Queens' College Cambridge

Logic and Proof

Alistair O'Brien

Department of Computer Science

June 25, 2021

Contents

1 Propositional Logic

1.1 Syntax

Definition 1.1.1. (**Propositional Logic**) $\Sigma_P = \{P_1, \ldots\}$ is the countably infinite set of propositional symbols. $\Omega_0 = \{\top, \bot, \neg, \wedge, \vee, \rightarrow, \longleftrightarrow\}$ is the set of operators with arity $\alpha : \Omega_0 \to \mathbb{N}$.

The formal language, or syntax, of the propositional logic is $\mathcal{L}_0(\Omega_0) = \mathbb{T}_{\Omega_0}(\Sigma_P)$, that is:

$$\begin{array}{rcl} \psi & \texttt{::=} & P \in \Sigma_P \\ & \texttt{|} & \underbrace{o(\psi_1, \ldots, \psi_n)}_{\texttt{where } \alpha(o)=n} \end{array}$$

- **Precedence**: (in order) of operators in Ω_0: $\longleftrightarrow < \rightarrow < \vee < \wedge < \neg$.
- $\psi_1 \equiv \psi_2$ denotes syntactically identical propositions (abstract syntax trees).

1.2 Semantics

- Boolean Algebra $\mathbf{B} = (\{0, 1\}, +, \cdot)$ where $\mathbb{B} = \{0, 1\}$.

Definition 1.2.1. (**Interpretation**) The interpretation $\mathcal{I}$ of the proposition $\psi \in \mathcal{L}_0$ is a function $\mathcal{I} : \Sigma_P \to |\mathbf{B}|$. The set of interpretations is denoted $\Sigma_{\mathcal{I}} = \mathcal{P}\left[\Sigma_P \to |\mathbf{B}|\right]$.

Definition 1.2.2. (**Valuation**) The *truth* value of the proposition $\psi \in \mathcal{L}_0$ in the context of the interpretation $\mathcal{I}$, denoted $\mathcal{T}\left[\!\left[\psi\right]\!\right]_{\mathcal{I}}$, where $\mathcal{T}\left[\!\left[\cdot\right]\!\right]_{\mathcal{I}} : \mathcal{L}_0 \to |\mathbf{B}|$

is inductively defined by

$$
\begin{array}{rlrl}
\mathcal{T}\,[\![\top]\!]_{\mathcal{I}} &= 1 & \mathcal{T}\,[\![\bot]\!]_{\mathcal{I}} &= 0 \\
\mathcal{T}\,[\![P]\!]_{\mathcal{I}} &= \mathcal{I}(P) & \mathcal{T}[\neg\psi] &= \overline{\mathcal{T}\,[\![\psi]\!]_{\mathcal{I}}} \\
\mathcal{T}\,[\![\psi_1 \land \psi_2]\!]_{\mathcal{I}} &= \mathcal{T}\,[\![\psi_1]\!]_{\mathcal{I}} \cdot \mathcal{T}\,[\![\psi_2]\!]_{\mathcal{I}} & \mathcal{T}\,[\![\psi_1 \lor \psi_2]\!]_{\mathcal{I}} &= \mathcal{T}\,[\![\psi_1]\!]_{\mathcal{I}} + \mathcal{T}\,[\![\psi_2]\!]_{\mathcal{I}} \\
\mathcal{T}\,[\![\psi_1 \to \psi_2]\!]_{\mathcal{I}} &= \overline{\mathcal{T}\,[\![\psi_1]\!]_{\mathcal{I}}} + \mathcal{T}\,[\![\psi_2]\!]_{\mathcal{I}} & \mathcal{T}\,[\![\psi_1 \longleftrightarrow \psi_2]\!]_{\mathcal{I}} &= \overline{\mathcal{T}\,[\![\psi_1]\!]_{\mathcal{I}} \oplus \mathcal{T}\,[\![\psi_2]\!]_{\mathcal{I}}}
\end{array}
$$

- **Notation**: $\vDash_{\mathcal{I}} \psi \iff \mathcal{T}\,[\![\psi]\!]_{\mathcal{I}} = 1$.

Lemma 1.2.1. (**Coincidence Lemma I**) For all $\psi \in \mathcal{L}_0$ and $\mathcal{I}, \mathcal{I}' \in \Sigma_{\mathcal{I}}$,

$$(\forall P \in [\![\psi]\!]_P\,.\mathcal{I}(P) = \mathcal{I}'(P)) \implies \mathcal{T}\,[\![\psi]\!]_{\mathcal{I}} = \mathcal{T}\,[\![\psi]\!]_{\mathcal{I}'}\,.$$

- $\implies \vDash \psi$ is decidable w/ $O(2^{|[\![\psi]\!]_P|})$ complexity via truth tables.

Definition 1.2.3. (**Tautology, Satisfiable, Contradiction**) For $\psi \in \mathcal{L}_0$:

(i) ψ is a tautology, or *valid*, iff $\forall \mathcal{I} \in \Sigma_{\mathcal{I}}.\ \vDash_{\mathcal{I}} \psi$.

(ii) ψ is satisfiable, iff $\exists \mathcal{I} \in \Sigma_{\mathcal{I}}.\ \vDash_{\mathcal{I}} \psi$.

(iii) ψ is unsatisfiable, or a contradiction, iff $\forall \mathcal{I} \in \Sigma_{\mathcal{I}}.\ \nvDash_{\mathcal{I}} \psi$.

Definition 1.2.4. (**Entailment and Equivalence**) A proposition ψ_1 entails ψ_2, denoted $\psi_1 \vDash \psi_2$ iff $\forall \mathcal{I} \in \Sigma_{\mathcal{I}}.\ \vDash_{\mathcal{I}} \psi_1 \implies \vDash_{\mathcal{I}} \psi_2$. The propositions ψ_1 and ψ_2 are equivalent, denoted $\psi_1 \simeq \psi_2 \iff \psi_1 \vDash \psi_2 \land \psi_2 \vDash \psi_1$.

- **Notation**: $\vDash \Delta$ is equivalent to $\emptyset \vDash \Delta$, $\{\psi_1\} \vDash \psi_2$ is equivalent to $\psi_1 \vDash \psi_2$, and $\Gamma_1, \Gamma_2 \vDash \Delta$ is equivalent to $\Gamma_1 \cup \Gamma_2 \vDash \Delta$.

Theorem 1.2.1. For all $\Gamma, \Delta \in \mathcal{P}(\mathcal{L}_0)$:

(i) $\Gamma \vDash \Delta \iff \neg\Gamma \cup \Delta$ is contradicting.

(ii) Γ is contradicting $\implies \Gamma \vDash \Delta$.

(iii) $\vDash \Delta \iff \Delta$ is a tautology $\iff \neg\Delta$ is contradicting.

Theorem 1.2.2. (**Preorder** $\vDash$) The tuple $(\mathcal{L}_0, \vDash)$ is a preorder:

(R) *Reflexive*: $\forall \psi \in \mathcal{L}_0 . \psi \vDash \psi$

(T) *Transitive*: $\forall \psi, \phi, \varphi \in \mathcal{L}_0 . \psi \vDash \phi \wedge \phi \vDash \varphi \implies \psi \vDash \varphi$

Theorem 1.2.3. (**Monotonicity of** $\vDash$)

$$\forall \Gamma_1, \Gamma_2, \Delta \in \mathcal{P}(\mathcal{L}_0) . \Gamma_1 \vDash \Delta \wedge \Gamma_1 \subseteq \Gamma_2 \implies \Gamma_2 \vDash \Delta .$$

Theorem 1.2.4. (**Equivalence Relation** $\simeq$) $\simeq : \mathcal{L}_0 \leftrightarrow \mathcal{L}_0$ is an equivalence relation on $\mathcal{L}$:

(R) *Reflexive*: $\forall \psi \in \mathcal{L}_0 . \psi \simeq \psi$

(S) *Symmetric*: $\forall \psi, \phi \in \mathcal{L}_0 . \psi \simeq \phi \implies \phi \simeq \psi$

(T) *Transitive*: $\forall \psi, \phi, \varphi \in \mathcal{L}_0 . \psi \simeq \phi \wedge \phi \simeq \varphi \implies \psi \simeq \varphi$

Theorem 1.2.5. (**Congruence** $\simeq$) $\simeq : \mathcal{L}_0 \leftrightarrow \mathcal{L}_0$ is a congruence relation on $\mathcal{L}_0$, that is

$$\forall \psi, \phi \in \mathcal{L}_0 . \psi \simeq \phi \implies (\forall C \in \Sigma_C . C[\psi] \simeq C[\phi]),$$

where $C \in \Sigma_C$ is the set of contexts of $\mathcal{L}_0$, defined by:

$$\begin{aligned} C \ \texttt{::=} \ & [\cdot] \\ \texttt{|} \ & \neg C \\ \texttt{|} \ & C * \psi \ \texttt{|} \ \psi * C \end{aligned}$$

where $* \in \{\wedge, \vee, \rightarrow, \longleftrightarrow\} \subset \Sigma_\Omega$.

Theorem 1.2.6. (**Deduction Theorem**) For all $\psi, \phi \in \mathcal{L}_0$:

(i) $\vDash \psi \rightarrow \phi \iff \psi \vDash \phi$

(ii) $\vDash \psi \longleftrightarrow \phi \iff \psi \simeq \phi$

1.2.1 Equivalences

- Idempotent laws:
$$\psi \land \psi \simeq \psi \quad \psi \lor \psi \simeq \psi.$$

- Commutative laws:
$$\psi_1 \land \psi_2 \simeq \psi_2 \land \psi_1 \quad \psi_1 \lor \psi_2 \simeq \psi_2 \lor \psi_1.$$

- Associative laws:
$$(\psi_1 \land \psi_2) \land \psi_3 \simeq \psi_1 \land (\psi_2 \land \psi_3) \quad (\psi_1 \lor \psi_2) \lor \psi_3 \simeq \psi_1 \lor (\psi_2 \lor \psi_3)\,.$$

- Distributive laws:
$$\psi_1 \lor (\psi_2 \land \psi_3) \simeq (\psi_1 \lor \psi_2) \land (\psi_1 \lor \psi_3) \quad \psi_1 \land (\psi_2 \lor \psi_3) \simeq (\psi_1 \land \psi_2) \lor (\psi_1 \land \psi_3).$$

- Negation laws:
$$\neg\neg\psi \simeq \psi \quad \psi \lor \neg\psi \simeq \top \quad \psi \land \neg\psi \simeq \bot.$$

- Identity laws:
$$\psi \land \top \simeq \psi \quad \psi \lor \bot \simeq \psi.$$

- Annihilation laws:
$$\psi \land \bot \simeq \bot \quad \psi \lor \top \simeq \top.$$

- De Morgans' laws:
$$\neg(\psi_1 \land \psi_2) \simeq \neg\psi_1 \lor \neg\psi_2 \quad \neg(\psi_1 \lor \psi_2) \simeq \neg\psi_1 \land \neg\psi_2.$$

- Connective equivalence laws:
$$\psi_1 \longleftrightarrow \psi_2 \simeq (\psi_1 \to \psi_2) \land (\psi_2 \to \psi_1) \simeq (\neg\psi_1 \land \neg\psi_2) \lor (\psi_1 \land \psi_2)$$
$$\psi_1 \to \psi_2 \simeq \neg\psi_1 \lor \psi_2$$

- Contrapositive:
$$\psi_1 \to \psi_2 \simeq \neg\psi_2 \to \neg\psi_1.$$

1.2.2 Normal Forms

- **Problem**: Existence of *adequate* propositional logics $\implies$ $\mathcal{L}_0$ contains redundancy.

- **Examples**:

  - $\mathcal{L}_0(\{\top, \bot, \neg, \vee, \wedge\}) \cong \mathcal{L}_0$, by connective equivalence laws.
  - $\mathcal{L}_0(\{\neg, \vee, \wedge\}) \cong \mathcal{L}_0$, by negation laws.
  - $\mathcal{L}_0(\{\neg, \wedge\}) \cong \mathcal{L}_0(\{\neg, \vee\}) \cong \mathcal{L}_0$ by De Morgans' laws

Definition 1.2.5. (**Primitive Propositional Logic**) The primitive propositional logic is $\mathcal{L}_0^P = \mathcal{L}_0\left(\{\top, \bot, \neg, \vee, \wedge\}\right)$, henceforth denoted $\mathcal{L}_0^P \subset \mathcal{L}_0$.

Definition 1.2.6. (**Dual**) The dual of a primitive proposition $\psi \in \mathcal{L}_0^P$, denoted ψ^*, where $\cdot^* : \mathcal{L}_0^P \to \mathcal{L}_0^P$ is inductively defined by

$$\begin{array}{ccc} P^* = \neg P & \top^* = \bot & \bot^* = \top \\ (\neg\psi)^* = \neg\psi^* & (\psi_1 \wedge \psi_2)^* = \psi_1^* \vee \psi_2^* & (\psi_1 \vee \psi_2)^* = \psi_1^* \vee \psi_2^* \end{array}$$

Theorem 1.2.7. (**Principle of Duality**)

$$\forall \psi \in \mathcal{L}_0^P . \psi^* \simeq \neg\psi.$$

Definition 1.2.7. (**Negation Normal Form**) A literal is defined by $\ell \ ::= \ P \ \mid \ \neg P$. A primitive proposition $\psi \in \mathcal{L}_0^P$ is said to be in negation normal form, iff

$$\psi \in \mathcal{L}_0(\{\neg P : P \in \Sigma_P\} \cup \{\wedge, \vee\}) = \mathcal{L}^{NNF}.$$

Definition 1.2.8. (**Conjuctive and Disjunctive Normal Forms**) A negation normalized proposition $\psi \in \mathcal{L}_0^{NNF}$ is said to be in conjunctive normal form (CNF) if $\psi \in \mathcal{L}_0^{CNF} \cong \mathcal{L}_0^{NNF}$, defined by:

$$C \ ::= \ \ell \ \vee \ C \ \mid \ \ell \qquad\qquad \psi \ ::= \ C \ \wedge \ \psi \ \mid \ C$$

That is $\psi \equiv \bigwedge_{i=0}^{n} \bigvee_{j=0}^{m_i} \ell_{ij}$.

A negation normalized proposition $\psi \in \mathcal{L}_0^{NNF} \cong \mathcal{L}_0^{NNF}$ is said to be in disjunctive normal form (DNF) if $\psi \in \mathcal{L}_0^{DNF}$, defined by:

$$C \ ::= \ \ell \ \wedge \ C \ \mid \ \ell \qquad\qquad \psi \ ::= \ C \ \vee \ \psi \ \mid \ C$$

That is $\psi \equiv \bigvee_{i=0}^{n} \bigwedge_{j=0}^{m_i} \ell_{ij}$.

- Translation from $\mathcal{L}_0$ to CNF (or DNF):
  - Eliminate $\rightarrow$ and $\longleftrightarrow$.
  - Push $\neg$ using $\neg\neg\psi \simeq \psi$ and De Morgans' laws.
  - Push $\vee$ (or $\wedge$) using distributive laws.
  - Simplify w/ *absorption law*: $\psi_1 \wedge (\psi_1 \vee \psi_2) \simeq \psi_1$ and $(\neg\psi_1 \vee \psi_2) \wedge (\psi_1 \vee \psi_2) \simeq \psi_2$.

1.2.3 Clauses

Definition 1.2.9. (**Clause**) A (set-based) *clause* is a finite set of literals $C \in \mathcal{P}(\Sigma_\ell) = \Sigma_C$. A family of clauses $\Delta \in \mathcal{P}(\Sigma_C) = \Sigma_\Delta$ The empty clause $\emptyset$ is semantically equivalent to $\bot$ ($\bigvee \emptyset = \bot$, by identity).

- Σ_Δ and $\mathcal{L}_0$ are congruent.
- The sets of positive and negative literals in a clause C are denoted $P(C), N(C) \subseteq C$, respectively.

Theorem 1.2.8. A family of clauses $\Delta \in \Sigma_\Delta$ may be simplified:

1. For all $C, C' \in \Delta$,
$$C \subseteq C' \implies \Delta \simeq_\Delta \Delta \setminus \{C'\} .$$
2. For all C,
$$P(C) \cap N(C) \neq \emptyset \implies \Delta \simeq_\Delta \Delta \setminus \{C\} .$$

- **Kowalski Notation**: The clause $\{\neg P_0, \dots, \neg P_k, P_{k+1}, \dots, P_n\}$ are written as $P_0 \wedge \cdots \wedge P_k \rightarrow P_{k+1} \vee \cdots \vee P_n$.

1.3 Proof Systems

- **Problem**: Decidable methods to determine whether $\Gamma \vDash \psi$ holds.
- **Solution**: Proof Systems

1.3.1 Hilbert-Style Proof System

- A proof system is said to be *Hilbert-style* if it has a minimal set of axiom and inference rules *with* a Modus Ponens inference rule. Useful for **LCF** style ATP.

Definition 1.3.1. (**Hilbert-Style $\mathscr{H}_0$**) $\mathscr{H}_0$, the Hilbert-style proof system for Propositional logic, is defined on the language $\mathcal{L}_0(\{\neg, \rightarrow\})$ (henceforth denoted $\mathcal{L}_0$) with the following axioms and inference rules:

$$(\mathrm{S})\ \frac{}{(\psi \rightarrow (\phi \rightarrow \chi)) \rightarrow ((\psi \rightarrow \phi) \rightarrow (\psi \rightarrow \chi))} \qquad (\mathrm{K})\ \frac{}{\psi \rightarrow (\phi \rightarrow \psi)}$$

$$(\mathrm{N})\ \frac{}{(\neg\phi \rightarrow \neg\psi) \rightarrow ((\neg\phi \rightarrow \psi) \rightarrow \phi)}$$

$$(\mathrm{MP})\ \frac{\psi \qquad \psi \rightarrow \phi}{\phi}$$

Theorem 1.3.1. (**Deduction Theorem**) For all $\Gamma \in \mathcal{P}(\mathcal{L}_0)$ and propositions $\psi, \phi \in \mathcal{L}_0$,

$$\Gamma, \psi \vdash_{\mathscr{H}_0} \phi \iff \Gamma \vdash_{\mathscr{H}_0} \psi \rightarrow \phi.$$

- The deduction theorem justifies the standard: "Assume ψ, prove ϕ. So we have $\psi \rightarrow \phi$" argument $\implies$ *Natural Deduction* or Sequent forms.

Theorem 1.3.2. (**Soundness and Completeness of $\mathscr{H}_0$**) $\mathscr{H}_0$ is sound and complete, that is

$$\forall \Gamma \in \mathcal{P}(\mathcal{L}), \psi \in \mathcal{L}. \Gamma \vdash_{\mathscr{H}_0} \psi \implies \Gamma \vDash \psi,$$

and

$$\forall \Gamma \in \mathcal{P}(\mathcal{L}_0), \psi \in \mathcal{L}_0. \Gamma \vDash \psi \implies \Gamma \vdash_{\mathscr{H}_0} \psi.$$

1.3.1.1 The Sequent Form

- **Idea**: Explicit movement of assumptions via a *sequent*

Definition 1.3.2. (**Sequent**) A sequent in the proof system $\mathscr{P}$ for $\mathcal{L}$ is a meta-formula of the form $\Gamma \vdash \psi$, where $\Gamma \in \mathcal{P}(\mathcal{L})$ and $\psi \in \mathcal{L}$.

- The *sequent form* of a proof system $\mathscr{P}$ explicitly specifies the assumptions Γ in the proof trees $\mathscr{T}$.
- The set of sequents on a language $\mathcal{L}$ is denoted $\mathscr{S}_{\mathcal{L}}$.
- By substitutivity (theorem ??) we may simplify our proofs by incorporating theorems (and meta-theorems) as *derived rules* (denoted with a $'$) of the proof system.

Definition 1.3.3. (**The Sequent Form of $\mathscr{H}_0$**) $\mathscr{H}_0^{\varsigma}$, the sequent form of $\mathscr{H}_0$ is a proof system, is defined on the language $\mathscr{S}_{\mathcal{L}_0}$ with the following axioms and inference rules:

$$(\mathrm{R}')\ \frac{\psi \in \Gamma}{\Gamma \vdash \psi} \qquad (\mathrm{S})\ \frac{}{\Gamma \vdash (\psi \to (\phi \to \chi)) \to ((\psi \to \phi) \to (\psi \to \chi))}$$

$$(\mathrm{K})\ \frac{}{\Gamma \vdash \psi \to (\phi \to \psi)} \qquad (\mathrm{N})\ \frac{}{\Gamma \vdash (\neg\phi \to \neg\psi) \to ((\neg\phi \to \psi) \to \phi)}$$

$$(\mathrm{MP})\ \frac{\Gamma \vdash \psi \qquad \Gamma \vdash \psi \to \phi}{\Gamma \vdash \phi}$$

$$(\mathrm{DT}\ \mathsf{I}')\ \frac{\Gamma, \psi \vdash \phi}{\Gamma \vdash \psi \to \phi} \qquad (\mathrm{DT}\ \mathsf{E}')\ \frac{\Gamma \vdash \psi \to \phi}{\Gamma, \psi \vdash \phi}$$

- $\Delta \vdash_{\mathscr{H}_0^{\varsigma}} (\Gamma \vdash \psi) \iff \Delta, \Gamma \vdash_{\mathscr{H}_0} \psi$.
- The sequent form $\mathscr{H}_0^{\varsigma}$ w/ derived rules and operators provides a richer proof system. (See notes for derived rules).

Definition 1.3.4. (**Derived Operator**) A *derived operator* $O^{\Delta} \notin \Omega$ is an operator o defined in terms of operators in Ω, given by $O^{\Delta}(\psi_1, \ldots, \psi_n) \triangleq$

$O(\psi_1, \ldots, \psi_n)$ where $O(\psi_1, \ldots, \psi_n) \in \mathcal{L}_0(\Omega)$.

$$\begin{aligned}
\top &\triangleq \psi \to \psi \\
\bot &\triangleq \neg(\psi \to \psi) \\
\psi \lor \phi &\triangleq \neg\psi \to \phi \\
\psi \land \phi &\triangleq \neg(\psi \to \neg\phi)
\end{aligned}$$

Each derived operator $O^\Delta(\psi_1, \ldots, \psi_n) \triangleq O(\psi_1, \ldots, \psi_n)$ has the introduction and elimination rules:

$$\frac{\Gamma \vdash O^\Delta(\psi_1, \ldots, \psi_n)}{\Gamma \vdash O(\psi_1, \ldots, \psi_n)} \quad \frac{\Gamma \vdash O(\psi_1, \ldots, \psi_n)}{\Gamma \vdash O^\Delta(\psi_1, \ldots, \psi_n)}$$

1.3.2 Gentzen's Natural Deduction System

- **Idea**: Derived rules from $\mathscr{H}_0^\varsigma$ results in a *natural system*. A non-minimal system that consists of *introduction* and *elimination* (or left or right) rules for each operator.

Definition 1.3.5. ($\mathscr{G}_0$ **Proof System**) The $\mathscr{G}_0$ proof system, Gentzen's Natural Deduction System, is defined on the language $\mathscr{S}_{\mathcal{L}_0}$ with the following axioms and inference rules:

Operator	**Introduction**	**Elimination**
$\bot$	$(\bot\mathsf{I})\ \dfrac{\Gamma \vdash \psi \land \neg\psi}{\Gamma \vdash \bot}$	$(\bot\mathsf{E})\ \dfrac{\Gamma \vdash \bot}{\Gamma \vdash \psi}$
$\top$	$(\top\mathsf{I})\ \dfrac{}{\Gamma \vdash \top}$	$(\top\mathsf{E})\ \dfrac{\Gamma \vdash \top}{\Gamma \vdash \psi \lor \neg\psi}$
$\neg$	$(\neg\mathsf{I})\ \dfrac{\Gamma, \psi \vdash \bot}{\Gamma \vdash \neg\psi}$	$(\neg\mathsf{E})\ \dfrac{\Gamma, \neg\psi \vdash \bot}{\Gamma \vdash \psi}$
$\neg\neg$	$(\neg\neg\mathsf{I})\ \dfrac{\Gamma \vdash \psi}{\Gamma \vdash \neg\neg\psi}$	$(\neg\neg\mathsf{E})\ \dfrac{\Gamma \vdash \neg\neg\psi}{\Gamma \vdash \psi}$
$\lor$	$(\lor\mathsf{I}_1)\ \dfrac{\Gamma \vdash \psi}{\Gamma \vdash \psi \lor \phi}$ $(\lor\mathsf{I}_2)\ \dfrac{\Gamma \vdash \phi}{\Gamma \vdash \psi \lor \phi}$	$(\lor\mathsf{E})\ \dfrac{\Gamma \vdash \psi \lor \phi \qquad \Gamma \vdash \psi \to \chi \qquad \Gamma \vdash \phi \to \chi}{\Gamma \vdash \chi}$
$\land$	$(\land\mathsf{I})\ \dfrac{\Gamma \vdash \psi \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi \land \phi}$	$(\land\mathsf{E}_1)\ \dfrac{\Gamma \vdash \psi \land \phi}{\Gamma \vdash \psi}$ $(\land\mathsf{E}_2)\ \dfrac{\Gamma \vdash \psi \land \phi}{\Gamma \vdash \phi}$
$\to$	$(\to\mathsf{I})\ \dfrac{\Gamma, \psi \vdash \phi}{\Gamma \vdash \psi \to \phi}$	$(\to\mathsf{E})\ \dfrac{\Gamma \vdash \psi \qquad \Gamma \vdash \psi \to \phi}{\Gamma \vdash \phi}$
$\longleftrightarrow$	$(\longleftrightarrow\mathsf{I})\ \dfrac{\Gamma \vdash \psi \to \phi \qquad \Gamma \vdash \phi \to \psi}{\Gamma \vdash \psi \longleftrightarrow \phi}$	$(\longleftrightarrow\mathsf{E}_1)\ \dfrac{\Gamma \vdash \psi \longleftrightarrow \phi}{\Gamma \vdash \psi \to \phi}$ $(\longleftrightarrow\mathsf{E}_2)\ \dfrac{\Gamma \vdash \psi \longleftrightarrow \phi}{\Gamma \vdash \phi \to \psi}$

1.3.3 Sequent Calculus

- **Idea**: Extends $\mathscr{G}_0$ w/ *generalized sequents*.

Definition 1.3.6. (**Generalized Sequent**) An generalized sequent in a proof system $\mathscr{P}$ for $\mathcal{L}_0(\Omega)$ where $\vee \in \Omega$ is a meta-formula of the form $\Gamma \vdash \Delta$, where $\Gamma, \Delta \in \mathcal{P}(\mathcal{L})$, with the semantic definition

$$\Gamma \vdash \Delta \iff \Gamma \vdash \bigvee \Delta.$$

- Semantically, by deduction theorem and soundness and completeness:

$$\Gamma \vdash \Delta \iff \models \bigwedge \Gamma \to \bigvee \Delta$$

- The generalized sequent: explicitly specifies the assumptions Γ *and* reduces non-determinism (branching) on $\vee$.

Definition 1.3.7. (Sequent Calculus $\mathscr{S}_0$ Proof System) $\mathscr{S}_0$, the Sequent calculus proof system for Propositional logic, is defined on the generalized sequent form language of $\mathcal{L}_0(\Omega_0)$ with the following axioms and inference rules:

Operator	**Left**	**Right**
Axiom	$(\mathrm{A})\,\dfrac{}{\Gamma, \psi \vdash \Delta, \psi}$	
$\neg$	$(\neg l)\,\dfrac{\Gamma \vdash \Delta, \psi}{\Gamma, \neg\psi \vdash \Delta}$	$(\neg r)\,\dfrac{\Gamma, \neg\psi \vdash \bot}{\Gamma \vdash \Delta, \neg\psi}$
$\wedge$	$(\wedge l)\,\dfrac{\Gamma, \psi, \phi \vdash \Delta}{\Gamma, \psi \wedge \phi \vdash \Delta}$	$(\wedge r)\,\dfrac{\Gamma \vdash \Delta, \psi \qquad \Gamma \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi \wedge \phi}$
$\vee$	$(\vee l)\,\dfrac{\Gamma, \psi \vdash \Delta \qquad \Gamma, \phi \vdash \Delta}{\Gamma, \psi \wedge \phi \vdash \Delta}$	$(\vee r)\,\dfrac{\Gamma \vdash \Delta, \psi, \phi}{\Gamma \vdash \Delta, \psi \vee \phi}$
$\rightarrow$	$(\rightarrow l)\,\dfrac{\Gamma \vdash \Delta, \psi \qquad \Gamma, \phi \vdash \Delta}{\Gamma, \psi \rightarrow \phi \vdash \Delta}$	$(\rightarrow r)\,\dfrac{\Gamma, \psi \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi \rightarrow \phi}$
$\longleftrightarrow$	$(\longleftrightarrow l)\,\dfrac{\Gamma \vdash \Delta, \psi, \phi \qquad \Gamma, \psi, \phi \vdash \Delta}{\Gamma, \psi \longleftrightarrow \phi \vdash \Delta}$	$(\longleftrightarrow r)\,\dfrac{\Gamma, \psi \vdash \Delta, \phi \qquad \Gamma, \phi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \psi \longleftrightarrow \phi}$

Theorem 1.3.3. (**Soundness and Completeness of $\mathscr{S}_0$**) $\mathscr{S}_0$ is sound and complete, that is

$$\forall \Gamma, \Delta \in \mathcal{P}(\mathcal{L}).\Gamma \vdash_{\mathscr{S}_0} \Delta \iff \Gamma \vDash \bigvee \Delta.$$

Proof. By the soundness and completeness of $\mathscr{H}_0$ and the derived rules of $\mathscr{H}_0$ (see notes), then it follows that $\mathscr{S}_0$ is sound and complete. $\square$

1.3.3.1 Structural Rules

- Structural rules apply to generalized sequents, as opposed to operators.

Lemma 1.3.1. (**Weakening**) We have the following weakening rules:

$$(\text{Weaken } l)\,\frac{\Gamma \vdash \Delta}{\Gamma, \psi \vdash \Delta} \qquad (\text{Weaken } r)\,\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \psi}$$

- *Contradiction* not required for *our formalization* due to the usage of sets since $\{x, x\} = \{x\}$.

$$(\text{Contradiction } l)\ \frac{\Gamma, \psi, \psi \vdash \Delta}{\Gamma, \psi \vdash \Delta} \qquad (\text{Contradiction } r)\ \frac{\Gamma \vdash \Delta, \psi, \psi}{\Gamma \vdash \Delta, \psi}$$

Lemma 1.3.2. (**Contradiction**) We have the following contradiction rules:

Theorem 1.3.4. (**Cut Elimination Theorem**) The rule

$$(\text{Cut})\ \frac{\Gamma \vdash \Delta, \psi \qquad \Gamma, \psi \vdash \Delta}{\Gamma \vdash \Delta}$$

is *derived*.

1.4 Automated Theorem Proving

- Proof systems $\mathscr{P}$ yield *decidable methods* for determining whether $\Gamma \vDash \psi$ holds *given* a proof tree $\mathscr{T}$
- **Problem**: Determining whether $\Gamma \vDash \psi$ holds *without* a proof tree $\implies$ Automated Theorem Proving.
- Many automated methods use search algorithms on proof trees (see Tableux Calculus) or *clause-based* methods (See section ?? for *clauses*).

1.4.1 Tautology Checking

- **Approach**: Reduce $\Gamma \vDash \psi$ to $\vDash \underbrace{\bigwedge \Gamma \to \psi}_{\phi}$ via deduction theorem and uncurrying.
- **Solutions**:
  - Truth tables, considering $\mathcal{T}\,[\![\cdot]\!]_{\mathcal{I}}$ under the finite $2^{|[\![\phi]\!]_P|}$ interpretations.
  - *Tautology checking*: Determine whether $\nvDash \phi$ is true. (*falsifying*)
- **Approach**: Determine whether $\nvDash \phi$ using *clauses*

Theorem 1.4.1. For a family of clauses $\Delta \in \Sigma_\Delta$:

(i) $\nvDash C \iff P(C) \cap N(C) = \emptyset$

(ii) $\nvDash \Delta \iff \exists C \in \Delta.\, \nvDash C$

Definition 1.4.1. ($\mathscr{T}_0$ **Proof System**) The $\mathscr{T}_0$ (tautology checking) proof system is defined on the language Σ_Δ with the following axiom and inference rule:

$$\text{(i)}\ \frac{P(C) \cap N(C) = \emptyset}{\{C\}}$$

$$\text{(ii)}\ \frac{\{C_k\}}{\{C_1, \ldots, C_n\}}\ [1 \leq k \leq n]$$

with the axioms and inference rules corresponding to statements in Theorem ??.

Theorem 1.4.2. (**Completeness and Soundness of $\mathscr{T}_0$**) The proof system $\mathscr{T}_0$ satisfies

$$\nvdash_{\mathscr{T}_0} \Delta \iff \Gamma \vDash \psi.$$

- Method to prove $\Gamma \vDash \psi$:
  1. Compute $\Delta = [\![[\![\bigwedge \Gamma \to \psi]\!]_{CNF}]\!]_{\Delta}$
  2. Determine whether $\vdash_{\mathscr{T}_0} \Delta$ is true, a *tautological refutation* using $\mathscr{T}$. Performing simplification on Δ improves efficiency (see theorem ??).
  3. If $\vdash_{\mathscr{T}_0} \Delta$ is true, then $\Gamma \nvDash \psi$.
- **Advantage**: If a refutation cannot be found, then it is easy to determine a satisfiable interpretation.

1.4.2 Propositional Resolution

- **Problem**: CNF of $\bigwedge \Gamma \to \psi$ has an exponential space complexity (due to distributive law).
- **Solution**: Use $\Gamma \vDash \psi \iff \bigwedge \Gamma \wedge \neg\psi$ is contradicting.

  The (set-based) family of clause representation of $\bigwedge \Gamma \wedge \neg\psi$ computed using:
  $$\left[\!\!\left[\bigwedge \Gamma \wedge \neg\psi \right]\!\!\right]_{\Delta} = \bigcup_{\varphi \in \Gamma \cup \{\neg\psi\}} [\![[\![\varphi]\!]_{CNF}]\!]_{\Delta}.$$

  Improved efficiency by computing the CNF of smaller propositions.

Theorem 1.4.3. (**Resolution Theorem**) For all $\psi_1, \psi_2, \psi_3 \in \mathcal{L}_0$,

$$(\psi_1 \vee \psi_2) \wedge (\neg\psi_1 \vee \psi_3) \text{ is satisfiable} \implies \psi_2 \vee \psi_3 \text{ is satisfiable.}$$

Definition 1.4.2. ($\mathscr{R}_0$ **Proof System**) The $\mathscr{R}_0$ (propositional resolution) proof system is defined on the language Σ_Δ with the following axiom and inference rules:

$$(\emptyset)\ \frac{\emptyset \in \Delta}{\Delta}$$

$$(\mathrm{R})\ \frac{\Delta \cup \left\{C \setminus \{p\} \cup \overline{C} \setminus \{\neg p\} : C \in \Lambda_p, \overline{C} \in \overline{\Lambda}_p\right\}}{\Delta \cup \Lambda_p \cup \overline{\Lambda_p}}$$

where $\Lambda_p = \{p \in C : C \in \Delta'\}, \overline{\Lambda}_p = \left\{\neg p \in \overline{C} : \overline{C} \in \Delta'\right\}$ and $\Delta' = \Delta \cup \Lambda_p \cup \overline{\Lambda_p}$.

- This yields a $O(|\llbracket\Delta\rrbracket_P|)$ algorithm. Since each application of (R) removes a predicate symbol $\implies$ terminiating.

Theorem 1.4.4. (**Completeness and Soundness of** $\mathscr{R}_0$) The proof system $\mathscr{R}_0$ satisfies

$$\vdash_{\mathscr{R}_0} \Delta \iff \Delta \text{ is unsatisfiable.}$$

- Method to prove $\Gamma \vDash \psi$:
  1. Compute $\Delta = \llbracket \bigwedge \Gamma \wedge \neg\psi \rrbracket_\Delta$
  2. Determine whether $\vdash_{\mathscr{R}_0} \Delta$ is true, a *refutation* using $\mathscr{R}_0$. Performing simplification on Δ improves efficiency (see theorem ??).
  3. If $\vdash_{\mathscr{R}_0} \Delta$ is true, then Δ is contradicting. Hence $\Gamma \vDash \psi$ is true.
- Often useful to use resolution trees, e.g.

$$\dfrac{\dfrac{\{\neg P, R\} \qquad \{P\}}{\{R\}} \qquad \{\neg R\}}{\emptyset}$$

  with the resolution rule: $\dfrac{P, \Delta \qquad \neg P, \Gamma}{\Delta, \Gamma}$.
- **Strategies**:
  - Ignore irrelavant clauses: Not all clauses are or can be used in a resolution proof (e.g. clauses containing *pure literals*)

- Set of support: Initial application of resolution must contain the clause of the consequence ($\neg\psi$).
- Linear resolution: Each resolvent is the parent clause for the next resolvent w/ the other parent being drawn from the set of axiom clauses e.g.

$$\dfrac{\dfrac{\dfrac{\{\neg P\} \qquad \{P, Q\}}{\{Q\}} \qquad \{P, \neg Q\}}{\{P\}} \qquad \{\neg P\}}{\emptyset}$$

  Additional space complexity improvement by only storing the current resolvent (starting w/ the set of support).
- Cuts: Using a cut (or case split):

$$\dfrac{\neg P, \Gamma \qquad P, \Gamma}{\Gamma}$$

  is often useful to reduce clause sizes.

1.4.3 DPLL

- DPLL: simple claused-based ATP procedure that determines unsatisfiablity.

Definition 1.4.3. (**Pure Literal**) A literal ℓ is pure in $\Delta \iff$ no clause $C \in \Delta$ contains $\neg\ell$.

- **Algorithm**:
  1. Delete all tautological clauses: $\{P, \neg P, \ldots\}$. $\top \wedge C \simeq C$
  2. Delete all clauses containing *pure literals*.
  3. Unit propagation: For each unit clause $\{\ell\}$:
     - Delete all clauses containing ℓ. $\ell \wedge (\ell \vee C) \simeq C$.
     - Delete $\neg\ell$ from all clauses. $\ell \wedge (\neg\ell \vee C) \simeq C \wedge \psi$
  4. Case split: Perform a case split (cut) on some literal ℓ, recursively applying the DPLL method on Δ, ℓ and $\Delta, \neg\ell$. Satisfiable $\iff$ one of the cases is satisfiable. $(\ell \wedge \psi) \vee (\neg\ell \wedge \psi) \simeq \psi$.

5. If the empty clause is generated $\implies$ unsatisfiable (a refutation). If all clauses are deleted $\implies$ satisfiable.

```
let dpll Δ
    | S.is_empty Δ = True
    | S.empty ∈ Δ = False
    | otherwise = rule1
    where
        rule1 = maybe rule2 dpll (unit_prop Δ)
        rule2 = maybe rule3 dpll (pure_lit Δ)
        rule3 = dpll (S.insert {p} Δ)
                || dpll (S.insert {¬p} Δ)

        // arbitrary choice. Could optimize based on occurrence of literal etc
        p = max (S.filter is_pos (S.unions Δ))
```

- **Terminates**: Each unit propagation removes a propositional symbol and $[\![\Delta]\!]_P$ is finite.
- The set of unit propagations $\{\ell_1, \ldots\}$ (for a satisfiable termination) defines a satisfying interpretation $\mathcal{I}$ s.t $\forall 1 \leq i \leq n.\ \vDash_{\mathcal{I}} \ell_i$.

Definition 1.4.4. (**DPLL Proof System**) The $\mathscr{D}_0$ DPLL proof system is defined on the sequents of Σ_Δ w/ the following axioms and inference rules:

$$(\text{Unit})\ \frac{\Gamma, \ell \vdash \Delta}{\Gamma \vdash \Delta, \{\ell\}}$$

$$(\text{Unit } \mathsf{E}_1)\ \frac{\Gamma, \ell \vdash \Delta}{\Gamma, \ell \vdash \Delta, C \cup \{\ell\}} \qquad (\text{Unit } \mathsf{E}_2)\ \frac{\Gamma, \ell \vdash \Delta, C}{\Gamma, \ell \vdash \Delta, C \cup \{\neg\ell\}}$$

$$(\text{Split})\ \frac{\Gamma, \ell \vdash \Delta \qquad \Gamma, \neg\ell \vdash \Delta}{\Gamma \vdash \Delta} \qquad (\text{Unsat})\ \frac{}{\Gamma \vdash \Delta, \emptyset}$$

Theorem 1.4.5. (**Completeness and Soundness of $\mathscr{D}_0$**) The proof system $\mathscr{D}_0$ satisfies

$$\vdash_{\mathscr{D}_0} \Delta \iff \Delta \text{ is unsatisfiable.}$$

1.4.4 Binary Decision Diagrams

- **Problem**: $\mathscr{T}_0, \mathscr{D}_0, \mathscr{R}_0$ proof systems still suffer from exponential increase in number of literals (due to distributivity) for clause-based methods.
- **Observation**: Semantic mapping of boolean algebra operators $\{\bar{\cdot}, \cdot, +, \oplus\}$ and syntactic operators $\Omega_0 = \{\neg, \wedge, \vee, \longleftrightarrow, \rightarrow\}$. Reason about tautologies using semantics expressions.
- The homogenous Boolean algebra $\mathbf{B} = (\{0,1\}, \{\bar{\cdot}, \cdot, +, \oplus\}, \{=_{\mathbf{B}}\})$ defines the term algebra $\mathbf{B}(V) = (\mathbb{B}_\Omega(V), \Omega, \{=_{\mathbf{B}})\})$ where $s, t, u \in \mathbb{B}(V)$ is the set of *boolean expressions* and $V = \{a, b, c, \ldots\}$ is the set of boolean variables.

Definition 1.4.5. (**Tenrary Operator**) We extend $\mathbf{B} = (\{0,1\}, \{\bar{\cdot}, \cdot, +, \ldots\}, \{=\})$ to $\mathbf{B}'$ by introducing the *ternary operator* $a?b:c$, defined by

$$a?b:c = a \cdot b + \overline{a} \cdot c.$$

Lemma 1.4.1. The algebra $\mathbf{B}_? = (\{0,1\}, \{\cdot ? \cdot : \cdot\}, \{=\})$ is adequate, that is $\mathbb{B}_?(V) \lesssim \mathbb{B}(V)$.

Proof. The following identities prove the lemma:

$$\begin{aligned}
\overline{a} &= a?0:1 \\
a \cdot b &= a?b:0 = b?a:0 \\
a + b &= a?1:b = b?1:a \\
a \oplus b &= a?b:(b?0:1)
\end{aligned}$$

□

Lemma 1.4.2. For boolean expressions, $s^0, s^1, t^0, t^1 \in \mathbb{B}'(V)$, define $s = a?s^1 : s^0$ and $t = a?t^1 : t^0$, then

(i) $\overline{s} = a?\overline{s^1} : \overline{s^0}$,

(ii) For all $\odot \in \{\cdot, +, \oplus\}$,

$$s \odot t = a?(s^1 \odot t^1) : (s^0 \odot t^0),$$

and by extension, for all $o_n : \mathbb{B}^n \to \mathbb{B}$ n-ary boolean operators, then

$$\forall 1 \leq i \leq n. t_i = a?t_i^1 : t_i^0 \implies o_n(t_1, \ldots, t_n) = a?o_n(t_1^1, \ldots, t_n^1) : o_n(t_1^0, \ldots, t_n^0).$$

Proof. Let s^0, s^1, t^0, t^1 be arbitrary boolean expressions. For a boolean variable a, define $s = a?s^1 : s^0$ and $t = a?t^1 : t^0$.

(i) We have

$$\begin{aligned}
\overline{s} &= \overline{a \cdot s^1 + \overline{a} \cdot s^0} && \text{(Definition ??)}\\
&= \overline{a \cdot s^1} \cdot \overline{\overline{a} \cdot s^0} && \text{(De Morgan's Law)}\\
&= (\overline{a} + \overline{s^1}) \cdot (a + \overline{s^0}) && \text{(De Morgan's Law)}\\
&= \overline{a} \cdot \overline{s^0} + a \cdot \overline{s^1} + \overline{s^0} \cdot \overline{s^1} && \text{(Distributive Law)}\\
&= \overline{a} \cdot \overline{s^0} + a \cdot \overline{s^1} && (a \cdot b + \overline{a} \cdot c + b \cdot c = a \cdot b + \overline{a} \cdot c)\\
&= a?\overline{s^1} : \overline{s^0}
\end{aligned}$$

as required.

(ii) For

$\odot = \cdot$, we have

$$\begin{aligned}
s \cdot t &= (a \cdot s^1 + \overline{a} \cdot s^0) \cdot (a \cdot t^1 + \overline{a} \cdot t^0) && \text{(Definition ??)}\\
&= a \cdot s^1 \cdot t^1 + \overline{a} \cdot s^0 \cdot t^0 && \text{(Distributive Law)}\\
&= a?s^1 \cdot t^1 : s^0 \cdot t^0
\end{aligned}$$

a as required.

Similar proofs hold for $\odot \in \{+, \oplus\}$, with the extension by induction.

□

Theorem 1.4.6. $\mathcal{L}_0(\{\bot, \top, ?:\})$ and $\mathcal{L}_0$ are congruent.

Proof. Follows from the homomorphism μ between semantic and syntactic operators and lemma ??. □

Definition 1.4.6. (**TNF**) A boolean expression $s \in \mathbb{B}(V)$ is said to be in *ternary normal form* (TNF) if $s \in \mathbb{B}_?(V)$, where $\mathbb{B}_?(V)$ is defined by

$$s \;\; \texttt{::=} \;\; \texttt{0} \;\; | \;\; \texttt{1} \;\; | \;\; a \;\; \texttt{?} \;\; s^1 \;\; \texttt{:} \;\; s^0$$

where $a \in V, s \in \mathbb{B}_?(V)$.

- A boolean expression s with variables $a_1, \ldots, a_n$ is denoted $s(a_1, \ldots, a_n)$.

Theorem 1.4.7. All boolean expressions $s \in \mathbb{B}(V)$ may be expressed in TNF

Proof. Follows from Lemma ?? $\square$

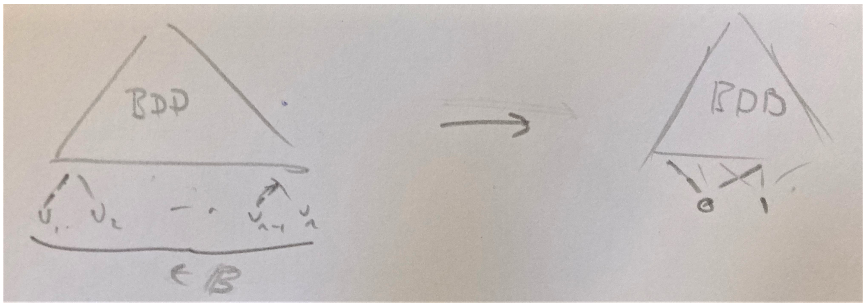
- **Idea**: The truth-table of some expression $s(a_1, \ldots, a_n)$ yields a TNF of $s(a_1, \ldots, a_n)$.

a	b	c	d	s
0	0	0	0	0
			1	0
		1	0	0
			1	1
	1	0	0	0
			1	0
		1	0	0
			1	0
1	0	0	0	0
			1	1
		1	0	0
			1	1
	1	0	0	0
			1	0
		1	0	1
			1	1

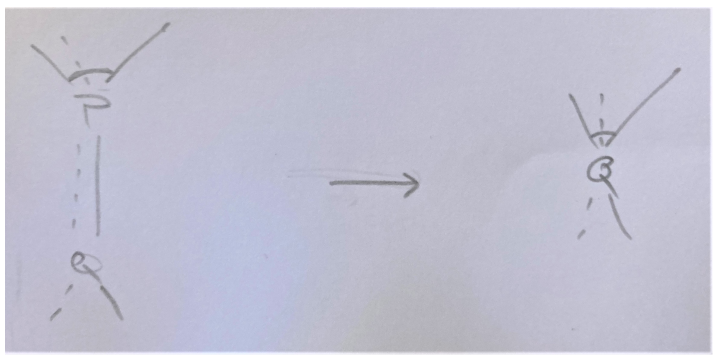
- **Idea**: Truth-tables may be represented using *trees* $\implies$ BDDs

Definition 1.4.7. (**BDD**) A *binary decision diagram* (BDD) is a DAG $G = (V, E)$ satisfying

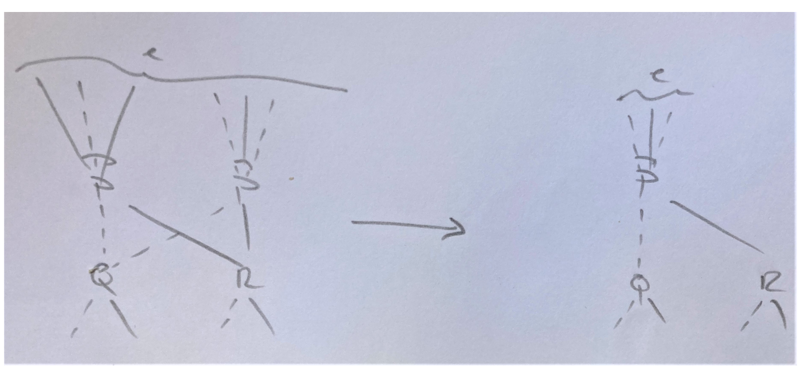
- **Leaf nodes**: There are at least 2 distinct leaf nodes with the labels `0` and `1` (respectively).
- **Internal nodes**: Each internal node $v \in V \setminus L$ has a boolean variable label a with two out-going edges $e_0, e_1 \in E$, referred to as the `0` (or *low*) edge (dashed) and the `1` (or *high*) edge, respectively.
- A BDD has the following $\rightarrow$ *reductions*:
    1. **Eliminating Duplicate Terminals**:



2. **Eliminating Redundant Vertices**:



3. **Eliminating Duplicate Vertices**:



- The variable (or label) of a non-terminal v w/ variable a, low vertex u and high w is associated with

$$var(v) = a, lo(v) = u, hi(v) = w.$$

This is denoted as $v = \langle a, u, w \rangle \in V \setminus L$. Leaves $v \in L$ are denote $v = \langle k \rangle$ where $k \in \mathbb{B}$.

Definition 1.4.8. (**RBDD**) A BDD is a *reduced BDD* if no more $\rightarrow$ reductions may be applied.

Definition 1.4.9. (**OBDD**) A BDD is an *ordered BDD* (OBDD) with total order $(V, \leq)$, if for all (v_{x_1}, v_{x_n}) paths

$$v_{x_1} \rightarrow v_{x_2} \rightarrow \cdots \rightarrow v_{x_n},$$

$x_1 \leq x_2 \leq \cdots \leq x_n$ holds.

- An *reduced ordered BDD* (ROBDD) is a ordered BDD that is reduced.

Theorem 1.4.8. (**ROBDD Representation**) For a given total ordering $(V, \leq)$, every ROBDD $G = (V, E)$ represents a *unique boolean expression* s.

Proof. We proceed by rule induction on an ROBDD $G = (V, E)$, with the statement

$$P(v) = \exists! s^v \in \mathbb{B}_?(V).$$

Base Case: For a leaf $v = \langle k \rangle \in L$, we have the following cases:

- $v = \langle 0 \rangle$. So we have $s^v = 0$.
- $v = \langle 1 \rangle$. So we have $s^v = 1$.

So we have $P(v)$.

Inductive Step: For a vertex $v = \langle a, u, w \rangle \in V$, we wish to show that $P(u) \wedge P(w) \implies P(v)$. Let us assume that $P(u)$ and $P(w)$ hold, then we have s^u and s^w. We define

$$s^v = a ? s^w : s^u,$$

where uniqueness follows from the uniqueness of s^u, s^w and a (on subpaths). So we have $P(v)$.

By the Principle of Rule Induction, we conclude the statement $P(v)$ holds for all $v \in V$. $\square$

Theorem 1.4.9. (**ROBDD Canonicity**) For a given total ordering $(V, \leq)$ s.t $a_n \leq \cdots \leq a_1$, for all boolean expressions $s(a_1, \ldots, a_n)$ there exists a unique ROBDD representing $s(a_1, \ldots, a_n)$.

Proof. We proceed by induction on $n \in \mathbb{N}$ with the statement

$P(n) = \forall s(a_1, \dots, a_n) \in \mathbb{B}_?(V).\exists!\text{ROBDD } G = (V, E).G \text{ represents } s(a_1, \dots, a_n)$.

Base Case: For $n = 0$, there exists exactly two ground expressions `0` and `1`, with ROBDDs $G = (\{0\}, \emptyset)$ and $G = (\{1\}, \emptyset)$ respectively. So we have $P(0)$.

Inductive Step: We wish to show that $\forall n \in \mathbb{N}.P(n) \implies P(n+1)$. Let $n \in \mathbb{N}$ be an arbitrary natural. Let $s(a_1, \dots, a_{n+1}) \in \mathbb{B}_?(V)$. Define $s^0(a_1, \dots, a_n) = s(a_1, \dots, a_n, 0)$ and $s^1(a_1, \dots, a_n) = s(a_1, \dots, a_n, 1)$. Then it follows that

$$s(a_1, \dots, a_{n+1}) = a_{n+1} ? s^1(a_1, \dots, a_n) : s^0(a_1, \dots, a_n).$$

Let us assume that $P(n)$ holds. Instantiating for s^1 and s^0 yields the ROBDDs $G^1 = (V^1, E^1)$ and $G^0 = (V^0, E^0)$, with roots v_0 and v_1 respectively. We have the following cases:

- $G^1 \neq G^0$. Let us assume that $G^1 = G^0$. Hence $s^0 = s^{v_0} = s^{v_1} = s^1$. Hence $s = s^1 = s^0$. So we have $G = G^1 = G^0$.
- $G^1 \neq G^0$. So we have $s^{v_1} = s^1 \neq s^0 = s^{v_0}$. Define a new vertex $v = \langle a_{n+1}, v_0, v_1 \rangle$. This yields a new ROBDD $G = (V^1 \cup V^2 \cup \{v\}, E^1 \cup E^2 \cup \{(v, v_0), (v, v_1)\})$ representing s. The uniqueness of G follows from the uniqueness of G^1, G^2 and the ordering $(V, \leq)$.

So we have $P(n+1)$.

By the Principle of Mathematical Induction, we conclude the statement $P(n)$ holds for all $n \in \mathbb{N}$. □

- **Consequences**:
  - Tautology checking $\Gamma \vDash \psi$ consists of checking whether the ROBDD for ψ is equal to `1`.
  - Checking semantic equivalence is determined by checking whether the ROBDDs are equal.

2 First Order Logic

2.1 Syntax

Definition 2.1.1. (**Homogenous Signature**) A signature $\Omega = (S, \mathscr{F}, \mathscr{R})$ is homogenous, or *uni-typed* iff $S = \{s\}$, where s is some arbitrary type.

Definition 2.1.2. (**Ω-Terms**) For a homogenous signature $\Omega = (S, \mathscr{F}, \mathscr{R})$, the set of Ω-terms $\mathbb{T}_\Omega(V)$ (in context of $\mathcal{L}_1$) is defined by

$$s, t, u \ ::= \ x \in V \ \mid \ f(t_1, \dots, t_n)$$

where $f : s^n \to s \in \Omega$.

- $\mathbb{T}_\Omega$ is the set of *ground terms*.

Definition 2.1.3. (**First Order Logic**) For a homogenous signature Ω and set of Ω-terms $\mathbb{T}_\Omega(V)$:

- $\Sigma_A(\Omega) = \{p(t_1, \dots, t_n) : p : s^n \in \mathscr{R} \wedge t_i \in \mathbb{T}_\Omega(V)\}$ is the set of Ω-atoms.
- $\Omega_1 = \Omega_0 \cup \{\forall x.\cdot, \exists x.\cdot : x \in V\}$ is the set of operators.
- The formal language, or *syntax*, of the first order logic is $\mathcal{L}_1(\Omega_1, \Omega) = \mathbb{T}_{\Omega_1}(\Sigma_A(\Omega))$, often denoted $\mathcal{L}_1(\Omega)$, that is

$$\begin{aligned}
\psi \ ::= \ & p(t_1, \dots, t_n) \in \Sigma_A(\Omega) \\
\mid \ & \top \mid \bot \mid \neg\psi \\
\mid \ & \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \\
\mid \ & \psi_1 \to \psi_2 \mid \psi_1 \longleftrightarrow \psi_2 \\
\mid \ & \forall x.\psi \mid \exists x.\psi
\end{aligned}$$

Definition 2.1.4. (**Variables**) For any term $t \in \mathbb{T}_\Omega(V)$, $var(t)$ is the set of variables in t:

$$var(x) = \{x\}$$
$$var(f(t_1, \dots, t_n)) = \bigcup_{1 \le i \le n} var(t_i)$$

- $\mathcal{Q}x.\psi$ binds x in ψ where $\mathcal{Q} \in \{\exists, \forall\}$ is a *quantifier*.

Definition 2.1.5. (**Free and bound variables**) For any formula $\psi \in \mathcal{L}_1(\Omega)$, $fv(\psi)$ and $var(\psi)$ are the sets of *free* variables and *variables* in t, respectively:

$$\begin{aligned} fv(p(t_1, \dots, t_n)) &= \bigcup_{1 \le i \le n} var(t_i) & var(p(t_1, \dots, t_n)) &= \bigcup_{1 \le i \le n} var(t_i) \\ fv(o(\psi_1, \dots, \psi_n)) &= \bigcup_{1 \le i \le n} fv(\psi_i) & var(o(\psi_1, \dots, \psi_n)) &= \bigcup_{1 \le i \le n} var(\psi_i) \\ fv(\mathcal{Q}x.\psi) &= fv(\psi) \setminus \{x\} & var(\mathcal{Q}x.\psi) &= var(\psi) \cup \{x\} \end{aligned}$$

The bound variables of ψ is defined as $bv(\psi) = var(\psi) \setminus fv(\psi)$.

- **Notation**: ψ may be written as $\psi(x_1, \dots, x_n)$ to denote $fv(\psi) \subseteq \{x_1, \dots, x_n\}$.

Definition 2.1.6. (**Closed Formulae and Closures**) $\psi \in \mathcal{L}_1$ is *closed* iff $fv(\psi) = \emptyset$. $\forall \mathbf{x}.\psi$ and $\exists \mathbf{x}.\psi$ are the *universal closure*, *existential closure* of $\psi(\mathbf{x})$.

Definition 2.1.7. (**Substitution**) A **substitution** θ is a partial function $\theta : V \rightharpoonup \mathbb{T}_\Omega(V)$.

- **Notation**: $\{t_1/x_1, \dots, t_n/x_n\}$ denotes a substitution θ, where $\theta(x_i) = t_i$ and $t/x \in \theta \iff \theta(x) = t$.

Definition 2.1.8. (**Application (Terms)**) The application of a substitution θ to $t \in \mathbb{T}_\Omega(V)$, denoted θt, is inductively defined by

$$\begin{aligned} \theta x &= \begin{cases} \theta(x) & \text{if } x \in \operatorname{dom}\theta \\ x & \text{otherwise} \end{cases} \\ \theta\, f(t_1, \dots, t_n) &= f(\theta t_1, \dots, \theta t_n) \end{aligned}$$

Definition 2.1.9. (**Application (Formulae)**) The application of a substitution θ to $\psi \in \mathcal{L}_1(\Omega)$, denoted $\theta\psi$, is inductively defined by

$$\begin{aligned} \theta p(t_1, \dots, t_n) &= p(\theta t_1, \dots, \theta t_n) \\ \theta\, o(\psi_1, \dots, \psi_n) &= o(\theta\psi_1, \dots, \theta\psi_n) \\ \theta\, \mathcal{Q}x.\psi &= \begin{cases} \mathcal{Q}x.\left[(\theta \setminus \{t/x\})\psi\right] & t/x \in \theta \\ \mathcal{Q}x.\theta\psi & x \notin \operatorname{dom}\theta \wedge x \notin fv(\operatorname{rng}\theta) \end{cases} \end{aligned}$$

- Substitutions are *capture avoiding* (see quantifier case).

Definition 2.1.10. (**α-equivalence**) The $\equiv_\alpha$: $\mathbb{T}_\Omega(V) \longleftrightarrow \mathbb{T}_\Omega(V)$ is inductively defined by

$$\frac{}{x \equiv_\alpha x} \qquad \frac{\forall 1 \leq i \leq n. t_i \equiv_\alpha s_i}{o(t_1, \ldots, t_n) \equiv_\alpha o(s_1, \ldots, s_n)}.$$

and $\equiv_\alpha$: $\mathcal{L}_1(\Omega) \longleftrightarrow \mathcal{L}_1(\Omega)$ is defined by

$$\frac{\forall 1 \leq i \leq n. t_i \equiv_\alpha s_i}{p(t_1, \ldots, t_n) \equiv_\alpha p(s_1, \ldots, s_n)} \quad \frac{\forall 1 \leq i \leq n. \psi_i \equiv_\alpha \phi_i}{o(\psi_1, \ldots, \psi_n) \equiv_\alpha o(\phi_1, \ldots, \phi_n)} \quad \frac{z \notin var(\psi) \cup var(\phi) \qquad \{z/x\}\,\psi \equiv_\alpha \{z/y\}\,\phi}{\mathcal{Q}x.\psi \equiv_\alpha \mathcal{Q}y.\phi}$$

- α-equivalence is used w/ capture avoiding substitutions.

2.2 Semantics

Definition 2.2.1. (**Homogeneous Algebra**) A **homogeneous algebra**, $\mathbf{A}$ is a the tuple $(\mathbb{A}, \mathscr{F}_\mathbf{A}, \mathscr{R}_\mathbf{A})$ such that $(\{\mathbb{A}\}, \mathbb{A} \cup \mathscr{F}_\mathbf{A}, \mathscr{R}_\mathbf{A})$ is an algebra, with the (*implicit*) homogenous signature $(\{\mathbb{A}\}, \mathbb{A} \cup \mathscr{F}, \mathscr{R})$ where:

- $\mathscr{F}_\mathbf{A}$ is the set of functions, where for each symbol $f \in \mathscr{F}$ of type $\mathbb{A}^n \to \mathbb{A}$, there is a function $f_\mathbf{A} \in \mathscr{F}_\mathbf{A}$ of type $f_\mathbf{A} : \mathbb{A}^n \to \mathbb{A}$.
- $\mathscr{R}_\mathbf{A}$ is the set of relations, where for each symbol $p \in \mathscr{R}$ of type $\mathbb{A}^n$, there is a relation $p_\mathbf{A} \in \mathscr{R}_\mathbf{A}$ of type $p_\mathbf{A} \subseteq \mathbb{A}^n$.

- m-ary partial functions $f_\mathbf{A} : \mathbb{A}^m \rightharpoonup \mathbb{A}$ are defined as $m+1$-ary relations $p^f_\mathbf{A} \subseteq \mathbb{A}^{m+1}$. We often define a *guard* relation $p^f_\mathbf{A} \downarrow \subseteq \mathbb{A}^m$, where $p^f_\mathbf{A}(x) \downarrow$ is true if $x \in \operatorname{dom} f$.

Definition 2.2.2. (**Valuation**) For an Ω-homogenous algebra $\mathbf{A}$. A *valuation* $v_\mathbf{A} : V \to |\mathbf{A}|$ is a total function associating each variable $x \in V$ with a unique value $a \in |\mathbf{A}|$. Set of $\mathbf{A}$ valuations is $\Sigma_v(\mathbf{A}) = \mathcal{P}\left[V \to |\mathbf{A}|\right]$

- The domain $|\mathbf{A}|$ must be *non-empty* for a valid valuation.

Definition 2.2.3. (**Ω-interpretation**) For an Ω-homogenous algebra $\mathbf{A}$ and valuation $v_\mathbf{A} : V \to |\mathbf{A}|$, the tuple $\mathcal{I} = (\mathbf{A}, v_\mathbf{A})$ is a Ω-interpretation. The set of Ω-interpretations is given by $\Sigma_\mathcal{I}(\Omega)$.

Definition 2.2.4. (**Value of terms**) For a Ω-interpretations $\mathcal{I} = (\mathbf{A}, v_{\mathbf{A}})$, the value of a term t in context of $\mathcal{I}$ is inductively defined by

$$\begin{aligned}\mathcal{V}_{\mathbf{A}} [\![x]\!]_{v_{\mathbf{A}}} &= v_{\mathbf{A}}(x) \\ \mathcal{V}_{\mathbf{A}} [\![f(t_1, \ldots, t_n)]\!]_{v_{\mathbf{A}}} &= f_{\mathbf{A}} \left(\mathcal{V}_{\mathbf{A}} [\![t_1]\!]_{v_{\mathbf{A}}}, \ldots, \mathcal{V}_{\mathbf{A}} [\![t_n]\!]_{v_{\mathbf{A}}}\right)\end{aligned}$$

Lemma 2.2.1. (**Coincidence Lemma for Terms**) For all Ω-interpretations $(\mathbf{A}, v_{\mathbf{A}}), (\mathbf{A}, v'_{\mathbf{A}}) \in \Sigma_{\mathcal{I}}(\Omega)$ and terms $t \in \mathbb{T}_{\Omega}(V)$,

$$\forall x \in var(t). v_{\mathbf{A}}(x) = v'_{\mathbf{A}}(x) \implies \mathcal{V}_{\mathbf{A}} [\![t]\!]_{v_{\mathbf{A}}} = \mathcal{V}_{\mathbf{A}} [\![t]\!]_{v'_{\mathbf{A}}}.$$

Definition 2.2.5. (**Valuation variant**) For any set variables $X \subseteq V$ and valuations $v_{\mathbf{A}}, v'_{\mathbf{A}} \in \Sigma_v(\Omega)$. $v'_{\mathbf{A}}$ is said to be an *X-variant* of $v_{\mathbf{A}}$, denoted $v_{\mathbf{A}} =_{\setminus X} v'_{\mathbf{A}}$, if

$$\forall y \in V \setminus X. v_{\mathbf{A}}(y) = v'_{\mathbf{A}}(y).$$

- **Notation**:
  - For $X = \{x\}$, v and v' are x-variants, denoted $v =_{\setminus x} v'$.
  - For $X = \{x_1, \ldots, x_n\}$, if $v_X =_{\setminus X} v$ and $v_X(x_i) = a_i \in |\mathbf{A}|$ for all $x_i \in X$, then we write $v_X = \{a_1/x_1, \ldots, a_n/x_n\}\, v$.

Definition 2.2.6. (**Semantics of First Order Logic**) Let $\mathcal{I} = (\mathbf{A}, v_{\mathbf{A}}) \in \Sigma_{\mathcal{I}}(\Omega)$ be a Ω-interpretation. The truth value of a formula $\psi \in \mathcal{L}_1(\Omega)$ in the context of the interpretation $\mathcal{I}$, denoted $\mathcal{T}_{\mathbf{A}} [\![\psi]\!]_{v_{\mathbf{A}}}$, where $\mathcal{T}_{\mathbf{A}} [\![\cdot]\!]_{v_{\mathbf{A}}} : \mathcal{L}_1(\Omega) \to |\mathbf{B}|$ is inductively defined by

$$\begin{aligned}\mathcal{T}_{\mathbf{A}} [\![p(t_1, \ldots, t_n)]\!]_{v_{\mathbf{A}}} &= \begin{cases} 1 & \text{if } (\mathcal{V}_{\mathbf{A}} [\![t_1]\!]_{v_{\mathbf{A}}}, \ldots, \mathcal{V}_{\mathbf{A}} [\![t_n]\!]_{v_{\mathbf{A}}}) \in p_{\mathbf{A}} \\ 0 & \text{otherwise} \end{cases} \\ \mathcal{T}_{\mathbf{A}} [\![\forall x.\psi]\!]_{v_{\mathbf{A}}} &= \prod_{v'_{\mathbf{A}} =_{\setminus x} v_{\mathbf{A}}} \mathcal{T}_{\mathbf{A}} [\![\psi]\!]_{v'_{\mathbf{A}}} \\ \mathcal{T}_{\mathbf{A}} [\![\exists x.\psi]\!]_{v_{\mathbf{A}}} &= \sum_{v'_{\mathbf{A}} =_{\setminus x} v_{\mathbf{A}}} \mathcal{T}_{\mathbf{A}} [\![\psi]\!]_{v'_{\mathbf{A}}}\end{aligned}$$

- The number of x-variants of v is $|\mathbf{A}|$.
- **Notation**: $\models_{(\mathbf{A}, v_{\mathbf{A}})} \psi \iff \mathcal{T}_{\mathbf{A}} [\![\psi]\!]_{v_{\mathbf{A}}} = 1$.

Lemma 2.2.2. (**Coincidence Lemma II**) For all $\psi \in \mathcal{L}_1(\Omega)$ and $(\mathbf{A}, v_{\mathbf{A}}), (\mathbf{A}, v'_{\mathbf{A}}) \in \Sigma_{\mathcal{I}}(\Omega)$,

$$(\forall x \in fv(\psi). v_{\mathbf{A}}(x) = v'_{\mathbf{A}}(x)) \implies \mathcal{T}_{\mathbf{A}} [\![\psi]\!]_{v_{\mathbf{A}}} = \mathcal{T}_{\mathbf{A}} [\![\psi]\!]_{v'_{\mathbf{A}}}.$$

Definition 2.2.7. (**Satisfiable**)

- A Ω-interpretation $\mathcal{I} = (\mathbf{A}, v_{\mathbf{A}}) \in \Sigma_{\mathcal{I}}(\Omega)$ *satisfies* $\psi \in \mathcal{L}_1(\Omega)$ iff $\vDash_{(\mathbf{A}, v_{\mathbf{A}})} \psi$.
- $\psi \in \mathcal{L}_1(\Omega)$ is said to be *satisfiable in* **A** iff $\exists v_{\mathbf{A}} \in \Sigma_v(\Omega). \vDash_{(\mathbf{A}, v_{\mathbf{A}})} \psi$.
- $\psi \in \mathcal{L}_1(\Omega)$ is said to be *satisfiable* iff $\exists (\mathbf{A}, v_{\mathbf{A}}) \in \Sigma_{\mathcal{I}}(\Omega). \vDash_{(\mathbf{A}, v_{\mathbf{A}})} \psi$.

Definition 2.2.8. (**Models**) A Ω-homogenous algebra **A** is a *model* (or Ω-model) for $\psi \in \mathcal{L}_1(\Omega)$ iff

$$\forall v_{\mathbf{A}} \in \Sigma_v(\Omega). \vDash_{(\mathbf{A}, v_{\mathbf{A}})} \psi,$$

denoted $\vDash_{\mathbf{A}} \psi$. For $\Delta \in \mathcal{P}(\mathcal{L}_1(\Omega))$:

(i) **A** is a model of Δ (denoted $\vDash_{\mathbf{A}} \Delta$) iff $\forall \psi \in \Delta. \vDash_{\mathbf{A}} \psi$.

(ii) Δ is *consistent* iff there exists an Ω-model **A** of Δ.

Definition 2.2.9. (**Entailment and Equivalence**) A formula ψ_1 entails ψ_2, denoted $\psi_1 \vDash \psi_2$ iff $\forall \mathbf{A}. \vDash_{\mathbf{A}} \psi_1 \implies \vDash_{\mathbf{A}} \psi_2$. The formulae $\psi_1, \psi_2 \in \mathcal{L}_1(\Omega)$ are equivalent, denoted $\psi_1 \simeq \psi_2 \iff \psi_1 \vDash \psi_2 \land \psi_2 \vDash \psi_1$.

Definition 2.2.10. (**Validity**) Let **A** be a Ω-homogenous algebra and $\psi \in \mathcal{L}_1(\Omega)$.

- ψ is *valid in* **A** $\iff \vDash_{\mathbf{A}} \psi$.
- ψ is *valid, or a tautology* $\iff \vDash \psi$.

- A tautology ψ may have infinite models.

2.2.1 Equivalences

- Negation laws:

$$\neg(\forall x.\psi) \simeq \exists x.\neg\psi \quad \neg(\exists x.\psi) \simeq \forall x.\neg\psi.$$

- Quantifier expansion (*left*) laws:

$$(\forall x.\psi) \land \phi \simeq \forall x.(\psi \land \phi)$$
$$(\forall x.\psi) \lor \phi \simeq \forall x.(\psi \lor \phi)$$
$$(\exists x.\psi) \land \phi \simeq \exists x.(\psi \land \phi)$$
$$(\exists x.\psi) \lor \phi \simeq \exists x.(\psi \lor \phi)$$

  given $x \notin fv(\phi)$. By commutativity, there equivalent *right* laws.

- Distributive laws:

$$(\forall x.\psi) \land (\forall x.\phi) \simeq \forall x.(\psi \land \phi)$$
$$(\exists x.\psi) \lor (\exists x.\phi) \simeq \exists x.(\psi \lor \phi)$$

- Implication laws:

$$(\forall x.\psi) \to \phi \simeq \exists x.(\psi \to \phi)$$
$$(\exists x.\psi) \to \phi \simeq \forall x.(\psi \to \phi)$$

  given $x \notin fv(\phi)$, and

$$\psi \to (\forall x.\psi) \simeq \forall x.(\psi \to \phi)$$
$$\psi \to (\exists x.\psi) \simeq \exists x.(\psi \to \phi)$$

  given $x \notin fv(\psi)$. (*Derived using the equivalence* $\psi \to \phi \simeq \neg\psi \lor \phi$).

- Expansion laws:

$$\forall x.\psi \simeq (\forall x.\psi) \land \{t/x\}\,\psi$$
$$\exists x.\psi \simeq (\exists x.\psi) \lor \{t/x\}\,\psi$$

- Alpha equivalence laws:

$$\psi \equiv_\alpha \phi \implies \psi \simeq \phi$$

2.3 Proof Systems

- First-order proof systems $\mathscr{P}$ on $\mathcal{L}_1(\Omega)$ consist of:
  - **Logical** Axioms and Rules: A conventional proof system $\mathscr{P}(\Omega)$ (see section ??) parameterized on Ω (due to substitutions, constants, etc).
  - **Non-logical** Axioms: Axioms defined by the algebra or *model* on Ω. e.g. Group axioms, etc.

2.3.1 Hilbert-Style Proof System

Definition 2.3.1. (**Hilbert-Style $\mathscr{H}_1(\Omega)$**) $\mathscr{H}_1(\Omega)$, the Hilbert-style proof system for first-order logic, is defined on the language $\mathcal{L}_1(\{\neg, \rightarrow, \forall\}, \Omega)$ (henceforth denoted $\mathcal{L}_1(\Omega)$) with the following axioms and inference rules:

$$(\mathrm{S})\ \frac{}{(\psi \rightarrow (\phi \rightarrow \chi)) \rightarrow ((\psi \rightarrow \phi) \rightarrow (\psi \rightarrow \chi))} \qquad (\mathrm{K})\ \frac{}{\psi \rightarrow (\phi \rightarrow \psi)}$$

$$(\mathrm{N})\ \frac{}{(\neg\phi \rightarrow \neg\psi) \rightarrow ((\neg\phi \rightarrow \psi) \rightarrow \phi)} \qquad (\forall\mathsf{D})\ \frac{}{(\forall x.\psi \rightarrow \phi) \rightarrow (\psi \rightarrow \forall x.\phi)}\ [x \notin fv(\psi)]$$

$$(\forall\mathsf{E})\ \frac{}{\forall x.\psi \rightarrow \{t/x\}\,\psi}$$

$$(\mathrm{MP})\ \frac{\psi \qquad \psi \rightarrow \phi}{\phi} \qquad (\forall\mathsf{I})\ \frac{\{y/x\}\,\psi}{\forall x.\psi}\ [x \equiv y \vee y \notin fv(\psi)]$$

Lemma 2.3.1. (**Alpha Equivalence for $\mathscr{H}_1$**) For all $\psi, \phi \in \mathcal{L}_1(\Omega)$,

$$\psi \equiv_\alpha \phi \implies \psi \dashv\vdash_{\mathscr{H}_1} \phi,$$

where $\psi \dashv\vdash_{\mathscr{H}_1} \phi$ iff $\psi \vdash_{\mathscr{H}_1} \phi$ and $\phi \vdash_{\mathscr{H}_1} \psi$.

Theorem 2.3.1. (**The Deduction Theorem for $\mathscr{H}_1$**) For all $\Gamma \subseteq \mathcal{L}_1(\Omega)$ and $\psi, \phi \in \mathcal{L}_1(\Omega)$:

(i) If $\Gamma \vdash_{\mathscr{H}_1} \psi \rightarrow \phi$, then $\Gamma, \psi \vdash_{\mathscr{H}_1} \phi$.

(ii) If $\Gamma, \psi \vdash_{\mathscr{H}_1} \phi$ and ψ is closed, then $\Gamma \vdash_{\mathscr{H}_1} \psi \rightarrow \phi$

Definition 2.3.2. (**The Sequent Form of $\mathscr{H}_1(\Omega)$**) $\mathscr{H}_1^{\varsigma}(\Omega)$, the sequent form of $\mathscr{H}_1(\Omega)$ is a proof system, is defined on the language $\mathscr{S}_{\mathcal{L}_1(\Omega)}$ with the following axioms and inference rules:

$$(\mathrm{R}')\ \frac{\psi \in \Gamma}{\Gamma \vdash \psi}$$

$$(\mathrm{S})\ \frac{}{\Gamma \vdash (\psi \to (\phi \to \chi)) \to ((\psi \to \phi) \to (\psi \to \chi))}$$

$$(\mathrm{K})\ \frac{}{\Gamma \vdash \psi \to (\phi \to \psi)}$$

$$(\mathrm{N})\ \frac{}{\Gamma \vdash (\neg\phi \to \neg\psi) \to ((\neg\phi \to \psi) \to \phi)}$$

$$(\forall \mathsf{D})\ \frac{}{\Gamma \vdash (\forall x.\psi \to \phi) \to (\psi \to \forall x.\phi)}\ [x \notin fv(\psi)]$$

$$(\forall \mathsf{E})\ \frac{}{\Gamma \vdash \forall x.\psi \to \{t/x\}\,\psi}$$

$$(\mathrm{MP})\ \frac{\Gamma \vdash \psi \qquad \Gamma \vdash \psi \to \phi}{\Gamma \vdash \phi}$$

$$(\forall \mathsf{I})\ \frac{\Gamma \vdash \{y/x\}\,\psi}{\Gamma \vdash \forall x.\psi}\ [x \equiv y \vee y \notin fv(\psi) \cup fv(\Gamma)]$$

$$(\mathrm{DT}\ \mathsf{I}')\ \frac{\Gamma, \psi \vdash \phi}{\Gamma \vdash \psi \to \phi}$$

$$(\mathrm{DT}\ \mathsf{E}')\ \frac{\Gamma \vdash \psi \to \phi}{\Gamma, \psi \vdash \phi}$$

- Existential quantification is introduced via a derived operator.

Definition 2.3.3. (**Existential Quantification in $\mathscr{H}_1(\Omega)$**) Existential quantification in $\mathscr{H}_1(\Omega)$ is the *derived operator* defined by

$$\exists x.\psi \triangleq \neg\forall x.\neg\psi.$$

Theorem 2.3.2. Existential quantification introduction, denoted as the derived rule $(\exists \mathsf{I}')$

$$(\exists \mathsf{I}')\ \frac{\Gamma \vdash \{t/x\}\,\psi}{\Gamma \vdash \exists x.\psi}$$

Proof. Let $t \in \mathbb{T}_V(\Omega)$ be arbitrary. We have

$$\dfrac{\dfrac{\dfrac{}{\vdash \forall x.\neg\psi \to \neg\{t/x\}\,\psi}(\forall \mathsf{E}) \qquad \dfrac{}{\vdash (\forall x.\neg\psi \to \neg\{t/x\}\,\psi) \to (\neg\neg\{t/x\} \to \neg\forall x.\neg\psi)}(\mathrm{CP}\ \mathsf{E} \leftarrow')}{\vdash \neg\neg\{t/x\} \to \neg\forall x.\neg\psi}(\mathrm{MP}) \qquad \dfrac{}{\vdash \{t/x\}\,\psi \to \neg\neg\{t/x\}\,\psi}(\mathrm{DN}\ \mathsf{I} \to')}{\vdash \{t/x\}\,\psi \to \neg\forall x.\neg\psi}(\mathrm{T} \to')$$

□

- The rule $(\exists \mathsf{E}')$ *cannot* be expressed as a *derived rule*

$$(\exists \mathsf{E}')\ \frac{\Gamma \vdash \exists x.\psi}{\Gamma \vdash \{x_0/x\}\,\psi}\ [x_0 \notin fv(\Gamma) \cup fv(\exists x.\psi)]$$

Proofs involving $(\exists \mathsf{E}')$ are denoted $\Gamma \vdash_{\exists} \psi$.

Theorem 2.3.3. (**($\exists\mathsf{E}'$) Elimination Theorem**) For all $\Gamma \in \mathcal{P}(\mathcal{L}_1(\Omega)), \psi \in \mathcal{L}_1(\Omega)$

$$\Gamma \vdash_\exists \psi \implies \Gamma \vdash_{\mathscr{H}_1} \psi,$$

assuming no variable introduced by ($\exists\mathsf{E}'$) occurs in ψ.

Proof. (*sketch*) Assume there are k applications of ($\exists\mathsf{E}'$) in $\Gamma \vdash_\exists \psi$. We show, for all $1 \le i \le k$, the statement $P(i)$ holds, that is

$$\Gamma, \left\{y_1^0/y_1\right\}\psi_1, \dots \left\{y_{i-1}^0/y_{i-1}\right\}\psi_{i-1} \vdash_{\mathscr{H}_1} \exists y_i.\psi_i,$$

and

$$\Gamma, \left\{y_1^0/y_1\right\}\psi_1, \dots, \left\{y_i^0/y_i\right\}\psi_i \vdash_\exists \psi,$$

with $(k-i)$ applications of ($\exists\mathsf{E}'$).

Proof.
Base Case: *trivial.*
Inductive Step: Replace

$$(\exists\mathsf{E}')\,\frac{\Gamma, \{y_1^0/y_1\}\psi_1, \dots \left\{y_{i-1}^0/y_{i-1}\right\}\psi_{i-1} \vdash \exists y_i.\psi_i}{\Gamma, \{y_1^0/y_1\}\psi_1, \dots \left\{y_{i-1}^0/y_{i-1}\right\}\psi_{i-1} \vdash_\exists \{y_i^0/y_i\}\psi_i}$$

with

$$(\mathrm{R}')\,\frac{}{\Gamma, \{y_1^0/y_1\}\psi_1, \dots, \{y_i^0/y_i\}\psi_i \vdash_{\mathscr{H}_1} \{y_i^0/y_i\}\psi_i}$$

By the Principle of Mathematical Induction, the statement $P(i)$ holds for all $1 \le i \le k$. □

We show, for all $0 \le i \le k$, the statement $Q(i)$ holds, that is

$$\Gamma, \left\{y_1^0/y_1\right\}\psi_1, \dots, \left\{y_{k-i}^0/y_{k-i}\right\}\psi_{k-i} \vdash_{\mathscr{H}_1} \psi.$$

Proof.
Base Case: We have $Q(0) = P(k)$.
Inductive Step: We have

$$\frac{\dfrac{\Gamma, \{y_1^0/y_1\}\psi_1, \dots, \left\{y_{k-i}^0/y_{k-i}\right\}\psi_{k-i} \vdash \psi}{\Gamma, \{y_1^0/y_1\}\psi_1, \dots, \{y_{k-(i+1)}^0/y_{k-(i+1)}\}\psi_{k-(i+1)} \vdash \left\{y_{k-i}^0/y_{k-i}\right\}\psi_{k-i} \to \psi}}{\Gamma, \{y_1^0/y_1\}\psi_1, \dots, \{y_{k-(i+1)}^0/y_{k-(i+1)}\}\psi_{k-(i+1)} \vdash \forall y_{k-i}^0.(\left\{y_{k-i}^0/y_{k-i}\right\}\psi_{k-i} \to \psi)}$$

We have the derived rule (see equivalences)

$$(\exists \rightarrow') \frac{\Gamma \vdash \forall x.\psi \rightarrow \phi}{\Gamma \vdash (\exists x.\psi) \rightarrow \phi} [x \notin fv(\phi)]$$

So by lemma ??, the derived rule $(\exists \rightarrow')$, and $P(k-(i+1))$ we have:

$$(\mathrm{MP}) \frac{\Gamma, \{y_1^0/y_1\}\,\psi_1, \ldots, \{y_{k-(i+1)}^0/y_{k-(i+1)}\}\psi_{k-(i+1)} \vdash \exists y_{k-i}.\psi_{k-i} \qquad (\exists \rightarrow') \dfrac{\Gamma, \{y_1^0/y_1\}\,\psi_1, \ldots, \{y_{k-(i+1)}^0/y_{k-(i+1)}\}\psi_{k-(i+1)} \vdash \forall y_{k-i}^0.(\{y_{k-i}^0/y_{k-i}\}\,\psi_{k-i} \rightarrow \psi)}{\Gamma, \{y_1^0/y_1\}\,\psi_1, \ldots, \{y_{k-(i+1)}^0/y_{k-(i+1)}\}\psi_{k-(i+1)} \vdash \exists y_{k-i}.\psi_{k-i} \rightarrow \psi}}{\Gamma, \{y_1^0/y_1\}\,\psi_1, \ldots, \{y_{k-(i+1)}^0/y_{k-(i+1)}\}\psi_{k-(i+1)} \vdash \psi}$$

By the Principle of Mathematical Induction, the statement $Q(i)$ holds for all $0 \leq i \leq k$. □

By $Q(k)$, we have $\Gamma \vdash_{\mathscr{H}_1} \psi$. So we are done. □

- $\implies$ $(\exists\mathsf{E}')$ is a sound and complete rule in a non-minimal system.

Theorem 2.3.4. (Soundness and Completeness of $\mathscr{H}_1(\Omega)$) $\mathscr{H}_1(\Omega)$ is sound and complete, that is

$$\forall \Gamma \in \mathcal{P}(\mathcal{L}), \psi \in \mathcal{L}_1(\Omega).\Gamma \vdash_{\mathscr{H}_1} \psi \iff \Gamma \vDash \psi.$$

2.3.2 Sequent Calculus

- Extends $\mathscr{S}_0$ w/ introduction and elimination rules for quantifiers $\mathscr{Q} \in \{\exists, \forall\}$.

Definition 2.3.4. (Sequent Calculus $\mathscr{S}_1(\Omega)$ Proof System) $\mathscr{S}_1(\Omega)$, the Sequent calculus proof system for Propositional logic, is defined on the generalized sequent form language of $\mathcal{L}_1(\Omega)$ with the following axioms and inference rules:

Operator	**Left**	**Right**
Axiom	$(\text{A})\,\dfrac{}{\Gamma, \psi \vdash \Delta, \psi}$	
$\neg$	$(\neg l)\,\dfrac{\Gamma \vdash \Delta, \psi}{\Gamma, \neg\psi \vdash \Delta}$	$(\neg r)\,\dfrac{\Gamma, \neg\psi \vdash \bot}{\Gamma \vdash \Delta, \neg\psi}$
$\wedge$	$(\wedge l)\,\dfrac{\Gamma, \psi, \phi \vdash \Delta}{\Gamma, \psi \wedge \phi \vdash \Delta}$	$(\wedge r)\,\dfrac{\Gamma \vdash \Delta, \psi \qquad \Gamma \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi \wedge \phi}$
$\vee$	$(\vee l)\,\dfrac{\Gamma, \psi \vdash \Delta \qquad \Gamma, \phi \vdash \Delta}{\Gamma, \psi \wedge \phi \vdash \Delta}$	$(\vee r)\,\dfrac{\Gamma \vdash \Delta, \psi, \phi}{\Gamma \vdash \Delta, \psi \vee \phi}$
$\rightarrow$	$(\rightarrow l)\,\dfrac{\Gamma \vdash \Delta, \psi \qquad \Gamma, \phi \vdash \Delta}{\Gamma, \psi \rightarrow \phi \vdash \Delta}$	$(\rightarrow r)\,\dfrac{\Gamma, \psi \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi \rightarrow \phi}$
$\longleftrightarrow$	$(\longleftrightarrow l)\,\dfrac{\Gamma \vdash \Delta, \psi, \phi \qquad \Gamma, \psi, \phi \vdash \Delta}{\Gamma, \psi \longleftrightarrow \phi \vdash \Delta}$	$(\longleftrightarrow r)\,\dfrac{\Gamma, \psi \vdash \Delta, \phi \qquad \Gamma, \phi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \psi \longleftrightarrow \phi}$
$\forall$	$(\forall l)\,\dfrac{\Gamma, \{t/x\}\,\psi \vdash \Delta}{\Gamma, \forall x.\psi \vdash \Delta}$	$(\forall r)\,\dfrac{\Gamma \vdash \Delta, \{y/x\}\,\psi}{\Gamma \vdash \Delta, \forall x.\psi}\,[x \equiv y \vee y \notin fv(\Gamma, \Delta, \psi)]$
$\exists$	$(\exists l)\,\dfrac{\Gamma, \{x_0/x\}\,\psi \vdash \Delta}{\Gamma, \exists x.\psi \vdash \Delta}\,[x_0 \notin fv(\Gamma, \Delta, \psi)]$	$(\exists l)\,\dfrac{\Gamma \vdash \Delta, \{t/x\}\,\psi}{\Gamma \vdash \Delta, \exists x.\psi}$

- Note that $(\forall r)$ and $(\exists l)$ are *dual* rules.

Theorem 2.3.5. (**Soundness and Completeness of $\mathscr{S}_1(\Omega)$**) $\mathscr{S}_1(\Omega)$ is sound and complete, that is

$$\forall \Gamma, \Delta \in \mathcal{P}(\mathcal{L}_1(\Omega)). \Gamma \vdash_{\mathscr{S}_1} \Delta \iff \Gamma \vDash \bigvee \Delta,$$

Proof. By the soundness and completeness of $\mathscr{H}_1(\Omega)$ and the derived rules of $\mathscr{H}_1(\Omega)$, then it follows that $\mathscr{S}_1(\Omega)$ is sound and complete. □

2.4 Skolemization

- **Notation**: $\overrightarrow{\mathcal{Q}\mathbf{x}}$ denotes $\mathcal{Q}_1 x_1 . \mathcal{Q}_2 x_2 . \ldots \mathcal{Q}_n x_n$. $\mathcal{Q}^*$ denotes the *dual quantifier* of $\mathcal{Q}$.

Lemma 2.4.1. (**Quantifier Movement**) Let $\psi, \phi \in \mathcal{L}_1(\Omega)$, $z \notin fv(\psi, \phi) \cup \mathbf{x}$. For all $\mathcal{Q}, \mathcal{O} \in \{\forall, \exists\}$:

$$\overrightarrow{\mathcal{Q}\mathbf{x}} \neg \mathcal{O} y . \psi \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O}^* y . \neg \psi$$
$$\overrightarrow{\mathcal{Q}\mathbf{x}} \left(\mathcal{O} y . \psi \vee \phi \right) \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O} z . \left(\{z/y\} \psi \vee \phi \right)$$
$$\overrightarrow{\mathcal{Q}\mathbf{x}} \left(\psi \vee \mathcal{O} y . \phi \right) \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O} z . \left(\psi \vee \{z/y\} \phi \right)$$

Corollary 2.4.0.1.

$$\overrightarrow{\mathcal{Q}\mathbf{x}} \left(\mathcal{O} y . \psi \wedge \phi \right) \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O} z . \left(\{z/y\} \psi \wedge \phi \right)$$
$$\overrightarrow{\mathcal{Q}\mathbf{x}} \left(\psi \wedge \mathcal{O} y . \phi \right) \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O} z . \left(\psi \wedge \{z/y\} \phi \right)$$
$$\overrightarrow{\mathcal{Q}\mathbf{x}} \left[(\mathcal{O} y . \psi) \rightarrow \phi \right] \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O}^* z . \left(\{z/y\} \psi \rightarrow \phi \right)$$
$$\overrightarrow{\mathcal{Q}\mathbf{x}} \left(\psi \rightarrow \mathcal{O} y . \phi \right) \simeq \overrightarrow{\mathcal{Q}\mathbf{x}} \mathcal{O} z . \left(\psi \rightarrow \{z/y\} \phi \right)$$

Proof. Follows from De Morgan's Laws, and $\rightarrow$ equivalences. □

Definition 2.4.1. (**Quantifier-free Formulae**) The set of quantifier-free formulae $\mathcal{L}_1^{QF}(\Omega)$ is defined by

$$\begin{aligned} \chi, \xi \ ::= \ & p(t_1, \ldots, t_n) \in \Sigma_A(\Omega) \\ \mid \ & \top \mid \bot \mid \neg \chi \\ \mid \ & \chi_1 \wedge \chi_2 \mid \chi_1 \vee \chi_2 \\ \mid \ & \chi_1 \rightarrow \chi_2 \mid \chi_1 \longleftrightarrow \chi_2 \end{aligned}$$

Definition 2.4.2. (**Prenex Normal Form (PNF)**) A formula $\psi \in \mathcal{L}_1(\Omega)$ is said to be in *prenex normal form* if $\psi \in \mathcal{L}_1^{PNF}(\Omega)$, where $\mathcal{L}_1^{PNF}(\Omega)$ is defined by

$$\psi, \phi \ ::= \ \chi \in \mathcal{L}_1^{QF}(\Omega) \ \mid \ \forall x.\psi \ \mid \ \exists x.\psi$$

That is $\psi = \overrightarrow{\mathcal{Q}\mathbf{x}}\chi$.

- $\overrightarrow{\mathcal{Q}\mathbf{x}}$ is the *prenex* and χ is the *body* of ψ.
- $\mathcal{L}_1^{PNF}(\Omega) \cong \mathcal{L}_1(\Omega)$.
- Translation to PNF:
    1. Use α-equivalence to obtain unique variables for all bound and free variables
    2. Use the equivalences of lemma ?? to push quantifiers out.
- PNF contains redundancy $\implies$ PCNF

Definition 2.4.3. (**Prenex Conjunctive Normal Form (PCNF)**) A formula $\psi \in \mathcal{L}_1(\Omega)$ is said to be in *prenex conjunctive normal form* if $\psi \in \mathcal{L}_1^{PNF}(\Omega)$ and the body of ψ (χ) is in CNF.

- Translation from PNF to PCNF:
    1. Convert the "propositional" body χ to CNF. (see section ??)

Theorem 2.4.1. (**Skolem Normal Form Theorem**) Let $\psi \equiv \overrightarrow{\forall\mathbf{x}}\exists y.\phi \in \mathcal{L}_1(\Omega)$ where $\mathbf{x} = \{x_1, \ldots, x_n\}, y$ are distinct, and $\mathcal{Q}x_i \notin [\![\psi]\!]_{\mathcal{Q}}$.

Let $\Omega' = \Omega \cup \{g : s^n \to s\}$ be an *expansion* of Ω. Then

(i) For all Ω' models of $\psi' \equiv \overrightarrow{\forall\mathbf{x}}\, \{g(x_1, \ldots, x_n)/y\}\, \phi \in \mathcal{L}_1(\Omega')$ is a Ω' model of ψ.

(ii) For all Ω models of ψ can be expanded to a Ω' model of ψ'.

Proof.

(i) We have $\models \psi' \to \psi$. Hence for all Ω' homogenous algebra $\mathbf{A}$, $\models_{\mathbf{A}} \psi' \implies \models_{\mathbf{A}} \psi$ by the Deduction Theorem.

(ii) Let $\mathbf{A}$ be a Ω-model of ψ, that is $\vDash_{\mathbf{A}} \psi$. Hence for all $\mathbf{a} \in |\mathbf{A}|^n$, there exists $a \in |\mathbf{A}|$ s.t

$$\mathcal{T}_{\mathbf{A}} [\![\phi]\!]_{v_{\mathbf{A}}\{(x_i,a_i),(y,a)\}} = 1.$$

Define a function $g_{\mathbf{A}} : |\mathbf{A}|^n \to |\mathbf{A}|$ s.t

$$g(a_1, \ldots, a_n) = a \iff \mathcal{T}_{\mathbf{A}} [\![\phi]\!]_{v_{\mathbf{A}}} = 1.$$

So we have

$$\mathcal{T}_{\mathbf{A}} [\![\phi]\!]_{v_{\mathbf{A}}\{(x_i,a_i),(y,g_{\mathbf{A}}(a_1,\ldots,a_n))\}} = 1$$

Let $\mathbf{B}$ be an extension of $\mathbf{A}$ w/ signature Ω' and $g_{\mathbf{B}} = g_{\mathbf{A}}$. Then it follows that for all $v_{\mathbf{B}} \in \Sigma_v(\mathbf{B})$:

$$\mathcal{T}_{\mathbf{A}} [\![\{g(x_1, \ldots, x_n)/y\} \, \phi]\!]_{v_{\mathbf{B}}} = 1.$$

So we have $\vDash_{\mathbf{B}} \psi'$.

$\square$

Corollary 2.4.1.1. (**Equisatisfiablity**) Let $\psi \in \mathcal{L}_1(\Omega), \psi' \in \mathcal{L}_1(\Omega')$ be as defined.

(i) $\exists \mathbf{A}. \vDash_{\mathbf{A}} \psi \implies \exists \mathbf{B}. \vDash_{\mathbf{B}} \psi'$.

(ii) ψ is unsatisfiable $\iff$ ψ' is unsatisfiable.

- g is said to be a *Skolem function* (for $n = 0$, $c = g()$ is a *Skolem constant*).

Definition 2.4.4. (**Skolem normal form (SNF)**) A formula $\psi \in \mathcal{L}_1(\Omega)$ is said to be in *skolem normal form* if $\psi \equiv \forall \mathbf{x}.\chi$ where $\chi \in \mathcal{L}_1^{QF}(\Omega)$. The set of SNF formulae is denoted $\mathcal{L}_1^{SNF}(\Omega)$.

If χ is in CNF, then ψ is in *skolem conjunctive normal form* (SCNF).

- Translating ψ to SCNF, denoted $[\![\psi]\!]_{SCNF}$:
  - Translate ψ into CNF. (see section ??)
  - Push existential quantifiers out using lemma ?? (or push universal quantifiers in: *miniscoping*) Until we have quantifier form: $\forall \overrightarrow{\mathbf{x}} \exists y.\phi$.
  - Choose $|\mathbf{x}|$ function symbol g, delete $\exists y$ and *replace free occurrences* of y w/ g: $\forall \overrightarrow{\mathbf{x}} \, \{g(x_1, \ldots, x_n)/y\} \, \phi$.
- Using a PNF (pushing out quantifiers) is harder. Push quantifiers in for better clauses. This is called *miniscoping*.

2.5 Herbrand's Theorem

Definition 2.5.1. (**The Herband Universe**) Let Ω be a homogenous signature containing at least one constant. The set of *ground terms* $\mathbb{T}_\Omega \subseteq \mathbb{T}_\Omega(V)$ is called the **Herbrand Universe**.

Definition 2.5.2. (**Herbrand Algebra**) A Ω-algebra $\mathbf{H}(\Omega)$ where Ω contains at least one constant, is a **Herbrand Algebra** iff $|\mathbf{H}(\Omega)| = \mathbb{T}_\Omega$.

- For all $f \in \mathscr{F}$, $f_\mathbf{H} = f$. $\mathbf{H}$ must define $p_\mathbf{H} \subseteq \mathbb{T}_\Omega^n$.
- $|\mathbf{H}(\Omega)|$ is non-empty since Ω contains at least one constant.
- Valuations $v_\mathbf{H}$ are *ground substitutions*: $v_\mathbf{H} : V \to \mathbb{T}_\Omega$ (or $|\mathbf{H}|$).

Definition 2.5.3. (**Herbrand Interpretation**) A Herbrand interpretation is $\mathcal{I} = (\mathbf{H}, v_\mathbf{H})$ where $v_\mathbf{H} : V \to \mathbb{T}_\Omega$. For all $t \in \mathbb{T}_V(\Omega)$ with $var(t) = \{x_1, \ldots, x_n\}$,

$$\mathcal{V}_\mathbf{H} [\![t]\!]_{v_\mathbf{H}} = \{v(x_i)/x_i : 1 \leq i \leq n\}\, t.$$

Definition 2.5.4. (**Herbrand Model**) A **Herbrand model** of a set $\Delta \in \mathcal{P}(\mathcal{L}_1(\Omega))$, denoted $\vDash_\mathbf{H} \Delta$, is a Herbrand algebra $\mathbf{H}$ s.t

$$\forall v_\mathbf{H} \in \Sigma_v(\mathbf{H}).\forall \psi \in \Delta.\ \vDash_{(\mathbf{H}, v_\mathbf{H})} \psi,$$

where $v_\mathbf{H}$ is a Herbrand valuation (defined on the $fv(\Delta)$).

Theorem 2.5.1. Let Ω be a homogenous signature containing at least one constant. Let $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ be a finite set of *ground literals.*

(i) $\bigwedge \Lambda$ has a model $\iff P(\Lambda) \cap N(\Lambda) = \emptyset$.

(ii) $\bigwedge \Lambda$ is never valid.

(iii) $\bigvee \Lambda$ always has a model.

(iv) $\bigvee \Lambda$ is valid $\iff P(\Lambda) \cap N(\Lambda) \neq \emptyset$.

Definition 2.5.5. (**Ground Instances**) Let Ω be a homogenous signature containing at least one constant. Let $\Delta \subseteq \left\{\overrightarrow{\forall \mathbf{x}}\chi : \chi \in \mathcal{L}_1^{QF}(\Omega) \wedge \mathbf{x} = fv(\chi)\right\} = \mathcal{L}_1^{\forall QF}(\Omega)$ be a non-empty set of formulae. The **ground instance** of $\psi \equiv \overrightarrow{\forall \mathbf{x}}\chi \in \Delta$, denoted $\mathfrak{g}(\psi)$, is

$$\mathfrak{g}(\psi) = \{\{t_1/x_1, \ldots, t_n/x_n\}\, \chi : t_1, \ldots, t_n \in \mathbb{T}_\Omega\}.$$

- $\mathfrak{g}(\Delta) = \bigcup_{\psi \in \Delta} \mathfrak{g}(\psi)$.

Theorem 2.5.2. (**Herbrand's Theorem**) Let Ω and Δ be as in definition ??. Then

$$\begin{aligned} &\Delta \text{ has a model} \\ \iff &\Delta \text{ has a Herbrand model} \\ \iff &\mathfrak{g}(\Delta) \text{ has a model} \\ \iff &\mathfrak{g}(\Delta) \text{ has a Herbrand model} \end{aligned}$$

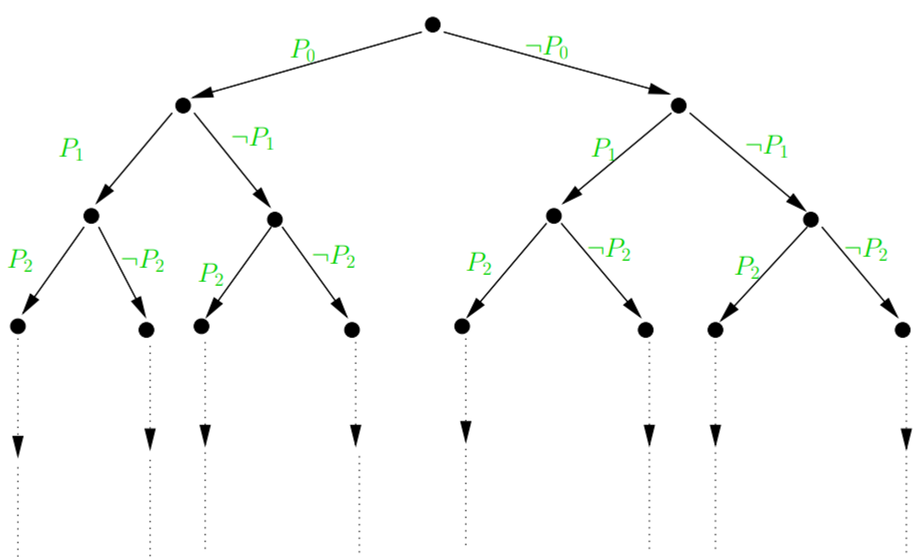
Proof. (*Sketch*) It suffices to show that for all $\psi \in \mathcal{L}_1(\Omega)$, ψ has a model $\implies$ ψ has a Herbrand model.

Assume $\models_{\mathbf{A}} \psi$. We define the Herbrand interpretation $(\mathbf{H}, v_{\mathbf{H}})$ where for all $p \in \mathscr{R}$

$$p_{\mathbf{H}} = \{(t_1, \ldots, t_n) \in \mathbb{T}_\Omega : \models_{\mathbf{A}} p(t_1, \ldots, t_n)\}.$$

So we have $p_{\mathbf{H}} = p_{\mathbf{A}}$. By induction, on $\mathcal{T}[\![\cdot]\!]$ and ψ, we deduce that $\models_{\mathbf{A}} \psi$. $\square$

- Set of Herbrand algebras may be though paths on trees $\mathscr{T}_{|\mathbf{H}|}$ that enumerate the countably infinite set of *ground atomic formulae*: $p(t_1, \ldots, t_n)$.



- Given a vertex v, $\mathbf{H}_\pi$ is the Herbrand algebra defined by labels of the path $\pi \in \mathscr{T}_{|\mathbf{H}|}$ from the root to v.

Lemma 2.5.1. Let $\Delta \subseteq \mathfrak{g}(\mathcal{L}_1^{QF}(\Omega))$ be a set of ground quantifier-free formulae. Δ has a model $\iff \forall$ finite $\Gamma \in \mathcal{P}(\Delta).\Gamma$ has a model.

Proof.
$(\implies)$. *Trivial.*
$(\impliedby)$. Assume $\forall$ finite $\Gamma \in \mathcal{P}(\Delta).\Gamma$ has a model. We proceed by contradiction, assume Δ does not have a model.

By Herbrand theorem, Γ has a Herbrand model and Δ does not have a Herbrand model. Hence for all paths $\pi \in \mathscr{T}_{|\mathbf{H}|}$, there exists $\chi_\pi \in \Delta$ s.t $\not\models_{\mathbf{H}_\pi} \chi_\pi$.

Since χ_π consists of a finite set of ground atoms, there exists a finite path π s.t $\not\models_{\mathbf{H}_\pi} \chi_\pi$. Hence the set $\{\chi_\pi : \not\models_{\mathbf{H}_\pi} \chi_\pi\} \in \mathcal{P}(\Delta)$ is a finite subset of Δ that doesn't have a Herbrand model. Hence by Herbrand's Theorem, $\{\chi_\pi : \not\models_{\mathbf{H}_\pi} \chi_\pi\}$ doesn't have a model. A contradiction!

□

Theorem 2.5.3. Let $\Delta \in \mathcal{P}(\mathcal{L}_1(\Omega))$. Δ has a model $\iff \forall$ finite $\Gamma \in \mathcal{P}(\Delta).\Gamma$ has a model.

Proof. (*Sketch*)
By lemma ??, Δ has a model $\iff [\![\Delta]\!]^{SNF} = \left\{[\![\psi]\!]^{SNF} : \psi \in \Delta\right\}$ has a model. By Herbrand's theorem, $\iff \mathfrak{g}([\![\Delta]\!]^{SNF})$ has a model. By lemma ??, $\iff \forall$ finite $\Gamma' \in \mathcal{P}(\mathfrak{g}([\![\Delta]\!]^{SNF}))$ has a model.
$(\implies)$. *Trivial*
$(\impliedby)$. Assume Δ doesn't have a model. Hence finite Γ' does not have a model. Since Γ' is a subset of a ground instantiation of some finite $\Gamma \in \mathcal{P}(\Delta)$, denoted $\Gamma' \subseteq v_{\mathbf{H}}(\Gamma)$, then it follows that Γ does not have a model. A contradiction!

□

Theorem 2.5.4. (**Skolem-Godel-Herbrand Theorem**) Let $\Delta \in \mathcal{P}(\mathcal{L}_1(\Omega))$. Δ is unsatisfiable, iff $\exists$ finite $\Gamma \in \mathcal{P}(\mathfrak{g}(\Delta)).\Gamma$ is unsatisfiable.

Proof. See theorem ??. □

- $\implies$ Decidable method for determining whether Δ is unsatisfiable:

– Given ψ, compute $\psi' \leftarrow [\![\psi]\!]^{SCNF}$.
– Compute:

```
Γ ← {new_instance_of(ψ')}
while (Γ is satisfiable) {
    Γ ← Γ ∪ {new_instance_of(ψ')}
}
```

Generating new instances of ψ' consists of enumerating the ground substitutions $v_{\mathbf{H}} : V \to \mathbb{T}_\Omega$, which is countable.

2.6 Unification

Definition 2.6.1. (**Instance**) A term $t \in \mathbb{T}_\Omega(V)$ is an instance of $s \in \mathbb{T}_\Omega(V)$ iff there exists a substitution θ s.t $t \equiv \theta s$.

- t is a *common instance* of $t_1, \ldots, t_n$ iff there exists $\theta_1, \ldots, \theta_n$ s.t $t \equiv \theta_1 t_1 \equiv \theta_2 t_2 \equiv \cdots \equiv \theta_n \theta_n$.
- **Problem**: Finding common instances $\implies$ unification. The process of solving the "equation" $\theta s \equiv \theta t$.

Definition 2.6.2. (**Unifiability**) A term $t \in \mathbb{T}_\Omega(V)$ is *unifiable* with $s \in \mathbb{T}_\Omega(V)$ if there exists a substitution θ s.t $\theta t \equiv \theta s$, denoted $t \sim s : \theta$. θ is the *unifier* of s, t.

- Some unifiers may be regarded as being "more general"

Definition 2.6.3. Let θ, τ be substitutions.

– θ is *more* **general** than τ, denoted $\theta \gtrsim \tau$, iff there exists χ s.t $\tau = \chi \circ \theta$.

– θ is *strictly more* **general** than τ, denoted $\theta \succ \tau$ if $\theta \gtrsim \tau$ and $\tau \not\gtrsim \theta$.

- $\gtrsim$ is a preorder on $\mathbf{S}_\Omega(V)$. $\theta \sim \tau \iff \theta \gtrsim \tau \wedge \tau \gtrsim \theta$, defines an *equivalence relation* on $\mathbf{S}_\Omega(V)$.

Definition 2.6.4. (**Most General Unifier**) A subsitution θ is the *most general unifier (mgu)* of $s, t \in \mathbb{T}_\Omega(V) \iff$ for all unifiers $s \sim t : \tau$, there exists χ s.t $\tau = \chi \circ \theta$

- **Note**: There may be **multiple** mgus. If θ and τ are mgu's of $s, t \in \mathbb{T}_\Omega(V)$, then $\theta \sim \tau$.

Theorem 2.6.1. (**Unification Algorithm**) For all $t, s \in \mathbb{T}_\Omega(V)$, the mgu θ of t, s satisfies $t \sim s \rhd \theta$, inductively defined by:

$$(\mathsf{Var})\ \frac{}{x \sim x \rhd \emptyset}$$

$$(\mathsf{Var\text{-}Left})\ \frac{x \notin fv(\psi)}{x \sim \psi \rhd \{t/x\}} \qquad (\mathsf{Var\text{-}Right})\ \frac{x \notin fv(\psi)}{\psi \sim x \rhd \{t/x\}}$$

$$(\mathsf{Comp})\ \frac{\psi_1 \sim \phi_1 \rhd \theta_1 \qquad \dots \qquad (\theta_{n-1} \circ \dots \circ \theta_1)\psi_n \sim (\theta_{n-1} \circ \dots \circ \theta_1)\phi_n \rhd \theta_n}{o(\psi_1, \dots, \psi_n) \sim o(\phi_1, \dots, \phi_n) \rhd \theta_n \circ \dots \circ \theta_1}$$

where $x \in V, o \in \Omega$.

- $\implies$ natural recursive unification algorithm.

2.7 Automated Theorem Proving

2.7.1 First-Order Resolution

- **Recall**:
  - For all $\Gamma \in \mathcal{P}(\mathcal{L}_1(\Omega)), \psi \in \mathcal{L}_1(\Omega)$, $\Gamma \vDash \psi \iff \Delta \cup \{\neg\psi\}$ is unsatisfiable.
  - Δ has an equi-unsatisfiable set $[\![\Delta]\!]^{SNF}$

Definition 2.7.1. (**SCNF Clauses**) A (set-based) SCNF family of clauses of $[\![\psi]\!]^{SCNF}$ for $\psi \in \mathcal{L}_1(\Omega)$ is the set $\Delta = \{C_i : 1 \leq i \leq n\}$ s.t $[\![\psi]\!]^{SCNF} \equiv \forall \overrightarrow{\mathbf{x}}. \bigwedge_{1 \leq i \leq n} C_i$, where each clause $C_i \equiv \bigvee_{1 \leq j \leq m_i} \lambda_j$ has the (set-based) clause $C_i = \{\lambda_j : 1 \leq j \leq_{,i}\}$.

- **Notation**:
  - For any substitution θ, $\theta C = \{\theta\lambda_j : 1 \leq j \leq m\}$
  - $\mathfrak{g}(C) = \{\theta C : \theta : V \to \mathbb{T}_\Omega\}$

Lemma 2.7.1. Let $\{C_i : 1 \leq i \leq n\} \in \Sigma_\Delta(\Omega)$ be a family of clauses. Then

$$\overrightarrow{\forall \mathbf{x}} \bigwedge_{1 \leq i \leq n} C_i \simeq \bigwedge_{1 \leq i \leq n} \overrightarrow{\forall \mathbf{x}_i} C_i.$$

Proof. $\forall$ and $\wedge$ cases of lemma ?? $\square$

- Removes common variables between clauses, allowing clauses: $\{p(x)\}$ and $\{\neg p(g(x))\}$ are unifiable.

Definition 2.7.2. ($\mathscr{R}_1(\Omega)$ **Proof System**) The $\mathscr{R}_1(\Omega)$ resolution proof system is defined on the language $\Sigma_\Delta(\Omega)$ with the following axioms and inference rules:

$$(\emptyset)\ \frac{\emptyset \in \Delta}{\Delta}$$

$$(\mathrm{R})\ \frac{\Delta \cup \left\{\theta(C_i' \cup C_j')\right\}}{\Delta \cup \left\{(C_i' \cup \Lambda_p^i), (C_j' \cup \overline{\Lambda_p^j})\right\}}\ [\theta = \mathsf{unify}(\Lambda_p^i \cup \overline{\Lambda_p^j})]$$

where $i \neq j, \Lambda_p^i = \{p(\mathbf{s}) \in C_i\} \neq \emptyset$, and $\overline{\Lambda_p^j} = \{\neg p(\mathbf{t}) \in C_j\} \neq \emptyset$.

- **Non-terminating**: Each application of (R) may not remove *all* occurrences of p. Since Λ need not exhaust all literals in either clauses (and other clauses may contain occurrences of p).

Theorem 2.7.1. (**Soundness and Completeness of** $\mathscr{R}_1(\Omega)$) $\mathscr{R}_1(\Omega)$ is sound and complete, that is

$$\forall \Delta \in \Sigma_\Delta(\Omega).\ \vdash_{\mathscr{R}_1} \Delta \iff \Delta \text{ is unsatisfiable.}$$

- $\mathscr{R}_1(\Omega)$ may be defined using a *binary resolution and factoring rule*:

$$(\emptyset)\,\frac{}{\emptyset}$$

$$(\text{BR})\,\frac{\psi, C \qquad \phi, C'}{\theta(C, C')}\,[\psi \sim \phi : \theta]$$

$$(\text{F})\,\frac{\psi_1, \ldots, \psi_n, C}{\theta(\psi_1, C)}\,[\theta\psi_1 \equiv \cdots \theta\psi_n]$$

- The binary resolution rule (BR) increases the size of clauses (assuming C and C' are disjoint). Hence factoring rule (F) is required for completeness of $\mathscr{R}_1(\Omega)$ since a refutation in $\mathscr{R}_1(\Omega)$ requires the empty clause $\emptyset$, thus a rule is required to *reduce* the size of clauses.

Definition 2.7.3. (**Subsumption**) A clause C subsumes C' iff there exists θ s.t $\theta C \subseteq C'$.

- In $\mathscr{R}_1(\Omega)$, we delete subsumed clauses from Δ, as they don't the satisfiability of Δ.
- **Redundant Clauses**:
  - Tautological clauses. e.g. $\{P, \neg P, \ldots\}$
  - Subsumed clauses. e.g. $\{P, Q\}$ is subsumed by $\{P\}$.

2.7.1.1 Prolog

Definition 2.7.4. (**Horn Clause**) A Horn Clause, or *definite clause*, is a clause of the form: $\{\neg p_1(\mathbf{t}_1), \ldots, \neg p_n(\mathbf{t}_n), p(\mathbf{s})\}$, or in Kowalski notation, $p_1(\mathbf{t}_1), \ldots, p_n(\mathbf{t}_n) \to p(\mathbf{s})$

- **Notation**:
  - $p(\mathbf{s}) \leftarrow p_1(\mathbf{t}_1), \ldots, p_n(\mathbf{t}_n)$
    e.g. `friends(A, B)` $\leftarrow$ `likes(A, B), likes(B, A).`
  - If $n \geq 1$, then the clause is a *rule*. If $n = 0$, then the clause is a *fact*.
- Prolog uses **linear resolution** in $\mathscr{R}_1(\Omega)$, with a program being stored in a database $\mathcal{D}$ of clauses, and a query (or goal clause): $p(\mathbf{t}) \leftarrow$ (Prolog notation: `?-` $p(\mathbf{t})$`.`)

- Linear resolution $\implies$ improved space complexity, reduced search space (only (BR) rule may be used). Deterministic search.

2.7.2 Tableaux Calculus

- **Problem**: Dual rules w/ connectives in $\mathscr{S}_1(\Omega)$ $\implies$ redundancy

Definition 2.7.5. (**Tableaux Calculus**) $\mathscr{T}_1(\Omega)$, the Tableaux calculus proof system for first order logic, defined on NNF $\mathcal{L}_1^{NNF}(\Omega)$, with the following axioms and inference rules:

$$(\text{Basic})\ \frac{}{\neg\psi, \psi, \Gamma \vdash} \qquad (\text{Cut})\ \frac{\neg\psi, \Gamma \vdash \qquad \psi, \Gamma \vdash}{\Gamma \vdash}$$

$$(\wedge l)\ \frac{\psi, \phi, \Gamma \vdash}{\psi \wedge \phi, \Gamma \vdash} \qquad (\vee l)\ \frac{\psi, \Gamma \vdash \qquad \phi, \Gamma}{\psi \vee \phi, \Gamma \vdash}$$

$$(\forall l)\ \frac{\{t/x\}\,\psi, \Gamma \vdash}{\forall x.\psi, \Gamma \vdash} \qquad (\exists l)\ \frac{\{x_0/x\}\,\psi, \Gamma \vdash}{\exists x.\psi, \Gamma \vdash}\,[x_0 \notin fv(\psi, \Gamma)]$$

- $\mathscr{T}_0^{\Box}$ uses the left modal rules of $\mathscr{S}_0^{\Box}$.
- To prove $\Gamma \vDash \psi$:
  - Convert to $[\![\Gamma]\!]_{NNF}, [\![\psi]\!]_{NNF} \vdash$, a *refutation system.*
  - Find a proof tree $\mathscr{T}$ in $\mathscr{T}_1(\Omega)$ $\iff$ $\Gamma \vDash \psi$
- **Problem**: Choice of term in $(\forall l)$ still yields non-determinism.
- **Solution**: Unification w/ Skolemization $\implies$ free-variable tableaux calculus

Definition 2.7.6. (**Free-Tableaux Calculus**) $\mathscr{T}_1^{fv}(\Omega)$, the Tableaux calculus proof system for first order logic, defined on Skolem NNF $\mathcal{L}_1^{SNNF}(\Omega)$, with the following axioms and inference rules:

$$\text{(Basic)}\ \frac{\phi \sim \psi : \theta}{\neg\phi, \psi, \Gamma \vdash} \qquad \text{(Cut)}\ \frac{\neg\psi, \Gamma \vdash \qquad \psi, \Gamma \vdash}{\Gamma \vdash}$$

$$(\wedge l)\ \frac{\psi, \phi, \Gamma \vdash}{\psi \wedge \phi, \Gamma \vdash} \qquad (\vee l)\ \frac{\psi, \Gamma \vdash \qquad \phi, \Gamma}{\psi \vee \phi, \Gamma \vdash}$$

$$(\forall l)\ \frac{\{y/x\}\, \psi, \Gamma \vdash}{\forall x.\psi, \Gamma \vdash}\ [y \notin fv(\psi, \Gamma)]$$

- **Note**: Free variables in $\Gamma \vdash$ must unify to the same terms. Otherwise the proof fails, by the $(\forall l)$ rule in $\mathscr{T}_1(\Omega)$

3 Decision Procedures

- **Decidability**: A set of problems is *decidable* $\iff$ there exists a algorithm that determines whether an instance of the problem has a solution. (See Computation Theory).
- The algorithm is a *decision procedure*.

3.1 Fourier-Motzkin Elimination

- Decision procedure for solving systems of linear constraints:

$$\bigwedge_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_j \leq b_i.$$

  By eliminating a n-variable system to a $(n-1)$-variable system.

- **Procedure**:
  1. For all $1 \leq i \leq m$, we have the following cases:
     - $a_{in} = 0 \implies$ constraint doesn't involve x_n.
     - $$a_{in} > 0 \implies x_n \leq \frac{1}{a_{in}} \left(b_i - \sum_{j=1}^{n-1} a_{ij} x_j \right).$$
     - $$a_{in} < 0 \implies x_n \geq \frac{1}{a_{in}} \left(b_i - \sum_{j=1}^{n-1} a_{ij} x_j \right).$$
  2. This yields the set of constraint

$$\bigwedge_{i=1}^{k} L_i(x_1, \ldots, x_{n-1}) \leq x_n \quad \bigwedge_{i=1}^{\ell} x_n \leq U_i(x_1, \ldots, x_{n-1}),$$

where L_i, U_i are lower and upper bounds w/ $n-1$ variables and $k + \ell \leq m$

3. Set of constraints are valid iff

$$\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{\ell} L_i(\mathbf{x}) \leq U_j(\mathbf{x}) \iff \bigwedge_{1 \leq i \leq k, 1 \leq j \leq \ell} L_i(\mathbf{x}) - U_j(\mathbf{x}) \leq 0,$$

yielding $k \cdot \ell$ constraints w/ $n-1$ variables.

4. Repeat 1 - 3 until system of 0 (or 1) variables. A contradicting constraint $\implies$ unsatisfiablity. Otherwise satisfiable.

- **Complexity**: Doubly exponential $\Theta\left(\frac{m^{2^n}}{2^{2^{n+1}-1}}\right)$ (for average # of upper and lower bounds: $m/2$):

$$T(m, 0) = \Theta(m)$$
$$T(m, n) = T\left(\frac{m^2}{4}, n-1\right)$$

3.2 Satisfiability Modulo Theories

- SMTs are decision procedures for propositional logic w/ propositions ranging over relations on integers, reals, etc.
- $\mathcal{T}$-solvers: domain specific solvers that determine $\Delta \vDash_{\mathcal{T}} C$ (defined on $\Sigma_\Delta(\Omega_{\mathcal{T}})$). Set of $\mathcal{T}$-solver atoms: $\Sigma_A(\Omega_{\mathcal{T}})$.

Definition 3.2.1. (**DPLL($\mathcal{T}$)**) DPLL($\mathcal{T}$) is an extension of DPLL that determines a model for a formula in $\mathcal{L}_0$ w/ $\Sigma_P = \Sigma_A(\Omega_{\mathcal{T}})$ (an extension of propositional logic w/ domain specific propositions).

- DPLL($\mathcal{T}$) procedure:
  1. Convert a formula to a family of clauses ($\mathcal{T}$ propositions are literals e.g. $x \geq 7$ is a literal).
  2. Use the DPLL algorithm (without pure literal elimination) until either unsatisfiablity or a model.

3. If a model (interpretation) $\mathcal{I}$, $\mathcal{T}$-solver (a domain specific decision procedure) determines validity of $\mathcal{I}$.
4. If $\mathcal{I}$ (represented by set of literals Γ) is invalid by $\mathcal{T}$-solver, then backtrack.

Definition 3.2.2. (**DPLL($\mathcal{T}$) Proof System**) The $\mathscr{D}_0(\mathcal{T})$ DPLL($\mathcal{T}$) proof system is defined on the sequents of Σ_Δ w/ the following axioms and inference rules:

$$\text{(Unit)}\ \frac{\Gamma, \ell \vdash \Delta}{\Gamma \vdash \Delta, \{\ell\}}$$

$$\text{(Unit } \mathsf{E}_1\text{)}\ \frac{\Gamma, \ell \vdash \Delta}{\Gamma, \ell \vdash \Delta, C \cup \{\ell\}} \qquad \text{(Unit } \mathsf{E}_2\text{)}\ \frac{\Gamma, \ell \vdash \Delta, C}{\Gamma, \ell \vdash \Delta, C \cup \{\neg\ell\}}$$

$$\text{(Split)}\ \frac{\Gamma, \ell \vdash \Delta \qquad \Gamma, \neg\ell \vdash \Delta}{\Gamma \vdash \Delta}$$

$$\text{(Unsat)}\ \frac{}{\Gamma \vdash \Delta, \emptyset} \qquad (\mathcal{T}\text{-Solve})\ \frac{\Gamma \vDash_{\mathcal{T}}}{\Gamma \vdash}$$

- Example $\mathcal{T}$-solver: Fourier-Motzkin Elimination.

4 Modal Logic

- Logic based on "necessary" and "possibly".

4.1 Syntax

Definition 4.1.1. (**Modal Logic**) Given Σ_P as countably infinite set of propositional symbols:

- $\Omega_0^\Box = \Omega_0 \cup \{\Box, \Diamond\}$ is the set of operators, where $\Box$ and $\Diamond$ are the *necessary* and *possibly* operators.
- The formal language of modal logic is $\mathcal{L}_0^\Box(\Omega_0^\Box) = \mathbb{T}_{\Omega_0^\Box}(\Sigma_P)$, often denoted $\mathcal{L}_0^\Box$

$$\begin{aligned} \psi \ ::= &\ P \in \Sigma_P \\ \mid &\ \ldots \\ \mid &\ \Box\psi \ \mid \ \Diamond\psi \end{aligned}$$

- **Precedence**: (in order) of operators in $\Omega_0^\Box$:
$\longleftrightarrow < \rightarrow < \vee < \wedge < \neg < \Diamond < \Box$.

4.2 Semantics

- **Idea**: Reason about "necessarily" and "possibly" using worlds (states) w/ transitions.

Definition 4.2.1. (**Modal Frame**) A *modal frame* is the pair $(\mathscr{W}, R)$, where $\mathscr{W}$ is the non-empty set of *possible worlds* and $R : \mathscr{W} \leftrightarrow \mathscr{W}$ is the *accessibility relation*.

Definition 4.2.2. (**Modal Interpretation**) The modal interpretation $\mathcal{I}$ defined on the frame $(\mathscr{W}, R)$ is a function $\mathcal{I} : \Sigma_P \to \mathcal{P}(\mathscr{W})$.

- $\mathcal{I}(P)$ is the set of worlds that propositional symbol P is true.
- Modal operators $\Box, \Diamond$ relate to universal and existential quantification over $(\mathscr{W}, R)$

Definition 4.2.3. (**Valuation**) The *truth* value of the proposition $\psi \in \mathcal{L}_0^{\Box}$ in the context of modal frame $(\mathscr{W}, R)$ and interpretation $\mathcal{I} \in \Sigma_{\mathcal{I}}(\mathscr{W})$ in world $w \in \mathscr{W}$, denoted $\mathcal{T}_w [\![\psi]\!]_{\mathcal{I}}$, where $\mathcal{T}_w [\![\cdot]\!]_{\mathcal{I}} : \mathcal{L}_0^{\Box} \to |\mathbf{B}|$ is inductively defined by

$$\begin{aligned}
\mathcal{T}_w [\![\top]\!]_{\mathcal{I}} &= 1 & \mathcal{T}_w [\![\bot]\!]_{\mathcal{I}} &= 0 \\
\mathcal{T}_w [\![P]\!]_{\mathcal{I}} &= w \in \mathcal{I}(P) & \mathcal{T}_w[\neg\psi] &= \overline{\mathcal{T}_w [\![\psi]\!]_{\mathcal{I}}} \\
\mathcal{T}_w [\![\psi_1 \wedge \psi_2]\!]_{\mathcal{I}} &= \mathcal{T}_w [\![\psi_1]\!]_{\mathcal{I}} \cdot \mathcal{T}_w [\![\psi_2]\!]_{\mathcal{I}} & \mathcal{T}_w [\![\psi_1 \vee \psi_2]\!]_{\mathcal{I}} &= \mathcal{T}_w [\![\psi_1]\!]_{\mathcal{I}} + \mathcal{T}_w [\![\psi_2]\!]_{\mathcal{I}} \\
\mathcal{T}_w [\![\psi_1 \to \psi_2]\!]_{\mathcal{I}} &= \overline{\mathcal{T}_w [\![\psi_1]\!]_{\mathcal{I}}} + \mathcal{T}_w [\![\psi_2]\!]_{\mathcal{I}} & \mathcal{T}_w [\![\psi_1 \longleftrightarrow \psi_2]\!]_{\mathcal{I}} &= \overline{\mathcal{T}_w [\![\psi_1]\!]_{\mathcal{I}} \oplus \mathcal{T}_w [\![\psi_2]\!]_{\mathcal{I}}} \\
\mathcal{T}_w [\![\Box\psi]\!] &= \prod_{w' \in \mathscr{W} : R(w,w')} \mathcal{T}_{w'} [\![\psi]\!]_{\mathcal{I}} & \mathcal{T}_w [\![\Diamond\psi]\!] &= \sum_{w' \in \mathscr{W} : R(w,w')} \mathcal{T}_{w'} [\![\psi]\!]
\end{aligned}$$

- **Notation**: $w \Vdash_{(\mathscr{W},R),\mathcal{I}} \psi \iff \mathcal{T}_w [\![\psi]\!] = 1$ in modal frame $(\mathscr{W}, R)$.

Definition 4.2.4. (**Validity**) For $\psi \in \mathcal{L}_0^{\Box}$:

- ψ is valid, denoted $\Vdash_{(\mathscr{W},R),\mathcal{I}} \psi$, iff $\forall w \in \mathscr{W} . w \Vdash_{(\mathscr{W},R),\mathcal{I}} \psi$.
- ψ is *universally valid*, denoted $\Vdash_{(\mathscr{W},R)} \psi$, iff $\forall \mathcal{I} \in \Sigma(\mathscr{W}). \Vdash_{(\mathscr{W},R),\mathcal{I}} \psi$.

- All propositional tautologies are *universally valid*.

Definition 4.2.5. (**Entailment and Equivalence**) For $\psi_1, \psi_2 \in \mathcal{L}_0^{\Box}$:

- ψ_1 entails ψ_2, denoted $\psi_1 \Vdash_{(\mathscr{W},R)} \psi_2$ iff $\forall \mathcal{I} \in \Sigma_{\mathcal{I}}(\mathscr{W}). \Vdash_{(\mathscr{W},R),\mathcal{I}} \psi_1 \implies \Vdash_{(\mathscr{W},R),\mathcal{I}} \psi_2$.
- ψ_1 and ψ_2 are equivalent, denoted $\psi_1 \simeq_{(\mathscr{W},R)} \psi_2 \iff \psi_1 \Vdash_{(\mathscr{W},R)} \psi_2 \wedge \psi_2 \Vdash_{(\mathscr{W},R)} \psi_1$.

- **Notation**: Modal frame is often implicit e.g. $\Vdash \psi$.

Theorem 4.2.1. (**Deduction Theorem** $\implies$) For all $\psi, \phi \in \mathcal{L}_0^{\Box}$:

(i) $\Vdash \psi \to \phi \implies \psi \Vdash \phi$

(ii) $\Vdash \psi \longleftrightarrow \phi \implies \psi \simeq \phi$

4.2.1 Equivalences

- Dual laws:
$$\Box\psi \simeq \neg\Diamond\neg\psi \quad \Diamond\psi \simeq \neg\Box\neg\psi.$$
(ψ *is necessarily true iff not* ψ *is not possible*)

- Conjunctive laws:
$$\Box(\psi \wedge \phi) \simeq \Box\psi \wedge \Box\phi \quad \Diamond(\psi \wedge \phi) \Vdash \Diamond\psi \wedge \Diamond\phi.$$

- Disjunctive laws:
$$\Box(\psi \vee \phi) \simeq \Box\psi \vee \Box\phi \quad \Diamond(\psi \vee \phi) \simeq \Diamond\psi \vee \Diamond\phi.$$

- Implication laws:
$$\Box(\psi \to \phi) \Vdash \Box\psi \to \Box\phi \quad \Diamond(\psi \to \phi) \Vdash \Box\psi \to \Diamond\phi.$$

4.3 Proof Systems

4.3.1 Hilbert-Style Proof System

Definition 4.3.1. (**Hilbert-Style** $\mathscr{H}_0^\Box$) $\mathscr{H}_0^\Box$, the Hilbert-style proof system for modal propositional logic, is defined on the language $\mathcal{L}_0^\Box(\{\neg, \to, \Box\})$ (henceforth denoted $\mathcal{L}_0^\Box$) with the following axioms and inference rules:

$$(\mathrm{S})\ \frac{}{(\psi \to (\phi \to \chi)) \to ((\psi \to \phi) \to (\psi \to \chi))} \qquad (\mathrm{K})\ \frac{}{\psi \to (\phi \to \psi)}$$

$$(\mathrm{N})\ \frac{}{(\neg\phi \to \neg\psi) \to ((\neg\phi \to \psi) \to \phi)}$$

$$(\Box\ \mathrm{K})\ \frac{}{\Box(\psi \to \phi) \to (\Box\psi \to \Box\phi)} \qquad (\Box\ \mathrm{N})\ \frac{\psi}{\Box\psi}$$

$$(\mathrm{MP})\ \frac{\psi \qquad \psi \to \phi}{\phi}$$

- ($\Box$ K) is the distributive law (often called K) and ($\Box$ N) is the necessitation law.

- $\diamond$ is a *derived operator* w/ $\diamond\psi \triangleq \neg\Box\neg\psi$.
- $\mathscr{H}_0^{\Box}$ is a *pure*, or *normal*, modal logic (sometimes referred to as K).
- Pure logics are extended w/ axioms dependent, called *class axioms*, on characteristics of R:

  ($S1$) R is serial: $\forall w \in \mathscr{W}.\exists w' \in \mathscr{W}.R(w, w')$. Axiom (D): $\Box\psi \to \diamond\psi$.

  ($S3$) R is reflexive. Axiom (T): $\Box\psi \to \psi$.

  ($S4$) R is transitive. Axiom (4): $\Box\psi \to \Box\Box\psi$.

  ($S5$) R is symmetric. Axiom (B): $\psi \to \Box \diamond \psi$.

- **Notation**: $\mathscr{A}(R)$ is the set of class axioms defined by frame $(\mathscr{W}, R)$. $\mathscr{H}_0^{\Box}(R)$ denotes $\mathscr{H}_0^{\Box}$ w/ class axioms $\mathscr{A}(R)$.

Theorem 4.3.1. (**Soundness and Completeness of $\mathscr{H}_0^{\Box}(R)$**) $\mathscr{H}_0^{\Box}(R)$ is sound and complete in $(\mathscr{W}, R)$, that is

$$\forall \Gamma \in \mathcal{P}(\mathcal{L}_0^{\Box}), \psi \in \mathcal{L}_0^{\Box}.\Gamma \vdash_{\mathscr{H}_0^{\Box}} \psi \iff \Gamma \Vdash_{(\mathscr{W},R)} \psi,$$

4.3.2 Sequent Calculus for $S4$

- $S4 \implies$ Temporal logic. *Intuitively*, worlds are *futures*, each future has multiple futures. Paths are *timelines*.
- $S4$ equivalences:

$$\Box\Box\psi \simeq \Box\psi \qquad \diamond\diamond\psi \simeq \diamond\psi$$
$$\Box\diamond\Box\diamond\psi \simeq \Box\diamond\psi \qquad \diamond\Box\diamond\Box\psi \simeq \diamond\Box\psi$$

- $S4$ operator strings:
  - $\Box\psi$: ψ is true from now on. In all futures, ψ is true. ψ is true forever.
  - $\diamond\psi$: ψ is true at some point in the future. In some future, ψ is true.
  - $\Box\diamond\psi$: ψ will be true infinitely often.
  - $\Box\Box\psi$: ψ is true from now on.

- $\Box \diamond \Box\psi$: In all futures, at some point, ψ will be true forever.
- $\diamond\Box \diamond \psi$: At some point, ψ will be true infinitely often.

Definition 4.3.2. (Sequent Calculus $\mathscr{S}_0^\Box$ Proof System) $\mathscr{S}_0^\Box$, the Sequent calculus proof system for modal propositional logic, is defined on the generalized sequent form language of $\mathcal{L}_0^\Box(\Omega_0^\Box)$ with the following axioms and inference rules:

Operator	**Left**	**Right**
Axiom	(A) $\dfrac{}{\Gamma, \psi \vdash \Delta, \psi}$	
$\neg$	$(\neg l)\ \dfrac{\Gamma \vdash \Delta, \psi}{\Gamma, \neg\psi \vdash \Delta}$	$(\neg r)\ \dfrac{\Gamma, \neg\psi \vdash \bot}{\Gamma \vdash \Delta, \neg\psi}$
$\wedge$	$(\wedge l)\ \dfrac{\Gamma, \psi, \phi \vdash \Delta}{\Gamma, \psi \wedge \phi \vdash \Delta}$	$(\wedge r)\ \dfrac{\Gamma \vdash \Delta, \psi \qquad \Gamma \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi \wedge \phi}$
$\vee$	$(\vee l)\ \dfrac{\Gamma, \psi \vdash \Delta \qquad \Gamma, \phi \vdash \Delta}{\Gamma, \psi \wedge \phi \vdash \Delta}$	$(\vee r)\ \dfrac{\Gamma \vdash \Delta, \psi, \phi}{\Gamma \vdash \Delta, \psi \vee \phi}$
$\rightarrow$	$(\rightarrow l)\ \dfrac{\Gamma \vdash \Delta, \psi \qquad \Gamma, \phi \vdash \Delta}{\Gamma, \psi \rightarrow \phi \vdash \Delta}$	$(\rightarrow r)\ \dfrac{\Gamma, \psi \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi \rightarrow \phi}$
$\longleftrightarrow$	$(\longleftrightarrow l)\ \dfrac{\Gamma \vdash \Delta, \psi, \phi \qquad \Gamma, \psi, \phi \vdash \Delta}{\Gamma, \psi \longleftrightarrow \phi \vdash \Delta}$	$(\longleftrightarrow r)\ \dfrac{\Gamma, \psi \vdash \Delta, \phi \qquad \Gamma, \phi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \psi \longleftrightarrow \phi}$
$\Box$	$(\Box l)\ \dfrac{\Gamma, \psi \vdash \Delta}{\Gamma, \Box\psi \vdash \Delta}$	$(\Box r)\ \dfrac{\Gamma^* \vdash \Delta^*, \psi}{\Gamma \vdash \Delta, \Box\psi}$
$\diamond$	$(\diamond l)\ \dfrac{\Gamma^*, \psi \vdash \Delta^*}{\Gamma, \diamond\psi \vdash \Delta}$	$(\diamond r)\ \dfrac{\Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \diamond\psi}$

where $\Gamma^* = \{\Box\psi : \Box\psi \in \Gamma\}$, $\Delta^* = \{\diamond\psi : \diamond\psi \in \Delta\}$.

- Γ^*, Δ^* needed for world independence.