Versions of Matiyasevich's Theorem in subsystems of Arithmetic

Ch. Cornaros[1] & Henri - Alex Esbelin[2]

[1]University of the Aegean & [2]Université Clermont Auvergne

40ème Journées sur les Arithmétiques Faibles
25 October 2021

Basic Induction schemes and axioms

$I\Sigma_n$: induction for Σ_n formulas (plus base theory)

$B\Sigma_n$: $I\Delta_0$ + collection for Σ_n formulas

IE_n: induction for E_n formulas.
$I\exists_n$: induction for E_n formulas.
$IOpen$: induction for open formulas.

exp: "exponentiation is total"
Ω_1: "the function $x^{|y|}$ is total"

$\mathcal{L} = \{0, 1, +, \cdot, <\}$.

MT Theorem (Matiyasevich et. al, 1970)

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 $\mathbb{N} \models \forall \vec{x}[\theta(\vec{x}) \leftrightarrow \exists \vec{y}\, p(\vec{x},\vec{y})=0]$.

Theorem (Gaifman-Dimitracopoulos, 1982)

$I\Delta_0 + exp \vdash \mathrm{MT}$

Problems

1. Is the MT for bounded formulas provable in $I\Delta_0$?
   That is: Is every bounded formula equivalent in $I\Delta_0$ to an existential formula?
2. Is MT provable in $I\Delta_0 + \Omega_1$?

Theorem (R. Kaye, 1990)

$IE_1^- + E \vdash$ MT

where IE_1^- denotes the theory of parameter-free bounded existential induction and E denotes a specific $\forall\exists$ axiom expressing the existence of a function of exponential growth.

$IE_1^- + E$ is equivalent to $I\Delta_0 + exp$.

Negative Results

- (R. Kaye, 1991) MT is not provable in *IOpen*, i.e., the theory of open induction.
- (C. Pollett, 2003) MT is not provable in I^5E_1, i.e., in the theory of five-lengths induction on E_1 definable predicates.

  A. J. Wilkie observed that, by a result due to L. M. Adleman and K. Manders, a positive solution to either Problem 1 or to Problem 2 would imply that $NP{=}co{-}NP$.

Rough sketch of a proof of MT from $I\Delta_0 + exp$.

Basic steps

1. For every Σ_1 formula $\theta(\vec{x})$ there exists $p(\vec{x},\vec{y}) \in \mathbb{Z}(\vec{x},\vec{y})$ such that
$$PA^- \vdash \forall\vec{x}[\theta(\vec{x}) \leftrightarrow Q_1 \ldots Q_m\, p(\vec{x},\vec{y})=0],$$
where each of the Q_i's is of the form $\exists u$ or $\forall u<v$ (with u, v taken from $\vec{x},\vec{y}$) and $p(\vec{x},\vec{y}) = 0$ denotes an atomic formula.
2. Each unbounded existential quantifier $Q_i : \exists u$ after a block of bounded uiniversal quantifiers $\forall v < y$ can be bounded.

   $B\Sigma_1 : \forall\vec{z}\forall t\,[\forall x<t\exists\vec{y}\phi(x,\vec{y},\vec{z}) \rightarrow \exists s\forall x<t\exists\vec{y}<s\phi(x,\vec{y},\vec{z})]$.

Rough sketch of a proof of MT from $I\Delta_0 + exp$.

Basic steps

3. Use coding tools to eliminate all bounded universal quantifiers from the formula of Step 2.

   Example $\exists v \forall z{<}y \exists x_1{<}v \exists x_2{<}v\, (p(y, z, x_1, x_2){=}0)$
   $$\Updownarrow$$
   $$\exists v \exists u_1 \exists u_2\, \psi(y, z, x_1, x_2, u_1, u_2)$$

4. Replace the graph of exponentiation, of factorial and of binomial coefficients by $\exists_1$ formulas.

Question

How can we make it possible to mimic the above strategy to obtain a partial version of MT in $I\Delta_0{+}\Omega_1$?

D'Aquino considered an $E_1^{\#}$ formula defining the exponential function in $I\Delta_0{+}\Omega_1$, where # is an extra function symbol, but could not obtain a formula of the same complexity that could define the function $(k+1)\cdots(2k)$.

Quantifier Exchange Property

$(\forall x \leq |s|)(\exists y \leq t)A(x,y) \leftrightarrow$
$(\exists w{\leq}(2s{+}1)\#(4(2t{+}1)^2))(\forall x{\leq}|s|)(A(x,\beta(x{+}1,w))\wedge\beta(x{+}1,w){\leq}t)$

$\Sigma^b_{0,1}$ formulas

The class of $\Sigma^b_{0,1}$ formulas in $\mathcal{L}$ is the standard Δ_0, where all bounded universal quantifiers are "sharply bounded", i.e., their bounds will be replaced by "small" elements (in the sense of the specific model used).

Examples Given $M \models I\Delta_0$ and $a \in M$, we say a is "small" (in M), if $M \models$ "b^{a^n} exists", for all $b \in M$ and $n \in \mathbb{N}$.

In $M \models I\Delta_0 + \Omega_1$ if a is logarithmic then a is small!

MAIN result

For any $\Sigma^b_{0,1}$ formula $\theta(\vec{x}, \vec{y}, \vec{w})$, where the bounds of universal quantifiers of θ are (exactly) $\vec{y}$, there exists a polynomial $p(\vec{x}, \vec{y}, \vec{z}, \vec{u}, \vec{w}) \in \mathbb{Z}[\vec{x}, \vec{y}, \vec{z}, \vec{u}, \vec{w}]$ such that

$$I\Delta_0 \vdash \forall\vec{x}\forall\vec{y}[\text{``}\vec{y} \text{ are small''} \rightarrow (\exists\vec{w}\theta(\vec{x}, \vec{y}, \vec{w}) \leftrightarrow \exists\vec{u}\, Q(\vec{z})\, p(\vec{x}, \vec{y}, \vec{z}, \vec{u}, \vec{w}){=}0)],$$

where $Q(\vec{z})$ denotes a block of (normal) bounded universal quantifiers.

We should make use of a *low complexity definition of exponentiation* (for "small" exponents) and avoid of factorials and binomial coefficients!

Pell Equations (Julia Robinson 1971)

$p_R(a,x,y) : x^2-(a^2-1)y^2-1 = 0,\ a \geq 2$

Example: Let $a = 5$. The solution of index 0 is the pair $(x, y) = (1, 0)$. The pairs of positive solutions of the equation have exponential rate of growth:

$$(x_1^R, y_1^R) = (5, 1), (x_2^R, y_2^R) = (49, 10), (x_3^R, y_3^R) = (485, 99),$$
$$(x_4^R, y_4^R) = (4801, 980), (x_5^R, y_5^R) = (47525, 9701), \ldots$$

The pairs of remainders by division modulo $a - 1 = 4$ are

$$(1, 1), (1, 2), (1, 3), (1, 0), (1, 1), \ldots$$

so the index of (x_n^R, y_n^R) for $1 \leq n \leq a - 1$ can be easily found by dividing y_n^R by $a - 1$.

The solutions of $p_R(a, x, y) = 0$ correspond to powers of the $a + \sqrt{a^2 - 1}$: $(a + \sqrt{a^2 - 1})^2 = (5 + \sqrt{24})^2 = 49 + 10\sqrt{24}$, $(a + \sqrt{a^2 - 1})^3 = 485 + 99\sqrt{24}$, and generally $(a + \sqrt{a^2 - 1})^n = x_n^R + y_n^R \sqrt{a^2 - 1}$.

Definition

For any $a \geq 2$, $\psi_0(a, b, x, y)$ is the following formula, which is ∇_1 in IE_1:

$$(p_R(a, x, y) = 0 \wedge b > 0 \wedge a > b \wedge y > 0 \wedge x > 0 \wedge x \leq ay$$

$$\wedge y \equiv b \pmod{a-1} \wedge x \equiv 1 \pmod{a-1}) \vee (b = 0 \wedge y = 0 \wedge x = 1).$$

Lemma

Let $M \models I\Delta_0, a \geq 2, b \leq a-2$ and $y > 0$ be the smallest element of M such that for some x, $\psi_0(a, b+1, x, y)$. Then $(2a)^b$ exists and $(2a-1)^b \leq y \leq (2a)^b$.

Lemma

Let $M \models IE_1$ and $a \geq 2$. If $b \leq a-1$ and v is the smallest number such that $\exists u \leq av+1\, \psi_0(a, b, u, v)$, then

$$\forall c \leq b \forall v_1, v_2 \leq v \forall u_1 \leq av_1+1 \forall u_2 \leq av_2+1$$

$$[\psi_0(a, c, u_1, v_1) \wedge \psi_0(a, c, u_2, v_2) \rightarrow u_1 = u_2 \wedge v_1 = v_2]$$

$$\wedge$$

$$\forall c \leq b \exists v_1 \leq v \exists u_1 \leq av_1+1 \psi_0(a, c, u_1, v_1).$$

Definition

Let $a \geq 2, m \geq 0, y > 0$. We say y is an $(m+1)$-th a-power, if there is some $x > 0$ such that $\psi_0(a, m+1, x, y)$.

We denote this power with $y_{m+1}(a)$.

From the above Lemmas we have:

If $1 \leq b \leq a-1$ and there exists a number V (the smallest one) such that $\exists u \leq aV \psi_0(a, b, u, V)$ then, for any $m < b$, there is only *one* $y_{m+1}(a) \leq V$ such that

$$(2a-1)^m \leq y_{m+1}(a) \leq (2a)^m.$$

E_1 Parametric definition of exponation for models of IE_1

Theorem Let $M \models IE_1, a \geq 2$ and $b \leq 2a - 3$. Also suppose that b is small enough so that $A = y_{b+2}(2a)$ and $B = y_b(A)$ are defined in M. Then there is an E_1 formula $\phi_{A,B}(a, x, z)$ which satisfies all the basic properties of $z = a^x$ for all values $x \leq b$. Also, $z < 2ay_{x+2}(2a) - a^2 - 1$.

Lemma 5.5 p. 192 in the book *Logical Number Theory I, An introduction*

Corollary

Let $M \models I\Delta_0$ and $a \geq 2, b \leq 2a-3$. If $c' = a^{b^2}$ exists, then the elements A, B of the above Theorem also exist and the formula $\phi_{A,B}(a,x,z)$ is a good E_1 definition of exponentiation $a^x = z$, for all $x \leq b$ (with definable parameters A, B).

Quantifier Excange Property for models of $M \models I\Delta_0$

Lemma. Let $a \geq 2$ and $b \leq 2a-3$ such that a^{b^2} exists in M and let $\theta(x,y,a,b,d)$ be a Δ_0 formula such that $M \models \forall x \leq b \exists y < a\, \theta(x,y,a,b,d)$.Then

$$M \models \exists c < a^{b+1} \forall x \leq b\, \theta(x,(c)_x,a,b,d),$$

where $(c)_x$ denotes the $(x+1)$-th coefficient of the expansion of c to the base a.

Proof of the main result.

- Repeat Steps 1 and 2. We will take a formula of the form $\exists\vec{u}Q_1 \ldots Q_m\,[p(\vec{x},\vec{y},\vec{u})=0]$ where all blocks of existential quantifiers among $Q_1, \ldots Q_m$ have the *same* bound and all blocks of "sharply" bounded universal quantifiers among $Q_1, \ldots Q_m$ have also the same "small" bound.
- Don't go through step 3 or 4. Replace all existential quantifiers with their appropriate codes.

Note. All codes exists and $u = (c)_x$ can always replaced by a suitable ∇_1 formula using $\phi_{A,B}$:

$$(\exists z \leq c)(\exists s \leq c)(\exists z' \leq c)(\phi_{A,B}(a, x, z') \wedge z = [\tfrac{c}{z'}] \wedge s = [\tfrac{c}{az'}] \wedge u = z - as).$$

E_{log} denotes the axiom

$$\forall a, a' \geq 2 \forall b [\exists u, v \psi_0(a, b, u, v) \wedge b^2 < a' \rightarrow \exists u', v' \psi_0(a', b^2, u', v')].$$

E_{log} can be considered as the analog of Ω_1 over $I\Delta_0$. In fact, it can be proved that, E_{log} **is equivalent** to Ω_1 over $I\Delta_0$.

$I\Sigma^b_{0,1}$ is PA^- together with the schema of induction for all $\Sigma^b_{0,1}$ formulas of the form $\psi^{a,b}(x)$, in which any universally bounded quantified variable is bounded by a "logarithmic" b, i.e., the schema

$$\forall a \forall b [\text{“}b \text{ is logarithmic”} \wedge \psi^{a,b}(0) \wedge \forall x (\psi^{a,b}(x) \rightarrow \psi^{a,b}(x+1)) \rightarrow \forall x \psi^{a,b}(x)].$$

"**Smallness**" in models of IE_1:

Let $M \models IE_1$ and $b \in M$. We say "b is logarithmic" if

$$M \models \exists a \geq 2 \exists x \exists y \psi_0(a, b, x, y).$$

The system $IE_1 + E_{log}$ is a subsystem of $I\Sigma^b_{0,1} + E_{log}$ and strong enough to prove the expected properties of logarithmic elements: Let $M \models IE_1 + E_{log}$. The sum and product of any logarithmic elements $b_1, b_2 \in M$ is also logarithmic.

Proving MT Beyond $I\Delta_0 + \Omega_1$

Theorem

For any $\Sigma^b_{0,1}$ formula θ with parameters a, b, d, where a is the (uniform) bound of existential quantifiers and b is the (uniform) bound of universal quantifiers, there exist an E_2 formula ψ with new definable parameters and an $\exists U_1$ formula χ without new parameters such that

$$I\Sigma^b_{0,1} + E_{log} \vdash \forall a \forall b [\text{“b is logarithmic”} \rightarrow (\theta \leftrightarrow \psi) \wedge (\theta \leftrightarrow \chi)].$$

Problems

Theorem

$IE_2{+}E_{\log} \vdash I\Sigma^b_{0,1}$.

Open Problems

- Is $IE_2{+}E_{\log}$ equivalent with $I\Delta_0 + \Omega_1$?
- Can we prove that every $\exists\Sigma^b_{0,1}$ formula (of $\mathcal{L}$) with "sharply bounded" universal quantifiers is equivalent, over $I\Delta_0{+}\Omega_1$, to a Diophantine formula?
- Can we prove that every $\exists\Sigma^b_{0,0}$ formula (of $\mathcal{L}$) with all of its quantifiers "sharply bounded" is equivalent, over $I\Delta_0{+}\Omega_1$, to a Diophantine formula?
- Is every $\exists$SR formula equivalent, over $I\Delta_0{+}\Omega_1$, to a Diophantine formula?

SR= strictly rudimentary class of formulae introduced by Wilkie and Paris in 1987.

Thanks for your attetion!