GUILLERMO MATERA, Universidad Nacional de General Sarmiento and CONICET, Argentina
On the bit complexity of polynomial system solving

We describe a probabilistic algorithm which solves a polynomial system over the rationals defined by a reduced regular sequence. Its bit complexity is roughly quadratic in the Bézout number of the system and linear in its bit size. Our algorithm solves the input system modulo a prime number p and applies p-adic lifting. Our approach is based on a new result on the bit length of a "lucky" prime p, namely one for which the reduction of the input system modulo p preserves certain fundamental geometric and algebraic properties of the original system. These results rely on the analysis of Chow forms associated to the set of solutions of the input system and effective arithmetic Nullstellensätze. Joint work with Nardo Giménez.