$\mathfrak{D}$ versus $\mathfrak{E}$

Eugenio G. Omodeo

Le sommatorie $S_k(a) = \sum_{i=0}^{a} i^k$ si possono scrivere anche come polinomi

$$S_k(a) = \frac{1}{k+1} \sum_{i=0}^{k} (-1)^i \binom{k+1}{i} B_i \, a^{k+1-i}$$

di grado $k+1$ nell'indeterminata a, dove $B_0, B_1, B_2, \ldots$ sono i numeri razionali individuati da Jakob Bernoulli nel 1713, calcolabili tramite la formula di ricorrenza

$$B_0 = 1, \qquad B_m = -\sum_{j=0}^{m-1} \binom{m}{j} \frac{B_j}{m-j+1} \quad \text{per} \quad m > 0 \, .$$

Figura 2.5: Augusta Ada Byron, contessa di Lovelace, qui raffigurata in un '*doodle*' della Google, implementò attorno al 1843 quello che viene considerato il primo programma per *computer* della storia: aveva il compito di calcolare i numeri di Bernoulli (v. `http://it.wikipedia.org/wiki/Algoritmo_di_Ada_Lovelace_per_i_numeri_di_Bernoulli`).

Trieste, March 31, 2021

Outline

1. *Existentially definable*, in particular *Diophantine*, sets

2. Existential definitions of the *binomial coefficient*, *bitwise dominance*, *factorial*, *primality*

3. Should *bounded universal* quantifiers enter the kit ?

4. *The Davis-Putnam-Robinson theorem*
   with its enrichment due to Matiyasevich

Outline

5. Relations of *exponential growth*

Outline

1. *Existentially definable*, in particular *Diophantine*, sets
2. Existential definitions of the *binomial coefficient, bitwise dominance, factorial, primality*
3. Should *bounded universal* quantifiers enter the kit ?
4. *The Davis-Putnam-Robinson theorem* with its enrichment due to Matiyasevich
5. Relations of *exponential growth*
6. An open problem

Diophantine, and existentially definable, sets

A relation $\mathcal{D} \subseteq \mathbb{N}^{m}$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\blacksquare, \dots, \blacksquare)$ iff

$$\mathcal{D}(a_1, \dots, a_m) \iff \exists\, x_1 \cdots \exists\, x_k \quad \varphi(\underbrace{a_1, \dots, a_m}, \underbrace{x_1, \dots, x_k})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

A relation $\mathcal{D} \subseteq \mathbb{N}^{\boldsymbol{m}}$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\blacksquare, \ldots, \blacksquare)$ iff

$$\mathcal{D}(a_1, \ldots, a_{\boldsymbol{m}}) \iff \exists\, x_1 \cdots \exists\, x_{\boldsymbol{k}} \quad \varphi(\overbrace{\underbrace{a_1, \ldots, a_{\boldsymbol{m}}}_{\text{parameters}},\ \underbrace{x_1, \ldots, x_{\boldsymbol{k}}}_{\text{unknowns}}}^{\text{p.w. distinct variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- individual variables, specifically (as free var's) the shown ones,
- *positive* integer constants,

A relation $\mathcal{D} \subseteq \mathbb{N}^{m}$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\centerdot, \ldots, \centerdot)$ iff

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists\, x_1 \cdots \exists\, x_k \quad \varphi(\overbrace{\underbrace{a_1, \ldots, a_m}_{\text{parameters}}\,,\,\underbrace{x_1, \ldots, x_k}_{\text{unknowns}}}^{\text{p.w. distinct variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- addition operator, multiplication operator,
- the logical connectives $\&$, $\vee$, $\exists\, \upsilon$, $=$

A relation $\mathcal{D} \subseteq \mathbb{N}^m$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\blacksquare, \ldots, \blacksquare)$ iff

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{\underbrace{a_1, \ldots, a_m}_{\text{parameters}}, \underbrace{x_1, \ldots, x_k}_{\text{unknowns}}}^{\text{p.w. distinct variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- individual variables, specifically (as free var's) the shown ones,
- *positive* integer constants,
- addition operator, multiplication operator,
- the logical connectives $\&$, $\vee$, $\exists v$, $=$, and
- a predicate for $\mathcal{J}$.

A relation $\mathcal{D} \subseteq \mathbb{N}^{m}$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\blacksquare,\ldots,\blacksquare)$ iff

$$\mathcal{D}(a_1,\ldots,a_m) \iff \exists\, x_1 \cdots \exists\, x_k \quad \varphi(\overbrace{\underbrace{a_1,\ldots,a_m}_{\text{parameters}}\,,\,\underbrace{x_1,\ldots,x_k}_{\text{unknowns}}}^{\text{p.w. distinct variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- individual variables, specifically (as free var's) the shown ones,
- *positive* integer constants,
- addition operator, multiplication operator,
- the logical connectives $\&$, $\vee$, $\exists\,\mathfrak{v}$, $=$, and
- a predicate for $\mathcal{J}$.

When $\mathcal{J}(\mathfrak{b},\mathfrak{n},\mathfrak{c})$ is $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$, one calls $\mathcal{D}$ **exponential *Diophantine***.

A relation $\mathcal{D} \subseteq \mathbb{N}^{m}$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\blacksquare, \ldots, \blacksquare)$ iff

$$\mathcal{D}(a_1, \ldots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{\underbrace{a_1, \ldots, a_m}_{\text{parameters}}, \underbrace{x_1, \ldots, x_k}_{\text{unknowns}}}^{\text{p.w. distinct variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- individual variables, specifically (as free var's) the shown ones,
- *positive* integer constants,
- addition operator, multiplication operator,
- the logical connectives $\&$, $\vee$, $\exists v$, $=$, and
- a predicate for $\mathcal{J}$.

When $\mathcal{J}(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$ is $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$, one calls $\mathcal{D}$ **exponential *Diophantine***.

When $\mathcal{J}$ does not occur in φ, one simply calls $\mathcal{D}$ ***Diophantine***.

A relation $\mathcal{D} \subseteq \mathbb{N}^m$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\blacksquare, \dots, \blacksquare)$ iff

$$\mathcal{D}(a_1, \dots, a_m) \iff \exists x_1 \cdots \exists x_k \quad \varphi(\overbrace{\underbrace{a_1, \dots, a_m}_{\text{parameters}}, \underbrace{x_1, \dots, x_k}_{\text{unknowns}}}^{\text{p.w. distinct variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- individual variables, specifically (as free var's) the shown ones,
- *positive* integer constants,
- addition operator, multiplication operator,
- the logical connectives $\&$, $\vee$, $\exists v$, $=$, and
- a predicate for $\mathcal{J}$.

When $\mathcal{J}(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$ is $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$, one calls $\mathcal{D}$ **exponential *Diophantine***.

When $\mathcal{J}$ does not occur in φ, one simply calls $\mathcal{D}$ ***Diophantine***.

$\mathfrak{E}$

$\mathfrak{D}$

- $$(a+1)\cdot(a+1) \;=\; 1\;,$$
- $$a^a \;=\; 1 \quad \& \quad x^x \;=\; a+1$$

existentially define . . . *in terms of* triadic ***exponentiation*** $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

1

Both of

- $(a+1)\cdot(a+1) \;=\; 1\;,$
- $a^a \;=\; 1 \quad \& \quad x^x \;=\; a+1$

existentially define $\{\,0\,\}$ *in terms of* triadic ***exponentiation*** $\mathfrak{b}^{\mathfrak{n}}=\mathfrak{c}$.

Like 0, many other useful Diophantine constructs, e.g.

$$\blacksquare > \blacksquare,\quad \blacksquare \leqslant \blacksquare,\quad \blacksquare \nmid \blacksquare,\quad \blacksquare = \square,\quad \lfloor \blacksquare / \blacksquare \rfloor,\quad \blacksquare \,\%\, \blacksquare,$$

can—and will, tacitly—be added to the language of existential definitions.

1

Both of

- $$(a+1)\cdot(a+1) \;=\; 1\;,$$
- $$a^a \;=\; 1 \quad \& \quad x^x \;=\; a+1$$

existentially define $\{\,0\,\}$ *in terms of* triadic ***exponentiation*** $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

Like 0, many other useful Diophantine constructs, e.g.[1]

$$\blacksquare > \blacksquare,\quad \blacksquare \leqslant \blacksquare,\quad \blacksquare \nmid \blacksquare,\quad \blacksquare = \square,\quad \lfloor \blacksquare / \blacksquare \rfloor,\quad \blacksquare \,\%\, \blacksquare,$$

can—and will, tacitly—be added to the language of existential definitions.

[1] E.g.,

$$a \nmid b \iff \exists\, q\, \exists\, r\, \exists\, d\, \big(q\cdot a + r + 1 = b \;\&\; r + 1 + d + 1 = a\big)\,.$$

Definition (Univocal existential definitions)

An existential definition

$$\exists \vec{x} \quad \varphi(\, \vec{a},\, \vec{x}\,)$$

(as above) is ***single-fold*** if

$$\forall \vec{a}\, \exists \vec{y}\, \forall \vec{x} \Big[\quad \varphi(\, \vec{a},\, \vec{x}\,) \implies \vec{y} = \vec{x} \quad \Big]$$

(i.e., $\varphi(\, a_1, \ldots, a_{\boldsymbol{m}}\, ,\, x_1, \ldots, x_{\boldsymbol{k}}\,)$ never has multiple solutions).

Definition (Univocal existential definitions)

An existential definition

$$\exists \vec{x} \quad \varphi(\, \vec{a},\, \vec{x} \,)$$

(as above) is ***single-fold*** if

$$\forall \vec{a} \, \exists \vec{y} \, \forall \vec{x} \Big[\quad \varphi(\, \vec{a},\, \vec{x} \,) \implies \vec{y} = \vec{x} \quad \Big]$$

(i.e., $\varphi(\, a_1, \ldots, a_{\boldsymbol{m}} \,,\, x_1, \ldots, x_{\boldsymbol{k}} \,)$ never has multiple solutions).

Finite-fold existential definitions

The definition of ***finite-fold***-ness is akin:

$$\forall \vec{a} \, \exists y \, \forall \vec{x} \Big[\quad \varphi(\, \vec{a},\, \vec{x} \,) \implies y > \sum \vec{x} \quad \Big]$$

To each $\vec{a}$ there must correspond a *finite* number of solutions.

Existential definitions of the binomial coefficient, etc.

$$\binom{r}{j} = \left\lfloor \frac{(u+1)^r}{u^j} \right\rfloor \,\%\, u \quad \text{for any } u \geqslant 2^r + 0^{r+j}$$

$$j\,! = \left\lfloor \frac{r^j}{\binom{r}{j}} \right\rfloor \quad \text{for any } r > (2\,j)^{j+1}$$

$$\neg\,\exists\, x\,\exists\, y\,\big(\,p = (x+2)\,(y+2) \vee p = 0 \vee p = 1\,\big)$$
$$\iff\ \exists\, q\,\exists\, u\,\exists\, v\,\big(\,p = 2 + q\ \&\ p\,u - (q+1)!\,v = 1\,\big)$$

Fig. Binomial coefficient, factorial, and "p is a prime" are existentially definable by means of exponential Diophantine equations, cf. [Rob52, pp. 446–447]. Throughout, '%' designates the integer remainder operation.

$$\binom{r}{j} = \left\lfloor \frac{(u+1)^r}{u^j} \right\rfloor \% \; u \quad \text{for any } u \geqslant 2^r + 0^{r+j}$$

$$j\,! = \left\lfloor \frac{r^j}{\binom{r}{j}} \right\rfloor \quad \text{for any } r > (2\,j)^{j+1}$$

$$\begin{aligned}
& \neg\,\exists x\,\exists y\,\big(p = (x+2)\,(y+2) \vee p = 0 \vee p = 1\,\big) \\
\Longleftrightarrow\; & \exists q\,\exists\,u\,\exists v\,\big(p = 2 + q \;\&\; p\,u - (q+1)!\,v = 1\,\big) \\
\Longleftrightarrow\; & \exists q\,\exists\,u \qquad \big(p = 2 + q \;\&\; p\,u = (q+1)! \;\; + 1\,\big) \\
\Longleftrightarrow\; & \exists q\,\exists\,u \qquad \Big(p = 2 + q \cdot 0^{\left((q+1)!\,+1-(2+q)\,u\right)^2}\Big)
\end{aligned}$$

Fig. Binomial coefficient, factorial, and "p is a prime" are existentially definable by means of exponential Diophantine equations, cf. [Rob52, pp. 446–447]. Throughout, '%' designates the integer remainder operation.

$$\binom{r}{j} = \left\lfloor \frac{(u+1)^r}{u^j} \right\rfloor \,\%\, u \quad \text{for any } u \geqslant 2^r + 0^{r+j}$$

$$j\,! = \left\lfloor \frac{r^j}{\binom{r}{j}} \right\rfloor \quad \text{for any } r > (2\,j)^{j+1}$$

$$\neg\,\exists x\,\exists y\,(\,p = (x+2)\,(y+2) \vee p = 0 \vee p = 1\,)$$
$$\iff \exists q\,\exists\,u\,\exists v\,(\,p = 2 + q \;\&\; p\,u - (q+1)!\,v = 1\,)$$
$$\iff \exists q\,\exists\,u \quad (\,p = 2 + q \;\&\; p\,u = (q+1)! \;\; + 1\,)$$
$$\iff \exists q\,\exists\,u \quad \left(p = 2 + q \cdot 0^{\left((q+1)!\,+1-(2+q)\,u\right)^2}\right)$$

Fig. Binomial coefficient, factorial, and "p is a prime" are existentially definable by means of exponential Diophantine equations, cf. [Rob52, pp. 446–447]. Throughout, '%' designates the integer remainder operation.

Ibn al-Haytham (Alhazen)

Exercise

Explain the above specifications of primality, by means of Bézout's lemma and Wilson's theorem.

ℓ	chiave	base	coefficiente binomiale $\binom{\ell}{j}$						
0	1	2	$\cdots$	0	0	0	0	0	1
1	2	4	$\cdots$	0	0	0	0	1	1
2	3	8	$\cdots$	0	0	0	1	2	1
3	4	16	$\cdots$	0	0	1	3	3	1
4	5	32	$\cdots$	0	1	4	6	4	1
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
			$\underbrace{\qquad}_{j=\ldots,5,4,3,2,1,0}$						

FIGURA: Riguardo alla cifratura del coefficiente binomiale

$$\mathrm{digit}(a,b,j) \;=\; d \iff_{\mathrm{Def}} \exists\, v\, \exists\, w\, \exists\, z \,\big(\; a = w\, b^{z} + d\, b^{j} + v \;\;\&\;\; z = j+1 \;\;\&\;\; d < b \;\;\&\;\; v < b^{j} \,\big)$$

$$\iff \left\lfloor \frac{a}{b^{j}} \right\rfloor \% \; b \;=\; d\,,$$

$$\mathrm{entry}(a,k,j) \;=\; c \iff_{\mathrm{Def}} \mathrm{digit}(a\,,\,2^{k}\,,\,j) \;=\; c\,,$$

$$\binom{\ell}{j} \;=\; c \iff_{\mathrm{Def}} \mathrm{entry}\left((2^{\ell+1}+1)^{\ell}\,,\,\ell+1\,,\,j\right)\,.$$

Capturing bitwise dominance via Lucas's thm.

Lucas's congruence

$$\binom{\sum_{i=0}^{k} b_i\, p^i}{\sum_{i=0}^{k} a_i\, p^i} \equiv \prod_{i=0}^{k} \binom{b_i}{a_i} \pmod{p}$$

holds when p is a prime number and

$$\{a_0, b_0, \ldots, a_k, b_k\} \subseteq \{0, \ldots, p-1\}$$

Consider the relationship

$$a \sqsubseteq b$$

holding between $a = \sum_{i=0}^{k} a_i 2^i$ and $b = \sum_{i=0}^{k} b_i 2^i$, with $a_0, b_0, \ldots, a_k, b_k \in \{0, 1\}$, when $a_i \leqslant b_i$ for $i = 0, \ldots, k$.

Bearing in mind that

$$\binom{0}{1} = 0 \quad \text{and} \quad 1 = \binom{0}{0} = \binom{1}{0} = \binom{1}{1},$$

we get that $a \sqsubseteq b$ holds if and only if $\binom{b}{a}$ is odd.

Summation of a generalized geometric progression

Yuri V. Matiyasevich [Mat93, pp. 202 and 203] shows that the triadic relation

$$\left\{ \left\langle \sum_{i=0}^{a} b^i \, i^k, \; a, \; b \right\rangle \; : a \in \mathbb{N}, \; b \in \mathbb{N} \right\}$$

is exponential Diophantine for each $k \in \mathbb{N}$.

Yuri V. Matiyasevich [Mat93, pp. 202 and 203] shows that the triadic relation

$$\left\{ \left\langle \sum_{i=0}^{a} b^i \, i^k, \; a, \; b \right\rangle \; : a \in \mathbb{N}, \; b \in \mathbb{N} \right\}$$

is exponential Diophantine for each $k \in \mathbb{N}$.

Jacob Bernoulli (XVII century) had a resut of the same flavour: For each $k \in \mathbb{N}$, the dyadic relation

$$\left\{ \left\langle \underbrace{\sum_{i=0}^{a} i^k}_{c}, \; a \right\rangle \; : a \in \mathbb{N} \right\}$$

is defined by an equation

$$c \; = \; B(a) \, ,$$

where $B \in \mathbb{Q}[a]$ has degree $k+1$.

Would we make the assembly kit stronger by adding bounded $\forall$ to it ?

EXAMPLE ("b IS A POWER OF 2")

$$
\begin{aligned}
& \exists \ell \;\; 2^{\ell} = b \\
\Longleftrightarrow\;\; & \forall u \leqslant b \;\; \forall v \leqslant b \;\;\; b \neq (2\,u + 3) \cdot v \\
\Longleftrightarrow\;\; & \forall u \leqslant b \;\; \forall v \leqslant b \;\;\; \exists w \; \big[\, b - (2\,u + 3) \cdot v \,\big]^2 = 1 + w
\end{aligned}
$$

Arithmetical specifications involving $\forall\, \upsilon \leqslant t$

Example ("b is a power of 2")

$$
\begin{aligned}
& \exists\, \ell \;\; 2^{\ell} = b \\
\Longleftrightarrow \;\; & \forall\, u \leqslant b \;\; \forall\, v \leqslant b \;\;\; b \neq (2\,u+3)\cdot v \\
\Longleftrightarrow \;\; & \forall\, u \leqslant b \;\; \forall\, v \leqslant b \;\;\; \exists\, w \; \left[\, b-(2\,u+3)\cdot v\,\right]^2 = 1+w \\
\Longleftrightarrow \;\; & \exists\, \ell\, \exists\, s\, \exists\, d \Big[\;\; 1 = s \,\%\, \big(1+d\big) \;\;\&\; \\
& \qquad\qquad b = s \,\%\, \big(1+(\ell+1)\cdot d\big) \;\;\&\; \\
& \qquad\qquad \forall i \leqslant \ell \;\Big[\; s \,\%\, \big(1+(i+2)\cdot d\big) \;=\; \\
& \qquad\qquad\qquad\qquad 2\cdot \big[s \,\%\, \big(1+(i+1)\cdot d\big]\;\Big]\Big] .
\end{aligned}
$$

The collection $\mathfrak{P}$ of ***primitive recursive functions*** is the smallest[2] set of (total) functions, with arguments and result in $\mathbb{N}$:

- to which all *initial functions* belong;
- which is closed with respect to *composition* and to *recursion*.

[2] I.e., minimum with respect to $\subseteq$.

The collection $\mathfrak{P}$ of ***primitive recursive functions*** is the smallest[2] set of (total) functions, with arguments and result in $\mathbb{N}$:

- to which all *initial functions* belong;
- which is closed with respect to *composition* and to *recursion*.

Our ***initial functions*** are: The everywhere null functions, the successor function:

$$\langle x_1, \ldots, x_n \rangle \stackrel{\mathsf{O}_n}{\longmapsto} 0 \qquad (n = 0, 1, \ldots),$$
$$x \stackrel{\mathsf{S}}{\longmapsto} x + 1,$$

and all

[2] I.e., minimum with respect to $\subseteq$.

The collection $\mathfrak{P}$ of ***primitive recursive functions*** is the smallest[2] set of (total) functions, with arguments and result in $\mathbb{N}$:

- to which all *initial functions* belong;
- which is closed with respect to *composition* and to *recursion*.

Our ***initial functions*** are: The everywhere null functions, the successor function:

$$\langle x_1, \ldots, x_n \rangle \overset{\mathsf{O}_n}{\longmapsto} 0 \qquad (\; n = 0, 1 \qquad) \,,$$

$$x \overset{\mathsf{S}}{\longmapsto} x + 1 \,,$$

and all projections associated with positive integers:

$$\langle x_1, \ldots, x_n \rangle \overset{\mathsf{I}_{n,k}}{\longmapsto} x_k \qquad (\; n \geqslant k \geqslant 1 \;).$$

[2] I.e., minimum with respect to $\subseteq$.

Let:

f	be a function of k arguments,
$g_1, \ldots, g_k$	be functions of M arguments.

One defines the ***composition*** h of f with $g_1, \ldots, g_k$ thus:

$$\langle x_1, \ldots, x_M \rangle \stackrel{h}{\longmapsto} f\big(g_1(x_1, \ldots, x_M), \ldots, g_k(x_1, \ldots, x_M)\big)\,.$$

Let:

$$\begin{array}{ll} f & \text{be a function of } k \text{ arguments,} \\ g_1, \ldots, g_k & \text{be functions of } M \text{ arguments.} \end{array}$$

One defines the ***composition*** h of f with $g_1, \ldots, g_k$ thus:

$$\langle x_1, \ldots, x_M \rangle \stackrel{h}{\longmapsto} f\big(g_1(x_1, \ldots, x_M), \ldots, g_k(x_1, \ldots, x_M)\big) .$$

Example. Through composition, from O_1 and S, one gets all constant functions:

$$\overbrace{S(\cdots S(}^{c \text{ times}}\ O_1(\,x\,)\ \overbrace{)\cdots)}^{c \text{ times}} .$$

Recursion, when applied to f and g such that

f is an n–adic function
(when $n = 0$, this means that f is a *constant*)

g is an $n+2$ adic function

yields the $n+1$ adic function

h such that:

$$\begin{array}{rcl} h(\vec{x},0) & = & f(\vec{x}) \\ h(\vec{x},t+1) & = & g\big(\vec{x},t,h(\vec{x},t)\big) \end{array}$$

(Here $\vec{x} =_{\mathrm{Def}} x_1, \ldots, x_n$)

THEOREM (GÖDEL–DAVIS)

The graph

$$\{ \langle \vec{a},\ h(\vec{a}) \rangle \ : \vec{a} \in \mathbb{N}^{\boldsymbol{m}} \}$$

of any $\boldsymbol{m}$*-adic primitive recursive function* h *is expressible through an arithmetical formula in which:*

- $\forall$*-quantifiers appear only in the bounded form* $\forall\, a \leqslant t$,
- *negation* ($\neg$, $\neq$) *does not appear.*
- ($\exists$*-quantifiers can occur without restrictions*)

THEOREM (DAVIS NORMAL FORM 1950 TANTALIZING !)

Given a $\boldsymbol{m}$*-tuple* $\langle h_1, \dots, h_{\boldsymbol{m}} \rangle$ *of monadic primitive recursive functions, one can construct a polynomial* D *with integer coefficients such that*

$$\langle a_1, \dots, a_{\boldsymbol{m}} \rangle \ \in \ \{ \langle h_1(i), \dots, h_{\boldsymbol{m}}(i) \rangle \ : i \in \mathbb{N} \}$$

$$\Longleftrightarrow$$

$$\exists\, y\, \forall\, u \leqslant y\ \exists\, v_1 \leqslant y \cdots \exists\, v_\kappa \leqslant y\ \ D(a_1, \dots, a_{\boldsymbol{m}}, y, u, v_1, \dots, v_\kappa) = 0\,.$$

$$\mathsf{O}_n(a_1, \ldots, a_n) = b \quad \rightsquigarrow \quad b = 0\,,$$
$$\mathsf{S}(a) = b \quad \rightsquigarrow \quad b = a + 1\,,$$
$$\mathsf{I}_{n,k}(a_1, \ldots, a_n) = b \quad \rightsquigarrow \quad b = a_k\,.$$

When h results from composition of f with $g_1, \ldots, g_k$:

$$h(a_1, \ldots, a_M) = b \quad \rightsquigarrow \quad \exists\, y_1 \cdots \exists\, y_k \big(f(y_1, \ldots, y_k) = b \;\&\; \textstyle\bigwedge_{j=1}^{k} g_j(a_1, \ldots, a_M) = y_j \big)\,.$$

When h results through recursion from f and g,

$$h(\vec{a}, \ell) = b \quad \rightsquigarrow \quad \exists\, s\, \exists\, d \Big[\; f(\vec{a}) = s \,\%\, (1 + d) \;\& \; b = s \,\%\, (1 + (\ell + 1) \cdot d) \;\& \; \forall i \leqslant \ell \big[\, s \,\%\, (1 + (i + 2) \cdot d) \; = \; g\Big(\vec{a},\, i,\, s \,\%\, (1 + (i + 1) \cdot d)\Big) \,\big] \,\Big]\,.$$

Gödel's lemma 1931

Lemma (Gödel's variant of Chinese remainder th'm)

For any tuple $\langle a_1, \ldots, a_\ell \rangle \in \mathbb{N}^\ell$*, there exist* $\boldsymbol{s}, \boldsymbol{\kappa} \in \mathbb{N}$ *such that*

$$a_i \quad = \quad \boldsymbol{s} \,\%\, (\, i\, \boldsymbol{\kappa} + 1\,)\,, \quad \textit{for} \quad i = 1, \ldots, \ell\,.$$

LEMMA (GÖDEL'S VARIANT OF CHINESE REMAINDER TH'M)

For any tuple $\langle a_1, \ldots, a_\ell \rangle \in \mathbb{N}^\ell$, *there exist* $\boldsymbol{s}, \kappa \in \mathbb{N}$ *such that*

$$a_i \;=\; \boldsymbol{s} \,\%\, (\, i\,\kappa + 1\,)\,, \quad \textit{for} \quad i = 1, \ldots, \ell\,.$$

One may also

- *require that* κ *be a multiple of* $\ell\,!$ *and, for each* κ,
- *enforce uniqueness of* $\boldsymbol{s}$ *by requiring that* $\boldsymbol{s} < \prod_{i=1}^{\ell}(i\,\kappa + 1)$.

Pairing theorem:

There exist primitive recursive,
Diophantine functions

$[a, b]$, $\mathrm{sn}(c)$, $\mathrm{dx}(c)$,

with operands and result in $\mathbb{N}$,
satisfying the conditions

1. $\mathrm{sn}\big([a, b]\big) = a$, $\mathrm{dx}\big([a, b]\big) = b$;
2. $\big[\mathrm{sn}(c), \mathrm{dx}(c)\big] = c$;
3. $\mathrm{sn}(c) \leqslant c$, $\mathrm{dx}(c) \leqslant c$.

$$\langle a, b \rangle \quad \mapsto \quad \frac{(a+b)^2 + 3\,a + b}{2}$$

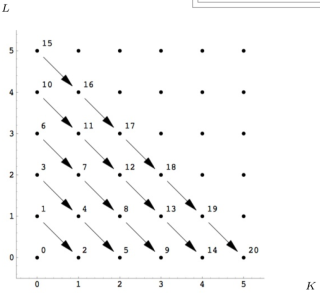
Pairing theorem:

There exist primitive recursive, Diophantine functions

$[a, b]$, $\mathrm{sn}(c)$, $\mathrm{dx}(c)$,

with operands and result in $\mathbb{N}$, satisfying the conditions

1. $\mathrm{sn}\big([a, b]\big) = a$, $\quad \mathrm{dx}\big([a\,,\ b]\big) = b$;
2. $\big[\mathrm{sn}(c), \mathrm{dx}(c)\big] = c$;
3. $\mathrm{sn}(c) \leqslant c$, $\qquad \mathrm{dx}(c) \leqslant c$.



u	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ku	0	0	1	0	1	2	0	1	2	3	0	1	2	3	4	0
Lu	0	1	0	2	1	0	3	2	1	0	4	3	2	1	0	5

Pairing, after George Cantor (1878), and its projections

LEMMA (USEFUL EXERCISE!)

Let $[\cdot, \cdot]$ comply with the pairing theorem. If P is a polynomial with integer coefficients in the variables $a_1, \ldots, a_n, w, u, v_1, \ldots, v_r$, then the two formulae

$$\exists\, w\, \forall\, u \leqslant w\, \exists\, v_1 \cdots \exists\, v_r\ P = 0\,,$$

$$\exists\, y\, \forall\, u \leqslant y\, \exists\, v_1 \leqslant y \cdots \exists\, v_r \leqslant y\, \exists\, w \leqslant y\, \exists\, z \leqslant y\, \exists\, t \leqslant y$$
$$\Big(y = [w, z]\ \&\ \big(u = w + 1 + t\ \vee\ P = 0 \big) \Big)$$

are equivalent to each other over $\mathbb{N}$.

The DPR theorem and
its single-fold improvement

A crucial result

Now consider listable[3] (aka r.e.) sets.

[3] **Clue:** A set is *listable* if its elements can be generated exhaustively by an algorithmic (perhaps non-terminating) procedure.

A crucial result

DPR theorem (See [DPR61])

Each listable set is *existentially definable in terms of exponentiation*.

This was discovered by

Martin Davis,

Hilary Putnam,

Julia Robinson.

[3] **Clue:** A set is *listable* if its elements can be generated exhaustively by an algorithmic (perhaps non-terminating) procedure.

DPR THEOREM (SEE [DPR61])

Graph, as well as *domain* $\mathcal{D}$, of any partially computable function

$$\mathcal{F} : \mathbb{N}^{\boldsymbol{m}} \rightharpoonup \mathbb{N}$$

are exponential Diophantine.

DPR THEOREM (SEE [DPR61])

Graph, as well as *domain* $\mathcal{D}$, of any partially computable function

$$\mathcal{F} : \mathbb{N}^{m} \longrightarrow \mathbb{N}$$

are exponential Diophantine.

$$\mathcal{F}(a_1, \ldots, a_m) = c \iff (\exists\, x_1 \cdots \exists\, x_k)\ \varphi(\underbrace{a_1, \ldots, a_m, c}_{\text{parameters}}, \underbrace{x_1, \ldots, x_k}_{\text{unknowns}})$$

$$\mathcal{D}(a_1, \ldots, a_m) \iff (\exists\, y\, \exists\, x_1 \cdots \exists\, x_k)\ \varphi(\underbrace{a_1, \ldots, a_m}_{\text{parameters}}, \underbrace{y, x_1, \ldots, x_k}_{\text{unknowns}})$$

DPR theorem (See [DPR61])

Graph, as well as *domain* $\mathcal{D}$, of any partially computable function

$$\mathcal{F} : \mathbb{N}^{\boldsymbol{m}} \longrightarrow \mathbb{N}$$

are exponential Diophantine.

Significant improvement to DPR (see [Mat74])

Both of the above relations admit existential *single-fold* definitions in terms of exponentiation.

$$\mathcal{F}(a_1, \dots, a_{\boldsymbol{m}}) = c \iff (\exists x_1 \cdots \exists x_{\boldsymbol{k}})\ \varphi(\underbrace{a_1, \dots, a_{\boldsymbol{m}}, c}_{\text{parameters}}, \underbrace{x_1, \dots, x_{\boldsymbol{k}}}_{\text{unknowns}})$$

$$\mathcal{D}(a_1, \dots, a_{\boldsymbol{m}}) \iff (\exists y \exists x_1 \cdots \exists x_{\boldsymbol{k}})\ \varphi(\underbrace{a_1, \dots, a_{\boldsymbol{m}}}_{\text{parameters}}, \underbrace{y, x_1, \dots, x_{\boldsymbol{k}}}_{\text{unknowns}})$$

DPR THEOREM (SEE [DPR61])

Graph, as well as *domain* $\mathcal{D}$, of any partially computable function

$$\mathcal{F} : \mathbb{N}^{\boldsymbol{m}} \rightharpoonup \mathbb{N}$$

are exponential Diophantine.

SIGNIFICANT IMPROVEMENT TO DPR (SEE [MAT74])

Both of the above relations admit existential *single-fold* definitions in terms of exponentiation.

Specifically, for some polynomial G with integral coefficients,

$$\mathcal{F}(a_1, \ldots, a_{\boldsymbol{m}}) = c \iff (\exists\, x_0\, \exists\, x_1 \cdots \exists\, x_{\boldsymbol{k}})\big[\; 4^{x_0} + x_0 = G(\, a_1, \ldots, a_{\boldsymbol{m}}, c\,, x_1, \ldots, x_{\boldsymbol{k}}\,)\;\big].$$

Dyadic relations of exponential growth

Diophantine reduction of exponentiation to any $\mathcal{J}$ of exponential growth [Rob52]

Suppose now that $\mathcal{J}$ is a dyadic relation satisfying:

Diophantine reduction of exponentiation to <u>any</u> $\mathcal{J}$ of exponential growth [Rob52]

Suppose now that $\mathcal{J}$ is a dyadic relation satisfying:

1. $\mathcal{J}(u,v) \implies v < u^u$;
2. $\forall\, k\, \exists\, u\, \exists\, v \left[\, \mathcal{J}(\, u\, ,\, v\,)\ \&\ u^k < v \,\right]$;
3. $\mathcal{J}(u,v) \implies u > 1$.

After [Rob52], such a relation is said to be of ***exponential growth***.

Suppose now that $\mathcal{J}$ is a dyadic relation satisfying:

1. $\mathcal{J}(u, v) \implies v < u^u$;
2. $\forall k \, \exists u \, \exists v \, [\, \mathcal{J}(u, v) \; \& \; u^k < v \,]$;
3. $\mathcal{J}(u, v) \implies u > 1$.

After [Rob52], such a relation is said to be of ***exponential growth***.

HISTORICAL EXAMPLE ⌣̈ DIOPHANTINE! ⌣̈

Take

$$\mathcal{J} = \left\{ \langle u \,, \phi_{2u} \rangle \mid u > 1 \right\} ,$$

where

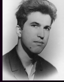
$$\phi_0 = 0 \,, \quad \phi_1 = 1 \,, \quad \phi_{h+2} = \phi_{h+1} + \phi_h \,,$$

for $h = 0, 1, 2, \ldots$ (See [Mat70b])

$$
\begin{aligned}
\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c} \iff (\exists\, a, d, \ell, s, x, h)\Big[\; & (\mathfrak{c}-1)^2 + \mathfrak{n} = 0 && \vee \\
& (\mathfrak{n} \geqslant 1 \,\&\, \mathfrak{c} + \mathfrak{b} = 0) && \vee \\
\Big(& \mathfrak{n} \geqslant 1 \;\&\; \mathfrak{b} \geqslant 1 \;\&\; \boxed{\mathcal{J}(a,d)} \;\&\; d > \ell && \& \\
& \ell^2 = (a^2-1)\,\big[(a-1)\,s + \mathfrak{n}\big]^2 + 1 && \& \\
& x^2 = (\mathfrak{b}+\mathfrak{n})^3\,(\mathfrak{b}+\mathfrak{n}+2)\,(h+1)^2 + 1 && \& \\
& 2\,a\,\mathfrak{b} - \mathfrak{b}^2 - 1 \geqslant (\mathfrak{b}+\mathfrak{n}+1)\,x \;\&\; a > \mathfrak{b}+\mathfrak{n} && \& \\
& (2\,a\,\mathfrak{b} - \mathfrak{b}^2 - 1)\,\%\,\big[\ell - (a-\mathfrak{b})\big((a-1)\,s+\mathfrak{n}\big)\big] = \mathfrak{c} \Big)\Big].
\end{aligned}
$$

Conclusions

Open p.: Does exponentiation admit a single-fold (or at least finite-fold) Diophantine definition ?



"After the DPR-theorem was proved in 1961, in order to establish the existence of Diophantine representations for *every* effectively enumerable set it was sufficient to find a Diophantine representation for *one particular* set of triples

$$\{\langle a, b, c\rangle \quad | \quad a = b^c\} \ . \qquad (12)$$

Today we are in a similar position with respect to single-fold (and finite-fold) Diophantine representations: now that we can construct single-fold exponential Diophantine representations for all effectively enumerable sets, in order to transform them into single-fold (or finite-fold) genuinely Diophantine representations, it would be sufficient to find a single-fold (or, respectively, finite-fold) Diophantine representation for the same set of triples (12) $\cdots$" [Mat10, p. 748]

Voci bibliografiche

Martin Davis, Hilary Putnam, and Julia Robinson.
The decision problem for exponential Diophantine equations.
Annals of Mathematics, Second Series, 74(3):425–436, 1961.

Ju. V. Matijasevič.
Enumerable sets are Diophantine.
Soviet Mathematics. Doklady, 11(3):354–358, 1970.
(Translated from [Mat70b]).

Yu. V. Matiyasevich.
Diofantovost' perechislimykh mnozhestv.
Doklady Akademii Nauk SSSR, 191(2):279–282, 1970.
(Russian. Available in English translation as [Mat70a]; translation reprinted in [Sac03, pp. 269–273]).

Yu. V. Matiyasevich.
Sushchestvovanie neèffektiviziruemykh otsenok v teorii èkponentsial'no diofantovykh uravneniĭ.
Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI), 40:77–93, 1974.
(Russian. Translated into English as Yu. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations, *Journal of Soviet Mathematics*, 8(3):299–311, 1977).

Yuri Vladimirovich Matiyasevich. *Hilbert's tenth problem*.
The MIT Press, Cambridge (MA) and London, 1993.

Yu. Matiyasevich.
Towards finite-fold Diophantine representations.
Journal of Mathematical Sciences, 171(6):745–752, Dec 2010.

Julia Robinson.
Existential definability in arithmetic.
Transactions of the American Mathematical Society, 72(3):437–449, 1952.
Reprinted in [Rob96, p. 47ff.].

Julia Robinson.
Diophantine decision problems.
In W. J. LeVeque, editor, *Studies in Number Theory*, volume 6 of *Studies in Mathematics*, pages 76–116. Mathematical Association of America, 1969.

Julia Robinson.
The collected works of Julia Robinson, volume 6 of *Collected Works*.
American Mathematical Society, Providence, RI, 1996.
ISBN 0-8218-0575-4. With an introduction by Constance Reid. Edited and with a foreword by Solomon Feferman. xliv+338 pp.

Gerald E. Sacks, editor.
Mathematical Logic in the 20th Century.
Singapore University Press, Singapore; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.