Journal of Complexity 28 (2012) 489–517

Contents lists available at SciVerse ScienceDirect

Journal of Complexity

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

Bilinear complexity of algebras and the Chudnovsky–Chudnovsky interpolation method

Hugues Randriambololona

École nationale supérieure des télécommunications ("Telecom ParisTech") & LTCI CNRS UMR 5141, 46 rue Barrault, 75634 Paris cedex 13, France

ARTICLE INFO

Article history:
Received 2 August 2011
Accepted 8 February 2012
Available online 25 February 2012

Keywords:
Interpolation
Non-special divisors
Algebraic curves
Finite fields
Tensor rank
Multiplication algorithm

ABSTRACT

We give new improvements to the Chudnovsky–Chudnovsky method that provides upper bounds on the bilinear complexity of multiplication in extensions of finite fields through interpolation on algebraic curves. Our approach features three independent key ingredients.

- We allow asymmetry in the interpolation procedure. This allows to prove, via the usual cardinality argument, the existence of auxiliary divisors needed for the bounds, up to optimal degree.
- We give an alternative proof for the existence of these auxiliary divisors, which is constructive, and works also in the symmetric case, although it requires the curves to have sufficiently many points.
- We allow the method to deal not only with extensions of finite fields, but more generally with monogeneous algebras over finite fields. This leads to sharper bounds, and is designed also to combine well with base field descent arguments in case the curves do not have sufficiently many points.

As a main application of these techniques, we fix errors in, improve, and generalize, previous works of Shparlinski–Tsfasman–Vladut, Ballet, and Cenk–Özbudak. Besides, generalities on interpolation systems, as well as on symmetric and asymmetric bilinear complexities, are also discussed.

Contents

E-mail address: hugues.randriambololona@telecom-paristech.fr.

0885-064X/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2012.02.005

0. Introduction

The bilinear complexity $\mu(\mathcal{A}/K)$ of a finite-dimensional algebra $\mathcal{A}$ over a field K measures the essential minimal number of two-variable multiplications in K needed to perform a multiplication in $\mathcal{A}$, and considering other operations, such as multiplication by a constant, as having no cost. More intrinsically, it can be defined as the rank of the tensor in

$$\mathcal{A} \otimes \mathcal{A}^\vee \otimes \mathcal{A}^\vee \tag{1}$$

naturally deduced from the multiplication map in $\mathcal{A}$.

The study of $\mu(\mathcal{A}/K)$, and the effective derivation of multiplication algorithms, are of both theoretical and practical importance. Pioneering works in this field are Karatsuba's algorithm [23] for integer and polynomial multiplication, and Strassen's algorithm [33] for matrix multiplication.

There are (at least) two ways in which these questions could be addressed from an algebraic geometry point of view. These two approaches are seemingly unrelated, although, to the author's knowledge, possible links between the two have never been seriously studied (nor will they be here). The first one is to consider tensors of rank 1 as defining points of a certain Segre variety, and tensors of higher rank, points of its successive secant varieties. This leads to deep and beautiful problems [35,24], but we will not be interested in this approach here. The second one is through the theory of interpolation. Karatsuba's algorithm may be interpreted as follows: evaluate the polynomials at the points $0, 1, \infty$ of the projective line, multiply these values locally, and interpolate the results to reconstruct the product polynomial. Replacing the line with algebraic curves of higher genus allowed Chudnovsky and Chudnovsky in [17] to first prove that the bilinear complexity of multiplication in certain extensions of finite fields grows at most linearly with the degree. For example, letting $\mu_q(n) = \mu(\mathbb{F}_{q^n}/\mathbb{F}_q)$, their result implies

$$\liminf_{n\to\infty} \frac{1}{n}\mu_q(n) \leq 2\left(1 + \frac{1}{\sqrt{q}-3}\right) \tag{2}$$

for $q \geq 25$ a square.

Several improvements and variants of the Chudnovsky–Chudnovsky algorithm were then proposed by various authors in order to give sharper or more general asymptotic, as well as non-asymptotic, upper bounds. Roughly speaking, they all rely on the following three ingredients:

(a) A "generic" interpolation process which explains how to derive these upper bounds from the existence, postulated a priori, of certain geometric objects. These objects are:
(b) Algebraic curves having "good" parameters, meaning, most of the time, that they have sufficiently many points of various degrees, and controlled genus.
(c) Divisors on these curves, such that certain evaluation maps associated to them are injective or surjective. Often this can be reformulated as requiring the existence of systems of simultaneously zero-dimensional or non-special divisors of a certain form and appropriate degree.

These three points are important. However remark that a well-designed algorithm in (a) should make the existence of the objects (b) and (c) it needs easier to check. In this paper we will give new contributions to (a), and also to (c), and then proceed to some direct, but hopefully already significant, applications (further applications could be given, but they require combination with quite different methods, so they will be treated elsewhere).