Factors of Polynomials of Low Individual Degree

Rafael Oliveira
Princeton University
12/9/2015 at 11:00 am
CoRE 431

Abstract

In [kal89], Kaltofen proved the remarkable fact that multivariate polynomial factorization can be done efficiently, in randomized polynomial time. Still, more than twenty years after Kaltofen’s work, many questions remain unanswered regarding the complexity aspects of polynomial factorization, such as the question of whether factors of polynomials efficiently computed by arithmetic formulas also have small arithmetic formulas, asked in [KSS14], and the question of bounding the depth of the circuits computing the factors of a polynomial. We are able to answer these questions in the affirmative for the interesting class of polynomials of bounded individual degrees, which contains polynomials such as the determinant and the permanent. This partially answers the question above posed in [KSS14], who asked if this result holds without the dependence on the individual degree. Along the way, we introduce several new technical ideas that could be of independent interest when studying arithmetic circuits (or formulas). In this talk, we will give a brief survey of polynomial factorization and its relations to arithmetic complexity, and give an overview of the ideas used in the proof of our main result.

Organizer(s): Eric Allender, Michael Saks and Mario Szegedy