Math. Ann. 283, 203–209 (1989)

Mathematische Annalen

A Measure for Semialgebraic Sets Related to Boolean Complexity

Gilbert Stengle

Department of Mathematics, Lehigh University, Bethlehem, PA 18015, USA

1. Introduction and Basic Definitions

Let X be a real affine or spherical semialgebraic set over a real closed field R. By spherical set we mean a subset of the manifold of the rays through the origin in the affine space R^{N+1}, or equivalently a subset of $R^{N+1}\backslash\{0\}/R^+$, defined by homogeneous polynomial relations. It is clear that in this latter space, using equivalence by positive homogeneity, we can define semialgebraic sets by systems of homogeneous polynomial equations and inequalities just as we define projective varieties by systems of homogeneous equations. Spherical geometry enjoys advantages not to be found in affine or projective spaces and in this paper we will show, using natural mappings between spherical and affine spaces, how it can be applied to affine geometry as well. As an application (Proposition 5.1 below) we demonstrate lower bounds for the number of inequalities necessary to define certain affine semialgebraic sets. Our key ingredients are a coarse, highly structured measure for the complexity of affine or spherical semialgebraic sets, a complexity reducing operator for spherical sets, and several complexity-monotonic mappings between spherical and affine spaces.

We introduce our complexity measure and an associated filtered algebraic structure for semialgebraic subsets of X in the following sequence of definitions.

Definition 1.1. Let X be a semialgebraic set. Let $(\gamma(X), +, \cdot)$ be the Boolean algebra of all semialgebraic subsets of X equipped with the operations $Y_1+Y_2=(Y_1 \cup Y_2)\backslash(Y_1 \cap Y_2)$ and $Y_1 \cdot Y_2 = Y_1 \cap Y_2$.

This has the structure of a Z_2-algebra well known in measure theory (see Halmos [H]) in which addition is symmetric difference, ϕ is the additive identity and X is the multiplicative identity. For the moment it merely expresses the Boolean structure of $\gamma(X)$ in an alternate notation.

Definition 1.2. Let X be an affine (spherical) semialgebraic set. Let $\mathbb{U}(X)$ be the collection of all principal basic open subsets of X of the form $U=\{g>0\}\cap X$ where g is a polynomial (homogeneous polynomial).

Since the collection $\mathbb{U}(X)$ generates $\gamma(X)$ as a ring, any semialgebraic subset Y of X can be represented as a polynomial in the elements of $\mathbb{U}$. In terms of these representations one can define various measures of the complexity of Y: the minimum number of generators, the miniumum multiplicative or additive complexity among all polynomials representing Y, and so forth. From among these we choose a less obvious notion which, as we will show, is well suited to the semialgebraic category.

Definition 1.3. Let γ_0 be the subring of $\gamma=\gamma(X)$ generated by the algebraic subsets of X.

Obviously $\gamma=\gamma_0[\mathbb{U}]$, that is, every semialgebraic set can be written as a polynomial P in $\gamma_0[\mathbb{U}]$. This allows the following notion of complexity.

Definition 1.4. For $S\in\gamma$ let $\kappa(S)$, the complexity of S, be the minimum total degree of any polynomial representing S as an element of $\gamma_0[\mathbb{U}]$. Let γ_k be the γ_0-module of semialgebraic subsets of X of complexity not exceeding k. For $k<0$ let γ_k be the trivial ring $\{X,\phi\}$.

Thus the lowest level of complexity, complexity 0 in our scale, is represented by sets requiring for their definition, in addition to the defining relations of X, only equations or inequations but no true inequalities.

The author is indebted to Ludwig Bröcker for reading a preliminary version of this paper and suggesting many improvements.

2. Elementary Properties of Complexity

Lemma 2.1. *For Y, Z, $W\in\gamma(X)$*

1. $\kappa(Y^c)=\kappa(Y)$,
2. $\kappa(YZ)\leqq\kappa(Y)+\kappa(Z)$,
3. $\kappa(Y\cup Z)\leqq\kappa(Y)+\kappa(Z)$,
4. *If* $Y\cap Z=\phi$, *then* $\kappa(Y\cup Z)\leqq\max\{\kappa(Y),\kappa(Z)\}$ *and if* $\kappa(Y)\neq\kappa(Z)$, *then equality holds,*
5. $\kappa(Y)=0 \Leftrightarrow Y\in\gamma_0$,
6. *W algebraic* $\Rightarrow \kappa(WY)\leqq\kappa(Y)$.

Proof. 1. Since $Y^c=Y+X$, if P represents Y, then $P+X$ is a polynomial of the same degree representing Y^c.

2. An obvious property of the total degree of a polynomial over any ring.

3. This follows from 1 and 2 by DeMorgan's law.

4. If $Y\cap Z=\phi$ then $Y\cup Z=Y+Z$ and the inequality again expresses an obvious property of total degree of a polynomial. If inequality holds, say $\kappa(Y)=k$ but $\kappa(Z)<k$, then $Y+Z\in\gamma_{k-1}$ implies $Y=Y+Z+Z\in\gamma_{k-1}$, a contradiction.

5 and 6 follow directly from the definitions.

A few examples illustrate the character of the function κ.

Example 2.2. In R^3 let $Y=\{x_1^2+x_2^2+x_3^2<1\}\backslash\{x_1>0,\ x_2>0,\ x_3=0\}$. Then $\kappa(Y)=2$. But $\kappa(\{x_1^2+x_2^2+x_3^2\leqq 1\})=1$.

This example shows that complexity is not a generic property. It also shows that the operation of topological closure can reduce complexity. On the other hand it can easily happen that a set consists of disjoint pieces of low complexity, the closures of which intersect in a more complicated way, so that its topological closure has greater complexity.

Example 2.3. In R^3 let $Y=\{x_3 \neq 0\}\{x_1>0\}+\{x_3=0\}\{x_2>0\}$. Then

$$\{x_3=0\}\bar{Y}=\{x_3=0\}[\{x_1 \geqq 0\} \cup \{x_2 \geqq 0\}]=\{x_3=0\}+\{x_3=0\}\{x_1<0\}\{x_2<0\}$$

which has complexity 2. Hence, by Lemma 2.1.6, $\kappa(\bar{Y}) \geqq 2 > 1 = \kappa(Y)$.

Proposition 2.4. *For* $Y \in \gamma(R^N)(\gamma(S^N))$, $\kappa(Y) \leqq \dim(Y)\,(\dim(Y)+1)$.

Proof. By induction on $d=\dim(Y)$. If $d=0$ the conclusion is true in the affine case. However in the spherical case the estimate $\kappa(Y) \leqq 1$ cannot be improved since, even if $N=0$, we still need one inequality to separate a point from its antipode. More generally, since the decomposition $Y=Y\{x_0>0\}+Y\{x_0<0\}+Y\{x_0=0\}$ represents any Y by summands, the first two of which can be identified with affine sets and a third which is a subset of S^{N-1}, it follows by induction on N that the asserted affine estimate implies the spherical. If Y is affine it follows by results of Bröcker [B1] [B2] using the abstract theory of the stability index that Y is generically a disjoint union of basic open sets defined by no more than d inequalities. That is, there is an algebraic subset W of dimension less than d such that $\kappa(YW^c) \leqq d$. Applying Lemma 2.1 and the induction hypothesis to the decomposition $Y=YW+YW^c$ completes the proof.

Corollary 2.5. *If X is affine then the ascending sequence $\gamma_k(X)$, $k=0,1,2,\ldots$ gives a filtration of $\gamma(X)$ of length no greater than* $\dim(X)$.

3. An Operation Which Reduces Complexity

Definition 3.1. Let ϱ denote the involution $x \to -x$ of S^N. Let X be a ϱ-invariant semialgebraic set. Denote the operation induced on $\gamma(X)$ by $Y \to Y^\varrho$. Define $\delta: \gamma(X) \to \gamma(X)$ by $\delta Y = Y + Y^\varrho$.

From now on we will assume, unless we specify otherwise, that X is a ϱ-invariant subset of S^N.

It is plain from our definitions that $\kappa(\delta Y) \leqq \kappa(Y)$. Moreover it is easy to see that the raw number of Boolean operations needed to define a set is, in general, not reduced by the action of δ. However the following proposition shows that our complexity is strictly reduced by this action. We note that ϱ also acts on R^N but seems not to enjoy any useful properties there. Thus this proposition depends critically upon using spherical rather than affine geometry and upon using our complexity measure.

Proposition 3.2. 1. $\delta^2=\phi$.
2. $\delta\gamma_k(X) \subset \gamma_{k-1}(X)$.

Proof. 1. $\delta^2 Y = Y + Y^\varrho + (Y+Y^\varrho)^\varrho = Y + Y + Y^\varrho + Y^\varrho = \phi$.

2. By induction on k. For $k=0$ any element Y of γ_0 is ϱ-invariant and $\delta Y = Y + Y = \phi \in \gamma_{-1}$. For $k>0$, since δ is an γ_0-homomorphism of modules, it suffices to establish the property for basic open sets defined by k inequalities. Any such set has the form $Y = Z\{g>0\}$ where $Z \in \gamma_{k-1}$. If g is an even form then $\delta Y = \{g>0\}(Z+Z^\varrho\}$ which, by induction hypothesis, belongs to $\{g>0\}\gamma_{k-2} \subset \gamma_{k-1}$. If g is an odd form then

$$\{g>0\}^\varrho = \{g<0\} = X + \{g>0\} + \{g=0\}$$

and

$$\begin{aligned}\delta Y &= Z\{g>0\} + YZ^\varrho[X + \{g>0) + \{g=0\}] \\ &= \{g>0\}(Z+Z^\varrho) + Z^\varrho X + Z^\varrho\{g=0\}.\end{aligned}$$

Again by induction hypothesis this implies

$$\delta Y \subset \gamma_1\gamma_{k-2} + \gamma_{k-1}\gamma_0 + \gamma_{k-1}\gamma_0 \subset \gamma_{k-1}.$$

Remark 3.3. Let $h(X)$ be the length of the filtration $[\gamma_k(X)]$ of $\gamma(X)$. Then the sequence

$$\phi \hookrightarrow \delta\gamma_h \hookrightarrow \gamma_h \xrightarrow{\delta} \gamma_{h-1} \xrightarrow{\delta} \dots \xrightarrow{\delta} \gamma_0 \xrightarrow{\delta} \phi$$

(3.1) forms a complex.

Proposition 3.4. *The sequence* (3.1) *is exact.*

Proof. By induction on the dimension N of the ambient sphere. For $N=0$ (S^0 consists of two points) the assertion is trivial. For $N>0$ suppose that $Y \in \gamma_k$ and $\delta Y = \phi$ or, equivalently, $Y^\varrho = Y$. Then

$$\begin{aligned}Y &= Y\{x_N \neq 0\} + Y\{x_N = 0\} \\ &= Y\{x_N>0\} + Y^\varrho\{x_N<0\} + Y\{x_N=0\} \\ &= \delta(Y\{x_N>0\}) + Y\{x_N=0\}.\end{aligned}$$

The set $Y\{x_N=0\}$ can be identified with a subset Y' of S^{N-1} satisfying $\delta Y' = \phi$. By induction $Y' = \delta Z'$. Morover Z' can be identified with the cylindrical subset defined by the same relations in S^N. Then

$$\begin{aligned}Y &= \delta(Y\{x_N>0\}) + \{x_N=0\}\delta Z' \\ &= \delta[Y\{x_N>0\} + \{x_N=0\}Z'] \in \delta\gamma_{k+1}.\end{aligned}$$

4. Some Mappings Between Affine and Spherical Sets

We next describe some mappings useful in applying the structure $\{\gamma_k, \delta\}$ to affine geometry.

Definition 4.1 (lifting from S^N to R^{N+1}). For $Y \subset S^N$ let $Y^* \subset R^{N+1} \backslash \{0\}$ be the union of the open rays in R^{N+1} parameterized by the points of Y.

Observation 4.2.

1. The mapping $Y \to Y^*$ gives an injection of the semialgebraic subsets of S^N into $R^{N+1} \setminus \{0\}$. If $Y \subset S^N$ is defined by any set $\mathbb{P}$ of homogeneous polynomial relations then Y^* consists of the nonzero solutions of $\mathbb{P}$ regarded as relations in R^{N+1}.

2. $\kappa(Y) = \kappa(Y^*)$.

Definition 4.3 (restriction from R^N (S^N) to $R^{N-1}(S^{N-1})$). For $Y \subset R^N(S^N)$ and λ a nonconstant affine function (linear form), let $Y|_{\lambda=0}$ be the image of the restriction of Y to the hyperplane (hypersphere) $\{\lambda = 0\}$ under some fixed isomorphism of $\{\lambda = 0\}$ with $R^{N-1}(S^{N-1})$.

Observation 4.4.

1. If Y is defined by any set $\mathbb{P}$ of polynomial relations and λ has the form $x_N - \mu$, then $Y|_{x_N=\mu}$ can be identified with the subset of $R^{N-1}(S^{N-1})$ determined by substituting $x_N = \mu$ into each polynomial in $\mathbb{P}$.

2. $\kappa(Y|_{\lambda=0}) \leqq \kappa(Y)$ since

a) any representation of Y in γ descends to a representation of the restriction of Y of no greater degree upon multiplication by the element $\{\lambda = 0\}$ of the ground ring γ_0 and

b) complexity is preserved by an isomorphism.

We also require the following somewhat subtler mapping from affine spaces to spheres. Geometrically it is a mapping from R^N to the generating $(N-1)$-sphere of its tangent cone at a point.

Definition 4.5. Let a be a point of R^N (or ∞). For $Y \in \gamma(R^N)$ let $\tau_a Y$ be the set of rays through a (the origin) which sufficiently near a (ultimately) lie in Y.

Proposition 4.6. *If* $Y \in \gamma(R^N)$ *then*

1. $\tau_a Y \in \gamma(S^{N-1})$,
2. $\kappa(\tau_a Y) \leqq \kappa(Y)$.

Proof. By definition $\tau_a Y$ is a subset of S^{N-1}. We need to show that it is semialgebraic. Consider the case $a = \infty$. Suppose Y is an open set determined by a single polynomial inequality $\{g > 0\}$. Let the decomposition of g into its homogeneous parts be $g = g_0 + g_1 + \ldots + g_m$ where g_j is a [degree$(g) - j$]-form. Then $\tau_\infty \{g > 0\}$ is given explicitly by

$$\tau_\infty \{g>0\} = \{g_0 > 0\} + \{g_0 = 0\}\{g_1 > 0\} + \ldots + \{g_0 = g_1 = \ldots = g_{m-1} = 0\}\{g_m > 0\}.$$

Hence $\tau_\infty \{g > 0\}$ is semialgebraic and has complexity not greater than 1.

We next check that τ_∞ is a ring homomorphism by observing that it preserves intersections and complements. It is obvious from its definition that it preserves intersections. Less obvious is $\tau_\infty(Y^c) = (\tau_\infty(Y))^c$. For example, if Y is the spiral $\{r = \log\theta\}$ in R^2, then $\tau_\infty(Y) = \tau_\infty(Y^c) = \phi$. However in the semialgebraic category such pathology cannot occur. For if a ray lies ultimately in $X = Y \cup Y^c$ it can cross between Y and Y^c only finitely many times and hence must lie ultimately in one or the other. Since τ_∞ is a ring homorphism, properties 1 and 2, already established for generators, follow for general Y. For $a \in R^N$ we simply replace the decomposition of g into homogeneous parts by its Taylor expansion around $x = a$.

5. Applications

As an application we use the structure $\{\gamma_k(X), \delta\}$ to obtain lower bounds for the complexity of certain semialgebraic sets. Our reasoning imitates the following very crude argument in the topological category with the structure $\{C_k, \partial\}$ where C_k denotes the Z_2-module of k-dimensional chains and ∂ is the usual boundary operator of algebraic topology. Here it is obvious that: 1) ∂ reduces dimension and 2) restriction to a subchain does not increase dimension. These weak properties suffice, for example, to prove the primitive result that the dimension of S^N is not less than N. For otherwise by 2) $\dim\{x_N \geqq 0\} < N$ and by 1) $\dim \partial\{x_N \geqq 0\} = \dim S^{N-1} < N-1$. Iterating, we find that S^0 is empty, a contradiction.

Proposition 5.1. *In R^N let $X_N = \bigcap_i \{x_i \geqq 1\}$, $Y_N = \bigcup_i \{x_i \leqq 0\}$. If $S \in \gamma(R^N)$ satisfies $X_N \subset S \subset Y_N^c$ then $\kappa(S) \geqq N$.*

Proof. Using coordinates $(x_0, x_1, \ldots, x_{j-1})$ in R^j and the operations defined in Sects. 3 and 4, for $Y \in \gamma(R^j)$ define $\varphi_j Y = (\delta \tau_\infty Y)^*|_{x_{j-1}=1}$. Then the following check of the four indicated operations shows that

$$\varphi_j \gamma_k(R^j) \subset \gamma_{k-1}(R^{j-1}). \tag{5.1}$$

First, if $\kappa(Z) = k$, then, by Proposition 4.6, τ_∞ maps Z into $\gamma_k(S^{j-1})$. Next, by Proposition 3.2, δ reduces the complexity by at least 1. Finally, the lifting $(\ )^*$ from S^j to R^j and restriction $x_{j-1} = 1$ to R^{j-1}, by observations of Sect. 4, do not increase the complexity.

We now derive a contradiction from the assumption that $S \in \gamma_{N-1}(R^N)$ by producing a disagreement between an algebraic and a geometric calculation. For, let $T = \varphi_2 \varphi_3 \ldots \varphi_N S$. Then repeated use of (5.1) shows that $T \in \gamma_0(R)$. But at the level of point sets it is easy to check that $X_{j-1} \subset \varphi_j(X_j)$ and $\varphi_j(Y_j) = Y_{j-1}$. Hence we find $X_1 \subset T \subset Y_1^c$ or $[1, \infty) \subset T \subset (0, \infty)$. Since $\gamma_0(R)$, the ring generated by the algebraic subsets of R, is precisly the ring of finite and cofinite subsets, this is impossible.

Corollary 5.2. *The positive orthant in R^N has complexity exactly N.*

Proof. Obviously N is an upper bound for the complexity. What is less obvious is that N is also a lower bound. But this follows immediately from the preceding proposition.

Other proofs of this fact can be given but these also seem rather complicated by comparison with the very simple conclusion. However it is reasonable that some delicacy is required since, for example, the relation $x + y - (x^2 + y^2)^{1/2} > 0$ defines the positive quadrant with a single inequality of a more general type. A circle of related questions involves the Mostowski separation theorem [BE] [C] [M] and the Mostowski number $m(N)$. This number, roughly speaking, is the largest number of square roots of definite polynomials which must be adjoined to the polynomial ring to obtain a function which separates a disjoint pair of closed semialgebraic sets in a variety of dimension N. Proposition 5.1 can be used to give lower bounds for $m(N)$ along the lines given in [S]. However, since other methods give sharper estimates, we merely give a corollary which shows the principle of the argument.

Corollary 5.3. *For $N \leqq 2$ the Mostowski number satisfies $m(N) \geqq N-1$.*

Proof. By contradiction. If $m(2)=0$, then any disjoint pair of closed semialgebraic sets in the plane can be separated by a polynomial function. In particular (recalling the sets X_N and Y_N defined in the proof of Proposition 5.1) there exists a polynomial function f positive on X_2 and negative on Y_2. But then the set $\{f>0\}$ violates Proposition 5.1. Similarly if $m(3)<2$ then X_3 and Y_3 can be separated by a function of the form $f=a+b\sqrt{g}$ where a and b are polynomials and g is a definite polynomial. Let $D=a^2-b^2g$. Then it is easy to check that $\{f>0\}=\{a>0\}\{D>0\}+\{b>0\}\{D<0\}+\{b>0\}\{a>0\}\{D=0\}$. It follows that $\kappa(\{f>0\})\leqq 2$ and again the set $\{f>0\}$ violates Proposition 5.1.

References

[B1] Bröcker, L.: Minimal generation of basic semialgebraic sets. Rocky Mt. J. Math. **14** (no. 4), 935–938 (1984)

[B2] Bröcker, L.: Minimale Erzeugung von Positivbereichen. Geom. Dedicata **16** (no. 3), 335–350 (1984)

[BE] Bochnak, J., Efroymson, G.: Real algebraic geometry and the 17th Hilbert problem. Math. Ann. **251**, 213–241 (1980)

[C] Coote, M.: Ensembles Semi-algebrique et fonctions de Nash. Seminaire de geometrie reelle de Paris 7, Fascicole no. 18, Ferrier (1981)

[H] Halmos, P.: Measure theory. New York: Van Nostrand 1950

[M] Mostowski, T.: Some properties of the ring of Nash functions. Ann. Sc. Norm. Super., Pisa, Cl. Sci., IV. Ser. Sci. **24**, 597–632 (1970)

[S] Stengle, G.: A lower bound for the complexity of separating functions. Rocky Mt. J. Math. **14** (no. 4), 927–929 (1984)

Received August 13, 1986; in revised form February 16, 1988