

ON THE CARDINALITY OF A SEMI-ALGEBRAIC SET

G. KHIMSHIASHVILI

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]

$$X = \{f_i = 0, g_j > 0; i \in I, j \in J\} \subset K^n, \quad (1)$$

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 when $K = \mathbb{R}$ 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, cases considered below are principal in the sense that most of 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 the 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 \bar{K}^n , where $\bar{K} = K(\sqrt{-1})$ 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 generalisation 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 more sophisticated algebraical tools used by G.Khimshiasvili [7], also 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 when 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 $\bar{f} : \bar{K}^n \rightarrow \bar{K}^n$ with simple roots. Nondegeneracy here means as usual the absence of "roots at the infinity", that is, the "leaders" (homogeneous forms of the highest degree $\deg f_i$) f_i^* have no nontrivial common roots in \bar{K}^n [2] (for $K = \mathbb{R}$ this is equivalent to \bar{f} being proper).

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

Without loss of generality we may assume that the first coordinates of 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 not more than $N(N-1)/2$ 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 K^N which depends on an arbitrary $g \in K_n$:

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

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

roots which do not belong to K^n appear in conjugated pairs with respect to the natural "complex conjugation" operation in \bar{K} , which implies the assertion.

Recall that one can define as usual the rank $\text{rk } Q_f^g$ and the signature $\text{sig } Q_f^g$ of the form Q_f^g [1].

The following result provides a multidimensional analogue of the Sturm algorithm [1] and enables one to solve the problem for $\#J = 1$, i.e. for domains of the type $\{g > 0\}$.

Theorem 1. *If $f : K^n \rightarrow K^n$ is a separable polynomial endomorphism over a real closed field K and $g \in K_n$, then the rank and signature of the form (2) satisfy the relations:*

$$N - \text{rk } Q_f^g = \#(f^{-1}(0) \cap g^{-1}(0)), \tag{3}$$

$$\text{sig } Q_f^g = \#[f^{-1}(0) \cap \{g > 0\}] - \#[f^{-1}(0) \cap \{g < 0\}]. \tag{4}$$

Denoting by Q_f the form (2) for $g \equiv 1$, we are able to derive some corollaries.

Corollary 1. *Under conditions of the theorem the form Q_f is nondegenerate and one has:*

$$\text{sig } Q_f = \#f^{-1}(0) \tag{5}$$

Corollary 2. *Under the same conditions for $X = f^{-1}(0) \cap \{g > 0\}$ one has:*

$$\#X = (\text{sig } Q_f + \text{sig } Q_f^g + \text{rk } Q_f^g - N)/2 \tag{6}$$

Using some simple combinatorics we may also increase the number of inequalities determining X .

Corollary 3. *If besides $f^{-1}(0) \cap g_j^{-1}(0) = \emptyset$ holds for every $j \in J$, then*

$$\#X = \left(\sum_{\alpha} \text{sig } Q_f^{\alpha} \right) / 2^{\#J},$$

where α runs through all multiindices of the form $\alpha = (\alpha_1, \dots, \alpha_k)$ with $1 \leq k \leq \#J$ and $\alpha_1 < \dots < \alpha_k$, and $Q_f^{\alpha} = Q_f^{g_{\alpha}}$ with $g_{\alpha} = g_{\alpha_1} \cdot \dots \cdot g_{\alpha_k}$.

For the sake of simplicity we have excluded here degenerations connected with the presence of roots on boundaries of domains $\{g_j > 0\}$.

Before presenting the proof of the theorem let us explain why it gives a solution of our problem. It suffices to show that coefficients of the form (2) may be computed by a finite sequence of rational operations over coefficients of f_j and g .

After trivial modifications of the formula (2) it is easy to see that the coefficients c_{ij} in the standard presentation of the form $Q_f^g(\xi) = \sum c_{ij} \xi_i \xi_j$

are expressed algebraically in terms of the so-called mixed Newton sums of roots

$$S_\alpha(f) = \sum_{j=0}^{N-1} (z_j^1)^{\alpha_1} \cdots (z_j^n)^{\alpha_n}, \quad (7)$$

where $\alpha \in (\mathbb{Z}_+)^n$, $z_j = (z_j^1, \dots, z_j^n)$, $j = 0, 1, \dots, N-1$.

In fact, certain sums S_α may be easily computed using iterated resultants. For example, this is so for small $|\alpha|$ and for "pure" Newton sums with only one nonzero α_j and this enables one already to provide the separation of roots, which was the original classical problem [3]. There are some hints in [3] about such a possibility but without any details and with a remark that this is not a universal method. For $n = 2$ the storage of easily computable Newton sums was described by T. Aliashvili who has also shown using the Hilbert theorem on invariants that all Newton sums may be computed algebraically in this case [4], [5]. Unfortunately, this approach is not constructive and it meets with serious difficulties for arbitrary n .

For $K = \mathbb{R}$ a radical tool for suppressing this difficulties is provided by an ingenious algebraic device called the Grothendieck residue symbol [6, 13]. It was shown in [7] and [8] how this residue serves to compute the topological degree of a smooth map-germ and so we naturally used it in our situation. In fact, here we need the global variant of this notion which was outlined in [6] and further investigated in [13].

For the sake of completeness we recall that the global residue of a polynomial $g \in \mathbb{R}_n$ with respect to a nondegenerate endomorphism $f \in (\mathbb{R}_n)^n$ is defined by the integral

$$\text{Res}_f g = \frac{1}{(2\pi i)^n} \int_{\Gamma_R} \frac{g(z)}{f_1(z) \cdots f_n(z)} d\mu, \quad (8)$$

where the cycle $\Gamma_R = \{z \in \mathbb{C}^n : |f_j(z)| = R \text{ for } j = 1, \dots, n\}$ is defined for sufficiently large $R > 0$, its orientation is induced by the differential form $d(\arg f_1) \wedge \cdots \wedge d(\arg f_n)$ and the integral is taken with respect to the usual Lebesgue measure.

This integral doesn't depend on R and vanishes on the ideal (f) generated by the components of f in \mathbb{R}_n [13]. Moreover, if all roots of f are simple, one has the relation

$$\text{Res}_f g = \sum_{z \in f^{-1}(0)} \frac{g(z)}{J_f(z)}, \quad (9)$$

where $J_f(z) = \det(\partial f_j / \partial z_k)(z)$ is the Jacobian of f .

Now it is clear that in the situation of Theorem 1 we have

$$S_\alpha(f) = \text{Res}_f (J_f e_\alpha), \quad (10)$$

where $\alpha \in (\mathbb{Z}_+)^n$, $e_\alpha = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ is a monomial in \mathbb{R}_n .

Consequently, it remains to show that $\text{Res}_f g$ itself can be computed by the coefficients of f and g . This circumstance should not seem strange because the global residue is the sum of local residues [13] and the latter are known to be algebraically computable but, of course, a technical difficulty arises here because we cannot assume the positions z_j of local residues are known.

Nevertheless, it turns out that the situation can be saved by means of a clever use of the transformation formula for global residues [13]. In fact, one may always reduce the problem to the case of the so-called "pure powers" $f_j = z_j^{k_j}$, where it is trivialized. The necessary transformation can be obtained from the so-called Hefer decomposition of polynomials f_j and all the procedures rise up to algorithms. We have no space here for presenting details which may be borrowed from [13], but for future generalizations it is important to notice that the main point was just the transformation formula. Thus we conclude that the Newton sums can be also computed algebraically, which gives a principal solution of our problem.

Now we observe that the same arguments can be used also for an arbitrary real closed field K because there exists a pure algebraic definition of the Grothendieck residue symbol [6] which generalizes (8) and possesses the same functorial properties.

As was already mentioned, a straightforward analysis of the residue computation in [13] shows that it uses, in fact, only the formal properties of residues and therefore also extends to the general case.

Thus we arrive to the following conclusion which complements Theorem 1 and completes the desired solution.

Theorem 2. *Under the conditions of Theorem 1 coefficients of the form Q_f^g may be algebraically expressed through coefficients of given polynomials.*

Now it is time to return to the proof of Theorem 1 which proceeds as follows. Write first $\bar{f}^{-1}(0)$ in the form $\bar{f}^{-1}(0) = \{x_1, \dots, x_r, z_1, \dots, z_k, \bar{z}_1, \dots, \bar{z}_k\}$, where $x_1, \dots, x_r \in K^n$, $z \notin K^n$, $r + 2k = N$, which is always possible in virtue of the observation following the formula (2).

Define now a linear transformation T in K^N by the formulas

$$\begin{cases} \eta_j = \xi_0 + \xi_1 u_j + \dots + \xi_{N-1} u_j^{N-1}, & j = 1, \dots, r; \\ \eta_{r+j} = \text{Re}(\xi_0 + \dots + \xi_{N-1} u_{r+j}^{N-1}), & j = 1, \dots, k; \\ \eta_{r+k+j} = \text{Im}(\xi_0 + \dots + \xi_{N-1} u_{r+j}^{N-1}), & j = 1, \dots, k. \end{cases}$$

Evidently, this transformation diagonalizes our form, this immediately implying (3) and (4). It remains to verify that this is a genuine change of coordinates, that is its determinant is nonzero. Anyone who is fond of linear algebra can easily compute it by reducing it to a Vandermonde of the first

coordinates which is nonzero due to the separability of f . Another way is to observe that the form Q_f becomes nondegenerate; hence $\text{rk} T \geq N$, which again finishes the proof. ■

All corollaries become immediate now. We have only to introduce numbers m_α of roots belonging to $U_\alpha = \cap\{g_{\alpha_k} > 0\}$ and to sum up all relations (4) for functions g_α , which terminates all the numbers m except the required $m_{1,\dots,n} = \#X$.

Turning again to the proof of Theorem 2 we shall also point out that there were two nearly equivalent possibilities of deducing the general case from the case of real numbers. Firstly, one can mimic the algorithm from [13] referring to the properties of the general notion from [6]. Secondly, one can directly define the global residue $\text{Res}_f g$ by the formula presented in [13], page 60, and verify that it possesses all necessary properties forcing it to coincide with the residue from [6].

In both cases details are routine and we have omitted them. In fact, the shortest though a little mistifying way is concerned with the Zaidenberg–Tarski principle [12], which makes all these troubles unnecessary as soon as a formula for Res_f is proven for reals so that the proof of our generalization becomes complete.

Nevertheless, we preferred to recall the analytical formula for the global residue having in mind an effective algorithm for dealing with the problem in practice, which is by no means available by the Zaidenberg–Tarski yoga.

A number of curious questions arise here. For example, one can try to estimate the computational complexity of corresponding algorithms and compare it with that of the cylindrical decomposition method from [14]. When $g = J_f$ and we are dealing with the topological degree of f necessary estimates were obtained by T. Aliashvili [5] and they witness in favour of the approach outlined above.

3. Let now X be an affine algebraic subset of K^n , that is a set of the type (1) with $J = \emptyset$. We are going to describe another solution of our problem also valid without assuming that all points of X are simple.

As is well known, every such subset may be represented as a hypersurface $X = \{F = 0\}$ with $F = f_1^2 + \dots + f_{\#I}^2$ so that we may assume that X is a hypersurface consisting of a finite number of points. At first glance such an object may seem unusual but the point is that for a hypersurface one can always compute its Euler characteristic in a pure algebraic form as in [7, 9, 10]. In our situation the Euler characteristic simply reduces to the number of geometrically distinct points so that we become able to give a very concise solution of our problem.

The discussion below can be adapted for arbitrary real closed fields, but this requires some caution and additional work so that we consider here only the case when $K = \mathbb{R}$.

Recall that we deal with the usual Euler characteristic $\chi(X)$ which is the alternated sum of homology groups ranks (Betti numbers) of a topological space X under consideration. We write $\deg_p f$ for the local degree of an endomorphism $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ in an isolated preimage of the origin $p \in f^{-1}(0)$ which is defined as the topological degree of a mapping $\hat{f} = f/\|f\| : S_\varepsilon^{n-1}(p) \rightarrow S_1^{n-1}(0) = S^{n-1}$.

All the results below are based on the following formulas obtained by the author in [7].

Theorem 3. *Let $F : \mathbb{R}^n \rightarrow \mathbb{R}$ be a polynomial with an isolated singularity at the origin. Then for a sufficiently small enough $\lambda > 0$ one has*

$$\chi(\{F < \lambda\} \cap B_\delta^n) = 1 + (-1)^{n-1} \deg_0(\text{grad } F), \tag{11}$$

where B_δ^n is a ball of the small radius δ .

If the polynomial F is homogeneous then for sufficiently small $\lambda, \delta > 0$ one has also the equality

$$\chi(\{F \geq 0\} \cap S_\delta^{n-1}) = 1 + (-1)^{n-1} \deg_0(\text{grad } F). \tag{12}$$

These results are local but there is a natural link with the global ones provided by the projectivization.

With this in mind, suppose that f_1, \dots, f_p are homogeneous polynomials of the degrees $d_1 \leq d_2 \leq \dots \leq d_p$, respectively. Then, besides X , they also define a projective algebraic variety V_f in \mathbb{RP}^{n-1} which can also be determined by a single homogeneous polynomial $f = \sum f_j^2 \cdot \|x\|^{2(d_p-d_j)}$ of the degree $2d_p$, where $\|x\|$ is the usual euclidean norm of $x \in \mathbb{R}^n$. Now it is not difficult to tie together the invariants of X with those of its projectivization using the following lemma established in [10].

Lemma. *Under these conditions for all $\lambda \neq 0$ the polynomial $F_\lambda = f^2 - \lambda^2(\sum x_j^{2d+2})$ has an isolated singularity at 0 and for a sufficiently small $|\lambda|$ the real hypersurface $\{F_\lambda = 0\}$ does not have singularities inside small balls and is transversal to their boundaries. Moreover, denoting $Z = \{x \in S_1^{n-1} : f(x) = 0\}$, $Z_\lambda = \{x \in S_1^{n-1} : F_\lambda(x) \leq 0\}$, one has that $Z_\lambda \setminus Z$ is diffeomorphic to $Y_\lambda \times (0, \lambda]$, where $Y_\lambda = \{x \in S_1^{n-1} : F_\lambda(x) = 0\}$.*

Collecting together these observations, we are able to obtain the final result.

Theorem 4. *Let $f_1, \dots, f_p \in \mathbb{R}_n$ be real polynomials of degrees not exceeding d . Suppose that they have only a finite number M of real common*

zeroes. Set

$$h_i(x_0, x_1, \dots, x_n) = x_0^{d+1} f_i(x_1/x_0, \dots, x_n/x_0),$$

$$H = \sum_{i=1}^p h_i^2 - \sum_{k=0}^n x_k^{2d+4}.$$

Then H has an algebraically isolated critical point at the origin and the following equality holds:

$$M = [(-1)^n - \deg_0(\text{grad } H)]/2. \quad (13)$$

Proof. Evidently, all polynomials h_j are homogeneous of the degree $d+1$, which enables us to transplant considerations on the unit sphere $S^n \subset \mathbb{R}^{n+1}$ and use the lemma.

With this purpose we introduce a subset $Y = S^n \cap \{h_1 = \dots = h_p = 0\}$ and observe that $Y = Y_+ \cup Y_- \cup S^{n-1}$ with $Y_{\pm} = \{x \in S^n : \pm x_0 > 0, h_1(x) = \dots = h_p(x) = 0\}$.

Evidently, Y_+ and Y_- are homeomorphic to X so that we obtain $\chi(Y) = 2\chi(X) - \chi(S^{n-1})$ or, equivalently, $\chi(X) = [\chi(Y) + \chi(S^{n-1})]/2$ and it remains to compute $\chi(Y)$, which is already possible using (11) for H .

Working with homology with integer coefficients, in virtue of the Lefschetz duality [2] we obtain

$$\begin{aligned} \chi(S \setminus Y) &= \sum (-1)^k \text{rk } H_k(S \setminus Y) = \sum (-1)^k \text{rk } H_{n-k-1}(S, Y) = \\ &= (-1)^{n+1} \chi(S, Y) = (-1)^{n+1} [\chi(S) - \chi(Y)] = \\ &= (-1)^n \chi(Y) + (-1)^{n+1} + 1. \end{aligned}$$

On the other hand, applying the lemma to H instead of F one gets $S \setminus Y = (S \cap \{F_{\lambda} \leq 0\}) \cup (S \cap \{F_{\lambda} \geq 0\})$.

The first set is fibred in virtue of the lemma and the second one cannot contain any points of Y because there we have $\sum x_j^{2d+4} > 0$. Consequently, we obtain

$$\begin{aligned} \chi(S \setminus Y) &= \chi(\{F_{\lambda} = 0\} \cap S) + \chi(\{F_{\lambda} \geq 0\} \cap S) - \chi(\{F_{\lambda} = 0\} \cap S) = \\ &= \chi(\{F_{\lambda} \geq 0\}) = 1 + (-1)^{n+1} \deg_0(\text{grad } F_{\lambda}). \end{aligned}$$

This naturally implies

$$\chi(Y) = (-1)^n [(-1)^n + (-1)^{n+1} \deg_0(\text{grad } F_{\lambda})] = 1 - \deg_0(\text{grad } F_{\lambda}).$$

Now, our lemma yields that the family F provides an admissible homotopy with $F_1 = H$ so that we may put $\lambda = 1$ and get $\chi(Y) = 1 - \deg_0(\text{grad } H)$, which immediately gives (13) and finishes the proof. \square

Granted formula (13) we have only to observe that the local topological degree is algebraically computable being, in fact, equal to the signature of an effectively constructible quadratic form on the coordinate algebra of a given mapping [7, 8]. Thus, we obtain another way of computing $\#X$, which turns out to be more convenient and effective than the method of §2.

One could now combine our results with those on algorithmic computation of the local degree in order to estimate the computational complexity of this method. We shall not pursue this topic here but rather make several remarks in conclusion.

An interesting open problem is to generalize all these things for arbitrary real closed fields. In fact, most of necessary algebraical and topological notions are also available in the general case. One has only to obtain a formula expressing the local Euler characteristic in terms of the local topological degree as in [7]. The author feels that a portion of the semi-algebraic topology in the spirit of [15] should be helpful here. One could also try to combine this with the discussion of real singularities in [16].

Some concrete results become more or less immediate now. For example, one can directly verify a result of R.Thom stating that the number of cusps of a stable smooth mapping from the real projective plane into real plane is always odd because such maps may be approximated by rational ones given by ratios of polynomials of even degrees for which the result follows directly from the formula (11). Perhaps, some other "oddity results" may be obtained in a similar manner.

One can also give a closed algebraical formula for the number of cusps of a polynomial Whitney mapping (stable mapping of \mathbb{R}^2 in itself) which complements recent results of K.Aoki and T.Fukuda [17] and provides sharp estimates for such numbers.

REFERENCES

1. S. Lang, Algebra. *Addison-Wesley, New York*, 1965.
2. I. Shafarevich, Foundations of Algebraic Geometry. (Russian) "*Nauka*", Moscow, 1972.
3. M. Krein and M. Neimark, Method of quadratic forms for separation of roots of polynomials. (Russian) "*GNTI*", Kharkov, 1936.
4. G. Khimshiashvili, On the number of zeroes of a real polynomial endomorphism. *Bull. Acad. Sci. Georgia*, **146**(1992), No.3, 469-473.
5. T. Aliashvili, On the topological degree of a polynomial endomorphism. (Russian) *Collection of works in the homology theory. 6. (Russian) Trudy Tbiliss. Mat. Inst. Razmadze* **103**, to appear.
6. R. Hartshorne, Residues and Duality. *Lect. Notes Math.***11**, Springer, Berlin etc., 1971.

7. G. Khimshiashvili, On the local degree of a smooth mapping. (Russian) *Soobsch. Akad. Nauk Gruzin. SSR* **85**(1977), No.2, 27-30.
8. D. Eisenbud and H. Levine, An algebraic formula for the degree of a smooth map-germ. *Ann. Math.* **106**(1977), No.1, 64-79.
9. Z. Szafraniec, On the Euler characteristics of real algebraic varieties. *Topology*, **25**(1986), No.3, 253-259.
10. J. Bruce, The Euler characteristic of a real affine algebraic variety. *Bull. Lond. Math. Soc.* **22**(1990), No.4, 213-219.
11. A. Khovansky, Newton polyedra. (Russian) *Current problems in mathematics. Fundamental directions, vol. 36 (Russian)*, 75-110, *Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuzn. Inst. Nauchn. i Tekh. Inform., Moscow*, 1990.
12. J. Bochnak, J. Cost and M.-F. Roy, *Geometrie Algébrique Réelle. Springer, Berlin etc.*, 1988.
13. A. Tsikh, Multidimensional residues and their applications. (Russian) "*Nauka*", *Novosibirsk*, 1988.
14. J. Davenport, Y. Siret and E. Tournier, *Calcul formel. Masson, Paris*, 1987.
15. H. Delfs and M. Knebusch, Algebraic varieties over real closed fields. *Lect. Notes Math.* **1173**, *Springer, Berlin etc.*, 1985.
16. J. Milnor, Singular points of complex hypersurfaces. *Princeton Lecture Notes, Princeton*, 1967.
17. K. Aoki and T. Fukuda, On the number of branches of zero loci. *Top. and Comp. Sci.* **3**(1987), 347-363.

(Received 15.01.1993)

Author's address:
A.Razmadze Mathematical Institute
Georgian Academy of Sciences
1, Z.Rukhadze St., 380093 Tbilisi
Republic of Georgia