Electronic Colloquium on Computational Complexity, Report No. 140 (2009)

A COMPLEX ANALOGUE OF TODA'S THEOREM

SAUGATA BASU

Abstract. Toda [19] proved in 1989 that the (discrete) polynomial time hierarchy, **PH**, is contained in the class $\mathbf{P}^{\#\mathbf{P}}$, namely the class of languages that can be decided by a Turing machine in polynomial time given access to an oracle with the power to compute a function in the counting complexity class #**P**. This result which illustrates the power of counting is considered to be a seminal result in computational complexity theory. An analogous result (with a compactness hypothesis) in the complexity theory over the reals (in the sense of Blum-Shub-Smale real Turing machines [3]) was proved in [1]. Unlike Toda's proof in the discrete case, which relied on sophisticated combinatorial arguments, the proof in [1] is topological in nature in which the properties of the topological join is used in a fundamental way. However, the constructions used in [1] was semi-algebraic in nature – they used real inequalities in an essential way and as such do not extend to the complex case. In this paper, we extend the techniques developed in [1] to the complex case. A key role is played by the complex join of quasi-projective complex varieties. As a consequence we obtain a complex analogue of Toda's theorem. As in the real case, the complex analogue of Toda's theorem is proved with a compactness assumption which we are unable to remove presently. We also relate the computational hardness of two well-studied problems in algorithmic complex geometry – namely the problem of deciding sentences in the first order theory of algebraically closed fields of characteristic 0 with a constant number of quantifier alternations, and that of computing Betti numbers of constructible sets. We obtain a polynomial time reduction in the Blum-Shub-Smale model of the compact version of the first problem to the second.

1. Introduction and Main Results

1.1. **History and Background.** The primary motivation for this paper comes from classical (i.e. discrete) computational complexity theory. In classical complexity theory, there is a seminal result due to Toda [19] linking the complexity of counting with that of deciding sentences with a fixed number of quantifier alternations.

More precisely, Toda's theorem gives the following inclusion (see Section 1.2 below or refer to [13] for precise definitions of the complexity classes appearing in the theorem).

Theorem 1.1 (Toda [19]).

$$\mathbf{PH} \subset \mathbf{P}^{\#\mathbf{P}}.$$

Date: **December 17, 2009**.

1991 *Mathematics Subject Classification.* Primary 14F25, 14Q15; Secondary 68Q15.

Key words and phrases. Polynomial hierarchy, Betti numbers, constructible sets, Toda's theorem.

The author was supported in part by an NSF grant CCF-0915954.

ISSN 1433-8092

In other words, any language in the (discrete) polynomial hierarchy can be decided by a Turing machine in polynomial time, given access to an oracle with the power to compute a function in $\#\mathbf{P}$.

Remark 1.2. The proof of Theorem 1.1 in [19] is quite non-trivial. While it is obvious that the classes $\mathbf{P}, \mathbf{NP}, \mathbf{coNP}$ are contained in $\mathbf{P}^{\#\mathbf{P}}$, the proof for the higher levels of the polynomial hierarchy is quite intricate and proceeds in two steps: first proving that the $\mathbf{PH} \subset \mathbf{BP} \cdot \oplus \cdot \mathbf{P}$ (using previous results of Schöning [14], and Valiant and Vazirani [20]), and then showing that $\mathbf{BP} \cdot \oplus \cdot \mathbf{P} \subset \mathbf{P}^{\#\mathbf{P}}$. Aside from the obvious question about what should be a proper analogue of the complexity class $\#\mathbf{P}$ over the reals or complex numbers, because of the presence of the intermediate complexity class in the proof, there seems to be no direct way of extending such a proof to real or complex complexity classes in the sense of Blum-Shub-Smale model of computation [3, 16]. The proof of the main theorem (Theorem 2.1) of this paper, which can be seen as a complex analogue of Theorem 1.1, proceeds along completely different lines and is mainly topological in nature.

In the late eighties Blum, Shub and Smale [3, 16] introduced the notion of Turing machines over more general fields, thereby generalizing the classical problems of computational complexity theory such as $\mathbf{P}$ vs $\mathbf{NP}$ to corresponding problems over arbitrary fields (such as the real, complex, p-adic numbers etc.) If one considers languages accepted by a Blum-Shub-Smale machine over a finite field one recovers the classical notions of discrete complexity theory. Over the last two decades there has been a lot of research activity towards proving real as well as complex analogues of well known theorems in discrete complexity theory. The first steps in this direction were taken by the authors Blum, Shub, and Smale (henceforth B-S-S) themselves, when they proved the $\mathbf{NP}_{\mathbb{C}}$-completeness of the problem of deciding whether a systems of $n+1$ polynomial equations in n variables of has a solution (in affine space) (this is the complex analogue of Cook-Levin's theorem that the satisfiability problem is $\mathbf{NP}$-complete in the discrete case), and subsequently through the work of several researchers (Koiran, Bürgisser, Cucker, Meer to name a few) a well-established complexity theory over the reals as well as complex numbers have been built up, which mirrors closely the discrete case.

It is thus quite natural to seek a real as well as complex analogues of Toda's theorem. Indeed, there has been a large body of recent research on obtaining appropriate real (as well as complex) analogues of results in discrete complexity theory, especially those related to counting complexity classes (see [12, 4, 6, 5]).

In [1] a real analogue of Toda's theorem was proved (with a compactness hypothesis). In this paper we prove a similar result in the complex case. Even though the basic approach is similar in both cases, the topological tools in the complex case are different enough to merit a separate treatment. This is elaborated further in the next section (the main difficulty in extending the real arguments in [1] to the complex case is that we can no longer use inequalities in our constructions). Aside from the obvious motivation of proving a complex version of Toda's theorem, a second motivation comes from the fact that it can be considered as a first step towards proving the classical Toda's theorem using algebro-geometric techniques – something that we do not explore further in the current paper.

In order to formulate our result it is first necessary to define precisely complex counter-parts of the discrete polynomial time hierarchy $\mathbf{PH}$ and the discrete complexity class $\#\mathbf{P}$, and this is what we do next.

1.2. **Complex counter-parts of PH and #P.** For the rest of the paper C will denote an algebraically closed field of characteristic zero (there is no essential loss in assuming that $\mathrm{C} = \mathbb{C}$) (indeed by a transfer argument it suffices to prove all our results in this case). By a ***complex machine*** we will mean a machine in the sense of Blum-Shub-Smale [3]) over the ground field C.

Notational convention. Since in what follows we will be forced to deal with multiple blocks of variables in our formulas, we follow a notational convention by which we denote blocks of variables by bold letters with superscripts (e.g. $\mathbf{X}^i$ denotes the i-th block), and we use non-bold letters with subscripts to denote single variables (e.g. X^i_j denotes the j-th variable in the i-th block). We use $\mathbf{x}^i$ to denote a specific value of the block of variables $\mathbf{X}^i$. We will call a quantifier-free first-order formula (in the language of fields), $\phi(\mathbf{X}^1; \cdots ; \mathbf{X}^\omega)$, having several blocks of variables $(\mathbf{X}^1, \ldots, \mathbf{X}^\omega)$ to be ***multi-homogeneous*** if each polynomial appearing in it are multi-homogeneous in the blocks of variables $(\mathbf{X}^1, \ldots, \mathbf{X}^\omega)$ and such that ϕ is satisfied whenever any one of the blocks $\mathbf{X}^i = 0$. Clearly such a formula defines a constructible subset of $\mathbb{P}^{k_1}_{\mathrm{C}} \times \cdots \mathbb{P}^{k_\omega}_{\mathrm{C}}$ where the block $\mathbf{X}^i$ is assumed to have $k_i + 1$ variables. If $\omega = 1$, that is there is only one block of variables, then we call ϕ a *homogeneous formula.*

1.2.1. *Complex analogue of* **PH**. We recall the definition of the polynomial hierarchy over C. It mirrors the discrete case very closely (see [18]).

Definition 1.3 (The class $\mathbf{P}_{\mathrm{C}}$)**.** Let $k(n)$ be any polynomial in n. A sequence

$$\left(T_n \subset \mathrm{C}^{k(n)}\right)_{n>0}$$

of constructible subsets is said to belong to the class $\mathbf{P}_{\mathrm{C}}$ if there exists a B-S-S machine M over C (see [3, 2]), such that for all $\mathbf{x} \in \mathrm{C}^{k(n)}$, the machine M tests membership of $\mathbf{x}$ in T_n in time bounded by a polynomial in n.

Definition 1.4. Let $k(n), k_1(n), \ldots, k_\omega(n)$ be polynomials in n. A sequence

$$\left(S_n \subset \mathrm{C}^{k(n)}\right)_{n>0}$$

of constructible subsets is said to be in the complexity class $\mathbf{\Sigma}_{\mathrm{R},\omega}$, if for each $n > 0$, the constructible set S_n is described by a first order formula

$$(Q_1\mathbf{Y}^1) \cdots (Q_\omega\mathbf{Y}^\omega)\phi_n(X_1, \ldots, X_{k(n)}, \mathbf{Y}^1, \ldots, \mathbf{Y}^\omega), \tag{1.1}$$

with ϕ_n a quantifier free formula in the first order theory of C, and for each $i, 1 \leq i \leq \omega$, $\mathbf{Y}^i = (Y^i_1, \ldots, Y^i_{k_i(n)})$ is a block of $k_i(n)$ variables, $Q_i \in \{\exists, \forall\}$, with $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$, and the sequence

$$\left(T_n \subset \mathrm{C}^{k(n)} \times \mathrm{C}^{k_1(n)} \times \cdots \times \mathrm{C}^{k_\omega(n)}\right)_{n>0}$$

of constructible subsets defined by the quantifier-free formulas $(\phi_n)_{n>0}$ belongs to the class $\mathbf{P}_{\mathrm{C}}$.

Similarly, the complexity class $\mathbf{\Pi}_{\mathrm{C},\omega}$ is defined as in Definition 1.4, with the exception that the alternating quantifiers in (1.1) start with $Q_1 = \forall$. Since, adding an additional block of quantifiers on the outside (with new variables) does not change the set defined by a quantified formula we have the following inclusions:

$$\mathbf{\Sigma}_{\mathrm{C},\omega} \subset \mathbf{\Pi}_{\mathrm{C},\omega+1}, \text{ and } \mathbf{\Pi}_{\mathrm{C},\omega} \subset \mathbf{\Sigma}_{\mathrm{C},\omega+1}.$$

Note that by the above definition the class $\mathbf{\Sigma}_{\mathrm{C},0} = \mathbf{\Pi}_{\mathrm{C},0}$ is the familiar class $\mathbf{P}_{\mathrm{C}}$, the class $\mathbf{\Sigma}_{\mathrm{C},1} = \mathbf{NP}_{\mathrm{C}}$ and the class $\mathbf{\Pi}_{\mathrm{C},1} = \text{co-}\mathbf{NP}_{\mathrm{C}}$.

Definition 1.5 (Complex polynomial hierarchy)**.** The complex polynomial time hierarchy is defined to be the union

$$\mathbf{PH}_{\mathrm{C}} \stackrel{\text{def}}{=} \bigcup_{\omega \geq 0} (\mathbf{\Sigma}_{\mathrm{C},\omega} \cup \mathbf{\Pi}_{\mathrm{C},\omega}) = \bigcup_{\omega \geq 0} \mathbf{\Sigma}_{\mathrm{C},\omega} = \bigcup_{\omega \geq 0} \mathbf{\Pi}_{\mathrm{C},\omega}.$$

As in the real case studied in [1] for technical reasons we need to restrict to compact constructible sets. However, unlike in [1] where the compact languages consisted of closed semi-algebraic subsets of spheres, in this paper we consider closed subsets of projective spaces instead. This is a much more natural choice for defining compact complex complexity classes (indeed, the sphere is not a constructible set over the complex numbers).

We now define the compact analogue of $\mathbf{PH}_{\mathrm{C}}$ that we will denote $\mathbf{PH}_{\mathrm{C}}^{c}$. Unlike in the non-compact case, we will assume all variables vary over certain compact sets (namely complex projective spaces of varying dimensions).

We first need to be precise about what we mean by a complexity class of sequences of constructible subsets of complex projective spaces.

Notation 1.6. For any constructible subset $S \subset \mathbb{P}_{\mathrm{C}}^{k}$ we denote by $C(S) \subset \mathrm{C}^{k+1}$ the affine cone over S.

Definition 1.7. Let $k(n)$ be a polynomial in n. We say that a sequence

$$\left(S_n \subset \mathbb{P}_{\mathrm{C}}^{k(n)}\right)_{n>0}$$

of constructible subsets is in the complexity class $\mathbf{P}_{\mathrm{C}}$, if the sequence of affine cones $(C(S_n) \subset \mathrm{C}^{k(n)+1})_{n>0} \in \mathbf{P}_{\mathrm{C}}$.

Remark 1.8. Since a product of any constant number, ω, of projective spaces, $\mathbb{P}_{\mathrm{C}}^{k_1} \times \cdots \times \mathbb{P}_{\mathrm{C}}^{k_\omega}$, can be embedded into the projective space $\mathbb{P}_{\mathrm{C}}^{(k_1+1)\cdots(k_\omega+1)-1}$ by the classical Segre embedding [15, Chap. 1, Sec. 5] (which we will denote by $\mathrm{Seg}_{k_1,\ldots,k_\omega}$), and the Segre map is polynomial time computable (for fixed ω), we will occasionally abuse notation and identify the sequence

$$\left(S_n \subset \mathbb{P}_{\mathrm{C}}^{k_1(n)} \times \cdots \times \mathbb{P}_{\mathrm{C}}^{k_\omega(n)}\right)_{n>0}$$

with its image sequence

$$\left(\mathrm{Seg}_{k_1(n),\ldots,k_\omega(n)}(S_n) \subset \mathbb{P}_{\mathrm{C}}^{(k_1(n)+1)\cdots(k_\omega(n)+1)-1}\right)_{n>0}$$

under the Segre map. In particular, we will sometime say that a sequence $(S_n \subset \mathbb{P}_{\mathrm{C}}^{k_1(n)} \times \cdots \times \mathbb{P}_{\mathrm{C}}^{k_\omega(n)})_{n>0}$ is in $\mathbf{P}_{\mathrm{C}}$, when strictly speaking we mean that the sequence

$$\left(\mathrm{Seg}_{k_1(n),\ldots,k_\omega(n)}(S_n) \subset \mathbb{P}_{\mathrm{C}}^{(k_1(n)+1)\cdots(k_\omega(n)+1)-1}\right)_{n>0}$$

is in $\mathbf{P}_{\mathrm{C}}$. As long as ω is a fixed number, and $k_1, \ldots, k_\omega$ polynomially bounded, this abuse of notation does not cause any problem.

Definition 1.9 (Compact version of $\mathbf{\Sigma}_{\mathrm{C},\omega}$)**.** Let

$$k(n), k_1(n), \ldots, k_\omega(n)$$

be polynomials in n. A sequence

$$\left(S_n \subset \mathbb{P}_{\mathrm{C}}^{k(n)}\right)_{n>0}$$

of constructible subsets is in the complexity class $\mathbf{\Sigma}^c_{\mathrm{C},\omega}$, if for each $n > 0$, S_n is described by a first order formula

$$(Q_1\mathbf{Y}^1 \in \mathbb{P}_{\mathrm{C}}^{k_1(n)}) \cdots (Q_\omega \mathbf{Y}^\omega \in \mathbb{P}_{\mathrm{C}}^{k_\omega(n)})\phi_n(X_0,\ldots,X_{k(n)};\mathbf{Y}^1;\cdots;\mathbf{Y}^\omega),$$

with ϕ_n a quantifier-free first order multi-homogeneous formula defining a *closed* (in the Zariski topology) subset of $\mathbb{P}_{\mathrm{C}}^{k(n)} \times \mathbb{P}_{\mathrm{C}}^{k_1(n)} \times \cdots \times \mathbb{P}_{\mathrm{C}}^{k_\omega(n)}$, and for each $i, 1 \leq i \leq \omega$, $\mathbf{Y}^i = (Y^i_0,\ldots,Y^i_{k_i})$ is a block of $k_i(n)+1$ variables, $Q_i \in \{\exists,\forall\}$, with $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$, and the sequence of constructible sets $(T_n)_{n>0}$ defined by the formulas $(\phi_n)_{n>0}$ belongs to the class $\mathbf{P}_{\mathrm{C}}$.

Example 1.10. The following is an example of a language in $\mathbf{\Sigma}^c_{\mathrm{C},1}$ (i.e. the compact version of $\mathbf{NP}_{\mathrm{C}}$).

Let $k(n,d) = \binom{n+d}{d}$ and identify $\mathbb{P}_{\mathrm{C}}^{(n+1)k(n,d)-1}$ with systems of $n+1$ polynomial equations in n variables of degree at most d. Let $S_{n,d} \subset \mathbb{P}_{\mathrm{C}}^{(n+1)k(n,d)-1}$ be defined by

$$S_{n,d} = \{(P_1:\ldots:P_{n+1}) \in \mathbb{P}_{\mathrm{C}}^{(n+1)k(n,d)-1} \mid \exists \mathbf{x} = (x_0:\cdots:x_n) \in \mathbb{P}^n_{\mathrm{C}} \text{ with } P^h_1(\mathbf{x}) = \cdots = P^h_{n+1}(\mathbf{x}) = 0\};$$

where P^h denotes the homogenization of a polynomial P (in degree d). In other words $S_{n,d}$ is the set of systems of $(n+1)$ polynomial equations of degree at most d, which have a zero in the complex projective space $\mathbb{P}^n_{\mathrm{C}}$. Then it is clear from the definition of the class $\mathbf{\Sigma}^c_{\mathrm{C},1}$ that for any fixed $d > 0$,

$$\left(S_{n,d} \subset \mathbb{P}_{\mathrm{C}}^{(n+1)k(n,d)-1}\right)_{n>0} \in \mathbf{\Sigma}^c_{\mathrm{C},1}.$$

Note that it is *not known* if for any fixed d

$$\left(S_{n,d} \subset \mathbb{P}_{\mathrm{C}}^{(n+1)k(n,d)-1}\right)_{n>0}$$

is $\mathbf{NP}_{\mathrm{C}}$-complete, while the non-compact version of this language i.e. the language consisting of systems of polynomials having a zero in $\mathbb{A}^n_{\mathrm{C}}$ (instead of $\mathbb{P}^n_{\mathrm{C}}$), has been shown to be $\mathbf{NP}_{\mathrm{C}}$-complete for $d \geq 2$ [2].

We define analogously the class $\mathbf{\Pi}^c_{\mathrm{C},\omega}$, and finally define:

Definition 1.11. The ***compact complex polynomial hierarchy*** is defined to be the union

$$\mathbf{PH}^c_{\mathrm{C}} \stackrel{\text{def}}{=} \bigcup_{\omega\geq 0}(\mathbf{\Sigma}^c_{\mathrm{C},\omega} \cup \mathbf{\Pi}^c_{\mathrm{C},\omega}) = \bigcup_{\omega\geq 0}\mathbf{\Sigma}^c_{\mathrm{C},\omega} = \bigcup_{\omega\geq 0}\mathbf{\Pi}^c_{\mathrm{C},\omega}.$$

Notice that the constructible subsets belonging to any language in $\mathbf{PH}^c_{\mathrm{C}}$ are all compact (in fact Zariski closed subsets of complex projective spaces). Also, note the inclusion

$$\mathbf{PH}^c_{\mathrm{C}} \subset \mathbf{PH}_{\mathrm{C}}.$$

1.2.2. *Complex Analogue of* $\#\mathbf{P}$. We now define the complex analogue of $\#\mathbf{P}$ (cf. the class $\#\mathbf{P}^{\dagger}_{\mathrm{R}}$ defined in [1] in the real case).

We first need a notation.

Notation 1.12. For any constructible subset $S \subset \mathrm{C}^k$ we denote by $b_i(S)$ the i-th Betti number (that is the rank of the singular homology group $\mathrm{H}_i(S) = \mathrm{H}_i(S,\mathbb{Z})$) of S.

We also let $P_S \in \mathbb{Z}[T]$ denote the ***Poincaré polynomial*** of S, namely

$$P_S(T) \overset{\mathrm{def}}{=} \sum_{i \geq 0} b_i(S)\, T^i. \tag{1.2}$$

Definition 1.13 (The class $\#\mathbf{P}^{\dagger}_{\mathrm{C}}$)**.** We say a sequence of functions

$$(f_n : \mathrm{C}^n \rightarrow \mathbb{Z}[T])_{n>0}$$

is in the class $\#\mathbf{P}^{\dagger}_{\mathrm{C}}$, if there exists a language

$$(S_n \subset \mathrm{C}^n)_{n>0} \in \mathbf{P}_{\mathrm{C}},$$

as well as a polynomial $m(n)$, such that

$$f_n(\mathbf{x}) = P_{S_{m+n,\mathbf{x}}}$$

for each $\mathbf{x} \in \mathrm{C}^n$, where $S_{m+n,\mathbf{x}} = S_{m+n} \cap \pi^{-1}(\mathbf{x})$ and $\pi : \mathrm{C}^{m+n} \rightarrow \mathrm{C}^n$ is the projection along the first m co-ordinates.

Remark 1.14. We make a few remarks about the class $\#\mathbf{P}^{\dagger}_{\mathrm{C}}$ defined above. First of all notice that the class $\#\mathbf{P}^{\dagger}_{\mathrm{C}}$ is quite robust. For instance, given two sequences $(f_n)_{n>0}, (g_n)_{n>0} \in \#\mathbf{P}^{\dagger}_{\mathrm{C}}$ it follows (by taking disjoint union of the corresponding constructible sets) that $(f_n + g_n)_{n>0} \in \#\mathbf{P}^{\dagger}_{\mathrm{C}}$, and also $(f_n g_n)_{n>0} \in \#\mathbf{P}^{\dagger}_{\mathrm{C}}$ (by taking Cartesian product of the corresponding constructible sets and using the multiplicative property of the Poincaré polynomials, which itself is a consequence of the Kunneth formula in homology theory.)

Remark 1.15. The connection between counting points of varieties and their Betti numbers is more direct over fields of positive characteristic via the zeta function. The zeta function of a variety defined over $\mathbb{F}_p$ is the exponential generating function of the sequence whose n-th term is the number of points in the variety over $\mathbb{F}_{p^n}$. The zeta function of such a variety turns out to be a rational function in one variable (a deep theorem of algebraic geometry first conjectured by Andre Weil [21] and proved by Dwork [9] and Deligne [7, 8]), and its numerator and denominator are products of polynomials whose degrees are the Betti numbers of the variety with respect to a certain (ℓ-adic) co-homology theory. The point of this remark is that the problems of "counting" varieties and computing their Betti numbers, are connected at a deeper level, and thus our choice of definition for a complex analogue of $\#\mathbf{P}$ is not altogether ad hoc.

Remark 1.16. A different definition of the class $\#P^{\dagger}_{\mathrm{C}}$ (more in line with previous work of Burgisser et al. [6]) would be obtained by replacing in Definition 1.13 the Poincaré polynomial, $P_S(T)$, by the Euler-Poincaré characteristic i.e. the value of P_S at $T = -1$. The Euler-Poincaré characteristic is additive (at least in the category of compact varieties), and thus has some attributes of being a discrete analogue of volume. But at the same time it should be noted that the Euler-Poincaré characteristic is a rather weak invariant – for instance, it does not determine the number of connected components of a given variety. Also notice that in the case of finite fields referred to in Remark 1.15, all the Betti numbers, not just their alternating sum, enter (as degrees of factors) in the rational expression for the zeta function of a variety. While it would certainly be a much stronger reduction result if one could obtain a Toda-type theorem using only the Euler-Poincaré characteristic instead of the whole Poincaré polynomial, it is at present unclear if such a theorem can be proven.

2. Statements of the main theorems

We can now state the main result of this paper.

Theorem 2.1 (Complex analogue of Toda's theorem)**.**

$$\mathbf{PH}^{\mathrm{c}}_{\mathrm{C}} \subset \mathbf{P}_{\mathrm{C}}^{\#\mathbf{P}^{\dagger}_{\mathrm{C}}}.$$

Remark 2.2. We leave it as an open problem to prove Theorem 2.1 with $\mathbf{PH}_{\mathrm{C}}$ instead of $\mathbf{PH}^{\mathrm{c}}_{\mathrm{C}}$ on the left hand side.

As a consequence of our method, we obtain a reduction (Theorem 2.5) that might be of independent interest. We first define the following two problems:

Definition 2.3 (Compact general decision problem with at most ω quantifier alternations ($\mathbf{GDP}^{\mathbf{c}}_{\mathrm{C},\omega}$))**.** The input and output for this problem are as follows.

- **Input.** A sentence Φ
$$(Q_1\mathbf{X}^1 \in \mathbb{P}^{k_1}_{\mathrm{C}}) \cdots (Q_\omega \mathbf{X}^\omega \in \mathbb{P}^{k_\omega}_{\mathrm{C}})\phi(\mathbf{X}^1;\ldots;\mathbf{X}^\omega),$$
where for each $i, 1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, with $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, and ϕ is a quantifier-free multi-homogeneous formula defining a *closed* subset S of $\mathbb{P}^{k_1} \times \cdots \times \mathbb{P}^{k_\omega}$.
- **Output.** True or False depending on whether Φ is true or false.

Definition 2.4 (Computing the Poincaré polynomial of constructible sets (***Poincaré***))**.** The input and output for this problem are as follows.

- **Input.** A quantifier-free formula defining a constructible subset $S \subset \mathrm{C}^k$.
- **Output.** The Poincaré polynomial $P_S(T)$.

Theorem 2.5. *For every $\omega > 0$, there is a deterministic polynomial time reduction in the Blum-Shub-Smale model of* $\mathbf{GDP}^{\mathbf{c}}_{\mathrm{C},\omega}$ *to* ***Poincaré****.*

2.1. **Outline of the main ideas and contributions.** The basic idea behind the proof of a real analogue of Toda's theorem in [1] is a topological construction, which given a semi-algebraic set $S \subset \mathrm{R}^{m+n}$, $p \geq 0$, and $\pi : \mathrm{R}^{m+n} \subset \mathrm{R}^n$ the projection along (say) the first m co-ordinates, constructs *efficiently* a semi-algebraic set, $D^p(S)$, such that

$$b_i(\pi(S)) = b_i(D^p(S)), \quad 0 \leq i < p. \tag{2.1}$$

Moreover, membership in $D^p(S)$ can be tested efficiently if the same is true for S. Note that this last property will not hold in general for the set $\pi(S)$ itself (unless of course $\mathbf{P}_{\mathrm{R}} = \mathbf{NP}_{\mathrm{R}}$).

The topological construction used in the definition of $D^p(X)$ in [1] is the iterated fibered join, $J^p_\pi(X)$, of a semi-algebraic set X with itself over a projection map π.

The fibers of the induced map $J_\pi(X) : J^p_\pi(X) \to \pi(X)$, over a point $y \in \pi(X)$, are then ordinary $(p+1)$-fold joins of the fiber $\pi^{-1}(y)$, and by connectivity properties of the join are p-connected. It is now possible using a version of the Vietoris-Beagle theorem that the map $J_\pi(X)$ is a p-equivalence (see [1] for the precise definition of p-equivalence). The main construction in [1] was to realize efficiently the fibered join $J^p_\pi(X)$ upto homotopy by a semi-algebraic set. This construction however is semi-algebraic in nature – i.e. it uses real inequalities in an essential way and thus does not generalize in a straightforward way to the complex case. Thus, a different construction is needed in the complex case.

In the complex case, the role of the fibered join is played by the *complex join fibered over a map* defined below (see Definition 3.12). The fibers of the $(p+1)$-fold complex join fibered over a projection π, $J^p_{\mathrm{C},\pi}(X)$, of a compact constructible set X are not quite p-connected as in the real case, but are reasonably nice – namely they are homologically equivalent to a projective space of dimension p (see Proposition 3.9). This allows us to relate the Poincaré polynomial of X with that of its image image $\pi(X)$, even though the relation is not as straightforward as in the real case (see Theorem 3.14 below).

We remark that Theorem 3.14 can be used to express directly the Betti numbers of the image under projection of a projective variety in terms of those another projective variety obtained directly without having to perform effective quantifier elimination (which has exponential complexity). The description of this second variety is *much simpler and algebraic* in nature compared to the one used in [1] in the real semi-algebraic case, and thus might be of independent interest. Theorem 3.14 can also be viewed as an improvement over the descent spectral sequence argument used in [10] to bound the Betti numbers of projections (of semi-algebraic sets). A similar construction using the projective join is also available in the real case (using $\mathbb{Z}/2\mathbb{Z}$ coefficients) but we omit its description in the current paper.

The rest of the paper is organized as follows. In Section 3 we state and prove the necessary ingredients from algebraic topology needed to prove the main theorems. In Section 4 we prove the main results of the paper.

3. Topological Ingredients

3.1. The complex join of constructible sets.

Let $X \subset \mathbb{P}^k_{\mathrm{C}}$ and $Y \subset \mathbb{P}^\ell_{\mathrm{C}}$ be two constructible sets defined by homogeneous formulas $\phi(X_0, \ldots, X_k)$ and $\psi(Y_0, \ldots, Y_\ell)$ respectively, where $(X_0 : \cdots : X_k)$ (respectively $(Y_0 : \cdots : Y_\ell)$) are homogeneous co-ordinates in $\mathbb{P}^k_{\mathrm{C}}$ (respectively $\mathbb{P}^\ell_{\mathrm{C}}$).

Definition 3.1 (Complex join)**.** The ***complex join***, $J_{\mathrm{C}}(X, Y)$, of X and Y is defined to be the constructible subset of $\mathbb{P}^{k+\ell+1}_{\mathrm{C}}$ defined by the formula

$$\phi(Z_0, \cdots, Z_k) \wedge \psi(Z_{k+1}, \cdots, Z_{k+\ell+1}),$$

where $(Z_0 : \cdots : Z_{k+\ell+1})$ are homogeneous coordinates in $\mathbb{P}^{k+\ell+1}_{\mathrm{C}}$.

Remark 3.2. Notice that $J_{\mathrm{C}}(X, Y)$ does not depend on the formulas ϕ and ψ used to define X and Y respectively.

Intuitively, if X and Y are both non-empty then $J_{\mathrm{C}}(X, Y)$ is obtained by joining each point of X with each point of Y by a complex projective line i.e. $\mathbb{P}^1_{\mathrm{C}}$.

Also, it is important to note that if X and Y are *both* empty then so is $J_{\mathrm{C}}(X, Y)$. Indeed, if $X = \emptyset$ then $J_{\mathrm{C}}(X, Y)$ is isomorphic to Y.

Example 3.3. It is easy to check from the above definition that the join, $J_{\mathbb{C}}(\mathbb{P}^k_{\mathbb{C}}, \mathbb{P}^\ell_{\mathbb{C}})$, of two projective spaces is again a projective space, namely $\mathbb{P}^{k+\ell+1}_{\mathbb{C}}$.

Remark 3.4. The projective join as defined above is a classical object in algebraic geometry. Amongst many other applications, the complex suspension of a projective variety X (i.e. the complex join $J_{\mathbb{C}}(X, \mathbb{P}^1_{\mathbb{C}})$) plays an important role in defining Lawson homology of projective varieties [11].

Definition 3.5. For $p > 0$, we denote by $J^p_{\mathbb{C}}(X)$ the $(p+1)$-fold iterated complex join of X with itself.

In other words

$$J^p_{\mathbb{C}} X = \underbrace{J_{\mathbb{C}}(J_{\mathbb{C}}(\cdots(J_{\mathbb{C}}(X))\cdots))}_{(p+1) \text{ times}}.$$

If $X \subset \mathbb{P}^k_{\mathbb{C}}$ is defined by a first-order homogeneous formula $\phi(X_0, \ldots, X_k)$, then $J^p_{\mathbb{C}}(X) \subset \mathbb{P}^{(p+1)(k+1)-1}_{\mathbb{C}}$ is defined by the homogeneous formula

$$J^p_{\mathbb{C}}(\phi)(X^0_0, \ldots, X^0_k, \ldots, X^p_0, \ldots, X^p_k) \overset{\text{def}}{=} \bigwedge_{i=0}^{p} \phi(X^i_0, \ldots, X^i_k).$$

where $(X^0_0 : \cdots : X^p_k)$ are homogeneous co-ordinates in $\mathbb{P}^{(p+1)(k+1)-1}_{\mathbb{C}}$.

Note that by Remark 3.2, if X is empty then $J^p_{\mathbb{C}}(X)$ is empty for every $p > 0$.

3.2. **Topological Join and its properties.** We also need to introduce the ***topological join*** of two spaces. The following is mostly taken from [1].

Definition 3.6. The join $X * Y$ of two topological spaces X and Y is defined by

$$X * Y \overset{\text{def}}{=} X \times Y \times \Delta^1 / \sim, \tag{3.1}$$

where

$$(x, y, t_0, t_1) \sim (x', y', t_0, t_1)$$

if $t_0 = 1, x = x'$ or $t_1 = 1, y = y'$.

Intuitively, $X * Y$ is obtained by joining each point of X with each point of Y by a unit interval.

We will need the fact that the iterated join of a topological space is highly connected. In order to make this statement precise we first define

Definition 3.7 (p-equivalence)**.** A map $f : A \to B$ between two topological spaces is called a ***p-equivalence*** if the induced homomorphism

$$f_* : \mathrm{H}_i(A) \to \mathrm{H}_i(B)$$

is an isomorphism for all $0 \leq i < p$, and an epimorphism for $i = p$, and we say that A is ***p-equivalent*** to B.

Theorem 3.8. *Let X be a compact semi-algebraic set. Then, the $(p+1)$-fold join $\underbrace{X * \cdots * X}_{(p+1) \text{ times}}$ is p-equivalent to a point.*

3.3. **Properties of the complex join.**

Proposition 3.9. *Let $X \subset \mathbb{P}^k_{\mathbb{C}}$ be a non-empty constructible subset and $p > 0$. Let*

$$i : J^p_{\mathbb{C}}(X) \hookrightarrow \mathbb{P}^{(p+1)(k+1)-1}_{\mathbb{C}}$$

denote the inclusion map. Then the induced homomorphism

$$i_* : \mathrm{H}_j(J^p_{\mathbb{C}} X) \to \mathrm{H}_j(\mathbb{P}^{(p+1)(k+1)-1}_{\mathbb{C}})$$

is an isomorphism for $0 \leq j < p$.

Before proving Proposition 3.9 we first fix some notation.

Notation 3.10. For any $k \geq 0$, we will denote by $\pi : \mathbb{C}^{k+1} \setminus \{0\} \to \mathbb{P}^k_{\mathbb{C}}$ the tautological line bundle over $\mathbb{P}^k_{\mathbb{C}}$, and by

$$\tilde{\pi} : \mathbf{S}^{2k+1} \to \mathbb{P}^k_{\mathbb{C}},$$

the ***Hopf fibration***, namely the restriction of π to the unit sphere in $\mathbb{C}^{k+1}$ defined by the equation $|z_1|^2 + \cdots + |z^{k+1}|^2 = 1$. Finally for any subset $S \subset \mathbb{P}^k_{\mathbb{C}}$, we will denote by $\widetilde{S}$ the subset $\tilde{\pi}^{-1}(S) \subset \mathbf{S}^{2k+1}$. Restricting the map $\tilde{\pi}$ to $\widetilde{S}$ we obtain the restriction of the Hopf fibration to the base S i.e. we have the following commutative diagram.

$$\begin{tikzcd}
\widetilde{S} \arrow[r, hook, "i"] \arrow[d, "\tilde{\pi}"] & \mathbf{S}^{2k+1} \arrow[d, "\tilde{\pi}"] \\
S \arrow[r, hook, "i"] & \mathbb{P}^k_{\mathbb{C}}
\end{tikzcd}$$

We need the following lemma.

Lemma 3.11. *Let $X \subset \mathbb{P}^k_{\mathbb{C}}, Y \subset \mathbb{P}^\ell_{\mathbb{C}}$ be constructible subsets. Then $J_{\mathbb{C}}\widetilde{(X, Y)} \subset \mathbf{S}^{2(k+\ell)+3}$ is homeomorphic to the (topological) join $\widetilde{X} * \widetilde{Y}$.*

Proof. Consider $\mathbf{x} \in X$ and $\mathbf{y} \in Y$ and the projective line $L \subset J(X, Y)$ joining $\mathbf{x}$ and $\mathbf{y}$. It is easy to see that the preimage $\tilde{L} = \tilde{\pi}^{-1}(L) \cong \mathbf{S}^3$ is a topological join of $\tilde{\pi}^{-1}(\mathbf{x})$ and $\tilde{\pi}^{-1}(\mathbf{y})$ (each homeomorphic to $\mathbf{S}^1$). Now since $\tilde{X}$ (resp. $\tilde{Y}$) is fibered by the various $\tilde{\pi}^{-1}(\mathbf{x})$ (resp. $\tilde{\pi}^{-1}(\mathbf{y})$), it follows that $J_{\mathbb{C}}\widetilde{(X, Y)}$ is homeomorphic to $\widetilde{X} * \widetilde{Y}$. □

Proof of Proposition 3.9. It follows from repeated applications of Lemma 3.11 that $\widetilde{J^p_{\mathbb{C}}(X)}$ is homeomorphic to

$$\underbrace{\widetilde{X} * \cdots * \widetilde{X}}_{(p+1) \text{ times}}.$$

We also have the commutative square

$$\begin{tikzcd}
\widetilde{J^p_{\mathbb{C}} X} \arrow[r, hook, "i"] \arrow[d, "\tilde{\pi}"] & \mathbf{S}^{2(p+1)(k+1)-1} \arrow[d, "\tilde{\pi}"] \\
J^p_{\mathbb{C}} X \arrow[r, hook, "i"] & \mathbb{P}^{(p+1)(k+1)-1}_{\mathbb{C}}
\end{tikzcd}$$

and a corresponding square

$$\begin{tikzcd}
\mathrm{H}_*(\widetilde{J^p_{\mathrm{C}}X}) \arrow[r, "i_*"] \arrow[d, "\tilde{\pi}_*"] & \mathrm{H}_*(\mathbf{S}^{2(p+1)(k+1)-1}) \arrow[d, "\tilde{\pi}_*"] \\
\mathrm{H}_*(J^p_{\mathrm{C}}X) \arrow[r, "i_*"] & \mathrm{H}_*(\mathbb{P}_{\mathrm{C}}^{(p+1)(k+1)-1})
\end{tikzcd}$$

of induced homomorphisms in the homology groups.

It follows from Theorem 3.8 that if $X \neq \emptyset$, then

$$\mathrm{H}_0(\widetilde{J^p_{\mathrm{C}}(X)}) \cong \mathbb{Z},$$
$$\mathrm{H}_i(\widetilde{J^p_{\mathrm{C}}X}) \cong 0, \quad 0 < i < p.$$

It is easy to see that for $p > 0$, $J^p_{\mathrm{C}}(X)$ is simply connected and hence $\widetilde{J^p_{\mathrm{C}}(X)}$ is a simple $\mathbf{S}^1$-bundle (i.e. a $\mathbf{S}^1$-bundle with a simply connected base) over $J^p_{\mathrm{C}}(X)$.

It now follows by a standard argument (which we expand below) involving the spectral sequence of the bundle $\tilde{\pi} : \widetilde{J^p_{\mathrm{C}}(X)} \to J^p_{\mathrm{C}}(X)$, that for $0 \leq i < p$,

$$\begin{aligned} \mathrm{H}_i(J^p_{\mathrm{C}}(X)) &\cong \mathbb{Z}, \text{ for } i \text{ even}, \\ \mathrm{H}_i(J^p_{\mathrm{C}}(X)) &\cong 0 \text{ for } i \text{ odd}. \end{aligned} \tag{3.2}$$

.

(The above claim also follows from the Gysin sequence of the $\mathbf{S}^1$-bundle $\tilde{\pi} : \widetilde{J^p_{\mathrm{C}}(X)} \to J^p_{\mathrm{C}}(X)$ but we give an independent proof below).

Consider the E_2-term of the (homological) spectral sequence of the bundle

$$\tilde{\pi} : \widetilde{J^p_{\mathrm{C}}(X)} \to J^p(X).$$

For $i, j \geq 0$, we have that

$$E_2^{i,j} = \mathrm{H}_i(J^p_{\mathrm{C}}(X)) \otimes \mathrm{H}_j(\mathbf{S}^1).$$

From this we deduce that

$$E_2^{i,0} = E_2^{i,1} = \mathrm{H}_i(J^p_{\mathrm{C}}(X)).$$

Also, from the fact that

$$\mathrm{H}_0(\widetilde{J^p_{\mathrm{C}}(X)}) = \mathbb{Z},$$

we get that

$$E_2^{0,0} = \mathbb{Z},$$

and hence,

$$E_2^{0,1} = \mathbb{Z}$$

as well. Moreover, we have that

$$E_3^{i,j} = E_4^{i,j} = \cdots = E_\infty^{i,j}$$

for all $i \geq 0$ and $j = 0, 1$. Now from the fact that the spectral sequence E_r converges to the homology of $\widetilde{J^p_{\mathrm{C}}(X)}$ we deduce that

$$\begin{aligned} E_3^{i,j} &= 0 \text{ for } 0 \leq i \leq p-1 \text{ and all } j, \\ E_3^{0,0} &= \mathbb{Z}. \end{aligned}$$

This implies that the differential

$$d_2 : E_2^{i,0} \to E_2^{i-2,1}$$

is an isomorphism for $1 \leq i \leq p-1$. Together with the fact that

$$E_2^{i,0} = E_2^{i,1} = \mathrm{H}_i(J^p_{\mathrm{C}}(X)),$$

this immediately implies (3.2). The proposition follows directly from this. □

3.4. **Complex join fibered over a map and its properties.** In our application we need the complex join fibered over certain maps.

Definition 3.12 (Complex join fibered over a map)**.** Let $A \subset \mathbb{P}^k_{\mathrm{C}} \times \mathbb{P}^\ell_{\mathrm{C}}$ be a constructible set defined by a first-order multi-homogeneous formula,

$$\phi(X_0, \ldots, X_k; Y_0, \ldots, Y_\ell)$$

and let $\pi_{\mathbf{Y}} : \mathbb{P}^k_{\mathrm{C}} \times \mathbb{P}^\ell_{\mathrm{C}} \to \mathbb{P}^k_{\mathrm{C}}$ be the projection along the $\mathbf{Y}$-co-ordinates.

For $p > 0$, the *p-fold complex join of A fibered over the map $\pi_{\mathbf{Y}}$*, $J^p_{\mathrm{C},\mathbf{Y}}(A) \subset \mathbb{P}^k_{\mathrm{C}} \times \mathbb{P}^{(\ell+1)(p+1)-1}_{\mathrm{C}}$, is defined by the formula

(3.3)

$$J^p_{\mathrm{C},\mathbf{Y}}(\phi)(X_0, \ldots, X_k; Y^0_0, \ldots, Y^0_\ell, \ldots, Y^p_0, \ldots, Y^p_\ell) \overset{\mathrm{def}}{=} \bigwedge_{i=0}^{p} \phi(X_0, \ldots, X_k; Y^i_0, \ldots, Y^i_\ell).$$

Remark 3.13. There is a natural induced map

$$J^p_{\mathrm{C},\mathbf{Y}} : J^p_{\mathrm{C},\mathbf{Y}}(A) \to \pi_Y(A)$$

sending $(x_0 : \cdots : x_k; y^0_0 : \cdots : y^p_\ell) \in J^p_{\mathrm{C},\mathbf{Y}}(A)$ to $(x_0 : \cdots : x_k) \in \pi_Y(A)$. It is easy to verify from Definition 3.12 that the map $J^p_{\mathrm{C},\mathbf{Y}}$ is well defined and is a surjection.

Now, let $A \subset \mathbb{P}^k_{\mathrm{C}} \times \mathbb{P}^\ell_{\mathrm{C}}$ be a constructible subset that is either open or closed, and let $\pi_{\mathbf{Y}} : \mathbb{P}^k_{\mathrm{C}} \times \mathbb{P}^\ell_{\mathrm{C}} \to \mathbb{P}^k_{\mathrm{C}}$ be the projection along the last co-ordinates.

The following theorem relates the Poincaré polynomial of $J^p_{\mathrm{C},\mathbf{Y}}(A)$ to that of the image $\pi_{\mathbf{Y}}(A)$.

Theorem 3.14. *For every $p \geq 0$, we have that*

$$P_{J^p_{\mathrm{C},\mathbf{Y}}(A)} = P_{\pi_{\mathbf{Y}}(A)} \cdot (1 - T^2)^{-1} \mod T^p. \tag{3.4}$$

Proof. We have the following commutative diagram.

$$\begin{tikzcd}
J^p_{\mathrm{C},\mathbf{Y}}(A) \arrow[r, hook, "i"] \arrow[d, "J^p_{\mathrm{C},\mathbf{Y}}"] & \pi_{\mathbf{Y}}(A) \times \mathbb{P}^{(p+1)(\ell+1)-1}_{\mathrm{C}} \arrow[d, "\pi_{\mathbf{Y}}"] \\
\pi_{\mathbf{Y}}(A) \arrow[r, "\mathrm{Id}"] & \pi_{\mathbf{Y}}(A)
\end{tikzcd}$$

The diagram above induces a morphism, $\phi^{i,j}_r : E^{i,j}_r \to {}'E^{i,j}_r$ between the (homological) Leray spectral sequences of the two vertical maps in the above diagram. Here, E_r (resp. ${}'E_r$) denotes the Leray spectral sequence of the map $J^p_{\mathrm{C},\mathbf{Y}} : J^p_{\mathrm{C},\mathbf{Y}}(A) \to \pi_{\mathbf{Y}}(A)$ (resp. $\pi_{\mathbf{Y}} : \pi_{\mathbf{Y}}(A) \times \mathbb{P}^{(p+1)(\ell+1)-1}_{\mathrm{C}} \to \pi_Y(A)$). The spectral sequence, ${}'E_r$, of the map $\pi_{\mathbf{Y}} : \pi_{\mathbf{Y}}(A) \times \mathbb{P}^{(p+1)(\ell+1)-1}_{\mathrm{C}} \to \pi_Y(A)$ degenerates at the ${}'E_2$-term where

$${}'E^{i,j}_2 = \mathrm{H}_i(\pi_{\mathbf{Y}}(A), \mathcal{H}_j(\mathbb{P}^{(p+1)(\ell+1)-1}_{\mathrm{C}})),$$

where $\mathrm{H}_i(\pi_{\mathbf{Y}}(A), \mathcal{H}_j(\mathbb{P}_{\mathrm{C}}^{(p+1)(\ell+1)-1}))$ denotes the i-th homology group of $\pi_{\mathbf{Y}}(A)$ with local coefficients taking values in the fibers $\mathrm{H}_j(\pi_Y^{-1}(\mathbf{x}))$, $\mathbf{x} \in \pi_{\mathbf{Y}}(A)$. Moreover, it follows from Proposition 3.9 that

$$\phi_2^{i,j} : E_2^{i,j} \to {}'E_2^{i,j}$$

are isomorphisms for $i+j < p$. Thus, $E_\infty^{i,j} = {}'E_\infty^{i,j}$ for $0 \leq i+j < p$. This implies that $\mathrm{H}_q(J^p_{\mathrm{C},\mathbf{Y}}(A)) \cong \mathrm{H}_q(\pi_{\mathbf{Y}}(A) \times \mathbb{P}_{\mathrm{C}}^{(p+1)(\ell+1)-1})$ for $0 \leq q < p$, and thus

$$P_{J^p_{\mathrm{C},\mathbf{Y}}(A)} = P_{\pi_{\mathbf{Y}}(A) \times \mathbb{P}_{\mathrm{C}}^{(p+1)(\ell+1)-1}} \mod T^p. \tag{3.5}$$

We also have that

$$\begin{aligned} P_{\pi_{\mathbf{Y}}(A) \times \mathbb{P}_{\mathrm{C}}^{(p+1)(\ell+1)-1}} &= P_{\pi_{\mathbf{Y}}(A)} \times P_{\mathbb{P}_{\mathrm{C}}^{(p+1)(\ell+1)-1}} \\ &= P_{\pi_{\mathbf{Y}}(A)} \times (1 + T^2 + \cdots + T^{2((p+1)(\ell+1)-1)}) \\ &= P_{\pi_{\mathbf{Y}}(A)} \times (1-T^2)^{-1} \mod T^p. \end{aligned} \tag{3.6}$$

The theorem follows from Eqns. (3.5) and (3.6). □

3.5. **Polynomial time membership testing in the complex join.**

We will use the following fact about the complex join over a projection introduced above.

Proposition 3.15 (Polynomial time membership testing)**.** *Suppose that the sequence of constructible sets $(S_n \subset \mathbb{P}_{\mathrm{C}}^{k(n)} \times \mathbb{P}_{\mathrm{C}}^{\ell(n)})_{n>0}$ in $\mathbf{P}_{\mathrm{C}}$, where for each $n > 0$, S_n is a closed (respectively open) constructible subset of $\mathbb{P}_{\mathrm{C}}^{k(n)} \times \mathbb{P}_{\mathrm{C}}^{\ell(n)}$ and $\mathbf{X}_n = (X_0 : \cdots : X_{k(n)})$ $\mathbf{Y}_n = (Y_0 : \cdots : Y_{\ell(n)})$ are homogeneous co-ordinates of $\mathbb{P}_{\mathrm{C}}^{k(n)}$ and $\mathbb{P}_{\mathrm{C}}^{\ell(n)}$ respectively. Let $p(n)$ be a polynomial. Then,*

$$\left(J^{p(n)}_{\mathrm{C},\mathbf{Y}_n}(S_n) \subset \mathbb{P}_{\mathrm{C}}^{k(n)} \times \mathbb{P}_{\mathrm{C}}^{(p(n)+1)(\ell(n)+1)-1}\right)_{n>0} \in \mathbf{P}_{\mathrm{C}}.$$

Proof. Obvious from the definition of $(J^{p(n)}_{\mathrm{C},\mathbf{Y}_n}(S_n))_{n>0}$. □

We now show how the formulas $J^p_{\mathrm{C},\mathbf{Y}}(\Phi)$ behave when the formula Φ involves quantified blocks of variables.

Lemma 3.16. *Suppose the first-order formula $\Phi(\mathbf{X}, \mathbf{Y})$ is of the form*

$$\Phi \overset{def}{=} (Q_1 \mathbf{Z}^1 \in \mathbb{P}_{\mathrm{C}}^{k_1})(Q_2 \mathbf{Z}^2 \in \mathbb{P}_{\mathrm{C}}^{k_2}) \ldots (Q_\omega \mathbf{Z}^\omega \in \mathbb{P}_{\mathrm{C}}^{k_\omega}) \Psi(\mathbf{X}; \mathbf{Y}; \mathbf{Z}^1; \cdots; \mathbf{Z}^\omega)$$

with $Q_i \in \{\exists, \forall\}$, and Ψ a quantifier-free first order multi-homogeneous formula.

Let $\pi_{\mathbf{Y}}$ denote the projection along the Y coordinates. Then, for each $p \geq 0$, the formula

$$J^p_{\mathrm{C},\mathbf{Y}}(\Phi)$$

is equivalent to the formula

$$\begin{gathered} \bar{J}^p_{\mathrm{C},\mathbf{Y}}(\Phi) \overset{def}{=} (Q_1 \mathbf{Z}^1 \in \mathbb{P}_{\mathrm{C}}^{k_1})(Q_2 \mathbf{Z}^2 \in \mathbb{P}_{\mathrm{C}}^{k_2}) \ldots (Q_\omega \mathbf{Z}^\omega \in \mathbb{P}_{\mathrm{C}}^{k_\omega}) \\ \Psi(\mathbf{X}; Y_0^0, \ldots, Y_\ell^p; \mathbf{Z}^1; \ldots; \mathbf{Z}^\omega). \end{gathered}$$

Proof. Obvious from the definition of $J^p_{\mathrm{C},\mathbf{Y}}(\Phi)$. □

3.6. **Alexander-Lefshetz duality.** We will also need the classical Alexander-Lefshetz duality theorem in order to relate the Betti numbers of a compact constructible subset K of $\mathbb{P}^n_{\mathbb{C}}$ to those of its complement, $\mathbb{P}^n_{\mathbb{C}} - K$.

Theorem 3.17 (Alexander-Lefshetz duality)**.** *Let $K \subset \mathbb{P}^n_{\mathbb{C}}$ be a closed constructible subset. Then for each odd i, $1 \leq i \leq 2n+1$, we have that*

$$b_{i-1}(K) - b_{i-2}(K) = b_{2n-i}(\mathbb{P}^n_{\mathbb{C}} - K) - b_{2n-i+1}(\mathbb{P}^n_{\mathbb{C}} - K) + 1. \tag{3.7}$$

Proof. Lefshetz duality theorem [17] gives for each $i, 0 \leq i \leq 2n$,

$$b_i(\mathbb{P}^n_{\mathbb{C}} - K) = b_{2n-i}(\mathbb{P}^n_{\mathbb{C}}, K).$$

The theorem now follows from the long exact sequence of homology,

$$\cdots \to \mathrm{H}_i(K) \to \mathrm{H}_i(\mathbb{P}^n_{\mathbb{C}}) \to \mathrm{H}_i(\mathbb{P}^n_{\mathbb{C}}, K) \to \mathrm{H}_{i-1}(K) \to \cdots$$

after noting that $\mathrm{H}_i(\mathbb{P}^n_{\mathbb{C}}) = 0$, for all $i \neq 0, 2, 4, \ldots, 2n$, and $\mathrm{H}_i(\mathbb{P}^n_{\mathbb{C}}) \cong \mathbb{Z}$, otherwise. □

For technical reasons (see Corollary 3.18 below) we need to consider the even and odd parts of the Poincaré polynomial of constructible sets.

Given $P = \sum_{i \geq 0} a_i T^i \in \mathbb{Z}[T]$, we write

$$P \overset{\text{def}}{=} P^{\text{even}}(T^2) + T P^{\text{odd}}(T^2),$$

where

$$P^{\text{even}}(T) = \sum_{i \geq 0} a_{2i} T^i,$$

and

$$P^{\text{odd}}(T) = \sum_{i \geq 0} a_{2i+1} T^i.$$

We also introduce for any $S \subset \mathbb{P}^n_{\mathbb{C}}$, a related polynomial, $Q_S(T)$, which we call the ***pseudo-Poincaré polynomial*** of S defined as follows.

$$Q_S(T) \overset{\text{def}}{=} \sum_{j \geq 0} (b_{2j}(S) - b_{2j-1}(S)) T^j. \tag{3.8}$$

In other words:

$$Q_S = P^{\text{even}}_S - T P^{\text{odd}}_S. \tag{3.9}$$

We have the following corollary of Theorem 3.17.

Corollary 3.18. *Let $A \subset \mathbb{P}^n_{\mathbb{C}}$ be an either open or closed constructible subset. Then,*

$$Q_A(T) = -T^n Q_{\mathbb{P}^n_{\mathbb{C}} - A}(\frac{1}{T}) + \sum_{i=0}^{n} T^i.$$

4. Proof of the main theorem

Notation 4.1. Let $\Phi(\mathbf{X})$ be a first-order multi-homogeneous formula with free variables $\mathbf{X} = (X_0 : \cdots : X_n)$. We let $\mathcal{R}(\Phi(\mathbf{X})) \subset \mathbb{P}^n_{\mathrm{C}}$ denote the *realization* of the formula Φ,

$$\mathcal{R}(\Phi(\mathbf{X})) = \{\mathbf{x} \in \mathbb{P}^n_{\mathrm{C}} \mid \Phi(\mathbf{x})\}.$$

We are now in a position to prove Theorem 2.1. The proof depends on the following key proposition.

(Note that we are going use Proposition 4.2 in the special case when the set of variables Y is empty).

Proposition 4.2. *Let $m(n), k_1(n), \ldots, k_\omega(n)$ be polynomials, and let*

$$(\Phi_n(\mathbf{X}, \mathbf{Y}))_{n>0}$$

be a sequence of multi-homogeneous formulas

$$\Phi_n(\mathbf{X}, \mathbf{Y}) \overset{def}{=} (Q_1 \mathbf{Z}^1 \in \mathbb{P}^{k_1}_{\mathrm{C}}) \cdots (Q_\omega \mathbf{Z}^\omega \in \mathbb{P}^{k_\omega}_{\mathrm{C}}) \phi_n(\mathbf{X}; \mathbf{Y}; \mathbf{Z}^1; \cdots ; \mathbf{Z}^\omega),$$

having free variables $(\mathbf{X}; \mathbf{Y}) = (X_0, \ldots, X_{k(n)}; Y_0, \ldots, Y_{m(n)})$, with

$$Q_1, \ldots, Q_\omega \in \{\exists, \forall\}, Q_i \neq Q_{i+1},$$

and ϕ_n a multi-homogeneous quantifier-free formula defining a closed (respectively open) constructible subset of

$$\mathbb{P}^k_{\mathrm{C}} \times \mathbb{P}^m_{\mathrm{C}} \times \mathbb{P}^{k_1}_{\mathrm{C}} \times \cdots \times \mathbb{P}^{k_\omega}_{\mathrm{C}}.$$

Suppose that

$$\left(\mathcal{R}(\phi_n(\mathbf{X}; \mathbf{Y}; \mathbf{Z}^1; \cdots ; \mathbf{Z}^\omega))\right)_{n>0} \in \mathbf{P}_{\mathrm{C}}.$$

Then, there exists blocks of homogeneous variables, $\mathbf{V}^1, \ldots, \mathbf{V}^\omega$, polynomially bounded $N_1, \ldots, N_\omega$, and a sequence of quantifier-free multi-homogeneous first order formulas

$$\left(\Theta_n(\mathbf{X}; \mathbf{Y}; \mathbf{V}^1; \cdots ; \mathbf{V}^\omega)\right)_{n>0}$$

such that for each $\mathbf{x} \in \mathbb{P}^{k(n)}_{\mathrm{C}}$, $\Theta_n(\mathbf{x}; \mathbf{Y}; \mathbf{V}^1; \cdots ; \mathbf{V}^\omega)$ describes a closed (respectively open) constructible subset T_n of $\mathbb{P}^m_{\mathrm{C}} \times \mathbb{P}^{N_1}_{\mathrm{C}} \times \cdots \times \mathbb{P}^{N_\omega}_{\mathrm{C}}$. To this sequence $(\Theta_n(\mathbf{X}; \mathbf{Y}; \mathbf{V}^1; \cdots ; \mathbf{V}^\omega))_{n>0}$, we can associate polynomial-time computable maps

$$F_n : \mathbb{Z}[T]_{\leq N} \to \mathbb{Z}[T]_{\leq m},$$

where $N = m + N_1 + \cdots + N_\omega$, such that the pseudo-Poincaré polynomials of the fibers over $\mathbf{x}$ verify

$$Q_{\mathcal{R}(\Phi_n(\mathbf{x}; \mathbf{Y}))} = F_n(Q_{\mathcal{R}(\Theta_n(\mathbf{x}; \mathbf{Y}; \mathbf{V}^1; \cdots ; \mathbf{V}^\omega))}).$$

Moreover,

$$\left(\mathcal{R}(\Theta_n(\mathbf{X}; \mathbf{Y}; \mathbf{V}^1; \cdots \ \mathbf{V}^\omega))\right)_{n>0} \in \mathbf{P}_{\mathrm{C}}.$$

Proof. The proof is by an induction on ω. We assume that the formula ϕ_n defines a closed constructible set. The open case can be handled analogously.

If $\omega = 0$ then we let $\Theta_n = \Phi_n$ and $N = m$, and F_n to be the identity map. Since there are no quantifiers, for each $n \geq 0$ the constructible set defined by Θ_n and Φ_n are the same, and thus the Betti numbers of the sets defined by Θ_n and Φ_n are equal.

If $\omega > 0$, we have the following two cases.

(A) Case 1, $Q_1 = \exists$: In this case consider the sequence of formulas $\bar{J}^{2m+1}_{\mathrm{C},\pi_{\mathbf{Z}^1}}(\Psi_n)$ (cf. Lemma 3.16), where Ψ_n is the following formula with free variables $\mathbf{X}, \mathbf{Y}, \mathbf{Z}^1$;

$$\Psi_n(\mathbf{X};\mathbf{Y};\mathbf{Z}^1) \overset{\mathrm{def}}{=} (Q_2\mathbf{Z}^2 \in \mathbb{P}^{k_2}_{\mathrm{C}}) \cdots (Q_\omega \mathbf{Z}^\omega \in \mathbb{P}^{k_\omega}_{\mathrm{C}}) \phi_n(\mathbf{X};\mathbf{Y};\mathbf{Z}^1;\cdots;\mathbf{Z}^\omega). \tag{4.1}$$

The formula $\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\Psi_n)$ is by definition equal to

$$(Q_2\mathbf{Z}^2 \in \mathbb{P}^{k_2}_{\mathrm{C}}) \cdots (Q_\omega \mathbf{Z}^\omega \in \mathbb{P}^{k_\omega}_{\mathrm{C}}) \phi_n(\mathbf{X};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1};\cdots;\mathbf{Z}^\omega).$$

Observe that the formula $\bar{J}^{2m+1}_{\mathrm{C},\pi_{\mathbf{Z}^1}}(\Psi_n)$ has one less quantifier alternation than the formula Φ_n.

We now apply the proposition inductively to obtain a sequence of formulas $(\Theta_n)_{n>0}$, and a sequence of polynomial time computable maps $(G_n)_{n>0}$. By inductive hypothesis we can suppose that we have for each $\mathbf{x} \in \mathbb{P}^{k(n)}_{\mathrm{C}}$

$$Q_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\Psi_n))} = G_n(Q_{\mathcal{R}(\Theta_n(\mathbf{x},\cdot))}).$$

Using Eqn. (3.4) we have that

$$\begin{aligned} P_{\mathcal{R}(\Phi_n(\mathbf{x},\mathbf{Y}))} &= P_{\pi_{\mathbf{Z}^1}(\mathcal{R}(\Psi_n(\mathbf{x};\mathbf{Y};\mathbf{Z}^1)))} \\ &= (1-T^2)P_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))} \mod T^{2m+1} \end{aligned}$$

and hence,

$$\begin{aligned} Q_{\mathcal{R}(\Phi_n(\mathbf{x},\mathbf{Y}))} &= Q_{\pi_{\mathbf{Z}^1}(\mathcal{R}(\Psi_n(\mathbf{x};\mathbf{Y};\mathbf{Z}^1)))} \\ &= ((1-T^2)P_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))})^{\mathrm{even}} - \\ &\quad T((1-T^2)P_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))})^{\mathrm{odd}} \mod T^{m+1} \end{aligned}$$

We set

$$F_n = \mathrm{Trunc}_m \circ G_n,$$

where Trunc_m is the operator that truncates a polynomial to one of degree at most m. This completes the induction in this case.

(B) Case 2, $Q_1 = \forall$: In this case consider the sequence of formulas $\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\neg\Psi_n)$ (cf. Lemma 3.16), where Ψ_n is defined as in the previous case (Eqn. (4.1)).

We now apply the proposition inductively as above to obtain a sequence $(\Theta_n)_{n>0}$, and maps $(G_n)_{n>0}$. By inductive hypothesis we can suppose that for each $\mathbf{x} \in \mathbb{P}^n_{\mathrm{C}}$ we have

$$Q_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\neg\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))} = G_n(Q_{\mathcal{R}(\Theta_n(\mathbf{x},\cdot))}).$$

By Eqn. 3.4

$$\begin{aligned} P_{\mathbb{P}^m_{\mathrm{C}} \setminus \mathcal{R}(\Phi_n(\mathbf{x};\mathbf{Y}))} &= P_{\pi_{\mathbf{Z}^1}(\mathcal{R}(\neg\Psi_n(\mathbf{x};\mathbf{Y};\mathbf{Z}^1)))} \\ &= (1-T^2)P_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\neg\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))} \mod T^{2m+1}. \end{aligned}$$

Hence,

$$\begin{aligned} Q_{\mathbb{P}^m_{\mathrm{C}} \setminus \mathcal{R}(\Phi_n(\mathbf{x};\mathbf{Y}))} &= Q_{\pi_{\mathbf{Z}^1}(\mathcal{R}(\neg\Psi_n(\mathbf{x};\mathbf{Y};\mathbf{Z}^1)))} \\ &= ((1-T^2)P_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\neg\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))})^{\mathrm{even}} - \\ &\quad T((1-T^2)P_{\mathcal{R}(\bar{J}^{2m+1}_{\mathrm{C},\mathbf{Z}^1}(\neg\Psi_n)(\mathbf{x};\mathbf{Y};\mathbf{Z}^{1,1},\ldots,\mathbf{Z}^{1,2m+1}))})^{\mathrm{odd}} \mod T^{m+1}. \end{aligned}$$

The set $K = \mathcal{R}(\Phi_n(\mathbf{x},\mathbf{Y}))$ is a constructible compact, so by Corollary 3.18 (corollary to Theorem 3.17), we have

$$Q_K(T) = -T^m \mathrm{Trunc}_m(Q_{\mathbb{P}^m_{\mathbb{C}}-K})(\frac{1}{T}) + \sum_{i=0}^{m} T^i.$$

We set F_n defined by

$$F_n(Q) = -T^m Q(\frac{1}{T}) + \sum_{i=0}^{m} T^i.$$

This completes the induction in this case as well.

□

Proof of Theorem 2.1. Follows immediately from Proposition 4.2 in the special case when the set of variables $\mathbf{Y}$ is empty. In this case the sequence of formulas $(\Phi_n)_{n>0}$ correspond to a language in the polynomial hierarchy and for each n, $\mathbf{x} = (x_0 : \cdots : x_{k(n)}) \in S_n \subset \mathbb{P}^{k(n)}_{\mathbb{C}}$ if and only if

$$F_n(Q_{\mathcal{R}(\Theta_n(\mathbf{x},\cdot))})(0) > 0$$

and this last condition can be checked in polynomial time with advice from the class $\#\mathbf{P}^{\dagger}_{\mathbb{C}}$. □

Remark 4.3. It is interesting to observe that in complete analogy with the proof of the classical Toda's theorem the proof of Theorem 2.1 also requires just one call to the oracle at the end.

Proof of Theorem 2.5. Follows from the proof of Proposition 4.2 since the formula Θ_n is clearly computable in polynomial time from the given formula Φ_n as long as the number of quantifier alternations ω is bounded by a constant. □

5. Acknowledgements

The author gratefully acknowledges discussions with James McClure, Donu Arapura and Andrei Gabrielov at various stages of this work.

References

1. S. Basu and T. Zell, *Polynomial hierarchy, Betti numbers, and a real analogue of Toda's Theorem*, Found. Comput. Math. **to appear** (2009).
2. L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and real computation*, Springer-Verlag, New York, 1998, With a foreword by Richard M. Karp. MR 99a:68070
3. L. Blum, M. Shub, and S. Smale, *On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines*, Bull. Amer. Math. Soc. (N.S.) **21** (1989), no. 1, 1–46. MR 90a:68022
4. P. Bürgisser and F. Cucker, *Variations by complexity theorists on three themes of Euler, Bézout, Betti, and Poincaré*, Complexity of computations and proofs (Jan Krajicek, ed.), Quad. Mat., vol. 13, Dept. Math., Seconda Univ. Napoli, Caserta, 2004, pp. 73–151. MR 2131406 (2006c:68053)
5. ______, *Counting complexity classes for numeric computations. II. Algebraic and semialgebraic sets*, J. Complexity **22** (2006), no. 2, 147–191. MR 2200367 (2007b:68059)
6. P. Bürgisser, F. Cucker, and M. Lotz, *Counting complexity classes for numeric computations. III. Complex projective sets*, Found. Comput. Math. **5** (2005), no. 4, 351–387. MR 2189543 (2006h:68039)

7. P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. MR 0340258 (49 #5013)
8. ______, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. (1980), no. 52, 137–252. MR 601520 (83c:14017)
9. B. Dwork, *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics **82** (1960), no. 3, 631–648.
10. A. Gabrielov, N. Vorobjov, and T. Zell, *Betti numbers of semialgebraic and sub-Pfaffian sets*, J. London Math. Soc. (2) **69** (2004), no. 1, 27–43. MR 2025325 (2004k:14105)
11. H. Blaine Lawson, Jr., *Algebraic cycles and homotopy theory*, Ann. of Math. (2) **129** (1989), no. 2, 253–291. MR 986794 (90h:14008)
12. K. Meer, *Counting problems over the reals*, Theoret. Comput. Sci. **242** (2000), no. 1-2, 41–58. MR 1769145 (2002g:68041)
13. C. Papadimitriou, *Computational complexity*, Addison-Wesley, 1994.
14. U. Schöning, *Probabilistic complexity classes and lowness*, J. Comput. System Sci. **39** (1989), no. 1, 84–100. MR 1013721 (91b:68041a)
15. Igor R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid. MR 1328833 (95m:14001)
16. M. Shub and S. Smale, *On the intractability of Hilbert's Nullstellensatz and an algebraic version of* "NP $\neq$ P*?"*, Duke Math. J. **81** (1995), no. 1, 47–54 (1996), A celebration of John F. Nash, Jr. MR 1381969 (97h:03067)
17. Edwin H. Spanier, *Algebraic topology*, McGraw-Hill Book Co., New York, 1966. MR 0210112 (35 #1007)
18. L. Stockmeyer, *The polynomial-time hierarchy*, Theoret. Comput. Sci. **3** (1976), no. 1, 1–22 (1977). MR 0438810 (55 #11716)
19. S. Toda, *PP is as hard as the polynomial-time hierarchy*, SIAM J. Comput. **20** (1991), no. 5, 865–877. MR 1115655 (93a:68047)
20. L. G. Valiant and V. V. Vazirani, *NP is as easy as detecting unique solutions*, Theoret. Comput. Sci. **47** (1986), no. 1, 85–93. MR 871466 (88i:68021)
21. A. Weil, *Number of solutions of equations over finite fields*, Bulletin of the American Mathematical Society **55** (1949), 497–508.

Department of Mathematics, Purdue University, West Lafayette, IN 47906, U.S.A.
E-mail address: sbasu@math.purdue.edu

ECCC ISSN 1433-8092
http://eccc.hpi-web.de