COMPUTING THE EULER-POINCARÉ CHARACTERISTICS OF SIGN CONDITIONS

Saugata Basu, Richard Pollack,
and Marie-Françoise Roy

Abstract. Computing various topological invariants of semi-algebraic sets in single exponential time is an active area of research. Several algorithms are known for deciding emptiness, computing the number of connected components of semi-algebraic sets in single exponential time etc. However, an algorithm for computing all the Betti numbers of a given semi-algebraic set in single exponential time is still lacking. In this paper we describe a new, improved algorithm for computing the Euler-Poincaré characteristic (which is the alternating sum of the Betti numbers) of the realization of each realizable sign condition of a family of polynomials restricted to a real variety. The complexity of the algorithm is $s^{k'+1}O(d)^k + s^{k'}((k' \log_2(s) + k\log_2(d))d)^{O(k)}$ where s is the number of polynomials, k the number of variables, d a bound on the degrees, and k' the real dimension of the variety. A consequence of our result is that the Euler-Poincaré characteristic of any locally closed semi-algebraic set can be computed with the same complexity. The best complexity of any previously known single exponential time algorithm for computing the Euler-Poincaré characteristic of semi-algebraic sets worked only for a more restricted class of closed semi-algebraic sets and had a complexity of $(ksd)^{O(k)}$.

Keywords. Semi-algebraic sets, Euler-Poincaré characteristic
Subject classification. 2000 Mathematics Subject Classification 14P10, 14P25

1. Introduction

Let R be a real closed field. For $Q \in \mathrm{R}[X_1, \ldots, X_k]$ we denote the set of zeros of Q in R^k by $\mathrm{Z}(Q, \mathrm{R}^k) = \{x \in \mathrm{R}^k \mid Q(x) = 0\}$. Now let $Q \in \mathrm{R}[X_1, \ldots, X_k]$, $\deg(Q) \leq d$, and k' the dimension of $Z = \mathrm{Z}(Q, \mathrm{R}^k)$. Given a family $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathrm{R}[X_1, \ldots, X_k]$, with degrees also bounded by d, there are several algorithms known for computing the number of realizable sign conditions of the family $\mathcal{P}$ restricted to the real variety Z, as well as computing the number of connected components of the realization of each such sign condition [10, 13, 12, 16, 18, 3, 4]. The complexity of the best known algorithm is $s^{k'+1}d^{O(k)}$ for the first problem [3], and $s^{k'+1}d^{O(k^2)}$ for the second [4]. In this paper, we consider the problem of computing the Euler-Poincaré characteristic of the realization of each realizable sign condition of $\mathcal{P}$ restricted to the real variety Z. (Here and elsewhere in the paper by the complexity of any algorithm we mean the number of arithmetic operations and sign comparisons performed on the elements of the ring generated by the coefficients of the input polynomials.)

Efficient algorithms for sign determination of univariate polynomials described in [7, 19] are amongst the most basic algorithms in algorithmic real algebraic geometry. Given $\mathcal{P} \subset \mathrm{R}[X], Q \in \mathrm{R}[X]$ with $\#\mathcal{P} = s$, and $\deg(P) \leq d$ for $P \in \mathcal{P} \cup \{Q\}$, these algorithms count for each realizable sign condition of the family $\mathcal{P}$, the cardinality of the set of real zeros of Q, lying in the realization of that sign condition. (Here and everywhere else in the paper $\#(S)$ denotes the cardinality of a set S.) The complexity of the algorithm in [19] is $sd^{O(1)}$. The main contribution of this paper may be viewed as a generalization of this algorithm to the multidimensional situation.

In the multidimensional case, it is no longer meaningful to talk about the cardinalities of the zero set of Q lying in the realizations of different sign conditions of $\mathcal{P}$. However, there exists another discrete valuation on semi-algebraic sets that properly generalizes the notion of cardinality. This valuation is the Euler-Poincaré characteristic.

The Euler-Poincaré characteristic, $\chi(S)$, of a closed and bounded semi-algebraic set $S \subset \mathrm{R}^k$ is defined as

$$\chi(S) = \sum_i (-1)^i b_i(S),$$

where $b_i(S)$ is the rank of the i-th simplicial homology group of S. Note that with this definition, $\chi(\emptyset) = 0$, and $\chi(S) = \#(S)$, whenever $\#(S) < \infty$. Moreover, χ is additive.

There is a natural generalization of the Euler-Poincaré characteristic to semi-algebraic sets which are locally closed (i.e. the intersection of a closed semi-algebraic set with an open one) which retains the additive property. This generalization is based on the theory of Borel-Moore homology groups [9] of locally closed semi-algebraic sets and is described in the next section.

Given $P \in \mathrm{R}[X_1, \ldots, X_k]$, and $S \subset \mathrm{R}^k$, a locally closed semi-algebraic set, we denote

$$\mathcal{R}(P = 0, S) = \{x \in S \mid P(x) = 0\},$$

$$\mathcal{R}(P > 0, S) = \{x \in S \mid P(x) > 0\},$$
$$\mathcal{R}(P < 0, S) = \{x \in S \mid P(x) < 0\}.$$

Notice that these sets are all locally closed. We let $\chi(P = 0, S)$ (respectively $\chi(P > 0, S), \chi(P < 0, S)$) denote the Euler-Poincaré characteristic of $\mathcal{R}(P = 0, S)$ (respectively $\mathcal{R}(P > 0, S)$, $\mathcal{R}(P < 0, S)$).

More generally, given a family of polynomials $\mathcal{P} \subset \mathrm{R}[X_1, \ldots, X_k]$ and a sign condition $\sigma \in \{0, -1, 1\}^{\mathcal{P}}$, we denote by

$$\mathcal{R}(\sigma, S) = \{x \in S \mid \wedge_{P \in \mathcal{P}} \mathrm{sign}(P(x)) = \sigma(P)\}$$

and

$$\chi(\sigma, S) = \chi(\mathcal{R}(\sigma, S))$$

(where $\mathrm{sign}(x) = 0$ (respectively, $= 1, = -1$) iff $x = 0$ (respectively, $> 0, < 0$)). The Euler-Poincaré-query of P with respect to S is

$$\mathrm{EQ}(P, S) = \chi(P > 0, S) - \chi(P < 0, S).$$

As a particular case, given a finite subset $Z \subset \mathrm{R}^k$, and $P \in \mathrm{R}[X_1, \ldots, X_k]$, the Sturm-query of P with respect to Z is the number

$$\mathrm{SQ}(P, Z) = \#(\{x \in Z \mid P(x) > 0\}) - \#(\{x \in Z \mid P(x) < 0\}).$$

Given $\mathcal{P} \subset \mathrm{R}[X], Q \in \mathrm{R}[X]$ with $\#\mathcal{P} = s$, and $\deg(P) \leq d$ for $P \in \mathcal{P} \cup \{Q\}$, the sign determination algorithm in [7] (see also [19]) uses as a basic building block, Sturm-query computations $\mathrm{SQ}(P, Z)$ for various polynomials P, where each such P is a product of certain polynomials in $\mathcal{P}$ or their squares, and $Z = \mathrm{Z}(Q, \mathrm{R})$. The main idea underlying these algorithms is to construct a matrix, M, with entries in $\{0, 1, -1\}$, such that the equation $M \cdot C = SQ$ holds. Here, C is the vector of cardinalities of sets of zeros of Q lying in the realizations of different sign conditions of $\mathcal{P}$, and SQ is a vector of Sturm-queries. Clearly, provided M is invertible, we can compute the vector C from M and SQ. The matrix M is built inductively by taking Kronecker products. If done naively this would lead to tripling its size at each step, leading to a matrix of size 3^s at the end. An obvious but crucial fact used to control the complexity of the algorithms in [7, 19] is that the number of realizable sign conditions of the family $\mathcal{P}$ on $\mathrm{Z}(Q, \mathrm{R})$ is bounded by d. This fact is used to prune the matrix M at each step of the algorithm so that its size never exceeds d. The main algorithm presented in this paper (Algorithm 4.8 in Section 4) is based on similar ideas. Instead of Sturm-queries, it uses the Euler-Poincaré-queries defined above. The role of the matrix equation $M \cdot C = SQ$ is played by Equation (4.2) in Proposition 4.1 below, and it uses a tight bound on the number of realizable sign conditions on a variety (see Proposition 2.12 below) to ensure that the size of the matrix does not grow exponentially in s.

Let $Q \in \mathrm{R}[X_1, \ldots, X_k]$, $Z = \mathrm{Z}(Q, \mathrm{R}^k)$. We denote by $\mathrm{Sign}(\mathcal{P}, Z)$ the list of $\sigma \in \{0, 1, -1\}^{\mathcal{P}}$ such that $\mathcal{R}(\sigma, Z)$ is non-empty. We denote by $\chi(\mathcal{P}, Z)$ the list of Euler-Poincaré characteristics $\chi(\sigma, Z) = \chi(\mathcal{R}(\sigma, Z))$ indexed by elements, σ, of $\mathrm{Sign}(\mathcal{P}, Z)$.

The problem of determining the Euler-Poincaré characteristic of closed semi-algebraic sets was considered in [1] where an algorithm was presented for computing the Euler-Poincaré characteristic of a given closed semi-algebraic set defined by a quantifier-free Boolean formula without negation, with atoms of the form, $P_i \geq 0, P_i \leq 0$, for $1 \leq i \leq s$, $\deg(P_i) \leq d$. The complexity of the algorithm is $(ksd)^{O(k)}$. Moreover, in the special case when the coefficients of the polynomials in $\mathcal{P}$ are integers of bit lengths bounded by τ, the algorithm performs at most $(ksd)^{O(k)}\tau^{O(1)}$ bit operations.

The rest of this paper is devoted to the proof of the following.

Main Result: We present an algorithm (Algorithm 4.8 in Section 4) which given an algebraic set $Z = \mathrm{Z}(Q, \mathrm{R}^k) \subset \mathrm{R}^k$ and a finite set of polynomials $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathrm{R}[X_1, \ldots, X_k]$, computes the list $\chi(\mathcal{P}, Z)$ indexed by elements, σ, of $\mathrm{Sign}(\mathcal{P}, Z)$. If the degrees of the polynomials in $\mathcal{P} \cup \{Q\}$ are bounded by d, and the real dimension of $Z = \mathrm{Z}(Q, \mathrm{R}^k)$ is k', then the complexity of the algorithm is

$$s^{k'+1}O(d)^k + s^{k'}((k' \log_2(s) + k \log_2(d))d)^{O(k)}.$$

If the coefficients of the polynomials in $\mathcal{P} \cup \{Q\}$ are integers of bitsizes bounded by τ, then the bitsizes of the integers appearing in the intermediate computations and the output are bounded by $\tau((k' \log_2(s) + k \log_2(d))d)^{O(k)}$.

In many applications, the combinatorial complexity of algorithms (the part depending on s) is considered more important than the algebraic complexity (the part depending on d). This is especially relevant in computational geometry, where it is customary to treat the degrees of polynomials as well as the dimension as fixed, with the number of polynomials allowed to be large (see [14]). As a result, there has been a lot of research aimed towards designing algorithms for computing various properties of semi-algebraic sets with tight combinatorial complexities. For instance, algorithms with tight combinatorial complexity has been designed for computing the set of all realizable sign conditions of a family of polynomials [3], testing connectivity of semi-algebraic sets

[4, 10] etc. From this point of view, the complexity of the algorithm presented in this paper is significantly better than that of the algorithm in [1] mentioned above, and nearly matches the complexity of the best known algorithm for computing the set of all realizable sign conditions on a variety [3]. Moreover, by the additive property of the Euler-Poincaré characteristic, it is clear that once we have computed the Euler-Poincaré characteristic of every realizable sign condition, it is possible to compute the same for any locally closed semi-algebraic set defined by a quantifier-free formula involving the input polynomials without any additional computational overhead. The algorithm in [1] deals only with closed semi-algebraic sets defined by formulas of a special type. Another interesting aspect of Algorithm 4.8 is that it is really a multidimensional generalization of the sign determination algorithms in [7, 19] for the univariate case and their multivariate generalization [17] for zero-dimensional systems.

The rest of the paper is organized as follows. In Section 2 we state some of the topological results which we will use. If the results have appeared before or are classical we omit the proofs and provide pointers to the appropriate papers. In Section 3 we use an algorithm for computing the Euler-Poincaré characteristic of algebraic sets described in [1] to design the building block for the main algorithm. Finally, in Section 4 we describe the algorithm for computing the Euler-Poincaré characteristics for all sign conditions.

2. Basic Results from Topology

2.1. Definition of the Euler-Poincaré Characteristic. In order to define the Euler-Poincaré characteristic of semi-algebraic sets we first recall the definitions of the simplicial homology groups of a closed and bounded semi-algebraic set $S \subset \mathrm{R}^k$, with R a real closed field.

A closed, bounded semi-algebraic set S can be triangulated by a simplicial complex K [8, 6]. Choose a semi-algebraic triangulation $f : |K| \to S$. The homology group $H_p(S)$ (with coefficients in $\mathbb{Q}$) are defined to be the simplicial homology group (with coefficients in $\mathbb{Q}$), $H_p(K)$, of the simplicial complex K, for $p = 0, 1, \ldots$.

The homology groups of S are all finite dimensional vector spaces over $\mathbb{Q}$. The dimension of $H_p(S)$ as a vector space over $\mathbb{Q}$ is called the p-th Betti number S and denoted $b_p(S)$. The Euler-Poincaré characteristic of S is

$$\chi(S) = \sum_i (-1)^i b_i(S).$$

We are now in a position to define the Euler-Poincaré characteristic for locally closed semi-algebraic sets. This definition agrees with the previously defined Euler-Poincaré characteristic for closed and bounded semi-algebraic sets and turns out to be additive as before. Since the Euler-Poincaré characteristic is a discrete topological invariant of semi-algebraic sets which generalizes the cardinality of a finite set, its additivity is a very natural property to require.

We first recall the definition of simplicial homology groups of pairs of closed and bounded semi-algebraic sets. Let K be a simplicial complex and A a subcomplex of K. Then, there is a natural inclusion homomorphism,

$$\iota : C_p(A) \to C_p(K)$$

between the corresponding chain groups (with coefficients in $\mathbb{Q}$). Defining, the group $C_p(K,A) = C_p(K)/\iota(C_p(A))$, it is easy to see that the the boundary maps $\partial_p : C_p(K) \to C_{p-1}(K)$ descend to maps $\partial_p : C_p(K,A) \to C_{p-1}(K,A)$, so that we have a short exact sequence of complexes,

$$0 \to C_*(A) \to C_*(K) \to C_*(K,A) \to 0.$$

Given a pair (K,A), where A is a subcomplex of K, the group

$$H_p(K,A) = H_p(C(K,A))$$

is the p-th simplicial homology group of the pair (K,A).

It is clear from the definition that $H_p(K,A)$ is a finite dimensional $\mathbb{Q}$-vector space. The dimension of $H_p(K,A)$ as a $\mathbb{Q}$-vector space is called the p-th Betti number of the pair (K,A) and denoted $b_p(K,A)$. The Euler-Poincaré characteristic of the pair (K,A) is

$$\chi(K,A) = \sum_i (-1)^i b_i(K,A).$$

The simplicial homology groups of a pair of closed and bounded semi-algebraic sets $T \subset S \subset \mathrm{R}^k$ are defined as follows. Such a pair of closed, bounded semi-algebraic sets can be triangulated [6] using a pair of simplicial complexes (K,A), where A is a sub-complex of K. The p-th simplicial homology group of the pair (S,T), $H_p(S,T)$, is $H_p(K,A)$. The dimension of $H_p(S,T)$ as a $\mathbb{Q}$-vector space is called the p-th Betti number of the pair (S,T) and denoted $b_p(S,T)$. The Euler-Poincaré characteristic of the pair (S,T) is

$$\chi(S,T) = \sum_i (-1)^i b_i(S,T).$$

The p-th Borel-Moore homology group of $S \subset \mathrm{R}^k$, denoted $H_p^{BM}(S)$, is defined in terms of the homology groups of a pair of closed and bounded semi-algebraic sets as follows. For $r > 0$, let $B_k(0,r)$ denote the open ball of radius r centered at the origin, and let $S_r = S \cap B_k(0,r)$ and $\overline{S_r}$ the closure of S_r. Note that, for a locally closed semi-algebraic set S, both $\overline{S_r}$ and $\overline{S_r} \setminus S_r$ are closed and bounded and hence $H_p(\overline{S_r}, \overline{S_r} \setminus S_r)$ is well defined. Moreover, it is a consequence of Hardt's triviality theorem [15] that the homology group $H_p(\overline{S_r}, \overline{S_r} \setminus S_r)$ is invariant for all sufficiently large $r > 0$. We define, $H_p^{BM}(S) = H_p(\overline{S_r}, \overline{S_r} \setminus S_r)$, for $r > 0$ sufficiently large, and it follows from the remark above that it is well defined. The Borel-Moore homology groups are invariant under semi-algebraic homeomorphisms [8]. It also follows clearly from the definition that for a closed and bounded semi-algebraic set, the Borel-Moore homology groups coincide with the simplicial homology groups.

2.2. Additivity of the Euler-Poincaré Characteristic. The following proposition is well-known (see for example [6]).

PROPOSITION 2.1. *Let $S \subset \mathrm{R}^k$ be a closed and bounded semi-algebraic set, K be a simplicial complex in R^k and $h : |K| \to S$ be a semi-algebraic homeomorphism. Let $n_i(K)$ be the number of simplices of dimension i of K. Then*

$$\chi(S) = \sum_i (-1)^i n_i(K).$$

The following proposition is an immediate consequence of Proposition 2.1.

PROPOSITION 2.2. *Let X_1, X_2 be two closed and bounded semi-algebraic sets. Then,*

$$\chi(X_1 \cup X_2) = \chi(X_1) + \chi(X_2) - \chi(X_1 \cap X_2). \tag{2.3}$$

The Euler-Poincaré characteristic of a locally closed semi-algebraic set S, is related to the Euler-Poincaré characteristic of the closed and bounded semi-algebraic sets $\overline{S_r}$ and $\overline{S_r} \setminus S_r$ for all large enough $r > 0$, by the following lemma.

LEMMA 2.4.

$$\chi(S) = \chi(\overline{S_r}) - \chi(\overline{S_r} \setminus S_r),$$

where $S_r = S \cap B_k(0,r)$ and $r > 0$ and sufficiently large.

Proof. Choose a pair of simplicial complexes (K, A) corresponding to a triangulation of the pair $(\overline{S_r}, \overline{S_r} \setminus S_r)$. From the short exact sequence of chain complexes,

$$0 \to C_*(A) \to C_*(K) \to C_*(K, A) \to 0,$$

we obtain the following long exact sequence of homology groups:

$$\cdots H_p(A) \to H_p(K) \to H_p(K, A) \to H_{p-1}(A) \to H_{p-1}(K) \to \cdots .$$

It follows that,

$$\chi(S) = \chi(K, A) = \chi(K) - \chi(A) = \chi(\overline{S_r}) - \chi(\overline{S_r} \setminus S_r).$$

□

Proposition 2.5. *Let $T \subset S \subset \mathrm{R}^k$ be a pair of closed and bounded semi-algebraic sets, (K, A) be a pair of simplicial complexes in R^k, with A being a subcomplex of K and let $h : |K| \to S$ be a semi-algebraic homeomorphism such that the image of $|K|$ is T. Let $n_i(K)$ be the number of simplices of dimension i of K, and let $m_i(A)$ be the number of simplices of dimension i of A. Then*

$$\chi(S, T) = \chi(K, A) = \sum_i (-1)^i n_i(K) - \sum_i (-1)^i m_i(A).$$

Proof. First note that $\chi(K, A) = \chi(K) - \chi(A)$ (see proof of Lemma 2.4). The proposition is now an immediate consequence of Proposition 2.1. □

Proposition 2.6 (Additivity of Euler-Poincaré characteristic). *Let X, X_1 and X_2 be locally closed semi-algebraic sets such that*

$$X_1 \cup X_2 = X, X_1 \cap X_2 = \emptyset.$$

Then

$$\chi(X) = \chi(X_1) + \chi(X_2).$$

Proof. This is an easy consequence of the invariance of the Borel-Moore homology groups under semi-algebraic homeomorphisms using Proposition 2.5.

□

Let $S \subset \mathrm{R}^k$ be a closed semi-algebraic set. Using the notation of the introduction, we have:

PROPOSITION 2.7. *The following equality holds:*

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} \chi(P=0,S) \\ \chi(P>0,S) \\ \chi(P<0,S) \end{bmatrix} = \begin{bmatrix} \mathrm{EQ}(1,S) \\ \mathrm{EQ}(P,S) \\ \mathrm{EQ}(P^2,Z) \end{bmatrix} \tag{2.8}$$

PROOF. We need to prove

$$\chi(P=0,S)+\chi(P>0,S)+\chi(P<0,S)=\mathrm{EQ}(1,S), \tag{2.9}$$

$$\chi(P>0,S)-\chi(P<0,S)=\mathrm{EQ}(P,S), \tag{2.10}$$

$$\chi(P>0,S)+\chi(P<0,S)=\mathrm{EQ}(P^2,S). \tag{2.11}$$

The claim is an immediate consequence of Proposition 2.6. □

2.3. Number of Connected Components of Realizable Sign Conditions. We will need a bound on the number of connected components of the realizations of all realizable sign conditions of a family of polynomials on a real variety, which we state below. Let $\mathcal{P} \subset \mathrm{R}[X_1,\ldots,X_k]$ and $Q \in \mathrm{R}[X_1,\ldots,X_k]$ and $Z = \mathrm{Z}(Q,\mathrm{R}^k)$.

For $\sigma \in \mathrm{Sign}(\mathcal{P},Z)$, let $b_i(\sigma)$ denote the i-th Betti number of

$$\mathcal{R}(\sigma,Z)=\{x\in\mathrm{R}^k \mid Q(x)=0 \bigwedge_{P\in\mathcal{P}} \mathrm{sign}(P(x))=\sigma(P)\}.$$

Let

$$b_i(\mathcal{P},Z)=\sum_{\sigma} b_i(\sigma).$$

Note that $b_0(\mathcal{P},Z)$ is the number of semi-algebraically connected components of basic semi-algebraic sets defined by $\mathcal{P}$ over $\mathrm{Z}(Q,\mathrm{R}^k)$.

We write $b_i(d,k,k',s)$ for the maximum of $b_i(\mathcal{P},Z)$ over all $\mathcal{P}$ and Q, with $\deg(P)\le d$ for all $P\in\mathcal{P}\cup\{Q\}$, $\#(\mathcal{P})=s$ and such that the algebraic set $Z=\mathrm{Z}(Q,\mathrm{R}^k)$ has dimension k'.

The following proposition is proved in [5].

PROPOSITION 2.12.

$$b_0(d,k,k',s)\le \sum_{1\le j\le k'} \binom{s}{j} 4^j d(2d-1)^{k-1}.$$

3. Computing the Euler-Poincaré query

An algorithm for computing the Euler-Poincaré characteristic of an algebraic set is described in [1]. We recall below the input, output and the complexity of this algorithm.

Algorithm 3.1. Euler-Poincaré Characteristic of an Algebraic Set.
Input: a polynomial $Q \in \mathrm{D}[X_1, \ldots, X_k]$, where D is an ordered domain.
Output: the Euler-Poincaré characteristic $\chi(\mathrm{Z}(Q, \mathrm{R}^k))$.

Complexity. The complexity of the algorithm is $d^{O(k)}$. When $\mathrm{D} = \mathbb{Z}$ and the bitsizes of the coefficients of Q are bounded by τ, the bitsizes of the intermediate computations and the output are bounded by $\tau d^{O(k)}$ [1].

We now outline an algorithm for computing Euler-Poincaré-queries which uses Algorithm 3.1 described above for computing the Euler-Poincaré characteristic of certain algebraic sets.

Algorithm 3.2. Euler-Poincaré-query.
Input: a polynomial $Q \in \mathrm{D}[X_1, \ldots, X_k]$, with $Z = \mathrm{Z}(Q, \mathrm{R}^k)$, a polynomial $P \in \mathrm{D}[X_1, \ldots, X_k]$.
Output: the Euler-Poincaré-query

$$\mathrm{EQ}(P, Z) = \chi(P > 0, Z) - \chi(P < 0, Z).$$

1. Introduce a new variable X_{k+1}, and let

$$Q_+ = Q^2 + (P - X_{k+1}^2)^2,$$
$$Q_- = Q^2 + (P + X_{k+1}^2)^2.$$

   Using Algorithm 3.1 (Euler-Poincaré Characteristic of an Algebraic Set), compute $\chi(\mathrm{Z}(Q_+, \mathrm{R}^{k+1}))$ and $\chi(\mathrm{Z}(Q_-, \mathrm{R}^{k+1}))$.
2. Output

$$\frac{1}{2}(\chi(\mathrm{Z}(Q_+, \mathrm{R}^{k+1})) - \chi(\mathrm{Z}(Q_-, \mathrm{R}^{k+1}))).$$

Proof of correctness: The algebraic set $\mathrm{Z}(Q_+, \mathrm{R}^{k+1})$ is semi-algebraically homeomorphic to the disjoint union of two copies of the semi-algebraic set defined by $(P > 0) \wedge (Q = 0)$, and the algebraic set defined by $(P = 0) \wedge (Q = 0)$. Hence, using Proposition 2.6, we have that

$$2\chi(P > 0, Z) = \chi(\mathrm{Z}(Q_+, \mathrm{R}^{k+1})) - \chi(\mathrm{Z}(Q^2 + P^2, \mathrm{R}^k)).$$

Similarly, we have that

$$2\chi(P<0,Z)=\chi(\mathrm{Z}(Q_-,\mathrm{R}^{k+1}))-\chi(\mathrm{Z}(Q^2+P^2,\mathrm{R}^k)).$$

COMPLEXITY ANALYSIS: The complexity of the algorithm is $d^{O(k)}$ using the complexity analysis of Algorithm 3.1.

When $\mathrm{D}=\mathbb{Z}$ and the bitsizes of the coefficients of P are bounded by τ, the bitsizes of the intermediate computations and the output are bounded by $\tau d^{O(k)}$.

4. Computing the Euler-Poincaré Characteristic of Sign Conditions

Our next aim is to give a method for determining the Euler-Poincaré characteristic of the realization of sign conditions realized by a finite set $\mathcal{P}\subset \mathrm{R}[X_1,\ldots,X_k]$ on an algebraic set $Z=\mathrm{Z}(Q,\mathrm{R}^k)$, with $Q\in\mathrm{R}[X_1,\ldots,X_k]$.

We compute the Euler-Poincaré characteristic of the non-empty realizations of sign conditions on $\mathcal{P}$ on the real variety Z using Euler-Poincaré-queries (defined in Section 1) as the basic building block. This should be compared with the sign determination algorithms in [7, 19], which compute the cardinalities of the non-empty realizations of sign conditions on a finite set and use Sturm-queries as the basic building block.

Let $S\subset\mathrm{R}^k$ be a locally closed semi-algebraic set.

We order lexicographically $\{0,1,-1\}^{\mathcal{P}}$ and $\{0,1,2\}^{\mathcal{P}}$ with $0\prec 1\prec -1$ in the first case and $0\prec 1\prec 2$ in the second.

For $A=(\alpha_1,\ldots,\alpha_m)$, a list of elements from $\{0,1,2\}^{\mathcal{P}}$, with

$$\alpha_1<_{\mathrm{lex}}\ldots<_{\mathrm{lex}}\alpha_m,$$

we write $\mathcal{P}^A$ for the list $(\mathcal{P}^{\alpha_1},\ldots,\mathcal{P}^{\alpha_m})$, and $\mathrm{EQ}(\mathcal{P}^A,S)$ for the vector

$$(\mathrm{EQ}(\mathcal{P}^{\alpha_1},S),\ldots,\mathrm{EQ}(\mathcal{P}^{\alpha_m},S))^t$$

(Here, for $\alpha\in\{0,1,2\}^{\mathcal{P}}$, $\mathcal{P}^\alpha$ denotes the polynomial $\prod_{P\in\mathcal{P}}P^{\alpha(P)}$ and ^{t} denotes the transpose.)

For $\Sigma=(\sigma_1,\ldots,\sigma_n)$, a list of elements from $\{0,1,-1\}^{\mathcal{P}}$, with

$$\sigma_1<_{\mathrm{lex}}\ldots<_{\mathrm{lex}}\sigma_n,$$

we write $\mathcal{R}(\Sigma,S)$ for the list

$$(\mathcal{R}(\sigma_1,S),\ldots,\mathcal{R}(\sigma_n,S))$$

and $\chi(\Sigma, S)$ for the vector

$$(\chi(\sigma_1, S), \ldots, \chi(\sigma_n, S))^t.$$

The matrix of signs of $\mathcal{P}^A$ on Σ, is the $m \times n$ matrix $M(\mathcal{P}^A, \Sigma)$, whose i, j-th entry is $\mathrm{sign}(\mathcal{P}^{\alpha_i}, \sigma_j)$.

We prove the following generalization of the main ingredient of the sign determination algorithms in [7, 19].

Proposition 4.1. *If* $\cup_{\sigma \in \Sigma} \mathcal{R}(\sigma, S) = S$, *(i.e.* $\{\sigma \mid \mathcal{R}(\sigma, S) \neq \emptyset\} \subset \Sigma$*) then*

$$M(\mathcal{P}^A, \Sigma) \cdot \chi(\Sigma, S) = \mathrm{EQ}(\mathcal{P}^A, S). \tag{4.2}$$

Proof. The proof is by induction on the number s of polynomials in $\mathcal{P}$. The statement when $s = 1$ follows from Proposition 2.7, since the Euler-Poincaré characteristic of an empty sign condition is zero.

Suppose the statement holds for $\mathcal{P}' = P_1, \ldots, P_{s-1}$ and consider $\mathcal{P} = P_1, \ldots, P_s$. Define

$$\begin{aligned} \Sigma_0 &= \{\sigma \in \Sigma \mid \sigma(P_s) = 0\}, \\ \Sigma_1 &= \{\sigma \in \Sigma \mid \sigma(P_s) = 1\}, \\ \Sigma_{-1} &= \{\sigma \in \Sigma \mid \sigma(P_s) = -1\}, \end{aligned}$$

and

$$\begin{aligned} S_0 &= \bigcup_{\sigma \in \Sigma_0} \mathcal{R}(\sigma, S), \\ S_1 &= \bigcup_{\sigma \in \Sigma_1} \mathcal{R}(\sigma, S), \\ S_{-1} &= \bigcup_{\sigma \in \Sigma_{-1}} \mathcal{R}(\sigma, S). \end{aligned}$$

Note that S_0, S_{-1}, and S_1 are all locally closed whenever S is locally closed. Let $\alpha \in \{0,1,2\}^{\mathcal{P}}$ and $\alpha' \in \{0,1,2\}^{\mathcal{P}'}$ defined by $\alpha'(P_j) = \alpha(P_j)$, $1 \leq j \leq s-1$. Using the additive property of Euler-Poincaré characteristic (Proposition 2.6),

$$\begin{aligned} \chi(\mathcal{P}^\alpha = 0, S) &= \chi(\mathcal{P}^\alpha = 0, S_0) + \chi(\mathcal{P}^\alpha = 0, S_1) + \chi(\mathcal{P}^\alpha = 0, S_{-1}), \\ \chi(\mathcal{P}^\alpha > 0, S) &= \chi(\mathcal{P}^\alpha > 0, S_0) + \chi(\mathcal{P}^\alpha > 0, S_1) + \chi(\mathcal{P}^\alpha > 0, S_{-1}), \\ \chi(\mathcal{P}^\alpha < 0, S) &= \chi(\mathcal{P}^\alpha < 0, S_0) + \chi(\mathcal{P}^\alpha < 0, S_1) + \chi(\mathcal{P}^\alpha < 0, S_{-1}). \end{aligned}$$

If $\alpha(P_s) = 0$,

$$\mathrm{EQ}(\mathcal{P}^{\alpha}, S) = \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_0) + \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_1) + \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_{-1}).$$

If $\alpha(P_s) = 1$,

$$\mathrm{EQ}(\mathcal{P}^{\alpha}, S) = \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_1) - \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_{-1}).$$

If $\alpha(P_s) = 2$,

$$\mathrm{EQ}(\mathcal{P}^{\alpha}, S) = \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_1) + \mathrm{EQ}(\mathcal{P}'^{\alpha'}, S_{-1}).$$

The claim follows from the induction hypothesis applied to S_0, S_1 and S_{-1}, the definition of $M(\mathcal{P}^A, \Sigma)$ and the additive property of Euler-Poincaré characteristic (Proposition 2.6), which implies, for every $\sigma \in \Sigma$,

$$\chi(\sigma, S) = \chi(\sigma, S_0) + \chi(\sigma, S_1) + \chi(\sigma, S_{-1}).$$

□

Let $Q \in \mathrm{R}[X_1, \ldots, X_k]$, $Z = \mathrm{Z}(Q, \mathrm{R}^k)$. We consider a list $A(Z)$ of elements in $\{0, 1, 2\}^{\mathcal{P}}$ adapted to sign determination for $\mathcal{P}$ on Z, i.e. such that the matrix of signs of $\mathcal{P}^A$ over $\mathrm{Sign}(\mathcal{P}, Z)$ is invertible. If $\mathcal{P} = P_1, \ldots, P_s$, let $\mathcal{P}_i = P_1, \ldots, P_i$, for $0 \leq i \leq s$.

We will now describe a method for determining inductively a list $A_i(Z)$ of elements in $\{0, 1, 2\}^{\mathcal{P}_i}$ adapted to sign determination for $\mathcal{P}_i$ on Z from $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)$.

Choose i, $1 \leq i \leq s$, and consider P_i. Let $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$, (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$) be the subset of $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)$ of sign conditions which are partitioned into at least two (respectively three) distinct subsets by sign conditions on P_i.

Let

$$Z_2 = \bigcup_{\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2} \mathcal{R}(\sigma, Z), \tag{4.3}$$

$$Z_3 = \bigcup_{\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3} \mathcal{R}(\sigma, Z). \tag{4.4}$$

Note that,

$$\mathrm{Sign}(\mathcal{P}_{i-1}, Z_2) = \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2,$$

$$\mathrm{Sign}(\mathcal{P}_{i-1}, Z_3) = \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3.$$

Let

$$\begin{aligned} r_{i-1} &= \#(\mathrm{Sign}(\mathcal{P}_{i-1}, Z)), \\ r_{i-1,1} &= \#(\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2), \\ r_{i-1,2} &= \#(\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3), \\ r_i &= \#(\mathrm{Sign}(\mathcal{P}_i, Z)). \end{aligned}$$

Then $r_i = r_{i-1} + r_{i-1,1} + r_{i-1,2}$.

Consider the matrix $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z_2))$ and extract from it the first $r_{i-1,1}$ linearly independent rows defining a list $A_{i-1}(Z_2)$ adapted to sign determination on Z_2.. Note, that the matrix $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z_2))$ consists of $r_{i-1,1}$ columns of the matrix $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z))$, which is of full rank by the induction hypothesis. Thus, the rank of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z_2))$ is $r_{i-1,1}$.

Similarly, consider the matrix $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z_3))$ and extract from it the first $r_{i-1,2}$ linearly independent rows defining a list $A_{i-1}(Z_3)$ adapted to sign determination on Z_3.

Define

$$A_i(Z) = (A_{i-1}(Z) \times 0, A_{i-1}(Z_2) \times 1, A_{i-1}(Z_3) \times 2).$$

One says that $\tau \in \mathrm{Sign}(\mathcal{P}_i, Z)$ extends $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)$ if $\sigma(P) = \tau(P), P \in \mathcal{P}_i$.

PROPOSITION 4.5. *The list $A_i(Z)$ is adapted to sign determination for $\mathcal{P}_i$ on Z.*

PROOF. The proof is by induction on i. The claim is obviously true for $i = 1$.

If $\mathcal{P} \neq \emptyset$, we want to prove that

$$M(\mathcal{P}_i^{A(\mathcal{P}_i, Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$$

is invertible. Denoting by C_τ its column indexed by τ, consider a zero linear combination of its columns:

$$\sum_{\tau \in \mathrm{Sign}(\mathcal{P}_i, Z)} \lambda_\tau C_\tau = 0.$$

We want to prove that all λ_τ are zero. If $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$, we denote by $\sigma_1 <_{\mathrm{lex}} \sigma_2 <_{\mathrm{lex}} \sigma_3$ the sign conditions of $\mathrm{Sign}(\mathcal{P}_i, Z)$ extending σ. Similarly, if $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2 \setminus \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$, we denote by $\sigma_1 <_{\mathrm{lex}} \sigma_2$ the sign conditions of $\mathrm{Sign}(\mathcal{P}_i, Z)$ extending σ. Finally if $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z) \setminus \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$, we denote by σ_1 the sign condition of $\mathrm{Sign}(\mathcal{P}_i, Z)$ extending σ.

Since $M(\mathcal{P}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z))$ is invertible by induction hypothesis, $\lambda_{\sigma_1} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z) \setminus \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$, $\lambda_{\sigma_1} + \lambda_{\sigma_2} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2 \setminus \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$, and $\lambda_{\sigma_1} + \lambda_{\sigma_2} + \lambda_{\sigma_3} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$.

Now using the fact that $M(\mathcal{P}^{A(\mathcal{P}_{i-1}, Z_2)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z_2))$ is invertible, $\sigma_1(P)\lambda_{\sigma_1} - \sigma_2(P)\lambda_{\sigma_2} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2 \setminus \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$, and $\lambda_{\sigma_2} - \lambda_{\sigma_3} = 0$ for every $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$. Thus, $\lambda_{\sigma_1} = \lambda_{\sigma_2} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}, Z)_2 \setminus \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$.

Finally, using the fact that $M(\mathcal{P}^{A(\mathcal{P}, Z_3)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z_3))$ is invertible, $\lambda_{\sigma_2} + \lambda_{\sigma_3} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$. Thus $\lambda_{\sigma_1} = \lambda_{\sigma_2} = \lambda_{\sigma_3} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$. $\square$

Remark 4.6. The list $A_i(Z) \subset \{0, 1, 2\}^{\mathcal{P}_i}$ adapted to sign determination constructed above depends only on the list of non-empty sign conditions $\mathrm{Sign}(\mathcal{P}, Z)$, since the list $A_i(Z) \subset \{0, 1, 2\}^{\mathcal{P}_i}$ is constructed inductively from $A_{i-1}(Z)$ and $\mathrm{Sign}(\mathcal{P}_i, Z)$.

We are ready to describe an algorithm for computing the Euler-Poincaré characteristic of the realizations of sign conditions. We use the following algorithm (see [3, 6]) as a basic building block.

Algorithm 4.7. Sampling on an Algebraic Set.

Input: a polynomial $Q \in \mathrm{D}[X_1, \ldots, X_k]$ of degree at most d, with $\mathrm{Z}(Q, \mathrm{R}^k)$ of real dimension k',

a set of s polynomials , $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathrm{D}[X_1, \ldots, X_k]$, each of degree at most d.

Output: the set $\mathrm{Sign}(\mathcal{P}, Z) \subset \{0, 1, -1\}^{\mathcal{P}}$ of all realizable sign conditions for $\mathcal{P}$ over $Z = \mathrm{Z}(Q, \mathrm{R}^k)$.

Complexity. The complexity is $s^{k'+1} d^{O(k)}$. If $\mathrm{D} = \mathbb{Z}$, and the bitsizes of the coefficients of the polynomials are bounded by τ, then the bitsizes of the integers appearing in the intermediate computations and the output are bounded by $\tau d^{O(k)}$.

Algorithm 4.8. Euler-Poincaré Characteristic of Sign Conditions.

Input: an algebraic set $Z = \mathrm{Z}(Q, \mathrm{R}^k) \subset \mathrm{R}^k$ and a finite list $\mathcal{P} = P_1, \ldots, P_s$ of polynomials in $\mathrm{R}[X_1, \ldots, X_k]$.

Output: the list $\chi(\mathcal{P}, Z)$.

1. Compute $\mathrm{Sign}(\mathcal{P}, Z)$ using Algorithm 4.7 (Sampling on an Algebraic Set).
2. Determine for every $1 \le i \le s$, a list $A_i(Z)$ adapted to sign determination for $\mathcal{P}_i$ on Z from $\mathrm{Sign}(\mathcal{P}_i, Z)$ using Proposition 4.5.
3. Define $A = A_s(Z)$, $M = M(\mathcal{P}^A, \mathrm{Sign}(\mathcal{P}, Z))$.
4. Compute $\mathrm{EQ}(\mathcal{P}^A, Z)$ using repeatedly Algorithm 3.2 (Euler-Poincaré-query).
5. Compute $\chi(\mathcal{P}, Z) = M^{-1}\mathrm{EQ}(\mathcal{P}^A, Z)$ using the fact that M is invertible.

Proof of correctness: Immediate from Proposition 4.1.

In order to study the complexity of Algorithm 4.8 we need the following proposition.

Proposition 4.9. *Let $Z = \mathrm{Z}(Q, \mathrm{R}^k) \subset \mathrm{R}^k$ and $r = \#(\mathrm{Sign}(\mathcal{P}, Z))$. Consider $A_s(Z) \subset \{0, 1, 2\}^{\mathcal{P}}$ computed by Algorithm 4.8. For every $\alpha \in A_s(Z)$, the number $\#(\{P \in \mathcal{P} \mid \alpha(P) \neq 0\})$ is at most $\log_2(r)$.*

We need the following definition. Let α and β be elements of $\{0, 1, 2\}^{\mathcal{P}}$. We say that β precedes α if for every $P \in \mathcal{P}$, $\beta(P) \neq 0$ implies $\beta(P) = \alpha(P)$. Note that if β precedes α, then $\beta <_{\mathrm{lex}} \alpha$.

Proof. (Proposition 4.9) Let α be such that $\#(\{P \in \mathcal{P} \mid \alpha(P) \neq 0\}) = k$. Since the number of elements β of $\{0, 1, 2\}^{\mathcal{P}}$ preceding α is 2^k, and the total number of polynomials in A_s is at most r, we have $2^k \le r$ and $k \le \log_2(r)$. So, the proposition follows immediately from the next lemma. $\square$

Lemma 4.10. *If β precedes α and $\alpha \in A_s(Z)$ then $\beta \in A_s(Z)$.*

Proof. We prove by induction on i that if $\beta \notin A_i(Z)$ then $\alpha \notin A_i(Z)$. The claim is obvious for $i = 1$. If $\alpha \in \{0, 1, 2\}^{\mathcal{P}_i}$ we denote by α' the element of $\{0, 1, 2\}^{\mathcal{P}_{i-1}}$ such that $\alpha'(P_j) = \alpha(P_j)$, $j < i$. Note that, by definition of $A_i(Z)$, if $\alpha' \notin A_{i-1}(Z)$, $\alpha \notin A_i(Z)$.

Suppose that β precedes α and that $\beta \notin A_i(Z)$. There are several cases to consider:

If $\alpha(P_i) = 0$, then $\beta(P_i) = 0$ and $\beta' \notin A_{i-1}(Z)$ by definition of A_i. By the induction hypothesis, $\alpha' \notin A_{i-1}(Z)$ and $\alpha = \alpha' \times 0 \notin A_i(Z)$ by the definition of $A_i(Z)$.

If $\alpha(P_i) = 1$ (respectively 2), and $\beta(P_i) = 0$, thus $\alpha' \notin A_{i-1}(Z)$ by induction hypothesis, and $\alpha \notin A_i(Z)$.

If $\alpha(P_i) = 1$ (respectively 2), and $\beta(P_i) = \alpha(P_i)$, then $\beta' \notin A_{i-1}(Z')$ (respectively $A_{i-1}(Z''))$. Thus, the row of signs of $\mathcal{P}_{i-1}^{\beta'}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$) is a linear combination of rows of signs of $\mathcal{P}_{i-1}^{\lambda}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$), with $\lambda <_{\mathrm{lex}} \beta'$ in the lexicographical order. Denoting by γ the element in $\{0, 1, 2\}^{\mathcal{P}_{i-1}}$ such that $\mathcal{P}_{i-1}^{\beta'}\mathcal{P}_{i-1}^{\gamma} = \mathcal{P}_{i-1}^{\alpha'}$, the row of signs of $\mathcal{P}_{i-1}^{\alpha'}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$) is a linear combination of rows of signs of $\mathcal{P}_{i-1}^{\lambda}\mathcal{P}_{i-1}^{\gamma}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$). Defining λ' by $\lambda'(P_j) = \lambda(P_j) + \gamma(P_j)$ modulo 2, the row of signs of $\mathcal{P}_{i-1}^{\lambda}\mathcal{P}_{i-1}^{\gamma}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$) coincides with the row of signs of $\mathcal{P}_{i-1}^{\lambda'}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$). Since it is clear that $\lambda' <_{\mathrm{lex}} \alpha'$ in the lexicographical order, $\alpha' \notin A_{i-1}(Z')$ (respectively $A_{i-1}(Z''))$. Thus $\alpha \notin A_i(Z)$.

□

COMPLEXITY ANALYSIS: Let k' be the dimension of Z, d a bound on the degree of Q and the elements of $\mathcal{P}$ and $s = \#(\mathcal{P}))$. By Proposition 2.12,

$$\#(\mathrm{Sign}(\mathcal{P}, Z)) \le \sum_{0 \le j \le k'} \binom{s}{j} 4^j d(2d-1)^{k-1} = s^{k'} O(d)^k.$$

The number of calls to Algorithm 3.2 (Euler-Poincaré-query) is equal to $\#(\mathrm{Sign}\,(\mathcal{P}, Z))$. The calls to Algorithm 3.2 (Euler-Poincaré-query) are done for polynomials which are products of at most

$$\log_2(\#(\mathrm{Sign}(\mathcal{P}, Z))) = k' \log_2(s) + k(\log_2(d) + O(1)$$

polynomials of the form P or P^2, $P \in \mathcal{P}$ by Proposition 4.9, hence of degree $(k' \log_2(s) + k(\log_2(d) + O(1))d$. Using the complexity analysis of Algorithm 4.7 (Sampling on an Algebraic Set) and the complexity analysis of Algorithm 3.2 (Euler-Poincaré-query), the number of arithmetic operations is

$$s^{k'+1} O(d)^k + s^{k'}((k' \log_2(s) + k \log_2(d))d)^{O(k)}.$$

The algorithm also involves the inversion of matrices size $s^{k'} O(d)^k$ whose entries are $0, 1$ or -1.

If $\mathrm{D} = \mathbb{Z}$, and the bitsizes of the coefficients of the polynomials are bounded by τ, then the bitsizes of the integers appearing in the intermediate computations and the output are bounded by $\tau((k' \log_2(s) + k \log_2(d))d)^{O(k)}$.

Acknowledgements

Saugata Basu was supported in part by an NSF Career Award 0133597 and a Sloan Foundation Fellowship. Richard Pollack was supported in part by NSF grant CCR-0098246.

References

[1] S. Basu, *On Bounding the Betti Numbers and Computing the Euler Characteristics of Semi-algebraic Sets*, Discrete and Computational Geometry, 22 1–18 (1999).

[2] S. Basu, R. Pollack, M.-F. Roy, *On the Combinatorial and Algebraic Complexity of Quantifier Elimination*, Journal of the ACM , 43 1002–1045, (1996).

[3] S. Basu, R. Pollack, M.-F. Roy, *On Computing a Set of Points meeting every Semi-algebraically Connected Component of a Family of Polynomials on a Variety*, Journal of Complexity, March 1997, Vol 13, Number 1, 28–37.

[4] S. Basu, R. Pollack, M.-F. Roy, *Computing Roadmaps of Semi-algebraic Sets on a Variety*, Journal of the AMS, vol 3, 1 55–82 (1999).

[5] S. Basu, R. Pollack, M.-F. Roy, *On the Betti numbers of sign conditions*, Proceedings of the AMS (to appear).

[6] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in Real Algebraic Geometry*, Springer-Verlag, 2003.

[7] M. Ben-Or, D. Kozen , J. Reif, *The complexity of elementary algebra and geometry*, J. of Computer and Systems Sciences, 18:251–264, (1986).

[8] J. Bochnak, M. Coste, M.-F. Roy, *Géométrie algébrique réelle,* Springer-Verlag (1987). *Real algebraic geometry*, Springer-Verlag (1998).

[9] A. Borel, J.C. Moore, *Homology theory for locally compact spaces*, Mich. Math. J., 7:137– 159, (1960).

[10] J. Canny, *Computing road maps in general semi-algebraic sets*, The Computer Journal, 36: 504–514, (1993).

[11] D. Cox, J. Little, D. O'Shea, *Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, New York (1997).

[12] L. Gournay, J. J. Risler, *Construction of roadmaps of semi-algebraic sets*, Appl. Algebra Eng. Commun. Comput. 4, No.4, 239-252 (1993).

[13] D. Grigor'ev, N. Vorobjov, *Counting connected components of a semi-algebraic set in subexponential time*, Comput. Complexity 2, No.2, 133-186 (1992).

[14] D. Halperin Arrangements, *Handbook of Discrete and Computational Geometry,* J. O'Rourke, J.E. Goodman editors, CRC Press, 389 412, 1997.

[15] R. M. Hardt, *Semi-algebraic Local Triviality in Semi-algebraic Mappings*, Am. J. Math. 102, 291-302 (1980).

[16] J. Heintz, M.-F. Roy, P. Solernò, *Description of the Connected Components of a Semialgebraic Set in Single Exponential Time*, Discrete and Computational Geometry, 11, 121-140 (1994).

[17] P. Pedersen, M.-F. Roy, A. Szpirglas, *Counting real zeroes in the multivariate case*, Computational algebraic geometry, Eyssette et Galligo ed. Progress in Mathematics 109, 203-224, Birkhauser (1993).

[18] J. Renegar. *On the computational complexity and geometry of the first order theory of the reals*, Journal of Symbolic Computation, 13: 255–352 (1992).

[19] M.-F. Roy, A. Szpirglas *Complexity of computation on real algebraic numbers*, Journal of Symbolic Computation 10, No.1, 39-51 (1990).

Manuscript received April 5, 2004.

Saugata Basu
School of Mathematics,
Georgia Institute of Technology,
Atlanta, GA 30332, U.S.A.
saugata@math.gatech.edu

Richard Pollack
Courant Institute of Mathematical Sciences,
New York University,
New York, NY 10012, U.S.A.,
pollack@cims.nyu.edu

Marie-Françoise Roy
Université de Rennes,
Campus de Beaulieu 35042
Rennes cedex FRANCE,
marie-francoise.roy@math.
univ-rennes1.fr