3.3 Models, Validity, and Satisfiability

$\phi$ is valid in $\mathcal{A}$ under assignment $\beta$: 

$\mathcal{A}, \beta \models \phi \iff \mathcal{A}(\beta)(\phi) = 1$

$\phi$ is valid in $\mathcal{A}$ ($\mathcal{A}$ is a model of $\phi$):

$\mathcal{A} \models \phi \iff \mathcal{A}, \beta \models \phi$, for all $\beta \in X \rightarrow U_\mathcal{A}$

$\phi$ is valid (or is a tautology):

$\models \phi \iff \mathcal{A} \models \phi$, for all $\mathcal{A} \in \Sigma$-$\text{Alg}$

$\phi$ is called satisfiable iff there exist $\mathcal{A}$ and $\beta$ such that $\mathcal{A}, \beta \models \phi$. Otherwise $\phi$ is called unsatisfiable.
Substitution Lemma

The following propositions, to be proved by structural induction, hold for all $\Sigma$-algebras $\mathcal{A}$, assignments $\beta$, and substitutions $\sigma$.

Lemma 3.3:
For any $\Sigma$-term $t$

$$\mathcal{A}(\beta)(t\sigma) = \mathcal{A}(\beta \circ \sigma)(t),$$

where $\beta \circ \sigma : X \rightarrow \mathcal{A}$ is the assignment $\beta \circ \sigma(x) = \mathcal{A}(\beta)(x\sigma)$.

Proposition 3.4:
For any $\Sigma$-formula $\phi$, $\mathcal{A}(\beta)(\phi\sigma) = \mathcal{A}(\beta \circ \sigma)(\phi)$. 
Corollary 3.5:
\[ \mathcal{A}, \beta \models \phi \sigma \iff \mathcal{A}, \beta \circ \sigma \models \phi \]

These theorems basically express that the syntactic concept of substitution corresponds to the semantic concept of an assignment.
Entailment and Equivalence

φ entails (implies) ψ (or ψ is a consequence of φ), written $\phi \models \psi$, if for all $A \in \Sigma$-Alg and $\beta \in X \to U_A$, whenever $A, \beta \models \phi$, then $A, \beta \models \psi$.

φ and ψ are called equivalent, written $\phi \equiv \psi$, if for all $A \in \Sigma$-Alg and $\beta \in X \to U_A$ we have $A, \beta \models \phi \iff A, \beta \models \psi$. 
Entailment and Equivalence

Proposition 3.6:
\( \phi \) entails \( \psi \) iff \( (\phi \rightarrow \psi) \) is valid

Proposition 3.7:
\( \phi \) and \( \psi \) are equivalent iff \( (\phi \leftrightarrow \psi) \) is valid.

Extension to sets of formulas \( N \) in the “natural way”, e.g.,
\( N \models \phi \)

\[ \iff \quad \text{for all } A \in \Sigma\text{-Alg and } \beta \in X \rightarrow U_A: \text{ if } A, \beta \models \psi, \text{ for all } \psi \in N, \text{ then } A, \beta \models \phi. \]
Validity vs. Unsatisfiability

Validity and unsatisfiability are just two sides of the same medal as explained by the following proposition.

Proposition 3.8:
Let $\phi$ and $\psi$ be formulas, let $N$ be a set of formulas. Then

(i) $\phi$ is valid if and only if $\neg \phi$ is unsatisfiable.

(ii) $\phi \models \psi$ if and only if $\phi \land \neg \psi$ is unsatisfiable.

(iii) $N \models \psi$ if and only if $N \cup \{\neg \psi\}$ is unsatisfiable.

Hence in order to design a theorem prover (validity checker) it is sufficient to design a checker for unsatisfiability.
Theory of a Structure

Let $\mathcal{A} \in \Sigma$-Alg. The (first-order) theory of $\mathcal{A}$ is defined as

$$Th(\mathcal{A}) = \{ \psi \in F_\Sigma(X) | \mathcal{A} \models \psi \}$$

Problem of axiomatizability:

For which structures $\mathcal{A}$ can one axiomatize $Th(\mathcal{A})$, that is, can one write down a formula $\phi$ (or a recursively enumerable set $\phi$ of formulas) such that

$$Th(\mathcal{A}) = \{ \psi | \phi \models \psi \}?$$

Analogously for sets of structures.
Two Interesting Theories

Let $\Sigma_{Pres} = (\{0/0, s/1, +/2\}, \emptyset)$ and $\mathbb{Z}_+ = (\mathbb{Z}, 0, s, +)$ its standard interpretation on the integers. $Th(\mathbb{Z}_+)$ is called \textbf{Presburger arithmetic} (M. Presburger, 1929). (There is no essential difference when one, instead of $\mathbb{Z}$, considers the natural numbers $\mathbb{N}$ as standard interpretation.)

Presburger arithmetic is decidable in $3\text{EXPTIME}$ (D. Oppen, JCSS, 16(3):323–332, 1978), and in $2\text{EXPSPACE}$, using automata-theoretic methods (and there is a constant $c \geq 0$ such that $Th(\mathbb{Z}_+) \not\in \text{NTIME}(2^{2^{cn}})$).
Two Interesting Theories

However, \( \mathbb{N}_* = (\mathbb{N}, 0, s, +, \cdot) \), the standard interpretation of \( \Sigma_{PA} = (\{0/0, s/1, +/2, \cdot/2\}, \emptyset) \), has as theory the so-called Peano arithmetic which is undecidable, not even recursively enumerable.

Note: The choice of signature can make a big difference with regard to the computational complexity of theories.
3.4 Algorithmic Problems

Validity($\phi$): $\models \phi$?

Satisfiability($\phi$): $\phi$ satisfiable?

Entailment($\phi, \psi$): does $\phi$ entail $\psi$?

Model($A, \phi$): $A \models \phi$?

Solve($A, \phi$): find an assignment $\beta$ such that $A, \beta \models \phi$.

Solve($\phi$): find a substitution $\sigma$ such that $\models \phi\sigma$.

Abduce($\phi$): find $\psi$ with “certain properties” such that $\psi \models \phi$. 
Gödel’s Famous Theorems

1. For most signatures $\Sigma$, validity is undecidable for $\Sigma$-formulas. (Later by Turing: Encode Turing machines as $\Sigma$-formulas.)

2. For each signature $\Sigma$, the set of valid $\Sigma$-formulas is recursively enumerable. (We will prove this by giving complete deduction systems.)

3. For $\Sigma = \Sigma_{PA}$ and $\mathbb{N}_* = (\mathbb{N}, 0, s, +, \cdot)$, the theory $Th(\mathbb{N}_*)$ is not recursively enumerable.

These complexity results motivate the study of subclasses of formulas (fragments) of first-order logic

Q: Can you think of any fragments of first-order logic for which validity is decidable?
Some Decidable Fragments

Some decidable fragments:

- **Monadic class**: no function symbols, all predicates unary; validity is NEXPTIME-complete.

- Variable-free formulas without equality: satisfiability is NP-complete. (why?)

- Variable-free Horn clauses (clauses with at most one positive atom): entailment is decidable in linear time.

- Finite model checking is decidable in time polynomial in the size of the structure and the formula.
Plan

Lift superposition from propositional logic to first-order logic.
3.5 Normal Forms and Skolemization

Study of normal forms motivated by

- reduction of logical concepts,
- efficient data structures for theorem proving,
- satisfiability preserving transformations (renaming),
- Skolem’s and Herbrand’s theorem.

The main problem in first-order logic is the treatment of quantifiers. The subsequent normal form transformations are intended to eliminate many of them.
Prenex Normal Form (Traditional)

Prenex formulas have the form

\[ Q_1 x_1 \ldots Q_n x_n \phi, \]

where \( \phi \) is quantifier-free and \( Q_i \in \{\forall, \exists\} \); we call \( Q_1 x_1 \ldots Q_n x_n \phi \) the quantifier prefix and \( \phi \) the matrix of the formula.
Prenex Normal Form (Traditional)

Computing prenex normal form by the rewrite system $\Rightarrow_P$: 

\[
(\phi \leftrightarrow \psi) \quad \Rightarrow_P \quad (\phi \rightarrow \psi) \land (\psi \rightarrow \phi)
\]

\[
\neg Qx\phi \quad \Rightarrow_P \quad \overline{Q}x\neg\phi
\]

\[
(((Qx\phi) \ \rho \ \psi) \quad \Rightarrow_P \quad Qy(\phi\{x \mapsto y\} \ \rho \ \psi), \ \rho \in \{\land, \lor\}
\]

\[
(((Qx\phi) \ \rightarrow \ \psi) \quad \Rightarrow_P \quad \overline{Q}y(\phi\{x \mapsto y\} \ \rightarrow \ \psi),
\]

\[
(\phi \ \rho \ (Qx\psi)) \quad \Rightarrow_P \quad Qy(\phi \ \rho \ \psi\{x \mapsto y\}), \ \rho \in \{\land, \lor, \rightarrow\}
\]

Here $y$ is always assumed to be some fresh variable and $\overline{Q}$ denotes the quantifier dual to $Q$, i.e., $\overline{\forall} = \exists$ and $\overline{\exists} = \forall$. 
Skolemization

**Intuition:** replacement of $\exists y$ by a concrete choice function computing $y$ from all the arguments $y$ depends on.

Transformation $\Rightarrow_S$ (to be applied outermost, not in subformulas):

$$\forall x_1, \ldots, x_n \exists y \phi \Rightarrow_S \forall x_1, \ldots, x_n \phi\{y \mapsto f(x_1, \ldots, x_n)\}$$

where $f / n$ is a new function symbol (Skolem function).
Theorem 3.9:
Let $\phi$, $\psi$, and $\chi$ as defined above and closed. Then

(i) $\phi$ and $\psi$ are equivalent.

(ii) $\chi \models \psi$ but the converse is not true in general.

(iii) $\psi$ satisfiable ($\Sigma$-Alg) $\iff$ $\chi$ satisfiable ($\Sigma^\prime$-Alg) where $\Sigma^\prime = (\Omega \cup SKF, \Pi)$, if $\Sigma = (\Omega, \Pi)$. 

Skolemization

Together: $\phi \Rightarrow^*_P \psi \Rightarrow^*_S \chi$

prenex

prenex, no $\exists$
The Complete Picture

\[ \phi \Rightarrow^*_{P} Q_1 y_1 \cdots Q_n y_n \psi \quad (\psi \text{ quantifier-free}) \]

\[ \Rightarrow^*_{S} \forall x_1, \ldots, x_m \chi \quad (m \leq n, \chi \text{ quantifier-free}) \]

\[ \Rightarrow^*_{OCNF} \forall x_1, \ldots, x_m \left( \bigwedge_{i=1}^{k} \bigvee_{j=1}^{n_i} L_{ij} \right) \]

\[ \phi' \]

\[ N = \{ C_1, \ldots, C_k \} \] is called the clausal (normal) form (CNF) of \( \phi \).

Note: the variables in the clauses are implicitly universally quantified.
The Complete Picture

Theorem 3.10:
Let $\phi$ be closed. Then $\phi' \models \phi$. (The converse is not true in general.)

Theorem 3.11:
Let $\phi$ be closed. Then $\phi$ is satisfiable iff $\phi'$ is satisfiable iff $\neg \phi$ is satisfiable
Optimization

The normal form algorithm described so far leaves lots of room for optimization. Note that we only can preserve satisfiability anyway due to Skolemization.

- size of the CNF is exponential when done naively; the transformations we introduced already for propositional logic avoid this exponential growth;
- we want to preserve the original formula structure;
- we want small arity of Skolem functions (see next section).
3.6 Getting Small Skolem Functions

A clause set that is better suited for automated theorem proving can be obtained using the following steps:

- produce a negation normal form (NNF)
- apply miniscoping
- rename all variables
- skolemize
Negation Normal Form (NNF)

Apply the rewrite system $\Rightarrow_{\text{NNF}}$:

$$\phi[\psi_1 \leftrightarrow \psi_2]_p \Rightarrow_{\text{NNF}} \phi[(\psi_1 \rightarrow \psi_2) \land (\psi_2 \rightarrow \psi_1)]_p$$

if $\text{pol}(\phi, p) = 1$ or $\text{pol}(\phi, p) = 0$

$$\phi[\psi_1 \leftrightarrow \psi_2]_p \Rightarrow_{\text{NNF}} \phi[(\psi_1 \land \psi_2) \lor (\neg \psi_2 \land \neg \psi_1)]_p$$

if $\text{pol}(\phi, p) = -1$
Negation Normal Form (NNF)

\[ \neg Qx \phi \implies_{\text{NNF}} \overline{Qx} \neg \phi \]
\[ \neg (\phi \lor \psi) \implies_{\text{NNF}} \neg \phi \land \neg \psi \]
\[ \neg (\phi \land \psi) \implies_{\text{NNF}} \neg \phi \lor \neg \psi \]
\[ \phi \rightarrow \psi \implies_{\text{NNF}} \neg \phi \lor \psi \]
\[ \neg \neg \phi \implies_{\text{NNF}} \phi \]
Apply the rewrite relation $\Rightarrow_{\text{MS}}$. For the rules below we assume that $x$ occurs freely in $\psi$, $\chi$, but $x$ does not occur freely in $\phi$: 

- $Qx (\psi \land \phi) \Rightarrow_{\text{MS}} (Qx \psi) \land \phi$
- $Qx (\psi \lor \phi) \Rightarrow_{\text{MS}} (Qx \psi) \lor \phi$
- $\forall x (\psi \land \chi) \Rightarrow_{\text{MS}} (\forall x \psi) \land (\forall x \chi)$
- $\exists x (\psi \lor \chi) \Rightarrow_{\text{MS}} (\exists x \psi) \lor (\exists x \chi)$
Variable Renaming

Rename all variables in $\phi$ such that there are no two different positions $p, q$ with $\phi|_p = Q\times \psi$ and $\phi|_q = Q'\times \chi$. 
Standard Skolemization

Apply the rewrite rule:

\[ \phi[\exists x \psi]_p \Rightarrow_{SK} \phi[\psi\{x \mapsto f(y_1, \ldots, y_n)\}]_p \]

where \( p \) has minimal length,
\( \{y_1, \ldots, y_n\} \) are the free variables in \( \exists x \psi \),
\( f/n \) is a new function symbol to \( \phi \)