First-Order Theorem Proving

Peter Baumgartner
NICTA, Logic and Computation Program, Canberra
Peter.Baumgartner@nicta.com.au

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

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

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

\[ y_1 \approx 1 \land z_0 \approx x_0 \land y_3 \approx x_0 \land y_1 \]
\[ y'_1 \approx 1 \land R_1 \approx x'_0 \land x_0 \land R_2 \approx R_3 \land y'_0 \approx R_2 \land y'_5 \approx R_1 + 1 \]
\[ \land x_0 \approx x'_0 \land y_0 \approx y'_0 \land z_0 \approx z'_0 \]
\[ \models y_3 \approx y'_5 \]

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

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

- **killed** : \( \overline{\text{killed}(x, y) \rightarrow \text{hates}(x, y)} \)
- **hates** : \( \overline{\text{hates}(c, y) \rightarrow \overline{\text{hates}(a, y)}} \)
- **killed** : \( \overline{\text{killed}(c, y) \rightarrow \overline{\text{hates}(a, y)}} \)
- **killed** : \( \overline{\text{killed}(c, y) \rightarrow \overline{\text{hates}(a, y)}} \)
- **killed** : \( \overline{\text{killed}(c, y) \rightarrow \overline{\text{hates}(a, y)}} \)

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

The Principle

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description of the situation in Dreadbury Mansion</strong></td>
<td>Who killed Agatha?</td>
</tr>
<tr>
<td>Charles killed Agatha</td>
<td>Murderer unknown</td>
</tr>
<tr>
<td>The butler killed Agatha</td>
<td>Agatha committed suicide</td>
</tr>
</tbody>
</table>

A Glimpse at FOTP

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.

\[ \neg a = b \]
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)

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?

Problems of the following, complementary kind are interesting, too:
- Does a formula (e.g.: killed(b, a)) not follow from other formulas?

Non-entailment is much harder a problem!

A Mathematical Example

The sum of two continuous function is continuous.

**Definition** 
A function $f : \mathbb{R} \to \mathbb{R}$ 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:

$$|h(x) - h(a)| = |f(x) + g(x) - f(a) - g(a)|$$
$$= |(f(x) - f(a)) + (g(x) - g(a))|$$
$$\leq |f(x) - f(a)| + |g(x) - g(a)| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

The Language of Predicate Logic

"$f$ 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:

all(Eps,  
0<Eps =>  
all(A,  
exists(Delta,  
0<Delta and  
all(X, abs(X-A)<Delta =>  
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 \( 0, | \cdot |, - \rightarrow f(\cdot) \)

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.

Example

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

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

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

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

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

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

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

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:

\[
\begin{align*}
  x + y &= y + x \\
  (x + y) + z &= x + (y + z) \\
  x - y &= x + (-y) \\
  -(x + y) &= (-x) + (-y)
\end{align*}
\]

Now one can prove:

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

It can even be proven fully automatically!

Algorithmic Problems

The following is a list of practically relevant problems:

Validity(\( F \)):

| \( F \) 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 . . .
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 \( \Rightarrow_p \):

- \( (F \leftrightarrow G) \Rightarrow_p (F \rightarrow G) \land (G \rightarrow F) \)
- \( \neg Q x F \Rightarrow_p \overline{Q} x \neg F \) (\( \neg Q \))
- \( (Q x F \rho G) \Rightarrow_p Q y (F[y/x] \rho G), \ y \text{ fresh}, \ \rho \in \{ \land, \lor \} \)
- \( (Q x F \rightarrow G) \Rightarrow_p \overline{Q} y (F[y/x] \rightarrow G), \ y \text{ fresh} \)
- \( (F \rho Q x G) \Rightarrow_p Q y (F \rho G[y/x]), \ y \text{ fresh}, \ \rho \in \{ \land, \lor, \rightarrow \} \)

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

∀ε(0 < ε → ∀a∃δ (0 < δ ∧ ∀x (|x − a| < δ → |f(x) − f(a)| < ε)))
⇒ p
∀ε∀a(0 < ε → 3δ (0 < δ ∧ ∀x (|x − a| < δ → |f(x) − f(a)| < ε)))
⇒ p
∀ε∀a3δ (0 < ε → 0 < δ ∧ ∀x (|x − a| < δ → |f(x) − f(a)| < ε))
⇒ p
∀ε∀a3δ (0 < ε → ∀x (0 < δ ∧ |x − a| < δ → |f(x) − f(a)| < ε))
⇒ p
∀ε∀a3δ ∀x (0 < ε → (0 < δ ∧ (|x − a| < δ → |f(x) − f(a)| < ε)))

Skolemization

**Intuition:** replacement of ∃y by a concrete choice function computing y from all the arguments y depends on. Transformation ⇒ S (to be applied outermost, not in subformulas):

∀x1, . . . , xn 3yF ⇒ S ∀x1, . . . , xn F[f(x1, . . . , xn)/y]

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

In the Example

∀ε∀a3δ ∀x (0 < ε → 0 < δ ∧ (|x − a| < δ → |f(x) − f(a)| < ε))
⇒ S
∀ε∀a∀x (0 < ε → 0 < d(ε, a) ∧ (|x − a| < d(ε, a) → |f(x) − f(a)| < ε))

Clausal Normal Form (Conjunctive Normal Form)

(F ↔ G) ⇒ K (F → G) ∧ (G → F)
(F → G) ⇒ K (¬F ∨ G)
¬(F ∨ G) ⇒ K (¬F ∧ ¬G)
¬(F ∧ G) ⇒ K (¬F ∨ ¬G)
¬¬F ⇒ K F
(F ∧ G) ∨ H ⇒ K (F ∨ H) ∧ (G ∨ H)
(F ∧ ⊤) ⇒ K F
(F ∧ ⊥) ⇒ K ⊥
(F ∨ ⊤) ⇒ K ⊤
(F ∨ ⊥) ⇒ K F

These rules are to be applied modulo associativity and commutativity of ∧ and ∨. The first five rules, plus the rule (¬Q), compute the negation normal form (NNF) of a formula.

Theorem: The given and the final formula are equi-satisfiable.
In the Example

∀ε ∀a ∀x (0 < ε → 0 < d(ε, a) ∧ (|x − a| < d(ε, a) → |f(x) − f(a)| < ε))
⇒K
0 < d(ε, a) ∨ ¬(0 < ε) ∧ (|x − a| < d(ε, a) → |f(x) − f(a)| < ε)

Note: The universal quantifiers for the variables ε, a and x, as well as the conjunction symbol ∧ between the clauses are not written, for convenience.

The Complete Picture

F ⇒ ∀x1...xn H (m ≤ n, H quantifier-free)
⇒ ∀x1...xm G (G quantifier-free)
⇒ ∀x1...xmk n i=1 j=1 Lij (G quantifier-free)

N = {C₁, ..., Ck} is called the clausal (normal) form (CNF) of F.

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 ∨ B ∨ ¬C ∨ ¬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 ⊨ G.
Equivalently, we can prove that F := H ∧ ¬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”

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.
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

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

\[
f_{\mathcal{A}}(\triangle, \ldots, \triangle) = f
\]

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 \( p_{\mathcal{A}} \subseteq T_{\Sigma}^m \).

**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.

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 \( \Sigma \))

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

is the set of **ground instances** of \( N \).
**Example of a \( G_{\Sigma} \)**

For \( \Sigma_{\text{Pres}} \) one obtains for

\[
C = (x < y) \lor (y \leq s(x))
\]

the following ground instances:

- \((0 < 0) \lor (0 \leq s(0))\)
- \((s(0) < 0) \lor (0 \leq s(0))\)
- \(\ldots\)
- \((s(0) + s(0) < s(0) + 0) \lor (s(0) + 0 \leq s(s(0) + s(0)))\)
- \(\ldots\)

**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.

---

**Herbrand’s Theorem**

**Theorem (Skolem-Herbrand-Theorem)**

\( \forall \phi \) 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 \( \Sigma \))

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

---

**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

\[
\begin{array}{c}
\text{premises} \\
F_1, \ldots, F_n \\
\end{array} \\
\overrightarrow{F_{n+1}} \\
\text{conclusion}
\]

**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 $(F_{i_1}, \ldots, F_{i_n}, F_i)$ in $\Gamma,$ such that $0 \leq i_j < i,$ for $1 \leq j \leq n_i.$

**Soundness and Completeness**

**Proposition**

1. Let $\Gamma$ be sound. Then $N \vdash_{\Gamma} F \Rightarrow N \models F$
2. $N \vdash_{\Gamma} F$ $\Rightarrow$ there exist $F_1, \ldots, F_n \in N$ s.t. $F_1, \ldots, F_n \vdash_{\Gamma} F$

(resembles compactness).

**Proofs as Trees**

<table>
<thead>
<tr>
<th>markings</th>
<th>$\equiv$ formulas</th>
</tr>
</thead>
<tbody>
<tr>
<td>leaves</td>
<td>$\equiv$ assumptions and axioms</td>
</tr>
<tr>
<td>other nodes</td>
<td>$\equiv$ inferences: conclusion $\equiv$ ancestor</td>
</tr>
<tr>
<td></td>
<td>premises $\equiv$ direct descendants</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
P(f(a)) \lor Q(b) & \quad \neg P(f(a)) \lor \neg Q(b) \\
\neg P(f(a)) \lor Q(b) & \quad \neg P(f(a)) \lor Q(b) \\
Q(b) \lor Q(b) & \quad \neg P(f(a)) \lor \neg Q(b) \\
P(g(a, b)) & \quad \neg P(g(a, b)) \\
\bot & \quad \bot
\end{align*}
\]
**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** \( \text{Res} \) can be used to decide the satisfiability problem of propositional clause logic.

---

**The Resolution Calculus** \( \text{Res} \)

**Resolution inference rule:**

\[
C \lor A \quad \neg A \lor D \\
\hline
\hline
C \lor D
\]

Terminology: \( C \lor D \): **resolvent**; \( A \): **resolved atom**

**(Positive) factorisation inference rule:**

\[
C \lor A \lor A \\
\hline
C \lor A
\]

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)
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.)
10. \( \bot \)  (Res. 4. into 9.)

---

**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) \( I \models \neg A \Rightarrow I \models C \Rightarrow I \models C \lor D \)

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

Central Point: Resolution performs intrinsic first-order reasoning

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

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

Redundancy concepts, e.g. subsumption deletion:

Not available in Gilmore’s method

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

... Versus Resolution
First-Order Resolution through Instantiation

**Idea:** instantiate clauses to ground clauses:

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

\[ \perp \]

Bears ressemblance with Gilmore's method.

First-Order Resolution

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

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

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

\[ \perp \]

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.

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.
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

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

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

Example

\[
\begin{align*}
Q(z) \lor P(z, z) & \quad \neg P(x, y) \\
\frac{}{Q(x)} & \quad \text{where } \sigma = [x/z, x/y] \quad [\text{resolution}] \\
Q(z) \lor P(z, a) \lor P(a, y) & \\
\frac{Q(a) \lor P(a, a)}{Q(a) \lor P(a, a)} & \quad \text{where } \sigma = [a/z, a/y] \quad [\text{factorization}]
\end{align*}
\]

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 \( E = \{ s_1 \equiv t_1, \ldots, s_n \equiv t_n \} \) \( (s_i, t_i \text{ terms or atoms}) \) 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

\[ t \doteq t, E \Rightarrow_{MM} E \]

\[ f(s_1, \ldots, s_n) \doteq f(t_1, \ldots, t_n), E \Rightarrow_{MM} s_1 \doteq t_1, \ldots, s_n \doteq t_n, E \]

\[ f(\ldots) \doteq g(\ldots), E \Rightarrow_{MM} \perp \]

\[ x \doteq t, E \Rightarrow_{MM} x \doteq t, E[x/t] \]

\[ x \doteq t, E \Rightarrow_{MM} \perp \]

\[ t \doteq x, E \Rightarrow_{MM} x \doteq t, E \]

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 \( E \Rightarrow_{MM} \perp \) 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

**MM: Main Properties**

If \( E = x_1 \doteq u_1, \ldots, x_k \doteq u_k \), 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 \( E \).

**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 \( \perp \) 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 \( \perp \).

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.

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, A187]

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]

Why compute models (cont’d)?

Natural Language Processing:
- Maintain models $I_1, \ldots, I_n$ as different readings of discourses:
  $$ I_i \models BG\cdot \text{Knowledge} \cup \text{Discourse so far} $$
- Consistency checks ("Mia’s husband loves Sally. She is not married.")
  $$ BG\cdot \text{Knowledge} \cup \text{Discourse so far} \not\models \neg \text{New utterance} $$
  iff
  $$ BG\cdot \text{Knowledge} \cup \text{Discourse so far} \cup \neg \text{New utterance} \text{ is satisfiable} $$
- Informativity checks ("Mia’s husband loves Sally. She is married.")
  $$ BG\cdot \text{Knowledge} \cup \text{Discourse so far} \not\models \text{New utterance} $$
  iff
  $$ BG\cdot \text{Knowledge} \cup \text{Discourse so far} \cup \neg \text{New utterance} \text{ is satisfiable} $$
### 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 tableaux

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

### Analytic Tableaux

Given a set of clauses, e.g., \( \{ R \land P \}, \{ P \land Q \}, \{ P \land Q \} \).

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

- \( \forall x (P(x) \lor Q(x)) \)
- \( P(a) \lor Q(b) \)
- \( P(a) \lor \neg Q(b) \)
- \( \neg P(a) \lor \neg Q(b) \)

**Model generation**
- First-Order Theorem Proving

---

### Clause Normalform Tableaux – Ground Case

**Given a set of clauses, e.g.**

- \( \{ R \land P \}, \{ P \land Q \}, \{ P \land Q \} \).

**Construct a tree by using Tableau extension rules:**

- Left branch is open (non-contradictory) and fully expanded: model
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

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

$P(X) \lor Q(X)$ \hspace{1cm} $\gamma$-rule: copy of clause with rigid variables

$P(X) \quad Q(X)$ \hspace{1cm} $\beta$-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, . . .

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.)

SATCHMO

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 \text{satisfiable}:

\[
\text{satisfy} :- \hspace{1cm} \text{assume}(X) :- \text{asserta}(X). \\
\text{(Head} \leftarrow \text{Body}), \hspace{1cm} \text{assume}(X) :- \\
\text{Body, not Head, !,} \hspace{1cm} \text{retract}(X), !, \text{fail.} \\
\text{component(}H\text{Lit, Head}), \hspace{1cm} \text{component}(E, (E ; \_)). \\
\text{assume}(H\text{Lit}), \hspace{1cm} \text{component}(E, (\_ ; R)) :- \\
\text{not false,} \hspace{1cm} !, \text{component}(E, R). \\
\text{satisfy.} \hspace{1cm} \text{satisfy.} \\
\text{component}(E, E).
\]