Exponential bounds for witnesses of diophantine definitions of Δ_0-formulas

Zoé Chatzidakis (CNRS - Université Paris 7)
Ehud Hrushovski[1,2] (The Hebrew University of Jerusalem)

(1.1) **Introduction and notation**. $\mathcal{L}_{ar} = \{+, \cdot, <, 0, 1\}$. We define $\exp^k(x)$ by induction as follows: $\exp^0(x) = x$, $\exp(x) = \exp^1(x) = 2^x$, and $\exp^{k+1}(x) = 2^{\exp^k(x)}$.

The famous Theorem of Matjasevič and Robinson, Davis, Putnam states that every subset of $\mathbb{N}^n$ defined by a Δ_0-formula $\varphi(\bar{z})$ is in fact definable by a diophantine formula, i.e., a formula $\exists \bar{u} P_1(\bar{z}, \bar{u}) = P_2(\bar{z}, \bar{u})$. We are interested in bounding the size of the witnesses $\bar{u}$ in terms of the size of a tuple $\bar{a}$ satisfying the formula $\varphi(\bar{x})$.

We will say that *the (eventual) bound for diophantine witnesses of the formula $\varphi(\bar{z})$ is* $\exp^k(\sup\{\bar{z}\}^\ell)$ if there are an integer m, and polynomials $P_1(\bar{Z}, \bar{U}), P_2(\bar{Z}, \bar{U})$ over $\mathbb{N}$ such that for every tuple $\bar{a}$ in $\mathbb{N}$ and $N = \sup\{\bar{a}, m\}$,

$$\mathbb{N} \models \varphi(\bar{a}) \iff \mathbb{N} \models \exists \bar{u} \leq \exp^k(N^\ell)\, P_1(\bar{a}, \bar{u}) = P_2(\bar{a}, \bar{u}).$$

Our aim is to give a proof of the following weak version of a result of Gaifman and Dimitracopoulos [DG]:

Proposition. Let $\varphi(\bar{z})$ be a Δ_0-formula of the language $\mathcal{L}_{ar} = \{+, \cdot, <, 0, 1\}$. The eventual bound for diophantine witnesses of $\varphi(\bar{z})$ is $\exp^3(\sup\{\bar{z}\}^\ell)$ for some ℓ. The eventual bound for diophantine witnesses of $y = 2^x$ is $\exp(\sup\{x, y\}^{15})$, i.e., $\exp^2(x^{15})$.

Remark. It follows that $\exp^4(\sup\{\bar{z}\})$ is an eventual bound for the witnesses of $\varphi(\bar{z})$ and for the values of the polynomials $P_1(\bar{z}, \bar{u}), P_2(\bar{z}, \bar{u})$ appearing in the associated diophantine formula.

This result is announced in [DG], with the better bound of $\exp^3(\sup\{\bar{z}\})$ for arbitrary Δ_0-formulas, but with only an indication of the proof. Here we give the proof we had found, before knowing of the result in [DG]. It is a simple inspection of the classical proof of Matjasevič and Robinson, Davis, Putnam. The references are to Chapter II of Smoryński's book [S].

(1.2) **Conventions**. We will use the notation $f(x) \gg g(x)$ to mean that $\lim_{x\to\infty} g(x)/f(x) = 0$. Thus for instance, if $p(\bar{X})$ is any polynomial with coefficients in $\mathbb{N}$, then $p(\bar{x}) \ll \exp(\sup\{\bar{x}\})$. For ease of reading, we will use freely the "minus sign" $-$ of $\mathbb{Z}$, and while all constants and variables (including those quantified upon) will range over $\mathbb{N}$, the validity of equations will come from $\mathbb{Z}$. We also allow ourselves the use of $\leq$ and $<$, and the use of the divisibility symbol $|$. Thus an expression of the form "$x|(y - z)$" is an abbreviation for the following formula:

$$\exists u\, (z \leq y \wedge ux + z = y) \vee (z > y \wedge ux + y = z),$$

[1] Supported by the Israel Science Foundation
[2] Research carried out for the Clay Mathematics Institute as a Clay Prize research fellow

where the variables range over $\mathbb{N}$.

(1.3) **Theorem**. Let $a \in \mathbb{N}$, $a \geq 2$, and consider the Pell equation

$$X^2 - (a^2-1)Y^2 = 1.$$

The solutions (in $\mathbb{N}$) of this equation are given by $x = X_a(n)$, $y = Y_a(n)$ for $n > 0$, where $X_a(n)$ and $Y_a(n)$ are defined by

$$X_a(n) + Y_a(n)\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n.$$

For $n \geq 1$, we have

$$Y_a(n) \leq (2a)^{n-1}, \quad X_a(n) \leq (2a)^n.$$

Proof. This is Theorem II.4.2, and Lemma II.4.7 for the bound on $Y_a(n)$. Note that $X_a(n)^2 = 1 + (a^2-1)Y_a(n)^2$, and this gives the bound on $X_a(n)$.

(1.4) **Lemma**. The eventual bound for diophantine witnesses of the formula $y = Y_a(x)$ is $\exp^2(\sup\{x, \log a\}^5)$.

Proof. By Theorem II.5.1, $y = Y_a(x)$ is defined by the formula

$$\begin{array}{l}\exists w, u, v, s, t, b \\ \begin{array}{cc} 2x \leq y & y|(b-1) \\ w^2 = 1 + (a^2-1)y^2 & u|(t-y) \\ u^2 = 1 + (a^2-1)v^2 & y|(t-x) \\ s^2 = 1 + (b^2-1)t^2 & y^2|v \\ u|(b-a) & v > 0. \end{array}\end{array}$$

This is clearly equivalent to a diophantine formula: all the divisibility relations are expressible by diophantine formulas, and a conjunction of diophantine equations is equivalent to a diophantine equation. Hence to finish the proof of the lemma, we need to find bounds on the size of w, u, v, s, t, b. The proof of Theorem II.5.1 shows that one can take

$$w = X_a(x).$$

Then, letting $m = yY_a(x)$, one takes

$$u = X_a(m), \qquad v = Y_a(m).$$

Choose b congruent to a modulo $X_a(m)$ and to 1 modulo y, and let

$$t = Y_b(x), \qquad s = Y_b(x).$$

For sufficiently large $N = \sup\{x, \log a\}$, we then have

$$\begin{array}{rc} & y, w \leq (2a)^x \ll \exp(N^3), \\ & m = yY_a(x) \leq (2a)^{2x} \ll \exp(N^3), \\ \text{hence} & u, v \leq (2a)^m \ll (2a)^{\exp(N^3)} \ll \exp^2(N^4), \\ & b < yX_a(m) \ll \exp^2(N^4) \\ & t, s \leq (2b)^x \ll (2\exp^2(N^4))^N \ll \exp^2(N^5). \end{array}$$

(1.5) **Lemma**. The eventual bound for diophantine witnesses of the formula $z = x^y$ is $\exp^2(\sup\{\log x, y\}^{15})$.

Proof. By Corollary II.5.4, we have

$$z = x^y \iff \exists a[a = Y_{2x}(y+2) \wedge (2ax - x^2 - 1 > z) \\ \wedge X_a(y) - Y_a(y)(a-x) \equiv z \bmod (2ax - x^2 - 1)].$$

We know that $z = x^y \leq \exp(N^2)$. By the previous lemma (1.4), the eventual bound for diophantine witnesses of $a = Y_{2x}(y+2)$ is $\exp^2((2\sup\{log(2x), y+2\})^5) \ll \exp^2(N^6)$, where $N = \sup\{\log x, y\}$ is sufficiently large. Similarly, the eventual bound for diophantine witnesses of $u = X_a(y)$, $v = Y_a(y)$ is $\exp^2(M^5)$, where $M = \sup\{\log(a), y\} \ll (y+2)log(4x) \ll N^3$. Hence eventual bound for diophantine witnesses of the formula $z = x^y$ is $\exp^2(N^{15})$.

(1.6) **Lemma**. The eventual bound for diophantine witnesses of each of the following formulas is of the form $\exp^2(\sup\{x, \log a, \log b\}^\ell)$ for some ℓ.

(1) $z = \binom{x}{y}$ $(y \leq x)$.
(2) $y = x!$
(3) $y = \prod_{k=0}^{x}(a + bk)$, where $a, b \in \mathbb{N}^{>0}$.
(4) $y = \prod_{k=0}^{x}(a - k)$, where $a \in \mathbb{N}^{>0}$.

Proof. We use II.2.9 and II.2.10 of [S].

(1) $z = \binom{x}{y}$ if and only if

$$\exists u, v, w\ (u = 2^x + 1) \wedge \big((u+1)^x = vu^{y+1} + zu^y + w\big) \wedge (z < u) \wedge (w < u^y).$$

The number u is given explicitly, and the numbers v, w are bounded above by $(u+1)^x$. The result follows by (1.5).

(2) $y = x!$ if and only if $\exists z = (2x)^{x+1}, \exists v < \binom{z}{x}\ z^x = y\binom{z}{x} + v$.

Use (1) and (1.5).

(3) $y = \prod_{k=0}^{x}(a + bk)$ if and only if

$$\exists p, z\ [p > (a+bx)^{x+1} > y \wedge p|(bz - a) \wedge p|(\tbinom{x+z}{x+1}(x+1)!b^{x+1} - y).]$$

Here p is any prime larger than $(a+bx)^{x+1}$, and there is such a prime $< 2(a+bx)^{x+1}$. The number z satisfies $p|(bz-a)$, and is $< p$. This gives us bounds on p and z, and the result follows by (1.5), (1) and (2).

(4) $y = \prod_{k=0}^{x}(a - k)$ if and only if

$$(a < x \wedge y = 0) \vee \exists z(z + x = a \wedge y = \textstyle\prod_{k=0}^{x}(z+k)).$$

Follows from (3).

(1.7) **Lemma**. Let $\varphi(\bar{z})$ be a Δ_0-formula of the language $\mathcal{L}_{ar} = \{+, \cdot, <, 0, 1\}$, $\bar{z} = (z_1, \ldots, z_n)$. There are polynomials $P_1(X, \bar{U}, \bar{V}, \bar{Z}), P_2(X, \bar{U}, \bar{V}, \bar{Z}) \in \mathbb{N}[X, \bar{U}, \bar{V}, \bar{Z}]$, and constants k, ℓ and m such that for all n-tuple $\bar{a}$ in $\mathbb{N}$,

$$\mathbb{N} \models \varphi(\bar{a}) \iff \exists \bar{u} \leq \exp(N^k)\, \forall x \leq N^\ell\, \exists \bar{v} \leq \exp(N^k)\, P_1(x, \bar{u}, \bar{v}, \bar{a}) = P_2(x, \bar{u}, \bar{v}, \bar{a}),$$

where $N = \sup\{m, a_1, \ldots, a_n\}$.

Proof. Note that our bounds are not sensitive to replacing some a by a^m, and we may therefore assume that our formula is of the form

$$\forall x_1 < z\, \exists y_1 < z \cdots \forall x_\ell < z\, \exists y_\ell < z P_1(\bar{x}, \bar{y}, \bar{z}) = P_2(\bar{x}, \bar{y}, \bar{z}),$$

where P_1, P_2 are polynomials with coefficients in $\mathbb{N}$, and $z = z_1 + 1$. The function $(x_1, \ldots, x_i) \mapsto x_1 + zx_2 + \cdots z^{i-1}x_i$ then defines a bijection between the n-tuples of elements smaller than z and the elements smaller than z^i. Hence our formula is equivalent to

$$\exists u_1, \ldots, u_\ell \forall x < z^\ell \, \exists x_1, \ldots, x_\ell, y_1, \ldots, y_\ell < z \, (x = \sum_{i=1}^{\ell} x_i z^{i-1}) \wedge$$
$$\wedge (\bigwedge_{i=1}^{\ell} \beta(u_i, \sum_{j=1}^{i} x_j z^{j-1}) = y_i) \wedge (P_1(\bar{x}, \bar{y}, \bar{z}) = P_2(\bar{x}, \bar{y}, \bar{z})).$$

Here β is the Gödel function. A bound for the elements $u_1, \ldots, u_\ell$ is then of the form $(1 + \ z^\ell (z^{\ell+1})!^{z^\ell}$ (see Thm I.7.3 in [S]), and therefore bounded above by $\exp(z^{2\ell+4})$ for z large enough. This also bounds the size of the witnesses used to express each subformula $\beta(u_i, \sum_{j=1}^{i} x_j z^{j-1}) = y_i$, and yields the result.

(1.8) *Proof of the Proposition.*

Lemma (1.7) shows how to transform a Δ_0-formula $\varphi(\bar{z})$ into a formula $\exists \bar{u} \, \psi(\bar{z}, \bar{u})$, where $\psi(\bar{z}, \bar{u})$ is of the form $\forall x \leq u \, \exists \bar{u} \leq u P_1(x, \bar{y}, \bar{z}, \bar{u}) = P_2(x, \bar{y}, \bar{z}, \bar{u})$. Moreover, we know that for large enough N, if $\bar{a} \leq N$, then the elements $\bar{u}$ can be chosen of size $\leq \exp(N^\ell)$ for some ℓ.

This reduces the problem to showing that the eventual bound for diophantine witnesses of a Δ_0-formula $\varphi(\bar{z})$ of the form $\forall x \leq z_1 \exists y_1, \ldots, y_\ell \leq z_1 \, P_1(x, \bar{y}, \bar{z}) = P_2(x, \bar{y}, \bar{z})$ is $\exp^2(\sup\{\bar{z}\}^k)$ (as $\exp^2((\exp(N^\ell)^k) \ll \exp^3(N^{\ell+1})$). [The bound given in [DG] for a formula of this type is $\exp(\sup\{\bar{z}\}^k)$.]

This is done by inspection of the proof of the "Bounded Quantifier Theorem" II.2.11 of [S].

We may assume that $\varphi(\bar{z})$ implies that all z_i are no bigger than z_1, by adding a variable and bounded existential quantifiers if necessary. Let $Q(\bar{Z})$ be the polynomial obtained by replacing each variable $X, Y_1, \ldots, Y_\ell$ by Z_1 in the polynomial $P_1(X, \bar{Y}, \bar{Z}) + P_2(X, \bar{Y}, \bar{Z})$ and multiplying it by Z_1.

Then we have (see II.2.11): for any $\bar{z} \in \mathbb{N}$

$$\mathbb{N} \models \forall x \leq z_1 \ \exists y_1, \ldots, y_\ell \leq z_1 \ P_1(x, \bar{y}, \bar{z}) = P_2(x, \bar{y}, \bar{z})$$
$$\iff$$
$$\mathbb{N} \models \exists c, t, v_1, \ldots, v_m \ \big[t = (Q(\bar{z})!) \wedge (1 + (c+1)t) = \prod_{j=0}^{z_1} (1 + (j+1)t)$$
$$\wedge (1 + (c+1)t) | \prod_{j=0}^{z_1} (v_1 - j) \wedge \cdots \wedge (1 + (c+1)t) | \prod_{j=0}^{z_1} (v_\ell - j)$$
$$\wedge (1 + (c+1)t) | (P_1(c, \bar{v}, \bar{z}) - P_2(c, \bar{v}, \bar{z}))\big].$$

The numbers c and t are explicitly given, and we have $Q(\bar{z}) \ll (z_1^s)$ for some s. For each $x \leq z_1$, we choose a solution $\bar{y}(x) = (y_1(x), \ldots, y_\ell(x)) \leq z_1$ of $P_1(x, \bar{y}, \bar{z}) = P_2(x, \bar{y}, \bar{z})$.

The v_i are then chosen so that

$$v_i \equiv y_i(x) \qquad \mod (1 + (x+1)t)$$

for all $i = 1, \ldots, \ell$ and $0 \leq x \leq z$. The v_i's can therefore be chosen $< \prod_{x=0}^{z_1}(1+(x+1)t) = 1 + (c+1)t$, and hence are less than $\exp(z_1^{2s})$ when z_1 is large enough.

This, together with Lemma (1.6), gives the result.

References

[DG] H. Gaifman, C. Dimitracopoulos, Fragments of Peano's arithmetic and MRDP theorem, in: *Logic and Algorithmic, An International Symposium help in Honour of Ernst Specker*, Monographie No 30 de l'Enseignement Mathématique, Genève 1982, 187 – 206.

[S] C. Smoryński, *Logical Number Theory I, An introduction*, Universitext, Springer-Verlag Berlin Heidelberg 1991.

UFR de Mathématiques
Université Paris 7 - Case 7012
2, place Jussieu
75251 Paris Cedex 05
France
e-mail: zoe@logique.jussieu.fr

Institute of Mathematics
The Hebrew University
Givat Ram
91904 Jerusalem
Israel
e-mail: ehud@math.huji.ac.il