

Shallow circuits with high-powered inputs

Pascal Koiran, Ecole Normale Supérieure de Lyon

A polynomial identity testing algorithm must determine whether an input polynomial (given for instance by an arithmetic circuit) is identically equal to 0. Following Kabanets and Impagliazzo (2004), it has become increasingly clear in recent years that efficient deterministic algorithms for polynomial identity testing would imply strong lower bounds (the connection between arithmetic circuit lower bounds and derandomization of polynomial identity testing was foreshadowed in a 30 years old paper by Heintz and Schnorr). This approach to lower bounds was advocated in particular by Agrawal (2005). In my talk I will present some further results on univariate polynomial identity testing. I will propose a real version of the tau-conjecture of Shub and Smale on integer roots of univariate polynomials. The real tau conjecture implies a superpolynomial lower bound on the arithmetic complexity of the permanent polynomial. This result was presented at ICS 2011. If time permits, I will also present some additional results and in particular an unconditional lower bound for the size of a restricted class of arithmetic circuits computing the permanent.