Polynomial construction of Chudnovsky-type algorithms with a linear bilinear complexity

Bastien Pacifico
Aix-Marseille Université

Abstract

Chudnovsky-type algorithms for the multiplication in finite extensions of finite fields are well-known for having a good bilinear complexity, both asymptotically and at finite distance. More precisely, for every degree n of the extension, the existence of a family of algorithms with linear bilinear complexity in n has been proved using the original method applied to an explicit recursive tower of function fields. However, there is currently no method to build these algorithms in polynomial time. Nevertheless, one can construct in polynomial time a Chudnovsky-type algorithm over the projective line for the multiplication in any extension degree, with a quasi-linear bilinear complexity. In this talk, we show that one can obtain algorithms both constructible in polynomial time and having a linear bilinear complexity by mixing up these two strategies.