Tarski's Exponential Function Problem

Lothar Sebastian Krapp

Universität Konstanz, Fachbereich Mathematik und Statistik

06 July 2017

Logic Colloquium

Statement of the Problem

Statement of the Problem

Question

Is $(\mathbb{R}, +, -, \cdot, 0, 1, <, \exp)$ decidable? (Tarski 1948)

Statement of the Problem

Question

Is $(\mathbb{R}, +, -, \cdot, 0, 1, <, \exp)$ decidable? (Tarski 1948)

— or equivalently —

Question

Is the theory of $(\mathbb{R}, +, -, \cdot, 0, 1, <, \exp)$ recursively axiomatizable?

Setting: Model Theory

Setting: Model Theory

- fixed logical framework (logical connectives, quantifiers, notion of provability, etc.)

Setting: Model Theory

- fixed logical framework (logical connectives, quantifiers, notion of provability, etc.)
- specific model theoretical language consisting of constants, unary functions, and relations
  (e.g. $\mathcal{L}_{\mathrm{or}} = \{+, -, \cdot, 0, 1, <\}$)

Setting: Model Theory

- fixed logical framework (logical connectives, quantifiers, notion of provability, etc.)
- specific model theoretical language consisting of constants, unary functions, and relations
  (e.g. $\mathcal{L}_{\mathrm{or}} = \{+, -, \cdot, 0, 1, <\}$)
- formulas in the language
  (e.g. $\forall x\ (x < 0 \to \exists y\ y \cdot y = x)$)

Setting: Model Theory

- fixed logical framework (logical connectives, quantifiers, notion of provability, etc.)
- specific model theoretical language consisting of constants, unary functions, and relations
  (e.g. $\mathcal{L}_{\mathrm{or}} = \{+, -, \cdot, 0, 1, <\}$)
- formulas in the language
  (e.g. $\forall x\ (x < 0 \to \exists y\ y \cdot y = x)$)
- structures interpreting the language
  (e.g. $(\mathbb{R}, +, -, \cdot, 0, 1, <)$)

Notation

Fix a language $\mathcal{L}$ and let ϕ be an $\mathcal{L}$-sentence and $\mathcal{M}$ an $\mathcal{L}$-structure.

Notation

Fix a language $\mathcal{L}$ and let ϕ be an $\mathcal{L}$-sentence and $\mathcal{M}$ an $\mathcal{L}$-structure.

$\mathcal{T}$ — an $\mathcal{L}$-theory, i.e. a set of $\mathcal{L}$-sentences ($\mathcal{L}$-formulas without free variables)

Notation

Fix a language $\mathcal{L}$ and let ϕ be an $\mathcal{L}$-sentence and $\mathcal{M}$ an $\mathcal{L}$-structure.

$\mathcal{T}$ — an $\mathcal{L}$-theory, i.e. a set of $\mathcal{L}$-sentences ($\mathcal{L}$-formulas without free variables)

$\mathcal{T} \vdash \phi$ — ϕ is provable from $\mathcal{T}$

(e.g. $\{\forall x \, \neg x \cdot x < 0\} \vdash \neg 1 \cdot 1 < 0$)

Notation

Fix a language $\mathcal{L}$ and let ϕ be an $\mathcal{L}$-sentence and $\mathcal{M}$ an $\mathcal{L}$-structure.

$\mathcal{T}$ — an $\mathcal{L}$-theory, i.e. a set of $\mathcal{L}$-sentences ($\mathcal{L}$-formulas without free variables)

$\mathcal{T} \vdash \phi$ — ϕ is provable from $\mathcal{T}$

(e.g. $\{\forall x \, \neg x \cdot x < 0\} \vdash \neg 1 \cdot 1 < 0$)

$\mathcal{M} \models \phi$ — ϕ is valid in $\mathcal{M}$

(e.g. $(\mathbb{R}, +, -, \cdot, 0, 1, <) \models \exists x \; x \cdot x = 1 + 1$,
but $(\mathbb{Q}, +, -, \cdot, 0, 1, <) \not\models \exists x \; x \cdot x = 1 + 1$)

Notation

Fix a language $\mathcal{L}$ and let ϕ be an $\mathcal{L}$-sentence and $\mathcal{M}$ an $\mathcal{L}$-structure.

$\mathcal{T}$ — an $\mathcal{L}$-theory, i.e. a set of $\mathcal{L}$-sentences ($\mathcal{L}$-formulas without free variables)

$\mathcal{T} \vdash \phi$ — ϕ is provable from $\mathcal{T}$

(e.g. $\{\forall x \, \neg x \cdot x < 0\} \vdash \neg 1 \cdot 1 < 0$)

$\mathcal{M} \models \phi$ — ϕ is valid in $\mathcal{M}$

(e.g. $(\mathbb{R}, +, -, \cdot, 0, 1, <) \models \exists x \, x \cdot x = 1 + 1$,
but $(\mathbb{Q}, +, -, \cdot, 0, 1, <) \not\models \exists x \, x \cdot x = 1 + 1$)

$\mathcal{T} \models \phi$ — for all $\mathcal{M} \models \mathcal{T}$ we have $\mathcal{M} \models \phi$

Notation

Fix a language $\mathcal{L}$ and let ϕ be an $\mathcal{L}$-sentence and $\mathcal{M}$ an $\mathcal{L}$-structure.

$\mathcal{T}$ — an $\mathcal{L}$-theory, i.e. a set of $\mathcal{L}$-sentences ($\mathcal{L}$-formulas without free variables)

$\mathcal{T} \vdash \phi$ — ϕ is provable from $\mathcal{T}$

(e.g. $\{\forall x \, \neg x \cdot x < 0\} \vdash \neg 1 \cdot 1 < 0$)

$\mathcal{M} \models \phi$ — ϕ is valid in $\mathcal{M}$

(e.g. $(\mathbb{R}, +, -, \cdot, 0, 1, <) \models \exists x \; x \cdot x = 1 + 1$,
but $(\mathbb{Q}, +, -, \cdot, 0, 1, <) \not\models \exists x \; x \cdot x = 1 + 1$)

$\mathcal{T} \models \phi$ — for all $\mathcal{M} \models \mathcal{T}$ we have $\mathcal{M} \models \phi$

$\mathrm{Th}(\mathcal{M}) = \{\psi | \; \psi \text{ is an } \mathcal{L}\text{-sentence and } \mathcal{M} \models \psi\}$ — the complete theory of $\mathcal{M}$

Decidability

Definition

An $\mathcal{L}$-structure $\mathcal{M}$ is called *decidable* if there exists an algorithm that determines whether for a given $\mathcal{L}$-sentence ϕ we have $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$.

Decidability

Definition

An $\mathcal{L}$-structure $\mathcal{M}$ is called *decidable* if there exists an algorithm that determines whether for a given $\mathcal{L}$-sentence ϕ we have $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$.

Definition

A complete $\mathcal{L}$-theory $\mathcal{T}$ is called *recursive* if there exists an algorithm that determines whether for a given $\mathcal{L}$-sentence ϕ we have $\mathcal{T} \models \phi$ or $\mathcal{T} \models \neg\phi$.

Decidability

Definition

An $\mathcal{L}$-structure $\mathcal{M}$ is called *decidable* if there exists an algorithm that determines whether for a given $\mathcal{L}$-sentence ϕ we have $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$.

Definition

A complete $\mathcal{L}$-theory $\mathcal{T}$ is called *recursive* if there exists an algorithm that determines whether for a given $\mathcal{L}$-sentence ϕ we have $\mathcal{T} \models \phi$ or $\mathcal{T} \models \neg\phi$.

Definition

An $\mathcal{L}$-theory $\mathcal{T}$ is *axiomatized* by an $\mathcal{L}$-theory Σ if for all $\mathcal{L}$-sentences ϕ it holds $\mathcal{T} \models \phi$ if and only if $\Sigma \models \phi$.

Decidability

Theorem

An $\mathcal{L}$-structure $\mathcal{M}$ is decidable if and only if $\mathrm{Th}(\mathcal{M})$ is recursively axiomatizable.

Decidability

Theorem

An $\mathcal{L}$-structure $\mathcal{M}$ is decidable if and only if $\mathrm{Th}(\mathcal{M})$ is recursively axiomatizable.

Sketch of proof.

$\Rightarrow$ If $\mathcal{M}$ is decidable, then $\mathrm{Th}(\mathcal{M})$ is recursive.

Decidability

Theorem

An $\mathcal{L}$-structure $\mathcal{M}$ is decidable if and only if $\mathrm{Th}(\mathcal{M})$ is recursively axiomatizable.

Sketch of proof.

$\Rightarrow$ If $\mathcal{M}$ is decidable, then $\mathrm{Th}(\mathcal{M})$ is recursive.

$\Leftarrow$ Let Σ be a recursive axiomatization of $\mathrm{Th}(\mathcal{M})$ and let $\{\phi_0, \phi_1, \ldots\}$ be a recursive enumeration of all sentences provable from Σ.

Decidability

Theorem

An $\mathcal{L}$-structure $\mathcal{M}$ is decidable if and only if Th($\mathcal{M}$) is recursively axiomatizable.

Sketch of proof.

$\Rightarrow$ If $\mathcal{M}$ is decidable, then Th($\mathcal{M}$) is recursive.

$\Leftarrow$ Let Σ be a recursive axiomatization of Th($\mathcal{M}$) and let $\{\phi_0, \phi_1, \ldots\}$ be a recursive enumeration of all sentences provable from Σ.
Given a sentence ψ, check in turn whether ψ or $\neg\psi$ is the *n*th entry of the list and terminate when the entry is found. If $\psi = \phi_n$, then $\Sigma \vdash \psi$, and hence (by Gödel's Completeness Theorem) $\Sigma \models \psi$. Thus, Th($\mathcal{M}$) $\models \psi$, i.e. $\mathcal{M} \models \psi$.

Decidability

Theorem

An $\mathcal{L}$-structure $\mathcal{M}$ is decidable if and only if $\mathrm{Th}(\mathcal{M})$ is recursively axiomatizable.

Sketch of proof.

$\Rightarrow$ If $\mathcal{M}$ is decidable, then $\mathrm{Th}(\mathcal{M})$ is recursive.

$\Leftarrow$ Let Σ be a recursive axiomatization of $\mathrm{Th}(\mathcal{M})$ and let $\{\phi_0, \phi_1, \ldots\}$ be a recursive enumeration of all sentences provable from Σ.
Given a sentence ψ, check in turn whether ψ or $\neg\psi$ is the *n*th entry of the list and terminate when the entry is found. If $\psi = \phi_n$, then $\Sigma \vdash \psi$, and hence (by Gödel's Completeness Theorem) $\Sigma \models \psi$. Thus, $\mathrm{Th}(\mathcal{M}) \models \psi$, i.e. $\mathcal{M} \models \psi$.
Similarly, if $\psi = \neg\phi_n$, then $\mathcal{M} \models \neg\phi_n$.

□

The Theorem

Fix language of ordered rings $\mathcal{L}_{\mathrm{or}} = \{+, -, \cdot, 0, 1, <\}$ and let $\mathcal{R} = (\mathbb{R}, +, -, \cdot, 0, 1, <)$.

The Theorem

Fix language of ordered rings $\mathcal{L}_{\text{or}} = \{+, -, \cdot, 0, 1, <\}$ and let $\mathcal{R} = (\mathbb{R}, +, -, \cdot, 0, 1, <)$.

Theorem (Tarski 1948)

The $\mathcal{L}_{\text{or}}$-structure $\mathcal{R}$ is decidable.

The Theorem

Fix language of ordered rings $\mathcal{L}_{\mathrm{or}} = \{+, -, \cdot, 0, 1, <\}$ and let $\mathcal{R} = (\mathbb{R}, +, -, \cdot, 0, 1, <)$.

Theorem (Tarski 1948)

The $\mathcal{L}_{\mathrm{or}}$-structure $\mathcal{R}$ is decidable.

Tarski provides an "inner-mathematical" decision algorithm.

Outline of Tarski's Decision Algorithm

First step: Construction of a quantifier elimination algorithm

Outline of Tarski's Decision Algorithm

First step: Construction of a quantifier elimination algorithm

- For each formula $\phi(x_1, \ldots, x_n)$ (with free variables from $x_1, \ldots, x_n$) we find a quantifier-free formula $\psi(x_1, \ldots, x_n)$ such that

$$\mathcal{R} \models \forall x_1 \ldots \forall x_n \, (\phi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)).$$

(E.g. $\exists y \; x \cdot x = y$ is equivalent to $(-32x < 0 \; \vee \; -32x = 0)$)

Outline of Tarski's Decision Algorithm

First step: Construction of a quantifier elimination algorithm

- For each formula $\phi(x_1, \ldots, x_n)$ (with free variables from $x_1, \ldots, x_n$) we find a quantifier-free formula $\psi(x_1, \ldots, x_n)$ such that

$$\mathcal{R} \models \forall x_1 \ldots \forall x_n \, (\phi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)).$$

(E.g. $\exists y \; x \cdot x = y$ is equivalent to $(-32x < 0 \; \vee \; -32x = 0)$)

- Quantifier elimination algorithm by structural induction: If ϕ and ϕ' are equivalent to quantifier-free formulas ψ and ψ', respectively, then
  - $\neg\phi$ is equivalent to $\neg\psi$.
  - $\phi \vee \phi'$ is equivalent to $\psi \vee \psi'$.
  - $\phi \wedge \phi'$ is equivalent to $\psi \wedge \psi'$.
  - $\exists x \; \phi$ is equivalent to ψ if x does not appear free in ψ.

Outline of Tarski's Decision Algorithm

First step (continued)

Outline of Tarski's Decision Algorithm

First step (continued)

- Special attention to the case $\exists x\ \phi$, where x appears free in ψ. Now, $\exists x\ \phi$ is equivalent to $\exists x\ \psi$, where ψ is quantifier-free.

Outline of Tarski's Decision Algorithm

First step (continued)

- Special attention to the case $\exists x\ \phi$, where x appears free in ψ. Now, $\exists x\ \phi$ is equivalent to $\exists x\ \psi$, where ψ is quantifier-free.
- Quantifier-free formulas in the variables $x, y_1, \ldots, y_m$ are equivalent to a formula of the form

$$\bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} \psi_{ij}(x, y_1, \ldots, y_m),$$

where each $\psi_{ij}(x, y_1, \ldots, y_m)$ is of the form

$$p_{ij}(x, y_1, \ldots, y_m) = 0 \qquad \text{or} \qquad p_{ij}(x, y_1, \ldots, y_m) > 0$$

for some polynomials $p_{ij} \in \mathbb{Z}[x, y_1, \ldots, y_m]$. (E.g. $x - y_1 = y_1 + y_2\ \wedge\ \neg y_1 < y_2$ is equivalent to $x - 2y_1 - y_2 = 0\ \wedge\ (y_1 - y_2 > 0 \vee y_1 - y_2 = 0)$.)

Outline of Tarski's Decision Algorithm

First step (continued)

Outline of Tarski's Decision Algorithm

First step (continued)

- Main technical step: For each formula of the form

$$\exists x \; p_{ij}(x, y_1, \ldots, y_m) = 0 \qquad \text{or} \qquad \exists x \; p_{ij}(x, y_1, \ldots, y_m) > 0$$

  we can use geometrical arguments to obtain an equivalent quantifier-free formula $\psi'_{ij}(x, y_1, \ldots, y_m)$.
  (E.g. $\exists x \; y_1 x^2 + y_2 x + y_3 = 0$ if and only if the discriminant $y_2^2 - 4y_1 y_3$ is non-negative or the polynomial is linear or the zero polynomial, i. e.
  $\neg y_2^2 - 4y_1 y_3 < 0 \vee (y_1 = 0 \wedge \neg \; y_2 = 0) \vee (y_1 = y_2 = y_3 = 0)$.)

Outline of Tarski's Decision Algorithm

Second step: Applying the Quantifier Elimination Algorithm

Outline of Tarski's Decision Algorithm

Second step: Applying the Quantifier Elimination Algorithm

- By Step 1, each sentence ψ is equivalent to a quantifier-free sentence. A quantifier-free sentence is equivalent to one of the form

$$\bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} \psi_{ij},$$

where each ψ_{ij} is of the form $z_{ij} = 0$ or $z_{ij} > 0$ for some $z_{ij} \in \mathbb{Z}$.
(E.g. $\exists y\ (1+1)\cdot(1+1) = y$ is equivalent to $(-64 < 0 \vee -64 = 0)$.)

Outline of Tarski's Decision Algorithm

Second step: Applying the Quantifier Elimination Algorithm

- By Step 1, each sentence ψ is equivalent to a quantifier-free sentence. A quantifier-free sentence is equivalent to one of the form

$$\bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} \psi_{ij},$$

where each ψ_{ij} is of the form $z_{ij} = 0$ or $z_{ij} > 0$ for some $z_{ij} \in \mathbb{Z}$.
(E.g. $\exists y\ (1+1) \cdot (1+1) = y$ is equivalent to $(-64 < 0 \vee -64 = 0)$.)

- Performing a numerical check gives us whether this sentence is valid in $\mathcal{R}$ or not.

- Tarksi's Decision Algorithm only used the following properties of the real numbers:

- Tarksi's Decision Algorithm only used the following properties of the real numbers:

  1. $\mathbb{R}$ is a field

- Tarksi's Decision Algorithm only used the following properties of the real numbers:

  1. $\mathbb{R}$ is a field
  2. it is linearly ordered

- Tarksi's Decision Algorithm only used the following properties of the real numbers:

  1. $\mathbb{R}$ is a field
  2. it is linearly ordered
  3. all positive elements are squares

- Tarksi's Decision Algorithm only used the following properties of the real numbers:

  1. $\mathbb{R}$ is a field
  2. it is linearly ordered
  3. all positive elements are squares
  4. polynomials of odd degree have zeros

- Tarksi's Decision Algorithm only used the following properties of the real numbers:

1. $\mathbb{R}$ is a field
2. it is linearly ordered
3. all positive elements are squares
4. polynomials of odd degree have zeros

Formalizing these statements yields the so called
THEORY OF REAL CLOSED FIELDS,
which is usually denoted by RCF.

- Tarksi's Decision Algorithm only used the following properties of the real numbers:
  - the field axioms (commutativity of $+$ and $\cdot$, distributivity, existence of inverses etc.)
  - the order axioms:
    - $\forall x \, \neg x < x$
    - $\forall x \forall y \forall z \, ((x < y \wedge y < z) \rightarrow x < z)$
    - $\forall x \forall y \, (x < y \vee x = y \vee y < x)$
    - $\forall x \forall y \forall z \, (x < y \rightarrow x + z < y + z)$
    - $\forall x \forall y \, ((0 < x \wedge 0 < y) \rightarrow 0 < x \cdot y)$
  - positive elements are squares:
    - $\forall x \, (0 < x \ \rightarrow \ \exists y \, x = y^2)$
  - polynomials of odd degree have zeros: For each $n \in \mathbb{N}$ we have:
    - $\forall x_0 \forall x_1 \ldots \forall x_{2n} \, \exists y \, y^{2n+1} + x_{2n} y^{2n} + x_{2n-1} y^{2n-1} + \ldots + x_1 y + x_0 = 0.$

The Theory of Real Closed Fields

Important Consequences

The Theory of Real Closed Fields

Important Consequences

- Each model of RCF has effective quantifier elimination and is decidable.

The Theory of Real Closed Fields

Important Consequences

- Each model of RCF has effective quantifier elimination and is decidable.
- RCF is complete, i.e. for each $\mathcal{L}_{\mathrm{or}}$-sentence ϕ we have RCF $\models \phi$ or RCF $\models \neg\phi$.

The Theory of Real Closed Fields

Important Consequences

- Each model of RCF has effective quantifier elimination and is decidable.
- RCF is complete, i.e. for each $\mathcal{L}_{\text{or}}$-sentence ϕ we have RCF $\models \phi$ or RCF $\models \neg\phi$.
- As RCF is a complete recursive theory, we obtain a second, recursion theoretic decision algorithm for $\mathcal{R}$.

The Theory of Real Closed Fields

Important Consequences

- Each model of RCF has effective quantifier elimination and is decidable.
- RCF is complete, i.e. for each $\mathcal{L}_{\mathrm{or}}$-sentence ϕ we have $\mathrm{RCF} \models \phi$ or $\mathrm{RCF} \models \neg\phi$.
- As RCF is a complete recursive theory, we obtain a second, recursion theoretic decision algorithm for $\mathcal{R}$. (This would not be the case if properties of $\mathbb{R}$ had been used which cannot be formalised as axioms.)

Decidability of the Real Exponential Field

Denote by $\mathcal{L}_{\mathrm{exp}} = \{+, -, \cdot, 0, 1, <, \exp\}$ the language of exponential rings and let $\mathcal{R}_{\mathrm{exp}} = (\mathbb{R}, +, -, \cdot, 0, 1, <, \exp)$ be the real exponential field.

Decidability of the Real Exponential Field

Denote by $\mathcal{L}_{\mathrm{exp}} = \{+, -, \cdot, 0, 1, <, \exp\}$ the language of exponential rings and let $\mathcal{R}_{\mathrm{exp}} = (\mathbb{R}, +, -, \cdot, 0, 1, <, \exp)$ be the real exponential field.

Question

Tarski (1948): Is $\mathcal{R}_{\mathrm{exp}}$ decidable?

Progress

Progress

- 1980s (Dahn and Wolter): Several candidates for recursive axiomatizations of $\mathcal{R}_{\exp}$

Progress

- 1980s (Dahn and Wolter): Several candidates for recursive axiomatizations of $\mathcal{R}_{\mathrm{exp}}$
- 1996 (Wilkie): $\mathcal{R}_{\mathrm{exp}}$ is model complete

Progress

- 1980s (Dahn and Wolter): Several candidates for recursive axiomatizations of $\mathcal{R}_{\text{exp}}$
- 1996 (Wilkie): $\mathcal{R}_{\text{exp}}$ is model complete: That means that for every $\mathcal{L}_{\text{exp}}$-formula $\phi(x_1, \ldots, x_n)$ there exists an equivalent $\mathcal{L}_{\text{exp}}$-formula of the form $\exists y_1 \ldots \exists y_m \, \psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, where ψ is quantifier-free.

Progress

- 1980s (Dahn and Wolter): Several candidates for recursive axiomatizations of $\mathcal{R}_{\exp}$
- 1996 (Wilkie): $\mathcal{R}_{\exp}$ is model complete: That means that for every $\mathcal{L}_{\exp}$-formula $\phi(x_1, \ldots, x_n)$ there exists an equivalent $\mathcal{L}_{\exp}$-formula of the form $\exists y_1 \ldots \exists y_m \, \psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, where ψ is quantifier-free.
- 1996 (Macintyre and Wilkie): Assuming Real Schanuel's Conjecture, $\mathcal{R}_{\exp}$ is decidable.

Progress

- 1980s (Dahn and Wolter): Several candidates for recursive axiomatizations of $\mathcal{R}_{\text{exp}}$
- 1996 (Wilkie): $\mathcal{R}_{\text{exp}}$ is model complete: That means that for every $\mathcal{L}_{\text{exp}}$-formula $\phi(x_1, \ldots, x_n)$ there exists an equivalent $\mathcal{L}_{\text{exp}}$-formula of the form $\exists y_1 \ldots \exists y_m \, \psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, where ψ is quantifier-free.
- 1996 (Macintyre and Wilkie): Assuming Real Schanuel's Conjecture, $\mathcal{R}_{\text{exp}}$ is decidable.
- 1998 (van den Dries): $\mathcal{R}_{\text{exp}}$ does not admit quantifier elimination.

Progress

- 1980s (Dahn and Wolter): Several candidates for recursive axiomatizations of $\mathcal{R}_{\text{exp}}$
- 1996 (Wilkie): $\mathcal{R}_{\text{exp}}$ is model complete: That means that for every $\mathcal{L}_{\text{exp}}$-formula $\phi(x_1, \ldots, x_n)$ there exists an equivalent $\mathcal{L}_{\text{exp}}$-formula of the form $\exists y_1 \ldots \exists y_m \, \psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, where ψ is quantifier-free.
- 1996 (Macintyre and Wilkie): Assuming Real Schanuel's Conjecture, $\mathcal{R}_{\text{exp}}$ is decidable.
- 1998 (van den Dries): $\mathcal{R}_{\text{exp}}$ does not admit quantifier elimination.
- 2006 (Berarducci, Servi): Assuming Transfer Conjecture, $\mathcal{R}_{\text{exp}}$ is decidable.

Schanuel's Conjecture

Schanuel's Conjecture (SC)

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Then

$$\mathrm{td}_{\mathbb{Q}}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})) \geq n.$$

Schanuel's Conjecture

Schanuel's Conjecture (SC)

Let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Then

$$\mathrm{td}_{\mathbb{Q}}(\mathbb{Q}(\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n})) \geq n.$$

$\rightarrow$ (SC) relates the algebraic complexity of complex numbers with the algebraic complexity of their exponentials.

Schanuel's Conjecture

Schanuel's Conjecture (SC)

Let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Then

$$\mathrm{td}_{\mathbb{Q}}(\mathbb{Q}(\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n})) \geq n.$$

$\rightarrow$ (SC) relates the algebraic complexity of complex numbers with the algebraic complexity of their exponentials.

Example: (SC) implies that e and π are algebraically independent over $\mathbb{Q}$. This means that expressions like $\frac{1}{26}e^3 + e\pi - \frac{\pi^4}{2} + \frac{e^2\pi^2}{2} + e \quad (\approx -0,2104...)$ are never equal to 0.

Macintyre and Wilkie's conditional proof

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\text{exp}}$-theory $\mathcal{T}_0 \subseteq \text{Th}(\mathcal{R}_{\text{exp}})$ such that $\mathcal{T}_0 \cup \mathcal{T}_\exists(\mathcal{R}_{\text{exp}})$ axiomatizes $\text{Th}(\mathcal{R}_{\text{exp}})$.

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\text{exp}}$-theory $\mathcal{T}_0 \subseteq \text{Th}(\mathcal{R}_{\text{exp}})$ such that $\mathcal{T}_0 \cup \mathcal{T}_\exists(\mathcal{R}_{\text{exp}})$ axiomatizes $\text{Th}(\mathcal{R}_{\text{exp}})$.
   $\rightarrow$ Problem reduces to finding a recursive axiomatization of $\text{Th}_\exists(\mathcal{R}_{\text{exp}})$.

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\exp}$-theory $\mathcal{T}_0 \subseteq \mathrm{Th}(\mathcal{R}_{\exp})$ such that $\mathcal{T}_0 \cup \mathcal{T}_{\exists}(\mathcal{R}_{\exp})$ axiomatizes $\mathrm{Th}(\mathcal{R}_{\exp})$.
   $\rightarrow$ Problem reduces to finding a recursive axiomatization of $\mathrm{Th}_{\exists}(\mathcal{R}_{\exp})$.
2. Each existential sentence in $\mathrm{Th}(\mathcal{R}_{\exp})$ is equivalent to one of the form

$$\exists z_1 \ldots \exists z_n \; p(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) = 0$$

   for some $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\exp}$-theory $\mathcal{T}_0 \subseteq \mathrm{Th}(\mathcal{R}_{\exp})$ such that $\mathcal{T}_0 \cup \mathcal{T}_\exists(\mathcal{R}_{\exp})$ axiomatizes $\mathrm{Th}(\mathcal{R}_{\exp})$.
   $\rightarrow$ Problem reduces to finding a recursive axiomatization of $\mathrm{Th}_\exists(\mathcal{R}_{\exp})$.
2. Each existential sentence in $\mathrm{Th}(\mathcal{R}_{\exp})$ is equivalent to one of the form

$$\exists z_1 \ldots \exists z_n \; p(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) = 0$$

   for some $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.
   Example: $\exists x \exists y \;\; \exp(\exp(x)) > y + x$

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\exp}$-theory $\mathcal{T}_0 \subseteq \mathrm{Th}(\mathcal{R}_{\exp})$ such that $\mathcal{T}_0 \cup \mathcal{T}_\exists(\mathcal{R}_{\exp})$ axiomatizes $\mathrm{Th}(\mathcal{R}_{\exp})$.
   $\rightarrow$ Problem reduces to finding a recursive axiomatization of $\mathrm{Th}_\exists(\mathcal{R}_{\exp})$.
2. Each existential sentence in $\mathrm{Th}(\mathcal{R}_{\exp})$ is equivalent to one of the form

   $$\exists z_1 \ldots \exists z_n \; p(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) = 0$$

   for some $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.
   Example: $\exists x \exists y \; \exp(\exp(x)) > y + x$ is equivalent to
   $\exists x \exists y \exists z_1 \exists z_2 \; (z_1 - \exp(x) = 0 \wedge \exp(z_1) - y + x - z_2^2 = 0)$.

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\exp}$-theory $\mathcal{T}_0 \subseteq \mathrm{Th}(\mathcal{R}_{\exp})$ such that $\mathcal{T}_0 \cup \mathcal{T}_\exists(\mathcal{R}_{\exp})$ axiomatizes $\mathrm{Th}(\mathcal{R}_{\exp})$.
   $\rightarrow$ Problem reduces to finding a recursive axiomatization of $\mathrm{Th}_\exists(\mathcal{R}_{\exp})$.
2. Each existential sentence in $\mathrm{Th}(\mathcal{R}_{\exp})$ is equivalent to one of the form

$$\exists z_1 \ldots \exists z_n \; p(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) = 0$$

   for some $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.
   Example: $\exists x \exists y \; \exp(\exp(x)) > y + x$ is equivalent to $\exists x \exists y \exists z_1 \exists z_2 \; (z_1 - \exp(x) = 0 \wedge \exp(z_1) - y + x - z_2^2 = 0)$.This, however, is equivalent to $\exists x \exists y \exists z_1 \exists z_2 \; ((z_1 - \exp(x))^2 + (\exp(z_1) - y + x - z_2^2)^2 = 0)$.

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\exp}$-theory $\mathcal{T}_0 \subseteq \mathrm{Th}(\mathcal{R}_{\exp})$ such that $\mathcal{T}_0 \cup \mathcal{T}_\exists(\mathcal{R}_{\exp})$ axiomatizes $\mathrm{Th}(\mathcal{R}_{\exp})$.
   $\to$ Problem reduces to finding a recursive axiomatization of $\mathrm{Th}_\exists(\mathcal{R}_{\exp})$.
2. Each existential sentence in $\mathrm{Th}(\mathcal{R}_{\exp})$ is equivalent to one of the form

$$\exists z_1 \ldots \exists z_n \; p(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) = 0$$

   for some $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.
   Example: $\exists x \exists y \;\; \exp(\exp(x)) > y + x$ is equivalent to
   $\exists x \exists y \exists z_1 \exists z_2 \; (z_1 - \exp(x) = 0 \wedge \exp(z_1) - y + x - z_2^2 = 0)$.This, however, is equivalent to
   $\exists x \exists y \exists z_1 \exists z_2 \; ((z_1 - \exp(x))^2 + (\exp(z_1) - y + x - z_2^2)^2 = 0)$.
   $\to$ Problem reduces to finding an algorithm which determines whether a polynomial $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ has a zero of the form $(a_1, \ldots, a_n, \exp(a_1), \ldots, \exp(a_n))$ or not.

Macintyre and Wilkie's conditional proof

1. There exists a recursive $\mathcal{L}_{\exp}$-theory $\mathcal{T}_0 \subseteq \mathrm{Th}(\mathcal{R}_{\exp})$ such that $\mathcal{T}_0 \cup \mathcal{T}_{\exists}(\mathcal{R}_{\exp})$ axiomatizes $\mathrm{Th}(\mathcal{R}_{\exp})$.
   $\rightarrow$ Problem reduces to finding a recursive axiomatization of $\mathrm{Th}_{\exists}(\mathcal{R}_{\exp})$.
2. Each existential sentence in $\mathrm{Th}(\mathcal{R}_{\exp})$ is equivalent to one of the form
   $$\exists z_1 \ldots \exists z_n \; p(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) = 0$$
   for some $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.
   Example: $\exists x \exists y \; \exp(\exp(x)) > y + x$ is equivalent to
   $\exists x \exists y \exists z_1 \exists z_2 \; (z_1 - \exp(x) = 0 \wedge \exp(z_1) - y + x - z_2^2 = 0)$.This, however, is equivalent to
   $\exists x \exists y \exists z_1 \exists z_2 \; ((z_1 - \exp(x))^2 + (\exp(z_1) - y + x - z_2^2)^2 = 0)$.
   $\rightarrow$ Problem reduces to finding an algorithm which determines whether a polynomial $p(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ has a zero of the form $(a_1, \ldots, a_n, \exp(a_1), \ldots, \exp(a_n))$ or not.
3. Assuming (SC), there exists a recursive theory $\mathcal{T}_1$ axiomatizing $\mathrm{Th}_{\exists}(\mathcal{R}_{\exp})$.

Consequences

As (SC) is "probably true", the proposed recursive theory $\mathcal{T}_0 \cup \mathcal{T}_1$ "probably" gives us a decision algorithm for $\mathcal{R}_{\text{exp}}$.

Consequences

As (SC) is "probably true", the proposed recursive theory $\mathcal{T}_0 \cup \mathcal{T}_1$ "probably" gives us a decision algorithm for $\mathcal{R}_{\text{exp}}$.

BUT: Its computational complexity makes it useless for applications in the real world.

References

[1] A. Berarducci and T. Servi, 'An effective version of Wilkie's theorem of the complement and some effective o-minimality results', *Ann. Pure Appl. Logic* 125 (2004) 43–74.

[2] A. Macintyre and A. Wilkie, 'On the decidability of the real exponential field', *Kreiseliana: about and around Georg Kreisel* (ed. P. Odifreddi; A. K. Peters, Wellesley, MA, 1996) 441–467.

[3] A. Tarski, *A decision method for elementary algebra and geometry* (RAND Corporation, Santa Monica, CA, 1948).

[4] A. 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.