ON THE INTRACTABILITY OF HILBERT'S NULLSTELLENSATZ AND AN ALGEBRAIC VERSION OF "$NP \neq P$?"

MICHAEL SHUB AND STEVE SMALE

Section 1. Introduction. In this paper, we relate an elementary problem in number theory to the intractability of deciding whether an algebraic set defined over the complex numbers (or any algebraically closed field of characteristic zero) is empty.

More precisely, we first conjecture: The Hilbert nullstellensatz is intractable. The Hilbert nullstellensatz is formulated as a decision problem as follows.

Given $f_1, \ldots, f_\ell$: $\mathbf{C}^n \to \mathbf{C}$, and complex polynomials of degree d_i, $i = 1, \ldots, \ell$, decide if there is a $z \in \mathbf{C}^m$ such that $f_i(z) = 0$ for all i.

There is an algorithm for accomplishing this task. From Hilbert, the answer is no if and only if there are polynomials g_i: $\mathbf{C}^m \to \mathbf{C}$, $i = 1, \ldots, \ell$ with the property

$$(*) \qquad \sum_{i=1}^{\ell} g_i f_i = 1 .$$

Brownawell [2] has made the most decisive next step by finding a good bound on the degrees of these g_i. With that, one may decide if (*) has a solution by linear algebra, since (*) is a finite-dimensional linear system with the g_i's as unknowns. This procedure is called the "effective nullstellensatz."

To say what "intractable" means in our conjecture, it is necessary to have a formal definition of algorithm in this context. That is done in Blum-Shub-Smale [1]. In that paper, algebraic algorithms (called algorithms over $\mathbf{C}$) are described in terms of "machines," which make arithmetical computations and branch according to whether a variable (the first state variable) is zero or not.

In [1], furthermore, one has the concept of a polynomial time algorithm, in particular, a polynomial time decision algorithm over $\mathbf{C}$. This may be expressed in the present setting as

$$T(f) \leqslant s(f)^c \qquad (\text{the } c \text{ power of } s(f) \text{ all } f).$$

Here $f = (f_1, \ldots, f_\ell)$ is the input, $T(f)$ is the number of operations (arithmetic, branching) used to accomplish the decision, and $s(f)$ is the total number of coeffi-

Received 26 May 1994.

The authors were partially supported by National Science Foundation grants. The work was carried out at Instituto de Matemática Pura e Aplicada, Rio de Janeiro.