ON THE CARDINALITY OF A SEMI-ALGEBRAIC SET

G. KHMISHIAVILI

ABSTRACT. It is shown that the cardinality of a finite semi-algebraic subset over a real closed field can be computed in terms of signatures of effectively constructed quadratic forms.

1. The problem under consideration may be described as follows. Let $X$ be a semi-algebraic set over an ordered field $K$ [1]

$$X = \{f_i = 0, g_j > 0; \ i \in I, \ j \in J\} \subset K^n,$$

where $I$ and $J$ are some finite sets of indices, and suppose we are a priori guaranteed that $X$ is finite (e.g., it is a part of the zero-set of a non-degenerate polynomial endomorphism). Now the problem is how to estimate its cardinality in some reasonable way without solving any equations.

More formally, there are given $f_i, g_j$ belonging to the ring $K_n$ of polynomials in $n$ variables with coefficients from $K$ and we want to find effectively (by means of some algebraic operations over coefficients of these polynomials) the cardinality $\# X$, i.e., the number of elements in $X$ (geometrically distinct or counted with the multiplicities).

Similar problems for the case where $K = \mathbb{R}$ is the usual field of reals often arise in applications [2] and they are well studied [3]. We will show below that a number of general results may be formulated in terms which are valid in the context of real closed fields. We will not treat the problem in full even for reals, preferring to exclude various possible degenerations. In fact, the cases considered below are principal in the sense that most of the reasonable situations may be reduced to them.

From now on we always suppose $K$ to be a real closed field and all points of $X$ to be simple in the sense of the algebraic geometry (i.e., having multiplicity $1$). Thus we are going to deal, in fact, with the number of geometrically distinct points.

1991 Mathematics Subject Classification. 14G30, 58C27.
We will consider two important cases: when $X$ is the zero-set of a non-degenerate endomorphism (i.e., $\#I = n$ and $f_i$ define a proper endomorphism of $\overline{K}^n$, where $\overline{K} = K(\sqrt{-1})$ is the algebraic closure of $K$), and when one has no inequalities (i.e., $J = \emptyset$).

In the first case the solution may be obtained by means of a suitable modification of the classical signature method going back to Hermite and Jacobi [3] which was outlined in [4] and then thoroughly studied in the Candidate Dissertation of T. Aliashvili for the field of reals (see [5]). The proposed generalization is based on the existence of a purely algebraic definition of the Grothendieck residue symbol [6].

The same approach is also valid in the second case, but better results may be obtained by means of the more sophisticated algebraical tools used by G. Khimshiashvili [7] and by D. Eisenbud and H. Levine [8], and developed later in [9] and [10]. This enables us to get rid of the multiplicity-one assumption, which seems impossible in the framework of the signature method.

In fact, some other approaches, e.g., the so-called Newton polygon method developed in the works of A. G. Khovansky [11], are possible, but the author has never seen any published results of that kind. Moreover, it seems that the named method does not in principle enable one to consider the case where inequalities are really present in the definition of $X$.

2. Consider now a set $X$ of the type (1) and let $f_j$ define a nondegenerate polynomial endomorphism $\bar{f}: \overline{K}^n \to \overline{K}^n$ with simple roots. Nondegeneracy here means as usual the absence of “roots at infinity,” that is, the “leaders” (homogeneous forms of the highest degree $\deg f_i$) $f_i^*$ have no nontrivial common roots in $\overline{K}^n$ [2] (for $K = \mathbb{R}$ this is equivalent to $f$ being proper).

The Bezout theorem for real closed fields [12] implies that $\bar{f}$ has exactly $N = \prod \deg f_j$ roots in $\overline{K}^n$ so that we have $\bar{f}^{-1}(0) = \{z_0, z_1, \ldots, z_{N-1}\}$ with $z_i \neq z_j$ for $i \neq j$.

Without loss of generality we may assume that the first coordinates of the roots are pairwise distinct and in such a case we say that the endomorphism is separable. This condition may always be verified effectively in terms of resultants, and one can always reduce the problem to this case by performing at most $N(N - 1)/2$ rotations of the coordinate system.

Write now every root in the form $z_j = (u_j, z'_j)$ with the first coordinate singled out and introduce an auxiliary quadratic form on $\mathbb{K}^N$ which depends on an arbitrary $g \in K_n$:

$$Q^g_j(\xi) = \sum_{j=0}^{N-1} g(z_j)(\xi_0 + u_j \xi_1 + \cdots + u_j^{N-1} \xi_{N-1})^2.$$ (2)

It is easy to verify that all coefficients of this form belong to $K$ because here we have a complete analogy with the case of reals. More precisely, the