Polynomial complexity of solving systems of few algebraic equations with small degrees

Dima Grigoriev (Lille)

CNRS

11/09/2012, Berlin

Complexity of solving polynomial systems

Let a system of polynomial equations

$$f_1 = \cdots = f_k = 0 \qquad (1)$$

be given where $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$, degrees $\deg(f_i) \le d$, $1 \le i \le k$ and the absolute values of integer coefficients of polynomials $f_1, \ldots, f_k$ do not exceed 2^M.

The algorithm (Chistov-G.) finds the irreducible components of the variety in $\mathbb{C}^n$ given by system (1) within complexity polynomial in k, d^{n^2}, M.

A similar complexity bound $(k \cdot d)^{n^{O(1)}}$, M holds for the algorithm (G.-Vorobjov) which finds the connected components of the semialgebraic set in $\mathbb{R}^n$ given by system of inequalities

$$f_1 \ge 0, \ldots, f_k \ge 0. \qquad (2)$$

Renegar: testing solvability of (2) (respectively, of (1)) within complexity polynomial in $(kd)^n$, M (respectively, k, d^n, M) and producing a solution in case it does exist.

Complexity of solving polynomial systems

Let a system of polynomial equations

$$f_1 = \cdots = f_k = 0 \qquad (1)$$

be given where $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$, degrees $\deg(f_i) \le d$, $1 \le i \le k$ and the absolute values of integer coefficients of polynomials $f_1, \ldots, f_k$ do not exceed 2^M.

The algorithm (Chistov-G.) finds the irreducible components of the variety in $\mathbb{C}^n$ given by system (1) within complexity polynomial in $k,\ d^{n^2},\ M$.

A similar complexity bound $(k \cdot d)^{n^{O(1)}}$, M holds for the algorithm (G.-Vorobjov) which finds the connected components of the semialgebraic set in $\mathbb{R}^n$ given by system of inequalities

$$f_1 \ge 0, \ldots, f_k \ge 0. \qquad (2)$$

Renegar: testing solvability of (2) (respectively, of (1)) within complexity polynomial in $(kd)^n$, M (respectively, k, d^n, M) and producing a solution in case it does exist.

Complexity of solving polynomial systems

Let a system of polynomial equations

$$f_1 = \cdots = f_k = 0 \qquad (1)$$

be given where $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$, degrees $\deg(f_i) \le d$, $1 \le i \le k$ and the absolute values of integer coefficients of polynomials $f_1, \ldots, f_k$ do not exceed 2^M.

The algorithm (Chistov-G.) finds the irreducible components of the variety in $\mathbb{C}^n$ given by system (1) within complexity polynomial in $k,\ d^{n^2},\ M$.

A similar complexity bound $(k \cdot d)^{n^{O(1)}}, M$ holds for the algorithm (G.-Vorobjov) which finds the connected components of the semialgebraic set in $\mathbb{R}^n$ given by system of inequalities

$$f_1 \ge 0, \ldots, f_k \ge 0. \qquad (2)$$

Renegar: testing solvability of (2) (respectively, of (1)) within complexity polynomial in $(kd)^n$, M (respectively, k, d^n, M) and producing a solution in case it does exist.

Complexity of solving polynomial systems

Let a system of polynomial equations

$$f_1 = \cdots = f_k = 0 \qquad (1)$$

be given where $f_1, \dots, f_k \in \mathbb{Z}[X_1, \dots, X_n]$, degrees $\deg(f_i) \le d$, $1 \le i \le k$ and the absolute values of integer coefficients of polynomials $f_1, \dots, f_k$ do not exceed 2^M.

The algorithm (Chistov-G.) finds the irreducible components of the variety in $\mathbb{C}^n$ given by system (1) within complexity polynomial in $k,\ d^{n^2},\ M$.

A similar complexity bound $(k \cdot d)^{n^{O(1)}},\ M$ holds for the algorithm (G.-Vorobjov) which finds the connected components of the semialgebraic set in $\mathbb{R}^n$ given by system of inequalities

$$f_1 \ge 0, \dots, f_k \ge 0. \qquad (2)$$

Renegar: testing solvability of (2) (respectively, of (1)) within complexity polynomial in $(kd)^n$, M (respectively, k, d^n, M) and producing a solution in case it does exist.

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0, \deg(f_i) \leq 2, 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in n^k, M, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}}, M$ and produce a solution if it does exist.

In particular, the complexity is polynomial when k, d are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard: $X_i^2 = X_i, 1 \leq i \leq n, c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem)

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0,\ \deg(f_i) \leq 2,\ 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in $n^k,\ M$, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}},\ M$ and produce a solution if it does exist.

In particular, the complexity is polynomial when $k,\ d$ are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard: $X_i^2 = X_i,\ 1 \leq i \leq n,\ c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem).

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0, \deg(f_i) \leq 2, 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in n^k, M, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}}, M$ and produce a solution if it does exist.

In particular, the complexity is polynomial when k, d are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard: $X_i^2 = X_i, 1 \leq i \leq n, c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem)

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0, \deg(f_i) \leq 2, 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in n^k, M, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}}, M$ and produce a solution if it does exist.

In particular, the complexity is polynomial when k, d are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard: $X_i^2 = X_i, 1 \leq i \leq n, c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem).

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0, \deg(f_i) \leq 2, 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in n^k, M, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}}$, M and produce a solution if it does exist.

In particular, the complexity is polynomial when k, d are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard: $X_i^2 = X_i, 1 \leq i \leq n, c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem)

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0, \deg(f_i) \leq 2, 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in n^k, M, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}}, M$ and produce a solution if it does exist.

In particular, the complexity is polynomial when k, d are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard: $X_i^2 = X_i, 1 \leq i \leq n, c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem).

Polynomial systems with few equations

G.-Pasechnik: for a system of quadratic inequalities $f_i \geq 0, \deg(f_i) \leq 2, 1 \leq i \leq k$ the algorithm tests solvability within complexity polynomial in n^k, M, so it is polynomial when the number k of inequalities is a constant.

Question: does anything similar hold for equations over $\mathbb{C}$ beyond quadratic polynomials?

Theorem

One can test solvability of a system of polynomial equations over $\mathbb{C}$ within complexity polynomial in $n^{d^{3k}}, M$ and produce a solution if it does exist.

In particular, the complexity is polynomial when k, d are both constant.

One can extend the Theorem to solvability over algebraically closed fields of arbitrary characteristics (then M bounds the bit-size of the coefficients of the polynomials).

For $d = 2$ and $k = n + 1$ the problem of solvability is NP-hard:
$X_i^2 = X_i, 1 \leq i \leq n, c_1 \cdot X_1 + \cdots + c_n \cdot X_n = c$ (KNAPSACK problem)

Testing points for sparse polynomials

A polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ is called t-sparse if it contains at most t monomials. Let p_i denote the i-th prime and a point $s_j = (p_1^j, \ldots, p_n^j) \in \mathbb{Z}^n$, $j \geq 0$.

Lemma

For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \ldots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

Corollary

Let $\deg f \leq D$. There exists $0 \leq j < \binom{n+D}{n}$ such that $f(s_j) \neq 0$.

Testing points for sparse polynomials

A polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ is called t-sparse if it contains at most t monomials. Let p_i denote the i-th prime and a point $s_j = (p_1^j, \ldots, p_n^j) \in \mathbb{Z}^n$, $j \geq 0$.

Lemma

For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \ldots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

Corollary

Let $\deg f \leq D$. There exists $0 \leq j < \binom{n+D}{n}$ such that $f(s_j) \neq 0$.

Testing points for sparse polynomials

A polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ is called t-sparse if it contains at most t monomials. Let p_i denote the i-th prime and a point $s_j = (p_1^j, \ldots, p_n^j) \in \mathbb{Z}^n$, $j \geq 0$.

Lemma

For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \ldots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

Corollary

Let $\deg f \leq D$. There exists $0 \leq j < \binom{n+D}{n}$ such that $f(s_j) \neq 0$.

Testing points for sparse polynomials

A polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ is called t-sparse if it contains at most t monomials. Let p_i denote the i-th prime and a point $s_j = (p_1^j, \ldots, p_n^j) \in \mathbb{Z}^n$, $j \geq 0$.

Lemma

For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \ldots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

Corollary

Let $\deg f \leq D$. There exists $0 \leq j < \binom{n+D}{n}$ such that $f(s_j) \neq 0$.

Testing points for sparse polynomials

A polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ is called t-sparse if it contains at most t monomials. Let p_i denote the i-th prime and a point $s_j = (p_1^j, \ldots, p_n^j) \in \mathbb{Z}^n$, $j \geq 0$.

Lemma

For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \ldots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

Corollary

Let $\deg f \leq D$. There exists $0 \leq j < \binom{n+D}{n}$ such that $f(s_j) \neq 0$.

Testing points for sparse polynomials

A polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ is called t-sparse if it contains at most t monomials. Let p_i denote the i-th prime and a point $s_j = (p_1^j, \ldots, p_n^j) \in \mathbb{Z}^n$, $j \geq 0$.

Lemma

For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \ldots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

Corollary

Let $\deg f \leq D$. There exists $0 \leq j < \binom{n+D}{n}$ such that $f(s_j) \neq 0$.

Reduction of solvability to systems in few variables

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Then $\dim V =: m \geq n - k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality.

Let variables $X_{i_1}, \ldots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \ldots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \ldots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \ldots, X_{i_m} = c_m\}$ for different $c_1, \ldots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \ldots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \ldots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \ldots, X_{i_m})$ for appropriate integers b_i. Moreover, there exist $n - m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \ldots, Y_{n-m}$ of this form. One can view $Y_1, \ldots, Y_{n-m}, X_{i_1}, \ldots, X_{i_m}$ as new coordinates.

Reduction of solvability to systems in few variables

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Then $\dim V =: m \geq n-k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality.

Let variables $X_{i_1}, \dots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \dots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \dots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \dots, X_{i_m} = c_m\}$ for different $c_1, \dots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \dots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \dots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \dots, X_{i_m})$ for appropriate integers b_i. Moreover, there exist $n-m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \dots, Y_{n-m}$ of this form. One can view $Y_1, \dots, Y_{n-m}, X_{i_1}, \dots, X_{i_m}$ as new coordinates.

Reduction of solvability to systems in few variables

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Then $\dim V =: m \geq n - k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality.

Let variables $X_{i_1}, \dots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \dots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \dots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \dots, X_{i_m} = c_m\}$ for different $c_1, \dots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \dots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \dots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \dots, X_{i_m})$ for appropriate integers b_i. Moreover, there exist $n - m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \dots, Y_{n-m}$ of this form. One can view $Y_1, \dots, Y_{n-m}, X_{i_1}, \dots, X_{i_m}$ as new coordinates.

Reduction of solvability to systems in few variables

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Then $\dim V =: m \geq n - k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality.

Let variables $X_{i_1}, \ldots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \ldots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \ldots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \ldots, X_{i_m} = c_m\}$ for different $c_1, \ldots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \ldots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \ldots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \ldots, X_{i_m})$ for appropriate integers b_i. Moreover, there exist $n - m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \ldots, Y_{n-m}$ of this form. One can view $Y_1, \ldots, Y_{n-m}, X_{i_1}, \ldots, X_{i_m}$ as new coordinates.

Reduction of solvability to systems in few variables

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Then $\dim V =: m \geq n - k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality.

Let variables $X_{i_1}, \ldots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \ldots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \ldots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \ldots, X_{i_m} = c_m\}$ for different $c_1, \ldots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \ldots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \ldots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \ldots, X_{i_m})$ for appropriate integers b_i. Moreover, there exist $n - m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \ldots, Y_{n-m}$ of this form. One can view $Y_1, \ldots, Y_{n-m}, X_{i_1}, \ldots, X_{i_m}$ as new coordinates.

Reduction of solvability to systems in few variables

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Then $\dim V =: m \geq n - k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality.

Let variables $X_{i_1}, \dots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \dots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \dots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \dots, X_{i_m} = c_m\}$ for different $c_1, \dots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \dots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \dots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \dots, X_{i_m})$ for appropriate integers b_i. Moreover, there exist $n - m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \dots, Y_{n-m}$ of this form. One can view $Y_1, \dots, Y_{n-m}, X_{i_1}, \dots, X_{i_m}$ as new coordinates.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \leq l \leq n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \leq \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \leq e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \leq d^k + d^{2k}$. Consider the product $H := \prod_{1 \leq l \leq n-m} H_l$, then $D := \deg H \leq (n-m) \cdot (d^k + d^{2k}) \leq d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q,\ h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: continued

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \le l \le n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \le j < \binom{D+m}{D} \le m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \ne 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \ne 0$, $1 \le l \le n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \le j < m^{d^{2k}}$ and $1 \le i_1, \dots, i_m \le n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \leq j < \binom{D+m}{D} \leq m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \leq l \leq n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \leq j < m^{d^{2k}}$ and $1 \leq i_1, \dots, i_m \leq n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \leq j < \binom{D+m}{D} \leq m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \leq l \leq n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \leq j < m^{d^{2k}}$ and $1 \leq i_1, \dots, i_m \leq n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \leq j < \binom{D+m}{D} \leq m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \ldots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \leq l \leq n-m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \leq j < m^{d^{2k}}$ and $1 \leq i_1, \ldots, i_m \leq n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \le j < \binom{D+m}{D} \le m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \le l \le n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \le j < m^{d^{2k}}$ and $1 \le i_1, \dots, i_m \le n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \le j < \binom{D+m}{D} \le m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \le l \le n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \le j < m^{d^{2k}}$ and $1 \le i_1, \dots, i_m \le n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \le j < \binom{D+m}{D} \le m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \ldots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \le l \le n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \le j < m^{d^{2k}}$ and $1 \le i_1, \ldots, i_m \le n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j\}$ is not empty.

Reduction of solvability to systems in few variables: testing points

Due to testing points for sparse polynomials there exists $0 \le j < \binom{D+m}{D} \le m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \le l \le n - m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Corollary

For an irreducible component $V \subset \mathbb{C}^n$ of $\dim(V) = m$ of the variety given by a system of equations $f_1 = \cdots = f_k = 0$ there exist $0 \le j < m^{d^{2k}}$ and $1 \le i_1, \dots, i_m \le n$ such that intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

Test of solvability and its complexity

To test solvability of system $f_1 = \cdots = f_k = 0$ the algorithm chooses all possible subsets $\{i_1, \dots, i_m\} \subset \{1, \dots, n\}$ with $m \geq n - k$ treating $X_{i_1}, \dots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by this system. After that for each $0 \leq j < \binom{D+m}{D}$ where $D \leq d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j$ into polynomials $f_1, \dots, f_k$ and solves the resulting system of polynomial equations in $n - m \leq k$ variables applying the algorithm by Chistov-G. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e. a polynomial in $M \cdot n^{d^{3k}}$. Moreover, our algorithm yields a solution of a system, provided that it does exist. Summarizing

Theorem

One can test solvability over $\mathbb{C}$ of a system of k polynomials $f_1, \dots, f_k \in \mathbb{Z}[X_1, \dots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \leq M \cdot n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions.

Test of solvability and its complexity

To test solvability of system $f_1 = \cdots = f_k = 0$ the algorithm chooses all possible subsets $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ with $m \geq n - k$ treating $X_{i_1}, \ldots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by this system. After that for each $0 \leq j < \binom{D+m}{D}$ where $D \leq d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j$ into polynomials $f_1, \ldots, f_k$ and solves the resulting system of polynomial equations in $n - m \leq k$ variables applying the algorithm by Chistov-G. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e. a polynomial in $M \cdot n^{d^{3k}}$. Moreover, our algorithm yields a solution of a system, provided that it does exist. Summarizing

Theorem

One can test solvability over $\mathbb{C}$ of a system of k polynomials $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \leq M \cdot n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions.

Test of solvability and its complexity

To test solvability of system $f_1 = \cdots = f_k = 0$ the algorithm chooses all possible subsets $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ with $m \geq n - k$ treating $X_{i_1}, \ldots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by this system. After that for each $0 \leq j < \binom{D+m}{D}$ where $D \leq d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j$ into polynomials $f_1, \ldots, f_k$ and solves the resulting system of polynomial equations in $n - m \leq k$ variables applying the algorithm by Chistov-G. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e. a polynomial in $M \cdot n^{d^{3k}}$. Moreover, our algorithm yields a solution of a system, provided that it does exist. Summarizing

Theorem

One can test solvability over $\mathbb{C}$ of a system of k polynomials $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \leq M \cdot n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions.

Test of solvability and its complexity

To test solvability of system $f_1 = \cdots = f_k = 0$ the algorithm chooses all possible subsets $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ with $m \geq n - k$ treating $X_{i_1}, \ldots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by this system. After that for each $0 \leq j < \binom{D+m}{D}$ where $D \leq d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j$ into polynomials $f_1, \ldots, f_k$ and solves the resulting system of polynomial equations in $n - m \leq k$ variables applying the algorithm by Chistov-G. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e. a polynomial in $M \cdot n^{d^{3k}}$. Moreover, our algorithm yields a solution of a system, provided that it does exist. Summarizing

Theorem

One can test solvability over $\mathbb{C}$ of a system of k polynomials $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \leq M \cdot n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions.

Test of solvability and its complexity

To test solvability of system $f_1 = \cdots = f_k = 0$ the algorithm chooses all possible subsets $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$ with $m \geq n - k$ treating $X_{i_1}, \ldots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by this system. After that for each $0 \leq j < \binom{D+m}{D}$ where $D \leq d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \ldots, X_{i_m} = p_m^j$ into polynomials $f_1, \ldots, f_k$ and solves the resulting system of polynomial equations in $n - m \leq k$ variables applying the algorithm by Chistov-G. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e. a polynomial in $M \cdot n^{d^{3k}}$. Moreover, our algorithm yields a solution of a system, provided that it does exist. Summarizing

Theorem

One can test solvability over $\mathbb{C}$ of a system of k polynomials $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \leq M \cdot n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions.

Test of solvability and its complexity

To test solvability of system $f_1 = \cdots = f_k = 0$ the algorithm chooses all possible subsets $\{i_1, \dots, i_m\} \subset \{1, \dots, n\}$ with $m \geq n - k$ treating $X_{i_1}, \dots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by this system. After that for each $0 \leq j < \binom{D+m}{D}$ where $D \leq d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j$ into polynomials $f_1, \dots, f_k$ and solves the resulting system of polynomial equations in $n - m \leq k$ variables applying the algorithm by Chistov-G. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e. a polynomial in $M \cdot n^{d^{3k}}$. Moreover, our algorithm yields a solution of a system, provided that it does exist. Summarizing

Theorem

One can test solvability over $\mathbb{C}$ of a system of k polynomials $f_1, \dots, f_k \in \mathbb{Z}[X_1, \dots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \leq M \cdot n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions.