Notes for Logic (COMP0009)

Raphael Li

Sep 2025

Contents

1 Revision: Syntax and semantics of propositional and first-order logic

Formally, a *logic* consists of three components:

Component	Describes...
Syntax	The language and grammar for writing formulas
Semantics	How formulas are interpreted
Inference system (or proof system)	A syntactic device for proving true statements

Table 1: The three key components of a logic.

This module concerns algorithms that automatically parse and determine the validity of a formula.

1.1 Propositional logic

1.1.1 Syntax

Formulas are constructed by applying negation, conjunction and disjunction to propositions.

$$\begin{aligned} \text{proposition} &\coloneqq p \mid q \mid r \mid \cdots \\ \text{formula} &\coloneqq \text{proposition} \mid \neg\text{formula} \mid (\text{formula} \circ \text{formula}) \qquad (\text{where } \circ \text{ is } \wedge, \vee \text{ or } \rightarrow) \end{aligned}$$

A proposition or its negation is called a *literal*[1].

For any formula that isn't a proposition, the *main connective* is the one with the largest scope. In other words, it is not in the scope of any other connective.

$$((p \wedge q) \vee \neg(q \rightarrow r))$$

This is the connective with which evaluation begins. This is especially important when building parsers for algorithmically evaluating formulas[2].

1.1.2 Semantics

A valuation is a function v that maps each proposition to a truth value in $\{\top, \bot\}$.

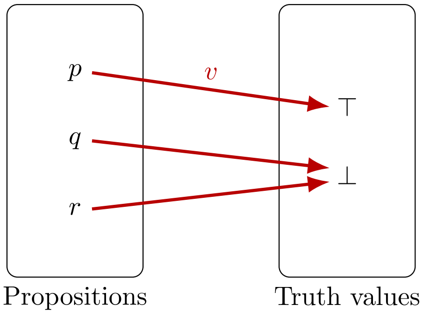


Figure 1: A valuation maps propositions to truth values.

A valuation v can be extended to a unique *truth function* defined on all possible formulas. A truth

[1] For example, p and $\neg p$ are both literals, but $\neg\neg q$ is not.

[2] Note that parsers working according to the above definition will recognise $(p \wedge q)$, but not $p \wedge q$, as a formula. Regardless, throughout this document we will use a looser definition where brackets may be ommitted in unambiguous cases.

function v' must satisfy

$$\begin{aligned}
v'(\neg\phi) = \top &\iff v'(\phi) = \bot \\
v'(\phi \vee \psi) = \top &\iff v'(\phi) = \top \text{ or } v'(\psi) = \top \\
v'(\phi \wedge \psi) = \top &\iff v'(\phi) = \top \text{ and } v'(\psi) = \top \\
v'(\phi \rightarrow \psi) = \top &\iff v'(\phi) = \bot \text{ or } v'(\psi) = \top \\
v'(\phi \leftrightarrow \psi) = \top &\iff v'(\phi) = v'(\psi)
\end{aligned}$$

for all formulas ϕ and ψ. From now on we use v to denote the more general truth function.

The result of applying a valuation v to a formula ϕ depends only on the propositional letters that occur in ϕ.

A formula ϕ is *valid* if $v(\phi) = \top$ for all valuations v, which we denote as $\models \phi$. A formula ϕ is *satisfiable* if $v(\phi) = \top$ for at least one valuation v. All valid formulas are satisfiable, but *not* vice versa.

Two formulas ϕ and ψ are *logically equivalent*, written as $\phi \equiv \psi$, if and only if for every valuation v we have $v(\phi) = v(\psi)$.

1.1.3 Truth tables

Consider the propositional formula $((p \vee \neg q) \wedge \neg(q \wedge r))$. We can check its validity and satisfiability by constructing its truth table.

p	q	r	$(p \vee \neg q)$	$\neg(q \wedge r)$	$((p \vee \neg q) \wedge \neg(q \wedge r))$
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	0	1	0
0	1	1	0	0	0
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	0	0

Table 2: The truth table for the formula $((p \vee \neg q) \wedge \neg(q \wedge r))$.

In this case, the formula is satisfiable but not valid.

1.1.4 Parse trees

A parser interprets the semantics of a formula by breaking down its symbols into a *parse tree*, which shows the syntactic relation between symbols. For example, the formula $((p \vee \neg q) \wedge \neg(q \wedge r))$ can be broken down into the following parse tree.

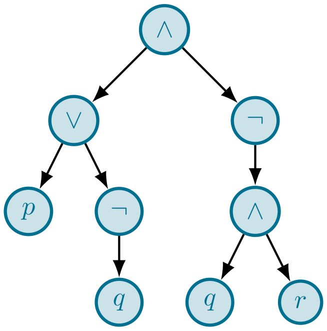


Figure 2: The parse tree for the formula $((p \vee \neg q) \wedge \neg(q \wedge r))$.

1.1.5 Disjunctive normal form (DNF)

A formula is said to be in *disjunctive normal form* (DNF) if it is a disjunction of one or more conjunctions of one or more literals.

$$\begin{aligned}
\text{proposition} &\coloneqq p \mid q \mid r \mid \cdots \\
\text{literal} &\coloneqq \text{proposition} \mid \neg\text{proposition} \\
\text{conjunctiveClause} &\coloneqq \text{literal} \mid \text{literal} \ \wedge \ \text{conjunctiveClause} \\
\text{DNF} &\coloneqq \text{conjunctiveClause} \mid \text{conjunctiveClause} \ \vee \ \text{DNF}
\end{aligned}$$

Below is an example of a formula in DNF.

$$\underbrace{(p \wedge \neg q \wedge \neg r)}_{\substack{\text{conjunctive}\\ \text{clause}}} \vee \underbrace{(\neg p \wedge \neg q \wedge r)}_{\substack{\text{conjunctive}\\ \text{clause}}} \vee \underbrace{(q \wedge \neg r)}_{\substack{\text{conjunctive}\\ \text{clause}}}$$

Any propositional formula has a DNF equivalent. For instance, the formula $(p \vee \neg q) \wedge \neg(q \wedge r)$ can be rewritten as follows.

$$\begin{aligned}
&(p \vee \neg q) \wedge \neg(q \wedge r) \\
\Longleftrightarrow\ &(p \vee \neg q) \wedge (\neg q \vee \neg r) && \text{(De Morgan's law, to remove outer negation)} \\
\Longleftrightarrow\ &((p \vee \neg q) \wedge \neg q) \vee ((p \vee \neg q) \wedge \neg r) && \text{(distributing conjunctions over disjunctions)} \\
\Longleftrightarrow\ &(p \wedge \neg q) \vee (\neg q \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg q \wedge \neg r) && \text{(distributing conjunctions over disjunctions)} \\
\Longleftrightarrow\ &(p \wedge \neg q) \vee \neg q \vee (p \wedge \neg r) \vee (\neg q \wedge \neg r)
\end{aligned}$$

Alternatively, this can also be achieved by referring to the truth table. From Table 2, we see that the formula can be written in DNF as

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r).$$

1.1.6 Conjunctive normal form (CNF)

A formula is said to be *conjunctive normal form* (CNF) if it is a conjunction of one or more disjunctions of one or more literals.

$$\begin{aligned}
\text{disjunctiveClause} &\coloneqq \text{literal} \mid \text{literal} \ \vee \ \text{disjunctiveClause} \\
\text{CNF} &\coloneqq \text{disjunctiveClause} \mid \text{disjunctiveClause} \ \wedge \ \text{CNF}
\end{aligned}$$

Below is a formula in CNF.

$$\underbrace{(p \vee \neg q \vee \neg r)}_{\substack{\text{conjunctive}\\ \text{clause}}} \wedge \underbrace{(\neg p \vee q \vee r)}_{\substack{\text{conjunctive}\\ \text{clause}}}$$

To find the CNF equivalent of a formula ϕ, we first express its negation $\neg\phi$ in DNF. Then, we negate it again to get $\neg\neg\phi$. Using De Morgan's law, the resultant formula will be in CNF.

For example, let ϕ be the formula $(p \vee \neg q) \wedge \neg(q \wedge r)$. To rewrite it in CNF, we start by constructing the truth table of its negation $\neg\phi$. This allows us to express $\neg\phi$ in DNF.

p	q	r	$((p \lor \neg q) \land \neg(q \land r))$	Negation of $((p \lor \neg q) \land \neg(q \land r))$
0	0	0	1	0
0	0	1	1	0
0	1	0	0	1
0	1	1	0	1
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	0	1

Table 3: The truth table for the negation of $((p \lor \neg q) \land \neg(q \land r))$. This is obtained by flipping the results of Table 2.

Hence we have

$$\begin{aligned}
\neg\phi &= (\neg p \land q) \lor (p \land q \land r) && \text{(DNF of } \neg\phi\text{)} \\
\neg\neg\phi &= \neg((\neg p \land q) \lor (p \land q \land r)) && \text{(negating both sides)} \\
\phi &= (p \lor \neg q) \land (\neg p \lor \neg q \lor \neg r) && \text{(double negation; De Morgan's laws)}
\end{aligned}$$

which gives us ϕ in CNF.

1.2 First-order logic

1.2.1 Syntax

A first-order language $L(C, F, P)$ is determined by a set C of constant symbols, a set F of function symbols and a non-empty set P of predicate symbols. Each function symbol and predicate symbol has an associated *arity* $n \in \mathbb{N}$. We write f^n and p^n to represent an n-ary function symbol and an n-ary predicate symbol respectively. Moreover, let V be a countably infinite set of variable symbols.

$$\begin{aligned}
\text{term} &\coloneqq c \mid v \mid f^n(\text{term}_0, \text{term}_1, \cdots, \text{term}_{n-1}) && \text{(where } c \in C,\ v \in V \text{ and } f^n \in F\text{)} \\
\text{atom} &\coloneqq p^n(\text{term}_0, \text{term}_1, \cdots, \text{term}_{n-1}) && \text{(where } p^n \in P\text{)} \\
\text{formula} &\coloneqq \text{atom} \mid \neg\text{formula} \mid (\text{formula}_0 \lor \text{formula}_1) \mid \exists v \text{ formula} && \text{(where } v \in V\text{)}
\end{aligned}$$

This definition is functionally complete. Formulas involving universal quantifiers, implications and equivalence symbols can always be rewritten using only symbols defined above.

A *closed term* is a term with no variable symbols. A *sentence* is a formula with no free variables.

1.2.2 Semantics

For a first-order language $L(C, F, P)$, we may construct a corresponding first-order structure[3] $S = (D, I)$ where $I = (I_c, I_f, I_p)$.

$$S = (\underbrace{D}_{\substack{\text{non-empty} \\ \text{domain}}},\ \overbrace{(I_c, I_f, I_p)}^{\text{interpretation } I})$$

Here,

- I_c maps each constant symbol in C to an element of D.
- I_f maps each n-ary function symbol in F to an n-ary function over D.
- I_p maps each n-ary predicate symbol $p \in P$ to an n-ary relation over D (i.e. a subset of D^n).

[3] Also known as an L-structure.

- We may occasionally use I to denote a general interpretation function where

$$\begin{aligned} I(c) &= I_c(c) && \text{(for all } c \in C) \\ I(f) &= I_f(f) && \text{(for all } f \in F) \\ I(p) &= I_p(p) && \text{(for all } p \in P) \end{aligned}$$

If P includes the equality symbol $=$, then it is always interpreted as the binary relation of true equality.

$$I_p(=) = \{(d, d) : d \in D\}$$

Given a structure $S = (D, I)$, a variable assignment A is a map from V to D. For any variable $v \in V$, two variable assignments A and A^* are said to be v-equivalent if $A(x) = A^*(x)$ for all $x \in V \setminus \{v\}$. In other words, two variable assignments are said to be v-equivalent if they are completely identical except possibly for the element in D assigned to v. This is written as $A \equiv_v A^*$.

Given a structure S and a variable assignment A, we may interpret any term as follows.

$$\begin{aligned} c^{S,A} &= I_c(c) \\ v^{S,A} &= A(v) \\ f^n(t_0, t_1, \cdots, t_{n-1})^{S,A} &= \underbrace{(I_f(f^n))}_{\text{interpreted function}}(t_0^{S,A}, t_1^{S,A}, \cdots, t_{n-1}^{S,A}) \end{aligned}$$

Formulas are evaluated as follows.

$$\begin{aligned} S \models_A p^n(t_0, t_1, \cdots, t_{n-1}) &\iff (t_0^{S,A}, t_1^{S,A}, \cdots, t_{n-1}^{S,A}) \in I_p(p^n) \\ S \models_A \neg\text{formula} &\iff S \not\models_A \text{formula} \\ S \models_A (\text{formula}_0 \vee \text{formula}_1) &\iff S \models_A \text{formula}_0 \text{ or } S \models_A \text{formula}_1 \\ S \models_A \exists v \text{ formula} &\iff S \models_{A[x \mapsto d]} \text{formula for some } d \in D \end{aligned}$$

Given a structure S and a formula ϕ, we say that

- ϕ is "valid in S" if $S \models_A \phi$ for every variable assignment A. This is written as $S \models \phi$.
- ϕ is "satisfiable in S" if $S \models_A \phi$ for some variable assignment A.
- ϕ is "valid" if ϕ is valid in all possible structures. This is written as $\models \phi$.
- ϕ is "satisfiable" if there exists some structure in which ϕ is satisfiable.

A formula ϕ is valid if and only if $\neg\phi$ is not satisfiable.

> **Proof.** Let $\neg\phi$ be a formula that is not satisfiable. Hence we have
>
> $$\begin{aligned} \neg\exists S\ \exists A \quad S \models_A \neg\phi &\iff \neg\exists S\ \exists A \quad S \not\models_A \phi \\ &\iff \forall S\ \neg\exists A \quad S \not\models_A \phi \\ &\iff \forall S\ \forall A \quad \neg S \not\models_A \phi \\ &\iff \forall S\ \forall A \quad S \models_A \phi \end{aligned}$$
>
> which means S is valid.

If ϕ is a sentence, then ϕ is valid in S if and only if it is also satisfiable in S.

1.2.3 Example: Arithmetic in the set of natural numbers

Consider the first-order language $L(C, F, P)$ defined as follows. Also assume a countably infinite set V of variable symbols.

$$\begin{aligned}
C &= 1, 2, 3, \cdots && \text{(constant symbols)} \\
F &= \{+, \times\} && \text{(function symbols, both binary)} \\
P &= \{=, <\} && \text{(predicate symbols, both binary)} \\
V &= \{x, y, z, \cdots\} && \text{(variable symbols)}
\end{aligned}$$

A term is a string of symbols that represents a “thing” or an “object” — this can be a constant, a variable, or a function output.

- x
- $1 + 3$
- $2 \times x + 1$

Of the terms shown above, only the second one is a closed terms because it has no variable symbols.

An atom is a string of symbols that represents the output of a predicate, which is a truth value.

- $1 = 2$
- $y < 3$
- $x + 1 < 2 \times z + 3$

Finally, a formula is constructed by applying negations, disjunctions, and existential quantifiers to atoms.

- $1 = 2 \ \wedge \ y < 3$
- $\neg \exists z \ \ x + 1 < 2 \times z + 3$

The latter example is a sentence because all of its variable symbols are bounded.

For this particular first-order language, we may use the structure of ordinary arithmetic[4], defined as $N = \{\mathbb{N}, \{I_c, I_f, I_p\}\}$ where

- I_c is a function that maps numerical symbols to the corresponding natural number.

$$\begin{aligned}
I_c(1) &= 1 \\
I_c(2) &= 2 \\
I_c(3) &= 3 \\
&\vdots
\end{aligned}$$

- I_f maps $+$ and $\times$ to the addition and multiplication operations in arithmetic respectively.
- I_p maps $=$ and $<$ to the following relations.

$$\begin{aligned}
I_p(=) &= \{(n, n) : n \in \mathbb{N}\} \\
I_p(<) &= \{(m, n) \in \mathbb{N}^2 : m < n\}
\end{aligned}$$

[4] There is also a similar structure $R = (\mathbb{R}, I)$ where the domain is the set of real numbers.

1.2.4 First-order structures and directed graphs

Consider a first-order language with only one binary predicate symbol p.

$$L(C, F, \{p\})$$

Any first-order structure $S = \{D, \{I_c, I_f, I_p\}\}$ for this language can be represented as a directed graph, where each vertex is an element of D and each directed edge represents an element of the relation $I_p(p)$.

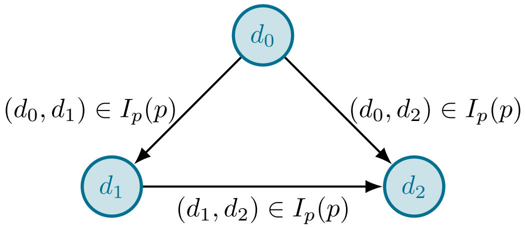


Figure 3: The first-order structure S can be visualised as a directed graph.

2 Axiomatic Proofs for Propositional Logic

A *proof system* is a system for determining the validity of formulas.

An obvious system would be to construct a truth table and check that all rows give a true result. However, this naive approach has an exponential time complexity[5], meaning that it will become increasingly impractical as more and more propositions are introduced.

To alleviate this issue, we shall introduce a different approach called a *Hilbert-style proof system.* This is an *axiomatic proof system* in which theorems are generated using axioms and inference rules.

2.1 Hilbert-style proof system

Firstly, we limit our propositional language to only use the connectives $\neg$ and $\rightarrow$. Double negations are prohibited.

Moreover, we will note some *axioms* that are known to be valid, and then try to derive other valid formulas from the axioms. Below we list three examples of *schemas*, from which axioms may be obtained by substituting any formulas in place of p, q and r.

I. $p \rightarrow (q \rightarrow p)$ (implication is true if consequent is true)

II. $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$ (implication chain as hypothetical syllogism)

III. $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$ (contrapositive)

Axioms on their own are insufficient in establishing a proof system. We also need *inference rules*, which stipulate how conclusions can be derived from premises. One of the main inference rules is *modus ponens*, which states that if you have proved both the formula ϕ and the implication $(\phi \rightarrow \psi)$, then you may deduce the conclusion ψ.

$$\frac{\phi \quad (\phi \rightarrow \psi)}{\psi} \qquad \text{(modus ponens)}$$

In this system, a *proof* is a sequence of formulas

$$\phi_0,\ \phi_1,\ \phi_2,\ \cdots,\ \phi_n$$

such that for each $i \leq n$, the formula ϕ_i is either

- an axiom; or
- obtained from two previous formulas ϕ_j and ϕ_k in the sequence via modus ponens (for some $j, k < i$).

If such a proof exists, then the final formula ϕ_n is called a *theorem* and we may write $\vdash \phi_n$.

[5] Using this system, checking the validity of a formula with n proposition symbols requires 2^n computations.

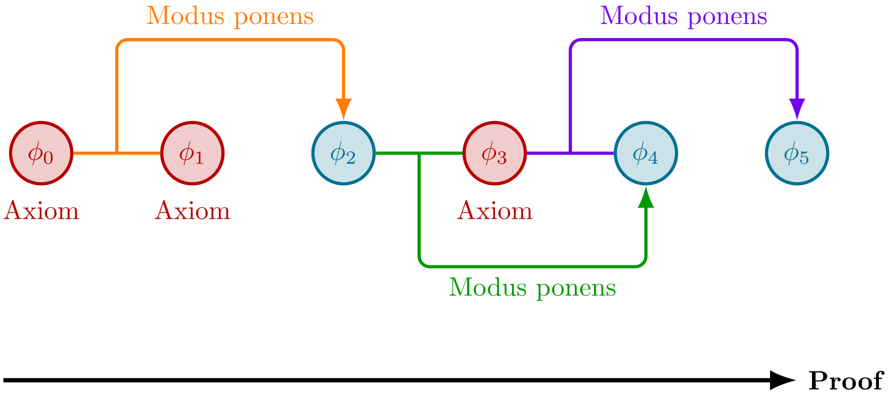


Figure 4: In a proof, every formula must be either an axiom, or derived from previous formulas via modus ponens.

For example, the theorem

$$\vdash (p \to p)$$

may be proved using the above proof system as follows.

1. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ (Axiom I, replacing p, q, r by $p, (p \to p), p$)

2. $p \to ((p \to p) \to p)$ (Axiom II, replacing p, q by $p, (p \to p)$)

3. $(p \to (p \to p)) \to (p \to p)$ (modus ponens, via 1 and 2)

4. $p \to (p \to p)$ (Axiom I, replacing p, q by p, p)

5. $p \to p$ (modus ponens, via 3 and 4)

To include double negations and other connectives like $\wedge$ and $\vee$, we may add more axioms to our proof system.

IV. $p \to \neg\neg p$ and $\neg\neg p \to p$ (double negation)

V. $(p \vee q) \to (\neg p \to q)$ and $(\neg p \to q) \to (p \vee q)$ (implication as disjunction)

VI. $(p \wedge q) \to \neg(p \to \neg q)$ and $\neg(p \to \neg q) \to (p \wedge q)$ (implication as conjunction)

2.2 Proofs with assumptions and the principle of explosion

Let Γ be a set of *assumptions*, i.e. formulas that are assumed to be true. Under these assumptions, a proof is defined as a sequence of formulas

$$\phi_0,\ \phi_1,\ \phi_2,\ \cdots \phi_n$$

such that for each $i \leq n$, the formula ϕ_i is either

- an axiom;
- an assumption $\phi_i \in \Gamma$; or
- obtained from two previous formulas ϕ_j and ϕ_k in the sequence via modus ponens (for some $j, k < i$).

If such a proof exists, then we may write $\Gamma \vdash \phi_n$.

For example, given the set of assumptions $\Gamma = \{p\}$, we may prove that $q \to p$ using the Hilbert-style proof system, as demonstrated below.

1. $p \to (q \to p)$ (Axiom I)

2. p (Assumption)

3. $q \to p$ (modus ponens, via 1 and 2)

Proving with assumptions can be quite tricky due to the *principle of explosion*[6], which states that any statement can be proven from a contradiction. In other words, it is possible to prove any given statement, true or false, using a proof system as long as at least one of the assumptions in Γ is false.

We shall illustrate this principle as follows. Let Γ be the set containing the invalid assumption $\neg(q \to q)$. We will use the Hilbert-style proof system to prove an arbitrary formula p under this assumption.

5. $q \to q$ (proven previously)

6. $(q \to q) \to \neg\neg(q \to q)$ (Axiom IV, replacing p by q)

7. $\neg\neg(q \to q)$ (modus ponens, via 5 and 6)

8. $\neg\neg(q \to q) \to (\neg p \to \neg\neg(q \to q))$ (Axiom I, replacing p, q by $\neg\neg(q \to q), \neg p$)

9. $\neg p \to \neg\neg(q \to q)$ (modus ponens, via 7 and 8)

10. $(\neg p \to \neg\neg(q \to q)) \to (\neg(q \to q) \to p)$ (Axiom III, replacing p, q by $p, \neg\neg(q \to q)$)

11. $\neg(q \to q) \to p$ (modus ponens, via 9 and 10)

12. $\neg(q \to q)$ (assumption)

13. p (modus ponens, via 11 and 12)

2.3 Soundness, completeness and termination

A proof system is said to be *sound* if it can only prove valid theorems. In other words, anything proven using a sound system must be valid.

$$\underbrace{\vdash \phi}_{\text{proven}} \implies \underbrace{\models \phi}_{\text{valid}} \qquad \text{(soundness)}$$

Conversely, a proof system is said to be *complete* if it can prove any given valid theorem. In other words, if a formula is valid, it must be possible to prove it under a complete system.

$$\underbrace{\models \phi}_{\text{valid}} \implies \underbrace{\vdash \phi}_{\text{proven}} \qquad \text{(completeness)}$$

The main problem with the Hilbert-style proof system is that although it is relartively easy to check that a proof of a formula is correct, there is no systematic way for efficiently constructing proofs.

Moreover, even if a system is sound and complete, we don't know how long the proof for a given formula might be. Since it is impossible for us to check all the possibilities to see if a proof exists, testing the validity of a formula remains undecidable — there is no effective method for determining validity that terminates in finite time.

[6] This principle is sometimes referred to in Latin as *ex falso quodlibet*, which literally translates to "from falsehood, anything [follows]".

3 Propositional tableau

In view of the impracticality of Hilbert-style proof systems, we introduce below an easier and more implementable method for determining a formula's validity — *tableaus.*

Here is a brief overview of how a tableau works. Suppose we want to check the satisfiability of a formula ϕ. This formula will be placed at the root of a binary tree, called a tableau. We use a variety of expansion rules to grow the tree until it is complete. An *open* tableau indicates that ϕ is satisfiable, while a *closed* tableau indicates that ϕ is unsatisfiable.

To determine the validity of a formula, simply construct a tableau for $\neg\phi$. If the resultant tableau is open, then $\neg\phi$ is satisfiable, so ϕ is invalid. On the contrary, if the resultant tableau is closed, then $\neg\phi$ must be unsatisfiable, so ϕ is valid.

3.1 Constructing a tableau

In a tableau, every node is marked with a formula. To build a tableau for a formula ϕ, begin by placing ϕ at the root of a binary tree. Then, we repeat the following process:

1. Select a formula in the tree that has not been selected before. The formula must not be a literal.
2. Choose the expansion rule (see below) that applies to the selected formula.
3. For each leaf node, add new children nodes in accordance to the chosen expansion rule.
4. Place a tick beside the selected formula to make sure we don't expand it again.

There are two types of expansion rules:

- α-rules, which create one new child per leaf node; and
- β-rules, which create two new children per leaf node.

Figures 5 and 6 depict the α- and β rules respectively. Nodes that are newly created by each rule are highlighted in blue.

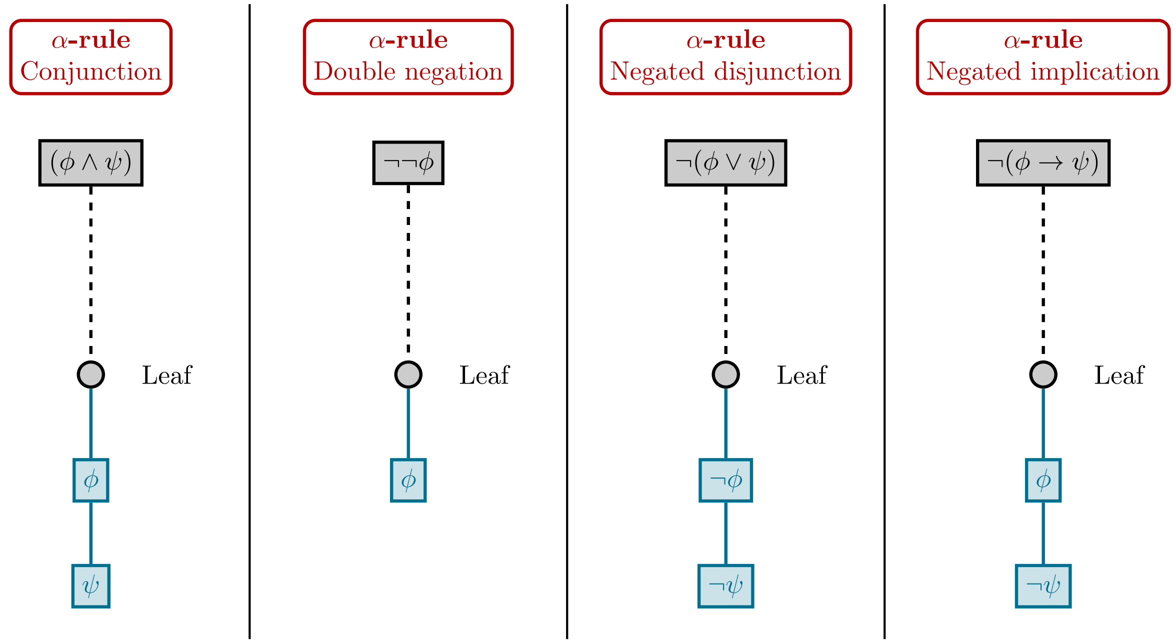


Figure 5: The four α-rules for constructing propositional tableaus.

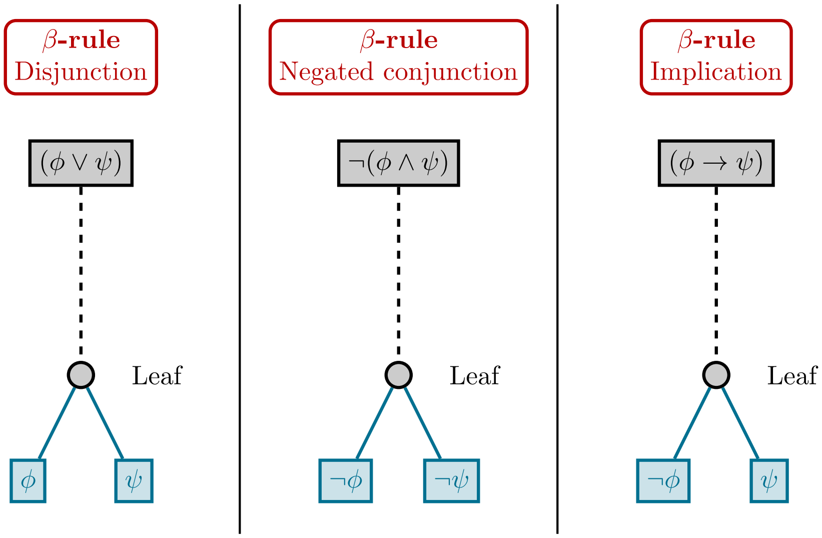


Figure 6: The three β-rules for constructing propositional tableaus.

In general, nodes located in the same branch[7] are considered in conjunction while the different branches are considered to be disjuncted. As a result, a tableau is a tree-like representation of a formula that is a disjunction of conjunctions, à la disjunctive normal form (DNF).

A tableau is considered *complete* if every node is either ticked (already expanded) or a literal. When a tableau is complete, we can determine the original formula's satisfiability as follows.

- A branch containing both a propositional letter and its negation (p and $\neg p$) is said to be *closed*, which we denote as $\oplus$. Otherwise, it is *open*.

- A tableau where all branches are closed is said to be *closed*, meaning that the formula at its root is unsatisfiable. Contrarily, a tableau with at least one open branch is said to be *open*, indicating that the formula is satisfiable.

3.2 Example of constructing a tableau and converting to DNF

To check if the formula

$$((p \lor q) \land (\neg p \to \neg q))$$

is satisfiable, we construct its tableau, as shown in figure 7.

Since only one of the four branches is closed, this formula is satisfiable. In fact, the literals in each open branch give a possible valuation that satisfies the given formula. For instance, the second branch from the left contains the literals p and $\neg q$. This indicates that the formula is true when p is true and q is false.

[7] A *branch* is defined as a path from the root of the tableau to one of its leaves.

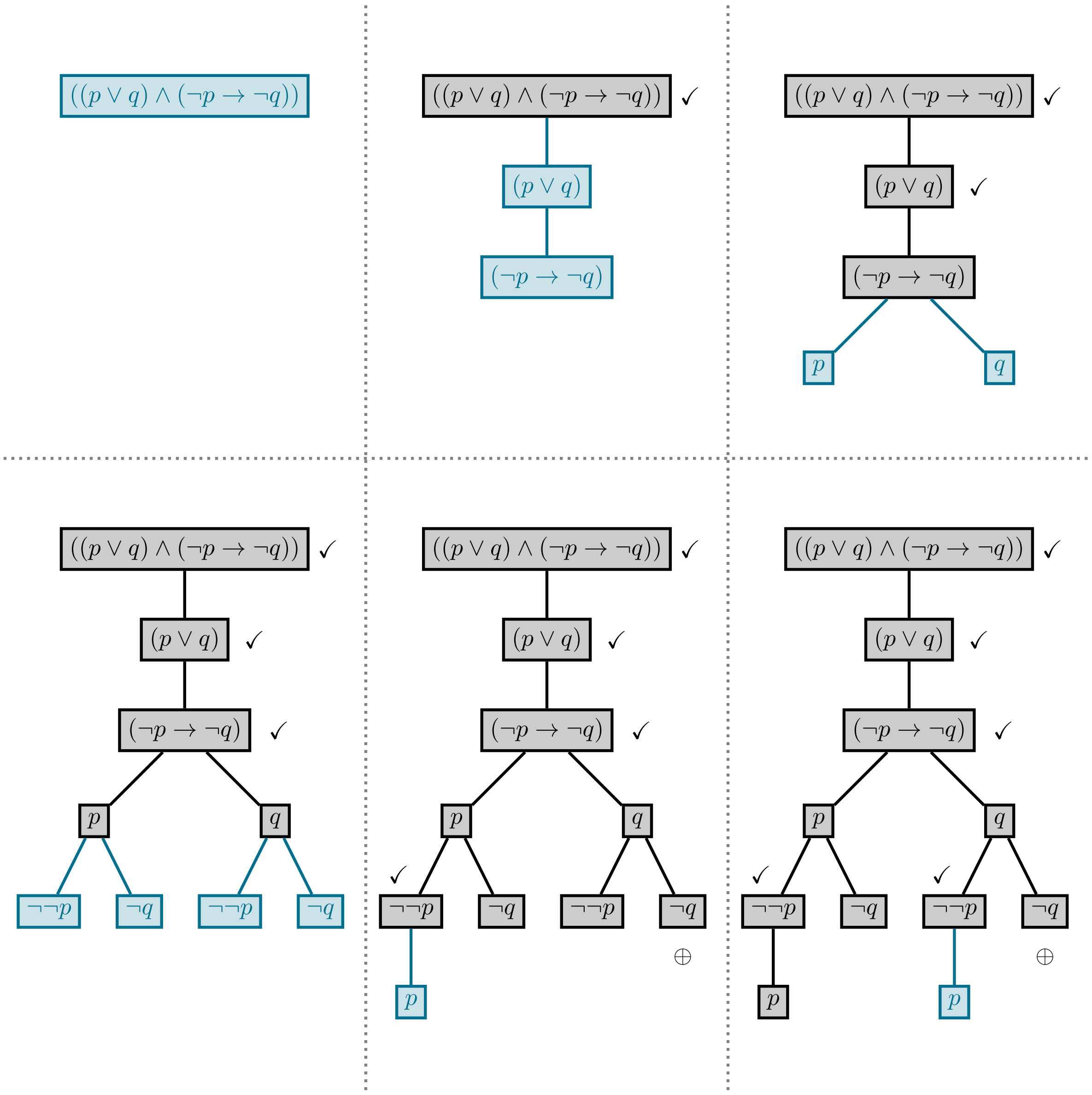


Figure 7: Constructing the tableau of $((p \lor q) \land (\neg p \to \neg q))$. Read from left to right and from top to bottom.

It follows that given the tableau of a formula, its DNF equivalent can be expressed as

$$\bigvee_{\text{open branch }\Theta} \left(\bigwedge \{\text{literals in } \Theta\} \right).$$

As always, the CNF of a formula can be obtained by negating the DNF form of its negation.

4 Predicate tableau

In first-order logic, a *literal* is an atom or its negation, i.e.

$$r^n(t_1, t_2, \cdots, t_n)$$

or

$$\neg r^n(t_1, t_2, \cdots, t_n)$$

where r^n is an n-ary predicate and t_i is a term.

The method for tableau construction in first-order logic is identical to that in propositional logic, but with a few extra expansion rules for dealing with quantifiers.

4.1 Expansion rules

In addition to α- and β-rules, we also require δ- and γ-rules, as depicted in Figures 8 and 9.

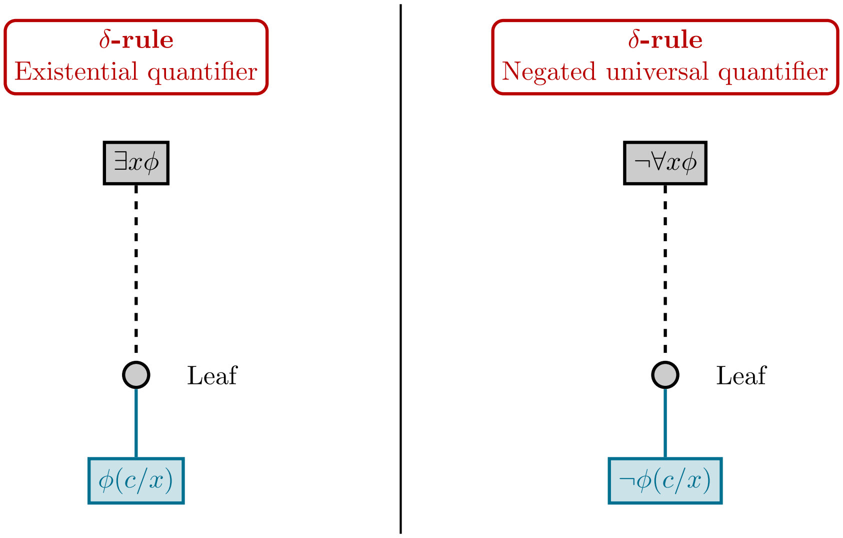


Figure 8: The two δ-rules for constructing predicate tableaus. In both rules, c should be a new constant that has not been used in the tableau before.

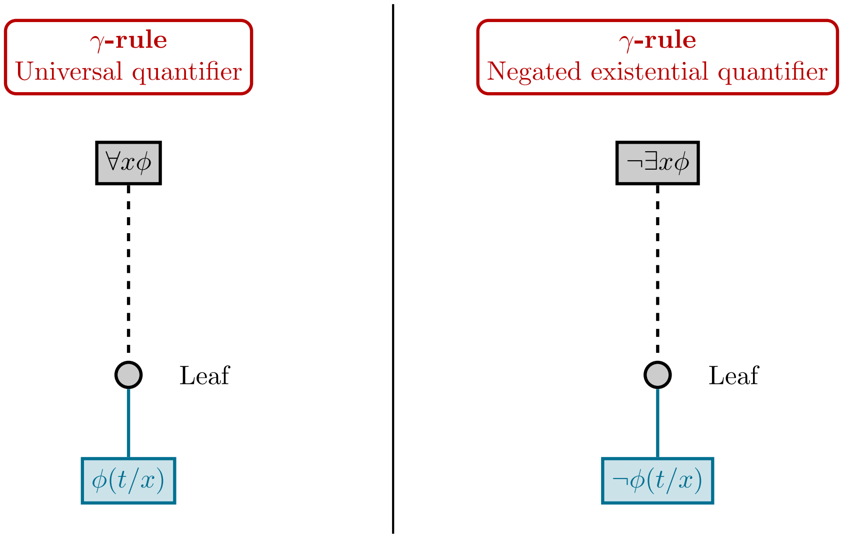


Figure 9: The two γ-rules for constructing predicate tableaus. In both rules, t is a closed term. Formulas should **not** be ticked following a γ-rule expansion.

When applying a δ-rule, make sure to introduce a new constant symbol that is not used anywhere before in the tableau. This new constant acts as a *witness*[8] for the existential statement.

Compared to the other rules, γ-rules are usually applied last. When applying a γ-rule, instantiate x with a closed term that appeared earlier in the current branch[9]. Formulas expanded via a γ-rule should **not** be ticked.

4.2 Termination

Similar to propositional tableaus, a predicate tableau's branch is closed if it contains both a literal $P(t_1, t_2, \cdots, t_n)$ and its negation $\neg P(t_1, t_2, \cdots, t_n)$. Otherwise, it is open.

The tableau terminates when:

- Every branch is closed. This shows that the root formula is unsatisfiable.
- All formulas are fully expanded and no further rules can be applied. If at least one branch remains open and cannot be further expanded, the tableau is open, indicating the root formula's satisfiability.

4.3 Example

Suppose we want to check whether the formula

$$(\forall x\ \neg p(x) \rightarrow \neg\exists y\ p(y))$$

is valid. To do this, we place its negation at the root of our tableau.

[8] Or: *Skolem witness.*

[9] This closed term should **not** be new.

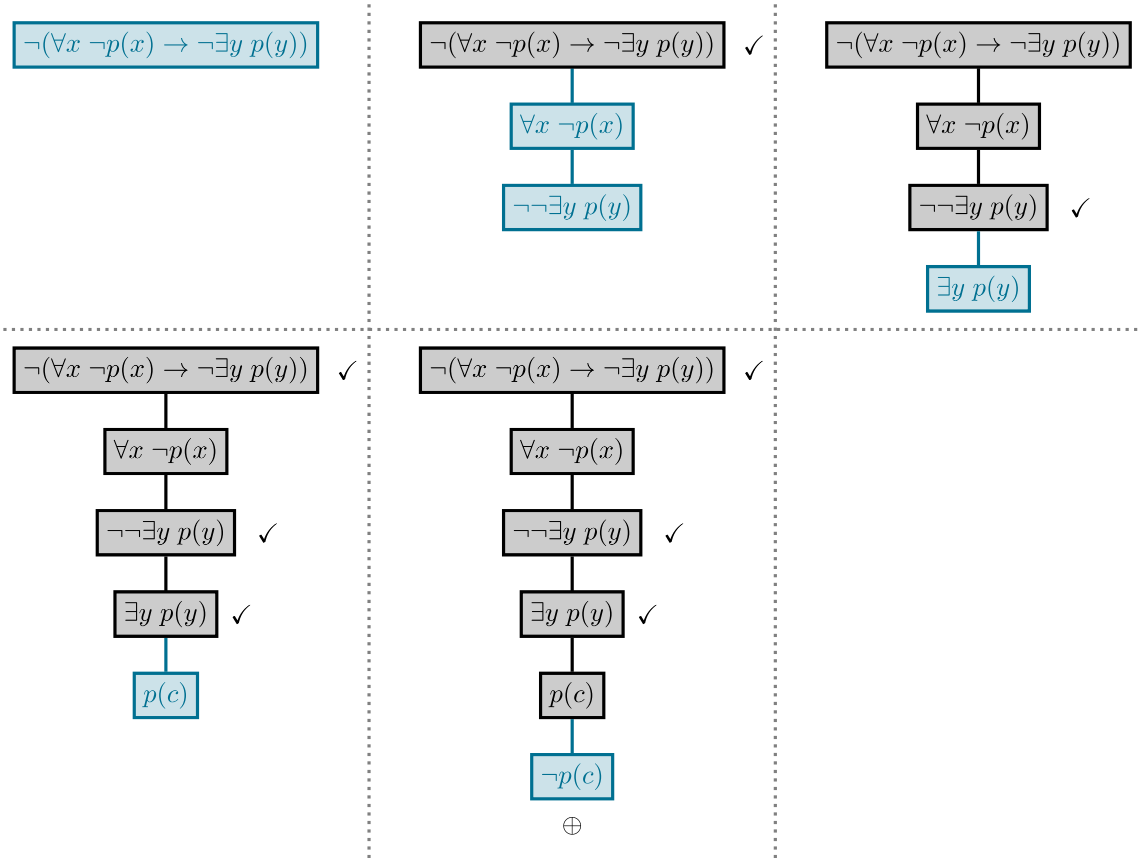


Figure 10: Constructing the tableau of $\neg(\forall x\ \neg p(x) \rightarrow \neg\exists y\ p(y))$. Read from left to right and from top to bottom. In the fourth step (bottom left), the existential formula $\exists y\ p(y)$ is expanded via a δ-rule by introducing a new constant c. In the last step (bottom middle), the universal formula $\forall x\ \neg p(x)$ is expanded via a γ-rule by replacing all bounded instances of x with the closed term c from earlier in the current branch, thereby producing both $p(c)$ and $\neg p(c)$ in the same branch. This results in a closed branch and hence a closed tableau, indicating that the formula at the root is unsatisfiable.

As shown, the negation $\neg(\forall x\ \neg p(x) \rightarrow \neg\exists y\ p(y))$ is unsatisfiable. This means that our original formula must be valid.

4.4 Non-termination

Predicate tableaus may not always terminate.

For instance, if a tableau unendingly generates nodes that require expansion via δ-rules, more and more constants would be introduced, and the number of γ-rule applications required would increase dramatically. This may result in non-termination.

Before we elaborate on this non-terminating scenario, we must note that in order to systematically handle possibly infinite expansions, we should adopt a fair application strategy. A tableau construction is *fair* if

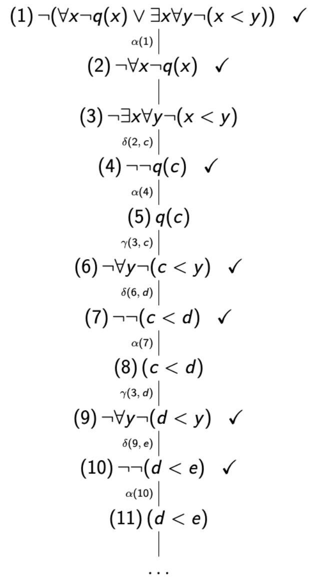
- Every formula that can be expanded eventually will be, and
- Every formula that falls under a γ-rule will eventually be instantiated via that rule using all closed terms that appear in its branch.

This ensures that if the tableau can close, it will close after finitely many steps. We won't miss a contradiction because we ignored a rule.

Now, assuming a fair application strategy,

- If a branch keeps repeating the same configuration of formulas over and over with no new information, it is effectively saturated. This branch is then considered open, meaning that the root formula is satisfiable. This is because we may construct an infinite model for the root formula by reading off literals in the limit of the infinitely "looping" branch in the same way as we did for propositional tableaus. See Figure 11 for an example.

- If a branch runs indefinitely without closure, the satisfiability of the root formula is **undecided** and **inconclusive**.



Open tableau — the tableau will never close, hence the **root formula is satisfiable and the original formula is not valid.**

Figure 11: A non-terminating tableau where the root formula is satisfiable.

4.5 Free variables

Predicate tableaus are predominantly designed to work on sentences, where free variables are not allowed. To prove the validity of a formula with free variables, we may prefix it with an appropriate universal quantifier. For instance, if we want to show that

$$x < 5$$

is valid, where x is a free variable. Notice that this is equivalent to showing the validity of

$$\forall x \; x < 5$$

which uses a universal quantifier to remove the free variable. Consequently, we can simply construct a tableau with

$$\neg\forall x \; x < 5$$

at its root and check its satisfiability as usual.

4.6 More on fairness

Note that when applying expansion rules in non-terminating predicate tableaus, it is always possible to find a fair application strategy.

To see why this is, consider a countably infinite set of processes $P = \{P_1, P_2, \cdots, P_i, \cdots\}$, each awaiting some input. When a process receives an input, this may result in the creation of a new process, which is subsequently added to P. We want to find some fair schedule where if any process P_i is awaiting input at time t, then eventually at some time $t' > t$ it will receive some input.

Since the set P always remains countable even when a new process is created and added to it, such a schedule must exist.

5 More on tableaus, their representations and their properties

5.1 Preliminaries: On subsets and subformulas

In this subsection, we present two lemmas on subsets and subformulas. Given a formula ϕ, a subformula is a substring of ϕ that is also a formula.

Lemma. *A set S of cardinality n has 2^n subsets.*

Proof. To construct a subset $S' \subseteq S$, each element of S can either appear or not appear in S'. This involves a total of n independent binary choices. Hence, there are 2^n possible subsets. □

Lemma. *A formula ϕ has at most $|\phi|$ subformulas.*

Proof. Consider the parse tree of ϕ, where every node contains exactly one symbol and is the root of a subtree that represents a subformula of ϕ. Hence we have

$$\begin{aligned}
&\text{Number of subformulas of } \phi \\
=\ &\text{Number of nodes in parse tree of } \phi \\
=\ &\text{Number of symbols that appear in parse tree of } \phi \\
\leq\ &\text{Number of symbols in } \phi \qquad\qquad \text{(as brackets do not appear in parse trees)} \\
=\ &|\phi|. \qquad\qquad \square
\end{aligned}$$

5.2 Tableaus as lists of theories

While tableaus can be visualised as trees, they can also be represented as lists. To see how this works, let us first review the α- and β- rules. As shown in tables 4 and 5, each α-rule produces at most two new nodes α_1 and α_2, while each β-rule produces at most two new nodes β_1 and β_2.

α	α_1	α_2
$(A \wedge B)$	A	B
$\neg(A \vee B)$	$\neg A$	$\neg B$
$\neg(A \to B)$	A	$\neg B$
$\neg\neg A$	A	-

Table 4: The α-rules tabulated.

β	β_1	β_2
$(A \vee B)$	A	B
$(A \to B)$	$\neg A$	B
$\neg(A \wedge B)$	$\neg A$	$\neg B$

Table 5: The β-rules tabulated.

Instead of a tree, we represent a tableau as a list of *theories*, where each theory is a set of unticked formulas in a branch that has not yet closed. Figure 12, based on Figure 7, shows the construction of a propositional tableau in both tree and list form.

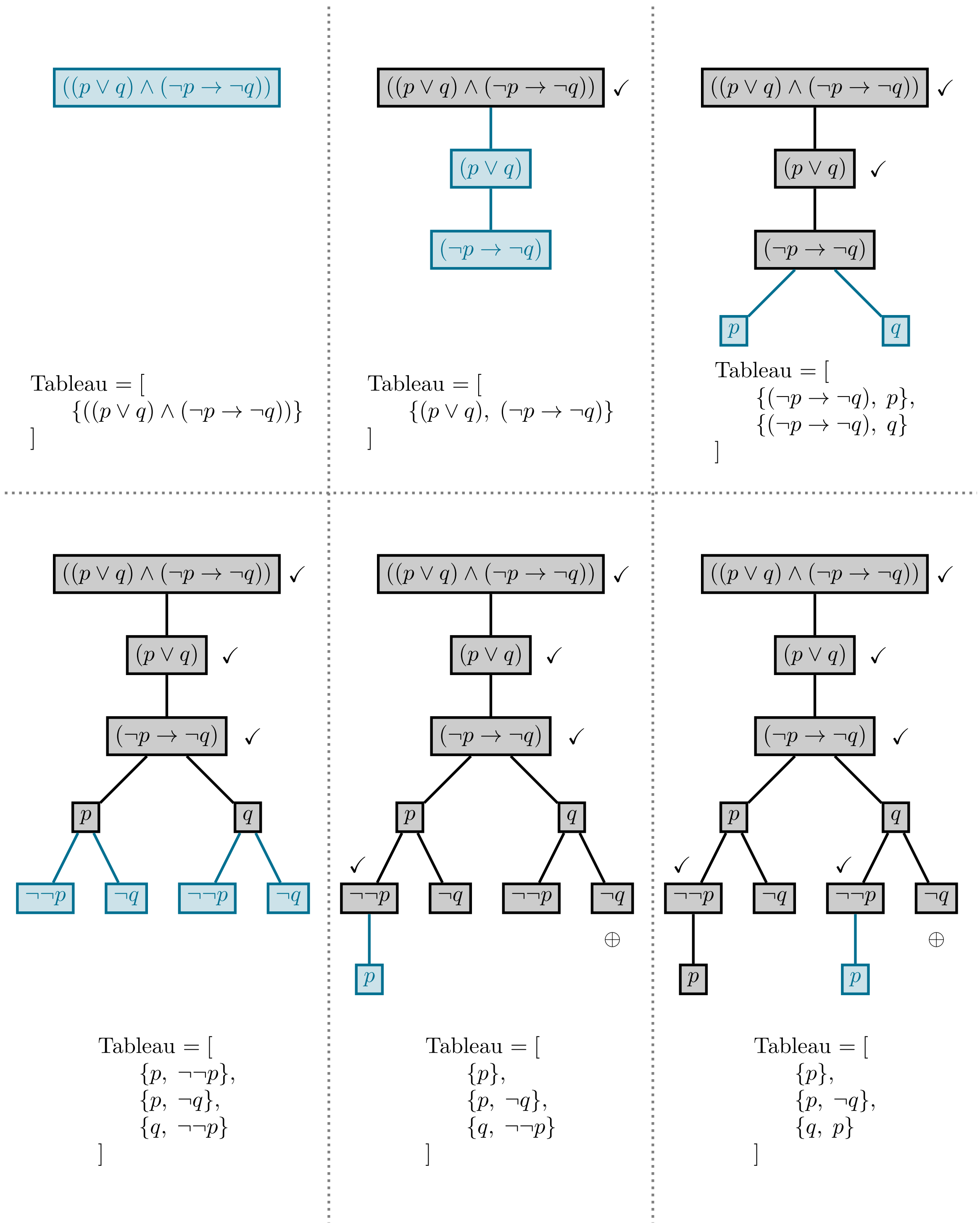


Figure 12: Constructing the tableau of $((p \lor q) \land (\neg p \to \neg q))$ as a tree and as a list. Read from left to right and from top to bottom.

Below is a pseudocode snippet outlining how the propositional tableau method can be implemented programmatically using the list representation. Here, `Tableau` is initialised as a queue of theories. The variables α_1, α_2, β_1 and β_2 refer to the ones labelled in Tables 4 and 5.

```
def is_satisfiable($\phi$):
    Tableau = Queue()
    Tableau.enqueue($\phi$)

    while Tableau is not empty:
        # Dequeue a theory $\Sigma$ from the tableau
        $\Sigma$ = Tableau.dequeue()

        if $\Sigma$ is fully expanded and has no contradictory literals:
            return True
        else:
            fairly select a non-literal $\psi$ from $\Sigma$

            if $\alpha$-rule is applicable to $\psi$:
                $\Sigma$ = $\Sigma$ with $\psi$ replaced by $\alpha_1$ and $\alpha_2$
                if $\Sigma$ has no contradictory literals and is not in Tableau:
                    Tableau.enqueue($\Sigma$)

            elif $\beta$-rule is applicable to $\psi$:
                $\Sigma_1$ = $\Sigma$ with $\psi$ replaced by $\beta_1$
                if $\Sigma_1$ has no contradictory literals and is not in Tableau:
                    Tableau.enqueue($\Sigma_1$)

                $\Sigma_2$ = $\Sigma$ with $\psi$ replaced by $\beta_2$
                if $\Sigma_2$ has no contradictory literals and is not in Tableau:
                    Tableau.enqueue($\Sigma_2$)

    # Empty queue in Tableau
    return False
```

We can easily modify this algorithm to represent predicate tableaus by adding the following cases to the innermost `if-elif` statement.

```
elif $\delta$-rule is applicable to $\psi$:
    if $\psi = \exists x \, \theta(x)$:
        $\Sigma$ = $\Sigma$ with $\psi$ replaced by $\theta(c)$ for some new constant $c$
    elif $\psi = \neg\forall x \, \theta(x)$:
        $\Sigma$ = $\Sigma$ with $\psi$ replaced by $\neg\theta(c)$ for some new constant $c$

    if $\Sigma$ has no contradictory literals and is not in Tableau:
        Tableau.enqueue($\Sigma$)

elif $\gamma$-rule is applicable to $\psi$:
    if $\psi = \forall x \, \theta(x)$:
        fairly select a closed term $t$ from $\Sigma$
        $\Sigma$ = $\Sigma$ with $\theta(t)$ added
    elif $\psi = \neg\exists x \, \theta(x)$:
        fairly select a closed term $t$ from $\Sigma$
        $\Sigma$ = $\Sigma$ with $\neg\theta(t)$ added

    if $\Sigma$ has no contradictory literals and is not in Tableau:
        Tableau.enqueue($\Sigma$)
```

5.3 Proving the termination and soundness of tableaus

Here we will use the list representation of tableaus to prove several of their properties.

Theorem. *The propositional tableau algorithm must terminate for any root formula ϕ.*

Proof. Let X be the set of subformulas of ϕ and negations thereof. Double negations of subformulas are excluded. Since ϕ has at most $|\phi|$ subformulas, the cardinality of X cannot exceed $2|\phi|$.

Notice that any theory in the tableau of ϕ must be a subset of X. Since each theory can only be enqueued to the tableau at most once, the number of enqueued theories must not exceed $2^{2|\phi|}$. Therefore, the algorithm must terminate in no more than $2^{2|\phi|}$ steps. □

Theorem. *The propositional tableau algorithm is sound.*

Proof. To prove soundness, we must show that $\vdash \phi \implies \models \phi$, i.e.

$$\text{Tableau of } \neg\phi \text{ is closed} \implies \neg\phi \text{ is unsatisfiable.}$$

Taking the contrapositive and renaming our variables, we see that this is equivalent to showing that

$$\phi \text{ is satisfiable} \implies \text{tableau of } \phi \text{ never closes.}$$

Assume ϕ is satisfiable. This means there is some truth function v for which $v(\phi) = \top$. We want to prove by induction that the following statement $P(n)$ holds for any $n \in \mathbb{N}$.

Statement. After executing n iterations of the `while` loop, there exists a theory Σ in the tableau where $\theta \in \Sigma \to v(\theta) = \top$.

Base case. When $n = 0$, the tableau is given by $[\{\phi\}]$. The base case holds trivially by taking $\Sigma = \{\phi\}$ and noting $v(\phi) = \top$.

Step case. Assume $P(n)$ holds for some $n \in \mathbb{N}$. This means that after n iterations there exists some Σ in the tableau where $\theta \in \Sigma \to v(\theta) = \top$. For $P(n+1)$, consider executing an additional iteration.

- If any theory other than Σ is dequeued, Σ will still remain in the tableau unchanged by the end of the iteration. Therefore, $P(n+1)$ holds.
- If Σ is dequeued and a non-literal $\psi \in \Sigma$ is selected, we have $v(\psi) = \top$ (by induction hypothesis).
  - If an α-rule is applicable to ψ, then ψ will be replaced by two formulas α_1 and α_2 which — according to properties of truth functions — satisfy $v(\alpha_1) = v(\alpha_2) = \top$. Therefore, the statement $\theta \in \Sigma[\psi/\{\alpha_1, \alpha_2\}] \to v(\theta) = \top$ is still true.
  - If a β-rule is applicable to ψ, then we enqueue two new theories: Σ_1 where ψ is replaced by β_1; and Σ_2 where ψ is replaced by β_2. According to properties of truth functions, at least one of $v(\beta_1) = \top$ and $v(\beta_2) = \top$ is true. Therefore, we have either $\theta \in \Sigma_1 \to v(\theta) = \top$ or $\theta \in \Sigma_2 \to v(\theta) = \top$.

Hence proved. □

Theorem. *The predicate tableau algorithm is sound.*

Proof. Similar to the above, we want to show that

$$\phi \text{ is satisfiable} \implies \text{tableau of } \phi \text{ never closes.}$$

Assume ϕ is satisfiable. This means there is some first-order structure S and variable assignment A for which $S \models_A \phi$. We want to prove by induction that the following statement $P(n)$ holds for any $n \in \mathbb{N}$.

Statement. After executing n iterations of the `while` loop, there exists a theory Σ in the tableau where $\theta \in \Sigma \to S \models_A \theta$ for some structure S and variable assignment A.

Base case. When $n = 0$, the tableau is given by $[\{\phi\}]$. The base case holds trivially by taking $\Sigma = \{\phi\}$ and noting $S \models_A \phi$.

Step case. Assume $P(n)$ holds for some $n \in \mathbb{N}$. This means that after n iterations there exists some Σ in the tableau where $\theta \in \Sigma \to S \models_A \phi$ for some structure S and variable assignment A. For $P(n+1)$, consider executing an additional iteration.

- If any theory other than Σ is dequeued, Σ will still remain in the tableau unchanged by the end of the iteration. Therefore, $P(n+1)$ holds.

- If Σ is dequeued and a non-literal $\psi \in \Sigma$ is selected, we have $S \models_A \psi$ (by induction hypothesis).

  - If an α-rule is applicable to ψ, then ψ will be replaced by two formulas α_1 and α_2 which — according to properties of truth functions — satisfy $S \models_A \alpha_1$ and $S \models_A \alpha_2$. Therefore, the statement $\theta \in \Sigma[\psi/\{\alpha_1, \alpha_2\}] \to S \models_A \theta$ is still true.

  - If a β-rule is applicable to ψ, then we enqueue two new theories: Σ_1 where ψ is replaced by β_1; and Σ_2 where ψ is replaced by β_2. According to properties of truth functions, at least one of $S \models_A \beta_1$ and $S \models_A \beta_2$ is true. Therefore, we have either $\theta \in \Sigma_1 \to S \models_A \theta$ or $\theta \in \Sigma_2 \to S \models_A \theta$.

  - If a δ-rule is applicable to ψ, then it is either of the form $\exists x\ \theta(x)$ or $\neg\forall x\ \theta(x)$.

    For $\exists x\ \theta(x)$, we know by induction hypothesis that $S \models_A \exists x\ \theta(x)$. This means there exists some s within the domain of S such that $S \models_{A[x \to s]} \theta(x)$. The δ-rule replaces ψ with $\theta(c)$ where c is a new constant. Let S' be a first-order structure identical to S except $I(c) = s$. Then $S' \models_A \Sigma[\exists x\ \theta(x)/\theta(c)]$ holds.

    A similar argument can be made for $\neg\forall x\ \theta(x)$, but is omitted here for brevity.

  - If a γ-rule is applicable to ψ, then it is either of the form $\forall x\ \theta(x)$ or $\neg\exists x\ \theta(x)$.

    For $\forall x\ \theta(x)$, we know by induction hypothesis that $S \models_A \forall x\ \theta(x)$. It follows that $S \models_A \theta(t)$ for any closed term t. Therefore, the statement $\theta \in \Sigma[\psi/\theta(t)]$ is still true.

    A similar argument can be made for $\neg\exists x\ \theta(x)$, but is omitted here for brevity.

    Note that unlike in the δ-rule case, this case does not involve the modification of S or A.

Hence proved. □

5.4 Hypotheses

Similar to how assumptions can be added to axiomatic proof systems, we can use tableaus to prove from *hypotheses*. Suppose we want to show that the formula ϕ is valid under a set of hypotheses $\Gamma = \{\gamma_0, \gamma_1, \gamma_2, \cdots, \gamma_{n-1}\}$. There are several ways of doing this via tableaus.

- **As a tree:** Place $\neg\phi$ at the root of a tableau. Continue to construct the tableau as usual, but with the additional rule that at any stage we may select some hypothesis $\gamma_i \in \Gamma$ and add a node labelled γ_i at any leaf.

- **As a tree, assuming a finite set of hypotheses:** Place $\neg\phi$ along with all hypotheses $\gamma_0, \gamma_1, \gamma_2, \cdots, \gamma_{n-1}$ all in a single tableau branch. Continue to construct the tableau as usual.

- **As a list/queue:** Initialise the tableau as $[\Gamma \cup \{\neg\phi\}]$. Continue to construct the tableau as usual.

If the tableau eventually closes (or becomes empty, in the case of the list/queue representation), we may write

$$\Gamma \vdash \phi$$

to denote that ϕ is valid under the hypotheses Γ.

5.5 Equality rules

Recall that in predicate logic, the equality symbol “=” is always interpreted as true equality. Therefore, when constructing a tableau for a formula containing an equality symbol, we must also assume the following equality rules.

- If in some branch we have both $A(t)$ and $t = s$, then we may add $A(s)$ to its leaf.

- If in some branch we have both $A(t)$ and $s = t$, then we may add $A(s)$ to its leaf.

- If a branch contains a formula in the form $\neg(t = t)$, that branch is closed.

For example, suppose we want to prove that under the hypothesis $s = t$, the formula $t = s$ is valid, i.e.

$$s = t \vdash t = s.$$

We set up a tableau containing the hypothesis, followed by the formula’s negation. We then complete the tableau as normal. See Figure 13.

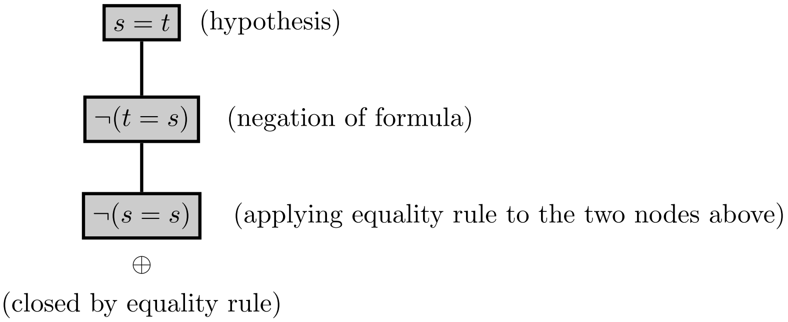


Figure 13: Proving the validity of $s = t \vdash t = s$ by constructing a predicate tableau using equality rules.

5.6 Parents and ancestors

If a theory Σ in the tableau is dequeued and a new theory Σ_1 (and possibly Σ_2) is subsequently enqueued, then Σ is a *parent* of Σ_1 and Σ_2. We denote this relationship using the function P, defined as follows.

$$\begin{aligned} P(\Sigma) &= \Sigma' \qquad \text{if the parent of } \Sigma \text{ is } \Sigma' \\ P^0(\Sigma) &= \Sigma \\ P^{n+1}(\Sigma) &= P(P^n(\Sigma)) \end{aligned}$$

We say that Σ' is an *ancestor* of Σ' if

$$P^n(\Sigma) = \Sigma'$$

for some $n \in \mathbb{N}$. For example, if a tableau is initialised with only one theory, then that theory is an ancestor of every theory in the tableau, including itself.

5.7 Proving the completeness of propositional tableaus

Theorem. *The propositional tableau algorithm is complete.*

Proof. To prove completeness, we must show that $\models \phi \implies \vdash \phi$, i.e.

$$\neg\phi \text{ is unsatisfiable } \implies \text{ tableau of } \neg\phi \text{ is closed.}$$

Taking the contrapositive and renaming our variables, we see that this is equivalent to showing that

$$\text{Tableau of } \phi \text{ does not close } \implies \phi \text{ is satisfiable.}$$

Assume that the tableau of ϕ does not close. This means that there is some theory in the tableau that, when dequeued, is found to be fully expanded and have no contradictory literals, thus causing `is_satisfiable(`ϕ`)` to return `True`. We denote this theory by Σ.

Let v be a valuation where for each propositional letter p, we have

$$v(p) = \top \iff p \in \Sigma.$$

Extending v to a truth function, it follows that

$$\phi \in \Sigma \implies v(\phi) = \top \qquad (*)$$

for all formulas ϕ.

We shall now prove by induction that the statement

$$\phi \in P^n(\Sigma) \implies v(\phi) = \top$$

is true for all $n \in \mathbb{N}$.

Base case. For $n = 0$, we want to show that $\phi \in P^0(\Sigma) \implies v(\phi) = \top$. This was already established by equation (*).

Step case. Assume for some $n \in \mathbb{N}$ that the theory $P^n(\Sigma)$ satisfies $\phi \in P^n(\Sigma) \implies v(\phi) = \top$. Now consider its parent $P^{n+1}(\Sigma)$. We know that some expansion rule — α or β — is used to replace some formula in the parent theory $P^{n+1}(\Sigma)$ with a new formula to form the child theory $P^n(\Sigma)$.

- If this is an α-rule, then both formulas α_1 and α_2 will be present in the child theory $P^n(\Sigma)$. By the induction hypothesis, we have $v(\alpha_1) = v(\alpha_2) = \top$, so $v(\alpha) = \top$.

- If this is an β-rule, then one of the formulas β_1 and β_2 will be present in the child theory $P^n(\Sigma)$. By the induction hypothesis, we have either $v(\beta_1) = \top$ or $v(\beta_2) = \top$. In either case we have $v(\beta) = \top$.

Since no other formulas are changed when generating $P^n(\Sigma)$ from $P^{n+1}(\Sigma)$, we have $\phi \in P^{n+1}(\Sigma) \implies v(\phi) = \top$, establishing the step case.

By the principles of induction, we have

$$\phi \in P^n(\Sigma) \implies v(\phi) = \top$$

for all $n \in \mathbb{N}$. Since the initial theory $\{\phi\}$ is the ancestor of all theories in the tableau, we have $v(\phi) = \top$, implying satisfiability. □

5.8 Herbrand structures

A closed term contains only constant symbols and function symbols, with no free variables. A *Herbrand structure* is a first-order structure $H = (D, I)$ where

- the domain D is defined as the set of closed terms; and
- the interpretation $I = (I_c, I_f, I_p)$ is such that

$$I_c(c) = c \qquad \text{(interpret each constant symbol as the symbol itself)}$$
$$I_f(f^n(d_1, d_2, \cdots, d_n)) = f^n(d_1, d_2, \cdots, d_n) \qquad \text{(interpret each function as the string itself)}$$

  and I_p can be chosen freely.

It follows that for any closed term t and any variable assignment[10] A, we have $[t]^{H,A} = t$.

Herbrand's theorem, which we will not prove here, states that if ϕ does not contain the equality symbol "=" but is satisfiable in some structure S and variable assignment A, then it must also be satisfiable in some Herbrand structure H and variable assignment B.

5.9 Ranks

We define the *rank* of a first-order formula ϕ, denoted as $\text{Rk}(\phi)$, as follows.

$$\begin{aligned}
\text{Rk}(P(t_0, t_1, \cdots, t_{k-1})) &= 1 \\
\text{Rk}(\neg\phi) &= \text{Rk}(\phi) + 1 \\
\text{Rk}(\phi \circ \psi) &= \text{Rk}(\phi) + \text{Rk}(\psi) + 1 \qquad \text{(where } \circ \text{ is a binary connective)} \\
\text{Rk}(\exists x\ \phi) &= \text{Rk}(\phi) + 1 \\
\text{Rk}(\forall x\ \phi) &= \text{Rk}(\phi) + 1
\end{aligned}$$

In other words, $\text{Rk}(\phi)$ is number of nodes in the parse tree of ϕ.

5.10 Proving the completeness of the predicate tableaus

Lemma (König's Tree Lemma)**.** *Let T be a tree where each node has only finitely many immediate successors. If each branch is of finite length, then the number of nodes in the tree is finite.*

Proof. We prove the contrapositive of the lemma: Assuming that T has infinitely many nodes, it must contain an infinite branch.

Assume T has infinitely many nodes. Let P be a path starting at the root of T. We say that a node n in T is *bottomless* if there are infinitely many nodes below n in the tree. It follows that the root of T is bottomless.

Recall that each node has only finitely many immediate successors. Therefore, the root must only have finitely many (immediate) children. If all of these children are not bottomless, then they must all have finitely many children, which contradicts the fact that the root is bottomless and has infinitely many nodes beneath it[11]. Hence, the root has at least one bottomless child. Select any one of these bottomless children and append it to the path P.

This process of selecting a bottomless child of the last node of P and then adding it to P can be repeated indefinitely to create an infinite branch. □

Theorem. *Predicate tableaus are complete.*

[10] The variable assignment here is irrelevant since t is a closed term.

[11] This is because the sum of a finite number of finite numbers is finite.

Proof. To prove completeness, we must show that $\models \phi \implies \vdash \phi$, i.e.

$$\neg\phi \text{ is unsatisfiable} \implies \text{tableau of } \neg\phi \text{ is closed.}$$

Taking the contrapositive and renaming our variables, we see that this is equivalent to showing that

$$\text{Tableau of } \phi \text{ never closes under fair expansion schedule} \implies \phi \text{ is satisfiable.}$$

Assume the tableau of a formula ϕ never closes under a fair expansion schedule. By the contrapositive of König's Tree Lemma, there must exist an infinite sequence of theories $\Sigma_0, \Sigma_1, \Sigma_2, \cdots$ from the tableau where $\Sigma_n = P(\Sigma_{n+1})$. Let $\Sigma = \cup_{n\in\mathbb{N}} \Sigma_n$. Since a fair schedule is used, we have

$$\begin{aligned}
\alpha \in \Sigma &\implies \alpha_1 \in \Sigma \text{ and } \alpha_2 \in \Sigma \\
\beta \in \Sigma &\implies \beta_1 \in \Sigma \text{ or } \beta_2 \in \Sigma \\
\exists x\, \theta(x) \in \Sigma &\implies \theta(c) \in \Sigma \quad \text{for some } c \\
\neg\forall x\, \theta(x) \in \Sigma &\implies \neg\theta(c) \in \Sigma \quad \text{for some } c \\
\forall x\, \theta(x) \in \Sigma &\implies \theta(t) \in \Sigma \quad \text{for all closed terms } t \\
\neg\exists x\, \theta(x) \in \Sigma &\implies \neg\theta(t) \in \Sigma \quad \text{for all closed terms } t.
\end{aligned} \tag{*}$$

Let H be a Herbrand structure where

- the domain is the set of closed terms in Σ;
- $I(t) = t$ for all closed terms t; and
- for each n-ary predicate R^n, let

$$(t_0, t_1, \cdots, t_{n-1}) \in I(R^n) \iff R^n(t_0, t_1, \cdots, t_{n-1}) \in \Sigma.$$

We now prove by complete induction on $\text{Rk}(\theta)$ that for any sentence θ, we have

$$\theta \in \Sigma \implies H \models \theta.$$

Strong induction does not require a base case.

Step case. Assume that for some $n \in \mathbb{N}$, we have

$$\theta \in \Sigma \implies H \models \theta$$

for all formulas θ with $\text{Rk}(\theta) < n$. Now consider a new formula with rank n. By equations (*) and our induction hypothesis, the expansions of this new formula — all of which must have rank strictly less than n — are valid in H. It follows that this new formula is also valid in H, completing the step case.

This shows that $\theta \in \Sigma \implies H \models \theta$. Since $\phi \in \Sigma$, we have $H \models \phi$, so ϕ is satisfiable. □

6 Axiomatic proofs for Predicate Logic

6.1 Recap: Axiomatic proof system for propositional logic

Recall that axiomatic proofs for propositional logic are constructed using the following axiom schemas:

I. $p \to (q \to p)$ (implication is true if consequent is true)

II. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$ (implication chain as hypothetical syllogism)

III. $(\neg p \to \neg q) \to (q \to p)$ (contrapositive)

IV. $p \to \neg\neg p$ and $\neg\neg p \to p$ (double negation)

V. $(\neg p \to q) \leftrightarrow (p \vee q)$ (implication as disjunction)

VI. $\neg(p \to \neg q) \leftrightarrow (p \wedge q)$ (implication as conjunction)

alongside the inference rule modus ponens.

$$\frac{A \quad (A \to B)}{B} \qquad \text{(modus ponens)}$$

For the sake of convenience, we may sometimes want to make use of the deduction theorem. We will prove this theorem later.

$$A \vdash B \iff \vdash (A \to B) \qquad \text{(deduction theorem)}$$

We may also want to incorporate extra inference rules, as listed below.

$$\frac{(A \to B) \quad (B \to C)}{A \to C} \qquad \text{(hypothetical syllogism)}$$

$$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B} \qquad \frac{A \quad B}{A \wedge B} \qquad \frac{A}{A \vee B} \qquad \frac{B}{A \vee B} \qquad \text{(etc.)}$$

6.2 Creating an axiomatic proof system for predicate logic

To adopt this proof system for predicate logic, we must add seven more axiom schemas, as listed below. An instance of an axiom is obtained by replacing $A, B, C, \cdots$ by arbitrary formulas. Axioms VII through IX are quantifier axioms, whereas Axioms X through XIII are equality axioms.

VII. $\forall x \, \neg A \leftrightarrow \neg \exists x \, A$ (negated existential statement)

VIII. $\forall x \, A(x) \to A(t/x)$ if t is substitutable for x in A. (universal statement)

IX. $\forall x \, (A \to B) \to (\forall x \, A \to \forall x \, B)$ (universal implication)

X. $x = x$ (equality is reflexive)

XI. $(x = y) \to (y = x)$ (equality is symmetric)

XII. $(x = y) \to (t(x) = t(y/x))$ (term is unchanged by substitution)

XIII. $(x = y) \to (A(x) \to A(y/x))$ if y is substitutable for x in A.

(predicate's truth value is unchanged by substitution)

A term t is *substitutable* for x in A if no variable in t becomes bound after replacing x in A by t. For instance, if we have

$$t = \text{“}f(y)\text{”}$$
$$A = \text{“}\forall x\ \exists y\ (f(x) = y)\text{”}$$

then we **may not** use Axiom VIII and modus ponens to deduce

$$\exists y(f(f(y) = y)).$$

This is because the originally free instance of y in t (in blue) becomes bound by the existential quantifier in A (in red) after the substitution, which is not allowed.

The axiomatic proof system for predicate logic is made complete by a new inference rule called *universal generalisation*.

$$\frac{A(x)}{\forall x\ A(x)} \tag{universal generalisation}$$

This inference rule states that if $A(x)$ is valid, then $\forall x\ A(x)$ is also valid[12].

We summarise our description of this axiomatic proof system as follows.

Axiomatic proof system for predicate logic

Axiom schemas.

I. $p \to (q \to p)$

II. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$

III. $(\neg p \to \neg q) \to (q \to p)$

IV. $p \to \neg\neg p$ and $\neg\neg p \to p$

V. $(\neg p \to q) \leftrightarrow (p \lor q)$

VI. $\neg(p \to \neg q) \leftrightarrow (p \land q)$

VII. $\forall x\ \neg A \leftrightarrow \neg\exists x\ A$

VIII. $\forall x\ A(x) \to A(t/x)$ if t is substitutable for x in A.

IX. $\forall x\ (A \to B) \to (\forall x\ A \to \forall x\ B)$

X. $x = x$

XI. $(x = y) \to (y = x)$

XII. $(x = y) \to (t(x) = t(y/x))$

XIII. $(x = y) \to (A(x) \to A(y/x))$ if y is substitutable for x in A.

Inference rules.

- Modus ponens.

$$\frac{A \quad (A \to B)}{B}$$

[12] Note that while this rule is sound, $A(x) \implies \forall x\ A(x)$ is not an axiom.

- Universal generalisation.

$$\frac{A(x)}{\forall x\ A(x)}$$

Additional inference rules for convenience.

- Hypothetical syllogism.

$$\frac{(A \to B) \quad (B \to C)}{A \to C}$$

- Nature of AND and OR connectives.

$$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B} \qquad \frac{A \quad B}{A \wedge B} \qquad \frac{A}{A \vee B} \qquad \frac{B}{A \vee B} \qquad \text{(etc.)}$$

Deduction theorem.

$$A \vdash B \iff \vdash (A \to B)$$

Similar to in propositional logic, we define a *proof* to be a finite sequence of formulas

$$\phi_0,\ \phi_1,\ \phi_2,\ \cdots,\ \phi_n$$

such that for each $i \leq n$, the formula ϕ_i is either

- an axiom; or
- obtained from one or two previous formulas — ϕ_j and possibly ϕ_k — in the sequence via an inference rule (for some $j, k < i$).

If such a proof exists, then the final formula ϕ_n is called a *theorem* and we may write $\vdash \phi_n$.

So far, we have only proved the validity of formulas over arbitrary models. If we want to demonstrate validity in a particular model (or type of model), we may add a set of hypotheses Γ. If there is a sequence

$$\phi_0,\ \phi_1,\ \phi_2,\ \cdots,\ \phi_n$$

such that for each $i \leq n$, the formula ϕ_i is either

- an axiom;
- obtained from one or two previous formulas — ϕ_j and possibly ϕ_k — in the sequence via an inference rule (for some $j, k < i$); or
- a hypothesis in Γ,

then we may write $\Gamma \vdash \phi$.

For instance, suppose we want to prove a formula's validity in a *linearly ordered model.* We thus assume the following hypotheses.

- $\forall x\ \forall y\ (x < y \vee y < x \vee x = y)$ (totality)
- $\forall x\ \neg(x < x)$ (irreflexivity)
- $\forall x\ \forall y\ \forall z\ ((x < y \wedge y < z) \to (x < z))$ (transitivity)

Below shows an example of this, where we prove the validity of the formula

$$\forall x\, \forall y\, \neg(x < y \wedge y < x)$$

in a linearly ordered model.

1. $\forall x\, \forall y\, \forall z\, ((x < y \wedge y < z) \to (x < z))$ (hypothesis)
2. $\forall x\, \forall y\, \forall z\, ((x < y \wedge y < z) \to (x < z)) \to \forall y\, \forall z\, ((x < y \wedge y < z) \to (x < z))$ (Axiom VIII, with x as t)
3. $\forall y\, \forall z\, ((x < y \wedge y < z) \to (x < z))$ (modus ponens, via 1 and 2)
4. $\forall y\, \forall z\, ((x < y \wedge y < z) \to (x < z)) \to \forall z\, ((x < y \wedge y < z) \to (x < z))$ (Axiom VIII, with y as t)
5. $\forall z\, ((x < y \wedge y < z) \to (x < z))$ (modus ponens, via 3 and 4)
6. $\forall z\, ((x < y \wedge y < z) \to (x < z)) \to ((x < y \wedge y < x) \to (x < x))$ (Axiom VIII, with x as t)
7. $(x < y \wedge y < x) \to (x < x)$ (modus ponens, via 5 and 6)
8. $((x < y \wedge y < x) \to (x < x)) \to (\neg(x < x) \to \neg(x < y \wedge y < x))$ (instance of $(p \to q) \to (\neg q \to \neg p)$, provable in propositional logic)
9. $\neg(x < x) \to \neg(x < y \wedge y < x)$ (modus ponens, via 7 and 8)
10. $\forall x\, \neg(x < x)$ (hypothesis)
11. $\forall x\, \neg(x < x) \to \neg(x < x)$ (Axiom VIII, with x as t)
12. $\neg(x < x)$ (modus ponens, via 10 and 11)
13. $\neg(x < y \wedge y < x)$ (modus ponens, via 9 and 12)
14. $\forall y\, \neg(x < y \wedge y < x)$ (universal generalisation of y, from 13)
15. $\forall x\, \forall y\, \neg(x < y \wedge y < x)$ (universal generalisation of x, from 14)

6.3 Proving the deduction theorem

Here we will prove a more generalised version of the deduction theorem.

Theorem (Deduction theorem)**.** *Let A and B be sentences. For any (possibly infinite) set of assumptions Σ, a formula B is deducible from the assumptions $\Sigma \cup \{A\}$ if and only if the implication $A \to B$ is deducible from the assumptions Σ. In symbols, we have*

$$\Sigma \cup \{A\} \vdash B \iff \Sigma \vdash (A \to B).$$

Proof. ($\Leftarrow$): Assuming that $\Sigma \vdash (A \to B)$, there must exist a proof

$$\phi_0, \phi_1, \phi_2, \cdots, \phi_n$$

where $\phi_n = A \to B$, and each ϕ_i is an axiom, an element of Σ, or derived from two previous formulas via modus ponens.

We extend this proof as follows.

$$\phi_0, \phi_1, \phi_2, \cdots, \phi_n, A, B$$

Note that this is an acceptable proof of B under the assumptions $\Sigma \cup \{A\}$.

- Each of $\phi_0, \phi_1, \phi_2, \cdots, \phi_n$ is an axiom, an element of Σ, or derived from modus ponens.
- A is an assumption from $\Sigma \cup \{A\}$.
- B is derived from ϕ_n (i.e. $A \to B$) and A via modus ponens.

Hence we have $\Sigma \vdash (A \to B) \implies \Sigma \cup \{A\} \vdash B$.

($\Rightarrow$): Consider the following axiom schematas.

I. $p \to (q \to p)$

II. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$

Assuming that $\Sigma \cup \{A\} \vdash B$, there must exist a proof

$$\phi_0, \phi_1, \phi_2, \cdots, \phi_n$$

where $\phi_n = B$, and each ϕ_i is an axiom, an element of Σ, the additional assumption A, or derived from two previous formulas via modus ponens.

We will transform this sequence into a proof from Σ of $A \to B$. To do this, we will show by strong induction[13] that for each index i ($0 \leq i \leq n$), we can construct a proof of the implication $A \to \phi_i$ under the assumptions in Σ.

Induction hypothesis. For all natural numbers $k < i$, the formula $A \to \phi_k$ is a theorem under the assumptions Σ.

Step case. We want to construct a proof of $A \to \phi_i$ under the assumptions Σ.

- If ϕ_i is an axiom or an element of Σ, then we have the following proof.
  1. $\phi_i \to (A \to \phi_i)$ (Axiom I)
  2. ϕ_i (Axiom/Assumption)
  3. $A \to \phi_i$ (modus ponens, from 1 and 2)
- If $\phi_i = A$, then we have the following proof.
  1. $A \to ((A \to A) \to A)$ (Axiom I)
  2. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ (Axiom II)
  3. $(A \to (A \to A)) \to (A \to A)$ (modus ponens, from 1 and 2)
  4. $(A \to (A \to A))$ (Axiom I)
  5. $A \to A$ (modus ponens, from 3 and 4)
- Suppose ϕ_i is derived via modus ponens by two previous formulas ϕ_j and $\phi_j \to \phi_i$. By the induction hypothesis, we have $\Sigma \vdash A \to \phi_j$ and $\Sigma \vdash A \to (\phi_j \to \phi_i)$. Now consider the axiom

  $$(A \to (\phi_j \to \phi_i)) \to ((A \to \phi_j) \to (A \to \phi_i)). \qquad \text{(Axiom II)}$$

  Since both $\Sigma \vdash A \to \phi_j$ and $\Sigma \vdash A \to (\phi_j \to \phi_i)$ are theorems, we may obtain the theorem $(A \to \phi_i)$.

This completes the induction proof, giving us $\Sigma \vdash A \to \phi_n$, which can be rewritten as $\Sigma \vdash A \to B$. Hence we have $\Sigma \cup \{A\} \vdash B \implies \Sigma \vdash (A \to B)$. □

[13] Recall that strong (or complete) induction does not require a base case.

7 Entailment, consistency and recursive languages

7.1 What is entailment?

Let Γ be a set of sentences and let S be a first-order structure (L-structure). We say that S is a *model* of Γ if for each sentence $\phi \in \Gamma$ we have $S \models \phi$. This is denoted as $S \models \Gamma$.

Furthermore, we say that $\Gamma \models \psi$ for some sentence ψ if every model of Γ is also a model of ψ, i.e. $S \models \Gamma \implies S \models \psi$. This is written as $\Gamma \models \psi$.

It's worth taking a moment to review the many roles that the symbol "$\models$" takes on in first-order logic. This is summarised in table 6.

Expression	**Meaning**
$(D, I) \models_A \phi$	ϕ is true in the structure (D, I) under the variable assignment A.
$(D, I) \models \phi$	ϕ is valid in the structure (D, I).
$\models \phi$	ϕ is valid.
$\mathcal{K} \models \phi$	ϕ is valid in all structures $(D, I) \in \mathcal{K}$.
$(D, I) \models \Sigma$	For all $\phi \in \Sigma$ we have $(D, I) \models \phi$.
$\Sigma \models \phi$	Σ entails ϕ. (Every model of Σ is a model of ϕ.)

Table 6: The various meanings of the symbol $\models$ in first-order logic. Here, (D, I) is a first-order structure with domain D and interpretation I; A is a variable assignment; ϕ is a formula; $\mathcal{K}$ is a set of structures; and Σ is a set of sentences.

7.2 Soundness, strong completeness and consistency

Entailment has the following properties.

$$\Gamma \vdash \phi \implies \Gamma \models \phi \tag{Soundness}$$

$$\Gamma \models \phi \implies \Gamma \vdash \phi \tag{Strong completeness}$$

Soundness states that if ϕ holds under the assumptions Γ (as proven using a tableau or axiomatic system), then Γ entails ϕ. Strong completeness is the converse thereof.

If falsity is deducible from a set of sentences Σ,

$$\Sigma \vdash \bot$$

then Σ is said to be *inconsistent.* By soundness, we also have

$$\Sigma \models \bot$$

which means that any model where Σ holds is also a model where $\bot$ holds. Since $\bot$ is always false, this implies that Σ does not have a model.

On the contrary, if falsity is not deducible from Σ, then Σ is said to be *consistent.* By strong completeness (using the contrapositive), we have $\Sigma \not\models \bot$, so Σ must have a model.

7.3 Recursive and recursively enumerable languages

A *language* refers to a set L of strings over a finite alphabet Σ.

$$L \subseteq \Sigma^*$$

A language L is said to be *recursive* (also called *decidable* or *computable*) if there exists a computer program that

- takes an arbitrary string $s \in \Sigma^*$ as input;

- correctly outputs `yes` if $s \in L$ and `no` otherwise; and
- always terminates for any input.

For example, the set of all formulas of first-order logic is recursive, since it is possible to write a parser that decides whether a string is a well-formed formula. Meanwhile, the set of valid first-order statements form a language, but it is not recursive.

Moreover, a language L is *recursively enumerable* (abbreviated *r.e.*, or alternatively *semi-decidable*) if there exists a computer program that outputs strings from L, only strings from L, and will eventually output any given string from L.

Theorem. *The set of valid statements in first-order logic is recursively enumerable.*

Proof 1 — using Hilbert-style axiomatic proof systems. Let c be an injective function that encodes any Hilbert-style first-order logic proof

$$\overline{\phi} = (\phi_0, \phi_1, \phi_2, \cdots, \phi_{k-1})$$

as a number $c(\overline{\phi})$. Then, the following program will eventually output any first-order theorem in finite time.

```
for ($i = 0$, $i$++, forever):
    if $i$ is the code of a proof: # $i = c(\overline{\phi})$
        output the proved formula
```

Hence proved. □

Proof 2 — using predicate tableaus. Let $\phi_0, \phi_1, \cdots$ be an enumeration of all formulas. Consider the following program.

```
tableaus = []
for ($i = 0$, $i$++, forever):
    create a new tableau $T_i$ with $\neg\phi_i$ at root
    tableaus.append($T_i$)

    for each $j \leq i$:
        if the $j$-th tableau $T_j$ can be expanded:
            expand $T_j$ once with fair schedule
            if $T_j$ becomes closed:
                output $\phi_j$
```

For any formula ϕ_k,

- if ϕ_k is not valid, then T_k never closes (by soundness); and
- if ϕ_k is valid, then T_k will eventually close, resulting in ϕ_k being outputted in finite time.

Therefore, this program only outputs valid formulas, and any valid formula will eventually be outputted. □

Theorem. *All recursive sets are recursively enumerable.*

Proof. Let L be a recursive language. Let A be a terminating algorithm such that

$$A(s) = \begin{cases} 1 & \text{if } s \in L \\ 0 & \text{otherwise} \end{cases}$$

for any input string s. We then construct the following program.

```
for each string $s$ (sorted first by increasing length, then alphabetically):
    if $A(s) = 1$:
        output $s$
```

This program only outputs strings from L, and each $s \in L$ is eventually output. Therefore, L is recursively enumerable. □

Note that the converse of the above theorem does not hold. While all recursive sets are recursively enumerable, not all recursively enumerable sets are recursive.

If a language $L \subseteq \Sigma^*$ is recursively enumerable, then its complement $\Sigma^* \setminus L$ is said to be *co-recursively enumerable* (abbreviated *co-r.e.*).

Theorem. *If a set is both recursively enumerable and co-recursively enumerable, then it is decidable.*

Proof. Let L be a language that is both recursively enumerable and co-recursively enumerable.

Since L is recursively enumerable, there exists some program A that eventually outputs every string in L.

Since it is also co-recursively enumerable, there exists some program B that eventually outputs every string not in L.

We can thus construct the following program.

```
def is_in_L(string):
    for ($i = 0$, $i$++, forever):
        read $i$-th output from $A$ and store it in $A_i$
        if $A_i$ matches string:
            return 1

        read $i$-th output from $B$ and store it in $B_i$
        if $B_i$ matches string:
            return 0
```

Since $L \cup (\Sigma^* \setminus L) = \Sigma^*$, every string in Σ^* will eventually be outputted by either A or B in finite time. Therefore, the above program always terminates, so L is decidable. □

8 Compactness theorem

Proofs are finite. If for some formula ϕ and some set of assumptions Σ we have $\Sigma \vdash \phi$, then we must also have $\Sigma_0 \vdash \phi$ for some finite subset Σ_0 of Σ.

Theorem. *A set of formulas Σ has a model if and only if each finite subset of Σ has a model.*

Proof. ($\Rightarrow$): Assume that Σ has a model (D, I). Then trivially every finite subset of Σ must also have the same model (D, I).

($\Leftarrow$): We prove the contrapositive — if Σ does not have a model, then there is some finite subset of Σ that does not have a model either.

If Σ has no model, then $\Sigma \models \bot$. By strong completeness, this set must be inconsistent, with $\Sigma \vdash \bot$. Since proofs are finite, there exists some finite subset $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \vdash \bot$. By soundness, it follows that $\Sigma_0 \models \bot$, i.e. Σ does not have a model. Hence proved. □

Below we will see some examples of how the compactness theorem can be applied.

8.1 First-order logic cannot define connectedness

Let E be a binary predicate symbol denoting the edges of a directed graph. Let $=$ be a binary predicate symbol interpreted as true equality.

For any natural number k, we say that there is a *path* of length k from x to y if there is a sequence

$$x_0, x_1, \cdots, x_k$$

where $x = x_0$, $y = x_k$ and there is any edge from x_i to x_{i+1} for all $i < k$.

We can then write the following formulas.

- There is a path of length 0 from node x to node y.

$$x = y$$

- There is a path of length 1 from node x to node y.

$$E(x, y)$$

- There is a path of length 2 from node x to node y.

$$\exists z \ (E(x, z) \land E(z, y))$$

- There is a path of length 3 from node x to node y.

$$\exists w \ ((\exists z \ (E(x, z) \land E(z, w))) \land E(w, y))$$

Let $P_n(x, y)$ be the statement "There is a path of length n from node x to node y". In general, $P_n(x, y)$ can be expressed in first-order logic as follows.

$$P_0(x, y) = \text{“}x = y\text{”}$$
$$P_{n+1}(x, y) = \text{“}\exists m \ (P_n(x, m) \land E(m, y))\text{”}$$

A directed graph consists of a set of nodes G and a binary relation over G. Such a graph is said to be *connected* if for all $x, y \in G$ there is a path of finite length k from x to y. How can we define this concept of connectedness using first-order logic?

A possible approach might be something like

$$\bigvee_{n\in\mathbb{N}}(P_n(x,y))$$

or

$$\exists n\ P_n(x,y).$$

However, neither of these formulas are acceptable. The first formula is problematic because first-order logic does not allow an infinite number of connectives; the second formula does not work because $\exists n$ assumes a domain of $\mathbb{N}$, when the domain is actually G.

In fact, it is impossible to define connectedness using first-order logic, as we will prove below.

Theorem (First-order logic cannot define connectedness)**.** *There is no first-order formula ϕ such that a graph G satisfies ϕ if and only if G is connected.*

Proof. By contradiction. Let $L = (C, F, P)$ be the first-order lanaguage where $C = \{c, d\}$, $F = \emptyset$ and $P = \{E, =\}$, with E representing the edge relation. Suppose Σ is a theory that is satisfied by a graph G if and only if G is a connected graph.

Let $P_n(x, y)$ be a first-order formula expressing the statement "there is a path of length n from node x to node y", as defined earlier.

Consider the theory

$$\Sigma^+ = \underbrace{\Sigma}_{\substack{G\text{ is}\\ \text{connected}}} \cup \underbrace{\{\neg\phi_n(c,d) : n \in \mathbb{N}\}}_{\substack{\text{no path of any length}\\ \text{from } c \text{ to } d\\ (G\text{ is disconnected})}}$$

which does not have a model, as a graph cannot be both connected and disconnected. This can be denoted as $\Sigma^+ \models \bot$.

Now consider a finite subset $\Sigma_0^+ \subset \Sigma^+$. This gives us

$$\Sigma_0^+ = \Sigma_0 \cup \{\neg\phi_n(c,d) : n \in S\}$$

where Σ_0 is a finite subset of Σ and S is a finite set of natural numbers.

We show that Σ_0^+ has a model. Since S is finite, we can find some $N \in \mathbb{N}$ that is larger than any element in S. Construct a graph G where

- the nodes are $\{0, 1, 2, \cdots, N+1\}$;
- edges are present between consecutive numbers only; and
- $c = 0$ and $d = N + 1$.

Hence the shortest path between c and d has length $(N + 1)$. This is a model of Σ_0^+.

By the compactness theorem, since any finite subset of Σ^+ has a model, Σ^+ itself must also have a model. This contradicts our earlier proposition that Σ^+ does not have a model. □

8.2 First-order logic cannot define finiteness

Similarly, it is impossible to define the class of all finite structures (i.e. structures with finite domains) using a first-order sentence or theory.

Theorem (First-order logic cannot define finiteness)**.** *There is no first-order formula ϕ such that $(D, I) \models \phi$ if and only if the domain D is finite.*

Proof. By contradiction. Assume there is theory Σ where $(D, I) \models \Sigma$ if and only if the domain D is finite.

Let C be an infinite set of constant symbols. Consider the theory

$$\Sigma^+ = \underbrace{\Sigma}_{\substack{D \text{ is} \\ \text{finite}}} \cup \underbrace{\{\neg(c = d) : c \text{ and } d \text{ are different constant symbols in } C\}}_{\substack{\text{each constant symbol is interpreted as a different domain element,} \\ \text{so } D \text{ is infinite}}}$$

which does not have a model.

Now consider a finite subset $\Sigma_0^+ \subset \Sigma^+$. This gives us

$$\Sigma_0^+ = \Sigma_0 \cup \{\neg(c = d) : c \text{ and } d \text{ are different constant symbols in } C_0\}$$

where Σ_0 is a finite subset of Σ and C_0 is a finite subset of C.

Notice that the Herbrand structure (C_0, I), where each constant symbol in C_0 is interpreted as itself, is a model of Σ_0^+.

By the compactness theorem, since every finite subset of Σ_0^+ of Σ^+ has a model, the theory Σ^+ must also have a model. This contradicts our earlier proposition that Σ^+ does not have a model. □

8.3 Non-standard analysis

8.3.1 Non-standard model of arithmetic

Consider a language L with

- constant symbols $0, 1, 2, 3, \cdots$;
- binary function symbols $\times$ and $+$; and
- a binary predicate symbol $=$.

Let Σ be the set of all sentences in this language that represent valid statements about $\mathbb{N}$, such as

$$\text{“}2 + 2 = 4\text{”}$$

and

$$\forall x\, \forall y\, (x \times y = y \times x).$$

Clearly, Σ has a model. Specifically, Σ has the model $(\mathbb{N}, I)$ where I interprets each constant symbol as its corresponding natural number, “$\times$” as ordinary multiplication, “$+$” as ordinary addition and “$=$” as true equality.

Let L^+ be a language which is identical to L, except it includes a new constant symbol c. We will show that the following theory has a model.

$$\Sigma^+ = \Sigma \cup \{\neg(c = 0), \neg(c = 1), \neg(c = 2), \cdots\}$$

Consider a finite subset $\Sigma_0^+ \subset \Sigma^+$. This gives us

$$\Sigma_0^+ = \Sigma_0 \cup \{\neg(c = n) : n \in S\}$$

where Σ_0 is a finite subset of Σ and S is a finite set of constant symbols in L. Let N be the largest natural number that is the interpretation of a constant symbol in S. (This number must exist as S is finite.) This allows us to define a model for Σ_0^+ where c is interpreted as $(N + 1)$.

By the compactness theorem, since every finite subset of Σ^+ has a model, the theory Σ^+ must also have a model $(\mathbb{N}^+, I^+)$.

The newly introduced constant symbol c is said to be *non-standard*, and the resultant model Σ^+ is called the *non-standard model of arithmetic.*

Since $\Sigma \subset \Sigma^+$, any statement that is true about $\mathbb{N}$ must also be true about N^+.

Corollary (Commutativity of multiplication in $\mathbb{N}^+$)**.** $\forall x \, \forall y \, (x \times y = y \times x)$ *holds in* $\mathbb{N}^+$*.*

Corollary (All nonzero elements in $\mathbb{N}^+$ have predecessors)**.** *We say that* m *is a predecessor of* n *if* $m + 1 = n$*. Since* $\forall n \, (\neg(n = 0) \to \exists m \, (m + 1 = n))$ *holds in* $\mathbb{N}$*, this property also holds in* $\mathbb{N}^+$*.*

Note, however, that this only works for statements about $\mathbb{N}$ that can be written using the first-order language L. The principle of induction, for example, is represented as the second-order formula

$$\forall P \, ((P(0) \wedge \forall x \, (P(x) \to P(x+1))) \to \forall x \, P(x))$$

where P is quantified over all unary predicates. Therefore, the principle of induction does not necessarily hold in $\mathbb{N}^+$.

Theorem. *The principle of induction does not hold in* $\mathbb{N}^+$*.*

Proof. By counterexample. Let $P(n)$ be the statement "n is standard". In other words, $P(n)$ is true if and only if n does not involve the constant symbol c. Notice that the left-hand side of the implication

$$(P(0) \wedge \forall x \, (P(x) \to P(x+1)))$$

is true but the right-hand side

$$\forall x \, P(x)$$

is false, making this a counterexample. □

8.3.2 Non-standard model of the real numbers (hyperreals)

Similar to the above, let L be a language with a constant symbol for every real number, along with function and predicate symbols for common arithmetic operations. Let Σ be the set of all sentences representing valid statements about $\mathbb{R}$. Clearly, Σ has a model.

Let L^+ be an identical languge but with the addition of a new constant symbol ω. Consider the theory $\Sigma^+ = \Sigma \cup \{\omega > r : r \in \mathbb{R}\}$. Every finite subset of $\mathbb{R}$ has a model, since we can simply interpret every ω as a sufficiently large real number. By the compactness theorem, this implies that Σ^+ has a non-standard model $M = (\mathbb{R}^+, I^+)$.

It follows that $[\omega]^M$ is an "infinitely large" number that is greater than any real number $r \in \mathbb{R}$. Similarly, $[1/\omega]^M$ is an "infinitesimally small" positive real number.

This introduction of infinitesimals enables us to formalise differential and integral calculus. To begin with, we can show that

$$\forall x \, ((|x| < r) \to (x = \text{Standard}(x) + \text{Infinitesimal}(x)))$$

where r is a constant for any positive real number, Standard(x) is a standard real and Infinitesimal(x) is a non-standard (infinitesimal) real. We then define the derivative of a function $f(x)$ as

$$f'(x) = \text{Standard}\left(\frac{f(x + \delta x) - f(x)}{\delta x}\right)$$

where x is any standard real and δx is any infinitesimal. This formula can only be used if the value of $f'(x)$ does not depend on the choice of δx — this corresponds to when f is differentiable at x.

9 Gödel's incompleteness theorem

Theorem (Gödel's incompleteness theorem, 1931)**.** *Let Λ be a formal recursively enumerable logic that is sufficient for arithmetic, i.e.*

(a) Syntax: Its language $L = (C, F, P)$ should include constant symbols $0, 1 \in C$, binary function symbols $+, \times \in F$, and the binary predicate symbol $= \in P$;

(b) Semantics: Its first-order structure should interpret the aforementioned symbols in accordance with the domain $\mathbb{N}$; and

(c) Inference system: There should be an inference system, possibly axiomatic or tableau-based.

If Λ is sound, then it is not complete — in other words, if Λ cannot prove any false statements about arithmetic, then there must be true statements about arithmetic for which there exists no proof.

Informal proof sketch. Notice that any n-ary function can be rewritten as an $(n+1)$-ary predicate. For example, the binary addition function, which produces such properties as $2+3=5$ and $4+0=4$, can be represented as the trinary predicate $\{(2,3,5), (4,0,4), \cdots\}$. Hence, for this proof, we may assume without loss of generality that Γ has no function symbols, with $F = \emptyset$.

Let $G : C \cup P \to \mathbb{N} \setminus \{0\}$ be an injective function that uniquely encodes every symbol in Λ as a positive integer. This enables us to encode any formula of Λ as an integer. For example, if we have

$$\begin{aligned} G(\texttt{+}) &= 053 \\ G(\texttt{(}) &= 050 \\ G(\texttt{x}) &= 170 \\ G(\texttt{,}) &= 053 \\ G(\texttt{y}) &= 171 \\ G(\texttt{)}) &= 051 \\ G(\texttt{=}) &= 075 \\ G(\texttt{-}) &= 055 \\ G(\texttt{x}) &= 170 \end{aligned}$$

then the formula

$$+(x, y) = -x$$

can be encoded as the *Gödel number*

$$053\ 050\ 170\ 053\ 171\ 051\ 075\ 055\ 170.$$

Due to the injective nature of the encoding, it is possible to decode a formula from its Gödel number. Furthermore, we can define string concatenation on Gödel numbers as

$$m \mathbin{++} n = 10^{|n|} \times m + n$$

where $|n|$ is the length of the string n. We can also define various string properties on strings using first-order formulas, informally described as follows.

- Formula(n) determines whether n is the Gödel number of an acceptable first-order formula. It is the disjunction of Atom(n), Neg(n), Disj(n) and Exist(n), as defined below.
- Atom(n) determines whether n is the Gödel number of an atom. It checks whether there exists natural numbers y and z such that
  - n is the concatenation of y, $G(\texttt{(})$, z and $G(\texttt{)})$;
  - y is the Gödel number of a predicate symbol; and

  - z is the Gödel number of a term.

- Neg(n) determines whether n is the Gödel number of a negated formula. It checks whether there exists a natural number z with Formula(z) such that n is the concatenation of $G(\neg)$ and z.

- Disj(n) determines whether n is the Gödel number of a disjunction. It checks whether there exists natural numbers v and w with Formula(v) and Formula(w) such that n is the concatenation of $G($**(**$)$, v, $G($**,**$)$, w and $G($**)**$)$.

- Exist(n) determines whether n is the Gödel number of an existential formula. It checks whether there exists a natural number v with Formula(v) such that n is the concatenation of $G(\exists)$, a variable symbol's Gödel number and v.

This recursion is well-founded.

Similarly, every axiomatic proof can be represented as a string, using 000 as a delimiter to separate consecutive formulas. Therefore, a unique Gödel number can be assigned to each proof.

Let

$$A_0(x), A_1(x), A_2(x), \cdots$$

be an enumeration of all formulas in the language with one free variable x. We may then write

$$\theta(n,k,q) = \text{“The Gödel number } n \text{ represents a proof of } A_k(q)\text{”}$$

Now consider the following formula,

$$\neg\exists n\ \theta(n,x,x)$$

which reads as "there is no natural number n that represents a proof of $A_x(x)$", or "there is no proof of $A_x(x)$". Since this formula only has one free variable x, it must appear in the enumeration above. Thus, there exists some n_0 such that

$$\begin{array}{rcl} A_{n_0}(x) & = & \neg\exists n\ \theta(n,x,x) \\ \mathbb{N} \models A_{n_0}(x) & \iff & \mathbb{N} \models \neg\exists n\ \theta(n,x,x) \\ \mathbb{N} \models A_{n_0}(x) & \iff & \text{there is no proof of } A_x(x) \end{array}$$

If we substitute the free variable x with n_0, we get

$$\mathbb{N} \models A_{n_0}(n_0) \iff \text{there is no proof of } A_{n_0}(n_0).$$

Therefore, either

- $A_{n_0}(n_0)$ is valid in $\mathbb{N}$, but it has no proof (incompleteness); or

- $A_{n_0}(n_0)$ is invalid in $\mathbb{N}$, but can be proven (inconsistency). □

10 Modal logic

10.1 Syntax

In modal logic, formulas are constructed by applying negation, conjunction, disjunction, implication, as well as the box and diamond operators to propositions.

$$\begin{aligned} \text{proposition} &:= p \mid q \mid r \cdots \\ \text{formula} &:= \text{proposition} \mid \neg\text{formula} \mid (\text{formula} \circ \text{formula}) \mid \Box\text{formula} \mid \Diamond\text{formula} \\ & \qquad\qquad (\text{where } \circ \text{ is } \wedge, \vee \text{ or } \rightarrow) \end{aligned}$$

10.2 Semantics

A *Kripke frame* $\mathcal{F} = (W, R)$ contains a set W of worlds and a binary relation $R \subseteq W \times W$. This can be represented as a directed graph with nodes W and edges R.

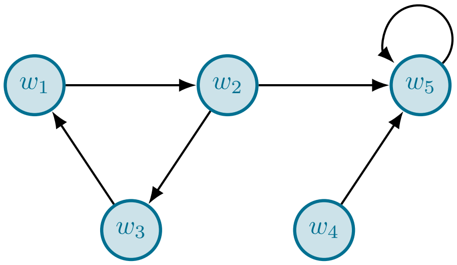


Figure 14: A Kripke frame $\mathcal{F} = (W, R)$ with worlds $W = \{w_1, w_2, w_3, w_4, w_5\}$ and the relation $R = \{(w_1, w_2), (w_2, w_3), (w_2, w_5), (w_3, w_1), (w_4, w_5)\}$.

A valuation V is a function that maps each propositional letter to a subset of W. For example, we may have

$$\begin{aligned} V(p) &= \{w_1, w_3, w_5\} \\ V(q) &= \{w_1, w_2\} \\ V(r) &= \emptyset \end{aligned}$$

A Kripke frame (W, R) combined with a valuation V gives a *Kripke model* $\mathcal{M} = (W, R, V)$.

Modal logic is a local logic where formulas are evaluated not just with a model, but at a specific world as well. For any given world $w \in W$, we define the semantics of modal logic as

$$\begin{aligned} \mathcal{M}, w \models p &\iff w \in V(p) \\ \mathcal{M}, w \models \neg\phi &\iff \mathcal{M}, w \not\models \phi \\ \mathcal{M}, w \models (\phi \wedge \psi) &\iff \mathcal{M}, w \models \phi \text{ and } \mathcal{M}, w \models \psi \\ \mathcal{M}, w \models \Diamond\phi &\iff \text{there exists some } w' \in W \text{ such that } (w, w') \in R \text{ and } \mathcal{M}, w' \models \phi \\ \mathcal{M}, w \models \Box\phi &\iff \text{for all } w' \in W, \text{ if } (w, w') \in R \text{ then } \mathcal{M}, w' \models \phi \end{aligned}$$

where p is a propositional letter and ϕ and ψ are formulas.

A formula may be valid in a model, in a frame, or over a class of frames.

$$\begin{aligned} (W, R, V) \models \phi &\iff (W, R, V), w \models \phi \text{ for all } w \in W && \text{(validity in a model)} \\ (W, R) \models \phi &\iff (W, R, V) \models \phi \text{ for all valuations } V && \text{(validity in a frame)} \\ \mathcal{K} \models \phi &\iff \mathcal{F} \models \phi \text{ for all frames } \mathcal{F} \in \mathcal{K} && \text{(validity over a class of frames)} \end{aligned}$$

Any formula that is valid in propositional logic is also valid in modal logic. Other valid formulas include

$$\Box(p \land q) \to (\Box p \land \Box q)$$
$$\Box(p \to q) \to (\Box p \to \Box q)$$

but not

$$\Box(p \lor q) \to (\Box p \lor \Box q).$$

10.3 Axiomatic proof system

In addition to the axioms for propositional logic, an axiomatic proof system for modal logic requires the following axiom.

$$\Box(p \to q) \to (\Box p \to \Box q)$$

We also use the following inference rules.

$$\frac{\phi \quad (\phi \to \psi)}{\psi} \qquad \text{(modus ponens)}$$

$$\frac{\phi}{\Box\phi} \qquad \text{(necessitation)}$$

10.4 Classes of frames, soundness and completeness

Frames with common properties may be grouped into a class $\mathcal{K}$. We say that a formula ϕ *defines* $\mathcal{K}$ if

$$\mathcal{F} \vdash \phi \iff \mathcal{F} \in \mathcal{K}.$$

Table 7 shows several examples of such classes and their defining modal formulas. Moreover, names are often assigned to classes with special properties, as shown in Table 8.

Class of...	**First-order definition**	**Defining modal formula**
Reflexive frames	$\forall w\ Rww$	$\Box p \to p$
Transitive frames	$\forall u\ \forall v\ \forall w\ ((Ruv \land Rvw) \to Ruw)$	$\Diamond\Diamond p \to \Diamond p$ or $\Box p \to \Box\Box p$
Symmetric frames	$\forall u\ \forall v\ (Ruv \to Rvu)$	$p \to \Box\Diamond p$
Dense frames	$\forall u\ \forall v\ (Ruv \to \exists w\ (Ruw \land Rwv))$	$\Diamond p \to \Diamond\Diamond p$ or $\Box\Box p \to \Box p$

Table 7: Classes of Kripke frames and the modal formulas that define them.

Name	**Class of...**
K	All frames
T	Reflexive frames
$S4$	Reflexive and transitive frames
$S5$	Frames with equivalence relations (reflexive, symmetric and transitive)

Table 8: Classes of Kripke frames and their names.

For a class $\mathcal{K}$ of frames, let A be the conjunction of its axioms and defining formulas. For any formula ϕ, we write $\vdash_A \phi$ if ϕ is provable using A through modus ponens and necessitation. It follows that

$$\mathcal{K} \models \phi \iff \vdash_A \phi$$

meaning that $\vdash_A$ is sound and complete for $\mathcal{K}$.

10.5 Modal tableaus

Like in propositonal and first-order logic, the satisfiability modal formulas can be verified with tableaus.

The tableau will consist of a queue of *labelled frames*. A labelled frame $((W, R), \lambda)$ contains a function λ which maps each world W to a set of modal formulas. We may visualise this as a frame where each world is labelled with zero or more formulas.

The following algorithm is used to determine the satisfiability of a formula ϕ.

```
def is_satisfiable($\phi$):
    Tableau = Queue()
    Tableau.enqueue(frame containing only one world labelled $\phi$)

    while Tableau is not empty:
        # Dequeue a labelled frame from the tableau
        $((W, R), \lambda)$ = Tableau.dequeue()

        if $\{p, \neg p\} \subseteq \lambda(w)$ for some $w \in W$ and propositional letter $p$:
            # There is a world with contradictory literals,
            # so don't enqueue this frame back
            continue

        if for all $w \in W$, each formula $\theta \in \lambda(w)$ is a literal, box or negated diamond:
            return True

        select a formula $\theta \in \lambda(w)$ $(w \in W)$ that is not a literal, box or negated diamond

        if $\theta$ is an $\alpha$-formula:
            let $\lambda'$ be identical to $\lambda$ except $\lambda'(w) = (\lambda(w) \setminus \{\theta\}) \cup \{\alpha_1, \alpha_2\}$
            Tableau.enqueue($((W, R), \lambda')$)

        elif $\theta$ is a $\beta$-formula:
            let $\lambda_1$ be identical to $\lambda$ except $\lambda_1(w) = (\lambda(w) \setminus \{\theta\}) \cup \{\beta_1\}$
            Tableau.enqueue($((W, R), \lambda_1)$)

            let $\lambda_2$ be identical to $\lambda$ except $\lambda_2(w) = (\lambda(w) \setminus \{\theta\}) \cup \{\beta_2\}$
            Tableau.enqueue($((W, R), \lambda_2)$)

        elif $\theta = \Diamond A$:
            let $W' = W \cup \{w_{\texttt{new}}\}$ with a new world $w_{\texttt{new}}$
            let $R' = R \cup \{(w, w_{\texttt{new}})\}$
            let $\lambda'$ be identical to $\lambda$ except $\lambda'(w_{\texttt{new}}) = \{A\} \cup \{B : \Box B \in \lambda(w)\} \cup \{\neg B : \neg\Diamond B \in \lambda(w)\}$
                                      and $\lambda'(w) = \lambda(w) \setminus \{\theta\}$
            Tableau.enqueue($((W', R'), \lambda')$)

        elif $\theta = \neg\Box A$:
            let $W' = W \cup \{w_{\texttt{new}}\}$ with a new world $w_{\texttt{new}}$
            let $R' = R \cup \{(w, w_{\texttt{new}})\}$
            let $\lambda'$ be identical to $\lambda$ except $\lambda'(w_{\texttt{new}}) = \{\neg A\} \cup \{B : \Box B \in \lambda(w)\} \cup \{\neg B : \neg\Diamond B \in \lambda(w)\}$
                                      and $\lambda'(w) = \lambda(w) \setminus \{\theta\}$
            Tableau.enqueue($((W', R'), \lambda')$)

    return False
```

We may adapt this tableau algorithm for determining satisfiability in specific classes of frames.

- To determine satisfiability of a formula ϕ in reflexive frames, initialise the tableau with a frame (W, R, λ) where $W = \{w\}$, $R = \{(w, w)\}$ and $\lambda(w) = \phi$. Construct the tableau as usual. Whenever a new world w_{new} is added:
    - add $(w_{\text{new}}, w_{\text{new}})$ to R;

  - if $\Box A \in \lambda(w_{\text{new}})$, also include $A \in \lambda(w_{\text{new}})$; and
  - if $\neg\Diamond A \in \lambda(w_{\text{new}})$, also include $\neg A \in \lambda(w_{\text{new}})$.

- To determine satisfiability of a formula in symmetric frames, construct the tableau as usual. For diamond formulas in world w, when a new world w_{new} is added with a new edge (w, w_{new}), also include the edge (w_{new}, w). Any boxed or negated diamond formulas in w_{new} should propagate back to w.

- To determine satisfiability of a formula in transitive frames, construct the tableau as usual. For diamond formulas in world w, when a new world w_{new} is added with a new edge (w, w_{new}), then

  - add the edge (v, w_{new});
  - if $\Box A \in \lambda(v)$, include $A \in \lambda(w)$; and
  - if $\neg\Diamond A \in \lambda(v)$, include $\neg A \in \lambda(w)$

  for each world v that has an outgoing edge to w. Note that tableaus for transitive models may not terminate.

10.6 Frame and model p-morphisms

Let (W, R) and (W', R') be frames. A function $f : W \to W'$ is called a *frame p-morphism* if

- $(x, y) \in R$ implies $(f(x), f(y)) \in R'$ (a homomorphism); and
- if $(f(x), y') \in R'$, then there is some $y \in W$ such that $f(y) = y'$ and $(x, y) \in R$.

Figure 15 shows an example of a frame p-morphism between two frames (W, R) and (W', R'), with a function f mapping worlds from $W = \{A, B, C, D, E\}$ to worlds from $W' = \{X, Y, Z\}$. Notice that

- Edges are retained by the mapping. If there are two worlds in W connected by an edge, they must remain connected after the mapping.
- If an edge connects two worlds in W', one of which can be "traced back" through f to a world $w \in W$, then it must also be possible to trace back the other world to some $w' \in W$ connected to w.

Let v and v' be valuations mapping proposition letters to subsets of W and W' respectively. If f is a frame p-morphism from (W, R) to (W', R') and $w \in v(p) \iff f(w) \in v'(p)$ for all worlds w and proposition letters p, then f is said to be a *model p-morphism* from model (W, R, v) to (W', R', v'). This is illustrated in Figure 16.

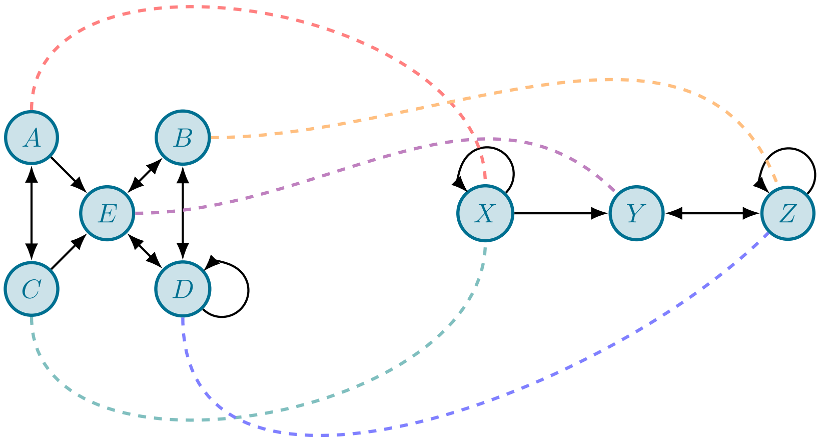


Figure 15: A frame p-morphism between a frame (W, R) with worlds $W = \{A, B, C, D, E\}$ and a frame (W', R') with worlds $W' = \{X, Y, Z\}$.

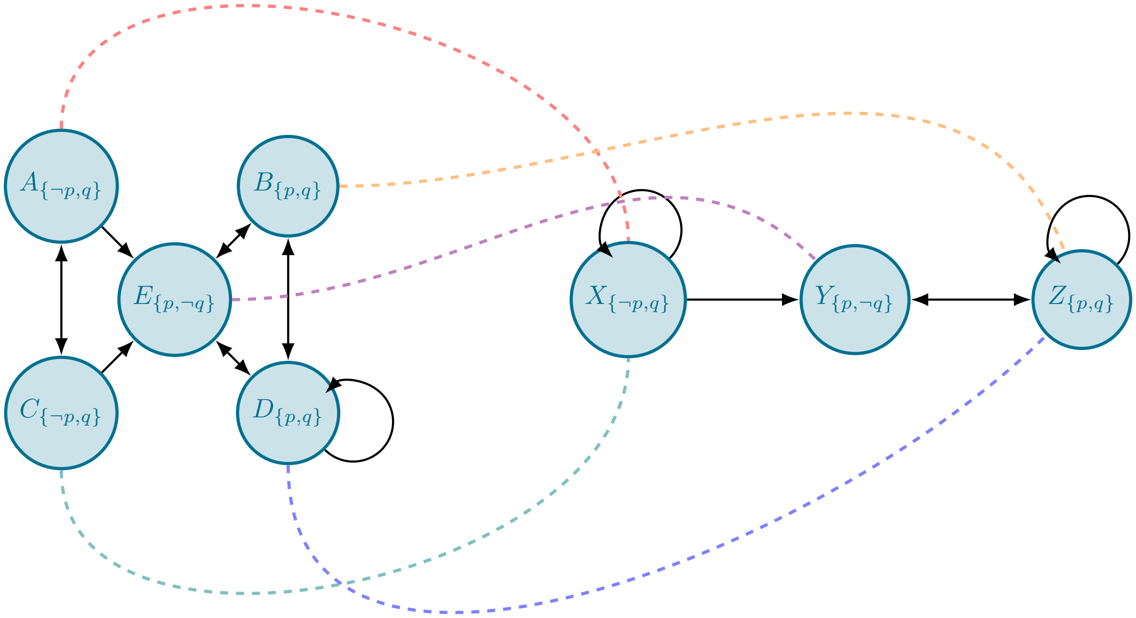


Figure 16: A model p-morphism between a model with worlds $W = \{A, B, C, D, E\}$ and a model with worlds $W' = \{X, Y, Z\}$. Valuations for each model are represented using subscripted curly brackets in each world.

From this we can prove the following theorem on model p-morphisms.

Theorem. *Let f be a model p-morphism from model (W, R, v) to model (W', R', v'). For any modal formula ϕ and world $w \in W$, we have*

$$W, R, v, w \models \phi \iff W', R', v', f(w) \models \phi$$

Proof. By structural induction on ϕ, with the syntax of modal formulas defined as follows.

$$\begin{aligned} \text{proposition} &:= p \mid q \mid r \cdots \\ \text{formula} &:= \text{proposition} \mid \neg\text{formula} \mid (\text{formula} \vee \text{formula}) \mid \Diamond\text{formula} \end{aligned}$$

Base case. For any proposition letter p, we have

$$\begin{aligned} W, R, v, w \models p &\iff w \in v(p) \\ &\iff f(w) \in v'(p) && \text{(by definition of model p-morphism)} \\ &\iff W', R', v', f(w) \models p \end{aligned}$$

which completes the base case.

Step case for "¬formula". Assume $W, R, v, w \models \phi \iff W', R', v', f(w) \models \phi$ for some formula ϕ. Then

$$\begin{aligned} W, R, v, w \models \neg\phi &\iff W, R, v, w \not\models \phi \\ &\iff W', R', v', f(w) \not\models \phi && \text{(by induction hypothesis)} \\ &\iff W', R', v', f(w) \models \neg\phi \end{aligned}$$

Step case for "formula ∨ formula". Assume

$$\begin{aligned} W, R, v, w \models \phi &\iff W', R', v', f(w) \models \phi \\ W, R, v, w \models \psi &\iff W', R', v', f(w) \models \psi \end{aligned}$$

for some formulas ϕ and ψ. Then

$$\begin{aligned} W, R, v, w \models \phi \vee \psi &\iff W, R, v, w \models \phi \text{ or } W, R, v, w \models \psi \\ &\iff W', R', v', f(w) \models \phi \text{ or } W', R', v', f(w) \models \psi \\ &\qquad\qquad \text{(by induction hypothesis)} \\ &\iff W', R', v', f(w) \models \phi \vee \psi \end{aligned}$$

Step case for "◊formula". Assume $W, R, v, w \models \phi \iff W', R', v', f(w) \models \phi$ for some formula ϕ. We want to prove that

$$W, R, v, w \models \Diamond\phi \iff W', R', v', f(w) \models \Diamond\phi.$$

($\Rightarrow$).

$$\begin{aligned} W, R, v, w \models \Diamond\phi &\Rightarrow \text{there is some } w' \in W \text{ where } Rww' \text{ and } W, R, v, w' \models \phi \\ &\Rightarrow \text{there is some } w' \in W \text{ where } (f(w), f(w')) \in R' \text{ and } W', R', v', f(w') \models \phi \\ &\qquad \text{(by induction hypothesis and definition of model p-morphism)} \\ &\Rightarrow W', R', v', f(w) \models \Diamond\phi \end{aligned}$$

($\Leftarrow$).

$$\begin{aligned}
W',R',v',f(w) \models \Diamond\phi &\Rightarrow \text{there is some } x \in W' \text{ where } (f(w),x) \in R' \text{ and } W',R',v',x \models \phi \\
&\Rightarrow \text{there is some } x_0 \in W \text{ where } (f(w),f(x_0)) \in R' \text{ and } W',R',v',f(x_0) \models \phi \\
&\qquad\qquad\qquad \text{(by definition of model p-morphism)} \\
&\Rightarrow \text{there is some } x_0 \in W \text{ where } (w,x_0) \in R \text{ and } W',R',v',f(x_0) \models \phi \\
&\qquad\qquad\qquad \text{(by definition of model p-morphism)} \\
&\Rightarrow \text{there is some } x_0 \in W \text{ where } (w,x_0) \in R \text{ and } W,R,v,x_0 \models \phi \\
&\qquad\qquad\qquad \text{(by induction hypothesis)} \\
&\Rightarrow W,R,v,w \models \Diamond\phi
\end{aligned}$$

Conclusion. By principles of structural induction, the theorem is proved. □

10.7 The class of irreflexive frames is not modally definable

A frame (W,R) is said to be *irreflexive* if for all worlds w we have $(w,w) \in R$.

Theorem. *There is no modal formula that defines irreflexive flames. In other words, there is no formula ϕ for which*

$$(W,R) \models \phi \iff (W,R) \textit{ is irreflexive.}$$

Proof. By contradiction. Suppose there is a modal formula ϕ that satisfies

$$(W,R) \models \phi \iff (W,R) \text{ is irreflexive.}$$

Consider the two-world irreflexive frame

$$\mathcal{F}_2 = (\{a,b\}, \{(a,b),(b,a)\})$$

and the one-world reflexive frame

$$\mathcal{F}_1 = (\{c\}, \{(c,c)\}).$$

Let $f : \mathcal{F}_2 : \mathcal{F}_1$ be a p-morphism where $f(a) = f(b) = c$.

Since $\mathcal{F}_1$ is not irreflexive, we have $\mathcal{F}_1 \not\models \phi$. Hence, there is some valuation v_1 for which $\mathcal{F}_1, c, v_1 \not\models \phi$. Define a valuation v_2 over $\mathcal{F}_2$ as

$$v_2(p) = \begin{cases} \{a,b\} & \text{if } v(p) = \{c\} \\ \emptyset & \text{if } v(p) = \emptyset \end{cases}.$$

Then f is a model p-morphism from $(\mathcal{F}_2, v_2)$ to $(\mathcal{F}_1, v_1)$. Hence $\mathcal{F}_2, x, v_2 \not\models \phi$ for all $x \in \{a,b\}$. This means that $\mathcal{F}_2 \not\models \phi$, which is absurd as $\mathcal{F}_2$ is irreflexive. □

11 Epistemic, temporal and dynamic logic

11.1 Multimodal logic

A multimodal logic is similar to ordinary modal logic, except that a frame may simultaneously include several different binary relations. A multimodal logic formula ϕ is defined as follows.

$$\phi := p \mid \neg\phi \mid \phi \vee \phi \mid \Diamond_i \phi \mid \Box_i \phi \qquad (i = 0, 1, 2, \cdots, k-1)$$

A multimodal Kripke frame is a tuple

$$(W, R_0, R_1, \cdots, R_{k-1})$$

where $R_i \subseteq W \times W$. Semantically, we have

$$\begin{aligned}&(W, R_0, R_1, \cdots, R_{k-1}), v, w \models \Diamond_i \phi \\ &\iff \text{there is some } w' \in W \text{ where } (w, w') \in R_i \text{ and } (W, R_0, R_1, \cdots, R_{k-1}), v, w' \models \phi.\end{aligned}$$

11.2 Introduction to epistemic logic

In philosophy, the word “epistemic” refers to the study of cognition, knowledge and how they are acquired. Similarly, *epistemic logic* is a specific type of modal logic that models and reasons about the knowledge and beliefs of an *agent* (e.g. an individual or machine).

There are many interpretations of what “knowledge” means. Here, we select the indistinguishability interpretation.

In epistemic logic, we write $K_s(\phi)$ and $B_s(\phi)$ to mean “the agent s knows ϕ” and “the agent s believes ϕ” respectively. Here, knowledge is defined as a belief that is both true and justified.

Consider two propositions as follows. Assume dogs always bark.

$$\begin{aligned}g &= \text{“there is a grasshopper in the garden”} \\ d &= \text{“there is a dog in the garden”}\end{aligned}$$

With these two propositions, let us define a set of four *possible worlds* $W = \{w_\emptyset, w_{\{g\}}, w_{\{d\}}, w_{\{g,d\}}\}$, where g is true in worlds $w_{\{g\}}$ and $w_{\{g,d\}}$, while d is true in worlds $w_{\{d\}}$ and $w_{\{g,d\}}$.

Figure 17: A set of four possible worlds $W = \{w_\emptyset, w_{\{g\}}, w_{\{d\}}, w_{\{g,d\}}\}$.

Assume that an agent a cannot see the garden. They can always tell whether there is a dog in the garden by listening for barks, but cannot do the same with grasshoppers. This means that the agent is unable to distinguish between worlds $w_\emptyset$ and $w_{\{g\}}$, since both worlds have no barking. Likewise, the agent cannot distinguish between worlds $w_{\{d\}}$ and $w_{\{g,d\}}$, as barking is audible in both worlds.

This notion of indistinguishability from the perspective of an agent can be represented by introducing a binary *indistinguishability relation*[14] R_a for agent a, thus creating a modal frame (W, R_a). Since indistinguishability is an equivalence relation with reflexive, symmetric and transitive properties, this is an S5 frame.

[14] The relation used in an epistemic frame is known as an *accessibility relation*.

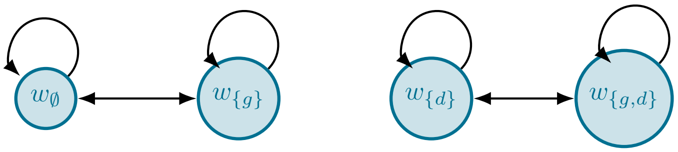


Figure 18: An S5 epistemic frame (W, R_a).

If at some world w the agent a “knows” that there is a dog in the garden (denoted as $K_a(d)$), then d must be true in all indisguishable worlds from w. On the contrary, if at some world w the agent a “knows” there is no dog in the garden (denoted as $K_a(\neg d)$), then d must be false in all indisguishable worlds from w.

Formally, the syntax and symantics of epistemic logic may be defined as follows.

- **Syntax.** A formula ϕ is defined as

  $$\phi = p \mid \neg\phi \mid (\phi \wedge \phi) \mid K_a\phi$$

  where p is a propositional letter.

- **Semantics.** A Kripke model M is a tuple $(W, R_1, R_2, \cdots, R_n, V)$ where W is a non-empty set of possible worlds, $R_i \subseteq W \times W$ is a binary indisguishability relation on W for each agent i, and V is a valuation function mapping each propositional letter to a subset of W. Let $(w, w') \in R_i$ hold if everything i knows about w is also true of w', and vice versa.

- **Inference system.** We incorporate the following axioms.

  $$\begin{aligned} K_s p &\to p \\ K_s p &\to K_s K_s p \\ p &\to K_s(\neg K_s(\neg p)) \end{aligned}$$

The above framework does not accommodate the concept of belief. However, for those that have this accommodation, the axiom $\neg B_s(\bot)$ is added.

11.3 Introduction to temporal logic

A temporal formula ϕ is defined as

$$\phi = p \mid \neg\phi \mid (\phi \vee \phi) \mid F\phi \mid P\phi$$

where p is a propositional letter. $F\phi$ means that “ϕ will be true at some point in the future” while $P\phi$ means that “ϕ was true at some point in the past”. Formally, in a Kripke frame (W, R) with valuation v and world $w \in W$, we have the following.

$$\begin{aligned} (W,R), v, w \models F\phi &\iff \text{there is some } w' \in W \text{ with } (w, w') \in R \text{ and } (W,R), v, w' \models \phi \\ (W,R), v, w \models P\phi &\iff \text{there is some } w' \in W \text{ with } (w', w) \in R \text{ and } (W,R), v, w' \models \phi \end{aligned}$$

We may then define the following symbols.

$$G\phi = \neg F \neg \phi \qquad (\phi \text{ will always be true in the future})$$
$$H\phi = \neg P \neg \phi \qquad (\phi \text{ was always true in the past})$$

In addition to the axioms for propositional logic, the basic temporal axioms K_t also include the following.

$$\begin{gathered} G(p \to q) \to (Gp \to Gq) \\ H(p \to q) \to (Hp \to Hq) \\ p \to GPp \\ p \to HFp \end{gathered}$$

To establish linear time, we create the additional axioms below.

$$\begin{aligned} Gp &\to GGp && \text{(transitivity)} \\ (Fp \land Fq) &\to (F(p \land Fq) \lor F(p \land q) \lor F(q \land Fp)) && \text{(totality)} \\ (Pp \land Pq) &\to (P(p \land Fq) \lor P(p \land q) \lor P(q \land Pp)) && \text{(totality)} \end{aligned}$$

11.4 Introduction to propositional dynamic logic (PDL)

Propositional dynamic logic (PDL) is a multimodal logic that allows us to evaluate the correctness of programs.

11.4.1 Syntax

Let $P = \{p_0, p_1, p_2, \cdots\}$ be a set of propositions. Let $\Pi = \{\pi_0, \pi_1, \cdots\}$ be a set of atomic programs.

The syntax of a program π is given by

$$\pi = \pi_i \mid (\pi; \pi) \mid (\pi + \pi) \mid \pi^* \mid \phi?$$

where π_i is an atomic program and ϕ is a formula.

The syntax of a formula ϕ is given by

$$\phi = p \mid \neg\phi \mid (\phi \lor \phi) \mid \langle\pi\rangle\phi \mid [\pi]\phi$$

where π is a program.

11.4.2 Semantics, as a labelled transition system

The semantics of PDL is given by a labelled transition system (LTS). Consider a model (W, R, v) where

- W is a non-empty set of worlds, each representing a possible program state;
- R is a function that maps each atomic program to a binary relation over W; and
- v is a valuation function mapping each propositional letter to a subset of W

Intuitively, each atomic program π_i may lead us from one program state to another program state, as directed by the binary relation $R(\pi_i)$. Propositions may be true in some program states and false in others.

We recursively extend R to map general programs to binary relations as follows.

$$\begin{aligned} R(\alpha; \beta) &= \{(w_1, w_2) \in W \times W : \text{there is some } w_3 \in W \text{ with } (w_1, w_3) \in R(\alpha) \text{ and } (w_3, w_2) \in R(\beta)\} \\ & && \text{(execute } \alpha\text{, then execute } \beta\text{)} \\ R(\alpha + \beta) &= R(\alpha) \cup R(\beta) && \text{(execute either } \alpha \text{ or } \beta\text{)} \\ R(\alpha^*) &= \cup_{n \in \mathbb{N}} R(\alpha^n) && \text{(execute } \alpha \text{ any number of times)} \\ R(\phi?) &= \{(w, w) \in W \times W : (W, R), v, w \models \phi\} && \text{(assert } \phi \text{ is true at the current program state)} \end{aligned}$$

Formulas may be evaluated as follows.

$$\begin{aligned} (W, R), v, w \models p &\iff w \in v(p) \\ (W, R), v, w \models \neg\phi &\iff (W, R), v, w \not\models \phi \\ (W, R), v, w \models (\phi_1 \lor \phi_2) &\iff (W, R), v, w \models \phi_1 \text{ or } (W, R), v, w \models \phi_2 \\ (W, R), v, w \models \langle\alpha\rangle\phi &\iff \text{there is some } w' \in W \text{ where } (w, w') \in R(\alpha) \text{ and } (W, R), v, w' \models \phi \\ (W, R), v, w \models [\alpha]\phi &\iff \text{for all } w' \in W \text{ if } (w, w') \in R(\alpha) \text{ then } (W, R), v, w' \models \phi \end{aligned}$$

For example, consider the model illustrated in Figure 19, with propositions p and q and atomic programs π_0 and π_1. Let x be the world highlighted in red.

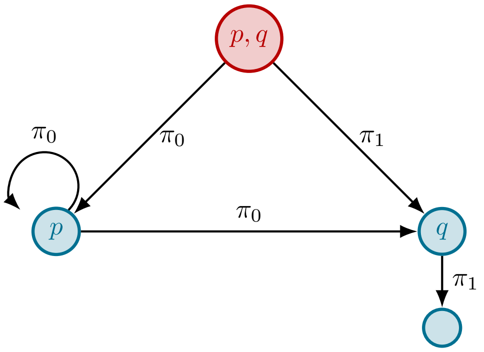


Figure 19: A set of four possible worlds $W = \{w_\emptyset, w_{\{g\}}, w_{\{d\}}, w_{\{g,d\}}\}$.

We then have the formula

$$(W, R), v, x \models p \wedge q \wedge [\pi_0^*](p \vee (q \wedge \langle \pi_1 \rangle (\neg p \wedge \neg q)))$$

which can be read as the following.

> Given the frame (W, R) and valuation v, it is true at world x that
>
> - both p and hold; and
> - from this world, all worlds reachable by executing π_0^* (i.e. by executing π_0 any number of times) satisfy the following condition:
>   - p holds; or
>   - q holds, and by executing π_1 it is possible to reach some world where neither p nor q holds.

Common programming constructs can be translated into programs in PDL. For example, the if-else statement

```
if $p$:
    execute $\pi$
else:
    execute $\pi'$
```

can be written in PDL as

$$((p?); \pi) + (((\neg p)?); \pi').$$

Meanwhile, the `while` loop

```
while $p$:
    execute $\pi$
```

can be written as

$$(p?; \pi)^*; (\neg p)?.$$

11.4.3 Inference system

In addition to propositional axioms, the inference system for PDL also requires the following axioms:

$$
\begin{aligned}
[\pi](A \to B) &\to ([\pi]A \to [\pi]B) \\
[\pi_1;\pi_2]A &\leftrightarrow [\pi_1][\pi_2]A \\
[\pi_1 + \pi_2]A &\leftrightarrow ([\pi_1]A \wedge [\pi_2]A) \\
[\pi^*]A &\leftrightarrow (A \wedge [\pi][\pi^*]A) \\
[A?]B &\leftrightarrow (A \to B)
\end{aligned}
$$

and the following inference rules.

$$\frac{A \quad (A \to B)}{B} \qquad \text{(modus ponens)}$$

$$\frac{A}{[\pi]A} \qquad \text{(necessitation)}$$

$$\frac{A \to [\pi]A}{A \to [\pi^*]A} \qquad \text{(loop invariance)}$$

PDL is useful for checking program correctness as the statement "given a pre-condition A, every terminating execution of π gives a state where the post-condition B holds" can be written as the PDL formula $(A \to [\pi]B)$.

12 Algebraic logic

12.1 Groups

A set G with a binary operation $\circ$ is said to be a *group* if the following conditions are satisified.

- **Closure.** The operation $\circ$ is closed in G, with $\circ : G \times G \to G$.
- **Associativity.** The operation $\circ$ is associative, with $(a \circ b) \circ c = a \circ (b \circ c)$ for all elements $a, b, c \in G$.
- **Identity.** There exists some identity element $e \in G$ for which $e \circ a = a \circ e = a$ for all elements $a \in G$.
- **Inverse.** Every element $a \in G$ has an inverse, denoted a^{-1}, such that $a \circ a^{-1} = a^{-1} \circ a = e$.

Such a group is typically denoted as the tuple

$$\mathcal{G} = (G, e, ^{-1}, \circ)$$

where $e \in G$ is the identity element, $^{-1} : G \to G$ is the inverse function, and the $\circ : G \times G \to G$ is the group operation. Table 9 lists some examples of groups.

Group	**Description**
$(\mathbb{Z}, 0, -, +)$	Additive group of integers
$(\mathbb{Q} \setminus \{0\}, 1, (q \mapsto 1/q), \times)$	Multiplicative group of nonzero rationals
$(\{M : M \text{ is a } n \times n \text{ invertible matrix}\}, I_n, ^{-1}, \times)$	General linear group of degree n
$(\{0, 1, \cdots, n-1\}, 0, -, +)$	Additive group of integers modulo n

Table 9: Examples of groups.

We now prove the following theorem.

Theorem (Cayley's theorem)**.** *Every group is isomorphic to a group of permutations.*

Proof. Consider a group $\mathcal{G}$ with set G and group operation $\circ$. We want to show that there exists some isomorphic group $\mathcal{P}$ with a set P of permutations and a composition operation (also denoted as $\circ$).

Let $G = \{g_1, g_2, g_3, \cdots, g_n\}$. Tabulate the output of the group operation $\circ$ by considering all possible pairs of inputs across $G \times G$.

		Left argument				
	$\circ$	g_1	g_2	g_3	$\cdots$	g_n
Right argument	g_1	$g_?$	$g_?$	$g_?$	$\cdots$	$g_?$
	g_2	$g_?$	$g_?$	$g_?$	$\cdots$	$g_?$
	g_3	$g_?$	$g_?$	$g_?$	$\cdots$	$g_?$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
	g_n	$g_?$	$g_?$	$g_?$	$\cdots$	$g_?$

Table 10: A tabulation of all possible values of $g_i \circ g_j$ where $g_i, g_j \in G$. To look up the result of the binary operation $g_i \circ g_j$, first search horizontally to locate the column marked with the left argument g_i, then search vertically to locate the row marked with the right argument g_j. Their intersection gives the operation's output.

Recall that a permutation is defined as the bijection from a set to itself. Hence, each row in this table represents a permutation of G.

$$\begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_n \\ g_? & g_? & g_? & \cdots & g_? \end{pmatrix}$$

For example, the uppermost row, which lists all possible outputs of $\circ$ with g_1 as the right argument, represents the permutation $(h \mapsto h \circ g_1)$. This permutation is a bijection because it has an inverse $(h \mapsto h \circ g_1^{-1})$.

Let $e \in G$ be the identity element. Let P be the set of permutations represented by the rows in this table. Let $\theta : G \to P$ be the function mapping each group element g_j to the permutation represented by its row. By definition, θ is surjective. Also, since

$$\begin{aligned} \theta(g_i) = \theta(g_j) &\implies e \circ g_i = e \circ g_j \\ &\implies g_i = g_j \end{aligned}$$

θ is injective. This means that θ is a bijection. Furthermore,

- $\theta(g_i \circ g_j) = \theta(g_i) \circ \theta(g_j)$ for all $g_i, g_j \in G$;
- $\theta(e)$ is the identity permutation; and
- $\theta(g^{-1}) = \theta(g)^{-1}$ for all $g \in G$.

Therefore, θ describes an isomorphism from $\mathcal{G}$ to $\mathcal{P}$. □

12.2 Boolean algebra

Let B be a set of elements including but not limited to 0 and 1. Let $+$ and $\cdot$ be binary operations on B, and let $-$ be a unary operation on B. We write the expression $-a$ as $\overline{a}$ for brevity.

The tuple $(B, 0, 1, +, \cdot, -)$ is a *Boolean algebra* if it satisfies the following axioms.

- Axioms for $+$.

$$\begin{aligned} (a + b) + c &= a + (b + c) && \text{(associativity)} \\ a + b &= b + a && \text{(commutativity)} \\ a + a &= a && \text{(idempotency)} \\ a + 0 &= a && \text{(zero law)} \end{aligned}$$

- Axioms for $-$.

$$\begin{aligned} \overline{\overline{a}} &= a \\ a + \overline{a} &= 1 \\ -1 &= 0 \\ a \cdot b &= \overline{\overline{a} + \overline{b}} && \text{(de Morgan)} \end{aligned}$$

- Distribution and absorption laws.

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c && \text{(distribution law)} \\ a + (a \cdot b) &= a && \text{(absorption law)} \end{aligned}$$

The simplest non-trivial Boolean algebra is given by the tuple $(\{0,1\},0,1,+,\cdot,-)$, where

$$a+b=\begin{cases}1 \text{ if } a=1 \text{ or } b=1\\ 0 \text{ otherwise}\end{cases}$$
$$a\cdot b=\begin{cases}1 \text{ if } a=b=1\\ 0 \text{ otherwise}\end{cases}$$
$$-a=\begin{cases}1 \text{ if } a=0\\ 0 \text{ otherwise.}\end{cases}$$

This Boolean algebra as applications in logic, interpreting 0 as "false", 1 as "true", $\cdot$ as "and", + as "or", and − as "not".

12.3 Boolean set algebra and representations

Let X be a non-empty set. This serves as our *base*, from which we construct various Boolean algebras. Let $P(X)$ be its power set.

A *Boolean set algebra* is a special kind of Boolean algebra that consists a subset B of $P(X)$ whose elements are closed under the operations of union ($\cup$), intersection ($\cap$) and complement relative to X.

$$\mathcal{B}(X)=(B,\emptyset,X,\cup,\cap,\setminus) \qquad (B\subseteq P(X))$$

The most typical example uses the entire power set $P(X)$, but any *subalgebra* (i.e. any Boolean algebra that uses a subset of $P(X)$) is also a Boolean set algebra. For example, take $X=\{1,2,3\}$. Its power set

$$P(X)=\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$$

gives the Boolean set algebra

$$\{P(X),\emptyset,X,\cup,\cap,\setminus\}.$$

Any subalgebra thereof, such as

$$\{\{\emptyset,\{1,2\},\{3\},X\},\emptyset,X,\cup,\cap,\setminus\}$$

is also a Boolean set algebra.

Let $\mathcal{B}=(B,0,1,+,\cdot,-)$ be a Boolean algebra. An injection $\theta:B\to P(X)$ for some set X is called a *representation* if it is an isomorphism from $\mathcal{B}$ to some Boolean set algebra $(P(X),\emptyset,X,\cup,\cap,\setminus)$.

$$\begin{aligned}\theta(0)&=\emptyset\\ \theta(1)&=X\\ \theta(a+b)&=\theta(a)\cup\theta(b)\\ \theta(a\cdot b)&=\theta(a)\cap\theta(b)\\ \theta(-a)&=X\setminus a\end{aligned}$$

12.4 Atoms

Define the transitive relation $a\le b$ as $a+b=b$. In a Boolean set algebra, this is equivalent to saying that $a\subseteq b$. We also write $a<b$ if and only if $a\le b\wedge b\not\le a$.

Let $\mathcal{B}=(B,0,1,+,\cdot,-)$ be a Boolean algebra. An *atom* of $\mathcal{B}$ is any minimal non-zero element of B, i.e. any element $a\in B$ such that $0<a$ and there is no element $b\in B$ with $0<b<a$. We denote the set of atoms as $\mathrm{At}(\mathcal{B})$.

In a Boolean set algebra, an atom corresponds to a bounded Venn diagram region that cannot be further subdivided.

A Boolean algebra is said to be *atomic* if every nonzero element is above an atom. All finite Boolean algebras are atomic; but some infinite Boolean algebras may have no atom whatsoever.

Theorem. *A Boolean algebra $\mathcal{B}$ with n atoms must have 2^n elements.*

Proof. Notice that any element $b \in \mathcal{B}$ can be expressed uniquely as a sum of zero or more atoms.

$$b = \sum \{a \in \mathrm{At}(\mathcal{B}) : a \leq b\}$$

Hence the number of elements is equal to the number of subsets of the set of atoms, which is 2^n. □

Theorem. *All atomic Boolean algebras are representable.*

Proof. For any atomic Boolean algebra $\mathcal{B}$, we show that the map $\theta : \mathcal{B} \to P(\mathrm{At}(\mathcal{B}))$ defined by

$$\theta(b) = \{a \in \mathrm{At}(\mathcal{B}) : a \leq b\}$$

is a representation of $\mathcal{B}$ over $\mathrm{At}(\mathcal{B})$. To do this, we must prove that

(a) θ is injective; and

(b) θ is an isomorphism.

We start by showing that (a) θ is injective. Let b and c be two distinct elements in $\mathcal{B}$. Since $b \neq c$, we must have either $b \not\leq c$ or $c \not\leq b$. We assume the former case without loss of generality.

$$\begin{aligned} b &\not\leq c \\ b + c &\neq c \end{aligned}$$

We prove by contradiction that $b \cdot \overline{c} \neq 0$.

> *Proof by contradiction:* $b \cdot \overline{c} \neq 0$.
>
> Assume that $b \cdot \overline{c} = 0$. Therefore, by the axioms of Boolean algebra,
>
> $$\begin{aligned} b + c &= (b \cdot 1) + c \\ &= (b \cdot (c + \overline{c})) + c \\ &= (b \cdot c + b \cdot \overline{c}) + c \\ &= (b \cdot c + 0) + c && \text{(by assumption)} \\ &= (b \cdot c) + c \\ &= c \end{aligned}$$
>
> which contradicts our previous result of $b + c \neq c$. Hence we have $b \cdot \overline{c} \neq 0$.

Since $b \cdot \overline{c} \neq 0$, there exists some atom $a \in \mathrm{At}(\mathcal{B})$ where $a \leq b \cdot \overline{c}$. Therefore, we have $a \leq b$ but $a \not\leq c$, which means that $a \in \theta(b)$ but $a \notin \theta(c)$. This implies $\theta(b) \neq \theta(c)$, so θ is injective.

Moreover, it can be shown that (b) θ is an isomorphism because

- it preserves the constants $\theta(0) = \emptyset$ and $\theta(1) = \mathrm{At}(\mathcal{B})$.
- it preserves the binary operations $\theta(a + b) = \theta(a) \cup \theta(b)$ and $\theta(a \cdot b) = \theta(a) \cap \theta(b)$.
- it preserves the negation operation $\theta(-a) = \mathrm{At}(\mathcal{B}) \setminus \theta(a)$. □

In fact, the above theorem can be generalised as follows.

Theorem (Stone's Theorem, 1936)**.** *All Boolean algebras is representable. In other words, every Boolean algebra, finite or not, is isomorphic to a Boolean set algebra.*

12.5 Free generation

Given a base set X of elements called *generators*, we may *freely generate* a Boolean algebra $\mathcal{B} = (B, 0, 1, +, \cdot, -)$ where elements of B are constructed from the generators via operations $+$, $\cdot$ and $-$.

$$B = \{b : b \text{ can be expressed in terms of generators in } X \text{ and operations } +, \cdot, -\}$$

No two elements in B can be equivalent under Boolean algebra axioms. Also, the generators must be as independent as possible with no presumed relationships among them.

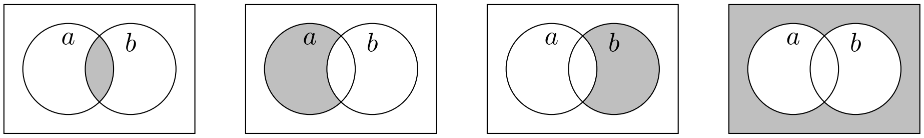
For example, taking $X = \{a, b\}$ produces a set B with 4 atoms

$$\mathrm{At}(B) = \{\overline{a} \cdot \overline{b},\ \overline{a} \cdot b,\ a \cdot \overline{b},\ a \cdot b\}$$

and 16 elements, expressed as sums of products below.

$$\begin{aligned}
B = \{&a \cdot \overline{a}, && \text{(equivalent to 0 or } \emptyset) \\
&\overline{a} \cdot b, \\
&a \cdot b, \\
&b, \\
&a \cdot \overline{b}, \\
&a \cdot \overline{b} + \overline{a} \cdot b, \\
&a, \\
&a + b, \\
&\overline{a} \cdot \overline{b}, \\
&\overline{a}, \\
&a \cdot b + \overline{a} \cdot \overline{b}, \\
&\overline{a} + b, \\
&\overline{b}, \\
&\overline{a} + \overline{b}, \\
&a + \overline{b}, \\
&a + \overline{a} && \text{(equivalent to 1)} \\
\}&
\end{aligned}$$

The atoms $\mathrm{At}(B)$ can be visualised as the four bounded and indivisible regions in a two-set Venn diagram, as shown in Figure 20. Likewise, B can be visualised as the set of possible fillings of a 2-set Venn diagram, as illustrated (in the order given above) in Figure 21.



$a \cdot b$ $\qquad$ $a \cdot \overline{b}$ $\qquad$ $\overline{a} \cdot b$ $\qquad$ $\overline{a} \cdot \overline{b}$

Figure 20: The 4 atoms of a Boolean algebra freely generated from a two-element base set $\{a, b\}$. The sets a and b are not disjoint since they are assumed to be as independent as possible.

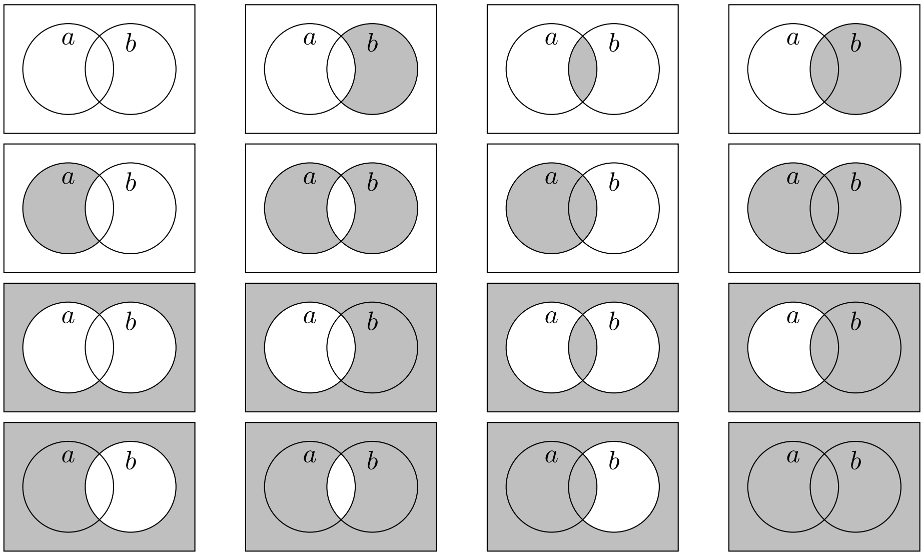


Figure 21: Each element of B corresponds to a possible filling of a 2-set Venn diagram. Read from left to right and from top to bottom.

Theorem. *A Boolean algebra freely generated from a set of* n*elements must have* 2^n *atoms and* 2^{2^n} *elements.*

Proof. Each atom corresponds to a unique truth assignment to the n generators. Since there are 2^n such assignments, there must be 2^n atoms. It follows from a previous theorem that such an algebra must have 2^{2^n} elements. □

Note that not all Boolean algebras have to be freely generated from a base set. Hence,

- In general, the number of atoms in a Boolean algebra is not necessarily a power of 2.
- However, the number of elements in a Boolean algebra is always 2^n, where n is the number of atoms.

12.6 Sum of products

Every Boolean term t, defined by

$$\text{term} = \text{variable} \mid 0 \mid 1 \mid (\text{term} + \text{term}) \mid (\text{term} \cdot \text{term}) \mid -\text{term}$$

can be expressed as a sum of products using any of the following methods.

- Treat t as a propositional formula by replacing the operations $+$, $\cdot$ and $-$ with $\vee$, $\wedge$ and $\neg$. Using a tableau, to identify an equivalent DNF formula, which is by definition a sum of products.
- Construct a truth table. The sum of products of possibly negated variables in the rows evaluating to 1 must equal t.
- Drive down negations by replacing
  - $\overline{a+b}$ by $\overline{a} \cdot \overline{b}$;
  - $\overline{a \cdot b}$ by $\overline{a} + \overline{b}$; and
  - $\overline{\overline{a}}$ by a.

Use the distribution law if $\cdot$ is above $+$.

$$(a+b)\cdot(c+d) = a\cdot c + a\cdot d + b\cdot c + b\cdot d$$

This ultimately results in a sum of products.

12.7 Relation algebras

For any base set X, a set $a \subseteq X \times X$ is said to be a *binary relation* over X.

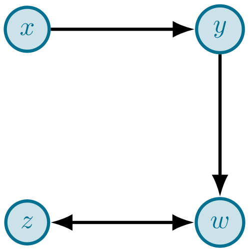


Figure 22: A binary relation a over a base set X can be visualised as a directed graph (X, a).

If $\mathrm{Rel}(X)$ denotes the set of all possible binary relations over X,

$$\mathrm{Rel}(X) = \{a : a \subseteq X \times X\} = P(X \times X)$$

then

$$(\mathrm{Rel}(X), \emptyset, X \times X, \cup, \cap, \setminus)$$

is a Boolean set algebra.

We denote the identity relation as $\mathrm{Id}_X = \{(x,x) : x \in X\}$.

Given a binary relation a, its *converse* is defined as $a^{\smile} = \{(x,y) : (y,x) \in a\}$.

Given two binary relations a and b, we can create a new binary relation using the *composition* operator, denoted using the semicolon.

$$a;b = \{(x,y) : \exists z\ (((x,z) \in a) \wedge ((z,y) \in b))\}$$

Figure 23: The identity relation.

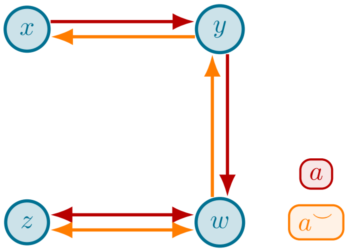


Figure 24: The converse of a relation can be obtained by reversing the arrows in its directed graph.

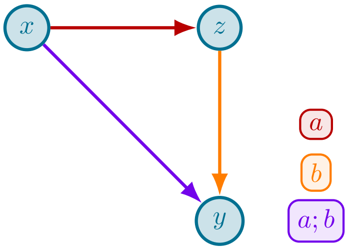


Figure 25: A composition of two relations.

A set of relations $A \in \mathrm{Rel}(X)$ is called a *proper relation algebra* if

- A contains a biggest relation $U \in \mathrm{Rel}(X)$ and a smallest relation $\emptyset$,
- $(A, \emptyset, U, \cup, \cap, U, \setminus)$ is a Boolean set algebra,
- A includes Id_X, and
- for each $a, b \in A$, we have $a^\smile \in A$ and $a;b \in A$.

A tuple

$$\mathcal{A} = (A, 0, 1, +, \cdot, -, 1', ^\smile, ;)$$

with

- a set $A \subseteq \mathrm{Rel}(X)$,
- Boolean constants 0, 1 and an identity relation $1'$,
- unary operations $-$ and $^\smile$, and
- binary operations $+$, $\cdot$ and ;

is called an *abstract relation algebra*, or simply a *relation algebra*, if it satisfies the following axioms.

- $(A, 0, 1, +, \cdot, -)$ is a Boolean algebra.
- $(A, 1', ;)$ is a monoid, i.e.
  - ; is associative.
  - for all $a \in A$, we have $1'; a = a; 1' = a$.
- Additivity holds for both ; and $^\smile$.

$$(a + b); (c + d) = a; c + a; d + b; c + b; d$$
$$(a + b)^\smile = a^\smile + b^\smile$$

- For all $a \in A$, we have $0^\smile = 0; a = a; 0 = 0$.
- Convolution: For all $a, b \in A$, we have

$$(a^\smile)^\smile = a$$
$$(a; b)^\smile = b^\smile; a^\smile.$$

- Triangle law: For all $a, b, c \in A$, we have $(a; b) \cdot c^\smile = 0 \iff (b; c) \cdot a^\smile = 0$.

The triangle law can be explained by considering its contrapositive.

$$(a;b) \cdot c^{\smile} \neq 0 \iff (b;c) \cdot a^{\smile} \neq 0$$

Suppose we have $(a;b) \cdot c^{\smile} \neq 0$. Since the relations $a;b$ and $c^{\smile}$ have a nonzero intersection, there must be some element of $(x,z) \in X \times X$ that is in $a;b$ and $c^{\smile}$. Visually, these two relations must share at least one arrow, as shown in Figure 26. Using the definition of composition, there must be some element $y \in X$ such that $(x,y) \in a$ and $(y,z) \in b$. Also, since $(x,z) \in c^{\smile}$, we have $(z,x) \in c$. This allows us to construct the triangular configuration shown in Figure 27.

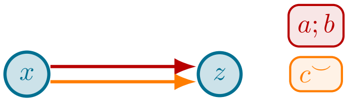


Figure 26: The inequality $(a;b) \cdot c^{\smile} \neq 0$ holds if and only if $a;b$ and $c^{\smile}$ share at least one arrow.

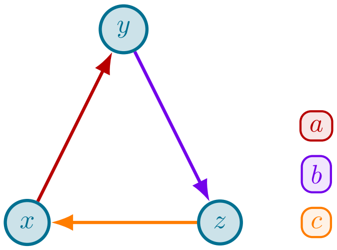


Figure 27: The inequality $(a;b) \cdot c^{\smile} \neq 0$ gives a triangular arrow configuration.

Since the arrows in Figure 27 all point in the same clockwise direction, rotating the figure preserves the triangular shape.

$$\begin{aligned}\text{Arrows in } a,b,c \text{ form a triangle} &\iff \text{Arrows in } b,c,a \text{ form a triangle}\\ &\iff \text{Arrows in } c,a,b \text{ form a triangle}\end{aligned}$$

Therefore,

$$\begin{aligned}(a;b) \cdot c^{\smile} \neq 0 &\iff (b;c) \cdot a^{\smile} \neq 0\\ &\iff (c;a) \cdot b^{\smile} \neq 0\end{aligned}$$

which gives the triangle law.

An isomorphism θ from an abstract relation algebra $\mathcal{A} = (A, 0, 1, +, \cdot, -, 1', {}^{\smile}, ;)$ into a proper relation algebra $\mathrm{Rel}(X)$ (for some non-empty set X) is called a *representation* of $\mathcal{A}$. RRA denotes the class of all representable relation algebras.

For example, consider an abstract relation algebra $\mathcal{P}$ with atoms $1'$, $<$ and $>$. Since there are 3 atoms, $\mathcal{P}$ must have a total of $2^3 = 8$ elements.

- Converses are defined as follows.

$$\begin{aligned}<^{\smile} &=>\\ >^{\smile} &=<\\ (1')^{\smile} &= 1'\end{aligned}$$

- Compositions are defined in the following table.

$;$	$1'$	$<$	$>$
$1'$	$1'$	$<$	$>$
$<$	$<$	$<$	$(1'+<+>)$
$>$	$>$	$(1'+<+>)$	$>$

- Other converses and compositions are defined on sums of atoms by additivity.

A representation θ of P can be constructed using the set $\mathbb{Q}$ of rational numbers as a base.

$$\theta(1') = \mathrm{Id}_{\mathbb{Q}} = \{(q,q) : q \in \mathbb{Q}\}$$
$$\theta(<) = \{(q,r) : q < r,\ q,r \in \mathbb{Q}\}$$
$$\theta(>) = \{(q,r) : q > r,\ q,r \in \mathbb{Q}\}$$

However, $\mathbb{P}$ has no representation over a finite base. This is because for any base X, there must exist two elements $x, y \in X$ such that $(x,y) \in \theta(<)$, as θ is injective and $\theta(0)$ gives the empty set. Since $< \cdot 1' = 0$, this implies that $(x,y) \notin \theta(1')$ and $x \neq y$. Since $<=<;<$, there must be some z such that $(x,z),(z,y) \in \theta(<)$. It follows that for any $n \in \mathbb{N}$ there are elements $z_0, z_1, \cdots, z_{n-1}$ such that

$$(x,z_0),(z_i,z_i+1),(z_{n-1},y) \in \theta(<)$$

for all $i < n-1$, with $x, z_0, z_1, \cdots, z_{n-1}, y$ all distinct. Therefore, X must be infinite.

12.8 Monk algebra

Named after logician J. Donald Monk, a *Monk algebra* refers to a specific type of relation algebra used in logic and combinatorics to study representability. For example, consider an abstract relation algebra $\mathcal{M}$ with the atoms $1'$, r and b. Suppose these atoms are *self-converse*, so their converses are themselves.

$$(1')^{\smile} = 1'$$
$$r^{\smile} = r$$
$$b^{\smile} = b$$

Their compositions are given by the composition table below.

$;$	$1'$	r	b
$1'$	$1'$	r	b
r	r	$(1'+b)$	$(r+b)$
b	b	$(r+b)$	$(1'+r)$

Using red and blue edges for relations r and b respectively, this means that any representation of $\mathcal{M}$ must not contain any monochromatic triangles, i.e. triangles with either three red edges or three blue edges. This is shown in Figure 28.

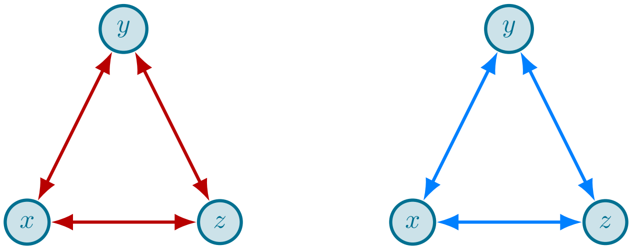


Figure 28: Monochromatic triangles are forbidden in any representation of $\mathcal{M}$.

In Ramsey theory, the *representability problem* asks whether Monk algebras, such as the one defined above, can be concretely represented as proper relation algebras. Here, we will specifically consider proper relation algebras that represent an edge coloring of a complete graph[15]. For instance, Figure 29 shows two base-isomorphic representations of $\mathcal{M}$ as a complete graph with five vertices.

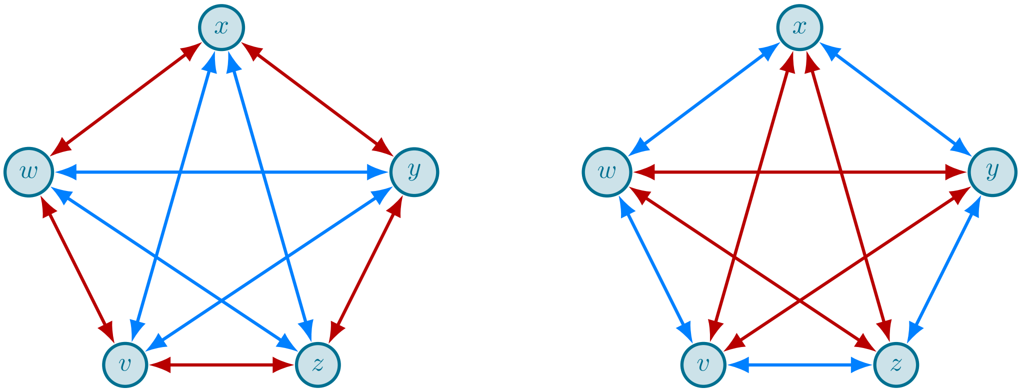


Figure 29: Two representations of $\mathcal{M}$, which are base isomorphic to each other.

Theorem (Special case of Ramsey's theorem)**.** *The Monk algebra $\mathcal{M}$, as defined above, does not have any representation in a complete graph of six vertices. In other words, it is impossible to colour the edges of a complete graph of six vertices without creating any monochromatic triangles.*

Proof. Proof by contradiction. Assume the contrary, meaning that there is some representation of $\mathcal{M}$ in a complete graph of six vertices $\{v_0, v_1, v_2, v_3, v_4, v_5\}$.

Since the graph is complete, v_0 must have 5 outgoing edges, each of which is either red or blue. By the pigeonhole principle, at least 3 of these edges must be the same colour. Without loss of generality, assume that the edges from v_0 to v_1, v_2 and v_3 are all red. See Figure 30.

Notice that both edges $v_0 \longleftrightarrow v_1$ and $v_0 \longleftrightarrow v_2$ are red. To avoid the monochromatic triangles, the edge $v_1 \longleftrightarrow v_2$ must be blue.

Similarly, the edges $v_2 \longleftrightarrow v_3$ and $v_1 \longleftrightarrow v_3$ must be blue too. However, this creates a monochromatic triangle with vertices v_1, v_2 and v_3, violating the original assumption. See Figure 31. □

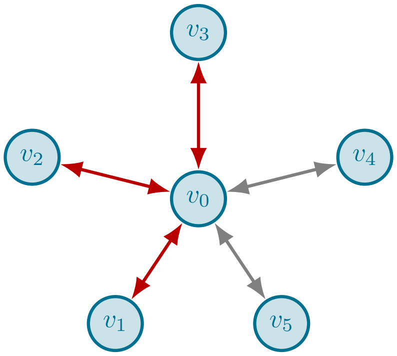


Figure 30: At least 3 of 5 outgoing edges from v_0 must be the same colour.

[15] A graph is said to be *complete* if every distinct pair of vertices is connected by a single unique edge.

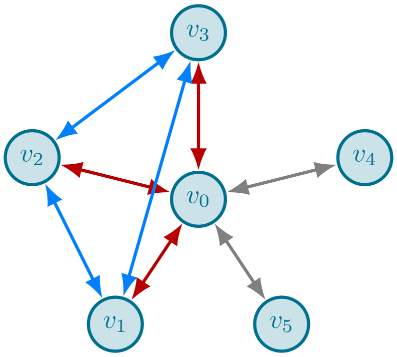


Figure 31: It is impossible to colour the edges of a complete graph of six vertices without creating any monochromatic triangles.

Now consider a slightly different Monk algebra $\mathcal{M}'$ where the red atom r has been split into two separate atoms r_1 and r_2. This gives a total of four self-converse atoms $1'$, r_1, r_2 and b, with the following composition table. Like before, this composition table forbids any monochromatic triangles.

;	$1'$	r_1	r_2	b
$1'$	$1'$	r_1	r_2	b
r_1	r_1	$(1' + b)$	b	$(r_1 + r_2 + b)$
r_2	r_2	b	$(1' + b)$	$(r_1 + r_2 + b)$
b	b	$(r_1 + r_2 + b)$	$(r_1 + r_2 + b)$	$(1' + r_1 + r_2)$

Theorem. *The Monk algebra $\mathcal{M}'$, as defined above, has no representation in any complete graph.*

Proof. Proof by contradiction. Assume the contrary that $\mathcal{M}'$ has a representation in a complete graph with n vertices.

Since $b > 0$, there must be at least one blue edge $x \longleftrightarrow y$. In order for the composition

$$r_1; r_2 = b$$

to hold, there must be some other vertex z_1 such that the edges $x \longleftrightarrow z_1$ and $z_1 \longleftrightarrow y$ have colours r_1 and r_2 respectively. This is shown in Figure 32.

Similarly, the compositions

$$\begin{aligned} r_1; r_1 &= (1' + b) \\ r_1; b &= (r_1 + r_2 + b) \\ r_2; r_1 &= b \\ r_2; r_2 &= (1' + b) \\ r_2; b &= (r_1 + r_2 + b) \\ b; r_1 &= (r_1 + r_2 + b) \\ b; r_2 &= (r_1 + r_2 + b) \end{aligned}$$

all require distinct intermediate vertices between x and y, as seen in Figure 33.

Clearly, this graph must have over six vertices. As previously proved, this graph must contain at least one monochromatic triangle and hence cannot be a representation of $\mathcal{M}'$, violating our original assumption. □

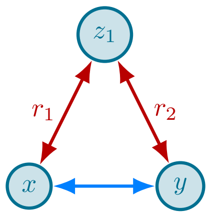


Figure 32: The presence of a blue edge requires a third intermediate vertex z_1.

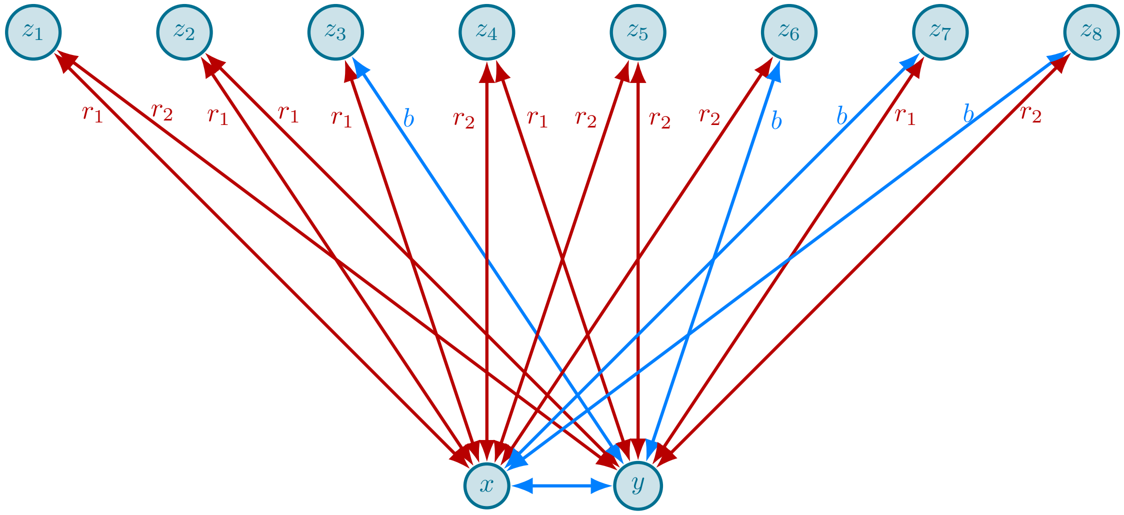


Figure 33: In total, eight intermediate vertices are required by a blue edge.

As exemplified by the theorem above, not all relation algebras are representable.

$$\mathrm{RRA} \subsetneq \mathrm{RA}$$

12.9 Characterising representability by games

Note: This section is written with reference to the article "Games in Algebraic Logic: Axiomatisations and Beyond" (2005) by Robin Hirsch and Ian Hodkinson.

Determining whether a relation algebra is representable is an undecidable problem. Here, we devise a two-player game to test the representability of atomic relation algebras.

Let $\mathcal{A}$ be a finite atomic relation algebra. Let G be a complete directed graph with nodes X and edges $X \times X$. We may label each edge in this complete graph with the corresponding atom using a labelling function $N : X \times X \to \mathrm{At}(\mathcal{A})$. This labelling function (or the resultant labelled graph) is called a *network* and must satisfy the following conditions.

$$N(x, y) \leq 1' \iff x = y$$
$$N(y, x) = (N(x, y))^{\smile}$$
$$N(x, y); N(y, z) \geq N(x, z)$$

These may be read as follows.

- All reflexive edges are labelled with atoms below the identity. Note that the identity does not necessarily have to be an atom.
- Whenever an edge is labelled with an atom, the converse must be labelled with the converse atom.

- No forbidden triangles are allowed.

The game consists of n *rounds* (where n is either finite or countably infinite) and has two players: $\forall$ (male) and $\exists$ (female).

- If $n = 0$, there are no rounds and $\exists$ is declared the winner.
- In round 0, $\forall$ selects some atom $a_0 \in \mathrm{At}(\mathcal{A})$. Then, $\exists$ responds by playing a network N_0 containing a_0 as a label.
- In round t $(1 \leq t < n)$,
  - Let N_{t-1} be the current network at the start of the round.
  - $\forall$ selects some existing edge (x, y) in the network with the label $N_{t-1}(x, y)$. Then, he selects atoms $a, b \in \mathrm{At}(\mathcal{A})$ such that $a; b \geq N_{t-1}(x, y)$.
  - If there already exists a node z such that $N_{t-1}(x, z) = a$ and $N_{t-1}(z, y) = b$, then $\exists$ does not have to do anything, resulting in $N_t = N_{t-1}$.
  - Otherwise, she must begin by adding a new node z to N_{t-1}, labelling the edges (x, z) with a and (z, y) with b. This forms the basis of the new network N_t. Finally, she must complete the labelling of N_t by defining $N_t(u, v)$ for all remaining pairs (u, v) of nodes. These are the ones other than (x, z), (z, y) and pairs of nodes of N_{t-1}, whose labels are already fixed.
  - If $\exists$ fails to complete the labelling and create a new network, she loses.
- It can be very hard for $\exists$ to complete the labelling. N_t must be a network, so all its triangles must be consistent. Moreover, N_t is then passed on to the next round (if any), in which $\forall$ can make new choices and potentially force a loss for $\exists$.
- If $\exists$ has a winning strategy where she always responds legally to $\forall$'s moves, she wins.

Note the following theorem regarding this game.

Theorem. *Let $\mathcal{A}$ be a finite relation algebra.*

- *$\mathcal{A}$ is a representable relation algebra if and only if $\exists$ has a winning strategy in a game of countably infinite rounds.*
- *$\exists$ has a winning strategy in a game of countably infinite rounds if and only if she has a winning strategy in a game of n rounds for all finite n.*
- *For all finite n, we can construct first-order sentences σ_n such that $A \models \sigma_n$ if and only if $\exists$ has a winning strategy in a game of n rounds.*

It follows from this theorem that for any finite relation algebra $\mathcal{A}$,

$$\mathcal{A} \in \mathrm{RRA} \iff \mathcal{A} \models \{\sigma_n : n \in \mathbb{N}\}.$$

For any infinite atomic relation algebra $\mathcal{A}$, we have

$$\mathcal{A} \models \{\sigma_n : n \in \mathbb{N}\} \Rightarrow \mathcal{A} \in \mathrm{RRA}.$$

12.10 An example of the representability game, using Ramsey numbers

Let K_n be the complete irreflexive undirected graph on n vertices. Given k colours

$$C_k = \{C_0, C_1, \cdots, C_{k-1}\}$$

a *k-colour edge colouring* of K_n is a function mapping each edge of K_n to a colour in C_k such that there are no monochromatic triangles.

Consider the following sequence.

$$M(k) = \begin{cases} 2 & \text{if } k = 0 \\ 2 + k \cdot (M(k-1) - 1) & \text{otherwise} \end{cases}$$

Theorem. *For all $k \in \mathbb{N}$, it is impossible to construct a k-colour edge colouring for a complete irreflexive undirected graph on $M(k)$ vertices.*

Proof. Proof by induction.

Base case. For $k = 0$, a complete irreflexive undirected graph has one edge. Since no colours are available, an edge colouring cannot be constructed.

Step case. Assume for some $k \in \mathbb{N}$ that it is impossible to construct a k-colour edge colouring for $K_{M(k)}$. We want to show that it is also impossible to construct a $(k+1)$-colour edge colouring for $K_{M(k+1)}$, where $M(k+1) = 2 + (k+1) \cdot (M(k) - 1)$.

Suppose, for contradiction, that such a colouring exists for $K_{M(k+1)}$.

Select any vertex v. As the graph is complete, the vertex v must be connected to

$$\begin{aligned} M(k+1) - 1 &= 2 + (k+1) \cdot (M(k) - 1) - 1 \\ &= 1 + (k+1) \cdot (M(k) - 1) \end{aligned}$$

other vertices. By the pigeonhole principle, there must be some colour c that appears on at least $M(k)$ of those edges.

Let G be the subgraph formed by vertices to which v is connected via an edge of colour c. Since the original graph forbids any monochromatic triangles, G must not contain any edge coloured c. (Otherwise, the original graph would have a monochromatic triangle, coloured c, involving the vertex v.) Hence, G is a complete irreflexive undirected graph which contains k colours but no monochromatic triangles. This is a contradiction which violates the induction hypothesis.

It follows that there is no $(k+1)$-colour edge colouring for $K_{M(k+1)}$.

By principles of induction, there is no k-colour edge colouring in $K_{M(k)}$ for any $k \in \mathbb{N}$. □

k	$M(k)$
0	2
1	3
2	6
3	17
$\vdots$	$\vdots$

Table 11: The sequence $M(k)$ serves upper bounds for Ramsay numbers $R(k, 3)$.

Now consider a Monk algebra $\mathcal{M}_n$ with $n+1$ atoms.

$$\text{At}(\mathcal{M}_n) = \{1'\} \cup \{a_i : i < n\}$$

We define composition as follows, forbidding any monochromatic triangles.

$$\begin{aligned} 1'; x &= x && \text{(for all } x \in \mathrm{At}(\mathcal{M}_n)\text{)} \\ x; 1' &= x && \text{(for all } x \in \mathrm{At}(\mathcal{M}_n)\text{)} \\ a_i; a_j &= \begin{cases} -a_i \text{ if } i = j \\ -1' \text{ otherwise} \end{cases} \end{aligned}$$

We know from the theorem above that $\mathcal{M}_n$ has no representation with $M(n)$ points or more.

Create a new Monk algebra $\mathcal{M}'_n$ by splitting the atom a_0 into $M(n)$ atoms. This means that $\mathcal{M}'_n$ has atoms

$$\mathrm{At}(\mathcal{M}'_n) = \{a_0^i : i < M(n)\} \cup \{1'\} \cup \{a_i : 1 \leq i < n\}.$$

Like $\mathcal{M}_n$, Any representation of this new algebra $\mathcal{M}'_n$ must have fewer than $M(n)$ points. However, this is not enough to witness all these atoms. Hence, $\mathcal{M}_n$ has no representation whatsoever.

We will investigate this by comparing with the representability game.

At the start of each round t ($1 \leq t < M(n)$), the network is N_{t-1}. $\forall$ selects some existing edge (x, y) in the network with the label $N_{t-1}(x, y)$. Then, he selects atoms $a, b \in \mathrm{At}(\mathcal{A})$ such that $a; b \geq N_{t-1}(x, y)$. $\exists$ must then respond by adding a new node and completing the labelling.

- $\exists$ has a winning strategy in $G_n(\mathcal{M}'_n)$. She can simply label new edges with colours that are distinct from each other and also distinct from a and b. However, this winning strategy only lasts for the first n rounds, as the colours will eventually run out.
- $\forall$ has a winning strategy in $G_{M(n)}(\mathcal{M}'_n)$.
  - In round 0, $\forall$ selects the atom a_1. Thus, $\exists$ must respond with a network with an edge (x, y) labelled a_1.
  - In each subsequent round, $\forall$ selects this edge (x, y). He also selects the atoms a_0^i and a_1, since $a_0^i; a_1 \geq a_1$. The value of i increases from 0 to $M(n) - 1$ as the rounds go on. It can be proven that $\exists$ must create a monochromatic triangle at some point in these rounds, giving $\forall$ the victory.

12.11 RRA is not finitely axiomatisable

Theorem. *The class of representable relation algebras, or RRA, is not finitely axiomatisable.*

Proof. Any finite set of axioms can be combined via conjunction to form a single equivalent axiom ϕ. Suppose, for contradiction, that there is some axiom ϕ such that for all relation algebras $\mathcal{A} \in \mathrm{RA}$, we have

$$\mathcal{A} \models \phi \iff \mathcal{A} \in \mathrm{RRA}.$$

Let Σ be the theory

$$\underbrace{\{\neg\phi\}}_{\mathcal{A} \text{ is not representable}} \cup \underbrace{\{\sigma_i : i \in \mathbb{N}\}}_{\exists \text{ has winning strategy}} \cup \underbrace{\{\forall x\ (x \neq 0 \to \exists y \in \mathrm{At}\ (y \leq x))\}}_{\mathcal{A} \text{ is atomic}}.$$

Any finite subset S of this theory must be contained in

$$\underbrace{\{\neg\phi\}}_{\mathcal{A} \text{ is not representable}} \cup \underbrace{\{\sigma_i : i < n\}}_{\exists \text{ has temporary winning strategy}} \cup \underbrace{\{\forall x\ (x \neq 0 \to \exists y \in \mathrm{At}\ (y \leq x))\}}_{\mathcal{A} \text{ is atomic}}$$

for some finite n.

Notice that $\mathcal{M}'_n$ is atomic, not representable, and provides $\exists$ with a temporary winning strategy. Therefore, $\mathcal{M}'_n \models S$.

By the compactness theorem, Σ has a model $\mathcal{A}$. By definition of Σ, this model $\mathcal{A}$ is an atomic relation algebra that is not representable but provides $\exists$ with a winning strategy, which is absurd.

Hence, RRA cannot be defined by finitely many axioms. $\square$