DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination

Saeed Salehi

University of Tabriz

http://SaeedSalehi.ir/

14 – 15 November 2012
Kerman

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (1/36)

Axiomatizing Theories

Dense Linear Orders Without Endpoints

Cantor: Every Countable Dense Linear Order Without Endpoints Is Isomorphic to $\langle\mathbb{Q},<\rangle$.

Thus, the theory of "dense linear orders without endpoints" is complete (and fully axiomatizes the theory of $\langle\mathbb{Q},<\rangle$):

- $\forall x,y(x<y\rightarrow y\not<x)$ Anti-Symmetric
- $\forall x,y,z(x<y<z\rightarrow x<z)$ Transitive
- $\forall x,y(x<y\vee x=y\vee y<x)$ Linear
- $\forall x,y(x<y\rightarrow\exists z[x<z<y])$ Dense
- $\forall x\exists y(x<y)$ No Last Point
- $\forall x\exists y(y<x)$ No Least Point

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (2/36)

Axiomatizing Theories

Dense Linear Orders Without Endpoints

Also $\langle \mathbb{R}, < \rangle$ is a model of this theory.
So, the theories of $\langle \mathbb{Q}, < \rangle$ and $\langle \mathbb{R}, < \rangle$ are decidable. (and can be axiomatized as "dense linear order without endpoints").

This fact can be proved by "Quantifier Elimination":

C. H. LANGFORD, *Some Theorems on Deducibility*, Annals of Mathematics 28 (1927) 16–40.

Though the First-Order Theories of $\langle \mathbb{Q}, < \rangle$ and $\langle \mathbb{R}, < \rangle$ are equal, these structures are very different: $\langle \mathbb{R}, < \rangle$ is complete (every bounded subset has a supremum) while $\langle \mathbb{Q}, < \rangle$ is not.

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (3/36)

Quantifier Elimination

Reducing First-Order to Propositional

Propositional Logic is Decidable.
Eliminating as many connectives as possible:

$\rhd$ $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$ $\rhd$ $\forall x \varphi(x) \equiv \neg\exists x \neg\varphi(x)$

Remaining: $\wedge, \vee, \neg, \exists$

$\rhd$ $\neg\neg A \equiv A$; $\neg(A \wedge B) \equiv \neg A \vee \neg B$; $\neg(A \vee B) \equiv \neg A \wedge \neg B$

$\rhd$ $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

Disjunction Normalizing: $\bigvee_i (\bigwedge_j \alpha_{i,j})$, $\alpha_{i,j}$ atom or $\neg$atom

$\rhd$ $\exists x(A \vee B) \equiv \exists x A \vee \exists x B$.

Theorem (The Main Lemma of Quantifier Elimination)

If every formula $\exists x(\bigwedge_j \alpha_{i,j})$ is equivalent to a quantifier-free formula, then we have quantifier elimination.

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (4/36)

Quantifier Elimination

Dense Linear Orders Without Endpoints

In case we have order $<$ relation, we may eliminate $\neg$ as well:

▷ $\neg(a = b) \equiv a < b \vee b < a$

▷ $\neg(a < b) \equiv a = b \vee b < a$

Quantifier Elimination for Dense Linear Orders Without Endpoints: $\varphi = \exists x(\bigwedge_i t_i < x \wedge \bigwedge_j x < s_j \wedge \bigwedge_k x = u_k)$

- If $k \neq 0$ then $\varphi \equiv \bigwedge_i t_i < u_1 \wedge \bigwedge_j u_1 < s_j \wedge \bigwedge_k u_1 = u_k$
- If $k = 0$ and $i = 0$ then $\varphi \equiv \top$
- If $k = 0$ and $j = 0$ then $\varphi \equiv \top$
- If $k = 0$ and $i, j \neq 0$ then $\varphi \equiv \bigwedge_{i,j} t_i < s_j$

Quantifier Elimination

Discrete Orders Without Endpoints

So far, we have a decision procedure for the theories of the structures $\langle \mathbb{Q}, < \rangle$ and $\langle \mathbb{R}, < \rangle$.

What about $\langle \mathbb{Z}, < \rangle$? and $\langle \mathbb{N}, < \rangle$?

For $\langle \mathbb{Z}, < \rangle$ we do not have quantifier elimination:
$\exists x(a < x < b)$ is not equivalent to a quantifier-free formula.

By adding the successor function $S : \mathbb{Z} \rightarrow \mathbb{Z}$ ($S(x) = x + 1$) to the language, we can have quantifier elimination:

Theorem

The theory of $\langle \mathbb{Z}, S, < \rangle$ admits quantifier elimination.

Order $<$

The Theory of Order is Decidable in Number Domains.

The Theory of Order in $\mathbb{Z}$ is Characterized as:

Linear Discrete Order Without EndPoints

In the Language $\{S, <\}$ where $S(x) = x + 1$ is the Successor Function, Definable by $<$: $S(x) = z \iff \forall y (x < y \leftrightarrow z \leqslant y)$.

- $\forall x, y (x < y \rightarrow y \not< x)$ — Anti-Symmetric
- $\forall x, y, z (x < y < z \rightarrow x < z)$ — Transitive
- $\forall x, y (x < y \vee x = y \vee y < x)$ — Linear
- $\forall x, y (x < y \leftrightarrow S(x) < y \vee S(x) = y)$ — Discrete Order
- $\forall x \exists y (x = S(y))$ — Predecessor

These Completely Axiomatize the Whole Theory of $\langle \mathbb{Z}, S, < \rangle$.

Order $<$

The Theory of Order is Decidable in Number Domains.

For $\langle \mathbb{N}, S, < \rangle$ we still do not have quantifier elimination:
$\exists x(a = S(x))$ is not equivalent to a quantifier-free formula.

Theorem (H. B. Enderton)

The theory of $\langle \mathbb{N}, 0, S, < \rangle$ *admits quantifier elimination, and can be completely axiomatized by*

- $\forall x, y(x < y \rightarrow y \not< x)$ — *Anti-Symmetric*
- $\forall x, y, z(x < y < z \rightarrow x < z)$ — *Transitive*
- $\forall x, y(x < y \vee x = y \vee y < x)$ — *Linear*
- $\forall x, y(x < y \leftrightarrow S(x) < y \vee S(x) = y)$ — *Discrete Order*
- $\forall x(x \neq 0 \rightarrow \exists y[x = S(y)])$ — *Successor*
- $\forall x(x \not< 0)$ — *Least Point*

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (8/36)

QUANTIFIER ELIMINATION

Decidability and Undefinability

The structures $\langle\mathbb{N}, 0, S, <\rangle$, $\langle\mathbb{Z}, S, <\rangle$, $\langle\mathbb{Q}, <\rangle$ and $\langle\mathbb{R}, <\rangle$ admit Quantifier Elimination, and so are Decidable.

Definability:

$\mathrm{Def}_{R_1}(\mathbb{N}, <)$ = Finite or Co-Finite Subsets of $\mathbb{N}$

$$\{2,3,7\} = \{x \in \mathbb{N} \mid x = S^2(0) \vee x = S^3(0) \vee x = S^7(0)\}$$
$$\{4,8,9,10,11,12\cdots\} = \{x \in \mathbb{N} \mid x = S^4(0) \vee S^7(0) < x\}$$

So, $+$ or $\cdot$ or ... are not definable in $\langle\mathbb{N}, <\rangle$.

$\mathrm{Def}_{R_1}(\mathbb{Z}, <) = \mathrm{Def}_{R_1}(\mathbb{Q}, <) = \mathrm{Def}_{R_1}(\mathbb{R}, <)$ = empty or the whole domain; Nothing Interesting.

Decidability of Mathematical Structures

Decision Problem for the Following Structures

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	$\langle\mathbb{N},<\rangle$	$\langle\mathbb{Z},<\rangle$	$\langle\mathbb{Q},<\rangle$	$\langle\mathbb{R},<\rangle$	–
$\{+\}$	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{Z},+\rangle$	$\langle\mathbb{Q},+\rangle$	$\langle\mathbb{R},+\rangle$	$\langle\mathbb{C},+\rangle$
$\{\cdot\}$	$\langle\mathbb{N},\cdot\rangle$	$\langle\mathbb{Z},\cdot\rangle$	$\langle\mathbb{Q},\cdot\rangle$	$\langle\mathbb{R},\cdot\rangle$	$\langle\mathbb{C},\cdot\rangle$
$\{+,<\}$	$\langle\mathbb{N},+,<\rangle$	$\langle\mathbb{Z},+,<\rangle$	$\langle\mathbb{Q},+,<\rangle$	$\langle\mathbb{R},+,<\rangle$	–
$\{+,\cdot\}$	$\langle\mathbb{N},+,\cdot\rangle$	$\langle\mathbb{Z},+,\cdot\rangle$	$\langle\mathbb{Q},+,\cdot\rangle$	$\langle\mathbb{R},+,\cdot\rangle$	$\langle\mathbb{C},+,\cdot\rangle$
$\{\cdot,<\}$	$\langle\mathbb{N},\cdot,<\rangle$	$\langle\mathbb{Z},\cdot,<\rangle$	$\langle\mathbb{Q},\cdot,<\rangle$	$\langle\mathbb{R},\cdot,<\rangle$	–
$\{+,\cdot,<\}$	\	\	\	\	–

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (10/36)

Definability of $<$ By $+$ and $\cdot$

Order Is Definable By Addition And Multiplication.

No need to consider $\{+,\cdot,<\}$:
The Order Relation $<$ is Definable by $+$ and $\cdot$ as

- in $\mathbb{N}$: $a \leqslant b \iff \exists x\,(x+a=b)$.
- in $\mathbb{R}$: $a \leqslant b \iff \exists x\,(x\cdot x+a=b)$.

for $\mathbb{Z}$ Use Lagrange's Four Square Theorem; Every Natural (Positive) Number Can Be Written As A Sum Of Four Squares.

- in $\mathbb{Z}$: $a \leqslant b \iff \exists u,v,x,y\,(a+u^2+v^2+x^2+y^2=b)$.

for $\mathbb{Q}$ Lagrange's Theorem Holds Too: $0\leqslant r=m/n=(mn)/n^2=(u^2+v^2+x^2+y^2)/n^2=(u/n)^2+(v/n)^2+(x/n)^2+(y/n)^2$.

- in $\mathbb{Q}$: $a \leqslant b \iff \exists u,v,x,y\,(a+u^2+v^2+x^2+y^2=b)$.

$\boxed{a<b \iff a\leqslant b \wedge a\neq b}$ $\boxed{a\leqslant b \iff a<b \vee a=b}$

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (11/36)

Addition $+$

The Theories of $\langle\mathbb{Q},+\rangle$, $\langle\mathbb{R},+\rangle$ and $\langle\mathbb{C},+\rangle$ have, surprisingly, the same theory: Non-Trivial Torsion-Free Divisible Abelian Groups:

- $\forall x,y,z\,\big(x+(y+z)=(x+y)+z\big)$
- $\forall x\,\big(x+0=x=0+x\big)$
- $\forall x\,\big(x+(-x)=0=(-x)+x\big)$
- $\forall x,y\,\big(x+y=y+x\big)$
- $\forall x\exists y\big(\underbrace{y+\cdots+y}_{n-\text{times}}=x\big),\ \ n=2,3,\cdots$
- $\forall x\,\big(\underbrace{x+\cdots+x}_{n-\text{times}}=0\rightarrow x=0\big),\ \ n=2,3,\cdots$
- $\exists x\,\big(x\neq 0\big)$

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (12/36)

Addition $+$

Quantifier Elimination for $\langle \mathbb{Q}, \mathbb{R}, \mathbb{C}, 0, -, + \rangle$

Write $\mathrm{n} \centerdot t$ for $\underbrace{t + \cdots + t}_{n-\text{times}}$. All terms $t(x)$: $\mathrm{n} \centerdot x + u$ ($n \in \mathbb{Z}$).

All atomic formulas $\varphi(x)$: $\mathrm{n} \centerdot x = t$; $\neg$atom: $\mathrm{n} \centerdot x \neq t$.

$$\exists x \big(\bigwedge_i \mathrm{n}_i \centerdot x = t_i \wedge \bigwedge_j \mathrm{m}_j \centerdot x \neq s_j \big)$$
$$\equiv \exists x \big(\bigwedge_i \mathrm{k} \centerdot x = t'_i \wedge \bigwedge_j \mathrm{k} \centerdot x \neq s'_j \big) \text{ where } k = lcm(\{\mathrm{n}_i\}_i \cup \{\mathrm{m}_j\}_j)$$
$$\equiv \exists y \big(\bigwedge_i y = t'_i \wedge \bigwedge_j y \neq s'_j \big) \text{ where } y = \mathrm{k} \centerdot x$$
$$\equiv \big(\bigwedge_i t'_1 = t'_i \wedge \bigwedge_j t'_1 \neq s'_j \big) \text{ if } i \neq 0$$
$$\equiv \top \text{ if } i = 0$$

The structures $\langle \mathbb{Q}, 0, -, + \rangle$, $\langle \mathbb{R}, 0, -, + \rangle$ and $\langle \mathbb{C}, 0, -, + \rangle$ admit Quantifier Elimination, and so are Decidable.

a model-theoretic proof: [D. MARKER, Model Theory: an introduction, Springer 2002].

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (13/36)

Addition $+$

Quantifier Elimination for $\langle \mathbb{Z}, + \rangle$ or $\langle \mathbb{N}, + \rangle$?

The formula $\exists y(\mathrm{n} \centerdot y = x)$ is not equivalent to a quantifier-free formula. Define $D_n(x)$ to hold when $n \mid x$.

Theorem (Presburger-Skolem)

The theory of the structure $\langle \mathbb{Z}, 0, -, +, D_2, D_3, D_4, \cdots \rangle$ admits quantifier elimination, and so $\mathrm{Th}(\mathbb{Z}, +)$ is decidable.

Write $a \equiv_m b$ when $m \mid a - b$.

Theorem (Presburger)

The theory of the structure $\langle \mathbb{Z}, 0, -, +, \equiv_2, \equiv_3, \equiv_4, \cdots \rangle$ admits quantifier elimination, and so $\mathrm{Th}(\mathbb{Z}, +)$ is decidable.

Addition $+$

Quantifier Elimination for $\langle\mathbb{Z},+\rangle$ or $\langle\mathbb{N},+\rangle$?

For a $q\in\mathbb{Q}$ and any $n\in\mathbb{Z}$ we have $[q\cdot n]\in\mathbb{Z}$.

Note that e.g. $[(3/4)\cdot 15]=[45/4]=11$,
but $3\,.\,[(1/4)\cdot 15]=[15/4]+[15/4]+[15/4]=3+3+3=9$.

Theorem (Skolem)

The theory of the structure $\langle\mathbb{Z},0,-,+,[q\cdot\Box]_{q\in\mathbb{Q}}\rangle$ admits quantifier elimination, and so $\mathrm{Th}(\mathbb{Z},+)$ is decidable.

G. S. BOOLOS, et. al., *Computability and Logic*, 5th ed. Cambridge University Press 2007.

C. SMORYŃSKI, *Logical Number Theory I: an introduction*, Springer 1991.

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (15/36)

Addition $+$ and Order $<$

Quantifier Elimination for $\langle \mathbb{Z}, +, < \rangle$ and $\langle \mathbb{N}, +, < \rangle$.

For $\langle \mathbb{N}, + \rangle$ the formula $\exists x (x + a = b)$ is not equivalent to a quantifier-free formula.

Theorem (Presburger)

The theory of $\langle \mathbb{N}, 0, S, +, <, \equiv_2, \equiv_3, \equiv_4, \cdots \rangle$ admits quantifier elimination, and so $\mathrm{Th}(\mathbb{N}, +)$ (and $\mathrm{Th}(\mathbb{N}, +, <)$) is decidable.

H. B. ENDERTON, *A Mathematical Introduction to Logic*, 2nd ed. Academic Press 2001.

Theorem (Presburger)

The theory of the structure $\langle \mathbb{Z}, 0, S, +, <, \equiv_2, \equiv_3, \equiv_4, \cdots \rangle$ admits quantifier elimination, and so $\mathrm{Th}(\mathbb{Z}, +, <)$ is decidable.

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (16/36)

Addition $+$ and Order $<$

Axiomatizing and Characterizing the Definable Subsets

Axiomatizing $\langle \mathbb{Z}, 0, 1, -, +, < \rangle$

Ordered Abelian Group with division algorithm

- $\forall x, y, z\, \big(x + (y + z) = (x + y) + z\big)$ • $\forall x, y\, \big(x + y = y + x\big)$
- $\forall x\, \big(x + 0 = x\big)$ • $\forall x\, \big(x + (-x) = 0\big)$ • $\forall x, y\, \big(x < y \rightarrow y \not< x\big)$
- $\forall x, y, z\, \big(x < y < z \rightarrow x < z\big)$ • $\forall x, y\, \big(x < y \vee x = y \vee y < x\big)$
- $\forall x, y\, \big(x < y \longleftrightarrow x + 1 < y \vee x + 1 = y\big)$
- $\forall x, y, z\, \big(x < y \rightarrow x + z < y + z\big)$ • $\forall x \exists y\, \big(\bigvee_{i<n} (x = n \centerdot y + i)\big)$

Definable Subsets of $\langle \mathbb{N}, + \rangle$

For $A \subseteq \mathbb{N}$ we have $A \in \mathrm{Def}_{R_1}(\mathbb{N}, +)$ if and only if

$$\exists M, p\colon \forall n > M\, \big(n \in A \longleftrightarrow n + p \in A\big).$$

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (17/36)

Addition $+$ and Order $<$

Quantifier Elimination for $\langle\mathbb{Q},+,<\rangle$ and $\langle\mathbb{R},+,<\rangle$.

The Theories of $\langle\mathbb{Q},0,-,+,<\rangle$ and $\langle\mathbb{R},0,-,+,<\rangle$ have, surprisingly, the same theory:

Non-Trivial Ordered Divisible Abelian Groups:

$\bullet\,\forall x,y,z\,\big(x+(y+z)=(x+y)+z\big)$ $\bullet\,\forall x,y\,\big(x+y=y+x\big)$
$\bullet\,\forall x\,\big(x+0=x\big)$ $\bullet\,\forall x\,\big(x+(-x)=0\big)$ $\bullet\,\forall x,y\,\big(x<y\rightarrow y\not< x\big)$
$\bullet\,\forall x,y,z\,\big(x<y<z\rightarrow x<z\big)$ $\bullet\,\forall x,y\,\big(x<y\vee x=y\vee y<x\big)$
$\bullet\,\forall x,y,z\,\big(x<y\rightarrow x+z<y+z\big)$ $\bullet\,\exists x\,\big(x\neq 0\big)$
$\bullet\,\forall x\exists y\big(n\centerdot y=x\big),\;\; n=2,3,\cdots$

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (18/36)

So Far ...

$\{<\}$, $\{+\}$ and $\{+,<\}$

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	$\langle\mathbb{N},<\rangle$	$\langle\mathbb{Z},<\rangle$	$\langle\mathbb{Q},<\rangle$	$\langle\mathbb{R},<\rangle$	–
$\{+\}$	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{Z},+\rangle$	$\langle\mathbb{Q},+\rangle$	$\langle\mathbb{R},+\rangle$	$\langle\mathbb{C},+\rangle$
$\{+,<\}$	$\langle\mathbb{N},+,<\rangle$	$\langle\mathbb{Z},+,<\rangle$	$\langle\mathbb{Q},+,<\rangle$	$\langle\mathbb{R},+,<\rangle$	–

Δ_1 = Decidable

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–

Multiplication

Skolem Arithmetic $\langle \mathbb{N}, \cdot \rangle$

Proof with “quantifier elimination” by

PATRICK CEGIELSKI, *Théorie Élémentaire de la Multiplication des Entiers Naturels*, in C. Berline, K. McAloon, J.-P. Ressayre (eds.) *Model Theory and Arithmetics*, LNM 890, Springer 1981, pp. 44–89.

Let $I(\prod_i p_i^{\alpha_i}) = \prod_i p_i^{\alpha_i+1}$; $T(\prod_i p_i^{\alpha_i}, \prod_j q_j^{\beta_j}) = \prod_k p_k^{\beta_k}$;
$S_n(\prod_i p_i^{\alpha_i}, \prod_j q_j^{\beta_j}) = \prod_{(\alpha_k<\beta_k)\&(\alpha_k\equiv_n\beta_k)} p_k$; and
$E_n(x) \equiv \exists p_1 \cdots \exists p_n \left(\bigwedge_i \mathrm{Prime}(p_i) \wedge \bigwedge_{i\neq j}(p_i \neq p_j) \wedge \bigwedge_i (p_i \mid x)\right)$.

Theorem (P. Cegielski 1980)

The theory of the structure $\langle \mathbb{N}, 0, 1, \cdot, I, T, S_0, S_1, S_2, \cdots, E_1, E_2, E_3, \cdots \rangle$ *admits quantifier elimination, and so* $\mathrm{Th}(\mathbb{N}, \cdot)$ *is decidable.*

Multiplication

$\langle \mathbb{Z}, \cdot \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{C}, \cdot \rangle$?

Missing in the literature. Maybe because:

– almost the same proofs can show the decidability of $\langle \mathbb{Z}, \cdot \rangle$
– the decidability of $\langle \mathbb{R}, \cdot \rangle$ and $\langle \mathbb{C}, \cdot \rangle$ follows from the decidability of $\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$ (Tarski's Theorems)
– and $\langle \mathbb{Q}, \cdot \rangle$? `Not Interesting ?`

Indeed, $\langle \mathbb{R}^{>0}, 1, \cdot, ^{-1} \rangle$ is a torsion-free divisible abelian group.

Theorem

The theory of $\langle \mathbb{R}, 0, 1, -1, \cdot, ^{-1}, \mathscr{P} \rangle$ admits quantifier elimination.

Where $\mathscr{P}(x) \equiv x > 0$. By Convention: $0^{-1} = 0$.

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (21/36)

Multiplication

$\langle\mathbb{Z},\cdot\rangle$, $\langle\mathbb{Q},\cdot\rangle$, $\langle\mathbb{R},\cdot\rangle$ and $\langle\mathbb{C},\cdot\rangle$

Let $\omega_k = \cos(2\pi/k) + i\sin(2\pi/k)$ be a $k-$th root of the unit; so $1, \omega_k, (\omega_k)^2, \cdots, (\omega_k)^{k-1}$ are all the $k-$th roots of the unit.

Theorem (NEW)

The theory of the structure $\langle\mathbb{C}, 0, 1, -1, \omega_2, \omega_3, \omega_4, \ldots, ^{-1}, \cdot\rangle$ *admits quantifier elimination.*

In $\mathbb{Q}$ let $R_n(x) \equiv \exists y(x = y^n)$. Recall $\mathscr{P}(x) \equiv x > 0$.

Theorem (NEW)

The theory of the structure $\langle\mathbb{Q}, 0, 1, -1, R_2, R_3, R_4, \ldots, ^{-1}, \cdot, \mathscr{P}\rangle$ *admits quantifier elimination.*

Addition and Multiplication

$\langle \mathbb{N}, +, \cdot \rangle$ and $\langle \mathbb{Z}, +, \cdot \rangle$ and $\langle \mathbb{Q}, +, \cdot \rangle$

Gödel's First Incompleteness Theorem:

$\mathrm{Th}(\mathbb{N}, +, \cdot)$ is Not Decidable.

So, $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ is Not Decidable, because $\mathbb{N}$ is definable in it:
for $m \in \mathbb{Z}$ we have

$$m \in \mathbb{N} \iff \exists a, b, c, d (\in \mathbb{Z}) \, (m = a^2 + b^2 + c^2 + d^2).$$

Also, $\langle \mathbb{Q}, +, \cdot \rangle$ can define $\mathbb{Z}$:

J. ROBINSON, *Definability and Decision Problems in Arithmetic*, JSL 14 (1949) 98–114.

B. POONEN, *Characterizing integers among rational numbers with a universal-existential formula*, American Journal of Mathematics 131 (2009) 675–682.

J. KOENIGSMANN, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, arXiv:1011.3424 [math.NT] (Nov. 2010)

So, $\mathrm{Th}(\mathbb{Q}, +, \cdot)$ is Not Decidable.

Addition and Multiplication

$\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$

$\langle \mathbb{R}, +, \cdot \rangle$: Real Closed (Ordered) Field
$\langle \mathbb{C}, +, \cdot \rangle$: Algebraically Closed Field

Theorem (Tarski {and Seidenberg and Chevalley})

The theories of the structures $\langle \mathbb{R}, 0, 1, -, +, \cdot, ^{-1}, < \rangle$ *and* $\langle \mathbb{C}, 0, 1, -, +, ^{-1}, \cdot \rangle$ *admit quantifier elimination.*

G. KREISEL, J. L. KRIVINE, *Elements of mathematical logic: model theory*, North Holland 1967.

Z. ADAMOWICZ, P. ZBIERSKI, *Logic of Mathematics: a modern course of classical logic*, Wiley 1997.

J. BOCHNAK, M. COSTE, M.-F. ROY, *Real Algebraic Geometry*, Springer 1998.

S. BASU, R. POLLACK, M.-F. COSTE-ROY, *Algorithms in Real Algebraic Geometry*, 2nd ed. Springer 2006.

State of the Art

(Un-)Decidability

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1
$\{\cdot,<\}$	✓	??	??	Δ_1	–

State of the Art

(Un-)Definability

$\mathrm{Def}_{R_1}(\mathbb{N}, <) =$ Finite or Co-Finite $= \mathrm{Def}_{R_1}(\mathbb{C}, +, \cdot)$

Minimal Structure // Strongly Minimal Theory

$\mathrm{Def}_{R_1}(\mathbb{N}, +) =$ Ultimately/Eventually Periodic (semi-linear)

$\mathrm{Def}_{R_1}(\mathbb{R}, +, \cdot) =$ Union of Some Points or Intervals

O-Minimal Structure // O-Minimal Theory

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (26/36)

Why Not Quantifier Elimination for $\langle \mathbb{N}, 0, 1, +, -, \cdot, < \rangle$?

Hilbert's Tenth Problem

$\exists x \left(\bigwedge_i p_i(x) = q_i(x) \wedge \bigwedge_j r_j(x) > s_j(x) \right) \equiv$
$\exists \overline{\mathbf{x}} \left(p(\overline{\mathbf{x}}) = q(\overline{\mathbf{x}}) \right)$ ... and its decidability is H10 (Undecidable!).

Hilbert's 10th Problem: Is $\mathrm{Th}_\exists(\mathbb{N}, +, \cdot) \in \Delta_1$?
Is $\mathrm{Th}_\exists(\mathbb{Z}, +, \cdot) \in \Delta_1$?
Is $\mathrm{Th}_\exists(\mathbb{Q}, +, \cdot) \in \Delta_1$?

DRPM: H10$\notin \Delta_1$ and so $\mathrm{Th}_\exists(\mathbb{N}, +, \cdot) \notin \Delta_1$

Because of a $\exists$ definition of $\mathbb{N}$ in $(\mathbb{Z}, +, \cdot)$, $\mathrm{Th}_\exists(\mathbb{Z}, +, \cdot) \notin \Delta_1$.

Open Question: H10$\mathbb{Q}$: Is $\mathrm{Th}_\exists(\mathbb{Q}, +, \cdot) \in \Delta_1$?
Is There an $\exists$ Definition for $\mathbb{Z}$ in $(\mathbb{Q}, +, \cdot)$?

Robinson (1949): $\forall^2\exists^7\forall^6$; Poonen (2009): $\forall^2\exists^7$; Koenigsmann (2010): $\forall^{418}$.

Multiplication and Order

$\langle \mathbb{N}, \cdot, < \rangle$ and $\langle \mathbb{R}, \cdot, < \rangle$

That $\mathrm{Th}(\mathbb{R}, \cdot, <) \in \Delta_1$ follows from Tarski-Seidenberg Principle.
Indeed, $\langle \mathbb{R}^{>0}, 1, \cdot, ^{-1} < \rangle$ is an ordered divisible abelian group.

Theorem

The theory of $\langle \mathbb{R}, 0, 1, -1, \cdot, ^{-1}, < \rangle$ *admits quantifier elimination.*

That $\mathrm{Th}(\mathbb{N}, \cdot, <) \notin \Delta_1$ follows from Tarski's Identity:
Addition is Definable by Multiplication and Order:

$$z = x + y \iff [x = y = z = 0] \vee [z \neq 0 \& S(x \cdot z) \cdot S(y \cdot z) = S(z \cdot z \cdot S(x \cdot y))]$$

$$u = 0 \iff \forall x\, (x \not< u)$$

$$v = S(u) \iff \forall w\, (u < w \longleftrightarrow v = w \vee v < w)$$

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (28/36)

Multiplication and Order

$\langle \mathbb{Z}, \cdot, < \rangle$ or $\langle \mathbb{Q}, \cdot, < \rangle$? – Missing in the Literature

Defining $+$ in $\langle \mathbb{Z}, \cdot, < \rangle$:
In $\mathbb{N}$ we had $x + y = 0 \longleftrightarrow x = y = 0$. But Not in $\mathbb{Z}$!
In $\mathbb{Z}$ we could have $x + y = 0 \longleftrightarrow S(x \cdot y) = S(x) \cdot S(y)$.
So, $\mathrm{Th}(\mathbb{Z}, \cdot, <) \notin \Delta_1$ again from
Gödel's Incompleteness Theorem and $\mathrm{Th}(\mathbb{Z}, +, \cdot) \notin \Delta_1$.

But, $\mathrm{Th}(\mathbb{Q}, \cdot, <) \in \Delta_1$

Theorem (NEW)

The theory of the structure $\langle \mathbb{Q}, 0, 1, -1, R_2, R_3, R_4, \ldots, {}^{-1}, \cdot, < \rangle$ *admits quantifier elimination.*

Recall: in $\mathbb{Q}$ we had $R_n(x) \equiv \exists y (x = y^n)$.

A Complete Picture

Decidability and Undecidability

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1
$\{\cdot,<\}$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1	–

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (30/36)

Exponentiation

in $\mathbb{N}, \mathbb{R}$ and $\mathbb{C}$

$\exp(x, y) = x^y$ Gödel: $\exp$ is definable in $\langle \mathbb{N}, +, \cdot \rangle$.

Also, $\cdot$ and $+$ are definable by $\exp$:

$x \cdot y = z \iff \forall u \big(\exp(u, z) = \exp(\exp(u, x), y) \big)$

$x + y = z \iff \forall u \big(\exp(u, z) = \exp(u, x) \cdot \exp(u, y) \big)$

So, $\mathrm{Th}(\mathbb{N}, \exp) \notin \Delta_1$.

For $\mathbb{R}$ and $\mathbb{C}$ we consider natural exponentiation: $\mathtt{E}(x) = e^x$.

Open Problem: Is $\mathrm{Th}(\mathbb{R}, +, \cdot, \mathtt{E})$ Decidable?

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (31/36)

Exponentiation

in $\mathbb{N}, \mathbb{R}$ and $\mathbb{C}$

Surprise: $\mathbb{Z}$ is definable in $\langle \mathbb{C}, +, \cdot, \mathtt{E} \rangle$:

$$z \in \mathbb{Z} \iff \forall x, y \left(x \cdot x + 1 = 0 \wedge \mathtt{E}(x \cdot y) = 1 \longrightarrow \mathtt{E}(x \cdot y \cdot z) = 1 \right)$$

And so are $\mathbb{N}$ and $\mathbb{Q}$ (definable in $\langle \mathbb{C}, +, \cdot, \mathtt{E} \rangle$.)

Whence, $\mathrm{Th}(\mathbb{C}, +, \cdot, \mathtt{E}) \notin \Delta_1$.

Open Problem: Is $\mathbb{R}$ definable in $\mathrm{Th}(\mathbb{C}, +, \cdot, \mathtt{E})$?
$\mathbb{R} \in \mathrm{Def}_{R_1}(\mathbb{C}, +, \cdot, \mathtt{E})$?

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (32/36)

Exponentiation

in $\mathbb{N}, \mathbb{R}$ and $\mathbb{C}$

Tarski's Exponential Function Problem

http://en.wikipedia.org/wiki/Tarski's_exponential_function_problem

D. MARKER, *Model Theory and Exponentiation*, Notices AMS 43 (1996) 753–759.

A. MACINTYRE, A. J. WILKIE, *On the Decidability of the Real Exponential Field*, in P. Odifreddi (ed.) Kreiseliana: about and around Georg Kreisel, A. K. Peters (1996) pp. 441–467.

Zilber's Conjecture: Every Definable Subset of $\langle \mathbb{C}, +, \cdot, \mathrm{E} \rangle$ is either Countable or Co-Countable.

D. MARKER, *A Remark on Zilber's Pseudoexponentiation*, JSL 71 (2006) 791–798.

D. MARKER, *Zilber's Pseudoexponentiation*, Slides of a Talk in "Algebra, Combinatorics and Model Theory", Istanbul, 22–26 August 2011. http://home.ku.edu.tr/∼modeltheory/Marker.pdf

A. J. WILKIE, *Some Results and Problems on Complex Germs With Definable Mittag-Lefler Stars*, MIMS EPrint 2012.86. http://eprints.ma.man.ac.uk/1877/01/covered/MIMS_ep2012_86.pdf

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (33/36)

A More Complete Picture

Decidability and Undecidability

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,<\}$	Δ_1	Δ_1	Δ_1	Δ_1	–
$\{+,\cdot\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1
$\{\cdot,<\}$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1	–
E	$\not\Delta_1$	–	–	¿?	$\not\Delta_1$

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (34/36)

Another Complete Picture

Definability and Undefinability

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$					–
$\{+\}$	$<$				
$\{\cdot\}$					
$\{+,<\}$		$\mathbb{N}$			–
$\{+,\cdot\}$	$<,\exp$	$<,\mathbb{N}$	$<,\mathbb{N},\mathbb{Z}$	$<$	
$\{\cdot,<\}$	$+,\exp$	$+,\mathbb{N}$			–
E	$+,\cdot,<$	–	–	$<$	$\mathbb{N},\mathbb{Z},\mathbb{Q}$ [¿$\mathbb{R}$?]

DECIDABILITY AND UNDEFINABILITY: A Case for Quantifier Elimination — Kerman, 14 &15 November 2012 (35/36)

Thank You!

Thanks To
The Participants
for Listening and for Your Patience!
and thanks to The Organizers.