First-Order Theorem Proving

Peter Baumgartner
NICTA, Logic and Computation Program, Canberra

Slides partially based on material by Uli Furbach, Harald Ganzinger, John Slaney, Viorica Sofronie-Stockermans and Uwe Waldmann
Contents

- Part I: What FOTP is about
- Part II: First-Order Predicate Logic (from the viewpoint of ATP)
- Part III: Proof Systems, including Resolution
- Part IV: Tableaux and Model Generation
Part I – What First-Order Theorem Proving is About

- Mission statement
- A glimpse at First-Order Theorem Proving
Mission Statement

Theorem proving is about …

**Logics:** Propositional, First-Order, Higher-Order, Modal, Description, …

**Calculi and proof procedures:** Resolution, DPLL, Tableaux, …

**Systems:** Interactive, Automated

**Applications:** Knowledge Representation, Verification, …
Mission Statement

Theorem proving is about …

**Logics:** Propositional, First-Order, Higher-Order, Modal, Description, …

**Calculi and proof procedures:** Resolution, DPLL, Tableaux, …

**Systems:** Interactive, Automated

**Applications:** Knowledge Representation, Verification, …

Milestones

**60s:** Calculi: DPLL, Resolution, Model Elimination

**70s:** Logic Programming

**80s:** Logic Based Knowledge Representation

**90s:** Modern Theory and Implementations, “A Basis for Applications”

**2000s:** Ontological Engineering, Verification
Mission Statement

In this talk, theorem proving is about …

Logics: Propositional, First-Order, Higher-Order, Modal, Description, …

Calculi and proof procedures: Resolution, DPLL, Tableaux, …

Systems: Interactive, Automated

Applications: Knowledge Representation, Verification, …

Milestones

60s: Calculi: DPLL, Resolution, Model Elimination

70s: Logic Programming

80s: Logic Based Knowledge Representation

90s: Modern Theory and Implementations, “A Basis for Applications”

2000s: Ontological Engineering, Verification
Application: Compiler Validation

Problem: prove equivalence of source and target program

Example:

1: y := 1
2: if z = x*x*x
3: then y := x*x + y
4: endif
5: y := R1+1

To prove: (indexes refer to values at line numbers; index 0 = initial values)

\[ y_1 \approx 1 \land z_0 \approx x_0 \times x_0 \times x_0 \land y_3 \approx x_0 \times x_0 + y_1 \]
\[ y'_1 \approx 1 \land R1_2 \approx x'_0 \times x'_0 \land R2_3 \approx R1_2 \times x'_0 \land z'_0 \approx R2_3 \land y'_5 \approx R1_2 + 1 \]
\[ \land x_0 \approx x'_0 \land y_0 \approx y'_0 \land z_0 \approx z'_0 \quad \models \quad y_3 \approx y'_5 \]
A logical puzzle:

Someone who lives in Dreadbury Mansion killed Aunt Agatha. Agatha, the butler, and Charles live in Dreadbury Mansion, and are the only people who live therein. A killer always hates his victim, and is never richer than his victim. Charles hates no one that Aunt Agatha hates. Agatha hates everyone except the butler. The butler hates everyone not richer than Aunt Agatha. The butler hates everyone Aunt Agatha hates. No one hates everyone. Agatha is not the butler.
A Glimpse at FOTP

A logical puzzle:

Someone who lives in Dreadbury Mansion killed Aunt Agatha. Agatha, the butler, and Charles live in Dreadbury Mansion, and are the only people who live therein. A killer always hates his victim, and is never richer than his victim. Charles hates no one that Aunt Agatha hates. Agatha hates everyone except the butler. The butler hates everyone not richer than Aunt Agatha. The butler hates everyone Aunt Agatha hates. No one hates everyone. Agatha is not the butler.

Who killed Aunt Agatha?
A Glimpse at FOTP

Before solving the problem with a theorem prover we have to formalize it:
A Glimpse at FOTP

Before solving the problem with a theorem prover we have to formalize it:

Someone who lives in Dreadbury Mansion killed Aunt Agatha.
Before solving the problem with a theorem prover we have to formalize it:

Someone who lives in Dreadbury Mansion killed Aunt Agatha.

\[ \exists x \, (\text{lives} \, x \, \text{at} \, \text{Dreadbury} \land \text{killed}(x, a)) \]
Before solving the problem with a theorem prover we have to formalize it:

Someone who lives in Dreadbury Mansion killed Aunt Agatha.

\[ \exists x \ (\text{lives\_at\_dreadbury}(x) \land \text{killed}(x, a)) \]

Agatha, the butler, and Charles live in Dreadbury Mansion, and are the only people who live therein.
Before solving the problem with a theorem prover we have to formalize it:

Someone who lives in Dreadbury Mansion killed Aunt Agatha.

\[ \exists x \ (\text{lives\_at\_dreadbury}(x) \land \text{killed}(x, a)) \]

Agatha, the butler, and Charles live in Dreadbury Mansion, and are the only people who live therein.

\[ \forall x \ (\text{lives\_at\_dreadbury}(x) \iff (x = a \lor x = b \lor x = c)) \]
A Glimpse at FOTP

A killer always hates his victim, and is never richer than his victim.

\[\forall x, y \ (\text{killed}(x, y) \rightarrow \text{hates}(x, y))\]
\[\forall x, y \ (\text{killed}(x, y) \rightarrow \neg \text{richer}(x, y))\]

Charles hates no one that Aunt Agatha hates.

\[\forall x \ (\text{hates}(c, x) \rightarrow \neg \text{hates}(a, x))\]

Agatha hates everyone except the butler.

\[\forall x \ (\neg \text{hates}(a, x) \leftrightarrow x = b)\]
The butler hates everyone not richer than Aunt Agatha.
\[ \forall x \ (\neg \text{richer}(x, a) \rightarrow \text{hates}(b, x)) \]

The butler hates everyone Aunt Agatha hates.
\[ \forall x \ (\text{hates}(a, x) \rightarrow \text{hates}(b, x)) \]

No one hates everyone.
\[ \forall x \ \exists y \ (\neg \text{hates}(x, y)) \]

Agatha is not the butler.
\[ \neg a = b \]
A Glimpse at FOTP

Now we can derive new formulas from the given ones. For instance:
A Glimpse at FOTP

Now we can derive new formulas from the given ones. For instance:

\[
\begin{align*}
\text{killed}(x, y) & \rightarrow \text{hates}(x, y) \quad \text{hates}(c, y) & \rightarrow & \neg \text{hates}(a, y) \\
\text{killed}(c, y) & \rightarrow \neg \text{hates}(a, y)
\end{align*}
\]
A Glimpse at FOTP

Now we can derive new formulas from the given ones. For instance:

\[
\begin{align*}
\text{killed}(x, y) & \rightarrow \text{hates}(x, y) & \text{hates}(c, y) & \rightarrow \neg \text{hates}(a, y) \\
\text{killed}(c, y) & \rightarrow \neg \text{hates}(a, y)
\end{align*}
\]

\[
\begin{align*}
\text{killed}(c, y) & \rightarrow \neg \text{hates}(a, y) & \neg \text{hates}(a, y) & \rightarrow y = b \\
\text{killed}(c, y) & \rightarrow y = b
\end{align*}
\]
A Glimpse at FOTP

Now we can derive new formulas from the given ones. For instance:

\[
\begin{align*}
\text{killed}(x, y) & \rightarrow \text{hates}(x, y) & \text{hates}(c, y) & \rightarrow \neg \text{hates}(a, y) \\
\text{killed}(c, y) & \rightarrow \neg \text{hates}(a, y)
\end{align*}
\]

\[
\begin{align*}
\text{killed}(c, y) & \rightarrow \neg \text{hates}(a, y) & \neg \text{hates}(a, y) & \rightarrow y = b \\
\text{killed}(c, y) & \rightarrow y = b
\end{align*}
\]

\[
\begin{align*}
\text{killed}(c, y) & \rightarrow y = b & \neg a = b \\
\neg \text{killed}(c, a)
\end{align*}
\]
By the previous reasoning we know that Charles is not the murderer. But the further reasoning is quite tedious.

Fortunately we can use a theorem prover!
A Glimpse at FOTP

By the previous reasoning we know that Charles is not the murderer. But the further reasoning is quite tedious.

Fortunately we can use a theorem prover!

Demo

- Theorem prover: Otter
  http://www-unix.mcs.anl.gov/AR/otter/

- Aunt Agatha puzzle: PUZ001-2 in the TPTP
  TPTP = Thousands of Problems for Theorem Provers
  http://www.cs.miami.edu/~tptp/
The Principle

**Problem**

Description of the situation in Dreadbury Mansion

Who killed Agatha?

**Solution**

Charles killed Agatha

The butler killed Agatha

*Agatha committed suicide*

Murderer unknown
The Principle

e.g. natural language

Problem

Formulas

Solution

precise description
The Principle

1. Formalization: from problems to formulas
   Can sometimes be done automatically
2. Solve the formalized problem
   In practice usually **very** many new formulas will be generated
   Computer support is necessary
   (even then the sheer number of formulas is the main problem)
The Principle

3. Translate back solution
   Can sometimes be done automatically
   Not always trivial!
Non-Theorems

So far, the problems had the following shape:

Does a formula (e.g.: killed(a, a)) follow from other formulas?
Non-Theorems

So far, the problems had the following shape:

Does a formula (e.g.: killed(a, a)) follow from other formulas?

Problems of the following, complementary kind are interesting, too:

Does a formula (e.g.: killed(b, a)) not follow from other formulas?
Non-Theorems

So far, the problems had the following shape:

Does a formula (e.g.: \textit{killed}(a, a)) follow from other formulas?

Problems of the following, complementary kind are interesting, too:

Does a formula (e.g.: \textit{killed}(b, a)) \textbf{not} follow from other formulas?

\textbf{Non-entailment is much harder a problem!}
Part II – First-Order Predicate Logic (from the viewpoint of ATP)

- A mathematical example
- Syntax and semantics of first-order predicate logic
- Normal forms
A Mathematical Example

The sum of two continuous function is continuous.

**Definition** $f : \mathbb{R} \rightarrow \mathbb{R}$ is **continuous** at $a$, if for every $\varepsilon > 0$ there is a $\delta > 0$, such that for all $x$ with $|x - a| < \delta$ it holds $|f(x) - f(a)| < \varepsilon$.

**Proposition** If $f$ and $g$ are continuous, so is their sum.

**Proof** Let $h = f + g$ assume $\varepsilon > 0$ given. With $f$ and $g$ continuous, there are $\delta_f$ and $\delta_g$ greater than 0 such that, if $|x - a| < \delta_f$, then $|f(x) - f(a)| < \varepsilon/2$ and, if $|x - a| < \delta_g$, then $|g(x) - g(a)| < \varepsilon/2$. Chose $\delta = \min(\delta_f, \delta_g)$. If $|x - a| < \delta$ then we approximate:

$$ |h(x) - h(a)| = |f(x) + g(x) - f(a) - g(a)| $$

$$ = |(f(x) - f(a)) + (g(x) - g(a))| $$

$$ \leq |f(x) - f(a)| + |g(x) - g(a)| < \varepsilon/2 + \varepsilon/2 = \varepsilon $$
"f ist continuous", expressed in first-order predicate logic:

\[ \forall \varepsilon (0 < \varepsilon \rightarrow \forall a \exists \delta (0 < \delta \land \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))) \]

in ASCII:

\[
\text{all(Eps, } \\
\text{0<Eps => } \\
\text{all(A, } \\
\text{exists(Delta, } \\
\text{0<Delta and } \\
\text{all(X, abs(X-A)<Delta => } \\
\text{abs(f(X)-f(A)) < Eps))))}
\]

Can pass this formula to a theorem prover?
What does it "mean" to the prover?
Predicate Logic Syntax

\[
\forall \varepsilon (0 < \varepsilon \rightarrow \forall a \exists \delta (0 < \delta \land \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)))
\]

**Variables** \( \varepsilon, a, \delta, x \)

**Function symbols** \( 0, |\_|, \_ - \_ , f(\_) \)

**Terms** are well-formed expressions over variables and function symbols

**Predicate symbols** \( \_ < \_ , \_ = \_ \)

**Atoms** are applications of predicate symbols to terms

**Boolean connectives** \( \land, \lor, \rightarrow, \neg \)

**Quantifiers** \( \forall, \exists \)

The function symbols and predicate symbols, each of given arity, comprise a signature \( \Sigma \).

A **ground term** is a term without any variables.
Predicate Logic Semantics

Universe (aka Domain): Set $U$

Variables $\mapsto$ values in $U$ (mapping is called “assignment”)

Function symbols $\mapsto$ (total) functions over $U$

Predicate symbols $\mapsto$ relations over $U$

Boolean connectives $\mapsto$ the usual boolean functions

Quantifiers $\mapsto$ “for all ... holds”, “there is a ..., such that”

Terms $\mapsto$ values in $U$

Formulas $\mapsto$ Boolean (Truth-) values

The underlying mathematical concept is that of a $\Sigma$-algebra.
Example

Let $\Sigma_{PA}$ be the standard signature of Peano Arithmetic. The standard interpretation for Peano Arithmetic then is:

\[
\begin{align*}
U_N &= \{0, 1, 2, \ldots\} \\
0_N &= 0 \\
s_N : n &\mapsto n + 1 \\
+_N : (n, m) &\mapsto n + m \\
\times_N : (n, m) &\mapsto n \times m \\
\leq_N &= \{(n, m) \mid n \text{ less than or equal to } m\} \\
<_{N} &= \{(n, m) \mid n \text{ less than } m\}
\end{align*}
\]

Note that $\mathbb{N}$ is just one out of many possible $\Sigma_{PA}$-interpretations.
Example

Values over $\mathbb{N}$ for sample terms and formulas:

Under the assignment $\beta : x \mapsto 1, y \mapsto 3$ we obtain

\[
\begin{align*}
\mathbb{N}(\beta)(s(x) + s(0)) &= 3 \\
\mathbb{N}(\beta)(x + y \approx s(y)) &= 1 \\
\mathbb{N}(\beta)(\forall x, y (x + y \approx y + x)) &= True \\
\mathbb{N}(\beta)(\forall z \ z \leq y) &= False \\
\mathbb{N}(\beta)(\forall x \exists y \ x < y) &= True
\end{align*}
\]

If $\phi$ is a closed formula, then, instead of $I(\phi) = True$ one writes $I \models \phi$ ("$I$ is a model of $\phi$").

E.g. $\mathbb{N} \models \forall x \exists y \ x < y$
Axiomatizing the Real Numbers

In our proof problem, we have to “axiomatize” all those properties of the standard functions and predicate symbols that are needed to get a proof. There are only some of them here.

Addition and Subtraction:

\[ x + y = y + x \]
\[ (x + y) + z = x + (y + z) \]
\[ x - y = x + (-y) \]
\[ -(x + y) = (-x) + (-y) \]
Axiomatizing the Real Numbers

Ordering:

\[ \neg x < x \]
\[ x < y \land y < z \rightarrow x < z \]
\[ x \leq x \]
\[ x \leq y \leftrightarrow x < y \lor x = y \]
\[ x \leq y \lor y < x \]

divide by 2 and absolute values:

\[ \frac{x}{2} \leq 0 \rightarrow x \leq 0 \]
\[ x < \frac{z}{2} \land y < \frac{z}{2} \rightarrow x + y < z \]
\[ |x + y| \leq |x| + |y| \]
Now one can prove:

\[ \text{Axioms over } \mathbb{R} \land \text{continuous}(f) \land \text{continuous}(g) \models \text{continuous}(f + g) \]
Now one can prove:

$$\text{Axioms over } \mathbb{R} \land \text{continuous}(f) \land \text{continuous}(g) \models \text{continuous}(f + g)$$

It can even be proven fully automatically!
Algorithmic Problems

The following is a list of practically relevant problems:

**Validity**($F$): $\models F$? (is $F$ true in every interpretation?)

**Satisfiability**($F$): $F$ satisfiable?

**Entailment**($F, G$): $F \models G$? (does $F$ entail $G$?),

**Model**($A, F$): $A \models F$?

**Solve**($A, F$): find an assignment $\beta$ such that $A, \beta \models F$

**Solve**($F$): find a substitution $\sigma$ such that $\models F\sigma$

**Abduce**($F$): find $G$ with “certain properties” such that $G$ entails $F$

Different problems may require rather different methods! But …

Suppose we want to prove $H \models G$. 
Refutational Theorem Proving

- Suppose we want to prove $H \models G$.
- Equivalently, we can prove that $F := H \rightarrow G$ is valid.
Suppose we want to prove $H \models G$.

Equivalently, we can prove that $F := H \rightarrow G$ is valid.

Equivalently, we can prove that $\neg F$, i.e. $H \land \neg G$ is unsatisfiable.
Refutational Theorem Proving

Suppose we want to prove $H \models G$.

Equivalently, we can prove that $F := H \rightarrow G$ is valid.

Equivalently, we can prove that $\neg F$, i.e. $H \land \neg G$ is unsatisfiable.

This principle of “refutational theorem proving” is the basis of almost all automated theorem proving methods.
Normal Forms

Study of normal forms motivated by

- reduction of logical concepts,
- efficient data structures for theorem proving.

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

Prenex formulas have the form

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

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

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

\[(F \leftrightarrow G) \Rightarrow_P (F \rightarrow G) \land (G \rightarrow F)\]

\[\neg QxF \Rightarrow_P \overline{Q}x\neg F\]

\[(QxF \rho G) \Rightarrow_P Qy(F[y/x] \rho G), \ y \text{ fresh}, \ \rho \in \{\land, \lor\}\]

\[(QxF \rightarrow G) \Rightarrow_P \overline{Q}y(F[y/x] \rightarrow G), \ y \text{ fresh}\]

\[(F \rho QxG) \Rightarrow_P Qy(F \rho G[y/x]), \ y \text{ fresh}, \ \rho \in \{\land, \lor, \rightarrow\}\]

Here $\overline{Q}$ denotes the quantifier dual to $Q$, i.e., $\overline{\forall} = \exists$ and $\overline{\exists} = \forall$. 
In the Example

\[ \forall \varepsilon (0 < \varepsilon \rightarrow \forall a \exists \delta (0 < \delta \land \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))) \]

\[ \Rightarrow P \]

\[ \forall \varepsilon \forall a (0 < \varepsilon \rightarrow \exists \delta (0 < \delta \land \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))) \]

\[ \Rightarrow P \]

\[ \forall \varepsilon \forall a \exists \delta (0 < \varepsilon \rightarrow 0 < \delta \land \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)) \]

\[ \Rightarrow P \]

\[ \forall \varepsilon \forall a \exists \delta (0 < \varepsilon \rightarrow \forall x (0 < \delta \land |x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)) \]

\[ \Rightarrow P \]

\[ \forall \varepsilon \forall a \exists \delta \forall x (0 < \varepsilon \rightarrow (0 < \delta \land (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))) \]
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):

\[
\forall x_1, \ldots, x_n \exists y F \Rightarrow_S \forall x_1, \ldots, x_n F[f(x_1, \ldots, x_n)/y]
\]

where \( f/n \) is a new function symbol (**Skolem function**).
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):

$$\forall x_1, \ldots, x_n \exists y F \Rightarrow_S \forall x_1, \ldots, x_n F[f(x_1, \ldots, x_n)/y]$$

where $f/n$ is a new function symbol (**Skolem function**).

**In the Example**

$$\forall \varepsilon \forall a \exists \delta \forall x (0 < \varepsilon \rightarrow 0 < \delta \land (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))$$

$\Rightarrow_S$

$$\forall \varepsilon \forall a \forall x (0 < \varepsilon \rightarrow 0 < d(\varepsilon, a) \land (|x - a| < d(\varepsilon, a) \rightarrow |f(x) - f(a)| < \varepsilon))$$
Skolemization

Together: $F \Rightarrow^*_{P} \begin{cases} G \Rightarrow^*_{S} \hline H \end{cases}$ prenex \quad prenex, \ no \ \exists$

Theorem: The given and the final formula are equi-satisfiable.
### Clausal Normal Form (Conjunctive Normal Form)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Deduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>((F \leftrightarrow G)) \implies_k (F \rightarrow G) \land (G \rightarrow F))</td>
<td></td>
</tr>
<tr>
<td>((F \rightarrow G)) \implies_k (\neg F \lor G)</td>
<td></td>
</tr>
<tr>
<td>((F \lor G)) \implies_k (\neg F \land \neg G)</td>
<td></td>
</tr>
<tr>
<td>((F \land G)) \implies_k (\neg F \lor \neg G)</td>
<td></td>
</tr>
<tr>
<td>((\neg \neg F)) \implies_k F</td>
<td></td>
</tr>
<tr>
<td>((F \land G) \lor H) \implies_k (F \lor H) \land (G \lor H)</td>
<td></td>
</tr>
<tr>
<td>((F \land \top)) \implies_k F</td>
<td></td>
</tr>
<tr>
<td>((F \land \bot)) \implies_k \bot</td>
<td></td>
</tr>
<tr>
<td>((F \lor \top)) \implies_k \top</td>
<td></td>
</tr>
<tr>
<td>((F \lor \bot)) \implies_k F</td>
<td></td>
</tr>
</tbody>
</table>

These rules are to be applied modulo associativity and commutativity of \(\land\) and \(\lor\). The first five rules, plus the rule \((\neg Q)\), compute the **negation normal form** (NNF) of a formula.
In the Example

\[ \forall \varepsilon \forall a \forall x (0 < \varepsilon \rightarrow 0 < d(\varepsilon, a) \land (|x - a| < d(\varepsilon, a) \rightarrow |f(x) - f(a)| < \varepsilon)) \]

\[ \Rightarrow \kappa \]

\[ 0 < d(\varepsilon, a) \lor \neg (0 < \varepsilon) \]

\[ \neg (|x - a| < d(\varepsilon, a)) \lor |f(x) - f(a)| < \varepsilon \lor \neg (0 < \varepsilon) \]

**Note:** The universal quantifiers for the variables \( \varepsilon, a \) and \( x \), as well as the conjunction symbol \( \land \) between the clauses are not written, for convenience.
The Complete Picture

\[ F \Rightarrow_P^* Q_1 y_1 \ldots Q_n y_n \ G \quad (G \text{ quantifier-free}) \]

\[ \Rightarrow_S^* \forall x_1, \ldots, x_m \ H \quad (m \leq n, \ H \text{ quantifier-free}) \]

\[ \Rightarrow_K^* \forall x_1, \ldots, x_m \left( \bigwedge_{i=1}^{k} \bigvee_{j=1}^{n_i} L_{ij} \right) \leavesout\ clauses \ C_i \]

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

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

\[ F \Rightarrow_P^* Q_1 y_1 \ldots Q_n y_n \quad G \quad \text{(G quantifier-free)} \]

\[ \Rightarrow_S^* \forall x_1, \ldots, x_m \ H \quad (m \leq n, \ H \text{ quantifier-free}) \]

\[ \Rightarrow_K^* \forall x_1, \ldots, x_m \ \left( \bigwedge_{i=1}^{k} \bigvee_{j=1}^{n_i} L_{ij} \right) \quad \text{leave out clauses } C_i \]

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

**Note:** the variables in the clauses are implicitly universally quantified.

Now we arrived at “low-level predicate logic” and the proof problem, proper, i.e. to prove that the clause set is unsatisfiable.
Propositional Clause Logic

A particular syntactically simple, yet practically most significant case. Propositional clause logic = clause logic without variables

**Propositional clause:** a disjunction of literals, e.g. $A \lor B \lor \neg C \lor \neg D$

**Propositional clause set:** a (finite) set of propositional clauses.
Propositional Clause Logic

A particular syntactically simple, yet practically most significant case. Propositional clause logic = clause logic without variables

**Propositional clause:** a disjunction of literals, e.g. \( A \lor B \lor \neg C \lor \neg D \)

**Propositional clause set:** a (finite) set of propositional clauses.

**Interpretation:** maps atoms to \( \{true, false\} \), e.g.

\[
\begin{array}{cccc}
A & B & C & D \\
true & false & true & false
\end{array}
\]

Represented as the set of its true atoms, e.g. \( \{A, C\} \)
Propositional Clause Logic

A particular syntactically simple, yet practically most significant case. Propositional clause logic = clause logic without variables

**Propositional clause:** a disjunction of literals, e.g. \( A \lor B \lor \neg C \lor \neg D \)

**Propositional clause set:** a (finite) set of propositional clauses.

**Interpretation:** maps atoms to \( \{true, false\} \), e.g.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>false</td>
<td>true</td>
<td>false</td>
</tr>
</tbody>
</table>

Represented as the set of its true atoms, e.g. \( \{A, C\} \)

We don’t specialize on methods for propositional logic here. See lecture by Toby Walsh.
Herbrand Theory

Some thoughts

Suppose we want to prove $H \models G$. 
Herbrand Theory

Some thoughts

- Suppose we want to prove $H \models G$.
- Equivalently, we can prove that $F := H \land \neg G$ is unsatisfiable.
Some thoughts

- Suppose we want to prove $H \models G$.
- Equivalently, we can prove that $F := H \land \neg G$ is unsatisfiable.
- We have seen how $F$ can be syntactically simplified to clause form $F'$ in a satisfiability preserving way.
Herbrand Theory

Some thoughts

- Suppose we want to prove $H \models G$.
- Equivalently, we can prove that $F := H \land \neg G$ is unsatisfiable.
- We have seen how $F$ can be syntactically simplified to clause form $F'$ in a satisfiability preserving way.
- It remains to prove that $F'$ is unsatisfiable.
Some thoughts

- Suppose we want to prove $H \models G$.
- Equivalently, we can prove that $F := H \land \neg G$ is unsatisfiable.
- We have seen how $F$ can be syntactically simplified to clause form $F'$ in a satisfiability preserving way.
- It remains to prove that $F'$ is unsatisfiable.
- Does this mean that “all interpretations have to be searched”? 
Suppose we want to prove $H \models G$.

Equivalently, we can prove that $F := H \land \neg G$ is unsatisfiable.

We have seen how $F$ can be syntactically simplified to clause form $F'$ in a satisfiability preserving way.

It remains to prove that $F'$ is unsatisfiable.

Does this mean that “all interpretations have to be searched”?

No! It suffices to “search only through Herbrand interpretations”
Herbrand Theory

**Significance:** semantical basis for most theorem proving systems

A **Herbrand interpretation** (over a given signature $\Sigma$) is a $\Sigma$-algebra $\mathcal{A}$ such that

1. $U_{\mathcal{A}} = T_{\Sigma}$ (= the set of ground terms over $\Sigma$)
2. $f_{\mathcal{A}} : (s_1, \ldots, s_n) \mapsto f(s_1, \ldots, s_n)$, $f/n \in \Omega$

\[
f_{\mathcal{A}}(\triangle, \ldots, \triangle) = \begin{array}{c}
\triangle \\
\cdots \\
\triangle
\end{array}
\]
Herbrand Interpretations

In other words, **values are fixed** to be ground terms and **functions are fixed** to be the **term constructors**. Only predicate symbols $p/m \in \Pi$ may be freely interpreted as relations $p_{\mathcal{A}} \subseteq T^m_{\Sigma}$.

**Proposition**

Every set of ground atoms $I$ uniquely determines a Herbrand interpretation $\mathcal{A}$ via

$$ (s_1, \ldots, s_n) \in p_{\mathcal{A}} \iff p(s_1, \ldots, s_n) \in I $$

Thus we shall identify Herbrand interpretations (over $\Sigma$) with sets of $\Sigma$-ground atoms.
Herbrand Interpretations

Example: $\Sigma_{Pres} = \{0/0, s/1, +/2\}, \{</2, \leq/2\}$

$\mathbb{N}$ as Herbrand interpretation over $\Sigma_{Pres}$:

$I = \{ 0 \leq 0, 0 \leq s(0), 0 \leq s(s(0)), \ldots, \\
0 + 0 \leq 0, 0 + 0 \leq s(0), \ldots, \\
\ldots, (s(0) + 0) + s(0) \leq s(0) + (s(0) + s(0)) \\
\ldots \\
s(0) + 0 < s(0) + 0 + 0 + s(0) \\
\ldots \}$
Existence of Herbrand Models

A Herbrand interpretation $I$ is called a **Herbrand model** of $F$ iff $I \models F$.

**Theorem**

Let $N$ be a set of $\Sigma$-clauses.

- $N$ is satisfiable $\iff$ $N$ has a Herbrand model (over $\Sigma$)
  $\iff$ $G_\Sigma(N)$ has a Herbrand model (over $\Sigma$)

where

$$G_\Sigma(N) = \{ C\sigma \text{ ground clause} | \ C \in N, \ \sigma : X \rightarrow T_\Sigma \}$$

is the set of **ground instances** of $N$. 
Example of a $\Sigma$

For $\Sigma_{Pres}$ one obtains for

$$C = (x < y) \lor (y \leq s(x))$$

the following ground instances:

$$(0 < 0) \lor (0 \leq s(0))$$
$$(s(0) < 0) \lor (0 \leq s(s(0)))$$

\[ \cdots \]

$$(s(0) + s(0) < s(0) + 0) \lor (s(0) + 0 \leq s(s(0) + s(0)))$$

\[ \cdots \]
Herbrand’s Theorem

Theorem (Skolem-Herbrand-Theorem)
∀φ is unsatisfiable iff some finite set of ground instances \( \{\phi\gamma_1, \ldots, \phi\gamma_n\} \) is unsatisfiable
Herbrand’s Theorem

Theorem (Skolem-Herbrand-Theorem)
∀φ is unsatisfiable iff some finite set of ground instances \( \{ \phi \gamma_1, \ldots, \phi \gamma_n \} \) is unsatisfiable

Applied to clause logic:

**Theorem**

Let \( N \) be a set of \( \Sigma \)-clauses.

\( N \) is unsatisfiable \( \iff \) \( G_\Sigma(N) \) has no Herbrand model (over \( \Sigma \))
\( \iff \) there is a **finite** subset of \( G_\Sigma(N) \)
that has no Herbrand model (over \( \Sigma \))
Herbrand’s Theorem

Theorem (Skolem-Herbrand-Theorem)
∀φ is unsatisfiable iff some finite set of ground instances \{φγ₁, \ldots, φγₙ\} is unsatisfiable

Applied to clause logic:

Theorem
Let \(N\) be a set of \(Σ\)-clauses.

\(N\) is unsatisfiable ⇔ \(G_Σ(N)\) has no Herbrand model (over \(Σ\))
⇔ there is a finite subset of \(G_Σ(N)\) that has no Herbrand model (over \(Σ\))

Significance: It’s the core argument to show that validity in first-order logic is semi-decidable.
Part III: Proof Systems

Two fundamental results limit what can be achieved:

**Theorem** (Gödel, 1929)
There are proof systems that enumerate all valid formulas of first-order predicate logic. (This is also a consequence of Herbrand’s Theorem)

**Theorem** (Church/Turing, about 1935)
The validity problem of first-order logic formulas is undecidable.
Part III: Proof Systems

Two fundamental results limit what can be achieved:

**Theorem** (Gödel, 1929)
There are proof systems that enumerate all valid formulas of first-order predicate logic. (This is also a consequence of Herbrand’s Theorem)

**Theorem** (Church/Turing, about 1935)
The validity problem of first-order logic formulas is undecidable.
(Thus, the model existence problem is undecidable, too.)
Part III: Proof Systems

Two fundamental results limit what can be achieved:

**Theorem** (Gödel, 1929)
There are proof systems that enumerate all valid formulas of first-order predicate logic. (This is also a consequence of Herbrand’s Theorem)

**Theorem** (Church/Turing, about 1935)
The validity problem of first-order logic formulas is undecidable.
(Thus, the model existence problem is undecidable, too.)

*Automated theorem proving is oriented at the first, positive result.*
Inference Systems and Proofs

**Inference systems** $\Gamma$ (proof calculi) are sets of tuples

$$ (F_1, \ldots, F_n, F_{n+1}), \ n \geq 0, $$

called **inferences** or **inference rules**, and written

$$ \begin{array}{c}
\text{premises} \\
\{F_1, \ldots, F_n\} \\
\hline \\
\text{conclusion} \\
F_{n+1}
\end{array} $$

**Clausal inference system**: premises and conclusions are clauses. One also considers inference systems over other data structures.
Proofs

A **proof** in \( \Gamma \) of a formula \( F \) from a set of formulas \( N \) (called **assumptions**) is a sequence \( F_1, \ldots, F_k \) of formulas where

1. \( F_k = F \),
2. for all \( 1 \leq i \leq k \): \( F_i \in N \), or else there exists an inference \((F_{i_1}, \ldots, F_{i_{n_i}}, F_i)\) in \( \Gamma \), such that \( 0 \leq i_j < i \), for \( 1 \leq j \leq n_i \).
Soundness and Completeness

Provability $\vdash_\Gamma$ of $F$ from $N$ in $\Gamma$:

$N \vdash_\Gamma F :\iff$ there exists a proof $\Gamma$ of $F$ from $N$.

$\Gamma$ is called sound $:\iff$

$$\frac{F_1 \ldots F_n}{F} \in \Gamma \Rightarrow F_1, \ldots, F_n \models F$$

$\Gamma$ is called complete $:\iff$

$$N \models F \Rightarrow N \vdash_\Gamma F$$

$\Gamma$ is called refutationally complete $:\iff$

$$N \models \bot \Rightarrow N \vdash_\Gamma \bot$$
Proposition

1. Let $\Gamma$ be sound. Then $N \vdash F \Rightarrow N \models F$

2. $N \vdash F \Rightarrow$ there exist $F_1, \ldots, F_n \in N$ s.t. $F_1, \ldots, F_n \vdash F$
   (resembles compactness).
Proofs as Trees

markings \(\cong\) formulas
leaves \(\cong\) assumptions and axioms
other nodes \(\cong\) inferences: conclusion \(\cong\) ancestor
premises \(\cong\) direct descendants

\[
\begin{align*}
  P(f(a)) \lor Q(b) & \quad \neg P(f(a)) \lor \neg P(f(a)) \lor Q(b) \\
  & \quad \neg P(f(a)) \lor Q(b) \lor Q(b) \\
  P(f(a)) \lor Q(b) & \quad \neg P(f(a)) \lor Q(b) \\
  & \quad Q(b) \lor Q(b) \\
  P(g(a, b)) & \quad Q(b) \\
  & \quad \neg P(f(a)) \lor \neg Q(b) \\
  & \quad \neg P(f(a)) \lor \neg Q(b) \\
  & \quad \neg P(g(a, b)) \\
  & \quad \bot
\end{align*}
\]
Proof Systems

The Aunta Agatha puzzle has shown that a proof system has to combine

- instantiation of variables with

- treatment of Boolean connectives.

In the subsequent slides we will concentrate on the second aspect and assume ground clauses, i.e. clauses where all variables have been instantiated by ground terms.

We observe that ground clauses and propositional clauses are the same concept.

Thus, for the time being we only deal with propositional clauses.

The subsequent **Resolution Calculus** $Res$ can be used to decide the satisfiability problem of propositional clause logic.
The Resolution Calculus $\text{Res}$

Resolution inference rule:

$$
\begin{array}{c}
C \lor A \\
\neg A \lor D \\
\hline \\
C \lor D
\end{array}
$$

Terminology: $C \lor D$: resolvent; $A$: resolved atom

(Positive) factorisation inference rule:

$$
\begin{array}{c}
C \lor A \lor A \\
\hline \\
C \lor A
\end{array}
$$

These are schematic inference rules; for each substitution of the schematic variables $C$, $D$, and $A$, respectively, by ground clauses and ground atoms we obtain an inference rule.

As “$\lor$” is considered associative and commutative, we assume that $A$ and $\neg A$ can occur anywhere in their respective clauses.
Sample Refutation

By the just made observation, this is a propositional clause set:

1. \( \neg P(f(a)) \lor \neg P(f(a)) \lor Q(b) \) (given)
2. \( P(f(a)) \lor Q(b) \) (given)
3. \( \neg P(g(b, a)) \lor \neg Q(b) \) (given)
4. \( P(g(b, a)) \) (given)
Sample Refutation

By the just made observation, this is a propositional clause set:

1. $\neg P(f(a)) \lor \neg P(f(a)) \lor Q(b)$  \hspace{1cm} (given)
2. $P(f(a)) \lor Q(b)$  \hspace{1cm} (given)
3. $\neg P(g(b, a)) \lor \neg Q(b)$  \hspace{1cm} (given)
4. $P(g(b, a))$  \hspace{1cm} (given)
5. $\neg P(f(a)) \lor Q(b) \lor Q(b)$  \hspace{1cm} (Res. 2. into 1.)
Sample Refutation

By the just made observation, this is a propositional clause set:

1. \( \neg P(f(a)) \lor \neg P(f(a)) \lor Q(b) \) (given)
2. \( P(f(a)) \lor Q(b) \) (given)
3. \( \neg P(g(b, a)) \lor \neg Q(b) \) (given)
4. \( P(g(b, a)) \) (given)
5. \( \neg P(f(a)) \lor Q(b) \lor Q(b) \) (Res. 2. into 1.)
6. \( \neg P(f(a)) \lor Q(b) \) (Fact. 5.)
Sample Refutation

By the just made observation, this is a propositional clause set:

1. \( \neg P(f(a)) \lor \neg P(f(a)) \lor Q(b) \) (given)
2. \( P(f(a)) \lor Q(b) \) (given)
3. \( \neg P(g(b, a)) \lor \neg Q(b) \) (given)
4. \( P(g(b, a)) \) (given)
5. \( \neg P(f(a)) \lor Q(b) \lor Q(b) \) (Res. 2. into 1.)
6. \( \neg P(f(a)) \lor Q(b) \) (Fact. 5.)
7. \( Q(b) \lor Q(b) \) (Res. 2. into 6.)
Sample Refutation

By the just made observation, this is a propositional clause set:

1. \( \neg P(f(a)) \lor \neg P(f(a)) \lor Q(b) \) (given)
2. \( P(f(a)) \lor Q(b) \) (given)
3. \( \neg P(g(b, a)) \lor \neg Q(b) \) (given)
4. \( P(g(b, a)) \) (given)
5. \( \neg P(f(a)) \lor Q(b) \lor Q(b) \) (Res. 2. into 1.)
6. \( \neg P(f(a)) \lor Q(b) \) (Fact. 5.)
7. \( Q(b) \lor Q(b) \) (Res. 2. into 6.)
8. \( Q(b) \) (Fact. 7.)
Sample Refutation

By the just made observation, this is a propositional clause set:

1. \[ \neg P(f(a)) \lor \neg P(f(a)) \lor Q(b) \] (given)
2. \[ P(f(a)) \lor Q(b) \] (given)
3. \[ \neg P(g(b, a)) \lor \neg Q(b) \] (given)
4. \[ P(g(b, a)) \] (given)
5. \[ \neg P(f(a)) \lor Q(b) \lor Q(b) \] (Res. 2. into 1.)
6. \[ \neg P(f(a)) \lor Q(b) \] (Fact. 5.)
7. \[ Q(b) \lor Q(b) \] (Res. 2. into 6.)
8. \[ Q(b) \] (Fact. 7.)
9. \[ \neg P(g(b, a)) \] (Res. 8. into 3.)
Sample Refutation

By the just made observation, this is a propositional clause set:

1. ¬P(f(a)) ∨ ¬P(f(a)) ∨ Q(b) (given)
2. P(f(a)) ∨ Q(b) (given)
3. ¬P(g(b, a)) ∨ ¬Q(b) (given)
4. P(g(b, a)) (given)
5. ¬P(f(a)) ∨ Q(b) ∨ Q(b) (Res. 2. into 1.)
6. ¬P(f(a)) ∨ Q(b) (Fact. 5.)
7. Q(b) ∨ Q(b) (Res. 2. into 6.)
8. Q(b) (Fact. 7.)
9. ¬P(g(b, a)) (Res. 8. into 3.)
10. ⊥ (Res. 4. into 9.)
Soundness of Resolution

Proposition
Propositional resolution is sound.

Proof:
Let $I \in \Sigma$-Alg. To be shown:

1. for resolution: $I \models C \lor A$, $I \models D \lor \neg A \Rightarrow I \models C \lor D$
2. for factorization: $I \models C \lor A \lor A \Rightarrow I \models C \lor A$
Soundness of Resolution

**Proposition**
Propositional resolution is sound.

**Proof:**
Let $I \in \Sigma$-Alg. To be shown:

1. for resolution: $I \models C \lor A$, $I \models D \lor \neg A$ $\Rightarrow$ $I \models C \lor D$
2. for factorization: $I \models C \lor A \lor A$ $\Rightarrow$ $I \models C \lor A$

Ad (i): Assume premises are valid in $I$. Two cases need to be considered:
(a) $A$ is valid in $I$, or (b) $\neg A$ is valid in $I$. 
Soundness of Resolution

**Proposition**
Propositional resolution is sound.

**Proof:**
Let \( I \in \Sigma\text{-Alg} \). To be shown:

1. for resolution: \( I \models C \lor A, \ I \models D \lor \neg A \Rightarrow I \models C \lor D \)
2. for factorization: \( I \models C \lor A \lor A \Rightarrow I \models C \lor A \)

Ad (i): Assume premises are valid in \( I \). Two cases need to be considered:
(a) \( A \) is valid in \( I \), or (b) \( \neg A \) is valid in \( I \).

a) \( I \models A \Rightarrow I \models D \Rightarrow I \models C \lor D \)
Soundness of Resolution

Proposition
Propositional resolution is sound.

Proof:
Let \( I \in \Sigma\text{-Alg} \). To be shown:

1. for resolution: \( I \models C \lor A, \ I \models D \lor \neg A \Rightarrow I \models C \lor D \)
2. for factorization: \( I \models C \lor A \lor A \Rightarrow I \models C \lor A \)

Ad (i): Assume premises are valid in \( I \). Two cases need to be considered:
(a) \( A \) is valid in \( I \), or (b) \( \neg A \) is valid in \( I \).

a) \( I \models A \Rightarrow I \models D \Rightarrow I \models C \lor D \)
b) \( I \models \neg A \Rightarrow I \models C \Rightarrow I \models C \lor D \)
Soundness of Resolution

Proposition
Propositional resolution is sound.

Proof:
Let $I \in \Sigma$-Alg. To be shown:

1. for resolution: $I \models C \lor A$, $I \models D \lor \neg A \Rightarrow I \models C \lor D$
2. for factorization: $I \models C \lor A \lor A \Rightarrow I \models C \lor A$

Ad (i): Assume premises are valid in $I$. Two cases need to be considered:
(a) $A$ is valid in $I$, or (b) $\neg A$ is valid in $I$.

a) $I \models A \Rightarrow I \models D \Rightarrow I \models C \lor D$

b) $I \models \neg A \Rightarrow I \models C \Rightarrow I \models C \lor D$

Ad (ii): even simpler.
Resolution is also refutationally complete.
Methods for First-Order Clause Logic

Treated here:

- Gilmore’s method (considered “naive” nowadays)
- The Resolution Calculus

The Resolution Calculus [Robinson 1965] (for first-order clause logic) is much better suited for automatization on a computer than earlier calculi:

- Simpler (one single inference rule)
- Less search space

There are other methods that are not based on Resolution:

- Tableaux and connection methods, Model Elimination (see later)
- Instance Based Methods (separate lecture)
Gilmore’s Method

Early method for FOTP, directly based on Herbrand’s theorem

Preprocessing:

Given Formula

\[ \forall x \exists y \ P(y, x) \wedge \forall z \neg P(z, a) \]

Clause Form

\[ P(f(x), x) \neg P(z, a) \]

Outer loop:
Grounding

Inner loop:
Propositional Method
Gilmore’s Method

Early method for FOTP, directly based on Herbrand’s theorem

Preprocessing:
Given Formula

\[ \forall x \exists y \ P(y, x) \land \forall z \neg P(z, a) \]

Clause Form

\[ P(f(x), x) \land \neg P(z, a) \]

Outer loop:
Grounding

\[ P(f(a), a) \land \neg P(a, a) \]

Inner loop:
Propositional Method
Gilmore’s Method

Early method for FOTP, directly based on Herbrand’s theorem

**Preprocessing:**

Given Formula

\[ \forall x \exists y P(y, x) \land \forall z \neg P(z, a) \]

Clause Form

\[ P(f(x), x) \]
\[ \neg P(z, a) \]

**Outer loop: Grounding**

\[ P(f(a), a) \]
\[ \neg P(a, a) \]

**Inner loop: Propositional Method**

Sat?

No

STOP: Proof found

Yes

Continue Outer Loop

First-Order Theorem Proving – Peter Baumgartner – p.59
Gilmore’s Method

Early method for FOTP, directly based on Herbrand’s theorem

Given Formula

\( \forall x \exists y \ P(y, x) \land \forall z \neg P(z, a) \)

Clause Form

\( P(f(x), x) \)
\( \neg P(z, a) \)

Preprocessing:

Outer loop: Grounding

\( P(f(a), a) \)
\( \neg P(a, a) \)

Inner loop: Propositional Method

\( P(f(a), a) \)
\( \neg P(a, a) \)
\( \neg P(f(a), a) \)
**Gilmore’s Method**

Early method for FOTP, directly based on Herbrand’s theorem

**Preprocessing:**

Given Formula: \(orall x \exists y \ P(y, x) \land \forall z \neg P(z, a)\)

Clause Form: \(P(f(x), x)\)

**Outer loop:**

Grounding

Given Formula: \(P(f(a), a)\)

Clause Form: \(P(f(a), a)\)

**Inner loop:**

Propositional Method

Given Formula: \(\neg P(a, a)\)

Clause Form: \(\neg P(f(a), a)\)

**Sat?**

No → **STOP:** Proof found

Yes → Continue Outer Loop

---

*First-Order Theorem Proving* – Peter Baumgartner – p.59
**Gilmore’s Method**

Early method for FOTP, directly based on Herbrand’s theorem

**Preprocessing:**

Given Formula: \( \forall x \exists y \ P(y, x) \land \forall z \neg P(z, a) \)

Clause Form: \( P(f(x), x) \land \neg P(z, a) \)

**Outer loop:**

Grounding

Given Formula: \( P(f(a), a) \land \neg P(a, a) \)

Clause Form: \( P(f(a), a) \land \neg P(a, a) \land \neg P(f(a), a) \)

**Inner loop:**

Propositional Method

**Problems/Issues:**

- Controlling the grounding process in **outer loop** (irrelevant instances)
- Repeat work **across** inner loops
- Weak redundancy criterion **within** inner loop

---

First Order Theorem Proving – Peter Baumgartner – p.59
... Versus Resolution

Central Point: Resolution performs **intrinsic first-order reasoning**
Central Point: Resolution performs intrinsic first-order reasoning

Resolution inferences on first-order clauses (clauses with variables):

\[
P(f(x), x) \quad \neg P(y, z) \lor Q(y, z)
\]

\[
Q(f(x), x)
\]
Versus Resolution

Central Point: Resolution performs intrinsic first-order reasoning

Resolution inferences on first-order clauses (clauses with variables):

\[
P(f(x), x) \quad \neg P(y, z) \lor Q(y, z)
\]

\[
Q(f(x), x)
\]

One inference may represent infinitely many propositional resolution inferences ("lifting principle")
Central Point: Resolution performs intrinsic first-order reasoning

Resolution inferences on first-order clauses (clauses with variables):

\[ P(f(x), x) \quad \neg P(y, z) \lor Q(y, z) \]

\[ \quad \quad \quad \quad \quad \quad \quad \quad \quad Q(f(x), x) \]

One inference may represent infinitely many propositional resolution inferences ("lifting principle")

Redundancy concepts, e.g. subsumption deletion:

\[ P(y, z) \quad \text{subsumes} \quad P(y, y) \lor Q(y, y) \]
Central Point: Resolution performs **intrinsic first-order reasoning**

Resolution inferences on first-order clauses (clauses with variables):

\[
P(f(x), x) \quad \neg P(y, z) \lor Q(y, z) \\
\quad Q(f(x), x)
\]

One inference may represent infinitely many propositional resolution inferences ("lifting principle")

Redundancy concepts, e.g. **subsumption deletion**:

\[
P(y, z) \quad \text{subsumes} \quad P(y, y) \lor Q(y, y)
\]

Not available in Gilmore’s method
First-Order Resolution through Instantiation

**Idea:** Instantiate clauses to ground clauses:

\[
egin{align*}
P(z', z') \lor \neg Q(z) & \quad \neg P(a, y) & \quad P(x', b) \lor Q(f(x', x)) \\
[a/z', f(a, b)/z] & \quad [a/y] & \quad [b/y] & \quad [a/x', b/x]
\end{align*}
\]

\[
egin{align*}
P(a, a) \lor \neg Q(f(a, b)) & \quad \neg P(a, a) & \quad \neg P(a, b) & \quad P(a, b) \lor Q(f(a, b)) \\
\neg Q(f(a, b)) & \quad Q(f(a, b)) & \quad & \quad \bot
\end{align*}
\]

Bears ressemblance with Gilmore’s method.
First-Order Resolution through Instantiation

Problems

- More than one instance of a clause can participate in a proof.
- Even worse: There are infinitely many possible instances.
First-Order Resolution through Instantiation

Problems

- More than one instance of a clause can participate in a proof.
- Even worse: There are infinitely many possible instances.

Observation

- Instantiation must produce complementary literals (so that inferences become possible).
First-Order Resolution through Instantiation

Problems

- More than one instance of a clause can participate in a proof.
- Even worse: There are infinitely many possible instances.

Observation

- Instantiation must produce complementary literals (so that inferences become possible).

Idea

- Do not instantiate more than necessary to get complementary literals.
First-Order Resolution

**Idea:** do not instantiate more than necessary:

\[
P(z', z') \lor \neg Q(z) \quad \neg P(a, y) \quad P(x', b) \lor Q(f(x', x))
\]

\[
[a/z'] \quad [a/y] \quad [b/y] \quad [a/x']
\]

\[
P(a, a) \lor \neg Q(z) \quad \neg P(a, a) \quad \neg P(a, b) \quad P(a, b) \lor Q(f(a, x))
\]

\[
[\neg Q(z)] \quad [\neg P(a, a)] \quad [\neg P(a, b)] \quad [P(a, b) \lor Q(f(a, x))]
\]

\[
[f(a, x)/z] \quad [Q(f(a, x))]
\]

\[
[\neg Q(f(a, x))] \quad [Q(f(a, x))]
\]

\[
\bot
\]
Lifting Principle

Problem: Make closure under Resolution and Factorization of infinite sets of clauses as they arise from taking the (ground) instances of finitely many first-order clauses (with variables) effective and efficient.

Idea (Robinson 65):

- Resolution for first-order clauses:

  - Equality of ground atoms is generalized to unifiability of general atoms;
  - Only compute most general (minimal) unifiers.
Lifting Principle

Significance: The advantage of the method in (Robinson 65) compared with (Gilmore 60) is that unification enumerates only those instances of clauses that participate in an inference. Moreover, clauses are not right away instantiated into ground clauses. Rather they are instantiated only as far as required for an inference. Inferences with non-ground clauses in general represent infinite sets of ground inferences which are computed simultaneously in a single step.
Resolution for First-Order Clauses

\[
\begin{align*}
C \lor A & \quad D \lor \neg B \\
\frac{\neg \exists \sigma}{(C \lor D)\sigma} & \quad \text{if } \sigma = \text{mgu}(A, B) \quad \text{[resolution]} \\
C \lor A \lor B & \\
\frac{(C \lor A)\sigma}{(C \lor A)\sigma} & \quad \text{if } \sigma = \text{mgu}(A, B) \quad \text{[factorization]}
\end{align*}
\]

In both cases, \(A\) and \(B\) have to be renamed apart (made variable disjoint).
Resolution for First-Order Clauses

\[
\frac{C \lor A \quad D \lor \neg B}{(C \lor D)\sigma} \quad \text{if } \sigma = \text{mgu}(A, B) \quad \text{[resolution]}
\]

\[
\frac{C \lor A \lor B}{(C \lor A)\sigma} \quad \text{if } \sigma = \text{mgu}(A, B) \quad \text{[factorization]}
\]

In both cases, \(A\) and \(B\) have to be renamed apart (made variable disjoint).

Example

\[
\frac{Q(z) \lor P(z, z) \quad \neg P(x, y)}{Q(x)} \quad \text{where } \sigma = [x/z, x/y] \quad \text{[resolution]}
\]

\[
\frac{Q(z) \lor P(z, a) \lor P(a, y)}{Q(a) \lor P(a, a)} \quad \text{where } \sigma = [a/z, a/y] \quad \text{[factorization]}
\]
Unification

A substitution $\sigma$ is a mapping from variables to terms which is the identity almost everywhere.
Example: $\sigma = [f(a,x)/z, b/y]$
Unification

A substitution $\sigma$ is a mapping from variables to terms which is the identity almost everywhere.
Example: $\sigma = [f(a, x)/z, b/y]$

A substitutions can be **applied** to a term $t$, written as $t\sigma$.
Example, where $\sigma$ is from above: $g(x, y, z)\sigma = g(x, b, f(a, x))$. 
Unification

A substitution $\sigma$ is a mapping from variables to terms which is the identity almost everywhere.
Example: $\sigma = [f(a, x)/z, b/y]$

A substitutions can be applied to a term $t$, written as $t\sigma$.
Example, where $\sigma$ is from above: $g(x, y, z)\sigma = g(x, b, f(a, x))$.

Let $E = \{s_1 \doteq t_1, \ldots, s_n \doteq t_n\}$ ($s_i, t_i$ terms or atoms) a multi-set of equality problems.
A substitution $\sigma$ is called a unifier of $E$ if $s_i\sigma = t_i\sigma$ for all $1 \leq i \leq n$.

If a unifier of $E$ exists, then $E$ is called unifiable.
Unification

A substitution $\sigma$ is called more general than a substitution $\tau$, denoted by $\sigma \leq \tau$, if there exists a substitution $\rho$ such that $\rho \circ \sigma = \tau$, where $(\rho \circ \sigma)(x) := (x\sigma)\rho$ is the composition of $\sigma$ and $\rho$ as mappings.

If a unifier of $E$ is more general than any other unifier of $E$, then we speak of a most general unifier of $E$, denoted by $\text{mgu}(E)$. 
Unification after Martelli/Montanari

\[ t \equiv t, E \quad \Rightarrow_{MM} \quad E \]
\[ f(s_1, \ldots, s_n) \equiv f(t_1, \ldots, t_n), E \quad \Rightarrow_{MM} \quad s_1 \equiv t_1, \ldots, s_n \equiv t_n, E \]
\[ f(\ldots) \equiv g(\ldots), E \quad \Rightarrow_{MM} \quad \bot \]
\[ x \equiv t, E \quad \Rightarrow_{MM} \quad x \equiv t, E[t/x] \]
\[ \text{if } x \in \text{var}(E), x \notin \text{var}(t) \]
\[ x \equiv t, E \quad \Rightarrow_{MM} \quad \bot \]
\[ \text{if } x \neq t, x \in \text{var}(t) \]
\[ t \equiv x, E \quad \Rightarrow_{MM} \quad x \equiv t, E \]
\[ \text{if } t \notin X \]
If $E = x_1 = u_1, \ldots, x_k = u_k$, with $x_i$ pairwise distinct, $x_i \notin \text{var}(u_j)$, then $E$ is called (an equational problem) in **solved form** representing the solution $\sigma_E = [u_1/x_1, \ldots, u_k/x_k]$.

**Proposition**

If $E$ is a solved form then $\sigma_E$ is an mgu of $E$. 
MM: Main Properties

Theorem

1. If $E \Rightarrow_{MM} E'$ then $\sigma$ is a (most general) unifier of $E$ iff $\sigma$ is a (most general) unifier of $E'$
Main Properties

Theorem

1. If $E \Rightarrow_{MM} E'$ then $\sigma$ is a (most general) unifier of $E$ iff $\sigma$ is a (most general) unifier of $E'$

2. If $E \Rightarrow^*_{MM} \bot$ then $E$ is not unifiable.
MM: Main Properties

Theorem

1. If $E \Rightarrow_{MM} E'$ then $\sigma$ is a (most general) unifier of $E$ iff $\sigma$ is a (most general) unifier of $E'$

2. If $E \Rightarrow^*_{MM} \bot$ then $E$ is not unifiable.

3. If $E \Rightarrow^*_{MM} E'$ with $E'$ in solved form, then $\sigma_{E'}$ is an mgu of $E$. 
**MM: Main Properties**

**Theorem**

1. If $E \Rightarrow_{MM} E'$ then $\sigma$ is a (most general) unifier of $E$ iff $\sigma$ is a (most general) unifier of $E'$

2. If $E \not\Rightarrow_{MM} \perp$ then $E$ is not unifiable.

3. If $E \Rightarrow_{MM}^* E'$ with $E'$ in solved form, then $\sigma_{E'}$ is an mgu of $E$.

**Theorem**

$E$ is unifiable if and only if there is a most general unifier $\sigma$ of $E$, such that $\sigma$ is idempotent and $\text{dom}(\sigma) \cup \text{codom}(\sigma) \subseteq \text{var}(E)$.

Problem: **exponential growth** of terms possible
Properties of Resolution

**Theorem:** Resolution is sound. That is, all derived formulas are logical consequences of the given ones.
Properties of Resolution

**Theorem:** Resolution is *sound*. That is, all derived formulas are logical consequences of the given ones.

**Theorem:** Resolution is *refutationally complete*. That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause $\bot$ eventually.
Properties of Resolution

**Theorem:** Resolution is **sound**. That is, all derived formulas are logical consequences of the given ones.

**Theorem:** Resolution is **refutationally complete**. That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause $\bot$ eventually.

More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factorization inference rules, then it contains the empty clause $\bot$. 
Properties of Resolution

**Theorem:** Resolution is **sound**. That is, all derived formulas are logical consequences of the given ones.

**Theorem:** Resolution is **refutationally complete**. That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause ⊥ eventually.

More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factorization inference rules, then it contains the empty clause ⊥.

Perhaps easiest proof: Herbrand Theorem + Semantic Tree proof technique + Lifting Theorem

(This result can be considerably strengthened using other techniques)
Properties of Resolution

**Theorem:** Resolution is *sound*. That is, all derived formulas are logical consequences of the given ones.

**Theorem:** Resolution is *refutationally complete*. That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause $\bot$ eventually.

More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factorization inference rules, then it contains the empty clause $\bot$.

Perhaps easiest proof: Herbrand Theorem + Semantic Tree proof technique + Lifting Theorem

(This result can be considerably strengthened using other techniques)

Closure can be achieved by the “Given Clause Loop” on next slide.
The “Given Clause Loop”

As used in the Otter theorem prover:
Lists of clauses maintained by the algorithm: usable and sos.
Initialize sos with the input clauses, usable empty.

**Algorithm** (straight from the Otter manual):

While (sos is not empty and no refutation has been found)
   1. Let given_clause be the ‘lightest’ clause in sos;
   2. Move given_clause from sos to usable;
   3. Infer and process new clauses using the inference rules in effect; each new clause must have the given_clause as one of its parents and members of usable as its other parents; new clauses that pass the retention tests are appended to sos;
End of while loop.

**Fairness:** define clause weight e.g. as “depth + length” of clause.
The “Given Clause Loop” - Graphically
The “Given Clause Loop” - Graphically

usable list

set of support
The “Given Clause Loop” - Graphically

- Given clause
- Usable list
- Set of support
The “Given Clause Loop” - Graphically

- Given clause
- Usable list
- Set of support
- Consequences

First-Order Theorem Proving – Peter Baumgartner – p.74
The “Given Clause Loop” - Graphically
The “Given Clause Loop” - Graphically

Given clause → usable list → set of support → filters

Consequences

First-Order Theorem Proving – Peter Baumgartner – p.74
Part IV: Model Generation and Tableaux

No “theorem” clause, cannot use Resolution to derived a contradiction. Ideally, can detect satisfiability by computing a model.

**Why compute models?**

**Planning:** Can be formalised as propositional satisfiability problem.

[Kautz & Selman, AAAI96; Dimopolous et al, ECP97]

**Diagnosis:** Minimal models of *abnormal* literals (circumscription).

[Reiter, AI87]

**Databases:** View materialisation, View Updates, Integrity Constraints.

**Nonmonotonic reasoning:** Various semantics (GCWA, Well-founded, Perfect, Stable,...), all based on minimal models. [Inoue et al, CADE 92]

**Software Verification:** Counterexamples to conjectured theorems.

**Theorem proving:** Counterexamples to conjectured theorems. Finite models of quasigroups, (MGTP/G). [Fujita et al, IJCAI 93]
Part IV: Model Generation and Tableaux

Why compute models (cont’d)?

Natural Language Processing:

Maintain models $J_1, \ldots, J_n$ as different readings of discourses:

\[ J_i \models BG-Knowledge \cup Discourse_{so\_far} \]
Part IV: Model Generation and Tableaux

Why compute models (cont’d)?

Natural Language Processing:

- Maintain models $I_1, \ldots, I_n$ as different readings of discourses:

$$I_i \models BG\text{-Knowledge} \cup Discourse\_so\_far$$

- Consistency checks (“Mia’s husband loves Sally. She is not married.”)

$$BG\text{-Knowledge} \cup Discourse\_so\_far \not\models \neg New\_utterance$$

iff

$$BG\text{-Knowledge} \cup Discourse\_so\_far \cup New\_utterance \text{ is satisfiable}$$
Part IV: Model Generation and Tableaux

Why compute models (cont’d)?

Natural Language Processing:

- Maintain models $J_1, \ldots, J_n$ as different readings of discourses:
  \[
  J_i \models BG\text{-}Knowledge \cup \text{Discourse}_{so\_far}
  \]

- Consistency checks ("Mia’s husband loves Sally. She is not married.")
  \[
  BG\text{-}Knowledge \cup \text{Discourse}_{so\_far} \not\models \neg \text{New\_utterance}
  \]
  iff \quad BG\text{-}Knowledge \cup \text{Discourse}_{so\_far} \cup \text{New\_utterance} \text{ is satisfiable}

- Informativity checks ("Mia’s husband loves Sally. She is married.")
  \[
  BG\text{-}Knowledge \cup \text{Discourse}_{so\_far} \not\models \text{New\_utterance}
  \]
  iff \quad BG\text{-}Knowledge \cup \text{Discourse}_{so\_far} \cup \neg \text{New\_utterance} \text{ is satisfiable}
Tableaux

Calculi with a long history

- Beth 1955, Hintikka 1955, Schütte 1956: Calculi without meta-language constructs, such as sequents. Nodes in derivation tree labeled by formulae.

- Lis 1960, Smullyan 1968: Analytic tabaleaux
Tableaux

**Calculi with a long history**

- Beth 1955, Hintikka 1955, Schütte 1956: Calculi without meta-language constructs, such as sequents. Nodes in derivation tree labeled by formulae.
- Lis 1960, Smullyan 1968: Analytic tabaleaux

**Some later FOTP Calculi can be rephrased as Tableaux**

- Loveland 1968 Model elimination, Kowalski, Kuehner 1971 SL-resolution
Tableaux

Calculi with a long history
- Beth 1955, Hintikka 1955, Schütte 1956: Calculi without meta-language constructs, such as sequents. Nodes in derivation tree labeled by formulae.
- Lis 1960, Smullyan 1968: Analytic tabaleaux

Some later FOTP Calculi can be rephrased as Tableaux
- Loveland 1968 Model elimination, Kowalski, Kuehner 1971 SL-resolution

Significance
- Various non-classical logics (modal, sub-structural, ...)
- ATP in Description Logics (cf. Knowledge Representation lectures)
Tableaux

Calculi with a long history

Beth 1955, Hintikka 1955, Schütte 1956: Calculi without meta-language constructs, such as sequents. Nodes in derivation tree labeled by formulae.

Lis 1960, Smullyan 1968: Analytic tabaleaux

Some later FOTP Calculi can be rephrased as Tableaux

Loveland 1968 Model elimination, Kowalski, Kuehner 1971 SL-resolution

Bibel 1975, Andrews 1976 Connection or matings methods.

Significance

Various non-classical logics (modal, sub-structural, …)

ATP in Description Logics (cf. Knowledge Representation lectures)

Model generation
Analytic Tableaux

Given set of propositional formulae, e.g. \{\neg P \land \neg(Q \lor R), \neg(Q \land \neg R)\}

Construct a tree by using Tableau extension rules:

\[
\neg P \land \neg(Q \lor R)
\]

\[
\neg(Q \land \neg R)
\]

\[
\neg Q \quad \neg R
\]

\[
\neg P \quad R
\]

\[
\neg(Q \lor R)
\]

\[
\neg Q \quad \star
\]

\[
\neg R
\]
Analytic Tableaux

Given set of propositional formulae, e.g. \( \{\neg P \land \neg (Q \lor R), \neg (Q \land \neg R)\} \)

Construct a tree by using Tableau extension rules:

\[
\neg P \land \neg (Q \lor R)
\]

\[
\neg (Q \land \neg R)
\]

\[
\neg Q \quad \neg R
\]

\[
\neg P \quad R
\]

\[
\neg (Q \lor R)
\]

\[
\neg Q
\]

\[
\neg R
\]

Left branch is open (non-contradictory) and fully expanded: model
Clause Normalform Tableaux – Ground Case

Given a set of clauses, e.g. \{\{R, P\}, \{P, Q\}, \{\neg P, Q\}, \{\neg Q, P\}, \{\neg P, \neg Q\}\}.

From a one-path tree, consisting of a node for each clause, construct a tree by using the \(\beta\)-rule:

```
{R, P}
{P, Q}
{\neg P, Q}
{P, \neg Q}
{\neg P, \neg Q}
```

```
R
  /\  \
/ \  \
P
  /\  \
/  \  \
P
  /\  \
/   \  \
P
  /\  \
/    \  \
\neg P
  /\  \
/   \  \
\neg Q
```

“Link condition” not satisfied
Can be demanded (or not)
First-Order Tableaux: The $P(x) \lor Q(x)$ problem

No Problem:
\[
\forall x, y \ (P(x) \lor Q(y)) \iff \forall x \ P(x) \lor \forall y \ Q(y)
\]

Problem:
\[
\forall x \ (P(x) \lor Q(x)) \iff \forall x \ P(x) \lor \forall x \ Q(x)
\]

\[\begin{array}{c}
\forall x \ P(x) \\
\forall y \ Q(y) \\
\neg P(a) \\
\neg Q(b)
\end{array}\]

\[\begin{array}{c}
P(X) \\
Q(X)
\end{array}\]

$x, y$ branch-local

$x$ split variable

universal variables

rigid variable, stands for one ground term
Clause Normalform Tableaux – First Order Case

Allow max number $n$ of $\gamma$-rule applications, arbitrary $\beta$-rule applications

Try **simultaneously** closing all branches by unifying literals; increase $n$ if unsuccessful and restart

\[
\forall x (P(x) \lor Q(x)) \\
\neg Q(b) \\
\neg P(a) \\
\neg Q(a) \lor r \\

P(X) \lor Q(X) \quad \gamma\text{-rule: copy of clause with rigid variables} \\

\]

\[
P(X) \quad Q(X) \quad \beta\text{-rule: splitting} \\

\]

Branch closure candidate subst: $\sigma = [a/X]$
Clause Normalform Tableaux – First Order Case

Allow max number $n$ of $\gamma$-rule applications, arbitrary $\beta$-rule applications

Try simultaneously closing all branches by unifying literals; increase $n$ if unsuccessful and restart

$$\forall x (P(x) \lor Q(x))$$
$$\neg Q(b)$$
$$\neg P(a)$$
$$\neg Q(a) \lor r$$

$\gamma$-rule: copy of clause with rigid variables

$$P(X) \lor Q(X)$$
$$P(X) \quad Q(X)$$

$\beta$-rule: splitting

Branch closure candidate subst: $\sigma = [a/X]$ 

This formalism can be used to describe Prolog’s SLD Resolution, Model Elimination, Connection Methods, Hyper Tableaux, …
Significance: an early and simple method for model computation, can also be described as a tableaux method (without rigid variables)

1. Convert clauses to range-restricted form:

   \[ q(x) \lor p(x, y) \leftarrow q(x) \quad \sim \quad q(X) ; p(X, Y) \leftarrow q(X), \, \text{dom}(Y) \]

2. assert range-restricted clauses and \text{dom} clauses in Prolog database.

3. Call satisfiable:

   ```prolog
   satisfy :-
   (Head <- Body),
   Body, not Head, !,
   component(HLit, Head),
   assume(HLit),
   not false,
   satisfy.
   satisfy.
   ```

   ```prolog
   assume(X) :- asserta(X).
   assume(X) :-
   retract(X), !, fail.
   component(E, (E ; _)) :-
   component(E, (_ ; R)) :-
   !, component(E, R).
   component(E, E).
   ```
Further Considerations

Choice. There have been many inference systems developed. Which one is best suited for my application?
Further Considerations

**Choice.** There have been many inference systems developed. Which one is best suited for my application?

**Local search space.** Design small inference systems that allow for as little as inferences as possible.
Further Considerations

**Choice.** There have been many inference systems developed. Which one is best suited for my application?

**Local search space.** Design small inference systems that allow for as little as inferences as possible.

**Global redundancy elimination.** In general there are many proofs of a given formula. Proof attempts that are “subsumed” by previous attempts should be pruned.
Further Considerations

**Choice.** There have been many inference systems developed. Which one is best suited for my application?

**Local search space.** Design small inference systems that allow for as little as inferences as possible.

**Global redundancy elimination.** In general there are many proofs of a given formula. Proof attempts that are “subsumed” by previous attempts should be pruned.

**Efficient data structures.** Determine as fast as possible the possible inferences.
Further Considerations

**Choice.** There have been many inference systems developed. Which one is best suited for my application?

**Local search space.** Design small inference systems that allow for as little as inferences as possible.

**Global redundancy elimination.** In general there are many proofs of a given formula. Proof attempts that are “subsumed” by previous attempts should be pruned.

**Efficient data structures.** Determine as fast as possible the possible inferences.

**Building-in theories.** Specialized reasoning procedures for “data structures”, like $\mathbb{R}$, $\mathbb{Z}$, lists, arrays, sets, etc. (These can be axiomatized, but in general this leads to nowhere.)