Available online at www.sciencedirect.com
SCIENCE DIRECT
C. R. Acad. Sci. Paris, Ser. I 339 (2004) 371–376
COMPTES RENDUS MATHEMATIQUE

Computer Science/Algebraic Geometry

The complexity to compute the Euler characteristic of complex varieties

Peter Bürgisser [a,1], Felipe Cucker [b,2], Martin Lotz [a,1]

[a] Institute of Mathematics, University of Paderborn, 33095 Paderborn, Germany
[b] Department of Mathematics, City University of Hong Kong, 83, Tat Chee Avenue, Kowloon, Hong Kong

Received 7 June 2004; accepted 14 June 2004

Available online 28 July 2004

Presented by Philippe G. Ciarlet

Abstract

We extend one of the main results of Bürgisser and Cucker (http://www.arxiv.org/abs/cs/cs.CC/0312007), which asserts that the computation of the Euler characteristic of a semialgebraic set is complete in the counting complexity class $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$. The goal is to prove a similar result over $\mathbb{C}$: the computation of the Euler characteristic of an affine or projective complex variety is complete in the class $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$. ***To cite this article: P. Bürgisser et al., C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Résumé

La complexité du calcul de la caractéristique d'Euler des variétés complexes. Dans cette Note, nous étendons un des résultats principaux de Bürgisser et Cucker (http://www.arxiv.org/abs/cs/cs.CC/0312007), qui établit que le calcul de la caractéristique d'Euler d'un ensemble semialgébrique est complet dans la classe de complexité de comptage $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$. Nous prouvons un résultat similaire sur $\mathbb{C}$: le calcul de la caractéristique d'Euler d'une variété algébrique (affine ou projective) est complet dans la classe $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$. ***Pour citer cet article : P. Bürgisser et al., C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Version française abrégée

L'objectif de cette Note est de prouver que le calcul de la caractéristique d'Euler d'une variété algébrique (affine ou projective) est complet dans la classe $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$.

Nous rapellons ici (cf. [3]) que $\#\mathrm{P}_{\mathbb{R}}$ désigne la classe des fonctions de $\mathbb{R}^\infty$, espace des suites finies de nombres réels, dans $\mathbb{N}\cup\{\infty\}$, et qui, en gros, comptent le nombre de témoins pour une entrée d'un problème de $\mathrm{NP}_{\mathbb{R}}$. Cette

E-mail addresses: pbuerg@upb.de (P. Bürgisser), macucker@math.cityu.edu.hk (F. Cucker), lotzm@upb.de (M. Lotz).
[1] Partially supported by DFG grant BU 1371.
[2] Partially supported by City University SRG grant 7001558.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.06.008

classe de fonctions étend au calcul sur les nombres réels la classe #P introduite par L. Valiant dans son article fondamental [9], dans lequel il prouve que le calcul du permanent est #P-complet. Nous rapelons aussi que $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$ est la classe des fonctions $f:\mathbb{R}^\infty \to \mathbb{R}^\infty$ calculables en temps polynomial avec des oracles fonctionnels dans $\#\mathrm{P}_{\mathbb{R}}$. Des telles définitions s'appliquent également sur $\mathbb{C}$.

Pour décrire nos résultats et les relier à des travaux antérieurs, nous considérons les problèmes suivants :

DEGREE (*Degré géométrique*) Etant donné un ensemble fini de polynômes complexes, calculer le degré géométrique de l'ensemble des zéros dans $\mathbb{C}^n$.

$\mathrm{EULER}_{\mathbb{C}}$ (*Caractéristique d'Euler de variétés affines*) Etant donné un ensemble fini de polynômes complexes, calculer la caractéristique d'Euler de l'ensemble des zéros dans $\mathbb{C}^n$.

$\mathrm{PROJEULER}_{\mathbb{C}}$ (*Caractéristique d'Euler des variétés projectives*) Etant donné un ensemble fini de polynômes complexes homogènes, calculer la caractéristique d'Euler de l'ensemble des zéros dans $\mathbb{P}^n$.

$\mathrm{EULER}_{\mathbb{R}}$ (*Caractéristique d'Euler*) Etant donné un ensemble semialgébrique par une réunion d'ensembles semialgébriques de base, décider s'il est vide ou non et calculer sa caractéristique d'Euler.

Les principaux résultats de [3] établissent que le problème DEGREE est $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$-complet et que le problème $\mathrm{EULER}_{\mathbb{R}}$ est $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$-complet. Le résultat principal de cette Note est le suivant.

Théorème 0.1. *Les problèmes* $\mathrm{EULER}_{\mathbb{C}}$ *et* $\mathrm{PROJEULER}_{\mathbb{C}}$ *sont* $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$*-complets pour des réductions de Turing.*

Lorsque les polynômes définissant la variété Z ont des coefficients tous entiers, le calcul de la caractéristique d'Euler $\chi(Z)$ peut être considéré dans le modèle de calculabilité de Turing. Le Théorème 0.1 a pour conséquence directe que les problèmes discrets correspondants sont complets dans la classe $\mathsf{FP}^{\mathsf{GCC}}$. Ici, FP désigne la classe des fonctions calculables par machine de Turing en temps polynomial et GCC est une classe de comptage de fonctions booléennes introduite dans [3].

Les démonstrations complètes sont données dans [4].

1. Introduction

This Note extends one of the main results in [3], which asserts that the computation of the Euler characteristic of a semialgebraic set is complete in the counting class $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$. We prove a similar result over $\mathbb{C}$, namely, that the computation of the Euler characteristic of an algebraic variety (affine or projective) is complete in the class $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$.

Here, we recall from [3] that $\#\mathrm{P}_{\mathbb{R}}$ denotes the class of functions from the space $\mathbb{R}^\infty$ of finite sequences of real numbers into $\mathbb{N} \cup \{\infty\}$ which, roughly speaking, count the number of satisfying witnesses for an input to a problem in $\mathrm{NP}_{\mathbb{R}}$. This class of functions extends to the setting of computations over $\mathbb{R}$ the class #P introduced by L. Valiant in his seminal paper [9], where he proved that the computation of the permanent is #P-complete. Also, the complexity class $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$ consists of all functions $f:\mathbb{R}^\infty \to \mathbb{R}^\infty$, which can be computed in polynomial time using oracle calls to functions in $\#\mathrm{P}_{\mathbb{R}}$. Similar definitions apply over $\mathbb{C}$.

The Euler characteristic of Z, denoted by $\chi(Z)$, can be characterized in several different ways. For instance, for spaces Z admitting a finite triangulation, it is the alternate sum of the number of i-simplices of the triangulation. In general, it is also the alternate sum over i of the Betti numbers of Z, that is, of the ranks of the homology groups $H_i(Z;\mathbb{Z})$. Also, for manifolds Z, $\chi(Z)$ can be characterized as the alternate sum over i of the number of critical points of index i of any Morse function $f:Z\to\mathbb{R}$. It is this last characterization, together with the elimination of generic quantifiers via partial witness sequences, that lies at the heart of the proof of completeness for the Euler characteristic given in [3]. Ultimately, this characterization reduces the problem of computing $\chi(Z)$ to that of counting points satisfying a certain property, and counting points is precisely what functions in $\#\mathrm{P}_{\mathbb{R}}$ are able to do.

If Z is now a complex (affine or projective) variety and we want to compute $\chi(Z)$ with machines over $\mathbb{C}$, the use of Morse functions as described above is not possible. This is due to the fact that machines over $\mathbb{C}$ cannot compute signs or recognize elements in $\mathbb{R}$. Therefore, to extend the completeness result of [3] to complex varieties requires yet another characterization of $\chi(Z)$, for a complex variety Z, which again reduces the computation of $\chi(Z)$ to counting points. Such a characterization was recently found by Aluffi [1].

To describe our results and to relate them to previous work, consider the following problems.

DEGREE (*Geometric degree*) Given a finite set of complex polynomials, compute the geometric degree of its affine zero set.

EULER$_{\mathbb{C}}$ (*Euler characteristic of affine varieties*) Given a finite set of complex polynomials, compute the Euler characteristic of its affine zero set.

PROJEULER$_{\mathbb{C}}$ (*Euler characteristic of projective varieties*) Given a finite set of complex homogeneous polynomials, compute the Euler characteristic of its projective zero set.

EULER$_{\mathbb{R}}$ (*Euler characteristic*) Given a semialgebraic set, decide whether it is empty and if not, compute its Euler characteristic.

The main results of [3] state that the problem DEGREE is $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$-complete and the problem EULER$_{\mathbb{R}}$ is $\mathrm{FP}_{\mathbb{R}}^{\#\mathrm{P}_{\mathbb{R}}}$-complete, both for Turing reductions. The main result of this Note is the following.

Theorem 1.1. *Both problems* EULER$_{\mathbb{C}}$ *and* PROJEULER$_{\mathbb{C}}$ *are* $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$*-complete for Turing reductions.*

If the polynomials defining the variety Z are restricted to have integer coefficients, then the problem of computing $\chi(Z)$ can be considered in the Turing model of computation. An easy consequence of Theorem 1.1 is the fact that the corresponding discrete problems are complete in the class $\mathsf{FP}^{\mathsf{GCC}}$. Here FP is the class of functions computed by Turing machines in polynomial time and GCC is a counting class of Boolean functions introduced in [3].

Complete proofs will be found in [4].

2. Preliminaries

2.1. Machines and complexity classes

We denote by $\mathbb{C}^\infty$ the disjoint union $\mathbb{C}^\infty = \bigsqcup_{n\geqslant 0}\mathbb{C}^n$, where for $n \geqslant 0$, $\mathbb{C}^n$ is the standard n-dimensional space over $\mathbb{C}$. The space $\mathbb{C}^\infty$ is a natural one to represent problem instances of arbitrarily high dimension. For $x \in \mathbb{C}^n \subset \mathbb{C}^\infty$, we call n the *size* of x.

In this Note we will consider Blum–Shub–Smale-machines over $\mathbb{C}$ as they are defined in [2]. Roughly speaking, such a machine takes an input from $\mathbb{C}^\infty$, performs a number of arithmetic operations and tests for zero following a finite list of instructions, and halts returning an element in $\mathbb{C}^\infty$ (or loops forever). The computation of a machine on an input $x \in \mathbb{C}^\infty$ is well-defined and notions such as a function being computed by a machine or a subset of $\mathbb{C}^\infty$ being decided by a machine easily follow. We denote by $\mathrm{FP}_{\mathbb{C}}$ the class of functions that can be computed in polynomial time.

2.2. Projective algebraic varieties

We denote by $\mathbb{P}^n := \mathbb{P}^n(\mathbb{C})$ the *projective space* of dimension n over $\mathbb{C}$. A *projective variety* is defined as the zero set $\mathcal{Z}(f_1,\dots,f_r) := \{x \in \mathbb{P}^n \mid f_1(x) = 0,\dots,f_r(x) = 0\}$ of finitely many homogeneous polynomials $f_1,\dots,f_r \in \mathbb{C}[X_0,\dots,X_n]$. Boolean combinations of projective varieties are called *quasialgebraic sets*.

For $0 \leqslant k \leqslant n$ the *Grassmannian* $\mathbb{G}(k,n)$ is the set of all $(k+1)$-dimensional vector subspaces of $\mathbb{C}^{n+1}$. Elements in $\mathbb{G}(k,n)$ are in bijective correspondence with subspaces $\mathbb{P}^k \subseteq \mathbb{P}^n$. We will often write L^{n-k} for an element in $\mathbb{G}(k,n)$, the superscript emphasizing the codimension.

We will consider projective varieties as input data for machines over $\mathbb{C}$. In this case, a variety Z is encoded by a family of polynomials of which Z is the zero set. Our results are valid for both the dense and sparse encoding of polynomials.

2.3. Counting complexity classes

We now recall the definition of counting classes over $\mathbb{C}$ in [3]. This definition follows the lines used in discrete complexity theory to define #P [9].

Definition 2.1. (i) We say that a function $f:\mathbb{C}^\infty \to \mathbb{N}\cup\{\infty\}$ belongs to the class $\#\mathrm{P}_\mathbb{C}$ when there exists a machine M working in polynomial time and a polynomial p such that, for all $x \in \mathbb{C}^n$, $f(x) = |\{y \in \mathbb{C}^{p(n)} \mid M \text{ accepts } (x,y)\}|$. The complexity class $\mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$ consists of all functions $f:\mathbb{C}^\infty \to \mathbb{C}^\infty$, which can be computed in polynomial time using oracle calls to functions in $\#\mathrm{P}_\mathbb{C}$. (ii) We say that f *Turing reduces to* g when there exists an oracle machine which, with oracle g, computes f in polynomial time. (iii) We say that a function g is *Turing-hard* for $\mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$ when, for every $f \in \mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$, there is a Turing reduction from f to g. We say that g is $\mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$*-complete* when, in addition, $g \in \mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$.

An example of a problem in $\#\mathrm{P}_\mathbb{C}$ is the following:

$\#\mathrm{BIPROJQAS}_\mathbb{C}$ (*Counting points in biprojective quasialgebraic sets*) Given a quasialgebraic set $S \subseteq \mathbb{P}^n \times \mathbb{P}^n$, count the number of points in S returning ∞ if this number is not finite.

2.4. Projective degrees

Let $f_0,\ldots,f_n \in \mathbb{C}[X_0,\ldots,X_n]$ be homogeneous nonzero polynomials of the same degree d and let $\Sigma := \mathcal{Z}(f_0,\ldots,f_n)$ denote their projective zero set. Then these polynomials define a *regular morphism* $\varphi:U\to\mathbb{P}^n$, $(x_0:\cdots:x_n)\mapsto(f_0(x):\cdots:f_n(x))$ on the domain of definition $U := \mathbb{P}^n\setminus\Sigma$. We will call such φ a *rational morphism* and sometimes write shortly $\varphi:\mathbb{P}^n \dashrightarrow \mathbb{P}^n$. Let $\Gamma_U \subseteq \mathbb{P}^n\times\mathbb{P}^n$ denote the graph of φ and let Γ denote the closure of Γ_U in the Zariski topology. It is easy to see that $\Gamma = \Gamma_U \cup \Gamma_\Sigma$, where Γ_Σ is the inverse image of Σ under the projection $\pi_1:\Gamma\to\mathbb{P}^n$ onto the first factor.

Consider $L^i \in \mathbb{G}(n-i,n)$ and $L^{n-i}\in\mathbb{G}(i,n)$ in the Grassmannians. Since $\dim\Gamma = n$, for generic (L^i,L^{n-i}) the intersection $\Gamma\cap(L^i\times L^{n-i})$ is finite and we may wonder under which conditions the number of points in this intersection does not depend on (L^i,L^{n-i}). The next proposition gives an answer and leads to the concept of projective degrees.

Proposition 2.2. *Let $\varphi:\mathbb{P}^n \dashrightarrow \mathbb{P}^n$ be a rational morphism defined on U and let Γ be the closure of the graph of φ.* (i) *For $0\leqslant i<n$ there exists a nonnegative integer d_i such that, if $\Gamma_U \pitchfork (L^i\times L^{n-i})$ and $\Gamma_\Sigma\cap(L^i\times L^{n-i})=\emptyset$, then $|\Gamma_U\cap(L^i\times L^{n-i})| = |L^i\cap\varphi^{-1}(L^{n-i})| = d_i$. Here $U\pitchfork V$ means that U and V intersect transversally.* (ii) *The above conditions are satisfied for generic $(L^i,L^{n-i})\in\mathbb{G}(n-i,n)\times\mathbb{G}(i,n)$.*

The integers $d_0,\ldots,d_{n-1}$ are called the *projective degrees* of the rational morphism φ (see [6, Chapter 19]).

2.5. Euler characteristic

The Euler characteristic satisfies an additivity property expressed in the following principle of inclusion and exclusion.

Lemma 2.3. *Let $Z_1,\ldots,Z_r$ be complex quasialgebraic sets. Write $Z_I := \bigcup_{i\in I} Z_i$ for an index set $I\subseteq\{1,\ldots,r\}$. Then we have $\chi(Z_1\cap\cdots\cap Z_r) = \sum_{I\neq\emptyset}(-1)^{|I|-1}\chi(Z_I)$.*

For a smooth irreducible hypersurface $\subset \mathbb{P}^n$ of degree d, the Euler characteristic can be expressed by the known formula $\chi(Z) = ((1-d)^{n+1} - 1)d^{-1} + n + 1$ (cf. [5]). The following generalizes this to the case of possibly singular hypersurfaces.

Theorem 2.4 (Aluffi [1]). *Let $f \in \mathbb{C}[X_0, \ldots, X_n]$ be a nonconstant homogeneous polynomial and let $\Sigma := \mathcal{Z}_{\mathbb{P}^n}(\partial_0 f, \ldots, \partial_n f)$. Then the Euler characteristic of the projective hypersurface $Z = \mathcal{Z}(f)$ satisfies $\chi(Z) = n + \sum_{i=1}^{n}(-1)^{i-1} d_{n-i}$, where $d_0, \ldots, d_{n-1}$ are the projective degrees of the gradient morphism $\mathbb{P}^n \setminus \Sigma \to \mathbb{P}^n$, $x = (x_0 : \cdots : x_n) \mapsto (\partial_0 f(x) : \cdots : \partial_n f(x))$.*

2.6. Generic quantifiers and partial witness sequences

Several completeness results in the Blum–Shub–Smale-model rely on Koiran's method to eliminate generic quantifiers in parametrized formulas [7].

We denote by $\mathcal{F}_{\mathbb{R}}$ the set of first order formulas over the language of the theory of ordered fields with constant symbols for real numbers. Let $F \in \mathcal{F}_{\mathbb{R}}$ have free variables $a_1, \ldots, a_k$. We say that F is *Zariski-generically true* if the set of values $a \in \mathbb{R}^k$ not satisfying $F(a)$ has dimension strictly less than k. We express this fact by writing $\forall^* a\, F(a)$ using the *generic universal quantifier* $\forall^*$.

Definition 2.5. Let $F(u, a) \in \mathcal{F}_{\mathbb{R}}$ with free variables $u \in \mathbb{R}^{2m}$ and $a \in \mathbb{R}^k$. A sequence $\alpha = (\alpha^{(1)}, \ldots, \alpha^{(4m+1)})$ of points in $\mathbb{R}^k$ is called a *partial witness sequence* for F iff $\forall u \in \mathbb{R}^{2m}\ ((\forall^* a \in \mathbb{R}^k\ F(u, a)) \Rightarrow |\{i \in \{1, \ldots, 4m+1\} \mid F(u, \alpha^{(i)})\}| > 2m)$.

The next result, Theorem 2.7 below, summarizes the main properties of partial witness sequences that we will need in this paper. The proof relies on efficient quantifier elimination over $\mathbb{R}$ (cf. [8]).

Definition 2.6. Let $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$. We say that R is *definable by short enough formulas* when there exists a polynomial p such that, for all $m \in \mathbb{N}$, (i) $\forall u \in \mathbb{C}^m\ \forall a \in \mathbb{C}^\infty\ (R(u, a) \Rightarrow |a| \leqslant p(m))$, (ii) the predicate $(u, a) \in R \cap (\mathbb{C}^m \times \mathbb{C}^{p(m)})$ can be expressed by a formula $F_m(u, a)$ in the language $\mathcal{F}_{\mathbb{R}}$ that has $m^{O(1)}$ bounded variables, a bounded number of quantifier blocks, and $2^{m^{O(1)}}$ atomic predicates containing integer polynomials with degree and bit size at most $2^{m^{O(1)}}$.

Note that the definition above requires the formula $F_m(u, a)$ to be in the language $\mathcal{F}_{\mathbb{R}}$ of the theory of ordered fields and not in the language of the theory of fields. The points $u \in \mathbb{C}^m$ and $a \in \mathbb{C}^{p(m)}$ are represented by points in $\mathbb{R}^{2m}$ and $\mathbb{R}^{2p(m)}$ in the obvious way.

Theorem 2.7. *Let $R \subseteq \mathbb{C}^\infty \times \mathbb{C}^\infty$ be a relation definable by short enough formulas with associated p and $\{F_m(u, a)\}_{m \in \mathbb{N}}$. Then there is a constant-free machine over $\mathbb{C}$ which computes on input $m \in \mathbb{N}$ a partial witness sequence α_m for $F_m(u, a)$ in time polynomial in m.*

3. Outline of the proof of Theorem 1.1

We need to study the following auxiliary problem:

PROJDEGREE$_{\mathbb{C}}$ (*Projective degrees*) Given homogeneous polynomials $f_0, \ldots, f_n$ in $\mathbb{C}[X_0, \ldots, X_n]$ of the same degree and $i \in \mathbb{N}$, $0 \leqslant i < n$, compute the ith projective degree d_i of the rational map $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ defined by them.

Proposition 3.1. *The problem* PROJDEGREE$_{\mathbb{C}}$ *is in* $\mathrm{FP}_{\mathbb{C}}^{\#\mathrm{P}_{\mathbb{C}}}$.

Idea of the proof. Let $u \in \mathbb{C}^m$ be a vector parameterizing the homogeneous polynomials $f_0, \ldots, f_n$ and let $\Gamma^u =$

$\Gamma_U^u \cup \Gamma_\Sigma^u \subseteq \mathbb{P}^n \times \mathbb{P}^n$ be the graph associated to $f_0, \ldots, f_n$. Also, to a point $a \in \mathbb{C}^{i(n+1)}$ (seen as a matrix with i rows and $n+1$ columns), we associate the linear space $L_a := \{x \in \mathbb{C}^{n+1} \mid ax = 0\}$. For generic a, $\dim L_a = n + 1 - i$, that is, $L_a \in \mathbb{G}(n-i, n)$. Similarly we define L_b^{n-i} for $b \in \mathbb{C}^{(n-i)(n+1)}$.

We use the following lemma.

Lemma 3.2. *For all $i, n \in \mathbb{N}$, $0 \leqslant i < n$, there is a family of short enough formulas $\{F_m^{(i,n)}(u, a, b)\}_{m\in\mathbb{N}}$ such that, for all $m \in \mathbb{N}$ and all $u \in \mathbb{C}^m$, we have: $\forall (a, b) \in \mathbb{C}^{i(n+1)} \times \mathbb{C}^{(n-i)(n+1)}$ $(F_m^{(i,n)}(u, a, b)) \Leftrightarrow (\Gamma_\Sigma^u \cap (L_a^i \times L_b^{n-i}) = \emptyset \wedge \Gamma_U^u \pitchfork (L_a^i \times L_b^{n-i}))$.*

To prove Proposition 3.1 it is enough to see that ProjDegree$_\mathbb{C}$ Turing reduces to #BiProjQAS$_\mathbb{C}$, i.e., to give a polynomial time algorithm solving ProjDegree$_\mathbb{C}$ with oracle #BiProjQAS$_\mathbb{C}$. The algorithm doing so, with input $u \in \mathbb{C}^m$, computes a description of Γ_U^u and then computes a partial witness sequence (α_m, β_m) for the formula $F_m^{(i,n)}(u, a, b)$ in Lemma 3.2 (use Theorem 2.7). Then, it computes the values $d_i^{(j)} = |\Gamma_U^u \cap (L^i_{\alpha_m^{(j)}} \times L^{n-i}_{\beta_m^{(j)}})|$ for $j = 1, \ldots, 4m+1$ with queries to #BiProjQAS$_\mathbb{C}$, and returns d_i, the winner of a majority vote on $d_i^{(1)}, \ldots, d_i^{(4m+1)}$. □

Idea of the proof of Theorem 1.1. If Z is a projective hypersurface, the membership ProjEuler$_\mathbb{C} \in \mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$ follows readily from Proposition 3.1 and Theorem 2.4.

For the general case, we use Lemma 2.3 to reduce the computation of $\chi(Z)$ to the case of a hypersurface. Note, however, that the addition in Lemma 2.3 involves exponentially many terms. This difficulty can be overcome by passing the cost of this addition to the oracle. The details are in [4].

To prove the membership Euler$_\mathbb{C} \in \mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$ one reduces Euler$_\mathbb{C}$ to ProjEuler$_\mathbb{C}$. This is done by embedding $Z \subseteq \mathbb{C}^n$ into $Z_h \subseteq \mathbb{P}^n$ (described by the homogenization of the equations which describe Z), using that $\chi(Z) = \chi(Z_h) - \chi(Z_h \setminus Z)$ and noting that $Z_h \setminus Z \subseteq \mathbb{P}^{n-1}$.

To prove the $\mathrm{FP}_\mathbb{C}^{\#\mathrm{P}_\mathbb{C}}$-hardness of ProjEuler$_\mathbb{C}$ and Euler$_\mathbb{C}$ it is enough to do so for the latter (since, we just argued, the latter reduces to the former). To do so, we establish a Turing reduction from Degree to Euler$_\mathbb{C}$. The idea for this reductions is that for a sequence of generic affine subspaces $A_0, A_1, \ldots, A_n$ of $\mathbb{C}^n$ such that $\dim A_i = i$, we have $A_i \cap Z_u = \emptyset$ for $i < k$ as well as $A_k \pitchfork Z_u \neq \emptyset$ and $\chi(A_k \cap Z_u) = |A_k \cap Z_u| = \deg Z_u$. One thus computes $\deg Z$ to be the first nonzero element of the sequence $(\chi(Z_u \cap A_0), \ldots, \chi(Z_u \cap A_n))$ if this is not the zero sequence; otherwise we put $\deg Z = 0$. Genericity is dealt with partial witness sequences, similarly as in the proof of Proposition 3.1. □

Acknowledgements

We are grateful to J. von zur Gathen for pointing out to us Aluffi's article [1].

References

[1] P. Aluffi, Computing characteristic classes of projective schemes, J. Symbolic Comput. 35 (1) (2003) 3–19.
[2] L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and Real Computation, Springer-Verlag, New York, 1998.
[3] P. Bürgisser, F. Cucker, Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets, in: Proc. 36th Ann. ACM STOC, 2004. Full version in http://www.arxiv.org/abs/cs/cs.CC/0312007.
[4] P. Bürgisser, F. Cucker, M. Lotz, Counting complexity classes for numeric computations III: Complex projective sets. Full version in http://math-www.upb.de/agpb, 2004, in preparation.
[5] A. Dimca, Singularities and Topology of Hypersurfaces, Universitext, Springer-Verlag, 1992.
[6] J. Harris, Algebraic Geometry, Graduate Texts in Math., vol. 133, Springer-Verlag, New York, 1995.
[7] P. Koiran, Randomized and deterministic algorithms for the dimension of algebraic varieties, in: Proc. 38th FOCS, 1997, pp. 36–45.
[8] J. Renegar, On the computational complexity and geometry of the first-order theory of the reals. Part I, II, III, J. Symbolic Comput. 13 (3) (1992) 255–352.
[9] L.G. Valiant, The complexity of computing the permanent, Theoret. Comput. Sci. 8 (1979) 189–201.