Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method

Hugues Randriambololona

(Submitted on 1 Jul 2011 (v1), last revised 16 Mar 2012 (this version, v5))

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:
(1) 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.
(2) 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.
(3) We allow the method to deal not only with extensions of finite fields, but more generally with monogenous 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-Ozbudak. Besides, generalities on interpolation systems, as well as on symmetric and asymmetric bilinear complexity, are also discussed.

Comments: 40 pages; difference with previous version: modified Lemma 5.6
Subjects: **Computational Complexity (cs.CC)**; Algebraic Geometry (math.AG)
Cite as: **arXiv:1107.0336 [cs.CC]**
(or **arXiv:1107.0336v5 [cs.CC]** for this version)

Submission history

From: Hugues Randriam [view email]
[v1] Fri, 1 Jul 2011 20:57:31 GMT (40kb)
[v2] Mon, 1 Aug 2011 15:09:32 GMT (32kb)
[v3] Tue, 2 Aug 2011 15:57:55 GMT (31kb)
[v4] Fri, 13 Jan 2012 19:05:45 GMT (33kb)
[v5] Fri, 16 Mar 2012 13:47:09 GMT (34kb)

Which authors of this paper are endorsers?