Journal of Complexity 27 (2011) 151–187

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

Lower complexity bounds for interpolation algorithms

Nardo Giménez [a], Joos Heintz [b,c,*], Guillermo Matera [d], Pablo Solernó [e]

[a] *Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina*

[b] *Departamento de Computación, Universidad de Buenos Aires and CONICET, Ciudad Universitaria, Pab.I, 1428 Ciudad Autónoma de Buenos Aires, Argentina*

[c] *Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, 39071 Santander, Spain*

[d] *Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento and CONICET, J.M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Buenos Aires, Argentina*

[e] *Departamento de Matemática, Universidad de Buenos Aires and CONICET, Ciudad Universitaria, Pab.I, 1428 Ciudad Autónoma de Buenos Aires, Argentina*

ARTICLE INFO

Article history:
Received 3 July 2010
Accepted 7 October 2010
Available online 17 October 2010

Dedicated to Francisco Marcellán.

Keywords:
Hermite–Lagrange interpolation
Interpolation problem
Interpolation algorithm
Lower complexity bound
Constructible map
Geometrically robust map

ABSTRACT

We introduce and discuss a new computational model for the Hermite–Lagrange interpolation with nonlinear classes of polynomial interpolants. We distinguish between an interpolation problem and an algorithm that solves it. Our model includes also coalescence phenomena and captures a large variety of known Hermite–Lagrange interpolation problems and algorithms. Like in traditional Hermite–Lagrange interpolation, our model is based on the execution of arithmetic operations (including divisions) in the field where the data (nodes and values) are interpreted and arithmetic operations are counted at unit cost. This leads us to a new view of rational functions and maps defined on arbitrary constructible subsets of complex affine spaces. For this purpose we have to develop new tools in algebraic geometry which themselves are mainly based on Zariski's Main Theorem and the theory of places (or equivalently: valuations). We finish this paper by exhibiting two examples of Lagrange interpolation problems with nonlinear classes of interpolants, which do not admit efficient interpolation algorithms (one of these interpolation problems requires even an exponential quantity of arithmetic

* Corresponding author at: Departamento de Computación, Universidad de Buenos Aires and CONICET, Ciudad Universitaria, Pab.I, 1428 Ciudad Autónoma de Buenos Aires, Argentina.

E-mail addresses: nardogimenez@yahoo.com.ar (N. Giménez), joos@dc.uba.ar (J. Heintz), gmatera@ungs.edu.ar (G. Matera), psolerno@dm.uba.ar (P. Solernó).

0885-064X/$ – see front matter
doi:10.1016/j.jco.2010.10.003

operations in terms of the number of the given nodes in order to represent some of the interpolants).

In other words, classic Lagrange interpolation algorithms are asymptotically optimal for the solution of these selected interpolation problems and nothing is gained by allowing interpolation algorithms and classes of interpolants to be nonlinear. We show also that classic Lagrange interpolation algorithms are almost optimal for generic nodes and values. This generic data cannot be substantially compressed by using nonlinear techniques.

We finish this paper highlighting the close connection of our complexity results in Hermite–Lagrange interpolation with a modern trend in software engineering: architecture tradeoff analysis methods (ATAM).

1. Introduction

This paper discusses complexity issues of well-known problems of (mainly multivariate) polynomial interpolation from a systematic nonlinear point of view. Instead of analyzing the run-time behavior of concrete interpolation algorithms, we ask what are the best possible complexity bounds we can hope for when we have freedom to chose the data structures and types which represent the interpolants. This question leads in a natural way to the consideration of classes of interpolants which do not form linear spaces, but more general geometric structures, as e.g. algebraic varieties.

A universal framework for the *mathematical* aspects of interpolation is developed in [10, Section 2]. Here we are concerned with the *algorithmic*, and in particular with the *computational complexity* aspects of interpolation problems and procedures. Therefore we have to deal not only with structural concepts like functionals and interpolants, but also with the (possible) data structures and types which represent them. Although our algorithmic view may be combined with the general framework for interpolation of [10], the outcome would be a rather clumsy formalism, difficult or impossible to decipher for the non-specialist, and hiding instead of unveiling the ideas behind our argumentation. Therefore we focus our attention on Hermite–Lagrange interpolation problems and algorithms. Our interpolants will always be multivariate polynomials over the complex numbers $\mathbb{C}$. This turns structural mathematical formulations much simpler and the context is better known to non-specialists than the general model of interpolation introduced in [10].

Classical interpolation algorithms return the interpolating polynomials in dense or sparse representation and the (finite) dimension of the vector space where they live becomes then a lower bound for the complexity of these procedures. In this paper we address the question of the intrinsic complexity of Hermite–Lagrange interpolation algorithms admitting more general representations of the interpolants, e.g., their straight-line program encoding.

A general feature of interpolation problems and algorithms consists of the identity of *input object* and *input representation* (see [9] for a motivation and a mathematical discussion of the distinction of these concepts). In Hermite–Lagrange interpolation, input object and representation are always given by a finite list of nodes and the corresponding function values. This setting will be maintained through this paper. However we shall admit more freedom as usual in the representation of the *output objects*, i.e., the interpolants, which always will be polynomials of bounded degree, that however may become exponential in the number of nodes.

We shall make a substantial use of the identity of input object and input representation in order to establish a general mathematical model for the intuitive meaning of the Hermite–Lagrange interpolation problem and algorithm with polynomial interpolants (see the discussion in Section 3.1 and Definition 7).

In Section 4 we motivate by geometric arguments a notion of coalescence for interpolation algorithms (and problems) which will become fundamental in this paper: geometric robustness.

Our mathematical model for Hermite–Lagrange interpolation has a direct translation to fundamental concepts of software engineering. In Appendix A we establish a dictionary which

identifies the components of our model with current classical notions of software architecture. Geometric robustness turns out to be a non-functional requirement on the routine which represents an interpolation algorithm.

The remaining results we are going to present in this paper all have a negative flavor. One might hope that nonlinear data structures and algorithmic techniques could help to improve the complexity of interpolation procedures. However, nonlinearity is not a panacea for everything. In this spirit we shall exhibit in Section 5 two families of natural Hermite–Lagrange interpolation problems which under a suitable coalescence restriction (called "geometrical robustness") require for their algorithmic solution procedures of intrinsically high complexity, even if we admit nonlinear interpolation techniques (see Proposition 22 for an incompressibility result and Theorem 23 for an exponential lower bound for the output size). It is not very hard to prove, but worth to state, that nonlinear techniques are not able to compress the output size when they are applied to the usual context of Lagrange interpolation of generic input data (see Proposition 21).

In conclusion, the main outcome of the paper is twofold. On the one hand, we establish a general mathematical model for Hermite–Lagrange interpolation. The components of this model may be identified with basic concepts of software engineering. In this sense, our model seems to be "natural", since it is reflected by the contemporary thinking on programming. On the other hand, we show that a non-functional requirement that is well-motivated by interpolation theory and numerical analysis, namely geometric robustness, may produce an exponential blow up of another quality attribute of the procedure, namely the computational complexity. We do not know of any other example in software engineering where such a tradeoff of quality attributes is certified by a mathematical argument.

Let us say a word about our presentation of proofs. The paper deals with a subject which belongs to applied mathematics (interpolation theory) and computer science (mainly algebraic complexity theory with a view to software engineering). However, the proofs rely on methods which come from pure mathematics, namely (elementary and not so elementary) algebraic geometry and commutative algebra.

We use elementary concepts from algebraic geometry like (affine) algebraic varieties, constructible sets, coordinate rings and function fields (of an affine variety) and rational maps. Not elementary is Zariski's Main Theorem which becomes also to be applied. Elementary notions of commutative algebra that we rely on are place, localization and finite module. For a reader with a background in applied mathematics or computer science these notions may be unfamiliar. For this reason we illustrate by numerous examples the main concepts of algebraic geometry and commutative algebra applied in this paper.

We hope that this will contribute to the insight that our notions from algebraic geometry and commutative algebra are not abstract, but have a concrete and relevant meaning for our subject.

2. Basic definitions and notations

In this section we collect the basic algebraic and geometric facts which allow us to establish a mathematical model for the Hermite–Lagrange interpolation with multivariate polynomials. We use standard notions and notations of commutative algebra and algebraic geometry, which can be found in, e.g., [20,29,19,26].

For any $n \in \mathbb{N}$, we denote by $\mathbb{A}^n := \mathbb{A}^n(\mathbb{C})$ the n-dimensional affine space $\mathbb{C}^n$, equipped with its respective Zariski and Euclidean topologies over $\mathbb{C}$. In algebraic geometry, the Euclidean topology of $\mathbb{A}^n$ is also called the *strong topology*. We shall use this terminology only exceptionally. In general it will be clear by the context to which one of these two topologies we are going to refer.

Let $X_1, \ldots, X_n$ be indeterminates over $\mathbb{C}$ and let $X := (X_1, \ldots, X_n)$. We denote by $\mathbb{C}[X]$ the ring of polynomials in the variables X with complex coefficients.

Let V be a closed affine subvariety of $\mathbb{A}^n$, that is, the set of common zeros in $\mathbb{A}^n$ of a finite set of polynomials belonging to $\mathbb{C}[X]$. As usual, we write $\dim V$ for the dimension of the variety V. For $f_1, \ldots, f_s, g \in \mathbb{C}[X]$ we shall use the notation $\{f_1 = 0, \ldots, f_s = 0\}$ and $\{f_1 = 0, \ldots, f_s = 0, g \neq 0\}$ in order to denote the closed affine subvariety V of $\mathbb{A}^n$ defined by $f_1, \ldots, f_s$ and the Zariski open subset

V_g of V defined by the intersection of V with the complement of $\{g = 0\}$. Observe that V_g is a locally closed affine subvariety of $\mathbb{A}^n$ whose coordinate ring is the localization $\mathbb{C}[V]_g$ of $\mathbb{C}[V]$.

We denote by $I(V) := \{f \in \mathbb{C}[X] : f(x) = 0 \text{ for any } x \in V\}$ the ideal of definition of V in $\mathbb{C}[X]$ and by $\mathbb{C}[V] := \{\varphi : V \to \mathbb{C} : \text{ there exists } f \in \mathbb{C}[X] \text{ with } \varphi(x) = f(x) \text{ for any } x \in V\}$ its coordinate ring. Observe that $\mathbb{C}[V]$ is isomorphic to the quotient $\mathbb{C}$-algebra $\mathbb{C}[V] = \mathbb{C}[X]/I(V)$. If V is irreducible, then $\mathbb{C}[V]$ is zero-divisor free and the rational functions of V with maximal domain form a field, denoted by $\mathbb{C}(V)$, which is called the rational function field of V. Observe that $\mathbb{C}(V)$ is isomorphic to the fraction field of the integral domain $\mathbb{C}[V]$.

In the general situation, when V is an arbitrary closed affine subvariety of $\mathbb{A}^n$, the notion of a rational function of V has also a precise meaning. The only point to underline is that the domain, say U, of a rational function of V has to be a maximal Zariski open and dense subset of V (hence, in particular, U has a nonempty intersection with any of the irreducible components of V). The rational functions of V form a $\mathbb{C}$-algebra which we also denote by $\mathbb{C}(V)$. In algebraic terms, $\mathbb{C}(V)$ is the total quotient ring of $\mathbb{C}[V]$ and is isomorphic to the direct product of the rational function fields of the irreducible components of V.

A partial map $\phi : V \dashrightarrow W$, where W is a closed subvariety of some affine space $\mathbb{A}^m$ and $\phi_1, \ldots, \phi_m$ are the components of ϕ, is called a *morphism* of affine varieties (or just *polynomial map*) if the complex valued functions $\phi_1, \ldots, \phi_m$ belong to $\mathbb{C}[V]$ (thus, in particular, ϕ is a total map). If the domain U of ϕ is a Zariski open and dense subset of V and $\phi_1, \ldots, \phi_m$ are the restrictions of suitable rational functions of V to U, we call ϕ a *rational map* of V to W. Observe that our definition of a rational map differs from the usual one in algebraic geometry, since we do not require that the domain U of ϕ is maximal. Hence, in the case $m := 1$, our concepts of a rational function and a rational map do not coincide.

2.1. Constructible sets and constructible maps

Let $\mathcal{M}$ be a subset of the affine space $\mathbb{A}^n$ and, for a nonnegative integer m, let $\phi : \mathcal{M} \dashrightarrow \mathbb{A}^m$ be a partial map. We call the set $\mathcal{M}$ *constructible* if $\mathcal{M}$ is definable by a Boolean combination of polynomial equations. A basic fact we shall use in the sequel is that if $\mathcal{M}$ is constructible, then its Zariski closure is equal to its Euclidean closure (see, e.g., [23, Chapter I, Section 10, Corollary 1]).

In the same vein we call the partial map ϕ *constructible* if the graph of ϕ is constructible as a subset of the affine space $\mathbb{A}^n \times \mathbb{A}^m$. We say that ϕ is *polynomial* if ϕ is the restriction of a morphism of affine varieties $\mathbb{A}^n \to \mathbb{A}^m$ to a constructible subset $\mathcal{M}$ of $\mathbb{A}^n$ (and hence a total map from $\mathcal{M}$ to $\mathbb{A}^m$). Furthermore we call ϕ a *rational* map of $\mathcal{M}$ if the domain U of ϕ is contained in $\mathcal{M}$ and ϕ is the restriction to $\mathcal{M}$ of a rational map of the Zariski closure $\overline{\mathcal{M}}$ of $\mathcal{M}$. In this case U is a Zariski open and dense subset of $\mathcal{M}$.

Since the elementary (i.e., first order) theory of algebraically closed fields with constants in $\mathbb{C}$ admits quantifier elimination, constructibility means just elementary definability. In particular, ϕ constructible implies that the domain and the image of ϕ are constructible subsets of $\mathbb{A}^n$ and $\mathbb{A}^m$, respectively. A useful fact concerning constructible maps we are going to use in the sequel is the following result (see, e.g., [21, Proposition 3.2.14]).

Lemma 1. *Let $\mathcal{M}$ be a constructible subset of $\mathbb{A}^n$ and let $\phi : \mathcal{M} \dashrightarrow \mathbb{A}^m$ be a partial map. Then ϕ is constructible if and only if there exists a partition of its domain in finitely many constructible subsets, say $\mathcal{M}_1, \ldots, \mathcal{M}_s$, such that for any $1 \le k \le s$ the restriction of ϕ to $\mathcal{M}_k$ is a rational map of $\mathcal{M}_k$ which is defined at any point of $\mathcal{M}_k$.*

In particular, if $\phi : \mathcal{M} \to \mathbb{A}^m$ is a total constructible map, then there exists a Zariski open and dense subset U of $\mathcal{M}$ such that the restriction $\phi|_U$ of ϕ to U is a rational map.

We are now going to introduce the notions of a weakly continuous, a strongly continuous, a topologically robust and a hereditary map of the constructible set $\mathcal{M}$. These four notions will constitute a fundamental tool for the meaningful modeling of Hermite–Lagrange interpolation problems and algorithms in Sections 3 and 4.

Definition 2. Let $\mathcal{M}$ be a constructible subset of $\mathbb{A}^n$ and let $\phi : \mathcal{M} \to \mathbb{A}^m$ be a (total) constructible map. We consider the following four conditions:

(i) there exists a Zariski open and dense subset U of $\mathcal{M}$ such that the restriction $\phi|_U$ of ϕ to U is a rational map of $\mathcal{M}$ and the graph of ϕ is contained in the Zariski closure of the graph of $\phi|_U$ in $\mathcal{M} \times \mathbb{A}^m$;
(ii) ϕ is continuous with respect to the Euclidean (i.e. strong) topologies of $\mathcal{M}$ and $\mathbb{A}^m$;
(iii) for any sequence $(x_k)_{k\in\mathbb{N}}$ of points of $\mathcal{M}$ which converges in the Euclidean topology to a point of $\mathcal{M}$, the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ is bounded;
(iv) for any constructible subset $\mathcal{N}$ of $\mathcal{M}$ the restriction $\phi|_{\mathcal{N}} : \mathcal{N} \to \mathbb{A}^m$ is an extension of a rational map of $\mathcal{N}$ and the graph of $\phi|_{\mathcal{N}}$ is contained in the Zariski closure of this rational map in $\mathcal{N} \times \mathbb{A}^m$.

We call the map ϕ
- *weakly continuous* if ϕ satisfies condition (i),
- *strongly continuous* if ϕ satisfies condition (ii),
- *topologically robust* if ϕ satisfies conditions (i) and (iii),
- *hereditary* if ϕ satisfies condition (iv).

Remark 3. Let $\phi : \mathcal{M} \to \mathbb{A}^m$ be a total constructible map. Then ϕ is topologically robust if and only if there exists a Zariski open and dense subset U of $\mathcal{M}$ for which condition (i) is satisfied and, for any sequence $(x_k)_{k\in\mathbb{N}}$ of points of U which converges in the Euclidean topology to a point of $\mathcal{M}$, the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ is bounded.

Proof. The *only if* part is obvious. We are going to prove the *if* part: assume that the second condition in the statement of the remark is satisfied and let U be the corresponding Zariski open and dense subset of $\mathcal{M}$. Let $(x_k)_{k\in\mathbb{N}}$ be an arbitrary sequence of points of $\mathcal{M}$ which converges in the Euclidean topology to a point $x \in \mathcal{M}$. Then we deduce from condition (i) that there exists a sequence $(y_k)_{k\in\mathbb{N}}$ of points of U such that $\|(x_k, \phi(x_k)) - (y_k, \phi(y_k))\| < 1/k$ holds for any $k \in \mathbb{N}$, where $\|\cdot\|$ denotes the Euclidean norm of $\mathcal{M} \times \mathbb{A}^m$. This implies that the sequence $(y_k)_{k\in\mathbb{N}}$ converges to x and that $\|\phi(x_k) - \phi(y_k)\| < 1$ holds for any $k \in \mathbb{N}$. Therefore the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ is bounded. We conclude that the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is topologically robust. This finishes the proof of the Remark 3. □

Let us now analyze the interdependence of the notions of a weakly continuous, a strongly continuous, a topologically robust and a hereditary map.

Lemma 4. *Let $\phi : \mathcal{M} \to \mathbb{A}^m$ be a strongly continuous constructible map. Then ϕ is weakly continuous, topologically robust and hereditary.*

Proof. First we prove that ϕ is weakly continuous. According to Lemma 1, there exists a Zariski open and dense subset U of $\mathcal{M}$ such that $\phi|_U$ is a rational map. Then the strong continuity of ϕ implies that the graph of ϕ is contained in the Euclidean closure of the graph of $\phi|_U$. Since the Euclidean and the Zariski closure of a constructible set agree, we deduce that ϕ is weakly continuous.

The constructible map ϕ is topologically robust since condition (ii) implies condition (iii). It is now clear that ϕ is hereditary. □

On the other hand, a weakly continuous or a topologically robust map is not necessarily strongly continuous, as the following example shows.

Example 5. Let $\mathcal{M} \subset \mathbb{A}^2$ be the constructible set $\mathcal{M} := \{(x_1, x_2) \in \mathbb{A}^2 : x_1 \cdot x_2 = 0\}$ and let $\phi : \mathcal{M} \to \mathbb{A}^1$ be the total map defined by

$$\phi(x_1, x_2) := \begin{cases} \dfrac{x_1}{x_1 + x_2} & \text{for } (x_1, x_2) \neq (0, 0), \\ 0 & \text{for } (x_1, x_2) = (0, 0). \end{cases}$$

Let $\mathbf{0} := (0, 0)$ and let $U := \mathcal{M} \setminus \{\mathbf{0}\}$. It is clear that ϕ is a constructible map, U is a Zariski open and dense subset of $\mathcal{M}$ and the restriction $\phi|_U$ of ϕ to U is a rational map of $\mathcal{M}$. Furthermore, we claim

that the graph $\mathcal{G}$ of ϕ is contained in the Zariski closure of the graph $\mathcal{G}_U$ of $\phi|_U$. Indeed, since $\mathcal{G}_U$ is a constructible set, the Zariski closure of $\mathcal{G}_U$ is equal to the strong closure of $\mathcal{G}_U$. Therefore, in order to show our claim it suffices to prove that the graph $\mathcal{G}$ of ϕ is contained in the strong closure of $\mathcal{G}_U$. By definition, the constructible set $\mathcal{G} \setminus \mathcal{G}_U$ consists only of the point $(\mathbf{0}, 0)$. Nevertheless, $(\mathbf{0}, 0)$ belongs to the strong closure of $\mathcal{G}_U$, since it is the limit of the sequence $\left(x^{(k)}, \phi|_U(x^{(k)})\right)_{k\in\mathbb{N}}$ of points of $\mathcal{G}_U$ defined by $x^{(k)} := (0, 1/k)$ for any $k \in \mathbb{N}$. This finishes the proof of our claim and shows that the map ϕ is weakly continuous.

Now we show that ϕ is topologically robust. For this purpose, we observe $\phi(x_1, 0) = 1$ for any $x_1 \in \mathbb{A}^1 \setminus \{0\}$ and $\phi(0, x_2) = 0$ for any $x_2 \in \mathbb{A}^1$. This proves that the map ϕ is bounded. Therefore ϕ satisfies condition (iii) and hence ϕ is topologically robust.

Finally, we show that ϕ is not strongly continuous. Let $(x^{(k)})_{k\in\mathbb{N}}$ be the sequence of points of $\mathcal{M}$ defined by $x^{(k)} := (1/k, 0)$ for any $k \in \mathbb{N}$. Then it is easy to see that

$$\lim_{k\to\infty} x^{(k)} = \mathbf{0} \in \mathcal{M} \quad \text{and} \quad \lim_{k\to\infty} \phi(x^{(k)}) = 1 \neq \phi(\mathbf{0})$$

holds. This proves that ϕ is not strongly continuous.

If the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is weakly continuous, then there is no guarantee that the restriction of ϕ to an arbitrary constructible subset of $\mathcal{M}$ is also weakly continuous, as it is shown by the following example. Therefore restrictions of topologically robust maps to constructible subsets of their domains may happen not to be topologically robust. If the map $\phi : \mathcal{M} \to \mathbb{A}^m$ is polynomial, then ϕ is strongly continuous (and hence weakly continuous, topologically robust and hereditary by Lemma 4).

Example 6. Consider again the constructible set $\mathcal{M} \subset \mathbb{A}^2$ and the total map $\phi : \mathcal{M} \to \mathbb{A}^1$ of Example 5, namely $\mathcal{M} := \{(x_1, x_2) \in \mathbb{A}^2 : x_1 \cdot x_2 = 0\}$ and

$$\phi(x_1, x_2) := \begin{cases} \dfrac{x_1}{x_1 + x_2} & \text{for } (x_1, x_2) \neq (0, 0), \\ 0 & \text{for } (x_1, x_2) = (0, 0). \end{cases}$$

Then the restriction $\phi|_{\mathcal{N}} : \mathcal{N} \to \mathbb{A}^1$ to the constructible subset $\mathcal{N} := \{(x_1, 0) \in \mathbb{A}^2 : x_1 \in \mathbb{A}^1\}$ of $\mathcal{M}$ is not weakly continuous. In particular, ϕ is not hereditary.

The concept of hereditarity sounds rather abstract and axiomatic. We shall need it in the sequel for a mathematically correct and complete formulation of our algorithmic model. In Section 4 we shall establish an algorithmically meaningful condition which implies hereditarity of suitable topologically robust maps (see Definition 14, Proposition 16 and Corollary 18).

2.2. Straight-line programs

Algorithms in computational algebraic geometry are usually described using the standard dense (or sparse) complexity model, i.e., encoding multivariate polynomials by means of the vector of all (or of all nonzero) coefficients. Taking into account that a generic n-variate polynomial of degree $d \geq 2$ has $\binom{d+n}{n} = O(d^n)$ nonzero coefficients, we see that the dense representation of multivariate polynomials requires an exponential size, and their manipulation usually requires an exponential number of arithmetic operations with respect to the parameters d and n. In order to avoid this exponential behavior, we are going to use alternative encodings of input and intermediate results of our computations, e.g., by means of straight-line programs (see [8]). A *straight-line program* β over $\mathbb{C}(X) := \mathbb{C}(X_1, \ldots, X_n)$ is a finite sequence of rational functions $(f_1, \ldots, f_k) \in \mathbb{C}(X)^k$ such that for $1 \leq i \leq k$, the function f_i is an element of the set $\{X_1, \ldots, X_n\}$ (an *input*), or an element of $\mathbb{C}$ (a *parameter*), or there exist $1 \leq i_1, i_2 < i$ such that $f_i = f_{i_1} \circ_i f_{i_2}$ holds, where $\circ_i$ is one of the arithmetic operations $+, -, \times, \div$. Access to inputs and parameters is considered as free (random access model). The elements of the set $\{f_1, \ldots, f_k\}$ are called *intermediate results* of β. The straight-line program β is called (essentially) *division-free*, if for $1 \leq i \leq k$ the arithmetic operation $\circ_i$ is different

from $\div$ (or alternatively, if divisions are restricted to nonzero parameters). Observe that the intermediate results of β belong to the polynomial ring $\mathbb{C}[X]$, if β is division-free.

A natural measure of the complexity of β is its *length*, namely the total number of arithmetic operations performed during the evaluation process defined by β. Another relevant measure of complexity is the *nonscalar length* of β, which is defined as the number of operations $\circ_i \in \{\times, \div\}$ with $f_{i_1}, f_{i_2} \notin \mathbb{C}$ for $\circ_i = \times$ and $f_{i_2} \notin \mathbb{C}$ for $\circ_i = \div$. The (nonscalar) length of β models the sequential execution time of the program.

We say that the straight-line program β *computes*, *represents*, or *encodes* a subset S of $\mathbb{C}(X)$ if S is contained in the list of intermediate results $\{f_1, \ldots, f_k\}$ of β. In this case we call the elements of S *outputs* of β.

3. A computational model for Hermite–Lagrange interpolation

Let n, D, K, L, M and N be six discrete parameters belonging to $\mathbb{N}$. As before, let $X := (X_1, \ldots, X_n)$, where $X_1, \ldots, X_n$ are indeterminates over $\mathbb{C}$, and denote by Π (or, more precisely, by $\Pi^{(n)}$) the polynomial ring $\mathbb{C}[X] = \mathbb{C}[X_1, \ldots, X_n]$ and by Π_D (or by $\Pi_D^{(n)}$) the $\mathbb{C}$-vector space of polynomials of Π of degree at most D.

In the present paper we shall be concerned with discrete families (depending on part or all of the parameters n, D, K, L, M and N) of Hermite–Lagrange interpolation problems and algorithms. Before we introduce a general computation model that contains these two concepts we are going to discuss them in the more intuitive context of Lagrange interpolation.

3.1. Lagrange interpolation revisited

3.1.1. Lagrange interpolation problems

Informally, a Lagrange interpolation problem is determined by a class $\mathcal{D}$ of *interpolation data* and a class $\mathcal{O}$ of *interpolants*. In this paper we shall think that for fixed parameters n, D and K the classes $\mathcal{D}, \mathcal{O}$ and the relationship between them become realized by the following mathematical structures:

- The class $\mathcal{D}$ is a constructible subset of the affine ambient space $\mathbb{A}^{(n+1)\times K}$ consisting of suitable K-tuples $((x_1, y_1), \ldots, (x_K, y_K))$ of nodes $x_i \in \mathbb{A}^n$ and values $y_i \in \mathbb{C}$, $1 \leq i \leq K$, such that $x_i \neq x_j$ holds for any choice of indices $1 \leq i < j \leq K$.
- The class $\mathcal{O}$ is a constructible subset of the finite dimensional vector space Π_D, such that for any interpolation datum $d := ((x_1, y_1), \ldots, (x_K, y_K))$ belonging to $\mathcal{D}$ there exists exactly one interpolant $f \in \mathcal{O}$ which solves the Lagrange interpolation problem for d, i.e., which satisfies the condition $f(x_i) = y_i$ for any index $1 \leq i \leq K$.
- There exists a constructible map $\Phi : \mathcal{D} \to \Pi_D$ whose image is contained in $\mathcal{O}$ and which associates to each interpolation datum $d \in \mathcal{D}$ the interpolant $\Phi(d)$.

In the context of classic Lagrange interpolation, the class of interpolants $\mathcal{O}$ is always a finite-dimensional subspace of the polynomial ring Π (and hence contained in Π_D for some D) and $\mathcal{D}$ is usually a suitable constructible Zariski dense subset of $\mathbb{A}^{(n+1)\times K}$. In the present paper the class $\mathcal{O}$ may have a nonlinear geometric structure, e.g., $\mathcal{O}$ may be an algebraic subvariety of higher degree of the affine space Π_D and the interpolation data may be interdependent, i.e., $\mathcal{D}$ may be contained in a proper algebraic subvariety of $\mathbb{A}^{(n+1)\times K}$.

In classical interpolation theory one would like that any convergent sequence of Lagrange interpolants converges to a Hermite interpolant. Unfortunately this is not true in general. Therefore we shall require that the map Φ satisfies a more modest, however quite natural, coalescence condition which may be paraphrased as a weak kind of "continuity" of Φ with respect to the Euclidean topologies of $\mathcal{D}$ and $\mathcal{O}$. The map Φ establishes a certain interdependence between the interpolation data from $\mathcal{D}$ and the interpolants from $\mathcal{O}$. We shall also require that the essential (topological or geometrical) features of this interdependence become preserved when we restrict the class $\mathcal{D}$ to an arbitrary constructible subset. In more technical terms we may think $\Phi : \mathcal{D} \to \Pi_D$ given as a constructible, topologically robust and hereditary map in the sense of Section 2. If this is the case, then Φ surely

meets our (informal) requirements. Needless to say that in classic Lagrange interpolation theory the map which corresponds to Φ is always strongly continuous (and hence topologically robust and hereditary by Lemma 4).

This is now the way we are going to formalize the notion of a *Lagrange interpolation problem*, namely by a constructible subset $\mathcal{D}$ of the affine space $\mathbb{A}^{(n+1)\times K}$, representing as above the interpolation data of the problem, and by a topologically robust and hereditary map $\Phi : \mathcal{D} \to \Pi_D$ which for any $d := ((x_1, y_1), \ldots, (x_K, y_K))$ belonging to $\mathcal{D}$ satisfies the condition $\Phi(d)(x_i) = y_i$ for $1 \le i \le K$.

3.1.2. Lagrange interpolation algorithms

In order to develop our model for the informal concept of a family of Lagrange interpolation problems, we made only reference to "objective" mathematical structures, like interpolation data, interpolants and the map Φ. Following the terminology of [9] the elements of $\mathcal{D}$, interpreted as interpolation data, may be considered as *input objects* and the elements of $\mathcal{O}$ as *output objects* which become related by the (mathematical) map Φ. However this does not suffice, since for the modeling of the concept of a Lagrange interpolation algorithm, we need to deal with data structures and types which represent input and output objects.

As mentioned in Section 1, a particular feature of Lagrange (and also Hermite) interpolation consists of the identification of the concepts of input object and the code that represents it. Thus the constructible subset $\mathcal{D}$ of $\mathbb{A}^{(n+1)\times K}$ has not only to be considered as a set of (objective) interpolation data, but also, and simultaneously, as a *data structure* containing the *input codes* (or *representations*) which encode the interpolation data. This is nothing but a computer science interpretation of something that is already common sense in interpolation theory. Thus, in the context of this paper, interpolation datum and input code are notions which reflect distinct aspects of the same mathematical object.

However our point of view differs from the standard one with respect to the interpolants and their representations, since we do not fix in advance the *output data structure*, say $\mathcal{D}^*$, that encodes the output object class of interpolants $\mathcal{O}$. In the context of classical Lagrange (and Hermite) interpolation, $\mathcal{D}^*$ is always the dense (or suitable sparse) representation of the interpolants by their coefficients. In the present paper we wish to admit as $\mathcal{D}^*$ more general data structures like, e.g., the domain of parameter instances of a suitable straight-line program representation of the interpolants. In order to explain our view we are now going to analyze the relation between Lagrange interpolation and the straight-line program representation of polynomials in more detail.

We now fix the parameters n and L. Let $D := 2^L$, $K := 4(L+n+1)^2+2$, $M := (L+n+1)^2$, and let $\mathcal{O}$ be the subset of $\Pi^{(n)}$ of n-variate polynomials that can be evaluated by a division-free straight-line program of nonscalar length L. From [8, Exercise 9.18] we deduce that $\mathcal{O}$ is a constructible subset of the finite-dimensional vector space $\Pi_D = \Pi_D^{(n)}$. Moreover, since $M = (L+n+1)^2$, there exists a fixed division-free straight line program β of nonscalar length L in M *generic* parameters (also called a *computation scheme* of nonscalar length L) with the following property:
For any polynomial $f \in \mathcal{O}$ there exists a parameter instance $z \in \mathbb{A}^M$ such that the specialization $\beta(z)$ of β in z is a straight-line program of nonscalar length L (with complex parameters z) which encodes the polynomial f. Considering $\mathcal{O}$ as a (constructible) subset of the finite-dimensional vector space Π_D, we may describe this encoding by a *polynomial* map (i.e., morphism of affine varieties) $\omega^* : \mathbb{A}^M \to \Pi_D$. In particular we have $\omega^*(z) = f$. Observe that the image of ω^* is $\mathcal{O}$, hence $\mathcal{O}$ is irreducible.

Suppose that there are given suitable, mutually distinct points $\gamma_1, \ldots, \gamma_K$ of $\mathbb{A}^n$ and a suitable constructible subset $\mathcal{D}$ of $\mathbb{A}^K$ such that for $\gamma := (\gamma_1, \ldots, \gamma_K)$ the set $\mathcal{D}_\gamma := \{((\gamma_1, y_1), \ldots, (\gamma_K, y_K)) : (y_1, \ldots, y_K) \in \mathcal{D}\}$ represents the interpolation data of a Lagrange interpolation problem for the class of interpolants $\mathcal{O}$. According to our comments in Section 3.1.1 this Lagrange interpolation problem may be modeled by a topologically robust and hereditary map $\Phi : \mathcal{D} \to \Pi_D$ with image $\mathcal{O}$. Thus $\mathcal{D}$ and Φ describe a Lagrange interpolation problem. In Section 3.3.3, using the assumption $K = 4(L+n+1)^2+2$, we shall exhibit a concrete example of this situation.

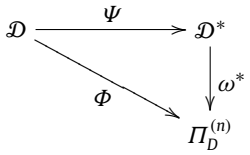
The algorithmic task is now to *compute* (in a uniform and deterministic manner), for each input code $d \in \mathcal{D}$, an output code, say $\Psi(d)$, which belongs to $\mathbb{A}^M$ and which represents the interpolant $\Phi(d)$ in the following way: $\Psi(d)$ is a complex parameter instance of the computation scheme β satisfying

the condition $\omega^*(\Psi(d)) = \Phi(d)$. We model therefore the notion of a Lagrange interpolation algorithm using a (total) map $\Psi : \mathcal{D} \to \mathbb{A}^M$ which has to satisfy certain conditions we are going to explain now.

Let $\mathcal{D}^*$ be a given constructible subset of $\mathbb{A}^M$ with $\omega^*(\mathcal{D}^*) = \mathcal{O}$. For the sake of notational simplicity we shall also write $\omega^* : \mathcal{D}^* \to \Pi_D$ for the restriction of $\omega^* : \mathbb{A}^M \to \Pi_D$ to $\mathcal{D}^*$. We consider $\mathcal{D}^*$ as the output data structure and ω^* as the encoding of output objects of the interpolation algorithm represented by the map Ψ. Consequently we require that Ψ maps $\mathcal{D}$ into $\mathcal{D}^*$.

Further we wish that Ψ is in some sense "computable" and that Ψ remains "computable" if we restrict it to an arbitrary constructible subset of $\mathcal{D}$, according to the requirement made before on the interpolation problem Φ. Since a rational map may be considered as "computable only on generic inputs", we require that Ψ is hereditary.

This condition is very weak, since it includes the case that the Lagrange interpolation algorithm behind the map Ψ is implemented by a computer program that contains branchings. A typical case of a branching-free algorithm would arise if Ψ could be a *polynomial* map. However, from Theorem 23 we deduce that no polynomial map $\Psi : \mathcal{D} \to \mathcal{D}^*$ exists such that, for $M \leq 2^{c\sqrt{K}}$, where $c > 0$ is a universal constant, the following diagram commutes:



(1)

In fact, Theorem 23 makes the same assertion for a much larger class of topologically robust and hereditary maps Ψ, namely for the class of geometrically robust maps which will be introduced in Section 4.2.

The data $\mathcal{D}^*$, ω^* and Ψ determine now an *interpolation algorithm* which solves the interpolation problem given by Φ.

Our interest for the straight-line program encoding of polynomials is motivated by the fact that there exist computationally relevant examples of high degree polynomials like $(1+T)^{2^L}$ or $\sum_{0\leq j\leq 2^L} T^j$ which can be evaluated using only a few, namely $O(L)$ arithmetical operations, whereas there exist other examples of high interest, like the Pochhammer–Wilkinson polynomial $\prod_{0\leq j\leq 2^L}(T-j)$ or the polynomial $\sum_{0\leq j\leq 2^L} T^j/j$, whose complexity status is unknown (here T denotes a new indeterminate). On the other hand, the (multivariate) polynomials which occur as by- or end products of elimination procedures in effective algebraic and semialgebraic geometry may be encoded by straight-line programs whose length is *polynomial* in the degree of these polynomials. This implies in typical cases an exponential improvement of the data structure with respect to the classical ones, namely the dense (or sparse) encoding of polynomials.

One may now raise the question whether such elimination polynomials admit also straight-line program encodings whose length is *polylogarithmic* in the degree of the given polynomial. The expected answer is no, since otherwise we would have $P = NP$ in the BSS complexity model over the real or complex numbers (see, e.g., [7,5,6,15] for more details).

If the concept of "elimination polynomial" is interpreted in a more comprehensive way, namely beyond the classical examples of resultants, then it can be even *proved* that general elimination procedures are not always able to produce polylogarithmic straight-line program representations for their output polynomials, unless they introduce arbitrary and uncontrolled branchings (see [12,9]).

3.2. The general model

We are now ready to describe the announced computation model which also includes Hermite interpolation. Replacing in the previous discussion of Lagrange interpolation the quantity $(n+1)K$ (or just K) by the parameter N, we arrive to the following formulation:

Definition 7. Let n, D, M and N be fixed natural numbers. We say that a given Hermite–Lagrange *interpolation problem* is *determined* by a (suitable) constructible subset $\mathcal{D}$ of the affine space $\mathbb{A}^N$, acting as input data structure, and a (suitable) topologically robust and hereditary map $\Phi : \mathcal{D} \to \Pi_D^{(n)}$.

Furthermore we say that a Hermite–Lagrange *interpolation algorithm* (solving the given interpolation problem) is *determined* by a constructible subset $\mathcal{D}^*$ of the affine space $\mathbb{A}^M$, acting as output data structure, a polynomial encoding $\omega^* : \mathcal{D}^* \to \Pi_D^{(n)}$ of output objects and a hereditary map $\Psi : \mathcal{D} \to \mathcal{D}^*$, namely the algorithm in the narrow sense, such that the diagram (1) commutes.

Of course, this model captures much more general situations than just the Hermite–Lagrange interpolation in the usual intuitive sense. Nevertheless, it represents all what we need for our mathematical discussion of the subject of this paper. In particular there will be no need to model *exactly* the informal meaning of Hermite–Lagrange interpolation.

3.3. Three critical families of examples

The purpose of this section is to illustrate the notions of the previous sections, which are discussed on three significant families of interpolation problems. These families of interpolation problems constitute our prototypic examples, and shall be further discussed in Sections 4.3 and 5.

The first two families we consider here come from standard univariate Lagrange interpolation. Their input data structures are (nonempty) Zariski open subsets of suitable affine spaces and therefore smooth varieties. Then we analyze two cases of multivariate Hermite–Lagrange interpolation on *singular* curves. Our last example is that of a family of *nonlinear* interpolation problems, that is, the set of interpolants is not a linear subspace, but a constructible set of the corresponding affine ambient space.

3.3.1. Univariate Lagrange interpolation

In terms of the notations introduced before, let $K \geq 2$ be a given natural number, $n := 1, D := K-1, M := K, N := 2K, X := X_1$ and $\Pi_D := \Pi_D^{(1)}$.

Lagrange interpolation at fixed nodes Fix an arbitrary point $\gamma := (\gamma_1, \ldots, \gamma_K) \in \mathbb{A}^K$ with $\gamma_i \neq \gamma_j$ for $1 \leq i < j \leq K$. The (generic) univariate Lagrange interpolation problem at (fixed) nodes $\gamma_1, \ldots, \gamma_K$ consists in finding, for any $y := (y_1, \ldots, y_K) \in \mathbb{A}^K$, the (unique) polynomial $f_{\gamma,y} \in \Pi_D$ satisfying the condition

$$f_{\gamma,y}(\gamma_j) = y_j \quad \text{for } 1 \leq j \leq K. \tag{2}$$

Let $\mathcal{D}_\gamma$ be the constructible subset $\mathcal{D}_\gamma := \{\gamma_1\} \times \mathbb{A}^1 \times \cdots \times \{\gamma_K\} \times \mathbb{A}^1$ of $\mathbb{A}^N$. Then the *univariate Lagrange interpolation problem at fixed nodes* $\gamma_1, \ldots, \gamma_K$ is represented by the map $\Phi_\gamma : \mathcal{D}_\gamma \to \Pi_D$ which associates to each $d := (\gamma_1, y_1, \ldots, \gamma_K, y_K) \in \mathcal{D}_\gamma$ the unique polynomial $f_d := f_{\gamma,y}$ of Π_D determined by condition (2). Since Φ_γ is a polynomial map, we conclude that $\mathcal{D}_\gamma$ and Φ_γ determine a Lagrange interpolation problem in the sense of Definition 7.

Let $\mathcal{D}^* := \mathbb{A}^M$ and let $\omega^* : \mathcal{D}^* \to \Pi_D$ be the encoding of the elements of Π_D by their dense representation, i.e., let $\omega^*(a_0, \ldots, a_{K-1}) := \sum_{j=0}^{K-1} a_j X^j$ for $(a_0, \ldots, a_{K-1}) \in \mathcal{D}^*$. Then we know that for every $d := \big((\gamma_1, y_1), \ldots, (\gamma_K, y_K)\big) \in \mathcal{D}_\gamma$ with $y := (y_1, \ldots, y_K)$, the dense representation of $f_d \in \Pi_D$ is given by $V_\gamma^{-1} y$, where $V_\gamma := (\gamma_i^{j-1})_{1 \leq i,j \leq K} \in \mathbb{A}^{K \times K}$ is the Vandermonde matrix associated to γ. Hence, the polynomial map $\Psi_\gamma : \mathcal{D}_\gamma \to \mathcal{D}^*$ defined by $\Psi_\gamma(d) := V_\gamma^{-1} y$ determines an algorithm in the sense of Definition 7 which solves the Lagrange interpolation problem given by $\mathcal{D}_\gamma$ and Φ_γ.

Lagrange interpolation at generic nodes The previous construction can easily be modified in order to also model the classic univariate Lagrange interpolation in generic nodes. With the same notations as above, let $\mathcal{U}$ be the Zariski open subset of $\mathbb{A}^K$ defined by $\mathcal{U} := \{(\gamma_1, \ldots, \gamma_K) \in \mathbb{A}^K : \gamma_i \neq \gamma_j \text{ for } 1 \leq i < j \leq K\}$ and let $\mathcal{D}$ be the constructible subset of $\mathbb{A}^N$ defined by $\mathcal{D} := \mathcal{U} \times \mathbb{A}^K$. For any $d := (\gamma, y) \in \mathcal{D}$ we denote by f_d the unique polynomial of Π_D determined by the condition (2). Then the *generic univariate Lagrange interpolation problem* is represented by $\mathcal{D}$ and the regular, i.e., everywhere on

$\mathcal{D}$ well-defined, rational map $\Phi : \mathcal{D} \to \Pi_D$ which associates to each $d \in \mathcal{D}$ the polynomial $f_d \in \Pi_D$. This implies that Φ is strongly continuous (hence topologically robust and hereditary). Therefore we conclude that $\mathcal{D}$ and Φ determine a Lagrange interpolation problem in the sense of Definition 7. Since the dense representation of f_d with $d = (\gamma, y) \in \mathcal{D}$ is given by the vector $V_\gamma^{-1} y$, we see that for $\mathcal{D}^* := \mathbb{A}^M$, the encoding $\omega^* : \mathcal{D}^* \to \Pi_D$ defined by $\omega^*(a_0, \ldots, a_{K-1}) := \sum_{j=0}^{K-1} a_i X^i$, and the regular rational map $\Psi : \mathcal{D} \to \mathcal{D}^*$ defined by $\Psi(d) := V_\gamma^{-1} y$, determine an algorithm in the sense of Definition 7 solving the interpolation problem given by $\mathcal{D}$ and Φ, because Ψ is hereditary.

3.3.2. Bivariate Hermite–Lagrange interpolation over singular curves

Let X_1, X_2 be indeterminates over $\mathbb{C}$ and let $\Pi^{(2)} := \mathbb{C}[X_1, X_2]$. In this section we consider two examples of bivariate Hermite–Lagrange interpolation defined over a Zariski open subset $\mathcal{D}$ of a singular curve $\mathcal{C} \subset \mathbb{A}^2$. In the first example the interpolation problem is determined by a strongly continuous map $\Phi : \mathcal{D} \to \Pi_1^{(2)}$, while in the second example the problem is determined by a topologically robust and hereditary map $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ which is not strongly continuous.

Interpolation over the curve $X_1^3 - X_2^2 = 0$ We consider the irreducible algebraic curve $\mathcal{C}$ of $\mathbb{A}^2$ defined by the equation $X_1^3 - X_2^2 = 0$, containing the non-empty Zariski open subset $\mathcal{D} := \mathcal{C} \setminus \{(-1, \pm \mathrm{i})\}$. Let a polynomial map $f : \mathbb{A}^2 \to \mathbb{A}^1$ be given. It is clear that the restriction $f|_{\mathcal{D}}$ of f to $\mathcal{D}$ is topologically robust and hereditary. Observe that the point $\mathbf{0} := (0, 0)$ belongs to $\mathcal{D}$.

We consider now the problem of interpolating f from the values $f(d)$ and $f(\mathbf{0})$ for any $d \in \mathcal{D}$ by means of polynomials belonging to $\Pi_1^{(2)}$.

Observe that for any point $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ there exists a unique polynomial g_d of the linear subspace $E_d := \mathbb{C} + \mathbb{C} \cdot (d_1 X_1 + d_2 X_2)$ of $\Pi_1^{(2)}$ satisfying the condition $g_d(d) = f(d)$ and $g_d(\mathbf{0}) = f(\mathbf{0})$. Taking into account $d_1^2 + d_2^2 \neq 0$, the polynomial g_d can be written as

$$g_d := f(\mathbf{0}) + \frac{\big(f(d) - f(\mathbf{0})\big) d_1}{d_1^2 + d_2^2} X_1 + \frac{\big(f(d) - f(\mathbf{0})\big) d_2}{d_1^2 + d_2^2} X_2.$$

The $\mathbb{C}$-linear space of interpolants E_d represents the *"least solution space"* introduced in [10] (see also [11]).

Finally, we define $g_{\mathbf{0}}$ as the unique polynomial of the $\mathbb{C}$-linear subspace $\mathbb{C} + \mathbb{C} \cdot X_1$ of $\Pi_1^{(2)}$ which interpolates f and its partial derivative $\partial f / \partial X_1$ at the point $\mathbf{0} \in \mathbb{A}^2$, namely,

$$g_{\mathbf{0}} := f(\mathbf{0}) + \frac{\partial f}{\partial X_1}(\mathbf{0}) X_1.$$

Thus we have $g_{\mathbf{0}}(\mathbf{0}) = f(\mathbf{0})$ and $(\partial g_{\mathbf{0}} / \partial X_1)(\mathbf{0}) = (\partial f / \partial X_1)(\mathbf{0})$.

One sees now easily that the map $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ defined by $\Phi(d) := g_d$ is constructible and that $\Phi|_{\mathcal{D} \setminus \{\mathbf{0}\}}$ is a rational function of $\mathcal{D}$ which is regular on $\mathcal{D} \setminus \{\mathbf{0}\}$.

We claim that Φ is strongly continuous (and thus, topologically robust and hereditary). In order to see this, it suffices to show that, for any sequence $(d^{(k)})_{k \in \mathbb{N}}$ of points of $\mathcal{D} \setminus \{\mathbf{0}\}$ which converge to $\mathbf{0}$, the sequence $(\Phi(d^{(k)}))_{k \in \mathbb{N}}$ converges to $\Phi(\mathbf{0})$.

Fix $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$. Then we have $d_1^3 = d_2^2$, $d_1 \neq 0$, $d_1^2 + d_2^2 \neq 0$ and $(d_2/d_1)^2 = d_1$. This implies

$$\frac{(f(d) - f(\mathbf{0})) d_1}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0})) d_1}{d_1^2 (1 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1} \frac{1}{1 + d_1} \tag{3}$$

and

$$\frac{(f(d) - f(\mathbf{0})) d_2}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0})) d_2}{d_1^2 (1 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1} \frac{d_2}{d_1} \frac{1}{1 + d_1}. \tag{4}$$

Furthermore, considering the Taylor expansion of f at $\mathbf{0}$, we conclude that there exist polynomials Q_1, Q_2 of $\Pi^{(2)}$ with $Q_1(\mathbf{0}) = Q_2(\mathbf{0}) = 0$ such that

$$f(d) - f(\mathbf{0}) = \left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d)\right)d_1 + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d)\right)d_2$$

holds.

Let $(d^{(k)})_{k\in\mathbb{N}}$ be a sequence of points of $\mathcal{D}\setminus\{\mathbf{0}\}$ which converges to $\mathbf{0}\in\mathcal{D}$. Since $(d_2^{(k)}/d_1^{(k)})^2 = d_1^{(k)}$ holds for any $k\in\mathbb{N}$, we conclude

$$\lim_{k\to\infty}\frac{f(d^{(k)}) - f(\mathbf{0})}{d_1^{(k)}} = \lim_{k\to\infty}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d^{(k)}) + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d^{(k)})\right)\frac{d_2^{(k)}}{d_1^{(k)}}\right) = \frac{\partial f}{\partial X_1}(\mathbf{0}).$$

Combining this identity with (3) and (4) we infer that Φ is strongly continuous.

Therefore $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ determines a Hermite–Lagrange interpolation problem in the sense of Definition 7.

Now let $\mathcal{D}^* := \mathbb{A}^3$ and consider the canonical dense representation ω^* of the bivariate polynomials over $\mathbb{C}$ of degree at most one as the output encoding. More precisely, we define $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$ by $\omega^*(a_0, a_1, a_2) := a_0 + a_1X_1 + a_2X_2$. Furthermore, let $\Psi : \mathcal{D} \to \mathcal{D}^*$ be the constructible map defined for $d := (d_1, d_2) \in \mathcal{D}\setminus\{\mathbf{0}\}$ by

$$\Psi(d) := \left(f(\mathbf{0}), \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2}, \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2}\right)$$

and for $d = \mathbf{0}$ by

$$\Psi(\mathbf{0}) := \left(f(\mathbf{0}), \frac{\partial f}{\partial X_1}(\mathbf{0}), 0\right).$$

Then Ψ is a strongly continuous map which solves the Hermite–Lagrange problem determined by Φ.

Interpolation over the curve $X_2^2 = X_1^2 + X_1^3$ We consider now the irreducible algebraic curve $\mathcal{C}$ of $\mathbb{A}^2$ defined by the equation $X_2^2 = X_1^2 + X_1^3$, containing the non-empty Zariski open subset $\mathcal{D} := \mathcal{C}\setminus\{(-2, \pm 2\mathrm{i})\}$. Again let $f : \mathbb{A}^2 \to \mathbb{A}^1$ be given a polynomial map. It is clear that the restriction $f|_{\mathcal{D}}$ of f to $\mathcal{D}$ is topologically robust and hereditary. Observe that the origin $\mathbf{0} := (0, 0)$ belongs to $\mathcal{D}$.

We now consider the problem of interpolating f from the values $f(d)$ and $f(\mathbf{0})$ for any $d\in\mathcal{D}$ by means of polynomials belonging to $\Pi_1^{(2)}$.

For any point $d := (d_1, d_2) \in \mathcal{D}\setminus\{\mathbf{0}\}$ there exists a unique polynomial g_d in the "least solution space" of [11,10], namely the linear subspace $E_d := \mathbb{C} + \mathbb{C}\cdot(d_1X_1 + d_2X_2)$ of $\Pi_1^{(2)}$, satisfying the condition $g_d(d) = f(d)$ and $g_d(\mathbf{0}) = f(\mathbf{0})$. Since $d_1^2 + d_2^2$ is different from zero, the polynomial g_d can be written as

$$g_d := f(\mathbf{0}) + \frac{\big(f(d) - f(\mathbf{0})\big)d_1}{d_1^2 + d_2^2}X_1 + \frac{\big(f(d) - f(\mathbf{0})\big)d_2}{d_1^2 + d_2^2}X_2.$$

Finally, we define $g_{\mathbf{0}}$ as the unique polynomial of the $\mathbb{C}$-linear subspace $\mathbb{C} + \mathbb{C}\cdot(X_1 + X_2)$ of $\Pi_1^{(2)}$ which interpolates f and the sum of its first partial derivatives at $\mathbf{0}$, namely

$$g_{\mathbf{0}} := f(\mathbf{0}) + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_1 + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_2.$$

Thus we have $g_{\mathbf{0}}(\mathbf{0}) = f(\mathbf{0})$ and $(\partial g_{\mathbf{0}}/\partial X_1 + \partial g_{\mathbf{0}}/\partial X_2)(\mathbf{0}) = (\partial f/\partial X_1 + \partial f/\partial X_2)(\mathbf{0})$.

One sees now easily that the map $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ defined by $\Phi(d) := g_d$ is constructible and that $\Phi|_{\mathcal{D}\setminus\{\mathbf{0}\}}$ is a rational function of $\mathcal{D}$ which is regular on $\mathcal{D}\setminus\{\mathbf{0}\}$.

We claim that Φ is also topologically robust. In order to see this, we show first that $\Phi(d)$ remains bounded when $d \in \mathcal{D}$ approximates $\mathbf{0} \in \mathcal{D}$. Let $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$. Then we have $d_1^2 + d_2^2 = 2d_1^2 + d_1^3$, $d_1 \neq 0$ and $d_1^2 + d_2^2 \neq 0$. This implies

$$\frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2(2 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1}\frac{1}{2 + d_1} \tag{5}$$

and

$$\frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2} = \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2(2 + d_1)} = \frac{f(d) - f(\mathbf{0})}{d_1}\frac{d_2}{d_1}\frac{1}{2 + d_1}. \tag{6}$$

Furthermore, by considering the Taylor expansion of f at $\mathbf{0}$, we deduce that there exist polynomials Q_1, Q_2 of $\Pi^{(2)}$ with $Q_1(\mathbf{0}) = Q_2(\mathbf{0}) = 0$ such that

$$f(d) - f(\mathbf{0}) = \left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d)\right)d_1 + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d)\right)d_2 \tag{7}$$

holds.

Let $(d^{(k)})_{k\in\mathbb{N}}$ be a sequence of points of $\mathcal{D} \setminus \{\mathbf{0}\}$ which converges to $\mathbf{0} \in \mathcal{D}$. For any $k \in \mathbb{N}$ we have

$$\frac{f(d^{(k)}) - f(\mathbf{0})}{d_1^{(k)}} = \frac{\partial f}{\partial X_1}(\mathbf{0}) + Q_1(d^{(k)}) + \left(\frac{\partial f}{\partial X_2}(\mathbf{0}) + Q_2(d^{(k)})\right)\frac{d_2^{(k)}}{d_1^{(k)}}.$$

From the identity $(d_2^{(k)}/d_1^{(k)})^2 = 1 + d_1^{(k)}$ and the fact that Q_1, Q_2 define strongly continuous functions in a neighborhood of $\mathbf{0}$ we conclude that the sequence $\left(\left(f(d^{(k)}) - f(\mathbf{0})\right)/d_1^{(k)}\right)_{k\in\mathbb{N}}$ is bounded. Combining this observation with (5) and (6), we see that Φ satisfies condition (iii) of Definition 2.

In order to see that Φ is topologically robust it remains to prove that Φ is weakly continuous. We claim that the graph of Φ is contained in the Zariski closure of the graph of the restriction $\Phi|_U$ of Φ to the Zariski open and dense subset $U := \mathcal{D} \setminus \{\mathbf{0}\}$ of $\mathcal{D}$. Indeed, let $(r_k)_{k\in\mathbb{N}}$ be a sequence of positive reals converging to $0 \in \mathbb{R}$ and let $(s_k)_{k\in\mathbb{N}}$ be the sequence of positive reals defined by $s_k := r_k\sqrt{1 + r_k}$ for any $k \in \mathbb{N}$. It is easy to see that $(r_k, s_k)_{k\in\mathbb{N}}$ is a sequence of points of U and that $\lim_{k\to\infty} s_k/r_k = 1$ holds. Combining this remark with (5)–(7) we easily conclude

$$\lim_{k\to\infty} \Phi(r_k, s_k) = g_{\mathbf{0}}.$$

This shows that the point $(\mathbf{0}, g_{\mathbf{0}})$ belongs to the Euclidean closure, and thus to the Zariski closure, of the graph of the restriction $\Phi|_U$ of Φ to $U := \mathcal{D} \setminus \{\mathbf{0}\}$, as claimed. Therefore, Φ also satisfies condition (i) of Definition 2. Since $\mathcal{D}$ is an irreducible open curve, we conclude that $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ is also hereditary.

Therefore Φ determines a Hermite–Lagrange interpolation problem in the sense of Definition 7.

Now let $\mathcal{D}^* := \mathbb{A}^3$ and consider the canonical dense representation $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$, $\omega^*(a_0, a_1, a_2) := a_0 + a_1X_1 + a_2X_2$ of the bivariate polynomials over $\mathbb{C}$ of degree at most one as the output encoding. Furthermore, let $\Psi : \mathcal{D} \to \mathcal{D}^*$ be the constructible map defined for $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ by

$$\Psi(d) := \left(f(\mathbf{0}), \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2}, \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2}\right)$$

and for $d = \mathbf{0}$ by

$$\Psi(\mathbf{0}) := \left(f(\mathbf{0}), \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right), \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)\right).$$

Then Ψ is a hereditary (and even topologically robust) map which solves the Hermite–Lagrange problem determined by Φ.

It is important to observe that, in general, neither Φ nor Ψ are strongly continuous. In fact, let $(r_k)_{k\in\mathbb{N}}$ be a sequence of positive reals converging to $0 \in \mathbb{R}$ and let $(s_k)_{k\in\mathbb{N}}$ be the sequence of positive reals defined by $s_k := -r_k\sqrt{1+r_k}$ for any $k \in \mathbb{N}$. It is easy to see that $(r_k, s_k)_{k\in\mathbb{N}}$ is a sequence of points of $\mathcal{D}$ converging to $\mathbf{0}$ and that $\lim_{k\to\infty} s_k/r_k = -1$ holds. Combining this remark with (5)–(7) we easily conclude

$$\lim_{k\to\infty} \Phi(r_k, s_k) = f(\mathbf{0}) + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) - \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_1 + \frac{1}{2}\left(-\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_2.$$

For $(\partial f/\partial X_2)(\mathbf{0}) \neq 0$, the right-hand side of the previous identity is not equal to $g_{\mathbf{0}}$. This shows that Φ is not strongly continuous. A similar argument proves that Ψ is not strongly continuous.

3.3.3. A nonlinear example: identification sequences and interpolation

We retake here the example from Section 3.1.2.

Let $n, L \in \mathbb{N}$ satisfy the condition $2^{L/4} \geq n$, and let $\mathcal{O}$ be the subset of $\Pi^{(n)} = \mathbb{C}[X]$ of the n-variate polynomials with complex coefficients that can be evaluated by a division-free straight-line program of nonscalar length at most L.

We remark that any polynomial $f \in \mathcal{O}$ has a degree bounded by 2^L. Moreover $\mathcal{O} \subset \Pi^{(n)}_{2^L}$ may be considered as a constructible subset of $\mathbb{A}^{n_L}$, where $n_L := \binom{2^L+n}{n}$ (see [16, Theorem 3.2] or [8, Exercise 9.18]). Observe that $\mathcal{O}$ is a cone of $\mathbb{A}^{n_L}$.

Let $\overline{\mathcal{O}}$ denote the closure of $\mathcal{O}$ with respect to the strong or Zariski topology of $\mathbb{A}^{n_L}$. It turns out that $\overline{\mathcal{O}}$ is an irreducible variety that also forms a cone in $\mathbb{A}^{n_L}$. The elements of $\overline{\mathcal{O}}$ may be considered as polynomials of $\Pi^{(n)}_{2^L}$ which have *approximate complexity* bounded by L (see [1, Lemma 2 and Satz 4]).

Let $K := 4(L+n+1)^2 + 2$. According to [9, Corollary 2] (see also [16, Theorem 4.4]), there exist integer points $\gamma_1, \ldots, \gamma_K \in \mathbb{A}^n$ of bit length at most $4(L+1) \leq 2\sqrt{K}$ such that for any two polynomials $f, g \in \overline{\mathcal{O}}$ the equalities $f(\gamma_j) = g(\gamma_j)$ for $1 \leq j \leq K$ imply $f = g$. Such a sequence $\gamma := (\gamma_1, \ldots, \gamma_K)$ of points of $\mathbb{A}^n$ is called an *identification sequence* for the class of polynomials $\overline{\mathcal{O}}$. Let $\gamma := (\gamma_1, \ldots, \gamma_K)$ be a given identification sequence for $\overline{\mathcal{O}}$ and let $\Xi : \overline{\mathcal{O}} \to \mathbb{A}^K$ be the polynomial map defined for $f \in \overline{\mathcal{O}}$ by

$$\Xi(f) := \big(f(\gamma_1), \ldots, f(\gamma_K)\big).$$

Furthermore, let $N := K$ and let $\mathcal{D}$ be the constructible subset of $\mathbb{A}^N$ defined by $\mathcal{D} := \Xi(\mathcal{O})$. Then [9, Corollary 3] implies that $\overline{\mathcal{D}}$ is an affine, closed and irreducible cone of $\mathbb{A}^N$ and $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ is a homeomorphic (with respect to the Zariski and the strong topology), birational, finite morphism of irreducible affine varieties. In particular, the map $\Phi := \Xi^{-1} : \mathcal{D} \to \Pi_{2^L}$ is constructible. Moreover, in terms of Definition 14 of Section 4.2, Φ is geometrically robust. Thus Proposition 16 and Corollary 18 of Section 4.2 imply that Φ is topologically robust and hereditary. Therefore Φ determines a Lagrange interpolation problem in the sense of Definition 7.

Observe that the choice of $\gamma = (\gamma_1, \ldots, \gamma_K)$ as an identification sequence for $\overline{\mathcal{O}}$ implies that for any point $y := (y_1, \ldots, y_K) \in \mathcal{D}$ there exists a *unique* interpolant $f \in \mathcal{O}$ which solves the Lagrange interpolation problem for the interpolation datum y. Therefore the constructible set $\mathcal{O}$ represents the output object class of a Lagrange interpolation problem determined by $\mathcal{D}$ and a well-defined constructible map $\Phi : \mathcal{D} \to \Pi^{(n)}_{2^L}$ with image $\mathcal{O}$. Observe also that this Lagrange interpolation problem is *nonlinear* in the sense that the space of interpolants $\mathcal{O}$ is nonlinear (it is not closed under additions).

Section 5.2 will be devoted to the study of the algorithmic hardness of solving this particular interpolation problem, i.e., to the hardness of reconstructing the polynomials of $\mathcal{O}$ from their values in an identification sequence.

3.4. A complexity measure for Hermite–Lagrange interpolation algorithms and problems

Let n, D and N be fixed natural numbers, let $\mathcal{D}$ be a constructible subset of the affine space $\mathbb{A}^N$ and let $\Phi : \mathcal{D} \to \Pi_D^{(n)}$ be a given topologically robust and hereditary map such that $\mathcal{D}$ and Φ determine a Hermite–Lagrange interpolation problem. We call N *the input size of the given interpolation problem*.

Let $\mathcal{D}^*$ be a constructible subset of an affine space $\mathbb{A}^M$ acting as output data structure, $\omega^* : \mathcal{D}^* \to \Pi_D^{(n)}$ a polynomial encoding of the output objects $\Phi(\mathcal{D})$ and $\Psi : \mathcal{D} \to \mathcal{D}^*$ a hereditary map such that $\mathcal{D}^*$, ω^* and Ψ represent a Hermite–Lagrange interpolation algorithm that solves the given interpolation problem. We measure the complexity of this interpolation algorithm by the size of the output data, namely M.

The complexity of the Hermite–Lagrange interpolation problem determined by $\mathcal{D}$ and Φ is the minimal nonnegative integer M such that there exists an interpolation algorithm with output data structure of size M which solves the problem.

For instance, the complexity of the (generic) univariate Lagrange interpolation problem at K fixed nodes introduced in Section 3.3.1 is at least $K = N$ (compare Proposition 21).

We observe that this notion of complexity is a suitable generalization of three common data size measures of complexity in effective elimination theory: the size of the dense or sparse representation and the (nonscalar) length of the straight-line program representation of multivariate polynomials. For instance, let $\mathcal{O}$ be the output object class of a given elimination problem and assume that the elements of $\mathcal{O}$ are of bounded degree. Then the polynomials contained in $\mathcal{O}$ generate a $\mathbb{C}$-linear ambient space of finite dimension, say M. Thus M is a lower bound for the dense representation of a "worst-case" element of $\mathcal{O}$. This implies that any algorithm that solves the underlying elimination problem and returns the output polynomials belonging to $\mathcal{O}$ in their dense representation, requires at least time M.

On the other hand, for a given polynomial $F \in \Pi^{(n)}$ we may consider the minimal nonscalar length $L(F)$ of a division-free straight-line program that evaluates F. Let $L \in \mathbb{N}$ and set $W_L := \{F \in \mathbb{C}[X_1, \ldots, X_n] : L(F) \leq L\}$. From [8, Exercise 9.18] (see also [16, Theorem 3.2]) we deduce that W_L is a constructible subset of $\Pi_{2^L}^{(n)}$ which is the image of a polynomial map $\mathbb{A}^{(L+n+1)^2} \to \Pi_{2^L}^{(n)}$, where $(L+n+1)^2$ is the number of parameters required to represent the elements of W_L as instances of a generic division-free straight-line program of nonscalar size L with n inputs. Thus the dimension $(L+n+1)^2$ of the parameter space $\mathbb{A}^{(L+n+1)^2}$ reflects the data size of the representation of the elements of W_L by means of division-free straight-line programs. Since a generic element of W_L requires such a representation of size at least $(L+n+1)^2$, we conclude that, in case that W_L is contained in $\mathcal{O}$, the quantity $(L+n+1)^2$ is a lower bound for the complexity of any algorithm which solves the elimination problem considered before and returns the output polynomials belonging to $\mathcal{O}$ in a straight-line program representation.

4. Robust interpolation algorithms

This section is devoted to the geometric and algebraic modeling of coalescence phenomena (see, e.g., [4,10,24]) in the context of Hermite–Lagrange interpolation.

The main issue is the notion of a *geometrically robust* map which captures simultaneously the concepts of topological robustness and hereditarity introduced in Section 2. This allows us to model geometrically and algebraically the intuitive meaning of limit interpolation problems and algorithms. The notion of topological robustness will serve us as an intermediate step for a better understanding of the rather technical concept of geometrical robustness.

To this end we shall begin with an algebraic characterization of the notion of a topologically robust map (Theorem 9 and Corollary 11). Then we shall introduce the notion of a geometrically robust map and show that such maps are always hereditary (Corollary 18). Using the concept of geometrical robustness of constructible maps we shall finally arrive at the notion of a geometrically robust interpolation problem and algorithm, which captures a certain meaning of coalescence. This notion will be discussed by means of concrete examples in Sections 4.3 and 5 under the aspects of interpolation and complexity theory.

We start by recalling some basic definitions and facts from the theory of valuations and places.

4.1. Basic notions and facts from the theory of places

We briefly state the definition of places and some basic algebraic facts concerning them (see [29,20] for more details and proofs). In order to avoid unnecessary generality, we limit our exposition to the context of $\mathbb{C}$-algebras and fields.

Let K and Ω be two (commutative) $\mathbb{C}$-fields. An *Ω-valued place* (or simply place) of the $\mathbb{C}$-field K is a ring homomorphism $\vartheta : R_\vartheta \to \Omega$ where R_ϑ is a $\mathbb{C}$-algebra contained in K such that R_ϑ and ϑ satisfy the following condition:

$$x \in K \setminus R_\vartheta \quad \text{implies} \quad 1/x \in R_\vartheta \quad \text{and} \quad \vartheta(1/x) = 0.$$

The $\mathbb{C}$-algebra R_ϑ with maximal ideal $\ker \vartheta$ is local, and is called the *valuation ring* of the place ϑ. Associating to $x \in K \setminus R_\vartheta$ the value "infinity" we shall write $\vartheta(x) := \infty$. Thus we may interpret the place ϑ as a (total) map $\vartheta : K \to \Omega \cup \{\infty\}$.

We recall the following two basic and well-known results.

Theorem I (*Extension of Places [29, Ch. VI, Section 4, Theorem 5'] and [20, Ch. VII, Section 3, Corollary 3.3]*)**.** *Let A be a $\mathbb{C}$-algebra contained in the field K and let $\epsilon : A \to \Omega$ be a $\mathbb{C}$-algebra homomorphism from A to the $\mathbb{C}$-field Ω. Then ϵ can be extended to a place ϑ of K. If Ω is algebraically closed, the place ϑ can be chosen to be Ω-valued.*

Theorem II (*Places and Integral Closure [20, Ch. VII, Section 3, proof of Proposition 3.5]*)**.** *Let A be a $\mathbb{C}$-algebra contained in the field K. Then the intersection $\bigcap_\vartheta R_\vartheta$, where ϑ runs over all places of K with $A \subset R_\vartheta$, is the integral closure of A in K.*

If A is an integral domain which is a local $\mathbb{C}$-algebra with residue class field $\mathbb{C}$ and is essentially of finite type (i.e., is a localization of a ring which is finitely generated over $\mathbb{C}$), then the integral closure of A in its fraction field is the intersection of the valuation rings of the $\mathbb{C}$-valued places containing A.

We are now going to paraphrase geometrically the rather abstract notion of a $\mathbb{C}$-valued place.

Let V be an irreducible affine variety and let x be a fixed point of V. Observe that evaluating the coordinate functions of V, namely the elements of $\mathbb{C}[V]$, at the point x yields a $\mathbb{C}$-algebra homomorphism $ev_x : \mathbb{C}[V] \to \mathbb{C}$ which characterizes the point $x \in V$. Let $A := \mathbb{C}[V], K := \mathbb{C}(V), \Omega := \mathbb{C}, \epsilon := ev_x$ and fix any $\mathbb{C}$-valued place $\vartheta : K \to \mathbb{C} \cup \{\infty\}$ such that ϑ extends ϵ. Then ϑ associates to each rational function φ of V a value $\vartheta(\varphi)$ which may be finite or infinite. In the first case we consider the rational function well defined and evaluable with value $\vartheta(\varphi)$ at the point $x \in V$. In the second case we consider the point $x \in V$ as a point of indeterminacy or pole of the rational function φ. In view of [28, 1.3.4, Corollaire 2] we may say that the place ϑ mimics the evaluation of rational functions on the normalization of a suitable curve germ at the point x of the variety V.

4.2. The notion of geometrical robustness

For the moment let us fix a constructible subset $\mathcal{M}$ of the affine space $\mathbb{A}^n$ and a (total) constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ with components $\phi_1, \ldots, \phi_m$. Suppose the ϕ is weakly continuous in the sense of Definition 2 in Section 2, namely

there exists a Zariski open and dense subset U of $\mathcal{M}$ such that the restriction $\phi|_U$ is a rational map of $\mathcal{M}$ and the graph of ϕ is contained in the Zariski closure Γ of the graph of $\phi|_U$ in $\mathcal{M} \times \mathbb{A}^m$.

Observe that Γ is a constructible subset of $\mathbb{A}^n \times \mathbb{A}^m$ that contains the graph of ϕ. Furthermore, let $\pi : \Gamma \to \mathcal{M}$ be the first projection of Γ onto $\mathcal{M}$ which for $(x, y) \in \Gamma$ is defined by $\pi(x, y) := x$. Observe that π is a polynomial map.

We recall from Definition 2 of Section 2 that the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is topologically robust if and only if it is weakly continuous and satisfies the following condition:

(∗) *for any sequence $(x_k)_{k\in\mathbb{N}}$ of $\mathcal{M}$ which converges in the Euclidean topology to a point of $\mathcal{M}$, the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ is bounded.*

This condition is equivalent to the robustness of the surjective polynomial map $\pi : \Gamma \to \mathcal{M}$ in the sense of [9, Definition 3]. More precisely, we have the following fact.

Remark 8. Let notations and assumptions be as above. The weakly continuous constructible map ϕ satisfies condition $(*)$ if and only if for any sequence $(x_k, y_k)_{k\in\mathbb{N}}$ of points of Γ such that $(x_k)_{k\in\mathbb{N}}$ converges to a point $x_0 \in \mathcal{M}$, there exists an accumulation point y_0 of the sequence $(y_k)_{k\in\mathbb{N}}$ with $(x_0, y_0) \in \Gamma$.

Proof. Assume that ϕ satisfies condition $(*)$ above and let $(x_k, y_k)_{k\in\mathbb{N}}$ be a sequence of points of Γ such that $(x_k)_{k\in\mathbb{N}}$ converges to a point $x_0 \in \mathcal{M}$. Let $(u_k, v_k)_{k\in\mathbb{N}}$ be a sequence of the graph of $\phi|_U$ with $\|(x_k, y_k) - (u_k, v_k)\| < 1/k$ for any $k \in \mathbb{N}$, where $\|\cdot\|$ denotes the Euclidean norm of $\mathbb{A}^n \times \mathbb{A}^m$. Then $(u_k)_{k\in\mathbb{N}}$ converges to $x_0 \in \mathcal{M}$ and thus condition $(*)$ implies that the sequence $(v_k)_{k\in\mathbb{N}} = (\phi(u_k))_{k\in\mathbb{N}}$ is bounded. We conclude that the sequence $(y_k)_{k\in\mathbb{N}}$ is also bounded, containing therefore a convergent subsequence. Hence the sequence $(x_k, y_k)_{k\in\mathbb{N}}$ has a convergent subsequence, whose limit (x_0, y_0) necessarily belongs to Γ because Γ is closed in $\mathcal{M} \times \mathbb{A}^m$ with respect to the Euclidean topology and x_0 belongs to $\mathcal{M}$.

Assume now that ϕ satisfies the second condition of the statement of the remark and let $(x_k)_{k\in\mathbb{N}}$ be a sequence of $\mathcal{M}$ which converges in the Euclidean topology to a point $x_0 \in \mathcal{M}$. Then there exists a sequence $(u_k)_{k\in\mathbb{N}}$ of U converging also to x_0. We claim that the sequence $(\phi(u_k))_{k\in\mathbb{N}}$ is bounded. Otherwise, there exists a sequence $(\phi(u_{k_l}))_{l\in\mathbb{N}}$ such that $(\|\phi(u_{k_l})\|)_{l\in\mathbb{N}}$ diverges to infinity. On the other hand, the sequence $(u_{k_l}, \phi(u_{k_l}))_{l\in\mathbb{N}}$ satisfies the hypothesis of the second condition of the statement of the remark, but the sequence $(\phi(u_{k_l}))_{l\in\mathbb{N}}$ has no accumulation point. This contradicts the hypothesis on ϕ and proves the claim. Hence the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ is bounded, which finishes the proof. □

We now consider the Zariski closure $\overline{\mathcal{M}}$ of the constructible subset $\mathcal{M}$ of $\mathbb{A}^n$. Observe that $\overline{\mathcal{M}}$ is a closed affine subvariety of $\mathbb{A}^n$ and that we may interpret $\mathbb{C}(\overline{\mathcal{M}})$ as a $\mathbb{C}[\overline{\mathcal{M}}]$-module (or algebra). Now fix an arbitrary point x of $\overline{\mathcal{M}}$. By $\mathfrak{M}_x$ we denote the maximal ideal of coordinate functions of $\mathbb{C}[\overline{\mathcal{M}}]$ which vanish at the point x, by $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ the local $\mathbb{C}$-algebra of the variety $\overline{\mathcal{M}}$ at the point x, i.e., the localization of $\mathbb{C}[\overline{\mathcal{M}}]$ at the maximal ideal $\mathfrak{M}_x$ and by $\mathbb{C}(\overline{\mathcal{M}})_{\mathfrak{M}_x}$ the localization of the $\mathbb{C}[\overline{\mathcal{M}}]$-module $\mathbb{C}(\overline{\mathcal{M}})$ at $\mathfrak{M}_x$.

We suppose now that the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is topologically robust. Then we may interpret $\phi_1, \ldots, \phi_m$ as rational functions of the affine variety $\overline{\mathcal{M}}$ and therefore as elements of the total fraction ring $\mathbb{C}(\overline{\mathcal{M}})$ of $\mathbb{C}[\overline{\mathcal{M}}]$. Thus $\mathbb{C}[\overline{\mathcal{M}}][\phi_1, \ldots, \phi_m]$ and $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ are $\mathbb{C}$-subalgebras of $\mathbb{C}(\overline{\mathcal{M}})$ and $\mathbb{C}(\overline{\mathcal{M}})_{\mathfrak{M}_x}$ which contain $\mathbb{C}[\overline{\mathcal{M}}]$ and $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$, respectively.

With these notations we are able to formulate the following statement which establishes the bridge to an algebraic understanding of the notion of topological robustness.

Theorem 9. *Let notations and assumptions be as before. Assume that the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is topologically robust and let x be an arbitrary point of $\mathcal{M}$. Then $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ is a finite $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$-module.*

Theorem 9 is an immediate consequence of Remark 8 and [9, Lemma 3], which in its turn is based on a non-elementary and deep result from algebraic geometry, namely Zariski's Main Theorem (see, e.g., [17, Section IV.2]). This illustrates that Theorem 9 is a nontrivial result of interpolation theory that requires sophisticated tools from algebraic geometry.

In what follows, Theorem 9 will be only used as a motivation for the more technical notion of geometric robustness which we are going to define later in this section. If we replace condition $(*)$ above by a stronger condition, namely

$(**)$ *for any sequence $(x_k)_{k\in\mathbb{N}}$ of points of $\mathcal{M}$ which converges in the Euclidean topology to a point $x \in \overline{\mathcal{M}}$, the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ remains bounded,*

the conclusion of Theorem 9 is easier to prove.

In this sense we shall give in Remark 10 an *elementary* proof of Theorem 9 under the assumption that $\mathcal{M}$ is *closed*, i.e., in case $\overline{\mathcal{M}} = \mathcal{M}$. Therefore, if we accept to restrict the notion of topological robustness to the cases where condition $(**)$ is satisfied, then Remark 10 allows us to keep the paper

self-contained. We observe that all statements of this paper about topologically robust maps remain valid if we replace in the condition $(*)$ in the definition of the notion of topologically robust maps by the requirement $(**)$.

The following arguments retake techniques of the proofs of [28, 1.3.4, Corollaire 2] and [1, Satz 2].

Remark 10 (*Proof of* Theorem 9 *in case* $\overline{\mathcal{M}} = \mathcal{M}$)**.** Suppose that $\overline{\mathcal{M}} = \mathcal{M}$ holds. Thus $\mathcal{M}$ is a closed subvariety of $\mathbb{A}^n$.

First of all we observe that we may assume without loss of generality that $\mathcal{M}$ is irreducible. Hence $\mathbb{C}[\mathcal{M}]$ is a zero-divisor-free $\mathbb{C}$-algebra, $\mathbb{C}(\mathcal{M})$ is a $\mathbb{C}$-field and for any $x \in \mathcal{M}$ the $\mathbb{C}$-algebras $\mathbb{C}[\mathcal{M}]_{\mathfrak{M}_x}$ and $\mathbb{C}[\mathcal{M}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ are extensions of $\mathbb{C}[\mathcal{M}]$ and $\mathbb{C}[\mathcal{M}][\phi_1, \ldots, \phi_m]$ respectively.

Under these conditions, Theorem 9 asserts that $\mathbb{C}[\mathcal{M}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ is an integral $\mathbb{C}$-algebra extension of $\mathbb{C}[\mathcal{M}]_{\mathfrak{M}_x}$.

Interpreted as a rational map, ϕ has a domain, say U, which is a nonempty Zariski open subset of $\mathcal{M}$. Denote by r the dimension of $\mathcal{M}$ and suppose without loss of generality that $X_1, \ldots, X_n$ are in a generic position with respect to $\mathcal{M}$. Furthermore, let us write $X' := (X_1, \ldots, X_r)$ and $\nu : \mathcal{M} \to \mathbb{A}^r$ for the finite surjective morphism of affine varieties defined for an arbitrary point $z := (z_1, \ldots, z_n)$ of $\mathcal{M}$ by $\nu(z) := (z_1, \ldots, z_r)$.

Suppose now that the conclusion of Theorem 9 is wrong. Then there exists a point $x := (x_1, \ldots, x_n)$ of $\mathcal{M}$ and a component of ϕ, say the rational function ϕ_1, such that ϕ_1 is not integral over $\mathbb{C}[\mathcal{M}]_{\mathfrak{M}_x}$.

Write $x' := (x_1, \ldots, x_r)$ and let $\mathfrak{M}_{x'}$ be the maximal ideal of $\mathbb{C}[X']$ generated by $X_1 - x_1, \ldots, X_r - x_r$. Then ϕ_1 is not integral over $\mathbb{C}[X']_{\mathfrak{M}_{x'}}$, either.

Let T be a new indeterminate and let $\alpha(X', T) := A_q T^q + \cdots + A_0$ with $A_q, \ldots, A_0 \in \mathbb{C}[X']$, $q > 0$ and $\deg A_q \geq 1$, be the primitive irreducible polynomial of ϕ_1 over $\mathbb{C}[X']$. Since ϕ_1 is not integral over $\mathbb{C}[X']_{\mathfrak{M}_{x'}}$, there exists an index $0 \leq h < q$ such that A_h/A_q does not belong to $\mathbb{C}[X']_{\mathfrak{M}_{x'}}$. Observe that the polynomial $\alpha(X', T)$ describes the Zariski closure of the image of the map $\mu : U \to \mathbb{A}^{r+1}$ defined for $z \in U$ by $\mu(z) := (\nu(z), \phi_1(z))$. Thus there exists a nonempty Zariski open subset $\mathcal{G}$ of $\mathbb{A}^r$ such that any $y \in \mathcal{G}$ satisfies the condition $A_q(y) \neq 0$ and such that for any $t \in \mathbb{C}$ with $\alpha(y, t) = 0$ there exists an element $z \in U$ with $\mu(z) = (\nu(z), \phi_1(z)) = (y, t)$.

In order to simplify notations, we shall assume without loss of generality that the nonzero polynomials A_h and A_q contain no common prime divisors. From [13, Chapter V, Theorem 3.12] we deduce that there exists a sequence $(s_k)_{k\in\mathbb{N}}$ of elements of $\mathcal{G}$ such that $(s_k)_{k\in\mathbb{N}}$ converges to x' in the Euclidean topology of $\mathbb{A}^r$ and such that the sequence $\left(\frac{A_h}{A_q}(s_k)\right)_{k\in\mathbb{N}}$ converges to infinity.

Therefore there exists an *unbounded* sequence $(t_k)_{k\in\mathbb{N}}$ of complex numbers which satisfies for any $k \in \mathbb{N}$ the condition $\alpha(s_k, t_k) = 0$.

This implies the existence of a sequence $(z_k)_{k\in\mathbb{N}}$ of elements of U such that $\mu(z_k) = (\nu(z_k), \phi_1(z_k)) = (s_k, t_k)$ holds for any $k \in \mathbb{N}$. Hence the sequence $(\phi_1(z_k))_{k\in\mathbb{N}}$ is unbounded, whereas the sequence $\nu(z_k)_{k\in\mathbb{N}}$ tends to x'. Since $\nu : \mathcal{M} \to \mathbb{A}^r$ is a finite morphism of affine varieties, we conclude that the sequence $(z_k)_{k\in\mathbb{N}}$ is bounded. Therefore we may assume without loss of generality that $(z_k)_{k\in\mathbb{N}}$ converges to a point $z \in \mathbb{A}^n$.

Since by assumption $\mathcal{M}$ is closed and z_k belongs to $\mathcal{M}$ for any $k \in \mathbb{N}$, we infer that z is an element of $\mathcal{M}$. We have therefore found a sequence of points of $\mathcal{M}$, namely $(z_k)_{k\in\mathbb{N}}$, which converges to an element of $\mathcal{M}$, namely z, such that the sequence $(\phi_1(z_k))_{k\in\mathbb{N}}$ is unbounded. This implies the unboundedness of the sequence $(\phi(z_k))_{k\in\mathbb{N}}$, which contradicts by $(*)$ the assumption that ϕ is topologically robust. □

Corollary 11. *Let notations and assumptions be as before and suppose in particular that the constructible map* $\phi : \mathcal{M} \to \mathbb{A}^m$ *is weakly continuous. Then* ϕ *is topologically robust if and only if for any point* x *of* $\mathcal{M}$ *the* $\mathbb{C}$*-algebra* $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ *is a finite* $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$*-module.*

Proof. The *only if* part of this statement is the content of Theorem 9.

We are now going to show the *if* part. Our argumentation is self-contained and uses ideas of the proof of [9, Lemma 3].

Since ϕ is weakly continuous, there exists an open dense Zariski subset U of $\mathcal{M}$ which satisfies condition (i) of Definition 2. Let $(x_k)_{k\in\mathbb{N}}$ be a given sequence of points of U which converges to a point $x \in \mathcal{M}$. Following Remark 3, it suffices to show that the sequence $(\phi(x_k))_{k\in\mathbb{N}}$ is bounded.

By assumption $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}[\phi_1, \ldots, \phi_m]$ is a finite $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}$-module. Therefore there exists an element g of $\mathbb{C}[\overline{\mathcal{M}}]$ with $g(x) \neq 0$ such that $\mathbb{C}[\overline{\mathcal{M}}]_g[\phi_1, \ldots, \phi_m]$ is also a finite $\mathbb{C}[\overline{\mathcal{M}}]_g$-module.

There exist at most finitely many indices $k \in \mathbb{N}$ with $g(x_k) = 0$, since otherwise the continuity of g would imply $g(x) = 0$, a contradiction. Therefore we may suppose without loss of generality that $g(x_k) \neq 0$ holds for any $k \in \mathbb{N}$.

Let T be a new indeterminate. There exists a monic polynomial $P_1(T)$ of $\mathbb{C}[\overline{\mathcal{M}}]_g[T]$ with $P_1(\phi_1) = 0$. Observe that $P_1(T)$ may be specialized for x and $x_k, k \in \mathbb{N}$, into well-defined polynomials $P_1(x)(T), P_1(x_k)(T)$ of $\mathbb{C}[T]$ and complex numbers $P_1(x_k)(\phi_1(x_k))$. Moreover we have $\deg P_1(x)(T) = \deg P_1(x_k)(T) = \deg P_1(T)$ and there exists an upper bound for the roots of the polynomials $P_1(x_k)(T)$ which does not depend on $k \in \mathbb{N}$. From $P_1(\phi_1) = 0$ we infer therefore that $P_1(x_k)(\phi_1(x_k)) = 0$ holds for any $k \in \mathbb{N}$. This implies that the sequence $(\phi_1(x_k))_{k\in\mathbb{N}}$ is bounded. Repeating the same argument for $\phi_2, \ldots, \phi_m$ we conclude that $(\phi(x_k))_{k\in\mathbb{N}}$ is also bounded. □

Corollary 12. *Let $\phi : \mathcal{M} \to \mathbb{A}^m$ be topologically robust and suppose that the affine variety $\overline{\mathcal{M}}$ is normal at any point of $\mathcal{M}$. Then $\phi : \mathcal{M} \to \mathbb{A}^m$ is a rational map of $\overline{\mathcal{M}}$ whose domain contains $\mathcal{M}$ and is therefore strongly continuous.*

Proof. Let x be an arbitrary point of $\mathcal{M}$. Since $\overline{\mathcal{M}}$ is normal at x, it follows that x belongs to a unique irreducible component, say $\mathcal{M}_1$, of $\overline{\mathcal{M}}$. Observe now the identity $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x} = \mathbb{C}[\mathcal{M}_1]_{\mathfrak{m}_x}$. The topological robustness of ϕ implies that the $\mathbb{C}$-algebra extension $\mathbb{C}[\mathcal{M}_1]_{\mathfrak{m}_x} \hookrightarrow \mathbb{C}[\mathcal{M}_1]_{\mathfrak{m}_x}[\phi_1, \ldots, \phi_m]$ is integral. Taking into account that x is a normal point of $\mathcal{M}_1$, we infer that $\mathbb{C}[\mathcal{M}_1]_{\mathfrak{m}_x}$ is integrally closed in $\mathbb{C}(\mathcal{M}_1)$. Theorem 9 implies now that the rational functions $\phi_1, \ldots, \phi_m$ are contained in $\mathbb{C}[\mathcal{M}_1]_{\mathfrak{m}_x} = \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}$. Therefore the rational map ϕ is well defined at the point x. □

In case that the constructible set $\mathcal{M}$ is irreducible, we may characterize the topological robustness of the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ in a very natural way by means of places. In Section 5 the use of the notion of topological robustness will be limited to this case.

Proposition 13. *Let notations and assumptions be as before and suppose that $\mathcal{M}$ is irreducible. Then the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is topologically robust if and only if ϕ is weakly continuous and if for any point $x \in \mathcal{M}$ and any $\mathbb{C}$-valued place $\vartheta : \mathbb{C}(\overline{\mathcal{M}}) \to \mathbb{C} \cup \{\infty\}$ that extends the $\mathbb{C}$-algebra homomorphism $ev_x : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$, the values $\vartheta(\phi_1), \ldots, \vartheta(\phi_m)$ are finite.*

Proposition 13 is an immediate consequence of Corollary 11 and Theorem II and its proof will be omitted here.

By the way, let us observe that for $x \in \mathcal{M}$, the $\mathbb{C}$-valued place ϑ extends the $\mathbb{C}$-algebra homomorphism ev_x if and only if the local $\mathbb{C}$-algebra $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_x}$ is contained in the valuation ring of ϑ.

Proposition 13 motivates the following notion of geometrical robustness.

Definition 14. Let $\phi : \mathcal{M} \to \mathbb{A}^m$ be a constructible map with components $\phi_1, \ldots, \phi_m$ and assume that $\mathcal{M}$ is an irreducible constructible subset of the affine space $\mathbb{A}^n$. Then ϕ is called *geometrically robust* if it satisfies the following condition: for any point $x \in \mathcal{M}$ and any $\mathbb{C}$-valued place $\vartheta : \mathbb{C}(\overline{\mathcal{M}}) \to \mathbb{C} \cup \{\infty\}$ that extends the $\mathbb{C}$-algebra homomorphism $ev_x : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$, the values $\vartheta(\phi_1), \ldots, \vartheta(\phi_m)$ are finite and are *uniquely determined* by the point x (i.e., they do not depend on the particular extension of the $\mathbb{C}$-algebra homomorphism ev_x to a $\mathbb{C}$-valued place ϑ of $\mathbb{C}(\overline{\mathcal{M}})$). Moreover, they satisfy the identities $\vartheta(\phi_1) = \phi_1(x), \ldots, \vartheta(\phi_m) = \phi_m(x)$.

Remark 15. Regular maps and compositions of geometrically robust maps with polynomial maps are geometrically robust.

Proposition 16. *Let notations and assumptions be as in Definition 14 and suppose that the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is geometrically robust. Then ϕ is topologically robust.*

Proof. By assumption $\mathcal{M}$ is an irreducible constructible subset of the affine space $\mathbb{A}^n$. Therefore $\overline{\mathcal{M}}$ is an irreducible closed subvariety of $\mathbb{A}^n$. Let $\xi_1, \ldots, \xi_n$ be the coordinate functions of $\overline{\mathcal{M}}$ induced by the indeterminates $X_1, \ldots, X_n$. Let $X := (X_1, \ldots, X_n)$ and $\xi := (\xi_1, \ldots, \xi_n)$.

In view of Proposition 13 we have only to show that ϕ is weakly continuous.

Following Lemma 1, there exists a Zariski open and dense subset U of $\mathcal{M}$ such that $\phi|_U$ is a rational map. We claim that the graph of ϕ is contained in the Zariski closure of the graph of $\phi|_U$ in $\mathcal{M} \times \mathbb{A}^m$.

Let $Y := (Y_1, \ldots, Y_m)$, where $Y_1, \ldots, Y_m$ are new indeterminates, and let $Q \in \mathbb{C}[X, Y]$ be an arbitrary polynomial which satisfies the condition $Q(x, \phi(x)) = 0$ for any point $x \in U$. Then Q vanishes at any point of the Zariski closure of the graph of $\phi|_U$ in $\mathcal{M} \times \mathbb{A}^m$. It suffices to show that $Q(x, \phi(x)) = 0$ holds for any point $x \in \mathcal{M}$.

Observe that the assumption made on Q implies $Q(\xi, \phi) = Q(\xi, \phi_1, \ldots, \phi_m) = 0$, where $\phi_1, \ldots, \phi_m$ are interpreted as elements of $\mathbb{C}(\overline{\mathcal{M}})$. Let x be an arbitrary point of $\mathcal{M}$ and let $\vartheta : \mathbb{C}(\overline{\mathcal{M}}) \to \mathbb{C} \cup \{\infty\}$ be any $\mathbb{C}$-valued place that extends the $\mathbb{C}$-algebra homomorphism $ev_x : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$. Then $Q(\xi, \phi) = 0$ implies $Q(x, \vartheta(\phi_1), \ldots, \vartheta(\phi_m)) = 0$. By assumption we have $\vartheta(\phi_1) = \phi_1(x), \ldots, \vartheta(\phi_m) = \phi_m(x)$ and hence $Q(x, \phi(x)) = Q(x, \phi_1(x), \ldots, \phi_m(x)) = Q(x, \vartheta(\phi_1), \ldots, \vartheta(\phi_m)) = 0$. □

We are now going to show that a geometrically robust map $\phi : \mathcal{M} \to \mathbb{A}^m$ is always hereditary. For this purpose, we prove the stronger result that the restriction of ϕ to an irreducible constructible subset of $\mathcal{M}$ is geometrically robust.

Theorem 17. *Let notations and assumptions be as in Definition 14. Let $\phi : \mathcal{M} \to \mathbb{A}^m$ be a geometrically robust map and let $\mathcal{N}$ be an irreducible constructible subset of $\mathcal{M}$. Then the restriction map $\phi|_{\mathcal{N}}$ is a geometrically robust map.*

Proof. By assumption $\mathcal{M}$ is an irreducible constructible subset of the affine space $\mathbb{A}^n$ and hence $\overline{\mathcal{M}}$ is a closed and irreducible affine variety of $\mathbb{A}^n$.

Let $\mathcal{Z} := \overline{\mathcal{N}}$ be the Zariski closure of $\mathcal{N}$ in the affine ambient space $\mathbb{A}^n$. Then $\mathcal{Z}$ is a closed irreducible subvariety of $\overline{\mathcal{M}}$ and $\mathcal{N}$ contains a nonempty Zariski open (and hence Zariski dense) subset of $\mathcal{Z}$.

For any point $z \in \mathcal{Z}$, let $ev_z(\overline{\mathcal{M}}) : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}$ and $ev_z(\mathcal{Z}) : \mathbb{C}[\mathcal{Z}] \to \mathbb{C}$ be the $\mathbb{C}$-algebra homomorphisms given by the evaluation of the coordinate functions of $\mathbb{C}[\overline{\mathcal{M}}]$ and $\mathbb{C}[\mathcal{Z}]$ at z, respectively.

We are now going to show that there exist rational functions $\psi_1, \ldots, \psi_m \in \mathbb{C}(\mathcal{Z})$ such that for any point $z \in \mathcal{N}$ and any $\mathbb{C}$-valued place ϑ of $\mathbb{C}(\mathcal{Z})$ that extends the $\mathbb{C}$-algebra homomorphism $ev_z(\mathcal{Z})$, the following holds:

$$\text{the values of } \vartheta \text{ at } \psi_1, \ldots, \psi_m \text{ are finite and satisfy } \vartheta(\psi_1) = \phi_1(z), \ldots, \vartheta(\psi_m) = \phi_m(z).$$

Consider the canonical surjective $\mathbb{C}$-algebra homomorphism $\pi : \mathbb{C}[\overline{\mathcal{M}}] \to \mathbb{C}[\mathcal{Z}]$ induced by the natural embedding of $\mathcal{Z}$ into $\overline{\mathcal{M}}$. From Theorem I we deduce that there exists a field Ω containing $\mathbb{C}(\mathcal{Z})$ such that π can be extended to an Ω-valued place of $\mathbb{C}(\overline{\mathcal{M}})$ that we also denote by π. Let R_π be the valuation ring of the place π. Observe that R_π contains $\mathbb{C}[\overline{\mathcal{M}}]$ and even its localization $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_z}$ at the (maximal) vanishing ideal $\mathfrak{M}_z$ of any point z of $\mathcal{Z}$.

Let $1 \le j \le m$ and let z_0 be an arbitrary (but fixed) element of $\mathcal{Z}$. We denote by $\mathfrak{M}'_{z_0}$ the maximal ideal of the coordinate functions of $\mathbb{C}[\mathcal{Z}]$ that vanish at the point z_0. By assumption $\phi : \mathcal{M} \to \mathbb{A}^m$ is geometrically robust. Therefore, by Theorem II, the rational function ϕ_j belongs to the integral closure of $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$ in $\mathbb{C}(\overline{\mathcal{M}})$. Hence there exists a monic polynomial

$$\alpha = \alpha(T) = T^s + a_{s-1}T^{s-1} + \cdots + a_0$$

of $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[T]$ such that $\alpha(\phi_j) = 0$ holds in $\mathbb{C}(\overline{\mathcal{M}})$ (here s is a positive integer and T a new indeterminate). Taking into account that the valuation ring R_π contains $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$, we deduce from Theorem II that ϕ_j belongs to R_π. Therefore the value $\psi_j := \pi(\phi_j)$ is finite and integral over $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}$. In particular, $\psi_j \in \Omega$ is algebraic over $\mathbb{C}(\mathcal{Z})$ and

$$\pi(\alpha) = \pi(\alpha)(T) := T^s + \pi(a_{s-1})T^{s-1} + \cdots + \pi(a_0) \in \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$$

is an algebraic dependence relation for ψ_j over $\mathbb{C}(\mathcal{Z})$ (which is not necessarily of minimal degree).

Let $m_{\psi_j} \in \mathbb{C}(\mathcal{Z})[T]$ be the minimal (monic) polynomial of ψ_j over $\mathbb{C}(\mathcal{Z})$ and let $\Delta_{\psi_j} \in \mathbb{C}(\mathcal{Z})$ be its discriminant. Since m_{ψ_j} is irreducible and $\mathbb{C}(\mathcal{Z})$ is of characteristic zero, we have $\Delta_{\psi_j} \neq 0$. Therefore there exists a nonempty Zariski open subset $\mathcal{U}^*$ of $\mathcal{Z}$ such that for any $z \in \mathcal{U}^*$ the coefficients of the polynomial m_{ψ_j} (and hence also Δ_{ψ_j}) are well defined at z and such that $\Delta_{\psi_j}(z) \neq 0$ holds. Therefore $m_{\psi_j}(z, T)$ is square-free. Since $\mathcal{N}$ is Zariski dense in $\mathcal{Z}$ there exists a nonempty Zariski open subset $\mathcal{U}_j$ of $\mathcal{Z}$ which is contained in $\mathcal{N} \cap \mathcal{U}^*$ (and hence in $\mathcal{N}$). Now assume that $z_0 \in \mathcal{U}_j$. Then $m_{\psi_j}(T)$ belongs to $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$ and $m_{\psi_j}(z_0, T)$ is square-free.

Let $Q(T)$ be an arbitrary polynomial of $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[T]$ with $Q(\phi_j) = 0$ and let $\pi(Q)(T)$ be the polynomial of $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$ obtained by applying the place π to the coefficients of $Q(T)$. Since $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$ is contained in R_π, the place π takes only finite values on the coefficients of $Q(T)$. Thus $\pi(Q)(T)$ is well defined. From $Q(\phi_j) = 0$ we deduce $0 = \pi(Q(\phi_j)) = \pi(Q)(\pi(\phi_j)) = \pi(Q)(\psi_j)$. Therefore the polynomial $m_{\psi_j}(T)$ divides $\pi(Q)(T)$ in $\mathbb{C}(\mathcal{Z})[T]$ and hence also in $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]$, because $m_{\psi_j}(T)$ is monic. This implies that π induces a surjective $\mathbb{C}$-algebra homomorphism

$$\varphi : \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j] \to \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j}.$$

Summarizing we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}} & \xrightarrow{\pi'} & \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}} \\ \downarrow & & \downarrow \\ \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j] & \xrightarrow{\varphi} & \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j}, \end{array}$$

where the vertical arrows are injective and the horizontal arrows are surjective $\mathbb{C}$-algebra homomorphisms and π' is the restriction of the place π to $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}$.

Let $\tau \in \mathbb{C}$ be an arbitrary root of the monic polynomial $m_{\psi_j}(z_0, T) \in \mathbb{C}[T]$. Then evaluation at z_0 and τ induces a $\mathbb{C}$-algebra homomorphism $ev_\tau : \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j} \to \mathbb{C}$ such that the diagram

$$\begin{array}{ccc} \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}} & \xrightarrow{ev_{z_0}(\overline{\mathcal{M}})} & \mathbb{C} \\ \downarrow & \nearrow_{ev_\tau} & \\ \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j} & & \end{array}$$

commutes and such that $\varphi(\phi_j)$, namely the class of T in $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}[T]/m_{\psi_j}$, is mapped onto $\tau \in \mathbb{C}$. From Theorem I we deduce now that the $\mathbb{C}$-algebra homomorphism $ev_\tau \circ \varphi : \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j] \to \mathbb{C}$ may be extended to a $\mathbb{C}$-valued place ϑ_τ of the field $\mathbb{C}(\overline{\mathcal{M}})$. Observe that $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_{z_0}}[\phi_j]$ is contained in the valuation ring of ϑ_τ and that $\vartheta_\tau(\phi_j) = ev_\tau(\varphi(\phi_j)) = \tau$ holds. Since by assumption $\phi : \mathcal{M} \to \mathbb{A}^m$ is geometrically robust, the value $\vartheta_\tau(\phi_j)$ does not depend on the place ϑ_τ. Therefore the univariate polynomial $m_{\psi_j}(z_0, T)$ has a single zero in $\mathbb{C}$, namely τ. From $z_0 \in \mathcal{U}_j \subset \mathcal{U}^*$ we deduce that $m_{\psi_j}(z_0, T)$ is a square-free polynomial of $\mathbb{C}[T]$. Therefore we have $\deg m_{\psi_j}(T) = \deg m_{\psi_j}(z_0, T) = 1$, which implies that ψ_j belongs to $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}'_{z_0}}$.

We conclude that ψ_j is defined everywhere on $\mathcal{U}_j$ for $1 \leq j \leq n$. In this way we obtain rational functions $\psi_1, \ldots, \psi_m$ and nonempty Zariski open subsets $\mathcal{U}_1, \ldots, \mathcal{U}_m$ of $\mathcal{Z}$ such that for any $1 \leq j \leq m$ the rational function ψ_j is well defined in $\mathcal{U}_j$ and such that $\mathcal{U}_j$ is contained in $\mathcal{N}$.

Therefore $\mathcal{U} := \mathcal{U}_1 \cap \cdots \cap \mathcal{U}_m$ is a nonempty Zariski open subset of $\mathcal{N}$ where the rational functions $\psi_1, \ldots, \psi_m$ are well defined. Moreover, for any point $z \in \mathcal{U}$ we have $\psi_1(z) = \phi_1(z), \ldots, \psi_m(z) = \phi_m(z)$.

Let $\psi := (\psi_1, \ldots, \psi_m)$. Then ψ is a rational map from $\mathcal{Z}$ to $\mathbb{A}^m$ with $\psi|_{\mathcal{U}} = \phi|_{\mathcal{U}}$. We are going to show that $\phi|_{\mathcal{N}}$ is geometrically robust.

Let z be an arbitrary point of $\mathcal{N}$ and let ϑ be an arbitrary $\mathbb{C}$-valued place of $\mathbb{C}(\mathcal{Z})$ that extends the $\mathbb{C}$-algebra homomorphism $ev_z(\mathcal{Z}) : \mathbb{C}[\mathcal{Z}] \to \mathbb{C}$. Lifting, following Theorem I, the place ϑ to a $\mathbb{C}$-valued place of the field Ω and composing the result with the Ω-valued place π, we obtain a $\mathbb{C}$-valued place ϑ' of $\mathbb{C}(\overline{\mathcal{M}})$ which extends the $\mathbb{C}$-algebra homomorphism $ev_z(\overline{\mathcal{M}})$. Since by assumption $\phi : \mathcal{M} \to \mathbb{A}^m$ is geometrically robust, we conclude that for any $1 \le j \le m$ the value $\vartheta(\psi_j) = \vartheta(\pi(\phi_j)) = \vartheta \circ \pi(\phi_j) = \vartheta'(\phi_j)$ is finite and independent of the choice of ϑ' and hence also of the choice of ϑ. Moreover we have $\vartheta(\psi_j) = \vartheta'(\phi_j) = \phi_j(z)$ for $1 \le j \le m$. We conclude that $\psi|_{\mathcal{N}}$ is geometrically robust. □

Now we are able to prove that a geometrically robust map is hereditary.

Corollary 18. *Let notations and assumptions be as in Definition 14. Suppose that the constructible map $\phi : \mathcal{M} \to \mathbb{A}^m$ is geometrically robust. Then ϕ is hereditary.*

Proof. Let $\mathcal{N}$ be an arbitrary constructible subset of $\mathcal{M}$. We have to show that $\phi|_{\mathcal{N}} : \mathcal{N} \to \mathbb{A}^m$ is weakly continuous, namely that $\phi|_{\mathcal{N}}$ is an extension of a rational map of $\mathcal{N}$ such that the graph of $\phi|_{\mathcal{N}}$ is contained in the Zariski closure of the graph of this rational map in $\mathcal{N} \times \mathbb{A}^m$.

Without loss of generality we may assume that $\mathcal{N}$ is irreducible. According to Theorem 17, the restriction map $\phi|_{\mathcal{N}}$ is geometrically robust. Then Proposition 16 implies that $\phi|_{\mathcal{N}}$ is topologically robust, and in particular weakly continuous. This finishes the proof of the corollary. □

Definition 19. Let n and D be fixed natural numbers and let be given a Hermite–Lagrange interpolation problem determined by a topologically robust and hereditary map $\Phi : \mathcal{D} \to \Pi_D^{(n)}$. Furthermore, let $\omega^* : \mathcal{D}^* \to \Pi_D^{(n)}$ be given a polynomial map and a hereditary map $\Psi : \mathcal{D} \to \mathcal{D}^*$ determining a Hermite–Lagrange interpolation algorithm which solves this problem in the sense of Definition 7. We call this interpolation algorithm *geometrically robust* if Ψ has this property.

Remark 15 implies the following statement.

Remark 20. If for the interpolation problem determined by $\mathcal{D}$ and Φ in Definition 19 there exists a geometrically robust Hermite–Lagrange algorithm, then the constructible map Φ itself is geometrically robust.

4.3. Examples of geometrically robust interpolation algorithms

In this section we analyze whether the algorithms introduced in Sections 3.3.1 and 3.3.2 for the generic Lagrange interpolation problem and the bivariate Lagrange interpolation problem are robust.

4.3.1. Univariate Hermite–Lagrange interpolation of a fixed polynomial

With a slightly different view we turn now back to the second example of Section 3.3.1, namely to the Lagrange interpolation of univariate polynomials in $K \ge 2$ generic nodes. Thus let $n := 1, D := K - 1, M := K, N := K, X := X_1$ and $\Pi_D := \Pi_D^{(n)} = \Pi_D^{(1)}$. Let F be given a univariate polynomial of $\Pi := \mathbb{C}[X]$ with $\deg F \gg K$ and let $\mathcal{D} := \{(d_1, \ldots, d_N) \in \mathbb{A}^N : d_i \ne d_j \text{ for } 1 \le i < j \le N\}$. We consider the univariate Lagrange interpolation problem which consists in finding for any point $d := (d_1, \ldots, d_N) \in \mathcal{D}$ the unique polynomial f_d in Π_D interpolating F in the nodes $d_1, \ldots, d_N$.

Thus f_d is determined by the condition $f_d(d_i) = F(d_i)$ for any $1 \le i \le N$.

Let as in Section 3.3.1 be $\mathcal{D}^* := \mathbb{A}^M$ and denote by $\omega^* : \mathcal{D}^* \to \Pi_D$ the encoding of the elements of Π_D by their dense representation.

For any $d := (d_1, \ldots, d_N) \in \mathcal{D}$ let $V_d := (d_i^{j-1})_{1 \le i,j \le N}$ be the Vandermonde matrix associated to d and $F(d) := (F(d_1), \ldots, F(d_N))$. Then the dense representation of f_d is given by $V_d^{-1}F(d)$. Observe that the (regular) rational maps $\Psi_F : \mathcal{D} \to \mathcal{D}^*$ and $\Phi_F : \mathcal{D} \to \Pi_D$ defined for $d \in \mathcal{D}$ by $\Psi_F(d) := V_d^{-1}F(d)$ and $\Phi_F(d) := \omega^*(\Psi_F(d))$ are strongly continuous (hence topologically robust and hereditary). Therefore $\mathcal{D}$ and Φ_F, and $\mathcal{D}^*$, ω^* and Ψ_F determine a Lagrange interpolation problem and an algorithm in the sense of Definition 7.

The rational map Ψ_F is well defined at any point of $\mathcal{D}$ but it is not *a priori* clear whether Ψ_F has a rational (hence polynomial) extension to $\overline{\mathcal{D}} = \mathbb{A}^N$. However, we may deduce from the well-known Newton or divided difference interpolation method (see, for instance, [27]) that Ψ_F is a polynomial map.

In order to see this, let $T_1, \ldots, T_N$ be new indeterminates, $T := (T_1, \ldots, T_N)$ and let $\Psi_F^{(1)}(T), \ldots, \Psi_F^{(N)}(T) \in \mathbb{C}(T)$ be the components of $\Psi_F(T)$. Moreover, for $1 \leq j \leq N$ let $F[T_1, \ldots, T_j] \in \mathbb{C}[T]$ be the j-th divided difference of F. Observe that $\Psi_F^{(1)}(T), \ldots, \Psi_F^{(N)}(T)$ appear as the coefficients of the polynomial $\sum_{j=1}^{N} F[T_1, \ldots, T_j](X - T_1) \ldots (X - T_{j-1})$ with respect to the indeterminate X.

This implies that $\Psi_F : \mathcal{D} \to \mathcal{D}^*$ is a polynomial map and hence geometrically robust. In other words, the Hermite–Lagrange interpolation algorithm determined by $\mathcal{D}^*$, ω^* and Ψ_F is geometrically robust. Hence $\Phi_F : \mathcal{D} \to \Pi_D$ is also geometrically robust.

Let $\mathcal{D}^+ := \mathbb{A}^N$. Since Ψ_F is a polynomial map and $\mathcal{D}^* = \mathbb{A}^M$ we conclude that Ψ_F may be extended to a geometrically robust map $\Psi_F^+ : \mathcal{D}^+ \to \mathcal{D}^*$. Let $\Phi_F^+ := \omega^* \circ \Psi_F^+$. Then $\Phi_F^+ : \mathcal{D}^+ \to \Pi_D$ is also geometrically (and hence topologically) robust and hereditary. Thus $\mathcal{D}^+$ and Φ_F^+ determine a Hermite–Lagrange interpolation problem and the algorithm determined by $\mathcal{D}^*$, ω^* and Ψ_F^+ solves this problem in the sense of Definition 7.

We are now going to analyze the Hermite–Lagrange interpolation problem determined by $\mathcal{D}^+$ and Φ_F^+ for an arbitrary point $d := (d_1, \ldots, d_M) \in \mathcal{D}^+$.

If d belongs to $\mathcal{D}$ we have the Lagrange interpolation problem considered before. Therefore let $d \in \mathcal{D}^+ \setminus \mathcal{D}$. Then there exist repetitions between the complex numbers $d_1, \ldots, d_N$. For the sake of simplicity we shall assume $d_1 = d_2$ and that $d_1, d_3, \ldots, d_N$ are all distinct. Then $f_d := \omega^*(\Psi_F^+(d))$ is the (unique) polynomial of Π_D which satisfies the condition $f_d(d_1) = F(d_1), f_d'(d_1) = F'(d_1)$ and $f_d(d_i) = F(d_i)$ for $3 \leq i \leq N$ where f_d' and F' denote the first (formal) derivatives of the polynomials f_d and F.

Therefore $\mathcal{D}^+$ and Φ_F^+ determine a Hermite–Lagrange interpolation problem which is not simply of Lagrangian type.

On the other hand, in view of Corollary 12, this example is not very illustrative, since $\mathcal{D}^+ = \mathbb{A}^N$ implies that *any* algorithm determined by $\mathcal{D}^*$, ω^* and a topologically robust, hereditary map $\Psi : \mathcal{D}^+ \to \mathcal{D}^*$, which solves the Hermite–Lagrange interpolation problem given by $\mathcal{D}^+$ and Φ_F^+, is geometrically robust. In this case Ψ is even a polynomial map.

4.3.2. Robustness in presence of singular points: examples of Section 3.3.2 revisited

Let X_1, X_2 be indeterminates over $\mathbb{C}$ and let $\Pi^{(2)} := \mathbb{C}[X_1, X_2]$. We analyze now the algorithms of the two examples for bivariate Hermite–Lagrange interpolation considered in Section 3.3.2. In both examples, there is given a polynomial function $f : \mathbb{A}^2 \to \mathbb{A}^1$ which we wish to interpolate and, as input data structure, an open curve $\mathcal{D} \subset \mathbb{A}^2$ containing $\mathbf{0} := (0, 0)$ as singular point. These two examples differ from the previous one (classical univariate Hermite–Lagrange interpolation) in the fact that the input data structure $\mathcal{D}$ is singular at $\mathbf{0}$.

Interpolation over the curve $X_1^3 - X_2^2 = 0$ Let $\mathcal{D} := \{X_1^3 - X_2^2 = 0\} \setminus \{(-1, \pm \mathrm{i})\} \subset \mathbb{A}^2$ and let $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ be the constructible map defined for $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ by

$$\Phi(d) := f(\mathbf{0}) + \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} X_1 + \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2} X_2$$

and for $d := \mathbf{0}$ by

$$\Phi(\mathbf{0}) := f(\mathbf{0}) + \frac{\partial f}{\partial X_1}(\mathbf{0}) X_1.$$

In Section 3.3.2 we showed that Φ is strongly continuous. Hence $\mathcal{D}$ and Φ determine a Hermite–Lagrange interpolation problem.

As in Section 3.3.2, let $\mathcal{D}^* := \mathbb{A}^3$ and let $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$ be the canonical dense encoding of bivariate polynomials of degree at most one over $\mathbb{C}$. Furthermore, let $\Psi : \mathcal{D} \to \mathcal{D}^*$ be the

constructible map defined for $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ by

$$\Psi(d) := \left(f(\mathbf{0}), \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2}, \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2}\right)$$

and for $d := \mathbf{0}$ by

$$\Psi(\mathbf{0}) := \left(f(\mathbf{0}), \frac{\partial f}{\partial X_1}(\mathbf{0}), 0\right).$$

Then Ψ is hereditary and $\mathcal{D}^*, \omega^*$ and Ψ determine an algorithm that solves the Hermite–Lagrange interpolation problem given by $\mathcal{D}$ and Φ.

We are now going to prove that Ψ is geometrically robust.

Let $\Psi := (\Psi_1, \Psi_2, \Psi_3)$ and denote for any point $d \in \mathcal{D}$ by $\mathfrak{M}_d$ the maximal ideal of coordinate functions of $\mathbb{C}[\mathcal{C}]$, where $\mathcal{C} := \{X_1^3 - X_2^2 = 0\}$ is the (irreducible) Zariski closure of $\mathcal{D}$ in $\mathbb{A}^2$. The rational functions Ψ_1, Ψ_2, Ψ_3 belong to $\mathbb{C}[\mathcal{C}]_{\mathfrak{M}_d}$ for any $d \in \mathcal{D} \setminus \{\mathbf{0}\}$ and thus satisfy the condition of Definition 14 at any point $d \in \mathcal{D} \setminus \{\mathbf{0}\}$. Taking into account that $\Psi_1 = f|_{\mathcal{D}}$ is a polynomial function, we may restrict our attention to the local properties of Ψ_2 and Ψ_3 at the point $\mathbf{0} \in \mathcal{D}$.

Since the plane curve $\mathcal{C}$ is irreducible, $\mathbb{C}[\overline{\mathcal{D}}] = \mathbb{C}[\mathcal{C}]$ is an integral domain with fraction field $\mathbb{C}(\overline{\mathcal{D}})$. Let ξ_1 and ξ_2 be the coordinate functions of $\mathbb{C}[\overline{\mathcal{D}}]$ induced by the indeterminates X_1 and X_2 and let $\xi := (\xi_1, \xi_2)$. We have $\xi_1^3 = \xi_2^2$ and $\xi_1 \neq 0$.

We are now going to show that the rational functions Ψ_2 and Ψ_3 satisfy the condition of Definition 14 at the point $\mathbf{0} \in \mathcal{D}$, thus proving the geometrical robustness of Ψ.

For this purpose consider an arbitrary $\mathbb{C}$-valued place ϑ of $\mathbb{C}(\overline{\mathcal{D}})$ whose valuation ring R_ϑ contains the local algebra $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{\mathbf{0}}}$.

From $\xi_1^3 = \xi_2^2$ and $\xi_1 \neq 0$ we deduce that $(\xi_2/\xi_1)^2 - \xi_1 = 0$ holds in $\mathbb{C}(\overline{\mathcal{D}})$. Therefore ξ_2/ξ_1 is integral over $\mathbb{C}[\overline{\mathcal{D}}]$ and $(\xi_2/\xi_1)^2$ belongs to $\mathfrak{M}_{\mathbf{0}} R_\vartheta$. This implies that ξ_2/ξ_1 is an element of R_ϑ contained in the maximal ideal of R_ϑ. Therefore we have $\vartheta(\xi_2/\xi_1) = 0$. Observe that $\vartheta(\xi_1) = \vartheta(\xi_2) = 0$ and $\vartheta(1 + \xi_1) = 1$ holds. From the Taylor development of the polynomial f at the point $\mathbf{0}$ we see that there exist polynomials Q_1, Q_2, Q_3 of $\Pi^{(2)}$ such that

$$\frac{f(\xi) - f(\mathbf{0})}{\xi_1} = \frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\xi_2}{\xi_1}\frac{\partial f}{\partial X_2}(\mathbf{0}) + \xi_1 Q_1(\xi) + \frac{\xi_2^2}{\xi_1} Q_2(\xi) + \xi_2 Q_3(\xi)$$

holds in $\mathbb{C}(\overline{\mathcal{M}})$. This implies

$$\vartheta\left(\frac{f(\xi) - f(\mathbf{0})}{\xi_1(1 + \xi_1)}\right) = \frac{\partial f}{\partial X_1}(\mathbf{0}).$$

On the other hand we have $\xi_1^2 + \xi_2^2 = \xi_1^2(1 + \xi_1)$ and this implies

$$\Psi_2(\xi) = \frac{f(\xi) - f(\mathbf{0})}{\xi_1(1 + \xi_1)}, \quad \Psi_3(\xi) = \frac{f(\xi) - f(\mathbf{0})}{\xi_1(1 + \xi_1)}\frac{\xi_2}{\xi_1}.$$

Therefore the place ϑ has at $\Psi_2(\xi)$ and $\Psi_3(\xi)$ the finite values

$$\vartheta(\Psi_2(\xi)) = \frac{\partial f}{\partial X_1}(\mathbf{0}) = \Psi_2(\mathbf{0}), \qquad \vartheta(\Psi_3(\xi)) = 0 = \Psi_3(\mathbf{0}).$$

Thus the constructible map Ψ is geometrically robust. This means that the Hermite–Lagrange interpolation algorithm determined by $\mathcal{D}^*, \omega^*$ and Ψ is geometrically robust.

Interpolation over the curve $X_2^2 - X_1^2 - X_1^3 = 0$ Suppose now that the given polynomial map $f : \mathbb{A}^2 \to \mathbb{A}^1$ satisfies the condition $\left(\partial f/\partial X_1(\mathbf{0}), \partial f/\partial X_2(\mathbf{0})\right) \neq \mathbf{0}$. We consider the open curve $\mathcal{D} := \{X_2^2 - X_1^2 - X_1^3 = 0\} \setminus \{(-2, \pm 2\mathrm{i})\} \subset \mathbb{A}^2$ and the constructible map $\Phi : \mathcal{D} \to \Pi_1^{(2)}$ defined for $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ by

$$\Phi(d) := f(\mathbf{0}) + \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2} X_1 + \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2} X_2$$

and for $d := \mathbf{0}$ by

$$\Phi(\mathbf{0}) := f(\mathbf{0}) + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_1 + \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)X_2.$$

In Section 3.3.2 we showed that Φ is topologically robust and hereditary. Hence $\mathcal{D}$ and Φ determine a Hermite–Lagrange interpolation problem.

Again like in Section 3.3.2, let $\mathcal{D}^* := \mathbb{A}^3$ and let $\omega^* : \mathcal{D}^* \to \Pi_1^{(2)}$ be the canonical dense encoding of bivariate polynomials of degree at most one over $\mathbb{C}$. Furthermore, let $\Psi : \mathcal{D} \to \mathcal{D}^*$ be the constructible map defined for $d := (d_1, d_2) \in \mathcal{D} \setminus \{\mathbf{0}\}$ by

$$\Psi(d) := \left(f(\mathbf{0}), \frac{(f(d) - f(\mathbf{0}))d_1}{d_1^2 + d_2^2}, \frac{(f(d) - f(\mathbf{0}))d_2}{d_1^2 + d_2^2}\right)$$

and for $d := \mathbf{0}$ by

$$\Psi(\mathbf{0}) := \left(f(\mathbf{0}), \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right), \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right)\right).$$

Then Ψ is hereditary and $\mathcal{D}^*$, ω^* and Ψ determine an algorithm that solves the Hermite–Lagrange interpolation problem given by $\mathcal{D}$ and Φ.

We claim that Ψ is not geometrically robust.

Let $\Psi := (\Psi_1, \Psi_2, \Psi_3)$ and denote $\mathfrak{M}_{\mathbf{0}}$ the maximal ideal of coordinate functions of $\mathbb{C}[\mathcal{C}]$ at the point $\mathbf{0} \in \mathcal{D}$, where $\mathcal{C} := \{X_2^2 - X_1^2 - X_1^3 = 0\}$ is the (irreducible) Zariski closure of $\mathcal{D}$ in $\mathbb{A}^2$. Since the plane curve $\mathcal{C}$ is irreducible, $\mathbb{C}[\overline{\mathcal{D}}] = \mathbb{C}[\mathcal{C}]$ is an integral domain with fraction field $\mathbb{C}(\overline{\mathcal{D}})$. Let ξ_1 and ξ_2 be the coordinate functions of $\mathbb{C}[\overline{\mathcal{D}}]$ induced by the indeterminates X_1 and X_2 and let $\xi := (\xi_1, \xi_2)$. We have $\xi_2^2 = \xi_1^2 + \xi_1^3$ and $\xi_1 \neq 0$.

We are now going to show that the rational functions Ψ_2 and Ψ_3 do not satisfy the condition of Definition 14 at the point $\mathbf{0} \in \mathcal{D}$, thus finishing the proof of our claim.

For this purpose consider an arbitrary $\mathbb{C}$-valued place ϑ of $\mathbb{C}(\overline{\mathcal{D}})$ whose valuation ring R_ϑ contains the local algebra $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}_{\mathbf{0}}}$.

From $\xi_2^2 = \xi_1^2 + \xi_1^3$ and $\xi_1 \neq 0$ we deduce that $(\xi_2/\xi_1)^2 = 1 + \xi_1$ holds in $\mathbb{C}(\overline{\mathcal{D}})$. Therefore ξ_2/ξ_1 is integral over $\mathbb{C}[\overline{\mathcal{D}}]$ and $(\xi_2/\xi_1)^2 - 1$ belongs to $\mathfrak{M}_{\mathbf{0}} R_\vartheta$. This implies that ξ_2/ξ_1 is an element of R_ϑ and $(\vartheta(\xi_2/\xi_1))^2 = 1$ holds. Observe $\vartheta(\xi_1) = \vartheta(\xi_2) = 0$ and $\vartheta(2 + \xi_1) = 2$. From the Taylor development of the polynomial f at $\mathbf{0}$ we see that there exist polynomials Q_1, Q_2, Q_3 of $\Pi^{(2)}$ such that

$$\frac{f(\xi) - f(\mathbf{0})}{\xi_1} = \frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\xi_2}{\xi_1}\frac{\partial f}{\partial X_2}(\mathbf{0}) + \xi_1 Q_1(\xi) + \frac{\xi_2^2}{\xi_1}Q_2(\xi) + \xi_2 Q_3(\xi)$$

holds in $\mathbb{C}(\overline{\mathcal{M}})$. This implies

$$\vartheta\left(\frac{f(\xi) - f(\mathbf{0})}{\xi_1(2 + \xi_1)}\right) = \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \vartheta\left(\frac{\xi_2}{\xi_1}\right)\frac{\partial f}{\partial X_2}(\mathbf{0})\right).$$

On the other hand we have $\xi_1^2 + \xi_2^2 = \xi_1^2(2 + \xi_1)$ and this implies

$$\Psi_2(\xi) = \frac{f(\xi) - f(\mathbf{0})}{\xi_1(2 + \xi_1)}, \qquad \Psi_3(\xi) = \frac{f(\xi) - f(\mathbf{0})}{\xi_1(2 + \xi_1)}\frac{\xi_2}{\xi_1}.$$

Therefore the place ϑ has at $\Psi_2(\xi)$ and $\Psi_3(\xi)$ the finite values

$$\vartheta(\Psi_2(\xi)) = \frac{1}{2}\left(\frac{\partial f}{\partial X_1}(\mathbf{0}) + \vartheta\left(\frac{\xi_2}{\xi_1}\right)\frac{\partial f}{\partial X_2}(\mathbf{0})\right), \qquad \vartheta(\Psi_3(\xi)) = \frac{1}{2}\left(\vartheta\left(\frac{\xi_2}{\xi_1}\right)\frac{\partial f}{\partial X_1}(\mathbf{0}) + \frac{\partial f}{\partial X_2}(\mathbf{0})\right).$$

By assumption we have $\left(\partial f/\partial X_1(\mathbf{0}), \partial f/\partial X_2(\mathbf{0})\right) \neq \mathbf{0}$. Therefore, the condition $\vartheta(\Psi(\xi)) = \Psi(\mathbf{0})$ is equivalent to the condition $\vartheta(\xi_2/\xi_1) = 1$.

Let T be a new indeterminate over $\mathbb{C}$ and let $\mathbb{C}[[T]]$ be the ring of formal power series in T with coefficients in $\mathbb{C}$. Let $\sigma \in \mathbb{C}[[T]]$ be the unique formal power series satisfying the condition $\sigma^2 = 1+T$ and $\sigma(0) = -1$. Consider the $\mathbb{C}$-algebra homomorphism $\chi : \mathbb{C}[\mathcal{C}] \to \mathbb{C}[[T]]$ defined by $\chi(\xi_1) := T$ and $\chi(\xi_2) := T\sigma(T)$. Observe that χ is well defined since the identity $(T\sigma)^2 = T^2 + T^3$ holds in $\mathbb{C}[[T]]$. Furthermore, χ is injective since $Y^2 - 1 - T$ is the minimal polynomial of σ over $\mathbb{C}(T)$. We conclude that χ admits a well-defined extension $\mathbb{C}(\mathcal{C}) \to \mathbb{C}((T))$, which we also denote by χ. Finally, let $\nu : \mathbb{C}((T)) \to \mathbb{C}$ be the unique place extending the evaluation at 0 and let $\epsilon : \mathbb{C}(\mathcal{C}) \to \mathbb{C}$ be the composition $\epsilon := \nu \circ \chi$.

From $\epsilon(\xi_1) = \nu(T) = 0$ and $\epsilon(\xi_2) = \nu(T) \cdot \nu(\sigma) = 0$, we conclude that $\epsilon : \mathbb{C}(\mathcal{C}) \to \mathbb{C}$ is a place extending the evaluation homomorphism of $\mathbb{C}[\mathcal{C}]$ at the point $\mathbf{0}$. Furthermore, we have

$$\epsilon(\xi_2/\xi_1) = \nu\big(\chi(\xi_2)/\chi(\xi_1)\big) = \nu(\sigma) = \sigma(0) = -1.$$

As we have seen before, $\epsilon(\xi_2/\xi_1) \neq 1$ implies $\epsilon\big(\Psi(\xi)\big) \neq \Psi(\mathbf{0})$. Therefore, the map Ψ is not geometrically robust.

5. Lower complexity bounds for Hermite–Lagrange interpolation problems

This section is devoted to the presentation of the main results of this paper. We are going to exhibit lower complexity bounds (in the sense of Section 3.4) for (typically geometrically robust) algorithms which solve selected Lagrange interpolation problems. The lower complexity bounds are expressed in terms of the number K of nodes involved in the Lagrange interpolation under consideration and may be linear in K (incompressibility results) or exponential in K.

5.1. Incompressibility results

In this section we shall exhibit two Lagrange interpolation problems involving K nodes which require algorithms of complexity at least K for their solution.

We first consider the complexity of *generic* Lagrange interpolation by n-variate polynomials of degree at most D.

Then we exhibit a Lagrange interpolation problem involving K nodes such that the interpolants may be evaluated (in principle) using $O(\log K)$ arithmetical operations. However, any *geometrically robust* algorithm solving this problem requires an output data structure of size at least K. In particular it is not possible to retrieve the existing size $O(\log K)$ straight-line program representation of the interpolants by means of a geometrically robust interpolation algorithm.

5.1.1. Generic n-variate Lagrange interpolation problems

Let n, D, K and M be natural numbers and let $\mathcal{D}$ be a constructible Zariski dense subset of $\mathbb{A}^{(n+1)\times K}$ which will serve as an input data structure for the interpolation problems we are going to consider in this section. Observe that the size N of the input data structure $\mathcal{D}$ is $(n+1)K$.

A *generic n-variate Lagrange interpolation problem* in $\Pi_D^{(n)}$ is determined by $\mathcal{D}$ and a topologically robust and hereditary map $\Phi : \mathcal{D} \to \Pi_D^{(n)}$, such that for any input datum $d := (x_1, y_1, \ldots, x_K, y_K) \in \mathcal{D}$ with $x_1, \ldots, x_K \in \mathbb{A}^n$ and $y_1, \ldots, y_K \in \mathbb{A}^1$, the polynomial $\Phi(d)$ satisfies the condition $\Phi(d)(x_j) = y_j$ for any $1 \leq j \leq K$. For such an interpolation problem, the constructible set $\mathcal{O} := \Phi(\mathcal{D})$ constitutes the class of interpolants.

With these notations and assumptions we have the following incompressibility result.

Proposition 21. *Let $\mathcal{D}^* \subset \mathbb{A}^M$, $\omega^* : \mathcal{D}^* \to \mathcal{O}$ a polynomial encoding of the class of interpolants $\mathcal{O}$ and $\Psi : \mathcal{D} \to \mathcal{D}^*$ a constructible hereditary map, such that $\mathcal{D}^*$, Ψ and ω^* determine an algorithm which solves the generic n-variate Lagrange interpolation problem given by $\mathcal{D}$ and Φ. Then we have $M \geq K$, i.e., the complexity of the Lagrange interpolation algorithm determined by $\mathcal{D}^*$, ω^* and Ψ is at least $K = N/(n+1)$.*

Proof. Since $\mathcal{D}$ is constructible, there exists a nonempty Zariski open subset $\mathcal{U}$ of $\mathbb{A}^{(n+1)\times K}$ which is contained in $\mathcal{D}$. We choose now a point $\gamma := (\gamma_1, \ldots, \gamma_K)$ of $\mathbb{A}^{n\times K}$ with $\gamma_j \in \mathbb{A}^n$, $1 \leq j \leq K$, such that the set

$$\mathcal{D}_\gamma := \{(y_1, \ldots, y_K) \in \mathbb{A}^K : (\gamma_1, y_1, \ldots, \gamma_K, y_K) \in \mathcal{U}\}$$

is Zariski dense in $\mathbb{A}^K$. Such a point $\gamma \in \mathbb{A}^{n\times K}$ can be obtained as the image of a point of $\mathcal{U}$ under the canonical projection $\mathbb{A}^{(n+1)\times K} \to \mathbb{A}^{n\times K}$.

Let $\varphi_1 : \mathcal{D}_\gamma \to \mathcal{D}^*$ and $\varphi_2 : \mathcal{D}^* \to \mathbb{A}^K$ be the constructible maps defined for $y \in \mathcal{D}_\gamma$ and $d^* \in \mathcal{D}^*$ by $\varphi_1(y) := \Psi(\gamma, y)$ and $\varphi_2(d^*) := (\omega^*(d^*)(\gamma_1), \ldots, \omega^*(d^*)(\gamma_K))$.

Since $\mathcal{D}^*$, ω^* and Ψ determine an algorithm which solves the Lagrange interpolation problem given by $\mathcal{D}$ and Φ, we have $\omega^* \circ \Psi = \Phi$. This implies that for any $y \in \mathcal{D}_\gamma$ the identity

$$\begin{aligned}\varphi_2 \circ \varphi_1(y) = \varphi_2(\Psi(\gamma, y)) &= \big(\omega^*(\Psi(\gamma, y))(\gamma_1), \ldots, \omega^*(\Psi(\gamma, y))(\gamma_K)\big)\\ &= (\Phi(\gamma, y)(\gamma_1), \ldots, \Phi(\gamma, y)(\gamma_K)) = y\end{aligned}$$

holds. Therefore we have $\varphi_2 \circ \varphi_1 = \mathrm{id}_{\mathcal{D}_\gamma}$. We obtain the following estimates:

$$M = \dim \mathbb{A}^M \geq \dim \overline{\mathcal{D}^*} \geq \dim \overline{\varphi_1(\mathcal{D}_\gamma)} \geq \dim \overline{\varphi_2 \circ \varphi_1(\mathcal{D}_\gamma)} = \dim \overline{\mathcal{D}_\gamma} = \dim \mathbb{A}^K = K,$$

which imply the conclusion of Proposition 21. □

5.1.2. An incompressible Lagrange interpolation problem with interpolants which are "easy to compute"

The following example of a Lagrange interpolation problem is taken from [9], where it is analyzed from a different point of view.

Let K and M be natural numbers with $K \geq 2$, let $N := 2K$, $D := K - 1$, $\Pi := \Pi^{(1)}$, let T and X be indeterminates over $\mathbb{C}$ and let

$$F(X, T) := (T^{D+1} - 1) \sum_{k=0}^{D} T^k X^k.$$

Our input data structure is the constructible subset $\mathcal{D}$ of $\mathbb{A}^N$ defined by

$$\begin{aligned}\mathcal{D} := \{(x_1, y_1, \ldots, x_K, y_K) \in \mathbb{A}^N : \exists t \in \mathbb{C} \text{ with } F(x_i, t) = y_i \text{ for } 1 \leq i \leq K\\ \text{and } x_i \neq x_j \text{ for any } 1 \leq i < j \leq K\}.\end{aligned}$$

The constructible set $\mathcal{D}$ is irreducible. In order to see this, let $\mathcal{U} := \{(x_1, \ldots, x_K) \in \mathbb{A}^K : x_i \neq x_j \text{ for } 1 \leq i < j \leq K\}$ and let $\sigma : \mathcal{U} \times \mathbb{A}^1 \to \mathbb{A}^N$ be the polynomial map defined for $x = (x_1, \ldots, x_K) \in \mathcal{U}$ and $t \in \mathbb{A}^1$ by $\sigma(x, t) := (x_1, F(x_1, t), \ldots, x_K, F(x_K, t))$. Then clearly $\mathcal{D}$ is the image of σ and hence irreducible.

Moreover, for any $d \in \mathcal{D}$ the fiber $\sigma^{-1}(d)$ is a nonempty finite set (i.e., a zero-dimensional algebraic variety) and therefore the Theorem on the Dimension of Fibers of algebraic geometry (see, e.g., [26, Section I.6.3, Theorem 7]) implies that

$$\dim \overline{\mathcal{D}} = \dim \overline{\sigma(\mathcal{U} \times \mathbb{A}^1)} = \dim \overline{\mathcal{U} \times \mathbb{A}^1} = \dim \overline{\mathcal{U}} \times \mathbb{A}^1 = \dim \mathbb{A}^K \times \mathbb{A}^1 = K + 1$$

holds.

Let $\Phi : \mathcal{D} \to \Pi_D$ be the constructible map which associates to any interpolation datum $d := (x_1, y_1, \ldots, x_K, y_K)$ of $\mathcal{D}$ the *unique* polynomial of Π_D, namely $\Phi(d)$, which satisfies the condition $\Phi(d)(x_j) = y_j$ for $1 \leq j \leq K$. Taking into account the definition of $\mathcal{D}$, we see that there exists a (not necessarily unique) point $t \in \mathbb{A}^1$ such that $\Phi(d) = F(X, t)$ holds. From the discussion in Section 4.3.1 one deduces easily that Φ is a regular map. Hence Φ is geometrically robust and therefore also topologically robust and hereditary. Therefore $\mathcal{D}$ and Φ determine a Lagrange interpolation problem in the sense of Definition 7.

Observe that the input data structure $\mathcal{D}$ of this interpolation problem is not dense in its ambient space $\mathbb{A}^N$, since $\dim \overline{\mathcal{D}} = K + 1 < 2K = N = \dim \mathbb{A}^N$ holds. Thus our Lagrange interpolation problem is therefore not generic like the one of Section 5.1.1.

Let us denote by $\mathcal{O} := \{F(X,t) : t \in \mathbb{C}\}$ the class of interpolants of the Lagrange interpolation problem determined by $\mathcal{D}$ and Φ.

From the definition of F it follows that any interpolant $f \in \mathcal{O}$ may be evaluated by a division-free straight-line program of size $O(\log D) = O(\log K)$. Hence f is a univariate polynomial which is "easy to compute" (see [8] for this notion and the context). This is another particular feature of our Lagrange interpolation problem.

Proposition 22. *Let notations and assumptions be as before. Let $\mathcal{D}^*$ be a given constructible subset of $\mathbb{A}^M$, a polynomial encoding $\omega^* : \mathcal{D}^* \to \Pi_D$ of the space of interpolants $\mathcal{O}$ and a geometrically robust map $\Psi : \mathcal{D} \to \mathcal{D}^*$ such that $\mathcal{D}^*$, ω^* and Ψ determine an algorithm which solves the Lagrange interpolation problem represented by $\mathcal{D}$ and Φ (such a solution exists for a suitable natural number M, since Φ is geometrically robust). Then we have $M \geq K$, i.e. the complexity of the Lagrange interpolation algorithm determined by $\mathcal{D}^*$, ω^* and Ψ is at least $K = N/2$.*

Proof. Denote by $\mathbb{G}_D$ the subset of $\mathbb{A}^1$ consisting of the $(D+1)$-th roots of unity and let $\psi_1, \ldots, \psi_M$ be the components of $\Psi : \mathcal{D} \to \mathcal{D}^*$. By Lemma 1 there exists a nonempty Zariski open subset $\mathcal{U}$ of $\overline{\mathcal{D}}$ which is contained in $\mathcal{D}$ and where $\psi_1, \ldots, \psi_M$ are regular (i.e., well-defined) rational functions.

Let T be a new indeterminate. We now fix an arbitrary point $(a_1, b_1, \ldots, a_K, b_K)$ of $\mathcal{U}$ and write $a := (a_1, \ldots, a_K)$. Now we consider the polynomial map $\varepsilon : \mathbb{A}^1 \to \mathcal{D}$ which for $t \in \mathbb{A}^1$ is defined by

$$\varepsilon(t) := (a_1, F(a_1, t), \ldots, a_K, F(a_K, t)).$$

In particular there exists a complex number t_0 with $F(a_1, t_0) = b_1, \ldots, F(a_K, t_0) = b_K$ and therefore the image of ε and $\mathcal{U}$ have a nonempty intersection. This implies that $\lambda_1 := \psi_1 \circ \varepsilon, \ldots, \lambda_M := \psi_M \circ \varepsilon$ are well-defined rational functions which belong to $\mathbb{C}(T)$. Moreover, for any $\zeta \in \mathbb{G}_D$ we have $\varepsilon(\zeta) = (a_1, 0, \ldots, a_K, 0)$.

Claim. *The rational functions $\lambda_1, \ldots, \lambda_M$ are all well defined at any point of $\zeta \in \mathbb{G}_D$ and the values $\lambda_1(\zeta), \ldots, \lambda_M(\zeta)$ are independent from the choice of $\zeta \in \mathbb{G}_D$.*

Proof of Claim. Consider an arbitrary $(D+1)$-th root of unity $\zeta \in \mathbb{G}_D$ and an arbitrary index $1 \leq j \leq M$.

Let $\mathfrak{M}$ be the maximal ideal of the coordinate functions of $\mathbb{C}[\overline{\mathcal{D}}]$ which vanish at the point $\alpha := (a_1, 0, \ldots, a_K, 0) = \varepsilon(\zeta)$ of $\overline{\mathcal{D}}$. Since by assumption Ψ is geometrically robust, there exist $s \in \mathbb{N}$ and $p_0, \ldots, p_{s-1} \in \mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}}$ such that the identity

$$\psi_j^s + p_{s-1}\psi_j^{s-1} + \cdots + p_0 = 0 \tag{8}$$

holds in $\mathbb{C}(\overline{\mathcal{D}})$. Since the rational functions $p_0, \ldots, p_{s-1}$ are well defined at the point α, the compositions $\pi_0 := p_0 \circ \varepsilon, \ldots, \pi_{s-1} := p_{s-1} \circ \varepsilon$ are well defined at ζ. Therefore $\pi_0, \ldots, \pi_{s-1}$ belong to the local ring $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$, where $\mathfrak{N}_\zeta = \mathbb{C}[T] \cdot (T - \zeta)$ is the maximal ideal generated by $T - \zeta$ in $\mathbb{C}[T]$.

Identity (8) implies that

$$\lambda_j^s + \pi_{s-1}\lambda_j^{s-1} + \cdots + \pi_0 = 0$$

holds in $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$. Therefore λ_j is integral over $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$. Since λ_j belongs to $\mathbb{C}(T)$ and $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$ is integrally closed in $\mathbb{C}(T)$, we conclude $\lambda_j \in \mathbb{C}[T]_{\mathfrak{N}_\zeta}$. This means that the rational function λ_j is well defined at ζ. Since $\zeta \in \mathbb{G}_D$ was chosen arbitrarily we conclude that λ_j is well defined at *any* point $\zeta \in \mathbb{G}_D$. This proves the first part of the claim for $1 \leq j \leq M$. We are now going to show the second part.

The morphism of irreducible varieties $\varepsilon : \mathbb{A}^1 \to \overline{\mathcal{D}}$ induces a $\mathbb{C}$-algebra homomorphism $\varepsilon^* : \mathbb{C}[\overline{\mathcal{D}}] \to \mathbb{C}[T]$. From Theorem I we deduce that there exists a field Ω containing $\mathbb{C}(T)$ such that ε^* can be extended to an Ω-valued place of $\mathbb{C}(\overline{\mathcal{D}})$ that we also denote by ε^*. Let R_{ε^*} be the valuation ring of the place ε^*. Observe that R_{ε^*} contains $\mathbb{C}[\overline{\mathcal{D}}]$ and its localization $\mathbb{C}[\overline{\mathcal{D}}]_{\mathfrak{M}}$ at the maximal ideal $\mathfrak{M}$. Therefore identity (8) implies that $\varepsilon^*(\psi_j)$ is finite. Moreover, since ψ_j is a rational function of $\mathbb{C}(\overline{\mathcal{D}})$ and the composition $\psi_j \circ \varepsilon$ is well defined, we have $\varepsilon^*(\psi_j) = \psi_j \circ \varepsilon = \lambda_j$.

Let ζ and η be arbitrary elements of $\mathbb{G}_D$. Then ζ and η induce by evaluation two $\mathbb{C}$-algebra homomorphisms $\mu_\zeta : \mathbb{C}[T] \to \mathbb{C}$ and $\mu_\eta : \mathbb{C}[T] \to \mathbb{C}$. From Theorem I we conclude that μ_ζ and

μ_η can be extended to two $\mathbb{C}$-valued places of Ω which we also denote by μ_ζ and μ_η. Let R_{μ_ζ} and R_{μ_η} be the valuation rings of the places μ_ζ and μ_η. Then R_{μ_ζ} contains $\mathbb{C}[T]_{\mathfrak{N}_\zeta}$ and R_{μ_η} contains $\mathbb{C}[T]_{\mathfrak{N}_\eta}$. Composing now the evaluation ε^* with the valuation μ_ζ, and with the valuation μ_η, we obtain two $\mathbb{C}$-valued valuations ν_ζ and ν_η of $\mathbb{C}(\overline{\mathcal{D}})$ which extend the evaluation of the coordinate functions of $\mathbb{C}[\overline{\mathcal{D}}]$ at the point $\alpha \in \mathcal{D}$. Since by assumption Ψ is geometrically robust we have $\nu_\zeta(\psi_j) = \nu_\eta(\psi_j)$. On the other hand, from $\lambda_j \in \mathbb{C}[T]_{\mathfrak{N}_\zeta}$ we infer $\nu_\zeta(\psi_j) = \mu_\zeta(\varepsilon^*(\psi_j)) = \mu_\zeta(\lambda_j) = \lambda_j(\zeta)$ and similarly $\nu_\eta(\psi_j) = \lambda_j(\eta)$. This implies $\lambda_j(\zeta) = \lambda_j(\eta)$. Therefore the value of $\lambda_j(\zeta)$ does not depend on $\zeta \in \mathbb{G}_D$. Since $1 \le j \le M$ was chosen arbitrarily, the claim is proved. □

We conclude now that $\lambda := (\lambda_1, \ldots, \lambda_M)$ is a rational map of $\mathbb{C}(T)^M$ which is well defined at any point $\zeta \in \mathbb{G}_D$ and whose value $\alpha^* := \lambda(\zeta)$ is independent from ζ.

Consider now the polynomial map $\varphi : \mathcal{D}^* \to \mathbb{A}^K$ which at any point $h \in \mathcal{D}^*$ is defined by $\varphi(h) := (\omega^*(h)(a_1), \ldots, \omega^*(h)(a_K))$.

Observe that $\theta := \varphi \circ \lambda$ is a well-defined rational map (with maximal domain) from $\mathbb{A}^1$ to $\mathbb{A}^K$. For any point $t \in \mathbb{A}^1$, such that ψ_j is well defined at $\varepsilon(t)$, we have

$$\begin{aligned}\theta(t) &= \varphi(\lambda(t)) = \varphi(\Psi(\varepsilon(t))) = (\omega^*(\Psi(\varepsilon(t)))(a_1), \ldots, \omega^*(\Psi(\varepsilon(t)))(a_K))\\ &= (\Phi(\varepsilon(t))(a_1), \ldots, \Phi(\varepsilon(t))(a_K))\\ &= (F(a_1, t), \ldots, F(a_K, t)).\end{aligned}$$

Thus θ is a polynomial map from $\mathbb{A}^1$ to $\mathbb{A}^K$ and is therefore well defined at any point t of $\mathbb{A}^1$.

From

$$\frac{\partial}{\partial T}F(T, X) = (D+1)T^D \sum_{k=0}^{D} T^k X^k + (T^{D+1} - 1)\frac{\partial}{\partial T}\sum_{k=0}^{D} T^k X^k$$

we deduce that for any $\zeta \in \mathbb{G}_D$ and any $x \in \mathbb{A}^1$ the identity

$$\frac{\partial F}{\partial T}(\zeta, x) = (D+1)\zeta^D \sum_{k=0}^{D} \zeta^k x^k$$

holds.

Let $\zeta_1, \ldots, \zeta_{D+1}$ be the (distinct) elements of $\mathbb{G}_D$. The chain rule for differential maps and the previous claim imply now that for any $1 \le \ell \le D+1$ the identity

$$(D+1)\zeta_\ell^D \begin{pmatrix} \sum_{k=0}^{D} \zeta_\ell^k a_1^k \\ \vdots \\ \sum_{k=0}^{D} \zeta_\ell^k a_K^k \end{pmatrix} = (\mathrm{d}\theta)(\zeta_\ell)$$

$$= (\mathrm{d}\varphi)(\lambda(\zeta_\ell)) \cdot (\mathrm{d}\lambda)(\zeta_\ell) = (\mathrm{d}\varphi)(\alpha^*) \cdot (\mathrm{d}\lambda)(\zeta_\ell) \tag{9}$$

is meaningful and valid (here $\mathrm{d}\theta$ denotes the total derivative of θ and $(\mathrm{d}\theta)(\zeta_\ell)$ its value at the point ζ_ℓ).

For $1 \le \ell \le D+1$ let $v_\ell := ((D+1)\zeta_\ell^D)^{-1}((\mathrm{d}\theta)(\zeta_\ell))$ and let C be the complex $(K \times M)$-matrix $C := (\mathrm{d}\varphi)(\alpha^*)$, namely the Jacobian of φ at the point α^*, which is independent of the index ℓ. Observe that $K = D+1$ holds. From (9) we deduce that $v_1, \ldots, v_K$ are $\mathbb{C}$-linear combinations of the columns of C. We assert that $v_1, \ldots, v_K$ are $\mathbb{C}$-linearly independent. In order to see this, let $\mathcal{V}$ the complex $(K \times K)$-matrix whose column vectors are $v_1, \ldots, v_K$, $V_K := (\zeta_\ell^{k-1})_{1 \le \ell, k \le K}$ and $W_\alpha := (a_\ell^{k-1})_{1 \le \ell, k \le K}$. Then we have $\mathcal{V} = W_\alpha V_K^t$. Since V_K and W_α are invertible Vandermonde matrices we conclude that $\mathcal{V}$ is of maximal rank K. This implies that the rank of the complex $(K \times M)$-matrix C is at least K and therefore we have $M \ge K = N/2$. This proves Proposition 22. □

5.2. Straight-line program encoded polynomials: Lagrange interpolation is hard

Let n, L, M be natural numbers with $2^{L/4} \geq n, K := 4(L+n+1)^2+2$ and $N := K$. In terms of the notions and notations introduced in Sections 3.1.2 and 3.3.3, we are now going to show that any *geometrically robust* interpolation algorithm, which reconstructs the n-variate polynomials that can be evaluated by a division-free straight-line program of nonscalar length at most L from their values on an identification sequence of length K, has exponential complexity of order $2^{\Omega(Ln)} = 2^{\Omega(\sqrt{K})} = 2^{\Omega(\sqrt{N})}$. This means that traditional Lagrange interpolation at $n_L := \binom{2^L+n}{n} = 2^{O(Ln)}$ nodes is almost optimal for this very special and meager class of polynomials.

The following result, with a slightly coarser complexity bound, was exhibited in the context of constraint databases in [14].

Theorem 23. *Let notations and assumptions be as before, let $\mathcal{D}$ be the irreducible, constructible subset of $\mathbb{A}^N$ and let $\Phi : \mathcal{D} \to \Pi_{2^L}^{(n)}$ be the geometrically robust map introduced in Section 3.3.3. Thus $\mathcal{D}$ and Φ determine a Lagrange interpolation problem in the sense of Definition 7 and the interpolants $\mathcal{O} := \Phi(\mathcal{D})$ are the polynomials in $\Pi^{(n)}$ which can be evaluated by a division-free straight-line program of nonscalar length at most L.*

Let $\mathcal{D}^*$ be a given constructible subset of $\mathbb{A}^M$, a polynomial encoding $\omega^* : \mathcal{D}^* \to \mathcal{O}$ of the class of interpolants $\mathcal{O}$ and a geometrically robust map $\Psi : \mathcal{D} \to \mathcal{D}^*$ such that $\mathcal{D}^*, \omega^*$ and Ψ determine an algorithm which solves the Lagrange interpolation problem represented by $\mathcal{D}$ and Φ (such a solution exists for a suitable natural number M, since Φ is geometrically robust). Then we have

$$M \geq \binom{2^{\lfloor \frac{L}{2}+1 \rfloor} - 1 + n}{n} = 2^{\Omega(Ln)} = 2^{\Omega(\sqrt{K})} = 2^{\Omega(\sqrt{N})}.$$

In other words, the complexity of the Lagrange interpolation algorithm determined by $\mathcal{D}^*, \omega^*$ and Ψ is at least exponential in L and n or alternatively in $\sqrt{K} = \sqrt{N}$.

Proof. Let $\ell := \lfloor \frac{L}{2} + 1 \rfloor$ and let $\mathcal{Y}$ be the subset of $\Pi_{2^L} := \Pi_{2^L}^{(n)}$ defined by

$$\mathcal{Y} := \left\{ t \sum_{k=0}^{2^\ell - 1} (\lambda_1 X_1 + \cdots + \lambda_n X_n)^k : (t, \lambda_1, \ldots, \lambda_n) \in \mathbb{A}^{n+1} \right\}.$$

Taking into account that any polynomial $h \in \mathcal{Y}$ can be evaluated by a division-free straight-line program of nonscalar length at most $2(\ell - 1)$, we conclude that $\mathcal{Y}$ is contained in the class of interpolants $\mathcal{O}$. Let $\overline{\mathcal{Y}}$ denote the Zariski closure of $\mathcal{Y}$ in its ambient space $\mathbb{A}^{n_L}$ (here we identify Π_{2^L} with $\mathbb{A}^{n_L}$). Observe that $\overline{\mathcal{Y}}$ is an irreducible affine subvariety of $\overline{\mathcal{O}}$, because $\overline{\mathcal{Y}}$ is the Zariski closure of the image of a polynomial morphism which maps the irreducible affine variety $\mathbb{A}^{n+1}$ to $\mathbb{A}^{n_L}$.

In Section 3.3.3 we already fixed points $\gamma_1, \ldots, \gamma_K$ of $\mathbb{A}^n$ (e.g., integer points of bit length at most $4(L+1) \leq 2\sqrt{K}$) such that $\gamma := (\gamma_1, \ldots, \gamma_K)$ becomes an identification sequence for the class of polynomials $\overline{\mathcal{O}}$. Let $\Xi : \overline{\mathcal{O}} \to \mathbb{A}^N$ be the polynomial map defined for $f \in \overline{\mathcal{O}}$ by $\Xi(f) := (f(\gamma_1), \ldots, f(\gamma_K))$. Recall $\mathcal{D} := \Xi(\mathcal{O})$.

Then $\overline{\mathcal{D}}$ is an affine, closed and irreducible subvariety of $\mathbb{A}^N = \mathbb{A}^K$ and $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ is a homeomorphic (with respect to the strong topology), birational, finite morphism of irreducible affine varieties. In particular, the map $\Phi := \Xi^{-1} : \mathcal{D} \to \Pi_{2^L}$ is geometrically robust and $\mathcal{D}$ and Φ determine the Lagrange interpolation problem under consideration.

Let $\mathcal{Z}$ be the irreducible constructible subset of $\overline{\mathcal{D}} \subset \mathbb{A}^N$ defined by $\mathcal{Z} := \Xi(\overline{\mathcal{Y}})$. Observe that $\mathcal{Z}$ is Zariski closed because $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ is a finite morphism of affine varieties (i.e., the associated ring homomorphism is an integral monomorphism). Thus $\mathcal{Z}$ is an irreducible and closed affine subvariety of $\overline{\mathcal{D}}$ and $\mathbb{A}^N$. Observe that the point $(0, \ldots, 0) \in \mathbb{A}^N$ belongs to $\mathcal{Z} \cap \mathcal{D}$. The closeness of $\mathcal{Z}$ in the strong topology follows also easily from the above mentioned fact that $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{D}}$ is a homeomorphism.

Let $\psi_1, \ldots, \psi_M$ be the components of the given constructible map $\Psi : \mathcal{D} \to \mathbb{A}^M$. Following Lemma 1, there exists a (nonempty Zariski) open affine subvariety $\mathcal{U}$ of $\overline{\mathcal{D}}$ with $\mathcal{U} \subset \mathcal{D}$, where the rational functions $\psi_1, \ldots, \psi_M$ are regular. Thus $\psi_1|_{\mathcal{U}}, \ldots, \psi_M|_{\mathcal{U}}$ are coordinate functions of the $\mathbb{C}$-algebra $\mathbb{C}[\mathcal{U}]$ which is contained in the rational function field $\mathbb{C}(\overline{\mathcal{D}})$.

Theorem 17 justifies now the following argumentation: There exist rational functions $\eta_1, \ldots, \eta_M$ of $\mathbb{C}(\mathcal{Z})$ such that, for any point z of the intersection of their domains and $\mathcal{D}$, the condition $\eta_1(z) = \psi_1(z), \ldots, \eta_M(z) = \psi_M(z)$ is satisfied. Moreover, if $\mathfrak{M}$ denotes the (maximal) vanishing ideal of $\mathbb{C}[\mathcal{Z}]$ at the point $(0, \ldots, 0) \in \mathcal{Z} \cap \mathcal{D}$, since by assumption Ψ is geometrically robust and $\mathcal{Z}$ is an irreducible closed subvariety of $\overline{\mathcal{D}}$, the rational functions $\eta_1, \ldots, \eta_M$ are integral over $\mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$ (see also Proposition 16 and Theorem 9).

Therefore there exist $s \in \mathbb{N}$ and rational functions $p_{ij} \in \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$, $0 \le i \le s-1$, $1 \le j \le M$, such that

$$\eta_j^s + p_{s-1,j}\eta_j^{s-1} + \cdots + p_{0j} = 0 \tag{10}$$

holds in $\mathbb{C}(\mathcal{Z})$ for any $1 \le j \le M$.

Let $T, U_1, \ldots, U_n$ and $Y_1, \ldots, Y_K$ be new indeterminates, let $U := (U_1, \ldots, U_n)$ and $X := (X_1, \ldots, X_n)$, and let $G_{T,U}(X)$ be the polynomial of $\mathbb{C}[T, U, X]$ defined by

$$G_{T,U}(X) := T \sum_{k=0}^{2^\ell - 1} (U_1X_1 + \cdots + U_nX_n)^k.$$

Moreover, let $g_{T,U} := (G_{T,U}(\gamma_1), \ldots, G_{T,U}(\gamma_K))$. Then $g_{T,U}$ induces a dominating morphism of affine varieties $\mathbb{A}^{n+1} \to \mathcal{Z}$. This morphism induces a $\mathbb{C}$-algebra isomorphism between the $\mathbb{C}$-algebras $\mathbb{C}[\mathcal{Z}]$ and $\mathbb{C}[g_{T,U}]$, where $\mathbb{C}[g_{T,U}]$ is interpreted as the subalgebra of $\mathbb{C}[T, U]$ generated by $G_{T,U}(\gamma_1), \ldots, G_{T,U}(\gamma_K)$. This isomorphism maps the maximal ideal $\mathfrak{M}$ of $\mathbb{C}[\mathcal{Z}]$ onto the maximal ideal $\widetilde{\mathfrak{M}}$ of $\mathbb{C}[g_{T,U}]$ generated by $G_{T,U}(\gamma_1), \ldots, G_{T,U}(\gamma_K)$. Further, this isomorphism maps the rational functions $p_{ij} \in \mathbb{C}[\mathcal{Z}]_{\mathfrak{M}}$, $1 \le i \le s-1$, $1 \le j \le M$, onto rational functions $\widetilde{p}_{ij} \in \mathbb{C}[g_{T,U}]_{\widetilde{\mathfrak{M}}}$ and induces a $\mathbb{C}$-field isomorphism between $\mathbb{C}(\mathcal{Z})$ and $\mathbb{C}(g_{T,U})$ which maps $\eta_1, \ldots, \eta_K$ onto rational functions $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_K \in \mathbb{C}(g_{T,U})$. More precisely, we have $\widetilde{\eta}_1 = \eta_1 \circ g_{T,U}, \ldots, \widetilde{\eta}_K = \eta_K \circ g_{T,U}$ with well-defined compositions.

Let $Y := (Y_1, \ldots, Y_K)$ and $S := \{P(g_{T,U}) : P \in \mathbb{C}[Y], P(0, \ldots, 0) \ne 0\}$. Then S is a multiplicative subset of $\mathbb{C}[g_{T,U}]$ and hence of $\mathbb{C}[T, U]$. Observe $\mathbb{C}[g_{T,U}]_{\widetilde{\mathfrak{M}}} = S^{-1}\mathbb{C}[g_{T,U}]$. Identity (10) implies that

$$\widetilde{\eta}_j^s + \widetilde{p}_{s-1,j}\widetilde{\eta}_j^{s-1} + \cdots + \widetilde{p}_{0j} = 0 \tag{11}$$

holds in $\mathbb{C}(T, U)$ for any $1 \le j \le M$. Therefore $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_M$ are integral over $\mathbb{C}[g_{T,U}]_{\widetilde{\mathfrak{M}}} = S^{-1}\mathbb{C}[g_{T,U}]$ and hence over $S^{-1}\mathbb{C}[T, U]$. Since $\mathbb{C}[T, U]$ is integrally closed, the $\mathbb{C}$-algebra $S^{-1}\mathbb{C}[T, U]$ is also integrally closed (see, e.g., [20, Ch. VII, Section 1, Proposition 1.9]). Moreover, $S^{-1}\mathbb{C}[T, U]$ contains $S^{-1}\mathbb{C}[g_{T,U}]$. We conclude now that the rational functions $\widetilde{\eta}_1, \ldots, \widetilde{\eta}_M$ of $\mathbb{C}(T, U)$ belong to $S^{-1}\mathbb{C}[T, U]$.

Let u be an arbitrary point of $\mathbb{A}^n$ and P an arbitrary polynomial of $\mathbb{C}[Y]$ with $P(0, \ldots, 0) \ne 0$. We have $G_{0,u}(X) = 0$ and therefore $g_{0,u} = (0, \ldots, 0)$. This implies $P(g_{0,u}) = P(0, \ldots, 0) \ne 0$. Hence any rational function of $S^{-1}\mathbb{C}[T, U]$ is well defined at the point $(0, u) \in \mathbb{A}^{n+1}$. In particular the rational functions $\widetilde{\eta}_j$ and $\widetilde{p}_{ij}$, $1 \le i \le s-1$, $1 \le j \le M$, are well defined at $(0, u)$. Moreover, the value $\alpha_{ij} := \widetilde{p}_{ij}(0, u)$ does not depend on u, since $\widetilde{p}_{ij}$ belongs to $\mathbb{C}[g_{T,U}]_{\widetilde{\mathfrak{M}}}$.

Therefore (11) implies that

$$\widetilde{\eta}_j(0, u)^s + \alpha_{s-1,j}\widetilde{\eta}_j(0, u)^{s-1} + \cdots + \alpha_{0,j} = 0$$

holds in $\mathbb{C}$. Hence for $\widetilde{\eta}_j(0, u)$, $u \in \mathbb{A}^n$, there are only finitely many possible values. On the other hand, the map $\mathbb{A}^n \to \mathbb{A}^1$ which assigns to any point $u \in \mathbb{A}^n$ the value $\widetilde{\eta}_j(0, u) \in \mathbb{A}^1$ is a rational function which is regular everywhere on $\mathbb{A}^n$ and therefore a polynomial map whose image consists of finitely many points. We conclude now that the values $\widetilde{\eta}_1(0, u), \ldots, \widetilde{\eta}_M(0, u)$ are independent from the point $u \in \mathbb{A}^n$.

Let $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$ and, for $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, let $|\alpha| := \alpha_1 + \cdots + \alpha_n$. For a given nonnegative integer m, let

$$\Sigma_m := \{\alpha \in \mathbb{N}_0^n : |\alpha| \leq m\}.$$

Observe that Σ_m consists of $\binom{m+n}{n}$ elements.

Since every polynomial of $\overline{\mathcal{O}}$ has degree at most 2^L, we may consider for any $\alpha \in \Sigma_{2^L}$ with $\alpha := (\alpha_1, \ldots, \alpha_n)$ the coordinate function θ_α of $\mathbb{C}[\overline{\mathcal{O}}]$ which, applied to $f \in \overline{\mathcal{O}}$, yields the coefficient of the polynomial $f \in \Pi_{2^L}^{(n)}$ which corresponds to the monomial $X^\alpha := X_1^{\alpha_1} \ldots X_1^{\alpha_n}$. Moreover, for any $t \in \mathbb{A}^1$ and any $u := (u_1, \ldots, u_n) \in \mathbb{A}^n$ we have

$$\begin{aligned} G_{t,u} &= t \sum_{0 \leq k \leq 2^\ell - 1} \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ |\alpha| = k}} \frac{k!}{\alpha_1! \alpha_2! \ldots \alpha_n!} u_1^{\alpha_1} X_1^{\alpha_1} \ldots u_n^{\alpha_n} X_n^{\alpha_n} \\ &= t \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ 0 \leq |\alpha| \leq 2^\ell - 1}} \frac{|\alpha|!}{\alpha_1! \alpha_2! \ldots \alpha_n!} u_1^{\alpha_1} X_1^{\alpha_1} \ldots u_n^{\alpha_n} X_n^{\alpha_n}. \end{aligned}$$

Observe that $\deg G_{t,u} \leq 2^\ell - 1 \leq 2^L$ holds and that $G_{t,u}$ can be evaluated by a division-free straight-line program of nonscalar length $2(\ell - 1) \leq L$. Therefore $G_{t,u}$ belongs to $\Pi_{2^L}^{(n)}$ and in particular to $\mathcal{O}$. Thus for $\alpha \in \Sigma_{2^L}$ the value $\theta_\alpha(G_{t,u})$ is well defined and we have

$$\theta_\alpha(G_{t,u}) = \begin{cases} \dfrac{t|\alpha|!}{\alpha_1! \cdots \alpha_n!} u^\alpha & \text{if } \alpha \in \Sigma_{2^\ell - 1}, \\ 0 & \text{if } \alpha \in \Sigma_{2^L} \setminus \Sigma_{2^\ell - 1}. \end{cases}$$

For any $\rho \in \mathbb{A}^1$, let $\overline{\rho} := (\rho, \rho^{2^\ell}, \rho^{2^{2\ell}}, \ldots, \rho^{2^{(n-1)\ell}})$ and let $\beta_\rho : \mathbb{A}^1 \to \mathbb{A}^{n+1}$ be the (polynomial) map defined for $t \in \mathbb{A}^1$ by

$$\beta_\rho(t) := (t, \rho, \rho^{2^\ell}, \rho^{2^{2\ell}}, \ldots, \rho^{2^{(n-1)\ell}}).$$

From our previous argumentation, we infer that the composition

$$\sigma_\rho := \omega^* \circ \widetilde{\eta} \circ \beta_\rho \tag{12}$$

of the rational maps $\omega^*, \widetilde{\eta} := (\widetilde{\eta}_1, \ldots, \widetilde{\eta}_M)$ and β_ρ is well defined and regular at the point $t := 0$.

We now choose a small open polydisc Δ of $\mathbb{A}^2 = \mathbb{C}^2$ around the origin such that for any $(t, \rho) \in \Delta$ the rational map $\widetilde{\eta}$ is well defined at $\beta_\rho(t)$. Let $\eta := (\eta_1, \ldots, \eta_M)$. Then we have for $(t, \rho) \in \Delta$ the identities

$$\widetilde{\eta}(\beta_\rho(t)) = \eta(g_{t,\overline{\rho}}) = \Psi(g_{t,\overline{\rho}})$$

and therefore

$$\sigma_\rho(t) = \omega^*(\widetilde{\eta}(\beta_\rho(t))) = \omega^*(\eta(g_{t,\overline{\rho}})) = \omega^*(\Psi(g_{t,\overline{\rho}})) = \Phi(g_{t,\overline{\rho}}) = G_{t,\overline{\rho}}.$$

This implies that for any $\alpha \in \Sigma_{2^L}$ with $\alpha := (\alpha_1, \ldots, \alpha_n)$, we have that

$$\theta_\alpha(\sigma_\rho(t)) = \frac{t|\alpha|!}{\alpha_1! \cdots \alpha_n!} \overline{\rho}^\alpha = \frac{t|\alpha|!}{\alpha_1! \cdots \alpha_n!} \rho^{\alpha_1 + \alpha_2 2^\ell + \alpha_3 2^{2\ell} + \cdots + \alpha_n 2^{(n-1)\ell}} \tag{13}$$

holds if $\alpha \in \Sigma_{2^\ell - 1}$ and $\theta_\alpha(\sigma_\rho(t)) = 0$ holds if $\alpha \in \Sigma_{2^L} \setminus \Sigma_{2^\ell - 1}$.

Observe that the elements of the sequence $\left(\alpha_1 + \alpha_2 2^\ell + \cdots + \alpha_n 2^{(n-1)\ell}\right)_{(\alpha_1, \ldots, \alpha_n) \in \Sigma_{2^\ell - 1}}$ are all distinct, since $(\alpha_1, \ldots, \alpha_n) \in \Sigma_{2^\ell - 1}$ implies that $\alpha_1, \ldots, \alpha_n$ are nonnegative integers which are bounded by $2^\ell - 1$.

Let us fix $\rho \in \mathbb{A}^1$ with $(0,\rho) \in \Delta$. Applying the chain rule to the functional decomposition $\sigma_\rho(t) = \omega^* \circ \widetilde{\eta} \circ \beta_\rho(t)$ with $(t,\rho) \in \Delta$ we obtain

$$\frac{\mathrm{d}}{\mathrm{d}t}\sigma_\rho(0) = (\mathrm{d}\omega^*)(\widetilde{\eta}(\beta_\rho(0))) \cdot \frac{\mathrm{d}}{\mathrm{d}t}(\widetilde{\eta} \circ \beta_\rho)(0),$$

where $(\mathrm{d}\sigma_\rho/\mathrm{d}t)(0)$ denotes the derivative of σ_ρ at the point $t := 0$. As we have seen before, the value

$$\mu := \widetilde{\eta}(\beta_\rho(0)) = \widetilde{\eta}(0,\overline{\rho}) = (\widetilde{\eta}_1(0,\overline{\rho}), \ldots, \widetilde{\eta}_K(0,\overline{\rho}))$$

is independent from ρ.

Let C be the complex $(n_L \times M)$-matrix $C := (\mathrm{d}\omega^*)(\widetilde{\eta}(\beta_\rho(0))) = \mathrm{d}\omega^*(\mu)$, namely the Jacobian of ω^* at the point μ, which is independent from the value ρ. Then

$$\frac{\mathrm{d}}{\mathrm{d}t}\sigma_\rho(0) = (\mathrm{d}\omega^*)(\widetilde{\eta}(\beta_\rho(0))) \cdot \frac{\mathrm{d}}{\mathrm{d}t}(\widetilde{\eta} \circ \beta_\rho)(0) = C \cdot \frac{\mathrm{d}}{\mathrm{d}t}(\widetilde{\eta} \circ \beta_\rho)(0)$$

implies that $(\mathrm{d}\sigma_\rho/\mathrm{d}t)(0)$ is a $\mathbb{C}$-linear combination of the columns of C. From Lemma 24 we deduce that there exist suitable values $\rho_l \in \mathbb{C} \setminus \{0\}$, $1 \le l \le \#\Sigma_{2^\ell-1}$, with $(0,\rho_l) \in \Delta$ such that the column vectors $(\mathrm{d}\sigma_{\rho_l}/\mathrm{d}t)(0) \in \mathbb{A}^{n_L}$ are $\mathbb{C}$-linearly independent. This implies that the rank of the $(n_L \times M)$-matrix C is at least

$$\#\Sigma_{2^\ell-1} = \binom{2^\ell - 1 + n}{n} = \binom{2^{\left\lfloor \frac{L}{2}+1 \right\rfloor} - 1 + n}{n}.$$

Therefore we have

$$M \ge \binom{2^{\left\lfloor \frac{L}{2}+1 \right\rfloor} - 1 + n}{n}.$$

From of our assumption $2^{L/4} \ge n$ we deduce

$$\binom{2^{\left\lfloor \frac{L}{2}+1 \right\rfloor} - 1 + n}{n} \ge \frac{(2^{\frac{L}{2}} - 1)^n}{n!} \ge \frac{(2^{\frac{L}{2}} - 1)^n}{n^n} = 2^{\Omega(\frac{L}{2} - \log n)n} = 2^{\Omega(Ln)}$$

and from $N = K = (L+n+1)^2 + 2$ we conclude

$$Ln = \Omega(\sqrt{K}) = \Omega(\sqrt{N}).$$

Thus we obtain the lower bound

$$M \ge \binom{2^{\left\lfloor \frac{L}{2}+1 \right\rfloor} - 1 + n}{n} = 2^{\Omega(Ln)} = 2^{\Omega(\sqrt{K})} = 2^{\Omega(\sqrt{N})}.$$

In order to finish the proof of Theorem 23, we make use of the following result.

Lemma 24. *Let $m \in \mathbb{N}$, $n_1 < n_2 < \cdots < n_m \in \mathbb{N}_0$ be given and nonzero elements $a_1, \ldots, a_m \in \mathbb{A}^1$. Let $Z_1, \ldots, Z_m$ be indeterminates over $\mathbb{C}$ and let $P := (P_{i,j})_{1 \le i,j \le m} \in \mathbb{C}[Z_1, \ldots, Z_m]^{m \times m}$ be the $(m \times m)$-matrix whose entries are the polynomials $P_{i,j} := a_j Z_i^{n_j}$, $1 \le i,j \le m$. Then we have $\det P \ne 0$. In particular, there exist elements $\rho_1, \ldots, \rho_m \in \mathbb{C}$ with arbitrarily small norm for which the matrix $P(\rho_1, \ldots, \rho_m) = (a_j \rho_i^{n_j})_{1 \le i,j \le m}$ is nonsingular.*

Proof. We argue by induction on m. Since the case $m = 1$ is obvious, we may suppose $m > 1$. For $1 \le i \le m$, let Q_i be the $(m-1) \times (m-1)$-submatrix of P obtained deleting row number i and column number m. Observe that $\det Q_i$ does not contain the indeterminate Z_i. Then we have

$$\det P = (-1)^{m+1} a_m Z_1^{n_m} \det Q_1 + (-1)^{m+2} a_m Z_2^{n_m} \det Q_2 + \cdots + a_m Z_m^{n_m} \det Q_m.$$

For any $1 \leq i, j \leq m$, we have $\deg_{Z_j}(\det Q_i) \leq n_{m-1}$. Since Q_1 has the shape required by the statement of the lemma for the case $m-1$, we may apply the induction hypothesis to Q_1. We have therefore $\det Q_1 \neq 0$. Thus $(-1)^{n+m} a_m \det Q_1 \neq 0$ is the coefficient of the highest power, namely n_m, of Z_1 in P. This implies $\det P \neq 0$. The rest of the statement of the lemma is then obvious. □

We now apply Lemma 24 to the column vectors $(\mathrm{d}\sigma_\rho/\mathrm{d}t)(0) \in \mathbb{A}^{n_L}$ with $(0, \rho) \in \Delta$ and $\rho \neq 0$.

End of the proof of Theorem 23. With the notations of Lemma 24 and the proof of Theorem 23, let $m := \#\Sigma_{2^\ell-1} = \binom{2^\ell-1+n}{n} = \binom{2^{\lfloor \frac{L}{2} \rfloor+1}-1+n}{n}$ and let $0 \leq n_1 < \cdots < n_m$ be the elements of the sequence $\left(\alpha_1+\alpha_2 2^\ell+\cdots+\alpha_n 2^{(n-1)\ell}\right)_{(\alpha_1,\ldots,\alpha_n)\in\Sigma_{2^\ell-1}}$ in ordered form (recall that the elements of this sequence are all distinct). For $1 \leq j \leq m$ and $\alpha := (\alpha_1, \ldots, \alpha_n) \in \Sigma_{2^\ell-1}$ with $n_j = \alpha_1+\alpha_2 2^\ell+\cdots+\alpha_n 2^{(n-1)\ell}$, let $a_j := |\alpha|!/(\alpha_1!\cdots\alpha_n!)$ and $P \in \mathbb{C}[Z_1, \ldots, Z_m]^{m\times m}$ the $(m \times m)$-matrix defined in the statement of Lemma 24. Then there exist $\rho_1, \ldots, \rho_m \in \mathbb{C}^m$ with $(0, \rho_1) \in \Delta, \ldots, (0, \rho_m) \in \Delta$ such that $\det P(\rho_1, \ldots, \rho_m) \neq 0$ holds.

Let H be the complex $(n_L \times m)$-matrix consisting of the column vectors $(\mathrm{d}\sigma_{\rho_1}/\mathrm{d}t)(0), \ldots, (\mathrm{d}\sigma_{\rho_m}/\mathrm{d}t)(0)$. Then the identities (13) of the proof of Theorem 23 imply that the $(m \times m)$-submatrix of H determined by the rows corresponding to the elements of $\Sigma_{2^\ell-1}$ is the matrix $P(\rho_1, \ldots, \rho_m)$. From $\det P(\rho_1, \ldots, \rho_m) \neq 0$ we conclude now that H is of maximal rank m.

Therefore the $m := \#\Sigma_{2^\ell-1}$ column vectors $(\mathrm{d}\sigma_{\rho_l}/\mathrm{d}t)(0) \in \mathbb{A}^{n_L}$, $1 \leq l \leq m$, are $\mathbb{C}$-linearly independent. This completes the proof of Theorem 23. □

Acknowledgments

The authors wish to thank Marc Giusti, École Polytechnique, Palaiseau–Paris, and Andrés Rojas Paredes, Universidad de Buenos Aires, for their technical advice, and Verónica Becher, Universidad de Buenos Aires, for her insistent encouragement to finish this work.

The first author's research was partially supported by the grants UNGS 30/3084, CIC (2007–2009), PIP 11220090100421 CONICET. The second author's research was partially supported by the following Argentinian and Spanish agencies and grants: UBACYT X-098, UBACYT X-113, PICT-2006-02067, MTM 2007-62799. The third author's research was partially supported by the grants UNGS 30/3084, CIC (2007-2009), MTM 2007-62799, PIP 11220090100421 CONICET. The fourth author's research was partially supported by the grants UBACYT X-112, UBACYT X-211 and PICT 2007 No. 816.

Appendix A. A dictionary to the language of software engineering

In this Appendix we are going to translate to the language of software engineering the terminology previously introduced for the mathematical modeling of the concept of a Hermite–Lagrange interpolation problem and algorithm with polynomial interpolants. This translation was done by Andrés Rojas Paredes, Universidad de Buenos Aires, and can be found in full extent in [25].

A.1. The algorithmic model of this paper and its terminology

We start with the presentation of the more general terminology of [9, Sections 2.2, 3 and 5.4] which we then specialize to the case of Hermite–Lagrange interpolation. Let $\mathcal{O}$ and $\mathcal{O}^*$ be classes of mathematical objects (typically polynomials) which we think embedded as constructible sets in (typically high-dimensional) affine spaces. Furthermore, let $\mathcal{D}$ and $\mathcal{D}^*$ be given constructible subsets of (typically low-dimensional) affine spaces $\mathbb{A}^N$ and $\mathbb{A}^M$ and bijective constructible maps $\omega : \mathcal{D} \to \mathcal{O}$ and $\omega^* : \mathcal{D}^* \to \mathcal{O}^*$. Finally, let $\Psi : \mathcal{D} \to \mathcal{D}^*$ and $\Phi : \mathcal{O} \to \mathcal{O}^*$ be given constructible maps such that the diagram

$$\begin{array}{ccc} \mathcal{D} & \xrightarrow{\Psi} & \mathcal{D}^* \\ {\scriptstyle\omega}\downarrow & & \downarrow{\scriptstyle\omega^*} \\ \mathcal{O} & \xrightarrow{\Phi} & \mathcal{O}^* \end{array} \tag{A.1}$$

commutes. We call $\mathcal{O}$ and $\mathcal{O}^*$ *input* and *output object classes* (and their members mathematical input and output objects) and $\mathcal{D}$ and $\mathcal{D}^*$ *input* and *output data structures* (and their members input and output codes). The constructible maps ω and ω^* are called encodings of $\mathcal{O}$ and $\mathcal{O}^*$. The input and output code sizes are N and M. The constructible map Ψ is called a (continuous) *algorithm* which implements the (abstract) map Φ. The output code size M is considered as a lower bound for the complexity of Ψ.

The main concern in [9] is the case where ω and ω^* are polynomial maps, i.e., where the encodings are *holomorphic* and Ψ is at least topologically robust and hereditary, whereas Φ is typically a polynomial map. In case that $\mathcal{D}$ is irreducible one even supposes that Ψ is geometrically robust. If this condition is satisfied the continuous algorithm Ψ is called *branching-free*. In the typical case where $\mathcal{O}$ (and $\mathcal{O}^*$) are classes of n-variate polynomials we consider two queries, called the *identity* and the *value question*:

- For two given codes $d, d' \in \mathcal{D}$, decide whether d and d' represent the same object of $\mathcal{O}$, i.e., decide whether $\omega(d) = \omega(d')$ holds.
- For a given code $d \in \mathcal{D}$ and an argument point $x \in \mathbb{A}^n$, compute the value $\omega(d)(x)$ of the polynomial $\omega(d) \in \mathcal{O}$ at x.

In the case of Hermite–Lagrange interpolation a fundamental simplification occurs. In this case the input data structure $\mathcal{D}$ and the class of mathematical input objects coincide and ω becomes the identity map. This is the deeper sense of the double interpretation of $\mathcal{D}$ as an input data structure and as a class of interpolation data in Section 3. An element $d \in \mathcal{D}$ may be interpreted as input code as well as a mathematical object, called "interpolation datum", associated to another mathematical object, namely an interpolant belonging to $\mathcal{O}$.

A.2. The algorithmic model and its terminology in software engineering

We translate now this terminology to the language of software engineering in object oriented programming. The particular terms we use from software engineering are borrowed from [22]. We turn now back to the general situation at the beginning of the section.

We start by interpreting $\mathcal{D}$, $\mathcal{D}^*$ and $\mathcal{O}$, $\mathcal{O}^*$ as data types. For this purpose we assume that $\mathcal{O}$ and $\mathcal{O}^*$ are sets of polynomials. Let us only consider $\mathcal{D}$ and $\mathcal{O}$ (the case of $\mathcal{D}^*$ and $\mathcal{O}^*$ is similar). Since $\mathcal{D}$ is embedded in $\mathbb{A}^N$ we may suppose that the data type represented by $\mathcal{D}$ contains as constructors the restrictions to $\mathcal{D}$ of the canonical projections of $\mathbb{A}^N$ onto $\mathbb{A}^1$ and the arithmetic operations with them. Furthermore, the data type $\mathcal{D}$ contains the identity relation between elements of $\mathcal{D}$. By assumption $\mathcal{D}$ is a constructible subset of $\mathbb{A}^N$. Therefore there are constraints (i.e., a Boolean combination of polynomial equations) which decide in $\mathbb{A}^N$ membership to $\mathcal{D}$. The constructible set $\mathcal{D}$ is called a class and its elements are called objects. If the membership query for $\mathcal{D}$ in $\mathbb{A}^N$ belongs to the data type of $\mathcal{D}$ we call the (given) constraints defining $\mathcal{D}$ a *class invariant*.

The data type represented by $\mathcal{O}$ is slightly different since we shall avoid the reference to the given embedding of $\mathcal{O}$ in a (possibly high-dimensional) affine space. Since by assumption $\mathcal{O}$ is a set of polynomials we may suppose that the data type $\mathcal{O}$ contains as creators the arithmetic operations with elements of $\mathcal{O}$. Again we suppose that the data type $\mathcal{O}$ contains the identity relation between the elements of $\mathcal{O}$. Since the query for membership of polynomials to $\mathcal{O}$ does not belong to the data type of $\mathcal{O}$, we do not refer to $\mathcal{O}$ as a class and consequently we do not speak about class invariants in this context. The relevant properties of $\mathcal{O}$ inherited by its embeddings in an affine space and in a polynomial ring are expressed by certain *axioms* satisfied by the data type of $\mathcal{O}$ (e.g., the associativity of the addition of elements of $\mathcal{O}$). In this sense we refer to $\mathcal{O}$ as an *abstract data type*. The elements of

$\mathcal{O}$ are called objects. In order to distinguish the nature of the objects contained in $\mathcal{O}$ and $\mathcal{D}$, we refer to them as *abstract* and *concrete*, respectively.

The constructible map $\omega : \mathcal{D} \to \mathcal{O}$ is called an *abstraction function* and the data type of $\mathcal{D}$ an *implementation* of $\mathcal{O}$. We refer to $\Phi : \mathcal{O} \to \mathcal{O}^*$ as an *operation* (or *abstract function*) on the abstract data type $\mathcal{O}$ and to $\Psi : \mathcal{D} \to \mathcal{D}^*$ as an implementation of Φ. A query which is expressible by the data type of $\mathcal{O}$ and returns Boolean or complex values is called an (abstract) *function* of $\mathcal{O}$. The term function is also used for queries on the class $\mathcal{D}$ which implement abstract functions of $\mathcal{O}$. Examples of functions are the identity and the value question. In the context of this paper, namely the Hermite–Lagrange interpolation, we may interpret the routine $\Psi : \mathcal{D} \to \mathcal{D}^*$ as a function or as a *procedure* (or method). In the first case the values of Ψ are considered as outputs and in the second case the values of Ψ are only "intermediate results", whereas the values of $\omega^* \circ \Psi$ are considered as outputs. In any case, $\Psi : \mathcal{D} \to \mathcal{D}^*$ represents the *concrete* and $\Phi : \mathcal{O} \to \mathcal{O}^*$ the *abstract level* of our program design. The final aim of a computer program is the evaluation of abstract functions. Procedures may be interpreted as components of such programs. On the other hand, routines which are functions form the essential ingredients of a program library. The diagrams (1) and (A.1) represent the design of a program architecture. The (possible) requirement that ω and ω^* are polynomial maps forms part of the design.

This paper is devoted to the analysis of algorithms which may be implemented numerically in fixed precision as well as symbolically in infinite precision. This is the reason why we have chosen as a "platform" the algebraic complexity model with the arithmetic operations implemented at unit costs. Consequently, classes and routines have to be constructible. If we require that routines admit specifications and correctness proofs, the abstract data types, the operations on them and the abstraction functions have also to be constructible.

If we now require that in the architectural design of Hermite–Lagrange interpolation the abstraction function ω^* is polynomial, then we deal with a restriction of the design. This restriction is well motivated if we think about the representation of polynomials by their coefficients or by division-free straight-line programs. In the algebraic complexity model, the sequential time complexity of Ψ (measured in terms of the number of arithmetic operations) is a (quantitative) *quality attribute* of Ψ. Without loss of generality we may assume that the complexity of Ψ is at least M.

Another (dichotomic) quality attribute of Ψ is geometric robustness. If we think about numerical implementations, the *non-functional requirement* (or quality attribute) that Ψ is geometrically robust seems well motivated because it allows to avoid branchings.

Now we are ready to paraphrase in terms of software engineering Theorem 23 of Section 5.2:
Under the architectural design of Hermite–Lagrange interpolation contained in Definition 7, *the non-functional requirement that Ψ is geometrically robust implies an exponential blow up of the complexity* of Ψ.

We do not know of any other example in software engineering where a tradeoff between two quality attributes is certified by a mathematical proof. On the other hand, architecture tradeoff analysis methods (ATAM) represent a modern trend in software engineering (see, e.g., [2,3,18]).

References

[1] A. Alder, Grenzrang und Grenzkomplexität aus algebraischer und topologischer sicht, Ph.D. Thesis, Universität Zürich, Philosophische Fakultät II, 1984.
[2] M. Barbacci, M. Klein, T. Longstaff, C. Weinstock, Quality attributes, Technical Report CMU/SEI-95-TR-021, ESC-TR-95-021, Software Engineering Institute, Carnegie Mellon University, 1995.
[3] L. Bass, P. Clements, R. Kazman, Software Architecture in Practice, second ed., Addison-Wesley, Boston, MA, 2003.
[4] T. Bloom, J.-P. Calvi, A continuity property of multivariate Lagrange interpolation, Math. Comp. 66 (220) (1997) 1561–1577.
[5] L. Blum, F. Cucker, M. Shub, S. Smale, Algebraic settings for the problem "$P \neq NP$"? in: J. Renegar, M. Shub, S. Smale (Eds.), The Mathematics of Numerical Analysis: 1995 AMS-SIAM Summer Seminar in Applied Mathematics, July 17–August 11, 1995, Park City, Utah, in: Lectures in Applied Mathematics, vol. 32, Amer. Math. Soc., Providence, RI, 1996, pp. 125–144.
[6] L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and Real Computation, Springer, New York, Berlin, Heidelberg, 1998.
[7] L. Blum, M. Shub, S. Smale, On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines, Bull. Amer. Math. Soc. 21 (1) (1989) 1–46.
[8] P. Bürgisser, M. Clausen, M. Shokrollahi, Algebraic Complexity Theory, in: Grundlehren Math. Wiss., vol. 315, Springer, Berlin, 1997.
[9] D. Castro, M. Giusti, J. Heintz, G. Matera, L.M. Pardo, The hardness of polynomial equation solving, Found. Comput. Math. 3 (4) (2003) 347–420.

[10] C. de Boor, A. Ron, The least solution for the polynomial interpolation problem, Math. Z. 210 (3) (1992) 347–378.
[11] C. de Boor, A. Ron, On multivariate polynomial interpolation, Constr. Approx. 6 (3) (1990) 287–302.
[12] M. Giusti, J. Heintz, Kronecker's smart, little black-boxes, in: A. Iserles, R. Devore, E. Süli (Eds.), Proceedings of Foundations of Computational Mathematics, FoCM'99, Oxford 1999, in: London Math. Soc. Lecture Note Ser., vol. 284, Cambridge Univ. Press, Cambridge, 2001, pp. 69–104.
[13] H. Grauert, K. Fritzsche, Several Complex Variables, in: Grad. Texts in Math., vol. 38, Springer, New York, Heidelberg, Berlin, 1976.
[14] J. Heintz, B. Kuijpers, Constraint databases, data structures and efficient query evaluation, in: B. Kuijpers (Ed.), Constraint Databases, First International Symposium, CDB 2004, Paris, France, June 12–13, 2004, in: Lecture Notes in Comput. Sci., vol. 3074, Springer, Berlin, 2004, pp. 1–24.
[15] J. Heintz, J. Morgenstern, On the intrinsic complexity of elimination theory, J. Complexity 9 (1983) 471–498.
[16] J. Heintz, C.-P. Schnorr, Testing polynomials which are easy to compute, in: International Symposium on Logic and Algorithmic, Zurich 1980, in: Monogr. Enseig. Math., vol. 30, 1982, pp. 237–254.
[17] B. Iversen, Generic Local Structure of the Morphisms in Commutative Algebra, in: Lecture Notes in Math., vol. 310, Springer, New York, 1973.
[18] R. Kazman, M. Klein, M. Barbacci, T. Longstaff, H. Lipson, S. Jeromy Carrière, The architecture tradeoff analysis method, in: Proceedings 4th International Conference on Engineering of Complex Computer Systems, ICECCS'98, 10–14 August, 1998, IEEE Computer Society, Monterrey, CA, USA, 1998, pp. 68–78.
[19] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, 1985.
[20] S. Lang, Algebra, third ed., Addison-Wesley, Reading, Massachusetts, 1993.
[21] O. Marker, Model Theory: An Introduction, in: Grad. Texts in Math., vol. 217, Springer, New York, 2002.
[22] B. Meyer, Object-Oriented Software Construction, second ed., Prentice-Hall, Upper Saddle River, NJ, 2000.
[23] D. Mumford, The Red Book of Varieties and Schemes, in: Lecture Notes in Math., vol. 1358, Springer, New York, 1988.
[24] P. Olver, On multivariate interpolation, Stud. Appl. Math. 116 (2) (2006) 201–240.
[25] A. Rojas Paredes, Complexity as quality attribute in software design, Master Thesis, Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, 2010.
[26] I.R. Shafarevich, Basic Algebraic Geometry: Varieties in Projective Space, Springer, Berlin, Heidelberg, New York, 1994.
[27] J. Stoer, R. Bulirsch, Introduction to Numerical Analysis, second ed., Springer, Berlin, Heidelberg, New York, 1993.
[28] B. Teissier, Variétés polaires. II: multiplicités polaires, sections planes et conditions de Whitney, in: J. Aroca, R. Buchweitz, M. Giusti, M. Merle (Eds.), Algebraic Geometry, Proc. Int. Conf., La Rábida/Spain 1981, in: Lect. Notes Math., vol. 961, Springer, Berlin, Heidelberg, New York, 1982, pp. 314–491.
[29] O. Zariski, P. Samuel, Commutative Algebra II, in: Grad. Texts in Math., vol. 39, Springer, New York, 1960.