Journal of Complexity 34 (2016) 1–29

Contents lists available at ScienceDirect

Journal of Complexity

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

Quiz games as a model for information hiding☆

Bernd Bank [a], Joos Heintz [b,c,*], Guillermo Matera [c,d], José Luis Montaña [e], Luis M. Pardo [e], Andrés Rojas Paredes [b]

[a] *Humboldt-Universität zu Berlin, Institut für Mathematik, 10099 Berlin, Germany*

[b] *Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Univ., Pab. I, 1428 Buenos Aires, Argentina*

[c] *National Council of Science and Technology (CONICET), Argentina*

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

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

ARTICLE INFO

Article history:
Received 1 August 2015
Accepted 16 November 2015
Available online 2 December 2015

Keywords:
Quiz game
Lower complexity bound
Interpolation problem
Elimination problem
Neural network
Geometrically robust constructible map

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

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

* Corresponding author at: Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Univ., Pab. I, 1428 Buenos Aires, Argentina.

E-mail addresses: bank@mathematik.hu-berlin.de (B. Bank), joos@dc.uba.ar (J. Heintz), gmatera@ungs.edu.ar (G. Matera), joseluis.montana@unican.es (J.L. Montaña), luis.m.pardo@gmail.com (L.M. Pardo), arojas@dc.uba.ar (A. Rojas Paredes).

http://dx.doi.org/10.1016/j.jco.2015.11.005
0885-064X/

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, 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 [6,12]. 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 it 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 [4,15,18,19]. In Section 2.2 we introduce the notions and definitions which constitute the fundamental tool for our algorithmic model. Most of these notions and their definitions are taken from [6,12].

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