Computing sampling points in a semi-algebraic set defined by non-strict inequalities, application to Pattern-Matching Problems

Colas Le Guernic Fabrice Rouillier Mohab Safey El Din

April, 2004

Abstract

We focus on the problem of computing sampling points in a semi-algebraic set defined by equations and non-strict inequalities. This problem is reduced to computing sampling points in several real algebraic varieties, represent these points by rational parametrizations and decide the sign of some polynomials at the real solutions of these parametrizations. We show how these tasks can be deduced from existing algorithms and proceed to a complexity analysis. Then, we study a pattern-matching problems and show how our implementation can solve some instances of these problems.

Introduction

Consider a polynomial family $(f_1, \ldots, f_k, g_1, \ldots, g_s)$ in the polynomial ring $\mathbb{Q}[X_1, \ldots, X_n]$. We are interested in the computation of at least one point in each connected component of the semi-algebraic set $\mathcal{S} \subset \mathbb{R}^n$ defined by:

$$f_1 = \ldots = f_k = 0, \quad g_1 \geq 0, \ldots, g_s \geq 0.$$

In [1], this problem is reduced to the problem of computing sampling points in several real algebraic varieties and determining the sign of some polynomials at the computed points. Several practical algorithms, based on the critical point method, have been provided for computing sampling points in real algebraic sets. In [6], the authors provide an algorithm having the latter specification, which is based on critical points of projections on generic affine sub-spaces. They prove results on its arithmetic complexity. In [7], some bounds on its output are proved. As soon as sampling points are computed, applying the results of [1] imply to determine the signs of some polynomials at the computed points. This can be done by ?????. We show in the sequel how to use these contributions to obtain an efficient algorithm in practice computing sampling points in a semi-algebraic set defined by non-strict inequalities. We also provide complexity results.

Finally, we use these results to solve an application on Pattern-Matching problems. This consists in deciding if there exists a linear transformation sending a polygonal geometric object to the neighbourhood of an other one. We show that our implementation can solve many of these problems. This implementation will be included in the next release of the RAGLib.

1 The Algorithm

The following result reduces the computation of sampling points in a semi-algebraic set to the computation of sampling points in several real algebraic set.

Theorem 1.1. *[1] Let $(f_1, \dots, f_k, g_1, \dots, g_s)$ be a polynomial family in $\mathbb{Q}[X_1, \dots, X_n]$, $\mathcal{S} \subset \mathbb{R}^n$ be the semi-algebraic set defined by:*

$$f_1 = \dots = f_k = 0, \quad g_1 \geq 0, \dots, g_s \geq 0$$

and S be a connected component of $\mathcal{S}$. Then there exists $\{i_1, \dots, i_\ell\}$ such that the algebraic variety defined by:

$$f_1 = \dots = f_k = g_{i_1} = \dots = g_{i_\ell} = 0$$

has a connected component C included in S.

To compute sampling points in a real algebraic set, we use the following result.

Theorem 1.2. *[6] Let $(f_1, \dots, f_k)$ be a polynomial family in $\mathbb{Q}[X_1, \dots, X_n]$ generating a radical and equidimensional ideal and defining a smooth algebraic variety $\mathcal{V} \subset \mathbb{C}^n$ of dimension d. Let $E_1 \subset \cdots \subset E_d$ be d* generic *affine linear subspaces, π_i be the projection on E_i (for $i = 1, \dots, d$), W_i be the critical locus of π_i restricted to $\mathcal{V}$ (for $i = 1, \dots, d$) and $(p_1, \dots, p_d)$ arbitrary rational points such that $(p_1, \dots, p_i) \in E_i$. Then, the algebraic set:*

$$\mathcal{V} \cap \pi_d^{-1}(p_1, \dots, p_d), W_d \cap \pi_{d-1}^{-1}(p_1, \dots, p_{d-1}), \dots, W_2 \cap \pi_1^{-1}(p_1), W_1$$

is zero-dimensional and intersects each connected component of $\mathcal{V} \cap \mathbb{R}^n$.

In generic cases, the output complexity of this algorithm is given in [7] and leads to bounds improving the Thom-Milnor bound on the first Betti number of a real algebraic set. The arithmetic complexity depends on the elimination tool which is used.

Once sampling points in the algebraic variety defined by $f_1 = \dots = f_k = g_{i_1} = \dots = g_{i_\ell} = 0$ (with $\{i_1, \dots, i_\ell\} \subset \{1, \dots, s\}$) are computed, one has to decide the existence of solutions for which the polynomials $g_{j_1}, \dots, g_{j_{s-\ell}}$ (with $\{j_1, \dots, j_{s-\ell}\} = \{1, \dots, s\} \setminus \{i_1, \dots, i_\ell\}$) are positive.

Given polynomials $g_1, \dots, g_s$ and a zero-dimensional ideal I encoding sampling points, this can be done by computing, via a Rational Univariate Representation of the solution set of I and pseudo-remainder computations, univariate polynomials $\widetilde{g}_1, \dots, \widetilde{g}_s$ whose real roots are the real values of $g_1, \dots, g_s$ at the solutions of I. The complexity of such a technique is $\mathcal{O}(s.\mathcal{D}^3)$ where $\mathcal{D}$ denotes the degree of I.

We have developed a strategy which deduces a Gröbner basis of the ideal generated by $G_i - T_i$ (for $i = 1, \dots, s$) and a Gröbner basis of I, where $T_1, \dots, T_s$ are new variables for which we consider a degree ordering. Then, we can compute a Rational Univariate Representation of the solution set of the latter ideal, by taking advantage of informations, such as finding a separating element and the table of multiplication modulo I, appearing during the computation of a Rational Univariate Representation of the solution set of I. Using the algorithms provided in [5] or [2], the arithmetic complexity of this strategy is $\mathcal{O}(s.\mathcal{D}^2)$, which is better than the routines for sign determination given in [1]. The whole algorithm has a better complexity than the preceeding ones. It is a product of a combinatorial factor and a Bézout bound.

2 Application to pattern matching and experimental results

Description of the problem. Let $\mathcal{P}$ and $\mathcal{Q}$ be two geometric objects in an euclidean space E, with a distance function d over such objects, and G a group of transformations. Given a real positive number ϵ, the typical geometric pattern matching problem is to decide if there exists a transformation g in G such that $d(\mathcal{P}, g\mathcal{Q}) < \epsilon$.

To describe our specific problem we need the following notations and definitions. First, a polygonal curve $\mathcal{P}$ is a function from $[0:m]$ to $\mathbb{R}^3$ such as $\mathcal{P}(i) = p_i$ is the i^{th} vertex of $\mathcal{P}$. Then we denote by $Mon(X, Y)$ the set of all non-strictly increasing surjective mappings from a set X to a set Y, where X and Y are finite subsets of $\mathbb{N}$. This set of mappings will be useful to reindex the vertex of polygonal curves. The discrete Fréchet distance between two polygonal curves $\mathcal{P}$ and $\mathcal{Q}$ is:

$$d_F(\mathcal{P}, \mathcal{Q}) = \min_{(\kappa,\lambda)} \parallel \mathcal{P} \circ \kappa - \mathcal{Q} \circ \lambda \parallel_\infty$$

where the pairs (κ, λ) range over $Mon_{m,n} = Mon([1:m+n],[0:m]) \times Mon([1:m+n],[0:n])$. In our case, $\mathcal{P}$ and $\mathcal{Q}$ are polygonal curves in $\mathbb{R}^3$ represented as the list of their vertex, the distance under consideration is the discrete Fréchet distance and $G = SO(3, \mathbb{R})$ is the group of rotations in $\mathbb{R}^3$. Our problem is to decide whether $G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F)$, the set of all g in G such that $d_F(\mathcal{P}, g\mathcal{Q}) \leq \epsilon$, is empty or not. Since it is easier to work on points than to work with curves we introduce (G, ϵ)-transporter set for points p and q in $\mathbb{R}^3$:

$$\tau_{p,q}^{G,\epsilon} = \{g \in G \mid \parallel p - gq \parallel \leq \epsilon\}$$

In [4, 3] the following straightforward relation between $G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F)$ and transporter sets is given:

$$G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F) = \bigcup_{(\kappa,\lambda) \in Mon_{m,n}} \bigcap_{s \in [1:m+n]} \tau^{G,\epsilon}_{p_{\kappa(s)}, q_{\lambda(s)}}$$

Deciding the emptiness of $G(\mathcal{P}, \mathcal{Q}, \epsilon, d_F)$ is equivalent to deciding the emptiness of

$$\bigcap_{s \in [1:m+n]} \tau^{G,\epsilon}_{p_{\kappa(s)}, q_{\lambda(s)}}$$

for each κ, λ in $Mon_{m,n}$.

Transporter polynomials. To describe $\tau^{G,\epsilon}_{p_{\kappa(s)},q_{\lambda(s)}}$ with polynomials, the group $SO(3,\mathbb{R})$ is parametrized by unit quaternions. We will also use the following mapping:

$$\begin{array}{ccc} \mathbb{R}^3 & \rightarrow & \mathbb{H} \\ (x,y,z) & \mapsto & (1,x,y,z) \end{array}$$

The matrix of rotation $g_{(w,x,y,z)}$ is:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & w^2+x^2-y^2-z^2 & 2xy-2wz & 2xz+2wy \\ 0 & 2xy+2wz & w^2-x^2+y^2-z^2 & 2yz-2wx \\ 0 & 2xz-2wy & 2yz+2wx & w^2-x^2-y^2+z^2 \end{bmatrix}$$

A $(SO(3,\mathbb{R}),\epsilon)$ transporter polynomial for p and q is calculated as follows:

$$g^{\epsilon}_{p,q} = \epsilon^2 - \parallel (1,p_x,p_y,p_z) - g_{(w,x,y,z)}(1,q_x,q_y,q_z) \parallel^2$$

where ϵ, (p_x,p_y,p_z), and (q_x,q_y,q_z) are rationals. This leads to the following polynomial system in four unknowns

$$w^2+x^2+y^2+z^2=1,\ g^{\epsilon}_{p_{\kappa(1)},q_{\lambda(1)}} \geq 0,\ \ldots,\ g^{\epsilon}_{p_{\kappa(m+n)},q_{\lambda(m+n)}} \geq 0$$

for each κ,λ in $Mon_{m,n}$. Other parametrization for $SO(3,\mathbb{R})$ can be used. A rotation around a vector u can be decomposed into three rotation around the axis x, y, and z (xyz-convention), this leads to a matrix with 6 variables and 3 constraints:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta_y\cos\theta_z & -\cos\theta_y\sin\theta_z & \sin\theta_y \\ 0 & \sin\theta_x\sin\theta_y\cos\theta_z+\cos\theta_x\sin\theta_z & -\sin\theta_x\sin\theta_y\sin\theta_z+\cos\theta_x\cos\theta_z & -\sin\theta_x\cos\theta_y \\ 0 & -\cos\theta_x\sin\theta_y\cos\theta_z+\sin\theta_x\sin\theta_z & \cos\theta_x\sin\theta_y\sin\theta_z+\sin\theta_x\cos\theta_z & \cos\theta_x\cos\theta_y \end{bmatrix}$$

$\cos\theta_x^2+\sin\theta_x^2=1$, $\cos\theta_y^2+\sin\theta_y^2=1$, $\cos\theta_z^2+\sin\theta_z^2=1$.

Other groups of transformation Other groups of transformation can be considered, the following tabular presents the matrix and constraints used for translations, scalings, and isomorphisms.

	Translation	Scaling	Isomorphism
Matrix	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda_x & 0 & 0 \\ 0 & 0 & \lambda_y & 0 \\ 0 & 0 & 0 & \lambda_z \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x_{1,1} & x_{1,2} & x_{1,3} \\ 0 & x_{2,1} & x_{2,2} & x_{2,3} \\ 0 & x_{3,1} & x_{3,2} & x_{3,3} \end{bmatrix}$
Constraints		$\lambda_x\lambda_y\lambda_z\Lambda=1$	$det(M)D=1$

These transformations can be combined and several polynomial systems of equations and non-strict inequalities can be generated. More specific problems, like uniform scalings or translations following a fixed direction, can also be considered by adding constraints to the system.

3 Computations

The computations have been performed on Pentium III 1GHz with 512 MBytes of RAM. We used the following softwares:

- GB: written in C++ by J.-C. Faugère which computes Gröbner bases;
- RS: written in C by F. Rouillier which computes Rational Univariate Representations and the values taken by a polynomial family at the roots of a zero-dimensional polynomial system;
- RAGLIB: written in Maple, which provides functionalities to compute sampling points in a real algebraic set.

The systems we studied are downloadable at: `http://www-calfor.lip6.fr/~safey/Applications/`. We considered polygonal curves with 10 vertices. On 2-dimensional problems, our implementation solves the problem in at most few minutes. On 3-dimensional problems, our implementation allows a resolution when only 2 linear transformations are considered. The general problem suffers of the intrinsic combinatorial factor involved in our complexity.

References

[1] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry.* Springer-Verlag, 2003.

[2] A. Bostan, B. Salvy, and É. Schost. Fast algorithms for zero-dimensional polynomial systems using duality. *Applicable Algebra in Engineering, Communication and Computing*, 14(4):239–272, 2003.

[3] A. Mosig. *Efficient algorithms for shape and pattern matching.* PhD thesis, Bonn University, to appear, 2004.

[4] A. Mosig and M. Clausen. Approximately matching polygonal curves with respect to the fréchet distance. *submitted to Computational Geometry – Theory and Applications*, 2004.

[5] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *AAECC Journal*, 9(5):433–461, 1999.

[6] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings of the 2003 international symposium on Symbolic and algebraic computation*, pages 224–231. ACM Press, 2003.

[7] M. Safey El Din and P. Trébuchet. Strong bihomogeneous bézout theorem and degree bounds for algebraic optimization. *submitted to Journal of Pure and Applied Algebra*, 2004.