_n$ polynomials and $\mathrm{GCD}(F_2, F_3) = 1$. Note that the denominator F_3 divides $(Z_0 R \prod_{0 \le i \le n} R_i)^a$ for some integer $a \ge 1$. So the rational function

$$F_2(\varepsilon, U_0, U_{s+1}, \ldots, U_n)/F_3(\varepsilon, U_0, U_{s+1}, \ldots, U_n)$$

is defined on the component W_2 and the polynomial $F_2(\varepsilon, U_0, U_{s+1}, \ldots, U_n)$ is vanishing on W_2. Since W_1 is a component of $\mathrm{st}(W_2)$ the polynomial H_1 coincides with an irreducible factor of $F_2(0, Z_0, Z_{s+1}, \ldots, Z_n)$.

¿From the described construction using [2] and the ascertained estimations for degrees and lengths of integer coefficients of $\chi_{i,j}$ we get immediately (6). The lemma is proved.

Now our aim is to prove Theorem 2. In what follows when it is required to construct a system of polynomial equations for any affine algebraic variety $U \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ we shall construct system of homogeneous polynomial equations corresponding to the generic projection of its closure in $\overline{U} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ by Lemma 2 and [2]. This will gives a system for U. The condition (c) when it is required will be satisfied by Lemma 1.

Compute using [2] all the irreducible and defined over $\mathbb{Q}$ components W_i of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k) = V_1$. Then according to [2] the estimations of Theorem 2 for $D_1^{(s)}$ and $M_1^{(s)}$ are fulfilled for the components of $V_1^{(s)}$, $1 \leq s \leq n$.

Let $1 \leq r < n$ and suppose that we have constructed recursively all the components W_i, $i \in I_r$ of the algebraic variety V_r. Further, suppose that (a)–(c) hold and the required estimations for $D_r^{(s)}$ and $M_r^{(s)}$ are fulfilled for the components of $V_r^{(s)}$, $r \leq s \leq n$.

Let us show how to construct all the components of $V_{r+1}^{(s)}$ for all s such that $r+1 \leq s \leq n$. Let W_i and W_j be irreducible and defined over $\mathbb{Q}$ components of V_r of codimensions s_i and s_j and degrees D_i and D_j respectively, herewith $s_i \geq s_j$. Denote by $B_i' = A^s \times \{1, \ldots, n\}^s$. For every

$$\beta = ((\alpha_1, \ldots, \alpha_s), (j_1 \ldots, j_s)) \in B_i'$$

compute the Jacobian

$$J_\beta = \det \left(\frac{\partial h_{\alpha_u}}{\partial X_{j_v}} \right)_{1 \leq u, v \leq s}.$$

Compute a maximal subset $B_i \subset B_i'$ such that all the Jacobians J_β, $\beta \in B_i$ are linearly independent. We have by (c)

$$\operatorname{Sing} W_i = W_i \cap \mathcal{Z}(\{J_\beta\}_{\beta \in B_i}),$$

Further, $\deg J_\beta \leq s_i(D_i - 1) < s_i D_i$ and the degree of the union of all the components of codimension $s_i + w$ of $\operatorname{Sing} W_i$ is less than $D_i(s_i D_i)^w$. So if $s > s_i$ then the degree of the union of all the components of codimension s of $\operatorname{Sing} W_i$ is less than $D_i(s_i D_i)^{s-s_i}$. Similarly if $s > s_i$ then the degree of the union of all the components of codimension s of the intersection $W_i \cap W_j$ is less than $D_i D_j^{s-r_i}$. Note that

$$\sum_{\{i : s_i = u\}} D_i \leq (ud)^{2^u - 1}$$

for every $r \leq u \leq n$. Therefore, the degree of $V_{r+1}^{(s)}$ is less than

$$\sum_{\{i : s > s_i\}} D_i(s_i D_i)^{s-s_i} + \sum_{\{(i,j) : s > s_i \geq s_j\}} D_i D_j^{s-s_i} \leq$$

$$\sum_{1\le u\le s-1}\sum_{\{i:s_i=u\}} D_i(uD_i)^{s-u} + \sum_{1\le u\le s-1}\sum_{1\le v\le u}\sum_{\{(i,j):s_i=u,s_j=v\}} D_iD_j^{s-u} \le$$

$$\sum_{1\le u\le s-1}(ud)^{(2^u-1)(s-u+1)}u^{s-u} + \sum_{1\le u\le s-1}\sum_{1\le v\le u}(ud)^{2^u-1}(vd)^{(2^v-1)(s-u)} \le$$

$$d^{2^s-1}(\sum_{1\le u\le s-1}u^{2^u-1}(u^{2^u(s-u)} + \sum_{1\le v\le u}v^{(2^v-1)(s-u)})) \le$$

$$d^{2^s-1}\sum_{1\le u\le s-1}u^{2^u-1}(2u^{2^u(s-u)}) \le d^{2^s-1}\sum_{1\le u\le s-1}2u^{2^u(s-u+1)-1} \le$$

$$d^{2^s-1}s^{2^s-1}\sum_{1\le u\le s-1}2(u^{2^u(s-u+1)-1}/s^{2^s-1}) \le (sd)^{2^s-1}2(s-1)(1-1/s)^{2^s-1} \le$$

$$(sd)^{2^s-1}$$

Thus, we have proved the required estimations of Theorem 2 for $D_{r+1}^{(s)}$.

Now to complete the proof it is sufficient to prove the estimation for $M_{r+1}^{(s)}$. Each component of $V_{r+1}^{(s)}$ is a component of $\operatorname{Sing} W_i$ or $W_i\cap W_j$ where W_i and W_j are components of V_r, see above.

Suppose that W is a component of $\operatorname{Sing} W_i$. Then there are polynomials $F_{u+1},\ldots,F_s$ which are linear combinations of J_β, $\beta\in B_i$, with integer coefficients of the lengths $O(n\log(s_iD_i))$ satisfying the following property. There is a sequence of irreducible and defined over $\mathbb{Q}$ algebraic varieties

$$W^{(u)} = W_i,\ W^{(u+1)},\ \ldots,\ W^{(s)} = W$$

such that $W^{(j+1)}$ is a component of $W^{(j)}\cap\mathcal{Z}(F_{j+1})$ for every $u\le j<s$. Similarly in the case when W is a component of $W_i\cap W_j$ there are analogous sequences of polynomials and irreducible and defined over $\mathbb{Q}$ algebraic varieties (for estimations one should take $s_i\ge s_j$).

In the both cases the estimation for $M_{r+1}^{(s)}$ can be obtained now by subsequent applying Lemma 2 using the ascertained inequalities for $M_r^{(a)}$. One should only take the degree of the polynomial $\mathcal{P}$ from Theorem 2 sufficiently great relative to the degree of the polynomials from Lemma 2. It is convenient also for recursive estimations to write the statement of Theorem 2 in the form

$$M_r^{(s)} \le 3^s(M+n^2)\mathcal{P}((sd)^{2^s-1})$$

which allows easily to take into account the addition $M'+M''+n^2$ when Lemma 2 is applied. The theorem is proved.

The proof of Theorem 3 is completely analogous to the one of Theorem 2 and even easier since one should not consider the intersections of different components but only the sets of singular points of the components. Theorem 3 is also proved.

2 Solvability of systems over p-adics and branched smooth stratification

Our aim is to prove Theorem 4. Let $a \neq 0$ be an integer. Set $\mathrm{ord}_p(a) = b \in \mathbb{Z}$ if and only if $a/p^b \in \mathbb{Z}$ but $a/p^{b+1} \notin \mathbb{Z}$. If $z \in \mathbb{R}$ then set $[z]$ to be the maximal integer z_0 such that $z_0 \leq z$ and define $[z]_+ = \max\{[z], 1\}$.

It is convenient also to introduce the algebraic variety $W_1 = \mathbb{A}^n(\overline{\mathbb{Q}})$ and set $M_0 = M$, $D_0 = d$. So the codimension $\mathrm{codim}\, W_1 = 0$, the degree $\deg W_1 = 1$ and W_1 is given by an empty system of equations. Let $W_{i_1,\ldots,i_r} \neq \emptyset$ and $V_{i_1,\ldots,i_r} = \emptyset$ for some $1 \leq r \leq n_0 + 1$. Then set $W_{i_1,\ldots,i_r,i_{r+1}} = \emptyset$ where $i_{r+1} \in I_{i_1,\ldots,i_r}$ and $I_{i_1,\ldots,i_r}$ is an one element set. Set also $\deg W_{i_1,\ldots,i_r,i_{r+1}} = 0$, $\mathrm{codim}\, W_{i_1,\ldots,i_r,i_{r+1}} = n+1$ if $V_{i_1,\ldots,i_r} = \emptyset$. In this case the algebraic variety $W_{i_1,\ldots,i_r,i_{r+1}}$ is given by one equation $1 = 0$.

We shall construct integers $c^{(s)}$, $0 \leq s \leq n$, which are less than $M_s\mathcal{P}(((s+1)D_s)^{n^2})$ for a polynomial $\mathcal{P}$ and satisfy the property described below.

Set

$$\Delta = \prod_{0 \leq s \leq n} (c^{(s)})^{2^s \prod_{0\leq t\leq s}((t+1)D_t)^n}.$$

Let $x \in \mathbb{Z}^n$ be a point such that $f_i(x) = 0 \bmod p^N$, $1 \leq i \leq k$. Set $N_0 = N$ and

$$N_u = [\sum_{u\leq s\leq n} 2^{s-u}\, \mathrm{ord}_p(c^{(s)}) \prod_{u\leq t\leq s} ((t+1)D_t)^n]_+.$$

So $N_0 = N$ and $1 \leq N_u \in \mathbb{Z}$ for all $0 \leq u \leq n+1$. If $N_u = 1$ then $\mathrm{ord}_p(c^{(s)}) = 0$ and $N_s = 1$ for all $s \geq u$. Recall that $h_\alpha = 0$, $\alpha \in A_{i_1,\ldots,i_r}$ is the system of polynomial equations of the algebraic variety $W_{i_1,\ldots,i_r}$, $1 \leq r \leq n_0 + 2$, from the described construction of branched smooth stratification (and the previous remark).

The property of the integers $c^{(s)}$ is the following one. Let $1 \leq r \leq n_0+1$ and there is an algebraic variety $W_{i_1,\ldots,i_r}$ with the codimension $\mathrm{codim}\, W_{i_1,\ldots,i_r} = u$, $0 \leq u \leq n$ such that

$$h_\alpha(x) = 0 \bmod p^{N_u}. \tag{9}$$

Then the similar statement holds for $r+1$ or $r \geq 2$ and there is a point in $W_{i_1,\ldots,i_r}$ with coordinates from $\mathbb{Z}_p$.

Let us show that it is sufficient to construct $c^{(s)}$ and prove this property to finish the proof of the theorem. Indeed, suppose that $c^{(s)}$ are constructed and this property is proved. Suppose that there are no points with coordinates from $\mathbb{Z}_p$ in any $W_{i_1,\ldots,i_r}$ with $r \geq 2$. Then (9) is valid for some empty $W_{i_1,\ldots,i_r}$,

$1 \leq r \leq n_0 + 2$. We get a contradiction $1 = 0 \bmod p^{N_u}$ which proves our assertion.

Thus, suppose that $0 \leq r \leq n_0 + 1$ and we have proved by induction that there is an algebraic variety $W_{i_1,\dots,i_r}$ with the codimension $\operatorname{codim} W_{i_1,\dots,i_r} = u$, $0 \leq u \leq n$ such that (9) holds for all α. Our aim will be to prove the similar statement for $r+1$ or if $r \geq 2$ to show that there is a point in $W_{i_1,\dots,i_r}$ with coordinates from $\mathbb{Z}_p$ (more precisely, in the latter case we shall show how to construct such a point).

If $r \geq 2$ then the degrees of the Jacobians J_β, $\beta \in B$, (from the considered construction) defining the set of singular points of the algebraic variety $W_{i_1,\dots,i_r}$ are less than uD_u and lengths of integer coefficients of these Jacobians are less than $(M+n^2)P_1(uD_u)$ for a polynomial P_1. Set $N'_u = N_u/2$ if N_u is even and $N'_u = (N_u+1)/2$ if N_u is odd. If

$$J_\beta(x) \neq 0 \bmod p^{N'_u}, \tag{10}$$

then the standard Hensel lemma (one should fix the variables to which there are no partial derivatives in the Jacobian matrix) shows that there is a point in $W_{i_1,\dots,i_r}$ with coordinates from $\mathbb{Z}_p$. Note that $[N_u/2]_+ \leq N'_u$ since $1 \leq N_u \in \mathbb{Z}$. So we shall suppose without loss of generality that

$$J_\beta(x) = 0 \bmod p^{[N_u/2]_+},$$

for all β. Recall that if $r \geq 2$ then

$$V_{i_1,\dots,i_r} = W_{i_1,\dots,i_r} \cap \mathcal{Z}(\{J_\beta\}_{\beta \in B}).$$

Denote by $G_\rho = 0$, $\rho \in R$, the system of polynomial equations defining the algebraic variety $V_{i_1,\dots,i_r}$ in our construction. In the case when $r \geq 2$ this system consists of all equations $h_\alpha = 0$ and $J_\beta = 0$. When $r = 1$ the polynomials G_ρ coincide with the initial polynomials $f_1, \dots, f_k$.

Set $\delta = (uD_u)^n$, $\mu = M_u$ $\nu = [N_u/2]_+$ if $r \geq 2$ and $\delta = d^n$, $\mu = M$, $\nu = N_0$ if $r = 1$. Note that $\# I_{i_1,\dots,i_r} \leq \delta$ by the Bézout inequality.

Let $i_{r+1} \in I_{i_1,\dots,i_r}$. Consider the vector space $S_{i_{r+1}}$ over the field $\mathbb{Q}$ of all polynomials of degrees at most $\deg W_{i_1,\dots,i_r,i_{r+1}}$ vanishing on $W_{i_1,\dots,i_r,i_{r+1}}$. Note that

$$\deg W_{i_1,\dots,i_r,i_{r+1}} \leq \delta.$$

Let the dimension $\dim S_{i_{r+1}} = w_{i_{r+1}}$. Note that $w_{i_{r+1}} \leq \delta^n$. Set

$$w = \max_{i_{r+1} \in I_{i_1,\dots,i_r}} w_{i_{r+1}}.$$

According to [2] the set of zeroes of the polynomials from $S_{i_{r+1}}$ coincides with $W_{i_1,\dots,i_r,i_{r+1}}$ and there is a basis $s_0,\dots,s_\kappa \in \mathbb{Z}[X_1,\dots,X_n]$ of $S_{i_{r+1}}$ consisting of polynomials with the lengths of integer coefficients less than $\mu P_2(\delta^n)$ for a polynomial P_2. We shall suppose without loss of generality that all the polynomials h_α, $\alpha \in A_{i_1,\dots,i_{r+1}}$ are linearly independent and are contained in the basis $s_0,\dots,s_\kappa$.

Consider the polynomials $G_{i_{r+1},\gamma} = \sum_j \gamma^j s_j$ where $0 < \gamma \in \mathbb{Z}$. So the set of zeroes of the family $G_{i_{r+1},\gamma}$, $1 \le \gamma \le \Gamma_{i_1,\dots,i_r} = w\delta$, coincides with $W_{i_1,\dots,i_r,i_{r+1}}$, any $w' \le w_{i_{r+1}}$ of polynomials $G_{i_{r+1},\gamma}$ are linearly independent over $\mathbb{Q}$ and the lengths of their integer coefficients are less than $\mu P_3(\delta^n)$ for a polynomial P_3.

By the efficient Hilbert Nullstellensatz [6] we have

$$c_{i_1,\dots,i_r,\gamma}(\prod_{i_{r+1}} G_{i_{r+1},\gamma})^\delta = \sum_{\rho\in R} G_\rho q_{\rho,\gamma} \tag{11}$$

where $c_{i_1,\dots,i_r,\gamma} \in \mathbb{Z}$, $q_{\rho,\gamma} \in \mathbb{Z}[X_1,\dots,X_n]$ are polynomials for all ρ,γ. The coefficients of polynomials $q_{\rho,\gamma}$ can be estimated from solving a linear system. This gives also an estimation for $c_{i_1,\dots,i_r,\gamma}$. So we get $|c_{i_1,\dots,i_r,\gamma}| \le 2^{\mu P_4(\delta^n)}$ for a polynomial P_4. Construct $c_{i_1,\dots,i_r,\gamma}$ solving linear system (11). Construct also the set

$$C_u = \{(i_1,\dots,i_\kappa,\gamma) \,:\, \operatorname{codim} W_{i_1,\dots,i_\kappa} = u,\, 0 \le \kappa \le n_0+1,\, 1 \le \gamma \le w\delta\}.$$

Define the integers

$$c_1^{(u)} = \prod_{1\le i_1<i_2\le w\delta} (i_2 - i_1), \quad c_2^{(u)} = \prod\nolimits_{(i_1,\dots,i_\kappa,\gamma)\in C_u} c_{i_1,\dots,i_\kappa,\gamma}, \quad c^{(u)} = c_1^{(u)} c_2^{(u)}.$$

for $0 \le u \le n$. We have by our construction $\#C_u \le (D_u)^{n_0} w\delta \le (D_u)^n \delta^{n+1}$ and $|c^{(u)}| \le 2^{\mu P_5(\delta^n)}$ for a polynomial P_5. Hence, $|c^{(u)}| \le 2^{M_u P_5(((u+1)D_u)^{n^2})}$ for a polynomial $\mathcal{P}$. Compute Δ. We get now

$$\Delta \le 2^{M\mathcal{P}(d^{n^2}) + \sum_{1\le s\le n} M_s \mathcal{P}((sD_s)^{n^2}) \prod_{0\le t<s} (tD_t)^n}$$

for a polynomial $\mathcal{P}$.

Let $V_{i_1,\dots,i_r} \ne \emptyset$. Denote $\operatorname{ord}_p(c_2^{(u)}) = m''_u$ and $\operatorname{ord}_p(c^{(u)}) = m_u$. Since we chose $\Gamma_{i_1,\dots,i_r} = w\delta$ there exists i_{r+1} such that

$$G_{i_{r+1},\gamma_j}(x) = 0 \bmod p^{[(\nu - \operatorname{ord}_p(c_{i_1,\dots,i_r,\gamma}))/\delta]_+}$$

for w different indices γ_j, $1 \le j \le w$. Hence,

$$G_{i_{r+1},\gamma_j}(x) = 0 \bmod p^{[(\nu - m''_u)/\delta]_+}$$

for w different indices γ_j, $1 \leq j \leq w$. The set of zeroes of these polynomials G_{i_{r+1},γ_j} coincides with $W_{i_1,\ldots,i_r,i_{r+1}}$. Since every polynomial h_α, $\alpha \in A_{i_1,\ldots,i_{r+1}}$ is a linear combination of G_{i_{r+1},γ_j} we have also by the definition of $c^{(u)}$

$$h_\alpha(x) = 0 \bmod p^{[(\nu - m_u)/\delta)]_+}. \tag{12}$$

Let the codimension of $W_{i_1,\ldots,i_r,i_{r+1}}$ is v. Since $v > u$ we get immediately from (12) that

$$h_\alpha(x) = 0 \bmod p^{N_v}.$$

for all $\alpha \in A_{i_1,\ldots,i_{r+1}}$. The theorem is proved.

REMARK 1 *It is not necessary to use the result from [6] to prove Theorem 1. For the proof of Theorem 1 it is sufficient to take in (11), e.g.* δ^{2^n} *instead of* δ.

References

[1] **Birch B. J., McCann K.:** *"A criterion for p-adic solubility of Diophantine equations"*, Quart. J. Math. Oxford 18 # 2 (1967), pp. 59–63.

[2] **Chistov A. L.:** *"Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137 (1984), pp. 124–188 (Russian) [English transl.: J. Sov. Math. 34 (4) (1986)].

[3] **Chistov A. L.:** *"Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic"*, Journal of Pure and Applied Algebra, 117 & 118 (1997) pp. 145–175.

[4] **Hodge W. V. D., Pedoe D.** *"Methods of algebraic geometry"*, v. 2, Cambridge 1952.

[5] **Karpinski M., van der Poorten, Shparlinski I.:** *"Zero testing of p-adic and Modular Polynomials"*, Research Report No. 85175-CS, Univ. Bonn, 1997.

[6] **Kollar J.:** *"Sharp effective Nullstellensatz"*, J.A.M.S. 1 (1988), pp. 963–975.