Undecidability in abstract algebraic logic

Tommaso Moraschini

Universitat de Barcelona

July 2015

Contents

The problem

- Abstract algebraic logics classifies logics into two hierarchies:

  Leibniz hierarchy $\longmapsto$ definability of equivalence and of truth predicates

  Frege hierarchy $\longmapsto$ replacement properties

- Can we classify mechanically logics of Hilbert-style calculi in these hierarchies?
- We begin by the Leibniz hierarchy.

Definability of equivalence

- Given an algebra $\boldsymbol{A}$, the Leibniz congruence of $F \subseteq A$ is

$$\boldsymbol{\Omega}^{\boldsymbol{A}} F \coloneqq \max\{\theta \in \mathrm{Con}\boldsymbol{A} : F = \bigcup_{a \in F} a/\theta\}.$$

  $\boldsymbol{\Omega}^{\boldsymbol{A}} F$ represents equivalence from the point of view of F.
- A logic $\mathcal{L}$ is protoalgebraic if equivalence is definable, i.e., if there is a set of formulas $\Delta(x, y, \overline{z})$ such that for every model $\langle \boldsymbol{A}, F \rangle$ of $\mathcal{L}$:

$$\langle a, b \rangle \in \boldsymbol{\Omega}^{\boldsymbol{A}} F \Longleftrightarrow \Delta(a, b, \overline{c}) \subseteq F \text{ for every } \overline{c} \in A.$$

- A logic $\mathcal{L}$ is equivalential if it is protoalgebraic and $\Delta(x, y)$ has only variables x, y.

Definability of truth predicates

- The reduced models of a logic $\mathcal{L}$ are

$$\mathrm{Mod}^*\mathcal{L} = \{\langle \boldsymbol{A}, F\rangle : F \text{ is a filter of } \mathcal{L} \text{ and } \boldsymbol{\Omega}^{\boldsymbol{A}} F = \mathrm{Id}_{\boldsymbol{A}}\}.$$

  If $\langle \boldsymbol{A}, F\rangle$ is a matrix, then F can be thought as a truth predicate.

- A logic is truth-equational if truth predicates in $\mathrm{Mod}^*\mathcal{L}$ are definable, i.e., if there is a set of equations $\boldsymbol{\tau}(x)$ such that for every $\langle \boldsymbol{A}, F\rangle \in \mathrm{Mod}^*\mathcal{L}$:

$$F = \{a \in A : \boldsymbol{A} \vDash \boldsymbol{\tau}(a)\}.$$

The Leibniz hierarchy

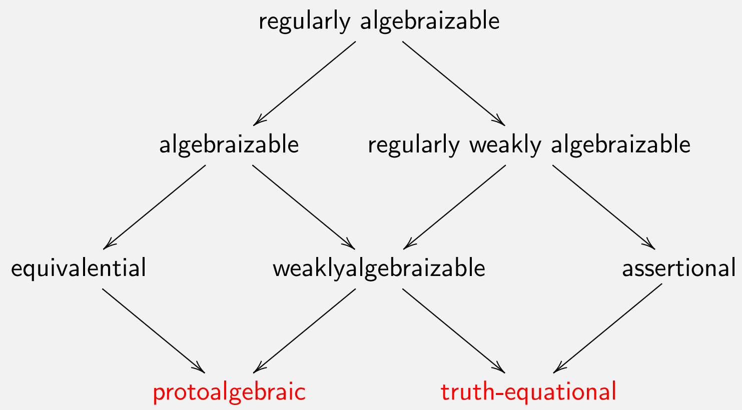


Figure: Some classes of the Leibniz hierarchy.

Basic logic of a variety

Definition

Let V be a non-trivial variety. $\mathcal{L}_{\mathrm{V}}$ is the logic determined by the following class of matrices:

$$\{\langle \boldsymbol{A}, F\rangle : \boldsymbol{A} \in \mathrm{V} \text{ and } F \subseteq A\}.$$

- Given $\Gamma \cup \{\varphi\} \subseteq Fm$, we will write $\Gamma \vdash_{\mathrm{V}} \varphi$ as a shortening for $\Gamma \vdash_{\mathcal{L}_{\mathrm{V}}} \varphi$.

Lemma

Let V be a non-trivial variety and $\Gamma \cup \{\varphi\} \subseteq Fm$.

1. $\mathrm{Alg}\,\mathcal{L}_{\mathrm{V}} = \mathrm{V}$.
2. $\Gamma \vdash_{\mathrm{V}} \varphi$ if and only if there is $\gamma \in \Gamma$ such that $\mathrm{V} \vDash \gamma \approx \varphi$.

Strategy and problems

- We want to reproduce Hilbert's tenth problem into the one of classifying logics of Hilbert calculi in the Leibniz hierarchy.

To speak about the variety of commutative rings with unit CR we will use the logic $\mathcal{L}_{\mathrm{CR}}$. Then we need:

- An explicit and finite axiomatization of $\mathcal{L}_{\mathrm{CR}}$.

Unfortunately, in general:

- No clever way to axiomatize $\mathcal{L}_{\mathrm{V}}$ out of a base for V.
- Even if V is finitely based, $\mathcal{L}_{\mathrm{V}}$ need not to be finitely axiomatizable.

Some examples

- The idea of converting equational bases into Hilbert rules does not work.

Let SL be the variety of semilattices. The rules

$$x \dashv\vdash x \wedge x \qquad x \wedge y \dashv\vdash y \wedge x \qquad x \wedge (y \wedge z) \dashv\vdash (x \wedge y) \wedge z$$

define a logic $\mathcal{R}$ strictly weaker than $\mathcal{L}_{\mathrm{SL}}$. Why? The matrix

$$\langle \boldsymbol{Z}_2, \{0\}\rangle \text{ where } \boldsymbol{Z}_2 = \langle \{0, 1\}, +\rangle$$

is a reduced model of $\mathcal{R}$. A complete axiomatization of $\mathcal{L}_{\mathrm{SL}}$ is obtained by adding:

$$u \wedge x \dashv\vdash u \wedge (x \wedge x) \quad u \wedge (x \wedge y) \dashv\vdash u \wedge (y \wedge x)$$

$$u \wedge (x \wedge (y \wedge z)) \dashv\vdash u \wedge ((x \wedge y) \wedge z)$$

Some examples

- Finitely based varieties can have a non-finitely axiomatizable logic.

Let CM be the variety of commutative magmas.
It has a finite base: $x \cdot y \approx y \cdot x$.
$\mathcal{L}_{\mathrm{CM}}$ is not finitely axiomatizable:

- Let Σ be a finite set of deductions holding in $\mathcal{L}_{\mathrm{CM}}$.
- There is a natural $n \geq 2$ that bounds the number of occurrences of (possibly equal) variables in terms appearing in the rules of Σ.

Some examples

Then consider the algebra $\boldsymbol{A} = \langle \{0, 1, 2, \ldots, n\}, \cdot\rangle$ with a binary operation such that $1 \cdot 2 \coloneqq 2$ and $2 \cdot 1 \coloneqq 1$ and

$$a \cdot b = b \cdot a \coloneqq \begin{cases} a & \text{if } a \neq n \text{ and } b = 0 \\ 0 & \text{if } a = n \text{ and } b = 0 \\ a & \text{if } b = a - 1 \text{ and } a \geq 3 \\ a - 1 & \text{if } b = a - 2 \text{ and } a \geq 3 \\ 1 & \text{otherwise} \end{cases}$$

for every $a, b \in A$ such that $\{a, b\} \neq \{1, 2\}$.

- $\langle \boldsymbol{A}, \{0\}\rangle$ is a model of Σ (drawing subformula tree).
- $\langle \boldsymbol{A}, \{0\}\rangle$ is not a model of $\mathcal{L}_{\mathrm{CM}}$.
- Why? It is reduced: if $a, b \in A \smallsetminus \{0\}$ and $a < b$, we consider the polynomial

  $$p(x) \coloneqq (\ldots((\ldots(\ldots((1 \cdot 2) \cdot 3) \cdot \ldots a) \cdot \cdots b - 1) \cdot x) \cdot \cdots n) \cdot 0.$$

  Then

  $$p(b) = 0 \text{ and } p(a) \neq 0.$$

A logic for commutative rings

Definition

Let $\mathcal{CR}$ be the logic axiomatized by the rules:

$$w + (u \cdot ((x \cdot y) \cdot z)) \dashv\vdash w + (u \cdot (x \cdot (y \cdot z))) \tag{A}$$
$$w + (u \cdot (x \cdot y)) \dashv\vdash w + (u \cdot (y \cdot x)) \tag{B}$$
$$w + (u \cdot (x \cdot 1)) \dashv\vdash w + (u \cdot x) \tag{C}$$
$$w + (u \cdot ((x + y) + z)) \dashv\vdash w + (u \cdot (x + (y + z))) \tag{D}$$
$$w + (u \cdot (x + y)) \dashv\vdash w + (u \cdot (y + x)) \tag{E}$$
$$w + (u \cdot (x + 0)) \dashv\vdash w + (u \cdot x) \tag{F}$$
$$w + (u \cdot (x + -x)) \dashv\vdash w + (u \cdot 0) \tag{G}$$
$$w + (u \cdot (x \cdot (y + z))) \dashv\vdash w + (u \cdot ((x \cdot y) + (x \cdot z))) \tag{H}$$
$$w + (u \cdot -(x + y)) \dashv\vdash w + (u \cdot (-x + -y)) \tag{I}$$
$$w + (u \cdot -(x \cdot y)) \dashv\vdash w + (u \cdot (-x \cdot y)) \tag{L}$$
$$w + (u \cdot -(x \cdot y)) \dashv\vdash w + (u \cdot (x \cdot -y)) \tag{M}$$
$$0 + x \dashv\vdash x \tag{N}$$
$$x + (1 \cdot y) \dashv\vdash x + y \tag{O}$$

A logic for commutative rings

Definition

Let $\mathcal{CR}$ be the logic axiomatized by the rules:

$$
\begin{aligned}
w + (u \cdot ((x \cdot y) \cdot z)) &\dashv\vdash w + (u \cdot (x \cdot (y \cdot z))) && \text{(A)}\\
w + (u \cdot (x \cdot y)) &\dashv\vdash w + (u \cdot (y \cdot x)) && \text{(B)}\\
w + (u \cdot (x \cdot 1)) &\dashv\vdash w + (u \cdot x) && \text{(C)}\\
w + (u \cdot ((x + y) + z)) &\dashv\vdash w + (u \cdot (x + (y + z))) && \text{(D)}\\
w + (u \cdot (x + y)) &\dashv\vdash w + (u \cdot (y + x)) && \text{(E)}\\
w + (u \cdot (x + 0)) &\dashv\vdash w + (u \cdot x) && \text{(F)}\\
w + (u \cdot (x + -x)) &\dashv\vdash w + (u \cdot 0) && \text{(G)}\\
w + (u \cdot (x \cdot (y + z))) &\dashv\vdash w + (u \cdot ((x \cdot y) + (x \cdot z))) && \text{(H)}\\
w + (u \cdot -(x + y)) &\dashv\vdash w + (u \cdot (-x + -y)) && \text{(I)}\\
w + (u \cdot -(x \cdot y)) &\dashv\vdash w + (u \cdot (-x \cdot y)) && \text{(L)}\\
w + (u \cdot -(x \cdot y)) &\dashv\vdash w + (u \cdot (x \cdot -y)) && \text{(M)}\\
0 + x &\dashv\vdash x && \text{(N)}\\
x + (1 \cdot y) &\dashv\vdash x + y && \text{(O)}
\end{aligned}
$$

Completeness

Theorem

The rules $\mathcal{CR}$ axiomatize $\mathcal{L}_{\mathsf{CR}}$.

Proof.

- The relation $\dashv\vdash_{\mathcal{CR}}$ is a congruence. Then:

$$
\begin{aligned}
\alpha \approx \beta \text{ is in the base of } CR &\Longrightarrow \alpha \dashv\vdash_{\mathcal{CR}} \beta\\
&\Longrightarrow \mathsf{Alg}\mathcal{CR} \vDash \alpha \approx \beta\\
&\Longrightarrow \mathsf{Alg}\mathcal{CR} \subseteq CR.
\end{aligned}
$$

- Since $\langle \boldsymbol{A}, F\rangle$ is a model of $\mathcal{L}_{CR}$ for every $\boldsymbol{A} \in CR$, we conclude that $\mathcal{L}_{\mathsf{CR}} \leq \mathcal{CR}$.
- Recall that: $\mathsf{CR} \vDash \alpha \approx \beta \Longleftrightarrow \alpha \dashv\vdash_{\mathsf{CR}} \beta$.
- This implies $\mathcal{CR} \leq \mathcal{L}_{\mathsf{CR}}$.

□

From equations to logics

Definition

Given a Diophantine equation $p(z_1, \ldots, z_n) \approx 0$, we pick two new variables x and y, a new binary symbol $\leftrightarrow$ and consider the logic $\mathcal{L}(p \approx 0)$ axiomatized by the rules:

$$
\begin{aligned}
\emptyset &\vdash x \leftrightarrow x && \text{(R)}\\
x \leftrightarrow y &\vdash y \leftrightarrow x && \text{(S)}\\
x \leftrightarrow y, y \leftrightarrow z &\vdash x \leftrightarrow z && \text{(T)}\\
x \leftrightarrow y &\vdash -x \leftrightarrow -y && \text{(Re1)}\\
x \leftrightarrow y, z \leftrightarrow u &\vdash (x + z) \leftrightarrow (y + u) && \text{(Re2)}\\
x \leftrightarrow y, z \leftrightarrow u &\vdash (x \cdot z) \leftrightarrow (y \cdot u) && \text{(Re3)}\\
x \leftrightarrow y, z \leftrightarrow u &\vdash (x \leftrightarrow z) \leftrightarrow (y \leftrightarrow u) && \text{(Re4)}\\
p(z_1, \ldots, z_n) \leftrightarrow 0, x, x \leftrightarrow y &\vdash y && \text{(MP')}\\
p(z_1, \ldots, z_n) \leftrightarrow 0, x &\dashv\vdash x \leftrightarrow (x \leftrightarrow x), p(z_1, \ldots, z_n) \leftrightarrow 0 && \text{(A3')}\\
p(z_1, \ldots, z_n) \leftrightarrow 0, x, y &\vdash x \leftrightarrow y && \text{(G')}
\end{aligned}
$$

plus the axioms of the form $\emptyset \vdash \alpha \leftrightarrow \beta$ for every $\alpha \dashv\vdash \beta \in \mathcal{CR}$.

Main result

The key result is the following:

Lemma

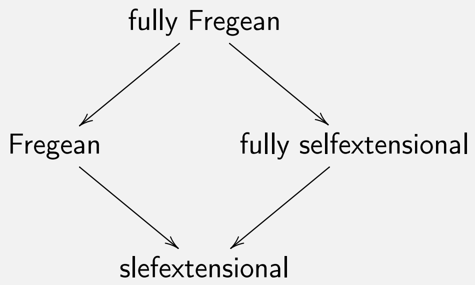
Let $p(z_1, \ldots, z_n) \approx 0$ be a Diophantine equation. The following conditions are equivalent:

(i) $\mathcal{L}(p \approx 0)$ is finitely regularly algebraizable.
(ii) $\mathcal{L}(p \approx 0)$ is truth-equational.
(iii) $\mathcal{L}(p \approx 0)$ is protoalgebraic.
(iv) The equation $p(z_1, \ldots, z_n) \approx 0$ has an integer solution.

Theorem

Let K a level of the Leibniz hierarchy. The problem of determining whether the logic of a finite Hilbert calculus in a finite language belongs to K is undecidable.

Frege hierarchy



- With a different strategy:

Theorem

Let K a level of the Frege hierarchy. The problem of determining whether the logic of a finite Hilbert calculus in a finite language belongs to K is undecidable.

Further work

- We saw that it is impossible to classify mechanically logics of Hilbert calculi into the Leibniz and Frege hierarchies.
- Is it possible to do this for logics of a finite set of finite matrices?
- For the Leibniz hierarchy yes.
- The Frege hiearchy seems more complicated, since it involves semantic notions.
- We have a positive solution for selfextentionality and Fregeanity, but the problem for their fully-versions in open.

Finally...

Thank you!