Title: Fast Multivariate Multipoint Evaluation over Finite Fields

Abstract:

Multivariate multipoint evaluation is the problem of evaluating a multivariate polynomial, given as a coefficient vector, simultaneously at multiple evaluation points. The straightforward algorithm for this problem is to iteratively evaluate the input polynomial at each input point. The question of obtaining faster-than-naive (ideally, linear time) algorithms for this problem is a natural and fundamental question in computational algebra. Besides, fast algorithms for this problem are closely related to fast algorithms for other natural algebraic questions like polynomial factorization and modular composition.

Nearly linear time algorithms have been known for the univariate instance of multipoint evaluation for close to five decades due to the work of Borodin and Moenck. However, fast algorithms for the multivariate version have been much harder to come by. In a significant improvement to the state of art for this problem, Umans in 2008 and Kedlaya-Umans in 2011 gave nearly linear time algorithms for this problem over field of small characteristic and over all finite fields respectively, provided that the number of variables m is at most d^{o(1)} where the degree of the input polynomial in every variable is less than d. They also stated the question of designing fast algorithms for the large variable case as an open problem.

In this talk, we present two new algorithms for this problem. The first one is a nearly linear time (algebraic) algorithm for not-too-large fields of small characteristics. For the large variable case, this is the first nearly linear time algorithm for this problem over any large enough field. The second gives a nearly linear time (non-algebraic) algorithm over all finite fields.

The talk is based on joint work with Vishwas Bhargava, Zeyu Guo, Mrinal Kumar, Chandra Kanta Mohapatra, and Chris Umans.