An Introduction to Mathematical Logic

Jesse Maltese

June 16th, 2021

Outline

What is Mathematical Logic?

Languages, Structures, Truth

- Languages
- Structures
- Truth
- $\vdash$ and $\models$

Soundness, Consistency, and Completeness

- The Completeness Theorem
- The Compactness Theorem

Fun Problems!

- Finite Four Colour implies Infinite Four Colour
- The Ax-Grothendieck Theorem

Logic Is...

"... the study of formal languages, and connections between those languages, and their structures (interpretations)"
Thomas Scanlon

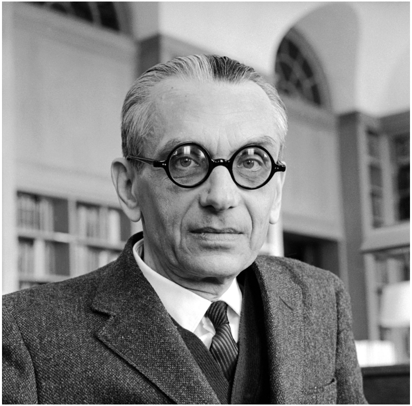
"... the study of reasoning; and mathematical logic is the study of the type of reasoning done by mathematicians"
Joseph Schoenfield

The main fields of mathematical logic are: Set theory, Proof theory, Model theory, and Recursion or Computability theory.

Early Names in Logic: Hilbert

Hilbert, by way of his program, contributed heavily to the development of the formalist school of the philosophy of mathematics.

Early Names in Logic: Gödel



The Completeness Theorem, The Incompleteness Theorems, The Compactness Theorem

Languages

Definition

A **first-order language**, $\mathcal{L}$ is specified by,

- A set of predicate symbols of various -arities, $Pred_{\mathcal{L}}$
- A set of function symbols of various -arities, $Func_{\mathcal{L}}$
- A set of constant symbols, $Const_{\mathcal{L}}$
- Whether or not we include $=$

Note that $Pred_{\mathcal{L}}, Func_{\mathcal{L}}, Const_{\mathcal{L}}$ symbols are not necessarily non-empty.

Language Example

Example. Denote the language of arithmetic as $\mathcal{L}_A$ with equality as:

- The constant symbol o,
- A unary function symbol, s,
- Two binary function symbols, $+$, $\times$,
- One binary relation/predicate symbol, $\leq$

Interpretation Functions

Definition

A **universe**, $\mathcal{U}$, is a non-empty set.

Definition

Given a universe $\mathcal{U}$, an **interpretation function** $\mathcal{I}$ for a language $\mathcal{L}$ is a function such that,

- For any n-ary $P \in Pred_{\mathcal{L}}$, $\mathcal{I}(P) = S \subset \mathcal{U}^n$
- For any n-place $f \in Func_{\mathcal{L}}$, $\mathcal{I}(f) = F$, where $F : \mathcal{U}^n \to \mathcal{U}$ is an n-ary function on $\mathcal{U}$.
- For any $c \in Const_{\mathcal{L}}$, $\mathcal{I}(c) = x$, for some $x \in \mathcal{U}$.

Structure

Definition

A **structure** for a language $\mathcal{L}$, is a pair $\mathcal{M} = \langle \mathcal{U}, \mathcal{I} \rangle$ where $\mathcal{U}$ denotes the universe, and $\mathcal{I}$ denotes an interpretation function for $\mathcal{L}$.

A Simple Example

Example. Let $\mathcal{L} = \{\leq\}$ be a language with just one binary symbol. Then a structure for $\mathcal{L}$ could be:

- $\mathcal{M} = \langle \mathbb{Q}, \mathcal{I} \rangle$ where $\mathcal{I}(\leq)$ is the standard order on $\mathbb{Q}$

A Simple Example

Example. Let $\mathcal{L} = \{\leq\}$ be a language with just one binary symbol. Then a structure for $\mathcal{L}$ could be:

- $\mathcal{M} = \langle \mathbb{Q}, \mathcal{I} \rangle$ where $\mathcal{I}(\leq)$ is the standard order on $\mathbb{Q}$
- $\mathcal{N} = \langle \mathbb{Q}, \mathcal{I} \rangle$ where $\mathcal{I}(\leq)$ is the standard ordering on the numbers, $\bmod 3$. (Thus $4 \leq 2$ since $4 \bmod 3 = 1$, $2 \bmod 3 = 2$).

A Simple Example

Example. Let $\mathcal{L} = \{\leq\}$ be a language with just one binary symbol. Then a structure for $\mathcal{L}$ could be:

- $\mathcal{M} = \langle \mathbb{Q}, \mathcal{I} \rangle$ where $\mathcal{I}(\leq)$ is the standard order on $\mathbb{Q}$
- $\mathcal{N} = \langle \mathbb{Q}, \mathcal{I} \rangle$ where $\mathcal{I}(\leq)$ is the standard ordering on $\mathbb{Q}$, $\bmod 3$.
- $\mathcal{O} = \langle \mathbb{Q}, \mathcal{I} \rangle$ where $\mathcal{I}(\leq)$ is the lexographic ordering on $\mathbb{Q}$ indexed by the first element.
  That is, the fraction representations of elements of $\mathbb{Q}$ are represented as (a, b) such that $(a, b) \leq (c, d) \Leftrightarrow b \leq d$.
  Then $\frac{3}{2} \leq \frac{1}{3}$ since $(3, 2) \leq (1, 3)$ on the first element.

A Structure for Arithmetic

Example. Let $\mathcal{L}_A$ denote the language of arithmetic as in the previous example. Then let $\mathcal{M} = \langle \mathcal{U}, \mathcal{I} \rangle$. Then we have,

- $\mathcal{U} = \mathbb{N}$,
- $\mathcal{I}(\mathsf{o}) = 0$,
- $\mathcal{I}(\leq) = \{(m, n) \mid m, n \in \mathbb{N}, m \leq n\}$
- $\mathcal{I}(\mathsf{s})(n) = n + 1,\ n \in \mathbb{N}$
- $\mathcal{I}(+)(m, n) = m + n,\ n \in \mathbb{N}$
- $\mathcal{I}(\times)(m, n) = m \times n,\ m, n \in \mathbb{N}$

We'll call $\mathcal{M}$ the **standard model for arithmetic**. Since these are the standard interpretations of these symbols, we can write: $\mathcal{M} = \langle \mathbb{N}, 0, S, +, \times, < \rangle$.

Why Truth?

How do we determine truth in zero-order logic?
How do we determine truth in first-order logic?
Consider $\forall x \forall y (P(x, y) \rightarrow \exists z (P(x, z) \wedge P(z, y)))$.

A Translation.

Example. $\varphi := \exists x \forall y (x \leq y)$. Then, with $\mathcal{M}$ as the standard model for arithmetic, we have,

φ is true relative to $\mathcal{M}$

iff

there exists $x \in \mathbb{N}$ such that for every $y \in \mathbb{N}$, $x \leq y$.

A Theory of Truth

Definition

Let $\mathcal{M} = \langle \mathcal{U}, \mathcal{I} \rangle$. We define the relation $\mathcal{M} \vDash \varphi$ to mean that $\mathcal{M}$ **satifies** φ if and only if the translation of φ as determined by $\mathcal{M}$ is true.

$\models$

Definition

Let Γ denote some set of sentences, and φ some sentence. We write $\Gamma \models \varphi$ if and only if for any structure $\mathcal{M}$ if $\forall \gamma \in \Gamma$, $\mathcal{M} \models \gamma$, then $\mathcal{M} \models \varphi$. We say that φ is a **logical consequence** or is **semantically implied** by Γ.

$\vdash$

Definition

A sentence φ is **provable** from a set of sentences Γ if there is some finite sequence $\langle \gamma_1, \gamma_2, \ldots, \gamma_n \rangle$ of sentences such that $\gamma_n = \varphi$ and any other γ_i is the result of an application of a valid rule of deduction

In other words - $\Gamma \vdash \varphi$ if and only if there exists a proof of φ from Γ.

"Has a Model"

Definition

For some set of sentences Γ, and structure $\mathcal{M}$, if for every sentence $\gamma \in \Gamma$, $\mathcal{M} \models \gamma$, then we say that $\mathcal{M}$ is a model of Γ, or that Γ "has a model".

Consistency of a theory

Definition

A set of sentences Γ is **consistent** if and only if there is no sentence φ such that $\mathcal{M} \vdash \varphi$ and $\mathcal{M} \vdash \neg\varphi$.

Soundness!

"If you can prove it, then it's true"

Theorem (The Soundness Theorem)

For any set of sentences Γ, *and any sentence* φ, *if* $\Gamma \vdash \varphi$ *then* $\Gamma \vDash \varphi$.

Theorem (The Soundness Theorem 2)

Given some set of sentences Γ, *if* Γ *has a model, then* Γ *is consistent.*

The Completeness Theorem

Theorem (Gödel's Completeness Theorem, 1930)

If a theory Γ *is consistent, then* Γ *has a model.*

The Compactness Theorem

Recall: A theory "has a model" if there is some model $\mathcal{M}$ such that for any $\gamma \in \Gamma$, $\mathcal{M} \vDash \gamma$.

Theorem (The Compactness Theorem)

A set of sentences Γ *has a model if and only if every finite subset of* Γ *has a model.*

A Proof of the Compactness Theorem

Proof.

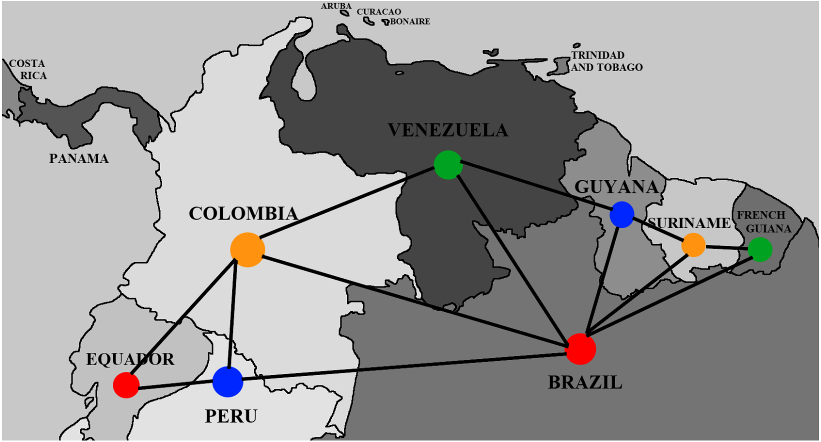
- ($\Leftarrow$). Suppose for contradiction that every finite subset of Γ, say Γ_0 has a model, but Γ does not.
- Then, by the contrapositive of the Completeness Theorem, we have that Γ is inconsistent.
- So, there exists some sentence φ such that $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$.
- Thus there are some finite sets of sentences $\Gamma', \Gamma'' \subseteq \Gamma$ such that $\Gamma' \vdash \varphi$ and $\Gamma'' \vdash \neg\varphi$.
- Then, clearly, $\Gamma' \cup \Gamma'' \vdash \varphi$, and $\Gamma' \cup \Gamma'' \vdash \neg\varphi$.
- But note that the union of two finite sets is still finite, and so $\Gamma' \cup \Gamma''$ is a finite set that proves a contradiction.
- So by the contrapositive of the soundness theorem, $\Gamma' \cup \Gamma''$ is a finite subset of Γ that does not have a model. Contradiction.

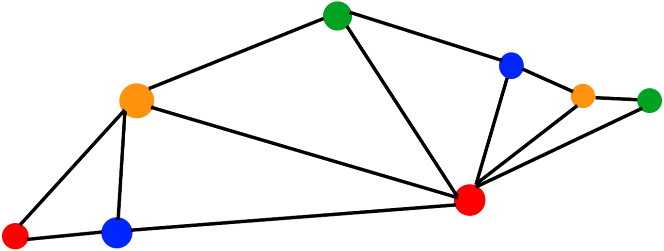
$\square$

Problem Statement

Theorem (Finite Four Colour Theorem, 1976)

Any map of a finite number of countries can be coloured by four colours such that no two adjacent countries have the same colour.


ARUBA
CURACAO
BONAIRE
COSTA RICA
TRINIDAD AND TOBAGO
PANAMA
VENEZUELA
GUYANA
COLOMBIA
SURINAME
FRENCH GUIANA
EQUADOR
BRAZIL
PERU



The Proof

Theorem (Infinite Four Colour Theorem)

Any infinite map of a finite number of countries can be coloured by four colours such that no two adjacent countries have the same colour.

Proof.

Suppose the finite four colour theorem holds. Then, define the set of sentence letters: $\{C_n^i \mid n \in \mathbb{N}, 1 \leq i \leq 4\}$ such that C_n^i denotes the nth country coloured with the ith colour.
So then, let Σ be the set of sentences:

1. $C_n^1 \vee C_n^2 \vee C_n^3 \vee C_n^4$, for any $n \in \mathbb{N}$.
2. $\neg(C_n^i \wedge C_n^j)$, $1 \leq i < j \leq 4$, for any $n \in \mathbb{N}$.
3. $\neg(C_n^i \wedge C_m^i)$, where n, m are adjacent countries.

Clearly, then, any finite subset of Σ is satisfiable by the finite four colour theorem. So, by the Compactness theorem, Σ is satisfiable. □

A similar problem

Suppose that you can tile finite subsets of $\mathbb{R}^2$ (the plane) with some set of polyominoes. Can you tile the entire plane with the same set? More precisely,

Theorem

Divide $\mathbb{R}^2$ into disjoint unit squares. Let T be a tiles. If for every finite $S \subset \mathbb{R}^2$, there exists a tiling with T-tiles such that S is a subset of the tiling, then there is a tiling of R^2 with T-tiles.

Proof.

Exercise! *Hint: It uses compactness.* □

The Ax-Grothendieck Theorem

Theorem (Ax-Grothendieck)

Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.

Algebraic Preliminaries

Definition

A field F is **algebraically closed** if and only if every non-constant polynomial with coefficients from F has a root in F.

Definition

The characteristic of a field F, denoted $char(F)$, is the smallest n such that

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ times}} = 0$$

where 1 is the multiplicative identity, and 0 is the additive identity of the field. We'll denote this sentence by $1 \cdot n = 0$. If no such n exists, we say the field has characteristic 0.

Algebraic Preliminaries

Definition

The **language of fields** $\mathcal{L}_F := \{+, \cdot, 0, 1\}$. Then the theory/axioms of algebraically closed fields (of characteristic p) are denoted ACF_p, consisting of the field axioms, an axiom for algebraic closure, and an axiom that says the field has $\mathrm{char}\ p$.

If a field has characteristic p, then the axiom is that $1 \cdot p = 0$. But if a field has characteristic 0, then for each prime p, there is an axiom denoting that the field *isn't of characteristic p*. More specifically, for any prime p, $1 \cdot p \neq 0 \in \mathrm{ACF}_p$.

Important Theorem!

Definition

A theory T is **complete** if and only if for any sentence φ, either $T \vdash \varphi$ or $T \vdash \neg\varphi$.

Theorem

ACF_p *is complete for any prime* p*, or* $p = 0$*.*

So, ACF_p being complete means that φ, $\mathrm{ACF}_p \vDash \varphi$ or $\mathrm{ACF}_p \vdash \neg\varphi$.

Another important theorem

Theorem (Lefschetz Principle)

Given a sentence φ *in the language of fields, any sentence that is true in* ACF_0 *(specifically* $\mathbb{C}$ *in our case) if and only if* φ *is true in* ACF_p *for arbitrarily high prime* p*.*

A Proof of Lefschetz Principle

We present a proof that if for arbitrarily large prime p, $\mathrm{ACF}_p \vDash \varphi$ then $\mathrm{ACF}_0 \vDash \varphi$. The converse is similar.

Proof.

- Define $T = \mathrm{ACF}_0 \cup \varphi$. Then, let T_0 be a finite subset of T.
- Then T_0 contains finitely many sentences of the form "$p \cdot 1 \neq 0$" for primes p. Each sentence says that "This field is not characteristic p".
- So for large enough p, there is no such sentence in T_0. So choose such a p.
- Then by assumption, there is some model K such that $K \vDash \mathrm{ACF}_p \cup \varphi$. So then $K \vDash T_0$.
- Then, by compactness, there is some model K' such that $K' \vDash T$.
- So $K' \vDash \mathrm{ACF}_0$ and $K' \vDash \varphi$. Thus, $\mathrm{ACF}_0 \nvDash \neg\varphi$ and so by completeness of ACF_0, $\mathrm{ACF}_0 \vDash \varphi$

The Ax-Grothendieck Theorem

Theorem (Ax-Grothendieck)

Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.

Lemma

Let $\bar{\mathbb{F}}_p$ denote the algebraic closure of a p-element field. Then, any injective polynomial mapping $(\bar{\mathbb{F}}_p)^n \to (\bar{\mathbb{F}}_p)^n$ is surjective.

Proof of Ax-Grothendieck

Theorem (Ax-Grothendieck)

Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.

Proof.

- First, let $\Phi_{n,d}$ be the sentence such that for any field K: $K \vDash \Phi_{n,d}$ if and only if every injective polynomial of degree d from $K^n \to K^n$ is surjective
- Then, we have that for any n, d, $\bar{\mathbb{F}}_p \vDash \Phi_{n,d}$ for some prime p by the lemma on the previous slide.
- So by the Lefschetz principle, since it is the case that $\bar{\mathbb{F}}_p \vDash \Phi_{n,d}$ and $\bar{\mathbb{F}}_p$ is an ACF_p theory, we must have that any $\mathrm{ACF}_0 \vDash \Phi_{n,d}$
- So specifically $\mathbb{C} \vDash \Phi_{n,d}$. So every injective polynomial on $\mathbb{C}^n \to \mathbb{C}^n$ is surjective.

□

End of talk.

Here are some references for further learning:

1. MATC09, PHLC51, PHLD51, PHL354
2. Enderton, *An Introduction to Mathematical Logic*
3. Marker, *Model Theory: An Introduction*
4. Hodges, *A Shorter Model Theory*
5. Chang & Keisler, *Model Theory*
6. Marker, *Model Theory of Fields*
7. Victor Zhang's 2015 UChicago REU paper
8. Ben Call's 2015 UChicago REU paper