VERSIONS OF MATIJASEVIČ'S THEOREM IN SUBSYSTEMS OF ARITHMETIC

CHARALAMPOS CORNAROS AND HENRI-ALEX ESBELIN

Matijasevič's theorem (MT), also known as MRDP (Matijasevič-Robinson-Davis-Putnam) theorem or DMPR theorem, states that Diophantine sets of natural numbers are precisely the recursively enumerable sets of natural numbers. This result is usually stated as follows (see [8]).

Theorem 1. *For any Σ_1 formula $\theta(\vec{x})$ there exists a polynomial $p(\vec{x},\vec{y})\in\mathbb{Z}[\vec{x},\vec{y}]$ such that $\mathbb{N}\models\forall\vec{x}[\theta(\vec{x})\leftrightarrow\exists\vec{y}\,p(\vec{x},\vec{y})=0]$.*

Because of the MT's considerable importance, due to the fact that it was highly instrumental for proving that Hilbert's Tenth Problem has a negative solution, as well as for showing that several problems are undecidable (see [9]), it was thought worthwhile to study its provability in subsystems of Peano Arithmetic, especially systems strictly weaker than $I\Sigma_1$, i.e., the theory of induction for Σ_1 definable sets.

The first such result was proved by Gaifman and Dimitracopoulos (see [4]) and states that MT is provable in the theory $I\Delta_0{+}exp$. This result raised many questions, including the following one (see Problem (d) in section 1.1 in [3]):

Problem 1. *Is the Matijasevič theorem for bounded formulas provable in $I\Delta_0$? That is: Is every bounded formula equivalent in $I\Delta_0$ to an existential formula?*

Given that the proof of MT involves heave use of coding means, while the coding capability of $I\Delta_0$ is very limited, attacking Problem 1 seems to be a highly nontrivial aim. So, work focused on improving the Gaifman-Dimitracopoulos result. In this direction, the following result was proved by R. Kaye (see [5]).

Theorem 2. *$IE_1^-{+}E$ proves MT, where IE_1^- denotes the theory of parameter-free bounded existential induction and E denotes an $\forall\exists$ axiom expressing the existence of a function of exponential growth.*

At first sight, one might think that the theory $IE_1^-{+}E$ is strictly weaker than the theory $I\Delta_0{+}exp$ considered earlier by Gaifman and Dimitracopoulos. However, as proved by Kaye in [5], as a corollary of Theorem 2 we obtain

Theorem 3. *$IE_1^-{+}E$ is equivalent to $I\Delta_0{+}exp$.*

Work in the same direction was also done by P. D'Aquino, who studied in [2] the following version of Problem 1.

Problem 2. *Is MT provable in* $I\Delta_0{+}\Omega_1$*?*

In particular, D'Aquino considered an $E_1^{\#}$ formula defining the exponential function in $I\Delta_0{+}exp$, where # is an extra function symbol, but could not obtain a formula of the same complexity that could define the function $(k+1)\dots(2k)$.

We recall that the theory $I\Delta_0{+}\Omega_1$ is conservatively extendable to Buss's theory S_2 (or T_2), i.e. the theory in the language $\mathcal{L}^*{=}\mathcal{L}\cup\{\lfloor\frac{x}{2}\rfloor, |x|, x\#y\}$, where $x\#y$ denotes $2^{|x|\cdot|y|}$, having axioms (a) a set $BASIC$ expressing basic properties of the non-logical symbols of $\mathcal{L}^*$ and (b) $\bigcup_{n\in\mathbb{N}} S_2^n$, where S_2^n is the schema of induction for Σ_n^b formulas of $\mathcal{L}^*$, i.e., formulas constructed like E_n formulas, but allowing the use of sharply bounded quantifiers, i.e., quantifiers of the form $\exists x{<}|t|$ and $\forall x{<}|t|$, in addition to regular bounded quantifiers (for a precise definition, see, e.g., [7], p. 21).

We should note that A. J. Wilkie observed (see [12]) that, by a result due to L. M. Adleman and K. Manders (see [1]), a positive solution to either Problem 1 or to Problem 2 would imply that $NP{=}co{-}NP$.

Finally, we mention two negative results, the first of which was proved by R. Kaye (see [6]) and the second by C. Pollett (see [10]), working in the same direction of research.

Theorem 4. *MT is not provable in* $IOpen$*, i.e., the theory of open induction.*

Theorem 5. *MT is not provable in* I^5E_1*, i.e., in the theory of five-lengths induction on* E_1 *definable predicates.*

In view of the above results/problems, one wonders whether or not it is possible to mimic the strategy used to obtain Theoremw 1 and 2, in order to prove a partial version of MT in $I\Delta_0{+}\Omega_1$. A first thought could be to restrict our attention to subclasses of the class of Σ_1 formulas, by controlling in some way the kind of bounded quantifiers occurring in the formulas. For example, we could allow the use of only sharply bounded quantifiers or one kind of regular bounded quantifiers and one kind of sharply bounded quantifiers.

The specific approach we have taken is based on the following assumptions:

(a) instead of considering Σ_1 formulas, we will consider formulas of the form $\exists\vec{z}\psi(\vec{x})$, where $\psi(\vec{x})$ is a formula involving (regular) bounded existential quantifiers plus sharply bounded universal quantifiers. We will denote this class of formulas by $\Sigma_{1,1}^b$, since it reminds us of Buss's class Σ_1^b, i.e., the class of formulas (of $\mathcal{L}^*$) closed under (regular) bounded existential quantifiers and sharply bounded quantifiers of any kind.

(b) we employ a low complexity definition of exponentiation (for small exponents), avoiding the use of binomial coefficients, and factorials and

(c) we allow the presence of a block of bounded universal quantifiers in front of the polynomial equation $p(\vec{x},\vec{y})=0$,

we were able to prove the following version of MT in $I\Delta_0+\Omega_1$.

Theorem 6. *For any $\Sigma^b_{1,1}$ formula $\theta(\vec{x},\vec{y})$ there exists a polynomial $p(\vec{x},\vec{y},\vec{z},\vec{u})\in\mathbb{Z}[\vec{x},\vec{y},\vec{z},\vec{u}]$ such that*

$$I\Delta_0+\Omega_1 \vdash \forall\vec{x}\forall\vec{y}[\text{“}\vec{y}\text{ are small”} \rightarrow (\theta(\vec{x},\vec{y}) \leftrightarrow \exists\vec{u}\, Q(\vec{z})\, p(\vec{x},\vec{y},\vec{z},\vec{u})=0)].$$

In this result, $\vec{y}$ are exactly the variables occurring as bounds of universal quantifiers in θ, $Q(\vec{z})$ denotes a block of (regular) bounded universal quantifiers and "$\vec{y}$ are small" means that all numbers of the form $a^{y_i^n}$ exist, where $n\in\mathbb{N}$ and y_i is one of the $\vec{y}$'s.

We can replace the system $I\Delta_0+\Omega_1$ in the above theorem with a suitable system extending $I\Delta_0$ that uses J. Robinson's Diophantine equation (see [11]) to define the notion of smallness and prove the same result. This system is $I\Sigma^b_{1,1}+E_{log}$, where the axiom E_{log} ensures that "small" numbers have all the standard properties of logarithms.

BIBLIOGRAPHY

[1] L. M. Adleman and K. Manders, Diophantine Complexity, in *17th Annual Symposium on Foundations of Computer Science*, 81–88, 1976.

[2] P. D' Aquino, Weak fragments of Peano Arithmetic, *The Notre Dame lectures*, 149–185, Lect. Notes Log., 18, *Assoc. Symbol. Logic, Urbana, IL*, 2005.

[3] P. Clote and J. Krajicek, Open problems, in *Arithmetic, Proof Theory, and Computational Complexity (Prague, 1991)*, vol. 23 of *Oxford Logic Guides*, Oxford University Press, 1993, 1–19.

[4] H. Gaifman and C. Dimitracopoulos, Fragments of Peano's arithmetic and the MRDP theorem. *Logic and algorithmic (Zurich, 1980)*, pp. 187–206, Monograph. Enseign. Math., 30, *Univ. Genève, Geneva*, 1982.

[5] R. Kaye. Diophantine Induction, *Ann. Pure Appl. Logic* 46 (1990), 1–40.

[6] R. Kaye. Open induction, Tennenbaum phenomena and complexity theory, in P. Clote and J. Krajicek (eds.), *Arithmetic, Proof Theory, and Computational Complexity (Prague, 1991)*, vol. 23 of *Oxford Logic Guides*, Oxford University Press, 1993, 222–37.

[7] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Cambridge University Press, 1995.

[8] Y. Matiyasevich, Enumerable sets are Diophantine, *Dokl. Acad. Nauk.* 191 (1970), 279–282.

[9] Y. Matyasevich, *Hilbert's Tenth Problem*, MIT Press, 1993.

[10] C. Pollett, On the bounded version of Hilbert's tenth problem, *Arch. Math. Logic* 42 (2003), 469–488.

[11] J. Robinson, Existential definability in arithmetic, *J. of Symbolic Logic* 36 (1971), 494–508.

[12] A. J. Wilkie. Applications of complexity theory to Σ_0-definability problems in arithmetic, *Model theory of algebra and arithmetic (Proc. Conf., Karpacz, 1979)*, pp. 363–369, Lecture Notes in Math., 834, Springer, Berlin, 1980.

Department of Mathematics, University of Aegean, 83200 Karlovassi, Greece
Email address: kornaros@aegean.gr

LIMOS, CNRS UMR 6158, Clermont Université, France
Email address: Alex.Esbelin@univ-bpclermont.fr