AXIOMATIZING MATHEMATICAL THEORIES: Multiplication

Saeed Salehi

University of Tabriz

http://SaeedSalehi.ir/

25–27 December 2012
Sharif University of Technology, Tehran

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication   Frontiers Math. Sci., Sharif, Tehran, Dec. 2012   (1/22)

Algebraic Geometry

$\mathbb{R}$ and $\mathbb{C}$ with $+$ and $\cdot$

Tarski & Chevalley:

The projection of a constructible set is constructible.

Constructible: Boolean (complementation, intersection, $\cdots$)
Combinations of $\{\overline{x} \mid \mathsf{p}(\overline{x}) = 0\}$'s.

Tarski & Seidenberg:

The projection of a semi-algebraic set is semialgebraic.

Semi-Algebraic:

Finite Union of $\{\overline{x} \mid \mathsf{p}(\overline{x}) = 0\}$'s and $\{\overline{x} \mid \mathsf{p}(\overline{x}) > 0\}$'s.

Mathematical Logic

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

Tarski: The (First-Order Logical) Theory of the Structure $\langle \mathbb{C}, +, \cdot, 0, 1, -, ^{-1} \rangle$ is Decidable and CAN BE AXIOMATIZED AS an **Algebraically Closed Field.**

- $x + (y + z) = (x + y) + z$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x + y = y + x$
- $x \cdot y = y \cdot x$
- $x + 0 = x$
- $x \cdot 1 = x$
- $x + (-x) = 0$
- $x \neq 0 \rightarrow x \cdot x^{-1} = 1$
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $0 \neq 1$
- $\exists x \big(x^n + \mathbf{a_1} x^{n-1} + \mathbf{a_2} x^{n-2} + \cdots + \mathbf{a_{n-1}} x + \mathbf{a_n} = 0\big)$

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication Frontiers Math. Sci., Sharif, Tehran, Dec. 2012 (3/22)

Mathematical Logic

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

Tarski: The (First-Order Logical) Theory of the Structure $\langle \mathbb{R}, +, \cdot, 0, 1, -, ^{-1}, < \rangle$ is Decidable and CAN BE AXIOMATIZED AS a **Real Closed (Ordered) Field.**

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + 0 = x$
- $x + (-x) = 0$
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $x < y < z \to x < z$
- $x < y \to x + z < y + z$
- $x < y \wedge 0 < z \to x \cdot z < y \cdot z$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x \cdot y = y \cdot x$
- $x \cdot 1 = x$
- $x \neq 0 \to x \cdot x^{-1} = 1$
- $0 \neq 1$
- $x < y \vee x = y \vee y < x$
- $x \not< x$
- $0 < z \to \exists y (z = y \cdot y)$
- $\exists x \big(x^{2n+1} + \mathbf{a_1} x^{2n} + \cdots + \mathbf{a_{2n}} x + \mathbf{a_{2n+1}} = 0 \big)$

Some References

- 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.

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication Frontiers Math. Sci., Sharif, Tehran, Dec. 2012 (5/22)

Axiomatizing Mathematical Structures

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:

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

The Theories of $\langle\mathbb{Q},+\rangle$, $\langle\mathbb{R},+\rangle$ and $\langle\mathbb{C},+\rangle$ Are Decidable.

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication Frontiers Math. Sci., Sharif, Tehran, Dec. 2012 (6/22)

Axiomatizing Mathematical Structures

Addition $+$

The Theory of $\langle\mathbb{Z},+\rangle$ is also Decidable, and Axiomatizable as Non-Trivial Torsion-Free Abelian Group with Division Algorithm.

Axioms of $\langle\mathbb{Z},+,0,1,-\rangle$:

- $\forall x,y,z\,\big(x+(y+z)=(x+y)+z\big)$
- $\forall x,y\,\big(x+y=y+x\big)$
- $0\neq 1$
- $\forall x\exists y\,\big(\bigvee_{i<n}(x=n\centerdot y+i)\big)$
- $\forall x\,\big(x+0=x\big)$
- $\forall x\,\big(x+(-x)=0\big)$
- $\forall x\,\big(n\centerdot x=0\rightarrow x=0\big)$

$n\centerdot\alpha=\underbrace{\alpha+\cdots+\alpha}_{n-\text{times}}$

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

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

Axiomatizing Mathematical Structures

Addition $+$

The Theory of $\langle\mathbb{N},+\rangle$ is also Decidable, and Axiomatizable as Non-Trivial Ordered Abelian Monoid with Division Algorithm.

Axioms of $\langle\mathbb{N},+,0,1,<\rangle$:

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

$$n\centerdot\alpha=\underbrace{\alpha+\cdots+\alpha}_{n-\text{times}}$$

Decidability of Mathematical Structures

Decision Problem for the Following Structures

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{+\}$	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{Z},+\rangle$	$\langle\mathbb{Q},+\rangle$	$\langle\mathbb{R},+\rangle$	$\langle\mathbb{C},+\rangle$
$\{\cdot\}$	$\langle\mathbb{N},\cdot\rangle$	$\langle\mathbb{Z},\cdot\rangle$	$\langle\mathbb{Q},\cdot\rangle$	$\langle\mathbb{R},\cdot\rangle$	$\langle\mathbb{C},\cdot\rangle$
$\{+,\cdot\}$	$\langle\mathbb{N},+,\cdot\rangle$	$\langle\mathbb{Z},+,\cdot\rangle$	$\langle\mathbb{Q},+,\cdot\rangle$	$\langle\mathbb{R},+,\cdot\rangle$	$\langle\mathbb{C},+,\cdot\rangle$
E	$\langle\mathbb{N},\exp\rangle$	$\setminus$	$\setminus$	$\langle\mathbb{R},+,\cdot,e^x\rangle$	$\langle\mathbb{C},+,\cdot,e^x\rangle$

The Theory of Multiplication

Mainly Missing ...

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

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.

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

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication Frontiers Math. Sci., Sharif, Tehran, Dec. 2012 (10/22)

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.

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
$\{\cdot\}$	Δ_1	¿ Δ_1	¿ ?	Δ_1 ?	Δ_1 ?
$\{+,\cdot\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication   Frontiers Math. Sci., Sharif, Tehran, Dec. 2012   (12/22)

Multiplicative Theory of

The Complex Numbers $\mathbb{C}$

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.

The Structure $\langle \mathbb{C}, \cdot, 0, ^{-1}, \omega_1, \omega_2, \omega_3, \omega_4, \ldots \rangle$ Is Axiomatized By:

- $\forall x, y, z\, \big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$
- $\forall x\, \big(x \cdot 1 = x\big)$
- $\forall x\, \big(x \neq 0 \rightarrow x \cdot x^{-1} = 1\big)$
- $\forall x, y\, \big(x \cdot y = y \cdot x\big)$
- $\forall x\, \big(x^n = 1 \longleftrightarrow \bigvee_{i<n} x = (\omega_n)^i\big)$
- $\forall x\, \big(x \cdot 0 = 0 \neq 1\big)$
- $\bigwedge_{i \neq j < n} (\omega_n)^i \neq (\omega_n)^j$

Multiplicative Theory of

The Real Numbers $\mathbb{R}$

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

- $\forall x, y, z \left(x \cdot (y \cdot z) = (x \cdot y) \cdot z \right)$
- $\forall x \left(x \cdot x^{-1} = 1 \right)$
- $\forall x \left(x^n = 1 \rightarrow x = 1 \right)$
- $\exists x \left(x \neq 1 \right)$
- $\forall x \left(x \cdot 1 = x \right)$
- $\forall x, y \left(x \cdot y = y \cdot x \right)$
- $\forall x \exists y \left(x = y^n \right)$

Multiplicative Theory of

The Real Numbers $\mathbb{R}$

The Structure $\langle \mathbb{R}, \cdot, 0, 1, -1, ^{-1}, \mathscr{P} \rangle$

$$\left[\mathscr{P}(x) \equiv \text{“}x > 0\text{”} \ \& \ 0^{-1} = 0\right]$$

Can Be Axiomatized By:

- $\forall x, y, z \left(x \cdot (y \cdot z) = (x \cdot y) \cdot z\right)$
- $\forall x \left(x \neq 0 \rightarrow x \cdot x^{-1} = 1\right)$
- $\forall x \left(\mathscr{P}(x) \longleftrightarrow \exists y \, [y \neq 0 \wedge x = y^{2n}]\right)$
- $\forall x \left(x^{2n} = 1 \longleftrightarrow x = 1 \vee x = -1\right)$
- $\forall x \left(x^{2n+1} = 1 \rightarrow x = 1\right)$
- $\forall x \left(x \neq 0 \rightarrow [\neg \mathscr{P}(x) \leftrightarrow \mathscr{P}(\backsim x)]\right)$
- $\forall x \left(x \cdot 1 = x\right)$
- $\forall x, y \left(x \cdot y = y \cdot x\right)$
- $\forall x \exists y \left(x = y^{2n+1}\right)$
- $\forall x \left(x \cdot 0 = 0 \neq 1\right)$
- $\neg \mathscr{P}(0) \wedge \mathscr{P}(1) \wedge \neg \mathscr{P}(-1)$

$\backsim x = (-1) \cdot x$

- $\forall x, y \left(\mathscr{P}(x \cdot y) \longleftrightarrow [\mathscr{P}(x) \wedge \mathscr{P}(y)] \vee [\mathscr{P}(\backsim x) \wedge \mathscr{P}(\backsim y)]\right)$

Multiplicative Theory of

The Rational Numbers $\mathbb{Q}$

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

Theorem (NEW)

The theory of the structure $\langle \mathbb{Q}^+, \cdot, 1, R_2, R_3, R_4, \ldots, ^{-1} \rangle$ admits quantifier elimination, and so is decidable.

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

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 $\exp$:

$x \cdot y = z \iff \forall u \left(u^z = (u^x)^y \right)$

$x + y = z \iff \forall u \left(u^z = u^x \cdot u^y \right)$

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

For $\mathbb{R}$ and $\mathbb{C}$ we consider natural exponentiation: $x \mapsto e^x$.

Open Problem: Is $\mathrm{Th}(\mathbb{R}, +, \cdot, e^x)$ Decidable?

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication Frontiers Math. Sci., Sharif, Tehran, Dec. 2012 (17/22)

Exponentiation

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

Surprise: $\mathbb{Z}$ is definable in $\langle \mathbb{C}, +, \cdot, e^x \rangle$:

$$z \in \mathbb{Z} \iff \forall x, y \left(x^2 + 1 = 0 \wedge e^{(x \cdot y)} = 1 \longrightarrow e^{(x \cdot y \cdot z)} = 1\right)$$

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

Whence, $\mathrm{Th}(\mathbb{C}, +, \cdot, e^x) \notin \Delta_1$.

Open Problem: Is $\mathbb{R}$ definable in $\mathrm{Th}(\mathbb{C}, +, \cdot, e^x)$?

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 $\langle \mathbb{C}, +, \cdot, e^x \rangle$ 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-Leffler Stars*, MIMS EPrint 2012.86. http://eprints.ma.man.ac.uk/1877/01/covered/MIMS_ep2012_86.pdf

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
$\{\cdot\}$	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\{+,\cdot\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1
E	$\not\Delta_1$	–	–	¿?	$\not\Delta_1$

Tarski's Exponential Function Problem is equivalent to Weak Schanuel's Conjecture:

there is an effective procedure that, given $n \geqslant 1$ and exponential polynomials in n variables with integer coefficients $f_1, \cdots, f_n, g$ produces an integer $\eta \geqslant 1$ that depends on $n, f_1, \cdots, f_n, g$ and such that if $\alpha \in \mathbb{R}^n$ is a non-singular solution of the system $\bigwedge_{1 \leqslant i \leqslant n} f_i(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$ then either $g(\alpha) = 0$ or $|g(\alpha)| > \eta^{-1}$.

Difficulty of Some Problems

With High School Definitions

L. HENKIN, *The Logic of Equality*, The American Mathematical Monthly 84 (1977) 597–612.

Every Equality of $\langle \mathbb{N}, +, 0 \rangle$ can be derived from the axioms:

Associativity:	$x + (y + z) = (x + y) + z$
Commutativity:	$x + y = y + x$
Zero Element:	$x + 0 = x$

The same holds for $\langle \mathbb{Z}, +, 0 \rangle$, $\langle \mathbb{N}^{+}, \cdot, 1 \rangle$, $\langle \mathbb{N}, \cdot, 1 \rangle$, $\langle \mathbb{Z}, \cdot, 1 \rangle$, ...

Equalities of $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ and $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ Are Axiomatized by

Associativity:	$x + (y + z) = (x + y) + z$	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Commutativity:	$x + y = y + x$	$x \cdot y = y \cdot x$
Unit Element:	$x + 0 = x$	$x \cdot 1 = x$
Distributivity & Zero:	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	$x \cdot 0 = 0$

Difficulty of Some Problems

With High School Definitions

Tarski's High School Algebra Problem:

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

Can Every Equality of $\langle \mathbb{N}, +, \cdot, \exp, 0, 1 \rangle$ be derived from:
Associativity and Commutativity of $+$ and $\cdot$, Identity of 0 and 1,
Distributivity of $\cdot$ over $+$, and Zero Property 0; plus

$$\begin{array}{l|l} x^0 = 1 & x^{y+z} = x^y \cdot x^z \\ x^1 = x & (x \cdot y)^z = (x^z) \cdot (y^z) \\ 1^x = 1 & x^{y \cdot z} = (x^y)^z \end{array}$$

?

AXIOMATIZING MATHEMATICAL THEORIES: Multiplication Frontiers Math. Sci., Sharif, Tehran, Dec. 2012 (22/22)

Thank You!

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