Logic and Foundation II

Part 6. Real-closed ordered fields: completeness and decidability

Kazuyuki Tanaka

BIMSA

April 9, 2024

北京雁栖湖应用数学研究院
Beijing Institute of Mathematical Sciences and Applications

Logic and Foundations II

- Part 5. Models of first-order arithmetic (continued)
- Part 6. Real-closed ordered fields: completeness and decidability
- Part 7. Theory of reals and reverse mathematics
- Part 8. Second order arithmetic and non-standard methods

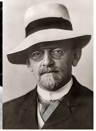
Part 6. Schedule

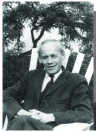
- March 28, (1) Basic properties of one-variable polynomials
- Apr. 2, (2) Real closed ordered fields and the Artin-Schreier theorem
- Apr. 9, (3) Quantifier elimination of RCOF
- Apr. 11, (4) Hilbert's 17th problem and o-minimal theories

Quantifier elimination of real closed ordered fields

- Tarski proved that the theory of real closed ordered fields admits elimination of quantifiers by improving Artin and Schreier's method for solving Hilbert's 17th problem.
- Subsequently, A. Robinson introduced the notion of model completeness, which is weaker than quantifier elimination but still has various applications.
- Furthermore, Shoenfield showed what conditions should be added to model completeness to lead to quantifier elimination.
- The general framework of the discussion today is based on [Schoenfield 67].
- For a proof of Tarski's theorem without using model theory, refer to [Adamowicz&Zbierski 97], [Kreisel&Krivine 71].


Tarski


Hilbert


Artin


Schreier


Robinson

Definition

A theory T satisfies the **isomorphism condition** if the following holds.
For each $i = 1, 2$, let $\mathfrak{L}_i$ be a model of T, and $\mathfrak{K}_i \subseteq \mathfrak{L}_i$.
Suppose there exists an isomorphism $f : \mathfrak{K}_1 \to \mathfrak{K}_2$. Then there exist models $\mathfrak{M}_i$ of T such that $\mathfrak{K}_i \subseteq \mathfrak{M}_i \subseteq \mathfrak{L}_i$, and f extends to an isomorphism between $\mathfrak{M}_1$ and $\mathfrak{M}_2$.

Definition

A theory T in a language $\mathcal{L}$ is **1-model complete** if the following holds:
Let $\mathfrak{K} \subseteq \mathfrak{L}$ be two models of T. For any open formula $\varphi(\vec{x}, y)$ in the language $\mathcal{L}$ and any tuple $\vec{a}$ from $\mathfrak{K}$, if $\mathfrak{L}_{\{\vec{a}\}} \models \exists y \varphi(\vec{a}, y)$, then $\mathfrak{K}_{\{\vec{a}\}} \models \exists y \varphi(\vec{a}, y)$.

As shown in the last lecture, the theory of real closed ordered fields RCOF is a 1-model complete theory that satisfies the isomorphism condition.

Theorem (Shoenfield)

A 1-model complete theory that satisfies the isomorphism condition admits elimination of quantifiers.

- Before proving the above theorem, we prepare two lemmas. Recall that a formula is said to be **open** if it has no quantifiers (i.e., no bound variables), and **closed** or a **sentence** if no free variables.
- When dealing with open sentences, instead of using variables, we add new constants to the language as needed. In this case, the following lemma is important.

Lemma (1)

If a theory T in a language $\mathcal{L}$ satisfies the isomorphism condition, then T also satisfies the isomorphism condition in the language $\mathcal{L} \cup C$, where C is a set of new constants. Similarly, a theory preserves 1-model completeness when the language is expanded by adding new constants.

Proof. Let T be a theory in a language $\mathcal{L}$ satisfying the isomorphism condition. For each $i = 1, 2$, let $\mathfrak{L}_i$ be a model of T in the language $\mathcal{L} \cup C$, where $\mathfrak{K}_i \subseteq \mathfrak{L}_i$, and suppose there exists an isomorphism $f : \mathfrak{K}_1 \to \mathfrak{K}_2$ in the language $\mathcal{L} \cup C$.

- Let $\mathfrak{K}'_i, \mathfrak{L}'_i$ be the reducts of $\mathfrak{K}_i, \mathfrak{L}_i$, respectively to the language $\mathcal{L}$ $(i = 1, 2)$. Then, $f : \mathfrak{K}_1 \to \mathfrak{K}_2$ induces an isomorphism $f' : \mathfrak{K}'_1 \to \mathfrak{K}'_2$.
- By the isomorphism condition of T in the language $\mathcal{L}$, there exist models $\mathfrak{M}'_i \subseteq \mathfrak{L}'_i$ of T in $\mathcal{L}$ and $f' : \mathfrak{K}'_1 \to \mathfrak{K}'_2$ extends to an isomorphism between $\mathfrak{M}'_1$ and $\mathfrak{M}'_2$.

- Since the constants of C are interpreted as elements of $\mathfrak{K}_i'$, we can define an expansion $\mathfrak{M}_i$ of $\mathfrak{M}_i'$ to $\mathcal{L} \cup C$ by adding this interpretation.
- Then, f' is naturally extended to an isomorphism between $\mathfrak{M}_1$ and $\mathfrak{M}_2$, which also extends $f : \mathfrak{K}_1 \to \mathfrak{K}_2$.
- Similar arguments hold for the preservation of 1-model completeness. □

Let $\mathfrak{A}$, $\mathfrak{B}$ be structures in a language containing one or more constants. We say that they are **equivalent with respect to the open sentences**, denote $\mathfrak{A} \equiv_0 \mathfrak{B}$, if for any open sentence φ, $\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{B} \models \varphi$.

Lemma (2)

Let $\mathcal{L}$ be a language containing one or more constants, and let T be a theory in $\mathcal{L}$. Then, for any sentence σ in $\mathcal{L}$, the following two conditions are equivalent:
(1) For any two models $\mathfrak{A}$ and $\mathfrak{B}$ of T with $\mathfrak{A} \equiv_0 \mathfrak{B}$,

$$\mathfrak{A} \models \sigma \Leftrightarrow \mathfrak{B} \models \sigma.$$

(2) There exists an open sentence φ of $\mathcal{L}$ such that $T \vdash \varphi \leftrightarrow \sigma$.

Proof. Since (2) $\Rightarrow$ (1) is obvious, we will prove (1) $\Rightarrow$ (2). Let

$$\Gamma = \{\varphi : T \vdash \sigma \to \varphi,\ \varphi \text{ is an open sentence.}\}$$

If we show $T \cup \Gamma \vdash \sigma$, there exists a finite subset $\{\varphi_1, \cdots, \varphi_n\} \subseteq \Gamma$ such that

$$T \vdash (\varphi_1 \land \cdots \land \varphi_n) \leftrightarrow \sigma$$

and thus (2) follows. Therefore, assuming $T \cup \Gamma \nvdash \sigma$, we derive a contradiction.

- By the completeness theorem, $T \cup \Gamma \cup \{\neg\sigma\}$ has a model $\mathfrak{A}$. Let Δ be the set of all open sentences that are true in $\mathfrak{A}$.
- Let $\mathfrak{B}$ be a model of $T \cup \Delta$. Then $\mathfrak{A} \equiv_0 \mathfrak{B}$. So by assumption (1), we have $\mathfrak{B} \models \neg\sigma$. Again by the completeness theorem, we obtain $T \cup \Delta \vdash \neg\sigma$.
- Then, there exists a finite subset $\{\psi_1, \cdots, \psi_m\} \subseteq \Delta$ such that

  $$T \vdash (\psi_1 \land \cdots \land \psi_m) \to \neg\sigma$$

  which implies

  $$T \vdash \sigma \to (\neg\psi_1 \lor \cdots \lor \neg\psi_m)$$

  Therefore, $(\neg\psi_1 \lor \cdots \lor \neg\psi_m) \in \Gamma \subseteq \Delta$, but this contradicts $\{\psi_1, \cdots, \psi_m\} \subseteq \Delta$. $\square$

Now we are ready to prove

Theorem (Shoenfield)

A 1-model complete theory that satisfies the isomorphism condition admits elimination of quantifiers.

Proof.

- Let T be a 1-model complete theory that satisfies the isomorphism condition. It is enough to show that for a formula in the form $\sigma \equiv \exists x \varphi$ with φ open, there exists an equivalent open formula.
- First, replace each free variable included in $\exists x \varphi$ with a new constant. So, we extend the language to include all of such constants. We may assume that the language $\mathcal{L}$ contains at least one constant. By Lemma (1), the isomorphism condition and 1-model completeness are preserved after expanding the language by adding new constants.
- By Lemma (2), it is sufficient to show that for any two models $\mathfrak{A} \equiv_0 \mathfrak{B}$ of T, we have $\mathfrak{A} \models \sigma \Leftrightarrow \mathfrak{B} \models \sigma$.

- Let $t^{\mathfrak{A}}$ and $t^{\mathfrak{B}}$ denote the interpretations of a term t (without variables) in $\mathfrak{A}$ and $\mathfrak{B}$, respectively. Define A' and B' as the sets of all such interpretations in $\mathfrak{A}$ and $\mathfrak{B}$, resp. Let $\mathfrak{A}'$ and $\mathfrak{B}'$ be substructures of $\mathfrak{A}$ and $\mathfrak{B}$ with restricted domains $\mathfrak{A}'$ and $\mathfrak{B}'$, resp.
- Let define a function $f : A' \to B'$ by $f(t^{\mathfrak{A}}) = t^{\mathfrak{B}}$ for each term t. Then it is easy to see that it is an isomorphism $f : \mathfrak{A}' \to \mathfrak{B}'$.
- Next, by isomorphism condition, there exists a model $\mathfrak{A}''$ of T such that $\mathfrak{A}' \subseteq \mathfrak{A}'' \subseteq \mathfrak{A}$ and a model $\mathfrak{B}''$ of T such that $\mathfrak{B}' \subseteq \mathfrak{B}'' \subseteq \mathfrak{B}$, and f can be extended to an isomorphism between $\mathfrak{A}''$ and $\mathfrak{B}''$.
- Since T is 1-model complete, for $\sigma \equiv \exists x \varphi$, we have

$$\mathfrak{A}'' \models \sigma \Leftrightarrow \mathfrak{A} \models \sigma, \quad \mathfrak{B}'' \models \sigma \Leftrightarrow \mathfrak{B} \models \sigma.$$

- On the other hand, since $\mathfrak{A}'' \cong \mathfrak{B}''$, we have $\mathfrak{A}'' \models \sigma \Leftrightarrow \mathfrak{B}'' \models \sigma$.
- Therefore,

$$\mathfrak{A} \models \sigma \Leftrightarrow \mathfrak{B} \models \sigma.$$

□

Corollary (Tarski)

The theory of real closed ordered fields RCOF *admits elimination of quantifiers.*

Definition (Lec03-02, last semester)

A theory T is **model complete** if for any model $\mathfrak{A}$, $\mathfrak{B}$ of T, $\mathfrak{A} \subseteq \mathfrak{B} \Rightarrow \mathfrak{A} \prec \mathfrak{B}$.

Remark: A theory is model-complete iff any formula is equivalent to a $\forall$-formula.

Corollary (Tarski)

RCOF *is model-complete, complete, and decidable.*

Proof. It is clear that RCOF is model-complete since it admits elimination of quantifiers. An atomic sentence of RCOF consists of constants $0, 1$, arithmetical operations $+, -, \cdot, /$ and relations $=, <$, and so its truth value can be easily obtained by rational calculation. Since an open sentence of RCOF is just a boolean combination of atomic sentences, its truth value is also finitely determined. Therefore, RCOF is complete and decidable. $\square$

Corollary (Tarski)

RCF *is model-complete, complete, and decidable.*

Proof.

- Let $\mathfrak{K} \subset \mathfrak{L}$ be two models of RCF. By defining $<$ as
$$x < y \leftrightarrow \exists z(z^2 + x = y \wedge z \neq 0),$$
$\mathfrak{K}$ and $\mathfrak{L}$ become models $\mathfrak{K}'$ and $\mathfrak{L}'$ of RCOF. By the model completeness of RCOF, $\mathfrak{K}'$ is an elementary substructure of $\mathfrak{L}'$, which remains the case even if $<$ is ignored. Hence, RCF is also model-complete.
- Every model of RCF has a substructure isomorphic to the real closure of the rational field $\mathfrak{Q} = (\mathbb{Q}, +, -, \cdot, /, 0, 1)$, which becomes an elementary substructure by model completeness. Thus, every model of RCF is elementary equivalent, hence it is complete.
- Since recursively axiomatizable complete theories are decidable, RCF is decidable. $\square$

Note that RCF does not admit elimination of quantifiers. In fact, we cannot construct an open formula expressing $x < y$ in RCF.

Additional remarks

- Mourgues-Ressayre (1993) shows that for any model $\mathfrak{M}$ of RCOF there exists a non-negative integer part $I \subset M$ that satisfies IOpen.
(Here, $I \subset M$ is a non-negative integer part, if for any element $r \geq 0$ of M, there is a unique $i \in I$ such that $i \leq r < i+1$)
- Furthermore, D'Aquino-Knight-Starchenko (2010) show that if a model $\mathfrak{M}$ of RCOF has a non-negative integer part that satisfies PA, it is recursively saturated. And the converse is also true when $\mathfrak{M}$ is countable.

Complex numbers and Hilbert's Nullstellensatz

- As we treated the structure of the real numbers as a real closed field, we will also treat the structure of complex numbers as an algebraically closed field.
- We can show that the theory of algebraically closed fields is model-complete, and admits elimination of quantifiers by similar arguments. From its model completeness, we can easily derive Hilbert's Nullstellensatz.

Definition

The theory ACF of **algebraically closed field** is a theory in the field language $\mathcal{L}_{\mathsf{AF}} = \{+, -, \cdot, /, 0, 1\}$ consisting of axioms of fields AF and the following axioms

$$\forall x_0 \forall x_1 \cdots \forall x_{n-1} \exists y \; x_0 + x_1 y + \cdots + x_{n-1} y^{n-1} + y^n = 0 \quad (n > 0).$$

Let ACF(p) be ACF plus the following axiom representing the characteristic $p \geq 2$.

$$\overbrace{1 + 1 + \cdots + 1}^{n-\text{times}} \neq 0 \quad (0 < n < p) \quad \text{and} \quad \overbrace{1 + 1 + \cdots + 1}^{p-\text{times}} = 0.$$

Note that p must be a prime number.

Let ACF(0) be ACF plus the following axioms representing the characteristic 0.

$$\overbrace{1+1+\cdots+1}^{n-\text{times}} \neq 0 \quad (n \geq 2).$$

- A typical model of ACF(0) is the field of complex numbers $\mathfrak{C} = (\mathbb{C}, +, -, \bullet, /, 0, 1)$.
- As shown in a lemma below, any model of ACF(0) is elementarily equivalent to the field of complex numbers $\mathfrak{C}$. So, to show a first-order property of the complex number field $\mathfrak{C}$, we may instead observe any other model of ACF$_0$, e.g., the algebraic closure $\overline{\mathfrak{Q}}$ of the rational number field $\mathfrak{Q}$.
- A typical model of ACF$_p$ is the algebraic closure Ω of the factor ring (field) $\mathfrak{F}_p = \mathfrak{Z}/p\mathfrak{Z}$ of the integer ring $\mathfrak{Z}$, that is, $\Omega = \cup_{n\geq 1}\mathfrak{F}_{p^n}$.

Lemma

ACF *does not have a finite model.*

Proof. Suppose there exists a finite model $\mathfrak{A}$ of ACF with $|\mathfrak{A}| = \{a_1, \cdots, a_k\}$. However, $f(x) = (x - a_1)\cdots(x - a_k) + 1$ has no roots in $\{a_1, \cdots, a_k\}$. □

- We know that any field $\mathfrak{A}$ can be embedded in an algebraically closed field. And the algebraic closure $\overline{\mathfrak{A}}$ is the minimum of such extensions (Part 3 Problem 9). Although we do not prove, the algebraic closure is unique up to isomorphism.
- Therefore, ACF is also a 1-model complete theory that satisfies the isomorphism condition, and hence it admits elimination of quantifiers.

As in the following proof, it is not difficult to eliminate quantifiers as direct transformation.

Theorem

ACF *admits elimination of quantifiers.*

Proof idea.

- Let $f(x, \vec{y})$ and $g(x, \vec{y})$ be polynomials. Consider the quantifier elimination of the following formula:

$$\exists x(f(x, \vec{y}) = 0 \wedge g(x, \vec{y}) \neq 0).$$

which is the negation of the following formula:

$$\forall x(f(x, \vec{y}) = 0 \rightarrow g(x, \vec{y}) = 0).$$

- The above formula can be rephrased as "$f(x, \vec{y})$ divides $g^n(x, \vec{y})$" for a large enough n.
- Then, divisibility of polynomials can be expressed as an open formula in coefficients.
- As a more general case, we consider

$$\exists x(f_1(x, \vec{y}) = 0 \wedge f_2(x, \vec{y}) = 0 \wedge g_1(x, \vec{y}) \neq 0 \wedge g_2(x, \vec{y}) \neq 0).$$

  Here, $g_1(x, \vec{y}) \neq 0 \wedge g_2(x, \vec{y}) \neq 0$ can be converted into one expression as follows

$$g_1(x, \vec{y}) \cdot g_2(x, \vec{y}) \neq 0$$

- To treat $f_1(x, \vec{y})$ and $f_2(x, \vec{y})$, we basically use the mutual division method to reduce the sum of their degrees. Suppose the degree of $f_1(x, \vec{y})$ is not lower than that of $f_2(x, \vec{y})$. Then, we let $f_1'(x, \vec{y})$ be the polynomial that is the remainder when $f_1(x, \vec{y})$ is divided by $f_2(x, \vec{y})$. Replacing $f_1(x, \vec{y})$ with it does not change the solution of simultaneous equations. And the sum of the degrees of the two equations decreases. □

From the above theorem, we have

Corollary

ACF *is model-complete and decidable.*

Corollary

ACF(0) *and* ACF(p) *are model-complete, complete, and decidable.*

Now, we show Hilbert's Nullstellensatz.

Theorem (Nullstellensatz)

Let $\mathfrak{K}$ be an algebraically closed field. For any sequence of polynomials with no common root in $\mathfrak{K}$,

$$P_1(X_1, \cdots, X_n), \cdots, P_m(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n],$$

There exist $Q_1(X_1, \cdots, X_n), \cdots, Q_m(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]$ *such that*

$$P_1(X_1, \cdots, X_n)Q_1(X_1, \cdots, X_n) + \cdots + P_m(X_1, \cdots, X_n)Q_m(X_1, \cdots, X_n) = 1.$$

Proof (by way of contradiction)

- Suppose that the conclusion does not hold for $P_1(X_1, \cdots, X_n), \cdots, P_m(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]$. Then we let
$$I = \{P_1(X_1, \cdots, X_n)Q_1(X_1, \cdots, X_n) + \cdots + P_m(X_1, \cdots, X_n)Q_m(X_1, \cdots, X_n) :$$
$$Q_1(X_1, \cdots, X_n), \cdots, Q_m(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]\}$$
That is, I is the ideal generated by $P_1(X_1, \cdots, X_n), \cdots, P_m(X_1, \cdots, X_n)$.
- Since it does not include 1, it is a proper subset of $K[X_1, \cdots, X_n]$.
- Using Zorn's lemma, we expand I to the maximal ideal J.
- We define the equivalence relation $P(X_1, \cdots, X_n) \sim Q(X_1, \cdots, X_n)$ by $P(X_1, \cdots, X_n) - Q(X_1, \cdots, X_n) \in J$.
- Considering the factor algebra $\mathfrak{K}[X_1, \cdots, X_n]/J$, it is easy to see that it is a field. In other words, $\mathfrak{K}[X_1, \cdots, X_n]/J$ can be considered as an field extension of $\mathfrak{K}$.

- On $\mathfrak{K}[X_1, \cdots, X_n]/J$, we have

$$P_1(X_1, \cdots, X_n) = 0, \cdots, P_m(X_1, \cdots, X_n) = 0,$$

and thus

$$\mathfrak{K}[X_1, \cdots, X_n]/J \models \exists x_1 \cdots \exists x_n (P_1(x_1, \cdots, x_n) = 0 \wedge \cdots \wedge P_m(x_1, \cdots, x_n) = 0)$$

- Then, the above equation also holds for the algebraic closure $\mathfrak{L}$ of $\mathfrak{K}[X_1, \cdots, X_n]/J$.
- By model completeness of an algebraically closed field, since $\mathfrak{K}$ is an elementary substructure of $\mathfrak{L}$, we have

$$\mathfrak{K} \models \exists x_1 \cdots \exists x_n (P_1(x_1, \cdots, x_n) = 0 \wedge \cdots \wedge P_m(x_1, \cdots, x_n) = 0)$$

- Therefore, $P_1(X_1, \cdots, X_n), \cdots, P_m(X_1, \cdots, X_n)$ have a common root on $\mathfrak{K}$, which contradicts the assumption.

Thank you for your attention!