LOWER BOUNDS FOR DIOPHANTINE APPROXIMATIONS

M. Giusti, K.Hägele, J. Heintz, J.E. Morais, J.L. Montaña, L.M. Pardo

June 18, 1996

Abstract

We introduce an algorithm for geometric solving of multivariate polynomial equation systems whose bit complexity depends only on *intrinsic geometric invariants* of the solution set. By "intrinsic" we mean algorithms that can distinguish between the possibly good semantical interpretation and the syntactical description of the input system in order to improve complexity estimates.

¿From this, we derive an algorithm to decide the consistency of polynomial equation systems whose bit complexity is of similar magnitude. Concerning bit complexity we show how the time is related to the affine degree and the (affine) logarithmic height of the corresponding diophantine variety. In this sense, [2] and [3] show that the (affine) degree of an input system is associated with the complexity when measured in terms of number of arithmetic operations. However, there are some drawbacks in this approach.

The first one is that the algorithms developed in [2] and [3] require some intermediate algebraic numbers: these algorithms are not "rational". A second drawback concerns the modeling used to measure complexity. The number of arithmetic operations is not enough to explain the behavior of "real life" computers when running an algorithm.

Both aspects are treated in this talk. First, the algorithm we present here is purely rational. It does not require constants other than those in the field of coefficients of the input system. The second aspect (bit complexity) is realized by introducing a notion of height of affine diophantine varieties which is inspired by the notions introduced for projective varieties (cf.[1], [4], [5], [7], [8],[9],[10]) and is related to the bit complexity of the procedures.

This notion of height combined with an efficient use of the trace yields some new intrinsic Liouville estimates. Liouville estimates are applied to obtain lower time bounds for the numerical analysis approach to solving systems of polynomial equations. In particular, we show the inefficiency of both floating point and binary encoding for obtaining approximations of zeroes of multivariate polynomial equations.

As techniques within the context of straight–line programs, we give a version of a symbolic adaptation of the Newton Operator for lifting varieties from a 0-dimensional fiber and a new version of the Trace Formula for Gorenstein algebras which does not depend on any monomial basis.