Logic and Foundation II

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

Kazuyuki Tanaka

BIMSA

March 28, 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, after the rest of Part 5
- Apr. 1, (2) Real closed ordered fields and the Artin-Schreier theorem
- to be continued

Rest of Part 5

- An $\mathcal{L}$-structure $\mathfrak{A}$ is **recursively saturated**, if any recursive 1-type on $\{\vec{a}\} \subseteq A$ is realized in $\mathfrak{A}$, that is, for any recursive type $\{\varphi_i(x, \vec{x}) \mid i \in \mathbb{N}\}$ and any $\{\vec{a}\} \subseteq A$,

$$\forall j \exists a \in A \forall i < j\, \mathfrak{A}_A \models \varphi_i(a, \vec{a}) \Rightarrow \exists a \in A \forall i\, \mathfrak{A}_A \models \varphi_i(a, \vec{a}).$$

Lemma

A countable structure in a countable language has a countable elementary extension which is recursively saturated.

- An $\mathcal{L}$-structure $\mathfrak{A}$ is **resplendent**, if for a sentence φ in a language $\mathcal{L}^+ \supseteq \mathcal{L}_A$ such that $\mathrm{Th}(\mathfrak{A}_A) \cup \{\varphi\}$ is consistent, there exists an $\mathcal{L}^+$-expansion $\mathfrak{A}^+$ of $\mathfrak{A}$ such that $\mathfrak{A}^+ \models \varphi$.

In other words, resplendent structures are considered to potentially possess the properties of relations and functions manifested in their elementary extensions.

- An $\mathcal{L}$-structure $\mathfrak{A}$ is **strongly resplendent**, if for any recursive type $\Phi(\vec{x})$ in a language $\mathcal{L}^+ = \mathcal{L} \cup \{\text{finitely many additional symbols}\}$ and $\vec{a} \in A^{<\omega}$ such that $\mathrm{Th}(\mathfrak{A}_A) \cup \Phi(\vec{a})$ is consistent, there exists an $\mathcal{L}^+$-expansion $\mathfrak{A}^+$ of $\mathfrak{A}$ which is a model of $\Phi(\vec{a})$.
- In the definition of **strongly resplendent**, if we restrict a type $\Phi(\vec{x})$ to be a single formula, we obtain the definition of **resplendent**, and if we let $\mathcal{L}^+ = \mathcal{L} \cup \{c\}$, it becomes the definition of **recursive saturation**. Hence, strongly resplendent structures are both resplendent and recursively saturated.

Theorem (Barwise-Ressayre)

Countable recursively saturated structures are strongly resplendent.

Corollary (Barwise)

A resplendent structure in a finite language $\mathcal{L}$ is strongly resplendent, and so recursively saturated.

Theorem (Robinson's Joint Consistency Theorem)

Let $\mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2$, and T be a complete theory in the language $\mathcal{L}$, with T_1 and T_2 as extensions of T in the languages $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively. Then, $T_1 \cup T_2$ is consistent if and only if T_1 and T_2 are separately consistent.

Proof. The necessity is clear, so we will prove the sufficiency. Assume T_1 and T_2 are consistent, but $T_1 \cup T_2$ is inconsistent.

- Since $T_1 \cup T_2$ is inconsistent, there exist finite subsets $S_1 \subseteq T_1$ and $S_2 \subseteq T_2$ such that $S_1 \cup S_2$ also leads to a contradiction.
- Suppose S_1 and S_2 are theories in finite languages $\mathcal{L}'_1$ and $\mathcal{L}'_2$, respectively. Define $\mathcal{L}' = \mathcal{L}'_1 \cap \mathcal{L}'_2$, and let T' be the set of $\mathcal{L}'$-sentences that can be deduced from T. Then, T' is a complete and consistent set in the language $\mathcal{L}'$, since T is a complete and consistent set in $\mathcal{L}$
- Moreover, let $S'_1 = S_1 \cup T'$ and $S'_2 = S_2 \cup T'$. Since S'_1 and S'_2 are subsets of T_1 and T_2, respectively, they are separately consistent.

- Consider a countable saturated model $\mathfrak{A}$ of T'. Since T' is complete, $T' = \mathrm{Th}(\mathfrak{A})$.
- Since $S_1' = S_1 \cup \mathrm{Th}(\mathfrak{A})$ is consistent, by resplendency of $\mathfrak{A}$, $\mathfrak{A}$ can be extended to a model $\mathfrak{A}_1$ of S_1 in $\mathcal{L}_1'$.
- Similarly, $\mathfrak{A}$ can be extended to a model $\mathfrak{A}_2$ of S_2 in $\mathcal{L}_2'$. Therefore, by defining the interpretation of symbols in $\mathcal{L}_1' - \mathcal{L}'$ to be the same as in $\mathfrak{A}_1$ and in $\mathcal{L}_2' - \mathcal{L}'$ to be the same as in $\mathfrak{A}_2$, we extend $\mathfrak{A}$ to a structure $\mathfrak{A}'$ in $\mathcal{L}_1' \cup \mathcal{L}_2'$.
- Then, $\mathfrak{A}'$ is a model of $S_1 \cup S_2$, which contradicts our assumption. Thus, we complete the proof.

□

Corollary (Craig's Interpolation Theorem)

If a formula $\varphi \to \psi$ is provable ($\vdash \varphi \to \psi$), then there exists a formula θ consisting of mathematical symbols appearing in φ and ψ commonly, besides logical symbols and $=$, such that $\vdash \varphi \to \theta$ and $\vdash \theta \to \psi$.

The formula θ satisfying the above theorem is called an **interpolant** for φ and ψ.

Proof

- Assume $\vdash \varphi \to \psi$ with no interpolant θ. Let $\mathcal{L}$ be the language consisting of symbols common to φ and ψ. Let T_0 be the set of formulas ξ in $\mathcal{L}$ such that $\vdash \varphi \to \xi$.
- Then, $T_0 \cup \{\neg\psi\}$ is consistent, since no finite subset of T_0 implies ψ.
- Consider a model $\mathfrak{A}$ of $T_0 \cup \{\neg\psi\}$, and let T be the set of all $\mathcal{L}$-formulas contained in $\mathrm{Th}(\mathfrak{A})$. Clearly, $T \cup \{\neg\psi\}$ is consistent.
- To show that $T \cup \{\varphi\}$ is also consistent, assume otherwise. Then there exists a formula σ in T such that $\vdash \varphi \to \neg\sigma$. Thus, $\neg\sigma \in T_0 \subseteq T$, which implies the inconsistency of T.
- By Robinson's joint consistency theorem, $T \cup \{\varphi, \neg\psi\}$ is also consistent, contradicting the assumption $\vdash \varphi \to \psi$. □

Introduction to the theory of real numbers

- After Gödel showed that the theory of natural numbers was inevitably incomplete, Tarski discovered a contrasting fact: the theory of real numbers and that of complex numbers are completely axiomatized. The key tool to show these facts is the technique of **quantifier elimination**.
- Various improvements were made later, but it is still not easy to demonstrate quantifier elimination by direct transformation of formulas for the theory of real numbers, although it is much easier for the theory of complex numbers.
- In this lecture, we use the results of the real closed field theory initiated by Artin and Schreier to indirectly (model-theoretically) derive the fact that quantifiers are eliminable.

One-variable polynomial with real coefficients

- As a warm-up for real number theory, we will look at the basic properties of one-variable polynomials with real coefficients .
- The following theorems look like popular theorems in calculus, but their proofs do not rely on analytical concepts such as limits. These theorems also serve as theorems of real closed ordered fields, as introduced in the subsequent lectures.
- For simplicity, We assume the "Fundamental Theorem of Algebra" without proof, which asserts that any complex polynomial $P(x)$ can be expressed as a product of linear factors.
- However, the dependence on this theorem can be eliminated in the following discussions. A rigorous proof of this theorem will be provided in Part 8.

Lemma

A real polynomial $P(x)$ with leading coefficient 1 (i.e., monic) can be expressed as the product of a linear polynomial $x + a$ and a quadratic polynomial $x^2 + bx + c$ with real coefficients, where $b^2 < 4c$.

Proof.

Assuming the Fundamental Theorem of Algebra, any real polynomial $P(x)$ can be expressed as a product of linear expressions using complex numbers.
For any complex number z and its conjugate complex number $\overline{z}$, we have

$$P(\overline{z}) = \overline{P(z)}$$

So, if a complex number z is a root of $P(x)$, then $\overline{z}$ is also a root. Thus, $P(x)$ has the quadratic equation as a factor:

$$(x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z}.$$

Here, letting $z = r + i\,s$ $(i = \sqrt{-1}, r, s \in \mathbb{R})$, we see the following are real numbers:

$$-b = z + \overline{z} = 2r, \;\; c = z\overline{z} = r^2 + s^2.$$

Finally, we have $b^2 < 4c$ since

$$(z + \overline{z})^2 - 4z\overline{z} = (z - \overline{z})^2 = (2is)^2 = -4s^2 < 0.$$

□

Theorem (Intermediate value theorem)

Let $P(x)$ be a polynomial with real coefficients, $a < b$ be two real numbers such that $P(a) \cdot P(b) < 0$. Then there exists c in the interval (a, b) such that $P(c) = 0$.

Proof.

- Without loss of generality, we assume that a given polynomial $P(x)$ is monic.
- From the above lemma, $P(x)$ can be expressed as a product of linear equations $x + r$ and quadratic equations $x^2 + sx + t$ (where $s^2 < 4t$).
- A quadratic factor $x^2 + sx + t$ is always positive as follows

$$x^2 + sx + t = \left(x + \frac{s}{2}\right)^2 + \frac{4t - s^2}{4} > 0.$$

- Therefore, if $P(a)P(b) < 0$, then there is a linear factor $x + r$ such that the signs of $a + r$ and $b + r$ are different.
- Since $a < b$, it should be the case that $a < -r < b$. Thus, by setting $c = -r$, we obtain $P(c) = 0$.

□

Theorem

If the polynomial $P(a) > 0$, then there exists $\epsilon > 0$ such that $P(x) > 0$ on the interval $(a-\epsilon, a+\epsilon)$.

Proof.

- Similar to the theorem above, assume that $P(x)$ is monic. And decompose it into a product of linear and quadratic equations.
- Let $x - r_1, \cdots, x - r_m$ be the linear factors.
- Take a positive number $\epsilon > 0$ which is smaller than the minimum value of $|a - r_1|, \cdots, |a - r_m|$.
- Since the sign of $x - r_i$ $(i = 1, \ldots, m)$ does not change in the interval $(a-\epsilon, a+\epsilon)$, we have $P(x) > 0$. □

Theorem (Role's theorem)

Let $P(x)$ be a polynomial with real coefficients, and $P'(x)$ be its derivative, which is also a polynomial. If $a < b$ and $P(a) = P(b)$, then there exists c in the interval (a, b) such that $P'(c) = 0$.

Proof.

- For simplicity, we assume that $P(a) = P(b) = 0$. Moreover, we may assume that there is no solution for $P(x) = 0$ on (a, b). In other words, a and b are adjacent solutions.
- Since $P(x)$ is divisible by $x - a$ and $x - b$, there exists a polynomial $Q(x)$ such that

  $$P(x) = (x-a)^m (x-b)^n Q(x),$$

  where $m \geq 1, n \geq 1$ and $Q(a) \neq 0, Q(b) \neq 0$. Since $Q(x) \neq 0$ on (a, b), we have $Q(a) \cdot Q(b) > 0$ by the contraposition of the intermediate value theorem.
- Now suppose $P'(x) = (x-a)^{m-1}(x-b)^{n-1}R(x)$. Then,

  $$R(x) = (m(x-b) + n(x-a))Q(x) + (x-a)(x-b)Q'(x).$$

- We easily compute $R(a) \cdot R(b) = -mn(a-b)^2 Q(a)Q(b) < 0$. Hence, by the intermediate value theorem, there exists c in (a, b) such that $R(c) = 0$. Therefore, we have $P'(c) = 0$, which completes the proof. □

Theorem

Let $P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ be a monic polynomial with real coefficients. Let M be the maximum value of $|a_{n-1}|, |a_{n-2}|, \cdots, |a_1|, |a_0|$. Then, all real solutions of $P(x) = 0$ are in the interval $(-M-1, M+1)$.

Proof.

- If $|x| \geq M + 1$, then we have

$$|P(x) - x^n| \leq M(|x|^{n-1} + |x|^{n-2} + \cdots + |x| + 1) = M\frac{|x|^n - 1}{|x| - 1} \leq |x|^n - 1.$$

- When $P(x) = 0$, the above inequality $(|x|^n \leq |x|^n - 1)$ does not hold. Therefore, $P(x) = 0$ has no solution at $|x| \geq M + 1$. □

The main result we are going to prove in this part is Tarski's theorem on the real field. This theorem is a generalization of a classical theorem due to Sturm. To state Sturm's theorem, we introduce some special terms. Let $P(x)$ be a real polynomial.

- Let $P_0 = P$, $P_1 = P'$, and define $P_2, P_3, \cdots$ as follows: $-P_{i+2}$ is the remainder of dividing P_i by P_{i+1}, that is, $P_i = Q_{i+1}P_{i+1} - P_{i+2}$.
- Then, for each $a \in \mathbb{R}$,

$$P_0(a), P_1(a), P_2(a), \cdots$$

is called a **Sturm sequence**. The number of times the sign (+, –) changes in the sequence is expressed as $\omega_P(a)$, e.g, for a Sturm sequence (1,0,2,–1,0,1), $\omega_P(a) = 2$.

Theorem (Sturm's theorem)

Let $P(x)$ be a polynomial with real coefficients, and let $a < b$ and $P(a)P(b) \neq 0$. Then, $\omega_P(a) - \omega_P(b)$ is the number of (different) roots that $P(x)$ has in the interval (a, b).

- The proofs can be found in Lang's *Algebra* and Jacobson's *Basic Algebra I and II*.
- While Sturm's theorem expresses only the number of roots of a polynomial within an interval (a, b) in terms of equations, Tarski's theorem asserts that any property expressed in the first order language can be represented by a combination of equations and inequalities.

Real closed ordered field

Definition

The theory AF of **fields** consists of the following axioms in the language $\mathcal{L}_{\mathrm{AF}} = \{+, -, \bullet, /, 0, 1\}$: (note $x/0 = 0$ for convenience)

$$x + 0 = x, \quad x + y = y + x, \quad x + (y + z) = (x + y) + z, \quad x + (-x) = 0,$$
$$x \bullet 0 = 0, \quad x \bullet 1 = x, \quad x \bullet y = y \bullet x, \quad x \bullet (y \bullet z) = (x \bullet y) \bullet z,$$
$$x/0 = 0, \quad x \neq 0 \to x \bullet (y/x) = y, \quad 1 \neq 0, \quad x \bullet (y + z) = (x \bullet y) + (x \bullet z).$$

The theory OF of **ordered fields** is AF added with the following axioms in the language $\mathcal{L}_{\mathrm{OF}} = \{+, -, \bullet, /, 0, 1, <\}$: $\;<$ is a linear order and $0 < 1$,

$$(x > 0 \wedge y > 0) \to (x + y > 0 \wedge xy > 0).$$

The theory RCOF of **real-closed ordered fields** is OF added with the following axioms:

$$\forall x_0 \forall x_1 \cdots \forall x_n \forall y \forall z ((y < z \wedge x_0 + x_1 y + \cdots + x_n y^n < 0 < x_0 + x_1 z + \cdots + x_n z^n) \\ \to \exists u (y < u < z \wedge x_0 + x_1 u + \cdots + x_n u^n = 0)) \quad (n > 0).$$

- In the above definition, we define “real closed property” in the form of the Intermediate Value Theorem. However, there is an alternative definition that demands the existence of square roots and roots of odd-degree polynomials as axioms. The latter is necessary for the theory RCF of (unordered) **real-closed fields**.
- However, in this course, we will not introduce the theory RCF; instead, we treat a real closed field as a reduct of a real closed ordered field.

Example 1

- The ordered field of real numbers $\mathfrak{R} = (\mathbb{R}, +, -, \bullet, /, 0, 1, <)$ is the standard model of RCOF.
- $\mathfrak{R}$ restricted to the algebraic real numbers (real numbers that are solutions of integer coefficient polynomials) is also a real closed ordered field, but it is countable.
- Any real closed ordered field contains a substructure that is isomorphic to the ordered field of algebraic reals.

- All the lemmas and theorems proved for $\mathfrak{R}$ in this lecture also hold for any real closed ordered field. The only problem is to prove the fundamental theorem of algebra in RCOF. But without using it, we can derive the other theorems.
- First, the intermediate value theorem is an axiom of RCOF, so there is no need to prove it. We also give another proof of the following theorem.

Theorem

In any ordered field, if a polynomial $P(a) > 0$, then there exists some $\epsilon > 0$ such that $P(x) > 0$ in the interval $(a - \epsilon, a + \epsilon)$.

Proof.

- It is clear when $P(x)$ is a constant. So we may assume its degree $N > 0$.
- $P(x + a) - P(a)$ is a polynomial that does not contain a constant term. Let M be the maximum of absolute values of its coefficients Then, for $|x| \leq 1$, we have $|P(x + a) - P(a)| \leq NM|x|$
- So, setting $\epsilon = \min\{1, |P(a)|/NM\}$, then we have $|P(x + a) - P(a)| < |P(a)|$.
- Since $P(a) > 0$, this inequality does not hold unless $P(x + a) > 0$. □

The Artin-Schreier theorem

- In the previous semester (Problem 9 in part 3), we show that all fields can be embedded in an algebraically closed field and that they also have an algebraic closure.
- Similarly, every ordered field can be embedded in a real closed ordered field, and it has a real closure.
- However, it is difficult to directly create a real closed field. Here, we will construct a real closed field with an algebraically closed field.

Theorem (Artin-Schreier)

All ordered fields can be embedded in a real closed ordered field.

Thank you for your attention!