Axiomatizing Mathematical Theories: Multiplication and Order

ZIBA ASSADI SAEED SALEHI

University of Tabriz

An Extended Abstract submitted to the 5th Annual Seminar of the Iranian Association for Logic.

The ordered structures of natural, integer, rational and real numbers will be studied. It is known that the theories of these numbers in the language of order are decidable and finitely axiomatizable. Also, their theories in the language of order and addition are decidable and infinitely axiomatizable. For the language of order and multiplication, it is known that the theories of $\mathbb{N}$ and $\mathbb{Z}$ are not decidable (and so not axiomatizable by any computably enumerable set of sentences). By Tarski's theorem, the multiplicative ordered structure of $\mathbb{R}$ is decidable also; we will give a direct proof for this result with an explicit axiomatization. The structure of $\mathbb{Q}$ in the language of order and multiplication seems to be missing in the literature; in this talk we will show the decidability of its theory by the technique of quantifier elimination and after presenting an infinite axiomatization for this structure we will prove that it is not finitely axiomatizable.

Entscheidungsproblem, one of the fundamental problems of (mathematical) logic, asks for a single-input Boolean-output algorithm that takes a formula φ as input and outputs `'yes'` if φ is logically valid and outputs `'no'` otherwise. Now, we know that this problem is not (computably) solvable. One reason for this is the existence of an essentially undecidable and finitely axiomatizable theory, see e.g. [10]; for another proof see [2, Theorem 11.2]. However, by Gödel's completeness theorem, the set of logically valid formulas is computably enumerable, i.e., there exists an input-free algorithms that (after running) lists all the valid formulas (and nothing else). For the structures, since their theories are complete, the story is different: the theory of a structure is either decidable or that structure is not axiomatizable (by any computably enumerable set of sentences; see e.g. [3, Corollaries 25G and 26I] or [5, Theorem 15.2]). For example, the additive theory of natural numbers $\langle \mathbb{N}; + \rangle$ was shown to be decidable by Presburger in 1929 (and by Skolem in 1930; see [9]). The multiplicative theory of the natural numbers $\langle \mathbb{N}; \times \rangle$ was announced

to be decidable by Skolem in 1930. Then it was expected that the theory of addition and multiplication of natural numbers would be decidable too; confirming Hilbert's Program. But the world was shocked in 1931 by Gödel's incompleteness theorem which implies that the theory of $\langle \mathbb{N}; +, \times \rangle$ is undecidable.

The theory of the structure $\langle \mathbb{N}; <, \times \rangle$ is not decidable (and so no computably enumerable set of sentences can axiomatize this structure). This is because:

- The addition operation is definable in $\langle \mathbb{N}; <, \times \rangle$, since
  - successor $\mathfrak{s}$ is definable from $<$: $y = \mathfrak{s}(x) \iff x < y \wedge \neg \exists z (x < z < y)$,
  - and addition is definable from the successor and multiplication: $z = x + y \iff$ $\big[\neg \exists u (\mathfrak{s}(u) = z) \wedge x = y = z\big] \vee \big[\exists u (\mathfrak{s}(u) = z) \wedge \mathfrak{s}(z \cdot x) \cdot \mathfrak{s}(z \cdot y) = \mathfrak{s}(z \cdot z \cdot \mathfrak{s}(x \cdot y))\big]$.

  This identity was introduced by Robinson [6]; see also [2, Chapter 24] or [3, Exercise 2 on page 281].
- Thus the structure $\langle \mathbb{N}; <, \times \rangle$ can interpret the structure $\langle \mathbb{N}; +, \times \rangle$ whose theory is undecidable (see e.g. [2, Theorem 17.4], [3, Corollary 35A], [4, Theorem 4.1.7], [5, Chapter 15] or [9, Corollary 6.4 in Chapter III]).

The undecidability of the theory of the structure $\langle \mathbb{N}; +, \times \rangle$ also implies the undecidability of the theories of the structures $\langle \mathbb{Z}; +, \times \rangle$ and $\langle \mathbb{Z}; <, \times \rangle$ as follows:

- By Lagrange's Four Square Theorem (see e.g. [5, Theorem 16.6]) $\mathbb{N}$ is definable in $\langle \mathbb{Z}; +, \times \rangle$, and so $\langle \mathbb{Z}; +, \times \rangle$ has an undecidable theory (see e.g. [5, Theorem 16.7] or [9, Corollary 8.29, Chapter III]).
- There is a beautiful definition for $+$ in terms of $\mathfrak{s}$ and $\times$ in $\mathbb{Z}$ on page 187 of [4]: $z = x + y \iff$ $[z \cdot \mathfrak{s}(z) = z \wedge \mathfrak{s}(x \cdot y) = \mathfrak{s}(x) \cdot \mathfrak{s}(y)] \vee [z \cdot \mathfrak{s}(z) \neq z \wedge \mathfrak{s}(z \cdot x) \cdot \mathfrak{s}(z \cdot y) = \mathfrak{s}(z \cdot z \cdot \mathfrak{s}(x \cdot y))]$.
- Whence, the structure $\langle \mathbb{Z}; <, \times \rangle$ can interpret the undecidable structure $\langle \mathbb{Z}; +, \times \rangle$.

Theorem 1 (Axiomatizablity of $\langle \mathbb{R}; <, \times \rangle$) *The following infinite theory completely axiomatizes the order and multiplicative theory of the real numbers and, moreover, the structure $\langle \mathbb{R}; <, \times, \square^{-1}, -\mathbf{1}, \mathbf{0}, \mathbf{1} \rangle$ admits quantifier elimination, and so its theory is decidable.*

(M_1)	$\forall x, y, z\, (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$	(O_1)	$\forall x, y (x < y \to y \not< x)$
(M_2°)	$\forall x (x \cdot \mathbf{1} = x \ \wedge \ x \cdot \mathbf{0} = \mathbf{0} = \mathbf{0}^{-1})$	(O_2)	$\forall x, y, z (x < y < z \to x < z)$
(M_3°)	$\forall x (x \neq \mathbf{0} \to x \cdot x^{-1} = \mathbf{1})$	(O_3)	$\forall x, y (x < y \vee x = y \vee y < x)$
(M_4)	$\forall x, y (x \cdot y = y \cdot x)$		
(M_5°)	$\forall x, y, z (x < y \wedge \mathbf{0} < z \to x \cdot z < y \cdot z)$	$(M_5^\bullet)$	$\forall x, y, z (x < y \wedge z < \mathbf{0} \to y \cdot z < x \cdot z)$
(M_6°)	$\exists y (-\mathbf{1} < \mathbf{0} < \mathbf{1} < y)$		
(M_7°)	$\forall x \exists y (x = y^{2n+1})$		
(M_8)	$\forall x (x^{2n} = \mathbf{1} \longleftrightarrow x = \mathbf{1} \vee x = -\mathbf{1})$		
(M_9)	$\forall x\, (\mathbf{0} < x \longleftrightarrow \exists y [y \neq \mathbf{0} \wedge x = y^2])$		

Definition 2 *Let $\Re_n(y)$ be the formula $\exists x (y = x^n)$, stating that "y is the nth power of a number".*

Now we can introduce our candidate axiomatization for the theory of the structure $\langle \mathbb{Q}^+; <, \times \rangle$.

Definition 3 *Let* TQ *be the theory axiomatized by the following*

(O_1) $\forall x, y(x < y \to y \not< x)$
(O_2) $\forall x, y, z(x < y < z \to x < z)$
(O_3) $\forall x, y(x < y \vee x = y \vee y < x)$
(M_1) $\forall x, y, z\,(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
(M_2) $\forall x(x \cdot \mathbf{1} = x)$
(M_3) $\forall x(x \cdot x^{-1} = \mathbf{1})$
(M_4) $\forall x, y(x \cdot y = y \cdot x)$
(M_5) $\forall x, y, z(x < y \to x \cdot z < y \cdot z)$
(M_6) $\exists y(y \neq \mathbf{1})$
(M_{10}) $\forall x, z \exists y(x < z \to x < y^n < z)$
(M_{11}) $\forall x_1, x_2, \cdots \exists y \forall z \bigwedge\!\!\!\bigwedge_{m_j \nmid n}(y^n \cdot x_j \neq z^{m_j})$ *for each* $n \geqslant 1$ (*and* $m_j > 1$).

The axiom $\mathtt{M}_{10}$, interpreted in $\mathbb{Q}^+$, states that $\mathbb{Q}^+$ is dense not only in itself but also in the radicals of its elements (for any $x, z \in \mathbb{Q}^+$ there exists some $y \in \mathbb{Q}^+$ that satisfies $\sqrt[n]{x} < y < \sqrt[n]{z}$). The axiom $\mathtt{M}_{11}$, interpreted in $\mathbb{Q}^+$ again, is actually equivalent with the fact that for any sequences $x_1, \cdots, x_q \in \mathbb{Q}^+$ and $m_1, \cdots, m_q \in \mathbb{N}^+$ none of which divides n (in symbols $m_j \nmid n$), there exists some $y \in \mathbb{Q}^+$ such that $\bigwedge\!\!\!\bigwedge_j \neg \Re_{m_j}(y^n \cdot x_j)$. This axiom is not true in $\mathbb{R}^+$ (while $\mathtt{M}_{10}$ is true in it) and to see that why $\mathtt{M}_{11}$ is true in $\mathbb{Q}^+$ it suffices to note that for given $x_1, \cdots, x_q$ one can take y to be a prime number which does not appear in the unique factorization (of the enumerators and denominators of the reduced forms) of any of x_j's. In this case $y^n \cdot x_j$ can be an m_j's power (of a rational number) only when m_j divides n. The condition $m_j \nmid n$ is necessary, since otherwise if x_j happens to satisfy $\Re_{m_j}(x_j)$ then no y can satisfy $\neg \Re_{m_j}(y^n \cdot x_j)$.

Theorem 4 (Axiomatizablity of $\langle \mathbb{Q}; <, \times \rangle$) *The infinite theory* TQ *completely axiomatizes the theory of* $\langle \mathbb{Q}^+; <, \times \rangle$, *and* $\langle \mathbb{Q}^+; <, \times, \square^{-1}, \mathbf{1}, \{\Re_n\}_{n>1} \rangle$ *admits quantifier elimination.*

Also, the structure $\langle \mathbb{Q}; <, \times \rangle$ *can be completely axiomatized by the theory that results from* TQ *by adding the axioms* M_8 (*in Theorem 1*) *and substituting its* M_2, M_3, M_5, M_6 *and* M_{10} *with the axioms* M_2°, M_3°, M_5°, $M_5^\bullet$, M_6° *and* (M_{10}°) $\forall x, z \exists y(\mathbf{0} < x < z \to x < y^n < z)$, *respectively.*

Moreover, the theory of the structure $\langle \mathbb{Q}; <, \times, \square^{-1}, -\mathbf{1}, \mathbf{0}, \mathbf{1}, \{\Re_n\}_{n>1} \rangle$ *admits quantifier elimination.*

In the following table the decidable structures are denoted by Δ_1 and the undecidable ones by $\not\Delta_1$:

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$
$\{<\}$	Δ_1	Δ_1	Δ_1	Δ_1
$\{<, +\}$	Δ_1	Δ_1	Δ_1	Δ_1
$\{<, \times\}$	$\not\Delta_1$	$\not\Delta_1$	Δ_1	Δ_1
$\{+, \times\}$	$\not\Delta_1$	$\not\Delta_1$	$\not\Delta_1$	Δ_1

References

[1] ZIBA ASSADI & SAEED SALEHI, *On the Decidability of the Ordered Structures of Numbers*, Submitted for Publication. **arXiv**:1709.05157. Available at https://arxiv.org/pdf/1709.05157.

[2] GEORGE S. BOOLOS & JOHN P. BURGESS & RICHARD C. JEFFREY, **Computability and Logic**, Cambridge University Press (5^{th} ed. 2007).

[3] HERBERT B. ENDERTON, **A Mathematical Introduction to Logic**, Academic Press (2^{nd} ed. 2001).

[4] PETER G. HINMAN, **Fundamentals of Mathematical Logic**, CRC Press (2005).

[5] J. DONALD MONK, **Mathematical Logic**, Springer (1976).

[6] JULIA ROBINSON, *Definability and Decision Problems in Arithmetic*, **The Journal of Symbolic Logic** 14:2 (1949) 98–114.

[7] SAEED SALEHI, "*Axiomatizing Mathematical Theories: Multiplication*", in: A. Kamali-Nejad (ed.) **Proceedings of Frontiers in Mathematical Sciences**, Sharif University of Technology, Tehran, Iran (2012), pp. 165–176. URL: https://arxiv.org/pdf/1612.06525.pdf

[8] SAEED SALEHI, "*Computation in Logic and Logic in Computation*", in: B. Sadeghi-Bigham (ed.) **Proceedings of the Third International Conference on Contemporary Issues in Computer and Information Sciences (CICIS 2012)**, Brown Walker Press, USA (2012), pp. 580–583. URL: https://arxiv.org/pdf/1612.06526.pdf

[9] CRAIG SMORYŃSKI, **Logical Number Theory I: An Introduction**, Springer (1991).

[10] ALBERT VISSER, *On* Q, **Soft Computing** 21:1 (2017) 39–56.