St. Petersburg Mathematical Society Preprint Series
Submitted 16.09.2021, version 2
Available at: http://www.mathsoc.spb.ru/preprint/

# An Effective Algorithm for Deciding Solvability of a System of Polynomial Equations over $p$-adic Integers

Alexander L. Chistov

St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia,
e-mail: alch@pdmi.ras.ru

2021

**Abstract**

Consider a system of polynomial equations in $n$ variables of degrees at most $d$ with integer coefficients with the lengths at most $M$. We show using the construction close to smooth stratification of algebraic varieties that one can construct a positive integer

$$\Delta < 2^{M(nd)^{c\,2^n n^3}}$$

(here $c > 0$ is a constant) depending on these polynomials and satisfying the following property. 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 $\Delta$. This improves the previously known, at present classical result by B. J. Birch and K. McCann.

## Introduction

Let $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials, $n \geqslant 1$. Assume that for all $i$ the degrees

$$\deg_{X_1,\ldots,X_n} f_i \leqslant d$$

and the lengths of integer coefficients of the polynomials $f_i$ are bounded from above by $M$ (it means that the absolute value of every coefficient of each $f_i$ is at most $2^{M-1}$). Here $d \geqslant 3$ and $M \geqslant 1$ are integers. We shall suppose without loss of generality that $f_1, \ldots, f_k$ are linearly independent over $\mathbb{Q}$ and $k \geqslant 1$. In particular $f_1 \neq 0$.

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 $\mathbb{Q}$. The dimension $\dim \mathcal{Z}(f_1, \ldots, f_k) \leqslant n-1$ since $f_1 \neq 0$.

Key words and phrases: $p$-adic integers, polynomial systems, decidability algorithm.
UDK 512.7+511.525
2000 Mathematics Subject Classification: 11D88, 14Q15.

By definition the degree of an irreducible affine (or quasiprojective) algebraic variety is equal to the degree of its closure in the corresponding projective space. The degree of an arbitrary affine (or quasiprojective) algebraic variety is equal to the sum of the degrees of its irreducible components.

By definition the codimension of an affine algebraic variety $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ is equal to $n - \dim V$ where $\dim V$ is the dimension of $V$ (the dimension of an empty variety is equal to $-1$). Put $m$ to be the codimension of the algebraic variety $\mathcal{Z}(f_1, \dots, f_k)$. So $1 \leqslant m \leqslant n+1$.

Let $\mathbb{Z}_p$ be the ring of all $p$-adic integers.

**THEOREM 1** *For given polynomials $f_1, \dots, f_k$ there are an absolute constant $c > 0$ and a positive integer*

$$\Delta < 2^{M(nd)^{c\, m\, 2^{n-m} n^3}} < 2^{M(nd)^{c\, 2^n\, n^3}}$$

*satisfying the following property. 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 $N$ such that $p^N$ does not divide $\Delta$. The constant $c$ can be computed explicitly from the proof of this theorem. The codimension $m$ can be computed within the time polynomial in $M$ and $d^{n^2}$. The integer $\Delta$ can be constructed within the time polynomial in $M(nd)^{m\, 2^{n-m} n^3}$.*

The previous result on this subject was obtained in the well known paper by B. J. Birch and K. McCann [8] 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 [8] gives

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

i.e.

$$\Delta < 2^{Md^{(Cn)^n}}.$$

for a constant $C \geqslant 1$. So our result improves the highest level exponent from $n \log_2(Cn)$ to $n(1 + o(1))$. As far as we know the estimate from Theorem 1 is the best known so far. Thus our result is important.

The present paper has an interesting history. Actually it contains our old unpublished result. Initially, more than twenty years ago, I wrote a preprint [9] during my stay in Bonn by the program “Volkswagen Stiftung”. There are two authors of this preprint. I suggested the main ideas of the preprint and their technical realization. Actually I did all the work. Marek Karpinski was the host of the program in Bonn. The contribution of M. Karpinski was mainly in stimulating me to investigate this problem by persistent discussions of the subject (but in truth they gave no new ideas). I would like to thank again M. Karpinski for hospitality and good conditions for my fruitful research at that time. Now due to the importance of this result and no new progress in this area (in the considered general situation) since that time I decided at last to publish the obtained result in a journal. One should note that the preprint [9] was written not very accurately. It was not ready for publishing in a journal. There are many small drawbacks in it. So I made a decision to revise this preprint completely. In the present paper a lot of work has been done to correct the inaccuracies from [9].

Now we would like to formulate some problems.

**PROBLEM 1** Is it possible to strengthen Theorem 1? Namely is it possible to replace $(nd)^{c\,m\,2^{n-m}n^3}$ by $d^{n^c}$ (where the constant $c > 0$ is absolute) in the statement of Theorem 1?

**PROBLEM 2** Are there an absolute constant $c > 0$ and constants $C(n) > 0$ (depending on $n$) satisfying the following property? Let $p$ be an arbitrary prime number. Then any system from Theorem 1 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 $N \log p \geqslant C(n) M d^{n^c}$.

The last problem is motivated by our deep result from [2]. There we construct a smooth stratification of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$ with strata given by equations of degrees bounded from above by $C(n)d$ and with the number of strata at most $C(n)d^{n^2}$, i.e., all the strata have the degrees bounded from above by a linear polynomial in $d^n$ for sufficiently large $d$ (the bound for $d$ here depends on $n$). In papers devoted to smooth stratification of algebraic varieties of all other authors the bound for degrees of strata is like $d^{n^{cn}}$ (or may be $d^{2^{cn}}$). This double exponential bound is proved always more or less straightforward. In [2] a slightly different definition of smooth stratification is used. There might be some long sequences $W_1, W_2, \ldots, W_m$ of smooth strata of the same dimension such that the intersections of closures $\overline{W}_i \cap \overline{W}_{i+1} \neq \varnothing$ for all $1 \leqslant i < m$. This is an obstacle to use directly the result of [2] (in place of Theorem 3, see below) to the subject of the present paper. However the question is not closed here.

We consider the ring $\mathbb{Z}_p$ of $p$-adic integers. But, of course, the main problem in this area remains to obtain an explicit complexity bound for the decidability of polynomial systems over the field $\mathbb{Q}_p$ of $p$-adic numbers. We could not solve it at that time in Bonn, more than twenty years ago. But I noticed that most likely an effective algorithm for the decidability of polynomial systems over $\mathbb{Q}_p$ is inseparably linked with obtaining an explicit complexity bound for desingularization of algebraic varieties in zero characteristic (possible it will be sufficient to get estimates for some numerical invariants related to the desingularization).

Let us return to the present paper. Note that the analogs of Theorem 1 and Theorem 4, see below, are true if one consider homogeneous polynomials $f_1, \ldots, f_k \in \mathbb{Z}[X_0, \ldots, X_n]$ and their nonzero solutions, i.e. the solutions in $\mathbb{Z}_p^{n+1} \setminus \{(0, \ldots, 0)\}$ and $(\mathbb{Z}/p^N\mathbb{Z})^{n+1} \setminus \{(0, \ldots, 0)\}$ respectively. The proofs are similar if we consider projective spaces in place of 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 nonzero solution in $\mathbb{Z}_p^{n+1} \setminus \{(0, \ldots, 0)\}$.

Theorem 1 is a consequence of a more precise Theorem 4. The proof of Theorem 4 is based on the construction which we call branching smooth stratification of an algebraic variety. In this construction one 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, see Definition 2 and Theorem 3. The branching smooth stratification is closely related to a smooth stratification of an algebraic variety. So it is quite natural to define and consider at first the latter, see Definition 1 and Theorem 2. The results of [1] are extensively used for the proofs of Theorem 2 and Theorem 3. In Section 2 for recursive estimations we prove basing on [1] also some additional facts related to the decomposition of algebraic varieties into irreducible components, for example, Lemma 3. Note that our estimations for smooth stratification and branching smooth stratification take into account the codimension of a given algebraic variety, see Theorem 2 and Theorem 3 below. The upper bounds from these theorems are also double exponential but rather accurate. Some efforts are needed to obtain such upper bounds for the lengths of integer coefficients of equations determining the strata.

By now we have significantly improved the results of [1] and their presentation in [3]–[5] (there is also the third part of [4], [5] but it is devoted mainly to the systems with parameters). At present one could refer to them in place of [1] in regard to solving systems of polynomial equations. So we recommend the papers [3]–[5] to the interested reader. Still we refer mainly to [1] in this paper (especially when it is necessary to use the algorithms for factoring polynomials).

# 1 Main definitions and more detailed formulations of the obtained results

**DEFINITION 1** *Put*

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

*We give a recursive definition. Suppose that the closed in $\mathbb{A}^n(\overline{\mathbb{Q}})$ defined over $\mathbb{Q}$ algebraic variety $V_r$ is already defined for some $1 \leqslant r \leqslant n$. If $V_r \neq \varnothing$ 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 $\mathrm{Sing} W_i$ the set of singular points of $W_i$ and set*

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

*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 $W_i \setminus V_{r+1} \neq \varnothing$ 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 components 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 shall suppose without loss of generality that each index from $I_r$ is not an integer (to avoid some ambiguity in what follows) for all $r$ and $I_{r_1} \cap I_{r_2} = \varnothing$ for all $r_1 \neq r_2$.*

*If $V_1 = \varnothing$ set $n_0 = 0$. If $V_1 \neq \varnothing$ set $n_0$ to be the maximal $r$ such that $V_r \neq \varnothing$. Put $J = \cup_{1 \leqslant r \leqslant n_0} I_r$. We have the decomposition*

$$\mathcal{Z}(f_1, \ldots, f_k) = \bigcup_{i \in J} U_i \tag{1}$$

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

Note that the codimension of every component of $V_r$ is at least $m + r - 1$ and hence $0 \leqslant n_0 \leqslant n - m + 1$.

Further, 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 (1) is uniquely defined (up to a choice of indices) and we shall call it *canonical smooth stratification of* $\mathcal{Z}(f_1, \ldots, f_k)$.

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 $1 \leqslant r \leqslant n_0$, $1 \leqslant s \leqslant n$. Let $W_i$, $i \in I_r^{(s)}$, be the family of all the defined and irreducible over $\mathbb{Q}$ components of the algebraic variety $V_r^{(s)}$. Note that $I_r^{(s)}$ can be empty for some $s$ and then also $V_r^{(s)} = \varnothing$.

By definition put $D_r^{(s)} = \sum_{i \in I_r^{(s)}} \deg W_i$ for all $1 \leqslant s \leqslant n$, $1 \leqslant r \leqslant n_0$ (so $0 \leqslant D_r^{(s)} \in \mathbb{Z}$). Hence the number of elements $\# I_r^{(s)} \leqslant D_r^{(s)}$ and the degree $\deg V_r^{(s)} = D_r^{(s)}$.

We shall assume that:

(a) Each irreducible and defined over $\mathbb{Q}$ component $W_i$, $i \in I_r^{(s)}$, is given as a set of all common zeroes of a family of polynomials $h_\alpha \in \mathbb{Z}[X_1, \ldots, X_n]$, $\alpha \in A_i$, herewith the number of polynomials $\# A_i \leqslant (D_r^{(s)})^n$, the degrees $\deg_{X_1, \ldots, X_n} h_\alpha \leqslant \deg W_i \leqslant D_r^{(s)}$ and the lengths of integer coefficients of $h_\alpha$ are at most $M_r^{(s)}$ for some integer $M_r^{(s)} \geqslant 1$ for all $\alpha \in A_i$, $i \in I_r^{(s)}$.

    More than that, see Definition 4 Section 2, $h_\alpha$, $\alpha \in A_i$, is a family of polynomials corresponding to the generic projection of the algebraic variety $W_i$.

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

The families of polynomials $h_\alpha$, $\alpha \in A_i$, satisfying (a) and (b) for all $i \in I_r^{(s)}$, $1 \leqslant r \leqslant n_0$, $m + r - 1 \leqslant s \leqslant n$, completely determine the canonical smooth stratification of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$ (it is obvious but see the next section for some details).

Factually condition (b) follows from (a) since $h_\alpha$, $\alpha \in A_i$, is a family of polynomials corresponding to the generic projection of the algebraic variety $W_i$, see Lemma 2 Section 2. But still it is convenient to formulate (b) separately.

**DEFINITION 2** *Let an algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$ be given. Set $I = \{i^*\}$ for some element $i^* \notin \mathbb{Z}$ (one should choose and fix this element $i^*$) and*

$$V_{i^*} = \mathcal{Z}(f_1, \ldots, f_k).$$

*We give a recursive definition. Assume that a family of defined over $\mathbb{Q}$ algebraic varieties $V_{i_1,\ldots,i_r}$, $i_\beta \in I_{i_1,\ldots,i_{\beta-1}}$, $1 \leqslant \beta \leqslant r$, is already defined for some $1 \leqslant r \leqslant n$. We suppose that for all $\beta$ each element from $I_{i_1,\ldots,i_{\beta-1}}$ is not an integer and $I_{i_1,\ldots,i_{\beta-1}} = I$ for $\beta = 1$. The base of the recursion $r = 1$.*

*If $V_{i_1,\ldots,i_r} = \varnothing$ put $I_{i_1,\ldots,i_r} = \varnothing$.*

*Let $V_{i_1,\ldots,i_r} \neq \varnothing$. Consider the decomposition*

$$V_{i_1,\ldots,i_r} = \bigcup_{i_{r+1} \in I_{i_1,\ldots,i_r}} W_{i_1,\ldots,i_r,i_{r+1}} \tag{2}$$

*into the union of irreducible and defined over $\mathbb{Q}$ components $W_{i_1,\ldots,i_r,i_{r+1}}$. So the set of indices $I_{i_1,\ldots,i_r}$ is defined by (2).*

*Let a smooth quasiprojective algebraic variety $U_{i_1,\ldots,i_r,i_{r+1}}$ be a non–empty open in the Zariski topology defined over $\mathbb{Q}$ subset of $W_{i_1,\ldots,i_r,i_{r+1}}$. Set*

$$V_{i_1,\ldots,i_r,i_{r+1}} = W_{i_1,\ldots,i_r,i_{r+1}} \setminus U_{i_1,\ldots,i_r,i_{r+1}}$$

*for all $i_{r+1} \in I_{i_1,\ldots,i_r}$. Thus, the family of algebraic varieties $V_{i_1,\ldots,i_{r+1}}$, $i_\beta \in I_{i_1,\ldots,i_{\beta-1}}$, $1 \leqslant \beta \leqslant r+1$, is defined. The recursive step of the definition is described.*

*If $V_{i^*} = \varnothing$ set $n_0 = 0$. If $V_{i^*} \neq \varnothing$ set $n_0$ to be the maximal $r$ such that there exists $V_{i_1,\ldots,i_r}$ which is non–empty. So $0 \leqslant n_0 \leqslant n - m + 1$.*

*Now by definition the family of all $U_{i_1,\ldots,i_{r+1}}$, $i_\beta \in I_{i_1,\ldots,i_{\beta-1}}$, $1 \leqslant \beta \leqslant r+1$, $1 \leqslant r \leqslant n_0$, is a branching smooth stratification of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$.*

Notice that if $r = n_0 + 1$ then $V_{i_1,\ldots,i_r} = \varnothing$ for all $i_\beta \in I_{i_1,\ldots,i_{\beta-1}}$, $1 \leqslant \beta \leqslant r$. Further, the codimension of every algebraic variety $W_{i_1,\ldots,i_r,i_{r+1}}$ is at least $m + r - 1$.

So the branching smooth stratification depends on the choice of $U_{i_1,\ldots,i_r,i_{r+1}}$. If $U_{i_1,\ldots,i_r,i_{r+1}}$ is always coincides with the set of all smooth points of $W_{i_1,\ldots,i_r,i_{r+1}}$ then such a branching smooth stratification is uniquely defined (up to a choice of indices) and we shall call it *canonical branching smooth stratification of* $\mathcal{Z}(f_1, \ldots, f_k)$.

Some our notations for the smooth stratification and the branching smooth stratification coincide. It will not lead to an ambiguity since the sense of notations always will be seen from a context.

For every $1 \leqslant r \leqslant n_0$, $1 \leqslant s \leqslant n$ denote by $I_r^{(s)}$ the family of all $(r+1)$-tuples $(i_1, \ldots, i_r, i_{r+1})$ of indices such that there is an algebraic variety $W_{i_1,\ldots,i_r,i_{r+1}}$ from Definition 2 of codimension $\mathrm{codim} W_{i_1,\ldots,i_r,i_{r+1}} = s$. We have $I_r^{(s)} = \varnothing$ for all $1 \leqslant r \leqslant n_0$, $1 \leqslant s < m + r - 1$.

By definition put $D_r^{(s)} = \sum_{(i_1,\ldots,i_{r+1}) \in I_r^{(s)}} \deg W_{i_1,\ldots,i_{r+1}}$ for all $1 \leqslant s \leqslant n$, $1 \leqslant r \leqslant n_0$ (so $0 \leqslant D_r^{(s)} \in \mathbb{Z}$). Hence the number of elements $\# I_r^{(s)} \leqslant D_r^{(s)}$.

We shall suppose that for branching smooth stratification conditions (a) and (b) are satisfied if one replaces in them $W_i$ by $W_{i_1,\ldots,i_r,i_{r+1}}$, and $i$ by $i_1, \ldots, i_r, i_{r+1}$. Hence for a branching smooth stratification the numbers $M_r^{(s)}$ are defined. Also the sets of indices $A_{i_1,\ldots,i_{r+1}}$ are defined.

The families of polynomials $h_\alpha$, $\alpha \in A_{i_1,\ldots,i_{r+1}}$, satisfying (a) and (b) for all $(i_1, \ldots, i_{r+1}) \in I_r^{(s)}$, $1 \leqslant r \leqslant n_0$, $m + r - 1 \leqslant s \leqslant n$, completely determine the canonical branching smooth stratification of the algebraic variety $\mathcal{Z}(f_1, \dots, f_k)$ (it is obvious but see the next section for some details).

In what follows in this paper we use the notation $\mathcal{P}$ for a polynomial in one variable with non-negative integer coefficients. Unless we state otherwise we don't assume that this polynomial is the same in different places of the text (even close to each other).

If $D_r^{(s)} = 0$ for some $r$ and $s$ then by definition put $M_r^{(s)} = 0$. Notice that $I_r^{(s)} = \varnothing$ and $D_r^{(s)} = 0$ for all $r$ and $s$ such that $1 \leqslant s < m+r-1$, see Definition 1 and Definition 2. Put

$$\tilde{M} = \max\{M_r^{(s)} \,:\, 1 \leqslant r \leqslant n_0,\, m+r-1 \leqslant s \leqslant n\},$$
$$\tilde{D} = \max\{(D_r^{(s)})^{n^2} \,:\, 1 \leqslant r \leqslant n_0,\, m+r-1 \leqslant s \leqslant n\}.$$

We shall prove in Section 2 the following results.

**THEOREM 2** *For given polynomials $f_1, \dots, f_k$ one can construct the canonical smooth stratification of $\mathcal{Z}(f_1, \dots, f_k)$ described above. More precisely, for all integers $r, s$ such that $1 \leqslant r \leqslant n_0$, $m+r-1 \leqslant s \leqslant n$ and all $i \in I_r^{(s)}$ we construct families of polynomials $h_\alpha$, $\alpha \in A_i$, satisfying (a) and (b). Herewith for all $1 \leqslant r \leqslant n_0$ and $m+r-1 \leqslant s \leqslant n$ the inequalities*

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

*hold true for some polynomial $\mathcal{P}$. The working time of the algorithm for constructing this canonical smooth stratification is polynomial in $M$, $n^{n^2}$, $d^{n^2}$, $\tilde{M}$ and $\tilde{D}$. Hence this working time is polynomial in $M$ and $(nd)^{m2^{n-m}n^2}$.*

**THEOREM 3** *For given polynomials $f_1, \dots, f_k$ one can construct the canonical branching smooth stratification of $\mathcal{Z}(f_1, \dots, f_k)$ described above. More precisely, for all integers $r, s$ such that $1 \leqslant r \leqslant n_0$, $m+r-1 \leqslant s \leqslant n$ and all $(i_1, \dots, i_{r+1}) \in I_r^{(s)}$ we construct families of polynomials $h_\alpha$, $\alpha \in A_{i_1,\dots,i_{r+1}}$, satisfying (a) and (b) (with corresponding changes). Herewith for all $1 \leqslant r \leqslant n_0$ and $m+r-1 \leqslant s \leqslant n$ the inequalities*

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

*hold true for some polynomial $\mathcal{P}$. The working time of the algorithm for constructing this canonical branching smooth stratification is polynomial in $M$, $n^{n^2}$, $d^{n^2}$, $\tilde{M}$ and $\tilde{D}$. Hence this working time is polynomial in $M$ and $(nd)^{m2^{n-m}n^2}$.*

Let us return to the question of solvability of polynomial systems over $p$-adic integers. For the canonical branching smooth stratification defined above put

$$S = \Big\{ s \,:\, \bigcup_{1 \leqslant r \leqslant n_0} I_r^{(s)} \neq \varnothing \quad \& \quad m \leqslant s \leqslant n \Big\}.$$

Further, for every $s \in S$ set

$$M_s = \max_{1 \leqslant r \leqslant n_0} M_r^{(s)}, \quad D_s = 1 + \max_{1 \leqslant r \leqslant n_0} \{D_r^{(s)}, 3\}. \tag{3}$$

(Here "1+" and "3" appear by a technical reason: to apply later in the proof the Effective Nullstellensatz.)

Recall that $\mathbb{Z}_p$ denotes the ring of $p$-adic integers. Theorem 1 is an immediate consequence of Theorem 3 and the following result which will be proved in Section 3.

**THEOREM 4** *Let polynomials $f_1, \ldots, f_k$ be given. Consider the canonical branching smooth stratification of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$ with corresponding $D_s$ and $M_s$, $s \in S$. Then one can construct a positive integer*

$$\Delta < 2^{M\mathcal{P}(d^{n^2})+\sum_{s\in S} M_s \mathcal{P}(D_s^{sn^2}) d^n \prod_{t\in S,\, t<s}(tD_t^{t+1})^n}$$

*for a polynomial $\mathcal{P}$ (the exact formula (13) for $\Delta$ is given in Section 3) satisfying the following property. For every prime $p$ the system*

$$f_1 = \ldots = f_k = 0 \tag{4}$$

*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 $\Delta$. The integer $\Delta$ can be constructed within the time polynomial in $M$, $d^{n^2}$, $\max_{s\in S} M_s$, $\max_{s\in S} D_s^{sn^2}$.*

*More than that, if for a given $p$ there is a solution of the system (4) in $(\mathbb{Z}/p^N\mathbb{Z})^n$ then one can construct a solution of this polynomial system in $\mathbb{Z}_p^n$ using the Hensel lifting (see (20) in Section 3 for details). The initial data to apply this Hensel lifting (not only the solution $\mod p^N$) can be constructed within the time polynomial in $p^{Nn}$, $M$, $d^{n^2}$, $\max_{s\in S} M_s$, $\max_{s\in S} D_s^{sn^2}$.*

## 2 Construction of the smooth stratification and branching smooth stratification of an algebraic variety

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

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

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

Denote by $\mathbb{Z}[\mathcal{U}]$ the ring of polynomials over $\mathbb{Z}$ in all all the variables $u_{i,j}$ from the family $\mathcal{U}$ (we shall use also other similar notations). Set $U_i = \sum_{0\leqslant j\leqslant n} u_{i,j}X_j$. Let $V \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ be an irreducible projective algebraic variety defined over $\mathbb{Q}$ of dimension $n-s$, $1 \leqslant s \leqslant n$. Then there is a unique (up to a factor $\pm 1$) irreducible polynomial

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

homogeneous with respect to $Z_0, Z_s, \ldots, Z_n$ 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 $\deg_{Z_0,Z_s,\ldots,Z_n} H = \deg V$, cf. [7], [1].

Put $\overline{f}_i = X_0^{\deg f_i} f_i(X_1/X_0, \ldots, X_n/X_0) \in \mathbb{Z}[X_0, \ldots, X_n]$, $1 \leqslant i \leqslant k$, i.e., $\overline{f}_i$ are homogenizations of the polynomials $f_i$.

**LEMMA 1** *Let $V$ be an irreducible component of the algebraic variety $\mathcal{Z}(\overline{f}_1, \ldots, \overline{f}_k)$ and $\dim V = n - s$, see above. Then the lengths of integer coefficients of the polynomial $H$ are bounded from above by $(M + n^2)\mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$. One can construct the polynomial $H$ within the time polynomial in $M$, $d^{n^2}$ and $(\deg(V))^{n^2}$.*

**PROOF** The polynomial $H$ is homogeneous with respect to $Z_0, Z_s, \ldots, Z_n$. Hence it is sufficient to construct the polynomial $H(\mathcal{U}, 1, Z_s, \ldots, Z_n)$ and estimate the lengths of integer coefficients of this polynomial.

Actually in what follows everything in the proof is a direct consequence of the construction from the algorithm for solving polynomial systems, see [1]. Namely, replacing if necessary the family of polynomials $\overline{f}_1, \ldots, \overline{f}_k$ by $\overline{f}_i X_j^{d-\deg f_i}$, $1 \leqslant i \leqslant k$, $0 \leqslant j \leqslant n$, we shall suppose without loss of generality that the degrees $\deg_{X_0,\ldots,X_n} \overline{f}_i = d$ for all $1 \leqslant i \leqslant k$. There are integers $g_{i,j}$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant k$ with lengths $O(\log(1 + d^{i-1}))$ (note that here also a weaker bound like $\mathcal{P}(d^s)$ is sufficient) satisfying the following property. Put $g_i = g_{i,1}\overline{f}_1 + g_{i,2}\overline{f}_2 + \ldots + g_{i,k}\overline{f}_k$, $1 \leqslant i \leqslant s$. Then $V$ is an irreducible component of the algebraic variety $\mathcal{Z}(g_1, \ldots, g_s)$.

Notice that one can construct all the integers $g_{i,j}$ within the time polynomial in $M$ and $d^{n^2}$ using the algorithm from [1].

Write for brevity the family

$$\mathcal{U}' = \{u_{i,j}\}_{i=0,s+1,\ldots,n,\, 0\leqslant j\leqslant n}. \tag{5}$$

There are unique linear forms $Y_0', \ldots, Y_n' \in \mathbb{Q}(\mathcal{U}')[X_0, \ldots, X_n]$ such that

$$Y_i'(U_0, X_1, \ldots, X_s, U_{s+1}, \ldots, U_n) = X_i, \quad 0 \leqslant i \leqslant n.$$

Denote by $\lambda$ the determinant of the matrix of coefficients of the linear forms $U_0, X_1, \ldots, X_s, U_{s+1}, \ldots, U_n$. Put $Y_i = \lambda Y_i'$. Then all $Y_i \in \mathbb{Z}[\mathcal{U}', X_0, \ldots, X_n]$ and the degrees $\deg_{u_{i,0},\ldots,u_{i,n}} Y_j \leqslant 1$ for all $0 \leqslant j \leqslant n$, $i = 0, s+1, \ldots, n$. We construct all the linear forms $Y_j$.

Put $g_i' = g_i(Y_0, \ldots, Y_n)$, $1 \leqslant i \leqslant s$ and $U_s' = U_s(Y_0, \ldots, Y_n)$. Let $\varepsilon$ be a transcendental element over the field $\mathbb{Q}(U)$. Let us extend the ground field $\mathbb{Q}$ till the field $K_1 = \mathbb{Q}(\mathcal{U})(\varepsilon, Z_s, \ldots, Z_n)$. Set also the field $K_2 = \mathbb{Q}(\mathcal{U}')(\varepsilon, Z_{s+1}, \ldots, Z_n)$. Put

$$\widetilde{g}_i = g_i'(X_0, \ldots, X_s, Z_{s+1}X_0, \ldots, Z_nX_0) - \varepsilon X_i^d, \quad 1 \leqslant i \leqslant s.$$

Hence all $\widetilde{g}_i \in \mathbb{Z}[\mathcal{U}', X_0, \ldots, X_s, \varepsilon, Z_{s+1}, \ldots, Z_n]$ and $\widetilde{g}_i$ are homogeneous with respect to $X_0, \ldots, X_s$. We construct all polynomials $\widetilde{g}_i$.

Let $\mathbb{P}^s(\overline{K_2})$ has homogeneous coordinates $X_0, \ldots, X_s$. By our construction, see [1] (and also [4], [5]) for more details, the dimension $\dim \mathcal{Z}(\widetilde{g}_1, \ldots, \widetilde{g}_s) = 0$ in $\mathbb{P}^s(\overline{K_2})$, or which is the same the system $\widetilde{g}_1 = \ldots = \widetilde{g}_s = 0$ has a finite number of solutions in the projective space $\mathbb{P}^s(\overline{K_2})$.

Put $N = sd - s + 1$. For every integer $\nu \geqslant 0$ denote by $\mathcal{H}_\nu$ the $K_1$–vector space of monomials in $X_0, \ldots, X_s$ of degree $\nu$. Let us choose the base of each $\mathcal{H}_\nu$ consisting of monomials in $X_0, \ldots, X_s$ with coefficients 1. Notice that the dimension of the space $\mathcal{H}_N = \binom{sd+1}{s} \leqslant \mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$.

Consider the $K_1$–linear mapping

$$\mathcal{H}_{N-d}^s \times \mathcal{H}_{N-1} \to \mathcal{H}_N,\ ((q_1, \ldots, q_s), r) \mapsto \sum_{1\leqslant i\leqslant s} \widetilde{g}_i q_i + (U_s' - Z_sX_0)r, \tag{6}$$

where all $q_i \in \mathcal{H}_{N-d}$ and $r \in \mathcal{H}_{N-1}$. Denote by $\mathcal{A}$ the matrix of this mapping in the chosen bases.

Recall the system $\widetilde{g}_1 = \ldots = \widetilde{g}_s = 0$ has a finite number of solutions $z$ in the projective space $\mathbb{P}^s(\overline{K_2})$. Furthermore $U_s'(z) \neq 0$ for every such solution $z$ since the coefficients of the linear form $U_s'$ are transcendental over the field $K_2$. Therefore also $(U_s' - Z_s X_0)(z) \neq 0$. This implies that the mapping (6) is surjective see e.g. [11] and also [4] Section 3. Hence $\operatorname{rank}\mathcal{A} = \dim \mathcal{H}_N$. So we can construct a nonzero minor $Q$ of order $\dim \mathcal{H}_N$ of the matrix $\mathcal{A}$. We have $0 \neq Q \in \mathbb{Z}[\mathcal{U}, \varepsilon, Z_s, \ldots, Z_n]$. Let us represent $Q = \varepsilon^a Q_1$ where an integer $a \geqslant 0$, the polynomial $Q_1 \in \mathbb{Z}[\mathcal{U}, \varepsilon, Z_s, \ldots, Z_n]$ and $Q_1|_{\varepsilon=0} \neq 0$. Put $Q_2 = Q_1|_{\varepsilon=0} = Q_1(\mathcal{U}, 0, Z_s, \ldots, Z_n)$. Then the polynomial $H(\mathcal{U}, 1, Z_s, \ldots, Z_n)$ is an irreducible factor of $Q_2$ in the ring $\mathbb{Z}[\mathcal{U}, Z_s, \ldots, Z_n]$, cf. [1] (and also [4], [5]).

From the described construction we get immediately that all the degrees $\deg_{Z_s,\ldots,Z_n} Q_2$, $\deg_{u_{i,0},\ldots,u_{i,n}} Q_2$, $i = 0, s, \ldots, n$, are bounded from above by $\mathcal{P}(d^s)$ and the lengths of integer coefficients of the polynomial $Q_2$ are bounded from above by $(M + n^2)\mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$. Now the required estimation for the lengths of integer coefficients of the polynomial $H(\mathcal{U}, 1, Z_s, \ldots, Z_n)$ follows from [6] Chapter III §4 Lemma 2 or [1].

It remains to find the polynomial $H$. Let $\xi \in \mathbb{Q}(t_{s+1}, \ldots, t_n)[\theta]$ be a generic point of the algebraic variety $V$ constructed in [1]. Here $t_{s+1}, \ldots, t_n$ are algebraically independent over $\mathbb{Q}$ and $\theta$ is an algebraic over $\mathbb{Q}(t_{s+1}, \ldots, t_n)$ element of degree $\deg V$. The point $\xi$ is constructed within the time polynomial in $M$ and $d^{n^2}$. Let $0 \leqslant i_0 \leqslant n$ be an index such that $X_{i_0}$ does not vanish on $V$. Then the representations are constructed

$$(X_i/X_{i_0})(\xi) = \frac{1}{a} \sum_{0 \leqslant j < \deg V} a_{i,j}\theta^j, \quad 0 \leqslant i \leqslant n, \tag{7}$$

where all $a, a_{i,j} \in \mathbb{Z}[t_{s+1}, \ldots, t_n]$, the degrees $\deg_{t_{s+1},\ldots,t_n} a$, $\deg_{t_{s+1},\ldots,t_n} a_{i,j}$ are bounded from above by $\mathcal{P}(d^s)$ and the lengths of integer coefficients of all $a$, $a_{i,j}$ are bounded from above by $(M + n)\mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$. The point $\xi$ is given by (7). Using (7) we find all the values $(U_j/X_{i_0})(\xi)$, $j = 0, s, \ldots, n$.

One can represent $H = \sum_{I,J} h_{I,J} u^I Z^J$ where $I, J$ are multiindices and $h_{I,J} \in \mathbb{Z}$, i.e., $H$ is a sum of monomials in the elements of the family $\mathcal{U}$ and $Z_0, Z_{s+1}, \ldots, Z_n$ with integer coefficients. We have

$$H(\mathcal{U}, (U_0/X_{i_0})(\xi), (U_s/X_{i_0})(\xi), \ldots, (U_n/X_{i_0})(\xi)) = 0.$$

Furthermore, using (7) we get that the last equality is equivalent to

$$\sum_{1 \leqslant r \leqslant R,\, 0 \leqslant q < \deg V} L_{r,q}\, m_r\, \theta^q = 0,$$

where $m_r$ are pairwise distinct monomials in the elements of the family $\mathcal{U}$ and $t_{s+1}, \ldots, t_n$; and $L_{r,q}$ are linear forms in $h_{I,J}$ with integer coefficients. Consider $h_{I,J}$ as unknowns. Then we get a linear system $L_{r,q} = 0$, $1 \leqslant r \leqslant R$, $0 \leqslant q < \deg V$ with respect to $h_{I,J}$. By the bounds for $a$ and $a_{i,j}$ from (7) the number of elements $\#R$ is bounded from above by a polynomial in $(d \deg(V))^{n^2}$ and the lengths of integer coefficients of the linear forms $L_{r,q}$ are bounded from above by $(M + n^2)\mathcal{P}(d^s)$. This is an immediate consequence of the bounds for the generic point $\xi$ from [1]. The number of unknowns $h_{I,J}$ is bounded from above by $(\deg(V)+1)^{n^2+n}$. The vector space over $\mathbb{Q}$ of solutions of this linear system is of dimension 1. Solving it we find all the integer coefficients $h_{I,J}$ . Thus we can construct the polynomial $H$ within the required working time. The lemma is proved. $\Box$

Let us represent

$$H(\mathcal{U}, U_0, U_s, \ldots, U_n) = \sum_{e=(e_{i,j})\in\mathbb{Z}^{(n-s+2)(n+1)}} H_e \prod_{i=0,s,s+1,\ldots,n,\, 0\leqslant j\leqslant n} u_{i,j}^{e_{i,j}} \qquad (8)$$

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

Notice that under conditions of Lemma 1 one can construct all the polynomials $H_e$, $e \in E'$ within the time polynomial in $M$, $d^{n^2}$, $(\deg V)^{n^2}$, and further the lengths of integer coefficients of all polynomials $H_e$, $e \in E'$ are bounded from above by $(M+n^2)\mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$ (this follows immediately from Lemma 1).

Choose a maximal subset $E \subset E'$ such that the polynomials $H_e$, $e \in E$, are linearly independent. So $\#E \leqslant (\deg(V))^n$.

We have, cf. the construction of the system of polynomial equations for the components of an algebraic variety from [1], $\mathcal{Z}(H_e, e \in E) = V$ (i.e. the set of all common zeroes of the polynomials $H_e$, $e \in E$, coincides with $V$; in what follows we shall use also other similar notations). 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 a defined and irreducible over $\mathbb{Q}$ projective 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 $E$.*

**DEFINITION 4** *Let $W \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ be a defined and irreducible over $\mathbb{Q}$ affine algebraic variety. Assume that $W$ is a set of all common zeroes in $\mathbb{A}^n(\overline{\mathbb{Q}})$ of a family of polynomials $h_\alpha \in \mathbb{Z}[X_1, \ldots, X_n]$, $\alpha \in A$. We shall say that $h_\alpha$, $\alpha \in A$, is a family of polynomials corresponding to the generic projection of the algebraic variety $W$ if and only if the following property hold true.*

*Denote by $V$ the closure of $W$ in the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$. Denote by $\overline{h}_\alpha \in \mathbb{Z}[X_0, \ldots, X_n]$ the homogenization of the polynomial $h_\alpha$ for every $\alpha \in A$. Then there is a system of polynomial equations $H_e = 0$, $e \in E$, corresponding to the generic projection of the algebraic variety $V$ such that $\#E = \#A$ and the sets of polynomials $\{\overline{h}_\alpha : \alpha \in A\} = \{H_e : e \in E\}$ coincide.*

**LEMMA 2** *Let $V \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ be a defined and irreducible over $\mathbb{Q}$ projective algebraic variety of degree $\deg V = D$ and dimension $n-s$ where $1 \leqslant s \leqslant n$. 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 $L \in \mathbb{Q}[X_0, \ldots, X_n]$ be a linear form such that $L(x) \neq 0$. Then there are $e_1, \ldots, e_s \in E$ such that $H_{e_1}/L^D, \ldots, H_{e_s}/L^D$ is a system of local parameters of $V$ at the point $x$.*

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

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

and

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

Denote by $\mathcal{Y}_i$ the family of coefficients of the linear forms $Y_0, Y_i, Y_{s+1}, \ldots, Y_n$ for $1 \leqslant i \leqslant s$. There are linear forms $Y_0, \ldots, Y_n$ such that $Y_0(x) \neq 0$ and

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

(ii) the inverse image $\pi^{-1}(\pi(x))$ consists of $\deg V$ pairwise distinct points,

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

(iv) the polynomial $H(\mathcal{Y}_i, Y_0, Y_i, Y_{s+1}, \ldots, Y_n) \neq 0$ for $1 \leqslant i \leqslant s$.

By (ii) the differential $d_x\pi$ at the point $x$ of the projection $\pi$ is an isomorphism. The projection $\pi_i$ is also finite for every $1 \leqslant i \leqslant s$. 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 $h_i \in \mathbb{Z}[Y_0, Y_i, Y_{s+1}, \ldots, Y_n]$ of the degree $\deg h_i = \deg V$ by (iii). By the Zariski main theorem the point $\pi_i(x)$ is smooth on $\pi_i(V)$. Now the differentials $d_x(h_1/L^D), \ldots, d_x(h_s/L^D)$ are linearly independent. Therefore $h_1/L^D, \ldots, h_s/L^D$ is a system of local parameters of the variety $V$ at the point $x$. By (iv) each $h_i$ coincides with $H(\mathcal{Y}_i, Y_0, Y_i, Y_{s+1}, \ldots, Y_n)$ up to a nonzero factor from the ground field. Hence $h_1, \ldots, h_s$ 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. $\square$

**LEMMA 3** *Let $V \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ be an irreducible and defined over $\mathbb{Q}$ projective algebraic variety of dimension $n - s$, $1 \leqslant s \leqslant n$. Let $V$ be given by the generic projection and $H = H_V$ be the corresponding polynomial. Let the degree $\deg V \leqslant D'$ where $D' \geqslant 2$ and lengths of integer coefficients of $H_V$ be at most $M'$ where $M' \geqslant 1$. Let $F \in \mathbb{Q}[X_0, \ldots, X_n]$ be a homogeneous polynomial of the degree at most $D''$ where $D'' \geqslant 2$, and lengths of integer coefficients of $F$ be at most $M''$ where $M'' \geqslant 1$. 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 $V \cap \mathcal{Z}(F)$. Then the degree of the intersection $V \cap \mathcal{Z}(F)$ is at most $D'D''$ and the component $W_1$ can be given by the generic projection. The corresponding polynomial $H_{W_1}$ has integer coefficients with the lengths bounded from above*

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

*for a polynomial $\mathcal{P}$. The polynomials $H_{W_1}$ corresponding to all the irreducible components $W_1$ of the intersection $V \cap \mathcal{Z}(F)$ can be constructed within the time polynomial in $(D'D'')^{n^2}$, $M'$, $M''$.*

**PROOF** Let $U_0, U_{s+1}, \ldots, U_n$ be generic linear forms such as above. Recall that their family of coefficients $\mathcal{U}'$ is defined by (5). For brevity set the field $K = \mathbb{Q}(\mathcal{U}')$.

Set

$$R_H = \mathrm{Res}_{Z_s}(H, H'_{Z_s}) \in \mathbb{Q}[\mathcal{U}, Z_0, Z_{s+1}, \ldots, Z_n]$$

to be the resultant of the polynomials $H$ and $H'_{Z_s}$ with respect to $Z_s$ (so $R_H$ coincides with the discriminant of the polynomial $H$ with respect to $Z_s$ multiplied by the leading coefficient $\mathrm{lc}_{Z_s} H$ of the polynomial $H$ with respect to $Z_s$).

There are integers $u_0, u_1, \ldots, u_n$ with lengths $O(\log(D'+1))$ such that the polynomial

$$R = R_H|_{u_{s,j}=u_j,\, 0 \leqslant j \leqslant n} \neq 0 \tag{9}$$

(here $R$ is a notation). Set $Y = \sum_{0 \leqslant j \leqslant n} u_j X_j$. 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 with respect to $Z_0, Z, Z_{s+1}, \ldots, Z_n$ polynomial such that

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

(one should substitute here the coefficients $u_j$ for the generic coefficients $u_{s,j}$, $0 \leqslant j \leqslant n$). Notice that the polynomial $\Phi(\mathcal{U}', U_0, Y, U_{s+1}, \ldots, U_n)$ is vanishing on $V$.

Note that the lengths of integer coefficients of the polynomial $\Phi$ are bounded from above by $(M' + n^2)\mathcal{P}(D')$ for a polynomial $\mathcal{P}$. The resultant $R = \mathrm{Res}_Z(\Phi, \Phi'_Z) \neq 0$. Put $\varphi = \mathrm{lc}_Z \Phi$ to be the leading coefficient of the polynomial $\Phi$ with respect to $Z$. Then $\varphi \neq 0$ since $R \neq 0$. Furthermore $\varphi \in \mathbb{Z}[\mathcal{U}']$, $\deg_Z \Phi = \deg V$ by (9) and since $\mathrm{lc}_Z H_V \in \mathbb{Z}[\mathcal{U}]$.

Denote by $K(V)$ the field of defined over the field $K$ rational functions of the algebraic variety $V$. The polynomial $\Phi$ is nonzero and separable and, therefore, irreducible since $V$ is irreducible. Therefore $\eta = Y/U_0$ is a primitive element of the extension

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

The minimal polynomial of the element $\eta$ is $\Phi(\mathcal{U}', 1, Z, U_{s+1}/U_0, \ldots, U_n/U_0)$. Hence there is a generic point $\chi$ of the algebraic variety $V$ over the field $K$ such that $(Y/U_0)(\chi) = \eta$ and all

$$(X_i/U_0)(\chi) \in K(U_{s+1}/U_0, \ldots, U_n/U_0)[\eta], \quad 0 \leqslant i \leqslant n.$$

Put $\chi_i = (X_i/U_0)(\chi)$, $0 \leqslant i \leqslant n$.

Let $T$ be a new variable. Put the field $K_3 = K(U_{s+1}/U_0, \ldots, U_n/U_0)[\eta]$ and the polynomial

$$h = H(\mathcal{U}, 1, T, U_{s+1}/U_0, \ldots, U_n/U_0) \in K_3[T, u_{s,0}, u_{s,1}, \ldots, u_{s,n}].$$

To construct all $\chi_i = (X_i/U_0)(\chi)$ we factor using the algorithm from [1], Chapter I §1 Proposition 1.1, the polynomial $h = h(T, u_{s,0}, u_{s,1}, \ldots, u_{s,n})$ over the field $K_3$. The polynomial $h$ has a linear factor $T - \sum_{0 \leqslant i \leqslant n} u_{s,i}\chi_i$. Thus by [1] there are representations

$$\chi_i = \sum_{0 \leqslant j < \deg V} \frac{b_{i,j}(\mathcal{U}', U_{s+1}/U_0, \ldots, U_n/U_0)\eta^j}{b(\mathcal{U}', U_{s+1}/U_0, \ldots, U_n/U_0)}, \quad 0 \leqslant i \leqslant n, \tag{10}$$

where all $b, b_{i,j} \in \mathbb{Z}[\mathcal{U}', Z_{s+1}, \dots, Z_n]$ are polynomials with degrees

$$\begin{aligned} &\deg_{Z_{s+1},\dots,Z_n} b, \quad \deg_{Z_{s+1},\dots,Z_n} b_{i,j}, \\ &\deg_{u_{i,0},\dots,u_{i,n}} b, \quad \deg_{u_{i,0},\dots,u_{i,n}} b_{i,j}, \quad i = 0, s+1, \dots, n, \end{aligned}$$

bounded from above by $\mathcal{P}(D')$ for a polynomial $\mathcal{P}$. The lengths of integer coefficients of all polynomials $b, b_{i,j}$ are bounded from above $(M' + n^2)\mathcal{P}(D')$ for a polynomial $\mathcal{P}$.

**LEMMA 4** *Let $q \geqslant D'$ be an integer. Then one can represent*

$$\eta^q = \frac{1}{\varphi^{q-D'+1}} \sum_{0 \leqslant j < \deg V} b_j^{(q)}(\mathcal{U}', U_{s+1}/U_0, \dots, U_n/U_0)\eta^j,$$

*where all $b_j^{(q)} \in \mathbb{Z}[\mathcal{U}', Z_{s+1}, \dots, Z_n]$ are polynomials with degrees*

$$\deg_{Z_{s+1},\dots,Z_n} b_j^{(q)}, \quad \deg_{u_{i,0},\dots,u_{i,n}} b_j^{(q)}, \quad i = 0, s+1, \dots, n,$$

*bounded from above by $\mathcal{P}(D')(q - D' + 1)$ for a polynomial $\mathcal{P}$. The lengths of integer coefficients of all polynomials $b_j^{(q)}$ are bounded from above*

$$(M' + \log_2(q - D' + 1))(q - D' + 1) + n^2 \log_2(\mathcal{P}(D')(q - D' + 1))$$

*for a polynomial $\mathcal{P}$.*

**PROOF** Let $\Phi = \sum_{0 \leqslant j \leqslant \deg V} \Phi_j Z^j$ where all $\Phi_j \in \mathbb{Z}[\mathcal{U}', Z_{s+1}, \dots, Z_n]$ (so $\Phi_{\deg V} = \varphi$). Set $q' = q - D' + 1$. One can represent $Z^q = \Phi A + B$ where $\varphi^{q'} A, \varphi^{q'} B \in \mathbb{Z}[\mathcal{U}', Z, Z_{s+1}, \dots, Z_n]$ and $\varphi^{q'} B = \sum_{0 \leqslant j < \deg V} b_j^{(q)} Z^j$. Then the polynomial $A$ can be found by solving a linear system over the field $K(Z_{s+1}, \dots, Z_n)$ with a square triangular matrix $\mathcal{T}$ of size $q'$. Each nonzero entry of this matrix is equal to some $\Phi_j$ and on the diagonal all the entries are equal to $\varphi$. Solving this linear system by Cramer's rule we get that the lengths of integer coefficients of the polynomial $\varphi^{q'} A$ are bounded from above by

$$M'(q' - 1) + n^2 \log_2(\mathcal{P}(D')q') + q' \log_2(q')$$

for a polynomial $\mathcal{P}$ (note that $(q' - 1)$ appears here since to obtain the coefficients of $\varphi^{q'} A$ from the field $K(Z_{s+1}, \dots, Z_n)$ we compute minors of the matrix $\mathcal{T}$ of order $(q' - 1)$). Hence the the lengths of integer coefficients of the polynomial $\varphi^{q'} B = \varphi^{q'} Z^q - \Phi \varphi^{q'} A$ are bounded from above by $(M' + \log_2(q'))q' + n^2 \log_2(\mathcal{P}(D')q')$.

The required estimations for the degrees of all $b_j^{(q)}$ are obtained in a similar way by solving the considered linear system by Cramer's rule. Lemma 4 is proved. $\Box$

Put

$$\bar{b} = Z_0^{\deg_{Z_{s+1},\dots,Z_n} b} b(\mathcal{U}', Z_{s+1}/Z_0, \dots, Z_n/Z_0) \in \mathbb{Z}[\mathcal{U}', Z_0, Z_{s+1}, \dots, Z_n].$$

to be the homogenization of $b$. Assume that $\bar{b}$ is vanishing on $W_1$. Then $H_{W_1}$ coincides with an irreducible factor of $\bar{b}$ in the ring $\mathbb{Z}[\mathcal{U}', Z_0, Z_{s+1}, \dots, Z_n]$. In this case the required estimate for the lengths of integer coefficients of the polynomial $H_{W_1}$ follows from [6] Chapter III §4 Lemma 2 or [1].

In what follows we shall assume that $\bar{b}$ is not vanishing on $W_1$. We have $F(\chi) \neq 0$ since $F$ is not vanishing on $V$. Using (10) and Lemma 4 one can represent

$$F(\chi_0, \ldots, \chi_n) = \frac{\sum_{0 \leqslant j < \deg V} \psi^{(j)}(\mathcal{U}', U_{s+1}/U_0, \ldots, U_n/U_0)\eta^j}{b(\mathcal{U}', U_{s+1}/U_0, \ldots, U_n/U_0)^{D''} \varphi^{(D'-1)D''-(D'-1)}},$$

where all $\psi^{(j)} \in \mathbb{Z}[\mathcal{U}', Z_{s+1}, \ldots, Z_n]$. By Lemma 4 and the estimates for degrees and lengths of integer coefficients of $b$ and $b^{(j)}$, see (10), we deduce that for all $j$ the degrees

$$\deg_{Z_{s+1},\ldots,Z_n} \psi^{(j)}, \quad \deg_{u_{i,0},\ldots,u_{i,n}} \psi^{(j)}, \quad i = 0, s+1, \ldots, n,$$

are bounded from above by $\mathcal{P}(D')D''$ for a polynomial $\mathcal{P}$. Further, the lengths of integer coefficients of all polynomials $\psi^{(j)}$ are bounded from above $(M' + M'' + n^2)\mathcal{P}(D'D'')$ for a polynomial $\mathcal{P}$.

Put

$$\nu = \max_{0 \leqslant j < \deg V} (j + \deg_{Z_{s+1},\ldots,Z_n} \psi^{(j)})$$

and

$$\Psi = Z_0^\nu \sum_{0 \leqslant j < \deg V} \psi^{(j)}(\mathcal{U}', Z_{s+1}/Z_0, \ldots, Z_n/Z_0)Z^j \in \mathbb{Z}[\mathcal{U}', Z_0, Z, \ldots, Z_n].$$

Then $\Psi \neq 0$, the degree $\deg_Z \Psi < \deg V$.

Recall that $\eta = Y/U_0 \in K(V)$. We have $X_i/U_0 - \chi_i = 0$, $0 \leqslant i \leqslant n$, in the field $K(V)$. The rational function $X_i/U_0 - \chi_i$ is defined for every $z \in V \setminus \mathcal{Z}(U_0)$ such that $b(z) \neq 0$, see (10). Hence if $z \in V \setminus \mathcal{Z}(U_0\bar{b})$ then $(X_i/U_0)(z) = \chi_i(z)$ for $0 \leqslant i \leqslant n$. Therefore the polynomial $\Psi(\mathcal{U}', U_0, Y, U_{s+1}, \ldots, U_n)$ is vanishing on $W_1 \setminus \mathcal{Z}(U_0\bar{b}) \neq \varnothing$. Hence $\Psi(\mathcal{U}', U_0, Y, U_{s+1}, \ldots, U_n)$ is vanishing on $W_1$.

If $\deg_Z \Psi = 0$ then $H_{W_1}$ coincides with an irreducible factor of $\Psi$. Now the required estimate for lengths of integer coefficients of the polynomial $H_{W_1}$ follows from [6] Chapter III §4 Lemma 2 or [1].

Assume that $\deg_Z \Psi > 0$. Put

$$R_1 = \mathrm{Res}_Z(\Phi, \Psi) \in \mathbb{Z}[\mathcal{U}', Z_0, Z_{s+1}, \ldots, Z_n]$$

to be the resultant of the polynomials $\Phi$ and $\Psi$ with respect to $Z$. Then $R_1 \neq 0$ since the polynomial $\Phi$ is irreducible over the field $K$ and $0 < \deg_Z \Psi < \deg_Z \Phi$. We have $W_1 \subset \mathcal{Z}(\Phi(\mathcal{U}', U_0, Y, U_{s+1}, \ldots, U_n), \Psi(\mathcal{U}', U_0, Y, U_{s+1}, \ldots, U_n))$. Hence $W_1 \subset \mathcal{Z}(R(\mathcal{U}', U_0, U_{s+1}, \ldots, U_n))$.

The bounds for degrees and lengths of integer coefficients of the polynomials $\Phi$ and $\Psi$ are known. Using them we get immediately that the lengths of integer coefficients of the resultant $R_1$ are bounded from above by $(M' + M'' + n^2)\mathcal{P}(D'D'')$ for a polynomial $\mathcal{P}$. Now $H_{W_1}$ coincides with an irreducible factor of $R_1$ in the ring $\mathbb{Z}[\mathcal{U}', Z_0, Z_{s+1}, \ldots, Z_n]$. Again the required estimate for lengths of integer coefficients of the polynomial $H_{W_1}$ follows from [6] Chapter III §4 Lemma 2 or [1].

Finally, using the algorithm from [1] and the described construction one can construct the polynomial $H_{W_1}$ within the required working time. Lemma 3 is proved. $\square$

At present our aim is to prove Theorem 2. In what follows when it is required to construct a system of polynomial equations determining an 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 the closure of this variety $\overline{U} \subset \mathbb{P}^n(\overline{\mathbb{Q}})$ using the algorithm from [1] and Lemma 1. This will gives also a system for $U$. The condition (b) when it is required will be satisfied by Lemma 2.

We proceed to the details. Compute using [1] all the irreducible and defined over $\mathbb{Q}$ components $W$ of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_k)$. After that we apply Lemma 1. Let the codimension of the variety $W$ is equal to $s \geqslant m$. Then according to Lemma 1 (with $W$ in place of $V$) the algebraic variety $W$ is given by a system of polynomial equations of degree at most $\deg W \leqslant d^s$ and the lengths of integer coefficients of these equations are bounded from above by $(M + n^2)\mathcal{P}(d^s)$ for a polynomial $\mathcal{P}$. Besides, $\sum_{\{W\,:\,\mathrm{codim} W = s\}} \deg W \leqslant d^s$ by the Bézout theorem. Notice that $(m+1)2^{s-m} - 1 \geqslant s$ for all integers $s \geqslant m \geqslant 1$. Hence the estimations of Theorem 2 hold true for $D_1^{(s)}$ and $M_1^{(s)}$. By Lemma 1 and Lemma 2 properties (a) and (b) hold for all $i \in I_1^{(s)}$, $m \leqslant s \leqslant n$.

Let $1 \leqslant r < n$ and suppose that we have constructed recursively all the algebraic varieties $W_i$, $i \in I_r^{(s)}$, $m + r - 1 \leqslant s \leqslant n$. We assume that $I_r^{(s)} \neq \varnothing$ for at least one $s$ such that $m + r - 1 \leqslant s \leqslant n$. Further, suppose that (a) and (b) hold and the required estimations for $D_r^{(s)}$ and $M_r^{(s)}$ are fulfilled for the considered $r, s$.

Let us show how to construct the families of algebraic varieties $W_i$, $i \in I_{r+1}^{(s)}$ for all $s$ such that $m + r \leqslant s \leqslant n$. We also ascertain the required upper bounds for $D_{r+1}^{(s)}$ and $M_{r+1}^{(s)}$ (if at least one $I_{r+1}^{(s)} \neq \varnothing$).

Let $\iota \in I_{r+1}^{(s)}$. Then either $W_\iota$ is an irreducible component of $\mathrm{Sing} W_i$ for some $i \in I_r^{(u)}$, $m + r - 1 \leqslant u < s$, or $W_\iota$ is an irreducible component of $W_i \cap W_j$ for some $i \in I_r^{(u)}$, $j \in I_r^{(v)}$, $m + r - 1 \leqslant v \leqslant u < s$, $i \neq j$. Put $\deg W_i = d_i$, $\deg W_j = d_j$ for all $i, j$.

Let $i \in I_r^{(u)}$, $m + r - 1 \leqslant u < s$. Put $B_i' = A_i^u \times \{1, \ldots, n\}^u$. For every

$$\beta = ((\alpha_1, \ldots, \alpha_u), (j_1 \ldots, j_u)) \in B_i'$$

compute the Jacobian

$$J_\beta = \det \left( \frac{\partial h_{\alpha_l}}{\partial X_{j_v}} \right)_{1 \leqslant l, v \leqslant u}. \tag{11}$$

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

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

Further, $\deg J_\beta \leqslant u(d_i - 1) < u d_i$. Hence by the Bézout theorem the degree of the union of all the components of codimension $s$ of $\mathrm{Sing} W_i$ is at most $d_i (u d_i)^{s-u}$.

For every integer $s$ such that $m + r \leqslant s \leqslant n$, for all $i, u$ such that $i \in I_r^{(u)}$, $m + r - 1 \leqslant u < s$ denote by $W_\iota$, $\iota \in I_{i,r+1}^{(s)}$, the family of all the defined and irreducible over $\mathbb{Q}$ components $W_\iota$ of the variety $\mathrm{Sing} W_i$ such that the codimension $\mathrm{codim} W_\iota = s$.

Similarly if $i \in I_r^{(u)}$, $j \in I_r^{(v)}$, $m + r - 1 \leqslant v \leqslant u < s$, $i \neq j$, then the degree of the union of all the components of codimension $s$ of the intersection $W_i \cap W_j$ is at most $d_i d_j^{s-u}$ (of course this degree is at most $d_i d_j$ by the Bézout theorem but it is not principal now).

For every integer $s$ such that $m+r \leqslant s \leqslant n$ for all $u, v, i, j$ such that $i \in I_r^{(u)}$, $j \in I_r^{(v)}$, $m + r - 1 \leqslant v \leqslant u < s$, $i \neq j$ denote by $W_\iota$, $\iota \in I_{i,j,r+1}^{(s)}$ the family of all the defined and irreducible over $\mathbb{Q}$ components $W_\iota$ of the variety $W_i \cap W_j$ such that the codimension $\mathrm{codim} W_\iota = s$.

We shall assume without loss of generality that the introduced sets of indices are pairwise non–intersecting, i.e. $I_{i_1,r+1}^{(s_1)} \cap I_{i_2,r+1}^{(s_1)} = \varnothing$ if $(i_1, s_1) \neq (i_2, s_2)$, further $I_{i_1,j_1,r+1}^{(s_1)} \cap I_{i_2,j_2,r+1}^{(s_2)} = \varnothing$ if $(i_1, j_1, s_1) \neq (i_2, j_2, s_2)$ and finally $I_{i_1,r+1}^{(s_1)} \cap I_{i_2,j_2,r+1}^{(s_2)} = \varnothing$ for all $(i_1, s_1)$ and $(i_2, j_2, s_2)$.

For every $m + r \leqslant s \leqslant n$ put $\widetilde{I}_{r+1}^{(s)}$ to be the union of all the introduced sets $I_{i,r+1}^{(s)}$ and $I_{i,j,r+1}^{(s)}$. Set $\widetilde{I}_{r+1} = \bigcup_{m+r \leqslant s \leqslant n} \widetilde{I}_{r+1}^{(s)}$.

Applying the algorithm from [1] one can construct the family of the algebraic varieties $W_\iota$, $\iota \in \widetilde{I}_{r+1}$. Further, again using the algorithm from [1] we construct a minimal (by inclusion) subset $I_{r+1} \subset \widetilde{I}_{r+1}$ satisfying the following property. For every $i_1 \in \widetilde{I}_{r+1}$ there is $i_2 \in I_{r+1}$ such that $W_{i_1} \subset W_{i_2}$. Put $I_{r+1}^{(s)} = \widetilde{I}_{r+1}^{(s)} \cap I_{r+1}$ for every $m + r \leqslant s \leqslant n$. Thus using the algorithm from [1] we construct the required families of algebraic varieties $W_\iota$, $\iota \in I_{r+1}^{(s)}$, $m + r \leqslant s \leqslant n$. After that applying Lemma 1 for every $\iota \in I_{r+1}^{(s)}$ for every $m + r \leqslant s \leqslant n$ we construct the polynomials $h_\alpha$, $\alpha \in A_\iota$. So now by Lemma 1 and Lemma 2 properties (a) and (b) hold for all these algebraic varieties $W_\iota$.

If $I_{r+1}^{(s)} = \varnothing$ for all $m + r \leqslant s \leqslant n$ then $n_0 = r$, the required smooth stratification is constructed and all the assertions of Theorem 2 are proved.

Assume that $I_{r+1}^{(s)} \neq \varnothing$ for at least one $s$ such that $m+r \leqslant s \leqslant n$. For brevity put $m_u = (m + 1)2^{u-m} - 1$ for all integers $u \geqslant m$. Note that by the recursive assumption $\sum_{i \in I_r^{(u)}} d_i \leqslant (ud)^{m_u}$ for every $u$ such that $m+r-1 \leqslant u \leqslant n$. Hence for every integer $a \geqslant 1$ we have

$$\sum_{i \in I_r^{(u)}} d_i^a \leqslant (ud)^{m_u\, a}.$$

Let us show that

$$\left(\frac{s-1}{s}\right)^{m_s} (s - m) \leqslant 1. \tag{12}$$

for all integers $s > m \geqslant 1$. Indeed, $(1 - 1/s)^s \leqslant e^{-1}$. Therefore (12) is a consequence of the inequality $e^{-m_s/s}(s - m) \leqslant 1$. Put $q = s - m$. Then the last inequality is equivalent to $-(m + 1)\, 2^q + 1 + (q + m) \log(q) \leqslant 0$. We have $2^q > \log(q)$ for $q \geqslant 1$. Hence (12) follows from $-2^{q+1} + 1 + (q + 1) \log(q) \leqslant 0$. One can check immediately that the last inequality holds true for all $q \geqslant 1$. The required assertion is proved.

Also for all integers $s > u \geqslant v \geqslant m \geqslant 1$ we have

$$m_u + m_v(s - u) \leqslant m_u(s - u + 1) \leqslant ((m + 1)2^{u-m} - 1)2^{s-u} \leqslant m_s - 1,$$
$$(m_u + 1)(s - u + 1) - 1 \leqslant (m + 1)2^{u-m}2^{s-u} - 1 = m_s.$$

Now

$$\begin{aligned}
&D^{(s)}_{r+1} = \sum_{\iota\in I^{(s)}_{r+1}} \deg W_\iota \leqslant \\
&\sum_{m+r-1\leqslant u<s,\, i\in I^{(u)}_r} d_i(ud_i)^{s-u} + \sum_{\substack{m+r-1\leqslant v\leqslant u<s,\\ i\in I^{(u)}_r,\, j\in I^{(v)}_r,\, i\neq j}} d_i d_j^{s-u} \leqslant \\
&\sum_{m+r-1\leqslant u<s,\, i\in I^{(u)}_r} d_i(ud_i)^{s-u} + \sum_{\substack{m+r-1\leqslant u<s,\, m+r-1\leqslant v\leqslant u,\\ i\in I^{(u)}_r,\, j\in I^{(v)}_r\; i\neq j}} d_i d_j^{s-u} \leqslant \\
&\sum_{m\leqslant u\leqslant s-1} (ud)^{m_u(s-u+1)}u^{s-u} + \sum_{m\leqslant u\leqslant s-1}\sum_{m\leqslant v\leqslant u} (ud)^{m_u}(vd)^{m_v(s-u)} \leqslant \\
&d^{m_s-1}\Big(\sum_{m\leqslant u\leqslant s-1} u^{m_u}\Big(u^{(m_u+1)(s-u)} + \sum_{m\leqslant v\leqslant u} v^{m_v(s-u)}\Big)\Big) \leqslant \\
&d^{m_s-1}\Big(\sum_{m\leqslant u\leqslant s-1} u^{m_u}\Big(u^{(m_u+1)(s-u)} + \sum_{m\leqslant v\leqslant u} u^{m_v(s-u)}\Big)\Big) \leqslant \\
&d^{m_s-1}\Big(\sum_{m\leqslant u\leqslant s-1} u^{m_u}\Big(u^{(m_u+1)(s-u)} + u^{m_u(s-u)+1}\Big)\Big) \leqslant \\
&d^{m_s-1}\sum_{m\leqslant u\leqslant s-1} u^{m_u}(2u^{(m_u+1)(s-u)}) \leqslant d^{m_s}\sum_{m\leqslant u\leqslant s-1} u^{(m_u+1)(s-u+1)-1} \leqslant \\
&(sd)^{m_s}\sum_{m\leqslant u\leqslant s-1}(u/s)^{m_s} \leqslant (sd)^{m_s}((s-1)/s)^{m_s}(s-m) \leqslant (sd)^{m_s}.
\end{aligned}$$

Thus, we have proved the required estimation from Theorem 2 for $D^{(s)}_{r+1}$.

At present to complete the proof it is sufficient to ascertain the estimate for $M^{(s)}_{r+1}$. Let $\iota \in I^{(s)}_{r+1}$.

Let $i \in I^{(u)}_r$, $m+r-1 \leqslant u < s$. Assume that $W_\iota$ is a component of $\mathrm{Sing}W_i$. Then there are polynomials $F_{u+1},\dots,F_s$ which are linear combinations of $J_\beta$, $\beta \in B_i$, with integer coefficients of the lengths $O(n\log(nd_i))$ and satisfy the following property (†).

(†) There is a sequence of irreducible and defined over $\mathbb{Q}$ algebraic varieties

$$W^{(u)} = W_i,\ W^{(u+1)},\ \dots,\ W^{(s)} = W_\iota$$

such that $W^{(j+1)}$ is an irreducible over $\mathbb{Q}$ component of $W^{(j)} \cap \mathcal{Z}(F_{j+1})$ for every $u \leqslant j < s$.

Similarly let $i \in I^{(u)}_r$, $j \in I^{(v)}_r$, $m+r-1 \leqslant v \leqslant u < s$, $i \neq j$, and $W_\iota$ is a component of $W_i \cap W_j$. Then there are polynomials $F_{u+1},\dots,F_s$ which are linear combinations of $h_\alpha$, $\alpha \in A_j$, with integer coefficients of the lengths $O(n\log((d_id_j))$ satisfying the property (†).

In the both cases the estimation for $M^{(s)}_{r+1}$ can be obtained straightforwardly by subsequent applying Lemma 3 using the ascertained inequalities for $M^{(w)}_r$, $w \leqslant u$. One should only take the degree of the polynomial $\mathcal{P}$ from Theorem 2 sufficiently large relative to the degree of the polynomials from Lemma 3.

Let us give more details. In what follows till the end of the proof $\mathcal{P}$ is the polynomial from the statement of Theorem 3 (it is fixed). By the Bézout theorem in the first case the degree of the algebraic variety $W^{(u+q)}$, $1 \leqslant q \leqslant s-u$, is bounded from above by $d_i(ud_i)^q \leqslant (ud)^{m_u(q+1)}u^q$ by the recursive assumption. In the second case $\deg W^{(u+q)} \leqslant d_i d_j^q \leqslant (ud)^{m_u(q+1)}$. In the first case by the recursive assumption the lengths of integer coefficients of the polynomial $F_{u+q}$, $1 \leqslant q \leqslant s-u$, are bounded from above by $uM_r^{(u)} + O(n^2 D_r^{(u)}) \leqslant C_1 u(M+n^2)\mathcal{P}((ud)^{m_u})$ for an absolute constant $C_1 > 0$ (of course, one can give here a better bound but it is not essential for the proof). Similarly in the second case the lengths of integer coefficients of the polynomial $F_{u+q}$ are bounded from above by $M_r^{(v)} + O(n^2(D_r^{(u)} + D_r^{(v)})) \leqslant C_1(M+n^2)\mathcal{P}((ud)^{m_u})$.

Now denote by $\mathcal{P}_0$ the polynomial $\mathcal{P}$ from the statement of Lemma 3 (to avoid an ambiguity we change the notation). Denote by $\overline{W}_\iota$ the closure of the algebraic variety $W_\iota$ in the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$. Then applying Lemma 3 subsequently $s-u$ times we get (here the details are left to the reader) that in the both cases the lengths of integer coefficients of the polynomial $H_{\overline{W}_\iota}$ are bounded from above by

$$(s-u+1)C_1 u(M+n^2)\mathcal{P}((ud)^{m_u}) \prod_{1\leqslant q\leqslant s-u} \mathcal{P}_0((ud)^{m_u(q+1)}u^q) \leqslant$$
$$(M+n^2)\mathcal{P}((ud)^{m_u})\mathcal{P}_1((ud)^{m_u(s-u)^2}).$$

for a polynomial $\mathcal{P}_1$ depending only on $\mathcal{P}_0$ and $C_1$. One can choose a polynomial $\mathcal{P}$ such that $\mathcal{P}((ud)^{m_u})\mathcal{P}_1((ud)^{m_u(s-u)^2}) \leqslant \mathcal{P}((sd)^{m_s})$ for all integers $d, s, u, m$ satisfying the inequalities $s > u \geqslant m \geqslant 1$, $d \geqslant 3$. The last assertion follows from the following fact. There is a constant $C > 0$ such that for all integers $s > u \geqslant 1$ we have $Cm_u + m_u(s-u)^2 \leqslant Cm_s$. The required estimation for $M_r^{(s)}$ is proved.

Thus we can construct all the algebraic varieties $W_\iota$, $\iota \in I_{r+1}^{(s)}$, within the required working time applying several times the algorithm from [1] and Lemma 1. Further, for the estimation of the lengths of integer coefficients we use Lemma 3. The theorem is proved. □

The proof of Theorem 3 is completely analogous to the one of Theorem 2 and even easier since here one should consider only the sets of singular points of the components but not the intersections of different components. Note also that in the proof of Theorem 3 we have a more complicated system of notaion. Namely, any index $i \in I_v^{(w)}$ from the proof of Theorem 2 is replaced by a $(v+1)$-tuple of indices $(i_1, \ldots, i_{v+1}) \in I_v^{(w)}$ for all $v, w$. This implies other changes of notations. In particular, in the proof of Theorem 3 the sets of indices $B'_{i_1,\ldots,i_{r+1}}$ and $B_{i_1,\ldots,i_{r+1}}$ are similar to $B'_i$ and $B_i$ from the proof of Theorem 2.

Besides, according to the Definition 2 in the proof of Theorem 3 for all $m + r \leqslant s \leqslant n$ we have $I_{r+1}^{(s)} = \widetilde{I}_{r+1}^{(s)}$, where $\widetilde{I}_{r+1}^{(s)}$ is a union of the sets $I_{i_1,\ldots,i_{u+1},r+1}^{(s)}$ (now they play the role of $I_{i,r+1}^{(s)}$ from the proof of Theorem 2, see above) over all $(i_1, \ldots, i_{u+1}) \in I_r^{(u)}$ and $m + r - 1 \leqslant u < s$. So here one don't need to consider the set $\widetilde{I}$. Theorem 3 is also proved. □

# 3 Solvability of systems over the ring of $p$-adics integers and branching 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 $\lceil z \rceil$ to be the minimal integer $z_0$ such that $z_0 \geqslant z$ and define $\lceil z \rceil_+ = \max\{\lceil z \rceil, 1\}$.

Let us apply Theorem 3 and construct the canonical branching smooth stratification (with all the objects corresponding to to it) of the algebraic variety $V_{i^*} = \mathcal{Z}(f_1, \ldots, f_k)$.

It is convenient also to introduce the algebraic variety $W_{i^*} = \mathbb{A}^n(\overline{\mathbb{Q}})$. So the codimension $\mathrm{codim} W_{i^*} = 0$, the degree $\deg W_{i^*} = 1$ and $W_{i^*}$ is given by an empty system of equations, i.e., $A_{i^*} = \varnothing$.

Set also $I_0^{(0)} = \{i^*\}$ and $I_0^{(u)} = \varnothing$ for all $1 \leqslant u \leqslant n$.

Recall that $D_t = 1 + \max_{1 \leqslant r \leqslant n_0}\{D_r^{(t)}, 3\}$, $M_t = \max_{1 \leqslant r \leqslant n_0} M_r^{(s)}$, $t \in S$, see (3). Put $D_0 = d$, $M_0 = M$.

We shall construct positive integers $c_i^{(s)}$, $s \in S \cup \{0\}$, $0 \leqslant i \leqslant 2$. Put

$$c^{(0)} = c_1^{(0)} \left(c_2^{(0)}\right)^{d^n}, \qquad c^{(s)} = c_0^{(s)} \left(c_1^{(s)}\right)^{D_s^{ns}} \left(c_2^{(s)}\right)^{(sD_s^{s+1})^n}, \quad s \in S.$$

For the constructed integers $c^{(s)}$ property (*) formulated below holds true (we shall ascertain it). Besides that, for every $s \in S \cup \{0\}$ the length of the integer $c^{(s)}$ is bounded from above by $M_s \mathcal{P}(((s+1)D_s^{s+1})^{n^2})$.

Furthermore, we shall prove that one can take

$$\Delta = \left(c^{(0)}\right)^2 \prod_{s \in S} \left(c^{(s)}\right)^{2d^n \prod_{t \in S,\, t < s} (tD_t^{t+1})^n}. \tag{13}$$

Therefore $N = \mathrm{ord}_p(\Delta) + 1$.

Put

$$N_0 = \Big\lceil 2\,\mathrm{ord}_p(c^{(0)}) + 2 \sum_{s \in S} \mathrm{ord}_p(c^{(s)}) d^n \prod_{t \in S,\, t < s} (tD_t^{t+1})^n \Big\rceil_+, \tag{14}$$

$$N_u = \Big\lceil 2 \sum_{s \in S,\, s \geqslant u} \mathrm{ord}_p(c^{(s)}) \prod_{t \in S,\, u \leqslant t < s} (tD_t^{t+1})^n \Big\rceil_+, \quad u \in S. \tag{15}$$

So $1 \leqslant N_u \in \mathbb{Z}$ for all $u \in S \cup \{0\}$. If $N_u = 1$ then $\mathrm{ord}_p(c^{(s)}) = 0$ and $N_s = 1$ for all $s \geqslant u$, $s \in S$. Notice that $N_0 = \lceil \mathrm{ord}_p(\Delta) \rceil_+$ and $N_0 \leqslant N \leqslant N_0 + 1$. We shall use the following simple fact.

**LEMMA 5** *Let $u \in S \cup \{0\}$ be an integer. Then*

$$N_u - 2\mathrm{ord}_p(c^{(u)}) \geqslant 0, \quad N_u - \mathrm{ord}_p(c^{(u)}) > 0.$$

**PROOF** If $\mathrm{ord}_p(c^{(u)}) = 0$ then the both these inequalities are obvious. Assume that $\mathrm{ord}_p(c^{(u)}) > 0$. Then (15) (or (14) for $u = 0$) holds true without $\lceil \ldots \rceil_+$ and hence $N_u - 2\mathrm{ord}_p(c^{(u)}) \geqslant 0$. Consequently $N_u - \mathrm{ord}_p(c^{(u)}) \geqslant \mathrm{ord}_p(c^{(u)}) > 0$. The lemma is proved. $\square$

In what follows we shall assume that there is a point $x \in \mathbb{Z}^n$ such that $f_i(x) = 0 \bmod p^N$, $1 \leqslant i \leqslant k$. We shall prove that in this case the system

$f_1 = \ldots = f_k = 0$ has a solution in $\mathbb{Z}_p^n$. Actually we shall use in the proof only that $f_i(x) = 0 \bmod p^{N_0}$, $1 \leqslant i \leqslant k$. Thus Theorem 4 will be proved.

Now $h_\alpha = 0$, $\alpha \in A_{i_1,\ldots,i_r}$, is the system of polynomial equations determining the algebraic variety $W_{i_1,\ldots,i_r}$ according to the described construction of the canonical branching smooth stratification.

Let $1 \leqslant r \leqslant n_0 + 1$ be an integer. Denote by $\mathcal{Q}_{i_1,\ldots,i_r}$ the following assertion.

- There is an algebraic variety $W_{i_1,\ldots,i_r}$ from the construction of the canonical branching smooth stratification such that the codimension $\operatorname{codim} W_{i_1,\ldots,i_r} = u$ for some $u \in S \cup \{0\}$ and

$$h_\alpha(x) = 0 \bmod p^{N_u} \quad \text{for all} \quad \alpha \in A_{i_1,\ldots,i_r}. \tag{16}$$

The property of the integers $c^{(s)}$ is the following one (one should ascertain it in the proof of the theorem).

(*) Assume that the assertion $\mathcal{Q}_{i_1,\ldots,i_r}$ holds true for some indices $i_1, \ldots, i_r$. Then either the assertion $\mathcal{Q}_{i_1,\ldots,i_r,i_{r+1}}$ holds true for some index $i_{r+1} \in I_{i_1,\ldots,i_r}$, or $r \geqslant 2$ and there is a point of the algebraic variety $W_{i_1,\ldots,i_r}$ with all the coordinates from $\mathbb{Z}_p$.

Let us show that it is sufficient to construct $c^{(s)}$, $s \in S \cup \{0\}$, and ascertain (*) to finish the proof of the theorem. Indeed, suppose that all $c^{(s)}$ are constructed and this property is proved. We have $A_{i^*} = \varnothing$. Hence the property $\mathcal{Q}_{i_1}$ with $i_1 = i^*$ is fulfilled. Assume that there are no points with coordinates from $\mathbb{Z}_p$ in any $W_{i_1,\ldots,i_r}$ with $r \geqslant 2$. Then applying several times property (*) we get that (16) is valid for some $W_{i_1,\ldots,i_r}$, $1 \leqslant r \leqslant n_0 + 1$ such that $V_{i_1,\ldots,i_r} = \varnothing$. In this case $I_{i_1,\ldots,i_r} = \varnothing$. It is a contradiction. Our assertion is proved.

Now we are going to define and compute the integers $c_i^{(u)}$, $0 \leqslant i \leqslant 2$, and after that $c^{(u)}$ for all $u \in S \cup \{0\}$.

Let $u \in S \cup \{0\}$. Let us enumerate integers $r \geqslant 1$ and elements $(i_1, \ldots, i_r) \in I_{r-1}^{(u)}$. Assume at first that $u \in S$ and hence $r \geqslant 2$. Then we have $\operatorname{codim} W_{i_1,\ldots,i_r} = u$. The degrees $\deg_{X_1,\ldots,X_n} h_\alpha \leqslant D_u - 1$ for all $\alpha \in A_{i_1,\ldots,i_r}$ by (3)

Let us enumerate elements $\beta = (\alpha_1, \ldots, \alpha_u, j_1, \ldots, j_u) \in B_{i_1,\ldots,i_r}$. Then $h_{\alpha_1}, \ldots, h_{\alpha_u}$ is a system of local parameters of the algebraic variety $W_{i_1,\ldots,i_r}$ with the Jacobian $J_\beta$, see (11). The degrees of the Jacobians $J_\beta$, $\beta \in B_{i_1,\ldots,i_r}$, defining the set of singular points of the algebraic variety $W_{i_1,\ldots,i_r}$ are at most $u(D_u - 2)$ and lengths of integer coefficients of these Jacobians are less than $uM_u + O(n^2 D_u)$ (of course, one can write a better estimate here but it is not essential for the proof).

By $W_{i_1,\ldots,i_r,\tau}$, $\tau \in T_{i_1,\ldots i_r,\beta}$, denote the family of all the defined and irreducible over $\mathbb{Q}$ components $W'$ of the algebraic variety $\mathcal{Z}(h_{\alpha_1}, \ldots, h_{\alpha_u})$ such that $W' \neq W_{i_1,\ldots,i_r}$ and $W' \setminus \mathcal{Z}(J_\beta) \neq \varnothing$. Note that the number $\#T_{i_1,\ldots i_r,\beta} \leqslant (D_u - 1)^u - 1$ and the degree $\deg W' \leqslant (D_u - 1)^u - \deg W_{i_1,\ldots,i_r} \leqslant (D_u - 1)^u - 1$ by the Bézout theorem. We shall assume in what follows without loss of generality that for any two distinct elements $(i_1, \ldots i_r, \beta)$ and $(i'_1, \ldots i'_{r'}, \beta')$ the intersection $T_{i_1,\ldots i_r,\beta} \cap T_{i'_1,\ldots i'_{r'},\beta'} = \varnothing$ is empty.

Using the algorithm from [1] we construct all the algebraic varieties $W_{i_1,\ldots,i_r,\tau}$, $\tau \in T_{i_1,\ldots i_r,\beta}$. Furthermore, for every $\tau$ construct the polynomials $\psi_1, \ldots, \psi_\sigma \in \mathbb{Z}[X_1, \ldots, X_n]$ such that

$$W_{i_1,\ldots,i_r,\tau} = \mathcal{Z}(\psi_1, \ldots, \psi_\sigma),$$

the degree $\deg_{X_1,\dots,X_n}\psi_i \leqslant \deg W_{i_1,\dots,i_r,\tau}$ and lengths of integer coefficients of these polynomials are less than $(M_u+n)\mathcal{P}(D_u^u)$ for all $1\leqslant i\leqslant\sigma$. The number of polynomials $\sigma\leqslant\mathcal{P}(D_u^u)$ for a polynomial $\mathcal{P}$. The working time of the algorithm from [1] for constructing these polynomials is polynomial in $M_u$ and $D_u^{n^2}$.

The Jacobian $J_\beta$ is vanishing on $W_{i_1,\dots,i_r}\cap W_{i_1,\dots,i_r,\tau}$. Notice that $D_u^u-1\geqslant \max_{\alpha,i}\{\deg_{X_1,\dots,X_n}\psi_i,\deg_{X_1,\dots,X_n}h_\alpha\}$ and $D_u^u-1\geqslant 3$, see (3). Hence by the efficient Hilbert Nullstellensatz, see [10], we have

$$c_{i_1,\dots,i_r,\tau}J_\beta^a=\sum_{1\leqslant i\leqslant\sigma}\psi_i q_i+\sum_{\alpha\in A_{i_1,\dots,i_r}}h_\alpha r_\alpha, \tag{17}$$

where $1\leqslant a\leqslant (D_u^u-1)^n$, $a\in\mathbb{Z}$ ($a$ depends on $\tau$), $1\leqslant c_{i_1,\dots,i_r,\tau}\in\mathbb{Z}$, $q_i, r_\alpha\in\mathbb{Z}[X_1,\dots,X_n]$ are polynomials such that the degrees

$$\deg_{X_1,\dots,X_n}(\psi_i q_i),\quad \deg_{X_1,\dots,X_n}(h_\alpha r_\alpha)$$

are bounded from above by $(1+\deg_{X_1,\dots,X_n}J_\beta)(D_u^u-1)^n<uD_u^{nu+1}$ for all $i,\alpha$, see [10]. Besides, $c_{i_1,\dots,i_r,\tau}$ is chosen to be minimal possible in the sense that the greatest common divisor of $c_{i_1,\dots,i_r,\tau}$ and all the integer coefficients of the polynomials $q_i$ and $r_\alpha$ is equal to 1.

For every $\tau$ solving linear systems over $\mathbb{Q}$ with respect to the unknown coefficients of the polynomials $q_i/c_{i_1,\dots,i_r,\tau}$, $1\leqslant i\leqslant\sigma$, and $r_\alpha/c_{i_1,\dots,i_r,\tau}$, $\alpha\in A_{i_1,\dots,i_r}$, we construct all $q_i$, $r_\alpha$ with integer coefficients and $c_{i_1,\dots,i_r,\tau}$. Note that the number of unknowns and the number of equations of any of these linear systems are bounded from above $\mathcal{P}(D_u^{n^2u})$ for a polynomial $\mathcal{P}$. The lengths of integer coefficients of these linear systems are bounded from above by $M_u\mathcal{P}(D_u^{nu})$. Thus we get that the maximum of lengths of all $c_{i_1,\dots,i_r,\tau}$ is less than $M_u\mathcal{P}(D_u^{n^2u})$ for a polynomial $\mathcal{P}$.

For all $u\in S$ construct the sets

$$E_u=\big\{(i_1,\dots,i_\kappa,\tau)\,:\,(i_1,\dots,i_\kappa)\in I_{\kappa-1}^{(u)},\,2\leqslant\kappa\leqslant n_0+1,\\ \tau\in T_{i_1,\dots,i_\kappa,\beta},\,\beta\in B_{i_1,\dots,i_\kappa}\big\}.$$

Recall that if $\kappa\geqslant 2$ then $\sum_{(i_1,\dots,i_\kappa)\in I_{\kappa-1}^{(u)}}\deg W_{i_1,\dots,i_\kappa}=D_{\kappa-1}^{(u)}$ and hence the number of elements $\#I_{\kappa-1}^{(u)}<D_u$. Further, $\#T_{i_1,\dots,i_\kappa,\beta}<D_u^u$, $\#B_{i_1,\dots,i_\kappa}<(\#A_{i_1,\dots,i_\kappa})^u n^u\leqslant (D_u^n)^u n^u$. Therefore the number of elements $\#E_u\leqslant\mathcal{P}(D_u^{nu})$ for a polynomial $\mathcal{P}$.

In what follows LCM denotes the least common multiple of a family of integers. Construct the integer $c_0^{(u)}=\mathrm{LCM}_{(i_1,\dots,i_\kappa,\tau)\in E_u}(c_{i_1,\dots,i_\kappa,\tau})$. So $c_0^{(u)}\geqslant 1$ and the length of $c_0^{(u)}$ is bounded from above by $M_u\mathcal{P}(D_u^{n^2u})$ for a polynomial $\mathcal{P}$.

Put

$$N'_u=\lceil (N_u-\mathrm{ord}_p(c_0^{(u)}))/D_u^{nu}\rceil_+,\quad u\in S. \tag{18}$$

Now we return to the general case $u\in S\cup\{0\}$ and $r\geqslant 1$. So at present $(i_1,\dots,i_r)\in I_{r-1}^{(u)}$ and $u=\mathrm{codim}W_{i_1,\dots,i_r}$. If $u=0$ then $r=1$ and $i_1=i^*$. By definition put $c_0^{(0)}=1$, $N'_0=N_0$.

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. If $r\geqslant 2$ then this system consists of all equations $h_\alpha = 0$, $\alpha \in A_{i_1,\dots,i_r}$, and $J_\beta = 0$, $\beta \in B_{i_1,\dots,i_r}$. When $r = 1$ then by definition the polynomials $G_\rho$ coincide with the initial polynomials $f_1, \dots, f_k$.

If $r \geqslant 2$ then set $\delta = (uD_u)^n$, $\mu = M_u$. If $r = 1$ then set $\delta = d^n$, $\mu = M$. Note that $I_{i_1,\dots,i_r}$ is a set of indices of the family of irreducible components of the algebraic variety $V_{i_1,\dots,i_r}$. Therefore $\# I_{i_1,\dots,i_r} \leqslant \delta$ by the Bézout theorem.

Let $i_{r+1} \in I_{i_1,\dots,i_r}$. Let $\alpha_1, \dots, \alpha_b$ be all the pairwise distinct elements of the set $A_{i_1,\dots,i_r,i_{r+1}}$ (here $b = \# A_{i_1,\dots,i_r,i_{r+1}}$ depends on $i_1, \dots, i_r, i_{r+1}$). For every integer $1 \leqslant \gamma \leqslant \delta^{n+1}$ put $G_{i_{r+1},\gamma} = \sum_{1 \leqslant j \leqslant b} \gamma^j h_{\alpha_j}$. Notice that any $b' \leqslant b$ pairwise distinct of polynomials $G_{i_{r+1},\gamma}$ are linearly independent over $\mathbb{Q}$.

Note that the degree $\deg W_{i_1,\dots,i_{r+1}} \leqslant \delta$ and $b \leqslant \delta^n$.

Recall that $h_\alpha$, $\alpha \in A_{i_1,\dots,i_r,i_{r+1}}$, is a family of polynomials corresponding to the generic projection of the algebraic variety $W_{i_1,\dots,i_{r+1}}$. At present we consider $W_{i_1,\dots,i_{r+1}}$ as a component of the algebraic variety $\mathcal{Z}(G_\rho, \rho \in R)$. Hence by Lemma 1 the lengths of integer coefficients of all the polynomials $h_\alpha$, $\alpha \in A_{i_1,\dots,i_r,i_{r+1}}$, are bounded from above by $(\mu+n^2)\mathcal{P}(\delta)$ for a polynomial $\mathcal{P}$. Hence the lengths of integer coefficients of all the polynomials $G_{i_{r+1},\gamma}$ are bounded from above by $\mu\mathcal{P}(\delta^n)$ for a polynomial $\mathcal{P}$.

We do not assume that $I_{i_1,\dots,i_r} \neq \varnothing$ (so it may happen that $I_{i_1,\dots,i_r} = \varnothing$ and then below the product in the left part of (19) is equal to 1). We have $\deg_{X_1,\dots,X_n} G_\rho \leqslant \delta^{1/n}$ for every $\rho \in R$ and $\delta^{1/n} \geqslant 3$. Hence by the efficient Hilbert Nullstellensatz [10] for every $1 \leqslant \gamma \leqslant \delta^{n+1}$

$$c_{i_1,\dots,i_r,\gamma}\Big(\prod_{i_{r+1} \in I_{i_1,\dots,i_r}} G_{i_{r+1},\gamma}\Big)^{a'} = \sum_{\rho \in R} G_\rho q_{\rho,\gamma} \tag{19}$$

where $1 \leqslant a' \leqslant \delta$, $a' \in \mathbb{Z}$ ($a'$ depends on $\gamma$), $1 \leqslant c_{i_1,\dots,i_r,\gamma} \in \mathbb{Z}$, $q_{\rho,\gamma} \in \mathbb{Z}[X_1, \dots, X_n]$ are polynomials such that the degrees $\deg_{X_1,\dots,X_n}(G_\rho q_{\rho,\gamma}) \leqslant a'(\delta^2 + 1) \leqslant \delta(\delta^2 + 1)$ for all $\rho, \gamma$, see [10]. Besides, $c_{i_1,\dots,i_r,\gamma}$ is chosen to be minimal possible in the sense that the greatest common divisor of $c_{i_1,\dots,i_r,\gamma}$ and all the integer coefficients of the polynomials $q_{\rho,\gamma}$ is equal to 1.

The coefficients of polynomials $q_{\rho,\gamma}/c_{i_1,\dots,i_r,\gamma}$ can be constructed by solving linear systems over $\mathbb{Q}$. These linear systems have integer coefficients with lengths bounded from above by $\mu\mathcal{P}(\delta^n)$. The numbers of unknowns and equations of any such linear system are bounded from above by $\mathcal{P}(\delta^n)$ for a polynomial $\mathcal{P}$. An estimation for a solution of any of the considered linear systems gives also an upper bound for $|c_{i_1,\dots,i_r,\gamma}|$. So we get $|c_{i_1,\dots,i_r,\gamma}| \leqslant 2^{\mu\mathcal{P}(\delta^n)}$ for a polynomial $\mathcal{P}$.

For all $u \in S \cup \{0\}$ construct the sets

$$C_u = \{(i_1, \dots, i_\kappa, \gamma) : (i_1, \dots, i_\kappa) \in I^{(u)}_{\kappa-1},\ 1 \leqslant \kappa \leqslant n_0 + 1,\ 1 \leqslant \gamma \leqslant \delta^{n+1}\}.$$

Construct all the integers $c_{i_1,\dots,i_r,\gamma}$, $(i_1, \dots, i_\kappa, \gamma) \in C_u$, solving linear systems corresponding to (19). Define the integers

$$c_1^{(u)} = \mathrm{LCM}_{(i_1,\dots,i_\kappa,\gamma) \in C_u}(c_{i_1,\dots,i_\kappa,\gamma}), \quad c_2^{(u)} = \prod_{1 \leqslant i_1 < i_2 \leqslant \delta^{n+1}} (i_2 - i_1)$$

for all $u \in S \cup \{0\}$.

Recall that if $\kappa \geqslant 2$ then $\# I_{\kappa-1}^{(u)} \leqslant D_{\kappa-1}^{(u)} < D_u$. If $\kappa = 1$ and $u = 0$ then $I_0^{(u)} = \{i^*\}$ and finally if $\kappa = 1$ and $u \neq 0$ then $I_0^{(u)} = \varnothing$, see the beginning of the section.

Consequently if $r \geqslant 2$ then $\# C_u \leqslant n_0 D_u \delta^{n+1}$. If $r = 1$ then $u = 0$ and $\# C_u \leqslant \delta^{n+1}$. Therefore in any case $|c_1^{(u)} c_2^{(u)}| \leqslant 2^{\mu \mathcal{P}(\delta^n)}$ for a polynomial $\mathcal{P}$. Recall that $M_0 = M$, $D_0 = d$. Then $|c^{(u)}| \leqslant 2^{M_u \mathcal{P}(D_u^{(u+1)n^2})}$ for a polynomial $\mathcal{P}$. Compute $\Delta$. As a result we get

$$\Delta < 2^{M\mathcal{P}(d^{n^2}) + \sum_{s \in S} M_s \mathcal{P}(D_s^{sn^2}) d^n \prod_{t \in S,\, t<s} (tD_t^{t+1})^n}$$

for a polynomial $\mathcal{P}$.

Now our aim is to prove (*). Thus, suppose that $1 \leqslant r \leqslant n_0 + 1$ and the property $\mathcal{Q}_{i_1,\ldots,i_r}$ holds true.

Assume at first that $r \geqslant 2$ and hence $u \in S$. Recall that the integer $N'_u$ is defined by (18) for $u \geqslant 1$. Suppose that there is $\beta \in B_{i_1,\ldots,i_r}$ such that

$$J_\beta(x) \neq 0 \bmod p^{N'_u}. \tag{20}$$

Then applying the standard Hensel lemma (one should fix the variables with respect to which there are no partial derivatives in the matrix of the Jacobian) we get that there is a point

$$\widetilde{x} \in \mathcal{Z}(h_{\alpha_1}, \ldots, h_{\alpha_u}) \setminus \mathcal{Z}(J_\beta)$$

with coordinates from $\mathbb{Z}_p$ such that $\widetilde{x} = x \bmod p^{N_u - N'_u + 1}$ (in the sense that this congruence takes place coordinate–wise).

Let us show that $N_u - (N'_u - 1) \geqslant N'_u$. Indeed, $D_u \geqslant 4$ by (3). Hence if $1 \leqslant N_u \leqslant 7$ then $N'_u = 1$ and consequently $N_u - (N'_u - 1) \geqslant N'_u$. If $N_u \geqslant 8$ then $N_u \geqslant 2N_u/4 + 1 = 2(N_u/4 + 1) - 1 \geqslant 2N'_u - 1$. The required assertion is proved. Hence $J(\widetilde{x}) \neq 0 \bmod p^{N'_u}$ and $\mathrm{ord}_p J(\widetilde{x}) \leqslant N'_u - 1$.

Let us show that $\widetilde{x} \in W_{i_1,\ldots,i_r}$. Suppose contrary. Then there is $\tau \in T_{i_1,\ldots i_r,\beta}$ such that $\widetilde{x} \in W_{i_1,\ldots,i_r,\tau}$. Obviously $q_i(\widetilde{x}) = 0$ for all $i$ and $h_\alpha(\widetilde{x}) = 0 \bmod p^{N_u - (N'_u - 1)}$ for all $\alpha$ since $h_\alpha(x) = 0 \bmod p^{N_u}$ and $\widetilde{x} = x \bmod p^{N_u - (N'_u - 1)}$. Now (17) at the point $\widetilde{x}$ implies that

$$\mathrm{ord}_p(c_{i_1,\ldots,i_r,\tau}) + (D_u^u - 1)^n (N'_u - 1) \geqslant N_u - (N'_u - 1).$$

This implies $N'_u - 1 \geqslant (N_u - \mathrm{ord}_p(c_0^{(u)}))/D_u^u$. But $(N_u - \mathrm{ord}_p(c_0^{(u)}))/D_u^u \geqslant (N_u - \mathrm{ord}_p(c^{(u)}))/D_u^u > 0$ by Lemma 5. Hence $N'_u - 1 \geqslant (N_u - \mathrm{ord}_p(c_0^{(u)}))/D_u^u > 0$ which contradicts to the definitions of the integer $N'_u$. Our assertion is proved.

So we shall suppose in what follows without loss of generality that

$$J_\beta(x) = 0 \bmod p^{N'_u}, \tag{21}$$

for all $\beta \in B_{i_1,\ldots,i_r}$.

Now we return to the general case $1 \leqslant r \leqslant n$. Consider the algebraic variety $V_{i_1,\ldots,i_r}$. Put $\nu_i^{(u)} = \mathrm{ord}_p(c_i^{(u)})$ for all $u \in S \cup \{0\}$, $0 \leqslant i \leqslant 2$.

Let $u \in S$. Then $N'_u > 0$, $\nu_1^{(u)} \geqslant 0$ and

$$N'_u - 2\nu_1^{(u)} \geqslant (N_u - 2\nu_0^{(u)} - 2\nu_1^{(u)} D_u^{nu})/(D_u^{nu}) \geqslant (N_u - 2\mathrm{ord}_p(c^{(u)}))/(D_u^{nu}) \geqslant 0$$

by Lemma 5. Hence $N'_u - \nu_1^{(u)} > 0$.

Similarly if $u = 0$ then $N'_0 = N_0 > 0$, $\nu_1^{(0)} \geqslant 0$ and

$$N'_0 - 2\nu_1^{(0)} \geqslant N_0 - 2\nu_1^{(0)} \geqslant N_0 - 2\mathrm{ord}_p(c^{(0)}) \geqslant 0$$

by Lemma 5. Hence $N'_0 - \nu_1^{(0)} > 0$.

Therefore according to (21) and the property $\mathcal{Q}_{i_1,\dots,i_r}$ for every $u \in S \cup \{0\}$ for every $\rho \in R$

$$\mathrm{ord}_p G_\rho(x) - \mathrm{ord}_p(c_{i_1,\dots,i_r,\gamma}) \geqslant N'_u - \nu_1^{(u)} > 0.$$

Hence $I_{i_1,\dots,i_r} \neq \varnothing$ and $V_{i_1,\dots,i_r} \neq \varnothing$ by (19). Therefore $u \neq \max S$. Put $u_1 = \min\{s : s \in S \,\&\, s > u\}$. Notice that if $u = 0$ then $u_1 = m$.

Recall that $1 \leqslant \gamma \leqslant \delta^{n+1}$. Hence again by (19) there exists an index $i_{r+1} \in I_{i_1,\dots,i_r}$ such that

$$G_{i_{r+1},\gamma_j}(x) = 0 \bmod p^{\lceil (N'_u - \nu_1^{(u)})/\delta \rceil_+}$$

for $\delta^n$ pairwise distinct indices $\gamma_j$, $1 \leqslant j \leqslant \delta^n$.

Set $N''_u = \lceil (N'_u - \nu_1^{(u)})/\delta \rceil_+$. Let $u \in S$. Then $N''_u > 0$, $\nu_2^{(u)} \geqslant 0$ and

$$\begin{aligned}
&N''_u - 2\nu_2^{(u)} \geqslant (N'_u - \nu_1^{(u)})/\delta - 2\nu_2^{(u)} \geqslant \\
&(N'_u - 2\nu_1^{(u)})/(uD_u)^n - 2\nu_2^{(u)} \geqslant \\
&(N_u - 2\nu_0^{(u)} - 2\nu_1^{(u)}(D_u)^{nu} - 2\nu_2^{(u)}(uD_u^{u+1})^n)/(uD_u^{u+1})^n = \\
&(N_u - 2\mathrm{ord}_p(c^{(u)}))/(uD_u^{u+1})^n \geqslant 0
\end{aligned}$$

by Lemma 5. Hence $N''_u - \nu_2^{(u)} > 0$.

Let us show that if $u \in S$ then

$$N''_u - \nu_2^{(u)} \geqslant N_{u_1}. \tag{22}$$

Indeed, if $N_{u_1} = 1$ then it is obvious. If $N_{u_1} > 1$ then $N_u > 1$ and (15) holds true for $u$ and $u_1$ (in place of $u$) without $\lceil \dots \rceil_+$. Hence

$$N''_u - \nu_2^{(u)} \geqslant (N_u - 2\mathrm{ord}_p(c^{(u)}))/(uD_u^{u+1})^n \geqslant N_{u_1}.$$

The required assertion is proved.

Similarly if $u = 0$ then $N''_0 > 0$, $\nu_2^{(0)} \geqslant 0$ and

$$N''_0 - 2\nu_2^{(0)} \geqslant (N_0 - 2\nu_1^{(0)} - 2\nu_2^{(0)} d^n)/d^n \geqslant 0.$$

Hence $N''_0 - \nu_2^{(0)} > 0$. Furthermore,

$$N''_0 - \nu_2^{(0)} \geqslant N_m. \tag{23}$$

The proof of (23) is analogous to the proof of (22).

The set of zeroes of the polynomials $G_{i_{r+1},\gamma_j}$, $1 \leqslant j \leqslant \delta^n$, coincides with $W_{i_1,\dots,i_r,i_{r+1}}$. Every polynomial $h_\alpha$, $\alpha \in A_{i_1,\dots,i_{r+1}}$ is a linear combination with rational coefficients of the polynomials $G_{i_{r+1},\gamma_j}$. Hence from the definition of $c_2^{(u)}$ we get

$$h_\alpha(x) = 0 \bmod p^{N''_u - \nu_2^{(u)}}, \quad \alpha \in A_{i_1,\dots,i_{r+1}}. \tag{24}$$

The codimension of $W_{i_1,\dots,i_r,i_{r+1}} = v > u$. We have $N_v \leqslant N_{u_1}$. Now (24) and (22), (23) imply immediately that

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

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

# References


[1] **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), p. 124–188 (Russian) [English transl.: J. Sov. Math. 34 (4) (1986)].

[2] **Chistov A. L.:** *"Efficient Smooth Stratification of an Algebraic Variety in Zero–Characteristic and its Applications"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 266 (2000) p.254–311 (in Russian), correction http://www.mathsoc.spb.ru/preprint/2004/04-13.ps.gz [English transl.: J. of Mathematical Sciences v.113, No.5, p.689-717].

[3] **Chistov A. L.:** *"An improvement of the complexity bound for solving systems of polynomial equations"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 390 (2011), p. 299–306.

[4] **Chistov A. L.:** *"Systems with Parameters, or Efficiently Solving Systems of Polynomial Equations 33 Years Later. I"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 462 (2017), p. 122–166 (in Russian) [English transl.: Journal of Mathematical Sciences, v. 232 (2018) Issue 2, p. 177-203].

[5] **Chistov A. L.:** *"Systems with Parameters or Efficiently Solving Systems of Polynomial Equations, 33 Years Later. II"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 468 (2018), p. 138–176 (in Russian) [English transl.: Journal of Mathematical Sciences, v. 240 (2019) Issue 5, p. 594-616].

[6] **Gelfond A.:** *"Transcendental and algebraic numbers"*, Dover, 1960.

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

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

[9] **Chistov A., Karpinski M.:** *"Complexity of Deciding Solvability of Polynomial Equations over p-adic Integers"*, Research report Institut für Informatik der Universität Bonn, 1997, 85183-CS.

[10] **Kollar J.:** *"Sharp effective Nullstellensatz"*, J. Amer. Math. Soc. 1 (1988), p. 963–975.

[11] **Lazard D.:** *"Résolution des systémes d'équations algébriques"*, Theor. Comput. Sci. v.15 (1981), p. 77–110.