COUNTER-EXAMPLES TO QUANTIFIER ELIMINATION FOR FEWNOMIAL AND EXPONENTIAL EXPRESSIONS

ANDREI GABRIELOV[†]

To Askold Georgievich Khovanskii on his 60th birthday

ABSTRACT. We construct a family of semialgebraic sets of bounded fewnomial complexity, with unbounded fewnomial complexity of their projections to a subspace. This implies impossibility of fewnomial quantifier elimination. We also construct a set defined by exponential algebraic functions such that its projection cannot be defined by a quantifier-free formula with exponential algebraic functions, even if division is permitted. Similar examples are constructed for the unrestricted frontier of fewnomial and exponential semialgebraic sets, and for the Hausdorff limits of families of such sets.

1. INTRODUCTION

The theory of fewnomials was created by Khovanskii [8, 9] in the end of 1970s as an important special case of his theory of Pfaffian functions (real analytic functions satisfying a triangular system of first order partial differential equations with polynomial coefficients). A fewnomial (see Definition 2.1 below) is a polynomial with a few nonzero monomials or, more general, a polynomial defined by a formula with bounded additive complexity [13]. The Bezout-Khovanskii theorem for Pfaffian functions establishes an efficient upper bound on the number of isolated real solutions of a system of Pfaffian (in particular, fewnomial) equations. This allows one to derive upper bounds on the topological complexity of semi- and sub-Pfaffian sets, and on the complexity of certain operations on semi-Pfaffian sets, such as stratification and restricted frontier (see review [7] for the definitions and further references). Examples presented in this paper show that upper bounds on complexity do not exist for quantifier elimination and the operations of unrestricted frontier and Hausdorff limit.

The famous Tarski-Seidenberg theorem [16, 14] asserts that projection of a real semialgebraic set to a subspace is again semialgebraic, i.e., *quantifier elimination* is possible in the semialgebraic category. An example of Osgood [12] shows that this result cannot be extended to semianalytic category, even if all variables remain bounded: the set

$$Y = \{(x, y, z) \in [-1, 1]^3,\ \exists u \in [-1, 1],\ y = xu,\ z = x \exp(u)\} \tag{1.1}$$

is not semianalytic, although it is a projection of a compact semianalytic set.

Let X be a *semianalytic* set in $\mathbb{R}^n$, defined by a formula (2.1) below with real analytic functions P_{ij}, and let Y be a *subanalytic* set, a relatively proper projection

Date: October 6, 2006.

Key words and phrases. fewnomials, quantifier elimination.

[†] Supported by NSF grants DMS-0200861 and DMS-0245628.

of X to a subspace of $\mathbb{R}^n$. Gabrielov's complement theorem [3, 4] for subanalytic sets states that the complement to Y is again a relatively proper projection of a semianalytic set $Z \subset \mathbb{R}^N$. This implies model completeness of the structure generated by *global* analytic functions, i.e., functions $y = f(x),\ x \in \mathbb{R}^n,\ y \in \mathbb{R}$ such that, after embedding of $\mathbb{R}^n$ in $\mathbb{RP}^n$ and $\mathbb{R}$ in $\mathbb{RP}^1$, the graph of f becomes a semianalytic subset of $\mathbb{RP}^n \times \mathbb{RP}^1$. Denef and van den Dries [1] proved that quantifier elimination is possible in that structure if *bounded division* is permitted, the ratio of two functions f and g being defined as $f(x)/g(x)$ when $g(x) \neq 0$ and $|f(x)| \leq |g(x)|$, and 0 otherwise. For example, the set Y in (1.1) can be defined as

$$\{(x, y, z) \in [-1, 1]^3,\ x \neq 0,\ |y| \leq |x|,\ z = x \exp(y/x)\} \cup \{(0, 0, 0)\}.$$

Without the properness condition, projection of a semianalytic set may be rather wild. However, this does not happen for semi-Pfaffian sets. Wilkie [18] (see also Speissegger [15]) proved that the structure generated by all Pfaffian functions is o-minimal. Accordingly, one should consider separately results for *restricted* (with the properness conditions, see Definition 2.4 below) and *unrestricted* semi- and sub-Pfaffian sets.

For a *restricted* semi-Pfaffian set X, the set Z in the complement theorem can be chosen also restricted semi-Pfaffian. Gabrielov and Vorobjov [6] proved that the Pfaffian complexity of Z can be bounded from above in terms of the Pfaffian complexity of X. A key step in establishing that upper bound was the complexity of the restricted frontier of a semi-Pfaffian set X (i.e., frontier within the domain of definition of the Pfaffian functions in the formula for X). According to [5], restricted frontier of X is a semi-Pfaffian set of the complexity bounded from above in terms of the Pfaffian complexity of X. In this paper, we show that this is not true for the unrestricted frontier, even in the fewnomial case, when the frontier is semialgebraic.

One of the most important results for the *unrestricted* case is the Wilkie's complement theorem for the structure generated by the exponential function [17]. Van den Dries, Macintyre and Marker [2] showed that quantifier elimination is possible if we allow bounded division in the structure generated by global analytic functions and unrestricted exponential and logarithmic functions. The complement theorem for unrestricted Pfaffian functions remains an open problem, although Lion and Speissegger [10] proved it for the closely related "Rolle leaves." No upper bounds on the complexity are known for the unrestricted case.

2. Counter-examples for fewnomial expressions

Definition 2.1. [9, 13]. *A polynomial $F(x)$ in n variables $x = (x_1, \dots, x_n)$ is a* fewnomial *of complexity m if it can be constructed from constants and independent variables with at most m additions and any number of multiplications. A point x is* regular *for a fewnomial F if, whenever there is a product of two polynomials P and Q in the expression for F, we have $P(x)Q(x) \neq 0$. The* domain of definition *of F is the set of all its regular points.*

For example, a polynomial with m nonzero monomials of arbitrary degree is a fewnomial of complexity $m - 1$. Its domain of definition is the complement to coordinate hyperplanes.

Definition 2.2. *A rational function $F(x)$ is a* fewnomial with division *of complexity m if it can be constructed from constants and independent variables with at*

most m additions, and any number of multiplications and divisions. A point x is regular *for F if, whenever there is a product or a ratio of two terms P and Q in the expression for F, both $P(x)$ and $Q(x)$ have finite nonzero values. The* domain of definition *of F is the set of all its regular points.*

Definition 2.3. *A semialgebraic set $X \subset \mathbb{R}^n$ is defined by a formula*

$$X = \Big\{ x \in \mathbb{R}^n,\ \bigcup_i \Big(\bigcap_j (P_{ij}(x)\ ?\ 0) \Big) \Big\} \tag{2.1}$$

with polynomials P_{ij} and $? \in \{>, <, =\}$.

Definition 2.4. *A* fewnomial semialgebraic set *X of complexity (m, q) is defined by a formula (2.1) with at most q operations $\cap$, $\cup$ and fewnomials P_{ij} of complexity at most m. The set X is* restricted *if it is bounded and all points of its closure are regular for all fewnomials P_{ij}. If P_{ij} in the formula for X are fewnomials with division, we say that* division is permitted.

The complexity of fewnomials (and fewnomials with division) is closely related to their Pfaffian complexity. The Bezout-Khovanskii theorem implies that the number of isolated real zeros of a system of n fewnomial equations (with division) of complexity m in n variables is bounded by a certain explicit function of (n, m).

For an integer $d > 1$, consider a set $X_d \subset \mathbb{R}^3$ defined by the following two equations:

$$t^d - xt + 1 = 0, \tag{2.2}$$

$$(y - t)^d - x(y - t) + 1 = 0. \tag{2.3}$$

The complexities of fewnomials in these equations are 2 and 3, independent of d. Let Y_d be projection of X_d to $\mathbb{R}^2$:

$$Y_d = \{(x, y) \in \mathbb{R}^2,\ \exists t \in \mathbb{R},\ (x, y, t) \in X_d\}. \tag{2.4}$$

Theorem 2.5. *The set Y_d in (2.4) cannot be defined by a quantifier-free formula (2.1) with fewnomials of the complexity independent of d, even if division is permitted.*

Proof. For a fixed real x, a point (x, y) belongs to Y_d when y is the sum of two real solutions, not necessarily distinct, to (2.2) considered as an equation on t.

Consider the complexification $\mathbb{C}Y_d$ of Y_d:

$$\mathbb{C}Y_d = \{(x, y) \in \mathbb{C}^2,\ \exists t \in \mathbb{C},\ t^d - xt = -1,\ (y - t)^d - x(y - t) = -1\}, \tag{2.5}$$

i.e., the set of complex values (x, y) for which (2.2) and (2.3), considered as equations on t, have a common complex solution.

Let $t = t(x)$ be a d-valued algebraic function of $x \in \mathbb{C}$ defined by (2.2). It is ramified at d points $x_k = x_0 e^{2k\pi i/d}$ where $x_0 = d/(d-1)^{(d-1)/d}$ is real positive. The values of $t(0)$ are $t_k = e^{(2k-1)\pi i/d}$, for $k = 0, \dots, d-1$. The monodromy group of $t(x)$ is the permutation group $\mathcal{S}_d$. To see this, one observes that, as x moves along the real axis from 0 towards the ramification point x_0, makes a small loop about x_0, and comes back to 0 along the real axis, the two values t_0 and t_1 of $t(0)$ are permuted (see the proof of Theorem 3.2 for a more detailed argument). Since (2.2) is invariant under

$$x \mapsto e^{-2\pi i/d} x, \quad t \mapsto e^{2\pi i/d} t, \tag{2.6}$$

the values t_{k-1} and t_k of $t(0)$ are permuted as x moves from 0 towards x_{-k}, makes a small loop, and returns to 0. These permutations generate $\mathcal{S}_d$.

Substituting $t = t(x)$ into (2.3), we define $d(d+1)/2$-valued function $y(x)$ with $y_{ij}(x) = t_i(x) + t_j(x)$, for $0 \le i \le j < d$. Here $t_i(x)$ are the values of the function $t(x)$. The monodromy group action on the values y_{ij} of $y(x)$ has two invariant subsets: $i = j$, of size d, corresponding to the subset $\{(y/2)^d - xy/2 = -1\}$ of $\mathbb{C}Y_d$, and $i \ne j$, of size $d(d-1)/2$, corresponding to an irreducible algebraic curve $\mathbb{C}Y'_d \subset \mathbb{C}Y_d$. For a small real c, the set $\mathbb{C}Y'_d \cap \{x = c\}$ contains $[d/2]$ real points, the sums of pairs of complex conjugate roots of (2.2).

Note that $Y'_d = \mathbb{C}Y'_d \cap \mathbb{R}^2$ is one-dimensional since, for real $x > x_0$, equation (2.2) has at least two real solutions. Any quantifier-free semialgebraic formula defining Y_d, even if division is permitted, should contain a nonzero rational function $P(x, y)$ vanishing on a one-dimensional subset of Y'_d. Since $\mathbb{C}Y'_d$ is irreducible, P should vanish identically on $\mathbb{C}Y'_d$. Hence the set $\{P = 0,\ x = c\}$, for a generic small real c, should contain at least $[d/2]$ isolated real points. Bezout-Khovanskii theorem implies that P cannot be a fewnomial with division of the complexity independent of d. □

The set X_d defined by (2.2) and (2.3) is not restricted, but $X_{d,c} = X_d \cap \{|x| \le c\}$ is a restricted fewnomial set. For any real $x > x_0$, equation (2.2) has at least two real solutions. Note that $x_0 \le 2$ for all d. In particular, $Y'_d \cap \{|x| \le 3\}$ is a nonempty one-dimensional set. Here Y'_d is the set defined in the proof of Theorem 2.5. The arguments in the proof of Theorem 2.5 can be repeated to prove the following statement.

Corollary 2.6. *The set $Y_{d,3} = Y_d \cap \{|x| \le 3\}$, a projection of a restricted fewnomial semialgebraic set $X_d \cap \{|x| \le 3\}$, cannot be defined by a quantifier-free formula (2.1) with fewnomials of the complexity independent of d, even if division is permitted.*

Consider the cone W_d over the set $X_{d,3}$:

$$W_d = \{0 < z \le 1\} \quad \cap \quad \{|x| \le 3\} \tag{2.7}$$
$$\cap \{t^d - xtz^{d-1} + z^d = 0,\ (yz - t)^d - x(yz - t)z^{d-1} + z^d = 0\}.$$

A point $(x, y, z, t) \in \mathbb{R}^4$ belongs to W_d if $0 < z \le 1$ and $(x, y, t/z) \in X_{d,3}$. The set W_d is fewnomial semialgebraic, with the complexity independent of d. It is not restricted, since the points of its frontier

$$\partial W_d = \bar{W}_d \setminus W_d = \{z = t = 0,\ (x, y) \in Y_{d,3}\}$$

are not regular for the fewnomials in (2.7). Note that ∂W_d is the Hausdorff limit at $z = 0$ of the family of restricted fewnomial sets $W_d \cap \{z = \text{const}\}$. The following statement follows immediately from Theorem 2.5.

Corollary 2.7. *The set ∂W_d, the frontier of a fewnomial semialgebraic set W_d and the Hausdorff limit of the family of restricted fewnomial semialgebraic sets $W_d \cap \{z = \text{const}\}$, cannot be defined by a quantifier-free formula (2.1) with fewnomials of the complexity independent of d, even if division is permitted.*

Note that there is an upper bound on the *topological* complexity of the Hausdorff limit of a family of restricted semi-Pfaffian, in particular, fewnomial semialgebraic sets of bounded complexity (Zell [19]).

3. Counter-examples for exponential expressions

Definition 3.1. *An* exponential algebraic function *is a function constructed from the constants and independent variables with additions, multiplications, and exponentiations. An* exponential semialgebraic set X *is defined by a formula (2.1) with exponential algebraic functions P_{ij}. An exponential algebraic function* with division *is constructed from constants and independent variables with additions, multiplications, divisions, and exponentiations.*

The set X is restricted *if it is bounded, all points of its closure are regular for all fewnomials in its formula, and the values of all exponentials in its formula can be separated from 0 and ∞.*

An exponential algebraic function (also with division) is a Pfaffian function. Bezout-Khovanskii theorem implies that the number of isolated real zeros of a system of equations with exponential algebraic functions is finite, bounded by a certain explicit function of the number of variables and the complexities of the functions.

We give here an example of a curve in $\mathbb{R}^5$ defined by an exponential algebraic equations and inequalities, such that its proper projection to $\mathbb{R}^2$ cannot be defined by a quantifier-free formula with exponential algebraic functions with division. A different approach to impossibility of exponential quantifier elimination was suggested in [11].

Assuming $0 < t < y$, one can consider a set $X_d^+ \subset \mathbb{R}^3$ defined by (2.2) and (2.3) for any real number d:

$$t^d - xt + 1 = 0, \quad t > 0, \tag{3.1}$$

$$(y-t)^d - x(y-t) + 1 = 0, \quad y > t. \tag{3.2}$$

Let Y_d^+ be projection of X_d^+ to $\mathbb{R}^2$:

$$Y_d^+ = \{(x,y) \in \mathbb{R}^2,\ \exists t \in \mathbb{R},\ (x,y,t) \in X_d^+\}. \tag{3.3}$$

Introducing new variables $u = \log(t)$ and $v = \log(y-t)$, one can represent Y_d^+ as a proper projection of a set $Z_d \subset \mathbb{R}^5$ defined by a system of equations with exponential algebraic functions:

$$\exp(u) - t = 0, \quad \exp(du) - xt + 1 = 0, \tag{3.4}$$

$$\exp(v) - y + t = 0, \quad \exp(dv) - x(y-t) + 1 = 0. \tag{3.5}$$

Theorem 3.2. *The set Y_d^+ in (3.3) cannot be defined by a quantifier-free formula with exponential algebraic functions, even if division is permitted.*

Proof. For a fixed real x, a point (x,y) belongs to Y_d^+ when y is the sum of two real positive solutions, not necessarily distinct, to (3.1) considered as an equation on t. For $d > 1$ and $x > x_0 = d/(d-1)^{(d-1)/d}$, equations (3.1) and (3.2) have two distinct real positive solutions, $t_0(x)$ and $t_1(x)$, hence Y_d^+ contains a one-dimensional semianalytic curve Y_d', the graph of the function $y(x) = t_0(x) + t_1(x)$. We want to define an irreducible complex analytic curve $\mathbb{C}Y_d' \subset \mathbb{C}^2$ by analytic continuation of $y(x)$.

We start with a multivalued ramified analytic function $t(x)$ for $x \in \mathbb{C}$ obtained as an analytic continuation of $t_0(x)$. Although t^d is a multivalued function with ramification at $t = 0$ and $t = \infty$, we can always choose its branch uniquely since,

for bounded complex values of x, solutions to (3.1) are bounded and separated from $t = 0$. At $x = x_0$, we have $t_0(x_0) = t_1(x_0) = 1/(d-1)^{1/d}$. As x makes a loop about x_0, the two solutions $t_0(x)$ and $t_1(x)$ are exchanged. Hence they represent two branches of the same multivalued function $t(x)$. As x passes through x_0 and continues towards 0 along the real axis, the two branches of $t(s)$ passing through $t(x_0) = 1/(d-1)^{1/d}$ become the two values $e^{\pm\pi i/d}$ of $t(0)$. This can be easily verified for $d = 2$ and extended to all $d > 1$ by continuity.

Let us fix an irrational value of d. Since (3.1) is invariant under the transformation (2.6), and the value $t_0 = e^{-\pi i/d}$ of $t(0)$ maps to its value $t_1 = e^{\pi i/d}$ under that transformation, the function $t(x)$ is invariant under (2.6). As x moves along the real axis from 0 towards x_0, makes a small loop about x_0, and comes back to 0 along the real axis, the values t_0 and t_1 of $t(0)$ are permuted. If the loop is small enough, the only other permuted values of $t(0)$ are $t_m = e^{(2m-1)\pi i/d}$ with $|m|$ large. Since $t(x)$ is invariant under (2.6), the same is true for the values t_{k-1} and t_k of $t(0)$, for any k. This implies that, for any finite permutation σ of the values of $t(0)$, acting as an identity on the values t_k with $|k| > k(\sigma)$, and any $k_0 \ge k(\sigma)$, there is an element of the monodromy group of $t(x)$ that acts as σ on all values t_k of $t(0)$ for $|k| \le k_0$. This implies that, for any x and any two distinct values t' and t'' of $t(x)$, there is a value $t' + t''$ of $y(x)$. In particular, for a generic real x, the function $y(x)$ has infinitely many real values, the sums of pairs of complex conjugate values of $t(x)$. Hence, for an irrational d and a generic real c, the set $\mathbb{C}Y'_d \cap \{x = c\}$ has infinitely many real points.

Any quantifier-free formula (2.1) with exponential algebraic functions defining Y_d^+, even if division is permitted, should contain a nonzero exponentional algebraic function with division $P(x, y)$ vanishing on a one-dimensional subset of Y'_d. Since $\mathbb{C}Y'_d$ is irreducible, P should vanish identically on $\mathbb{C}Y'_d$. Hence the set $\{P = 0,\ x = c\}$, for a generic real c, should contain infinitely many isolated real points, which contradicts the Bezout-Khovanskii theorem. □

The set Z_d defined by (3.4) and (3.5) is not restricted, but $Z_{d,c} = Z_d \cap \{|x| \le c\}$ is a restricted exponential semialgebraic set. For any real $x > x_0$, equation (3.1) has at least two real solutions. Note that $x_0 \le 2$ for all d. In particular, $Y'_d \cap \{|x| \le 3\}$ is a nonempty one-dimensional set. Here Y'_d is the subset of Y_d^+ defined in the proof of Theorem 3.2. The arguments in the proof of Theorem 3.2 can be repeated to prove the following statement.

Corollary 3.3. *The set $Y_d^+ \cap \{|x| \le 3\}$, a projection of a restricted exponential semialgebraic set $Z_d \cap \{|x| \le 3\}$, cannot be defined by a quantifier-free formula (2.1) with exponential algebraic functions, even if division is permitted.*

Consider the cone V_d over the set $Z_{d,3}$.

$$V_d = \{0 < z \le 1,\ (x, y, z, u, v, t) \in \mathbb{R}^6,\ (x, y, u/z, v/z, t/z) \in Z_{d,3}\}. \tag{3.6}$$

The set V_d is exponential semialgebraic with division. It is not restricted, since its frontier

$$\partial V_d = \bar{V}_d \setminus V_d = \{z = u = v = t = 0,\ (x, y) \in Y_d^+\} \cap \{|x| \le 3\}$$

contains points that are not regular. Note that ∂V_d can be considered as the Hausdorff limit of a family of restricted exponential semialgebraic sets $V_d \cap \{z = \text{const}\}$ as $z \searrow 0$. The following statement follows immediately from Theorem 3.2.

Corollary 3.4. *The set ∂V_d, the frontier of an exponential semialgebraic set with division V_d and the Hausdorff limit of a family of restricted exponential semialgebraic sets $V_d \cap \{z = \text{const}\}$, cannot be defined by a quantifier-free formula (2.1) with exponential algebraic functions, even if division is permitted.*

References

[1] J. Denef and L. van den Dries, P-adic and real subanalytic sets, *Ann. Math.*, **128** (1988), 79–138.

[2] L. van den Dries, A. Macintyre, and D. Marker, The elementary theory of restricted analytic fields with exponentiation, *Ann. Math.*, **140** (1994), 183–205.

[3] A. Gabrielov, Projections of semi-analytic sets, *Functional Anal. Appl.*, **2** (1968), 282–291.

[4] A. Gabrielov, Complements of subanalytic sets and existential formulas for analytic functions, *Invent. Math.*. **125** (1996), 1–12.

[5] A. Gabrielov, Frontier and Closure of a semi-Pfaffian set, *Discrete Comput. Geom.*, **19** (1998), 605–617. *Discrete Comput. Geometry* **14**, (1995), 71–91.

[6] A. Gabrielov and N. Vorobjov, Complexity of cylindrical decompositions of sub-Pfaffian sets, *J. Pure Appl. Algebra*, **164** (2001), 179–197.

[7] A. Gabrielov and N. Vorobjov, Complexity of computations with Pfaffian and Noetherian functions. In: *Normal forms, bifurcations and finiteness problems in differential equations*, 211–250, Kluwer Acad. Publ., Dordrecht, 2004.

[8] A. G. Khovanskii, On a class of systems of transcendental equations, *Soviet Math. Dokl.*, **22** (1980), 762–765.

[9] A. G. Khovanskii, *Fewnomials*. AMS Translation of mathematical monographs **88**, AMS, Providence RI, 1991. Russian original: *Malochleny*, Moscow, 1987; Revised Russian edition: Fazis, Moscow, 1996.

[10] J.-M. Lion and P. Speissegger, The theorem of the complement for sub-Pfaffian sets. Preprint arXiv:math.DG/0602196, 2006.

[11] A. Macintyre and D. Marker, A failure of quantifier elimination. *Rev. Mat. Univ. Complut. Madrid*, **10** (1997), Special Issue, suppl., 209–216.

[12] W. F. Osgood, On functions of several complex variables. *Trans. Amer. Math. Soc.*, **17** (1916), 1–8.

[13] J.-J. Risler, Additive complexity and zeros of real polynomials. *SIAM J. Comput.*, **14** (1985), 178–183.

[14] A. Seidenberg, A new decision method for elementary algebra, *Ann. Math.*, **60** (1954), 365–374.

[15] P. Speissegger, The Pfaffian closure of an o-minimal structure, *J. Reine Angew. Math.*, **508** (1999), 189–211.

[16] A. Tarski, A decision method for elementary algebra and geometry. Berkeley note, 1951.

[17] A. J. Wilkie, Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function, *J. Amer. Math. Soc.*, **9** (1996), 1051–1094.

[18] A. J. Wilkie, A theorem of the complement and some new o-minimal structures, *Selecta Math. (N.S.)*, **5** (1999), 397–421.

[19] T. Zell, Topology of definable Hausdorff limits, *Discrete Comput. Geom.*, **33** (2005), 423–443.

Department of Mathematics, Purdue University, 150 N University St., W.Lafayette, IN 47907-2067, USA

E-mail address: agabriel@math.purdue.edu