Logic and Proof

Computer Science Tripos Part IB
Michaelmas Term

Lawrence C Paulson
Computer Laboratory
University of Cambridge

lp15@cam.ac.uk

Copyright © 2006 by Lawrence C. Paulson
## Contents

1. Introduction ........................................... 1
2. Propositional Logic .................................. 6
3. Gentzen’s Logical Calculi ............................ 11
4. First-Order Logic ..................................... 16
5. Formal Reasoning in First-Order Logic .......... 22
6. Davis-Putnam & Propositional Resolution ....... 28
7. Skolem Functions and Herbrand’s Theorem ..... 34
8. Unification ............................................. 40
9. Resolution and Prolog ................................. 46
10. Binary Decision Diagrams ......................... 51
11. Modal Logics .......................................... 56
12. Tableaux-Based Methods ............................ 61
Logic concerns statements in some language.

The language can be informal (say English) or formal.

Some statements are true, others false or meaningless.

Logic concerns relationships between statements: consistency, entailment, . . .

Logical proofs model human reasoning (supposedly).

Statements are declarative assertions:

\[ \text{Black is the colour of my true love’s hair.} \]

They are not greetings, questions or commands:

\[ \text{What is the colour of my true love’s hair?} \]
\[ \text{I wish my true love had hair.} \]
\[ \text{Get a haircut!} \]
The \textit{meta-variables} $X$, $Y$, $Z$, \ldots range over ‘real’ objects

- $\text{Black is the colour of } X\text{'s hair.}$
- $\text{Black is the colour of } Y.$
- $Z$ is the colour of $Y$.

Schematic statements can express general statements, or questions:

- What things are black?

An \textit{interpretation} maps meta-variables to real objects:

The interpretation $Y \mapsto \text{coal}$ \textit{satisfies} the statement

- $\text{Black is the colour of } Y.$

but the interpretation $Y \mapsto \text{strawberries}$ does not!

A statement $A$ is \textit{valid} if all interpretations satisfy $A$.  

Lawrence C. Paulson  
University of Cambridge
Consistency, or Satisfiability

A set $S$ of statements is *consistent* if some interpretation satisfies all elements of $S$ at the same time. Otherwise $S$ is *inconsistent*.

Examples of inconsistent sets:

\{X \text{ part of } Y, \ Y \text{ part of } Z, \ X \text{ NOT part of } Z\}

\{n \text{ is a positive integer, } \ n \neq 1, \ n \neq 2, \ldots\}

*Satisfiable* means the same as consistent.

*Unsatisfiable* means the same as inconsistent.

Entailment, or Logical Consequence

A set $S$ of statements *entails* $A$ if every interpretation that satisfies all elements of $S$, also satisfies $A$. We write $S \models A$.

\{X \text{ part of } Y, \ Y \text{ part of } Z\} \models X \text{ part of } Z

\{n \neq 1, \ n \neq 2, \ldots\} \models n \text{ is NOT a positive integer}

$S \models A$ if and only if $\{\neg A\} \cup S$ is inconsistent

$\models A$ if and only if $A$ is valid, if and only if $\{\neg A\}$ is inconsistent.

Lawrence C. Paulson

University of Cambridge
We want to check $A$ is valid.

Checking all interpretations can be effective — but what if there are infinitely many?

Let $\{A_1, \ldots, A_n\} \models B$. If $A_1, \ldots, A_n$ are true then $B$ must be true. Write this as the inference rule

$$
\begin{array}{c}
A_1 \\
\vdots \\
A_n \\
\hline
B
\end{array}
$$

We can use inference rules to construct finite proofs!

A valid inference:

$$
\begin{array}{c}
X \text{ part of } Y \\
Y \text{ part of } Z \\
\hline
X \text{ part of } Z
\end{array}
$$

An inference may be valid even if the premises are false!

$$
\begin{array}{c}
cow \text{ part of chair} \\
chair \text{ part of ant} \\
\hline
cow \text{ part of ant}
\end{array}
$$
**Survey of Formal Logics**

- **propositional logic** is traditional *boolean algebra*.
- **first-order logic** can say *for all* and *there exists*.
- **higher-order logic** reasons about sets and functions.
- **modal/temporal logics** reason about what *must*, or *may*, happen.
- **type theories** support *constructive* mathematics.

All have been used to prove correctness of computer systems.

---

**Why Should the Language be Formal?**

Consider this ‘definition’:

The least integer not definable using eight words

Greater than *The number of atoms in the entire Universe*

Also greater than *The least integer not definable using eight words*

- A formal language prevents AMBIGUITY.
Syntax of Propositional Logic

- **Propositional letter**: P, Q, R, ...
- **t**: true
- **f**: false
- \( \neg A \): not A
- \( A \land B \): A and B
- \( A \lor B \): A or B
- \( A \rightarrow B \): if A then B
- \( A \leftrightarrow B \): A if and only if B

Semantics of Propositional Logic

\( \neg, \land, \lor, \rightarrow \) and \( \leftrightarrow \) are *truth-functional*: functions of their operands.

<table>
<thead>
<tr>
<th>( A )</th>
<th>( B )</th>
<th>( \neg A )</th>
<th>( A \land B )</th>
<th>( A \lor B )</th>
<th>( A \rightarrow B )</th>
<th>( A \leftrightarrow B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>t</td>
<td>t</td>
<td>f</td>
<td>t</td>
<td>t</td>
<td>t</td>
<td></td>
</tr>
<tr>
<td>t</td>
<td>f</td>
<td>f</td>
<td>f</td>
<td>t</td>
<td>f</td>
<td></td>
</tr>
<tr>
<td>f</td>
<td>t</td>
<td>t</td>
<td>f</td>
<td>t</td>
<td>f</td>
<td></td>
</tr>
<tr>
<td>f</td>
<td>f</td>
<td>t</td>
<td>f</td>
<td>f</td>
<td>t</td>
<td></td>
</tr>
</tbody>
</table>

Lawrence C. Paulson  
University of Cambridge
Interpretations of Propositional Logic

An interpretation is a function from the propositional letters to \{t, f\}. Interpretation I satisfies a formula A if the formula evaluates to t.

Write \( \models_I A \)

A is valid (a tautology) if every interpretation satisfies A.

Write \( \models A \)

S is satisfiable if some interpretation satisfies every formula in S.

Implication, Entailment, Equivalence

A → B means simply \( \neg A \lor B \).

A \models B means if \( \models_I A \) then \( \models_I B \) for every interpretation I.

A \models B if and only if \( \models A \rightarrow B \).

Equivalence

A \simeq B means A \models B and B \models A.

A \simeq B if and only if \( \models A \leftrightarrow B \).
**Equivalences**

\[
\begin{align*}
A \land A & \simeq A \\
A \land B & \simeq B \land A \\
(A \land B) \land C & \simeq A \land (B \land C) \\
A \lor (B \land C) & \simeq (A \lor B) \land (A \lor C) \\
A \land f & \simeq f \\
A \land t & \simeq A \\
A \land \neg A & \simeq f
\end{align*}
\]

Dual versions: exchange \land with \lor and \text{t} with \text{f} in any equivalence

**Negation Normal Form**

1. Get rid of \iff and \implies, leaving just \land, \lor, \neg:

\[
\begin{align*}
A \iff B & \simeq (A \implies B) \land (B \implies A) \\
A \implies B & \simeq \neg A \lor B
\end{align*}
\]

2. Push negations in, using de Morgan’s laws:

\[
\begin{align*}
\neg\neg A & \simeq A \\
\neg(A \land B) & \simeq \neg A \lor \neg B \\
\neg(A \lor B) & \simeq \neg A \land \neg B
\end{align*}
\]
From NNF to Conjunctive Normal Form

3. Push disjunctions in, using distributive laws:

\[ A \lor (B \land C) \simeq (A \lor B) \land (A \lor C) \]
\[ (B \land C) \lor A \simeq (B \lor A) \land (C \lor A) \]

4. Simplify:
   - Delete any disjunction containing \( P \) and \( \neg P \)
   - Delete any disjunction that includes another: for example, in \( (P \lor Q) \land P \), delete \( P \lor Q \).
   - Replace \( (P \lor A) \land (\neg P \lor A) \) by \( A \)

Converting a Non-Tautology to CNF

1. Elim \( \rightarrow \): \( \neg (P \lor Q) \lor (Q \lor R) \)

2. Push \( \neg \) in: \( (\neg P \land \neg Q) \lor (Q \lor R) \)

3. Push \( \lor \) in: \( (\neg P \lor Q \lor R) \land (\neg Q \lor Q \lor R) \)

4. Simplify: \( \neg P \lor Q \lor R \)

Not a tautology: try \( P \mapsto t \), \( Q \mapsto f \), \( R \mapsto f \)
Tautology checking using CNF

\[(P \rightarrow Q) \rightarrow P\]

1. Elim \(\rightarrow\): \(\neg[\neg\neg(P \lor Q) \lor P] \lor P\)

2. Push \(\neg\) in: \([\neg\neg(P \lor Q) \land \neg P] \lor P\)
   \([\neg\neg(P \lor Q) \land \neg P] \lor P\]

3. Push \(\lor\) in: \((\neg P \lor Q \lor P) \land (\neg P \lor P)\)

4. Simplify: \(t \land t\)
   \(t\)
   \(It's\ a\ tautology!\)
A Simple Proof System

Axiom Schemes

K \[ A \rightarrow (B \rightarrow A) \]

S \[ (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) \]

DN \[ \neg
\neg A \rightarrow A \]

Inference Rule: Modus Ponens

\[
\frac{A \rightarrow B \quad A}{B}
\]

A Simple (?) Proof of \( A \rightarrow A \)

\[
(A \rightarrow ((D \rightarrow A) \rightarrow A)) \rightarrow
\]

\[
(((A \rightarrow (D \rightarrow A)) \rightarrow (A \rightarrow A)) \quad \text{by S}
\]

\[
A \rightarrow ((D \rightarrow A) \rightarrow A) \quad \text{by K}
\]

\[
(A \rightarrow (D \rightarrow A)) \rightarrow (A \rightarrow A) \quad \text{by MP, (1), (2)}
\]

\[
A \rightarrow (D \rightarrow A) \quad \text{by K}
\]

\[
A \rightarrow A \quad \text{by MP, (3), (4)}
\]
### Some Facts about Deducibility

A is *deducible from* the set $S$ if there is a finite proof of $A$ starting from elements of $S$. Write $S \vdash A$.

**Soundness Theorem.** If $S \vdash A$ then $S \models A$.

**Completeness Theorem.** If $S \models A$ then $S \vdash A$.

**Deduction Theorem.** If $S \cup \{A\} \vdash B$ then $S \vdash A \rightarrow B$.

### Gentzen’s Natural Deduction Systems

The context of *assumptions* may vary.

Each logical connective is defined *independently*.

The *introduction* rule for $\land$ shows how to deduce $A \land B$:

\[
\frac{A \quad B}{A \land B}
\]

The *elimination* rules for $\land$ shows what to deduce *from* $A \land B$:

\[
\frac{A \land B}{A} \quad \frac{A \land B}{B}
\]
The Sequent Calculus

Sequent \( A_1, \ldots, A_m \Rightarrow B_1, \ldots, B_n \) means,

if \( A_1 \land \ldots \land A_m \) then \( B_1 \lor \ldots \lor B_n \)

\( A_1, \ldots, A_m \) are assumptions; \( B_1, \ldots, B_n \) are goals

\( \Gamma \) and \( \Delta \) are sets in \( \Gamma \Rightarrow \Delta \)

The sequent \( A, \Gamma \Rightarrow A, \Delta \) is trivially true (basic sequent).

Sequent Calculus Rules

\[ \frac{\Gamma \Rightarrow \Delta, A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \quad \text{(cut)} \]

\[ \frac{\Gamma \Rightarrow \Delta, A}{\neg A, \Gamma \Rightarrow \Delta} \quad \text{(-l)} \]

\[ \frac{\neg A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg A} \quad \text{(-r)} \]

\[ \frac{\Gamma \Rightarrow \Delta, A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, A \land B} \quad \text{(\land r)} \]

\[ \frac{\Gamma \Rightarrow \Delta, A \land B, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \quad \text{(\land l)} \]
More Sequent Calculus Rules

\[
egin{align*}
A, \Gamma & \Rightarrow \Delta \quad B, \Gamma & \Rightarrow \Delta \\
\frac{}{A \lor B, \Gamma \Rightarrow \Delta} & \quad \frac{\Gamma \Rightarrow \Delta, A, B}{\Gamma \Rightarrow \Delta, A \lor B} \quad (\lor l) \quad (\lor r) \\
\Gamma & \Rightarrow \Delta, A \quad B, \Gamma & \Rightarrow \Delta \\
\frac{}{A \rightarrow B, \Gamma \Rightarrow \Delta} & \quad \frac{A, \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \rightarrow B} \quad (\rightarrow l) \quad (\rightarrow r)
\end{align*}
\]

Easy Sequent Calculus Proofs

\[
egin{align*}
A, B & \Rightarrow A \\
\frac{}{A \land B \Rightarrow A} & \quad \rightarrow (A \land B) \rightarrow A \quad (\land l) \quad (\rightarrow r)
\end{align*}
\]

\[
egin{align*}
A, B & \Rightarrow B, A \\
\frac{}{A \Rightarrow B, B \rightarrow A} & \quad \rightarrow A \rightarrow B, B \rightarrow A \quad (\rightarrow r) \quad (\lor r)
\end{align*}
\]

\[
\Rightarrow (A \rightarrow B) \lor (B \rightarrow A)
\]

Lawrence C. Paulson
University of Cambridge
Part of a Distributive Law

\[
\begin{align*}
A \Rightarrow A, B & \quad \text{similar} \\
B, C \Rightarrow A, B & \quad (\land I) \\
A \land (B \land C) \Rightarrow A, B & \quad (\lor I) \\
A \lor (B \land C) \Rightarrow A \lor B & \quad (\lor I) \\
A \lor (B \land C) \Rightarrow (A \lor B) \land (A \lor C) & \quad (\land I)
\end{align*}
\]

Second subtree proves \( A \lor (B \land C) \Rightarrow A \lor C \) similarly

A Failed Proof

\[
\begin{align*}
A \Rightarrow B, C & \quad B \Rightarrow B, C \quad (\lor I) \\
A \lor B \Rightarrow B, C & \quad (\lor I) \\
A \lor B \Rightarrow B \lor C & \quad (\lor I) \\
\Rightarrow (A \lor B) \rightarrow (B \lor C) & \quad (\rightarrow I)
\end{align*}
\]

\( A \leftrightarrow t, B \leftrightarrow f, C \leftrightarrow f \) falsifies unproved sequent!
Outline of First-Order Logic

Reasons about functions and relations over a set of individuals:

\[
\text{father(father}(x)) = \text{father(father}(y))
\]
\[
\text{cousin}(x, y)
\]

Reasons about all and some individuals:

All men are mortal Socrates is a man
Socrates is mortal

Cannot reason about all functions or all relations, etc.

Function Symbols; Terms

Each function symbol stands for an \( n \)-place function.

A constant symbol is a 0-place function symbol.

A variable ranges over all individuals.

A term is a variable, constant or a function application

\[
f(t_1, \ldots, t_n)
\]

where \( f \) is an \( n \)-place function symbol and \( t_1, \ldots, t_n \) are terms.

We choose the language, adopting any desired function symbols.

Lawrence C. Paulson University of Cambridge
Relation Symbols; Formulae

Each *relation symbol* stands for an $n$-place relation.

*Equality* is the 2-place relation symbol $=$

An *atomic formula* has the form $R(t_1, \ldots, t_n)$ where $R$ is an $n$-place relation symbol and $t_1, \ldots, t_n$ are terms.

A *formula* is built up from atomic formulæ using $\neg$, $\land$, $\lor$, and so forth.

Later, we can add *quantifiers*.

The Power of Quantifier-Free FOL

It is surprisingly expressive, if we include strong induction rules.

It is easy to equivalence of mathematical functions:

\[
\begin{align*}
p(z, 0) &= 1 & q(z, 1) &= z \\
p(z, n + 1) &= p(z, n) \times z & q(z, 2 \times n) &= q(z \times z, n) \\
& & q(z, 2 \times n + 1) &= q(z \times z, n) \times z
\end{align*}
\]

The prover ACL2 uses this logic and has been used in major hardware proofs.
**Universal and Existential Quantifiers**

∀x A  for all x, the formula A holds

∃x A  there exists x such that A holds

*Syntactic variations:*

∀xyz A abbreviates ∀x ∀y ∀z A

∀z . A ∧ B is an alternative to ∀z (A ∧ B)

The variable x is *bound* in ∀x A; compare with ∫ f(x) dx

---

**The Expressiveness of Quantifiers**

*All men are mortal:*

∀x (man(x) → mortal(x))

*All mothers are female:*

∀x female(mother(x))

*There exists a unique x such that A, sometimes written ∃!x A*

∃x [A(x) ∧ ∀y (A(y) → y = x)]
The Point of Semantics

We have to attach meanings to symbols like 1, +, <, etc.

*Why is this necessary? Why can’t 1 just mean 1??*

The point is that mathematics derives its flexibility from allowing different interpretations of symbols.

- A group has a unit 1, a product \( x \cdot y \) and inverse \( x^{-1} \).
- In the most important uses of groups, 1 isn’t a number but a ‘unit permutation’, ‘unit rotation’, etc.

Constants: Interpreting mortal(Socrates)

An interpretation \( \mathcal{I} = (D, I) \) defines the semantics of a first-order language.

D is a non-empty set, called the domain or universe.

I maps symbols to ‘real’ elements, functions and relations:

- c a constant symbol \( I[c] \in D \)
- f an \( n \)-place function symbol \( I[f] \in D^n \rightarrow D \)
- P an \( n \)-place relation symbol \( I[P] \in D^n \rightarrow \{t, f\} \)
A valuation $V : \text{variables} \to D$ supplies the values of free variables.

An interpretation $I$ and valuation function $V$ jointly specify the value of any term $t$ by the obvious recursion.

This value is written $I_V[t]$, and here are the recursion rules:

$\begin{align*}
I_V[x] & \overset{\text{def}}{=} V(x) \quad \text{if } x \text{ is a variable} \\
I_V[c] & \overset{\text{def}}{=} I[c] \\
I_V[f(t_1, \ldots, t_n)] & \overset{\text{def}}{=} I[f](I_V[t_1], \ldots, I_V[t_n])
\end{align*}$

An interpretation $I$ and valuation function $V$ similarly specify the truth value ($t$ or $f$) of any formula $\Lambda$.

Quantifiers are the only problem, as they bind variables.

$V[\alpha/x]$ is the valuation that maps $x$ to $\alpha$ and is otherwise like $V$.

With the help of $V[\alpha/x]$, we now formally define $\models_{I,V} \Lambda$, the truth value of $\Lambda$. 
The Meaning of Truth—In FOL!

For interpretation $\mathcal{I}$ and valuation $\mathcal{V}$, define $\models_{\mathcal{I}, \mathcal{V}}$ by recursion.

- $\models_{\mathcal{I}, \mathcal{V}} P(t)$ if $\mathcal{I}[t] \in \mathcal{I}[P]$ holds
- $\models_{\mathcal{I}, \mathcal{V}} t = u$ if $\mathcal{I}[t]$ equals $\mathcal{I}[u]$
- $\models_{\mathcal{I}, \mathcal{V}} A \land B$ if $\models_{\mathcal{I}, \mathcal{V}} A$ and $\models_{\mathcal{I}, \mathcal{V}} B$
- $\models_{\mathcal{I}, \mathcal{V}} \exists x A$ if $\models_{\mathcal{I}, \mathcal{V}(m/x)} A$ holds for some $m \in D$

Finally, we define

- $\models_{\mathcal{I}} A$ if $\models_{\mathcal{I}, \mathcal{V}} A$ holds for all $\mathcal{V}$.

Formula $A$ is *satisfiable* if $\models_{\mathcal{I}} A$ for some $\mathcal{I}$. 
Slide 501

**Free vs Bound Variables**

All occurrences of \( x \) in \( \forall x \, A \) and \( \exists x \, A \) are **bound**

An occurrence of \( x \) is **free** if it is not bound:

\[
\forall y \, \exists z \, R(y, z, f(y, x))
\]

In this formula, \( y \) and \( z \) are bound while \( x \) is free.

May rename bound variables:

\[
\forall w \, \exists z' \, R(w, z', f(w, x))
\]

Slide 502

**Substitution for Free Variables**

\( A[t/x] \) means **substitute** \( t \) **for** \( x \) in \( A \):

\[
\begin{align*}
(B \land C)[t/x] & \quad \text{is} \quad B[t/x] \land C[t/x] \\
(\forall x \, B)[t/x] & \quad \text{is} \quad \forall x \, B \\
(\forall y \, B)[t/x] & \quad \text{is} \quad \forall y \, B[t/x] \quad (x \neq y) \\
(P(u))[t/x] & \quad \text{is} \quad P(u[t/x])
\end{align*}
\]

With \( A[t/x] \), no variable of \( t \) may be bound in \( A \)!

\[
(\forall y \, (x = y))[y/x] \quad \text{IS NOT EQUIVALENT TO} \quad \forall y \, (y = y)
\]
Some Equivalences for Quantifiers

\( \neg(\forall x \ A) \simeq \exists x \ \neg A \)

\( \forall x \ A \simeq \forall x \ A \land A[t/x] \)

\((\forall x \ A) \land (\forall x \ B) \simeq \forall x (A \land B) \)

But we do not have \((\forall x \ A) \lor (\forall x \ B) \simeq \forall x (A \lor B)\).

Dual versions: exchange \( \forall \) with \( \exists \) and \( \land \) with \( \lor \)

Further Quantifier Equivalences

These hold only if \( x \) is not free in \( B \).

\((\forall x \ A) \land B \simeq \forall x (A \land B) \)

\((\forall x \ A) \lor B \simeq \forall x (A \lor B) \)

\((\forall x \ A) \rightarrow B \simeq \exists x (A \rightarrow B) \)

These let us expand or contract a quantifier's scope.
Reasoning by Equivalences

\[ \exists x \left( x = a \land P(x) \right) \simeq \exists x \left( x = a \land P(a) \right) \]
\[ \simeq \exists x \left( x = a \right) \land P(a) \]
\[ \simeq P(a) \]

\[ \exists z \left( P(z) \rightarrow P(a) \land P(b) \right) \]
\[ \simeq \forall z \ P(z) \rightarrow P(a) \land P(b) \]
\[ \simeq \forall z \ P(z) \land P(a) \land P(b) \rightarrow P(a) \land P(b) \]
\[ \simeq t \]

Sequent Calculus Rules for \( \forall \)

\[ \frac{\Lambda[t/x], \Gamma \Rightarrow \Delta}{\forall x \ A, \Gamma \Rightarrow \Delta} \quad (\forall l) \quad \frac{\Gamma \Rightarrow \Delta, A}{\Gamma \Rightarrow \Delta, \forall x \ A} \quad (\forall r) \]

Rule (\( \forall l \)) can create many instances of \( \forall x \ A \)

Rule (\( \forall r \)) holds provided \( x \) is not free in the conclusion!

NOT allowed to prove

\[ \frac{P(y) \Rightarrow P(y)}{P(y) \Rightarrow \forall y \ P(y)} \quad (\forall r) \quad \text{THIS IS NONSENSE!} \]
A Simple Example of the $\forall$ Rules

\[
\begin{align*}
P(f(y)) &\Rightarrow P(f(y)) \\ \forall x \ P(x) &\Rightarrow P(f(y)) \\ \forall x \ P(x) &\Rightarrow \forall y \ P(f(y))
\end{align*}
\]

Slide 507

A Not-So-Simple Example of the $\forall$ Rules

\[
\begin{align*}
P &\Rightarrow Q(y), \ P \\ P, Q(y) &\Rightarrow Q(y) \\ P, \ P \rightarrow Q(y) &\Rightarrow Q(y) \\ P, \ \forall x (P \rightarrow Q(x)) &\Rightarrow Q(y) \\ P, \ \forall x (P \rightarrow Q(x)) &\Rightarrow \forall y Q(y) \\ \forall x (P \rightarrow Q(x)) &\Rightarrow P \rightarrow \forall y Q(y)
\end{align*}
\]

\[
\begin{align*}
P &\Rightarrow Q(y), \ P, Q(y) \\ P, Q(y) &\Rightarrow Q(y) \\ P, P \rightarrow Q(y) &\Rightarrow Q(y) \\ P, \ P \rightarrow Q(y) &\Rightarrow \forall y Q(y) \\ \forall x (P \rightarrow Q(x)) &\Rightarrow P \rightarrow \forall y Q(y)
\end{align*}
\]

\[
\begin{align*}
P &\Rightarrow Q(y), \ P, Q(y) \\ P, Q(y) &\Rightarrow Q(y) \\ P, P \rightarrow Q(y) &\Rightarrow Q(y) \\ P, \ P \rightarrow Q(y) &\Rightarrow \forall y Q(y) \\ \forall x (P \rightarrow Q(x)) &\Rightarrow P \rightarrow \forall y Q(y)
\end{align*}
\]

\[
\begin{align*}
P &\Rightarrow Q(y), \ P, Q(y) \\ P, Q(y) &\Rightarrow Q(y) \\ P, P \rightarrow Q(y) &\Rightarrow Q(y) \\ P, \ P \rightarrow Q(y) &\Rightarrow \forall y Q(y) \\ \forall x (P \rightarrow Q(x)) &\Rightarrow P \rightarrow \forall y Q(y)
\end{align*}
\]

In $(\forall l)$, we must replace $x$ by $y$.

Lawrence C. Paulson

University of Cambridge
Sequent Calculus Rules for $\exists$

\[
\frac{\Lambda, \Gamma \Rightarrow \Delta}{\exists x \; \Lambda, \Gamma \Rightarrow \Delta} \quad (\exists l) \quad \frac{\Gamma \Rightarrow \Delta, A[t/x]}{\Gamma \Rightarrow \Delta, \exists x \; A} \quad (\exists r)
\]

Rule $\exists l$ holds provided $x$ is not free in the conclusion!

Rule $\exists r$ can create many instances of $\exists x \; A$

For example, to prove this counter-intuitive formula:

\[
\exists z \; (P(z) \rightarrow P(a) \land P(b))
\]

Part of the $\exists$ Distributive Law

\[
\frac{P(x) \Rightarrow P(x), Q(x)}{P(x) \Rightarrow P(x) \lor Q(x)} \quad (\lor r) \quad \frac{P(x) \Rightarrow \exists y \; (P(y) \lor Q(y))}{\exists x \; P(x) \Rightarrow \exists y \; (P(y) \lor Q(y))} \quad (\exists l)
\]

Similar

\[
\frac{\exists x \; Q(x) \Rightarrow \exists y \; (P(y) \lor Q(y)) \ldots}{\exists x \; P(x) \lor \exists x \; Q(x) \Rightarrow \exists y \; (P(y) \lor Q(y))} \quad \lor l
\]

Second subtree proves $\exists x \; Q(x) \Rightarrow \exists y \; (P(y) \lor Q(y))$ similarly

In $\exists r$, we must replace $y$ by $x$. 

Lawrence C. Paulson  
University of Cambridge
A Failed Proof

\[
\begin{align*}
P(x), Q(y) &\Rightarrow P(x) \land Q(x) \\
P(x), Q(y) &\Rightarrow \exists z \, (P(z) \land Q(z)) \quad (\exists r) \\
P(x), \exists x \, Q(x) &\Rightarrow \exists z \, (P(z) \land Q(z)) \quad (\exists l) \\
\exists x \, P(x), \exists x \, Q(x) &\Rightarrow \exists z \, (P(z) \land Q(z)) \quad (\exists l) \\
\exists x \, P(x) \land \exists x \, Q(x) &\Rightarrow \exists z \, (P(z) \land Q(z)) \quad (\land 1)
\end{align*}
\]

We cannot use (\exists l) twice with the same variable

This attempt renames the x in \exists Q(x), to get \exists y \, Q(y)
**Clause Form**

Clause: a disjunction of literals

\[ \neg K_1 \lor \cdots \lor \neg K_m \lor L_1 \lor \cdots \lor L_n \]

Set notation: \( \{\neg K_1, \ldots, \neg K_m, L_1, \ldots, L_n\} \)

Kowalski notation: \( K_1, \ldots, K_m \rightarrow L_1, \ldots, L_n \)
\( L_1, \ldots, L_n \leftarrow K_1, \ldots, K_m \)

Empty clause: \( \Box \)

Empty clause is equivalent to \( f \), meaning CONTRADICTION!

---

**Outline of Clause Form Methods**

To prove \( A \), obtain a contradiction from \( \neg A \):

1. Translate \( \neg A \) into CNF as \( \Lambda_1 \land \cdots \land \Lambda_m \)
2. This is the set of clauses \( \Lambda_1, \ldots, \Lambda_m \)
3. Transform the clause set, preserving consistency

Deducing the empty clause refutes \( \neg A \).

An empty clause set (all clauses deleted) means \( \neg A \) is satisfiable.

The basis for SAT SOLVERS and RESOLUTION PROVERS.
The Davis-Putnam-Logeman-Loveland Method

1. Delete tautological clauses: \{P, \neg P, \ldots\}

2. For each unit clause \{L\},
   - delete all clauses containing L
   - delete \neg L from all clauses

3. Delete all clauses containing pure literals

4. Perform a case split on some literal

DPLL is a decision procedure: it finds a contradiction or a model.

Davis-Putnam on a Non-Tautology

Consider \(P \lor Q \rightarrow Q \lor R\)

Clauses are \{P, Q\} \{\neg Q\} \{\neg R\}

\{P, Q\} \{\neg Q\} \{\neg R\} initial clauses
\{P\} \{\neg R\} unit \neg Q
\{\neg R\} unit P (also pure)
unit \neg R (also pure)

Clauses satisfiable by \(P \leftrightarrow t\), \(Q \leftrightarrow f\), \(R \leftrightarrow f\)

Lawrence C. Paulson
University of Cambridge
Example of a Case Split on $P$

\[
\begin{array}{llllll}
\{\neg Q, R\} & \{\neg R, P\} & \{\neg R, Q\} & \{\neg P, Q, R\} & \{P, Q\} & \{\neg P, \neg Q\} \\
\{\neg Q, R\} & \{\neg R, Q\} & \{Q, R\} & \{\neg Q\} & \text{if } P \text{ is true} \\
\{\neg R\} & \{R\} & \text{unit } \neg Q \\
\hline
\{\neg Q, R\} & \{\neg R\} & \{\neg R, Q\} & \{Q\} & \text{if } P \text{ is false} \\
\{\neg Q\} & \{Q\} & \text{unit } \neg R \\
\hline
\end{array}
\]

\[
\begin{array}{ll}
\square & \text{unit } \neg Q \\
\end{array}
\]

\[
\begin{array}{ll}
\square & \text{unit } \neg R \\
\end{array}
\]

SAT solvers in the Real World

- Progressed from joke to killer technology in 10 years.
- Princeton’s zChaff has solved problems with more than one million variables and 10 million clauses.
- Applications include finding bugs in device drivers (Microsoft’s SLAM project).
- Typical approach: approximate the problem with a finite model; encode it using Boolean logic; supply to a SAT solver.
### The Resolution Rule

From $B \lor A$ and $\neg B \lor C$ infer $A \lor C$

In set notation,

$$\frac{\{B, A_1, \ldots, A_m\} \quad \{\neg B, C_1, \ldots, C_n\}}{\{A_1, \ldots, A_m, C_1, \ldots, C_n\}}$$

Some special cases:

$$\frac{\{B\} \quad \{\neg B, C_1, \ldots, C_n\}}{\{C_1, \ldots, C_n\}}$$

$$\frac{\{B\} \quad \{\neg B\}}{\square}$$

### Simple Example: Proving $P \land Q \rightarrow Q \land P$

*Hint:* use $\neg(A \rightarrow B) \simeq A \land \neg B$

1. Negate! $\neg[P \land Q \rightarrow Q \land P]$
2. Push $\neg$ in: $(P \land Q) \land \neg(Q \land P)$
   
   $(P \land Q) \land (\neg Q \lor \neg P)$

Clauses:

$$\{P\} \quad \{Q\} \quad \{\neg Q, \neg P\}$$

Resolve $\{P\}$ and $\{\neg Q, \neg P\}$ getting $\{\neg Q\}$.

Resolve $\{Q\}$ and $\{\neg Q\}$ getting $\square$: we have refuted the negation.

Lawrence C. Paulson  
University of Cambridge
Another Example

Refute $\neg[(P \lor Q) \land (P \lor R) \rightarrow P \lor (Q \land R)]$

From $(P \lor Q) \land (P \lor R)$, get clauses $\{P, Q\}$ and $\{P, R\}$.

From $\neg [P \lor (Q \land R)]$ get clauses $\{\neg P\}$ and $\{\neg Q, \neg R\}$.

Resolve $\{\neg P\}$ and $\{P, Q\}$ getting $\{Q\}$.

Resolve $\{\neg P\}$ and $\{P, R\}$ getting $\{R\}$.

Resolve $\{Q\}$ and $\{\neg Q, \neg R\}$ getting $\{\neg R\}$.

Resolve $\{R\}$ and $\{\neg R\}$ getting $\square$, contradiction.

The Saturation Algorithm

At start, all clauses are passive. None are active.

1. Transfer a clause (current) from passive to active.

2. Form all resolvents between current and an active clause.

3. Use new clauses to simplify both passive and active.

4. Put the new clauses into passive.

Repeat until CONTRADICTION found or passive becomes empty.
Heuristics and Hacks for Resolution

Orderings to focus the search on specific literals

Subsumption, or deleting redundant clauses

Indexing: elaborate data structures for speed

Preprocessing: removing tautologies, symmetries . . .

Weighting: giving priority to “good” clauses over those containing unwanted constants
Reducing FOL to Propositional Logic

- **Prenex**: Move quantifiers to the front
- **Skolemize**: Remove quantifiers, preserving consistency
- **Herbrand models**: Reduce the class of interpretations
- **Herbrand’s Thm**: Contradictions have finite, ground proofs
- **Unification**: Automatically find the right instantiations

Finally, combine unification with *resolution*.

---

Prenex Normal Form

*Convert to Negation Normal Form using additionally*

\[ \neg (\forall x \ A) \Leftrightarrow \exists x \neg A \]
\[ \neg (\exists x \ A) \Leftrightarrow \forall x \neg A \]

*Move quantifiers to the front using (provided x is not free in B)*

\[ (\forall x \ A) \land B \Leftrightarrow \forall x (A \land B) \]
\[ (\forall x \ A) \lor B \Leftrightarrow \forall x (A \lor B) \]

and the similar rules for \( \exists \)
Skolemization, or Getting Rid of \( \exists \)

Start with a formula of the form 

\[
\forall x_1 \forall x_2 \cdots \forall x_k \exists y \ A
\]

(Can have \( k = 0 \)).

Choose a fresh \( k \)-place function symbol, say \( f \)

Delete \( \exists y \) and replace \( y \) by \( f(x_1, x_2, \ldots, x_k) \). We get

\[
\forall x_1 \forall x_2 \cdots \forall x_k A[f(x_1, x_2, \ldots, x_k)/y]
\]

Repeat until no \( \exists \) quantifiers remain

Example of Conversion to Clauses

For proving \( \exists x \ [P(x) \rightarrow \forall y \ P(y)] \)

\[
\neg [\exists x \ [P(x) \rightarrow \forall y \ P(y)]] \quad \text{negated goal}
\]

\[
\forall x \ [P(x) \land \exists y \ \neg P(y)] \quad \text{conversion to NNF}
\]

\[
\forall x \ \exists y \ [P(x) \land \neg P(y)] \quad \text{pulling } \exists \text{ out}
\]

\[
\forall x \ [P(x) \land \neg P(f(x))] \quad \text{Skolem term } f(x)
\]

\( \{P(x)\} \quad \{\neg P(f(x))\} \quad \text{Final clauses} \)
Correctness of Skolemization

The formula $\forall x \exists y \ A$ is consistent

$\iff$ it holds in some interpretation $I = (D, I)$

$\iff$ for all $x \in D$ there is some $y \in D$ such that $A$ holds

$\iff$ some function $\hat{f}$ in $D \to D$ yields suitable values of $y$

$\iff$ $A[f(x)/y]$ holds in some $I'$ extending $I$ so that $f$ denotes $\hat{f}$

$\iff$ the formula $\forall x A[f(x)/y]$ is consistent.

Don’t panic if you can’t follow this reasoning!

Simplifying the Search for Models

$S$ is satisfiable if even one model makes all of its clauses true.

There are infinitely many models to consider!

Also many duplicates: “states of the USA” and “the integers 1 to 50”

Fortunately, nice models exist.

- They have a uniform structure based on the language’s syntax.
- They satisfy the clauses if any model does.
The Herbrand Universe for a Set of Clauses $S$

$H_0 \overset{\text{def}}{=} \text{the set of constants in } S \text{ (must be non-empty)}$

$H_{i+1} \overset{\text{def}}{=} H_i \cup \{f(t_1, \ldots, t_n) \mid t_1, \ldots, t_n \in H_i \text{ and } f \text{ is an } n\text{-place function symbol in } S\}$

$H \overset{\text{def}}{=} \bigcup_{i \geq 0} H_i \quad \text{Herbrand Universe}$

$H_i$ contains just the terms with at most $i$ nested function applications.

$H$ consists of the terms in $S$ that contain no variables (ground terms).

The Herbrand Semantics of Terms

In a Herbrand model, every constant stands for itself.

Every function symbol stands for a term-forming operation:

$f$ denotes the function that puts ‘$f$’ in front of the given arguments.

In a Herbrand model, $X + 0$ can never equal $X$.

Every ground term denotes itself.

This is the promised uniform structure!
The Herbrand Semantics of Predicates

\( \text{HB} \overset{\text{def}}{=} \{ P(t_1, \ldots, t_n) \mid t_1, \ldots, t_n \in H \) 

\text{and P is an n-place predicate symbol in S} \}

HB contains all \textit{ground atoms}: predicates applied to ground terms.

We view a ground atom as stating that the formula is true.

In a Herbrand model, each predicate \( P \) stands for

\textit{the set of ground atoms} \( P(x) \) \textit{that we want to be true}.

We can make whatever we want true!

---

Example of an Herbrand Model

\[-\text{even}(1) \]
\[
\text{even}(2)
\]
\[
\text{even}(X \cdot Y) \leftarrow \text{even}(X), \text{even}(Y)
\]

\( H = \{1, 2, 1 \cdot 1, 1 \cdot 2, 2 \cdot 1, 2 \cdot 2, 1 \cdot (1 \cdot 1), \ldots\} \)

\( \text{HB} = \{\text{even}(1), \text{even}(2), \text{even}(1 \cdot 1), \text{even}(1 \cdot 2), \ldots\} \)

\( I[\text{even}] = \{\text{even}(2), \text{even}(1 \cdot 2), \text{even}(2 \cdot 1), \text{even}(2 \cdot 2), \ldots\} \)

\text{(for model where \( \cdot \) means product; could instead use sum!)}
A Key Fact about Herbrand Interpretations

Let $S$ be a set of clauses.

$S$ is unsatisfiable $\iff$ no Herbrand interpretation satisfies $S$

- Holds because some Herbrand model mimics every ‘real’ model
- We must consider only a small class of models
- Herbrand models are syntactic, easily processed by computer

Herbrand’s Theorem

Let $S$ be a set of clauses.

$S$ is unsatisfiable $\iff$ there is a finite unsatisfiable set $S'$ of ground instances of clauses of $S$.

- Finite: we can compute it
- Instance: result of substituting for variables
- Ground: no variables remain—it’s propositional!

Example: $S$ could be $\{P(x)\}$ $\{\neg P(f(y))\}$,
and $S'$ could be $\{P(f(a))\}$ $\{\neg P(f(a))\}$.
Unification

Finding a common instance of two terms. Lots of applications:

- **Prolog** and other logic programming languages
- **Theorem proving**: resolution and other procedures
- Tools for reasoning with **equations**
- Tools for satisfying multiple **constraints**
- Polymorphic type-checking (**ML** and other functional languages)

It’s an intuitive generalization of pattern-matching.

Substitutions: A Mathematical Treatment

A substitution is a finite set of replacements

\[ \theta = [t_1/x_1, \ldots, t_k/x_k] \]

where \( x_1, \ldots, x_k \) are distinct variables and \( t_i \neq x_i \).

\[ f(t, u)\theta = f(t\theta, u\theta) \quad \text{(substitution in terms)} \]
\[ P(t, u)\theta = P(t\theta, u\theta) \quad \text{(in literals)} \]
\[ \{L_1, \ldots, L_m\}\theta = \{L_1\theta, \ldots, L_m\theta\} \quad \text{(in clauses)} \]
Composing Substitutions

Composition of $\phi$ and $\theta$, written $\phi \circ \theta$, satisfies for all terms $t$

$$t(\phi \circ \theta) = (t\phi)\theta$$

It is defined by (for all relevant $x$)

$$\phi \circ \theta \overset{\text{def}}{=} [(x\phi)\theta / x, \ldots]$$

Consequences include $\theta \circ [] = \theta$, and associativity:

$$(\phi \circ \theta) \circ \sigma = \phi \circ (\theta \circ \sigma)$$

Most General Unifiers

$\theta$ is a unifier of terms $t$ and $u$ if $t\theta = u\theta$.

$\theta$ is more general than $\phi$ if $\phi = \theta \circ \sigma$ for some substitution $\sigma$.

$\theta$ is most general if it is more general than every other unifier.

If $\theta$ unifies $t$ and $u$ then so does $\theta \circ \sigma$:

$$t(\theta \circ \sigma) = t\theta\sigma = u\theta\sigma = u(\theta \circ \sigma)$$

A most general unifier of $f(a, x)$ and $f(y, g(z))$ is $[a/y, g(z)/x]$.

The common instance is $f(a, g(z))$. 

Lawrence C. Paulson

University of Cambridge
The Unification Algorithm

Represent terms by binary trees.

Each term is a Variable x, y . . ., Constant a, b . . ., or Pair (t, t’)

Sketch of the Algorithm.

Constants do not unify with different Constants.

Constants do not unify with Pairs.

Variable x and term t: unifier is \([t/x]\), unless x occurs in t

Cannot unify \(f(x)\) with x!

The Unification Algorithm: The Case of Two Pairs

\(\theta \circ \theta'\) unifies (t, t’) with (u, u’)

if \(\theta\) unifies t with u and \(\theta'\) unifies t’\(\theta\) with u’\(\theta\).

*We unify the left sides, then the right sides.*

In an implementation, substitutions are formed by updating pointers.

Composition happens automatically as more pointers are updated.
Mathematical justification

It's easy to check that $\theta \circ \theta'$ unifies $(t, t')$ with $(u, u')$:

$$(t, t')(\theta \circ \theta') = (t, t')\theta\theta'$$

$$= (t\theta\theta', t'\theta\theta')$$

$$= (u\theta\theta', u'\theta\theta')$$

$$= (u, u')\theta\theta'$$

$$= (u, u')(\theta \circ \theta')$$

$\theta \circ \theta'$ is even a most general unifier, if $\theta$ and $\theta'$ are!

Four Unification Examples

<table>
<thead>
<tr>
<th></th>
<th>f(x, b)</th>
<th>f(x, x)</th>
<th>f(x, x)</th>
<th>j(x, x, z)</th>
</tr>
</thead>
<tbody>
<tr>
<td>f(a, y)</td>
<td>f(a, y)</td>
<td>f(a, b)</td>
<td>f(y, g(y))</td>
<td>j(w, a, h(w))</td>
</tr>
<tr>
<td>f(a, b)</td>
<td>None</td>
<td>None</td>
<td>j(a, a, h(a))</td>
<td></td>
</tr>
<tr>
<td>[a/x, b/y]</td>
<td>Fail</td>
<td>Fail</td>
<td>[a/w, a/x, h(a)/z]</td>
<td></td>
</tr>
</tbody>
</table>

Remember, the output is a substitution.

The algorithm yields a most general unifier.
Theorem-Proving Example 1

\((\exists y \forall x R(x, y)) \rightarrow (\forall x \exists y R(x, y))\)

After negation, the clauses are \(\{R(x, a)\}\) and \(\{\neg R(b, y)\}\).

The literals \(R(x, a)\) and \(R(b, y)\) have unifier \([b/x, a/y]\).

We have the contradiction \(R(b, a)\) and \(\neg R(b, a)\).

**THEOREM IS PROVED BY CONTRADICTION!**

Theorem-Proving Example 2

\((\forall x \exists y R(x, y)) \rightarrow (\exists y \forall x R(x, y))\)

After negation, the clauses are \(\{R(x, f(x))\}\) and \(\{\neg R(g(y), y)\}\).

The literals \(R(x, f(x))\) and \(R(g(y), y)\) are not unifiable.

(They fail the **occurs check**.)

We can’t get a contradiction. **FORMULA IS NOT A THEOREM!**
Variations on Unification

Efficient unification algorithms: near-linear time

Indexing & Discrimination networks: fast retrieval of a unifiable term

Associative/commutative unification

• Example: unify $a + (y + c)$ with $(c + x) + b$, get $[a/x, b/y]$ 
• Algorithm is very complicated 
• The number of unifiers can be exponential

Unification in many other theories (often undecidable!)
The Binary Resolution Rule

\[
\frac{\{B, A_1, \ldots, A_m\} \quad \{\neg D, C_1, \ldots, C_n\}}{\{A_1, \ldots, A_m, C_1, \ldots, C_n\}\sigma} \quad \text{provided } B\sigma = D\sigma
\]

First, rename variables apart in the clauses! For example, given

\[
\{P(x)\} \quad \text{and} \quad \{\neg P(g(x))\}
\]

rename \(x\) in one of the clauses before attempting unification.

Always use a most general unifier (MGU).

The Factoring Rule

This inference collapses unifiable literals in one clause:

\[
\frac{\{B_1, \ldots, B_k, A_1, \ldots, A_m\}}{\{B_1, A_1, \ldots, A_m\}\sigma} \quad \text{provided } B_1\sigma = \cdots = B_k\sigma
\]

Example: Prove \(\forall x \exists y \neg (P(y, x) \leftrightarrow \neg P(y, y))\)

The clauses are

\[
\{\neg P(y, a), \neg P(y, y)\} \quad \{P(y, y), P(y, a)\}
\]

Factoring yields

\[
\{\neg P(a, a)\} \quad \{P(a, a)\}
\]

Resolution yields the empty clause!
A Non-Trivial Proof

\[ \exists x \left[ P \rightarrow Q(x) \right] \land \exists x \left[ Q(x) \rightarrow P \right] \rightarrow \exists x \left[ P \leftrightarrow Q(x) \right] \]

Clauses are \{P, \neg Q(b)\} \{P, Q(x)\} \{\neg P, \neg Q(x)\} \{\neg P, Q(a)\}

Resolve \{P, \neg Q(b)\} with \{P, Q(x)\} getting \{P, P\}

Factor \{P, P\} getting \{P\}

Resolve \{\neg P, \neg Q(x)\} with \{\neg P, Q(a)\} getting \{\neg P, \neg P\}

Factor \{\neg P, \neg P\} getting \{\neg P\}

Resolve \{P\} with \{\neg P\} getting \Box

What About Equality?

In theory, it’s enough to add the equality axioms:

• The reflexive, symmetric and transitive laws.

• Substitution laws like \{x \neq y, f(x) = f(y)\} for each f.

• Substitution laws like \{x \neq y, \neg P(x), P(y)\} for each P.

In practice, we need something special: the paramodulation rule

\[
\frac{B[t'], A_1, \ldots, A_m}{B[u], A_1, \ldots, A_m, C_1, \ldots, C_n]} \quad (if \ t\sigma = t'\sigma)
\]
Prolog Clauses

Prolog clauses have a restricted form, with \textit{at most one} positive literal. The \textit{definite clauses} form the program. Procedure $B$ with body “commands” $A_1, \ldots, A_m$ is

$$B \leftarrow A_1, \ldots, A_m$$

The single \textit{goal clause} is like the “execution stack”, with say $m$ tasks left to be done.

$$\leftarrow A_1, \ldots, A_m$$

Prolog Execution

\textit{Linear} resolution:

- Always resolve some program clause with the goal clause.
- The result becomes the new goal clause.

Try the program clauses in \textit{left-to-right} order.

Solve the goal clause’s literals in \textit{left-to-right} order.

Use \textit{depth-first search}. (Performs \textit{backtracking}, using little space.)

Do unification without \textit{occurs check}. (UN SOUND, but needed for speed)

Lawrence C. Paulson 
University of Cambridge
A (Pure) Prolog Program

parent(elizabeth, charles).
parent(elizabeth, andrew).

parent(charles, william).
parent(charles, henry).

parent(andrew, beatrice).
parent(andrew, eugenia).

grand(X, Z) :- parent(X, Y), parent(Y, Z).
cousin(X, Y) :- grand(Z, X), grand(Z, Y).

Prolog Execution

:- cousin(X, Y).
    :- grand(Z1, X), grand(Z1, Y).
    :- parent(Z1, Y2), parent(Y2, X), grand(Z1, Y).
    *    :- parent(charles, X), grand(elizabeth, Y).

X = william
    :- grand(elizabeth, Y).
    *    :- parent(elizabeth, Y5), parent(Y5, Y).

Y = beatrice
    :- parent(andrew, Y).

* = backtracking choice point

16 solutions including cousin(william, william)

and cousin(william, henry)
Another FOL Proof Procedure: Model Elimination

A Prolog-like method to run on fast Prolog architectures.

Contrapositives: treat clause \( \{ A_1, \ldots, A_m \} \) like the \( m \) clauses

\[
A_1 \leftarrow \neg A_2, \ldots, \neg A_m \\
A_2 \leftarrow \neg A_3, \ldots, \neg A_m, \neg A_1 \\
\vdots \\
A_m \leftarrow \neg A_1, \ldots, \neg A_{m-1}
\]

Extension rule: when proving goal \( P \), assume \( \neg P \).

A Survey of Automatic Theorem Provers

Saturation (that is, resolution): E, Gandalf, SPASS, Vampire, …

Higher-Order Logic: TPS, LEO

Model Elimination: Prolog Technology Theorem Prover, SETHEO

Parallel ME: PARTHENON, PARTHEO

Tableau (sequent) based: LeanTAP, 3TAP, …
BDDs: Binary Decision Diagrams

A canonical form for boolean expressions: decision trees with sharing.

- ordered propositional symbols (‘variables’)
- sharing of identical subtrees
- hashing and other optimisations

Detects if a formula is tautologous (t) or inconsistent (f).

Exhibits models if the formula is satisfiable.

Excellent for verifying digital circuits, with many other applications.

Decision Diagram for \((P \lor Q) \land R\)
Converting a Decision Diagram to a BDD

P
Q
R
0
1

No duplicates

P
Q
R
0
1

No redundant tests

Building BDDs Efficiently

Do not construct full tree!
Do not expand $\rightarrow, \leftrightarrow, \oplus$ (exclusive OR) to other connectives.
Treat $\neg Z$ as $Z \rightarrow f$ or $Z \oplus t$.
Recursively convert operands to BDDs.
Combine operand BDDs, respecting the ordering and sharing.
Delete redundant variable tests.
Canonical Form Algorithm

To convert $Z \land Z'$, where $Z$ and $Z'$ are already BDDs:

Trivial if either operand is $t$ or $f$.

Let $Z = \text{if}(P, X, Y)$ and $Z' = \text{if}(P', X', Y')$

- If $P = P'$ then recursively convert $\text{if}(P, X \land X', Y \land Y')$.
- If $P < P'$ then recursively convert $\text{if}(P, X \land Z', Y \land Z')$.
- If $P > P'$ then recursively convert $\text{if}(P', Z \land X', Z \land Y')$.

Canonical Forms of Other Connectives

$Z \lor Z'$, $Z \rightarrow Z'$ and $Z \leftrightarrow Z'$ are converted to BDDs similarly.

Some cases, like $Z \rightarrow t$, reduce to negation.

Here is how to convert $\neg Z$, where $Z$ is a BDD:

- If $Z = \text{if}(P, X, Y)$ then recursively convert $\text{if}(P, \neg X, \neg Y)$.
- If $Z = t$ then return $f$, and if $Z = f$ then return $t$.

In effect we copy the BDD but swap $t$ and $f$ at the leaves.
Canonical Form (that is, BDD) of $P \lor Q$

Canonical Form of $P \lor Q \rightarrow Q \lor R$

Lawrence C. Paulson  
University of Cambridge
Optimisations Based On Hash Tables

Never build the same BDD twice, but share pointers. Advantages:

- If $X \simeq Y$, then the addresses of $X$ and $Y$ are equal.
- Can see if $\text{if}(P, X, Y)$ is redundant by checking if $X = Y$.
- Can quickly simplify special cases like $X \land X$.

Never convert $X \land Y$ twice, but keep a table of known canonical forms.

Final Observations

The variable ordering is crucial. Consider this formula:

$$(P_1 \land Q_1) \lor \cdots \lor (P_n \land Q_n)$$

A good ordering is $P_1 < Q_1 < \cdots < P_n < Q_n$: the BDD is linear.

With $P_1 < \cdots < P_n < Q_1 < \cdots < Q_n$, the BDD is exponential.

Many digital circuits have small BDDs: adders, but not multipliers.

BDDs can solve problems in hundreds of variables.

The general case remains hard (it is NP-complete).
Modal Operators

\( W \): set of possible worlds (machine states, future times, . . .)
\( R \): accessibility relation between worlds
\((W, R)\) is called a modal frame

\( \Box A \) means \( A \) is necessarily true \( \rightarrow \) in all accessible worlds
\( \Diamond A \) means \( A \) is possibly true

\( \neg \Diamond A \cong \Box \neg A \) \( A \) cannot be true \( \iff \) \( A \) must be false

Semantics of Propositional Modal Logic

For a particular frame \((W, R)\)

An interpretation \( I \) maps the propositional letters to subsets of \( W \)

\( w \models A \) means \( A \) is true in world \( w \)

\( w \models P \iff w \in I(P) \)
\( w \models A \land B \iff w \models A \) and \( w \models B \)
\( w \models \Box A \iff v \models A \) for all \( v \) such that \( R(w, v) \)
\( w \models \Diamond A \iff v \models A \) for some \( v \) such that \( R(w, v) \)
Truth and Validity in Modal Logic

For a particular frame \((W, R)\), and interpretation \(I\)

\[ w \models A \] means \( A \) is true in world \( w \)

\[ \models_{W,R,I} A \] means \( w \models A \) for all \( w \) in \( W \)

\[ \models_{W,R} A \] means \( w \models A \) for all \( w \) and all \( I \)

\[ \models A \] means \( \models_{W,R} A \) for all frames; \( A \) is universally valid

... but typically we constrain \( R \) to be, say, transitive

All tautologies are universally valid

A Hilbert-Style Proof System for \( K \)

Extend your favourite propositional proof system with

\[ \text{Dist} \quad \Box (A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B) \]

Inference Rule: Necessitation

\[
\frac{A}{\Box A}
\]

Treat \( \Diamond \) as a definition

\[ \Diamond A \overset{\text{def}}{=} \neg \Box \neg A \]
Start with pure modal logic, which is called $K$.

Add axioms to constrain the accessibility relation:

- **T**: $\square A \rightarrow A$  
  (reflexive) logic $T$
- **4**: $\square A \rightarrow \square \square A$  
  (transitive) logic $S4$
- **B**: $A \rightarrow \square \diamond A$  
  (symmetric) logic $S5$

And countless others!

We shall mainly look at $S4$.

---

### Extra Sequent Calculus Rules for $S4$

- **$\square$**: $\Gamma \Rightarrow \Delta$  
  $\Gamma \Rightarrow \Delta$, $\square A$  
  ($\Box l$) \hspace{1cm} $\Gamma \Rightarrow \Delta$, $\square \Gamma$  
  ($\Box r$)
- **$\diamond$**: $\Gamma \Rightarrow \Delta$  
  $\Gamma \Rightarrow \Delta$, $\diamond A$  
  ($\Diamond l$) \hspace{1cm} $\Gamma \Rightarrow \Delta$, $\diamond \Gamma$  
  ($\Diamond r$)

$\Gamma^* \overset{\text{def}}{=} \{ \Box B \mid \Box B \in \Gamma \}$ Erase non-$\Box$ assumptions

$\Delta^* \overset{\text{def}}{=} \{ \Diamond B \mid \Diamond B \in \Delta \}$ Erase non-$\Diamond$ goals!
A Proof of the Distribution Axiom

A ⇒ B, A, B, A ⇒ B
A → B, A ⇒ B
A → B, □A ⇒ B
□(A → B), □A ⇒ B
□(A → B), □A ⇒ □B

And thus □(A → B) → (□A → □B)

Must apply (□r) first!

Part of an Operator String Equivalence

□A ⇒ □A
□□A ⇒ □A
□□□A ⇒ □A
□□□□A ⇒ □A
□□□□□A ⇒ □□A

In fact, □□□□A ≃ □□A and also □□□A ≃ □A

The S4 operator strings are □ ◊ □ ◊ ◊ □ ◊□ ◊◊
Two Failed Proofs

\[ \begin{align*}
\Rightarrow & \; A \\
\Rightarrow & \; \Diamond A \\ & \; (\Diamond r) \\
\Rightarrow & \; \Box \Diamond A \\
& \; (\Box r)
\end{align*} \]

\[ \begin{align*}
B & \Rightarrow A \land B \\
\Rightarrow & \; \Diamond (A \land B) \\
& \; (\Diamond r) \\
\Rightarrow & \; \Box (A \land B) \\
& \; (\Diamond 1)
\end{align*} \]

Can extract a countermodel from the proof attempt
Simplifying the Sequent Calculus

7 connectives (or 9 for modal logic):

\[
\neg \land \lor \rightarrow \leftrightarrow \forall \exists (\square \Diamond)
\]

Left and right: so 14 rules (or 18) plus basic sequent, cut

Idea! Work in **Negation Normal Form**

Fewer connectives: \( \land \lor \forall \exists (\square \Diamond) \)

Sequents need **one side only**!

Simplified Calculus: Left-Only

\[
\frac{-A, A, \Gamma}{\Gamma} \quad \text{basic} \quad \frac{-A, \Gamma}{A, \Gamma, \Gamma} \quad \text{cut}
\]

\[
\frac{A, B, \Gamma}{A \land B, \Gamma} \quad (\land I) \quad \frac{A, \Gamma}{B, \Gamma} \quad (\lor I)
\]

\[
\frac{A[t/x], \Gamma}{\forall x A, \Gamma} \quad (\forall I) \quad \frac{A, \Gamma}{\exists x A, \Gamma} \quad (\exists I)
\]

Rule \( (\exists I) \) holds *provided* \( x \) is not free in the conclusion!
Left-Only Sequent Rules for $S4$

\[
\begin{align*}
\frac{A, \Gamma \Rightarrow}{\square A, \Gamma \Rightarrow} & \quad (\Box L) \\
\frac{A, \Gamma \Rightarrow}{\Diamond A, \Gamma \Rightarrow} & \quad (\Diamond L)
\end{align*}
\]

\[
\Gamma^* \overset{\text{def}}{=} \{ \Box B \mid \Box B \in \Gamma \}
\]

Erase non-$\Box$ assumptions

From 14 (or 18) rules to 4 (or 6)

Left-side only system uses **proof by contradiction**

Right-side only system is an exact dual

---

Proving $\forall x (P \rightarrow Q(x)) \Rightarrow P \rightarrow \forall y Q(y)$

Move the right-side formula to the left and convert to NNF:

$P \land \exists y \neg Q(y), \forall x (\neg P \lor Q(x)) \Rightarrow$

\[
\begin{align*}
\frac{P, \neg Q(y), \neg P \Rightarrow}{P, \neg Q(y), \neg P \lor Q(y) \Rightarrow} & \quad (\lor 1) \\
\frac{P, \neg Q(y), Q(y) \Rightarrow}{P, \neg Q(y), \forall x (\neg P \lor Q(x)) \Rightarrow} & \quad (\forall 1) \\
\frac{P, \neg Q(y), \exists y (\neg P \lor Q(x)) \Rightarrow}{P, \exists y \neg Q(y), \forall x (\neg P \lor Q(x)) \Rightarrow} & \quad (\exists 1) \\
\frac{P \land \exists y \neg Q(y), \forall x (\neg P \lor Q(x)) \Rightarrow}{P \land \exists y \neg Q(y), \forall x (\neg P \lor Q(x)) \Rightarrow} & \quad (\land 1)
\end{align*}
\]
Adding Unification

Rule $(\forall l)$ now inserts a new free variable:

$$
\frac{\Lambda[z/x], \Gamma \Rightarrow (\forall l)}{\forall x \Lambda, \Gamma \Rightarrow (\forall l)}
$$

Let unification instantiate any free variable

In $\neg \Lambda, B, \Gamma \Rightarrow$ try unifying $\Lambda$ with $B$ to make a basic sequent

Updating a variable affects entire proof tree

What about rule $(\exists l)$? Skolemize!

Skolemization from NNF

Don't pull quantifiers out! Skolemize

$[\forall y \exists z Q(y, z)] \land \exists x P(x)$ to $[\forall y Q(y, f(y))] \land P(a)$

It's better to push quantifiers in (called miniscoping)

Example: proving $\exists x \forall y [P(x) \rightarrow P(y)]$:

Negate; convert to NNF: $\forall x \exists y [P(x) \land \neg P(y)]$

Push in the $\exists y$: $\forall x [P(x) \land \exists y \neg P(y)]$

Push in the $\forall x$: $(\forall x P(x)) \land (\exists y \neg P(y))$

Skolemize: $\forall x P(x) \land \neg P(a)$
A Proof of $\exists x \forall y [P(x) \rightarrow P(y)]$

\[
\begin{align*}
y \mapsto f(z) \\
P(y), \neg P(f(y)), P(z), \neg P(f(z)) & \Rightarrow \text{(basic)} \\
P(y), \neg P(f(y)), P(z) \land \neg P(f(z)) & \Rightarrow \text{(\&I)} \\
P(y), \neg P(f(y)), \forall x [P(x) \land \neg P(f(x))] & \Rightarrow \text{(\&I)} \\
P(y) \land \neg P(f(y)), \forall x [P(x) \land \neg P(f(x))] & \Rightarrow \text{(\&I)} \\
\forall x [P(x) \land \neg P(f(x))] & \Rightarrow \text{(\forall I)}
\end{align*}
\]

Unification chooses the term for (\forall I)

A Failed Proof

Try to prove $\forall x [P(x) \lor Q(x)] \Rightarrow \forall x P(x) \lor \forall x Q(x)$

NNF: $\exists x \neg P(x) \land \exists x \neg Q(x), \forall x [P(x) \lor Q(x)] \Rightarrow$

Skolemize: $\neg P(a) \land \neg Q(b), \forall x [P(x) \lor Q(x)] \Rightarrow$

\[
\begin{align*}
y \mapsto a \\
\neg P(a), \neg Q(b), P(y) & \Rightarrow \text{(\forall I)} \\
\neg P(a), \neg Q(b), Q(y) & \Rightarrow \text{(\forall I)} \\
\neg P(a), \neg Q(b), P(y) \lor Q(y) & \Rightarrow \text{(\forall I)} \\
\neg P(a), \neg Q(b), \forall x [P(x) \lor Q(x)] & \Rightarrow \text{(\&I)} \\
\neg P(a) \land \neg Q(b), \forall x [P(x) \lor Q(x)] & \Rightarrow \text{(\&I)}
\end{align*}
\]

Lawrence C. Paulson University of Cambridge
prove((A,B),UnExp,Lits,FreeV,VarLim) :- !,
    and
    prove(A,[B|UnExp],Lits,FreeV,VarLim).
prove((A;B),UnExp,Lits,FreeV,VarLim) :- !,
    or
    prove(A,UnExp,Lits,FreeV,VarLim),
    prove(B,UnExp,Lits,FreeV,VarLim).
prove(all(X,Fml),UnExp,Lits,FreeV,VarLim) :- !,
    forall
    \+ length(FreeV,VarLim),
    copy_term((X,Fml,FreeV),(X1,Fml1,FreeV)),
    append(UnExp,[all(X,Fml)],UnExp1),
    prove(Fml1,UnExp1,Lits,[X1|FreeV],VarLim).
prove(Lit,[],Lits,_,_) :- literals; negation
    (Lit = -Neg; -Lit = Neg) ->
    (unify(Neg,L); prove(Lit,[],Lits,_,_)).
prove(Lit,[Next|UnExp],Lits,FreeV,VarLim) :- next formula
    prove(Next,UnExp,[Lit|Lits],FreeV,VarLim).