How to test in subexponential time whether two points can be connected by a curve in a semialgebraic set

(Extended Abstract)

D. Yu. Grigoriev
Leningrad Department of Mathematical V. A. Steklov
Institute of Academy of Sciences of the USSR
Fontanka embankment 27, 191011, Leningrad, USSR

A subexponential-time algorithm is designed which finds the number of connected components of a semialgebraic set given by a quantifier-free formula of the first-order theory of real closed fields (for a rather wide class of real close fields, cf. [GV 88], [Gr 88]). Moreover, the algorithm allows for any two points from the semialgebraic set to test, whether they belong to the same connected component.

Decidability of the mentioned problems follows from the quantifier elimination method in the first-order theory of real closed fields, described for the first time by A. Tarski ([Ta 51]). However, complexity bound of this method is nonelementary, in particular, one cannot estimate it by any finite iteration of the exponential function. G. Collins ([Co 75]) has proposed a construction of cylindrical algebraic decomposition, which allows to solve these problems in exponential time.

For an arbitrary ordered field F we denote by $\tilde{F} \supset F$ its uniquely defined real closure. In the sequel we consider input polynomials over the ordered ring $\mathbf{Z}_m = \mathbf{Z}[\delta_1, \ldots, \delta_m] \subset \mathbb{Q}_m = \mathbb{Q}(\delta_1, \ldots, \delta_m)$, where $\delta_1, \ldots, \delta_m$ are algebraically independent elements over $\mathbb{Q}$ and the ordering in the field $\mathbb{Q}_m$ is defined as follows. The element δ_1 is infinitesimal with respect to $\mathbb{Q}$ (i. e. $0 < \delta_1 < \alpha$ for any rational number $0 < \alpha \in \mathbb{Q}$) and for each $1 \leq i < m$ the element $\delta_{i+1} > 0$ is infinitesimal with respect to the field $\mathbb{Q}_i$ (cf. [GV 88], [Gr 88]).

Thus, let an input quantifier-free formula Ξ for the first-order theory of real closed fields be given, containing atomic subformulae of the form $f_i \geq 0$, $1 \leq i \leq k$ where $f_i \in \mathbf{Z}_m[X_1, \ldots, X_n]$.

Any rational function $g \in \mathbb{Q}_m(Y_1, \ldots, Y_s)$ can be represented as $g = g_1/g_2$ where the polynomials $g_1, g_2 \in \mathbf{Z}_m[Y_1, \ldots, Y_s]$ are reciprocately prime. Denote by $l(g)$ the maximum of bit-lengths of the (integer) coefficients of the polynomials g_1, g_2 (in the variables $Y_1, \ldots, Y_s, \delta_1, \ldots, \delta_m$). In the sequel we assume that the following bounds are valid:

$$\deg_{x_1,\ldots,x_n}(f_i) < d,\ deg_{\delta_1,\ldots,\delta_m}(f_i) < d_0,\ l(f_i) \leq M, \quad 1 \leq i \leq k \tag{1}$$

where d, d_0, M are some integers. Then the bit-length of the formula Ξ can be estimated by the value $L = kMd^n d_0^m$ (cf. [CG 83], [Gr 86]).

Note that in the case $m = 0$, i. e. for the polynomials with integer coefficients, the algorithms from [Co 75] allow to produce the connected components (in particular to solve the problems considered in the present paper) within polynomial in $M(kd)^{2^{O(n)}}$ time.

We use the notation $h_1 \leq P(h_2, \ldots, h_t)$ for the functions $h_1 > 0, \ldots, h_t > 0$ if for the suitable integers c, γ the inequality $h_1 \leq c(h_2 \cdot \ldots \cdot h_t)^\gamma$ is fulfilled.

Recall that a semialgebraic set (in F^n where F is a real closed field) is a set $\{\Pi\} \subset F^n$ of all points satisfying a certain quantifier-free formula Π of the first-order theory of the field F with the atomic subformulae of the form $(g \geq 0)$ where the polynomials $g \in F[X_1, \ldots, X_n]$.

A semialgebraic set $\{\Xi\} \subset (\tilde{\mathbb{Q}}_m)^n$ is (uniquely) decomposable in a union of a finite number of connected components $\{\Xi\} = \bigcup_{1 \leq i \leq t}\{\Xi_i\}$, each of them in its turn being a semialgebraic set determined by appropriate quantifier-free formula Ξ_i of the first-order theory of the field $\tilde{\mathbb{Q}}_m$ (see e. g. [Co 75] for the field $F = \mathbb{R}$, for an arbitrary real closed field one can involve Tarski ([Ta 51]). Note that $t \leq (kd)^{O(n)}$ (see e. g. [GV 88], [Gr 88]).

We use the following way of representing the points $u = (u_1, \ldots, u_n) \in (\tilde{\mathbb{Q}}_m)^n$ (cf. [GV 88]). Firstly, for

© 1990 ACM 089791-401-5 /90/0008/0104 $1.50

the field $\mathbb{Q}_m(u_1, \ldots, u_n)$ a primitive element η is produced such that $\mathbb{Q}_m(u_1, \ldots, u_n) = \mathbb{Q}_m[\eta]$, herewith a minimal polynomial $\varphi(Z) \in \mathbb{Q}_m[Z]$ for η is indicated, furthermore $\eta = \sum_{1 \le i \le n} \alpha_i u_i$ for some integers $0 \le \alpha_1, \ldots, \alpha_n \le \deg_Z(\varphi)$. Also the expressions $u_i = \sum_{0 \le j < \deg_Z(\varphi)} \beta_i^{(j)} \eta^j$ are yielded, where $\beta_i^{(j)} \in \mathbb{Q}_m$. Secondly, for specifying the root η of the polynomial φ a sequence of the signs of the derivatives of all orders $\varphi'(\eta), \varphi^{(2)}(\eta), \ldots, \varphi^{(\deg(\varphi))}(\eta)$ of the polynomial φ in the point η is given. Thom's Lemma (see e. g. [FGM 88]) entails that the latter condition uniquely determines the root η of φ.

We say that a point u satisfies (D, D_0, M)-bound if the following inequalities hold:

$$\deg_Z(\varphi) < D;\ \deg_{\delta_1, \ldots, \delta_m}(\varphi),\ \deg_{\delta_1, \ldots, \delta_m}(\beta_i^{(j)}) \le D_0;$$

$$l(\varphi), l(\beta_i^{(j)}) \le M$$

Then the bit-length of the representation of the point u does not exceed $P(M, D, D_0^m, n)$ (cf. [GV 88], [Gr 88]). The main purpose of the paper is to prove the following theorem (see also [VG 91]).

Theorem.

1. There is an algorithm, which for any formula of the form Ξ, satisfying the bounds (1), finds the number of connected components (in particular, tests the connectedness) of a semialgebraic set $\{\Xi\} \subset (\tilde{\mathbb{Q}}_m)^n$ in time $P(M, (d_0(kd)^{n^{19}})^{n+m}) \le L^{O(\log^{20} L)}$ (i. e. the time-bound is subexponential in L).

2. Moreover, for any two points $u^{(1)}, u^{(2)} \in \{\Xi\}$, satisfying $(\bar{d}, \bar{d}_0, \bar{M})$-bound, the algorithm can test, whether $u^{(1)}, u^{(2)}$ belong to the same connected component of $\{\Xi\}$ in time $P(M, \bar{M}, (d_0\bar{d}_0((kd)^n\bar{d})^{n^{16}})^{n+m})$ (i. e. subexponentially in L and in bit-lengths of the points $u^{(1)}, u^{(2)}$).

This theorem was obtained jointly with N. N. Vorobjov (jr.). As the authors have learned recently, a similar result was obtained by J. Heintz, M.-F. Roy, P. Solerno and besides, in [Ca 88] one can find a fruitful idea for treating the case when $\{\Xi\}$ determines a nonsingular bounded hypersurface.

References

[Ca 88] Canny, J. F., *The Complexity of Robot Motion Planning*, MIT Press, Cambridge (1988).

[CG 83] Chistov, A. L. and Grigoriev, D. Yu., *Subexponential-time Solving Systems of Algebraic Equations*, volumes I and II (1983), Preprints LOMI E-9-83 and E-10-83, Leningrad.

[Co 75] Collins, G. E., *Quantifier Eliminiation for Real Closed Fields by Cylindrical Algebraic Decomposition*, Springer Lecture Notes Comp. Sci. **33** (1975), pp. 134-183.

[FGM 88] Fitchas, N., Galligo, A. and Morgenstern, J., *Algorithmes Rapides en Séquential et en Parallele pour l'Elimination de Quantificateurs en Géométrie Élémentaire*, UER de Mathématiques Universéte de Paris VII (1988).

[Gr 86] Grigoriev, D. Yu., *Computational Complexity in Polynomial Algebra*, Proceedings of the International Congress of Mathematicians, Berkeley (1986), pp. 1452-1460.

[Gr 88] Grigoriev, D. Yu., *Complexity of Deciding Tarski Algebra*, J. Symbolic Computation **5** (1988), pp. 65-108.

[GV 88] Grigoriev, D. Yu. and Vorobjov, N. N., Jr., *Solving Systems of Polynomial Inequalities in Subexponential Time*, J. Symbolic Computation **5** (1988), pp. 37-64.

[Ta 51] Tarski, A., *A Decision Method for Elementary Algebra and Geometry*, University of California Press (1951).

[Vo 89] Vorobjov, N. N., Jr., *Deciding Consistency of Systems of Polynomial in Exponent Inequalities in Subexponential Time*, Notes of Sci. Seminars of Leningrad Department of Math. Steklov Institute **176** (1989), pp. 3-52 (in Russian).

[VG 91] Vorobjov, N. N., Jr. and Grigoriev, D. Yu., *Counting Connected Components of a Semialgebraic Set in Subexponential Time*, Soviet Math. Dokl. (to appear).