Beating binary powering for computing the Nth power

(Talk for JNCF23 at CIRM)

Sergey Yurkevich

March 7, 2023

Summary of the talk

The Nth power of a polynomial matrix of fixed size and degree can be computed by binary powering as fast as multiplying two polynomials of linear degree in N. When Fast Fourier Transform (FFT) is available, the resulting arithmetic complexity is *softly linear* in N, i.e. linear in N with extra logarithmic factors.

In this talk I show that it is possible to beat binary powering, by an algorithm whose complexity is *purely linear* in N, even in absence of FFT. The key result making this improvement possible is that the entries of the Nth power of a polynomial matrix satisfy linear differential equations with polynomial coefficients whose orders and degrees are independent of N.

I will also show similar algorithms for two related problems: computing the Nth term of a C-recursive sequence of polynomials, for example the Nth Fibonacci polynomial, and modular exponentiation to the power N for bivariate polynomials.

The talk is based on joint work with Alin Bostan and Vincent Neiger.