

# Quiz Games as a model for Information Hiding

Bernd Bank<sup>1</sup>, Joos Heintz<sup>2,3</sup>, Guillermo Matera<sup>3,4</sup>,  
José Luis Montaña<sup>5</sup>, Luis M. Pardo<sup>5</sup>, Andrés Rojas Paredes<sup>2</sup>

November 13, 2015

## Abstract

We present a general computation model inspired in the notion of information hiding in software engineering. This model has the form of a game which we call *quiz game*. It allows in a uniform way to prove exponential lower bounds for several complexity problems.

## 1 Introduction

We present a general computation model inspired in the notion of information hiding in software engineering. This model has the form of a game which we call *quiz game*. It consists of a one round two-party protocol between two agents, namely a *quizmaster* with limited and a *player* with unlimited computational power. We suppose that the quizmaster is honest and able to answer the player's questions. Using this model we are able to prove exponential lower bounds for several complexity problems in a uniform way,

---

<sup>0</sup>Research was partially supported by the following Spanish and Argentinean grants: MTM2010-16051, MTM2014-55262-P, PIP CONICET 11220130100598, PIO CONICET-UNGS 14420140100027 and UNGS 30/3084, UBACyT 20020130100433BA.

<sup>1</sup>Humboldt-Universität zu Berlin, Institut für Mathematik, 10099 Berlin, Germany.  
*Email address:* `bank@mathematik.hu-berlin.de`

<sup>2</sup>Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Univ., Pab. I, 1428 Buenos Aires, Argentina. *Email address:* `{joos,arojas}@dc.uba.ar`

<sup>3</sup>National Council of Science and Technology (CONICET), Argentina

<sup>4</sup>Instituto del Desarrollo Humano, Universidad Nacional General Sarmiento, J. M. Gutiérrez 1150 (B1613GSX) Los Polvorines, Provincia de Buenos Aires, Argentina. *Email address:* `gmatera@ungs.edu.ar`

<sup>5</sup>Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, 39071 Santander, Spain. *Email address:* `joseluis.montana@unican.es, luis.m.pardo@gmail.com`

for example for the continuous interpolation of multivariate polynomials of given circuit complexity (Theorem 13). It is also possible to exhibit sequences of families of multivariate polynomials which are easy to evaluate such that the continuous interpolation of these polynomials, or their derivatives or their indefinite integrals require an amount of arithmetic operations which is exponential in their circuit complexity (Theorem 16). On the other hand, we represent neural networks with polynomial activation functions in our model and show that there is no continuous algorithm able to learn relatively simple neural networks exactly (Theorem 18). Finally, we exhibit infinite families of first-order formulae over  $\mathbb{C}$  which can be encoded in polynomial time and determine classes of univariate parameterized elimination polynomials such that any representation of these classes is of exponential size (Theorems 20 and 23).

Ad hoc variants of the method we use and partial results already appeared elsewhere ([GHMS11], [HKR13b]). What is really new is the general framework which we develop to approach these complexity results in order to prove (and generalize) them in a uniform way.

The quiz games which constitute the core of our model admit two “protocols”, an “exact” and an “approximative” one. The exact protocol aims to represent symbolic procedures for solving parametric families of elimination problems and is first discussed in the context of robust arithmetic circuits and neural networks. The approximative protocol is able to deal with information of approximative nature. It is motivated by the notion of an approximative parameter instance which encodes a polynomial with respect to an abstract data type. The main outcome is that there exists an approximative parameter instance encoding a given polynomial if and only if that polynomial belongs to the closure of the corresponding abstract data type with respect to the Euclidean topology.

The idea behind this computational model is to restrict the information which quizmaster and player may interchange. This reflects the concept of information hiding in software engineering aimed to control and reduce the design complexity of a computer program.

In the most simple case the notion of an exact quiz game protocol may be explained roughly as follows. Suppose that there is given a continuous data structure carrier together with an abstraction function which encodes a parameterized family of polynomials. The quizmaster chooses from the data structure carrier a parameter which encodes a specific polynomial and hides them to the player. The player asks to the quizmaster questions about the hidden polynomial, whose answers constitute a vector of complex values which depend only on the polynomial itself and are independent of the hidden parameter. The quizmaster sends this vector to the player and the player

computes a representation of the polynomial in an alternative data structure carrier. Finally, the quizmaster tests whether this alternative representation encodes the hidden polynomial. Observe that polynomial interpolation is a typical situation that can be formulated in such a way.

The paper constitutes a mixture between ideas and concepts coming from software engineering, algebraic complexity theory and algebraic geometry. A fundamental tool is an algebraic characterization of the total maps whose graphs are first-order definable over  $\mathbb{C}$  and continuous with respect to the Euclidean topology. We call these maps *constructible and geometrically robust* (see Theorem 7).

## 2 Concepts and tools from algebraic geometry

In this section, we use freely standard notions and notations from commutative algebra and algebraic geometry. These can be found for example in [Eis95], [Kun85], [Mum88] and [Sha94]. In Section 2.2 we introduce the notions and definitions which constitute the fundamental tool for our algorithmic models. Most of these notions and their definitions are taken from [GHMS11] and [HKR13b].

### 2.1 Basic notions and notations

Let  $k$  be a fixed algebraically closed field of characteristic zero. For any  $n \in \mathbb{N}$ , we denote by  $\mathbb{A}^n(k)$  the  $n$ -dimensional affine space  $k^n$  equipped with its Zariski topology. For  $k = \mathbb{C}$ , we consider the complex  $n$ -dimensional affine space  $\mathbb{A}^n := \mathbb{A}^n(\mathbb{C})$ , equipped with its respective Zariski and Euclidean topologies.

Let  $X_1, \dots, X_n$  be indeterminates over  $k$  and let  $X := (X_1, \dots, X_n)$ . We denote by  $k[X] := k[X_1, \dots, X_n]$  the ring of polynomials in the variables  $X$  with coefficients in  $k$ .

Let  $V$  be a closed affine subvariety of  $\mathbb{A}^n(k)$ . We denote by  $I(V) := \{f \in k[X] : f(x) = 0 \text{ for any } x \in V\}$  the ideal of definition of  $V$  in  $k[X]$  and by  $k[V] := \{\phi : V \rightarrow k : \text{there exists } f \in k[X] \text{ with } \phi(x) = f(x) \text{ for any } x \in V\}$  its coordinate ring. The elements of  $k[V]$  are called coordinate functions of  $V$ . Observe that  $k[V]$  is isomorphic to the quotient  $k$ -algebra  $k[X]/I(V)$ . If  $V$  is irreducible, then  $k[V]$  has no zero divisors, and we denote by  $k(V)$  the field formed by the rational functions of  $V$  with maximal domain ( $k(V)$  is called the rational function field of  $V$ ). Observe that  $k(V)$  is isomorphic to the fraction field of the integral domain  $k[V]$ .

Let  $V$  and  $W$  be closed affine subsets of  $\mathbb{A}^n(k)$  and  $\mathbb{A}^m(k)$ , respectively, and let  $\Phi : V \rightarrow W$  be a (total) map. We call  $\Phi$  a *morphism* from the affine variety  $V$  to  $W$  if there exist polynomials  $f_1, \dots, f_m \in k[X]$  such that  $\Phi(x) = (f_1(x), \dots, f_m(x))$  holds for any  $x \in V$ .

Let  $V$  be irreducible, let  $U$  be a nonempty Zariski open subset of  $V$  and let  $\Phi : V \dashrightarrow W$  be a partial map with domain  $U$ . Let  $\Phi_1, \dots, \Phi_m$  be the components of  $\Phi$ . We call  $\Phi$  a *rational map* from  $V$  to  $W$  if  $\Phi_1, \dots, \Phi_m$  are the restrictions to  $U$  of suitable rational functions of  $V$ . Observe that our definition of a rational map differs slightly from the usual one in algebraic geometry, since we do not require that the domain  $U$  of  $\Phi$  is maximal. Hence in the case  $m := 1$  our concepts of rational function and rational map do not coincide. However we will not stick on this point and simply speak about rational functions when  $m = 1$ .

**Example 1.** Let  $f : \mathbb{A}^2 \dashrightarrow \mathbb{A}^1$  be the map defined as  $f(X_1, X_2) := \frac{X_1+X_2}{X_1-X_2}$  on  $U := \mathbb{A}^2 \setminus \{X_1^2 - X_2^2 = 0\}$ . Then  $f$  may be considered as a rational map in the sense above, but it is not a rational function on  $\mathbb{A}^2$ .

## 2.2 Geometrically robust constructible maps

Let  $\mathcal{M}$  be a subset of some affine space  $\mathbb{A}^n(k)$  and, for a given non-negative integer  $m$ , let  $\Phi : \mathcal{M} \dashrightarrow \mathbb{A}^m(k)$  be a partial map.

**Definition 2.** We call the set  $\mathcal{M}$  *constructible* if  $\mathcal{M}$  is definable by a Boolean combination of polynomial equations from  $k[X]$ , namely as a finite union of sets of solutions of equalities and inequalities defined by elements of  $k[X]$ .

Since the elementary theory of algebraically closed fields of characteristic zero admits quantifier elimination (see, e.g., [FJ05]), constructible and definable sets in the first-order logic over  $k$  are exactly the same.

For a constructible subset  $\mathcal{M}$  of  $\mathbb{A}^n(k)$ , we denote its Zariski closure by  $\overline{\mathcal{M}}$ . For  $k = \mathbb{C}$ , the Zariski closure of a constructible subset  $\mathcal{M}$  of  $\mathbb{A}^n$  coincides with its Euclidean closure (see, e.g., [Mum88, Chapter I, Section 10, Corollary 1]). Hence the notation  $\overline{\mathcal{M}}$  for the closure of  $\mathcal{M}$  with respect to both topologies is unambiguous.

A constructible subset  $\mathcal{M}$  of  $\mathbb{A}^n(k)$  is called *irreducible* if it cannot be written as a nontrivial union of two subsets of  $\mathcal{M}$  which are closed with respect to the Zariski topology of  $\mathcal{M}$ . Each constructible subset  $\mathcal{M}$  of  $\mathbb{A}^n(k)$  has a unique irredundant irreducible decomposition as a finite union of irreducible, constructible subsets of  $\mathcal{M}$ , which are closed in  $\mathcal{M}$ . These subsets are called the *irreducible components* of  $\mathcal{M}$ .

**Definition 3.** We call the partial map  $\Phi$  constructible if the graph of  $\Phi$  is constructible as a subset of the affine space  $\mathbb{A}^n(k) \times \mathbb{A}^m(k)$ .

We say that the constructible map  $\Phi$  is *polynomial* if  $\Phi$  is the restriction to  $\mathcal{M}$  of a morphism of affine varieties  $\mathbb{A}^n(k) \rightarrow \mathbb{A}^m(k)$ . A polynomial map  $\Phi : \mathcal{M} \rightarrow \mathbb{A}^m(k)$  is everywhere defined on  $\mathcal{M}$  and hence total. The constructible map  $\Phi$  is *rational* if the intersection of its domain with any irreducible component  $\mathcal{N}$  of  $\mathcal{M}$  is a nonempty open subset  $\mathcal{U}$  of the closure  $\overline{\mathcal{N}}$  of  $\mathcal{N}$  in the Zariski topology of  $\mathbb{A}^n(k)$  and the restriction  $\Phi|_{\mathcal{U}}$  of  $\Phi$  to  $\mathcal{U}$  is a rational map of  $\overline{\mathcal{N}}$ . In this case  $\mathcal{U}$  is a Zariski dense subset of  $\mathcal{N}$ .

**Remark 4.** A partial map  $\Phi : \mathcal{M} \dashrightarrow \mathbb{A}^m(k)$  is constructible if and only if it is piecewise rational. If  $\Phi$  is a total constructible map, then there exists an open subset  $\mathcal{U}$  of  $\mathcal{M}$  with nonempty intersection with any irreducible component of  $\mathcal{M}$  such that  $\Phi|_{\mathcal{U}}$  is a rational map of  $\mathcal{M}$ .

The first statement follows from quantifier elimination, whereas the second follows from [GHMS11, Lemma 1].

Fix for the moment an irreducible constructible subset  $\mathcal{M}$  of the affine space  $\mathbb{A}^n(k)$  and a total constructible map  $\Phi : \mathcal{M} \rightarrow \mathbb{A}^m(k)$  with components  $\Phi_1, \dots, \Phi_m$ . Observe that the closure  $\overline{\mathcal{M}}$  of  $\mathcal{M}$  is an irreducible closed affine subvariety of  $\mathbb{A}^n(k)$  and that we may interpret  $k(\overline{\mathcal{M}})$  as a  $k[\overline{\mathcal{M}}]$ -module (or  $k[\overline{\mathcal{M}}]$ -algebra). Fix now an arbitrary point  $x$  of  $\overline{\mathcal{M}}$ . By  $\mathfrak{M}_x$  we denote the maximal ideal of coordinate functions of  $\overline{\mathcal{M}}$  which vanish at the point  $x$ . By  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$  we denote the local  $k$ -algebra of the variety  $\overline{\mathcal{M}}$  at the point  $x$ , i.e., the localization of  $k[\overline{\mathcal{M}}]$  at the maximal ideal  $\mathfrak{M}_x$ .

Following Remark 4 we may interpret  $\Phi_1, \dots, \Phi_m$  as rational functions of the irreducible variety  $\overline{\mathcal{M}}$  and therefore as elements of  $k(\overline{\mathcal{M}})$ . Thus  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\Phi_1, \dots, \Phi_m]$  is a  $k$ -subalgebra of  $k(\overline{\mathcal{M}})$  which contains  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ .

**Definition 5.** Let  $\mathcal{M}$  be a constructible subset of a suitable affine space over  $k$  and let  $\Phi : \mathcal{M} \rightarrow \mathbb{A}^m(k)$  be a total constructible map with components  $\Phi_1, \dots, \Phi_m$ . If  $\mathcal{M}$  is irreducible, then we call  $\Phi$  *geometrically robust* if for any point  $x \in \mathcal{M}$  the following two conditions are satisfied:

- (i)  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\Phi_1, \dots, \Phi_m]$  is a finite  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ -module,
- (ii)  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\Phi_1, \dots, \Phi_m]$  is a local  $k[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ -algebra whose maximal ideal is generated by  $\mathfrak{M}_x$  and  $\Phi_1 - \Phi_1(x), \dots, \Phi_m - \Phi_m(x)$ .

In the general case, let  $\mathcal{N}_1, \dots, \mathcal{N}_s$  be the irreducible components of  $\mathcal{M}$ . We call then  $\Phi$  *geometrically robust* if the restrictions  $\Phi|_{\mathcal{N}_1}, \dots, \Phi|_{\mathcal{N}_s}$  are geometrically robust in the above sense.

If  $\Phi$  is a geometrically robust constructible map, we call  $\mathcal{M}$  the *domain of definition* of  $\Phi$ . The following statements characterize the unique properties of geometrically robust constructible maps which will be relevant in the sequel.

**Theorem 6.**

- (i) *The restriction of a geometrically robust constructible map to a constructible subset of its domain is geometrically robust.*
- (ii) *Compositions and cartesian products of geometrically robust constructible maps are geometrically robust.*
- (iii) *A geometrically robust constructible map defined on a normal (e.g., smooth) variety is a polynomial map.*
- (iv) *Polynomial maps are geometrically robust and constructible and the geometrically robust constructible functions of a constructible domain of definition form a  $k$ -algebra.*

For a proof of the statements (i) and (iii) we refer to [GHMS11, Theorem 17 and Corollary 12], respectively. The statements (ii) and (iv) are immediate consequences of Definition 5.

With some extra effort one can also show that geometrically robust constructible maps are continuous with respect to the Zariski topologies of their domain and range spaces. We shall prove this only in case  $k := \mathbb{C}$  (see Lemma 25(ii) in Appendix A). Furthermore, we have the following result (for a proof, see [HKR13b, Theorem 4]).

**Theorem 7.** *Let  $\mathcal{M}$  be a constructible subset of  $\mathbb{A}^n$  and let  $\Phi : \mathcal{M} \rightarrow \mathbb{A}^m$  be a constructible total map. Then  $\Phi$  is geometrically robust if and only if  $\Phi$  is continuous with respect to the Euclidean topologies of  $\mathcal{M}$  and  $\mathbb{A}^n$ .*

Theorem 7 gives a topological characterization of the notion of geometrically robust constructible maps over  $\mathbb{C}$ . This notion represents the real motivation of Definition 5, both from a geometric as well as from an algorithmic point of view.

In Appendix A we establish further facts on geometrically robust constructible maps which will be needed in the sequel.

### 3 The computation model

In this section we present our computation model. It will be expressed in terms of framed abstract data type carriers, framed data structures and abstraction functions. These notions are first informally discussed in the context of robust arithmetic circuits and neural networks, and then in a general setting. Then we introduce our model, which has the form of a game—a quiz game—and aims to represent the notion of information hiding in software engineering. We shall present two “protocols” of a quiz game: an “exact” and an “approximative” one. In this section we consider only the exact protocol, while the somewhat more subtle approximative protocol is discussed in the next section.

#### 3.1 Robust arithmetic circuits

Let us fix natural numbers  $r$  and  $n$ , indeterminates  $X_1, \dots, X_n$  and a non-empty constructible subset  $\mathcal{M}$  of  $\mathbb{A}^r$ . A *robust arithmetic circuit* (with parameter domain  $\mathcal{M}$  and inputs  $X_1, \dots, X_n$ ) is a labeled directed acyclic graph (labeled DAG)  $\beta$  satisfying the following conditions: each node of indegree zero is labeled by a robust constructible function (called parameter of  $\beta$ ) with domain of definition  $\mathcal{M}$  or by a variable  $X_1, \dots, X_n$  (called inputs of  $\beta$ ). All other nodes of  $\beta$  have indegree two and are called *internal*. They are labeled by the arithmetic operations addition, subtraction or multiplication. Moreover, exactly one node of  $\beta$  becomes labeled as output. We call the number of nodes the *size* of  $\beta$ .

We consider  $\beta$  as a syntactic object which we think equipped with the following semantics. There exists a canonical evaluation procedure of  $\beta$  assigning to each node a geometrically robust constructible function with domain of definition  $\mathcal{M} \times \mathbb{A}^n$  which, in case of a parameter node, may also be interpreted as a geometrically robust function with domain of definition  $\mathcal{M}$ . In either situation, we call such a function an *intermediate result* of  $\beta$ . The intermediate result associated with the output node will be called the *final result* of  $\beta$ . We refer to  $\mathcal{M}$  as the *parameter domain* of  $\beta$ .

By definition,  $\beta$  does not contain divisions involving the inputs. Divisions may appear, only implicitly, in the construction of the parameters of  $\beta$ . In this sense  $\beta$  is *essentially division-free*. Therefore all intermediate results of  $\beta$  are polynomials in  $X_1, \dots, X_n$  over the  $\mathbb{C}$ -algebra of geometrically robust constructible functions with domain of definition  $\mathcal{M}$ .

We may consider  $\beta$  as a program which solves the problem to evaluate, for each  $u \in \mathcal{M}$ , the polynomial function  $\mathbb{A}^n \rightarrow \mathbb{A}^1$  which we obtain by specializing to the point  $u$  the first argument of the geometrically robust

constructible function  $\mathcal{M} \times \mathbb{A}^n \rightarrow \mathbb{A}^1$  given by the final result of  $\beta$ . In this sense  $\beta$  defines an *abstraction function*  $\theta$  which assigns to each parameter instance  $u \in \mathcal{M}$  a polynomial function from  $\mathbb{A}^n$  into  $\mathbb{A}^1$ . These polynomial functions constitute a (unary) *abstract data type carrier*  $\mathcal{O}$  which is contained in a finite dimensional  $\mathbb{C}$ -vector subspace of  $\mathbb{C}[X_1, \dots, X_n]$  and forms there a constructible subset. We call therefore this carrier *framed*. The abstraction function  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  is geometrically robust and constructible. The constructible parameter domain  $\mathcal{M}$  constitutes a *framed data structure* which represents the elements of  $\mathcal{O}$  by means of the geometrically robust constructible map  $\theta$ .

Suppose that  $\beta$  contains  $K$  parameter nodes. The corresponding parameters of  $\beta$  realize a geometrically robust constructible map  $\mu : \mathcal{M} \rightarrow \mathbb{A}^K$  with constructible image  $\mathcal{N}$ . Since the circuit  $\beta$  is essentially division-free, there exists a polynomial map  $\omega : \mathcal{N} \rightarrow \mathcal{O}$  such that  $\theta = \omega \circ \mu$  holds.

In Section 3.3 we are going to axiomatize this situation and to define precisely what we mean by the up to now informal notions of framed abstract data type carrier, framed data structure and abstraction function. For more details about robust arithmetic circuits and their motivations we refer to [HKR13b].

Particular instances of robust arithmetic circuits are those whose parameter domain are affine spaces. In this case all parameters are polynomials (see Theorem 6(iii)). These circuits represent abstraction functions which encode polynomial functions defined on affine spaces by means of *ordinary division-free arithmetic circuits* (see [HKR13b] for this terminology).

Let  $L, n \in \mathbb{N}$  and let  $\mathcal{O}_{L,n}$  be the family of all polynomials of  $\mathbb{C}[X_1, \dots, X_n]$  which can be evaluated by an ordinary division-free arithmetic circuit with at most  $L$  *essential* multiplications, involving the input variables  $X_1, \dots, X_n$  meanwhile  $\mathbb{C}$ -linear operations are free. Then  $\mathcal{O}_{L,n}$  is an abstract data type whose abstraction function is represented by a robust arithmetic circuit with parameter domain  $\mathbb{A}^{(L+n+1)^2}$  (see [BCS97, Exercise 9.18]). We call this arithmetic circuit the *generic computation* of all  $n$ -variate polynomials which can be evaluated with at most  $L$  essential multiplications.

## 3.2 Neural networks with polynomial activation functions

In this section we will freely use well-established terminology on neural networks (see, e.g., [HKP91], [HKP99] or [HDB96]). Let be given a neural network architecture with  $n$  inputs  $X_1, \dots, X_n$  and one output and let  $r$  be the length of the corresponding weight vector. We suppose that all activa-



tion functions are given by univariate polynomials over  $\mathbb{R}$ . Observe that each weight vector instance  $w \in \mathbb{R}^r$  defines a neural network of this architecture and thus a polynomial target function from  $\mathbb{R}^n$  into  $\mathbb{R}$ . The dependency weight vector instance–target function is itself polynomial and can be extended to  $\mathbb{A}^r$ . The complex target functions we obtain in this way constitute a (unary) abstract data type carrier  $\mathcal{O}$  which is contained in a finite dimensional  $\mathbb{C}$ –vector subspace of  $\mathbb{C}[X_1, \dots, X_n]$  and forms there a constructible subset. In this sense, the abstract data type carrier  $\mathcal{O}$  is again framed. Thus we obtain for  $\mathcal{M} := \mathbb{A}^r$  a surjective polynomial map  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  which may be interpreted as an abstraction function which represents the elements of  $\mathcal{O}$  by means of complex weight vector instances belonging to  $\mathcal{M}$ . In this meaning  $\mathcal{M}$  constitutes a framed data structure. Since  $\theta$  is polynomial, we may obviously write it as a composition of a polynomial and a geometrically robust constructible map. Hence we shall interpret again  $\theta$  as an abstraction function.

### 3.3 Framed abstract data type carriers, framed data structures and abstraction functions

Now we define in a general context the notions of framed abstract data type carrier, framed data structure and abstraction function. Let  $(X_n)_{n \in \mathbb{N}}$  be a sequence of indeterminates over  $\mathbb{C}$  and let

$$\mathcal{R} := \bigcup_{n \in \mathbb{N}} \mathbb{C}[X_1, \dots, X_n].$$

A *framed (unary) abstract data type carrier of polynomials* is a constructible subset of a finite–dimensional  $\mathbb{C}$ –vector space contained in  $\mathcal{R}$ . In the following we shall only refer to unary abstract data type carriers and omit the expression “unary”. Only at the end of this section we shall briefly mention  $r$ –ary abstract data type carriers for arbitrary  $r \in \mathbb{N}$ .

By *framed data structures* we refer to constructible subsets of suitable affine ambient spaces over  $\mathbb{C}$ . For a framed data structure  $\mathcal{M}$ , the *size* of  $\mathcal{M}$  is the dimension of its ambient space.

Let  $\mathcal{O}$  be a framed abstract data type carrier of polynomials,  $\mathcal{M}$  and  $\mathcal{N}$  framed data structures,  $\mu : \mathcal{M} \rightarrow \mathcal{N}$  a geometrically robust constructible map and  $\omega : \mathcal{N} \rightarrow \mathcal{O}$  a polynomial map such that the geometrically robust constructible map  $\theta := \omega \circ \mu$  sends  $\mathcal{M}$  onto  $\mathcal{O}$ . The situation may be depicted

by the following commutative diagram:

$$\begin{array}{ccc}
 & \mathcal{O} & \\
 \theta \uparrow & \swarrow \omega & \\
 \mathcal{M} & \xrightarrow{\mu} & \mathcal{N}
 \end{array}$$

We call  $\theta$  the *abstraction function* associated with  $\mu$  and  $\omega$ . The maximal size of  $\mathcal{M}$  and  $\mathcal{N}$  is called the *size* of  $\theta$ . Observe that the topological closures of  $\mathcal{O}$  and  $\mathcal{N}$  are well defined with respect to the Zariski and Euclidean topologies and coincide. We denote them by  $\overline{\mathcal{O}}$  and  $\overline{\mathcal{N}}$ . The polynomial map  $\omega$  sends  $\overline{\mathcal{N}}$  into  $\overline{\mathcal{O}}$ .

The idea behind our notion of abstraction function is the following. The specification language we use to speak about  $\mathcal{R}$  consists of constants from  $\mathbb{C}$ , the arithmetic operations addition, subtraction and multiplication, and equality. Thus a framed abstract data type carrier  $\mathcal{O}$  of polynomials can always (not necessarily efficiently) be described by a formula or a division-free arithmetic circuit which depends on a suitable framed data structure  $\mathcal{N}$  of parameters. The coefficient-wise representation of the elements of  $\mathcal{O}$  defines a surjective polynomial map  $\omega : \mathcal{N} \rightarrow \mathcal{O}$ .

In the case of the representation of polynomials by essentially division-free, robust arithmetic circuits described in Section 3.1, the size of  $\theta$  is evidently a lower bound for the DAG size of the circuit  $\beta$ . This example shows that also in the general case the size of  $\theta$  is a reasonable measure for the representation complexity of the elements of  $\mathcal{O}$  by means of  $\theta$ .

We allow now that  $\mathcal{N}$  becomes *re-parameterized* by a geometrically robust constructible map  $\mu$  with domain of definition  $\mathcal{M}$  and with  $\mu(\mathcal{M}) \subset \mathcal{N}$  such that the composite map  $\theta = \omega \circ \mu$  sends  $\mathcal{M}$  onto  $\mathcal{O}$ . In this sense, our notion of abstraction function for framed abstract data type carriers of polynomials is absolutely natural and contains as first class citizens the representation of polynomial families by means of robust arithmetic circuits.

All we have said before (and we shall say in the sequel) about framed *unary* abstract data type carriers may be applied, *mutatis mutandis*, to the case where the ring  $\mathcal{R}$  is replaced by its cartesian product  $\mathcal{R}^r$ , for  $r \in \mathbb{N}$ . If this occurs, we speak about *framed  $r$ -ary abstract data type carriers*.

### 3.3.1 Identification sequences

Let be given two framed abstract data type carriers  $\mathcal{O}_1$  and  $\mathcal{O}_2$ , two framed data structures  $\mathcal{N}_1$  and  $\mathcal{N}_2$  and two surjective polynomial maps  $\omega_1 : \mathcal{N}_1 \rightarrow \mathcal{O}_1$  and  $\omega_2 : \mathcal{N}_2 \rightarrow \mathcal{O}_2$ . Then the number of variables and the degrees of the polynomials occurring in  $\mathcal{O}_1$  and  $\mathcal{O}_2$  are bounded. Therefore we may assume

without loss of generality that the elements of  $\mathcal{O}_1$  and  $\mathcal{O}_2$  are polynomials of  $\mathbb{C}[X_1, \dots, X_n]$  of degree bounded by a fixed integer parameter  $\Delta \geq 2$ . Let  $L$  be the size of the framed data structure  $\mathcal{N}_1 \times \mathcal{N}_2$  and suppose that there exist a quantifier-free first-order formula over  $\mathbb{C}$  which defines  $\mathcal{N}_1 \times \mathcal{N}_2$  involving  $K$  polynomial equations of degree at most  $\Delta$  in  $L$  variables. Taking into account that there are at most  $\Delta^L$  such equations which are linearly-independent over  $\mathbb{C}$ , we may assume without loss of generality  $K \leq \Delta^L$ . Finally we assume that the degree of the polynomials defining  $\omega_1 \times \omega_2 : \mathcal{N}_1 \times \mathcal{N}_2 \rightarrow \mathcal{O}_1 \times \mathcal{O}_2$  is bounded by  $\Delta$ .

For  $m \in \mathbb{N}$ , we call  $(\gamma_1, \dots, \gamma_m) \in (\mathbb{A}^n)^m$  an *identification sequence* for  $\mathcal{O}_1 \times \mathcal{O}_2$  if the equalities  $f(\gamma_1) = g(\gamma_1), \dots, f(\gamma_m) = g(\gamma_m)$  imply  $f = g$  for any  $f \in \overline{\mathcal{O}_1}, g \in \overline{\mathcal{O}_2}$ .

The next statement assures that there exist for  $\mathcal{O}_1 \times \mathcal{O}_2$  many integer identification sequences of small length  $m := 4L + 2$  and of small bit size  $O(L \log \Delta)$  which may be chosen randomly. For the proof of this result, we refer to [CGH<sup>+</sup>03, Lemma 4 and Corollary 1].

**Proposition 8.** *Let notations and assumptions be as before. Let  $M$  be a finite subset of  $\mathbb{A}^1$ . Suppose that the cardinality  $\#M$  of  $M$  satisfies the estimate  $\#M \geq \Delta^3(1 + L)^{\frac{1}{2}}(1 + K\Delta)$  and let be given an integer  $m \geq 4L + 2$ . Then there exist points  $\gamma_1, \dots, \gamma_m$  of  $M^n$  such that  $(\gamma_1, \dots, \gamma_m)$  forms an identification sequence for  $\mathcal{O}_1 \times \mathcal{O}_2$ .*

*Suppose that the points of the finite set  $M^n$  are equidistributed. Then the probability of finding by a random choice in  $(M^n)^m$  an identification sequence is at least  $1 - \frac{1}{\#M} \geq \frac{1}{2}$ .*

Suppose that for any  $(v_1, v_2) \in \overline{\mathcal{N}_1} \times \overline{\mathcal{N}_2}$  and any  $\xi \in \mathbb{A}^n$  we are able to evaluate  $\omega_1(v_1)(\xi)$  and  $\omega_2(v_2)(\xi)$  efficiently, i.e., using a number of arithmetic operations in  $\mathbb{C}$  which is polynomial in  $L$  (this occurs when families of polynomials are represented by robust arithmetic circuits or by neural network architectures as in Sections 3.1 and 3.2). Then we may set up an algebraic computation tree of size polynomial in  $L$  which for any pair  $(v_1, v_2) \in \overline{\mathcal{N}_1} \times \overline{\mathcal{N}_2}$  decides whether  $\omega_1(v_1) = \omega_2(v_2)$  holds.

We are now going to axiomatize this situation as follows. Let  $I$  be an index set and  $\mathcal{H} := \{(\theta_i, \mu_i, \omega_i)\}_{i \in I}$  be a collection of abstraction functions  $\theta_i : \mathcal{M}_i \rightarrow \mathcal{O}_i$  associated with geometrically robust constructible and polynomial maps  $\mu_i : \mathcal{M}_i \rightarrow \mathcal{N}_i$  and  $\omega_i : \mathcal{N}_i \rightarrow \mathcal{O}_i$ , respectively. We call the collection  $\mathcal{H}$  *compatible* if for any  $i, j \in I$  there is given an algebraic computation tree of depth polynomial in the sizes of  $\theta_i$  and  $\theta_j$  which for any pair  $(v_i, v_j) \in \overline{\mathcal{N}_i} \times \overline{\mathcal{N}_j}$  decides whether  $\omega_i(v_i) = \omega_j(v_j)$  holds.

### 3.4 Quiz games

We now exclusively consider framed unary abstract data type carriers. We are going to model mathematically, in the geometric context of this paper, the informal notion of *information hiding* in software engineering. For this purpose we present two games<sup>1</sup>, the first one in an exact and the second one in an approximate setting.

Let be given two abstraction functions  $\theta : \mathcal{M} \rightarrow \mathcal{O}$ ,  $\theta' : \mathcal{M} \rightarrow \mathcal{O}'$  as before, associated with geometrically robust constructible maps  $\mu : \mathcal{M} \rightarrow \mathcal{N}$ ,  $\mu' : \mathcal{M} \rightarrow \mathcal{N}'$ , and polynomial maps  $\omega : \mathcal{N} \rightarrow \mathcal{O}$ ,  $\omega' : \mathcal{N}' \rightarrow \mathcal{O}'$ , namely  $\theta = \omega \circ \mu$  and  $\theta' = \omega' \circ \mu'$ . Suppose that  $(\theta, \mu, \omega)$  and  $(\theta', \mu', \omega')$  belong to a compatible collection  $\mathcal{H}$ . Suppose further that there exists a geometrically robust constructible map  $\tau : \mathcal{O} \rightarrow \mathcal{O}'$  such that  $\tau \circ \theta = \theta'$  holds. The following commutative diagram of geometrically robust constructible maps summarizes this situation:

$$\begin{array}{ccccc}
 & & \mathcal{O} & \xrightarrow{\tau} & \mathcal{O}' \\
 & \nearrow \omega & \uparrow \theta & \nearrow \theta' & \uparrow \omega' \\
 \mathcal{N} & \xleftarrow{\mu} & \mathcal{M} & \xrightarrow{\mu'} & \mathcal{N}'
 \end{array}$$

We shall define two variants of a two-party protocol called the *exact* and the *approximative quiz game*. The agents in these protocols are called quizmaster and player. We suppose that the *quizmaster* has limited and the *player* unlimited computational power and that the quizmaster is honest and able to answer the player's questions. The quizmaster is able to evaluate  $\mu'$  whereas the player can compute all occurring functions.

#### 3.4.1 The protocol of the exact quiz game

The quizmaster chooses  $u \in \mathcal{M}$  and hides it from the player. The player asks the quizmaster's questions about the polynomial  $\theta(u)$  whose answers are tuples of complex numbers which depend only on  $\theta(u)$  but not directly on  $u$ . The quizmaster's answers to the player's questions are represented by a geometrically robust map  $\tilde{\sigma}$  with domain of definition  $\mathcal{O}$ . Thus the arguments of  $\tilde{\sigma}$  belong to the affine ambient space of  $\mathcal{O}$ .

In the aim to avoid the modeling of branchings, all the questions and their answers become realized by a single round. In other words, the game is not cooperative because the player's questions do not depend on previous answers of the quizmaster.

---

<sup>1</sup>We remark we are not using the word "game" in the sense of game theory, but rather in the informal sense of the popular guessing game "I spy".

Let  $\sigma := \tilde{\sigma} \circ \theta$  and  $\mathcal{M}^* := \tilde{\sigma}(\mathcal{O}) = \sigma(\mathcal{M})$ . We suppose now that there is given a framed abstract data type carrier  $\mathcal{O}^*$  and an abstraction function  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$ , associated with a geometrically robust map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , from the compatible collection  $\mathcal{H}$ , such that  $\theta^* = \omega^* \circ \mu^*$ . Moreover, we suppose that the quizmaster is able to evaluate  $\sigma = \tilde{\sigma} \circ \theta$ .

The quizmaster computes  $\sigma(u)$  and sends it to the player who computes now  $v^* := (\mu^* \circ \sigma)(u)$ . The player sends  $v^*$  back to the quizmaster. The quizmaster evaluates  $v' := \mu'(u)$  and checks whether  $\omega^*(v^*) = \omega'(v')$  holds. The maps  $\sigma : \mathcal{M} \rightarrow \mathcal{M}^*$  and  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  constitute the *strategy* of the player. The whole situation becomes depicted by the following commutative diagram of constructible maps:

$$\begin{array}{ccccc}
 & \mathcal{N} & & & \\
 & \uparrow \mu & \searrow \omega & \xrightarrow{\sigma} & \\
 \mathcal{M} & \xrightarrow{\theta} & \mathcal{O} & \xrightarrow{\tilde{\sigma}} & \mathcal{M}^* \\
 & \downarrow \mu' & \searrow \theta' & \downarrow \tau & \downarrow \mu^* \\
 \mathcal{N}' & \xrightarrow{\omega'} & \mathcal{O}' & \subset \mathcal{R} \supset \mathcal{O}^* & \xleftarrow{\omega^*} \mathcal{N}^*
 \end{array}$$

The player wins the instance of the game given by  $u$  if the condition  $\omega^*(v^*) = \omega'(v')$  is satisfied. We say that the player has a *winning strategy* if he wins the game for any  $u \in \mathcal{M}$ .

We say that the computational task determined by  $\theta$  and  $\theta'$  is *feasible* if the size of  $\theta'$  is polynomial in the size of  $\theta$ . A winning strategy is called *efficient* if the size of  $\theta^*$  is polynomial in the size of  $\theta$  (and therefore polynomial in the size of  $\theta'$  for a feasible computational task). Otherwise it is called *inefficient*. Observe that  $\sigma$  and  $\theta^* = \omega^* \circ \mu^*$  define a winning strategy for the exact game protocol if and only if  $\theta' = \omega^* \circ \mu^* \circ \tilde{\sigma} \circ \theta = \omega^* \circ \mu^* \circ \sigma = \theta^* \circ \sigma$  holds. In this case we have  $\mathcal{O}' = \mathcal{O}^*$ . The idea behind this computational model is to restrict the information which quizmaster and player may interchange. It is supposed that  $\sigma(u)$  and  $v^*$  are complex vectors of short length, whereas explicit descriptions of the framed abstract data type carriers  $\mathcal{O}$ ,  $\mathcal{O}'$  and  $\mathcal{O}^*$  may become huge.

### 3.4.2 The protocol of the approximative quiz game

Now we introduce the protocol of the approximative quiz game. In Appendix B below we show that this protocol captures the notions of approximative algorithms and approximative complexity of algebraic complexity theory (see, e.g., [BCS97, Chapter 15]).

As the game follows almost the same rules as in the exact case, we shall therefore only stick on the differences. The quizmaster's answers to the player's questions are now represented by a geometrically robust constructible map  $\sigma$  with domain of definition  $\mathcal{M}$ . We do not anymore assume that  $\sigma$  is a composition of  $\theta$  with another map.

We suppose that the quizmaster is able to evaluate  $\sigma$ . As before let  $\mathcal{M}^* := \sigma(\mathcal{M})$  and assume that there is given a framed abstract data type carrier  $\mathcal{O}^*$  and an abstraction function  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$ , associated with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , from the compatible collection  $\mathcal{H}$ , such that  $\theta^* = \omega^* \circ \mu^*$ . The situation is depicted now in the following commutative diagram:

$$\begin{array}{ccccc}
 & & \mathcal{N} & & \\
 & & \uparrow & \searrow \omega & \\
 & & \mathcal{M} & \xrightarrow{\theta} & \mathcal{O} & \xrightarrow{\sigma} & \mathcal{M}^* \\
 & & \downarrow \mu' & \searrow \theta' & \downarrow \tau & & \downarrow \mu^* \\
 \mathcal{N}' & \xrightarrow{\omega'} & \mathcal{O}' & \subset \mathcal{R} \supset & \mathcal{O}^* & \xleftarrow{\omega^*} & \mathcal{N}^*
 \end{array}$$

We suppose that the following condition is satisfied:

*For any (not necessarily convergent) sequence  $(u_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  and  $u \in \mathcal{M}$  such that  $(\theta(u_k))_{k \in \mathbb{N}}$  converges to  $\theta(u)$  in the Euclidean topology, the sequence  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$  is bounded.*

We remark that this condition is satisfied if and only if the map  $\mu^* \circ \sigma : \mathcal{M} \rightarrow \mathcal{N}^*$  is locally bounded with respect to the Euclidean metric of  $\mathcal{N}^*$  and the topology of  $\mathcal{M}$  induced from the Euclidean topology of  $\mathcal{O}$  by  $\theta : \mathcal{M} \rightarrow \mathcal{O}$ . As we shall see in Proposition 10 below, this implies that for any  $u \in \mathcal{M}$  the value  $(\mu^* \circ \sigma)(u)$  strongly depends on  $\theta(u)$ , although it may be not uniquely determined by  $\theta(u)$ .

The quizmaster chooses now a sequence  $(u_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  and an element  $u \in \mathcal{M}$  such that  $(\theta(u_k))_{k \in \mathbb{N}}$  converges to  $\theta(u)$ , and hides these data from the player. The quizmaster's answers to the player's questions encode the sequence  $(\sigma(u_k))_{k \in \mathbb{N}}$ , which is not necessarily convergent. From these answers the player infers the sequence  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$ , which is bounded. The player wins the approximative game if there is an accumulation point  $v^*$  of  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$  in the Euclidean topology with  $\omega^*(v^*) = \theta'(u)$ . The quizmaster verifies this by computing  $v' := \mu'(u)$  and checking whether  $\omega^*(v^*) = \omega'(v')$  holds.

Recall that the computational task determined by  $\theta$  and  $\theta'$  is called *feasible* if the size of  $\theta'$  is polynomial in the size of  $\theta$ . Again we say that the

maps  $\sigma : \mathcal{M} \rightarrow \mathcal{M}^*$  and  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  constitute the *strategy* of the player, that the player has a *winning strategy* if he wins for any  $u \in \mathcal{M}$ , and we call this winning strategy *efficient* if the size of  $\theta^*$  is polynomial in the size of  $\theta$  (and then polynomial in the size of  $\theta'$  for a feasible computational task). Otherwise, the strategy is called *inefficient*.

**Lemma 9.** *Suppose that  $\sigma$  and  $\theta^* = \omega^* \circ \mu^*$  define a winning strategy for the approximative quiz game protocol. Then we have  $\theta' = \omega^* \circ \mu^* \circ \sigma = \theta^* \circ \sigma$  and therefore  $\mathcal{O}' = \mathcal{O}^*$ .*

*Proof.* Let  $u$  be an arbitrary point of  $\mathcal{M}$  and consider the approximative game given by the sequence  $(u_k)_{k \in \mathbb{N}}$  defined by  $u_k := u$ , and  $u$ . Obviously  $v^* := (\mu^* \circ \sigma)(u)$  is the unique accumulation point of the sequence  $(\mu^* \circ \sigma(u_k))_{k \in \mathbb{N}}$ . Since  $\sigma$  and  $\theta^* = \omega^* \circ \mu^*$  define a winning strategy, we conclude  $\theta'(u) = \omega^*(v^*) = \omega^*((\mu^* \circ \sigma)(u)) = (\omega^* \circ \mu^* \circ \sigma)(u)$ . This implies the identities  $\theta' = \omega^* \circ \mu^* \circ \sigma$  and  $\mathcal{O}' = \mathcal{O}^*$ .  $\square$

We observe that a protocol of the exact quiz game gives always rise to a protocol of the approximative quiz game. To this end, let notations be as in our description of the exact model and let be given a sequence  $(u_k)_{k \in \mathbb{N}}$  of elements of  $\mathcal{M}$  and  $u \in \mathcal{M}$  such that  $(\theta(u_k))_{k \in \mathbb{N}}$  converges to  $\theta(u)$ . From the continuity of  $\tilde{\sigma}$  we deduce that the sequence  $(\sigma(u_k))_{k \in \mathbb{N}} = ((\tilde{\sigma} \circ \theta)(u_k))_{k \in \mathbb{N}}$  converges to  $\sigma(u) = (\tilde{\sigma} \circ \theta)(u)$ . The continuity of  $\mu^*$  implies now that  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$  converges to  $(\mu^* \circ \sigma)(u)$ . Therefore the sequence  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$  is bounded and has a single accumulation point, namely  $v^* = (\mu^* \circ \sigma)(u)$ . In particular, the player wins the exact game given by  $u \in \mathcal{M}$  if and only if he wins the approximative quiz game given by the sequence  $(u_k)_{k \in \mathbb{N}}$  defined by  $u_k := u$ , and  $u \in \mathcal{M}$ .

**Proposition 10.** *Let assumptions and notations be that of the approximative quiz game and let  $u \in \mathcal{M}$ . Suppose that the player has a winning strategy. Then there exists a finite subset  $\mathcal{S}_u$  of the ambient space of  $\mathcal{N}^*$  with the following property: for any sequence  $(u_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  with  $(\theta(u_k))_{k \in \mathbb{N}}$  converging to  $\theta(u)$ , all the accumulation points of  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$  belong to  $\mathcal{S}_u$ .*

*Proof.* Let

$$\begin{aligned} \mathcal{D}^+ &:= \{(\theta(u), (\mu^* \circ \sigma)(u)) : u \in \mathcal{M}\} \subset \mathcal{O} \times \mathcal{N}^*, \\ \mathcal{O}^+ &:= \{(\theta(u), \theta'(u)) : u \in \mathcal{M}\} \subset \mathcal{O} \times \mathcal{O}', \end{aligned}$$

and notice that  $\mathcal{D}^+$  and  $\mathcal{O}^+$  are constructible in their respective ambient spaces. Let  $\omega^+ : \mathcal{D}^+ \rightarrow \mathcal{O}^+$  be the polynomial map  $\omega^+ := (\text{id}, \omega^*)$ , namely

$$\omega^+(\theta(u), (\mu^* \circ \sigma)(u)) := (\theta(u), (\omega^* \circ \mu^* \circ \sigma)(u)) = (\theta(u), (\theta^* \circ \sigma)(u)).$$

By Lemma 9, the assumption that the player has a winning strategy implies that  $(\theta^* \circ \sigma)(u) = \theta'(u)$  holds for any  $u \in \mathcal{M}$ . Hence  $\omega^+$  is surjective.

We show that the surjective polynomial map  $\omega^+$  satisfies the condition of Lemma 24 in Appendix A. To this end, consider a sequence  $(u_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  and an element  $u \in \mathcal{M}$  such that  $((\theta(u_k), \theta'(u_k)))_{k \in \mathbb{N}}$  converges to  $(\theta(u), \theta'(u))$ . Then  $(\theta(u_k))_{k \in \mathbb{N}}$  converges to  $\theta(u)$ , which implies that  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$ , and therefore  $(\theta(u_k), (\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$ , are bounded.

Let  $u \in \mathcal{M}$  and let  $(u_k)_{k \in \mathbb{N}}$  be an arbitrary sequence in  $\mathcal{M}$  such that  $(\theta(u_k))_{k \in \mathbb{N}}$  converges to  $\theta(u)$ . Observe that  $\omega^+$  induces a  $\mathbb{C}$ -algebra extension  $\mathbb{C}[\overline{\mathcal{O}^+}] \hookrightarrow \mathbb{C}[\overline{\mathcal{D}^+}]$ . Let  $\mathfrak{m}$  be the maximal ideal of definition of the point  $(\theta(u), \theta'(u))$  of the affine variety  $\overline{\mathcal{O}^+}$ . From Lemma 24 we deduce that the  $\mathbb{C}[\overline{\mathcal{O}^+}]_{\mathfrak{m}}$ -module  $\mathbb{C}[\overline{\mathcal{D}^+}]_{\mathfrak{m}}$  is finite. Hence the  $\mathbb{C}$ -algebra extension  $\mathbb{C}[\overline{\mathcal{O}^+}]_{\mathfrak{m}} \hookrightarrow \mathbb{C}[\overline{\mathcal{D}^+}]_{\mathfrak{m}}$  is integral.

Let  $\lambda$  be the coordinate function of  $\overline{\mathcal{D}^+}$  corresponding to an arbitrary entry of  $\mu^* \circ \sigma$ . Then there exists  $s \in \mathbb{N}$  and elements  $a_0, a_1, \dots, a_s$  of  $\mathbb{C}[\overline{\mathcal{O}^+}]$  with  $a_0 \notin \mathfrak{m}$  such that the algebraic dependence relation  $a_0 \lambda^s + a_1 \lambda^{s-1} + \dots + a_s = 0$  is satisfied in  $\mathbb{C}[\overline{\mathcal{D}^+}]$ . This implies

$$\sum_{j=0}^s a_j (\theta(u_k), \theta'(u_k)) \lambda^{s-j} (\theta(u_k), (\mu^* \circ \sigma)(u_k)) = 0 \quad (1)$$

for any  $k \in \mathbb{N}$ . On the other hand, as  $a_0 \notin \mathfrak{m}$ , we deduce that  $a_0 (\theta(u), \theta'(u)) \neq 0$  holds. Let  $v^*$  be an accumulation point of the sequence  $((\mu^* \circ \sigma)(u_k))_{k \in \mathbb{N}}$ . From (1) we conclude that

$$\sum_{j=0}^s a_j (\theta(u), \theta'(u)) \lambda^{s-j} (\theta(u), v^*) = 0.$$

Since  $a_0 (\theta(u), \theta'(u)) \neq 0$ , only finitely many values of  $\lambda(\theta(u), v^*)$  satisfy this equation, independently of the sequence  $(u_k)_{k \in \mathbb{N}}$ . Since  $\lambda$  was the coordinate function of  $\overline{\mathcal{D}^+}$  corresponding to an arbitrary entry of  $\mu^* \circ \sigma$ , the conclusion of Proposition 10 follows.  $\square$

**Corollary 11.** *Let assumptions and notations be that of the approximative quiz game. Suppose that the player has a winning strategy. Then for any  $u \in \mathcal{M}$ , the set*

$$\{\mu^* \circ \sigma(v) : v \in \mathcal{M}, \theta(v) = \theta(u)\}$$

*is finite.*

*Proof.* Let  $v \in \mathcal{M}$  with  $\theta(v) = \theta(u)$  and let  $(v_k)_{k \in \mathbb{N}}$  be the sequence defined by  $v_k := v$  for any  $k \in \mathbb{N}$ . Then  $(\theta(v_k))_{k \in \mathbb{N}}$  converges to  $\theta(v)$  and  $(\mu^* \circ \sigma)(v)$  is an accumulation point of  $((\mu^* \circ \sigma)(v_k))_{k \in \mathbb{N}}$ . The assertion follows now from Proposition 10.  $\square$



### 3.4.3 Abstract datatype carriers, classes and routines

The content of this subsection is aimed to clarify our conceptual system from the point of view of software engineering and will not be used in the sequel. Our terminology is borrowed from [Mey97].

A subset of  $\mathcal{R}$  which can be countably covered by framed unary data type carriers is called a *unary abstract data type carrier*. A unary abstract data type carrier together with any such covering is called a *unary class*. Mutatis mutandis we may define the notions of *r-ary abstract data type carrier* and *r-ary class* for any  $r \in \mathbb{N}$  replacing in the above description  $\mathcal{R}$  by its cartesian product  $\mathcal{R}^r$ .

Let  $\mathcal{U}_1$  and  $\mathcal{U}_2$  be unary abstract data type carriers. An *abstract function* between  $\mathcal{U}_1$  and  $\mathcal{U}_2$  is a map  $\tau : \mathcal{U}_1 \rightarrow \mathcal{U}_2$  with the following properties. For each framed data structure  $\mathcal{M}_1$  and framed unary abstract data type carrier  $\mathcal{O}_1$  together with an abstraction function  $\theta_1 : \mathcal{M}_1 \rightarrow \mathcal{O}_1$ , such that  $\mathcal{O}_1$  is contained in  $\mathcal{U}_1$ , there exists a framed data structure  $\mathcal{M}_2$  and a framed unary abstract data type carrier  $\mathcal{O}_2$  together with an abstraction function  $\theta_2 : \mathcal{M}_2 \rightarrow \mathcal{O}_2$ , such that  $\tau(\mathcal{O}_1) \subset \mathcal{O}_2 \subset \mathcal{U}_2$  holds and there exists a geometrically robust constructible map, called a *routine*,  $\sigma : \mathcal{M}_1 \rightarrow \mathcal{M}_2$  with  $\tau \circ \theta_1 = \theta_2 \circ \sigma$ . Observe that quiz games with winning strategies instantiate these properties.

For any  $r_1, r_2 \in \mathbb{N}$ , this notion of abstract function between given  $r_1$  and  $r_2$ -ary abstract data type carriers may be generalized if we replace the ring  $\mathcal{R}$  by its cartesian products  $\mathcal{R}^{r_1}$  and  $\mathcal{R}^{r_2}$ , respectively. We speak then about an *abstract function with  $r_1$  inputs and  $r_2$  outputs*. This concept of abstract function is not exactly that of [Mey97], but comes close to it.

### 3.4.4 Quiz games and information hiding in software engineering

Let assumptions and notations be as before. Suppose that there is a programmer whose task is, in an object oriented manner, to implement the geometrically robust constructible map  $\tau : \mathcal{O} \rightarrow \mathcal{O}'$  between the framed abstract data type carriers  $\mathcal{O}$  and  $\mathcal{O}'$  which are represented by the abstraction functions  $\theta$  and  $\theta'$ .

His program uses observers and constructors. Information hiding means that the objects from  $\mathcal{M}$  which represent elements of  $\mathcal{O}$  and  $\mathcal{O}'$  are not accessible to him. He is only allowed to ask questions about these elements which involve complex values that he then processes. This situation becomes modeled by the exact quiz game with the programmer in the rôle of the player and the observers in the rôle of the quizmaster.

More subtle is the situation in the case of the approximative quiz game. Here we allow the programmer to access to a limited extent information

about the objects which represent the elements of  $\mathcal{O}$  and  $\mathcal{O}'$ . This information is of approximative nature and becomes provided by the observers. The programmer/player must then be able, by means of constructors, to compute a representation of the output. From Proposition 10 we deduce that the situation modeled by the approximative quiz game is not substantially different from that modeled by the exact one. For each input element of  $\mathcal{O}$  there exist only finitely many possible representations of the corresponding output element of  $\mathcal{O}'$  which can be computed by the programmer/player.

## 4 Selected complexity lower bounds

We are now going to use the computational model developed in Sections 3.4.1 and 3.4.2 to derive complexity lower bounds for selected computational problems.

From the seven series of examples we are going to consider in this section only three are really new. The other ones can be found in another context in [CGH<sup>+</sup>03], [GHMS11], [HKR13b] and [HKR13a]. What is new is our unified approach to them and the resulting generality of our complexity results.

### 4.1 Polynomial Interpolation

In this section we are going to consider four types of approximative quiz game protocols which generalize the intuitive meaning of interpolation of families of multivariate and univariate polynomials.

#### 4.1.1 Multivariate polynomial interpolation

Let be given a framed abstract data type carrier  $\mathcal{O}$ , framed data structures  $\mathcal{M}$  and  $\mathcal{N}$ , an abstraction function  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  associated with a geometrically robust constructible map  $\mu : \mathcal{M} \rightarrow \mathcal{N}$  and a polynomial map  $\omega : \mathcal{N} \rightarrow \mathcal{O}$ , and suppose that  $(\theta, \mu, \omega)$  belongs to a given compatible collection  $\mathcal{H}$ .

Let  $\mathcal{O}' := \mathcal{O}$ ,  $\tau := \text{id}_{\mathcal{O}}$ ,  $\theta' := \theta$ ,  $\mu' := \mu$ ,  $\omega' := \omega$  and let be given an approximative quiz game protocol with winning strategy for this situation. Then the player returns for a given parameter instance  $u \in \mathcal{M}$ , a point  $v^*$  of a suitable affine space such that  $v^*$  encodes  $\theta(u)$ . In other words, the player replaces the “hidden” encoding  $u$  of  $\theta(u)$  by a new encoding  $v^*$  which he computes from the quizmaster’s answers to his questions.

In the exact version of the quiz game the player is limited to ask questions about the polynomial  $\theta(u)$  itself and computes from the quizmaster’s answers his new encoding of  $\theta(u)$ . If the player’s questions refer only to values of the

polynomial  $\theta(u)$  at given inputs, the player solves an interpolation problem for  $\theta(u)$ . Below we are going to make more precise this aspect.

**Interpolation of a family easy to evaluate.** Let us now analyze the following concrete example of this general setting. Let  $l, n \in \mathbb{N}$  be discrete parameters with  $2^{\frac{l}{2}} \geq n$  and let  $\mathcal{M} := \mathbb{A}^{n+1}$ . For  $t \in \mathbb{A}^1$  and  $u = (u_1, \dots, u_n) \in \mathbb{A}^n$ , let  $\theta(t, u)$  be the polynomial

$$\theta(t, u) := t \sum_{k=0}^{2^l-1} (u_1 X_1 + \dots + u_n X_n)^k,$$

and let  $\mathcal{O} := \text{im } \theta$ . Observe that the family of polynomials  $\theta$  is evaluable by a robust arithmetic circuit of size  $2n + 3l - 1$  and that, for any  $t \in \mathbb{A}^1$  and any  $u \in \mathbb{A}^n$ , the polynomial  $\theta(t, u)$  can be computed using  $2l - 2$  essential multiplications. Thus there exists an injective affine linear map  $\mu : \mathcal{M} \rightarrow \mathbb{A}^{2n+3l-1}$  with constructible image  $\mathcal{N} := \mu(\mathcal{M})$  and a polynomial map  $\omega : \mathcal{N} \rightarrow \mathcal{O}$  such that  $\theta = \omega \circ \mu$  holds. Hence  $\mathcal{O}$  is a framed abstract data type carrier and  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  is an abstraction function of size  $2n + 3l - 1$  associated with  $\mu$  and  $\omega$ . From Proposition 8, and the comment that follows it, we deduce that  $(\theta, \mu, \omega)$  belongs to a suitable collection  $\mathcal{H}$  of abstraction functions.

Suppose that for the previously considered computation task given by  $\theta$  and  $\text{id}_{\mathcal{O}}$  there is given a protocol with winning strategy for the approximative quiz game. Thus we have a framed abstract data type carrier  $\mathcal{O}^*$ , framed data structures  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , an abstraction function  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$  of the compatible collection  $\mathcal{H}$ , associated with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , and a surjective geometrically robust constructible map  $\sigma : \mathcal{M} \rightarrow \mathcal{M}^*$  such that by Lemma 9 the identities  $\theta = \omega^* \circ \mu^* \circ \sigma = \theta^* \circ \sigma$  and  $\mathcal{O} = \mathcal{O}^*$  hold. We summarize the whole situation by the following commutative diagram of geometrically robust constructible maps:

$$\begin{array}{ccccc} & & \mathcal{O} & = & \mathcal{O}^* \\ & \nearrow \omega & \uparrow \theta & & \uparrow \theta^* \\ \mathcal{N} & \xleftarrow{\mu} & \mathcal{M} & \xrightarrow{\sigma} & \mathcal{M}^* & \xrightarrow{\mu^*} & \mathcal{N}^* \\ & & & & & \nwarrow \omega^* & \end{array}$$

With these notations and assumptions, we have the following statement.

**Lemma 12.** *The size of  $\theta^*$  is of order  $2^{\Omega(ln)}$ .*

*Proof.* Following [GHMS11, Section 5.2], one verifies easily for any  $t \in \mathbb{A}^1$  and  $u = (u_1, \dots, u_n) \in \mathbb{A}^n$  the following identities:

$$\begin{aligned} \theta(t, u) &= t \sum_{k=0}^{2^l-1} \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \\ \alpha_1 + \dots + \alpha_n = k}} \frac{k!}{\alpha_1! \dots \alpha_n!} u_1^{\alpha_1} \dots u_n^{\alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n} \\ &= t \sum_{k=0}^{2^l-1} \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \\ \alpha_1 + \dots + \alpha_n < 2^l}} \frac{(\alpha_1 + \dots + \alpha_n)!}{\alpha_1! \dots \alpha_n!} u_1^{\alpha_1} \dots u_n^{\alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}. \end{aligned}$$

For  $(\rho, t) \in \mathbb{A}^2$ , let  $\beta_\rho(t) := (t, \rho, \rho^{2^l}, \dots, \rho^{2^{(n-1)l}})$ . Then, for fixed  $\rho \in \mathbb{A}^1$ , the map which assigns to each  $t \in \mathbb{A}^1$  the value  $(\theta \circ \beta_\rho)(t)$  is represented by the polynomial

$$(\theta \circ \beta_\rho)(t) = t \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \\ \alpha_1 + \dots + \alpha_n < 2^l}} \frac{(\alpha_1 + \dots + \alpha_n)!}{\alpha_1! \dots \alpha_n!} \rho^{\alpha_1 + \alpha_2 2^l + \dots + \alpha_n 2^{(n-1)l}} X_1^{\alpha_1} \dots X_n^{\alpha_n},$$

and is therefore linear in  $t$ .

Observe that the set  $M_l := \{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n : \alpha_1 + \dots + \alpha_n < 2^l\}$  has  $K := \binom{2^l-1+n}{n}$  elements. Moreover, each element  $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$  of this set can be identified with its  $2^l$ -ary representation  $\alpha_1 + \alpha_2 2^l + \dots + \alpha_n 2^{(n-1)l}$ . From [GHMS11, Lemma 24] we deduce that there exists a non-empty Zariski open subset  $\mathcal{U}$  of  $\mathbb{A}^K$  such that for any point  $(\rho_1, \dots, \rho_K) \in \mathcal{U}$ , the  $(K \times K)$ -matrix

$$\mathbf{M}_{\rho_1, \dots, \rho_K} := \left( \frac{(\alpha_1 + \dots + \alpha_n)!}{\alpha_1! \dots \alpha_n!} \rho_s^{\alpha_1 + \alpha_2 2^l + \dots + \alpha_n 2^{(n-1)l}} \right)_{\substack{\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in M_l, \\ 1 \leq s \leq K}}$$

is nonsingular. Hence, for  $(\rho_1, \dots, \rho_K) \in \mathcal{U}$ , the vectors  $\frac{d}{dt}(\theta \circ \beta_{\rho_1})(0), \dots, \frac{d}{dt}(\theta \circ \beta_{\rho_K})(0)$  are  $\mathbb{C}$ -linearly independent.

The map which assigns to each  $(\rho, t) \in \mathbb{A}^2$  the value  $(\mu^* \circ \sigma \circ \beta_\rho)(t)$  is geometrically robust and constructible and hence polynomial by Theorem 6(iii). Since any  $u \in \mathbb{A}^n$  satisfies the condition  $\theta(0, u) = 0$  we conclude from Corollary 11 that the set  $\{(\mu^* \circ \sigma)(0, u) : u \in \mathbb{A}^n\}$  is finite. Therefore the set  $\{(\mu^* \circ \sigma \circ \beta_\rho)(0) : \rho \in \mathbb{A}^1\}$  is also finite. Hence there exists a cofinite subset  $\Gamma$  of  $\mathbb{C}$  such that for any point  $\rho \in \Gamma$ , the value  $(\mu^* \circ \sigma \circ \beta_\rho)(0)$  is the same, say  $v$ .

On the other hand,  $\mathcal{U} \cap \Gamma^K$  is a nonempty Zariski open subset of  $\mathbb{A}^n$ , because  $\Gamma$  is cofinite. Therefore there exist elements  $\rho_1, \dots, \rho_K \in \Gamma$  such

that the vectors  $\frac{d}{dt}(\theta \circ \beta_{\rho_1})(0), \dots, \frac{d}{dt}(\theta \circ \beta_{\rho_K})(0)$  are  $\mathbb{C}$ -linearly independent. For  $1 \leq j \leq K$ , the map  $t \mapsto (\mu^* \circ \sigma \circ \beta_{\rho_j})(t)$  is polynomial and hence holomorphic. The assumption that the player has a winning strategy for the given approximative quiz game implies

$$(\theta \circ \beta_{\rho_j})(t) = (\omega^* \circ \mu^* \circ \sigma \circ \beta_{\rho_j})(t)$$

for any  $t \in \mathbb{A}^1$ . We may now apply the chain rule to this situation to conclude

$$\begin{aligned} \frac{d}{dt}(\theta \circ \beta_{\rho_j})(0) &= (d\omega^*)((\mu^* \circ \sigma \circ \beta_{\rho_j})(0)) \cdot \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_j})(0) \\ &= (d\omega^*)(v) \cdot \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_j})(0), \end{aligned}$$

where  $d\omega^*$  denotes the total differential of the polynomial map  $\omega^*$ . Since  $\frac{d}{dt}(\theta \circ \beta_{\rho_1})(0), \dots, \frac{d}{dt}(\theta \circ \beta_{\rho_K})(0)$  are  $\mathbb{C}$ -linearly independent, we infer that the vectors  $\frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_1})(0), \dots, \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_K})(0)$  must generate a  $\mathbb{C}$ -linear space of dimension  $K$ . This and the assumption  $2^{\frac{l}{2}} \geq n$  imply now that the size of  $\mathcal{N}^*$ , and hence the size of  $\theta^*$ , is at least  $K = \binom{2^l - 1 + n}{n} = 2^{\Omega(ln)}$ .  $\square$

In conclusion, the winning strategy of the approximative quiz game under consideration is necessarily inefficient. We formulate now this conclusion in a more general setting.

**Theorem 13.** *Let  $L, n \in \mathbb{N}$  with  $2^{\frac{L}{4}} \geq n$  and let  $\mathcal{O}_{L,n}$  be the abstract data type of all polynomials of  $\mathbb{C}[X_1, \dots, X_n]$  which can be evaluated using at most  $L$  essential multiplications (see Section 3.1). We think the abstraction function of  $\mathcal{O}_{L,n}$  represented by the corresponding generic computation and consider the task of replacing the given hidden encoding of the elements of  $\mathcal{O}_{L,n}$  by a known one using an approximative quiz game with winning strategy. Then any such quiz game is inefficient requiring an abstraction function of size  $2^{\Omega(Ln)}$ .*

*Proof.* Let  $l := \lfloor \frac{L}{2} + 1 \rfloor$  and observe that for any  $t \in \mathbb{A}^1$  and  $u \in \mathbb{A}^n$  the polynomial  $\theta(t, u)$  belongs to  $\mathcal{O}_{L,n}$ . Then the above statement follows immediately from Theorem 6(i) and Lemma 12.  $\square$

The restriction of Theorem 13 to exact quiz games with winning strategy may be paraphrased in terms of learning theory as follows.

**Corollary 14.** *For  $L, n \in \mathbb{N}$  with  $2^{\frac{L}{4}} \geq n$ , the concept class  $\mathcal{O}_{L,n}$  has a representation of size  $(L + n + 1)^2$  by means of the corresponding generic computation, but its concepts require an amount of  $2^{\Omega(Ln)}$  arithmetic operations to be learned continuously.*

**Interpolation from an identification sequence.** We are now going to explain how the computational task of interpolating for  $L, n \in \mathbb{N}$  the family of polynomials  $\mathcal{O}_{L,n}$  *continuously* may be interpreted as a particular instance of an exact quiz game protocol. From Proposition 8 we deduce that there exist for  $\mathcal{O}_{L,n} \times \mathcal{O}_{L,n}$  (many) integer identification sequences of length  $m := 4(L+n+1)^2 + 2$  and bit size at most  $3L+1$ . Let us fix for the moment such an identification sequence  $\gamma = (\gamma_1, \dots, \gamma_m) \in (\mathbb{Z}^n)^m$  and let  $\tilde{\sigma} : \mathcal{O}_{L,n} \rightarrow \mathbb{A}^m$  be the map  $\tilde{\sigma}(f) := (f(\gamma_1), \dots, f(\gamma_m))$ . Then  $\tilde{\sigma}$  is a polynomial map with constructible image  $\mathcal{M}^* := \tilde{\sigma}(\mathcal{O}_{L,n})$  and  $\tilde{\sigma} : \mathcal{O}_{L,n} \rightarrow \mathcal{M}^*$  is bijective. Let  $\mathcal{N}^*$  be the constructible subset of  $\mathbb{A}^{\binom{2L+n}{n}}$  formed by the coefficient vectors of the elements of  $\mathcal{O}_{L,n}$  and let  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}_{L,n}$  be the map which assigns to each element of  $\mathcal{N}^*$  the corresponding polynomial of  $\mathbb{C}[X_1, \dots, X_n]$ . Then  $\omega^*$  is a polynomial map and  $\mathcal{M}^*$  and  $\mathcal{N}^*$  form framed data structures. According to [CGH<sup>+</sup>03, Corollary 3], there is a unique rational, everywhere defined, constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$ , which is continuous with respect to the Euclidean topologies of  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , whose composition  $\omega^* \circ \mu^*$  with  $\omega^*$  is the inverse map of  $\tilde{\sigma} : \mathcal{O}_{L,n} \rightarrow \mathcal{M}^*$ .

From Theorem 7 we deduce that  $\mu^*$  is geometrically robust. Let us consider the framed abstract data type carriers  $\mathcal{O} := \mathcal{O}_{L,n}$  and  $\mathcal{O}^* := \mathcal{O}_{L,n}$ , the framed data structures  $\mathcal{M} := \mathbb{A}^{(L+n+1)^2}$ ,  $\mathcal{M}^* := \tilde{\sigma}(\mathcal{O}_{L,n})$  and  $\mathcal{N}^*$ , the polynomial map  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  given by the generic computation corresponding to  $\mathcal{O}_{L,n}$ , the polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$  and the geometrically robust constructible maps  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$ ,  $\theta^* := \omega^* \circ \mu^*$ ,  $\tilde{\sigma} : \mathcal{O} \rightarrow \mathcal{M}^*$  and  $\sigma := \tilde{\sigma} \circ \theta$ . They form the following commutative diagram of geometrically robust constructible maps:

$$\begin{array}{ccccc}
 \mathcal{O} & = & \mathcal{O}^* & & \\
 \theta \uparrow & \searrow \tilde{\sigma} & \uparrow \theta^* & \swarrow \omega^* & \\
 \mathcal{M} & \xrightarrow{\sigma} & \mathcal{M}^* & \xrightarrow{\mu^*} & \mathcal{N}^*
 \end{array}$$

This diagram represents an exact quiz game protocol with winning strategy for the situation considered at the beginning of this section.

On the other hand, the geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  assigns to each element  $\tilde{\sigma}(f) = (f(\gamma_1), \dots, f(\gamma_m))$  of  $\mathcal{M}^*$  the coefficient vector  $\mu^*(\tilde{\sigma}(f))$  of the polynomial  $f$ , and therefore interpolates  $f$  at the points  $\gamma_1, \dots, \gamma_m \in \mathbb{Z}^n$ . Since  $\mu^*$  is continuous with respect to the Euclidean topologies of  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , it solves the corresponding interpolation task continuously. This solution is also effective because  $\mu^*$  is constructible.

Given any identification sequence  $\gamma = (\gamma_1, \dots, \gamma_m)$  for  $\mathcal{O}_{L,n} \times \mathcal{O}_{L,n}$ , any continuous solution of the task to interpolate the elements of  $\mathcal{O}_{L,n}$  in the points  $\gamma_1, \dots, \gamma_m$  may be depicted as in the commutative diagram above

with  $\mu^*$  and  $\omega^*$  representing a robust arithmetic circuit. Theorem 13 implies now that such a solution requires necessarily the use of  $2^{\Omega(Ln)}$  arithmetic operations. This is the content of [GHMS11, Theorem 23].

#### 4.1.2 Univariate polynomial interpolation

We are now going to analyze the three series of examples which generalize univariate polynomial interpolation. To this end, let us fix a discrete parameter  $D \in \mathbb{N}$ . Let  $l := 6\lceil \log D - 1 \rceil + 1$ ,  $\mathcal{M} := \mathbb{A}^1$  and  $X$  be an indeterminate. For  $t \in \mathcal{M}$ , let

$$\theta_D(t) := (t^{D+1} - 1) \sum_{0 \leq k \leq D} t^k X^k.$$

We put  $\mathcal{O}_D := \text{im } \theta_D$ . Observe that the family of polynomials  $\theta_D$  is evaluable by a robust arithmetic circuit of size  $l$ . Thus there exists an injective affine map  $\mu_D : \mathcal{M} \rightarrow \mathbb{A}^l$  with constructible image  $\mathcal{N}_D := \mu_D(\mathcal{M})$  and a polynomial map  $\omega_D : \mathcal{N}_D \rightarrow \mathcal{O}_D$  such that  $\theta_D = \omega_D \circ \mu_D$  holds. Hence  $\mathcal{O}_D$  is a framed abstract data type carrier and  $\theta_D : \mathcal{M} \rightarrow \mathcal{O}_D$  is an abstraction function of size  $l$  associated with  $\mu_D$  and  $\omega_D$ . From Proposition 8, and the comment that follows it, we deduce that  $(\theta_D, \mu_D, \omega_D)$  belongs to a suitable collection  $\mathcal{H}$  of abstraction functions.

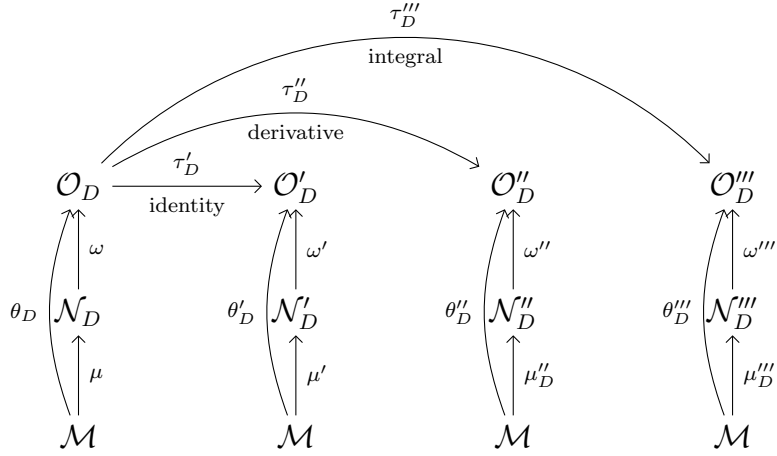
For any  $t \in \mathcal{M}$ , let  $\theta'_D(t) := \theta_D(t)$ ,  $\theta''_D(t)$  the derivative of  $\theta_D(t)$  with respect of the variable  $X$ , and  $\theta'''_D(t)$  the indefinite integral with respect to  $X$ , namely

$$\theta''_D(t) := (t^{D+1} - 1) \sum_{1 \leq k \leq D} kt^k X^{k-1}, \quad \theta'''_D(t) := (t^{D+1} - 1) \sum_{0 \leq k \leq D} \frac{t^k}{k+1} X^{k+1}.$$

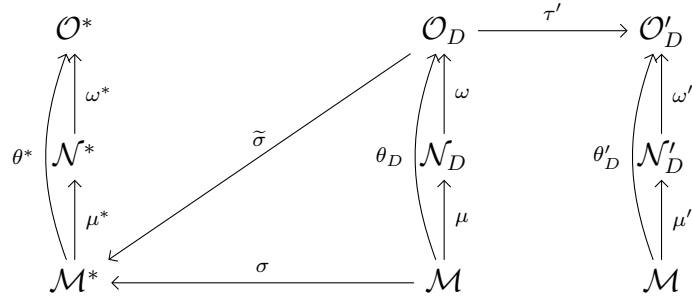
Let  $\mathcal{O}'_D := \text{im } \theta'_D$ ,  $\mathcal{O}''_D := \text{im } \theta''_D$  and  $\mathcal{O}'''_D := \text{im } \theta'''_D$ . We consider the geometrically robust constructible maps

$$\begin{aligned} \tau'_D : \quad \mathcal{O}_D &\rightarrow \mathcal{O}'_D, & \tau''_D : \quad \mathcal{O}_D &\rightarrow \mathcal{O}''_D, & \tau'''_D : \quad \mathcal{O}_D &\rightarrow \mathcal{O}'''_D, \\ \theta_D(t) &\mapsto \theta'_D(t), & \theta_D(t) &\mapsto \theta''_D(t), & \theta_D(t) &\mapsto \theta'''_D(t). \end{aligned}$$

Suppose that there are given framed data structures  $\mathcal{N}''_D$  and  $\mathcal{N}'''_D$  of size polynomial in  $l$ , geometrically robust constructible maps  $\mu''_D : \mathcal{M} \rightarrow \mathcal{N}''_D$  and  $\mu'''_D : \mathcal{M} \rightarrow \mathcal{N}'''_D$ , and polynomial maps  $\omega''_D : \mathcal{N}''_D \rightarrow \mathcal{O}''_D$  and  $\omega'''_D : \mathcal{N}'''_D \rightarrow \mathcal{O}'''_D$ , such that  $\theta''_D : \mathcal{M} \rightarrow \mathcal{O}''_D$  and  $\theta'''_D : \mathcal{M} \rightarrow \mathcal{O}'''_D$  are abstraction functions of the compatible collection  $\mathcal{H}$  associated with  $\mu''_D$ ,  $\omega''_D$  and  $\mu'''_D$ ,  $\omega'''_D$ , respectively. Finally, let  $\mathcal{N}'_D := \mathcal{N}_D$ ,  $\mu'_D := \mu_D$  and  $\omega'_D := \omega_D$ . Each of the three items  $(\theta_D, \tau'_D)$  and  $(\theta_D, \tau''_D)$  and  $(\theta_D, \tau'''_D)$  define a computation task for an exact quiz game. The following diagram illustrates this scenario. Notice that  $\theta_D$ ,  $\theta'_D$ ,  $\theta''_D$  and  $\theta'''_D$  have the same domain of definition  $\mathcal{M}$ .



Suppose that for any of these tasks, e.g., for that given by  $(\theta_D, \tau'_D)$ , there is given an exact quiz game protocol with winning strategy. Thus we have a framed abstract data type carrier  $\mathcal{O}^*$ , framed data structures  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , an abstraction function  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$  of the compatible collection  $\mathcal{H}$ , associated with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , and geometrically robust constructible maps  $\tilde{\sigma} : \mathcal{O}_D \rightarrow \mathcal{M}^*$  and  $\sigma := \tilde{\sigma} \circ \theta_D$  such that the identities  $\theta'_D = \omega^* \circ \mu^* \circ \sigma$  and  $\mathcal{O}'_D = \mathcal{O}^*$  hold. The following diagram illustrates this exact quiz game protocol.



**Lemma 15.** *The size of  $\theta^*$  is at least  $D + 1$ .*

*Proof.* Denote by  $\mathbb{G}_D$  the subset of  $\mathcal{M}$  consisting of all  $(D + 1)$ -th roots of unity. The cardinality of  $\mathbb{G}_D$  is  $D + 1$ . Observe that any  $\zeta \in \mathbb{G}_D$  satisfies the condition  $\theta_D(\zeta) = 0$  and therefore  $\sigma(\zeta) = (\tilde{\sigma} \circ \theta_D)(\zeta)$  does not depend on  $\zeta$ .

For any  $\zeta \in \mathbb{G}_D$ , let  $\beta_\zeta : \mathcal{M} \rightarrow \mathcal{M}$  be the affine linear function defined by  $\beta_\zeta(s) := s + \zeta$ . Then by Theorem 6(iii) the maps  $\theta'_D \circ \beta_\zeta$  and  $\mu^* \circ \sigma \circ \beta_\zeta = \mu^* \circ \tilde{\sigma} \circ \theta_D \circ \beta_\zeta$  are polynomial and hence holomorphic. Moreover,



$u := (\mu^* \circ \sigma \circ \beta_\zeta)(0)$  does not depend on  $\zeta$  and consequently  $(\theta'_D \circ \beta_\zeta)(0)$  depends neither on  $\zeta$ .

We have  $\frac{d}{dt}(\theta'_D \circ \beta_\zeta)(0) = (D+1)\zeta^D \sum_{0 \leq k \leq D} \zeta^k X^k$  and therefore the vectors  $\frac{d}{dt}(\theta'_D \circ \beta_\zeta)(0)$ ,  $\zeta \in \mathbb{G}_D$ , are  $\mathbb{C}$ -linearly independent. Since the player has a winning strategy,  $\mu^* \circ \sigma \circ \beta_\zeta$  is holomorphic and  $\omega^*$  is polynomial, we may apply the chain rule to get

$$\begin{aligned} \frac{d}{dt}(\theta'_D \circ \beta_\zeta)(0) &= d\omega^*((\mu^* \circ \sigma \circ \beta_\zeta)(0)) \cdot \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_\zeta)(0) \\ &= d\omega^*(u) \cdot \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_\zeta)(0) \end{aligned}$$

for any  $\zeta \in \mathbb{G}_D$ . We conclude that the vectors  $\frac{d}{dt}(\mu^* \circ \sigma \circ \beta_\zeta)(0)$ ,  $\zeta \in \mathbb{G}_D$ , generate a  $\mathbb{C}$ -linear space of dimension  $D+1$ . This implies that the size of  $\mathcal{N}^*$ , and hence the size of  $\theta^*$ , is at least  $D+1$ .

The argumentation in the case of the univariate polynomial interpolation problems given by  $(\theta_D, \tau''_D)$  and  $(\theta_D, \tau'''_D)$  is almost textually the same. The only difference is the form of the vectors  $\frac{d}{dt}(\theta''_D \circ \beta_\zeta)(0) = (D+1)\zeta^D \sum_{1 \leq k \leq D} k\zeta^k X^{k-1}$  and  $\frac{d}{dt}(\theta'''_D \circ \beta_\zeta)(0) = (D+1)\zeta^D \sum_{0 \leq k \leq D} \frac{1}{k+1}\zeta^k X^{k+1}$  for  $\zeta \in \mathbb{G}_D$ .  $\square$

Following [BCS97, §8.1], any polynomial  $f$  over  $\mathbb{C}$  requires at least  $\log \deg f$  essential multiplications to be evaluated by an ordinary division-free arithmetic circuit. Let  $(\theta_D)_{D \in \mathbb{N}}$  be the sequence of families of univariate polynomials considered before. Observe that for any  $t \in \mathcal{M}$ , the univariate polynomial  $\theta_D(t)$  can be evaluated by an ordinary division-free arithmetic circuit using  $4\lceil \log D - 2 \rceil$  essential multiplications and that  $\deg \theta_D(t) \leq D$  holds. For all but finitely many  $t \in \mathcal{M}$  we have even  $\deg \theta_D(t) = D$ . In this sense,  $(\theta_D)_{D \in \mathbb{N}}$  is a sequence of families of univariate polynomials which are *easy to evaluate*. From Lemma 15 we deduce now the following less technical statement.

**Theorem 16.** *There exists a sequence of families of univariate polynomials which are easy to evaluate such that the continuous interpolation of these polynomials, or their derivatives, or their indefinite integrals, requires an amount of arithmetic operations which is exponential in the number of essential multiplications of the most efficient ordinary division-free arithmetic circuits which evaluate these polynomials.*

Theorem 16 extends [GHMS11, Proposition 22], and simplifies its proof.

## 4.2 Learning in neural networks with polynomial activation functions

Let us analyze the following architectures of neural networks with polynomial activation functions. Let  $n \in \mathbb{N}$  be a discrete parameter and  $\mathcal{M} := \mathbb{A}^{n+1}$ .

For  $t \in \mathbb{A}^1$  and  $u = (u_1, \dots, u_n) \in \mathbb{A}^n$ , let  $\theta(t, u)$  be the polynomial

$$\theta(t, u) := t(u_1 X_1 + \dots + u_n X_n)^n.$$

Then the formula defining  $\theta(t, u)$  describes the architecture of a two layer network with two neurons, weight vector  $(t, u_1, \dots, u_n)$ , inputs  $X_1, \dots, X_n$ , one output and two activation functions, namely the polynomials  $Y^n$  and  $Y$ , where  $Y$  is a new indeterminate. This network is evaluable by  $2n + 2\lceil \log n \rceil$  arithmetic operations, including  $2\lceil \log n \rceil$  essential multiplications. Hence the family of polynomials  $\theta$  can be represented by a robust arithmetic circuit of size  $2n + 2\lceil \log n \rceil$ . Thus for  $\mathcal{O} := \text{im } \theta$ ,  $\mu := \text{id } \mathcal{M}$  and  $\omega := \theta$ , we have that  $\theta = \omega \circ \mu$  and  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  is an abstraction function associated with the geometrically robust constructible map  $\mu$  and the polynomial map  $\omega$ . By virtue of Proposition 8, and the comment that follows it,  $(\theta, \mu, \omega)$  belongs to a compatible collection  $\mathcal{H}$  of abstraction functions.

More precisely, using  $(4(n+2\lceil \log n \rceil+1)^2+2)(4n+4\lceil \log n \rceil+1)$  arithmetic operations in  $\mathbb{C}$ , we may check whether for given weight vectors  $(t, u)$  and  $(t', u')$  of  $\mathcal{M}$  the identity  $\theta(t, u) = \theta(t', u')$  holds for the target functions  $\theta(t, u)$  and  $\theta(t', u')$  of the neural networks given by  $(t, u)$  and  $(t', u')$ .

The learning of a target function  $\theta(t, u)$  can be interpreted as the task of interpolating  $\theta(t, u)$  in the manner prescribed by the given network architecture. In view of [GHMS11, Section 3.3.3], the continuous interpolation of the family of polynomials  $\theta$  can be performed, not necessarily efficiently, using  $m \geq 4(n+2\lceil \log n \rceil+1)^2$  random points of  $\mathbb{N}^n$  of bit size at most  $8\lceil \log n \rceil+4$  (see the end of this subsection).

Since interpolation is a particular case of an exact quiz game protocol, we are going to ask a more general question, namely whether for the computation task given by  $\theta$ ,  $\theta' := \theta$  and  $\tau := \text{id}_{\mathcal{O}}$  an approximative quiz game protocol with winning strategy can be efficient. The answer will be no. Hence our neural networks cannot be learned in a continuous manner. We confirmed this theoretical conclusion by computer experiments with the 8.3 (R2014a) Matlab version of the standard backpropagation algorithm (see [HKP91, Chapter 6.1]) which we adapted especially to the case of polynomial activation functions. It is not worth to reproduce here the particular experimental results because of the enormous errors they contain. In particular, if we interpret the steps of the back propagation algorithm as an infinite sequence of computations over  $\mathbb{C}$ , the resulting algorithm cannot converge *uniformly* to an exact learning process of our neural networks.

Suppose that for the previous computation task there is given an approximative quiz game protocol with winning strategy. Thus we have a framed abstract data type carrier  $\mathcal{O}^*$ , framed data structures  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , an abstraction function  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$  of the compatible collection  $\mathcal{H}$ , associated

with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , and a surjective geometrically robust constructible map  $\sigma : \mathcal{M} \rightarrow \mathcal{M}^*$  such that by Lemma 9 the identities  $\theta = \omega^* \circ \mu^* \circ \sigma = \theta^* \circ \sigma$  and  $\mathcal{O}^* = \mathcal{O}$  hold.

**Lemma 17.** *The size of  $\theta^*$  is at least  $\binom{2n-1}{n-1} \geq 2^{n-1}$ .*

*Proof.* The proof is similar to that of Lemma 12. Observe that

$$\theta(t, u) = t \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \\ \alpha_1 + \dots + \alpha_n = n}} \frac{n!}{\alpha_1! \dots \alpha_n!} u_1^{\alpha_1} \dots u_n^{\alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

holds for any  $t \in \mathbb{A}^1$  and  $u = (u_1, \dots, u_n) \in \mathbb{A}^n$ .

Let  $U_1, \dots, U_n$  be new indeterminates and let  $M_n := \{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n : \alpha_1 + \dots + \alpha_n = n\}$ . Since the  $K := \binom{2n-1}{n-1}$  monomials  $U_1^{\alpha_1} \dots U_n^{\alpha_n}$ ,  $\underline{\alpha} \in M_n$ , are  $\mathbb{C}$ -linearly independent, we may conclude that there exists a non-empty Zariski open subset  $\mathcal{U}$  of  $\mathbb{A}^{K \times n}$  such that for any point  $(\rho_1, \dots, \rho_K) \in \mathcal{U}$  with  $\rho_i = (\rho_{i1}, \dots, \rho_{in}) \in \mathbb{A}^n$ ,  $1 \leq i \leq K$ , the  $(K \times K)$ -matrix

$$\mathbf{M}_{\rho_1, \dots, \rho_K} := \left( \frac{n!}{\alpha_1! \dots \alpha_n!} \rho_{i1}^{\alpha_1} \dots \rho_{in}^{\alpha_n} \right)_{\substack{\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in M_n, \\ 1 \leq i \leq K}}$$

is nonsingular.

Let  $\rho = (\rho_1, \dots, \rho_n) \in \mathbb{A}^n$  and let  $\beta_\rho : \mathbb{A}^1 \rightarrow \mathcal{M}$  be defined by  $\beta_\rho(t) := (t, \rho)$ . Then the map  $t \mapsto (\theta \circ \beta_\rho)(t)$  is represented by the polynomial

$$(\theta \circ \beta_\rho)(t) = t \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n \\ \alpha_1 + \dots + \alpha_n = n}} \frac{n!}{\alpha_1! \dots \alpha_n!} \rho_1^{\alpha_1} \dots \rho_n^{\alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n},$$

and is therefore linear in  $t$ . On the other hand, the map  $\mu^* \circ \sigma \circ \beta_\rho : \mathbb{A}^1 \rightarrow \mathcal{N}^*$  is geometrically robust and constructible, and hence polynomial by Theorem 6(iii). Thus  $\mu^* \circ \sigma \circ \beta_\rho$  is holomorphic. Since any  $u \in \mathbb{A}^n$  satisfies the condition  $\theta(0, u) = 0$  we conclude from Corollary 11 that the set  $\{(\mu^* \circ \sigma)(0, u) : u \in \mathbb{A}^n\}$  is finite. Hence the set  $\{(\mu^* \circ \sigma \circ \beta_\rho)(0) : \rho \in \mathbb{A}^n\}$  is also finite. Therefore there exists a non-empty Zariski open subset  $\Gamma$  of  $\mathbb{A}^n$  such that for any point  $\rho \in \Gamma$ , the value  $(\mu^* \circ \sigma \circ \beta_\rho)(0)$  is the same, say  $v$ . Observe now that the set  $\mathcal{U} \cap \Gamma^K$  is non-empty, because  $\mathcal{U}$  and  $\Gamma^K$  are non-empty Zariski open subsets of  $\mathbb{A}^{K \times n}$ . Hence there exist elements  $\rho_1, \dots, \rho_K$  of  $\Gamma$  such that the complex  $(K \times K)$ -matrix  $\mathbf{M}_{\rho_1, \dots, \rho_K}$  is nonsingular.

Therefore the vectors  $\frac{d}{dt}(\theta \circ \beta_{\rho_1})(0), \dots, \frac{d}{dt}(\theta \circ \beta_{\rho_K})(0)$  are  $\mathbb{C}$ -linearly independent. The assumption that the player has a winning strategy for the given approximative quiz game implies

$$\theta \circ \beta_{\rho_j} = \omega^* \circ \mu^* \circ \sigma \circ \beta_{\rho_j}$$

for any  $1 \leq j \leq K$ . Since  $\mu^* \circ \sigma \circ \beta_{\rho_j}$  is holomorphic for  $1 \leq j \leq K$ , we may apply the chain rule to this situation to conclude

$$\begin{aligned} \frac{d}{dt}(\theta \circ \beta_{\rho_j})(0) &= d\omega^*((\mu^* \circ \sigma \circ \beta_{\rho_j})(0)) \cdot \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_j})(0) \\ &= d\omega^*(v) \cdot \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_j})(0) \end{aligned}$$

for  $1 \leq j \leq K$ . We infer that the vectors  $\frac{d}{dt}(\mu^* \circ \sigma \circ \beta_{\rho_1})(0), \dots, \frac{d}{dt}(\mu^* \circ \sigma \circ \beta_K)(0)$  generate a  $\mathbb{C}$ -linear space of dimension  $K$ . This implies that the size of  $\mathcal{N}^*$ , and hence the size of  $\theta^*$ , is at least  $K = \binom{2n-1}{n-1} \geq 2^{n-1}$ .  $\square$

Suppose now that it is possible to learn continuously for  $n > 3$  the neural networks corresponding to our network architecture. Then there exists a geometrically robust constructible map  $\tilde{\sigma} : \mathcal{O} \rightarrow \mathcal{M}$  such that the identity  $\theta = \theta \circ \tilde{\sigma} \circ \theta$  holds. This contradicts Lemma 17 with  $\mathcal{O}^* := \mathcal{O}$ ,  $\mathcal{M}^* := \text{im}(\tilde{\sigma} \circ \theta)$ ,  $\theta^* := \theta|_{\mathcal{M}^*}$ ,  $\mu^* := \text{id}|_{\mathcal{M}^*} = \mu|_{\mathcal{M}^*}$ ,  $\mathcal{N}^* := \mathcal{M}^*$ ,  $\omega^* := \theta|_{\mathcal{N}^*} = \omega|_{\mathcal{N}^*}$  and  $\sigma := \tilde{\sigma} \circ \theta$ , because in this case the size of  $\theta^*$  is at most  $n + 1$ , which is strictly smaller than  $2^{n-1}$ . Lemma 17 implies therefore the following learning result for neural network architectures.

**Theorem 18.** *Let  $n \in \mathbb{N}$  be a discrete parameter. There exists a two-layer neural network architecture with two neurons,  $n$  inputs, one output and two polynomial activation functions which can be evaluated using  $2\lceil \log n \rceil$  essential multiplications, such that there is no continuous algorithm able to learn exactly the corresponding neural networks.*

To conclude, we discuss the question how many random points are sufficient to interpolate the target functions of a general neural network architecture with polynomial activation functions.

Let be given a neural network architecture with  $n$  inputs  $X_1, \dots, X_n$  and  $K$  neurons and let  $r$  be the length of the corresponding weight vector. We suppose that all activation functions are given by univariate polynomials which can be evaluated by ordinary division-free arithmetic circuits with parameters in  $\mathbb{R}$  using at most  $L$  essential multiplications. Thus any weight vector of  $\mathbb{A}^r$  defines a (complex) neural network which can be evaluated using at most  $KL$  essential multiplications. Denote for any  $u \in \mathbb{A}^r$  the target function of the corresponding neural network by  $\theta(u) \in \mathbb{C}[X_1, \dots, X_n]$ . Let  $m \geq 4(KL + n + 1)^2 + 2$  and chose  $m$  random points  $\gamma_1, \dots, \gamma_m \in \mathbb{N}^n$  of bit size at most  $4(KL + 1)$ . Then  $\mathcal{M} := \{\theta(u)(\gamma_1), \dots, \theta(u)(\gamma_m) : u \in \mathbb{A}^r\}$  is a constructible subset of  $\mathbb{A}^m$ . From [GHMS11, Section 3.3.3] we deduce that the map which assigns to each element  $(\theta(u)(\gamma_1), \dots, \theta(u)(\gamma_m))$  of  $\mathcal{M}$  the coefficient vector of the polynomial  $\theta(u)$  is geometrically robust and

constructible (over  $\mathbb{R}$ ). This map solves in continuous (but not necessarily efficient) manner the interpolation problem given by  $\gamma_1, \dots, \gamma_m$  of the family of polynomial functions  $\theta$ .

### 4.3 Elimination

Finally we are going to analyze two series of examples of geometric elimination problems from the point of view of approximative quiz games. The first one is concerned with a parameterized family of elimination problems defined on a fixed hypercube and the second one is related to the computation of characteristic polynomials in linear algebra.

#### 4.3.1 A parameterized family of projections of a hypercube

Let  $n \in \mathbb{N}$  be a discrete parameter and let  $\mathcal{M} := \mathbb{A}^{n+1}$ . Let  $X_1, \dots, X_n, Y$  be indeterminates over  $\mathbb{C}$ . For  $t \in \mathbb{A}^1$  and  $u = (u_1, \dots, u_n) \in \mathbb{A}^n$ , let  $\theta(t, u)$  and  $\theta'(t, u)$  be the following polynomials:

$$\begin{aligned} \theta(t, u) &:= \sum_{1 \leq i \leq n} 2^{i-1} X_i + t \prod_{1 \leq i \leq n} (1 + (u_i - 1) X_i), \\ \theta'(t, u) &:= \prod_{\epsilon \in \{0,1\}^n} (Y - \theta(t, u)(\epsilon)) = \prod_{0 \leq j < 2^n} \left( Y - \left( j + t \prod_{1 \leq i \leq n} u_i^{[j]_i} \right) \right), \end{aligned}$$

where  $[j]_i$  denotes the  $i$ -th digit of the binary representation of the integer  $j$  for  $0 \leq j < 2^n$  and  $1 \leq i \leq n$ . Let  $\mathcal{O} := \text{im } \theta$ ,  $\mathcal{O}' := \text{im } \theta'$ ,  $\mathcal{N} := \mathcal{M}$ ,  $\mu := \text{id}_{\mathcal{M}}$ ,  $\omega := \theta$  and observe that the family of polynomials  $\theta$  is evaluable by a robust arithmetic circuit of size  $5n$ . We may therefore deduce from Proposition 8, and the comment following it, that  $(\theta, \mu, \omega)$  belongs to a suitable compatible collection  $\mathcal{H}$  of abstraction functions. We suppose that  $\theta'$  is an abstraction function associated with a geometrically robust constructible map  $\mu' : \mathcal{M} \rightarrow \mathcal{N}'$  and a polynomial map  $\omega : \mathcal{N}' \rightarrow \mathcal{O}'$ , such that  $(\theta', \mu', \omega')$  belongs to the compatible collection  $\mathcal{H}$ .

Observe that for  $t \in \mathbb{A}^1$  and  $u \in \mathbb{A}^n$ , the formulas

$$(\exists X_1) \dots (\exists X_n) (X_1^2 - X_1 = 0 \wedge \dots \wedge X_n^2 - X_n = 0 \wedge Y - \theta(t, u)(X_1, \dots, X_n) = 0)$$

and  $\theta'(t, u)(Y) = 0$  are logically equivalent. In fact,  $\theta'(t, u) = \prod_{\epsilon \in \{0,1\}^n} (Y - \theta(t, u)(\epsilon))$  is the elimination polynomial of the projection of the hypercube  $\{0,1\}^n$  along  $\theta(t, u)$ . Therefore there exists a geometrically robust constructible map  $\tau : \mathcal{O} \rightarrow \mathcal{O}'$  such that  $\tau \circ \theta = \theta'$  holds.

Suppose now that for the computation task determined by  $\theta$  and  $\tau$  there is given a winning strategy of the approximative quiz game protocol. Thus

we have a framed abstract data type carrier  $\mathcal{O}^*$ , framed data structures  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , an abstraction function  $\theta^*$  of the compatible collection  $\mathcal{H}$ , associated with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , and a surjective geometrically robust constructible map  $\sigma : \mathcal{M} \rightarrow \mathcal{M}^*$  such that by Lemma 9 the identities  $\theta' = \omega^* \circ \mu^* \circ \sigma = \theta^* \circ \sigma$  and  $\mathcal{O}' = \mathcal{O}^*$  hold.

**Lemma 19.** *The size of  $\theta^*$  is at least  $2^n$ .*

*Proof.* Let  $T, U_1, \dots, U_n$  be new indeterminates,  $U := (U_1, \dots, U_n)$  and let  $F := \prod_{0 \leq j < 2^n} (Y - (j + T \prod_{1 \leq i \leq n} U_i^{[j]_i}))$ . We write  $F = Y^{2^n} + B_1 Y^{2^n-1} + \dots + B_{2^n}$  with  $B_k \in \mathbb{C}[T, U]$  for  $1 \leq k \leq 2^n$ . Arguing as in [CGH<sup>+</sup>03, §4.2] we deduce that for  $1 \leq k \leq 2^n$ , the coefficient  $B_k$  is of the form

$$B_k = (-1)^k \sum_{0 \leq j_1 < \dots < j_k < 2^n} j_1 \dots j_k + T L_k + \text{terms of higher degree in } T,$$

where  $L_1, \dots, L_{2^n} \in \mathbb{C}[U] = \mathbb{C}[U_1, \dots, U_n]$  are  $\mathbb{C}$ -linearly independent. Therefore there exists a non-empty Zariski open subset  $\mathcal{U}$  of  $\mathbb{A}^{2^n \times n}$  such that for any point  $(u_1, \dots, u_{2^n}) \in \mathcal{U}$  with  $u_1, \dots, u_{2^n} \in \mathbb{A}^n$ , the  $(2^n \times 2^n)$ -matrix

$$\mathbb{M}_{L_1, \dots, L_{2^n}} := (L_k(u_l))_{1 \leq k, l \leq 2^n} \quad (2)$$

is nonsingular.

Since any  $u \in \mathbb{A}^n$  satisfies the condition  $\theta(0, u) = \sum_{1 \leq i \leq n} 2^{i-1} X_i$  and  $\theta(0, u)$  is therefore constant, we conclude from Corollary 11 that the set  $\{(\mu^* \circ \sigma)(0, u) : u \in \mathbb{A}^n\}$  is finite. Hence there exists a non-empty Zariski open subset  $\Gamma$  of  $\mathbb{A}^n$  such that for any point  $u \in \Gamma$ , the value  $(\mu^* \circ \sigma)(0, u)$  is the same, say  $v$ . On the other hand  $\mathcal{U} \cap \Gamma^{2^n}$  is nonempty. Therefore there exist elements  $u_1, \dots, u_{2^n} \in \Gamma$  such that the  $(2^n \times 2^n)$ -matrix  $\mathbb{M}_{L_1, \dots, L_{2^n}}$  of (2) is non-singular.

The maps  $\mu^* \circ \sigma : \mathbb{A}^{n+1} \rightarrow \mathcal{N}^*$  and  $\theta'(t, u) : \mathbb{A}^{n+1} \rightarrow \mathcal{O}^*$  are geometrically robust and constructible, and hence polynomial by Theorem 6(iii). For  $1 \leq k \leq 2^n$  and  $t \in \mathbb{A}^1$ , let  $\varepsilon_k(t) := (\mu^* \circ \sigma)(t, u_k)$  and  $\delta_k(t) := \theta'(t, u_k)$ . Observe that  $\varepsilon_k$  and  $\delta_k$  are polynomial maps with domain of definition  $\mathbb{A}^1$  and therefore holomorphic. Moreover we have  $\varepsilon_k(0) = (\mu^* \circ \sigma)(0, u_k) = v$  for  $1 \leq k \leq 2^n$ . Since  $\theta' = \omega^* \circ \mu^* \circ \sigma$ , we deduce  $\delta_k = \omega^* \circ \varepsilon_k$ . To this composition we may apply the chain rule to conclude that

$$\frac{d\delta_k}{dt}(0) = d\omega^*(\varepsilon_k(0)) \cdot \frac{d\varepsilon_k}{dt}(0) = d\omega^*(v) \cdot \frac{d\varepsilon_k}{dt}(0).$$

Observe now that  $L_1(u), \dots, L_{2^n}(u)$  are the coefficients of the polynomial  $\frac{\partial F}{\partial T}(0, u)$ . This implies that

$$d\omega^*(v) \cdot \frac{d\varepsilon_k}{dt}(0) = \frac{d\delta_k}{dt}(0) = \frac{\partial \theta'}{\partial t}(0, u_k) = (L_1(u_k), \dots, L_{2^n}(u_k))$$

for  $1 \leq k \leq 2^n$ . From the non-singularity of the  $(2^n \times 2^n)$ -matrix  $M_{L_1, \dots, L_{2^n}}$  of (2) we deduce that the vectors  $\frac{d\varepsilon_1}{dt}(0), \dots, \frac{d\varepsilon_{2^n}}{dt}(0)$  generate a  $\mathbb{C}$ -linear space of dimension  $2^n$ . This implies that the size of  $\mathcal{N}^*$ , and hence the size of  $\theta^*$ , is at least  $2^n$ .  $\square$

We are now going to elaborate an important aspect of this family of examples. Observe that any polynomial  $\theta(t, u)$  can be evaluated by a division-free arithmetic circuit using  $n - 1$  essential multiplications. From [GHMS11, Section 3.3.3] we deduce the following facts:

there exist  $K := 16n^2 + 2$  points  $\xi_1, \dots, \xi_K \in \mathbb{Z}^n$  of bit length at most  $4n$  such that for any two polynomials  $f, g \in \overline{\mathcal{O}}$ , the equalities  $f(\xi_1) = g(\xi_1), \dots, f(\xi_K) = g(\xi_K)$  imply  $f = g$ . Thus the polynomial map  $\tilde{\sigma} : \mathcal{O} \rightarrow \mathbb{A}^K$  defined by  $\tilde{\sigma}(f) := (f(\xi_1), \dots, f(\xi_K))$  is injective. Moreover  $\mathcal{M}^* := \tilde{\sigma}(\mathcal{O})$  is an irreducible constructible subset of  $\mathbb{A}^K$ . Finally the constructible map  $\Phi := \tilde{\sigma}^{-1}$  which maps  $\mathcal{M}^*$  onto  $\mathcal{O}$  is geometrically robust.

For  $\epsilon \in \{0, 1\}^n$ , we denote by  $\Phi_\epsilon : \mathcal{M}^* \rightarrow \mathbb{A}^1$  the map  $\Phi_\epsilon(v) := \Phi(v)(\epsilon)$ . One sees easily that  $\Phi_\epsilon$  is a geometrically robust constructible function. Observe that the identities

$$\Phi_\epsilon(\tilde{\sigma}(\theta(t, u))) = \Phi(\tilde{\sigma}(\theta(t, u)))(\epsilon) = (\tilde{\sigma}^{-1} \circ \tilde{\sigma})(\theta(t, u))(\epsilon) = \theta(t, u)(\epsilon)$$

hold for any  $t \in \mathbb{A}^1$  and  $u \in \mathbb{A}^n$ .

For a given point  $v \in \mathcal{M}^*$ , let

$$P(v, Y) := \prod_{\epsilon \in \{0, 1\}^n} (Y - \Phi_\epsilon(v)) := \prod_{\epsilon \in \{0, 1\}^n} (Y - \Phi(v)(\epsilon))$$

and let  $\mathcal{O}^* := \{P(v, Y) : v \in \mathcal{M}^*\}$ . Then the coefficients of  $P$  with respect to  $Y$  are geometrically robust constructible functions with domain of definition  $\mathcal{M}^*$  and  $\mathcal{O}^*$  is a framed abstract data type carrier. Hence the map  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$ ,  $\theta^*(v) := P(v, Y)$  is geometrically robust and constructible. Suppose now that there is given a framed data structure  $\mathcal{N}^*$  and that  $\theta^*$  is an abstraction function associated with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , such that  $(\theta^*, \mu^*, \omega^*)$  belongs to the compatible collection  $\mathcal{H}$ .

From the identities

$$P(\tilde{\sigma}(\theta(t, u)), Y) = \prod_{\epsilon \in \{0, 1\}^n} (Y - \Phi_\epsilon(\tilde{\sigma}(\theta(t, u)))) = \prod_{\epsilon \in \{0, 1\}^n} (Y - \theta(t, u)(\epsilon)) = \theta'(t, u)$$

we deduce that  $\omega^* \circ \mu^* \circ \tilde{\sigma} \circ \theta = \theta^* \circ \tilde{\sigma} \circ \theta = \theta'$  holds. This means that  $\tilde{\sigma} \circ \theta$  and  $\mu^*$  define a winning strategy for the exact quiz game protocol of the computation task given by  $\theta$  and  $\tau$ . This implies by Lemma 19 that the size

of  $\mathcal{N}^*$  is at least  $2^n$ . In other words, any representation of the polynomial  $P$  has size exponential in  $n$ .

We argue now that the polynomial  $P$  is a natural elimination object. Let  $\Theta := \sum_{1 \leq i \leq n} 2^{i-1} X_i + T \prod_{1 \leq i \leq n} (1 + (U_i - 1) X_i)$  and let  $V_1, \dots, V_k$  be new indeterminates. Observe that the existential first-order formula

$$(\exists X_1) \dots (\exists X_n) (\exists T) (\exists U_1) \dots (\exists U_n) \left( \bigwedge_{1 \leq i \leq n} X_i^2 - X_i = 0 \wedge \bigwedge_{1 \leq k \leq K} V_k = \Theta(T, U, \xi_k) \wedge Y = \Theta(T, U, X) \right) \quad (3)$$

describes the constructible subset  $\{(v, y) \in \mathbb{A}^{K+1} : v \in \mathcal{M}^*, y \in \mathbb{C}, P(v, y) = 0\}$  of  $\mathbb{A}^{K+1}$ . Interpreting the coefficients of  $P$  as elements of the function field  $\mathbb{C}(\overline{\mathcal{M}}^*)$  of the irreducible algebraic variety  $\overline{\mathcal{M}}^*$ , one sees easily that  $P$  is the greatest common divisor in  $\mathbb{C}(\overline{\mathcal{M}}^*)[Y]$  of all polynomials of  $\mathbb{C}[\overline{\mathcal{M}}^*][Y]$  which vanish identically on the constructible subset of  $\mathbb{A}^{K+1}$  defined by formula (3). Hence  $P$  is an elimination polynomial parameterized by  $\mathcal{M}^*$ .

Observe that the polynomials contained in the formula (3) can be represented by a robust arithmetic circuit of size  $O(n^3)$ . Therefore the formula (3) is also of size  $O(n^3)$ . Thus we have proved the following statement.

**Theorem 20.** *Let  $n \in \mathbb{N}$  be a discrete parameter. There exists a first-order formula of size  $O(n^3)$  of the elementary theory of  $\mathbb{C}$  determining a framed data structure  $\mathcal{M}^*$  of size  $O(n^2)$  and a family  $P$  of univariate elimination polynomials parameterized by  $\mathcal{M}^*$  such that the following holds. Let  $\mathcal{O}^*$  be the framed abstract data type carrier defined by the family of polynomials  $P$  and  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}^*$  the encoding of  $\mathcal{O}^*$  given by the parameterization of  $P$ . Then  $\theta^*$  is a surjective geometrically robust constructible map. Moreover, for any framed data structure  $\mathcal{N}^*$  and any geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and any polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , such that  $(\theta^*, \mu^*, \omega^*)$  determines an abstraction function associated with  $\mu^*$  and  $\omega^*$ , the size of  $\mathcal{N}^*$  is at least  $2^n$ .*

In conclusion, polynomial size formulas may produce elimination polynomials of exponential size for any (reasonable) representation. This conclusion is essentially the content of [CGH<sup>+</sup>03, Theorem 4] (see also [GH01, Theorem 5], [HKR13b, Theorem 15] and [HKR13a, Theorem 8]).

The leading idea of the proof of Theorem 20 was to use an existential formula, namely (3), to encode a suitable interpolation problem whose solution is the interpolation polynomial  $P \in \mathbb{C}(\overline{\mathcal{M}}^*)[Y]$ . This encoding relates elimination with interpolation in the sense of Section 4.1.1 and explains the similarity of the proofs of Theorem 13 and Theorem 20. In fact, the example



exhibited in the proof of Theorem 20 entails nothing but a hardness result for a suitable interpolation of a polynomial family, given by  $\Theta$ , on the constructible set  $\mathcal{M}^*$ . Using formula (3) we obtain finally our hardness result for elimination, namely Theorem 20.

### 4.3.2 Quiz games in elementary linear algebra: Characteristic polynomials

For every positive integer  $n \in \mathbb{N}$ , we first consider the ring  $(\mathbf{M}_n(\mathbb{C}), +, \times)$  of all square  $n \times n$  matrices with complex entries, with their usual addition and multiplication operations. Let  $\mathfrak{R}$  be the disjoint union of all these rings.

$$\mathfrak{R} := \bigcup_{n \in \mathbb{N}} \mathbf{M}_n(\mathbb{C})$$

A framed abstract data type carrier of *square matrices* is now a constructible subset of some  $\mathbf{M}_n(\mathbb{C})$ ,  $n \in \mathbb{N}$ , contained in  $\mathfrak{R}$ . We are now going to introduce two binary elementary operations on  $\mathfrak{R}$ , namely the Kronecker sum ( $\oplus$ ) and Kronecker product ( $\otimes$ ). However,  $(\mathfrak{R}, \oplus, \otimes)$  will not be a ring, because Kronecker sum and product are not distributive.

Recall that for two square matrices  $A := (a_{i,j})_{1 \leq i,j \leq n} \in \mathbf{M}_n(\mathbb{C})$  and  $B := (b_{k,\ell})_{1 \leq k,\ell \leq m} \in \mathbf{M}_m(\mathbb{C})$ , seen as elements of  $\mathfrak{R}$ , their *Kronecker product*  $A \otimes B$  is the square  $(mn \times mn)$ -matrix given by the following rule:

$$A \otimes B := \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & & & \vdots \\ a_{n,1}B & a_{n,2}B & \cdots & a_{n,n}B \end{pmatrix} \in \mathbf{M}_{nm}(\mathbb{C}).$$

Here  $a_{i,j}B \in \mathbf{M}_m(\mathbb{C})$  is the matrix obtained by multiplying each entry of the matrix  $B$  by the scalar  $a_{i,j}$ . The *Kronecker sum*  $A \oplus B$  of the matrices  $A$  and  $B$  is the square  $(mn \times mn)$ -matrix defined in terms of the Kronecker product as follows:

$$A \oplus B := A \otimes \text{Id}_m + \text{Id}_n \otimes B \in \mathbf{M}_{nm}(\mathbb{C}).$$

Here  $\text{Id}_n$  and  $\text{Id}_m$  denote the  $n \times n$  and  $m \times m$  identity matrices and  $+$  is the usual addition of  $nm$  square matrices.

Using the Kronecker sum and product of square matrices we are now going to introduce a suitable abstraction function. Let  $k$  be a non-negative integer and  $n := 2^k$ . The image of the abstraction function we are going to define will be a constructible subset of the  $\mathbb{C}$ -vector space  $\mathbf{M}_n(\mathbb{C})$  contained

in  $\mathfrak{R}$ . Let us consider the framed data structure  $\mathcal{M} := \mathbb{A}^{k+1}$ . We represent the elements of  $\mathcal{M}$  by  $(s, u_1, \dots, u_k) \in \mathbb{A}^{k+1}$ . Let  $\mathcal{N} := \mathbb{C} \times (\mathbf{M}_2(\mathbb{C}))^k$  and observe that it is a  $\mathbb{C}$ -vector space of dimension  $1 + 4k = 4 \log n + 1$  and hence constructible.

Consider the mapping

$$\begin{aligned} \mu: \mathcal{M} &\longrightarrow \mathcal{N} \\ (s, u_1, \dots, u_k) &\longmapsto \left( s, \begin{pmatrix} 1 & 0 \\ 0 & u_1 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 0 \\ 0 & u_k \end{pmatrix} \right), \end{aligned}$$

which is polynomial and hence geometrically robust and constructible. For  $s \in \mathbb{C}$  and  $A_1, \dots, A_k \in \mathbf{M}_2(\mathbb{C})$ , we define a polynomial mapping  $\omega: \mathcal{N} \rightarrow \mathbf{M}_n(\mathbb{C})$  by means of the Kronecker sum and product and  $\mathbb{C}$ -linear operations in  $\mathbf{M}_n(\mathbb{C})$  as follows:

$$\omega(s, A_1, \dots, A_k) := \left( \bigoplus_{i=1}^k \begin{pmatrix} 0 & 0 \\ 0 & 2^{k-i} \end{pmatrix} \right) + sA_1 \otimes \dots \otimes A_k.$$

Finally, let  $\theta := \omega \circ \mu$  and  $\mathcal{O}$  be the image of  $\theta$ . Then  $\mathcal{O}$  is a constructible subset of  $\mathbf{M}_n(\mathbb{C})$  contained in  $\mathfrak{R}$ . Moreover,  $\mu: \mathcal{M} \rightarrow \mathcal{N}$ ,  $\omega: \mathcal{N} \rightarrow \mathcal{O}$  and hence  $\theta: \mathcal{M} \rightarrow \mathcal{O}$  are polynomial, the surjective mapping  $\theta$  being an abstraction function associated with  $\mu$  and  $\omega$ . The abstraction function  $\theta: \mathcal{M} \rightarrow \mathcal{O}$  can be made explicit by means of the following identity:

$$\theta(s, u_1, \dots, u_k) = \left( \bigoplus_{i=1}^k \begin{pmatrix} 0 & 0 \\ 0 & 2^{k-i} \end{pmatrix} \right) + s \begin{pmatrix} 1 & 0 \\ 0 & u_k \end{pmatrix} \otimes \dots \otimes \begin{pmatrix} 1 & 0 \\ 0 & u_1 \end{pmatrix}.$$

This means that  $\theta$  can be expressed in terms of the Kronecker sum and product using only  $2k$  matrix and Kronecker operations.

Let  $\chi$  be the map which associates to each element of  $\mathfrak{R}$  its characteristic polynomial. Notice that the restriction of  $\chi$  to  $\mathbf{M}_n(\mathbb{C})$  is a polynomial map. Let  $\mathcal{O}' := \chi(\mathcal{O})$ ,  $\mathcal{N}' := \mathcal{M}$ ,  $\mu' := \text{id}_{\mathcal{M}}$ ,  $\omega' := \chi \circ \theta$ . Then  $\mathcal{O}'$  is a constructible subset of the  $\mathbb{C}$ -vector space of univariate polynomials of degree at most  $n$  and  $\omega'$  is polynomial. Hence  $\mathcal{O}'$  is a framed abstract data type carrier and  $\theta': \mathcal{M} \rightarrow \mathcal{O}'$  is an abstraction function associated with  $\mu'$  and  $\omega'$ . We have therefore the following commutative diagram of polynomial maps:

$$\begin{array}{ccccc} & & \mathcal{O} & \xrightarrow{\chi} & \mathcal{O}' \\ & \nearrow \omega & \uparrow \theta & \nearrow \theta' & \uparrow \omega' \\ \mathcal{N} & \xleftarrow{\mu} & \mathcal{M} & \xrightarrow{\mu'} & \mathcal{N}' \end{array}$$

**Lemma 21.** *With these notations, the following properties hold:*

$$\left( \bigoplus_{i=1}^k \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}^{k-i} \right) = \begin{pmatrix} 0 & 0 \\ 0 & 2^{k-1} \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 0 \\ 0 & 2^1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & n-1 \end{pmatrix}.$$

*Additionally,*

$$\begin{pmatrix} 1 & 0 \\ 0 & u_k \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 0 \\ 0 & u_1 \end{pmatrix} = \text{Diag} \left( \prod_{i=1}^k u_i^{[j]i} : 0 \leq j \leq n-1 \right),$$

where  $\text{Diag}$  denotes the diagonal matrix. Moreover, we have

$$\theta'(s, u) = \chi_{\theta(s, u_1, \dots, u_n)}(Y) = \prod_{0 \leq j \leq n-1} \left( Y - \left( j + s \prod_{1 \leq i \leq k} u_i^{[j]i} \right) \right) \in \mathcal{O}'.$$

*Proof.* The first equality holds by induction, observing that

$$\left( \bigoplus_{i=1}^k \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}^{k-i} \right) = \begin{pmatrix} 0 & 0 \\ 0 & 2^{k-1} \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 0 \\ 0 & 2^1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

holds. The second equality also follows by induction. As for the third one, it just follows combining the previous equalities with the definition of  $\theta$  and the definition of the characteristic polynomial.  $\square$

Suppose now that for the computational task determined by  $\theta$  and  $\chi$  there is given a winning strategy of the approximative quiz game protocol. Thus we have a framed abstract data type carrier  $\mathcal{O}^*$ , framed data structures  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , an abstraction function  $\theta^*$  of the compatible collection  $\mathcal{H}$  associated with a geometrically robust constructible map  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}^*$ , and a surjective geometrically robust constructible map  $\sigma : \mathcal{M} \rightarrow \mathcal{M}^*$ , such that by Lemma 9 the identities  $\theta' = \omega^* \circ \mu^* \circ \sigma = \theta^* \circ \sigma$  and  $\mathcal{O}' = \mathcal{O}^*$  hold. This situation is depicted by the following commutative diagram:

$$\begin{array}{ccccc} & \mathcal{N} & & & \\ & \uparrow & \searrow \omega & \xrightarrow{\sigma} & \\ \mathcal{M} & \xrightarrow{\theta} & \mathcal{O} & & \mathcal{M}^* \\ & \downarrow \mu' & \downarrow \chi & \swarrow \theta^* & \downarrow \mu^* \\ \mathcal{N}' & \xrightarrow{\omega'} & \mathcal{O}' & = & \mathcal{O}^* \xleftarrow{\omega^*} \mathcal{N}^* \end{array}$$

By similar arguments as in the proof of Lemma 19 we obtain the following statement.

**Lemma 22.** *The size of  $\theta^*$  is at least  $n = 2^k$ .*

This yields the following result, which may be seen as a linear algebra avatar of Theorem 20.

**Theorem 23.** *Let  $k \in \mathbb{N}$  be a discrete parameter and let  $n = 2^k$ . There exists a term of size  $O(k)$  in  $k + 1$  variables in the first-order language of  $(\mathfrak{R}, \oplus, \otimes)$  which involves also  $\mathbb{C}$ -linear operations in  $\mathbf{M}_n(\mathbb{C})$  and has the following properties.*

*Let  $\mathcal{M} := \mathbb{A}^{k+1}$ . The term describes a polynomial mapping from  $\mathcal{M}$  onto a constructible subset  $\mathcal{O}$  of  $\mathbf{M}_n(\mathbb{C})$  and represents therefore an abstraction function  $\theta : \mathcal{M} \rightarrow \mathcal{O}$ . Let  $\mathcal{O}'$  be the set of characteristic polynomials of the elements of  $\mathcal{O}$  and  $\chi : \mathcal{O} \rightarrow \mathcal{O}'$  the corresponding polynomial map. Then, by means of  $\chi \circ \theta$ , the mentioned term determines a family of univariate monic polynomials of degree  $n$  parameterized by  $\mathcal{M}$  and converts  $\mathcal{O}'$  into a framed abstract data type carrier together with a surjective polynomial mapping  $\theta' : \mathcal{M} \rightarrow \mathcal{O}'$  representing an abstraction function.*

*Moreover, any approximative quiz game with winning strategy giving rise to framed data structures  $\mathcal{M}^*$  and  $\mathcal{N}^*$ , geometrically robust constructible maps  $\sigma : \mathcal{O} \rightarrow \mathcal{M}^*$ ,  $\mu^* : \mathcal{M}^* \rightarrow \mathcal{N}^*$  and  $\theta^* : \mathcal{M}^* \rightarrow \mathcal{O}'$ , and a polynomial map  $\omega^* : \mathcal{N}^* \rightarrow \mathcal{O}'$ , such that  $\sigma$  is surjective and the diagram*

$$\begin{array}{ccccc}
 \mathcal{O} & \xrightarrow{\chi} & \mathcal{O}' & & \\
 \uparrow \theta & \searrow \sigma & \uparrow \theta^* & \swarrow \omega^* & \\
 \mathcal{M} & & \mathcal{M}^* & \xrightarrow{\mu^*} & \mathcal{N}^*
 \end{array}$$

*commutes, requires that  $\mathcal{N}^*$  has size at least  $n = 2^k$ .*

## A Further facts on geometrically robust constructible maps

In the proof of Proposition 10 we make use of the following statement, which is also a key ingredient of the proof of Theorem 6. It is a slight extension of [CGH<sup>+</sup>03, Lemma 2].

**Lemma 24.** *Let  $\mathcal{M}$  and  $\mathcal{N}$  be constructible subsets of suitable affine spaces over  $\mathbb{C}$  and let  $\Phi : \mathcal{M} \rightarrow \mathcal{N}$  be a surjective polynomial map (thus  $\Phi$  induces a structure of  $\mathbb{C}[\overline{\mathcal{N}}]$ -module on  $\mathbb{C}[\overline{\mathcal{M}}]$ ).*

*Suppose that  $\Phi$  satisfies the following condition: each sequence  $(x_k)_{k \in \mathbb{N}}$  of elements of  $\mathcal{M}$ , such that  $(\Phi(x_k))_{k \in \mathbb{N}}$  converges in the Euclidean topology of  $\mathcal{N}$  to a point of  $\mathcal{N}$ , is bounded. Then for any point  $y \in \mathcal{N}$  with maximal vanishing ideal  $\mathfrak{m}_y$  in  $\mathbb{C}[\overline{\mathcal{N}}]$ , the  $\mathbb{C}[\overline{\mathcal{N}}]_{\mathfrak{m}_y}$ -module  $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_y}$  is finite.*

Since Lemma 24 is of its own interest, we are going to give a simple geometric proof of it.

*Proof.* The surjective polynomial map  $\Phi : \mathcal{M} \rightarrow \mathcal{N}$  induces embeddings of  $\mathbb{C}[\overline{\mathcal{N}}]$  into  $\mathbb{C}[\overline{\mathcal{M}}]$  and, if  $\mathcal{M}$  is irreducible, of  $\mathbb{C}(\overline{\mathcal{N}})$  into  $\mathbb{C}(\overline{\mathcal{M}})$ . In this case, we claim that  $\mathbb{C}(\overline{\mathcal{M}})$  is a finite extension of  $\mathbb{C}(\overline{\mathcal{N}})$ . Indeed, let  $r \geq 0$  be the transcendence degree of  $\mathbb{C}(\overline{\mathcal{M}})$  over  $\mathbb{C}(\overline{\mathcal{N}})$ . Then there exists a nonempty Zariski open subset  $U$  of  $\overline{\mathcal{N}}$  such that  $\dim \Phi^{-1}(y) = r$  for any  $y \in U$ . Let  $y \in U \cap \mathcal{N}$ . If  $r > 0$ , then  $\Phi^{-1}(y)$  is unbounded by [CGH<sup>+</sup>03, Lemma 1]. In particular, there exists an unbounded sequence  $(x_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  with  $\Phi(x_k) = y$ , contradicting the assumptions of the lemma. We conclude that  $r = 0$ , and hence  $\mathbb{C}(\overline{\mathcal{M}})$  is a finite extension of  $\mathbb{C}(\overline{\mathcal{N}})$ .

Let  $\mathcal{A}$  be the integral closure of  $\mathbb{C}[\overline{\mathcal{N}}]$  in  $\mathbb{C}[\overline{\mathcal{M}}]$ . If  $\mathcal{M}$  is irreducible, as  $\mathbb{C}(\overline{\mathcal{M}})$  is a finite extension of  $\mathbb{C}(\overline{\mathcal{N}})$ , by, e.g., [Eis95, Corollary 13.13], we deduce that  $\mathcal{A}$  is a finite  $\mathbb{C}[\overline{\mathcal{N}}]$ -module. Since  $\mathbb{C}[\overline{\mathcal{N}}]$  is a reduced noetherian ring, one concludes now easily that the same is true in the general case, when  $\mathcal{M}$  is not necessarily irreducible. Therefore there exists an affine variety  $V$  over  $\mathbb{C}$  with  $\mathcal{A} \cong \mathbb{C}[V]$ . The embeddings of  $\mathcal{A}$  in  $\mathbb{C}[\overline{\mathcal{M}}]$  and of  $\mathbb{C}[\overline{\mathcal{N}}]$  in  $\mathcal{A}$  induce a commutative diagram of morphisms of affine varieties

$$\begin{array}{ccc}
 & & V \\
 & \nearrow \tilde{\Phi} & \downarrow \Psi \\
 \overline{\mathcal{M}} & & \overline{\mathcal{N}} \\
 & \searrow \Phi & 
 \end{array}$$

where the image of  $\tilde{\Phi}$ , and hence  $\tilde{\Phi}(\mathcal{M})$ , are Zariski dense in  $V$  and  $\Psi$  is finite.

Consider now an arbitrary point  $y \in \mathcal{N}$  with maximal vanishing ideal  $\mathfrak{m}_y$  in  $\mathbb{C}[\overline{\mathcal{N}}]$  and let  $z \in V$  an arbitrary point of  $V$  with  $\Psi(z) = y$ . Observe that such a point  $z$  exists because  $\Psi$  is a finite morphism. Moreover, let  $\mathfrak{M}_z$  be the maximal vanishing ideal of  $z$  in  $\mathbb{C}[V]$ .

**Claim 1.**  $\tilde{\Phi}^{-1}(z)$  is nonempty.

*Proof.* Since  $\tilde{\Phi}(\mathcal{M})$  is Zariski dense in  $V$ , it is also dense in  $V$  with respect to the Euclidean topology of  $V$ . Therefore there exists a sequence  $(x_k)_{k \in \mathbb{N}}$  of points of  $\mathcal{M}$  such that  $(\tilde{\Phi}(x_k))_{k \in \mathbb{N}}$  converges to  $z$ . Since  $\Psi$  is continuous with respect to the Euclidean topologies of  $V$  and  $\overline{\mathcal{N}}$ , the sequence  $(\Phi(x_k))_{k \in \mathbb{N}} = ((\Psi \circ \tilde{\Phi})(x_k))_{k \in \mathbb{N}}$  converges to  $y = \Psi(z)$ .

By assumption  $\Phi$  satisfies the condition of Lemma 24. Therefore the sequence  $(x_k)_{k \in \mathbb{N}}$  is bounded. Without loss of generality we may assume that  $(x_k)_{k \in \mathbb{N}}$  converges with respect to the Euclidean topology of  $\overline{\mathcal{M}}$  to a point  $x \in \overline{\mathcal{M}}$ . Then the continuity of  $\tilde{\Phi}$  implies  $\tilde{\Phi}(x) = \lim_{k \rightarrow \infty} \tilde{\Phi}(x_k) = z$ . Hence  $\tilde{\Phi}^{-1}(z)$  is nonempty.  $\square$

**Claim 2.**  $\tilde{\Phi}^{-1}(z)$  is finite.

*Proof.* Suppose on the contrary that  $\tilde{\Phi}^{-1}(z)$  is infinite. By [CGH<sup>+</sup>03, Lemma 1] there exists an unbounded sequence  $(v_k)_{k \in \mathbb{N}}$  in  $\tilde{\Phi}^{-1}(z)$ . Since  $\mathcal{M}$  is dense in  $\overline{\mathcal{M}}$  in the Euclidean topology, there exists for each  $k \in \mathbb{N}$  a sequence  $(x_{k_i})_{i \in \mathbb{N}}$  of points of  $\mathcal{M}$  which converges to  $v_k$  in the Euclidean topology. From the continuity of  $\tilde{\Phi}$  and the fact that  $v_k \in \tilde{\Phi}^{-1}(z)$ , we deduce that the sequence  $(\tilde{\Phi}(x_{k_i}))_{i \in \mathbb{N}}$  converges to  $z$  in the Euclidean topology. Without loss of generality we may assume  $\|v_k - x_{k_i}\| < \frac{1}{i}$  and  $\|z - \tilde{\Phi}(x_{k_i})\| < \frac{1}{i}$  for any  $k, i \in \mathbb{N}$ , where  $\|\cdot\|$  denotes the Euclidean norm of  $\overline{\mathcal{M}}$  and  $V$ , respectively. Therefore we have  $\|v_k - x_{k_k}\| < \frac{1}{k}$  for any  $k \in \mathbb{N}$ , and  $(\tilde{\Phi}(x_{k_k}))_{k \in \mathbb{N}}$  converges to  $z$  in the Euclidean topology of  $V$ . This implies that the sequence  $(\Phi(x_{k_k}))_{k \in \mathbb{N}} = (\Psi \circ \tilde{\Phi}(x_{k_k}))_{k \in \mathbb{N}}$  converges to  $y = \phi(z)$  in the Euclidean topology of  $\mathcal{N}$ . Since  $\Phi$  satisfies the condition of Lemma 24 we conclude that the sequence  $(x_{k_k})_{k \in \mathbb{N}}$  is bounded. From the inequality  $\|v_k - x_{k_k}\| < \frac{1}{k}$  for every  $k \in \mathbb{N}$  we infer now that the sequence  $(v_k)_{k \in \mathbb{N}}$  is also bounded, contrary to our assumption that  $(v_k)_{k \in \mathbb{N}}$  is unbounded.  $\square$

From Claims 1 and 2 we deduce that the fibre  $\tilde{\Phi}^{-1}(z)$  is a zero-dimensional affine variety and that there exists a prime ideal  $\mathfrak{p}$  of  $\mathbb{C}[\overline{\mathcal{M}}]$  with  $\mathfrak{p} \cap \mathbb{C}[V] = \mathfrak{M}_z$ , which is maximal and minimal under this condition. Considering  $\mathbb{C}[\overline{\mathcal{M}}]$  as a  $\mathbb{C}[V]$ -module and taking into account that  $\mathbb{C}[V]$  is integrally closed in  $\mathbb{C}[\overline{\mathcal{M}}]$  we may now deduce from Zariski's Main Theorem (see, e.g., [Ive73, IV.2]) that  $\mathbb{C}[V]_{\mathfrak{M}_z} = \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_z}$  holds. Since  $z$  was an arbitrary point of  $V$  with  $\Psi(z) = y$  we conclude  $\mathbb{C}[V]_{\mathfrak{m}_y} = \mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_y}$ . Finally  $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{m}_y}$  is a finite  $\mathbb{C}[\overline{\mathcal{N}}]_{\mathfrak{m}_y}$ -module, because  $\mathbb{C}[V]$  is finite over  $\mathbb{C}[\overline{\mathcal{N}}]$ .  $\square$

We finally state the following result, which is used in Appendix B below.

**Lemma 25.** *Let  $K \subset \mathcal{M}$  and  $\mathcal{N}$  constructible subsets of suitable affine spaces over  $\mathbb{C}$  and let  $\Phi : \mathcal{M} \rightarrow \mathcal{N}$  be a geometrically robust constructible map. Then the following assertions hold.*

- (i)  *$K$  is closed in the Zariski topology of  $\mathcal{M}$  if and only if it is closed in the Euclidean topology of  $\mathcal{M}$ .*
- (ii)  *$\Phi$  is continuous with respect to the Zariski topologies of  $\mathcal{M}$  and  $\mathcal{N}$ .*
- (iii) *If  $\mathcal{M}$  is irreducible, then the constructible set  $\Phi(\mathcal{M})$  is also irreducible.*

*Proof.* (iii) is an immediate consequence of (ii) and (ii) follows from (i) and Theorem 7. The only if part of (i) is trivial. Let us show the if part.

Suppose that the constructible set  $K$  is closed in the Euclidean topology of  $\mathcal{M}$ . Then the Euclidean closure  $\overline{K}$  of  $K$  satisfies the condition  $\overline{K} \cap \mathcal{M} = K$ . Since  $\overline{K}$  is closed with respect to the Zariski topology we see that  $K$  is also Zariski closed.  $\square$

## B Approximative representations and computational models

Complexity models dealing with objects of approximative nature have been used in computer algebra for several purposes. For example, the concept of border rank has been one of the keys to the fastest known matrix multiplication algorithms (see, e.g., [BCS97, Chapter 15]). The concepts of approximative complexity has also been applied to arbitrary polynomials and rational functions (see, e.g., [Ald84], [Gri86] or [Lic90]).

In this appendix we show that the approximative quiz game protocol of Section 3.4.2 models the standard concept of approximative complexity. For this purpose, we introduce a representation of polynomials by means of approximative information which is directly inspired in that of the references above, namely by a certain meromorphic map germ. Then we prove that a polynomial can be represented by an approximative parameter instance in this sense if and only if it can be represented in a model closed to that of Section 3.4.2, namely by a (not necessarily convergent) sequence of parameter instances.

Let  $\mathcal{O}$  be a framed abstract data type carrier,  $\mathcal{M}$  and  $\mathcal{N}$  framed data structures, where  $\mathcal{M}$  is irreducible,  $\theta : \mathcal{M} \rightarrow \mathcal{O}$  a surjective geometrically robust constructible map,  $\mu : \mathcal{M} \rightarrow \mathcal{N}$  a geometrically robust constructible map and  $\omega : \mathcal{N} \rightarrow \mathcal{O}$  a polynomial map such that  $\theta = \omega \circ \mu$  holds. Thus  $\theta$  is

an abstraction function associated with  $\mu$  and  $\omega$ . Suppose that the elements of  $\mathcal{O}$  are polynomials of  $\mathbb{C}[X_1, \dots, X_n]$ , where  $X_1, \dots, X_n$  are indeterminates.

Let  $U_1, \dots, U_r$  be new indeterminates, where  $r$  is the size of  $\mathcal{M}$ , and let  $U := (U_1, \dots, U_r)$  and  $X := (X_1, \dots, X_n)$ . Let  $\mathfrak{a}$  be the vanishing ideal of  $\overline{\mathcal{M}}$  in  $\mathbb{C}[U]$  and let us fix a polynomial  $P \in \mathbb{C}[U]$  such that  $\overline{\mathcal{M}}_P := \{u \in \overline{\mathcal{M}} : P(u) \neq 0\}$  is a Zariski open and dense subset of  $\mathcal{M}$ , and such that  $\theta$  as a rational function is everywhere defined on  $\overline{\mathcal{M}}_P$  (see Remark 4). Let  $\epsilon$  be a new indeterminate.

**Definition 26.** *An approximative parameter instance for  $\theta$  is a vector  $u(\epsilon) = (u_1(\epsilon), \dots, u_r(\epsilon)) \in \mathbb{C}((\epsilon))^r$  which constitutes a meromorphic map germ at the origin such that any polynomial of  $\mathfrak{a}$  vanishes at  $u(\epsilon)$  and  $P(u(\epsilon)) \neq 0$  holds.*

Let  $u(\epsilon)$  be an approximative parameter instance for  $\theta$ . Then there exists an open disc  $\Delta$  around 0 such that for any complex number  $c \in \Delta \setminus \{0\}$  the germ  $u(\epsilon)$  is holomorphic at  $c$  and such that  $P(u(c)) \neq 0$  holds. This implies that any polynomial of  $\mathfrak{a}$  vanishes at  $u(c)$ . In particular,  $u(c)$  belongs to  $\mathcal{M}$  for any  $c \in \Delta \setminus \{0\}$ .

For technical reasons we need the following result.

**Lemma 27.** *Let  $u(\epsilon)$  be an approximative parameter instance for  $\theta$ . Then there exists an open disc  $\Delta$  of  $\mathbb{C}$  around the origin and a germ  $\psi$  of meromorphic functions at the origin such that  $u(\epsilon)$  and  $\psi$  are holomorphic on  $\Delta \setminus \{0\}$  and such that any complex number  $c \in \Delta \setminus \{0\}$  satisfies the conditions  $P(u(c)) \neq 0$  and  $\psi(c) = \mu(u(c))$ .*

*Proof.* There exists an open disc  $\Delta'$  of  $\mathbb{C}$  around the origin such that  $u(\epsilon)$  is everywhere defined on  $\Delta' \setminus \{0\}$  and such that any  $c \in \Delta' \setminus \{0\}$  satisfies the condition  $P(u(c)) \neq 0$ . Let  $\mathcal{N}_0$  be the Zariski closure of the image of  $\Delta' \setminus \{0\}$  under  $u(\epsilon)$ .

**Claim 3.**  $\mathcal{N}_0$  is irreducible.

*Proof of the claim.* Let  $W_1, \dots, W_l$  be the irreducible components of  $\mathcal{N}_0$  and let  $C_1, \dots, C_l$  be the pre-images of  $W_1, \dots, W_l$  under the restriction of  $u(\epsilon)$  to  $\Delta' \setminus \{0\}$ . Then  $C_1, \dots, C_l$  are analytic subsets of the (connected) complex domain  $\Delta' \setminus \{0\}$  which satisfy the condition

$$\Delta' \setminus \{0\} = C_1 \cup \dots \cup C_l. \quad (4)$$

Each  $C_j$  is defined by means of a finite number of equalities and inequalities of holomorphic functions on  $\Delta' \setminus \{0\}$ . The Identity Theorem for holomorphic functions implies that either each point of  $C_j$  is isolated or there exists a nonempty open subset of  $\Delta' \setminus \{0\}$  contained in  $C_j$ . Since  $\Delta' \setminus \{0\}$  is an open



set and equality (4) holds, there exists an index  $j$ ,  $1 \leq j \leq l$ , which satisfies the latter condition. Because  $\Delta' \setminus \{0\}$  is connected, the Identity Theorem shows that  $C_j = \Delta' \setminus \{0\}$ . Therefore,  $u(C_j) = u(u^{-1}(W_j)) \subseteq W_j$  and, thus,  $W_j$  contains the image of  $\Delta' \setminus \{0\}$  under  $u(\varepsilon)$ . This implies  $W_j = \mathcal{N}_0$ .  $\square$

Since  $\mathcal{N}_0$  is irreducible, by Remark 4 there exists a Zariski open and dense subset  $\mathcal{U}$  of  $\mathcal{N}_0$  with  $\mathcal{U} \subset \mathcal{M}$  such that  $\mu$  is rational and everywhere defined on  $\mathcal{U}$ . Moreover there exists a non-zero polynomial  $Q \in \mathbb{C}[U]$  such that  $\mathcal{N}_Q$  is contained in  $\mathcal{U}$  and Zariski dense in  $\mathcal{N}_0$ . Therefore there exists a complex number  $c_0 \in \Delta' \setminus \{0\}$  with  $Q(u(c_0)) \neq 0$ . Replacing  $\Delta'$  by a smaller open disc whose closure is contained in  $\Delta'$  we may use the same arguments as in the proof of the claim above to show that without loss of generality  $K := \{c \in \Delta' \setminus \{0\} : Q(u(c)) = 0\}$  is finite. Thus we may choose an open disc  $\Delta$  around the origin with  $\Delta \subset \Delta'$  and  $\Delta \cap K = \emptyset$  such that the image of  $\Delta$  under  $u(\varepsilon)$  is contained in  $\mathcal{N}_Q$ . We conclude now that  $u(\varepsilon)$  is everywhere defined on  $\Delta \setminus \{0\}$  and that every  $c \in \Delta \setminus \{0\}$  satisfies the condition  $u(c) \in \mathcal{U}$ . For  $c \in \Delta \setminus \{0\}$ , let  $\psi(c) := \mu(u(c))$ . Then  $\psi : \Delta \setminus \{0\} \rightarrow \mathbb{C}^m$  is a well-defined meromorphic function. Let  $c \in \Delta \setminus \{0\}$  and let  $(c_k)_{k \in \mathbb{N}}$  be a sequence in  $\Delta \setminus \{0\}$  which converges to  $c$ . Then the sequence  $(u(c_k))_{k \in \mathbb{N}}$  of points of  $\mathcal{U}$  converges to  $u(c)$  and hence the sequence  $(\mu(u(c_k)))_{k \in \mathbb{N}}$  converges to  $\mu(u(c))$  and is therefore bounded. This implies that  $\psi$  is holomorphic at  $c$ . Thus  $\psi$  is holomorphic on  $\Delta \setminus \{0\}$  and for any  $c \in \Delta \setminus \{0\}$  we have  $\psi(c) = \mu(u(c))$  and  $P(u(c)) \neq 0$ . Therefore we may interpret  $\psi$  as a meromorphic map germ at the origin which is holomorphic on  $\Delta \setminus \{0\}$ .  $\square$

Let  $u(\varepsilon)$  be an approximative parameter instance for  $\theta$ . Then following Lemma 27 there exists an open disc  $\Delta$  of  $\mathbb{C}$  around the origin such that  $\mu(u(\varepsilon))$  is meromorphic on  $\Delta$  and holomorphic on  $\Delta \setminus \{0\}$ . Therefore the coefficients of the polynomial  $\theta(u(\varepsilon)) := \omega(\mu(u(\varepsilon)))$  with respect to  $X$  have the same property. Thus  $\theta(u(\varepsilon))$  can be interpreted as an element of  $\mathbb{C}((\varepsilon))[X]$ .

We say that the approximative parameter instance  $u(\varepsilon)$  for  $\theta$  *encodes* a polynomial  $H \in \mathbb{C}[X]$  if there exists a polynomial  $H' \in \mathbb{C}[[\varepsilon]][X]$ , whose coefficient vector with respect to  $X$  constitutes a germ of functions which are holomorphic at the origin, such that  $\theta(u(\varepsilon))$  can be written in  $\mathbb{C}((\varepsilon))[X]$  as

$$\theta(u(\varepsilon)) = H + \varepsilon H'.$$

The mere existence of an encoding of a given polynomial by an approximative parameter instance for  $\theta$  becomes characterized as follows.

**Theorem 28.** *Let notations and assumptions be as before and let  $H \in \mathbb{C}[X]$ . Then the following conditions are equivalent:*

- (i) *There exists an approximative parameter instance for  $\theta$  that encodes the polynomial  $H$ .*
- (ii) *There exists a sequence  $(u_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  such that  $(\theta(u_k))_{k \in \mathbb{N}}$  converges to  $H$  in  $\mathbb{C}[X]$ .*
- (iii)  *$H$  belongs to  $\overline{\mathcal{O}}$ .*

*Proof.* The conditions (ii) and (iii) are obviously equivalent because one is only a restatement of the other. It suffices therefore to show the implications (i)  $\Rightarrow$  (ii) and (ii) + (iii)  $\Rightarrow$  (i). We first prove (i)  $\Rightarrow$  (ii).

Suppose that there exists an approximative parameter instance  $u(\epsilon)$  for  $\theta$  such  $u(\epsilon)$  encodes  $H \in \mathbb{C}[X]$  by means of a polynomial  $H' \in \mathbb{C}[\epsilon][X]$  whose coefficient vector constitutes a holomorphic map germ at the origin. Thus we have  $\theta(u(\epsilon)) = H + \epsilon H'$  in  $\mathbb{C}((\epsilon))[X]$ . We may choose a sequence  $(\epsilon_k)_{k \in \mathbb{N}}$  of non-zero complex numbers converging to zero such that for any  $k \in \mathbb{N}$  the germ  $u(\epsilon)$  is holomorphic at  $\epsilon_k$  and satisfies the condition  $P(u(\epsilon_k)) \neq 0$ . Without loss of generality we may suppose that the coefficients of  $H'$  are holomorphic at  $\epsilon_k$  for any  $k \in \mathbb{N}$ .

For  $k \in \mathbb{N}$  let  $u_k := u(\epsilon_k)$ . Then  $u_k$  belongs to  $\mathcal{M}$  and  $(\theta(u_k))_{k \in \mathbb{N}} = (H(X) + \epsilon_k H'(\epsilon_k, X))_{k \in \mathbb{N}}$  converges to  $H$ . Therefore condition (ii) is satisfied.

The remaining implication is more cumbersome. In the proof below we adapt the argumentation of [Ald84, Lemmas 1 and 2] to our context.

By assumption  $\overline{\mathcal{M}}$  is an irreducible affine variety. Observe that  $\theta(\overline{\mathcal{M}}_P)$  is Zariski dense in  $\overline{\mathcal{O}}$ , because  $\theta$  is continuous with respect to the Euclidean and the Zariski topologies of  $\mathcal{M}$  and  $\mathcal{O}$  (see Theorem 7 and Lemma 25 (ii)). Thus  $B := \overline{\mathcal{O}} \setminus \theta(\overline{\mathcal{M}}_P)$  is a proper Zariski closed subset of  $\overline{\mathcal{O}}$ . Let  $q$  be the dimension of the irreducible affine variety  $\overline{\mathcal{O}}$ . By assumption we have  $H \in \overline{\mathcal{O}}$ . If  $q = 0$ , then  $H \in \mathcal{O}$  and we are done. Therefore we may suppose without loss of generality  $q > 0$ .

By Noether's Normalization Lemma there exists a surjective finite morphism of irreducible affine varieties  $\lambda : \overline{\mathcal{O}} \rightarrow \mathbb{A}^q$ . Since  $B$  is a proper Zariski closed subset of  $\overline{\mathcal{O}}$  we have  $\lambda(B) \subsetneq \mathbb{A}^q$ . We may therefore choose a point  $z \in \mathbb{A}^q \setminus \lambda(B)$ . Let  $L$  be a straight line of  $\mathbb{A}^q$  which passes through  $\lambda(H)$  and  $z$ . Then  $\lambda(H)$  belongs to  $L$  and  $\lambda(B) \cap L$  is a finite set. Since the morphism  $\lambda$  is finite, the irreducible components of  $\lambda^{-1}(L)$  are all closed curves of  $\overline{\mathcal{O}}$  which become mapped onto  $L$  by  $\lambda$ . In particular, there exists an irreducible component  $C$  of  $\lambda^{-1}(L)$  which contains  $H$ . Since  $\lambda(B) \cap L$  is finite, we have  $C \not\subseteq B$ . Therefore  $C \cap B$  is also finite. Suppose that  $\theta(\overline{\mathcal{M}}_P) \cap C$  is finite. Then we may conclude that  $C \cap B$  is infinite, a contradiction. Therefore  $\theta(\overline{\mathcal{M}}_P) \cap C$  is infinite. Hence the Zariski closure of  $\theta^{-1}(C)$  in  $\overline{\mathcal{M}}$  contains an irreducible component  $V$  such that the constructible set  $\theta(V_P)$  is Zariski

dense in  $C$ . Let  $q^* := \dim V$  and  $u \in V_P$ . Observe that  $q^* > 0$  and, by the continuity of  $\theta$ ,  $B^* := \overline{\theta^{-1}(\theta(u))} \cap V$  is a proper Zariski closed subset of  $V$ .

Again by Noether's Normalization Lemma there exists a surjective finite morphism of irreducible affine varieties  $\lambda^* : V \rightarrow \mathbb{A}^{q^*}$ . Since  $B^*$  is a proper Zariski closed subset of  $V$  we have  $\lambda^*(B^*) \subsetneq \mathbb{A}^{q^*}$ . Therefore we may choose again a point  $z^* \in \mathbb{A}^{q^*} \setminus \lambda^*(B^*)$  and a straight line  $L^*$  of  $\mathbb{A}^{q^*}$  which passes through  $\lambda^*(u)$  and  $z^*$ . Thus  $\lambda^*(B^*) \cap L^*$  is a finite set and  $\lambda^*(u)$  belongs to  $L^*$ . The irreducible components of  $(\lambda^*)^{-1}(L^*)$  are all closed curves of  $V$  which become mapped onto  $L^*$  by  $\lambda^*$ . In particular, there exists an irreducible component  $C^*$  of  $(\lambda^*)^{-1}(L^*)$  which contains  $u$ . Since  $\lambda^*(B^*) \cap L^*$  is finite we conclude  $C^* \not\subseteq B^*$ . Moreover, as  $C^*$  is irreducible,  $u \in C^*$  and  $u \in V_P$ , we infer that  $C_P^*$  is Zariski dense in  $C^*$ . Hence  $C^* \not\subseteq B^*$  implies that there exists a point  $u^* \in C_P^* \setminus B^*$ . By definition of  $B^*$ ,  $\theta(u^*) \neq \theta(u)$ . Moreover, we deduce from Lemma 25(iii) that the constructible set  $\theta(C_P^*)$  is irreducible. Therefore  $\theta(C_P^*)$  is Zariski dense in  $C$ .

In this way we have found two irreducible closed curves  $C^* \subseteq \overline{\mathcal{M}}$  and  $C \subseteq \overline{\mathcal{O}}$  with  $C_P^*$  nonempty such that  $\theta$  maps  $C_P^*$  into  $C$  and  $\theta(C_P^*)$  is Zariski dense in  $C$ . Moreover,  $H \in C$ . The restriction of  $\theta$  to  $C_P^*$  is, by assumption on  $P$ , a well-defined rational map with Zariski dense image in  $C$ . Therefore, the geometrically robust constructible map  $\theta$  induces a finite field extension  $\mathbb{C}(C) \subset \mathbb{C}(C^*)$ .

Let  $D^*$  be the normalization of the projective closure of  $C^*$  and let  $D$  be the projective closure of  $C$ . Then  $\theta$  induces a rational map  $\theta^* : D^* \dashrightarrow D$  whose image is dense in  $D$ . Since  $\theta^*$  is a smooth curve and  $D$  is projective,  $\theta^*$  is a regular map (see, e.g., [Sha94, §II.3, Corollary 1]). The situation is depicted in the following diagram:

$$\begin{array}{ccc} C^* & \overset{\theta}{\dashrightarrow} & C \\ \downarrow & & \downarrow \\ D^* & \xrightarrow{\theta^*} & D \end{array}$$

As  $\text{im}(\theta^*)$  is dense in  $D$ , we conclude that  $\theta^*$  is surjective. Hence there exists a point  $\eta$  of  $D^*$  with  $\theta^*(\eta) = H$ . Let  $\mathcal{S} := \mathcal{O}_{D^*, \eta}$  be the local ring of  $D^*$  at  $\eta$ . Thus  $\mathcal{S}$  is a regular  $\mathbb{C}$ -algebra of dimension one and therefore there exists an embedding of  $\mathcal{S}$  into a power series ring  $\mathbb{C}[[\epsilon]]$  which maps any generator of the maximal ideal of  $\mathcal{S}$  onto a power series of order one. Moreover, by the Jacobian criterion and the Implicit Function Theorem, the elements of  $\mathcal{S}$  become mapped onto power series which constitute holomorphic function germs at the origin. Hence the coordinate functions of  $C^*$  determined by the

restrictions of the canonical projections  $\mathbb{A}^r \rightarrow \mathbb{A}^1$  to  $C^*$  can be represented by Laurent series  $u_1(\epsilon), \dots, u_r(\epsilon)$  of  $\mathbb{C}((\epsilon))$  which constitute meromorphic function germs at the origin. Let  $u(\epsilon) := (u_1(\epsilon), \dots, u_r(\epsilon))$ . Then we deduce  $P(u(\epsilon)) \neq 0$  from the fact that  $C_P^*$  is Zariski dense in  $C^*$  and  $\theta(u(\epsilon))$  is a well-defined meromorphic map germ at the origin by the same argument as in the proof of Lemma 27.

Furthermore, we have  $\theta^* = \theta(u(\epsilon))$ , which implies that  $\theta(u(\epsilon))$  admits a holomorphic extension to  $\epsilon = 0$ . In particular, the entries of the vector  $\theta(u(\epsilon))$  are power series of  $\mathbb{C}[[\epsilon]]$  which constitute holomorphic function germs at the origin. Moreover  $H - \theta(u(\epsilon))$  belongs to the maximal ideal of the local ring of  $\mathbb{C}[D]$  at  $H$  and hence to that of  $\mathcal{S}$ . This means that  $\epsilon$  divides the entries of the coefficient vector of  $H - \theta(u(\epsilon))$  in  $\mathbb{C}[[\epsilon]]$ . We conclude now that there exists a polynomial  $H' \in \mathbb{C}[[\epsilon]][X]$ , whose coefficients constitute holomorphic function germs at the origin, such that the equality  $\theta(u(\epsilon)) = H + \epsilon H'$  holds in  $\mathbb{C}((\epsilon))[X]$ . Since  $C^*$  is contained in  $\overline{\mathcal{M}}$  we have finally  $A(u(\epsilon)) = 0$  for any polynomial  $A \in \mathfrak{a}$ . Thus  $u(\epsilon)$  is an approximative parameter instance for  $\theta$  that encodes the polynomial  $H$ .  $\square$

Theorem 28 suggests that we may consider a (not necessarily convergent) sequence  $(u_k)_{k \in \mathbb{N}}$  in  $\mathcal{M}$  such that  $(\theta(u_k))_{k \in \mathbb{N}}$  converges in the Euclidean topology to a polynomial  $H \in \mathbb{C}[X_1, \dots, X_n]$  as an *approximative encoding* of  $H$  with respect to  $\theta$ . This motivates the approximative quiz game of Section 3.4.2.

A symbolic variant of Theorem 28 for the representation of polynomials by robust arithmetic circuits with parameter domain  $\mathbb{A}^r$  is the main technical contribution of [Ald84] (see also [Lic90, §A]).

## References

- [Ald84] A. Alder, *Grenzzrang und Grenzkomplexität aus algebraischer und topologischer sicht*, Ph.D. thesis, Universität Zürich, 1984.
- [BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi, *Algebraic complexity theory*, Grundlehren Math. Wiss., vol. 315, Springer, Berlin, 1997.
- [CGH<sup>+</sup>03] D. Castro, M. Giusti, J. Heintz, G. Matera, and L.M. Pardo, *The hardness of polynomial equation solving*, Found. Comput. Math. **3** (2003), no. 4, 347–420.

- [Eis95] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Grad. Texts in Math., vol. 150, Springer, New York, 1995.
- [FJ05] M. Fried and M. Jarden, *Field arithmetic*, 2nd ed., Springer, Berlin, 2005.
- [GH01] M. Giusti and J. Heintz, *Kronecker’s smart, little black-boxes*, Proceedings of Foundations of Computational Mathematics, FoCM’99, Oxford 1999 (Cambridge) (A. Iserles R. Devore and E. Süli, eds.), London Math. Soc. Lecture Note Ser., vol. 284, Cambridge Univ. Press, 2001, pp. 69–104.
- [GHMS11] N. Giménez, J. Heintz, G. Matera, and P. Solernó, *Lower complexity bounds for interpolation algorithms*, J. Complexity **27** (2011), no. 2, 151–187.
- [Gri86] B. Griesser, *Lower bounds for the approximative complexity*, Theoret. Comput. Sci. **46** (1986), 329–338.
- [HDB96] M. Hagan, H. Demuth, and M. Beale, *Neural network design*, PWS Publishing Company, Boston, MA, 1996.
- [HKP91] J. Hertz, A. Krogh, and R. Palmer, *Introduction to the theory of neural computation*, Addison–Wesley, Reading, Massachusetts, 1991.
- [HKP99] S. Haykin, A. Krogh, and R. Palmer, *Neural networks, a comprehensive foundation*, second ed., Prentice Hall, Upper Saddle River, NJ, 1999.
- [HKR13a] J. Heintz, B. Kuijpers, and A. Rojas Paredes, *On the intrinsic complexity of elimination problems in effective algebraic geometry*, Recent advances in real complexity and computation (Providence, RI) (J. L. Montaña and L. M. Pardo, eds.), Contemp. Math., vol. 604, Amer. Math. Soc., 2013, pp. 129–150.
- [HKR13b] ———, *Software engineering and complexity in effective algebraic geometry*, J. Complexity **29** (2013), no. 1, 92–138.
- [Ive73] B. Iversen, *Generic local structure of the morphisms in commutative algebra*, Lecture Notes in Math., vol. 310, Springer, New York, 1973.

- [Kun85] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston, 1985.
- [Lic90] T. M. Lickteig, *On semialgebraic decision complexity*, Technical Report TR-90-052, Int. Comput. Sci. Inst., Berkeley, 1990.
- [Mey97] B. Meyer, *Object-oriented software construction*, second ed., Prentice-Hall, Inc., Upper Saddle River, NJ, 1997.
- [Mum88] D. Mumford, *The red book of varieties and schemes*, 1st ed., Lecture Notes in Math., vol. 1358, Springer, New York, 1988.
- [Sha94] I. R. Shafarevich, *Basic algebraic geometry: Varieties in projective space*, Springer, Berlin Heidelberg New York, 1994.