On Bounding the Betti Numbers and Computing the Euler Characteristic of Semi-algebraic Sets

Saugata Basu*

September 10, 1997

Abstract

In this paper we give a new bound on the sum of the Betti numbers of closed semi-algebraic sets. This extends a well-known bound due to Oleinik and Petrovsky [28], Thom [35] and Milnor [27]. In separate papers they proved that the sum of the Betti numbers of a semi-algebraic set $S \subset R^k$, defined by $P_1 \geq 0, \ldots, P_s \geq 0, deg(P_i) \leq d, 1 \leq i \leq s$, is bounded by $(O(sd))^k$. Given a closed semi-algebraic set $S \subset R^k$ defined as the intersection of a real variety, $Q = 0, deg(Q) \leq d$, whose real dimension is k', with a set defined by a quantifier-free Boolean formula with no negations with atoms of the form, $P_i = 0, P_i \geq 0, P_i \leq 0, deg(P_i) \leq d, 1 \leq i \leq s$, we prove that the sum of the Betti numbers of S is bounded by $s^{k'}(O(d))^k$. Additionally, when S is defined by $Q = 0, P_1 > 0, \ldots, P_s > 0$, we have a slightly tighter bound of $\binom{s}{k'}(O(d))^k$. This result generalizes the Oleinik-Petrovsky-Thom-Milnor bound in two directions. Firstly, our bound applies to arbitrary unions of basic closed semi-algebraic sets, not just for basic semi-algebraic sets. Secondly, the combinatorial part (the part depending on s) in our bound, depends on the dimension of the variety rather than that of the ambient space. It also generalizes a result in [5] where a similar bound is proven for the number of connected components.

We also investigate the case where the algebraic complexity of the input polynomials is measured in terms of the number of monomials present, the degrees being unbounded. Given a closed semi-algebraic set $S \subset R^k$ defined as the intersection of a real variety,

*Currently at the Mathematical Sciences Department, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598. This work was done while the author was a graduate student at the Courant Institute of Mathematical Sciences, New York University, New York, NY 10012, U.S.A., and was supported in part by NSF grants CCR-9402640 and CCR-9424398. A preliminary version of this paper appeared in the Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, 408-417, 1996.

$Q = 0, deg(Q) \leq d$, whose real dimension is k', with a set defined by a quantifier-free Boolean formula with no negations with atoms of the form, $P_i = 0, P_i \geq 0, P_i \leq 0$, such that the total number of monomials occurring in the polynomials in $\mathcal{P} \cup \{Q\}$ is m, we prove that the sum of the Betti numbers of S is bounded by $s^{k'} 2^{O(k^2 m^4)}$. The separation of these bounds into two parts, namely a combinatorial part depending on the number of polynomials involved and an algebraic part depending on the degrees of the polynomial is novel and is not immediately obtainable using the basic technique due to Oleinik, Petrovsky, Thom and Milnor.

In the second part of the paper we use the tools developed for the above results, as well as some additional techniques, to give the first single exponential time algorithm for computing the Euler characteristic of arbitrary semi-algebraic sets.

1 Introduction

Let $\mathcal{P} = \{P_1, \ldots, P_k\} \subset R[X_1, \ldots, X_k]$, be a family of polynomials whose degrees are bounded by d, and let S be a closed semi-algebraic set defined by a quantifier-free Boolean formula, without negations, whose atoms are of the form $P_i \sigma 0, \sigma \in \{\geq, \leq, =\}, 1 \leq i \leq s$.

Thus S is defined as a disjunction of weak sign conditions on the family $\mathcal{P}$, where a weak sign condition is a conjunction of the form,

$$P_1 \sigma_1 0, \ldots, P_s \sigma_s 0, \sigma_i \in \{\geq, \leq, =\}, 1 \leq i \leq s.$$

The Betti numbers, $\beta_i(S)$, which are the ranks of the singular homology groups of S, are a measure of the topological complexity of S and can be bounded in terms of s, d and k. Since by Collin's algorithm [9] for cylindrical algebraic decomposition, there exists a cellular decomposition of S into $(sd)^{2^{O(k)}}$ cells, the same bound applies to $\beta_i(S)$. In the case where the set S is a basic closed semi-algebraic set defined by, $P_1 \geq 0, \ldots, P_s \geq 0$, with $deg(P_i) \leq d$, there is a tighter bound of $(O(sd))^k$ on the sum of the Betti numbers of S. This was proved in separate papers by Oleinik and Petrovsky [28], Thom [35] and Milnor [27]. (Note that this includes the case when S is the real zeros of a set of polynomials.) This bound plays an important role in algorithmic real algebraic geometry [22], and has been used recently in proving lower bounds in the algebraic computation tree model (see [36], [29]).

A difficulty in extending this bound to an arbitrary semi-algebraic set defined by the polynomials $\mathcal{P}$, lies in the fact that the Betti numbers of the union of two disjoint sets, can be arbitrarily greater than the sum of the individual Betti numbers of the two sets (see [36] for an easy example).

We extend the same bound to arbitrary unions of basic closed semi-algebraic sets. More precisely, we prove the following theorem:

Theorem 1 *Let $S \subset R^k$, be the intersection of a closed semi-algebraic set defined by a quantifier-free Boolean formula without negations involving a family, $\mathcal{P} = \{P_1, \ldots, P_s\}$, of s polynomials whose atoms are of the form $P_i \sigma 0, \sigma \in \{\geq, \leq, =\}$ with the zero set, $Z(Q)$, of a polynomial Q. Let the geometric dimension of $Z(Q)$ be k', and the degrees of the polynomials in $\mathcal{P} \cup \{Q\}$ be bounded by d. Then, the sum of the Betti numbers of S is bounded by $s^{k'}(O(d))^k$.*

Secondly, if S is defined by $Q = 0, P_1 > 0, \ldots, P_s > 0$, we have a slightly tighter bound of $\binom{s}{k'}(O(d))^k = (\frac{s}{k'})^{k'}(O(d))^k$.

If Q is taken as the zero polynomial, then $Z(Q) = R^k$ and $k' = k$, and we get the Oleinik-Petrovsky-Thom-Milnor bound extended to arbitrary closed semi-algebraic sets as a special case. Note that a bound of $\binom{s}{k'}(O(d))^k$ on the zero-th Betti number for arbitrary semi-algebraic sets (which is just the number of connected components) was known before [5] and our bound is a generalization of this result to the higher Betti numbers in the case of closed semi-algebraic sets.

Note also that a lower bound of $(\frac{sd}{k'})^{k'}$ on the zero-th Betti number is easily obtained by considering the set of non-zeros of s polynomials, each of them a product of d linear polynomials, restricted to a k' dimensional linear subspace.

The dependence on k' instead of k in the combinatorial part (the part depending on s) of the bound in theorem 1 becomes important when we consider low dimensional semi-algebraic sets embedded in a higher dimensional space, and this is sometimes important in applications. For example, the bound on the number of connected components in [5] plays a crucial role in the proof of the main result in [13], where the variety is the real Grassmannian $G_{m,n}$ (the space of m dimensional subspaces of R^n), embedded as a $m(n-m)$ dimensional variety in R^{n^2}.

Remark 1: We note that a bound of $(O(sd))^{2k}$ on the sum of the Betti numbers can be deduced from Theorem 1 in [36] or from Theorem 1.10 in [29].

Remark 2: Even though we state our results for closed semi-algebraic sets over the reals the same bounds hold over any real closed fields through the application of well-known transfer principles. We refer the reader to the article by Knebusch [24] for the intricacies of semi-algebraic topology over general real closed fields.

In order to achieve the bound in theorem 1 we prove that an arbitrary closed semi-algebraic set has the same homology groups as a compact semi-algebraic set defined by polynomials in general position. This result generalizes a similar result in Canny [7] where it was proved for semi-algebraic sets defined by a single sign condition, and this intermediate result might be of independent interest.

Next we consider the problem of computing the Euler characteristic $\chi(S)$, of a closed semi-algebraic set S. The Euler characteristic, which is the alternating sum of the Betti numbers of S, is an important topological invariant and thus can be used as a test to rule out topological equivalence. Also, computing the Euler characteristic of semi-algebraic sets occur as an important sub-problem in some recent work due to Gabrielov [11] on computing multiplicities of the zeros of polynomial functions along the trajectories of a polynomial vector field.

We prove the following theorem.

Theorem 2 *Let $S \subset R^k$ be a real closed semi-algebraic set, defined by a quantifier-free Boolean formula without negation with atoms of the form, $P_i \sigma 0, \sigma \in \{\geq, \leq, =\}, 1 \leq i \leq s$, where $\mathcal{P} = \{P_1, \ldots, P_s\} \subset Z[X_1, \ldots, X_k]$, is a family of s polynomials whose degrees are bounded by d, and the bit lengths of the coefficients of P_i are bounded by L. Then, there exists an algorithm for computing $\chi(S)$ which performs at most $(ksd)^{O(k)}L^{O(1)}$ bit operations.*

We remark that computing stratifications of semi-algebraic sets, and thus computing their homology groups, in single exponential time, is a central open problem of computational real algebraic geometry (see the survey by Chazelle [8]). Single exponential algorithms for determining certain other (weaker) topological properties of semi-algebraic sets are known. For example, it is possible to compute the number of connected components [7, 18, 15, 20], semi-algebraic description of the connected components [21], as well as to decide whether two points are in the same connected component of a semi-algebraic set [7, 18, 20], in single exponential time.

Collin's algorithm for computing a cylindrical algebraic decomposition [9], gives sufficient topological information for computing the Euler characteristic, and in fact the homology groups of a given semi-algebraic set [34]. However, this algorithm has double exponential complexity $(sd)^{2^{O(k)}}$. Previously, this was the best algorithm for computing the Euler characteristic of general semi-algebraic sets. A single exponential algorithm for computing the Euler characteristic of a smooth algebraic hypersurface is mentioned in [31].

The rest of the chapter is organized as follows.

In section 2 we show how to perturb the polynomials to bring them into general position without changing the homology groups of the given semi-algebraic set.

In section 3 we prove our bound on the Betti numbers of closed semi-algebraic sets.

In section 4 we prove a bound on the sum of the Betti numbers of a closed semi-algebraic set, in which the algebraic part of the complexity depends only on the number of monomials appearing in the polynomials and is independent of the degree.

In section 5 we describe our algorithm for computing the Euler characteristic. In subsection 5.2 we give an algorithm for computing the Euler characteristic of a basic semi-algebraic set, and in subsection 5.3 we give an algorithm for computing the Euler characteristic of an arbitrary union of such sets.

2 Going to general position

We say that a family of polynomials $\mathcal{P}$ in k variables is in *general position* if no $k+1$ of them have a common real zero. In this section we show that given a semi-algebraic set, S, defined by a family, $\mathcal{P}$, of s polynomials with degrees bounded by d, we can define a new compact semi-algebraic set S', which has the same homology groups as S, but which is defined by a family, $\mathcal{P}'$, of polynomials in general position. Moreover, $|\mathcal{P}'| \leq 4s+1$, and the degrees of the polynomials in $\mathcal{P}'$ are bounded by d', where d' is the least even number greater than d. Similar results appear in [7], where they are proved for semi-algebraic sets defined by one single sign condition. Our proof techniques are similar to those used in [7], but our results apply to arbitrary closed semi-algebraic sets.

We first recall few facts from algebraic topology. Given a semi-algebraic set, $S \subset R^k$, we denote by $H_*(S)$ the graded singular homology group of S.

The following theorem appears in [33] (theorem 4.1.7).

Theorem 3 *The singular homology functor commutes with direct limits.*

We will also need the following fundamental property of the *Čech* homology groups of a compact space (see [10] page 257).

Theorem 4 *If X is compact and the inverse limit of compact sets X_α then the Čech homology group $H_*(X)$ is the inverse limit of the Čech homology groups $H_*(X_\alpha)$.*

Note that, since compact semi-algebraic sets are triangulable, their singular and *Čech* homologies coincide.

We first ensure that a given semi-algebraic set has the same homology groups as a bounded one.

Lemma 1 *Let S be any closed semi-algebraic set. Let, $S_\Omega = S \cap (X_1^2 + \cdots + X_k^2 \le \Omega)$. Then for sufficiently large Ω, $H_*(S) \cong H_*(S_\Omega)$.*

Proof: Let $S' \subset R^{k+1}$ be the set defined by the same formula as S plus the new inequality, $T(X_1^2 + \cdots + X_k^2) \le 1$. Let π and π_x denote the projections onto the T and the X co-ordinates respectively.

Then, by Hardt's triviality theorem [19], for all sufficiently large Ω, and for all $t \in (0, \frac{1}{\Omega})$, $S' \cap \pi^{-1}(t)$ is homeomorphic to $S' \cap \pi^{-1}(\frac{1}{\Omega})$.

Moreover, each $S' \cap \pi^{-1}(t)$ is compact and $S = \cup_{t>0} \pi_x(S' \cap \pi^{-1}(t))$. It is also clear that the singular chain complex of S is the direct limit of the singular chain complexes of $\pi_x(S' \cap \pi^{-1}(t))$. Now, by theorem 3 $H_*(S)$ is the direct limit of the groups $H_*((S' \cap \pi^{-1}(t)))$.

Hence, $H_*(S) \cong H_*(S' \cap \pi^{-1}(\frac{1}{\Omega})) \cong H_*(S_\Omega)$.

□

Let S be a compact semi-algebraic set defined by the formula,

$$(\vee_{1 \le j \le L} \sigma_j(\mathcal{P})) \wedge (X_1^2 + \cdots + X_k^2 \le \Omega),$$

where each σ_j is an non-empty sign condition for the family $\mathcal{P}$, and Ω is positive and sufficiently large.

For any sign condition σ, and a new variable ϵ we will denote by $\sigma(\mathcal{P}, \epsilon)$ the following formula: For every strict sign in σ we retain the corresponding conjunct in $\sigma(\mathcal{P}, \epsilon)$. For every equality in σ we replace the corresponding conjunct, $P_j = 0$, by the conjunct, $(P_j > -\epsilon) \wedge (P_j < \epsilon)$.

Let S_ϵ denote the semi-algebraic set defined by the formula $\vee_{1 \le j \le L} \sigma_j(\mathcal{P}, \epsilon)$.

We have the following lemma.

Lemma 2 *Let S be compact and S_ϵ be as above. Then, for sufficiently small $\epsilon > 0$, $H_*(S) \cong H_*(S_\epsilon)$.*

Proof: Let S'_ϵ denote the semi-algebraic set defined as S_ϵ with the difference that, for every equality in σ we replace the corresponding conjunct, $P_j = 0$, by the conjunct, $P_j \geq -\epsilon \wedge P_j \leq \epsilon$, and add the constraint $X_1^2 + \cdots + X_k^2 \leq R$ where R is the radius of a ball containing S. It follows that S'_ϵ is compact. Again by Hardt's triviality theorem, for sufficiently small $\epsilon > 0$, and all $0 < \delta < \epsilon$, S'_δ is homeomorphic to S'_ϵ.

Now, $S \subset S_\epsilon \subset S'_\epsilon$.

Also, $S = \cap_{\epsilon > 0} S'_\epsilon$. Hence, by theorem 4 $H_*(S)$ is the inverse limit of the groups $H_*(S'_\epsilon)$, and thus by the previous observation $H_*(S) \cong H_*(S'_\epsilon)$.

Finally, note that $S_\epsilon = \cup_{0<t<\epsilon} S'_t$, and the singular chain complex of S_ϵ is the direct limit of the singular chain complexes of S'_t.

Thus by theorem 3, $H_*(S_\epsilon)$ is the direct limit of the groups $H_*(S'_t)$. But, $H_*(S'_t) \cong H_*(S'_\epsilon)$ for $0 < t < \epsilon$. Thus, we have that $H_*(S_\epsilon) \cong H_*(S'_\epsilon)$ which implies that $H_*(S) \cong H_*(S_\epsilon)$. □

Note that, the set S_ϵ is defined by a disjunction of conjunctions of strict inequalities involving $3s$ polynomials,

$$\cup_{P \in \mathcal{P}} \{P, P + \epsilon, P - \epsilon\},$$

and that there are no equalities in the formula.

We next prove that given a semi-algebraic set defined by a disjunct of conjuncts of the form, $\wedge_j Q_j \; s_j \; 0$ where $s_j \in \{<, >\}$, then it is possible to define a new semi-algebraic set defined by polynomials in general position having the same homology group.

Let S be a semi-algebraic set, defined by the formula, $\vee_{1 \leq j \leq L} \sigma_j(\mathcal{Q}_j)$, where each σ_j is a sign-condition on a subset $\mathcal{Q}_j$ of a family of polynomial $\mathcal{Q}$, and σ_j does not contain equality.

Let $\mathcal{Q} = \{Q_1, \ldots, Q_s\}$, and $deg(Q_i) < d$, $1 \leq i \leq s$.

For $1 \leq i \leq 2s$ let, $H_i = 1 + \sum_{1 \leq j \leq k} i^j X_j^{2d}$.

For, $Q_i \in \mathcal{Q}$, let $Q_i^+ = (1 - \delta) Q_i + \delta H_{2i-1}$, and $Q_i^- = (1 - \delta) Q_i + \delta H_{2i}$, where δ is a new variable. Let $\mathcal{Q}'$ be the family $\cup_i \{Q_i^+, Q_i^-\}$.

Lemma 3 *For sufficiently small $\delta > 0$, the family of polynomials $\mathcal{Q}'$ is in general position.*

Proof: See [4]. □

For a sign condition σ on $\mathcal{Q}$, without any equalities, define $\sigma(\mathcal{Q}, \delta)$ to be the formula obtained as follows:

Every conjunct $Q_i > 0$ is replaced by $Q_i^- \geq \delta$, while every conjunct $Q_i < 0$ is replaced by $Q_i^+ \leq \delta$.

Let S_δ^- be the set defined by, $\vee_{1 \leq j \leq L} \sigma_j(\mathcal{Q}_j, \delta)$.

Lemma 4 *Let S and S_δ^- be as above. Then, for sufficiently small $\delta > 0$, $H_*(S_\delta^-) \cong H_*(S)$.*

Proof: Again by Hardt's triviality theorem, $H_*(S_t^-)$ are isomorphic for all $t \in (0, \delta)$ for sufficiently small δ. Also, $S = \cup_{0<t} S_t^-$, and the singular chain complex of S is the direct limit of the singular chain complexes of S_t^-. Again applying theorem 3 we have that $H_*(S) \cong H_*(S_\delta^-)$, for all sufficiently small $\delta > 0$. $\square$

Combining the previous four lemmas we obtain the following proposition.

Proposition 1 *Let S be any semi-algebraic set defined by a family of s polynomials with degrees bounded by d. Then, there exists a set $S(\Omega, \epsilon, \delta)$ defined by a family of at most $4s+1$ polynomials, in $X_1, \ldots, X_k, \epsilon, \delta, \Omega$ with degrees bounded by $2d$ such that for sufficiently small $\epsilon > 0$, $\frac{1}{\Omega} > 0$, $\delta > 0$, this new family of polynomials is in general position, and $H_*(S(\Omega, \epsilon, \delta)) \cong H_*(S)$. Moreover, the set $S(\Omega, \epsilon, \delta)$ is compact, and defined as a disjunction of conjunctions of weak inequalities.*

In our proofs we will need a slightly stronger notion of general position.

Let Q be a polynomial such that $Z(Q)$ has geometric dimension k'. We say that a family of polynomials $\mathcal{P}$ is in *general position with respect to* Q, if no $k'+1$ of the polynomials in $\mathcal{P}$ have a real zero in common with Q.

Moreover, consider the intersection of a semi-algebraic set defined by a family of polynomials $\mathcal{P}$ with $Z(Q)$. Using the same arguments as in the proof of proposition 1, always carrying along the extra condition $Q = 0$, and replacing the polynomials H_i by different infinitesimals (see [5]) we can replace $S \cap Z(Q)$ by a compact semi-algebraic set contained in $Z(Q)$, having the same homology, but defined by at most $4s+1$ polynomials in general position with respect to Q.

We also remark that if a family of polynomials $\mathcal{P}$ is in general position with respect to a polynomial Q, then for an infinitesimal ϵ the family $\cup_{P \in \mathcal{P}} \{P, P+\epsilon, P-\epsilon\}$ is also in general position with respect to Q as long as we consider zeros that are bounded over R. We use this implicitly in the proofs presented below.

3 Bounding the Betti Numbers

We make use of the following facts from algebraic topology which follows easily from the Mayer-Vietoris sequence (see [33]). Given a semi-algebraic set S we define $r(S) = \sum_i \beta_i(S)$. Let S_1 and S_2 be two compact semi-algebraic sets. Then, from the Mayer-Vietoris sequence,

$$\cdots \to H_{i+1}(S_1 \cup S_2) \to H_i(S_1 \cap S_2) \to H_i(S_1) \oplus H_i(S_2) \to$$

$$H_i(S_1 \cup S_2) \to H_{i-1}(S_1 \cap S_2) \to \cdots,$$

we can deduce the following:

$$r(S_1) + r(S_2) \leq r(S_1 \cup S_2) + r(S_1 \cap S_2), \tag{1}$$

and,

$$r(S_1 \cup S_2) \leq r(S_1) + r(S_2) + r(S_1 \cap S_2). \tag{2}$$

Lemma 5 *Let S be a semi-algebraic set defined by a conjunct $(Q = 0) \wedge (\sigma_1(\mathcal{P}) \vee \cdots \vee \sigma_L(\mathcal{P}))$, where Q is a polynomial, and σ_j, $1 \leq j \leq L$, are distinct sign conditions on a family of polynomials $\mathcal{P}$, such that none of the σ_j contain an equality. Then, $\beta_i(S) = \sum_{1 \leq j \leq L} \beta_i(S_j)$ and $\chi(S) = \sum_{1 \leq j \leq L} \chi(S_j)$, where S_j is the set defined by the conjunct $(Q = 0) \wedge \sigma_j(\mathcal{P})$.*

Proof: This follows immediately from the definition of singular homology groups. The singular chain of S being the direct sum of the singular chains of the S_js. □

3.1 Proof of Theorem 1

Proof: In view of proposition 1 and the remarks following it we can assume without loss of generality that S is a compact set defined by s polynomials in general position with respect to Q.

We next prove two lemmas that will imply the theorem.

Given a polynomial Q and a family of polynomials $\mathcal{P} = \{P_1, \ldots, P_s\}$, we define the *combinatorial level* of the system $(Q, \mathcal{P})$ to be the least integer m such that no $m + 1$ of the polynomials in $\mathcal{P}$ have a common real zero with Q.

For example, the combinatorial level of $(Q, \mathcal{P})$ is bounded by k' if the dimension of $Z(Q)$ is k' and the polynomials in $\mathcal{P}$ are in general position with respect to Q.

Lemma 6 *Let S be a semi-algebraic set, defined by $Q = 0, P_1 > 0, \ldots, P_s > 0$, where $Z(Q)$ is bounded and Q is non-negative everywhere. Let $\mathcal{P} = \{P_1, \ldots, P_s\}$, and the combinatorial level of the system $(Q, \mathcal{P})$ be bounded by $m \leq k$ and the degrees of the polynomials Q and P_i be bounded by $2d$ and d respectively. Then, $r(S) = \binom{s}{m}(O(d))^k$.*

Proof: Consider the set S_ϵ defined by

$$Q = 0, P_1 \geq \epsilon, \ldots, P_s \geq \epsilon,$$

where $\epsilon > 0$ is a new variable. Then, it is easy to prove that for sufficiently small $\epsilon > 0$ $H_*(S_\epsilon) \cong H_*(S)$. Let T denote the set defined by, $Q = 0, P_2 \geq \epsilon, \ldots, P_s \geq \epsilon$.

Consider the sets $U_1 = T \cap ((P_1 \geq \epsilon) \cup (P_1 \leq \epsilon))$, $V_1 = T \cap (-\epsilon \leq P_1 \leq \epsilon)$ and $W_1 = T \cap ((P_1 = \epsilon) \cup (P_1 = -\epsilon))$.

From inequality 1 we see that, $r(U_1) + r(V_1) \leq r(T) + r(W_1)$ and from lemma 5 that $r(S) \leq r(U_1)$. It immediately follows that, $r(S) \leq r(T) + r(W_1)$.

Moreover, let $r(s, d, m, k)$ be the maximum possible value of $r(S)$ for any set defined by a system with these parameters. Then, we have the recurrence,

$$r(s, d, m, k) \leq r(s-1, d, m, k) + 2r(s-1, d, m-1, k), m \leq k,$$

$$r(0, d, m, k) = (O(d))^k, r(s, d, 0, k) = (O(d))^k.$$

It follows easily that, $r(s, d, m, k) = \binom{s}{m}(O(d))^k$. □

Lemma 7 *Let S be a* compact *semi-algebraic set contained in the zero set of a polynomial Q and defined by a family of polynomials $\mathcal{P} = \{P_1, \ldots, P_s\}$. Suppose that Q is non-negative everywhere, the combinatorial level of the system $(Q, \mathcal{P})$ is bounded by $m \leq k$, and the degrees of the polynomials Q and P_i are bounded by $2d$ and d respectively. Then, $r(S) = s^m(O(d))^k$.*

Proof: Let S be defined by the conjunct $(Q = 0) \wedge (\sigma_1 \vee \ldots \sigma_L)$ where the σ_i are sign conditions on the family $\mathcal{P}$.

Let $\epsilon_1 \gg \epsilon_2 \gg \cdots \gg \epsilon_s$, be infinitesimals. Consider the sets, T_1, U_1, V_1, W_1', W_1 defined as follows:

$$T_1 = S \cap ((P_1 \geq \epsilon_1) \cup (P_1 \leq -\epsilon_1)),$$

$$U_1 = S \cap (P_1 = \epsilon_1),$$

$$V_1 = S \cap (P_1 = -\epsilon_1),$$
$$W_1' = S \cap (-\epsilon_1 \leq P_1 \leq \epsilon_1),$$

and

$$W_1 = S \cap (P_1 = 0).$$

Now, $S = T_1 \cup W_1'$, and it is clear that $T_1 \cap W_1' = U_1 \cup V_1$, and $U_1 \cap V_1 = \emptyset$. Using the inequality (2) twice along with the fact that $r(\emptyset) = 0$, we have,

$$r(S) \leq r(T_1) + r(W_1') + r(U_1) + r(V_1).$$

Moreover, using the same arguments as in lemmas 2 and 4, one can show that $H_*(W_1') \cong H_*(W_1)$. We omit the proof as the arguments are completely analogous.

Thus, we have,

$$r(S) \leq r(T_1) + r(W_1) + r(U_1) + r(V_1).$$

Note that, U_1, V_1, W_1 are defined by the systems, $(Q+(P_1-\epsilon_1)^2, \mathcal{P})$, $(Q+(P_1+\epsilon_1)^2, \mathcal{P})$, $(Q+P_1^2, \mathcal{P} \setminus \{P_1\})$, (note that Q is non-negative everywhere) respectively. Moreover, each of the above system has combinatorial level at most $m-1$.

We next consider T_1 which is defined by a set of sign conditions without the atom $P_1 = 0$, and eliminate the atom $P_2 = 0$.

We do this by replacing $P_2 < 0, P_2 > 0$ by $P_2 \leq -\epsilon_2, P_2 \geq \epsilon_2$ respectively. In this way we obtain the inequality,

$$r(T_1) \leq r(T_2) + r(W_2) + r(U_2) + r(V_2),$$

where U_2, V_2, W_2 are sets defined by systems with combinatorial level at most $m-1$.

The remaining set, T_2 has the same homology as the union of the sets defined by those sign conditions appearing in the definition of S, which contain neither $P_1 = 0$ nor $P_2 = 0$.

We continue this process till we have eliminated $P_s = 0$, and we get the inequality,

$$r(S) \leq r(T_s) + \sum_{1 \leq i \leq s} (r(U_i) + r(V_i) + r(W_i)),$$

The sets U_i, V_i, W_i are defined by systems of at most s polynomials having combinatorial level at most $m-1$. Moreover, the remaining term $r(T_s)$ is the bound on the Betti numbers of a semi-algebraic set defined by a union of sign conditions of the form, $Q = 0, P_i\ s_i\ 0$ for $1 \leq i \leq s$, with $s_i \in \{<, >\}$.

Again, by lemma 5, the Betti numbers of this set are the sum of the the Betti numbers of the non-empty sets defined by each individual sign condition. Now, consider the set T defined by $Q = 0, P_1^2 > 0, \ldots, P_s^2 > 0$. From the above remark it is clear that $r(T_s) \leq r(T)$. Moreover, applying the bound proved in lemma 6 we have, $r(T) = \binom{s}{m}(O(d))^k$.

Let, $r(s, d, k, m)$ denote the sum of the Betti numbers of a semi-algebraic set defined by a system $(Q, \mathcal{P})$ with $|\mathcal{P}| = s$, combinatorial level of the system bounded by m, and the degrees of the polynomial Q and those in $\mathcal{P}$ bounded by d. Then, we have the recurrence,

$$r(s, d, k, m) = \binom{s}{m}(O(d))^k + 3s\, r(s, d, k, m-1),\ m \leq k$$

$$r(s, d, k, 0) = (O(d))^k.$$

This recurrence solves to $r(s, d, k, m) = s^m(O(d))^k, m \leq k$, which proves the lemma. $\Box$

The theorem now follows since the combinatorial level of a system $(Q, \mathcal{P})$ with the family $\mathcal{P}$ in general position with respect to Q is bounded by k'. $\Box$

4 A Fewnomial Bound

In this section, we prove a bound on the sum of the Betti numbers of a closed semi-algebraic set, in which the algebraic part of the complexity depends only on the number of monomials appearing in the polynomials and is independent of the degree. This result is a consequence of the fewnomial bounds due to Khovansky [23] and the technique used to prove theorem 1.

The following proposition is crucial for the proving the bound and is used as well in our algorithms to compute the Euler characteristic. Let S be a compact, basic, semi-algebraic set defined by, $P_1 \geq 0, \ldots, P_s \geq 0$. Let the degrees of the polynomials, P_i be bounded by d. The next proposition proves that S is has the same homology groups as a certain set which is bounded by a smooth hypersurface.

Proposition 2 *Let* $Q = \prod_{1 \leq i \leq s}(\zeta + (1-\zeta)P_i) + \zeta^{s+1}(X_1^{2d'} + \cdots + X_k^{2d'} + 1)$, *where* ζ *is a new variable, and*

$$2d' > \sum_{1 \leq i \leq s} deg(P_i).$$

Let S_ζ be the set defined by $(Q \geq 0) \wedge_{1 \leq i \leq s} ((1-\zeta)P_i + \zeta \geq 0)$. Then, for all sufficiently small $\zeta > 0$, $H_*(S) = H_*(S_\zeta)$.

Moreover, S_ζ is bounded by connected components of a smooth hypersurface $Z(Q)$, which has a finite number of critical points for the projection map onto the X_1 co-ordinate and these critical points are non-degenerate and have distinct X_1 co-ordinates.

Proof: Let $S_\zeta = (Q \geq 0) \wedge_{1 \leq i \leq s} ((1-\zeta)P_i + \zeta \geq 0)$.

Since S is compact there exists a constant R such that, $x \in S \Rightarrow x_1^{2d'} + \cdots + x_k^{2d'} + 1 < R$. For $0 < \zeta < 1/R$, any point, $x = (x_1, \ldots, x_k)$, satisfying $P_1(x) \geq 0, \ldots, P_s(x) \geq 0$ will also satisfy $Q \geq 0$. This follows directly from the definition of Q and the fact that $x_1^{2d'} + \cdots + x_k^{2d'} + 1 < R$.

Thus, for every connected component C of S there exists a connected component C' of $Q \geq 0$ such that $C \subset C'$. Moreover, the signs of the polynomials $\zeta + (1-\zeta)P_i,\ 1 \leq i \leq s$, cannot change over C' because if one of them became zero Q would be negative at that point. But, since C' contains C, and ζ is sufficiently small, it is clear that $\zeta + (1-\zeta)P_i > 0,\ 1 \leq i \leq s$ over C'. Thus, for ζ small enough, $S \subset S_\zeta$.

Moreover, $S = \cap_{t>0} S_t$, and S and S_t are compact. Thus using Hardt's triviality and theorem 4, we have that for small enough $\zeta > 0$, $H_*(S) \cong H_*(S_\zeta)$.

We next show that the set S_ζ is bounded by connected components of the smooth hypersurface defined by $Q = 0$.

First observe that the set $Q \geq 0$ is bounded. This follows from the fact that $2d' > sd$ and thus the second term in Q dominates the first as $|x|$ becomes large.

Secondly, the polynomials $\zeta + (1-\zeta)P_i$ are all strictly positive over S_ζ. Hence, S_ζ must be bounded by the smooth hypersurface $Q = 0$.

It remains to show that the hypersurface $Q = 0$ is smooth and has a finite number of critical points for the projection map onto the X_1 co-ordinate, and that these critical points are non-degenerate with distinct X_1 co-ordinate.

Let $Q_t = \prod_{1 \leq i \leq s}(t + (1-t)P_i) + t^{s+1}(X_1^{2d'} + \cdots + X_k^{2d'} + 1)$, then it is clear that $Q_1 = 0$ defines a smooth hypersurface with all its critical points non-degenerate and having distinct X_1 co-ordinates. Moreover, these being stable conditions there is an open interval containing 1, such that for t in this interval, these are also true for Q_t. Now, by quantifier elimination over algebraically closed fields, we have that the set of real t for which the above conditions are not met is either a finite set of points or the complement of a finite set of points. It cannot be the latter, since it does not contain an open interval around 1, and hence it must be a finite set of points. Thus, there is an open interval $(0, t_0)$ such that for $\zeta \in (0, t_0)$ the conditions of the proposition are satisfied. $\square$

We first state the theorem for an algebraic set. This theorem appears in [23], but without a precise bound.

Theorem 5 *Let $Z(Q) \subset R^k$ be a real algebraic set, and let m be the number of distinct monomials that appear in Q. Then the sum of the Betti numbers of $Z(Q)$ is bounded by $2^{O(k^2m^4)}$.*

Proof: Replace $Z(Q)$ by the set V defined by, $Q_1 = (\zeta + (1-\zeta)Q^2) - \zeta^2(X_1^{2d} + \cdots + X_k^{2d} + 1) \geq 0, (\zeta + (1-\zeta)Q^2) \geq 0$ where $2d > deg(Q)$, and $\zeta > 0$ and sufficiently small. Then as in the proof of proposition 2 we can show that V is bounded by a smooth hypersurface and has a finite number of non-degenerate critical points for the projection map onto the X_1 co=ordinates. Moreover, V has the same homology groups as $Z(Q)$. The number of critical points bounds the sum of the Betti numbers of V and hence of $Z(Q)$. Moreover, the number of critical points is bounded by the number of real solutions of the system, $Q_1 = \frac{\partial Q_1}{\partial X_2} = \cdots = \frac{\partial Q_1}{\partial X_k} = 0$. The total number of non-zero monomials appearing in this system is bounded by $km^2 + 2k = O(km^2)$.

We can now apply Khovansky's bound on the number of real solutions of a system of k polynomials in k variables [23] to obtain the bound stated in the theorem. $\square$

We can now state and prove the theorem in the general case.

Theorem 6 *Let $S \subset R^k$, be the intersection of a closed semi-algebraic set defined by a quantifier-free Boolean formula without negations involving a family, $\mathcal{P} = \{P_1, \ldots, P_s\}$, of s polynomials, whose atoms are of the form $P_i \sigma 0, \sigma \in \{\geq, \leq, =\}$, with the zero set $Z(Q)$, of a polynomial Q. Let the geometric dimension of $Z(Q)$ be k', and the total number of monomials occurring in the polynomials in $\mathcal{P} \cup \{Q\}$ be bounded by m. Then, the sum of the Betti numbers of S is bounded by $s^{k'} 2^{O(k^2m^4)}$.*

Secondly, if S is defined by $Q = 0, P_1 > 0, \ldots, P_s > 0$, we have a slightly tighter bound of $\binom{s}{k'} 2^{O(k^2m^4)} = (\frac{s}{k'})^{k'} 2^{O(k^2m^4)}$.

Proof: The proof is the same as that of theorem 1 except that in the case of algebraic sets we use the bound in lemma 5 rather than the Thom-Milnor bound of $O(d)^k$. $\square$

Note that this bound is again separated into a combinatorial part of $s^{k'}$, and an algebraic part which depends only on m and k. Also note that the Thom-Milnor method does not give this bound even for the basic semi-algebraic sets. The reason is that in their method one replaces a basic semi-algebraic set by a set defined by a single polynomial which is a perturbed version of their product. However, the number of monomials in the product of s polynomials is exponentially large in s, and thus the separation of the combinatorial and the algebraic parts is no longer possible.

5 Computing the Euler Characteristic

By proposition 1 we can assume, without loss of generality, that the given semi-algebraic set is compact. If the given set is not compact then we make make the perturbations described in section 2 and compute the Euler characteristic of the perturbed set. The Euler characteristic of this new set is equal to the Euler characteristic of the original set. The new system will have at most $4s+1$ polynomials with degrees at most $2d$. Moreover, we now have to compute in a larger ring $Z[\delta, \epsilon, \Omega]$. However, since we have introduced only three infinitesimals, the asymptotic complexity of the algorithm is not affected.

5.1 Algorithmic Preliminaries

In our algorithm we will utilize several other algorithms from real algebraic geometry as subroutines. In this section we recall some of the algorithms that we use as subroutines, with appropriate pointers to the literature.

We use a subroutine [4] that constructs univariate representations of the zeros of a zero dimensional variety. This subroutine takes as input a Gröbner basis of a zero-dimensional ideal, I, of polynomials in k variables and outputs a set consisting of $(k+2)$-tuples of univariate polynomials, $(f, g_0, \ldots, g_k)$ such that the complex zeroes of I are among the points obtained by evaluating the rational functions $(\frac{g_1}{g_0}, \ldots, \frac{g_k}{g_0})$ at the roots of the univariate polynomial f, for all the tuples $(f, g_0, \ldots, g_k)$ in the output. We say that the real points corresponding to the tuple $(f, g_0, \ldots, g_k)$, are *associated* to the tuple, and the tuple itself is a *univariate representation* of these points. Moreover, if the degrees of the polynomials in the input are bounded by d, the degrees of the polynomials in the output as well as the complexity of this subroutine is bounded by $d^{O(k)}$.

We also make use of an algorithm, called the sample points subroutine [4], that computes a finite set of points which intersects every connected component of every non-empty sign condition (referred to as *cells* henceforth) of a family of polynomials $\mathcal{P}$, of size s and degrees bounded by d. The subroutine also outputs the sign vector of the polynomials of $\mathcal{P}$ at each output point. The complexity of this subroutine is $\binom{O(s)}{k} sd^{O(k)} = (s/k)^k sd^{O(k)}$.

Lastly, we make use of a multivariate sign determination subroutine [4]. The input is a system T of polynomial equations in k variables, with a finite number of zeros, along with a Gröbner basis for the ideal generated by the polynomials in T, and a set of s polynomials $\mathcal{P} = \{P_1, \ldots, P_s\}$. The output is the list of non-empty sign conditions $\sigma_1, \ldots, \sigma_M$ of $\mathcal{P}$ at the real zeros of the system T and the numbers $c_1, \ldots, c_M$, where c_i is the number of real zeros of T at which the sign vector of $\mathcal{P}$ is σ_i. Moreover, if the polynomials in the input have degrees bounded by d, the complexity of this subroutine is $d^{O(k)}$.

We will also use this subroutine in the special case of computing the index of a symmetric square matrix of size $k \times k$, with polynomial entries, at the real zeros of a zero-dimensional system. Again, if the degrees of the polynomials in the input are bounded by d, the complexity of the subroutine is bounded by $(kd)^{O(k)}$ (see [31]).

5.2 The algorithm for a semi-algebraic set defined by one sign condition

In this section, we describe an algorithm for computing the Euler characteristic of a semi-algebraic set defined by one single sign condition on a family of polynomials. Using lemma 4 we can assume, without loss of generality that the semi-algebraic set S is defined by, $P_1 \geq 0, \ldots, P_s \geq 0$.

From proposition 2 it follows that S has the same homology groups and hence the Euler characteristic, as the union of the connected components of the set defined by

$$(Q \geq 0) \wedge_{1 \leq i \leq s} (\zeta + (1-\zeta)P_i \geq 0,$$

where

$$Q = \prod_{1 \leq i \leq s} (\zeta + (1-\zeta)P_i) + \zeta^{s+1}(X_1^{2d'} + \cdots + X_k^{2d'} + 1),$$

and ζ is an infinitesimal.

We actually compute the Euler characteristic of the latter set which is equal to $\chi(S)$.

5.2.1 Description of the algorithm

Given a basic semi-algebraic set S defined by $P_1 \geq 0, \ldots, P_s \geq 0$, where $deg(P_i) < d$ for $1 \leq i \leq s$, the algorithm computes $\chi(S)$. We then introduce a positive infinitesimal ζ and construct the polynomial, $Q = \prod_{1 \leq i \leq s}(\zeta + (1-\zeta)P_i) + \zeta^{s+1}(X_1^{2d'} + \cdots + X_k^{2d'} + 1)$.

We then solve the zero-dimensional system, $Q = \frac{\partial Q}{\partial X_2} = \cdots = \frac{\partial Q}{\partial X_k} = 0$, using the univariate representation subroutine and for each real zero p of this system we check whether the polynomials $\zeta + (1-\zeta)P_1, \ldots, \zeta + (1-\zeta)P_s$ are all non-negative at the point p. We retain only those real solutions for which this is satisfied. For each critical point $p = (p_1, \ldots, p_k)$ retained in the previous step, check whether $(p_1 - \epsilon, p_2, \ldots, p_k)$ belongs to the set defined by $(Q \geq 0) \wedge_{1 \leq i \leq s} (\zeta + (1-\zeta)P_i \geq 0)$, where ϵ is a new infinitesimal. Note that, since the point p is given only as a univariate representation the last sentence is slightly misleading. However, it is clear that using the univariate representation of p and the sign determination subroutine, we can perform this check. Retain only those critical points p for which the above is false.

For each critical point p retained so far, compute the index of the critical point, which is the index of the Hessian matrix, $(\frac{\partial^2 Q}{\partial X_i \partial X_j})_{ij}, 2 \leq i, j \leq k$, evaluated at p. For $0 \leq i \leq k$ let c_i denote the number of critical points of index i. We output $\chi(S) = \sum_{0 \leq i \leq k}(-1)^i c_i$.

5.2.2 Proof of Correctness

Before giving the proof we need to recall certain facts from Morse theory of stratified sets [12].

A Whitney stratification of a space X is a decomposition of X into submanifolds called strata, which satisfy certain frontier conditions, (see [12] page 37). In particular, given a compact set bounded by a smooth hypersurface, the boundary and the interior form a Whitney stratification.

Now, let X be a compact Whitney stratified subset of R^k, and f a restriction to X of a smooth function. A critical point of f is defined to be a critical point of the restriction of f to any stratum, and a critical value of f is the value of f at a critical point.

The first fundamental result of stratified Morse theory is the following.

Theorem 7 *(Goresky-MacPherson, [12]) As c varies in the open interval between two adjacent critical values, the topological type of $X \cap f^{-1}((-\infty, c])$ remains constant.*

Stratified Morse theory actually gives a recipe for describing the topological change in $X \cap f^{-1}((-\infty, c])$ as c crosses a critical value. This is given in terms of Morse data, which consists of a pair of topological spaces $(A, B), A \supset B$, with the property that as c crosses the critical value $v = f(p)$, the change in $X \cap f^{-1}((-\infty, c])$ can be described by gluing in A along B.

A function is called a Morse function if it has only non-degenerate critical points when restricted to each strata, and all its critical values are distinct.(There is an additional non-degeneracy condition which states that the differential of f at a critical point p of a strata S should not annihilate any limit of tangent spaces to a stratum other than S. However, in our simple situation this will always be true.)

In stratified Morse theory the Morse data is presented as a product of two pairs, called the tangential Morse data and the normal Morse data. The notion of product of pairs is the standard one in topology, namely

$$(A, B) \times (A', B') = (A \times A', A \times B' \cup B \times A').$$

Instead of describing these in full generality, we restrict ourselves to the very simple situation in which we need them, namely when $X \subset R^k$ is compact and is bounded by a smooth hypersurface. The stratification we consider is the stratification of X into its boundary and interior and the function f is just the projection map onto the X_1 co-ordinate. In this case, all critical points occur on the boundary strata (the interior is open in R^k).

The tangential Morse data at a critical point p is then given by $(D^\lambda \times D^{k-\lambda}, (\partial D^\lambda) \times D^{k-\lambda})$ where D^k is the closed k dimensional disk, ∂ is the boundary map, and λ is the index of the Hessian matrix of f at p.

Let $p = (p_1, \ldots, p_k)$. The normal slice $N(p)$ at p is defined to be a sufficiently small segment of length 2ϵ given by, $N(p) = \{(t, p_2, \ldots, p_k) | -\epsilon \leq t \leq \epsilon\}$. Let $L(p) = \{(-\epsilon, p_2, \ldots, p_k)\} \cap X$. Note that, $L(p)$ is empty if X does not lie immediately to the left of p, and a single point otherwise. The normal Morse data at p is then $(N(p), L(p))$.

The example below illustrates the situation in the case of a solid torus in R^3.

5.2.3 The Example of a Solid Torus

Consider the set bounded by the smooth torus in R^3 (see figure 1.) There are four critical points p_1, p_2, p_3 and p_4 corresponding to the critical values v_1, v_2, v_3 and v_4 respectively, for the projection map onto the X_1 co-ordinate. The Morse data at these points are given in the following table:

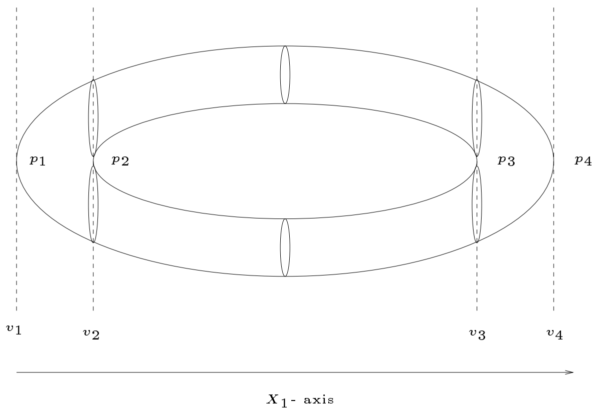

Figure 1: S is the solid torus in 3 space

Critical point	Index	Tangential data	Normal data
p_1	0	$(D^0 \times D^2, \emptyset)$	$([0,1], \emptyset)$
p_2	1	$(D^1 \times D^1, \partial D^1 \times D^1)$	$([0,1], \{0\})$
p_3	1	$(D^1 \times D^1, \partial D^1 \times D^1)$	$([0,1], \emptyset)$
p_4	2	$(D^2 \times D^0, \partial D^2 \times D^0)$	$([0,1], \{0\})$

The second fundamental theorem of stratified Morse theory states the following:

Theorem 8 *(Goresky-MacPherson, [12]) Let f be a Morse function on a compact Whitney stratified space X. Then, Morse data measuring the change in the topological type of $X \cap f^{-1}((-\infty, c])$ as c crosses the critical value v of the critical point p is the product of the normal Morse data at p and the tangential Morse data at p.*

We are now in a position to prove the main proposition of this section.

Proposition 3 *The above algorithm correctly computes the Euler characteristic of S.*

Proof: By proposition 2, $\chi(S)$ is equal to the Euler characteristic of the set defined by $Q \geq 0$ and $\zeta + (1-\zeta)P_i \geq 0$, for $1 \leq i \leq s$. Denote this set by S'.

Moreover, S' is compact, bounded by a smooth hypersurface, and the projection map π onto the X_1 co-ordinate is a Morse function.

By Theorem 7, the topological type of $S' \cap \pi^{-1}((-\infty, c])$ remains constant as c varies in the open interval between two adjacent critical values.

Let, $c_1, \ldots, c_m$ be the critical values of $Q = 0$ which lie in S'. And let, S'_i denote the set $S' \cap \pi^{-1}((-\infty, c_i])$, and let $S'_0 = \emptyset$. Let, (A_i, B_i) be the Morse data at the critical value c_i. Then for $1 \leq i \leq m$,

$$\chi(S'_i) = \chi(S'_{i-1}) + \chi(A_i, B_i).$$

This follows from a standard application of the excision property of homology theory.

Let $(A_i, B_i) = (C_i, D_i) \times (M_i, N_i)$, where (C_i, D_i) is the tangential Morse data, and (M_i, N_i) the normal Morse data. Then it is easy to see that $\chi(A_i, B_i) = \chi(C_i, D_i)\chi(M_i, N_i)$.

We next observe that, for a critical point $(p_1, \ldots, p_k)$, $\chi(M_i, N_i) = 0$ if $(p_1 - \epsilon, p_2, \ldots, p_k) \in S'$. In this case, N_i, consists of a single point, as S' intersect a sufficiently small segment parallel to the X_1 axis passing through the critical point. Moreover, M_i is the closed segment, and thus, $\chi(M_i, N_i) = \chi(M_i) - \chi(N_i) = 1 - 1 = 0$.

If the test in Step 3 returns false, then $N_i = \emptyset$, and in this case, $\chi(M_i, N_i) = \chi(M_i) = 1$.

Finally, $(C_i, D_i) = (D^\lambda \times D^{k-\lambda}, (\partial D^\lambda) \times D^{k-\lambda})$, where λ is the index of the critical point computed in Step 4. Thus, $\chi(C_i, D_i) = \chi(D^\lambda, \partial D^\lambda) = \chi(D^\lambda) - \chi(\partial D^\lambda)$.

Now, $\chi(D^\lambda) = 1$, and $\chi(\partial D^\lambda) = 1 - (-1)^\lambda$ and hence $\chi(C_i, D_i) = 1 - (1 - (-1)^\lambda) = (-1)^\lambda$.

Since $\chi(S') = \chi(S'_m)$ it is clear that the algorithm correctly computes $\chi(S')$. □

5.2.4 Complexity of the Algorithm

The polynomial Q has degree bounded by $O(sd)$. The cost of computing the indices of the Hessian matrices in the last step dominates the cost. We use the sign determination subroutine in the special case of computing the index of a symmetric square matrix of size $k \times k$, with polynomial entries, at the real zeros of a zero-dimensional system. If the degrees of the polynomials in the input are bounded by D, the complexity is bounded by $(kD)^{O(k)}$, (see [31]). Thus the total complexity of this algorithm is bounded by $(ksd)^{O(k)}$.

5.3 The case of a general semi-algebraic set

5.3.1 Description of the Algorithm

Using the algorithm in [4] list all non-empty sign conditions, $\sigma_1, \ldots, \sigma_m$ of the family $\mathcal{P}$, such that the set S_j defined by σ_j is contained in S for $1 \leq j \leq m$.

For each j, $1 \leq j \leq m$, do the following. Without loss of generality assume that σ_j is of the form, $P_1 = \cdots = P_l = 0, P_{l+1} > 0, \ldots, P_s > 0$. Let U_j be the set defined by, $P_1 = \cdots = P_l = 0, P_{l+1} \geq 0, \ldots, P_s \geq 0$, and let $V_j = U_j \cap Z(\prod_{l<i\leq s} P_i)$.

Using the algorithm described in section 5.2 for computing the Euler characteristic of basic semi-algebraic sets, compute $\chi(U_j)$ and $\chi(V_j)$.

Output, $\chi(S) = \sum_{1\leq j\leq m}(\chi(U_j) - \chi(V_j))$.

5.3.2 Proof of Correctness

First note that the set S is compact.

We utilize several results from [36]. We assume that the reader is familiar with algebraic decision trees ([36]). Consider the following fixed degree algebraic decision tree denoted by T. Let the polynomial associated to the root be the polynomial, $P_1 = X_1^2 + \cdots + X_k^2 - \Omega$. The associated polynomial to each node at level i, $2 \leq i \leq s$ is P_i. The sets associated to each of the leaf nodes correspond to the 3^s possible sign-conditions on the family $\mathcal{P}$. Let the set of leaves corresponding to the sign conditions which are non-empty and included in S be denoted by L_S. For a leaf $l \in L_s$, let S_l denote the set associated with it.

For any set A, following [36], we define $\beta_i'(A)$ to be the rank of the i-th homology group $H_i(\bar{A}, \partial A)$, where $\bar{A}$ is the closure of A in the topology of R^k and $\partial A = \bar{A} - A$.

Similarly we define, $\chi'(A) = \sum_{0\leq i\leq k}(-1)^i \beta_i'(A)$. If A is compact then $\beta_i'(A) = \beta_i(A)$, and $\chi'(A) = \chi(A)$.

We first prove a preliminary lemma.

Lemma 8 *Let X be a semi-algebraic set in R^k which is bounded and semi-closed. For some polynomial*

$$f \in R[X_1, \ldots, X_k],$$

let $A = X \cap (f \geq 0)$, and $B = X - A$. Then, $\chi'(X) = \chi'(A) + \chi'(B)$.

Proof: The proof is quite similar to the proof of lemma 5 in [36].

From the exact sequence,

$$\cdots \to H_i(\bar{A} \cup \partial X, \partial X) \to H_i(\bar{X}, \partial X) \to H_i(\bar{X}, \bar{A} \cup \partial X) \to \cdots,$$

we have $\chi(\bar{X}, \partial X) = \chi(\bar{X}, \bar{A} \cup \partial X) + \chi(\bar{A} \cup \partial X, \partial X)$. Moreover, $\beta_i(\bar{X}, \bar{A} \cup \partial X) = \beta_i'(B)$, and $\beta_i(\bar{A} \cup \partial X, \partial X) = \beta_i'(A)$ (see [36] for a proof). It follows easily that, $\chi'(X) = \chi'(A) + \chi'(B)$. □

Next, we prove that,

Lemma 9 $\chi(S) = \sum_{l \in L_S} \chi'(S_l)$.

Proof: The complexity of this algorithm is again bounded by $(ksd)^{O(k)}$. See subsections 5.3.2 and 5.3.3 of the appendix for the proof of correctness and the complexity analysis.

Note that since S is compact, $\chi'(S) = \chi(S)$. The lemma now follows by a simple induction on the levels of T, starting from the leaf nodes and going up, and using lemma 8 at each node. We omit the details. □

We next prove that, following the notation introduced in the algorithm, that $\beta_i'(S_j) = \beta_i(U_j, V_j)$, and thus $\chi'(S_j) = \chi(U_j, V_j)$. The proof of this appears in [36] (page 621) and is omitted.

It follows from the exact sequence,

$$\cdots \to H_i(V_j) \to H_i(U_j) \to H_i(U_j, V_j) \to H_{i-1}(V_j) \to \cdots,$$

we immediately deduce that, $\chi(U_j, V_j) = \chi(U_j) - \chi(V_j)$.

This in conjunction with lemma 9 shows that, $\chi(S) = \sum_{1 \le j \le m}(\chi(U_j) - \chi(V_j))$, and this proves the correctness of the algorithm.

5.3.3 Complexity Analysis

The cost of computing all the non-empty sign conditions of the family $\mathcal{P}$ is $s^{k+1}d^{O(k)}$. Moreover, there can be only $\binom{s}{k}(O(d))^k$ such non-empty sign conditions. For each such sign-condition included in S, we call the algorithm for computing the Euler characteristics of basic semi-algebraic sets twice. The sum of the degrees of the polynomials involved in each such call is $O(sd)$. Thus each call costs $(ksd)^{O(k)}$. Hence, the total complexity of the algorithm is bounded by $(ksd)^{O(k)}$.

The bound in the bit model follows easily once we note that bit sizes of the intermediate values are bounded by $L(skd)^{O(k)}$.

References

[1] A. I. Barvinok On the Betti Numbers of Semialgebraic Sets Defined by Few Quadratic Inequalities, to appear in *Mathematische Zeitschrift* .

[2] J. Bochnak, M. Coste, M.-F. Roy Géométrie algébrique réelle. Springer-Verlag (1987).

[3] M. Ben-Or *Lower Bounds for Algebraic Computation Trees, Proc. 15th Annual ACM Symposium on the Theory of Computing, 80-86 (1983).*

[4] S. Basu, R. Pollack, M.-F. Roy On the Combinatorial and Algebraic Complexity of Quantifier Elimination , *Journal of the ACM, Nov 1996, Vol. 43, Number 6, 1002-1045.* (Extended Abstract in *Proc. 35th Symposium on Foundations of Computer Science (1994).*)

[5] S. Basu, R. Pollack, M.-F. Roy *On the Number of Cells Defined by a Family of Polynomials on a Variety* , Mathematika, 43 (1996) 120-126.

[6] S. Basu *On Bounding the Betti Numbers and Computing the Euler Characteristics of Semi-algebraic Sets, Proc. 28th Annual ACM Symposium on the Theory of Computing*, 408-417 (1996).

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

[8] B. Chazelle *Computational Geometry: A Retrospective, Proc. 26th STOC, 75-94 (1994).*

[9] G. E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition* Springer Lecture Notes in Computer Science 33, 515- 532.

[10] S. Eilenberg, N Steenrod Foundations of Algebraic Topology, Princeton University Press, 1952.

[11] A. Gabrielov Multiplicities of zeroes of polynomials on trajectories of polynomial vector fields and bounds on degree of nonholonomy Math. Res. Lett. 2 (1995), no. 4, 437–451.

[12] M. Goresky, R. MacPherson *Stratified Morse Theory,* Springer-Verlag (1987).

[13] J.E. Goodman, R. Pollack, R. Wenger *Bounding the Number of Geometric Permutations Induced by k-transversals*, Journal of Combinatorial Theory Series A, (to appear).

[14] J.E. Goodman, R. Pollack *Upper Bounds for Configurations and Polytopes in R^d*, Journal of Discrete and Computational Geometry, 1, 219-227 (1986).

[15] L. Gournay, J. J. Risler *Construction of roadmaps of semi-algebraic sets.* Technical Report, DMI, Ecole Normale Superieure, Paris, France (1992).

[16] L. Gournay, J. J. Risler *Construction of roadmaps of semi-algebraic sets,* Technical Report, DMI, Ecole Normale Superieure, Paris, France (1992).

[17] D. Grigor'ev *The Complexity of deciding Tarski algebra* Journal of Symbolic Computation 5 (1988), 65-108.

[18] D. Grigor'ev, N. Vorobjov *Solving Systems of Polynomial Inequalities in Subexponential Time*, J. Symbolic Comput., 5:37-64 (1988).

[19] R. M. Hardt *Semi-algebraic Local Triviality in Semi-algebraic Mappings* American Journal of Math. 102, 1980, 291-302.

[20] J. Heintz, M.-F. Roy, P. Solernò *Single exponential path finding in semi-algebraic sets II : The general case,* Algebraic geometry and its applications, C. L. Bajaj editor, Springer Verlag (1993) 467-481.

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

[22] J. Heintz, T. Recio, M.-F. Roy *Algorithms in Real Algebraic Geometry and Applications to Computational Geometry Discrete and Computational Geometry: Selected Papers from the DIMACS Special Year,* Ed. J.E. Goodman, R. Pollack and W. Steiger, AMS and ACM, 6:137-164 (1991).

[23] A. G. Khovanskii *Fewnomials*, Translations of Mathematical Monographs, Vol.88, AMS (1991).

[24] M. Knebusch Semi-algebraic Topology in the last ten years, Real Algebraic Geometry, M. Coste, L. Mahe, M.-F. Roy Ed., Lecture Notes in Mathematics 1524, Springer, 1-36 (1992).

[25] T. Krick, L. M Pardo A Computational Method for Diophantine Approximation, To appear in MEGA 94.

[26] J. Milnor *Morse Theory*, Annals of Mathematical Studies, Princeton University Press.

[27] J. Milnor *On the Betti numbers of real varieties*, Proc. AMS 15, 275-280 (1964).

[28] O. A. Oleinik, I. B. Petrovskii *On the topology of real algebraic surfaces*, Izv. Akad. Nauk SSSR 13, 389-402 (1949).

[29] J. L. Montana, J. E. Morais, L. M. Pardo *Lower Bounds for Arithmetic Networks II: Sum of Betti Numbers*, Applicable Algebra in Engineering, Communication and Computing (1995).

[30] R. Pollack, M.-F. Roy *On the number of cells defined by a set of polynomials*, C. R. Acad. Sci. Paris, 316:573–577 (1993).

[31] 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).

[32] M.-F. Roy *Basic algorithms in real algebraic geometry: from Sturm theorem to the existential theory of reals,* Lectures on Real Geometry in memoriam of Mario Raimondo, de Gruyter Expositions in Mathematics, to appear.

[33] E. H. Spanier Algebraic Topology, McGraw-Hill Book Company, 1966.

[34] J. Schwartz, M. Sharir *On the 'piano movers' problem II. General techniques for computing topological properties of real algebraic manifolds.*, Advances in Applied Mathematics 4, 298-351.

[35] R. Thom *Sur l'homologie des varietes algebriques reelles*, Differential and Combinatorial Topology, Ed. S.S. Cairns, Princeton Univ. Press, 255-265 (1965).

[36] A. C. YAO *Decision Tree Complexity and Betti Numbers*, *Proc. 26th ACM Symp. on Theory of Computing, 615-624, (1994).*