Logic and Foundation I

Part 1. Equational system

Kazuyuki Tanaka

BIMSA

October 15, 2023

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

Logic and Foundations I

- **Part 1. Equational theory**
- **Part 2. First order theory**
- **Part 3. Model theory**
- **Part 4. First order arithmetic and incompleteness theorems**

Part 1. Schedule

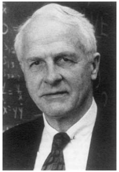
- Sep. 21, (1) Formal systems of equation
- Sep. 28, (2) Free algebras and Birkhoff's theorem
- Oct. 12, (3) Boolean algebras
- Oct. 19, (4) Computable functions and general recursive functions

Recap: Birkhoff's theorems

- For an equational theory T, the following holds.

Birkhoff's completeness theorem (1935)

$$T \models s = t \Leftrightarrow T \vdash s = t.$$



Garrett Birkhoff

- $T \models s = t \Leftarrow T \vdash s = t$ (the soundness of T) is easy. Let $\mathfrak{M}$ be any model of T. Then we can show by induction that all equations appearing in a proof tree for $T \vdash s = t$ holds in $\mathfrak{M}$. Especially the bottom $s = t$ holds in $\mathfrak{M}$.
- To show the contrapositive, we first assume $T \nvdash s = t$, and construct a structure $\mathfrak{M}$ such that $\mathfrak{M} \models T$ and $\mathfrak{M} \not\models s = t$. Such a structure is obtained as the "free algebra" generated by the variables appearing in s, t.

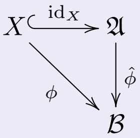
Variety theorem

A class $\mathcal{K}$ of structures is characterized by an equational theory $\Leftrightarrow$ $\mathcal{K}$ is closed under
- subalgebras,
- homomorphisms,
- Cartesian products.

Definition

Let $\mathcal{K}$ be a class of $\mathcal{L}$-algebras. $\mathfrak{A} \in \mathcal{K}$ is a **free $\mathcal{K}$-algebra** generated by $X \subseteq |\mathfrak{A}|$ if

1. $\mathfrak{A}$ is generated by X, that is, it has no proper subalgebra containing X.
2. Every map $\phi : X \to |\mathfrak{B}|$ with $\mathfrak{B} \in \mathcal{K}$ can be uniquely extended to the homomorphism $\hat{\phi} : \mathfrak{A} \to \mathfrak{B}$.



An $\mathcal{L}$-algebra $\mathcal{T}(X) = (\mathrm{Term}(X), \mathtt{f}_0^{\mathcal{T}(X)}, \mathtt{f}_1^{\mathcal{T}(X)}, \dots)$ is a **term algebra**, if $\mathrm{Term}(X)$ is the set of $\mathcal{L}$-terms with variables in X and for each function symbol $\mathtt{f}$ in $\mathcal{L}$,

$$\mathtt{f}^{\mathcal{T}(X)}(t_0, \dots, t_{n-1}) = \mathtt{f}(t_0, \dots, t_{n-1}).$$

Lemma

If a class of $\mathcal{L}$-algebra $\mathcal{K}$ contains $\mathcal{T}(X)$, then $\mathcal{T}(X)$ is a free $\mathcal{K}$-algebra generated by X.

Definition

$\mathfrak{A} \models \mathbf{s} = \mathbf{t}$ if for every homomorphism $\phi : \mathcal{T}(X) \to \mathfrak{A}$, we have $\phi(s) = \phi(t)$.

A homomorphism $\phi : \mathcal{T}(X) \to \mathfrak{A}$ can be viewed as an evaluation function of terms. The value of a term s is uniquely obtained from the values $\phi(x)$ for variables x in s.

Lemma

Let E be a set of equations on $\mathrm{Term}(X)$, and let $\equiv_E$ be a relation on $\mathrm{Term}(X)$ defined by $s \equiv_E t \Leftrightarrow E \vdash s = t$. Then, the following hold:
(1) $\equiv_E$ is a congruence relation.
(2) For any homom. $\phi : \mathcal{T}(X) \to \mathcal{T}(X)$, $\quad s \equiv_E t \Rightarrow \phi(s) \equiv_E \phi(t)$.
(3) For any homom. $\phi : \mathcal{T}(X) \to \mathcal{T}(X)/{\equiv_E}$, there exists a hom. $\psi : \mathcal{T}(X) \to \mathcal{T}(X)$ s.t.

$$\phi = \pi_{\equiv_E} \circ \psi.$$

Lemma

$\mathcal{T}(X)/{\equiv_E}$ is the free $\mathrm{Mod}(E)$-algebra generated by $\pi_{\equiv_E}(X)$.

Note. This lemma also holds for any invariant congruence $\equiv$.

Proof.

Claim 1. $\mathcal{T}(X)/{\equiv_E} \in \mathrm{Mod}(E)$

- It suffices to show that for any equation $s = t$ in E and any homomorphism $\phi : \mathcal{T}(X) \to \mathcal{T}(X)/{\equiv_E}$, we have $\phi(s) = \phi(t)$.

Claim 2. $\mathcal{T}(X)/{\equiv_E}$ is a free algebra.

- For any $\mathfrak{A} \models E$ and $\phi : X/{\equiv_E} \to |\mathfrak{A}|$, by the corollary to the homomorphism theorem, there exists $\hat{\phi} : \mathcal{T}(X)/{\equiv_E} \to \mathfrak{A}$ s.t. $\hat{\psi} = \hat{\phi} \circ \pi_{\equiv_E}$, which is a unique homomorphism extending ϕ □

Proof of the completeness theorem: Let $E \models s = t$. Since $\mathcal{T}(X)/{\equiv_E} \in \mathrm{Mod}(E)$, we have $\mathcal{T}(X)/{\equiv_E} \models s = t$. Then for any homomorphism $\phi : \mathcal{T}(X) \to \mathcal{T}(X)/{\equiv_E}$, we have $\phi(s) = \phi(t)$. In particular, letting $\phi = \pi_{\equiv_E}$, we have $s \equiv_E t$. Hence, $E \vdash s = t$.

Birkhoff's variety theorem

Definition

If a set $\mathcal{K}$ of $\mathcal{L}$-algebras is said to be an **equational class** (or **variety**) if it is characterized by a set E of equations, that is

$$\mathcal{K} = \mathrm{Mod}(E).$$

Theorem (Birkhoff's variety theorem)

$\mathcal{K}$ is an equational class $\Leftrightarrow$ $\mathcal{K}$ is closed under subalgebras, homomorphisms, and Cartesian products.

Proof.

To show $\Rightarrow$

- It is clear since an equation that holds in some algebraic structure also holds in its subalgebras and homomorphic images.
- The equality that holds for each $\mathfrak{A}_i$ also holds for the Cartesian product $\prod \mathfrak{A}_i$.

To show $\Leftarrow$

- Let $\mathcal{K}$ be closed under subalgebras, homomorphisms, and Cartesian products.
- Let X be an infinite set of variables. We define the following set of equations in $\mathrm{Term}(X)$ as follows:

$$E = \{s = t : \text{for any } \mathfrak{A} \in \mathcal{K}, \mathfrak{A} \models s = t\}.$$

- Our aim is to show $\mathrm{Mod}(E) = \mathcal{K}$.
- $\mathrm{Mod}(E) \supseteq \mathcal{K}$ is obvious. Hence, we will prove the following by two steps.

Claim. $\mathrm{Mod}(E) \subseteq \mathcal{K}$.

The idea of the poof: For any $\mathfrak{A} \in \mathrm{Mod}(E)$, it suffices to construct a homomorphism from $\mathfrak{C} \in \mathcal{K}$ onto $\mathfrak{A}$.
Suppose $\mathfrak{A} \in \mathrm{Mod}(E)$. Take a set Y of variables and a surjection $\chi : Y \to |\mathfrak{A}|$. This can be extended to an epimorphism (surjective homom.) $\hat{\chi} : \mathcal{T}(Y) \to \mathfrak{A}$.
By suitable replacement of variables, any equation in Y can be regarded as an equation in X. Thus, it is plausible to consider $\mathcal{T}(Y)/E$ as a desired algebra $\mathfrak{C}$.

Now, we are going to construct $\mathfrak{C}$ more rigorously so that we can see $\mathfrak{C} \in \mathcal{K}$.
For any $\mathfrak{B} \in \mathcal{K}$ and any homomorphism $\phi : \mathcal{T}(Y) \to \mathfrak{B}$, we define a congruence relation $\approx_\phi$ on $\mathcal{T}(Y)$ such that $s \approx_\phi t \Leftrightarrow \phi(s) = \phi(t)$.
By the homomorphism theorem, we have $\phi(\mathcal{T}(Y)) \simeq \mathcal{T}(Y)/\approx_\phi$. Since the left-hand side is a subalgebra of $\mathfrak{B} \in \mathcal{K}$, by assumption we have $\mathcal{T}(Y)/\approx_\phi \in \mathcal{K}$.

Let $\mathcal{D}$ be the set of congruence relations on $\mathcal{T}(Y)$ expressed as $\approx_\phi$ for some homomorphism ϕ. Since $\mathcal{K}$ is closed under Cartesian products, we have

$$\prod_{\approx \in \mathcal{D}} (\mathcal{T}(Y)/\approx) \in \mathcal{K}.$$

With a homom. $\pi_\approx : \mathcal{T}(Y) \to \mathcal{T}(Y)/\approx$ for each $\approx \in \mathcal{D}$, we can naturally define a homom.

$$\psi : \mathcal{T}(Y) \to \prod_{\approx \in \mathcal{D}} (\mathcal{T}(Y)/\approx).$$

Since $\mathcal{T}(Y)/\approx_\psi$ is isomorphic to a subalgebra of $\prod_{\approx \in \mathcal{D}}(\mathcal{T}(Y)/\approx)$, it also belongs to $\mathcal{K}$.
Here, we have: $s \approx_\psi t \Leftrightarrow \psi(s) = \psi(t) \Leftrightarrow$ for each $\approx \in \mathcal{D}$ $s \approx t \Leftrightarrow$ for all ϕ $\phi(s) = \phi(t) \Leftrightarrow$ for all $\mathfrak{B} \in \mathcal{K}$, $\mathfrak{B} \models s = t \Leftrightarrow s = t \in E$ (with suitable replacement of variables). Thus, $\mathcal{T}(Y)/\approx_\psi$ is a desired algebra $\mathfrak{C}$. □

Today's topics

Introduction to Boolean Algebras

- In the mid-19th century, British mathematician G. Boole attempted to clarify Aristotle's logic by treating logical relations algebraically.
- In modern times, Boolean algebra is often subsumed under the more general concepts of "order" and "lattice" and treated as equational theory.

Definition

- A binary relation $\leq$ on a nonempty set X is called a **(partial) order** if it satisfies **reflection** ($x \leq x$), **antisymmetry** (if $x \leq y$ and $y \leq x$, then $x = y$), as well as **transitivity** (if $x \leq y$ and $y \leq z$, then $x \leq z$).
- If an order $(X, \leq)$ additionally satisfies **comparability** ($x \leq y$ or $y \leq x$), then it is called a **total order** or **linear order**.

Let $(X, \leq)$ be a partial order. For a subset $A \subset X$, $\sup A$ denotes the **supremum** (minimum upper bound) of A (if it exists). Similarly, $\inf A$ is the **infimum** (maximum lower bound) of A. $\sup\{a, b\}$ and $\inf\{a, b\}$ are also denoted by $a \vee b$ and $a \wedge b$, respectively.

Definition

Theory of **lattices** consists of the following eight equations. A model of lattice theory $(L, \vee, \wedge)$ is called a **lattice**.

L1 :	$x \vee x = x, \ x \wedge x = x$	[Idempotence]
L2 :	$x \vee y = y \vee x, \ x \wedge y = y \wedge x$	[Commutativity]
L3 :	$x \vee (y \vee z) = (x \vee y) \vee z, \ x \wedge (y \wedge z) = (x \wedge y) \wedge z$	[Associativity]
L4 :	$(x \vee y) \wedge x = x, \ (x \wedge y) \vee x = x$	[Absorption]

Conversely, for a given lattice $(L, \vee, \wedge)$, if a relation $x \leq y$ is defined as follows

$$x \leq y \Leftrightarrow x \wedge y = x (\Leftrightarrow x \vee y = y)$$

then it is a partial order on L. In this case, the lattice operations $\vee, \wedge$ are the same as $\sup$ and $\inf$ regarding this partial order.

Note. We show $x \wedge y = x \Leftrightarrow x \vee y = y$. $\Leftarrow$ can be derived by substituting $y := x \vee y$ to the left side and using lattice axioms L2 and L4. Similarly for $\Rightarrow$.

Now, Boolean algebra is defined as an equational theory as follows.

Definition

The theory of **Boolean algebra** (BA) is defined in language $\mathcal{L}_{\mathrm{B}} = \{\vee, \wedge, \neg, 0, 1\}$ with the following axioms.

1. All the lattice axioms and the following distributive law:

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z), \quad (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z).$$

2. $x \vee 0 = x, \quad x \vee (\neg x) = 1, \quad x \wedge 1 = x, \quad x \wedge (\neg x) = 0.$

A model of theory BA is called a **Boolean algebra**.

In the definition of Boolean algebra, (1) can be reduced to only L2 and distributive laws. This is Problem 9.

Lemma (Uniqueness of complement)

If $x \vee y = 1$ and $x \wedge y = 0$, then $y = \neg x$.

Proof. Assume $x \vee y = 1$ and $x \wedge y = 0$. Apply the distributive law at $=^{(*)}$ to obtain the desired equation as follows.

$$\begin{aligned} y &= y \vee 0 = y \vee (x \wedge \neg x) =^{(*)} (y \vee x) \wedge (y \vee \neg x) = (x \vee y) \wedge (y \vee \neg x) \\ &= 1 \wedge (y \vee \neg x) = (x \vee \neg x) \wedge (y \vee \neg x) =^{(*)} (x \wedge y) \vee \neg x = 0 \vee \neg x = \neg x. \end{aligned}$$

□

- **Remark**. In the formal deduction system of equations, "a premise σ implies a conclusion δ" means that if σ holds with any substitution for all variables then δ also holds with any substitution for all variables.
  In contrast, the lemma should be interpreted as "for all x, y, if ($x \vee y = 1$ and $x \wedge y = 0$, then $y = \neg x$)". To state it strictly, we need first-order logic for the argument.

Lemma (Elimination of double negation)

$\neg\neg x = x$.

Proof. Apply the above lemma to $\neg x \vee x = 1$ and $\neg x \wedge x = 0$. □

Theorem (Duality theorem)

For an equation φ in $\mathcal{L}_{\mathrm{B}} = \{\vee, \wedge, \neg, 0, 1\}$, let $\tilde{\varphi}$ denote the equation (dual equation) obtained from φ by interchanging $\vee$ with $\wedge$ and 0 with 1. Then

$$\mathrm{BA} \vdash \varphi \Leftrightarrow \mathrm{BA} \vdash \tilde{\varphi}.$$

Proof. The dual formula $\tilde{\sigma}$ for each axiom σ of BA is also an axiom. Therefore, for a proof tree of theorem φ in BA, if we replace all expressions in the tree with dual expressions, we obtain a proof tree of $\tilde{\varphi}$. □

Problem 9

(Homework) In the definition of Boolean algebra, reduce (1) to only the commutative law and distributive law, and then prove the Idempotent, absorption law, and associative law.

Theorem (De Morgan's laws)

In BA, $\neg(x \vee y) = \neg x \wedge \neg y,\ \neg(x \wedge y) = \neg x \vee \neg y$ *holds.*

Proof They can be deduced from the following equations together with the uniqueness of the complement.

$$\begin{aligned}
(x \vee y) \vee (\neg x \wedge \neg y) &= [(x \vee y) \vee \neg x] \wedge [(x \vee y) \vee \neg y] \\
&= [(x \vee \neg x) \vee y] \wedge [x \vee (y \vee \neg y)] \\
&= (1 \vee y) \wedge (x \vee 1) = 1 \wedge 1 = 1. \\
(x \vee y) \wedge (\neg x \wedge \neg y) &= [x \wedge (\neg x \wedge \neg y)] \vee [y \wedge (\neg x \wedge \neg y] \\
&= [(x \wedge \neg x) \wedge \neg y] \vee [\neg x \wedge (y \wedge \neg y)] \\
&= (0 \wedge \neg y) \vee (\neg x \wedge 0) = 0 \vee 0 = 0.
\end{aligned}$$

Therefore, $\neg(x \vee y) = \neg x \wedge \neg y$. Also, $\neg(x \wedge y) = \neg x \vee \neg y$ follows from the duality theorem.

Example 12

Let X be any set and $\mathcal{P}(X)$ be the power set (all subsets) of X. Now, if $Y^c = X - Y$ for $Y \subseteq X$, then the power set algebra $\mathfrak{P}(X) = (\mathcal{P}(X), \cup, \cap, ^c, \varnothing, X)$ is a Boolean algebra. In particular, when X is a singleton $\{a\}$, $\mathcal{P}(X)$ is a trivial Boolean algebra, and isomorphic to $2 = (\{0, 1\}, \vee, \wedge, 0, 1)$.

Conversely, any finite Boolean algebra is isomorphic to a power set algebra, and more generally the following theorem holds. (The proof will be given in part 3)

Theorem (Stone's representation theorem)

For any Boolean algebra $\mathfrak{B}$, there exists a set X, $\mathfrak{B}$ can be embedded into the power set algebra $\mathfrak{P}(X)$. Especially, if $\mathfrak{B}$ is finite, it is isomorphic to $\mathfrak{P}(X)$.

- By a Boolean expression $\varphi(x_1, x_2, \ldots, x_n)$, we denote a term of $\mathcal{L}_\mathrm{B}$ with only variables $\{x_1, x_2, \ldots, x_n\}$.
- A Boolean expression $\varphi(x_1, x_2, \ldots, x_n)$ defines a function $f_\varphi : \{0, 1\}^n \to \{0, 1\}$. Such functions are called **Boolean functions**.
- We want to show that any function $f : \{0, 1\}^n \to \{0, 1\}$ can be expressed as f_φ with some Boolean expression φ. Moreover, if two Boolean expressions φ and ψ define the same function $f_\varphi = f_\psi$, then $\varphi = \psi$ is a theorem of BA. These can be obtained from the normal form theorem for Boolean expressions.

Shannon's expansion (decomposition) theorem

Lemma (Shannon's theorem)

$\mathrm{BA} \vdash \varphi(x_1, x_2, \ldots, x_n) \leftrightarrow (\varphi(0, x_2, \ldots, x_n) \wedge \neg x_1) \vee (\varphi(1, x_2, \ldots, x_n) \wedge x_1)$ [1].

Proof.

- Given a Boolean expression, we use de Morgan's laws and double negation elimination to push the negation symbols innermost so that each negation appears just before an variable. A Boolean expression in such a form is called a **negation normal form**.
- So, we may assume that a Boolean expression φ is in the negation normal form.
- Now, we prove the assertion of the lemma by induction on the number m of operators $\vee$ and $\wedge$ included in φ.

[1] This was already proved by Boole, but it is known as "Shannon's expansion (decomposition) theorem."

(i) In the case of $m = 0$.
φ is a variable or the negation of a variable.

- If φ is x_1, $(\varphi(0) \wedge \neg x_1) \vee (\varphi(1) \wedge x_1) = (0 \wedge \neg x_1) \vee (1 \wedge x_1) = x_1$.
- If φ is $\neg x_1$, $(\varphi(0) \wedge \neg x_1) \vee (\varphi(1) \wedge x_1) = (1 \wedge \neg x_1) \vee (0 \wedge x_1) = \neg x_1$.
- If φ is x_i or $\neg x_i (i \neq 1)$, no matter what is assigned to x_1, it is the same as φ, so $(\varphi \wedge \neg x_1) \vee (\varphi \wedge x_1) = \varphi \wedge (\neg x_1 \vee x_1) = \varphi$.

(ii) In the case of $m > 0$.
Let φ be $\varphi_1 \vee \varphi_2$, and by induction hypothesis

$$\varphi_i = (\varphi_i(0) \wedge \neg x_1) \vee (\varphi_i(1) \wedge x_1) \ (i = 1, 2).$$

Then,

$$\begin{aligned}
\varphi_1 \vee \varphi_2 &= [(\varphi_1(0) \wedge \neg x_1) \vee (\varphi_1(1) \wedge x_1)] \vee [(\varphi_2(0) \wedge \neg x_1) \vee (\varphi_2(1) \wedge x_1)] \\
&= [(\varphi_1(0) \vee \varphi_2(0)) \wedge \neg x_1] \vee [(\varphi_1(1) \vee \varphi_2(1)) \wedge x_1] \\
&= (\varphi(0) \wedge \neg x_1) \vee (\varphi(1) \wedge x_1).
\end{aligned}$$

Similarly we can prove for $\varphi \equiv \varphi_1 \wedge \varphi_2$. □

Notation. $\varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_n$ is also written as $\bigvee_{i=1,\ldots,n} \varphi_i$.
Furthermore, we set $x^b = x$ if $b = 1$ and $x^b = \neg x$ if $b = 0$.

Theorem (Disjunctive normal form)

For a Boolean expression $\varphi(x_1, x_2, \ldots, x_n)$,

$$\begin{aligned} \mathrm{BA} \vdash \varphi(x_1, x_2, \ldots, x_n) &= \bigvee_{b_1,\ldots,b_n=0,1} \varphi(b_1, b_2, \ldots, b_n) \wedge x_1^{b_1} \wedge x_2^{b_2} \wedge \cdots \wedge x_n^{b_n} \\ &= \bigvee_{f_\varphi(b_1,\ldots,b_n)=1} x_1^{b_1} \wedge x_2^{b_2} \wedge \cdots \wedge x_n^{b_n}. \end{aligned}$$

If there is no $b_1, \ldots, b_n$ such that $f_\varphi(b_1, \ldots, b_n) = 1$, then we set the right-hand side $= 0$.

Proof By Shannon's theorem, we can prove this by induction on the number of variables. □

The rightmost expression in the last theorem is called the **disjunctive normal form** of φ. In addition, if we rewrite $\neg\sigma$ into the disjunctive normal form, then we can easily obtain a conjunctive normal form of σ by de Morgan's laws and double negation elimination.

Corollary

For any function $f : \{0,1\}^n \to \{0,1\}$, there exists a Boolean expression φ such that $f = f_\varphi$.

Proof. Obvious from the theorem □

Corollary

If two Boolean expressions φ and ψ define the same function $f_\varphi = f_\psi$, then $\mathrm{BA} \vdash \varphi = \psi$.

Proof. In the theorem, both disjunctive normal forms are the same. □

Corollary

The number of equivalence classes of Boolean expressions of n variables is 2^{2^n}.

Proof. The number of equivalence classes of a Boolean expression with n variable is equal to the number of the function $f : \{0,1\}^n \to \{0,1\}$, that is, 2^{2^n}. □

Finally, we introduce Boolean rings, which are essentially equivalent to Boolean algebras.

Definition

The theory CR of **commutative ring** consists of the following axioms, in the language $\mathcal{L}_{\mathrm{R}} = \{+, \bullet, -, 0, 1\}$.

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

A model of the theory CR is called a **commutative ring**.

In BA and CR, we usually assume $0 \neq 1$ as an axiom. But since we want to treat them as an equational theory, we treat a structure where $0 = 1$ as a special case.

Example 13

The structure of integers $\mathfrak{Z} = (\mathbb{Z}, +, \bullet, -, 0, 1)$ is a commutative ring.

Example 14

For a commutative ring $\mathfrak{A}$, the set of polynomials with variables $X_1, X_2, \ldots, X_n$ and coefficients in A also becomes a commutative ring, denote $\mathfrak{A}[X_1, X_2, \ldots, X_n]$.

Definition

The theory BR of **Boolean rings** is the theory CR plus the following axiom.

$$x^2 = x.$$

A model of the theory BR is called a **Boolean ring**.

We first show that $x + x = 0$ holds in BR.

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x.$$

By subtracting $x + x$ from both sides, we get $x + x = 0$. So, $+$ in a Boolean ring has a different property from $+$ in a Boolean algebra. However, both are mutually translatable as shown in the next theorem.

Theorem (Stone theorem)

(1) For any Boolean algebra $\mathfrak{B} = (B, \vee, \wedge, \neg, 0, 1)$, *we set*

$$x + y = (x \wedge (\neg y)) \vee ((\neg x) \wedge y), \quad x \bullet y = x \wedge y, \quad -x = x.$$

Then, $\mathfrak{B}^\circ = (B, +, \bullet, -, 0, 1)$ *is a Boolean ring.*

(2) For any Boolean ring $\mathfrak{R} = (R, +, \bullet, -, 0, 1)$, *we set*

$$x \vee y = x + y + x \bullet y, \quad x \wedge y = x \bullet y, \quad \neg x = 1 + x$$

and then $\mathfrak{R}^\circ = (R, \vee, \wedge, \neg, 0, 1)$ *is a Boolean algebra.*

(3) By (1) and (2), for a Boolean algebra $\mathfrak{B}$ *and a Boolean ring* $\mathfrak{R}$,

$$\mathfrak{B}^{\circ\circ} = \mathfrak{B},$$

$$\mathfrak{R}^{\circ\circ} = \mathfrak{R}.$$

Propositional logic

- In this part, we will study **propositional logic** which treats the logical relationships between propositions in terms of **propositional connectives**: $\neg$ (not $\cdots$), $\wedge$ (and), $\vee$ (or), $\to$ (implies),
- Propositions are constructed from atomic propositions by way of propositional connectives. Atomic propositions are simply symbols that can take value either T (meaning true) or F (meaning false).
- Let v be a function that assigns truth values T (True) or F (False) to atomic propositions. Then, a **truth value assignment** V (also called a **truth value function**) for all propositions are uniquely defined as follows.

  (1) for an atomic proposition φ, $V(\varphi) = v(\varphi)$.

  (2a) $V(\neg\varphi) = \mathrm{T} \overset{\text{def}}{\Longleftrightarrow} V(\varphi) = \mathrm{F}$,

  (2b) $V(\varphi \wedge \psi) = \mathrm{T} \overset{\text{def}}{\Longleftrightarrow} V(\varphi) = \mathrm{T}$ and $V(\psi) = \mathrm{T}$,

  (2c) $V(\varphi \vee \psi) = \mathrm{T} \overset{\text{def}}{\Longleftrightarrow} V(\varphi) = \mathrm{T}$ or $V(\psi) = \mathrm{T}$,

  (2d) $V(\varphi \to \psi) = \mathrm{T} \overset{\text{def}}{\Longleftrightarrow} V(\varphi) = \mathrm{F}$ or $V(\psi) = \mathrm{T}$.

Definition

If a proposition φ is always true, i.e., $V(\varphi) = \mathrm{T}$ for any truth-value function V, then φ is said to be **valid** or a **tautology**, written as $\models \varphi$.

- We consider the structure of the tautologies.
- To this end, it is not necessary to deal with all four propositional symbols at once. By setting $\varphi \vee \psi := \neg\varphi \to \psi$, $\varphi \wedge \psi := \neg(\varphi \to \neg\psi)$, we omit $\vee$ and $\wedge$.

The followings are tautologies.

P1. $\varphi \to (\psi \to \varphi)$

P2. $\big(\varphi \to (\psi \to \theta)\big) \to \big((\varphi \to \psi) \to (\varphi \to \theta)\big)$

P3. $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$

Definition (Theorems)

The **theorems** of propositional logic are defined as follows.

(1) Axioms $\mathrm{P1}$, $\mathrm{P2}$, $\mathrm{P3}$ are theorems.

(2) If φ and $\varphi \to \psi$ are theorems, so is ψ. (detachment rule)

Detachment rule is also called **modus ponens** (**MP** for short) and **cut**.
We also define a "proof" as a process generating a theorem.

Definition (Proof)

A sequence of propositions $\varphi_0, \varphi_1, \cdots, \varphi_n$ is called a **proof** of φ_n if it satisfies the following conditions: For $k \leq n$,

(1) φ_k is one of axioms $\mathrm{P1}$, $\mathrm{P2}$, $\mathrm{P3}$, or

(2) There exist $i, j < k$ such that $\varphi_j = \varphi_i \to \varphi_k$ (MP).

Note that a "theorem" is the last component of a "proof".
By $\vdash \varphi$, we denote that φ is a theorem.

Completeness

The completeness theorem for propositional logic

$\vdash \varphi \Leftrightarrow \models \varphi.$

From propositional logic to Boolean algebra.

- We eliminate the operation $\to$ in a proposition by $\varphi \to \psi := \neg\varphi \vee \psi$.
  Then (prop. logic) $\vdash \varphi \Leftrightarrow \mathrm{BA} \vdash \varphi = 1$.

Homework

Consider the relation between the completeness theorem for propositional logic and that for Boolean algebra.

Homework 1

Hw1-Problem 1

Construct a proof tree for $\mathrm{G_p} \vdash xx^{-1} = \mathrm{e}$.

Solution:

Let $s = xx^{-1}$, and let P_4 be the proof tree of $ss = s$ given in Example 1.
The proof tree for $(s^{-1}s)s = s^{-1}(ss)$, $s = (s^{-1}s)s$, $s = s^{-1}s$ are denoted as P_5, P_6, and P_7 in the following.

$$\dfrac{\dfrac{\dfrac{(xy)z = x(yz)}{(s^{-1}y)z = s^{-1}(yz)}\,(\mathrm{sub})}{(s^{-1}s)z = s^{-1}(sz)}\,(\mathrm{sub})}{(s^{-1}s)s = s^{-1}(ss)}\,(\mathrm{sub})$$

$$\dfrac{\dfrac{\dfrac{ex = x}{es = s}\,(\mathrm{sub})}{s = es}\,(\mathrm{sym}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{x^{-1}x = e}{s^{-1}s = e}\,(\mathrm{sub})}{e = s^{-1}s}\,(\mathrm{sym}) \qquad \dfrac{}{s = s}}{es = (s^{-1}s)s}\,(\mathrm{comp})}{s = (s^{-1}s)s}\,(\mathrm{trans})$$

$$\dfrac{\dfrac{\dfrac{P_6}{s = (s^{-1}s)s} \qquad \dfrac{P_5}{(s^{-1}s)s = s^{-1}(ss)}}{s = s^{-1}(ss)}\ (\text{trans}) \qquad \dfrac{s^{-1} = s^{-1} \qquad \dfrac{P_4}{ss = s}}{s^{-1}(ss) = s^{-1}s}\ (\text{comp})}{s = s^{-1}s}\ (\text{trans})$$

The desired proof tree is

$$\dfrac{\dfrac{P_7}{s = s^{-1}s} \qquad \dfrac{x^{-1}x = e}{s^{-1}s = e}\ (\text{sub})}{s = e}\ (\text{trans})$$

Homework 2

Hw2-Problem 1

Let $\mathcal{L} = \{\mathtt{g}_1, \mathtt{g}_2, \mathtt{h}\}$. We define the set of equations E as follows.

$$E = \{\mathtt{h}(\mathtt{g}_1(x), \mathtt{g}_2(x)) = x,\ \mathtt{g}_1(\mathtt{h}(x, y)) = x,\ \mathtt{g}_2(\mathtt{h}(x, y)) = y\}$$

Let $\mathcal{K}$ be $\mathrm{Mod}(E)$, the class of models of E. Show that all finitely generated free $\mathcal{K}$-algebras are isomorphic.

Solution:

- Consider the free $\mathrm{Mod}(E)$-algebra $\mathcal{T}(X_1)/E$, $\mathcal{T}(X_2)/E$ generated by the finite set $X_1 = \{x\}$, $X_2 = \{x_1, x_2\}$.
- Since they are free $\mathrm{Mod}(E)$-algebra, we have a homomorphism $\phi : \mathcal{T}(X_1)/E \to \mathcal{T}(X_2)/E$, which is an extension of $x \mapsto h(x_1, x_2)$, and there exist $x_1 \mapsto g_1(x)$ and a homogeneous $\psi : \mathcal{T}(X_2)/E \to \mathcal{T}(X_1)/E$ which is an extension of $x_2 \mapsto g_2(x)$.

- Then,

$$\psi \circ \phi(x) = \psi(h(x_1, x_2)) = h(\psi(x_1), \psi(x_2)) = h(g_1(x), g_2(x)) = x$$

- Therefore, $\psi \circ \phi$ corresponds to the identity mapping from $\mathcal{T}(X_1)/E$ to itself.
- Similarly, $\phi \circ \psi$ is also an identity map, and $\phi = \psi^{-1}$ is isomorphic.
- All that remains is to extend this argument to the relationship between $X_1 = \{x\}$ and $X_n = \{x_1, \ldots, x_n\}$.
- For example, when $n = 3$, the homomorphism that is an extension of $x \mapsto h(h(x_1, x_2), x_3)$ is isomorphic.

Homework 2

Recall: Boolean algebra

The theory of Boolean algebra (BA) is defined in language $\mathcal{L}_\mathrm{B} = \{\vee, \wedge, \neg, 0, 1\}$ with the following axioms.

(1) All the lattice axioms and the following distributive law:

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z), \quad (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z).$$

(2) $x \vee 0 = x, \quad x \vee (\neg x) = 1, \quad x \wedge 1 = x, \quad x \wedge (\neg x) = 0.$

A model of theory BA is called a Boolean algebra.

Hw2-Problem 2

In the definition of Boolean algebra, reduce (1) to only the commutative law and distributive law, and then prove the Idempotent, absorption law, and associative law.

Homework 2

Solution:

Using only the commutative law and the distribution ratio, we show the following.

$$\textbf{Idempotent}: \quad x = x \vee 0 = x \vee (x \wedge \neg x) = (x \vee x) \wedge (x \vee \neg x) = (x \vee x) \wedge 1 = x \vee x.$$

Since the duality theorem holds, we have $x = x \wedge x$.

Absorption law: $(x \vee y) \wedge x = (x \vee y) \wedge (x \vee 0) = x \vee (y \wedge 0) = x \vee 0 = x$.

$(x \wedge y) \vee x = x$ is due to the duality theorem.

Associative law: By the distributive law and the absorption law,

$$\begin{aligned} x \vee (y \vee z) &= [x \vee (y \vee z)] \wedge (x \vee \neg x) \\ &= [x \vee (y \vee z)] \wedge x \vee [x \vee (y \vee z)] \wedge \neg x \\ &= x \vee [(y \wedge \neg x) \vee (z \wedge \neg x)] \\ &= [(x \vee y) \vee z] \wedge x \vee [(x \vee y) \vee z] \wedge \neg x \\ &= [(x \vee y) \vee z] \wedge (x \vee \neg x) \\ &= (x \vee y) \vee z. \end{aligned}$$

By duality theorem, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

Thank you for your attention!